МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Кваліфікаційна наукова
праця на правах рукопису

БЕШЛЕЙ МИКОЛА ІВАНОВИЧ

УДК 621.391

ДИСЕРТАЦІЯ

Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів

05.12.02 – телекомунікаційні системи та мережі
(шифр і назва спеціальності)

05 «Технічні науки»
(галузь знань)

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____М.І. Бешлей

Подається на здобуття наукового ступеня
доктора технічних наук

Науковий консультант –
Климаш Михайло Миколайович,
д.т.н., професор

Ідентичність всіх примірників дисертації
ЗАСВІДЧУЮ:
В.о. вченого секретаря спеціалізованої
вченої ради **/Р.Л. Голяка/**

Львів – 2021

АНОТАЦІЯ

Бешлей М.І. Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі. – Національний університет «Львівська політехніка» Міністерства освіти і науки України, м. Львів, 2021.

Із розвитком бізнесу, різноманітності сервісів та вимог користувачів до якості обслуговування, інтенційно-орієнтовані мережі (Intent-based Network, IBN) виходять на перший план, як інструмент для інтелектуального управління гетерогенними мережами, який дає змогу абстрагуватися від деталей конфігурації і функціонування окремих елементів мережі та зосередитися на поведінці цілої мережі, як системи для надання сервісу відповідно до вимог та гарантування якості обслуговування на основі намірів користувачів. Основний принцип IBN полягає в перетворенні інформаційних бізнес-намірів користувачів до відповідних конфігурацій мережі для всіх пристроїв на основі мережної аналітики та машинного навчання. Саме тому, дослідження принципів функціонування таких мереж та розроблення методів та засобів їх впровадження є важливим завданням як для гравців телекомунікаційного ринку, так і для науковців.

Дисертаційна робота присвячена вирішенню актуальної науково-прикладної проблеми розроблення методології аналізу та синтезу складних гетерогенних інфокомунікаційних систем з метою створення нової програмно-конфігурованої інтенційно-орієнтованої мережі, яка постійно на основі мінливих вимог користувачів щодо якості надання сервісів та розгортання інфраструктури навчається, адаптується, автоматизується і захищається від потенційних кібератак шляхом використання нових методів розподілу ресурсів, інженерії трафіку, мережевої аналітики та існуючих алгоритмів машинного навчання.

У першому розділі **«Аналіз проблем управління якістю надання сервісів в сучасних інфокомунікаційних системах та перспективи розвитку інтенційно-орієнтованих мереж»** проведено аналіз сучасного стану проблеми управління якістю надання сервісів в інформаційно-комунікаційних мережах. Встановлено, що з розвитком інфокомунікаційних систем вимоги користувачів і їх поведінка змінилися. Центр уваги зміщується від підвищення продуктивності мережі до покращення якості сприйняття послуг. Зокрема, для кінцевих бізнес-користувачів все більш важливим стає адаптивне надання сервісу, постійний зв'язок та індивідуалізація обслуговування. Встановлено, що головна проблема традиційних інформаційно-комунікаційних систем є використання пропрієтарного обладнання, яке унеможливлює автоматизоване внесення змін щодо функціонування мережі напрямленої на мінливі потреби користувачів, без втручання адміністратора. Частковим вирішенням даної проблеми є перехід на програмно-конфігуровані мережі (Software-Defined Networking, SDN), які дають змогу реалізувати централізований, програмований рівень управління інфраструктурою та абстракцію рівня даних. Проте існуючі програмно-конфігуровані мережі характеризуються рядом недоліків, щодо переходу до повної автоматизації та проведення гнучкості управління ресурсами на основі мінливих бізнес вимог користувачів, вирішення яких можливе з використанням алгоритмів машинного навчання та нових методів управління мережею, що дасть змогу створити інтенційно-орієнтовані мережі нового покоління, які базуються на намірах користувачів.

У другому розділі **«Моделі побудови програмно-конфігурованих інтенційно-орієнтованих мереж з адаптивним управлінням якістю надання сервісів»** для вирішення проблеми синтезу інфокомунікаційної мережі, використано основні принципи і методи системного аналізу, згідно якого запропоновано концептуальну модель побудови гетерогенної програмно-конфігурованої інтенційно-орієнтованої мережі, яка дає змогу забезпечити ефективний розподіл і перерозподіл загальних ресурсів адаптуючись під

мінливі вимоги бізнес-користувачів щодо якості надання сервісів. Запропоновано використати комплексний показник якості обслуговування користувачів сформованого у вигляді оцінки QoE, як основного критерію для адаптивного управління перерозподілом ресурсів в умовах зміни значимості бізнес-процесів в контексті реалізації концепції IBN. Розвинуто математичну модель визначення суб'єктивного рівня задоволеності користувача за оцінкою QoE в залежності від зміни об'єктивних показників якості обслуговування QoS, що забезпечуються в IBN/SDN мережі, зокрема для відео та аудіо сервісів реального часу. Розроблено модель енергоефективної маршрутизації для інтенційно-орієнтованих мереж, що дала змогу підтримувати компроміс між бажаною якістю обслуговування користувачів, завантаженістю та енергоефективністю мережі. Запропоновано централізований моніторинг та управління мережевою структурою з допомогою удосконаленої логіки SDN контролера, що дало змогу на основі отриманої поточної статистики про стан мережі адаптивно приймати рішення щодо побудови оптимальної топології мережі за критеріями QoS/QoE та енергоспоживання. Удосконалено алгоритм вимірювання затримки передавання даних в програмно-конфігурованих мережах шляхом формування контролером пробних пакетів меншого розміру із різними пріоритетами, що дало можливість для низько пріоритетних потоків покращити точність моніторингу. Формалізовано модель адаптивного вибору підсистеми граничних та хмарних обчислень в IBN мережі.

У третьому розділі **«Методи, алгоритми і моделі адаптивного розподілу мережевих ресурсів та управління трафіком для синтезу корпоративних інтенційно-орієнтованих мереж»** розроблено метод адаптивного клієнт-орієнтованого управління якістю надання послуг для інтенційно-орієнтованих мереж. Новизна методу полягає в тому, що в умовах високого навантаження мережі для формування якості послуги враховується як об'єктивна оцінка часових мережевих характеристик, так і замовлені згідно намірів клієнтів суб'єктивні QoE оцінки, що дало змогу кінцевим користувачам сервісів

опосередковано впливати на функціональну конфігурацію мережі, а з використанням алгоритмів машинного навчання для централізованої системи моніторингу та управління мережею реагувати на несприятливі поєднання значень показників якості і попереджати ситуації, коли користувач незадоволений якістю отриманих сервісів для адаптивного прогнозування моменту переконфігурації мережі. Для дослідження ефективності запропонованого методу розроблено імітаційну модель інтенційно-орієнтованої мережі. Перевагою даної моделі є можливість досліджувати нові рішення для майбутньої концепції інтенційно-орієнтованих мереж шляхом інтеграції унікальних алгоритмів у ядро мережі. Встановлено, що запропонований метод адаптивного клієнт-орієнтованого управління якістю послуг дає виграш в середньому від 2-5 разів за критерієм кількості користувачів, які вимагають високої якості сприйняття послуги.

У четвертому розділі **«Інтелектуальна система моніторингу та аналізу трафіку для автоматизованого виявлення аномалії і запобігання атак в інтенційно-орієнтованих мережах»** удосконалено метод виявлення аномалій мережевого трафіку та атак для майбутніх інтенційно-орієнтованих інфокомунікаційних мереж, який відрізняється від відомих способом формування набору інформативних ознак, що формалізують нормальну та аномальну поведінку системи на основі оцінки параметра Херста. Розроблено інтелектуальну DPI (Deep Packet Inspection) систему моніторингу та аналізу трафіку, яка дала змогу виявити складні атаки різного роду, зокрема таких як SYN Flood, фрагментація HTTP, UDP Flood, DNS Flood, Non-Spoofed UDP Flood та шляхом автоматизованого блокування виявленого шкідливого трафіку зменшити загальний рівень втрат на 5% у порівнянні із існуючою комерційною системою SolarWinds DPI. Новизною розроблювальної DPI системи є те, що вона базується на гармонійному поєднанні переваг методів сигнатурного, статистичного та фрактального аналізу інформативних ознак щодо детектування інформаційних протоколів і ранжування прихованих властивостей аномального трафіку.

У п’ятому розділі **«Методологія адаптивного структурно-функціонального синтезу гетерогенної інтенційно-орієнтованої мережі»** розроблено методи розподілу частотно-часових ресурсів, балансування навантаження та формування структури рівня радіодоступу для забезпечення адаптивного надання сервісів. Новизна методів полягає у безпосередньому врахуванні просторово-часової локалізації абонентського навантаження та замовлених вимог бізнес-користувачів на основі аналізу їх QoE оцінок. Розроблено імітаційну модель процесу функціонування інтенційно-орієнтованої гетерогенної мережі мобільного зв’язку. На основі імітаційної моделі оцінено ефективність запропонованого методу інтенційно-орієнтованого управління частотно-часовими ресурсами та формування структури рівня радіодоступу. Зокрема використання, розроблених методів дало змогу для операторів мобільного зв’язку ефективніше на 25% використовувати наявні частотно-часові ресурси та зменшити на 8,7% енергоспоживання мережі рівня радіодоступу із гарантуванням замовленої якості обслуговування користувачів у порівнянні із відомими методами. Основною перевагою розробленої імітаційної моделі є використання системно-об’єктного підходу проектування функціональних блоків мережі мобільного зв’язку на основі відомих LTE стандартів, що дало змогу адекватно формалізувати опис системи як єдине ціле, надавши повну інформацію про структуру, функціонування і поводження окремих елементів системи. Запропоновано методологію синтезу гетерогенної інтенційно-орієнтованої мережі, згідно якої можна інтелектуально виділяти зв’язки між структурно-функціональними елементами мережі, які можуть не тільки автоматизовано перебудовуватись з різною продуктивністю, але й виникати заново, вишукуючи шляхи найбільш адекватного пристосування до мінливих вимог користувачів щодо адаптивного надання сервісів. Новизною методології є те, що вона базується на розроблених у роботі нових методах адаптивного управління якістю надання послуг, енергоефективністю, захисту, розподілу та наскрізної віртуалізації ресурсів мережі.

У шостому розділі **«Практична реалізація інтенційно-орієнтованої мережі корпоративного сегменту з використанням технології SDN та автоматизації запропонованих управлінських рішень»** розроблено прототипи інтенційно-орієнтованої мережі на базі мікроконтролерних платформ, апаратних SDN комутаторів ZODIAC FX/GX та віртуалізації мережевих функцій компонентів технології SDN, в межах яких реалізовано та оцінено ефективність запропонованих рішень щодо адаптивного клієнт-орієнтованого управління ресурсами та якістю обслуговування. Розроблено унікальну систему моніторингу якості функціонування реалізованих прототипів IBN мереж. Особливістю системи є використання розробленого методу наскрізного вимірювання затримки передавання даних з кінця в кінець для кожного компонента мережі шляхом додавання власної мітки часу до метаданих. Розроблено прототип мобільного та операторського додатку для адаптивного клієнт-орієнтованого надання послуг в гетерогенній мережі, що дає змогу отримувати замовлену якість обслуговування на основі розробленого засобу зворотного зв'язку між користувачем та оператором мережі. Розроблені та підтверджені в процесі функціонування моделі та методи реалізовані у вигляді самостійних програмних модулів, які можуть бути використанні в подальших практичних дослідженнях в області дослідження та оптимізації програмно-конфігурованих інтенційно-орієнтованих мереж.

У **висновках** дисертаційної роботи викладено основні результати і рекомендації, які випливають з проведених досліджень, представлено та охарактеризовано кількісні оцінки показників ефективності в процесі синтезу та реалізації інтенційно-орієнтованих мереж.

У **додатках** до дисертації долучено обрані початкові коди розробленого програмного забезпечення, акти впровадження результатів дисертаційної роботи, а також список наукових праць і апробацій автора за темою дисертації.

Ключові слова: інтенційно-орієнтована мережа, програмно-конфігурована мережа, якість обслуговування, розподіл ресурсів, якість сприйняття, віртуалізація, маршрутизація.

Список публікацій здобувача:

Наукові праці, у яких опубліковані основні результати дисертації

1. M. Beshley, *Development and testbed of software router for critical application*. Saarbrücken, Germany: LAP Lambert Academic Publishing, 2019. ISBN: 978-613-9-46367-1.

2. М. М. Климаш, Т. А. Максимюк, М. І. Бешлей, *Методи та моделі побудови гетерогенних мереж мобільного зв'язку 4G/5G.* Львів, Україна: Видавництво "Львівська політехніка", 2020. ISBN: 978-966-941-552-3.

3. I. Demydov, N. Baydoun, M. Beshley, M. Klymash, O. Panchenko, "Development of basic concept of ICT platforms deployment strategy for social media marketing considering tectonic theory*," EUREKA: Physics and Engineering*, vol. 0, no.1, pp. 18–33, Jan. 2020. (Scopus Q2).

4. S. Jun, K. Przystupa, M. Beshley, O. Kochan, H. Beshley, M. Klymash, J. Wang, D. Pieniak, "A Cost-Efficient Software Based Router and Traffic Generator for Simulation and Testing of IP Network," *Electronics*, vol. 9, no. 1, pp. 40-1–40-24, Jan. 2020. (Scopus/Web of Science Q1).

5. W. Song, M. Beshley, K. Przystupa, H. Beshley, O. Kochan, A. Pryslupskyi, D. Pieniak, J. Su, "A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection," *Sensors*, vol. 20, no. 6, p. 1637-1–1637-41, March 2020. (Scopus/Web of Science Q1).

6. M. Beshley, N. Kryvinska, M. Seliuchenko, H. Beshley, E. Shakshuki, A. Yasar, "End-to-End QoS "Smart Queue" Management Algorithms and Traffic Prioritization Mechanisms for Narrow-Band Internet of Things Services in 4G/5G Networks," *Sensors*, vol. 20, no.8, pp.2324-1–2324-30, Apr. 2020. (Scopus/Web of Science Q1).

7. S. Wenguang, V. Andrushchak, M. Kaidan, M. Beshley, O. Kochan, S. Jun, "Methodology for Calculating the Energy Consumption of Information Communication Systems," *Technical Electrodynamics*, no. 4, pp. 80–88, July 2020. (Scopus Q3).

8. H. Xu, K. Przystupa, C. Fang, O. Kochan, M. Beshley, A. Marciniak, “A combination strategy of feature selection based on an integrated optimization algorithm and weighted k-nearest neighbor to improve the performance of network intrusion detection,” *Electronics,* vol. 9, no. 8, pp. 1206-1–1206-22, July 2020. (Scopus/Web of Science Q1).

9. M. Beshley, P. Vesely, A. Prislupskiy, H. Beshley, M. Kyryk, V. Romanchuk, I. Kahalo, “Customer-Oriented Quality of Service Management Method for the Future Intent-Based Networking,” *Applied Sciences,* vol. 10, no. 22, pp. 8223-1–8223-38. Nov. 2020. (Scopus/Web of Science Q1).

10. K. Przystupa, M. Beshley, M. Kaidan, V. Andrushchak, I. Demydov, O. Kochan, D. Pieniak, “Methodology and Software Tool for Energy Consumption Evaluation and Optimization in Multilayer Transport Optical Networks,” *Energies*, vol. 13, no. 23, pp. 6370-1–6370-21. Dec. 2020. (Scopus/Web of Science Q1).

11. V. Romanchuk. M. Beshley, A. Prislupskiy, H. Beshley, O. Panchenko, “Method of multiservice infrastructure decomposition with network resource slicing for IoT,” *Internet of Things (IoT) and Engineering Applications* (Canada), vol. 3, no.1, pp. 22–23. May 2018.

12. M. Klymash, M. Beshley, “Perspective directions of development and research in the field of information and communication technologies,” *BA Magazine “Wissen im Markt”*, no. 3, pp. 31–37, 2019.

13. М.М. Климаш, М.В. Кайдан, М.І. Бешлей, А.В. Редька, “Оптимізація багатошарової структури транспортної мережі на основі технологій IP/MPLS/DWDM за допомогою методу діакоптики,” *Наукові записки Українського науково-дослідного інституту зв'язку*, № 3, с. 32–42, 2015.

14. М.І. Бешлей, В.В. Червенець, І.В. Демидов, В.І. Романчук, О.М. Панченко, “Розвиток методів передавання даних реального часу шляхом вдосконалення процесів пріоритезації потоків у маршрутизаторах,” *Системи озброєння і військова техніка: наук. журнал - Х: Харк. ун-т Повітр. Сил ім. І. Кожедуба*, 5(142), с. 114 –123, 2016.

15. М.М. Климаш, М.І. Бешлей, Ю.Д. Дещинський, О.М. Панченко, “Розробка методу балансування навантаження в SDN мережах на основі модифікованого протоколу STP,” *Комп’ютерні технології друкарства*, №2, с. 146–155, 2015.

16. I. Demydov, M. Klymash, M. Beshley, O. Shpur, “Features of the cloud services implementation in the national network segment of Ukraine,” *Information and telecommunication science. K.: NTUU «KPI»,* No.1, pp. 31–38, 2016.

17. М.М. Климаш, В.І. Романчук, О.М. Панченко, М.І. Бешлей, А.В. Поліщук, “Розроблення програмного маршрутизатора з автоматичним розгортанням віртуальних вузлів,” *Вісник Національного університету “Львівська політехніка”. Радіоелектроніка та телекомунікації,* № 885, с. 22 – 30, 2017.

18. Г.В. Бешлей, М.О. Селюченко, І.А Берневек, С.І. Пущак, М.І. Бешлей, “Алгоритм кластеризації, агрегації та класифікації M2M пристроїв в гетерогенній мережі 4G/5G,” *Вісник Національного університету “Львівська політехніка”. Радіоелектроніка та телекомунікації*, № 874, с. 95–102, 2017.

19. V. Romanchuk, M. Klymash, M. Beshley, O. Panchenko, A. Polishchuk, “Development of software-based router model with adaptive selection of algorithms for queues servicing,” *Technology audit and production reserves,* №3/2(41), pp. 46–55, 2018.

20. В.І Романчук, М.І. Бешлей, О.М. Панченко, А.В. Поліщук, “Метод узгодженого розв’язання завдань балансування різнопріоритетного навантаження між чергами мережевих пристроїв,” *Наукові записки Українського науково-дослідного інституту зв’язку*, №2(50), с. 48–57, 2018.

21. В.І. Романчук, М.І. Бешлей, А.М. Прислупський, Г.В. Бешлей, “Метод декомпозиції структури мережного пристрою з віртуалізацією ресурсів,” *Наукові записки Української академії друкарства*, №1(56), с. 31– 42. 2018.

22. М.В. Кайдан, М.І. Бешлей, Т.А. Максимюк, Б.М. Стрихалюк, Р.З. Матвіїв, “Теорія Кернера та фазові переходи для потоків у телекомунікаційних

мережах,” *Вісник Національного університету “Львівська політехніка”. Радіоелектроніка та телекомунікації*, № 909, с. 29–34, 2018.

23. І.О. Кагало, М.І. Бешлей, М.М. Климаш, О.М. Панченко, Г.В. Бешлей, “Адаптивне формування багаторівневої радіоструктури інтегрованих мереж LTE/Wi-Fi,” *Телекомунікаційні та інформаційні технології*, № 3(64), с. 24 –38, 2019.

24. М.М. Климаш, А.Б. Нажм, О.Л. Костів, І.В. Демидов, М.І. Бешлей, “Створення ефективних ІКТ-платформ електронного урядування інтерактивного типу: аналіз архітектури систем розповсюдження контенту,” *Наукові записки Українського науково-дослідного інституту зв'язку*, № 3, с. 31– 45, 2019.

Наукові праці, які засвідчують апробацію матеріалів дисертації

25. M. Klymash, M. Seliuchenko, M. Beshley and S. Redchuk, "Increasing wavelengths utilization efficiency in OTNoDWDM network based on local resource distribution method," *2015 Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*, Kharkiv, 2015, pp. 157–160.

26. M. Klymash, O. Lavriv, T. Maksymyuk and M. Beshley, "State of the art and further development of information and communication systems," *2016 International Conference Radio Electronics & Info Communications (UkrMiCo)*, Kiev, 2016, pp. 1– 6.

27. M. Beshley, V. Romanchuk, V. Chervenets and A. Masiuk, "Ensuring the quality of service flows in multiservice infrastructure based on network node virtualization," *2016 International Conference Radio Electronics & Info Communications (UkrMiCo)*, Kiev, 2016, pp. 1–3.

28. M. Seliuchenko, M. Beshley, O. Panchenko and M. Klymash, “Development of monitoring system for end-to-end packet delay measurement in software-defined networks,” *IEEE International Conference on Modern Problems of*

Radio Engineering, Telecommunications and Computer Science (TCSET'2016), Lviv, 2016, pp. 667–670.

29. A. Masiuk, M. Beshley, O. Lavriv and Y. Deschynskiy, "Common radio resource management model for heterogeneous cellular networks," *IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2016)*, Lviv, 2016, pp. 661–663.

30. O. Panchenko, A. Polishuk, M. Seliuchenko and M. Beshley, "Method for adaptive client oriented management of quality of service in integrated SDN/CLOUD networks," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 452–455.

31. M. Klymash, H. Beshley, M. Seliuchenko and M. Beshley, "Algorithm for clusterization, aggregation and prioritization of M2M devices in heterogeneous 4G/5G network," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 182–186.

32. M. Klymash, H. Beshley, O. Panchenko and M. Beshley, "Method for optimal use of 4G/5G heterogeneous network resourses under M2M/IoT traffic growth conditions," *2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Odessa, 2017, pp. 1–5.

33. V. Romanchuk, M. Beshley, O. Panchenko and P. Arthur, "Design of software router with a modular structure and automatic deployment at virtual nodes," *2017 2nd International Conference on Advanced Information and Communication Technologies (AICT)*, Lviv, 2017, pp. 295–298.

34. M. Klymash, V. Romanchuk, M. Beshley and P. Arthur, "Investigation and simulation of system for data flow processing in multiservice nodes using virtualization mechanisms," *2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON)*, Kiev, 2017, pp. 989–992.

35. M. Beshley, M. Seliuchenko, O. Panchenko and A. Polishuk, "Adaptive flow routing model in SDN," *2017 14th International Conference The Experience of*

Designing and Application of CAD Systems in Microelectronics (CADSM), Lviv, 2017, pp. 298–302.

36. H. Beshley, M. Kyryk, M. Beshley and O. Panchenko, "Method of information flows engineering and resource distribution in 4G/5G heterogeneous network for M2M service provisioning," *2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)*, Lviv, 2018, pp. 229–233.

37. V. Romanchuk, M. Beshley, A. Polishuk and M. Seliuchenko, "Method for processing multiservice traffic in network node based on adaptive management of buffer resource," *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2018, pp. 1118 –1122.

38. T. Maksymyuk, M. Beshley, M. Klymash, O. Petrenko and Y. Matsevityi, "Eavesdropping-resilient wireless communication system based on modified OFDM/QAM air interface," *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2018, pp. 1127–1130.

39. M. Beshley, M. Seliuchenko, O. Panchenko, O. Zyuzko and I. Kahalo, "Experimental performance analysis of software-defined network switch and controller," *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2018, pp. 282–286.

40. H. Beshley, M. Beshley, T. Maksymyuk and I. Strykhalyuk, "Method of centralized resource allocation in virtualized small cells network with IoT overlay," *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2018, pp. 1147–1151.

41. M. Klymash, I. Demydov, M. Beshley and O. Kostiv, "Structures assessment of data-centers telecommunication systems for metadata fixation," *2018*

International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odessa, 2018, pp. 1–7.

42. M. Beshley, S. Toliupa, V. Pashkevych and R. Kolodiy, “Development of software system for network traffic analysis and intrusion detection,” *International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Kiev, 2018, pp. 1–3.

43. M. Seliuchenko, M. Kyryk, M. Beshley, M. Zhovtonoh, “Automated Recovery of Server Applications for SDN-Based Internet of Things,” *International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Lviv, 2019, pp. 25–29.

44. I. Kahalo, H. Beshley, M.Beshley and O. Panchenko, “Enhancing QoS and energy efficiency of LTE/LTE-U/Wi-Fi integrated network based on adaptive technique for radio structure formation,” *2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON)*, Kiev, 2019, pp. 1167–1170.

45. M. Beshley, A. Pryslupskyi, O. Panchenko and H. Beshley, “SDN/Cloud solutions for intent-based networking,” *2019 IEEE 3nd International Conference on Advanced Information and Communication Technologies (AICT)*, Lviv, 2019, pp. 95–98.

46. A. Pryslupskyi, O. Panchenko, M. Beshley and M. Seliuchenko, "Improvement of multiprotocol label switching network performance using software-defined controller," *2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM)*, Polyana, Ukraine 2019, pp. 106 –109.

47. H. Beshley, M. Klymash, M. Beshley and I. Kahalo, "Improving the efficiency of LTE spectral resources use by introducing the new of M2M/IoT multi-service gateway," *2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM)*, Polyana, Ukraine, 2019, pp.114 –117.

48. M. Beshley, A. Pryslupskyi, O. Panchenko and M. Seliuchenko, "Dynamic switch migration method based on QoE-aware priority marking for intent-based networking," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2020, pp. 864 –868.

49. Z. Cheng, M. Beshley, H. Beshley, O. Kochan and O. Urikova, "Development of deep packet inspection system for network traffic analysis and intrusion detection," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2020, pp. 877–881.

50. Z. Hu, M. Beshley, V. Vitalii, S. Jun and T. Volodymyr, "Modified EIRGP routing protocol for backbone infrastructure of wireless multimedia sensor networks," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2020, pp. 894–899.

51. M. Beshley, M. Klymash, M. Hamal, Y. Shkoropad and A. Branytskyy, "Method for Estimating service delay in edge and cloud computing architecture," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2020, pp. 915–919.

52. М.О. Селюченко, Г.В. Бешлей, А.Р. Масюк, М.І. Бешлей, “Багаторівневе управління ресурсами в гетерогенній мульти-операторській мережі,” *1st International Conference "Advanced information and communication technologies"(AICT’2015),* Lviv, 2015, pp. 125–128.

53. М.М. Климаш, В.І. Романчук, М.І. Бешлей, “Розроблення макету мультисервісної мережі на базі програмно-апаратної платформи для забезпечення навчально-наукового процесу кафедри телекомунікацій,” *1st International Conference "Advanced information and communication technologies"(AICT’2015)*, Lviv, 2015, pp. 175–178.

54. М.М. Климаш, В.І. Романчук, М.І. Бешлей, А.О. Лунтовський, “Дослідження ефективності використання ресурсів навчально-наукового центру паралельних обчислень,” *Міжнародна науково-технічна конференція (Сучасні інформаційно-телекомунікаційні технології)*, м. Київ, 2015, с. 61–63.

55. М.І. Бешлей, В.В. Червенець, В.І. Романчук, А.В. Поліщук, “Модель віртуального маршрутизатора з статичною та динамічною реконфігурацією ресурсів,” *Міжнародна науковотехнічна конференція «Проблемивтелекомунікаці» ПТ-2016: збірник матеріалів конференції* , м. Київ, 2016р., с. 140 –142.

56. М.І. Бешлей, М.О. Селюченко, П.О. Гуськов, А.Р. Масюк, “Підвищення ефективності роботи гетерогенних мереж методом динамічного перерозподілу ресурсів між різними безпроводовими технологіями,” *Міжнародна науково-технічна конференція «Сучасні інформаційно-телекомунікаційні технології»: матеріали науково-технічної конференції*, м. Київ, 2015 р., с. 49–50.

57. М.І. Бешлей, М.М. Климаш, А.Р. Масюк, “Розробка і дослідження імітаційної моделі безпровідної гетерогенної мережі,” *Міжнародна науково-технічна конференція «Проблеми телекомунікацій» ПТ-2016: збірник матеріалів конференції*, м. Київ, 2016 р., с. 70–72.

58. М.І. Бешлей, О.М. Панченко, І.В. Демидов, М.О Селюченко, “Метод динамічного управління якістю послуг в інтегрованій SDN/CLOUD мережі,” *Фізико-технологічні проблеми, обробки та зберігання інформації в інфокомунікаційних системах: матеріали V Міжнародної науково-практичної конференції*, м. Чернівці, 2016 р., с. 74 –75.

59. М.М. Климаш, А.Р. Масюк, Г.В. Бешлей, М.І. Бешлей, “Концепція програмно конфігурованої гетерогенної мережі мобільного зв'язку на основі технологій SDN/NFV та SDR,” *Фізико-технологічні проблеми , обробки та зберігання інформації в інфокомунікаційних системах: матеріали V Міжнародної науково-практичної конференції,* м. Чернівці, 2016 р., с. 35–36.

60. М.І. Бешлей, М.М. Климаш, О.М. Панченко, Г.В. Бешлей, “Розроблення системи моніторингу та аналізу трафіку інформаційно телекомунікаційної мережі для виявлення аномалії і запобігання атак,” *І міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно телекомунікаційних систем”(PCSITS)*, м. Київ, 2018р.,с.201– 203.

ABSTRACT

Beshley M.I. Synthesis and implementation of intent-based infocommunication networks for adaptive service provision. – Qualification research paper as a manuscript.

A thesis submitted in fulfilment of the Doctor of Engineering Science degree in technical sciences on specialty 05.12.02 – telecommunication systems and networks. – Lviv Polytechnic National University, Ministry of Education and Science of Ukraine.

With the development of business, a variety of services and user requirements for service quality, Intent-based Networks (IBN) come to the fore as a tool for intelligent management of heterogeneous networks, which allows to abstract from the details of configuration and operation of individual network elements and focus on the behavior of the entire network as a system for providing services in accordance with the requirements and guaranteeing the quality of service based on user intentions. The basic principle of IBN is to transform users' informational business intentions into appropriate network configurations for all devices based on network analytics and machine learning. That is why the study of the principles of operation of such networks and the development of methods and means of their implementation is an important task for both players in the telecommunications market and for scientists.

The thesis is devoted to solving the actual scientific problem of developing the methodology of analysis and synthesis of the complex heterogeneous infocommunication systems in order to develop a new intent-based software-defined

network, which is constantly learning, adapting, automating and protecting against potential cyber-attacks based on changing user requirements regarding the quality of service and infrastructure deployment by using the new methods of resource allocation, traffic engineering, network analytics and machine learning algorithms.

The first chapter **«Analysis of problems of quality management of services in modern infocommunication systems and prospects for the development of intent-based networks»** analyzes the current state of the problem of quality management of services in information and communication networks. It is established that with the development of infocommunication systems, user requirements and their behavior have changed. The focus is shifting from improving network performance to improving the quality of experience. In particular, adaptive service delivery, constant communication, and individualization of service are becoming increasingly important for end business users. It is established that the main problem of traditional information and communication systems is the use of proprietary equipment, which makes it impossible to automatically make changes to the operation of the network aimed at changing user needs, without the intervention of the administrator. A partial solution to this problem is the transition to software-defined networks (Software-Defined Networking, SDN), which allow the implementation of a centralized, programmable level of infrastructure management and data level abstraction. However, existing software-configured networks are characterized by a number of shortcomings in the transition to full automation and flexibility of resource management based on changing business requirements of users, which can be solved using machine learning algorithms and new network management methods, which will createintent-based network generations based on user intentions.

In the second chapter **«Models of designing intent-based software-defined network with adaptive quality management of service provision»** to solve the problem of synthesis of the infocommunication network, the basic principles and methods of system analysis are used, according to which a conceptual model is

proposed for efficient allocation and redistribution of common resources by adapting to changing requirements of business users regarding the quality of service provision. It is proposed to use a comprehensive indicator of customer service quality in the form of QoE assessment, as the main criterion for adaptive management of resource redistribution in terms of changing importance of business processes in the context of the IBN concept. A mathematical model has been developed for determining the subjective level of user satisfaction according to QoE depending on the change in objective indicators of quality of service provided in the IBN/SDN network, in particular for real-time video and audio services. An energy-efficient routing model has been developed for intent-based networks, which has made it possible to maintain a compromise between the desired quality of customer service, congestion, and energy efficiency of the network. Centralized monitoring and management of the network structure using the advanced logic of the SDN controller is proposed, which allowed based on the current statistics on the state of the network to make adaptive decisions on building the optimal network topology according to QoS/QoE and energy consumption. The algorithm for measuring data transmission delay in software-defined networks has been improved by the controller forming smaller test packets with different priorities, which made it possible to improve the accuracy of monitoring for low-priority flows. The model of adaptive choice of the subsystem of edge and cloud computing in the IBN network has been formalized.

In the third chapter **«Methods, algorithms and models of adaptive allocation of network resources and traffic management for synthesis of corporate intent-based networks»** a method of adaptive customer-oriented quality management of services for intent-based networks has been developed. The novelty of the method is that in conditions of high network load for the formation of service quality the method takes into account both the objective assessment of time network characteristics and the required subjective QoE estimates according to customer intentions, which allowed end-users to indirectly influence the functional configuration of the network and using machine learning algorithms to execute a

centralized network monitoring and management system to respond to adverse combinations of values of quality indicators and prevent situations when the user is dissatisfied with the quality of services for adaptive prediction of the moment of network reconfiguration. To study the effectiveness of the proposed method, a simulation model of an intent-based network was developed. The advantage of this model is the ability to explore new solutions for the future concept of intent-based networks by integrating unique algorithms into the network core. It is established that the proposed method of adaptive customer-oriented quality management of services gives an average of 2-5 times gain according to the criterion of the number of users who require a high level of QoE.

In the fourth chapter **«Intelligent traffic monitoring and analysis system for automated detection of anomalies and prevention of attacks in intent-based networks»** the method of detecting anomalies of network traffic and attacks for future intent-oriented info-communication networks has been improved. The method differs from known methods by the way of forming the set of informational characteristics the formalize the normal and anomalous behavior of the system based on the evaluation of the Hurst parameter. Moreover, an intelligent DPI (Deep Packet Inspection) system for monitoring and analyzing traffic has been developed. This system allows the detection of complex attacks of various kinds, including SYN Flood, HTTP fragmentation, UDP Flood, DNS Flood, Non-Spoofed UDP Flood. In addition, the system, through automatic blocking of the detected malicious traffic allows reducing the overall level of losses by 5% compared to the existing commercial SolarWinds DPI system. The novelty of the developed DPI system is that it is based on the combination of the advantages of methods of signature, statistical and fractal analysis of informative features for detecting information protocols and ranking the hidden properties of anomalous traffic.

In the fifth chapter **«Methodology of adaptive structural-functional synthesis of heterogeneous intent-based network»** the methods of distribution of time-frequency resources, load balancing and formation of the structure of the radio access level for maintenance of adaptive rendering of services have been developed. The

novelty of the methods lies in the direct consideration of the spatio-temporal localization of a load of subscribers and the requirements of business users based on the analysis of their QoE estimates. A simulation model of the process of functioning of an intent-based heterogeneous mobile communication network has been developed. Based on the simulation model, the effectiveness of the proposed intent-based management method of time-frequency resources and the formation of the structure of the radio access level is evaluated. In particular, the use of the developed methods allowed mobile operators to use the available time-frequency resources more efficiently by 25% and reduce the energy consumption of the radio access level by 8.7%, guaranteeing the required quality of customer service compared to known methods. The main advantage of the developed simulation model is the use of a system and object approach in the design of functional units of the mobile network based on known LTE standards, which allowed to adequately formalize the description of the system as a whole, providing complete information about the structure, operation and behavior of individual system elements. A methodology for the synthesis of a heterogeneous intent-based network is proposed, according to which it is possible to intellectually distinguish connections between structural and functional elements of the network, which can not only be automatically rebuilt with different performance but also re-emerge, finding ways to best adapt to changing user requirements for the adaptive provision of services. The novelty of the methodology is that it is based on the new methods of adaptive management of service quality, energy efficiency, protection, distribution and end-to-end virtualization of network resources.

In the sixth chapter **«Practical implementation of an intent-based network of the corporate segment using SDN technology and automation of proposed management solutions»** the prototypes of an intent-oriented network based on microcontroller platforms have been developed, in particular using hardware SDN switches ZODIAC FX/GX and virtualization of the components of an SDN technology. Using the developed prototypes the effectiveness of the proposed

solutions for adaptive customer-oriented management of resources and quality of service has been evaluated. A unique system for monitoring the quality of operation of the implemented prototypes of IBN networks has been developed. A special feature of the system is the use of the developed method of end-to-end data transmission measurement for each network component by adding its own timestamp to the metadata. A prototype of a mobile and operator application has been developed for the adaptive customer-oriented provision of services in a heterogeneous network, which allows receiving the required quality of service on the basis of the developed means of feedback between the user and the network operator. The developed models and methods are implemented in the form of independent software modules that can be used in further practical research in the field of research and optimization of intent-based software-defined networks.

In the **conclusions** of the dissertation, the main results and recommendations that follow from the research are presented, quantitative assessments of efficiency indicators in the process of synthesis and implementation of intent-based networks are presented and characterized.

The **appendices** to the dissertation include selected source codes of the developed software, acts of implementation of the results of the dissertation, as well as a list of scientific works and approbations of the author on the topic of the dissertation.

Key words: intent-based networking, software-defined networking, quality of service, resource allocation, quality of experience, virtualization, routing.

The list of author's publications:

Proceedings where basic scientific results of thesis were published

1. M. Beshley, *Development and testbed of software router for critical application*. Saarbrücken, Germany: LAP Lambert Academic Publishing, 2019. ISBN: 978-613-9-46367-1.

2. M.M. Klymash, T.A. Maksymyuk, M.I. Beshley, *Methods and models of the 4G/5G heterogeneous networks desing*. Lviv, Ukraine: Lviv Polytechnic Publishing House, 2020. ISBN: 978-966-941-552-3.

3. I. Demydov, N. Baydoun, M. Beshley, M. Klymash, O. Panchenko, "Development of basic concept of ICT platforms deployment strategy for social media marketing considering tectonic theory*," EUREKA: Physics and Engineering*, vol. 0, no.1, pp. 18–33, Jan. 2020. (Scopus Q2).

4. S. Jun, K. Przystupa, M. Beshley, O. Kochan, H. Beshley, M. Klymash, J. Wang, D. Pieniak, "A Cost-Efficient Software Based Router and Traffic Generator for Simulation and Testing of IP Network," *Electronics*, vol. 9, no. 1, pp. 40-1–40-24, Jan. 2020. (Scopus/Web of Science Q1).

5. W. Song, M. Beshley, K. Przystupa, H. Beshley, O. Kochan, A. Pryslupskyi, D. Pieniak, J. Su, "A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection," *Sensors*, vol. 20, no. 6, p. 1637-1–1637-41, March 2020. (Scopus/Web of Science Q1).

6. M. Beshley, N. Kryvinska, M. Seliuchenko, H. Beshley, E. Shakshuki, A. Yasar, "End-to-End QoS "Smart Queue" Management Algorithms and Traffic Prioritization Mechanisms for Narrow-Band Internet of Things Services in 4G/5G Networks," *Sensors*, vol. 20, no.8, pp.2324-1–2324-30, Apr. 2020. (Scopus/Web of Science Q1).

7. S. Wenguang, V. Andrushchak, M. Kaidan, M. Beshley, O. Kochan, S. Jun, "Methodology for Calculating the Energy Consumption of Information Communication Systems," *Technical Electrodynamics*, no. 4, pp. 80–88, July 2020. (Scopus Q3).

8. H. Xu, K. Przystupa, C. Fang, O. Kochan, M. Beshley, A. Marciniak, "A combination strategy of feature selection based on an integrated optimization algorithm and weighted k-nearest neighbor to improve the performance of network intrusion detection," *Electronics*, vol. 9, no. 8, pp. 1206-1–1206-22, July 2020. (Scopus/Web of Science Q1).

9. M. Beshley, P. Vesely, A. Prislupskiy, H. Beshley, M. Kyryk, V. Romanchuk, I. Kahalo, “Customer-Oriented Quality of Service Management Method for the Future Intent-Based Networking,” *Applied Sciences,* vol. 10, no. 22, pp. 8223-1–8223-38. Nov. 2020. (Scopus/Web of Science Q1).

10. K. Przystupa, M. Beshley, M. Kaidan, V. Andrushchak, I. Demydov, O. Kochan, D. Pieniak, “Methodology and Software Tool for Energy Consumption Evaluation and Optimization in Multilayer Transport Optical Networks,” *Energies*, vol. 13, no. 23, pp. 6370-1–6370-21. Dec. 2020. (Scopus/Web of Science Q1).

11. V. Romanchuk. M. Beshley, A. Prislupskiy, H. Beshley, O. Panchenko, “Method of multiservice infrastructure decomposition with network resource slicing for IoT,” *Internet of Things (IoT) and Engineering Applications* (Canada), vol. 3, no.1, pp. 22–23. May 2018.

12. M. Klymash, M. Beshley, “Perspective directions of development and research in the field of information and communication technologies,” *BA Magazine “Wissen im Markt”*, no. 3, pp. 31–37, 2019.

13. M.M. Klymash, M.V. Kaidan, M.I. Beshley, A.V. Redka, “Optimization multilayer structure of transport network based on technology IP/MPLS/DWDM using the diakoptics method,” *Scientific notes of Ukrainian Research Institute of communications*, № 3, pp. 32–42, 2015.

14. M.I. Beshley, V.V. Chervenets, I.V. Demydov, V.I. Romanchuk, O.M. Panchenko, “Development of real-time data transmission methods by improving streaming prioritization processes in routers,” *Systems of Arms and Military Equipment: Sciences. magazine - Kharkiv: Khar. Univ. Air. Forces named after Ivan Kozhedub,* 5(142), pp. 114-123, 2016

15. M.M Klymash, M.I Beshley, Yu.D. Deshchinsky, O.M Panchenko, “Development of a method of load balancing in SDN networks based on a modified STP protocol,” *Computer printing technologies*, № 2, pp. 146–155, 2015.

16. I. Demydov, M. Klymash, M. Beshley, O. Shpur, “Features of the cloud services implementation in the national network segment of Ukraine,” *Information and telecommunication science. K.: NTUU «KPI»*, No.1, pp. 31–38, 2016.

17. M.M. Klymash, VI Romanchuk, O. M. Panchenko, M.I. Beshley, AV Polischuk, “Development of software router with automatic deployment of virtual nodes,” *Herald of Lviv Polytechnic National University, Series of Radioelectronics and Telecommunications*, № 885, pp. 22–30, 2017.

18. H.V. Beshley, M.O. Seliuchenko, I.A. Bernevek, S.I. Pushchak, M.I. Beshley, “Algorithm for clustering, aggregation and classification of M2M devices in a heterogeneous 4G/5G network,” *Herald of Lviv Polytechnic National University, Series of Radioelectronics and Telecommunications*, № 874, pp. 95–102, 2017.

19. V. Romanchuk, M. Klymash, M. Beshley, O. Panchenko, A. Polishchuk, “Development of software-based router model with adaptive selection of algorithms for queues servicing,” *Technology audit and production reserves*, №3/2(41), pp. 46–55, 2018.

20. V.I. Romanchuk, M.I. Beshey, O.M. Panchenko, A.V. Polishchuk, “Method of coordinated solving of balancing tasks of different priority load balancing between queues of network devices,” *Scientific notes of the UNDIZ*, №2(50), pp. 48–57, 2018.

21. V.I. Romanchuk, M.I. Beshey, A.M. Pryslupskiy, H.V. Beshley, “ Method of decomposing the structure of a network device with virtualization of resources,” *Sientific notes of Ukrainian Printing Academy*, №1(56), pp. 31– 42. 2018.

22. M.V. Kaidan, M.I. Beshley, T.A. Maksymyuk, B.M. Strykhalyuk, P.3. Matviyiv, “Kerner's theory and phase transitions for flows in telecommunication networks,” *Herald of Lviv Polytechnic National University, Series of Radioelectronics and Telecommunications*, № 909, pp. 29–34, 2018.

23. I.O. Kahalo, M.I. Beshley, M.M. Klymash, O.M. Panchenko, H.V. Beshley, “Adaptive Formation of the Multilevel Radio Structure of LTE/Wi-Fi Integrated Networks,” *Telecommunication and information technologies* № 3(64), pp.24–38, 2019.

24. M.M. Klymash, A. N. Baydoun, O.L. Kostiv, I.V. Demydov, M.I. Beshley, “Creating effective ICT platforms for interactive e-government: an analysis of the content distribution systems architecture,” *Scientific notes of Ukrainian Research Institute of communications*, № 3, pp. 31– 45, 2019.

Proceedings that certify an approvement of thesis materials

25. M. Klymash, M. Seliuchenko, M. Beshley and S. Redchuk, "Increasing wavelengths utilization efficiency in OTNoDWDM network based on local resource distribution method," *2015 Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*, Kharkiv, 2015, pp. 157–160.

26. M. Klymash, O. Lavriv, T. Maksymyuk and M. Beshley, "State of the art and further development of information and communication systems," *2016 International Conference Radio Electronics & Info Communications (UkrMiCo)*, Kiev, 2016, pp. 1– 6.

27. M. Beshley, V. Romanchuk, V. Chervenets and A. Masiuk, "Ensuring the quality of service flows in multiservice infrastructure based on network node virtualization," *2016 International Conference Radio Electronics & Info Communications (UkrMiCo)*, Kiev, 2016, pp. 1–3.

28. M. Seliuchenko, M. Beshley, O. Panchenko and M. Klymash, “Development of monitoring system for end-to-end packet delay measurement in software-defined networks,” *IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET’2016)*, Lviv, 2016, pp. 667–670.

29. A. Masiuk, M. Beshley, O. Lavriv and Y. Deschynskiy, “Common radio resource management model for heterogeneous cellular networks,” *IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET’2016)*, Lviv, 2016, pp. 661–663.

30. O. Panchenko, A. Polishuk, M. Seliuchenko and M. Beshley, "Method for adaptive client oriented management of quality of service in integrated SDN/CLOUD networks," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 452–455.

31. M. Klymash, H. Beshley, M. Seliuchenko and M. Beshley, "Algorithm for clusterization, aggregation and prioritization of M2M devices in heterogeneous 4G/5G network," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 182–186.

32. M. Klymash, H. Beshley, O. Panchenko and M. Beshley, "Method for optimal use of 4G/5G heterogeneous network resourses under M2M/IoT traffic growth conditions," *2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Odessa, 2017, pp. 1–5.

33. V. Romanchuk, M. Beshley, O. Panchenko and P. Arthur, "Design of software router with a modular structure and automatic deployment at virtual nodes," *2017 2nd International Conference on Advanced Information and Communication Technologies (AICT)*, Lviv, 2017, pp. 295–298.

34. M. Klymash, V. Romanchuk, M. Beshley and P. Arthur, "Investigation and simulation of system for data flow processing in multiservice nodes using virtualization mechanisms," *2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON)*, Kiev, 2017, pp. 989–992.

35. M. Beshley, M. Seliuchenko, O. Panchenko and A. Polishuk, "Adaptive flow routing model in SDN," *2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)*, Lviv, 2017, pp. 298–302.

36. H. Beshley, M. Kyryk, M. Beshley and O. Panchenko, "Method of information flows engineering and resource distribution in 4G/5G heterogeneous network for M2M service provisioning," *2018 IEEE 4th International Symposium on*

Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), Lviv, 2018, pp. 229–233.

37. V. Romanchuk, M. Beshley, A. Polishuk and M. Seliuchenko, "Method for processing multiservice traffic in network node based on adaptive management of buffer resource," *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2018, pp. 1118 –1122.

38. T. Maksymyuk, M. Beshley, M. Klymash, O. Petrenko and Y. Matsevityi, "Eavesdropping-resilient wireless communication system based on modified OFDM/QAM air interface," *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2018, pp. 1127–1130.

39. M. Beshley, M. Seliuchenko, O. Panchenko, O. Zyuzko and I. Kahalo, "Experimental performance analysis of software-defined network switch and controller," *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2018, pp. 282–286.

40. H. Beshley, M. Beshley, T. Maksymyuk and I. Strykhalyuk, "Method of centralized resource allocation in virtualized small cells network with IoT overlay," *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET),* Lviv-Slavske, 2018, pp. 1147–1151.

41. M. Klymash, I. Demydov, M. Beshley and O. Kostiv, "Structures assessment of data-centers telecommunication systems for metadata fixation," *2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Odessa, 2018, pp. 1–7.

42. M. Beshley, S. Toliupa, V. Pashkevych and R. Kolodiy, “Development of software system for network traffic analysis and intrusion detection,” *International*

Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Kiev, 2018, pp. 1–3.

43. M. Seliuchenko, M. Kyryk, M. Beshley, M. Zhovtonoh, “Automated Recovery of Server Applications for SDN-Based Internet of Things,” *International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Lviv, 2019, pp. 25–29.

44. I. Kahalo, H. Beshley, M.Beshley and O. Panchenko, “Enhancing QoS and energy efficiency of LTE/LTE-U/Wi-Fi integrated network based on adaptive technique for radio structure formation,” *2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON)*, Kiev, 2019, pp. 1167–1170.

45. M. Beshley, A. Pryslupskyi, O. Panchenko and H. Beshley, “SDN/Cloud solutions for intent-based networking,” *2019 IEEE 3nd International Conference on Advanced Information and Communication Technologies (AICT)*, Lviv, 2019, pp. 95–98.

46. A. Pryslupskyi, O. Panchenko, M. Beshley and M. Seliuchenko, "Improvement of multiprotocol label switching network performance using software-defined controller," *2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM)*, Polyana, Ukraine 2019, pp. 106 –109.

47. H. Beshley, M. Klymash, M. Beshley and I. Kahalo, "Improving the efficiency of LTE spectral resources use by introducing the new of M2M/IoT multi-service gateway," *2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM)*, Polyana, Ukraine, 2019, pp.114 –117.

48. M. Beshley, A. Pryslupskyi, O. Panchenko and M. Seliuchenko, "Dynamic switch migration method based on QoE-aware priority marking for intent-based networking," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2020, pp. 864 –868.

49. Z. Cheng, M. Beshley, H. Beshley, O. Kochan and O. Urikova, "Development of deep packet inspection system for network traffic analysis and intrusion detection," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2020, pp. 877–881.

50. Z. Hu, M. Beshley, V. Vitalii, S. Jun and T. Volodymyr, "Modified EIRGP routing protocol for backbone infrastructure of wireless multimedia sensor networks," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2020, pp. 894–899.

51. M. Beshley, M. Klymash, M. Hamal, Y. Shkoropad and A. Branytskyy, "Method for Estimating service delay in edge and cloud computing architecture," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2020, pp. 915–919.

52. M.O. Seliuchenko, H.V. Beshley, A.R. Масюк, M.I. Beshley, “Multilevel resource management in a heterogeneous multi-operator network,” *1st international conference "Advanced information and communication technologies"(AICT’2015),* Lviv, 2015, pp. 125–128.

53. M.M. Klymash, V.I. Romanchuk, M.I. Beshley, “ Development of the layout of the multiservice network based on the software and hardware platform for providing the educational and scientific process of the telecommunication department,” *1st international conference "Advanced information and communication technologies"(AICT’2015)*, Lviv, 2015, pp. 175–178.

54. M.M. Klymash, V.I. Romanchuk, M.I. Beshley, A.O. Luntovsky, “Research of the efficiency of using resources of the educational and scientific center of parallel computing,” *International scientific and technical conference (Modern information and telecommunication technologies)*, Kyiv, 2015, pp. 61–63.

55. M M.I. Beshley, V.V. Chervenets, V.I. Romanchuk, A.V. Polishchuk, “Model of virtual router with static and dynamic reconfiguration of resources,” *X International scientific and technical conference "Problems of telecommunication» PT-2016: collection of conference materials*, Kyiv, 2016, pp. 140–142.

56. M.I. Beshley, M.O. Seliuchenko, P.O. Huskov, A.P. Masyuk, “Improving the efficiency of heterogeneous networks by the method of dynamic redistribution of resources between different wireless technologies,” *International scientific and technical conference "Modern information and telecommunication technologies": materials of the scientific and technical conference*, Kyiv, 2015, pp. 49–50.

57. M.I. Beshley, M.M. Klymash, A.R. Masyuk, “Development and research of simulation model of wireless heterogeneous network,” *X International scientific and technical conference "Problems of telecommunications" PT-2016: collection of conference materials*, Kyiv, 2016, pp. 70–72.

58. M.I. Beshley, O.M. Panchenko, I.V Demydov, M.O Seliuchenko, “Dynamic service quality management method in an integrated SDN/CLOUD network,” *V international scientific conference «Physical and technological problems of transfer, processing and storage information in infocommunication systems»*, Chernivtsi, 2016, pp. 74–75.

59. M.M. Klymash, A.R. Masyuk, H.V. Beshley, M.I. Beshley, “The concept of software-defined heterogeneous mobile network based on SDN/NFV and SDR technologies,” *V International scientific conference «Physical and technological problems of transfer, processing and storage information in infocommunication systems»*, Chernivtsi, 2016, pp. 35–36.

60. M.I. Beshley, M.M. Klymash, O.M. Panchenko, H.V. Beshley, “Development of monitoring and traffic analysis system of information telecommunication network for anomaly detection and attack prevention,” *I International scientific and practical conference "Problems of cybersecurity of information and telecommunication systems". (PCSITS)*, Kiev, 2018, pp. 201-203.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

IoT – Internet of Things, Інтернет речей.

LAN – Local Area Network, локальна мережа.

WAN – Wide Area Networ, глобальна мережа.

ACL – Access Control List, список контролю доступу..

VLAN – Virtual Local Area Network, віртуальна локальна комп'ютерна мережа

QoS – Quality of Service, якість обслуговування.

SDN – Software-Defined Networking, програмно-конфігурована мережа.

API – Application Programming Interface, прикладний програмний інтерфейс.

LTE – Long Term Evolution, довготерміновий розвиток.

NFV – Network Functions Virtualization, віртуалізація мережевих функцій.

EC – Edge Computing, граничне обчислення.

RAT – Radio Access Technology, технологія радіо доступу.

MVNO – Mobile Virtual Network Operator, віртуальний оператор стільникового зв'язку.

PRB – Physical resource block, блок фізичних ресурсів.

IBN – Intent-Based Networking, інтенційно-орієнтована мережа.

NB-IoT – Narrow Band Internet of Things, вузькосмуговий Інтернет речей.

UE – User Equipment, обладнання користувача.

QoE – Quality of Experience, якість сприйняття, ступінь задоволеності користувача.

ToS – Type of Service, тип обслуговування.

DMCQR – Deterministic Multiconstrained Centralized QoS Routing, централізована детермінована багатокритеріальна QoS маршрутизація.

IDS – Intrusion Detection System, система виявлення вторгнень.

IPS – Intrusion Prevention System, система запобігання вторгнень.

SLA – Service Level Agreements, угоди про рівень обслуговування.

ELA – Experience Level Agreements, угоди про рівень очікуваної якості сервісу.

SDR – Software Defined Radio, програмно-конфігурована радіосистема.

IBSDN – Intent-Based Software-Defined Network, програмно-конфігурована інтенційно-орієнтована мережа.

SGW – Serving Gateway, обслуговуючий шлюз мережі LTE.

RTT – Round Trip Time, це час, потрібний для пересилання сигналу від передавача до отримувача.

CC – Cloud Computing, хмарні обчислення.

EC – Edge Computing, крайові обчислення.

JSON – JavaScript Object Notation, це текстовий формат обміну даними між комп'ютерами.

CLI – Command-line Interface, інтерфейс командного рядка.

ARP – Address Resolution Protocol , протокол визначення адрес.

IP – Internet Protocol, інтернет протокол, в мережах з комутаціє пакетів.

CRC – Cyclic Redundancy Check, алгоритм обчислення контрольної суми.

OSI – Open Systems Interconnection Model, базова еталонна модель взаємодії відкритих систем.

TCP – Transmission Control Protocol, протокол керування передачею.

UDP – User Datagram Protocol, протокол датаграм користувача.

TTL – Time to Live, час життя.

TLS – Transport Layer Security, протокол захисту транспортного рівня.

DPI – Deep Packet Inspection, глибока перевірка пакетів.

DNS – Domain Name System, служба доменних імен.

RTP – Real-time Transport Protocol, протокол передачі даних в реальному часі.

HTTP – HyperText Transfer Protocol, протокол передачі гіпертексту.

uTP – Torrent UDP, UDP торент протокол

ISP – Internet Service Provider, провайдер інтернет мереж

RRM – Radio Resource Management, Управління радіоресурсами.

CQI – Channel Quality Indicator, індикатор якості каналу.

QCI – QoS Class Identifier, Ідентифікатор класу QoS.

E2E – End-to-End, з кінця в кінець.

SINR – Signal to interference plus noise ratio, відношення сигналу/шум.

GBR – Guaranteed Bit Rate, гарантована швидкість передачі даних.

non-GBR – no Guaranteed Bit Rate, не гарантована швидкість передачі даних.

MBR – Maximum Bit Rate, максимальна швидкість передачі;

MC – Macro cell, макрокомірка.

SC – Small cell, мала комірка, мікрокомірка.

RB – Resource block, ресурсний блок.

CSI – Channel State Information, інформація про державний канал.

RR – Round Robin, циклічний алгоритм розподілу ресурів.

PF/PFS – Proportional Fairness Scheduling, пропорційно-справедливий алгоритм розподілу ресурсів.

CDF – Cumulative Distribution Function, кумулятивна функція розподілу.

RAN – Radio Access Network, мережа радіодоступу.

VM – Virtual Machine, віртуальна машина.

RAM – Random Access Memory, пам'ять з довільним доступом.

CPU – Central processing unit, центральний процесор.

СМО – Система масового обслуговування.

OvS – Open vSwitch, віртуальний комутатор.

DMCQR – Deterministic multiconstrained centralized QoS routing, централізована детермінована багатокритеріальна QoS маршрутизація.

SSL – Secure Sockets Layer, рівень захищених сокетів.

TSL – Transport Layer Security, захист на транспортному рівні.

RT – Real Time, реальний час.

URLLC – Ultra Reliable Low Latency Communications, надійний зв’язок із низькою затримкою.

ВСТУП

Актуальність теми. Одним із пріоритетних напрямів державної політики є розвиток інформаційного суспільства в Україні та впровадження новітніх інформаційно-комунікаційних технологій (ІКТ) в усі сфери суспільного життя. Саме тому, вченні різних світових та українських шкіл особливу увагу приділяють вирішенню різноманітних наукових проблем в напрямку розвитку існуючих технологій безпровідних і провідних систем зв’язку, починаючи від оптимізації процесів управління трафіком та розподілу мережевих ресурсів пов’язаних з побудовою ефективних, гнучких структур – до підвищення надійності, якості обслуговування, безпечності передавання даних та швидкодії окремих компонент систем мережного управління.

Керівники департаментів розвитку телекомунікаційних технологій та зв'язку, що відповідають за інфраструктуру та експлуатацію інформаційних систем і мереж (2G-5G, IoT, LAN, WAN, Big Data, Cloud) одноголосно приходять до висновку, що велика кількість, складність і частота введення нових функцій у мережі зв'язку потребували нового підходу, який би кардинально змінив всі аспекти створення мереж, надання послуг та експлуатаційного управління. За їх висновками встановлено, що можливості традиційних мереж обмежені, не відповідають сучасним вимогам і є стримуючим чинником на шляху впровадження нових інфокомунікаційних послуг, що базуються на адаптивному надані сервісів, враховуючи наміри користувача чи корпоративної структури щодо захищеності та якості їх обслуговування. Розв'язання всього комплексу завдань адаптивного автоматичного управління потоками даних та цілою інфраструктурою в умовах змін значущості інформаційних бізнес-процесів складно реалізувати за допомогою існуючих методів та мережевих технологій. Оскільки зміна критеріїв оптимальності керуючих рішень вимагає постійного експертного та адміністративного втручання, яке в більшості призводить до значних операційних помилок і, як наслідок, часових та фінансових витрат на їх

вирішення. Головна проблема більшості інфокомунікаційних мереж в тому, що вони побудовані на основі пропрієтарного обладнання, функціонал якого реалізований апаратно, вимагає спеціалізованих знань системного адміністратора та є закритим для внесення змін щодо функціонування мережі напрямленої на потреби користувачів. Кожне додавання або зміна функцій системним адміністратором в мережевій інфраструктурі, як правило, призводить до складних завдань розгортання, які необхідно заздалегідь ретельно спланувати. В іншому випадку це додавання або зміна можуть негативно вплинути на ефективність функціонування цілої мережевої інфраструктури.

Таким чином, невідповідність технічних можливостей адаптації традиційної інфраструктури ІКТ до швидких мінливих вимог ринку, зумовила появу принципово нового концептуального підходу – до створення програмно-конфігурованих інтенційно-орієнтованих мереж (Intent-Based Software-Defined Network), які в майбутньому дадуть змогу трансформувати існуючі в даний момент статичні мережі в гнучкі, програмовані платформи з інтелектом для динамічного розподілу ресурсів, з масштабованістю для підтримки великомасштабних центрів обробки даних та із віртуалізацією – для роботи в динамічному, автоматизованому і безпечному хмарному середовищі.

Із розвитком бізнесу, різноманітності сервісів та вимог користувачів до якості обслуговування, інтенційно-орієнтовані мережі (Intent-based Network, IBN) виходять на перший план, як інструмент для інтелектуального управління гетерогенними мережами, який дає змогу абстрагуватися від деталей конфігурації і функціонування окремих елементів мережі та зосередитися на поведінці цілої мережі, як системи для надання сервісу відповідно до вимог та гарантування якості обслуговування на основі намірів користувачів. Основний принцип IBN полягає в перетворенні інформаційних бізнес-намірів користувачів до відповідних конфігурацій мережі для всіх пристроїв на основі мережної аналітики та машинного навчання. Саме тому, дослідження

принципів функціонування таких мереж та розроблення методів та засобів їх впровадження є важливим завданням як для гравців телекомунікаційного ринку, так і для науковців.

Помітний внесок у розробку теоретичних аспектів та концептуальних моделей, щодо проблематики побудови програмно-конфігурованих інформаційних мереж широко досліджувалася українськими та зарубіжними вченими. Зокрема, варто виділити роботи українських вчених, а саме: Лемешка О.В., Єременко О.С., Ложковського А.Г. в яких пропонуються рішення стосовно оптимізації процесу маршрутизації інформаційних потоків та розподілу мережевих ресурсів з метою покращення якості обслуговування кінцевих користувачів; Глоби Л.С., Скулиш М.А., Беркман Л.Н., Стрелковсьої І.В. в яких освітлено питання управління складною мережною інфраструктурою на основі технології SDN та NFV для забезпечення основних показників якості обслуговування; Толюпи С.В., Кулакова Ю.О., Конаховича Г.Ф., Радивилової Т.А. наукові праці яких, спрямовані на забезпечення захисту інформації в телекомунікаційних мережах. Серед численних напрацювань зарубіжних вчених, варто виділити напрацювання: D. Comerr останні роботи якого присвячені дослідженню побудови концепцій інтенційно-орієнтованих мереж на основі технології SDN; F.Callegati, X. Li, які досліджують автоматизоване управління та захист даних в майбутніх програмно-конфігурованих мережах; O. Ozkasap, J. Galán-Jiméne S. Abdellatif, які займаються розробкою методів для підвищення енергоефективності в програмно-конфігурованих мережах.

Аналіз напрацювань вітчизняних та зарубіжних учених підтверджує актуальність тематики досліджень як в Україні, так і за її межами. Проте, існуючі науково-теоретичні методи та технічні рішення є або концептуальними та важко реалізованими, або зосередженні лише в межах стандартизованої функціональності SDN, що не дають змоги в комплексі вирішити проблему синтезу та реалізації інтенційно-орієнтованих мереж, які повинні одночасно забезпечувати інтелектуальне управління мережею, необхідні параметри якості

обслуговування та безпеку даних в умовах обмеженості мережевих ресурсів та постійної потреби реінжинірингу бізнес-процесів користувачів корпоративних підприємств в режимі реального часу функціонування мережі. Для повноцінної реалізації таких мереж необхідно розробити уніфіковані програмно-апаратні засоби, які дають змогу реалізувати нові методи, моделі та алгоритми адаптивного інтелектуального управління ресурсами та якістю обслуговування в гетерогенних інфокомунікаційних мережах з гармонійним поєднанням сучасних методів мережної аналітики та машинного навчання. Таким чином, перетворюючи стандартні інфокомунікаційні мережі на автоматизовані інтелектуальні системи, що працюють на основі намірів користувачів та дають змогу вирішувати певний спектр технічних мережевих проблем і аналізувати їх без участі системного адміністратора.

Виходячи з ***існуючого протиріччя*** між функціональними можливостями сучасних пропрієтарних інформаційно-комунікаційних систем і необхідністю постійної адаптації під мінливі вимоги бізнес-користувачів щодо якості надання сервісів та автоматизованого розгортання мережевої інфраструктури для ефективного процесу обміну даними, актуальною ***науково-прикладною проблемою*** є розроблення методології аналізу та синтезу складних гетерогенних інфокомунікаційних систем з метою створення нової програмно-конфігурованої інтенційно-орієнтованої мережі, яка постійно на основі мінливих вимог користувачів щодо якості надання сервісів та розгортання інфраструктури навчається, адаптується, автоматизується і захищається від потенційних кібератак шляхом використання нових методів розподілу ресурсів, інженерії трафіку, мережевої аналітики та існуючих алгоритмів машинного навчання.

Зв’язок роботи з науковими програмами, планами, темами. Тематика дисертаційної роботи безпосередньо пов’язана з положеннями «Концепції розвитку телекомунікацій в Україні», «Стратегії розвитку інформаційного

суспільства в Україні» та рекомендацій щодо «Реформ галузі інформаційно-комунікаційних технологій та розвитку інформаційного простору України».

Дисертаційні дослідження виконувались у відповідності до наукового напряму кафедри телекомунікацій Національного університету «Львівська політехніка» - «Інфокомунікаційні системи та мережі», в межах низки держбюджетних науково-дослідних робіт: «Методи побудови та моделі інформаційно-телекомунікаційної інфраструктури на основі SDN-технологій для систем електронного урядування» (ДБ/SDN), (№ держреєстрації 0115U000444, (2015-2016 рр.) – учасник); «Методи побудови гетерогенних інформаційно-комунікаційних систем для розгортання програмно-конфігурованих мереж 5G подвійного використання» (ДБ/5G), (№ держреєстрації 0117U004449, (2017–2018 рр.) – відповідальний виконавець); «Розроблення методів адаптивного управління радіочастотним ресурсом у мережах мобільного зв'язку LTE-U для розвитку стандартів 4G/5G в Україні» (ДБ/LTE-U), (№ держреєстрації 0117U007177, (2018–2019 рр.) – відповідальний виконавець)); «Розроблення новітньої децентралізованої мережі мобільного зв'язку на основі блокчейн-архітектури та штучного інтелекту для впровадження технологій 5G/6G в Україні» (ДБ/Блокчейн), (№ держреєстрації 0120U100674, (2020-2022 рр.) – відповідальний виконавець); «Розробка методів та уніфікованих програмно-апаратних засобів для розгортання енергоефективних інтенційно-орієнтованих інфокомунікаційних мереж подвійного призначення» (ДБ/IBN), (№ держреєстрації 0120U102201, (2020-2022 рр.) – керівник)).

Результати дисертаційної роботи використані в ході виконання 4 госпдоговірних робіт: «Проектування та впровадження локальної мережі передавання мультимедійних даних на базі Ethernet технології» (ГД №0548) «Центр високих інформаційних технологій» (01.08.2016 р. – 31.10.2016 р.); «Розробка методів управління контентом в інформаційній системі підприємства з використанням технологій віртуалізації» (ГД №_741) ТОВ «ІнформКонсалт»

(29.09.2017 р. – 31.10.2017 р.); «Розробка енергоефективної SDN платформи для надання сервісів IoT в корпоративних мережах» (ГД №0632) ТОВ «ІнформКонсалт» (1.10.2019 р. – 30.11.2019 р.); «Розробка компонентів системи моніторингу та управління якістю надання послуг в інформаційних мережах з використанням технологій машинного навчання та мережної аналітики» (ГД №0655) ТОВ «МаксіТех» (15.10.2020 р. – 15.12.2020 р. – керівник).

Мета і завдання дослідження. Метою представленої дисертаційної роботи є підвищення ефективності функціонування інформаційно-комунікаційних систем шляхом розроблення методів і моделей адаптивного управління мережевими ресурсами та якістю надання сервісів у контексті реалізації основних ідей концепції інтенційно-орієнтованих мереж нового покоління.

Досягнення поставленої мети здійснюється розв’язанням таких завдань:

1. Аналіз існуючих методів і моделей управління ресурсами та якістю обслуговування у сучасних інформаційно-комунікаційних мережах.
2. Розроблення математичної моделі визначення суб’єктивного рівня задоволеності користувача за оцінкою QoE.
3. Розроблення потокової моделі енергоефективної QoE-маршрутизації для IBN.
4. Розроблення методу адаптивного клієнт-орієнтованого управління якістю надання послуг для IBN мереж.
5. Розроблення інтелектуальної DPI системи моніторингу та аналізу трафіку для автоматизованого виявлення аномалії і запобігання атак в інтенційно-орієнтованих мережах.
6. Розроблення методів розподілу частотно-часових ресурсів та балансування навантаження в гетерогенній мережі LTE/NB-IoT для адаптивного надання сервісів Інтернету речей.
7. Розроблення адаптивного інтенційно-орієнтованого методу розподілу ресурсів та формування структури рівня радіодоступу 4G/5G.

8. Розроблення імітаційної моделі інтенційно-орієнтованої гетерогенної мережі мобільного зв’язку.
9. Розроблення методології синтезу інтенційно-орієнтованої інфокомунікаційної мережі.
10. Практична реалізація та оцінювання ефективності запропонованих рішень на основі розроблених прототипів програмно-конфігурованої інтенційно-орієнтованої мережі корпоративного сегменту.

Об'єктом дослідження є процес синтезу програмно-конфігурованих інтенційно-орієнтованих мереж.

Предмет дослідження: моделі, методи та засоби синтезу інтенційно-орієнтованих інфокомунікаційних мереж для забезпечення високого рівня системної адаптивності щодо замовленої якості надання сервісів.

Методи дослідження. В процесі досліджень використано методи теорії графів, алгоритмів, ймовірності, фрактальних процесів, систем масового обслуговування, оптимізації, імітаційного моделювання, математичної статистики, об'єктно-орієнтованого програмування, комбінаторики, машинного навчання та експертних оцінок. Для підтвердження висунутих наукових гіпотез застосовано експериментальні методи дослідження.

Наукова новизна отриманих результатів.

1. Розвинуто *математичну модель визначення суб’єктивного рівня задоволеності користувача за оцінкою QoE* в залежності від зміни об’єктивних показників якості обслуговування QoS, що забезпечуються в мережі, зокрема для відео та аудіо сервісів реального часу, яка, на відміну від існуючих, базується на реальному експериментальному та експертному методі дослідження щодо пошуку математичної кореляції між нормалізованим значенням якості сприйняття сервісу QoE та інтегральним адитивним критерієм показників QoS із врахуванням функціонального параметру завантаженості мережевого вузла.

2. **Вперше** запропоновано *потокову модель енергоефективної QoE-маршрутизації для інтенційно-орієнтованих мереж*, яка, на відміну від відомих, для вибору оптимального шляху передавання даних використовує адаптивну QoE-орієнтовану метрику маршруту, що автоматизовано розраховується централізованим контролером мережі на основі розробленої математичної моделі кореляції нормалізованого значення замовленого рівня якості сприйняття сервісу та інтегрального адитивного критерію поточних показників якості обслуговування із врахуванням функціональних параметрів завантаженості мережевих вузлів, що дало змогу підтримувати компроміс між бажаною інтенційно-орієнтованою якістю обслуговування користувачів, завантаженістю та енергоефективністю мережі шляхом переведення в енергозберігаючий режим незадіяних вузлів.

3. **Вперше** запропоновано *метод адаптивного клієнт-орієнтованого управління якістю послуг для інтенційно-орієнтованих мереж*, який, на відміну від відомих, в умовах високого навантаження мережі для формування якості послуги включає в себе як об'єктивну оцінку часових мережевих характеристик, так і замовлені згідно намірів суб'єктивні QoE оцінки клієнтів, що дає змогу кінцевим користувачам сервісів опосередковано впливати на функціональну конфігурацію мережі, а з допомогою машинного навчання реагувати на несприятливі поєднання значень показників якості і попереджати ситуації, коли користувач незадоволений якістю отриманих сервісів для адаптивного прогнозування моменту переконфігурації мережі.

4. Удосконалено *метод виявлення аномалій мережевого трафіку*, який відрізняється від відомих формуванням набору інформативних ознак, що характеризують нормальну та аномальну поведінку інфокомунікаційної системи на основі оцінки параметра Херста із можливістю самонавчання, що дало змогу за короткий проміжок часу з високим ступенем точності автоматизовано виявляти та блокувати складні атаки різних типів в традиційних та майбутніх інтенційно-орієнтованих мережах.

5. **Вперше** розроблено *інтелектуальну DPI (Deep Packet Inspection) систему моніторингу та аналізу мережевого трафіку*, яка, на відміну від раніше відомих, для інтелектуального прийняття управлінських рішень процесом передавання даних базується на гармонійному поєднанні переваг методів сигнатурного, статистичного та фрактального аналізу інформативних ознак щодо детектування інформаційних протоколів та ранжування прихованих властивостей аномального трафіку, що дало змогу отримувати повну картину використання ресурсів мережі, виявляти користувачів, які споживають великі обсяги трафіку, ефективно управляти трафіком та сервісними політиками в режимі реального часу, автоматизовано створювати або оптимізувати сервісні пропозиції, підвищувати якість послуг та забезпечувати захист мережі і її користувачів.

6. **Вперше** запропоновано *метод розподілу частотно-часових ресурсів низхідного та висхідного каналу зв'язку гетерогенної мережі LTE/NB-IoT*, який, на відміну від відомих, враховує наміри користувачів щодо рівня якості надання сервісів Інтернету речей та проводить адаптивне інтелектуальне планування процесом виділення ресурсів на основі аналізу пріоритетності даних, зокрема у вузькосмуговому NB-IoT спектрі, що дало змогу забезпечити необхідну інтенційно-орієнтовану якість обслуговування із кінця в кінець.

7. Набув подальшого розвитку *метод балансування навантаження в мережі LTE/NB-IoT*, який, на відміну від відомих, в умовах недостатності необхідних ресурсів для обслуговування критично-важливих IoT даних в межах основної базової станції, дав змогу на основі розробленої централізованої системи моніторингу частотно-часових ресурсів та аналізу пріоритету забезпечити ультранадійний зв'язок з низькими затримками шляхом перенаправлення на обслуговування менш завантаженої альтернативної базової станції.

8. **Вперше** запропоновано *адаптивний інтенційно-орієнтований метод розподілу ресурсів та формування структури рівня радіодоступу 4G/5G*, який

відрізняється від відомих урахуванням локалізації групи інтенційно-орієнтованого користувацького навантаження та аналізом замовлених оцінок щодо забезпечення необхідного рівня якості сприйняття сервісу, що дало змогу ефективніше використовувати наявні енергетичні та частотно-часові ресурси із забезпеченням замовленої якості обслуговування.

9. Набула подальшого розвитку *імітаційна модель інтенційно-орієнтованої гетерогенної мережі мобільного зв'язку*, яка, на відміну від відомих, враховує значну кількість технічних параметрів мережі для створення реальних умов дослідження та автоматизує запропоновані методи інтенційно-орієнтованого управління частотно-часовими ресурсами та формування структури рівня радіодоступу, що дало змогу оцінити ефективність розроблених рішень в процесі оптимізації мережі за критерієм замовленої якості обслуговування з урахуванням обмеженості спектральних та енергетичних ресурсів у порівнянні із відомими методами.

10. **Вперше** запропоновано *методологію синтезу гетерогенної інтенційно-орієнтованої мережі*, яка відрізняється від відомих, багатоаспектним уявленням про структуру інфокомунікаційної системи як про цілісну централізовану програмовану мережну інфраструктуру, що складається з окремих підсистем та дало змогу інтелектуально виділяти зв'язки між структурно-функціональними елементами мережі, які можуть не тільки автоматизовано перебудовуватись з різною продуктивністю, але й виникати заново, вишукуючи шляхи найбільш адекватного пристосування до мінливих вимог користувачів для підвищення рівня адаптивності системи на основі розроблених методів управління енергоефективністю, якістю сприйняття сервісу, захищеності даних та розподілу ресурсів.

Практичне значення одержаних результатів. Основним практичним результатом дисертації, який одержаний на основі проведених теоретичних та практичних досліджень, є розвиток методології синтезу інфокомунікаційних систем шляхом конфігурування її мережно-незалежних рівнів для забезпечення

вимог до адаптивності мережної системи, якості обслуговування користувачів та оперативності доставки даних, що є основними цілями необхідних для реалізації мереж нового покоління IBN.

У межах запропонованої методології синтезу інфокомунікаційних систем для реалізації IBN використано наступні практичні особливості розроблених методів, моделей, засобів та алгоритмів:

1. Удосконалено алгоритм вимірювання затримки передавання даних в програмно-конфігурованих мережах шляхом формування IBN/SDN контролером пробних пакетів меншого розміру з різними пріоритетами, що дало можливість у високонавантажених каналах для низько пріоритетних потоків покращити точність моніторингу до **45%** та зменшити до **22%** сигналізаційне навантаження у порівнянні із відомими.

2. Розроблено імітаційну модель мережі з можливістю перемикання між двома методами управління якістю обслуговування (традиційного та клієнт-орієнтованого). Перевагою даної моделі є можливість досліджувати нові рішення для майбутньої концепції інтенційно-орієнтованих мереж шляхом інтеграції унікальних алгоритмів у ядро мережі. Встановлено що запропонований метод адаптивного клієнт-орієнтованого управління якістю послуг дає виграш в середньому від **2-5 разів** за критерієм кількості користувачів, які вимагають високої якості сприйняття послуги.

3. Розроблено адаптивний алгоритм вибору рівня технології граничних та хмарних обчислень для забезпечення необхідного рівня якості обслуговування сервісів в інтенційно-орієнтованій інфокомунікаційній мережі.

4. Розроблена інтелектуальна DPI система моніторингу та аналізу трафіку дала змогу виявити складні атаки різного роду, зокрема таких як **Non-Spoofed UDP Flood,** SYN Flood, фрагментація HTTP та шляхом автоматизованого блокування виявленого шкідливого трафіку зменшити загальний рівень втрат на **5%** у порівнянні із існуючою комерційною системою SolarWinds DPI.

5. На основі розробленої імітаційної моделі гетерогенної мережі LTE/NB-IoT встановлено, що комплексне використання розроблених методів пріоритезації IoT трафіку та балансування навантаження, дають змогу зменшити середню затримку передавання повідомлень реального часу з кінця в кінець на **68,8%** (або 3,21 рази), а також при використанні механізму пріоритезації, зменшити кількість відмов у обслуговуванні на **58%** для класу L1 (трафік RT) та **76%** для L2 (трафік URLLC) у порівнянні з існуючим методом пропорційного розподілу ресурсів в умовах високого навантаження. У випадку одночасного використання запропонованих рішень досягається мінімальна кількість відмов для сервісів IoT класу L1 та L2 в умовах недовантаженості альтернативних базових станцій.

6. Розроблений адаптивний інтенційно-орієнтований метод розподілу ресурсів та формування структури рівня радіодоступу мереж 4G/5G дав змогу ефективніше на **25 %** використовувати наявні частотно-часові ресурси та зменшити на **8,7%** енергоспоживання мережі рівня радіодоступу для забезпечення замовленої якості обслуговування користувачів у порівнянні із традиційними методами.

7. Розроблено алгоритм вибору безпровідної мережі доступу в гетерогенному середовищі з використанням Big Data, який, на відміну від відомих, враховує та аналізує оцінки замовленої якості сприйняття послуги та дає змогу покращити якість обслуговування високопріоритених послуг на вимогу та збільшити прибуток оператора.

8. Розроблено прототип мобільного та операторського додатку для адаптивного клієнт-орієнтованого надання послуг в гетерогенній мережі, що дає змогу отримувати замовлену якість обслуговування на основі зворотного зв’язку між користувачем та оператором мережі.

9. Розроблено прототипи корпоративного сегменту енергоефективної інтенційно-орієнтованої мережі різного призначення на базі мікроконтролерних платформ, апаратних SDN комутаторів ZODIAC FX/GX та віртуалізації

функцій компонентів технології SDN, в межах яких реалізовано та оцінено ефективність запропонованих рішень щодо адаптивного клієнт-орієнтованого управління ресурсами та якістю обслуговування.

10. Розроблено унікальну систему моніторингу якості функціонування реалізованих прототипів IBN мереж за критерієм затримки передавання даних, що є одним із ключових параметрів моніторингу якості надання сервісів реального часу критично-важливої інфраструктури. Особливістю системи є використання розробленого методу наскрізного вимірювання затримки з кінця в кінець для кожного компонента мережі шляхом додавання власної мітки часу до метаданих, так що, порівнюючи дві мітки між компонентами, можна визначити час затримки та в умовах перевищення норм сповіщати про прийняття необхідних керуючих рішень.

11. На основі експериментального дослідження в межах розробленого прототипу IBN мережі встановлено, що запропонована *модель енергоефективної QoE-маршрутизації* потоків даних у порівнянні із відомою концептуальною моделлю багатокритеріальної маршрутизації DMCQR для програмно-конфігурованих мереж, дала змогу досягти кращої збалансованості завантаження канальних ресурсів мережі за рахунок раціонального вибору шляхів передавання для різнорідного трафіку та зменшити до **3 разів** середню затримку обслуговування потоків реального часу з кінця в кінець для яких при використанні маршрутизації DMCQR не виконувались допустимі норми затримки, а також в умовах низької інтенсивності загального трафіку зменшити енергоспоживання мережі до **53,56%**.

Наукові та практичні результати виконаних досліджень використані у навчальному процесі кафедри телекомунікацій Національного університету «Львівська політехніка», зокрема для студентів спеціальності 172 «Телекомунікації та радіотехніка» в курсі лекцій з дисципліни «Побудова та протоколи гетерогенних мереж мобільного зв’язку», спеціальності 126 «Інформаційні системи та технології» в курсі лекцій з дисципліни «Технології

інформаційно-комунікаційних мереж», «Проектування інформаційних мереж», а також у держбюджетних науково-дослідних роботах з 2015 по 2020 рік.

Основні результати дисертаційної роботи використано і впроваджено з метою підвищення параметрів якості обслуговування та гнучкості управління ресурсами в телекомунікаційних корпоративних мережах Науково-дослідного інституту інтелектуальних комп'ютерних систем, ТОВ «ОСТВЕР СЕРВІСЕЗ», ТОВ «Телекомунікаційна компанія», ПАТ «Укртелеком», ТОВ ВТФ «Контех», ТОВ «МаксіТех», ТОВ «ІнформКонсалт», Hubei University of Technology, що підтверджено актами впровадження.

Особистий внесок здобувача. Основні наукові результати дисертаційної роботи отримано автором самостійно. У працях, опублікованих у співавторстві, авторові належать: у роботах [6, 14, 15, 18, 31, 40, 47] – методи балансування навантаження та розподілу частотно-часових ресурсів низхідного та висхідного каналу зв'язку гетерогенної мережі LTE/NB-IoT; [3, 9, 23, 29, 30, 45, 48, 58] – імітаційні моделі інфокомунікаційних мереж та метод адаптивного клієнт-орієнтованого управління якістю послуг для IBN мереж; [5, 8, 42, 49, 60] – метод виявлення аномалій мережевого трафіку та інтелектуальна DPI система; [35, 37, 50] – потокова модель маршрутизації для програмно-конфігурованих мереж; [11, 13, 21, 25, 46, 52] – методи оптимізації мережевих ресурсів інфокомунікаційних мереж та адаптивного управління трафіком; [2, 23, 36, 38] – адаптивний інтенційно-орієнтований метод розподілу ресурсів та формування структури рівня радіодоступу 4G/5G; [2, 32, 57] – імітаційна модель інтенційно-орієнтованої гетерогенної мережі 4G/5G; [2, 29, 56] – алгоритм вибору безпровідної мережі доступу в гетерогенному середовищі з використанням Big Data; [1, 17, 39, 43, 53] – прототипи корпоративного сегменту програмно-конфігурованої IBN мережі; [2, 16, 41, 51, 54] – адаптивний алгоритм вибору рівня технології граничних та хмарних обчислень для забезпечення необхідного рівня якості обслуговування сервісів в IBN; [4, 28] – алгоритм вимірювання затримки передавання даних в програмно-конфігурованих мережах; [7, 10, 24,

44] – моделі управління енергоспоживанням в інфокомунікаційних мережах; [15, 12, 19, 20, 26, 27, 33, 33, 55, 59] – методологія синтезу інфокомунікаційних мереж з віртуалізацією інфраструктури.

Апробація результатів дисертації. Основні наукові результати і положення дисертації представлені, доповідались та обговорені на 22-ох міжнародних і державних науково-технічних конференціях та наукових семінарах: Міжнародних науково-технічних конференціях «Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії» (TCSET, м. Львів-Славське 2016, 2018, 2020 рр.); IEEE Ukraine Conference on Electrical and Computer Engineering (UKRCON, м. Львів, 2017, 2019 рр.); International IEEE Conferences on Advanced Information and Communication Technologie (AICT, м. Львів, 2015, 2017, 2019 рр.); Міжнародних конференціях «Досвід розробки та застосування приладо-технологічних САПР в мікроелектроніці» (CADSM, м. Львів-Поляна, 2017, 2019 рр.); Міжнародних конференціях з інформаційно-телекомунікаційних технологій та радіоелектроніки (UkrMiCo, м. Київ 2016 р., м. Одеса, 2017, 2018 рр.); IEEE 4th International symposium on wireless systems within the international conferences on intelligent data acquisition and advanced computing systems (IDAACS-SWS, м. Львів, 2018р.); International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T, м. Харків, 2015, 2017 рр.); 5-ій міжнародній науково-практичній конференції «Фізико-технологічні проблеми передавання, обробки та зберігання інформації в інфокомунікаційних системах» (м. Чернівці 2016 р.); 1-й міжнародній науково-практичній конференції "Проблеми кібербезпеки інформаційно телекомунікаційних систем" (2018 р., м. Київ); 10-й міжнародній науково-технічній конференції «Проблеми телекомунікацій» (м. Київ, 2016 р.).

Публікації. За результатами досліджень, які викладені у дисертаційній роботі, опубліковано 60 наукових праць, серед них 1 – одноосібна монографія у закордонному виданні, 1 – колективна монографія, 7 – статей у закордонних виданнях, що входять до наукометричних баз Scopus/Web of Science, 1 – стаття

у фаховому виданні України, що входить до наукометричних баз Scopus, 2 – статті у закордонних періодичних виданнях, 12 – статей у наукових фахових виданнях України, 36 – у збірниках матеріалів і тез доповідей міжнародних та всеукраїнських конференцій, з них індексованих у наукометричній базі Scopus /Web of Science – 27.

Структура та обсяг роботи. Робота складається з переліку умовних скорочень, вступу, шести розділів, висновків, списку використаних джерел і 4 додатків. Загальний обсяг роботи складає 450 сторінок друкарського тексту, із них 16 сторінок вступу, 335 сторінок основного тексту, 189 рисунків, 20 таблиць, список використаних джерел із 280 найменувань. Додатки містять обрані початкові коди розробленого програмного забезпечення, акти впровадження результатів дисертаційної роботи, а також список праць автора.

РОЗДІЛ 1. АНАЛІЗ ПРОБЛЕМ УПРАВЛІННЯ ЯКІСТЮ НАДАННЯ СЕРВІСІВ В СУЧАСНИХ ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ІНТЕНЦІЙНО-ОРІЄНТОВАНИХ МЕРЕЖ

1.1. Аналіз існуючих обмежень традиційних мережевих технологій та моделей управління якістю надання послуг

На сьогоднішній час інфокомунікаційна мережа являє собою сукупність територіально розподілених інформаційних, обчислювальних ресурсів, програмних комплексів управління, що розміщуються в кінцевих системах мережі та термінальних системах користувачів, взаємодія між якими забезпечується за допомогою телекомунікацій, і які спільно утворюють єдину гетерогенну мультисервісну платформу, що включає в себе (2G-5G, IoT, LAN, WAN, Big Data, Cloud) [1].

Вимоги сучасного ринку телекомунікацій практично неможливо задовольнити за допомогою нинішніх мережевих архітектур. З обмеженим бюджетом IT-відділи компаній намагаються витягнути все зі своїх поточних мереж, використовуючи інструменти управління мережею на рівні пристроїв або виконуючи процеси ручного налаштування. Постачальники стикаються з аналогічними проблемами: попит на мобільність і високу пропускну здатність зростає, в той час як доходи знижуються в міру зростання вартості обладнання і зниження доходів [2]. В традиційних мережевих архітектурах не враховані сучасні вимоги бізнес-користувачів, компаній, провайдерів, а можливості проектувальників обмежені недоліками сучасних інформаційно-комунікаційних систем.

1. Складності налаштування та управління мережевою інфраструктурою.

Сучасні мережеві технології, які експлуатуються телекомунікаційними операторами в основному базуються на різноманітних протоколах, призначених для забезпечення якісного надання послуг. Для задоволення технічних і бізнес-потреб за останні кілька десятиліть телекомунікаційна галузь зосереджена в

напрямку розроблення нових мережевих протоколів, що забезпечують більш високу захищеність, продуктивність і надійність [3-5]. В результаті еволюції протоколів, більшість із них мають тенденцію визначатися ізольовано, і вирішувати конкретну проблему без будь-якої фундаментальної абстракції. У зв'язку з цим, складність конфігурації на основі сьогоднішніх протоколів є одним із основних обмежень сучасних інфокомунікаційних мереж. З точки зору системного адміністрування в межах домену корпоративної мереж, наприклад, переміщення або додавання одного кінцевого пристрою, включає в себе специфічну конфігурацію ряду комутаторів, маршрутизаторів, брандмауерів, порталів Web-аутентифікації і т.д., а також оновлення ACL, VLAN, Quality of Service (QoS) і інших механізмів та протоколів, які використовують складні засоби управління на рівні пристроїв [6]. Також слід враховувати мережеву топологію, моделі комутаторів різних виробників і версії програмного забезпечення.

Для управління мережевими ресурсами і забезпечення належної якості обслуговування застосовуються різноманітні технологічні рішення [9-11]. Існують дві фундаментальні моделі якості обслуговування (рис.1.1): Integrated Services (Intserv) і Differentiated services (Diffserv). Ці моделі містять різні типи механізмів, які забезпечують певні рішення для мережевого трафіку [12-14]. Метою Diffserv є пріоритезація трафіку за класами та оброблення різних класів трафіку в мережевих пристроях по-різному. У моделі DiffServ для визначення та управління мережевим трафіком використовується класифікація послуг, «клас» може бути позначений безпосередньо в заголовках пакетів, на відміну від моделі IntServ, де потрібно використовувати спеціальний сигналізаційний протокол резервування RSVP, щоб повідомити маршрутизаторів, які потоки пакетів вимагають гарантованого обслуговування. Можливість масштабування та простота пріоритетності трафіку в DiffServ забезпечують набагато менші витрати на реалізацію, також надають підвищену надійність, яка здійснюється за рахунок того, що класифікація відбувається на кордоні DiffServ-домена без

виконання сигналізаційних запитів, визначають гнучкість технології DiffServ. Однак, дана технологія лише забезпечує більшу пропускну здатність мережі для більш пріоритетних потоків, але не забезпечує ніяких гарантій щодо QoS.

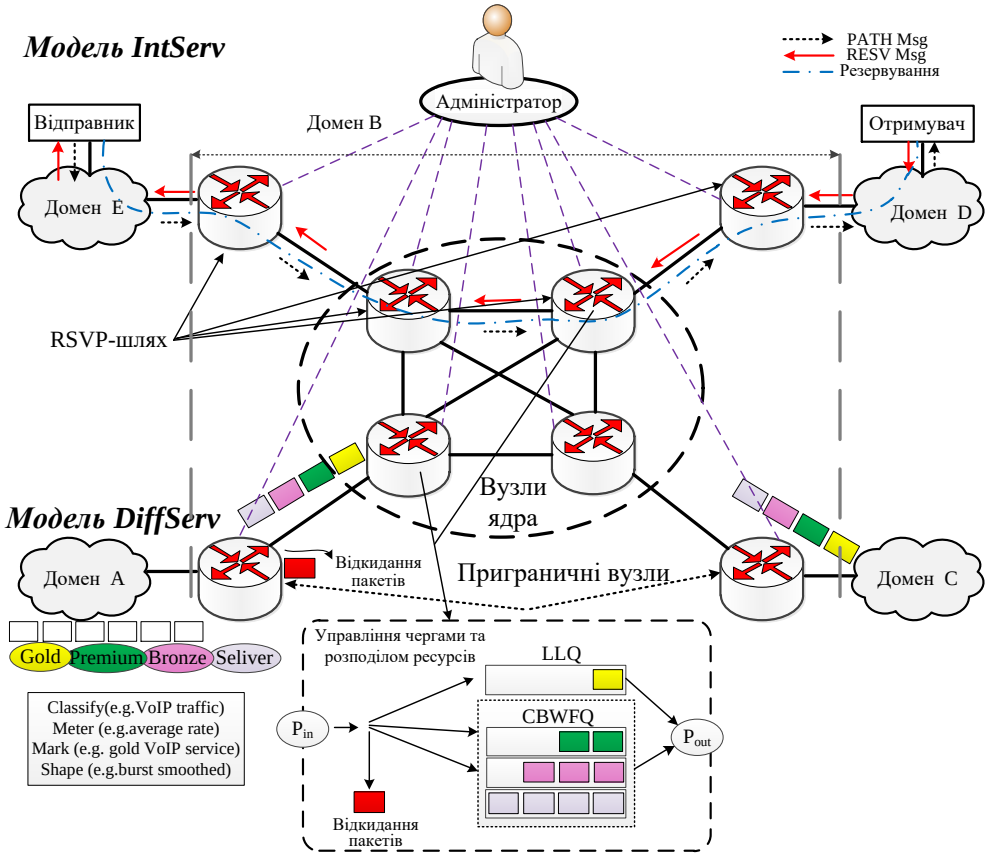


Рис.1.1. Фундаментальні моделі якості обслуговування Intserv та Diffserv

В традиційному мережевому обладнанні здійснено велику кількість механізмів управління чергами з погляду запобігання перевантаження та їх формування і обслуговування (FIFO, PQ, CQ, FQ/WFQ, CBQ, LLQ). Їх відмінність полягає у можливостях по налаштуванню, по диференціації обслуговування та ефективності в цілому. Адміністратор мережі приймає рішення про включення даних механізмів на конкретному інтерфейсі.

За допомогою даних механізмів визначається кількість організованих на інтерфейсі черг, орієнтовно розраховується максимально можлива довжина черги, контролюється завантаженість у черзі і здійснюється управління процесом відкидання пакетів у випадку перевантаження інтерфейсу [15-17].

Таблиця 1.1

Характеристика механізмів обслуговування черг

Параметри механізму	Назва механізму					
	FIFO	PQ	CQ	FQ/WFQ, FB-WFQ	CBWFQ	LLQ
Кількість черг	1	4	16	256	64	64+1
Форування черги	A*	P., CLI-ACLs	P., CLI-ACLs	A.	P.**,CLI-ACLs	P., CLI-ACLs
Обслуговування черги	A.	Strict Priority	Round Robin	A.	P., CLI	P., CLI
Забезпечення QoS-гарантій	-	-	-	-	+	+
* A. – автоматичне вирішення; ** P. –конфігурація вручну.						

Ряд механізмів дають можливість налаштування порядку черговості обслуговування пакетів. Деякі механізми можуть працювати у автоматичному режимі [18], а деякі з технологічних засобів управління чергами вимагають постійного втручання адміністратора мережі [19].

Сьогодні через ці проблеми мережі є відносно статичними, так як мережеві адміністратори прагнуть звести до мінімуму ризик простоїв в обслуговуванні через неправильність конфігурації. Статистична специфіка мереж різко контрастує з динамічною природою сьогоднішнього серверного середовища, при якій віртуалізація серверів значно збільшила кількість пристроїв, які потребують підключення до мережі, і фундаментально змінила припущення про фізичне розташування вузлів [20-22]. З появою технологій віртуалізації багато підприємств сьогодні використовують IP мережі для передачі голосу, відео і даних, але не дивлячись на те, що існуючі мережі можуть надавати різні рівні якості надання сервісу для різних додатків, процес конфігурації для надання цих ресурсів дуже довготривалий, складний, вимагає спеціальних навиків і виконується в ручному режимі. Для виконання цих завдань системним адміністраторам необхідно налаштовувати мережеве обладнання постачальника окремо, а також конфігурувати такі параметри, як пропускна здатність мережі і

методи забезпечення QoS на рівні сеансу для кожного сервісу [23-25]. У зв'язку зі своєю статичною природою традиційна мережа не в змозі динамічно адаптуватися до мінливих вимог трафіку, сервісів та користувачів.

2. Неузгоджені політики.

Щоб встановити певні політики обслуговування по всій мережі, системні адміністратори повинні налаштувати значну кількість мережевих пристроїв і механізмів [26-28]. Через складність нинішніх мереж системним адміністраторам стає досить проблематично застосовувати узгоджений набір політик доступу, безпеки, QoS і інших в умовах зростаючої кількості користувачів та їх мінливих вимог до якості обслуговування, що робить корпоративні мережі уразливими до порушень інформаційної безпеки, невідповідностей нормативам QoS та інших негативних наслідків.

3. Неможливість масштабування:

Хмарні рішення можна назвати технологіями, які допоможуть бізнесу швидше адаптуватися до нових реалій і зберегти прибуток на докризовому рівні. В останні роки чимало організацій придивлялися до хмарних технологій, однак пандемія підштовхнула їх до активного впровадження рішень. У міру того, як вимоги до хмарних сервісів неухильно ростуть, повинні зростати і вимоги до мереж, які їх об'єднують. Однак, мережа стає набагато складніша з додаванням безлічі або тисяч мережевих пристроїв, які повинні гнучко налаштовуватися і управлятися [29]. Крім того, системні адміністратори намагаються обчислити ресурси, закладені в мережу як резерв, з метою масштабування мережі, виходячи з передбачуваних закономірностей трафіку, але в сучасних віртуалізованих центрах обробки даних трафік характеризується мінливістю і випадковістю, не дає змогу передбачити деградацію QoS в умовах наявності достатньої кількості мережевих ресурсів. З постійним ростом клієнтських сервісів кількість обчислювальних серверних та мережевих елементів різко зростає, а обсяг даних, переданих між обчислювальними вузлами, може досягати петабайт. Згідно з даними провідних компаній,

потрібні так звані гіпермасштабні мережі, які можуть забезпечити високу продуктивність і низьку вартість з'єднання між сотнями тисяч фізичних серверів. Таке масштабування не може бути здійснено шляхом ручного управління. Для забезпечення конкурентоспроможності провайдери повинні надавати клієнтам все більш цінні, більш диференційовані послуги. Експлуатація масштабованих мереж ще більше ускладнює їх завдання, тому що мережа повинна обслуговувати групи користувачів з різними сервісами і різними вимогами до якості обслуговування. В існуючих мережах, особливо в масштабі провайдера, складно виконувати основні операції, які можуть здатися відносно простими, такі як управління потоками клієнтів для забезпечення контролю якості або надання послуг на вимогу. Для цього потрібні спеціалізовані пристрої на кордоні мережі, що збільшує капітальні та експлуатаційні витрати, а також час для впровадження нових послуг.

4. Залежність від виробника.

Прагнучи впроваджувати нові можливості і послуги, постачальники і підприємства реагують на швидко мінливі бізнес-потреби і вимоги користувачів. Однак їх здатність реагувати на теперішні бізнес виклики ускладнюється так званим товарним циклом обладнання постачальника, який може становити від трьох років і більше. Через відсутність стандартних, відкритих інтерфейсів традиційні оператори мереж не можуть адаптувати мережу до індивідуальних умов [29-31]. Навіть ті вендори, які постачають нібито «відкриті» системи, мають напоготові команди добре навчених і сертифікованих професіоналів, призначення яких полягає в підтримці безперебійної роботи систем.

1.2. Основні переваги та принципи функціонування програмно-конфігурованих мереж

Підприємства, оператори і постачальники послуг оточені рядом конкуруючих сил. Істотне зростання обсягу мультимедійного контенту,

бурхливий розвиток хмарних обчислень, збільшення використання мобільних пристроїв і постійна вимога скоротити витрати, зберігаючи при цьому стабільний дохід, призводять до руйнування традиційних бізнес-моделей.

Щоб залишатися в тренді, провайдери часто розглядають технологію SDN для корінного перетворення структури і рутинних операцій мережі [32]. SDN дає змогу централізовано програмувати поведінку мережі за допомогою програмного забезпечення і відкритих API [33]. Відкриття класичних закритих пропрієтарних мережевих платформ і впровадження рівня управління SDN дає змогу операторам узгоджено управляти всією мережею [34-36].

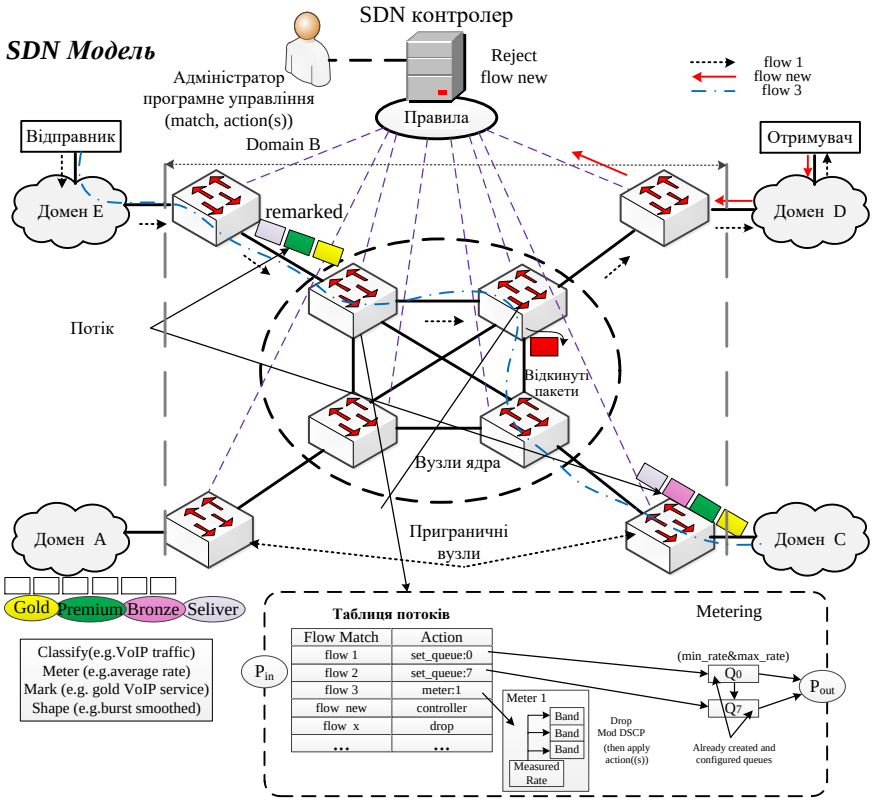


Рис.1.2. Фундаментальна модель управління якістю обслуговування в SDN

Функціональність SDN базується на чотирьох основних принципах.

1. Програмованість мережі. SDN дає змогу управляти поведінкою цілої мережі за допомогою програмного забезпечення, яке встановлене на центральному контролері мережі. В результаті оператори можуть налаштовувати поведінку своїх мереж для підтримки нових послуг і навіть

конкретних клієнтів [37]. Відділення апаратного забезпечення від програмного дає можливість операторам швидко впроваджувати інноваційні диференційовані послуги без обмежень, які накладають закриті пропрієтарні платформи [38].

2. Логічно централізований інтелектуальний контроль. Технологія SDN заснована на логічно централізованих мережевих топологіях, які забезпечують інтелектуальне управління ресурсами мережі. Традиційні методи управління мережею є розподіленими. Пристрої працюють автономно і характеризуються обмеженими відомостями про стан мережі. Централізований контроль, який забезпечується технологією SDN, дає змогу зробити управління пропускною здатністю, відновленням, захистом і політиками QoS високо інтелектуальними і оптимізованими, завдяки чому організація отримає комплексне уявлення про мережі [39-43].

3. Абстракція мережі. Послуги і програми на базі SDN виділяються з основних технологій, а обладнання, що забезпечує фізичне з'єднання, виводиться з мережевого управління. Замість інтерфейсів управління, прив'язаних до апаратного забезпечення, додатки взаємодіють з мережею через API, які дають змогу здійснювати загальне обслуговування мережі, включаючи маршрутизацію, безпеку, контроль доступу, управління пропускною здатністю, управління трафіком, якість обслуговування, оптимізацію процесора і зберігання даних, ефективне використання енергії, і всі форми управління політиками, виготовлені за індивідуальним замовленням для задоволення бізнес-цілей [45-47]. Наприклад, SDN архітектура дає змогу легко визначати і застосовувати узгоджену політику по провідному і безпровідному зв'язку на території кампуса. Аналогічним чином, SDN дає змогу управляти всією мережею за допомогою розумної оркестровки і систем попередньої підготовки.

4. Відкритість. Архітектура SDN забезпечує взаємодію різних постачальників і сприяє створенню комерційно нейтральної екосистеми, тим самим віщуючи нову епоху відкритості. Відкритість закладена в самій основі

SDN. Відкриті API підтримують різні додатки, включаючи рішення хмарного та мережного регулювання, а також критично важливі сервіси для бізнесу [48]. Крім того, інтелектуальне програмне забезпечення дає змогу управляти обладнанням різних постачальників за допомогою відкритих програмованих інтерфейсів, таких як OpenFlow [49]. Завдяки SDN передові мережеві послуги та програми можуть функціонувати в спільному програмному середовищі [50].

Крім того, можна створювати власні програми у вигляді додаткових модулів управління на контролері мережі, замість очікування впровадження певної функції в пропрієтарні і закриті програмні середовища в традиційних мережах. SDN дає змогу користувачам розробляти програми з урахуванням пропускної здатності мережі, відстежувати її стан і автоматично підлаштовувати конфігурацію під конкретні умови [51]. SDN технології на основі OpenFlow дають змогу системним адміністраторам вирішити проблеми високої пропускної здатності, динамічного характеру сучасних сервісів, адаптації мережі до постійно мінливих потреб бізнесу, складності функціонування та управління. Зокрема, для ознайомлення останніх досліджень в напрямку модифікації, забезпечення якості обслуговування, стандартів та особливостей функціонування програмно-конфігурованих мереж більш детально наводиться в статті [52], де автори провели колосальну оглядову роботу.

1.3. Аналіз концептуальних моделей побудови перспективних інфокомунікаційних мереж

1.3.1. Вимоги та інноваційні технічні рішення для сталого розвитку мереж мобільного зв’язку п’ятого покоління

Поява мобільних мереж четвертого покоління 4G LTE стало великим стрибком вперед для світу мобільних даних завдяки підтримці передавання даних з високою пропускною здатністю [53]. На даний момент мережі 4G підтримують смугу пропускання до 20 МГц, а теоретична швидкість передачі

даних технології LTE advanced може досягати декількох Гбіт/сек [54]. Однак постійно зростаючий попит на передачу мобільних даних вимагає істотного розвитку мереж 4G для забезпечення їх відповідності сучасним вимогам [55].

З метою забезпечення більш широкої смуги пропускання каналу і інформаційної ємності в порівнянні з поточними мережами четвертого покоління ведеться розробка мереж п'ятого покоління 5G [56]. Планується, що смуга каналу складе більше 100 МГц, а швидкість передачі даних буде досягати десятків гігабіт на секунду [57]. Як і у випадку з поточними системами четвертого покоління, у міру розвитку мереж 5G при їх впровадженні будуть застосовуватися нові технології і методи, спрямовані на ще більше збільшення пропускної здатності каналу передачі даних [58]. До деяких з нових технологій і методів, властивих мереж 5G відносяться багатоточковий прийом-передача (MIMO) з великою кількістю приймально-передавальних антен та адаптивне формування діаграми спрямованості [59].

На рис.1.3 показано розвиток мереж мобільного зв’язку. Згідно якої мобільні оператори стверджують, що в перспективі ядром мереж 5G буде технологія LTE [60]. Таким чином з появою 5G відбудеться повна зміна технічної стратегії, а саме перехід від розвитку виключно мереж мобільного зв’язку до гетерогенних систем та мереж доступу різних безпровідних технологій [61-63].

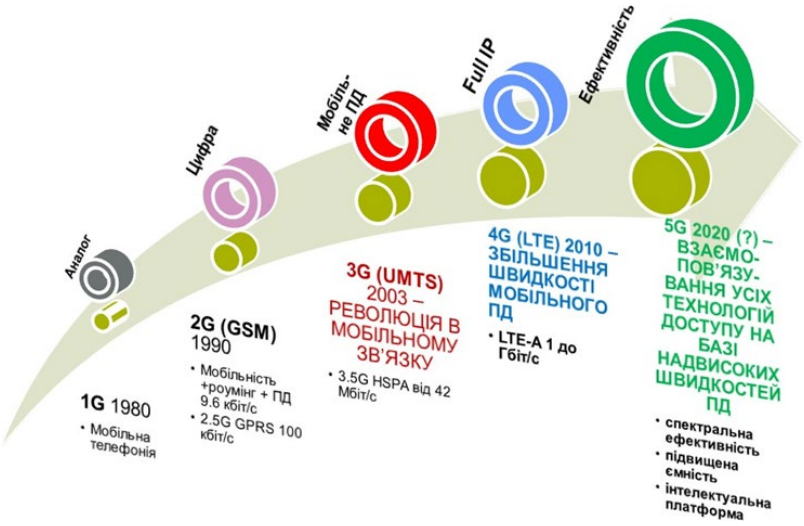


Рис.1.3. Еволюція мереж мобільного зв’язку

На рис. 1.4 показано загальний підхід щодо мереж 5-го покоління мобільного зв’язку (5G). Наглядно показано частотний план в діючих сучасних мережах мобільного зв’язку та в мережах нового покоління, зокрема:

– концепція 5G буде використовувати спільну інфраструктуру радіодоступу мобільних мереж 2G/3G/4G [64];

– бізнес-моделі для 5G будуть ґрунтуватися на бізнес-моделях 3G/4G з певними змінами [65].

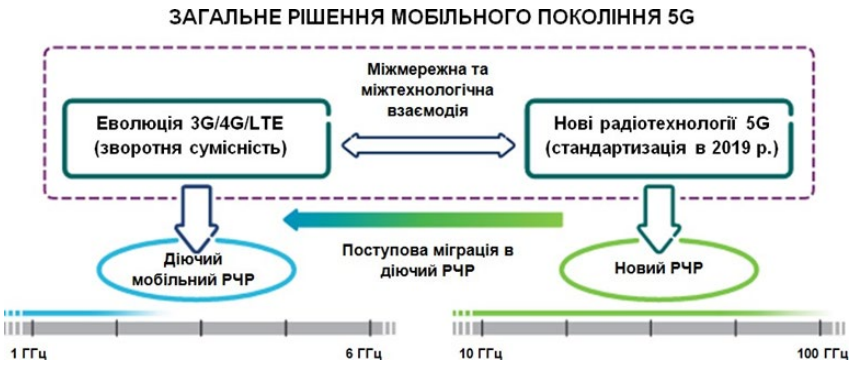


Рис. 1.4. Еволюція мереж мобільного зв’язку

Стандарт 5G повинен стати однією з опорних технологій в цифровій економіці. Він буде активно задіяний в таких напрямках як Інтернет речей, розумне місто, розумне виробництво, розумний будинок, розумний транспорт. 5G створить нові можливості для інтелектуальних і ефективних додатків, підключених до безлічі пристроїв, які працюють в самих різних комерційних областях і галузях економіки [66]. Взаємозв’язок поколінь мобільного зв’язку на шляху до 5G показано на рис.1.5.

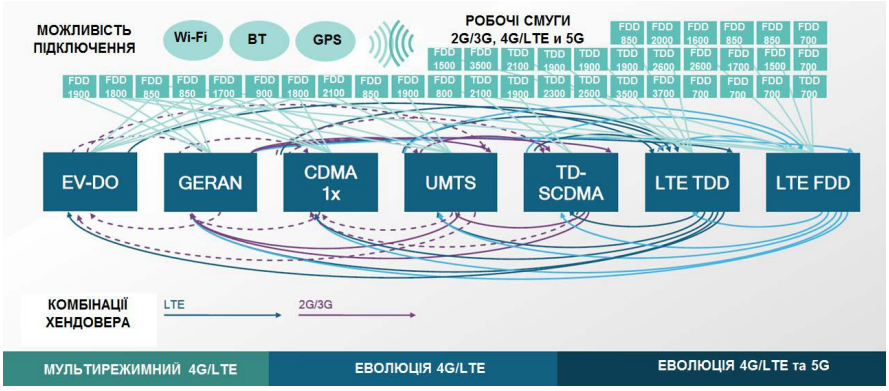
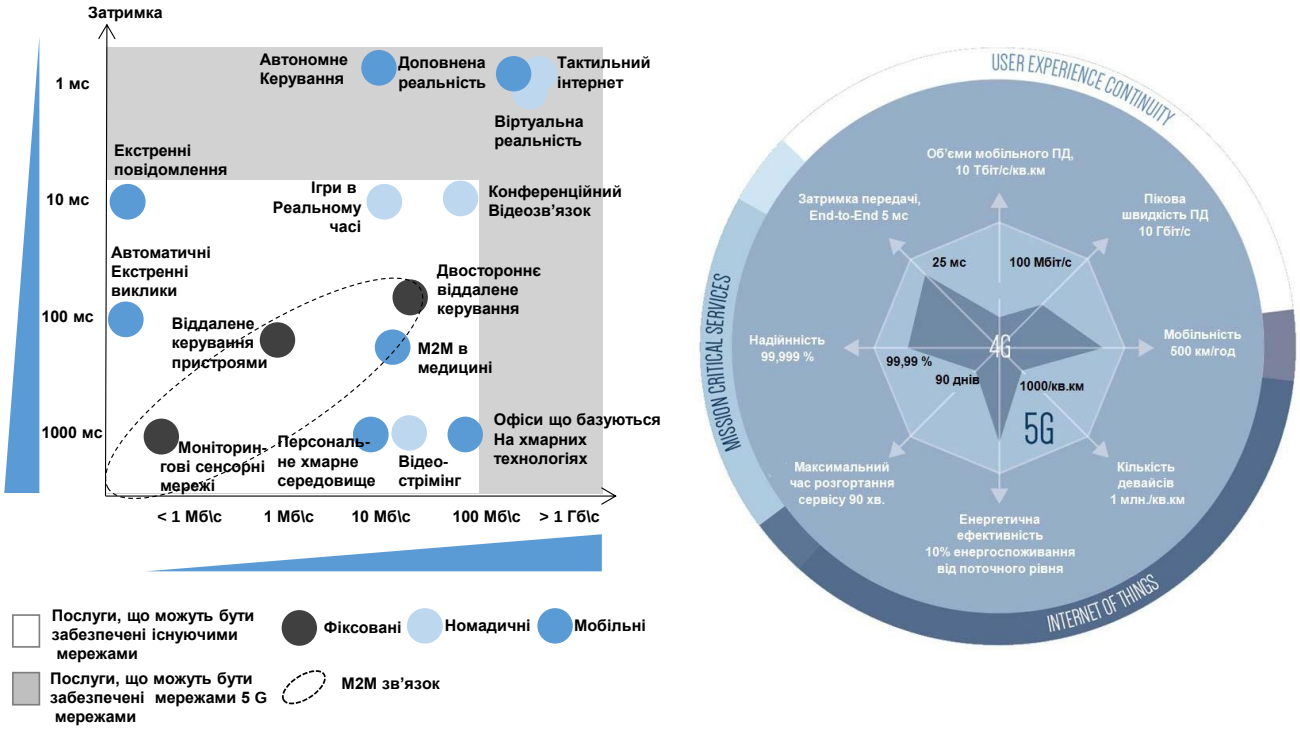


Рис.1.5. Взаємозв’язок поколінь мобільного зв’язку на шляху до 5G

Розвиток послуг рухомого широкосмугового зв'язку відбувається у відповідь на попит споживачів. Для прогнозованого зростання обсягів трафіку (за оцінками, в 10-100 разів в період 2020-2030 років), числа пристроїв і послуг, а також необхідного підвищення прийнятності в ціновому відношенні і поліпшення сприйняття користувачем послуг потрібні інноваційні рішення, а також нові підходи до використання об'єднаного потенціалу різних технологій 5G в галузях промисловості завдяки міжмашинній комунікації зв'язку, Інтернету речей (IoT) [67-69].

Очікується, що розвиток IMT-2020 (назва, яку використовують в МСЕ для стандартів 5G) продовжується і 2021 році, а випробування 5G і попередня комерційна діяльність вже ведуться, з тим щоб допомогти оцінити перспективні технології і смуги частот, які можуть використовуватися для цієї мети. Очікується, що перші повномасштабні комерційні розгортання мереж 5G будуть здійснені через деякий час після завершення підготовки специфікацій IMT-2020 [70]. Основні переваги від розвитку мереж 5G показано на рис.1.6.



а) б)

Рис.1.6. Потреби у розвитку мереж 5G – а) та їх вимоги – б) [71]

Розумне місто являє собою парадигму, яка пов'язана зі значним зміщенням інтересу до розвитку та використання безлічі інноваційних комунікаційних технологій, щоб зробити міста сьогодні більш інтелектуальними та покращити якість життя людей [72]. Впровадження п'ятого покоління мобільних мереж обіцяє стати революційним проривом в галузі зв'язку за рахунок наступних нововведень (рис.1.13):

Рис.1.7. Концепція побудови розумного міста на основі технології 5G [73]

– масивні MIMO. Ця технологія передбачає використання декількох антен на приймач. В результаті швидкість передачі даних і якість сигналу зросте пропорційно кількості антен за рахунок рознесеного прийому [74].

– нові діапазони. Сьогодні мережі LTE займають частоти нижче 3,5 ГГц. Стандарти 5G мають на увазі використання більш високочастотних діапазонів. Це дозволить позбутися від перешкод, однак змусить збільшити потужність передавачів і більш щільно розміщувати базові станції [75].

– network slicing (нарізка мережі). Ця технологія дозволяє мобільним операторам розгортати логічно ізольовані мережі, кожна з яких буде виділена

під певні потреби, наприклад для інтернету речей, широкосмугового доступу, трансляції відео і так далі. Таким чином мобільна мережа нового покоління зможе більш гнучко підлаштовуватися під різні застосування [76-78].

– мультитехнологічність. З метою забезпечення якісного обслуговування на мережах 5G потрібна підтримка існуючих стандартів, таких як UMTS, GSM, LTE, Wi-Fi реалізуючи нові алгоритми вертикального хендовера. Базові станції, що використовують технологію Wi-Fi, можуть бути задіяні для розвантаження трафіку в більш завантажених районах [79-81].

1.3.2. Сучасні світові моделі побудови перспективних програмно-конфігурованих мереж мобільного зв’язку з адаптивним наданням послуг

Управління та адміністрування інфокомунікаційних мереж зазвичай вимагають багато часу і навичок для гнучкого перепрограмування мережі, в основному, через архітектурну складність мережі, а також із-за обмеження використовуваних протоколів в традиційних мережевих архітектурах. Ці обмеження на реконфігурацію або перепрограмування мережі суперечать концепції еволюції мереж п'ятого покоління, які повинні будуть підтримувати широкий спектр пристроїв, що підключаються до мережі і їх використання з урахуванням різних характеристик по мобільності, безпеці, затримці, надійності. Збільшення потреб у використанні мережевих технологій для різних бізнес-задач, розподілених обчислень, поява великих дата-центрів і початок віртуалізації Інтернету, значне зростання числа мобільних пристроїв і контенту, віртуалізація серверів і поширення хмарних сервісів є основними причинами, які призвели до необхідності переосмислення традиційних мережевих архітектур.

В якості ефективного вирішення даних проблем виступають програмно-конфігуровані мережі, що працюють на базі протоколу OpenFlow. SDN дає змогу оптимізувати управління мережею більш ефективним і гнучким способом. Технологія SDN переглядає структуру традиційних мереж зв'язку,

розділяючи рівень управління і рівень передавання даних для спрощення адміністрування та контролю мережі, а також впровадження нових послуг.

SDN, NFV і EC технології пропонують потужні рішення для вирішення проблем при створенні мереж і систем п'ятого покоління 5G. Зокрема технологія NFV реалізує певні функції мережі за допомогою програмного забезпечення, що розміщується у віртуальному середовищі, що підвищує гнучкість всієї системи. Таким чином, технології NFV і SDN не суперечать один одному, а доповнюють свої можливості [82]. Перевага використання обох технологій полягає в зменшенні частки дорогого спеціалізованого апаратного забезпечення. На початку впровадження технології SDN використовувалися для центрів обробки даних, кампусних і приватних мереж. Згодом технологія знайшла своє місце і для використання в ядрі мобільних мереж. Що стосується технології NFV, то вона прагне замінити Middleboxes, використовувані в мобільних мережах [83]. При цьому, природно, здійснюється перехід від спеціалізованого апаратного обладнання до програмного забезпечення, що функціонує на покупному обладнанні (на менш дорогому серверному обладнанні). Концептуальна архітектура мобільної мережі 5G на основі технології SDN/NFV показано на рис.1.8.

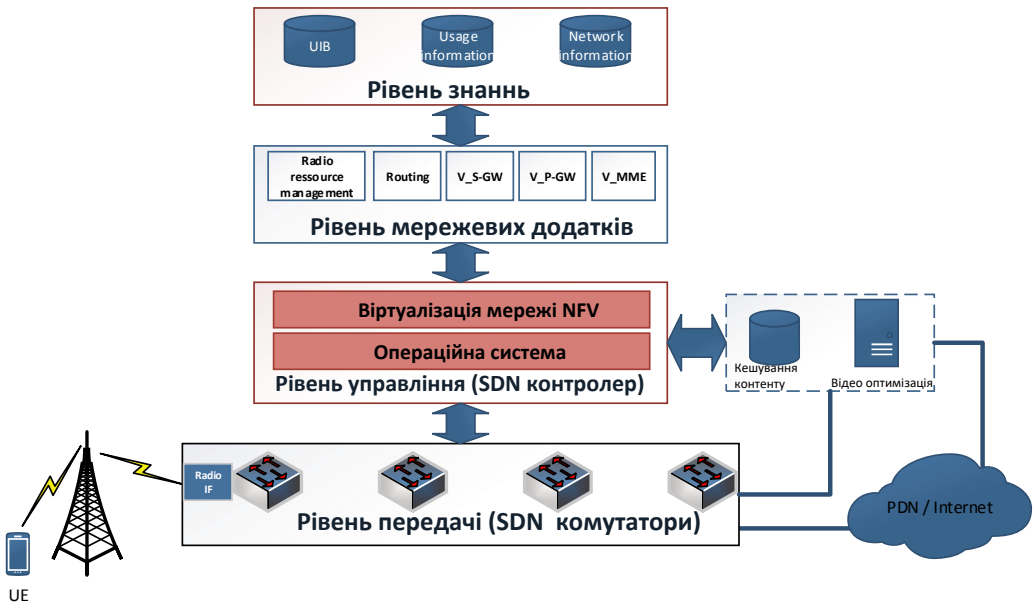


Рис.1.8. Архітектура мобільної мережі 5G на основі технології SDN [84]

Спільне використання SDN та NFV забезпечує можливість реалізації такої важливої концепції як мережевий слайсінг. Мережевий слайсінг можна розглядати як групу мережевих функцій, які працюють разом з певною технологією радіодоступу (RAT) для досягнення оптимального варіанта використання мережі. Іншими словами, мережевий слайсінг є способом підтримки послуг зв'язку за допомогою спеціального з'єднання. Мережевий слайсінг дає змогу оператору мережі побудувати кілька логічних мереж (кожна для певного варіанту використання) на одній фізичній інфраструктурі. Пропонований концептуальний підхід у роботах [85-87] полягає в створенні виділених логічних сегментів мереж, званих слайсами в архітектурі 5G з допомогою технології віртуалізації мережевих функцій NFV та SDN (рис.1.9)

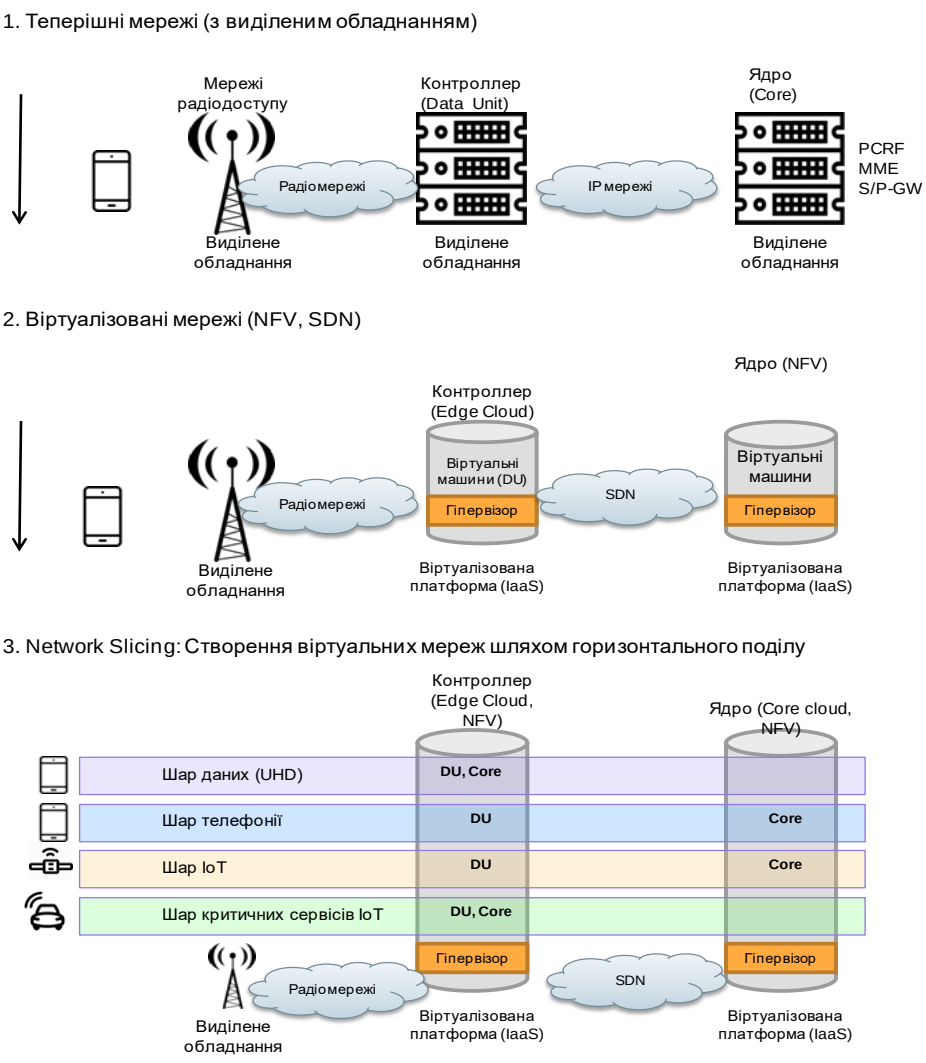


Рис.1.9. Network Slicing в мережах 5G

Інтегруючи SDN з 5G стільниковими технологіями, ряд механізмів управління мережею та управління (наприклад, управління трафіком, управління потужністю та розподіл спектру) може бути легко реалізований за допомогою централізованого SDN контролера через стандартизовані інтерфейси, без внесення значної модифікації в основні компоненти фізичної мережі. Крім того, за умови просунутого рівня абстрагування та віртуалізації фізичної інфраструктури віртуалізовані ресурси, такі як пропускна здатність, можна розділити на окремі фрагменти для спеціального використання та динамічно розподілити відповідно до потреб у режимі реального часу [88-90]. В основі будь-якої пропозиції віртуалізації eNodeB лежить гіпервізор LTE. Точно так само класичні менеджери віртуальних машин поділяють загальні обчислювальні ресурси, такі як цикли процесора, пам'ять та введення-виведення, а гіпервізор LTE відповідає за планування фізичних радіоресурсів, а саме блоків ресурсів LTE.

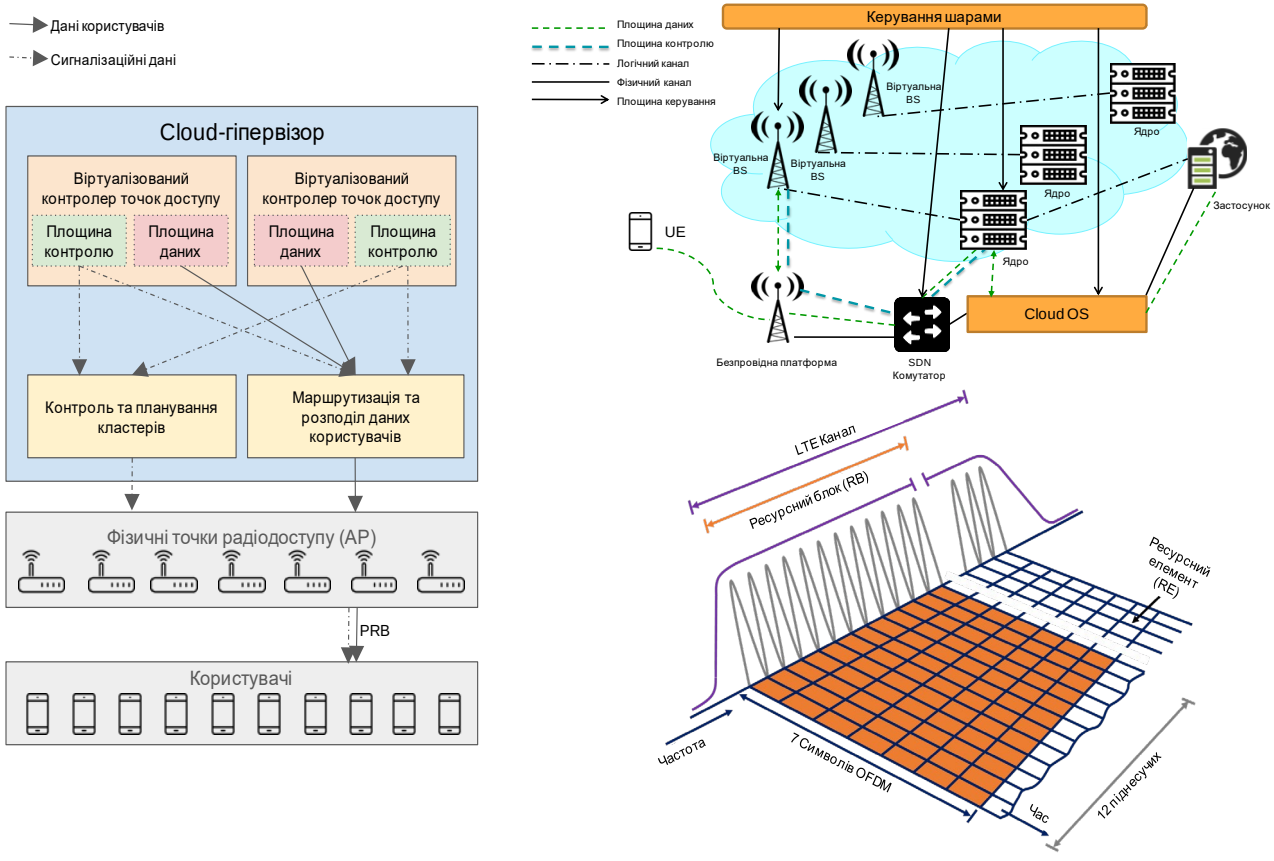


Рис. 1.10. Віртуалізація eNodeB з гіпервізором, що розподіляє PRB в 5G

Тільки тоді безпровідний спектр можна ефективно розподілити між незалежними власниками, що управляються або підтримуються окремим постачальником послуг або MVNO. Приклад представлено на рис. 1.10. Управляючи основними PRB, гіпервізор LTE збирає інформацію з підконтрольних eNodeB, а саме, навантаження трафіку, стан каналу та пріоритетні вимоги, а також контрактні вимоги кожного SP або MVNO для ефективного розподілу спектру. Цей розподіл може визначати гарантії на фіксовану або динамічну (максимальну) пропускну здатність, а також показники QoS з мінімальними гарантіями або без них.

Для успішної реалізації інтелектуального виділення пропускної здатності важливо адаптувати виділення пропускної здатності відповідно до просторово-часових потреб користувачів. Для провайдерів інтернет-послуг як і раніше складно впоратися з коливаннями трафіку даних для надійного надання послуг. Згідно [91], трафік в піковий час пандемії збільшився більш ніж на 50% за останній рік і, швидше за все, буде продовжувати зростати. Протягом пікового часу провайдеру важко забезпечити достатні ресурси пропускної здатності для задоволення потреб QoS всіх користувачів. І все-таки великий відсоток пропускної здатності залишається недостатньо використаним протягом періоду, що не перевищує пік. Тому важливо розробити інтелектуальні методи управління пропускною здатністю для провайдера, щоб вирівняти коливання попиту на трафіку, що важливо для покращення ефективності спектру та зменшення інвестиційних витрат.

Саме тому у роботі [92] запропоновано концептуальний підхід та проведено дослідження стосовно динамічно змінного тарифного плану в процесі користування послугами в умовах високого навантаження мережі в програмно-конфігурованих мережах 5G. Ціна за отримання послуг в умовах перевантаження та доступу за ресурси виставляється стосовно співвідношення ціна-якість. Що дає змогу клієнтам отримувати необхідну якість надання послуг в умовах високого навантаження мережі 5G. Відповідно для

користувачів, які хочуть отримувати сервіси в умовах перевантаження, ціна виставляється оператором вищою згідно тарифного плану. Такий підхід служить мотивуючим сигналом для нетерпимих до затримок користувачів отримати послуги за вищою ціною, а відповідно для терпимих користувачів, зберегти кошти в момент високого навантаження шляхом відкладання своїх вимог щодо отримання необхідних пропускних здатностей (чи послуг певної якості) в години пік. Розроблений підхід щодо тарифікації легко реалізується при умові, що мережа використовує SDN рішення. Чисельні результати підтверджують, що запропонований підхід тарифікації може дати задовільні результати з точки зору продуктивності перемикання попиту на трафік з пікового часу на непіковий час і ефективно справлятися з виникаючими тимчасовими перевантаженнями причому зберігаючи прибуток.

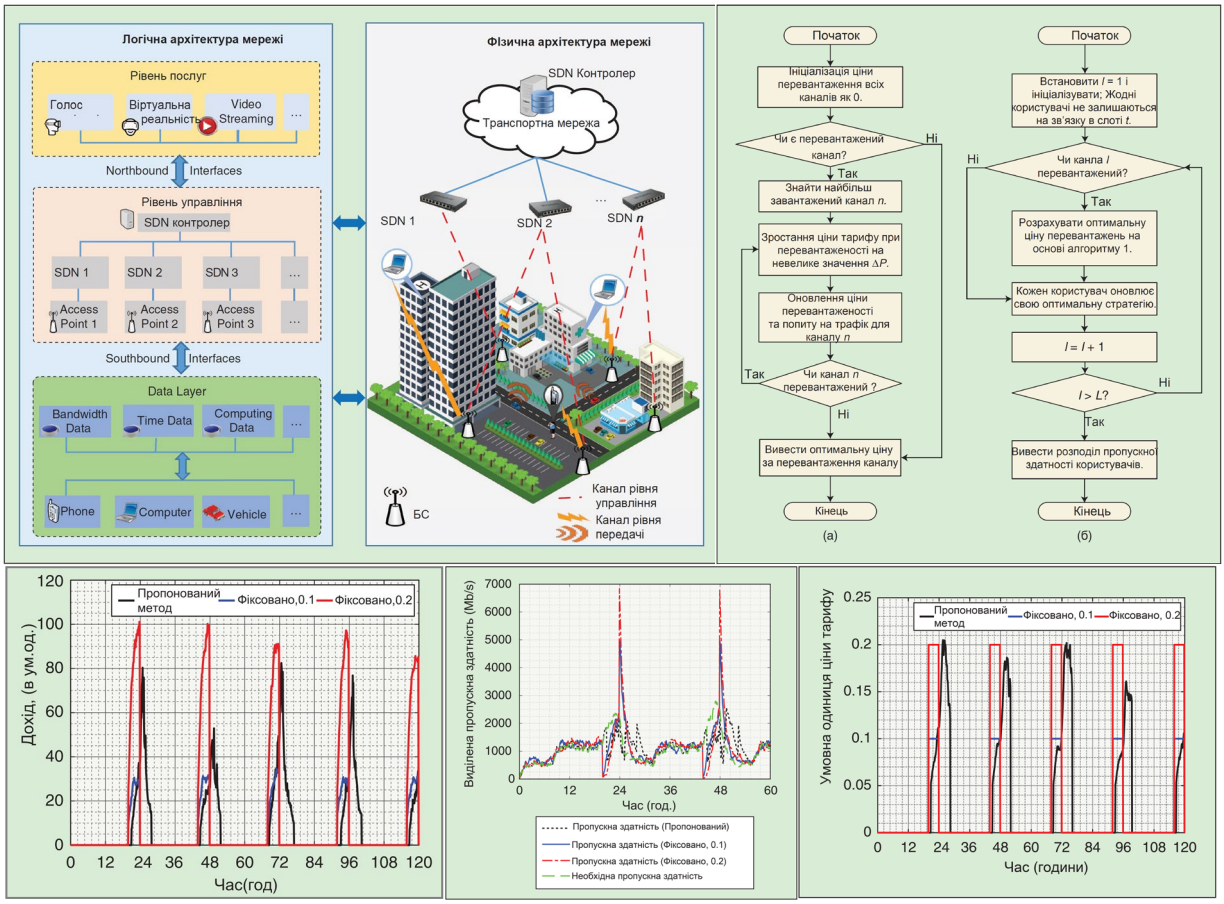


Рис.1.11. Концептуальна архітектура програмно-конфігурованої мобільної мережі 5G із адаптивною тарифікацією на надання послуг [92]

Концептуальна архітектура програмно-конфігурованої мобільної мережі 5G показана на рис.1.11. Програмований контролер SDN працює як центральний елемент мережі і здійснює всі функції управління за допомогою стандартизованих інтерфейсів. Розподілені базові станції, які відповідають за прийом та передачу даних, динамічно налаштовуються за допомогою централізованого контролера SDN з глобальними знаннями щодо замовлених вимог користувачів.

OpenFlow протокол має низьку ефективність в умовах масштабованості мережі для великих мереж [31]. Однак ця проблема може бути вирішена використанням окремих OpenFlow мереж в декількох різних областях мережі [93]. Таке рішення по використанню безлічі контролерів вимагає балансування навантаження і тоді проблема в цілому вирішується для мережі SDN. Базова концептуальна структура мобільної мережі 5G розгорнутої на базі SDN з мультиконтролерами показано на рис.1.12.

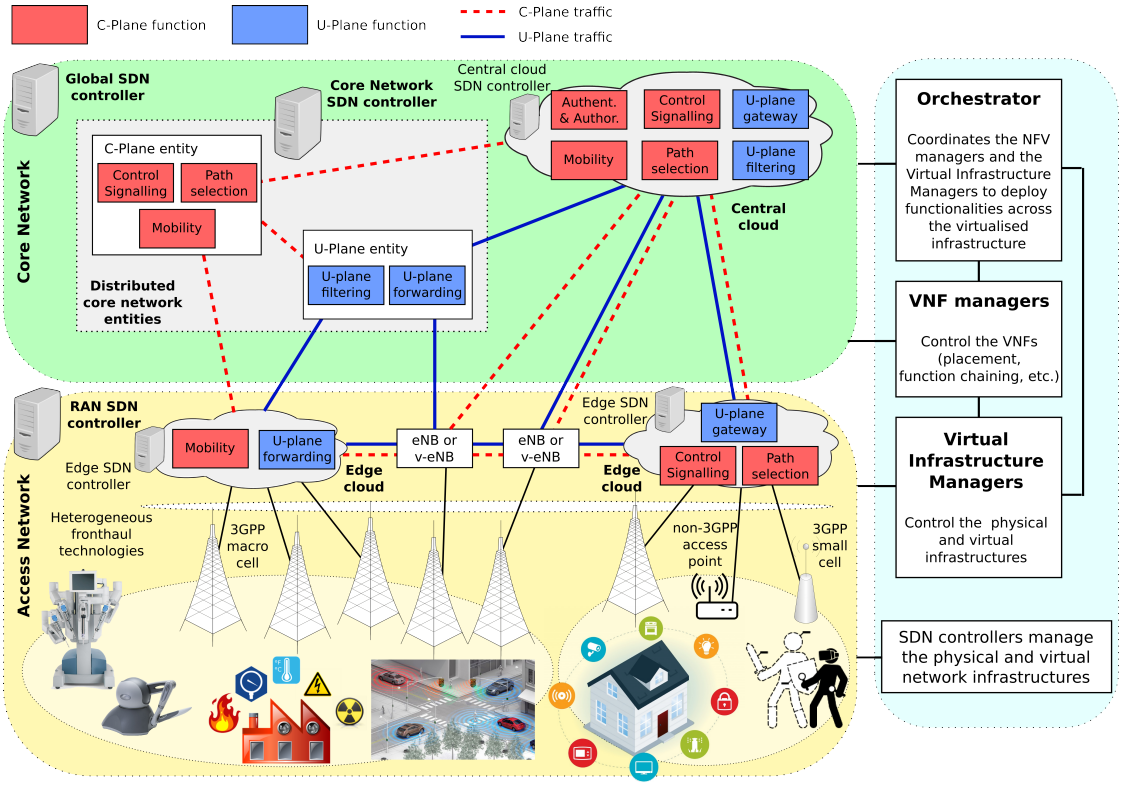


Рис. 1.12. Базова структура мобільної мережі 5G на базі SDN з мультиконтролерами [94]

Завдання розміщення контролерів полягає в тому, щоб розташувати контролери на мережі таким чином, щоб досягти різних необхідних цілей, включаючи, в першу чергу, зниження затримки, енергоефективність, балансування навантаження і підвищення надійності.

У роботі [95] пропонується алгоритм розвантаження даних та балансування навантаження на основі SDN в процесі інтеграції ліцензійного та неліцензійного діапазону Wi-Fi, щоб вирішити завдання з нестачею радіоспектру. Даний алгоритми використовує моніторинг функціонування мережі із допомогою контролера SDN, щоб досягнути зазначену вищу мету, враховуючи умови мережі та повторні запити QoS кінцевого користувача. Таким чином, рішення, засновані на SDN, знижують навантаження на мобільний зв'язок шляхом перерозподілу інформаційних потоків даних, забезпечуючи централізовану координацію та надійний контроль над структурою гетерогенної програмно-конфігурованої 5G мережі. Крім того, SDN контролер забезпечує ідеальну платформу для розробки оптимальних алгоритмів балансування навантаження. Концептуальна модель такої мережі показана на рис.1.13, яка містить базові станції 5G (BS) та точки доступу Wi-Fi (AP). BS використовують ліцензійний діапазон частот, тоді як точки доступу Wi-Fi використовують неліцензований діапазон.

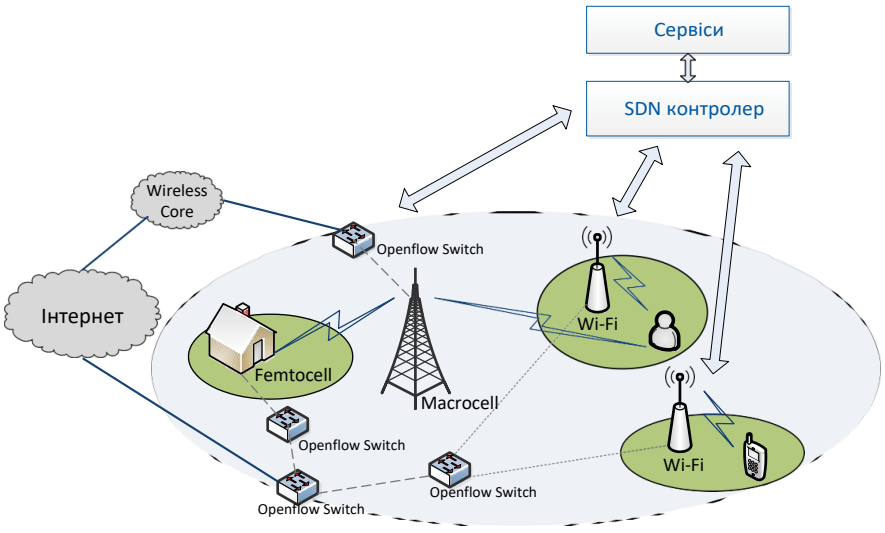


Рис. 1.13. Модель архітектури програмно-конфігурованої мережі 5G з Wi-Fi

Враховуючи різке зростання мобільного трафіку, обмежені спектральні ресурси та зростаючі мінливі вимоги до QoS, ефективне управління спектром та механізми розподілу стають важливим завданням для майбутніх безпровідних мереж повною мірою використовувати всі наявні ресурси спектру, підтримуючи при цьому підвищену швидкість передачі даних. Попередні рішення щодо спільного використання спектру, особливо такі, що базуються на когнітивному спектральному скануванні (когнітивне радіо), схильні до невірних рішень через невизначеності, що накладаються безпровідним середовищем. У поєднанні з великою залежністю від управління спектром на рівні пристроїв недоліки відштовхують мережевих операторів від прийняття ідеї спільного використання спектру. У роботі [96] запропоновано оркестрований підхід спільного використання спектру, який інтегрує розподілено розміщені приймачі UE/DTV, базові станції (БС), DTV станції та контролер програмно-конфігурованих мереж (SDN) в об'єднану мережу з обміном інформацією в реальному часі (рис.1.14).

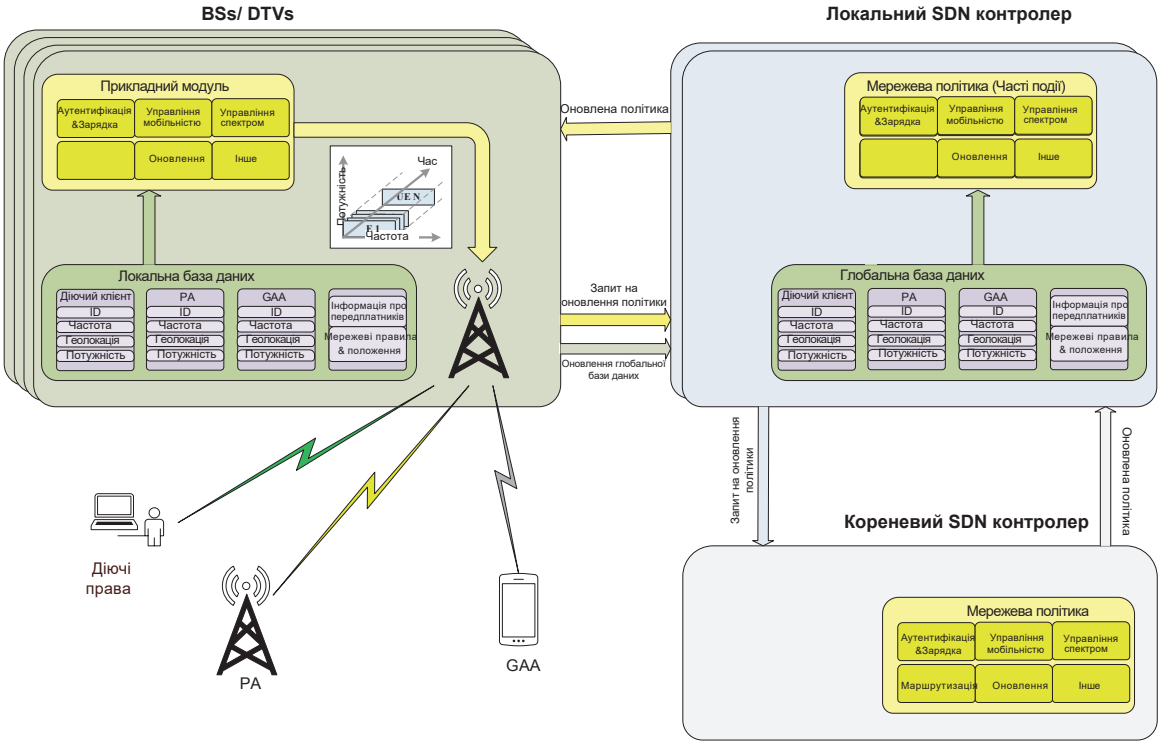


Рис. 1.14. Системна концептуальна модель 5G на основі SDN з підтримкою спільного використання спектра

Для адекватного захисту діючих користувачів DTV та ефективного розподілу об'єднаних ресурсів спектру, у роботі запропоновано 3D-інтерференційну кару в реальному часі, яка вважається орієнтувальною на доступ до спектру на основі глобального моніторингу з допомогою SDN. Також проведено моделювання в середовищі Matlab і перевірено ефективність застосування запропонованих рішень.

В роботі [97] запропонована архітектура мережі 5G з використанням технології програмно-конфігурованих мереж SDN для мереж з щільним розміщенням малих комірок. Використання концепції малих комірок призводить до частих хендоверів і, відповідно, затримки, пов'язаної з цим процесом. Автори пропонують рішення для подолання цих проблем за допомогою контролера SDN в ядрі мережі. Іншою важливою функцією контролера є розподіл ресурсів мережі радіодоступу і, відповідно, подолання проблем, пов'язаних з гетерогенністю мережі - використанням безлічі технологій радіодоступу. Контролер SDN при цьому забезпечує три типи програмованих інтерфейсів, які дають можливість запропонованій системі прогнозувати переміщення користувача і, таким чином, обробляти процедуру хендоверу за менший час.

Постійна мінливість трафіку, призводить до актуальності до адаптивної зміни числа задіяних на мережі контролерів, комутаторів, базових станцій та серверів. Коли трафік на мережі зростає, вузли повинні бути активовані, в той час як при зниженні трафіку навпаки. Частота зміни трафіку призводить до відповідного процесу активації і деактивації контролерів в мультиконтролерній мережі SDN. Сплячий режим може бути розглянутий як альтернативний варіант деактивації контролера [98]. Рішення про використання того чи іншого режиму для кожного з контролерів сприяє кращій продуктивності системи в цілому і може бути оптимізовано експериментальним шляхом.

Кожна з розглянутих вище робіт передбачає використання централізованого контролера в ядрі мережі, що вказує на майбутню трендовість

SDN. Всі ці запропоновані системи забезпечують високу ефективність мережі за швидкістю і затримкою передавання даних, проте із розглянутого переліку світових концептуальних моделей побудови інфокомунікаційної мережі майбутнього, у яких досі не враховано наміри користувача щодо індивідуалізації обслуговування та надання операторами замовленого рівня QoE в залежності від їх мінливих вимог, даючи змогу опосередковано впливати на конфігурацію мережі.

1.4. Огляд наукових робіт в напрямку вирішення проблем управління якістю надання сервісів та розвитку інфокомунікаційних мереж

На основі проведеного огляду останніх концептуальних моделей розвитку інфокомунікаційних мереж встановлено, що вони розвиваються в напрямку побудови гетерогенних інтелектуальних мереж, які поєднують в собі такі технології (рис.1.15) як NB-IoT, 5G, SDN, NFV, EC/CC, AI з метою створення майбутніх гетерогенних мереж нового покоління IBN [99-102].

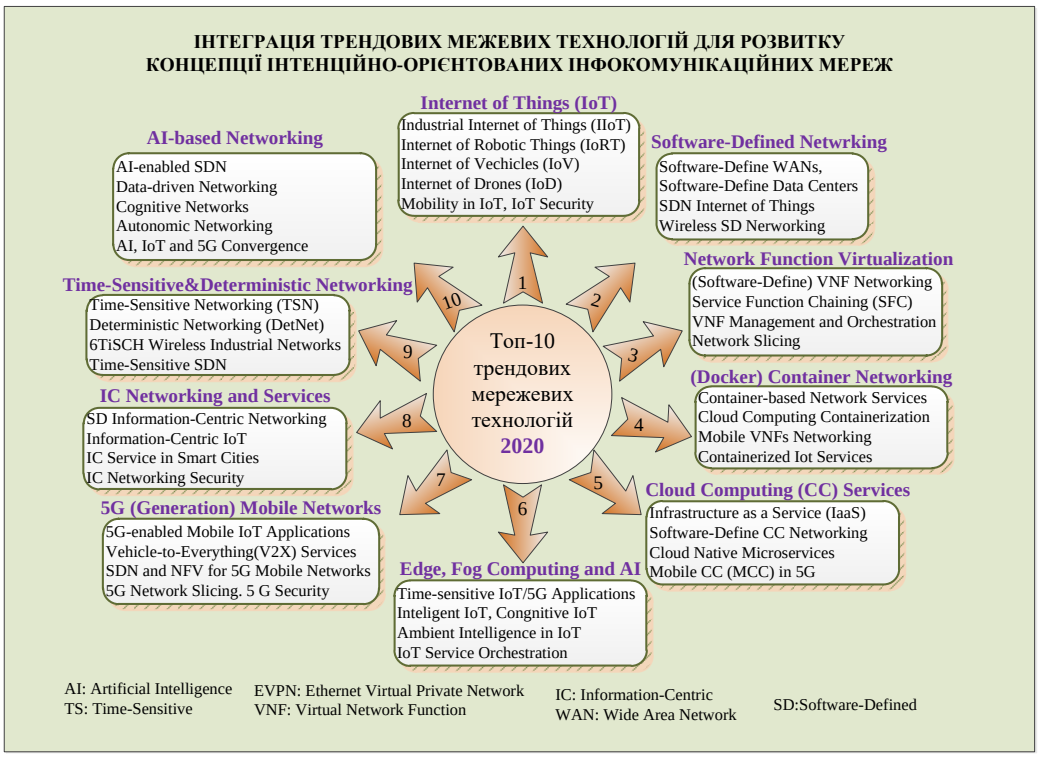


Рис.1.15. Інтеграція трендових межевих технологій для розвитку концепції інтенційно-орієнтованих інфокомунікаційних мереж

Інфокомунікаційна мережа на основі намірів є головним компонентом, який змінить спосіб роботи майбутніх мережевих інфраструктур із підтримкою SDN/NFV. Автономно керовані та самоадаптуючі мережі дадуть змогу використовувати можливості мереж 5G у нових бізнес-моделях та досягти безпрецедентного рівня ефективності надання послуг. Наміри відіграватимуть вирішальну роль у досягненні цього бачення нульового дотику до налаштування мереж, слугуючи механізмом, який формально визначає, що автономна система повинна робити. У такому контексті інтенційно-орієнтована мережа на основі намірів (intent-based networking, IBN) виникла як нова форма мережевого адміністрування, що дає змогу автоматизувати управління мережевими операціями та збільшити їх доступність. Концепція IBN пропонує адміністраторам мережі простий спосіб виразити свої бізнес-цілі, дозволяючи мережевому програмному забезпеченню автоматично досягати цих цілей. Намір покладається на функцію програмованості SDN для простого та гнучкого планування, проектування та експлуатації мереж, тим самим абстрагуючи складність мереж. Мережі, засновані на намірах, ставлять перед дослідниками нові завдання для дослідження, редизайну та розвитку мереж на базі SDN в еру 5G, що у свою чергу вимагає розробки нових методів управління якістю надання послуг, розподілу ресурсів, інженерії трафіку та мережевої безпеки. Для цього у роботі проведено огляд останніх релевантних наукових робіт в цьому напрямку.

1.4.1. Огляд наукових досліджень в напрямку майбутнього розвитку технології NB-IoT

Пандемія, яка сколихнула світ, наочно продемонструвала бізнесу, наскільки важливо мати рішення, які допомагають зменшити витрати, дозволяють працівникам працювати віддалено, замінювати ручну працю тощо. Багато таких ноу-хау пов'язані з використанням Інтернету речей (IoT). NB-IoT це безпровідна технологія Інтернету речей, яка надає користувачам великий

набір інструментів для оптимізації бізнес-процесів, зменшення експлуатаційних витрат за допомогою віддаленого моніторингу різних пристроїв.

Проект партнерства третього покоління (3GPP) [103-105], який визначає стандарти 5G зазначили, що NB-IoT буде частиною мереж 5G для масового розгортання сервісів Інтернету речей у найближчому майбутньому, проте із деякими відмінностями від сучасної технології NB-IoT, яка успішно розгортається в сьогоднішніх мережах LTE 4G. Це пов’язано із тим, що традиційна технологія NB-IoT/LTE не в змозі забезпечити вимоги щодо надійності чи затримки для критичних IoT сервісів. Не дивлячись на те, що більшість сьогоднішніх сервісів IoT не вимагають цих вимог, проте у ближчому майбутньому такі сервіси як тактильний та індустріальний Інтернет речей вимагатимуть затримки з кінця в кінець величиною в 10мс, що у свою чергу є найбільш складним завданням з точки зору IoT розгортання в мережах 5G.

У роботі [106] основна увага приділяється побудові імітаційної моделі NB-IoT на основі OPNET та тестуванню її характеристик в умовах високого навантаження на канали. Автори головним чином розглядають розробку та впровадження існуючої технології NB-IoT з точки зору характеристик фізичного рівня NB-IoT на основі LTE. Результати моделювання підтвердили продуктивність NB-IoT, де затримка висхідної лінії зв'язку менша 10с, використання каналу вище, ніж у мережі LTE, а зона покриття більша, ніж у мережі LTE. Також показано, що NB-IoT в сьогоднішньому вигляді не може використовуватися для критично важливих Інтернет-додатків через обмеження якості обслуговування. Якщо потрібно впровадити NB-IoT на основі мереж доступу LTE для критичних сервісів, потрібна модернізація NB-IoT.

Автори [107] систематично вимірюють фізичний рівень, а також перевіряють ефективність прикладного рівня. Особлива увага приділяється впливу радіопараметрів на прикладний рівень якості обслуговування. Робота досліджує послуги в режимі нереального часу через те, що існуюча технологія

NB-IoT не підходить для критично важливих сервісів, які вимагають низької затримки, і вимагає вдосконалення технології NB-IoT.

Нещодавно Чен та співавтори у [108] запропонували рішення щодо управління якістю послуг для IoT. Зокрема, автори вдосконалили алгоритм k-means для кластеризації пристроїв NB-IoT та встановлення пріоритету кластеру. Згідно пріоритетів, планувальник базової станції розподіляє сервіси IoT для завдань очікування в черзі. Недоліком такого рішення є складність реалізації в реальній мережі, оскільки даний підхід вимагає повного оновлення планувальника програмних ресурсів на базовій станції. Неясно, як це рішення вплине на роботу всієї мобільної мережі 5G.

1.4.2. Огляд наукових досліджень в напрямку розвитку методів планування, розподілу та формування рівня радіодоступу гетерогенних мереж нового покоління

На практиці, розгортання сучасних мереж мобільного зв'язку в умовах міста із щільною забудовою ускладнюється за рахунок неоднорідності абонентського навантаження та нерівномірного загасання сигналу, що порушує фіксовану геометричну структуру. Встановлення базових станцій за гексагональним шаблоном не дає змоги розрахувати оптимальний розмір комірок для забезпечення вимог до пропускної здатності. Тому, стохастична геометрія є більш прийнятним підходом до планування коміркових структур з випадковими параметрами [110-112]. Наразі немає оптимальних моделей, які б дали змогу аналізувати параметри багаторівневих гетерогенних мереж згідно мінливих вимог користувачів. Тому, подальші дослідження в даній області є необхідними для того щоб знайти ефективну модель для адаптивного планування та аналізу майбутніх гетерогенних мереж враховуючи вимоги користувачів щодо індивідуалізації обслуговування.

Енергоефективність майбутніх мереж мобільного зв'язку є важливим завданням для оператора, так як в гетерогенних мережах у порівнянні з

однорівневими з'являється велика кількість маленьких комірок [113-115]. Незважаючи на те, що вони малопотужні, сумарний рівень малих комірок споживає багато енергії [116]. Слід враховувати, що абонентське навантаження розподілено нерівномірно по площі. Більшість малих комірок взагалі не обслуговують абонентів [117]. У зв'язку з цим доцільно знизити енергоспоживання мережі, в результаті застосування нового методу адаптивного формування структури рівня радіодоступу на основі мінливих вимог користувачів, за допомогою якого малі комірки які не обслуговують абонентського навантаження, перейдуть в режим економії енергії, з можливістю швидкого переходу в нормальний режим при необхідності. Також шляхом завдання критеріїв обслуговування абонентів базовими станціями певного рівня досягається оптимальна конфігурація роботи мережі в залежності від поставлених цілей, серед яких може бути досягнення максимальної якості обслуговування і пропускної здатності мережі і т.д.

У роботах [118–120] автори аналізують енергоефективність базових станцій БС в гетерогенних мережах, що використовуються мультиоператорами. У роботі [118] автори використовують теорію розподілених ігор для економії енергії, де UE будь-якого оператора мобільної мережі обслуговуються іншим оператором мобільної мережі, а BS цих UE вимикаються. У роботі [119] автори пропонують спільну схему вимкнення БС, де БС вимикаються, коли навантаження на її трафік є низьким, а UE, що обслуговуються, можуть покриватися БС, що експлуатуються іншими операторами мобільної мережі. У роботі [120] автори пропонують рішення щодо ціноутворення та гру асоціації користувачів, засновану на взаємозв'язку між вартістю роумінгу та асоціацією користувачів. Для подальшого зменшення енергоспоживання в мережах 5G було запропоновано нову концепцію формування рівня радіодостпу, яка базується та адативно формується в залежності від мінливості навантаження створюваного користувачами [121].

Незважаючи на широке впровадження інтелектуальних інформаційних технологій для підвищення функціональної ефективності майбутніх інфокомунікаційних систем проблема адаптивного розподілу ресурсів за умови мінімізації енергозбереження при забезпеченні високої якості обслуговування користувачів все ще залишається невирішеною.

1.4.3. Огляд наукових досліджень в напрямку розвитку методів управління якістю надання послуг та трафіку інжинірингу

Автори роботи [122] представили основні виклики стосовно розвитку методів управління якістю надання послуг для майбутніх мереж, зосередившись на тих ключових факторах, які необхідні для остаточного перетворення управління мережею та сервісами на основі QoE користувачів у реальність.

Автори [123] запропонували уніфіковану систему оцінки якості, яка вимірює досвід користувачів практично для всіх типів мережевих послуг. По-перше, ця структура використовує модель машинного навчання (Random Forest) для класифікації мережевих служб, потім відбирає різні нелінійні вирази залежно від типу послуги та всебічно обчислює QoE за допомогою метрик QoS, включаючи затримку, втрату пакетів та пропускну здатність. Результати експериментів показують, що запропонований спосіб може застосовуватися майже до всіх видів мережевого трафіку. У роботі [124] Wahab та його колеги представили методологію, яка була адаптована для кількісної оцінки поширеної невизначеності QoE через статистичні помилки у вимірюванні параметрів QoS. Автори [125] запропонували евристичний, жадібний та QoE-орієнтований алгоритм розподілу ресурсів, беручи до уваги обмеження власного капіталу та загальну задоволеність користувачів, з метою максимізації прибутку операторів мобільного зв'язку при забезпеченні високоякісного досвіду (QoE). Запропонований алгоритм може справлятися з неоднорідним трафіком,

досягаючи значного прибутку та збільшуючи якість порівняно з найдосконалішими алгоритмами якості обслуговування.

Незважаючи на значний обсяг робіт з методу управління якістю послуг, вони в основному орієнтовані лише на технічні параметри якості обслуговування, тоді як сьогодні необхідні ефективні методи врахування мінливої думки клієнтів при управлінні якістю послуг даючи змогу враховувати їх наміри щодо переконфігурації мережі.

Маршрутизація в програмно-конфігурованих мережах нещодавно стала гарячою темою наукових досліджень. Дослідження, як правило, можна розділити на дві категорії залежно від цілей їх оптимізації. Один з них розглядає мережеву маршрутизацію з QoS як ціль оптимізації, а інший намагається уникнути потенційних перевантажень мережі або підвищити ефективність використання ресурсів мережі.

Традиційним децентралізованим методом балансування трафіку в пакетних мережах є використання протоколів динамічної маршрутизації [126]. Всі сучасні протоколи динамічної маршрутизації, такі як RIP, OSPF, IS-IS, EIGR, BGP, розраховують оптимальні шляхи проходження трафіку через мережу на підставі топологічних властивостей (група дистанційно-векторних протоколів) або властивостей каналів зв'язку (група протоколів, які враховують стан каналів) мережі, опираючись на математичний апарат алгоритмів найкоротших шляхів [127-129]. Дані протоколи здатні реагувати на втрату зв'язності в мережі, прокладаючи альтернативні маршрути, а деякі з них (наприклад, OSPF, EIGRP і BGP) дозволяють обмежено здійснювати балансування навантаження, при цьому в більшості випадків трафік розподіляється по шляхах, які мають рівні найкращі метрики [130]. Основною проблемою існуючих протоколів динамічної маршрутизації є прокладка шляхів без урахування поточного реального завантаження складових каналів зв'язку. В цьому випадку шляхи, які мають найкращу метрику, виявляються перевантаженими, тоді як альтернативні маршрути практично не

використовуються. Також варто відзначити досить відчутний період відновлення традиційної маршрутизації, що становить від 30 секунд до декількох хвилин [131], необхідних для виявлення втрати зв'язності і перестроювання маршруту. Така поведінка призводить до нераціонального використання наявної мережевої інфраструктури, збільшуючи нерівномірність розподілу трафіку в мережі.

Загальний напрямок розробок, що дає змогу розширити можливості традиційних протоколів маршрутизації і пом'якшити зазначені недоліки, отримав назву інжинірингу трафіку (Traffic Engineering, TE) [132], зокрема, що є актуально для майбутніх програмно-конфігурованих мереж. Методи інжинірингу трафіку спрямовані на збільшення продуктивності мережі, шляхом більш ефективного розподілу навантаження і дозволяють вибирати маршрути з урахуванням дотримання заданих умов QoS [133]. Математичною базою застосовуваних методів інжинірингу трафіку є потокові алгоритми на графах [135-137], що дають змогу знаходити оптимальні рішення при різних транспортних завданнях. Можна виділити дві основні групи розв'язуваних екстремальних задач:

– максимізація потоку, що проходить по мережі;

– мінімізація затримок проходження по мережі.

Перша група методів дозволяє підвищити продуктивність мережі, оптимально розподіляючи трафік за наявними маршрутами. Слід зазначити, що класичне розуміння інжинірингу трафіку ґрунтується саме на підходах оптимізації пропускної здатності мережі [138]. Методи другої групи забезпечують найменшу середню затримку, мінімізуючи завантаженість каналів мережі [139].

При використанні інжинірингу трафіку враховуються не тільки топологія мережі і пропускні здатності каналів, але також інтенсивність навантажень, що надходять в мережу, що вигідно відрізняє такі методи від простої маршрутизації по найкоротших шляхах. Для отримання відомостей про

інформаційні потоки використовуються спеціальні засоби, які здійснюють вимірювання завантаженості конкретних напрямків, розмірів надходжень пакетів, розподілу навантаження та інших параметрів [140]. Ґрунтуючись на зібраних даних про вхідний трафік мережі, вирішується оптимізаційна задача максимізації потоку, в результаті чого може бути здійснено ефективний розподіл навантаження в мережі. При цьому в якості вихідних умов задачі можуть виступати як усереднені статистичні дані, так і відомості про поточний стан мережі [141]. Одним із найбільш ефективних підхідів щодо маршрутизації потоків в програмно-конфігурованих мережах запропоновано у роботі [142], де автори розробили та реалізували модель централізованої детермінованої багатокритеріальної QoS (DMCQR) в середовищі Mininet для дослідження SDN. Результати експерименту показують, що запропонований алгоритм DMCQR має кращі показники з точки зору ефективного використання коефіцієнта завантаженості каналів, мінімізації втрат пакетів, пропускної здатності та наскрізної затримки в порівнянні з роботою алгоритму Дейсктри та із запропонованою багато шляховою маршрутизацією для SDN в роботі [143]. Розглянувши ряд робіт по маршрутизації вони все ще мають спільний недолік, а саме не можливість врахування мінливих намірів користувачів щодо замовленого рівня QoE, що є досить важливим для розвитку основних завдань трафіку інжинірингу у контексті реалізації майбутніх IBN.

1.4.4. Огляд наукових досліджень в напрямку розвитку методів виявлення мережевих аномалій та атак

Виявлення та класифікація аномалій передбачає безперервний процес моніторингу подій в інформаційних системах і мережах, у зв'язку з чим необхідна обробка великих обсягів даних, що генеруються цими джерелами. Для цього використовуються автоматизовані системи виявлення вторгнень у систему DPI [144]. DPI поєднує в собі функціональність системи виявлення вторгнень (IDS) та системи запобігання вторгненню (IPS) із традиційним

брандмауером із встановленим станом [145]. Ця комбінація дає змогу виявляти певні атаки, які IDS/IPS, не можуть виявити самостійно. Методи аналізу на основі сигнатур, що використовуються в сучасних системах виявлення вторгнень, призначені для виявлення відомих і точно описаних типів атак і не можуть виявити їх модифікації або нові типи, що робить використання таких систем неефективним. Наявні рішення для виявлення мережевих аномалій досі перешкоджали розробці єдиного універсального механізму виявлення раніше невідомих типів атак. DPI - це комерційні програмні продукти, які дозволяють аналізувати трафік на наявність аномалій та загроз у режимі реального часу. Обмежувальними факторами використання таких систем є висока вартість і закрита архітектура, що ускладнює їх адаптацію до організаційної інфраструктури.

На даний момент існує досить багато методів виявлення аномалій мережевого трафіку. Їх можна згрупувати наступним чином:

Методи на основі аналізу сигнатур. У сигнатурних методах системні події подаються у вигляді ланцюжків символів з деякого алфавіту. Суть цих методів полягає в завданні безлічі сигнатур атак у вигляді регулярних виразів (regular expressions) або правил на основі зіставлення зі зразком (pattern matching) і перевірці відповідності спостережуваних подій цим виразам. Типовими представниками систем, в яких реалізований такий метод, є Snort, SolarWind та Suricata. Основна перевага сигнатурного методу полягає в тому, що виявлення відомих зразків аномальних подій здійснюється максимально ефективно. Але в той же час використання бази сигнатур великого обсягу негативно впливає на продуктивність системи виявлення [146].

Нейронні мережі з використанням бази знань. Нейронні мережі вчаться виявляти аномалії протягом певного періоду, коли вся поведінка вважається нормальною. Після навчання нейронна мережа запускається в режимі розпізнавання. У ситуації, коли вхідний потік не розпізнає нормальну поведінку, атака реєструється. Таким чином, поєднавши дві різні нейронні

мережі, можна визначити та розпізнати інформаційні атаки з досить високим ступенем точності. Основними перевагами використання підходів, заснованих на нейронних мережах, є можливість адаптації до динамічних умов та показників продуктивності, що особливо важливо, коли система працює в режимі реального часу [147]. Недоліком є те, що розробка якісних баз знань вимагає великих зусиль та часу. Такі методи не можуть виявити рідкісну або невідому аномалію.

Імунні мережі. Виявлення аномалій є одним із можливих застосувань імунних методів. Оскільки кількість прикладів нормальної поведінки зазвичай на порядки перевищує кількість прикладів атак, використання імунних мереж для виявлення аномалій є більш обчислювально складним [148].

Експертні системи. Інформація про нормальну поведінку подається у таких системах у вигляді правил і моніторингової поведінки у вигляді фактів. На основі фактів та правил приймається рішення про те, чи є "відстежувана" поведінка "нормальною" чи є аномалія. Основним недоліком таких систем є висока обчислювальна складність (у загальному випадку). Зокрема, при виявленні аномалій [149].

Кластерний аналіз. Суть цієї групи методів полягає у розподілі набору спостережуваних векторів - властивостей системи на кластери, серед яких виділяються кластери нормальної поведінки. Кожен конкретний метод кластерного аналізу використовує власні метрики, що дозволяє оцінити, належить спостеріганий вектор властивостей системи до одного з кластерів чи поза відомими кластерами [150]. Більшість методів, заснованих на кластеризації, були запропоновані для обробки лише неперервних атрибутів. Припущення, що великі скупчення є нормою, а малі скупчення - аномалією. Якщо це не так, то робота методу важка. Використання невідповідної міри близькості об'єктів впливає на частоту помилкових тривог.

Статистичний аналіз. Ця група методів базується на побудові статистичного профілю поведінки системи протягом певного періоду "навчання", в якому поведінка системи вважається нормальною. Для кожного

параметра функціонування системи будується інтервал допустимих значень з використанням відомого закону розподілу. Далі, в режимі виявлення система оцінює відхилення спостережуваних значень від значень, отриманих під час тренування. Якщо відхилення перевищують деякі задані значення, реєструється аномалія (атака). Статистичний аналіз характеризується високим рівнем помилкових тривог при використанні в локальних мережах, де поведінка об'єктів не має плавного, усередненого характеру. Крім того, цей метод стабільний лише в межах певної системи, тобто побудовані статистичні профілі не можуть бути використані в інших подібних системах. Перевага цього підходу полягає в тому, що він не вимагає попередніх знань про властивості аномалій, і тому може бути ефективним при невідомих аномаліях і навіть при зміні існуючих відомих аномалій [151]. Одним із статистичних методів виявлення є метод, заснований на фрактальному аналізі [152].

Для більш ефективного виявлення нових атак у роботі запропонована модель виявлення аномалії з використанням вектора показника Херста та мультифрактального спектру [153]. Показано, що мультифрактальний аналіз показує чутливість до будь-яких відхилень властивостей мережевого трафіку в результаті аномалій. Запропоновані методи аналізу трафіку можуть бути ідеальними для захисту критично важливих даних та підтримки безперервності роботи Інтернет-послуг, включаючи IoT.

Використання описаних типів методів та систем виявлення аномалій дає змогу посилити політику безпеки та надати більшу гнучкість у процесі експлуатації мережевих ресурсів. Але будь-яка система має певні переваги, а також деякі недоліки. При аналізі роботи цих засобів виявляється, що більшість із них виконують лише одну або кілька специфічних функцій, які не можуть забезпечити в тій чи іншій мірі складності захисту інформації, що вимагається для майбутніх інфокомунікаційних мереж. В результаті проведеного аналізу методів і систем виявлення аномалій виділено, що лише завдяки поєднанню декількох методів і систем вдається досягти ефективного захисту та забезпечити протидію загрозам.

1.5. Формалізація вербальної моделі адаптивного управління якістю надання послуг та розподілом ресурсів для майбутніх інтенційно-орієнтованих мереж

Впровадження ефективних інформаційно-комунікаційних технологій (ІКТ) в усі сфери життя відіграє визначальну роль у поступальному розвитку України та покращення життя її громадян. Новітні ІКТ технології та інновації все більше проникають в усі сфери життя. Їх активне використання в бізнесі спричинене, перш за все, удосконаленням системи управління та контролю за бізнесом. Передусім це передбачає автоматизацію бізнес-процесів, таких як уведення електронного документообігу, організація відео та аудіо контенту, надання он-лайнових послуг населенню та клієнтам, що у свою чергу спричинило виникнення та поширення поняття «діджиталізації», як процесу перенесення інформації у цифрову форму. Нажаль, існуючі інформаційні системи та бізнес-процеси при цифровій трансформації перестають бути ефективними, старі методи комунікації зазнають перетворень, змінюються моделі та поведінка споживачів. Клієнтам все більш важливим стає адаптивне надання сервісу, постійний зв’язок, індивідуалізація пропозицій від компаній. Бізнес-організації, у свою чергу, зацікавлені у пошуку нових шляхів оптимізації власних бізнес-процесів та підвищенні ефективності й конкурентоспроможності [154].

В даний час відсутня єдина концепція створення системи управління мережевою інфраструктурою, а також відсутні чіткі стандарти управління перерозподілом мережних ресурсів. Сучасні моделі управління ресурсами, поряд з такими традиційними функціями як моніторинг і аналіз роботи телекомунікаційних мереж, повинні розв’язувати і такі важливі завдання як адаптивне управління розподілом і перерозподілом ресурсів в інфокомунікаційних системах в умовах їх обмеженості [155]. Актуальність даної проблеми обумовлена не тільки тим, що завжди в процесі функціонування мережі може виникнути конфлікт при зверненні кількох

користувачів до одного і того ж сервісного ресурсу, а й тим, що в будь-якій інфокомунікаційній мережі обов'язково рано чи пізно складається ситуація, коли мережні ресурси стають обмеженими і доводиться віддавати перевагу одному з сервісів. Обмеженість ресурсів може виникнути при появі та впровадженні нових сервісів без встановлення додаткових фізичних ресурсів (продуктивнішого серверного обладнання, маршрутизатора, комутатора), функціональної поломки або постановці на обслуговування серверів та мережного обладнання, підвищення вартості обслуговування та подальше зниження обсягів споживаних ресурсів, що надаються, наприклад, операторами телекомунікаційних послуг. Також тимчасове, але надмірне споживання ресурсів одним із сервісів, може призвести до підвищення завантаженості каналів зв'язку, мережевих пристроїв та серверів тощо. В процесі адаптивного управління ресурсами інфокомунікаційна система повинна керуватися значимістю всіх бізнес-процесів, що протікають в інфраструктурі корпоративних підприємств, відповідно, і типів сервісів, що відповідають за ефективність протікання самих бізнес процесів, а також аналізу пріоритетності виконуваних запитів щодо сервісного обслуговування та оцінкою їх потреб в загальних ресурсах інфокомунікаційної мережі. Природно, що в процесі повсякденної діяльності будь-якого корпоративного підприємства значущості бізнес-процесів можуть змінюватися. Ці зміни можуть бути обумовлені як факторами, що проявляються на організаційному рівні, зумовленими змінами бізнес-цілей підприємства, так і форс-мажорними непередбачуваними обставинами (зокрема поява пандемії 2020р. привела до значного росту інформаційного трафіку та нестачі ресурсів для його якісного обслуговування в у всіх класах мережної інфраструктури).

Таким чином, із розвитком бізнесу, різноманітності сервісів та вимог користувачів до якості обслуговування, концепція інтенційно-орієнтованих мереж виходить на перший план, як інструмент для інтелектуального управління інфокомунікаційними мережами, який дає змогу абстрагуватися від

деталей конфігурації і функціонування окремих елементів мережі та зосередитися на поведінці цілої мережі, як системи для надання сервісу відповідно до вимог та гарантування якості обслуговування на основі намірів користувачів. Основний принцип IBN полягає в перетворенні інформаційних бізнес-намірів користувачів до відповідних конфігурацій мережі для всіх пристроїв на основі мережної аналітики та машинного навчання [156].

Саме тому, важливим завданням як для гравців телекомунікаційного ринку так і для науковців націлених на розробку інтенційно-орієнтованих мереж є в першу чергу розроблення моделі адаптивного управління перерозподілом ресурсів інфокомунікаційних систем, в умовах обмеженості наявних мережних ресурсів при появі нових сервісних запитів, коли для свого виконання вони вимагають частини ресурсів, які вже використовуються іншими сервісами. Для цього модель повинна враховувати важливість бізнес сервісів, як тих, які виконуються, так і нових, а також можливість зміни в часі пріоритетів щодо виділення мережних ресурсів, зумовлених зміною значущості бізнес-процесів, які вони підтримують. Відповідно, нова модель управління ресурсами повинна мати можливість здійснювати діагностику та оцінювати функції і процедури бізнес процесів та їх взаємозв'язок, з метою раціонального управління мережними ресурсами адаптованих в контексті цілей розвитку самої інфраструктури.

Використання запропонованої моделі в системах управління функціонуванням інформаційно-комунікаційних систем дає змогу здійснювати ефективний розподіл і перерозподіл загальних ресурсів в процесі виникнення нових сервісів і зміні значимості їх бізнес-процесів. Запропонований формалізований підхід виділення ресурсів, що враховує мінливу значимість сервісів, може бути використаний в інтенційно-орієнтованих інфокомункаційних мережах нового покоління. Проте потрібно врахувати, що з розвитком інфокомунікаційних систем потреби клієнтів і їх поведінка змінилися. Центр уваги зміщується від підвищення продуктивності мережі для

отримання необхідних додаткових ресурсів, (зокрема для сервісів, що відповідають за важливі бізнес процеси) до покращення рівня якості сприйняття послуг користувачами (Quality of Experience, QoE) на основі наявних мережевих ресурсів шляхом раціонального управління ними. Таким чином у роботі пропонується поетапний перехід від традиційних угод про рівень послуг (Service Level Agreements, SLA) до нових угод про рівень очікуваної якості сприйняття послуг (Experience Level Agreements, ELA) [157] необхідних для реалізації концепції інтенційно-орієнтованих мереж.

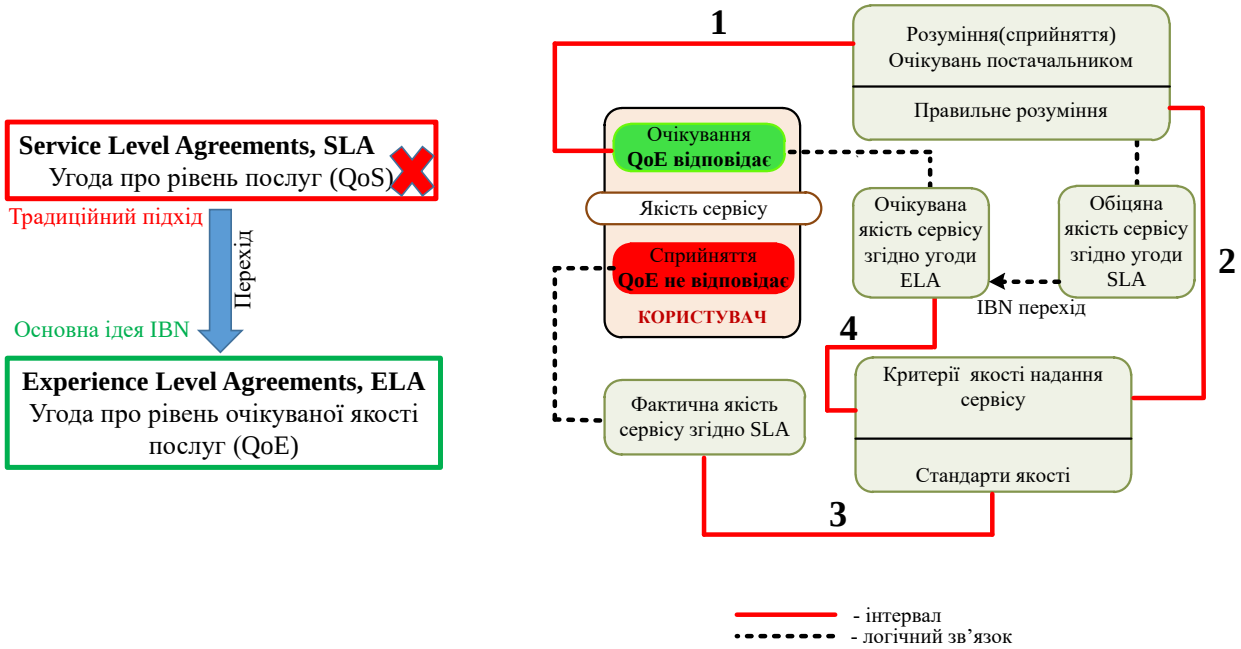


Рис. 1.16. Різниця між очікуваною і фактичною якістю послуг

При оцінці якості сприйняття послуги виділено чотири етапи (інтервали), що впливають на оцінку якості її надання, які можна визначити як інтервали між очікуваною і фактичною якістю сервісу. У даній роботі запропонована схема, що враховує відмінності між очікуваною і фактичною якістю надання послуг (див. рис. 1.16).

Перший інтервал - між очікуванням споживачем необхідної якості сервісу і сприйняттям даних очікувань постачальником сервісів. Якщо постачальник послуг не розуміє бажань і очікувань споживача, малоймовірно, що сервіс буде

наданий споживачу згідно його очікувань. Таким чином, потрібно, щоб постачальник послуг розумів бажання (наміри користувача), щоб сервіс був наданий споживачу згідно його очікувань.

Другий інтервал - між правильним розумінням очікувань споживача і критеріями якості надання сервісу, що надаються постачальником послуг з метою виправдати надії і очікування споживача. У такому випадку відбувається перехід від угод про рівень послуг (SLA) до угод про рівень очікуваної якості сервісу (ELA).

Третій інтервал - між стандартами якості і фактичною якістю сервісів, тобто здатністю постачальника надати необхідний рівень якості сервісів. Виконуючи вимоги, що пред'являються до надання сервісів, провайдер мережі повинен підтримати цей процес відповідними ресурсами. Де згідно існуючих рішень часто стандартні угоди SLA не виправдовують себе щодо очікуваного рівня якості сприйняття сервісу. Таким чином, використовуючи IBN мережі відбувається перехід до угод про рівень очікуваної якості сервісу та відповідно формується четвертий інтервал.

Четвертий інтервал - між очікуваною замовленою якістю користувача щодо отримання необхідного рівня якості сприйняття сервісу і наданою мережею якістю сервісу на основі намірів користувача.

Відповідно, основною перешкодою до широкого впровадження угод ELA для концепції інтенційно-орєнтованої мережі є відсутність єдиного погляду на питання формування вхідного математичного опису систем оцінювання QoE на основі відомих критеріїв QoS для різноманітних інфокомунікаційних сервісів та недослідженість проблеми оптимізації пов’язаних з цим витрат і відповідно отриманого прибутку.

Відповідно, більшість науковців стверджують, що в процесі проектування мереж нового покоління, у тому числі IBN необхідно зосередитись на виборі кількості показників якості обслуговування, які враховуються при синтезі мережі. Кількість часткових параметрів, які характеризують якість

функціонування реальної системи, може бути дуже різноманітною та великою. Це означає, що чим більша кількість часткових параметрів якості враховується при оптимізації інфокомунікаційних мереж, тим більш досконалою буде така система. Саме тому на практиці існує оптимальна кількість параметрів якості, яку необхідно враховувати. Введення додаткових параметрів якості призводить не до покращення, а до погіршення результатів оптимізації інфокомунікаційних мереж нового покоління. Проте більшість сучасних мереж враховують стандартні параметри якості обслуговування, для проведення оптимізації кожен, з яких має свої допустимі значення згідно встановлених рекомендацій електрозв'язку. Зміна парадигми в концепції надання послуг, яка була пов'язана із загальною зміною функціонування стандартних мереж в напрямку розвитку концепції IBN, виражається в першу чергу в тому, що ролі оператора і користувача значно змінилися. Тепер користувач і оператор виступають як союзники в єдиному процесі інформатизації, і таку взаємодію можна вважати еволюцією сучасних методів надання послуг.

Таким чином, при розробці нової системи управління якістю надання інформаційних послуг логічно використовувати системний підхід: проблема забезпечення якості повинна вирішуватися не ізольовано, а в межах взаємодії з користувачем. Задоволення вимог користувачів включає в себе як технічні (параметри якості функціонування мережі), так і нетехнічних (суб'єктивне сприйняття кінцевими користувачами) аспекти. В процесі адаптивного управління послугами необхідно контролювати як відповідність характеристик послуг нормативним показникам, так і, при необхідності, вносити адаптивні корективи в норми.

Таким чином, виходячи з вищевикладеного, формування якості послуги включає в себе як об'єктивну оцінку мережевих характеристик, так і суб'єктивну експертну оцінку користувача. І якщо параметри роботи мережі можуть бути визначені із застосуванням відповідного обладнання, то з урахуванням сприйняття користувачами якості отримуваних послуг, це

проводиться за допомогою співвідношення QoS, пропонованого оператором, і QoS, яка сприймається клієнтом, або QoE.

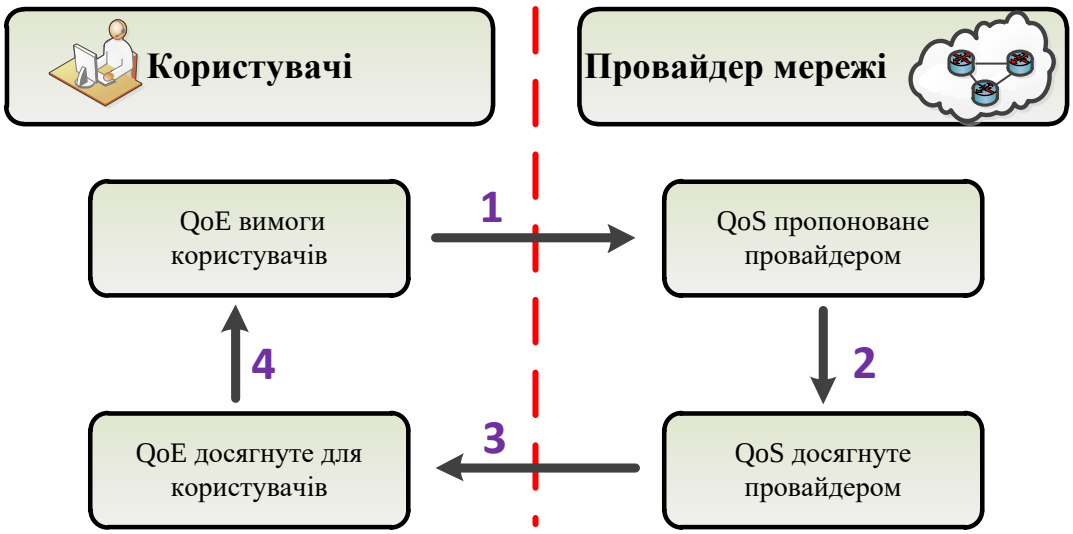


Рис.1.17. Співвідношення між точками зору замовника та постачальника на якість послуги

В цей час в мережі обов'язково має працювати пристрій, що здійснює порівняння різниці між необхідним рівнем якості і реально наданим мережевим провайдером, і якщо в процесі порівняння виявляється відхилення від допустимого значення, то за допомогою контрольних сигналів повідомляється про необхідність трансформації мережі. Мережа повинна пам'ятати і аналізувати стан мережі і відповідну оцінку якості обслуговування клієнтом, а також вміти налаштовувати конфігурацію мережі на основі накопиченого досвіду. Даний підхід може бути реалізований шляхом введення алгоритмів машинного навчання підкласу штучного інтелекту в систему управління послугами, що і є основною ідеєю IBN. Таким чином, конфігурація мережі і функціональність мережевого обладнання автоматично змінюються в залежності від мінливих вимог користувача. Мережа не тільки реагує на поточні запити користувача, але також аналізує його переваги і поточне оточення, надаючи відповідну інформацію контролеру мережі, що відповідає за централізоване управління всією мережею.

Також важливим є технологічна трансформація архітектурних моделей побудови інфокомунікаційних систем із використанням трендових мережевих технологій, зокрема основною із яких є технологія програмно-конфігурованих мереж, даючи змогу буквально програмувати і перепрограмувати мережі в реальному часі для задоволення конкретних потреб бізнесу і вимог користувачів в міру їх виникнення.

1.6. Постановка науково-прикладної проблеми, формулювання завдань та основних етапів дисертаційного дослідження

На сьогоднішній час створено і експлуатується велика кількість інфокомунікаційних систем управління мережами, які дають змогу узагальнити результати їх роботи і виділити загальні для них переваги та недоліки. Проте, одним із важливих спільних недоліків є те, що постійно поглиблюється розрив між зростаючими універсальними можливостями систем управління і реальними вимогами щодо адаптивного управління якістю обслуговування, орієнтованими на конкретні сервіси користувачів. Розв’язання всього комплексу завдань адаптивного надання сервісів в умовах змін значущості бізнес-процесів складно реалізувати на основі реалізації управління за допомогою існуючих методів та мережевих технологій, оскільки зміна критеріїв оптимальності керуючих рішень вимагає постійного експертного та адміністративного втручання. Показано, що в основному всі відомі методи управління якістю обслуговування відносяться до локального керування трафіком та мережевими ресурсами. В їх основу покладено переважно децентралізовані алгоритми та механізми управління ресурсами, що реалізуються на окремих вузлах мережі. Крім того, в процесі управління не координуються рішення, отримані на окремих рівнях мережевих вузлів.

Отже, виникло технічне протиріччя між тенденцією збільшення топологічної, експлуатаційної, функціональної складності мереж рівня радіодоступу, транспорту та розподілених систем в умовах зростання обсягів

інформації, і відсутністю науково-практичного обґрунтованого концептуального підходу до управління такими мережами, орієнтованих на адаптивне надання сервісів, зокрема, що вимагаються з боку мінливих бізнес-процесів користувачів. В процесі аналізу функціональності існуючих інфокомунікаційних систем (рис. 1.18), встановлено, що вони характеризуються відсутністю таких основних принципів, як програмованість, централізованість, відкритість та абстракція, а також відсутністю нових методів, моделей, засобів, алгоритмів та систем моніторингу необхідних для переходу до IBN мереж нового покоління з можливістю автоматичної конфігурації мережі та адаптації під мінливі вимоги користувачів щодо якості надання послуг.

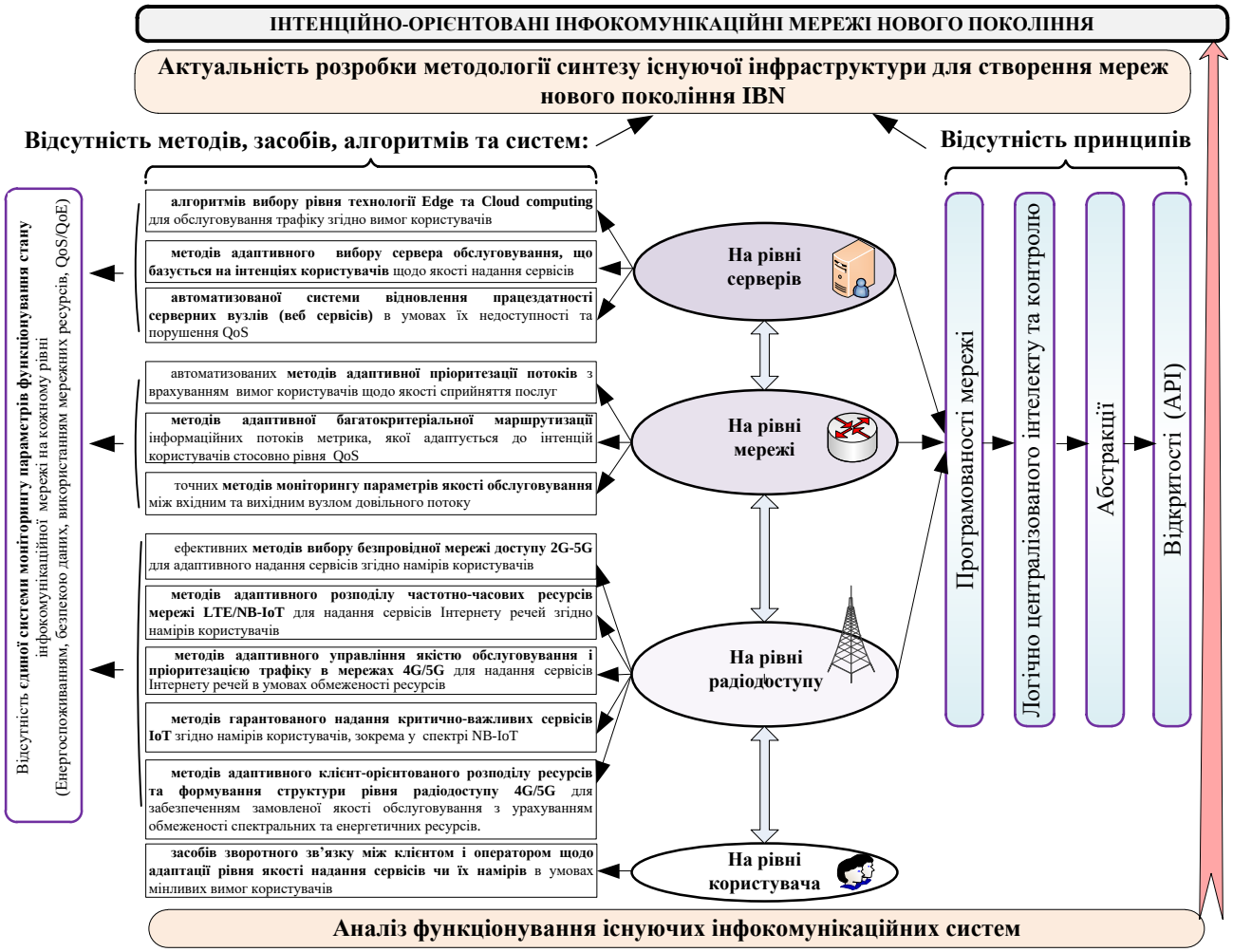


Рис. 1.18. Актуальність розробки методології синтезу існуючої інфраструктури для розвитку інтенційно-орієнтованих мереж нового покоління

Таким чином, актуалізується проблематика розроблення методології аналізу та синтезу складних гетерогенних інфокомунікаційних систем з метою створення нової програмно-конфігурованої інтенційно-орієнтованої мережі, яка постійно на основі мінливих вимог користувачів щодо якості надання сервісів та розгортання інфраструктури навчається, адаптується, автоматизується і захищається від потенційних кібератак шляхом використання нових методів розподілу ресурсів, інженерії трафіку, мережевої аналітики та існуючих алгоритмів машинного навчання.

Вирішення цієї проблеми дасть змогу досягти мети дисертаційного дослідження підвищення ефективності функціонування інформаційно-комунікаційних систем шляхом розроблення методів і моделей адаптивного управління мережевими ресурсами та якістю надання сервісів у контексті реалізації основних ідей концепції інтенційно-орієнтованих мереж нового покоління.

Для досягнення вказаної мети необхідно розв’язати ряд окремих систематизованих завдань:

1. Провести аналіз існуючих методів і моделей управління ресурсами та якістю обслуговування у сучасних інформаційно-комунікаційних мережах.
2. Розробити математичну модель визначення суб’єктивного рівня задоволеності користувача за оцінкою QoE в залежності від зміни показників мережі QoS.
3. Розробити потокову модель енергоефективної QoE-маршрутизації для інтенційно-орієнтованих мереж.
4. Розробити метод адаптивного клієнт-орієнтованого управління якістю надання послуг для IBN мереж.
5. Розробити інтелектуальну DPI систему моніторингу та аналізу трафіку для автоматизованого виявлення аномалії і запобігання атак в інтенційно-орієнтованих мережах.

6. Розробити методи розподілу частотно-часових ресурсів та балансування навантаження в гетерогенній мережі LTE/NB-IoT для адаптивного надання сервісів Інтернету речей.

7. Розробити адаптивний інтенційно-орієнтований метод розподілу ресурсів та формування структури рівня радіодоступу 4G/5G.

8. Розробити імітаційну модель інтенційно-орієнтованої гетерогенної мережі мобільного зв'язку.

9. Розробити методологію синтезу інтенційно-орієнтованої інфокомунікаційної мережі.

10. Провести практичну реалізацію та оцінювання ефективності запропонованих рішень на основі розроблених прототипів програмно-конфігурованої інтенційно-орієнтованої мережі корпоративного сегменту.

Процес реалізації системного аналізу для вирішенні сформульованої проблеми можна охарактеризувати послідовністю виконання основних етапів дисертаційного дослідження (рис. 1.19).

Рис. 1.19. Основні етапи дисертаційного дослідження

На етапі аналізу здійснюється детальне опрацювання інформаційно-комунікаційної системи, яка включає:

1. Структурно-функціональний аналіз існуючої системи, що дає змогу сформулювати вимоги до нової системи IBN. Він включає уточнення складу і закономірностей функціонування окремих елементів мережі, алгоритми функціонування та взаємодії підсистем (елементів), поділ керованих і некерованих характеристик функціонування, завдання просторово-часової локалізації користувачів та стану мережі, кількісних та часових параметрів QoS, аналіз цілісності системи, формування вимог до створюваної нової системи.

2. Аналіз аналогів, опис тенденцій мережевого розвитку і невизначеностей різного виду.

3. Аналіз ефективності результатів, використання ресурсів, своєчасності та оперативності. Аналіз включає в себе формування індикаторів і критеріїв ефективності, оцінку результатів.

4. Формулювання вимог до нової інформаціно-комунікаційної системи, формулювання критеріїв для оцінки і обмежень.

На етапі декомпозиції складної інфокомунікаційної гетерогенної мережі здійснюються:

1. Побудова концептуальної моделі майбутньої інфокомунікаційної системи. Сюди входить: певний математичний апарат, блочність і системність побудови.

2. Розкладання системи (проблеми) на окремі підсистеми (завдання).

3. Виділення системи із середовища за критерієм участі кожного елемента інформаційно-комунікаційної системи в процесі, що приводить до шуканого результату на основі розгляду системи в якості складової частини надсистеми.

4. Визначення впливаючих чинників на функціональність системи.

Рівень декомпозиції визначається виходячи з поставленої мети дослідження. Декомпозиція складної інфокомунікаційної гетерогенної мережі

здійснюється у вигляді підсистем, які являють собою послідовне (каскадне) з'єднання елементів, паралельне з'єднання елементів і з'єднання елементів зі зворотним зв'язком, зокрема із рівнем намірів користувачів щодо індивідуалізації обслуговування та адаптивного надання сервісів.

На етапі синтезу:

1. Створюється концептуальна модель майбутньої інфокомунікаційної системи. Сюди входить: моделювання, оцінювання моделі на адекватність, ефективність, похибки, баланс між складністю і точністю, різні варіанти імітаційної реалізації.

2. Проводиться синтез альтернативних структур підсистеми, що дають змогу вирішити проблему [158].

3. Проводиться синтез різних параметрів системи, з метою усунути проблему.

4. Проводиться оцінка варіантів синтезованої системи з обґрунтуванням самої схеми оцінки, обробкою результатів і вибору найефективнішого рішення;

5. Оцінка ступеня вирішення проблеми здійснюється при завершенні системного синтезу, формується методологія аналізу та синтезу.

На етапі реалізації:

1. Відбувається реалізація та тестування концептуальної моделі майбутньої інфокомунікаційної системи шляхом використання специфічного обладнання технології програмно-конфігурованих мереж та автоматизації запропонованих управлінських рішень шляхом написання програмного забезпечення.

2. Оцінка ефективності запропонованих рішень.

У майбутньому розроблена нова інфокомунікаційна система на основі технології IBN дасть змогу автоматизувати управління всіма доменами мережі, включаючи кампуси, філії, WAN, Інтернет речей, 5G та Big Data, забезпечуючи істотно новий рівень автоматизації, підвищуючи ефективність обслуговування, швидкість запуску інновацій та надійність роботи мережевої інфраструктури.

1.7. Висновки до 1-го розділу

1. Проведено аналіз сучасного стану проблеми управління якістю надання сервісів в інформаційно-комунікаційних мережах. Встановлено, що з розвитком інфокомунікаційних систем вимоги користувачів і їх поведінка змінилися. Центр уваги зміщується від підвищення продуктивності мережі до покращення якості сприйняття послуг. Зокрема, для кінцевих бізнес-користувачів все більш важливим стає адаптивне надання сервісу та індивідуалізація обслуговування.

2. Встановлено, що головна проблема традиційних інформаційно-комунікаційних систем є використання пропрієтарного обладнання, яке унеможливлює автоматизоване внесення змін щодо функціонування мережі напрямленої на мінливі потреби користувачів, без втручання адміністратора. Частковим вирішенням даної проблеми є перехід на програмно-конфігуровані мережі, які дають змогу реалізувати централізований, програмований рівень управління інфраструктурою та абстракцію рівня даних. Проте існуючі програмно-конфігуровані мережі характеризуються рядом недоліків, щодо переходу до повної автоматизації та проведення гнучкості управління ресурсами на основі мінливих бізнес вимог користувачів, вирішення яких можливе з використанням алгоритмів машинного навчання та нових методів управління мережею, що дасть змогу створити інтенційно-орієнтовані мережі нового покоління, які базуються на намірах користувачів.

3. Аналіз напрацювань вітчизняних та зарубіжних учених підтверджує актуальність тематики роботи як в Україні, так і за її межами. Проте, існуючі науково-теоретичні методи та технічні рішення є або концептуальними та важко реалізованими, або зосередженні лише в межах стандартизованої функціональності SDN, що не дають змоги в комплексі вирішити проблему синтезу та реалізації інтенційно-орієнтованих мереж, які повинні одночасно забезпечувати, інтелектуальне управління мережею, необхідні параметри якості обслуговування та безпеку даних в умовах обмеженості мережевих ресурсів та постійної потреби реінжинірингу інформаційних бізнес процесів користувачів

РОЗДІЛ 2. МОДЕЛІ ПОБУДОВИ ПРОГРАМНО-КОНФІГУРОВАНИХ ІНТЕНЦІЙНО-ОРІЄНТОВАНИХ МЕРЕЖ З АДАПТИВНИМ УПРАВЛІННЯМ ЯКІСТЮ НАДАННЯ СЕРВІСІВ

2.1. Концептуальна модель гетерогенної програмно-конфігурованої інтенційно-орієнтованої мережі

У роботі запропоновано концептуальну модель гетерогенної програмно-конфігурованої інтенційно-орієнтованої мережі, яка, на відміну від існуючих, дає змогу забезпечити ефективний розподіл і перерозподіл загальних ресурсів адаптуючись під мінливі вимоги бізнес-користувачів щодо якості надання сервісів. Головна ідея пропонованої концепції IBN полягає у зміні парадигми мережевої інфраструктури: тепер не користувач зі своїм додатком підлаштовується під можливості мережі, а мережа змінює свої налаштування з урахуванням вимог користувача. Забезпечення згідно намірів користувачів заданого рівня QoE послуг стає фундаментальною проблематикою для реалізації наскрізного керування ресурсами у концепції IBN. Таким чином, для розроблення нової системи адаптивного управління якістю надання інформаційних послуг у роботі використано системний підхід, зокрема проблема забезпечення якості вирішується не ізольовано операторами мереж, а у тісній взаємодії із користувачами послуг. Для цього IBN контролер аналізує стан мережі і відповідні замовлені QoE оцінки користувачів, що характеризують певний рівень якості обслуговування, а також автоматизовано налаштовує конфігурацію мережі на основі накопиченого досвіду та розроблених нових методів розподілу ресурсів і інженерії трафіку на кожному рівні концептуальної мережі. Даний підхід реалізовується шляхом введення алгоритмів машинного навчання підкласу штучного інтелекту в систему управління послугами. Таким чином, конфігурація мережі і функціональність мережевого обладнання автоматично змінюються в залежності від мінливих вимог користувача. Для цього концептуальна модель гетерогенної IBN мережі

базується на принципах централізованості, програмованості, абстракції та відкритості, використовуючи технології SDN, NFV, SDR, Big Data, IoT та Cloud computing. Концептуальна модель побудови інтенційно-орієнтованої інфокомунікаційної мережі з адаптивним управлінням якістю надання сервісів для національного оператора мобільного зв'язку показано на рис.2.1

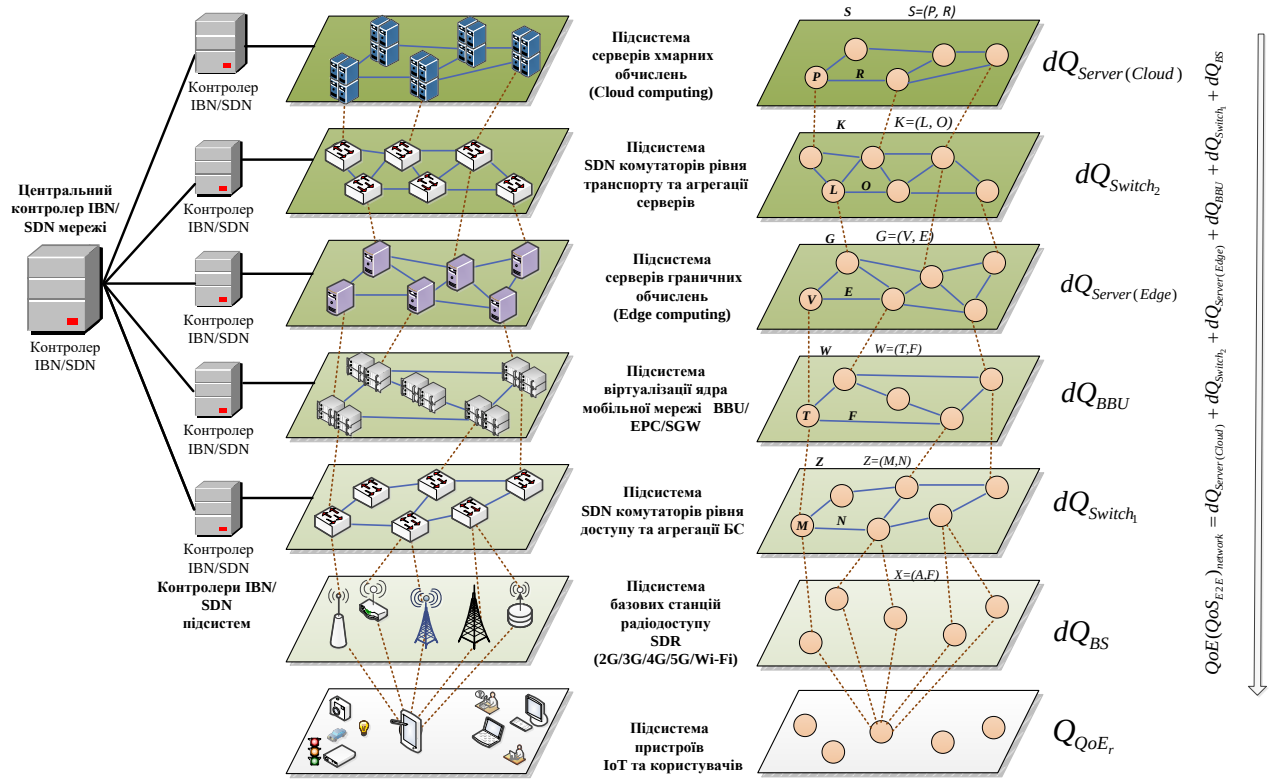


Рис. 2.1. Модель побудови інтенційно-орієнтованої інфокомунікаційної мережі з адаптивним управлінням якістю надання сервісів для оператора мобільного зв'язку

Сценарії обслуговування користувача у гетерогенній мережі нового покоління IBN формально можна описати наступним чином. Є множина N корпоративних сервісів $\phi : \phi = \{S_1, S_2, ..., S_N\}$, набір Θ, що є множиною бізнес-сервісів користувачів, які надаються провайдерами $\Theta : \Theta = \{P_1, P_2, ..., P_w\}$, та набір F, що складається із множини i користувачів $F : F = \{User_1, User_2, ..., User_i\}$. Кожен користувач може використати N різних мереж, що належать набору $X : X = \{D_1, D_2, ..., D_N\}$ для доступу до одного чи більшого числа інформаційних

сервісів, з певним замовленим рівнем якості обслуговування Q_{QoE_r}. Користувач $User_i$ під час сесії m у системі може бути уявлений кортежем:

$$c_{\langle m,i,QoE_r,w,N\rangle} = \left\langle m, User_i, S_N, \{P_1, P_2, ..., P_w\}, D_N, Q_{QoE_r} \right\rangle. \quad (2.1)$$

Значення $c_{\langle m,i,QoE_r,w,N\rangle}$ розуміється наступним чином: впродовж сесії номер m, користувач $User_i$ має доступ до послуг через мережу D_N, отримуючи сервіси S_N відповідно до набору $\{P_1, P_2, ..., P_w\}$, із замовленою якістю Q_{QoE_r}. Цей формалізм (2.1) пропонується використати для двох фундаментальних цілей необхідних для блоку знань контролера IBN мережі, зокрема для опису, представлення і контролю поведінки користувача у гетерогенній мережі та для отримання даних про зміну профіля користувача за критерієм замовленого рівня якості обслуговування шляхом дослідження аспектів його активності у мережі та інтуїтивного пояснення його поведінки.

До того ж наведена модель обслуговування користувача (1) у IBN мережі дає змогу інтуїтивно формалізувати кластери користувачів з однотипними вимогами щодо якості обслуговування Q_i на основі алгоритмів машинного навчання, зокрема за допомогою методу кластеризації *k*-середніх. Таким чином, для користувачів, що входять до певного кластеру $UC_{iCluster_{QoEr}}$ формується IBN/SDN контролером своя політика конфігурації мережі у вигляді програмного коду для адаптивного управління ресурсами та забезпечення необхідної якості надання послуг.

У загальному випадку *інтегральний показник якості надання послуг* Q пов'язаний певною залежністю з частковими показниками q_i, які також можуть перебувати у функціональній залежності один з одним:

$$F = Q(q_1, q_2, ..., q_i, ..., q_n). \quad (2.2)$$

Нехай у заданій залежності (2.2) всі часткові показники є незалежними змінними. Відповідно, вплив часткових показників на комплексний показник якості формалізується у вигляді повного диференціалу функції Q:

$$dQ = \frac{\partial Q}{\partial q_1} dq_1 + \frac{\partial Q}{\partial q_2} dq_2 + ... + \frac{\partial Q}{\partial q_i} dq_i + ... + \frac{\partial Q}{\partial q_n} dq_n . \quad (2.3)$$

Часткові похідні перед значеннями dq_i розглядаються як вагові коефіцієнти часткових показників якості $q_1, q_2, ..., q_i, ..., q_n$, пов'язаних функціональною залежністю з комплексним показником Q. Вираз $\partial Q_i / \partial q_i$ показує, як змінюється якість послуг Q при зміні часткового показника якості q_i (при фіксованих значеннях інших показників). На підставі викладеного формалізується вираз:

$$w_i = \left. \frac{\partial Q}{\partial q_i} \right| q_i = q_{i0,} \;\; i = \overline{(1,n)} , \quad (2.4)$$

де w_i – ваговий коефіцієнт і-го часткового показника якості.

Відповідно, рівняння (2.3) записується у вигляді комплексного показника якості надання послуг:

$$dQ = w_1 dq_1 + w_2 dq_2 + ... + w_i dq_i + ... + w_n dq_n . \quad (2.5)$$

Рівняння (2.5) є наслідком лінеаризації функції Q в точці, координати якої $q_i = q_{i0}$, $i = (1,n)$.

$$w_i = f_i(q_1, q_2, ..., q_i, ...q_n) . \quad (2.6)$$

З виразу (2.6) видно, що коефіцієнти ваги w_i виражені з (2.4), є функціями багатьох змінних часткових показників якості q_i. У випадках, коли значення q_i задані, чисельні значення w_i визначаються шляхом підстановки в рівняння (2.5) конкретних значень часткових показників якості.

Відповідно, систему диференціальних рівнянь для адаптивного інтенційно-орієнтованого управління якістю надання послуг в концептуальній гетерогенній IBN мережі оператора мобільного зв’язку (рис. 2.1) формалізовано у вигляді (2.7):

$$
\begin{cases}
dQ_{Server(Cloud)} = \dfrac{\partial Q_{Server(Cloud)}}{\partial q_1} dq_1 + \dfrac{\partial Q_{Server(Cloud)}}{\partial q_2} dq_2 + ... + \dfrac{\partial Q_{Server(Cloud)}}{\partial q_i} dq_i + ... + \dfrac{\partial Q_{Server(Cloud)}}{\partial q_x} dq_x; \\
dQ_{Switch2} = \dfrac{\partial Q_{Switch_2}}{\partial q_1} dq_1 + \dfrac{\partial Q_{Switch_2}}{\partial q_2} dq_2 + ... + \dfrac{\partial Q_{Switch_2}}{\partial q_i} dq_i + ... + \dfrac{\partial Q_{Switch_2}}{\partial q_y} dq_y; \\
dQ_{Server(Edge)} = \dfrac{Q_{Server(Edge)}}{\partial q_1} dq_1 + \dfrac{Q_{Server(Edge)}}{\partial q_2} dq_2 + ... + \dfrac{Q_{Server(Edge)}}{\partial q_i} dq_i + ... + \dfrac{Q_{Server(Edge)}}{\partial q_n} dq_n; \\
dQ_{BBU} = \dfrac{Q_{BBU}}{\partial q_1} dq_1 + \dfrac{Q_{BBU}}{\partial q_2} dq_2 + ... + \dfrac{Q_{BBU}}{\partial q_i} dq_i + ... + \dfrac{Q_{BBU}}{\partial q_z} dq_z; \\
dQ_{Switch1} = \dfrac{\partial Q_{Switch_1}}{\partial q_1} dq_1 + \dfrac{\partial Q_{Switch_1}}{\partial q_2} dq_2 + ... + \dfrac{\partial Q_{Switch_1}}{\partial q_i} dq_i + ... + \dfrac{\partial Q_{Switch_1}}{\partial q_m} dq_m; \\
dQ_{BS} = \dfrac{\partial Q_{BS}}{\partial q_1} dq_1 + \dfrac{\partial Q_{BS}}{\partial q_2} dq_2 + ... + \dfrac{\partial Q_{BS}}{\partial q_i} dq_i + ... + \dfrac{\partial Q_{BS}}{\partial q_v} dq_v; \\
QoE(QoS_{E2E})_{network} = dQ_{Server(Cloud)} + dQ_{Switch2} + dQ_{Server(Edge)} + dQ_{BBU} + dQ_{Switch1} + dQ_{BS}; \\
QoE(QoS_{E2E})_{network} \approx Q_{QoE_r}.
\end{cases}
\quad (2.7)
$$

З рівняння (2.7) випливає, що для забезпечення замовленого користувачем рівня якості обслуговування Q_{QoE_r} (в IBN ідеології розуміється, як інтенція користувача), необхідно, централізовано, гнучко, адаптивно та узгоджено управляти якістю обслуговування $dQ_{Server(Cloud)}, dQ_{Switch2}, dQ_{Server(Edge)}, dQ_{BBU}, dQ_{Switch1}, dQ_{BS}$ на кожному із рівнів концептуальної IBN мережі (рис. 2.1), забезпечуючи замовлену наскрізну якість обслуговування $QoE(QoS_{E2E})_{network}$. Де QoE – це суб'єктивна оцінка послуги на прикладному рівні користувачем, який користується сервісом. QoS – це набір технологій мережевого та канального рівнів, використання яких дають змогу ефективніше використовувати ресурси мережі, особливо під час потокових видів трафіку для забезпечення необхідного рівня QoE.

Виходячи із вищенаведеної концептуальної моделі побудови мережі, аналогічно можна забезпечити адаптивне управління якістю надання послуг для операторів провідного зв'язку, забираючи при цьому підсистеми: базових станцій радіодоступу SDR (2G/3G/4G/5G/Wi-Fi), SDN комутаторів рівня доступу та агрегації БС, підсистема віртуалізації ядра мобільної мережі BBU/EPC/SGW. Модель побудови інтенційно-орієнтованої мережі з

адаптивним управлінням якістю надання сервісів для оператора провідного зв'язку показано на рис.2.2.

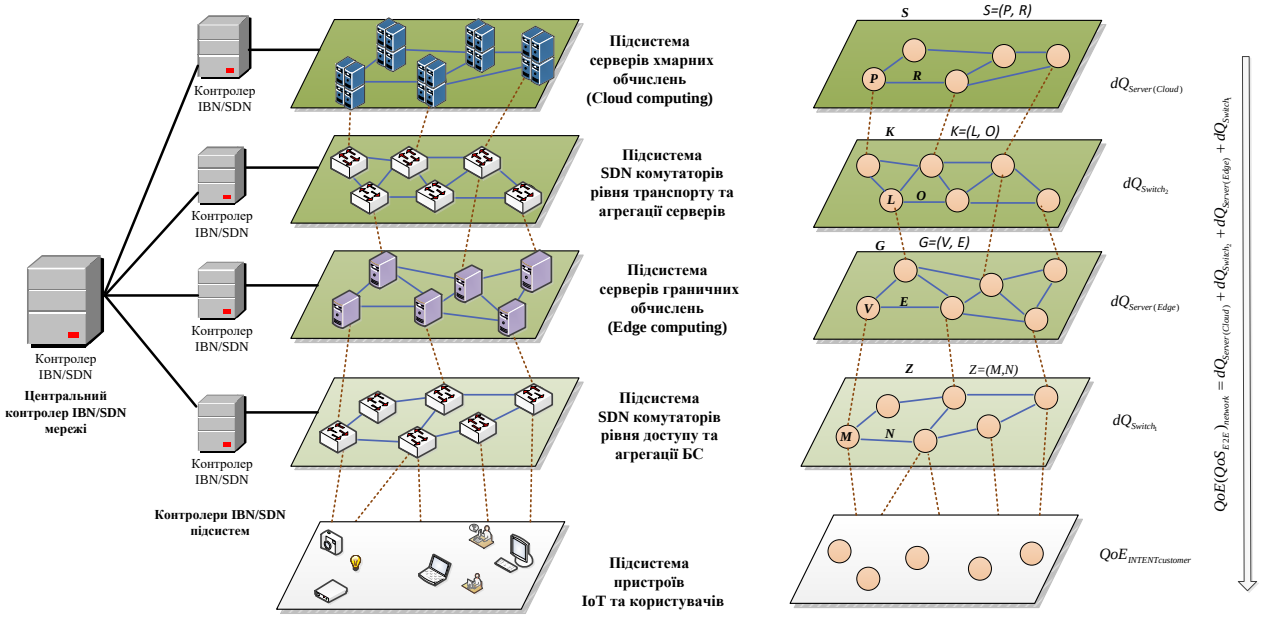


Рис. 2.2. Модель побудови інтенційно-орієнтованої мережі з адаптивним управлінням якістю надання сервісів для оператора провідного зв'язку

Відповідно, систему диференціальних рівнянь для адаптивного інтенційно-орієнтованого управління якістю надання послуг в концептуальній IBN мережі для оператора провідного зв'язку (рис. 2.2) формалізовано у вигляді (2.8):

$$\begin{cases} dQ_{Server(Cloud)} = \dfrac{\partial Q_{Server(Cloud)}}{\partial q_1} dq_1 + \dfrac{\partial Q_{Server(Cloud)}}{\partial q_2} dq_2 + \ldots + \dfrac{\partial Q_{Server(Cloud)}}{\partial q_i} dq_i + \ldots + \dfrac{\partial Q_{Server(Cloud)}}{\partial q_x} dq_x; \\ dQ_{Switch2} = \dfrac{\partial Q_{Switch_2}}{\partial q_1} dq_1 + \dfrac{\partial Q_{Switch_2}}{\partial q_2} dq_2 + \ldots + \dfrac{\partial Q_{Switch_2}}{\partial q_i} dq_i + \ldots + \dfrac{\partial Q_{Switch_2}}{\partial q_y} dq_y; \\ dQ_{Server(Edge)} = \dfrac{Q_{Server(Edge)}}{\partial q_1} dq_1 + \dfrac{Q_{Server(Edge)}}{\partial q_2} dq_2 + \ldots + \dfrac{Q_{Server(Edge)}}{\partial q_i} dq_i + \ldots + \dfrac{Q_{Server(Edge)}}{\partial q_n} dq_n; \\ dQ_{Switch1} = \dfrac{\partial Q_{Switch_1}}{\partial q_1} dq_1 + \dfrac{\partial Q_{Switch_1}}{\partial q_2} dq_2 + \ldots + \dfrac{\partial Q_{Switch_1}}{\partial q_i} dq_i + \ldots + \dfrac{\partial Q_{Switch_1}}{\partial q_m} dq_m; \\ QoE(QoS_{E2E})_{network} = dQ_{Server(Cloud)} + dQ_{Switch2} + dQ_{Server(Edge)} + dQ_{Switch1}; \\ QoE(QoS_{E2E})_{network} \approx Q_{QoE_r}. \end{cases} \quad (2.8)$$

Аналогічно модель побудови інтенційно-орієнтованої мережі корпоративного класу з адаптивним управлінням якістю надання сервісів наведено на рис.2.3.

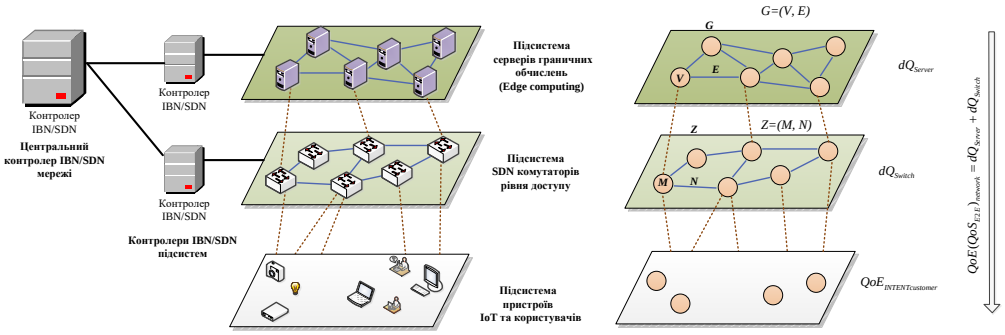


Рис. 2.3. Модель побудови інтенційно-орієнтованої мережі корпоративного класу з адаптивним управлінням якістю надання сервісів

Відповідно, систему диференціальних рівнянь для адаптивного інтенційно-орієнтованого управління якістю надання послуг в інтенційно-орієнтованої мережі корпоративного класу формалізовано у вигляді (2.9):

$$\begin{cases} dQ_{Server} = \dfrac{\partial Q_{Server}}{\partial q_1} dq_1 + \dfrac{\partial Q_{Server}}{\partial q_2} dq_2 + \ldots + \dfrac{\partial Q_{Server}}{\partial q_i} dq_i + \ldots + \dfrac{\partial Q_{Server}}{\partial q_n} dq_n; \\ dQ_{Switch} = \dfrac{\partial Q_{Switch}}{\partial q_1} dq_1 + \dfrac{\partial Q_{Switch}}{\partial q_2} dq_2 + \ldots + \dfrac{\partial Q_{Switch}}{\partial q_i} dq_i + \ldots + \dfrac{\partial Q_{Switch}}{\partial q_m} dq_m; \\ QoE(QoS_{E2E})_{network} = dQ_{Switch} + dQ_{Server}; \\ QoE(QoS_{E2E})_{network} \approx Q_{QoE_r}. \end{cases} \quad (2.9)$$

Таким чином, формується твердження, що з розвитком інфокомунікаційних систем потреби користувачів і їх поведінка змінилися. Центр уваги у контексті ідеології IBN зміщується від підвищення продуктивності мережі до покращення рівня сприйняття якості обслуговування QoE, який прямо пропорційно залежить від комплексного показника якості надання сервісу QoS, що визначається параметрами пропускної здатності, затримки, втрат та джитеру пакетів. Для реалізації послуг з прийнятним QoE необхідно дослідити вплив характеристик якості надання сервісу QoS з кінця в кінець на саму послугу, що дають змогу описати закони розподілу характеристики QoS і їхній вплив на параметри QoE (час встановлення з'єднання, час реакції на виконання команди, завмирання зображення, розбиття зображення, синхронізацію зображення та голосу, чіткість та розбірливість звуку).

2.2. Математична модель визначення суб’єктивного рівня задоволеності користувача за оцінкою QoE в залежності від зміни об’єктивних показників якості обслуговування QoS

У цьому підрозділі роботи проведено дослідження впливу технічних параметрів якості обслуговування в процесі передавання відео та аудіо потоків реального часу на рівень якості сприйняття сервісу кінцевим користувачем, визначеного шляхом використання методу експертного оцінювання за 5-бальною QoE шкалою. Представлені різні випадки, коли погіршення якості обслуговування може відбуватися під час потокової передачі мультимедійних програм, проводячи експерименти на спеціальній SDN топології мережі. Погіршення якості обслуговування спостерігається через обмеження, накладені умовами мережі, а також через нестабільність мережі, таку як збій зв'язку. Експерименти мають на меті проілюструвати безліч випадків, коли QoE в мережі страждає від деградації внаслідок стану мережі, а також вказати на необхідність розробки системи моніторингу QoS параметрів для пошуку математичної моделі кореляції QoS/QoE з метою реалізації QoE маршрутизації в майбутніх програмно-конфігурованих IBN мережах.

Для проведення дослідження стосовно впливу параметрів QoS на якість сприйняття відео та аудіо потоків реального часу побудовано експериментальну схему програмно-конфігурованої мережі (рис.2.3) у середовищі Mininet. Зокрема для цього на реальному клієнті (h1) та сервері (h2) запущено VLC плеєр для трансляції та перегляду відеопотоку реального часу . Для проведення цього дослідження було написано Python скрипт рис.2.4, що дає змогу змінювати параметри з’єднань між комутатором та хостами. Серед цих QoS параметрів: пропускна здатність, затримки, втрати, довжина черги. Шляхом зміни цих параметрів можна дослідити їх вплив на якість сприйняття послуги [105].

В даній експериментальні мережі існує два шляхи при передаванні даних від хоста1(h1) до хоста2(h2).

```python
class SingleSwitchTopo( Topo ):
    "Single switch connected to n hosts."
    def build( self, n=2 ):
        switch = self.addSwitch( 's1' )
        for h in range(n):
            # Each host gets 50%/n of system CPU
            host = self.addHost( 'h%s' % (h + 1),
                                 cpu=.5/n)

                # 100 Mbps, 1ms delay, 0% loss, 1000 packet queue
            self.addLink( host, switch, bw=100, delay='1ms', loss=0,
                          max_queue_size=1000, use_htb=True )

def myNetwork():
    topo = SingleSwitchTopo( n=1)
    net = Mininet( topo=topo,
                   host=CPULimitedHost, link=TCLink )

    print "*** Starting network"

    # Add NAT connectivity
    net.addNAT().configDefault()
    net.start()
    print "*** Hosts are running and should have internet connectivity"
    print "*** Type 'exit' or control-D to shut down network"

    CLI( net )
    # Shut down NAT
    net.stop()

if __name__ == '__main__':
    lg.setLogLevel( 'info')
    myNetwork()
```

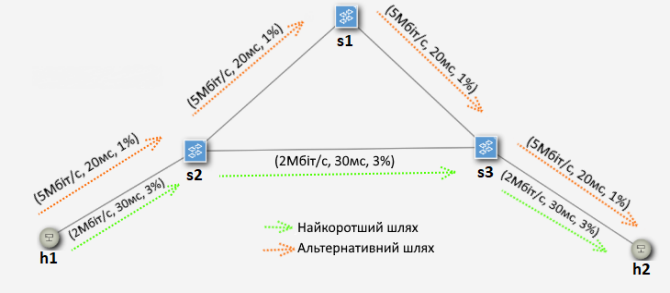


Рис. 2.4. Код Python скрипта для конфігурації каналів зв'язку з різними параметрами QoS

Розглянемо один із прикладів впливу QoS параметрів на якість сприйняття відео. Зокрема у роботі проведено порівняння процесу передавання відеопотоку через два шляхи, що забезпечують різні параметри QoS:

– Шлях №1 (h1-s2-s3-h2) - пропускна здатність – 2 Мбіт/с, затримка – 30 мс, штучні втрати пакетів – 3% та розмір буферу – 700 пакетів;

– Шлях №2 (h1-s2-s1-s3-h2) - пропускна здатність – 5 Мбіт/с, затримка – 20 мс, штучні втрати пакетів – 1% та розмір буферу – 850 пакетів.

При передаванні відеопотоку через Шлях №1, тобто найкоротшим шляхом, отримано наступну якість зображення, яка згідно власного експертного оцінювання описується рівнем сприйняття послуги за шкалою QoE=2.

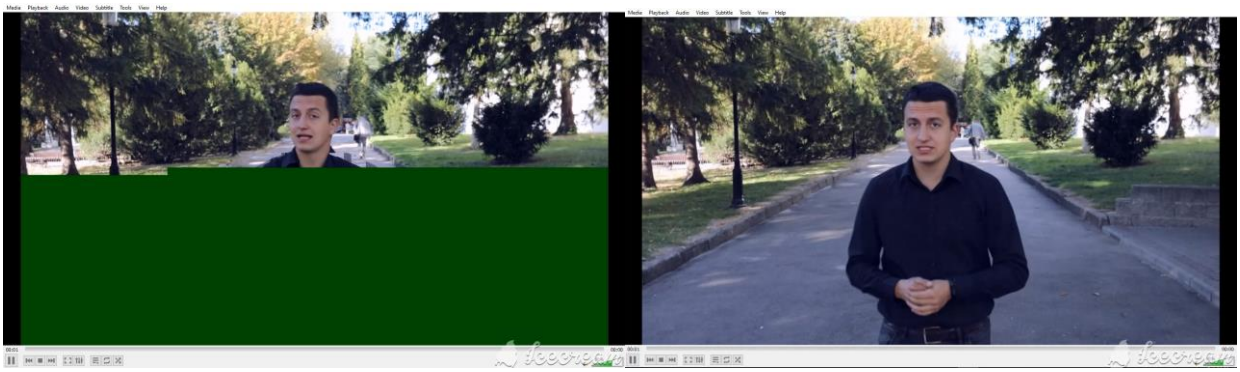


Рис. 2.5. Отримана якість відео при змінених параметрах каналу зв'язку

Таким чином шляхом проведення значної кількості експериментів було знайдено певну залежність між параметрами QoS та якістю сприйняття QoE. Виходячи із вищезазначеного у роботі розвинуто математичну модель [159] визначення суб'єктивного рівня задоволеності користувача за оцінкою QoE в залежності від зміни об'єктивних показників якості обслуговування QoS, що забезпечуються в IBN/SDN мережі, зокрема для відео та аудіо сервісів реального часу. Формування математичної моделі QoS/QoE кореляції здійснено на основі отриманих результатів від власного експериментального дослідження проведеного на реальному SDN обладнанні.

Таблиця 2.1

Оцінка QoS параметрів та їх влив на рівень QoE при перегляді відеопотоку реального часу визначеного методом експертного оцінювання

QoS параметр	добре	допустимо	погано
Затримка, *T*	<150 мс	150–200 мс	>200 мс
Джиттер, *J*	0–20 мс	20–50 мс	>50 мс
Втрати, *P*	0–1%	1-2%	>2%
Пропускна здатність, *C*	>2 мбіт/с	1–2 мбіт/с	<1 мбіт/с
Оцінка QoE	5–4	3.5–4	<3.5

Для того, щоб математично визначити відхилення параметрів якості QoS в оцінці QoE, потрібна нормалізація процедури розрахунку QoS. Для цього у роботі визначено еталоні мінімальні значення параметрів QoS та завантаженості вузла при яких забезпечується висока якість сприйняття досліджуваного відео потоку. Також в процесі дослідження встановлено рівень важливості QoS параметрів та параметра завантаженості вузла при перегляді відео у вигляді таблиці 2.2

Таблиця 2.2

Рівень важливості параметрів QoS

QoS параметр	Рівень важливості	Ваговий коефіцієнт
Втрата пакетів, *P*	15 %	0.15
Джиттер пакетів, *J*	25 %	0.25
Затримка пакетів, *T*	20 %	0.20
Пропускна здатність, *C*	18%	0.18
Завантаженість вузла, *L*	22%	0.22

Нормалізоване значення інтегрального адитивного критерію якості розраховується за формулою (2.10):

$$Q = QoS(X) = 1 - (w_1(\frac{P_{min}}{P}) + w_2(\frac{T_{min}}{T}) + w_3(\frac{C}{C_{max}}) + w_4(\frac{J_{min}}{J}) + w_5(\frac{L}{L_{max}})), \quad (2.10)$$

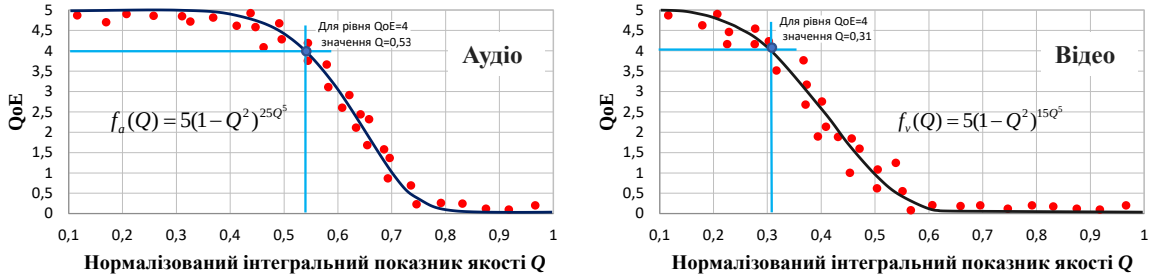
де w_1, w_2, w_3, w_4, w_5,- вагові коефіцієнти важливості параметрів $QoS(X)$, що змінюються в діапазоні від 0 до 1, і їх сума повинна дорівнювати одиниці.

Математичну модель кореляції рівня задоволеності користувача за оцінкою QoE для аудіо (2.11) та відео (2.12) сервісів в залежності від зміни інтегрального критерію параметрів QoS, представлено у вигляді функцій:

$$QoE_{audio} = f_a(Q) = 5(1-Q^2)^{25Q^5}. \ ; \quad (2.11)$$

$$QoE_{video} = f_v(Q) = 5(1-Q^2)^{15Q^5}. \quad (2.12)$$

Відповідно, графіки функцій (2.11) та (2.12) показано на рис.2.6.



а) б)

Рис. 2.6. Графічна модель визначення суб'єктивного рівня задоволеності користувача за оцінкою QoE в залежності від зміни об'єктивних показників якості обслуговування QoS для аудіо – а) та відео – б) сервісів реального часу

Таким чином, завдання забезпечення замовленого рівня якості сприйняття послуги користувачами згідно оцінок QoE, що вказують важливість сервісу для конкретного бізнес процесу полягатиме у пошуку необхідно нормалізованого значення інтегрального адитивного критерію QoS, розв'язання якого можна здійснити шляхом адаптивного управління мережними ресурсами та їх раціонального перерозподілу, зокрема одним із таких підходів є розроблення багатокритеріальної адаптивної маршрутизації потоків даних, метрика якої, базуватиметься на цьому ж інтегральному адитивному критерію.

2.3. Потокова модель енергоефективної QoE-маршрутизації для інтенційно-орієнтованих мереж

Багатокритеріальний підхід маршрутизації інформаційних потоків є ключовим у запропонованій концептуальній моделі IBN мережі, який дає змогу адаптивно призначати шлях пересилання даних з кінця в кінець з урахуванням параметрів QoS та QoE намірів користувачів.

Таким чином, у роботі запропоновано потокову модель енергоефективної QoE-маршрутизації для інтенційно-орієнтованих мереж, яка, на відміну від відомих, для вибору оптимального шляху даних використовує адаптивну QoE-орієнтовану метрику маршруту, що автоматизовано розраховується централізованим контролером мережі на основі вище розробленої математичної моделі кореляції QoS/QoE із врахуванням функціональних параметрів завантаженості мережевих вузлів, що дало змогу підтримувати компроміс між бажаною інтенційно-орієнтованою якістю обслуговування користувачів, завантаженістю та енергоефективністю мережі шляхом переведення в енергозберігаючий режим незадіяних вузлів.

Для змістовного розуміння процесу маршрутизації розглянемо структуру IBN мережі зв'язку, що складається з N мережевих вузлів [160]. Чисельні значення метрики каналів зв’язку $metrics_{(i,j)}$ представляються у вигляді матриці суміжності $A^{metrics}$ як:

$$A^{metrics} = \begin{bmatrix} metrics_{1,1} & \cdots & metrics_{1,N} \\ \vdots & \ddots & \vdots \\ metrics_{N,1} & \cdots & metrics_{N,N} \end{bmatrix}. \tag{2.13}$$

Варто зазначити, що матриця параметрів $A^{metrics}$ не є симетричною $(metrics_{(i,j)} \neq metrics_{(j,i)})$. Мінімізація цільової функції $metrics_{(i,j)}$ на яку можуть бути накладені кілька обмежень або граничних значень є задачею багатокритеріальної оптимізації, яка розв’язується IBN контролером з використанням методу інтегрального критерію оптимальності. Для цього як нормуючі дільники в цій задачі приймемо найкращі значення часткових критеріїв, що характеризують QoS:

– для кількості втрачених пакетів інформаційного потоку:

$$P_{N\times N}^{A^{metrics}} = \begin{bmatrix} P_{1,1} & \dots & P_{1,N} \\ \dots & \dots & \dots \\ P_{N,1} & \dots & P_{N,N} \end{bmatrix},\ P_{i,j} \in [0,1],\ P_{i,j} = \frac{S_{i,j}}{R_{i,j}}. \tag{2.14}$$

де $S_{i,j}$ – кількість прийнятих пакетів, $R_{i,j}$ – кількість переданих пакетів в матриці суміжності $A^{metrics}$ та $S_{i,j}, R_{i,j} > 0$.

– для часу затримки пакетів інформаційного потоку:

$$T_{N\times N}^{A^{metrics}} = \begin{bmatrix} T_{1,1} & \dots & T_{1,N} \\ \dots & \dots & \dots \\ T_{N,1} & \dots & T_{N,N} \end{bmatrix},\ T_{i,j} \in [0,1],\ T_{i,j} = \frac{t_{min}}{t_{i,j}}. \tag{2.15}$$

де t_{min} – мінімальне значення затримки в матриці суміжності $A^{metrics}$, і $t_{min}, t_{i,j} > 0$.

– для пропускної здатності каналу:

$$C_{N\times N}^{A^{metrics}} = \begin{bmatrix} C_{1,1} & \dots & C_{1,N} \\ \dots & \dots & \dots \\ C_{N,1} & \dots & C_{N,N} \end{bmatrix},\ C_{i,j} \in [0,1],\ C_{i,j} = \frac{C_{i,j}}{C_{max}}. \tag{2.16}$$

де C_{max} – максимальна пропускна здатність в матриці суміжності $A^{metrics}$ та $C_{max}, C > 0$.

– для джитера пакетів інформаційного потоку:

$$J_{N\times N}^{A^{metrics}} = \begin{bmatrix} J_{1,1} & \dots & J_{1,N} \\ \dots & \dots & \dots \\ J_{N,1} & \dots & J_{N,N} \end{bmatrix}, J_{i,j} \in [0,1],\ , J_{i,j} = \frac{jt_{min}}{jt_{i,j}}. \tag{2.17}$$

де jt_{min} – мінімальне значення джитера в матриці суміжності $A^{metrics}$, і $jt_{min}, jt_{i,j} > 0$.

– для завантаженості мережевого вузла:

$$L_{N\times N}^{A^{metrics}} = \begin{bmatrix} L_{1,1} & \dots & L_{1,N} \\ \dots & \dots & \dots \\ L_{N,1} & \dots & L_{N,N} \end{bmatrix}, L_{i,j} \in [0,1]\ , J_{i,j} = \frac{L_{i,j}}{L_{max}}. \tag{2.18}$$

де L_{max} – максимальна завантаженість вузла в матриці суміжності $A^{metrics}$ та $L_{max}, L > 0$.

Значення інтегрального адитивного критерію розраховується для кожного каналу зв'язку між вершинами *i* та *j*. Таким чином, метрика каналів зв'язку на основі п'яти параметрів матиме вигляд (2.19), та є тотожною до виразу (2.10):

$$metrics_{i,j} = 1 - (w_1 \cdot (P_{i,j}) + w_2 \cdot (T_{i,j}) + w_3 \cdot (C_{i,j}) + w_4 \cdot (J_{i,j}) + w_5 \cdot (L_{i,j})), \quad (2.19)$$

де w_1, w_2, w_3, w_4, w_5, – вагові коефіцієнти, що змінюються в діапазоні від 0 до 1, і їх сума повинна дорівнювати одиниці.

Змінюючи значення вагових коефіцієнтів в метриці $metrics_{i,j}$, ми, тим самим, створюємо апарат для адаптивного управління значимістю того чи іншого параметра метрики в підсумковій оцінці каналу даних від вузла *i* до вузла *j*, що є важливим для забезпечення різного рівня якості обслуговування. Вартість маршруту (загальна адаптивна метрика шляху QoE-орієнтованої маршрутизації) передбачає суму метрик кожного каналу.

$$M_{(i,j)} = \sum metrics_{i,j}, \quad 0 \le M_{(i,j)} \le 1. \quad (2.20)$$

Для забезпечення найвищого рівня якості обслуговування QoE=5 з безлічі альтернативних маршрутів буде обраний той, що має найменшу вартість (менше значення сумарної метрики), відповідно цільова функція записується у вигляді (2.21) і навпаки для найнижчого рівня якості обслуговування буде обраний той, що має найбільшу вартість, цільова функція записується у вигляді (2.22):

$$F(Q_{QoE_{max}}) = \sum_{n=1}^{k} metrics_{i,j} \to min. \quad ; \quad (2.21)$$

$$F(Q_{QoE_{min}}) = \sum_{n=1}^{k} metrics_{i,j} \to max. \quad (2.22)$$

де *k* – число усіх можливих маршрутів між заданою парою вузлів відправник-отримувач.

У роботі пропонується проводити централізований моніторинг та управління мережевою структурою з допомогою удосконаленої логіки SDN контролера (рис. 2.7а). Для цього розроблено та успішно реалізовано

функціональний блок “оптимізатор мережі” у вигляді програмної надбудови над існуючою логікою управління контролера SDN з метою створення IBN/SDN контролера. Суть якого полягає у збиранні статистики від комутаторів про топологію мережі та ступінь завантаження комутаторів. На основі отриманої поточної статистики про стан мережі приймається адаптивне рішення щодо побудови оптимальної топології мережі за критеріями QoS/QoE та енергоспоживання. А саме в умовах низького навантаження мережі з допомогою даного підходу IBN/SDN контролер згідно отриманих даних від блоку “оптимізатор мережі” прийме рішення про створення графу (топології) з меншою кількістю активних зв'язків і комутаторів, в той час як високе навантаження на мережу збільшить кількість активних комутаторів та зв’язків між ними в графі. На основі запропонованої вище моделі маршрутизації за допомогою вагових коефіцієнтів (2.19) контролер інтелектуально може коригувати вартість шляху з урахуванням того, наскільки затримка чи втрати пакетів важливі для цього інформаційного потоку, щоб забезпечити користувачам сервісів бажану оцінку QoE (рис. 2.7б). Відповідно, в умовах низького навантаження контролер перерозподіляє навантаження між каналами так, щоб отримати меншу кількість задіяних комутаторів та незадіяні комутатори перевести у енергозберігаючий (неактивний) режим, що дасть змогу підвищити енергоефективність мережі в цілому. По мірі зростання навантаження та деградації рівня QoE приймається автоматизоване рішення про активацію сплячих комутаторів та переведення їх в активний режим.

Таким чином, розв’язання завдання вибору оптимального маршруту для забезпечення адаптивного рівня якості обслуговування в IBN мережі зводитиметься до пошуку такого значення метрики маршруту, яке наближається до значення інтегрального адитивного критерію якості, що відповідає за певний замовлений рівень QoE (рис. 2.7в), використовуючи для цього математичну модель (2.10-2.12).

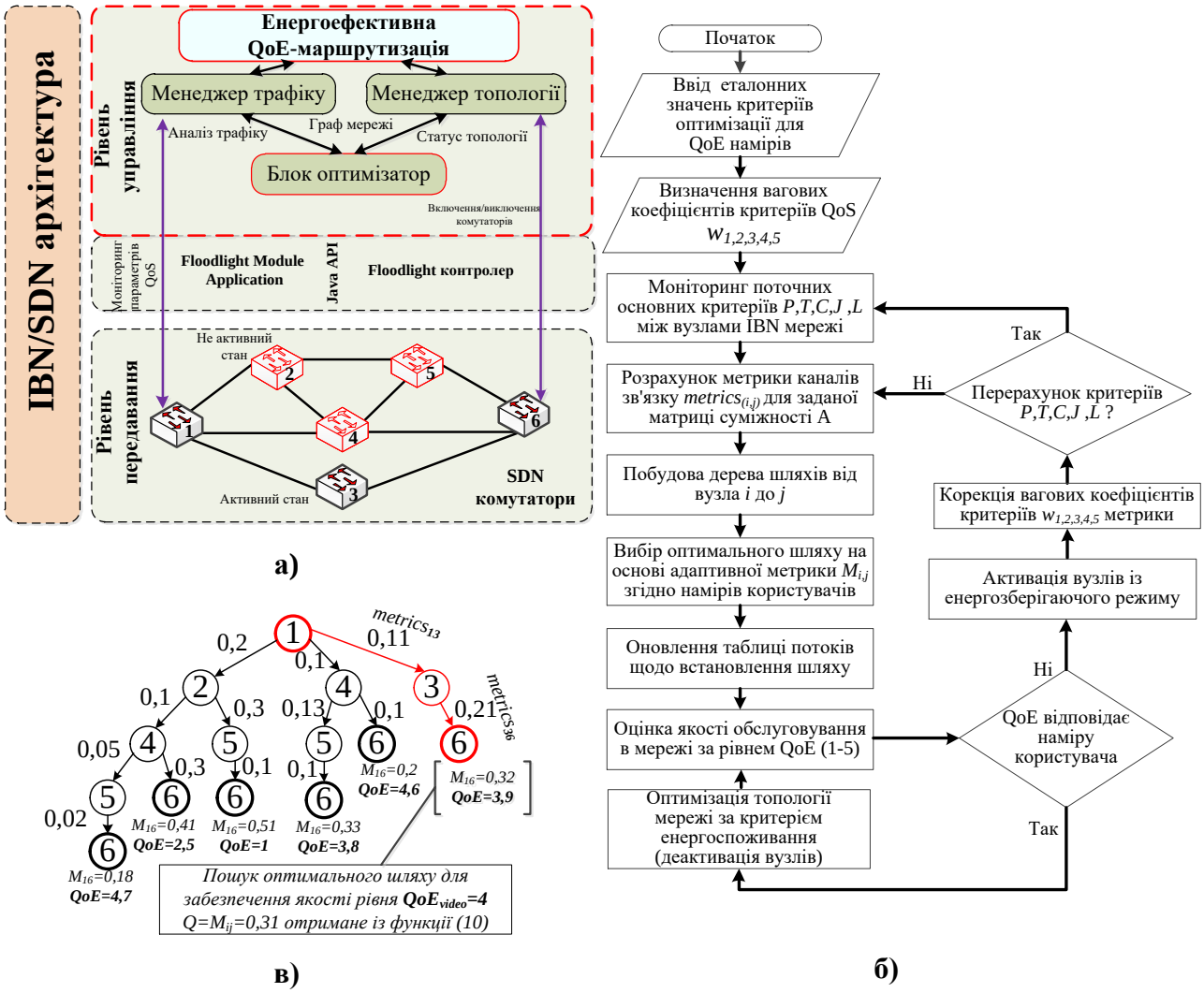


Рис. 2.7. Структурно-функціональна модель IBN/SDN мережі із QoE маршрутизацією – а), блок схема алгоритму роботи енергоефективної QoE-маршрутизації – б) та приклад розв'язку завдання маршрутизації для забезпечення замовленого рівня якості QoE_{video}=4 – в)

Представимо IBN/SDN мережу у вигляді двонаправленого зваженого графа $G=(N,M)$, де $N_i \in N$, N це кількість вузлів (SDN комутаторів), а i це номер комутатора. Між комутаторами N_i та N_j існує канал зв'язку $m_{ij} \in M$ із пропускною здатністю $B_{i,j}$. Нехай двійкові змінні V_i і L_{ij} позначають стан N_i-го комутатора та m_{ij}-го каналу таким чином, що:

$$V_i = \begin{cases} 1, & \text{якщо SDN комутатор } N_i \text{ є активний} \\ 0, & \text{в протилежному випадку} \end{cases}. \qquad L_{ij} = \begin{cases} 1, & \text{якщо канал } m_{ij} \text{ є включеним} \\ 0, & \text{в протилежному випадку} \end{cases}.$$

Позначимо, P_i та C_{ij} як енергоспоживання N_i-го комутатора та m_{ij}-го каналу зв'язку, виміряне у ватах (джоулях). Трафік у мережі представлений набором потоків F, де $f \in F$ визначається як $f = (sr, ds, \lambda_f)$, $sr\ i\ ds \in Z$ комутатори відправника та отримувача, а λ_f - швидкість потоку f, виміряна в байтах за секунду.

$$f_{ij} = \begin{cases} 1, & \textit{якщо потік } f \textit{ проходить через канал } e_{ij} \\ 0, & \textit{в протилежному випадку} \end{cases}. \qquad L\rho_{ij} = \begin{cases} 1, & \rho_{\min} \le \rho \le \rho_{\max} \\ 0, & \textit{в протилежному випадку} \end{cases},$$

де $\rho_{\min}$ мінімальна та $\rho_{\max}$ максимальна завантаженість каналів, щоб утримувати компроміс між продуктивністю та енергоефективністю мережі.

Логіка управління забезпечується розв'язанням задачі оптимізації сформованої у вигляді багатоцільової функції (2.23), що мінімізує енергоспоживання мережі з врахуванням наступних обмежень (2.24-2.31).

$$min\left(\sum_{\forall e_{ij}} L_{ij} \cdot C_{ij} + \sum_{\forall Z_i} V_i \cdot P_i \right). \tag{2.23}$$

$$subject\ to \sum_{\forall f} f_{ij} \cdot \lambda_f \le B_{ij}, \forall m_{ij}. \tag{2.24}$$

$$\sum_{\forall f} f_{ij} = \sum_{\forall f} f_{ij}, N_i\ \&\ N_j \ne sr, N_i\ \&\ N_j \ne ds. \tag{2.25}$$

$$f_{kj} = f_{iq}, N_k = sr, N_q = ds, \forall m_{kj}, \exists m_{iq}. \tag{2.26}$$

$$f_{ij} \le V_j\ and\ f_{ji} \le V_j, \forall N_j \in N. \tag{2.27}$$

$$V_i \le \sum_{\forall f} \left[f_{ij} + f_{ji} \right], \forall N_i \in N. \tag{2.28}$$

$$L_{ij} \le V_i, L_{ij} \le V_j \forall N_i. \tag{2.29}$$

$$V_i \le \sum_{\forall f} \left[f_{ij} + f_{ji} \right], \forall N_i \in N. \tag{2.30}$$

$$\sum metrics_{i,j} \le Q_{QoE_r},\ QoE_r = 1...,5,\ 0 \le Q_{QoE_r} \le 1. \tag{2.31}$$

Перший елемент цільової функції, відноситься до загального споживання енергії, створюваного всіма потоками, що проходять через канали зв'язку.

Другий це загальне споживання енергії всіх активних комутаторів у мережі. Умова 2.24 вказує на те, що загальна швидкість потоків між двома комутаторами не повинна перевищувати пропускної здатності каналів зв'язку. Вираз 2.25 і 2.26 стверджує, що потік не створюється і не втрачається в мережі. Обмеження виразів 2.27, 2.28 та 2.29 підтримують кореляцію між комутаторами та каналами за допомогою змінної стану комутатора та змінних каналів потоку. Хоча обмеження 2.27 і 2.28 стверджують, що жоден потік не повинен використовувати канал, що підключений до неактивного комутатора, обмеження 2.29 стверджує, що якщо жоден інформаційний потік не проходить через канали зв'язку, підключені до даного комутатора, тоді комутатор вимикається. Обмеження у рівнянні 2.30 говорить, що канал, який підключений до неактивного комутатора, повинен бути неактивним. Обмеження 2.31, вказує на те, що числове значення вартості маршруту даних повинне бути тотожним або меншим за нормалізоване значення коефіцієнта Q_{QoEr}, що характеризує замовлену якість користувача в IBN мережі. Таким чином, запропонований підхід дає змогу підвищити енергоефективність IBN мережі шляхом переведення в енергозберігаючий режим незадіяних вузлів при досягненні оптимальної продуктивності для забезпечення необхідних вимог QoE користувачів.

2.4. Удосконалення алгоритму вимірювання затримки даних в програмно-конфігурованих мережах для реалізації IBN

Виходячи із вищезазначеного, першим необхідним рішенням для проведення адаптивної реконфігурації мережі є реалізація моніторингу параметрів, що характеризують стан вузлів. Згідно проведеного аналізу встановлено, що протокол Open-Flow дає змогу контролювати більшу кількість параметрів. Проте, деякі із них потребують удосконалення, зокрема методи вимірювання затримки даних, які визначають тільки середню затримку в каналі між комутаторами для агрегованого потоку, що не дає змоги адекватно

відобразити затримку та в кінцевому випадку якість обслуговування для потоків з різним пріоритетом обслуговування [161]. У такому випадку, затримка для потоків високого пріоритету і низького відрізнятиметься суттєво (використання існуючих методів є не виправданими, оскільки дають не точні значення). Для реалізації вимірювання затримки у мережі за основу взято дослідження деяких відомих робіт [162], в якому для моніторингу затримки використовується контролер для вимірювання часу затримки, використовуючи повідомлення протоколу OpenFlow, описані в специфікації OpenFlow [163]. Чотири типи повідомлень, використовуються для даного рішення:

– STATISTICS_REQUEST: Повідомлення, надіслане від контролера комутатору, що вимагає його поточний набір статистичних даних (потоки, порти);

– STATISTICS_REPLY: Повідомлення, надіслане комутатором на контролер. Відповідь на попереднє повідомлення;

– PACKET_OUT: Повідомлення, надіслане від контролера комутатору, що містить пакет даних, який буде переадресовано через один або кілька портів (або ідентифікатор, якщо пакувальник буферизований);

– PACKET_IN: повідомлення, надіслане комутатором контролеру при зустрічі з невідомим пакетом (тобто в таблиці потоків комутатора немає відповідного запису).

Рішення щодо вимірювання затримки засноване на відправленні спеціально створених пакетів різного пріоритету через посилання від контролера та назад, одночасно вимірюючи час передавання. Для цього спочатку створюється пробний пакет, використовуючи широкомовну адресу як пункт призначення та апаратну адресу порту, який буде використовуватися для надсилання пакету як джерела. Для типу Ethernet використовується довільне значення (0x07c3), і корисне навантаження складається з номера порту, мітки часу створення пакета та додаткового поля пріоритету в полі ToS [164]. Потім контролер вказує комутатору s1 надіслати цей пакет через певний порт через повідомлення PACKET OUT; комутатор s2 на іншому кінці посилання не

знайде запис для цього типу пакету і надішле його назад контролеру за допомогою PACKET IN. Дозволяючи програмі моніторингу замінити програму переадресації контролера (яка за замовчуванням перекине цей невідомий пакет на всі порти комутатора), на контролер мережі можна отримати пакет і вивести з отриманого часу та позначки часу, скільки часу знадобилося пакету для передавання. Додаткове необов’язкове поле може бути використано для зберігання RTT низхідної лінії зв'язку у випадку, якщо пакет моніторингу отримує інший контролер, який не матиме цієї інформації.

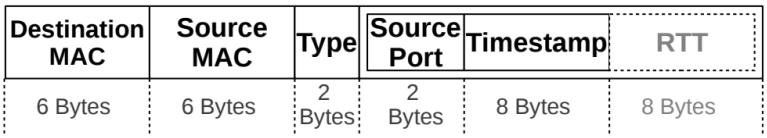


Рис. 2.8. Ethernet кадр для визначення затримки (існуючий підхід)

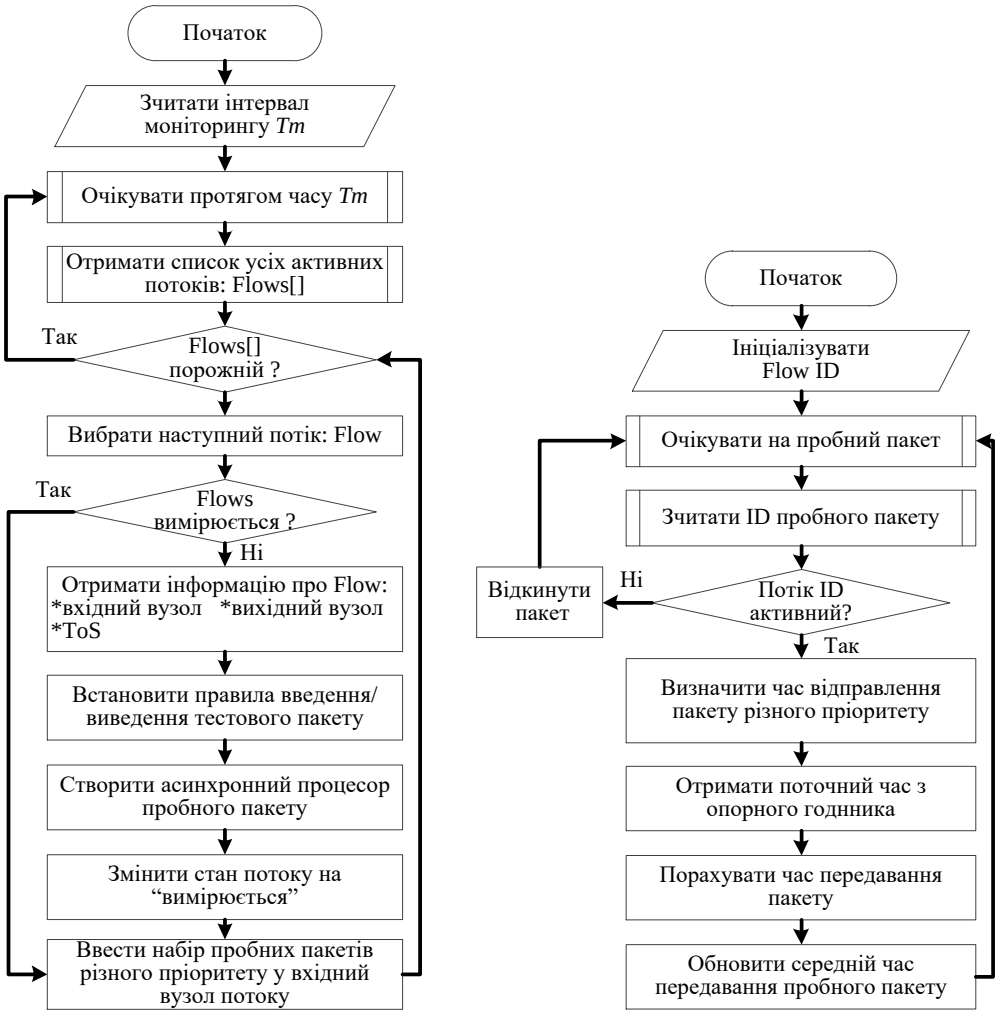
Зазвичай пакети повідомлення PACKET_OUT та PACKET_IN передаються, як сигнальна інформація з найвищим пріоритетом обслуговування, тому в процесі вимірюванню затримки в умовах високого навантаження даний пакет оброблятиметься першочергово, хоча в процесі експериментального дослідження на реальному обладнанні SDN за допомогою спеціалізованих команд виявлено, що утворюються черги для пакетів нижчого пріоритету. Саме тому, у роботі удосконалено алгоритм вимірювання затримки даних в програмно-конфігурованих мережах шляхом формування IBN/SDN контролером пробних пакетів меншого розміру з різними пріоритетами (рис.2.9а). У більшості OpenFlow-комутаторів кожен фізичний порт містить вісім черг [166]. Черга з номером вісім – найменш пріоритетна, відповідно затримка обслуговування для них буде найбільшою. Такими чином запропонований алгоритм дозволяє визначати точніше затримки пакетів для потоків різного пріоритету, оскільки пробні пакети будуть обслуговуватись з черг різної пріоритетності за тим же принципом, що і пакети реальних потоків, що мають високий пріоритет обслуговування. Тому, щоб відокремити тестовий новий пакет з пріоритетом на вихідному комутаторі з потоку, пропонується структура правила, подана в табл.0.

Таблиця 2.3

Приклад правила в таблиці потоків для вимірювання затримки потоку

Порт	DST MAC	SRC MAC	ETH TYPE	IP TOS	DST IP	SRC IP	IP PROTO	TCP/ UDP SRC	TCP/ UDP DST
*	*	*	*	*	*	*	*	*	40000/4

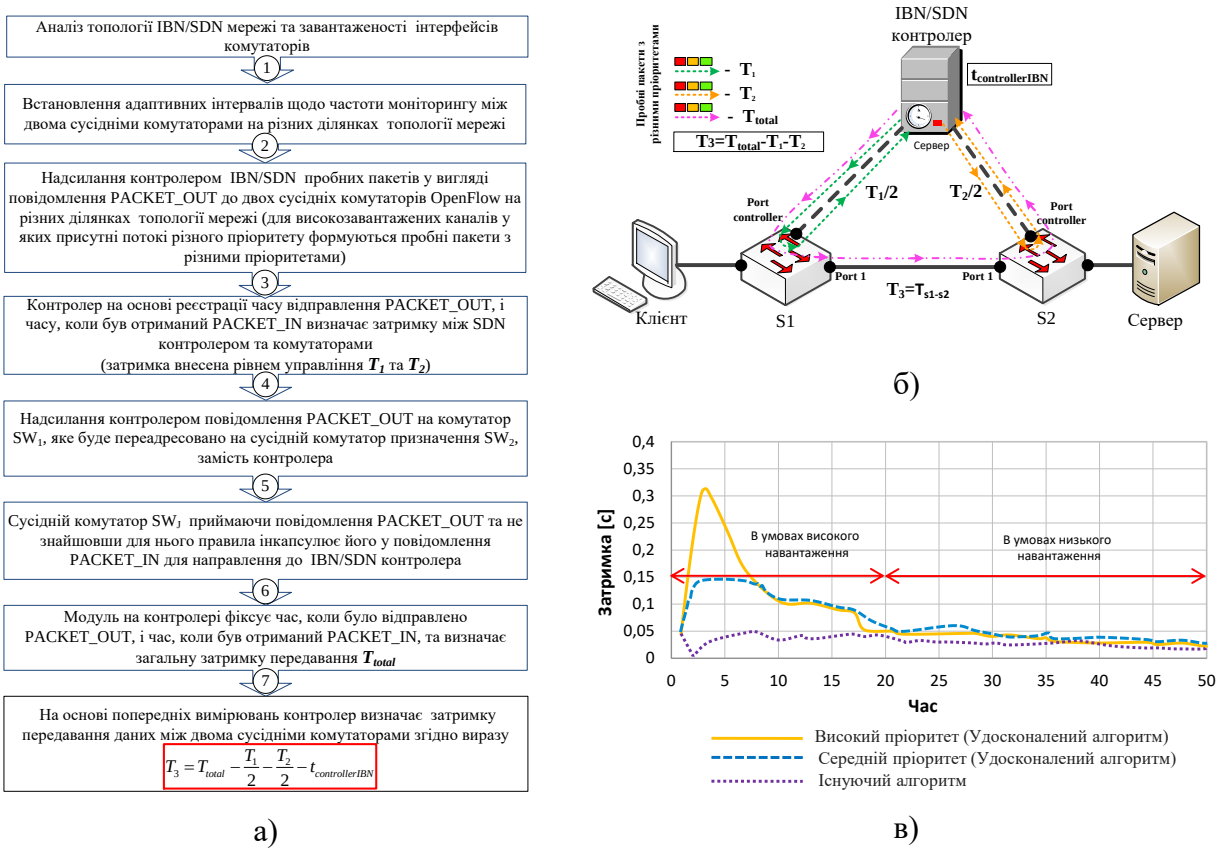
Особливістю пропонованого алгоритму (рис.2.9б) є те, яким саме чином пробний пакет передається по SDN мережі. Для цього у роботі вводиться додаткове правило, що встановлюється тільки на комутаторі, де потік покидає мережу. На всіх інших мережевих вузлах пакет порівнюється з тим же ж правилом, з яким порівнюються усі інші пакети потоку.



а) б)

Рис.2.9. Алгоритми відправки (а) та очікування (б) пробного пакету для вимірювання затримки потоку [166]

Зокрема, шляхом поетапної реалізації алгоритму вимірювання затримки на контролері SDN (рис.2.10а) та проведення експериментального дослідження на реальному обладнанні схема якого показано на рис. 2.10б доведено, що використання нового алгоритму вимірювання затримки в умовах високого канального навантаження підвищує точність моніторингу до 45% для низько пріоритетних потоків у порівнянні із відомим алгоритмом в SDN (рис. 2.10в).



а) б) в)

Рис. 2.10. Етапи удосконаленого алгоритму вимірювання затримки в програмно-конфігурованих IBN мережах – а), схема експериментального дослідження алгоритмів вимірювання затримки в SDN/IBN мережах – б), результати порівняння алгоритмів вимірювання затримки пакетів – в)

2.5. Модель адаптивного вибору підсистеми граничних та хмарних обчислень в інтенційно-орієнтованій інфокомунікаційній мережі

У даному підрозділі запропоновано математичну модель, що дає змогу описати функціонування багаторівневої хмарної системи для адаптивного

надання послуг в гетерогенній IBN мережі національного оператора мобільного зв'язку, загально концептуальні положення для якої були розглянуті у попередніх підрозділах. Модель буде застосовуватись для знаходження затримки системи внесеної рівнем серверного обслуговування. Зокрема оцінка параметра затримки є важливим завданням з метою забезпечення необхідного рівня якості обслуговування в процесі надання кінцевим користувачам IBN мережі різноманітних хмарних сервісів. На рис. 2.11. показана модель багаторівневої хмарної структури IBN мережі, зокрема що відповідає за підсистеми Cloud та Edge computing.

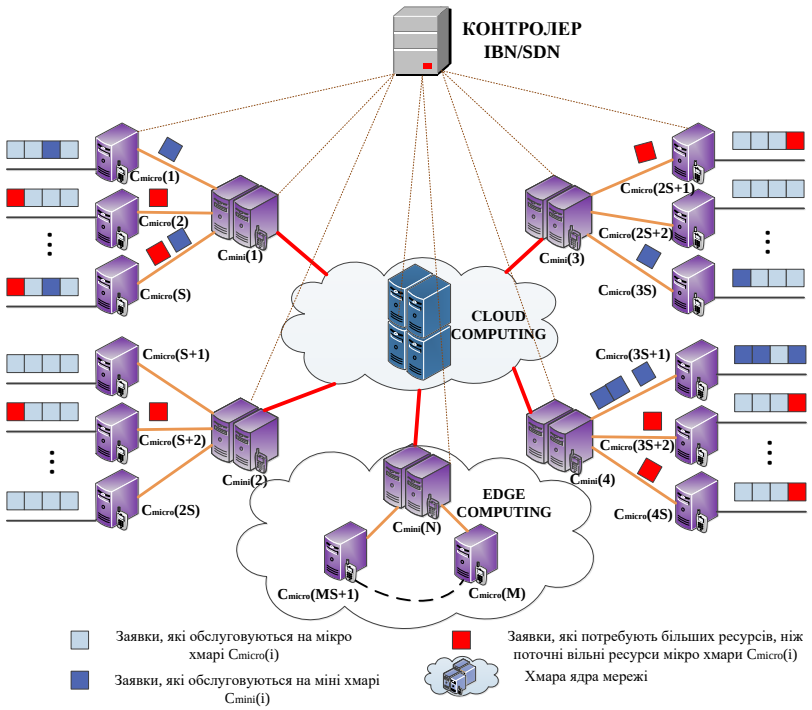


Рис. 2.11. Модель багаторівневої хмарної структури IBN мережі

У запропонованій концептуальній моделі IBN кожна базова станція SDR eNB чи комутатори рівня доступу з'єднані з мікро хмарою $C_{microEC}(i)$ з прийнятною продуктивністю, де $i \in \{1, 2 \dots M\}$ і M - загальне число мікро хмар. Кожна група мікро хмар пов'язана з великим за можливостями обробки і зберігання даних міні хмарою $C_{\min iEC}(j)$, де $j \in \{1, 2 \dots N\}$ і N - загальне число міні хмар в мережі. Міні хмара застосовується для тих операцій, які не можуть бути виконані мікро хмарами. Кожна міні хмара містить також контролер для

підключення мікро хмар. Міні хмари також містять шлюзи для взаємодії мікро хмар з ядром мережі при необхідності. У запропонованій моделі передбачається, що кожна міні хмара має з'єднання з фіксованим числом мікро хмар S в домені Edge computing.

Швидкість виконання вивантажених в мікро хмарі заявок ґрунтується на запитах користувачів, що надходять від рівня доступу. Будемо припускати, що розподіл надходження заявок можна описати певним законом розподілу, зокрема для прикладу припустимо, що процес надходження заявок описується Пуасонівським законом з інтенсивністю λ_i. Кожен елемент рівня доступу (базова станція SDR чи комутатор) виробляє на граничну мікро хмару $C_{microEC}(i)$ навантаження W_i з інтенсивністю Пуасонівського процесу λ_i. Кожна мікро хмара може обробляти заявки від відповідних базових станцій eNB чи комутаторів доступу, але в разі, якщо необхідні ресурси дорівнюють або перевищують, ніж максимальне значення $W_{microEC\max}(i)$, нові заявки відправляються в міні хмару до тих пір, поки ресурси мікро хмари зайняті. Таким чином, кожна мікро хмара підтримує робоче навантаження $W_{microEC}(i)$, а інші нездійсненні заявки відправляються в міні хмару. Кожна міні хмара обробляє навантаження $W_{mini_{EC}\max}(j)$, де $W_{mini_{EC}\max}(j)$ - максимальне робоче навантаження міні хмари $C_{mini_{EC}}(j)$. Заявки, які вимагають великих ресурсів, ніж поточні вільні ресурси міні хмари, відправляються на хмару ядра мережі.

Мультисерверна модель з чергами M/M/s використовується, як аналітична модель для мікро і міні хмар. Для мікро хмар ця модель записується $M/M/S_{micEC}$, а для міні хмар - як $M/M/S_{minEC}$ та для макро хмар ядра- як $M/M/S_{macroCC}$, де S_{micEC}, і S_{minEC} - число серверів в мікро і міні хмарах відповідно та $S_{macroCC}$ - число серверів в макро хмарах.

Загальна затримка при цьому складається з тривалості відгуку на заявку та тривалості взаємодії. Середня тривалість відгуку на заявку для мікро і міні хмар є сумою тривалості очікування в черзі і тривалості обробки заявок. Середня тривалість обробки заявок в мікро і міні хмарах може бути обчислена як

функція інтенсивності надходження заявок λ, грунтуючись на моделі з очікуванням *M/M/s* і *c* формулою Ерланга відповідно [167-171].

$$T_{micro_{EC}i-j}(\lambda)=\frac{C(S_i\frac{\lambda_i}{\mu_i})}{S_i\mu_{\ i}-\lambda_i}+\frac{1}{\mu_i} \tag{2.33}$$

$$T_{mini_{EC}i-j}(\lambda)=\frac{C(S_j\frac{\lambda_j}{\mu_j})}{S_j\mu_{\ j}-\lambda_j}+\frac{1}{\mu_j} \tag{2.34}$$

$$T_{macro_{CC}i-j}(\lambda)=\frac{C(S_j\frac{\lambda_j}{\mu_j})}{S_j\mu_{\ j}-\lambda_j}+\frac{1}{\mu_j} \tag{2.35}$$

$$C(n,\rho)=\frac{\left(\frac{(s\rho)^c}{n!}\right)\left(\frac{1}{1-\rho}\right)}{\sum_{k=0}^{n-1}\frac{(n\rho)^k}{k!}+\left(\frac{(n\rho)^c}{n!}\right)\left(\frac{1}{1-\rho}\right)}\quad , \tag{2.36}$$

де $T_{micro-i}$ - середня тривалість обробки заявки в мікро хмарі *i*, $T_{\min i-j}$ - середня тривалість обробки заявки в міні хмарі *j*, S_i - загальне число серверів в мікро хмарі *i*, S_j - загальна кількість серверів в міні хмарі *j*, λ_i і $\lambda_{\ j}$ - інтенсивності надходження заявок на обслуговування на мікро хмарі *i* і на міні хмара *j* відповідно, а μ_i і $\mu_{\ j}$ - відповідні інтенсивності обслуговування заявок.

У роботі запропоновано спосіб, який дає змогу оцінити затримку обслуговування на основі обчислювального кластера навантаження з урахуванням основних груп параметрів, а саме обчислювальної потужності кластерів, характеристики каналів зв'язку між кластерами, структури мережі, параметрів завдань: запропоновано. Потужність процесора кластера визначається кількістю процесорів кластера, тактовою частотою процесорів, кількістю оперативної пам’яті на один процесор. Інші показники кластеру, порівняно з вищезазначеними, мало впливають на швидкість роботи і, отже, на її потужність.

Розрахунок навантажувальних обчислень ґрунтується на припущенні, що Cloud система завантажується рівномірно, якщо кожен вузол обробляє лише одне завдання, і він буде оброблений центральним вузлом протягом години *Tefc*. Значення *T* вибирається індивідуально для кожної Cloud - системи залежно від її призначення та загальних завдань, що виконуються в ній. Cloud система складається з об'єднання кластерів, а кластери складаються із набору серверів. Загальні обчислювальні параметри Cloud системи розраховується за формулами [172] :

$$CPU_{pr} = \frac{\sum_{i=1}^{k} M_i \times CPU_i}{\sum_{i=1}^{k} M_i}; \tag{2.37}$$

$$RAM_{pr} = \frac{\sum_{i=1}^{k} M_i \times RAM_i}{\sum_{i=1}^{k} M_i}. \tag{2.38}$$

Після цього відбувається коригування значення T_{efc} для кожного кластеру Cloud системи. Оскільки цей параметр T_{efc} є часом виконання завдання вузлу з параметрами CPU_{pr} і RAM_{pr}, його слід перерахувати для кожної кластерної системи. Параметр T_{efc} коригується залежно від відхилення навантаження процесора від середнього значення для поточного кластера. Оскільки параметри *CPU* і *RAM* з точки зору швидкодії виконання завдання $CPU \geq RAM$, тому коефіцієнт коригування для параметра T_{efc} можна обчислити за формулою:

$$K = 0.6 \times \frac{CPU_{pr}}{CPU} + 0.4 \times \frac{RAM_{pr}}{RAM}. \tag{2.39}$$

Відповідно кориговане значення розраховується як:

$$Tefc_k = Tefc \times K. \tag{2.40}$$

Середній час обробки для виконання завдань на кластері буде:

$$T_{\text{avg processing time}} = \frac{\sum_{i=1}^{k} t_i}{N}, \tag{2.41}$$

де t_i - час виконання *i*-ї задачі ; *N* - кількість процесорів у кластері.

$$t_i = t_{task} + t_{transfer}, \tag{2.42}$$

де t_{task} – час виконання задачі; $t_{transfer}$ – час передавання даних.

Для обчислення $t_{tas}k$ визначається кількість запитів на вузол, де виконується завдання, а також на вузлі, який постачає або приймає дані. Для кожного з цих вузлів обчислюється пропускна здатність W:

$$W_i = \frac{W_{b1}}{X_{requests} + 1}, \tag{2.43}$$

де W_{bl} – максимальна пропускна здатність каналу, $X_{request}$ – кількість з'єднань на вузлі.

Після чого вибирається менше значення:

$$W = \min\{W_1, W_2\}. \tag{2.44}$$

Потім обчислюється час передавання даних:

$$t_{transfer} = \frac{V}{W}, \tag{2.45}$$

де V – об'єм даних, який передається між вузлами.

Співвідношення $T_{cluster}/T_{efc}$ дає змогу отримати параметр завантаженості і-кластеру:

$$R_i = \frac{T_{cluster}}{T_{efc}}. \tag{2.46}$$

Після розрахунку навантаження кожного кластера можна визначити навантаження Cloud системи в цілому:

$$R = \sum_{i=1}^{n} L_i \times R_i, \tag{2.47}$$

де R_i - відношення кількості процесорів у кластері до загальної кількості процесорів у системі; n_i - кількість кластерів у Cloud системі.

Отримане значення R відображає відносне навантаження L Cloud-системи у відсотках. Отже, 100% відповідає оптимальному навантаженню Grid-середовища. У цьому сценарії затримка мережі (network delay) та час обробки Cloud системи (processing time) є основними факторами, які впливають на якість обслуговування за критеріям затримки. Перший стосується часу,

необхідного для запиту користувача від пристрою користувача, щоб досягти крайового вузла послуги, і воно визначається фізичною відстанню вузла користувача, чергою та затримкою обробки кожного переходу (затримкою в мережевих пристроях) в мережевому маршруті та доступна пропускна здатність маршруту.

Середня затримка в мережі, може бути обчислена за формулою, запропонованою у роботі [173]:

$$T_{\text{avg network delay}} = \sum_{k=1}^{M} \tau_{ik} + \sum_{j=1}^{N} \rho \cdot \frac{(\rho)^{\frac{H_i\text{-}0.5}{1\text{-}H_i}}}{(1\text{-}\rho)^{\frac{H_i}{1\text{-}H_i}}} \cdot \frac{L_{sr_i} \cdot 8}{C_j}, \quad (2.48)$$

де M – загальне число каналів зв'язку між двома абонентами сервісу; τ_{ik} – величина часу затримки розповсюдження пакету послуги і-го пріоритету по k-каналу зв'язку; N – загальне число комутаційних пристроїв (вузлів) розміщених між двома абонентами сервісу; C – пропускна здатність j-го каналу; $L_{cep.i}$ – середня довжина пакету послуги і-го пріоритету; ρ – коефіцієнт завантаження пристрою; H – параметр Херста трафіку.

Загальна затримка (середній час обслуговування) обчислюється за формулою:

$$T_{avg\ service\ time} = T_{avg\ network\ delay} + T_{avg\ processing\ time}\ . \quad (2.49)$$

Цей підрозділ охоплює дослідження, в яких зміна кількості операцій визначалася обробкою програмного коду за допомогою одного віртуального сервера (Edge computing-EC) та шести серверів кластера (Cloud computing-CC). Дослідження проводилось за допомогою сервера розподілених обчислень MATLAB [174-176].

Клієнт через планувальник Scheduler запитує ресурси робочих процесів (workers). У його якості може виступати як вузол кластера, так і процесор Symmetric Multiprocessing (SMP) системи. Всі взаємодії відбуваються через запущену на кожному вузлі службу MDCE.

У роботі проведено дослідження часу обчислення задач за допомогою Edge computing та Cloud computing при різній кількості операцій (табл.3.1). Враховуючи, що для паралелізації планувальників завдань потрібен час, не у всіх випадках Cloud computing дасть найкращий результат. Відповідно в результаті експерименту отримано залежність часу обробки T в секундах від кількості операцій *O(N)*. За отриманими даними в результаті досліджень, представлених на рис.2.11, при перших трьох значеннях кількості виконуваних завдань видно, що Cloud computing система була менш ефективною, ніж обчислення на одній машині Egde computing, без підключення до системи.

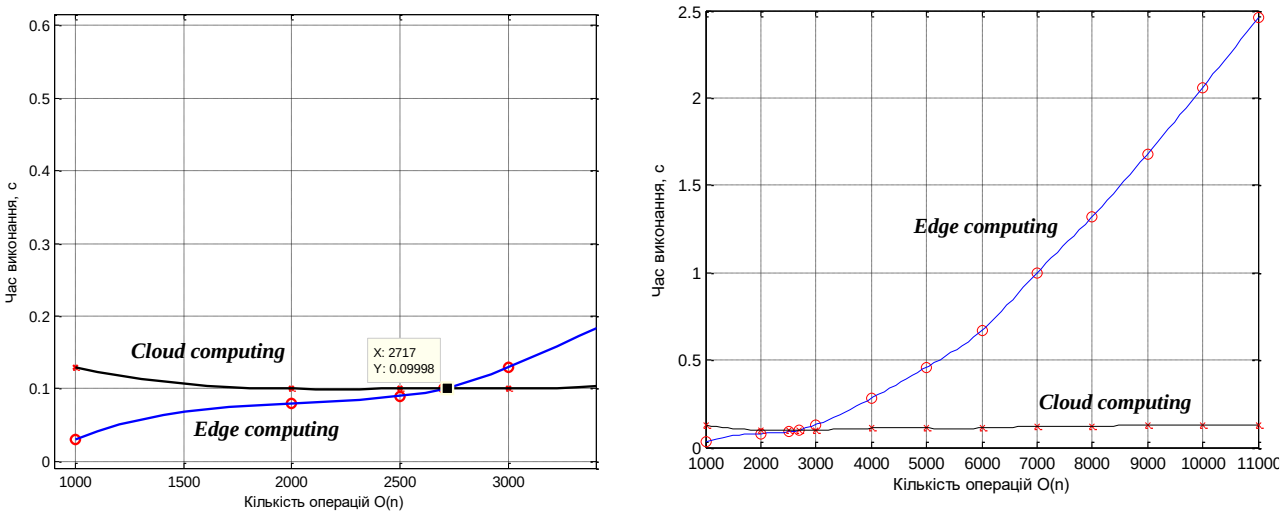
Таблиця 2.4

Результати дослідження

O(n) \ тип	Сервер (Edge computing) , с	6 серверів(Cloud computing) , с , с
1000.	0.03	0.13
20.00	0.08	0.1
250.0	0.09	0.1
…	…	…
1e+7	14 год – 1.3e+6	29,85

Згідно отриманих результатів дослідження, при перших трьох значеннях кількості операцій, які виконувались з рис.2.12 видно, що *CC* була менш ефективною за критерієм часу обслуговування, ніж обчислення на одній серверній машині *EC*. Отже провівши дослідження отримано залежність часу обробки *(t)* від кількості операцій *O(n)*. Оскільки після перших 10 результатів перевага Cloud computing є досить великою, то на рис.2.12б представлено залежність часу від кількості операцій для перших тринадцяти значень, згідно якого видно перетин графіків (демонстрація ефективності *CC* при обчисленні) та знайдено значення, при якому виконання даних операцій займає однакову тривалість часу як *Cloud computing (CC)*так і *Edge computing (EC)* (рис.2.12а).

) та Edge computing (EC) для перших 13 значень



а) б)

Рис. 2.12. Значення, при якому виконання даних операцій займає однакову тривалість часу обслуговування як для СС так і ЕС – а), та для всіх значень кількості операцій – б) [172]

Також у роботі згідно вище згадуваних формул оцінено затримку, яка вноситься мережею при підключенні різної кількості користувачів (запитів), які доступаються до СС та ЕС .

На рис. 2.13а показано порівняння середньої затримки мережі з використанням СС та ЕС. Як бачимо, ЕС забезпечує низьку затримку мережі порівняно з СС. Це пояснюється тим, що в процесі передачі задіяно менше мережевих вузлів, ніж у СС, оскільки ЕС знаходиться ближче до користувачів. На рис. 2.13б середній час обробки з використанням ЕС з невеликою кількістю користувачів нижчий, ніж з СС. Однак із збільшенням кількості користувачів СС через використання кластеризованої обробки та методів балансування навантаження забезпечить низьку затримку.

Таким чином, загальна затримка (середній час обслуговування) при використанні ЕС для простих завдань та в умовах низького завантаження забезпечує найкращий результат, що підходить для послуг із чутливою затримкою. А в умовах великого навантаження все-таки розумно використовувати СС.

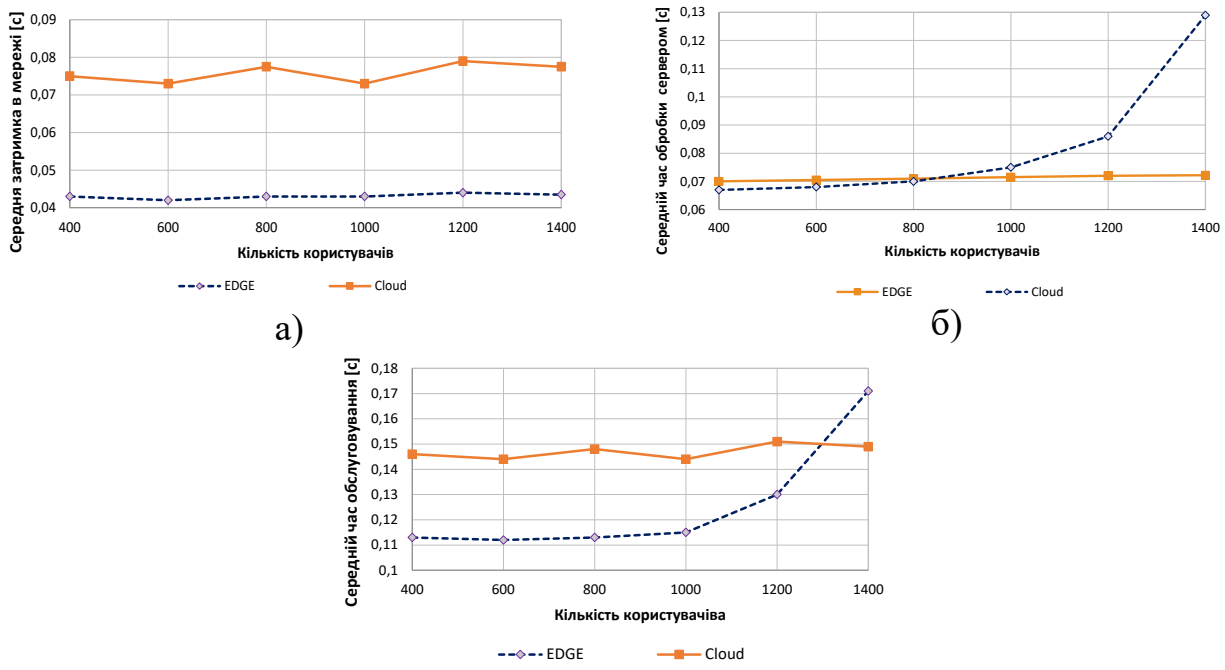


Рис. 2.13. Порівняння середніх затримок при доступі до СС та ЕС в залежності від кількості користувачів внесених мережею – а), внесених затримок в процесі оброблення запитів – б) та загальної затримок обслуговування – в)

2.6. Висновки до 2-го розділу

1. У другому розділі роботи запропоновано концептуальну модель побудови гетерогенної програмно-конфігурованої інтенційно-орієнтованої мережі, яка дає змогу забезпечити ефективний розподіл і перерозподіл загальних ресурсів адаптуючись під мінливі вимоги бізнес-користувачів щодо якості надання сервісів.

2. Запропоновано використати комплексний показник якості обслуговування користувачів сформованого у вигляді оцінки QoE, як основного критерію для адаптивного управління перерозподілом ресурсів в умовах зміни значимості бізнес-процесів в контексті реалізації концепції IBN.

3. Розвинуто математичну модель визначення суб'єктивного рівня задоволеності користувача за оцінкою QoE в залежності від зміни об'єктивних

показників якості обслуговування QoS, що забезпечуються в IBN/SDN мережі, зокрема для відео та аудіо сервісів реального часу.

4. Розроблено модель енергоефективної маршрутизації для інтенційно-орієнтованих мереж, що дала змогу підтримувати компроміс між бажаною якістю обслуговування користувачів, завантаженістю та енергоефективністю мережі. Запропоновано централізований моніторинг та управління мережевою структурою з допомогою удосконаленої логіки SDN контролера, що дало змогу на основі отриманої поточної статистики про стан мережі адаптивно приймати рішення щодо побудови оптимальної топології мережі за критеріями QoS/QoE та енергоспоживання.

5. Удосконалено алгоритм вимірювання затримки передавання даних в програмно-конфігурованих мережах шляхом формування контролером пробних пакетів меншого розміру із різними пріоритетами, що дало можливість для низько пріоритетних потоків покращити точність моніторингу. Формалізовано модель адаптивного вибору підсистеми граничних та хмарних обчислень в IBN мережі.

6. Запропоновано майбутню гетерогенну архітектура IBN мережі з реалізацією граничних обчислень (EC) і хмарних обчислень (CC). Така архітектура особливо важлива для підвищення якості послуг за рахунок скорочення затримок. Запропоновано підхід до вирішення недоліку, пов'язаного із забезпеченням низьких затримок для критично важливих додатків. Для цього був розроблений метод оцінки затримки сервісу в системі прикордонних і хмарних обчислень. Встановлено, що загальна затримка (середній час обслуговування) при використанні EC для простих завдань та в умовах низького завантаження забезпечує краший результат у порівнянні з Cloud Computing, що підходить для послуг із чутливою затримкою. А в умовах великого навантаження все-таки розумно використовувати Cloud Computing.

РОЗДІЛ 3. МЕТОДИ, АЛГОРИТМИ І МОДЕЛІ АДАПТИВНОГО РОЗПОДІЛУ МЕРЕЖНИХ РЕСУРСІВ ТА УПРАВЛІННЯ ТРАФІКОМ ДЛЯ СИНТЕЗУ КОРПОРАТИВНИХ ІНТЕНЦІЙНО-ОРІЄНТОВАНИХ МЕРЕЖ

3.1. Опис ідеї методу адаптивного клієнт-орієнтованого обслуговування інформаційних потоків у вузлах IBN

Швидкий розвиток і поширення комунікаційних технологій сьогодні стає глобальною інформаційною революцією [177]. Клієнти потребують послуг зв'язку, які можна гнучко налаштувати відповідно до їх вимог щодо якості сприйняття QoE. Традиційний метод управління якістю послуг, заснований на SLA (угода про рівень послуг), недостатній як засіб для забезпечення контрактів, що стосуються якості, між постачальниками послуг та клієнтами. Поточний метод SLA в основному обмежений і орієнтований на технічні аспекти якості обслуговування [178]. Крім того, вони не дотримуються в мережі принципів та семантичного підходу до специфікації QoS для служби зв'язку, що використовує параметри QoE. У цій роботі пропонується орієнтований на клієнта метод управління якістю надання послуг для майбутньої IBN (Intent-Based Networking) [179]. Даний метод базується на новій метриці QoE за шкалою від 1 до 5, що дає змогу врахувати комерційну цінність електронних послуг для кінцевих користувачів [180]. На основі цього підходу конфігурація мережі та функціональність мережевого обладнання автоматично змінюються залежно від вимог замовника. Для реалізації нового методу управління якістю послуг розроблено алгоритм маршрутизації пакетів даних у мережі з урахуванням поточного навантаження прогнозованого шляху. Створено алгоритм функціонування білінгової системи для клієнт-орієнтованого управління якістю надання послуг. Щоб дослідити ефективність запропонованого методу управління якістю послуг у порівнянні із традиційним

методом SLA, розроблено імітаційну модель мережі з реалізацією двох підходів.

На рис.3.1 запропоновано концептуальну модель IBN мережі для адаптивного надання сервісів згідно QoE намірів [124]. Даний підхід щодо адаптивного надання сервісів організовується шляхом встановлення QoE оцінок користувачами мережі, яка виставляється за шкалою від 1 до 5. Чим вища оцінка тим краща якість сервісу гарантується, тим і дорожче коштуватиме надання даного сервісу для кінцевого користувача, зокрема в умовах обмеженості мережевих ресурсів.

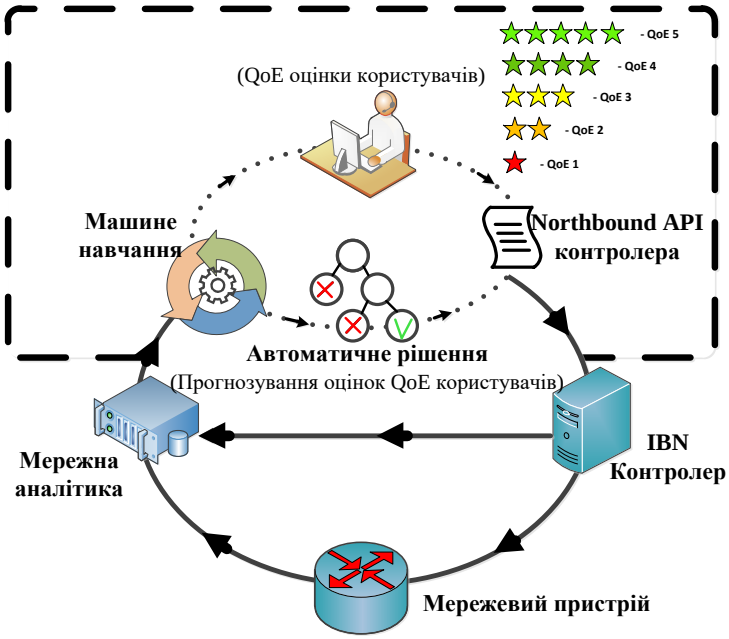


Рис. 3.1. Пропонована концептуальна модель IBN мережі для адаптивного надання сервісів згідно QoE намірів [178]

Практична реалізація цього підходу може бути здійснена шляхом встановлення програмного забезпечення на кінцевий пристрій замовника, де замовник може попросити змінити якість послуги на кращу в режимі реального часу та внести додаткову оплату. Використовуючи це програмне забезпечення, мережа пристосовується до потреб замовника, проводячи аналіз запитів від замовників щодо необхідної якості певного виду послуг у визначений час. Аналіз запитів виконується мережевим контролером. Контролер також

гарантує, що конфігурації пристрою відповідають одна одній. Це спрощує аудит мережевої конфігурації: всередині контролера конфігурація представлена у вигляді об'єктної моделі, яку можна будь-коли завантажити через інтерфейс прикладного програмування (API) для отримання останньої інформації про налаштування мережі [181]. Конфігурація підтримується контролером у поточному стані: якщо профіль програми буде видалено зі списку активних, його налаштування також будуть видалені з усіх мережевих пристроїв. Централізуючи стан мережі на рівні управління, система гарантує необхідний рівень обслуговування, використовуючи запропонований метод адаптивного клієнт-орієнтованого управління якістю надання послуг, враховуючи наміри користувачів. За рахунок централізації стану мережі на рівні управління, система гарантує необхідний рівень сервісу аналізуючи QoE оцінки користувачів, шляхом динамічного виставлення пріоритетів послуг згідно замовлених QoE оцінок, розподілу канальних ресурсів у мережевих вузлах, балансування навантаження на серверах та розроблення нових протоколів маршрутизації, які базуються на виборі оптимального вузла обслуговування, аналізу і оцінок характеристик мережі в режимі реального часу

Основним завданням, яке повинно виконуватися запропонованим методом, є забезпечення задовільного рівня обслуговування клієнтів при використанні рахунків та введення рейтингу якості. Основним показником є затримка надсилання наскрізних пакетів для кожного сеансу. Схема зв’язків між факторами, що впливають на задоволеність споживачів, зображена на рис. 3.2. Кожна можлива оцінка якості при наданні послуги має своє власне значення затримки доставки. Формування якості послуги включає як об’єктивну оцінку характеристик мережі, так і суб’єктивну оцінку експерта. І хоча параметри мережі можна визначити за допомогою відповідного обладнання, облік думки споживачів щодо якості отриманих послуг здійснюється на основі коефіцієнта QoS, запропонованого постачальником, і на коефіцієнті QoE, сприйнятому замовником. У цьому випадку на базі контролера IBN ми реалізували

програмний продукт, який порівнює різницю між необхідним рівнем якості та фактичним, і, якщо вона перевищує допустиме значення, визначає, які зміни конфігурації мережі потрібні, та генерує відповідні керуючі сигнали у режимі реального часу. Основні етапи функціонування моделі IBN для реалізації запропонованого методу показано на рис. 3.3.

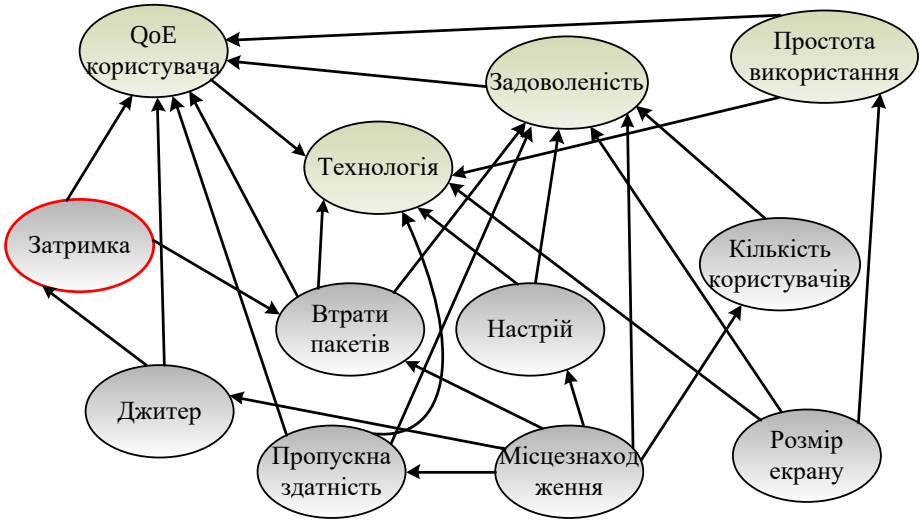


Рис. 3.2. Схема зв’язків між факторами, що впливають на QoE

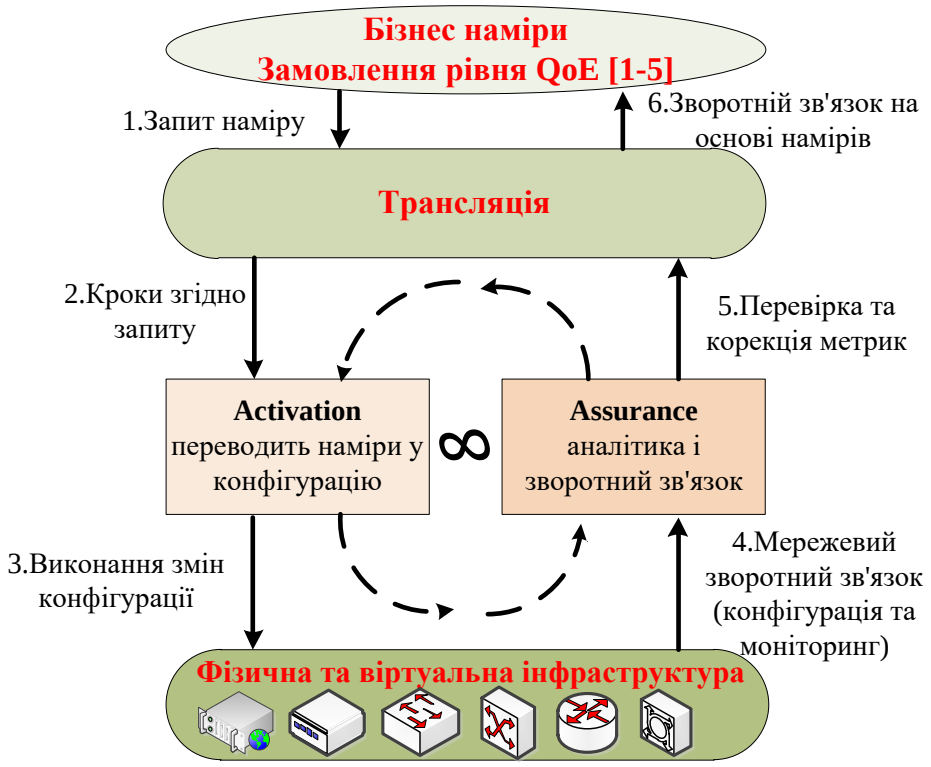


Рис. 3.3. Основні етапи функціонування моделі IBN [178]

Translation: трансляція бізнес-намірів. Трансляція включає в себе дві ключові функції. По-перше, адміністратор повинен мати можливість задати бажаний результат, тобто QoE бізнес-намір. У загальному випадку це зроблено за допомогою графічного інтерфейсу користувача, розробленого на базі спеціалізованої мови програмування JSON. Високорівневе завдання команд і їх абстрагування від низькорівневих деталей реалізації - важлива відмінність концепції IBN від традиційного підходу до експлуатації мережевої інфраструктури. Бізнес наміри такі як QoE оцінка задаються за допомогою інтерфейсів контролера - наприклад, через його GUI і «північні» (northbound) API, які можуть бути орієнтовані як на IT-сервіси, так і на бізнес-додатки. Фундаментально важливим етапом для забезпечення автоматизації є використання політик Model-Based Policy (MBP) [182]. Керуючі політики MBP генеруються автоматично програмним забезпеченням контролера.

Activation: активація бізнес-намірів в інфраструктурі. Завдання активації - впровадити політики MBP, задані на етапі трансляції, в усі області мережі, яких вони стосуються. Активація повинна забезпечувати генерацію відповідних конфігурацій елементів мережевої інфраструктури. При цьому бажано, щоб відомості про ці елементи, їх функціональні можливості і мережеві топології попередньо корелювали з даними MBP [183]. На практиці контролер мережі IBN зазвичай автоматично застосовує конфігурації через свій «південний» (southbound) API.

Assurance: аналітика і зворотний зв'язок. Цей функціонал передбачає створення зворотного зв'язку між інфраструктурою і контролером. Ідея полягає в тому, щоб контролер не тільки реалізовував бізнес-наміри, а й проводив надалі моніторинг і аналіз коректності їх реалізації, а в разі необхідності застосовував коригувальні дії автоматизовано. Ця ідея відображена в назві: assurance - від англ. «Впевненість, гарантія». Функціонал Assurance є критично важливим компонентом рішення IBN. Він використовує контекстний аналіз

даних, отриманих від елементів мережевої інфраструктури, дає змогу переконатися в коректності реалізації заданого наміру.

Існує три ключові аспекти функціоналу Assurance:

1. Безперервна верифікація. Необхідно бути впевненим в тому, що система правильно виконує заданий бізнес-намір протягом всього часу. Це передбачає постійний моніторинг стану і подій елементів мережевої інфраструктури. Отримана від них телеметрія дає змогу переконатися в забезпеченні необхідної продуктивності при реалізації наміру. Інструментарій Assurance може використовувати різні підходи - від формальних математичних моделей до засобів машинного навчання.

2. Формування висновків на основі аналітики: на додаток до верифікації поточного стану мережі та його відповідності заданому наміру, Assurance може надавати висновки (insights), більш глибоке бачення (visibility) мережевої інфраструктури і виконувати аналіз тенденцій. Наприклад, передбачати конкретні порушення заданого наміру перед його застосуванням, прогнозувати результати розвитку поточних тенденцій, виявляти аномалії.

3. Отримання зворотного зв'язку для реалізації коригувальних заходів і поліпшення параметрів мережі: порушення правил, SLA, ELA [184], виявлення аномалії та інші подібні ситуації, виявлені на попередньому етапі, можуть бути виправлені контролером шляхом повторного застосування необхідних функцій з розділу Activation. Таким чином, мережа IBN отримує механізм для автоматичного усунення порушень заданих бізнес-намірів, а також для постійної автоматичної оптимізації мережі. Такий інструментарій допомагає домогтися належного виконання заданих намірів протягом всього часу роботи мережі IBN. На практиці зворотний зв'язок зазвичай забезпечується шляхом отримання контролером інформації від елементів мережевої інфраструктури на базі різних протоколів і джерел (наприклад: NetFlow [185], syslog, SNMP, виведення show-команд інтерфейсу CLI, в тому числі що відносяться до функціоналу IP SLA і AVC). Далі інформація аналізується підсистемою

аналітики, реалізованої в програмному забезпеченні контролера. Результати аналізу або пропонуються адміністратору для прийняття ним рішення, або автоматизовано приймаються контролером.

3.2. Розробка імітаційної моделі інтенційно-орієнтованої мережі на основі замовлення QoE намірів

Запропоновано градацію якості надання сервісів за допомогою введення оцінки від «1» до «5». Відповідно оцінка «5» має найкращий показник, який зменшується до оцінки «1».В ході роботи буде показано декілька етапів покращення використовуваної мережі:

– Робота стандартної мережі без модифікацій;

– Робота стандартної мережі при модифікованій маршрутизації (змінений порядок обслуговування пакетів та введено можливість обрання якості послуги) та введено контролер для забезпечення можливості надання білінгу абонентам за відповідні послуги та бажану оцінку обслуговування;

– Робота комбінованої мережі: до стандартної мережі додаються маршрутизатори, які будуть обслуговуватися контролером IBN;

– Повністю нова IBN мережа, всі вузли якої обслуговуються контролером.

Кожен перехід до наступного етапу буде забезпечувати певне покращення якості надання послуг в мережі. Відповідно останній етап матиме найкращі показники. Далі розглянемо загальну структуру роботи мережі. Після цього проаналізуємо детально кожну складову частину програми. Моделювання мережі здійснено за допомогою мови програмування Java. Тому при детальному розгляді опишемо всі класи програми та алгоритми їх функціонування, як окремо, так і як єдиного цілого.

Схема роботи моделі мережі

Перед початком роботи проводиться ініціалізація досліджуваної мережі. Тут відбувається налаштування кількості маршрутизаторів, комутаторів та клієнтів мережі. Також встановлюються зв'язки між маршрутизаторами

(формується топологія мережі). Дослідження в моделі проводилися згідно топології мережі зображеної на рис. 3.4.

Після ініціалізації програма переходить безпосередньо до моделювання функціонування мережі, яку можна поділити на такі складові частини: (генерування пакетів абонентами мережі; обробка пакетів комутаторами; обробка пакетів маршрутизаторами; надсилання пакетів від клієнтів до комутаторів; надсилання пакетів (кадрів) комутаторами; надсилання пакетів маршрутизаторами; оновлення таблиць маршрутизації; збір статистики роботи мережі та оновлення графіків.

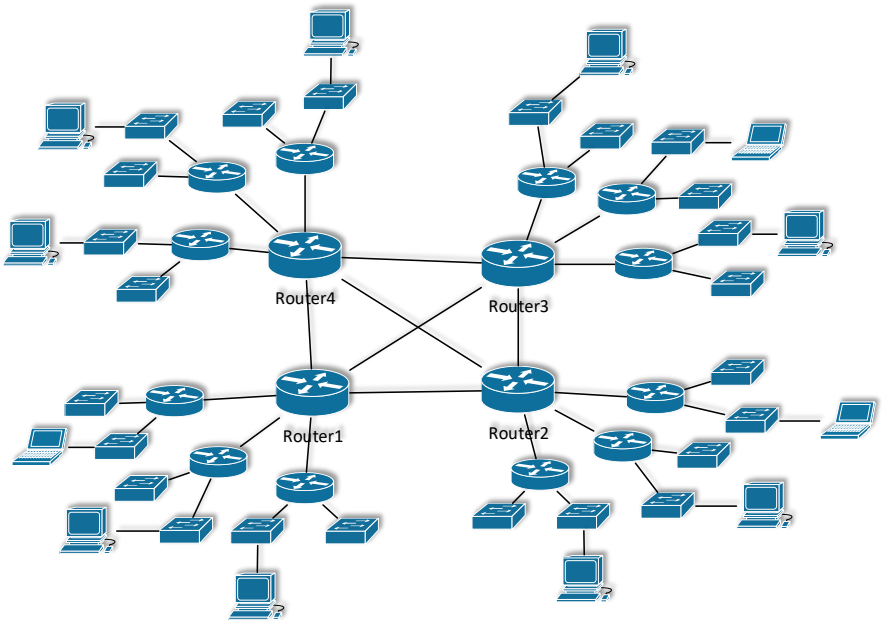


Рис. 3.4. Топологія досліджуваної мережі

Генерування пакетів абонентами мережі

Генерація пакетів абонентами відбувається в декілька етапів:

– Генеруємо сесію та обираємо її параметри такі як час користування сесією, вид сервісу, бажана оцінка QoE та вузол призначення.

– Генеруємо пакети для сесії поки вона не завершиться.

– Після завершення генеруємо нову сесію з новими параметрами.

В даній програмі обрано сім видів сервісів які можуть передаватися мережею: IP – телефонія; передача даних; інтерактивні дані; IPTV; сигнальні

пакети; відеоконференції; відео на вимогу. Кожен вид сервісу має власні параметри такі як: середній розмір одного пакету; відхилення від середнього розміру; максимальний час користування сервісом; кількість пакетів які генерує сервіс за секунду; максимальна кількість відкидань пакетів; максимальний час затримки при передачі пакета; ідентифікатор сервісу.

Розподіл ймовірностей використання сервісів обрано враховуючи середні показники користування абонентами в сучасних мережах. Значення ймовірностей подано в таблиці 3.1.

Таблиця 3.1

Розподіл використання сервісів в мережі

Тип сервісу	**Відсотковий еквівалент,%**
VoIP	15
Передача даних	15
Інтерактивні дані	5
IPTV	20
Сигнальні пакети	22
Відеоконференцзв’язок	21
Відео на вимогу	2

Кожен сервіс має свої параметри. В процесі моделюванні можна корегувати усі значення для конкретних варіантів. Використану конфігурацію параметрів зведено в таблиці 3.2.

Таблиця 3.2

Параметри сервісів

Тип сервісу	**Мінімальний розмір пакету, байт**	**Варіація розміру пакету, байт**	**Максимальний час користування, секунд**	**Пакети за секунду**
VoIP	100	199	260	60
Передача даних	800	700	320	90
Інтерактивні дані	350	299	400	60
IPTV	800	700	600	70
Сигнальні пакети	64	36	50	50
Відеоконференції	600	199	360	80

Для кращих результатів моделювання, при обранні кінцевого вузла враховується умова, що він має бути в іншій мережі. Оцінка обирається згідно рівномірного розподілу, проте так само може бути налаштована за бажанням. Після створення сесії абонентом будуть генеруватися пакети з відповідними параметрами кожної ітерації мережі.

Обробка пакетів комутатором

Кожен комутатор містить в собі список активних клієнтів, таблицю ARP для комутації пакетів та ідентифікатор назви вузла. Кожної ітерації комутатор збирає всі пакети від активних клієнтів та обслуговує згідно таблиці комутації. Якщо MAC адрес отримувача знаходиться в даній локальній мережі – пакет надсилатиметься на відповідний порт. Якщо MAC – адрес відповідає якійсь іншій мережі – пакет буде відправлено маршрутизатору.

В умовах використання стандартного методу обслуговування пакетів в мережі, комутатор оброблятиме пакети відповідно до часу їх надходження. При використанні запропонованого методу усі пакети будуть відсортовані. Детальніше робота нового методу буде розглянута пізніше.

Обробка пакетів маршрутизатором

Кожен маршрутизатор містить список IP-підмереж інтерфейсів, до яких підключені комутатори, пул IP-мереж (аналог DHCP), списки локальних та глобальних інтерфейсів, ідентифікатор імені вузла та таблиця маршрутизації. Також маршрутизатор має відповідні методи для створення нового комутатора, створення глобального інтерфейсу, надсилання і обробки таблиці маршрутизації сусідам, збору пакетів від комутаторів, обробку пакетів згідно обраного методу маршрутизації та відправки на відповідний інтерфейс, надсилання пакетів та отримання інформації по роботі вузла.

Маршрутизація пакетів відбувається згідно таблиці маршрутизації. Порядок обслуговування пакетів аналогічний як у комутаторів – залежно від використаного методу маршрутизації. При стандартному методі пакети будуть

обслуговуватися в порядку надходження, при модернізованому методі будуть сортуватися. Детальніше робота нового методу буде розглянута пізніше.

Надсилання пакетів комутаторами та маршрутизаторами

На цьому етапі відбувається надсилання оброблених пакетів інтерфейсами комутаторів та маршрутизаторів. Кожному інтерфейсу при ініціалізації мережі встановлюється сусідній інтерфейс, тому пакети, які прийшли певному інтерфейсу відправляються на сусідній інтерфейс. Тут немає різниці чи це глобальний, чи локальний інтерфейс, єдиний момент, що глобальний може мати більшу пропускну здатність.

Оновлення таблиць маршрутизації

Таблиця маршрутизації складається з записів про віддалені мережі. До такого запису належить IP – адрес віддаленої мережі, інтерфейс через який до неї можна доступитися, завантаженість даного інтерфейсу, кількість переходів та метрика маршруту. Після обробки та надсилання пакетів відбувається оновлення таблиць маршрутизації. При використанні стандартних маршрутизаторів поширенням таблиць маршрутизації займаються самі маршрутизатори. Недоліком такого варіанту є затримка на встановлення консистентності мережі при змінах в топології. Кращим варіантом в даному випадку є введення додаткового елементу мережі – контролера, який забере на себе процес маршрутизації та додасть багато інших хороших можливостей, таких як білінг, збір статистики, аналіз мережі та інші. Маршрутизація з використанням контролера буде набагато ефективніша, адже кожен маршрутизатор буде мати свій сигнальний канал, по якому будуть передаватися таблиці маршрутизації, статистика маршрутизатора та інші сервісні дані. Час на встановлення консистентності в такому випадку буде мінімальним.

Розглянемо формування таблиць маршрутизації.

Кожен маршрутизатор може мати локальні мережі та вихід до глобальної мережі. В таблиці маршрутизації для локальних мереж маршрутизатор призначатиме метрику рівну 0. Це означатиме що доступитися до цієї мережі

він може якнайшвидше. При передаванні своєї таблиці сусіднім маршрутизаторам метрика буде змінюватися. Нова метрика встановлюватиметься згідно формули 3.1

$$1 \qquad \mathrm{M} = n_{\mathrm{hops}} \cdot \rho_{\mathrm{port}} \tag{3.1}$$

де, $n_{\text{переходів}}$ – кількість переходів до даної мережі, $\rho_{\text{порта}}$ – завантаження порта маршрутизатора до цієї мережі.

Прийнявши таблиці маршрутизації від сусідніх маршрутизаторів відбувається оновлення. Аналізуються всі записи з наявними і до єдиної таблиці записуються дані по усіх унікальних маршрутах до наявних мереж. Збереження декількох маршрутів до однієї мережі виконується для можливості роботи балансувальника. Тобто коли є декілька маршрутів до певної мережі, і є декілька сесій які потрібно передати, при виборі одного найкращого маршруту ми відправлятимемо увесь трафік через один інтерфейс. В такому випадку інтерфейси іншого шляху можуть простоювати, тоді як інтерфейс найкращого шляху буде перевантажений. Також це дасть змогу відправляти трафік, який не сильно залежить від часу затримки, особливо коли ще й обрано якість «1» по довшому маршруту, звільняючи ресурси з основного шляху на пріоритетніші сесії.

Збір інформації для оновлення графіків

В даній моделі на кожному логічному рівні організації збираються дані про роботу мережі. Насамперед кожен клієнт, як було сказано раніше, збирає інформацію про активні сесії кожної ітерації. В свою чергу комутатори забирають дану інформацію в кожного клієнта. Далі аналогічно роблять маршрутизатори – збирають інформацію в комутаторів. Далі відбувається збір даної інформації в кожного маршрутизатора. В результаті ми маємо список по інформації по всіх активних сесіях в мережі.

В даній моделі графіки відображають декілька основних видів інформації.

На рис. 3.5. зображено кругові діаграми задоволеності кількості сесій для усіх можливих оцінок QoE якості обробки сервісів в мережі. Результати формуються згідно алгоритму, зображеного на рис. 3.3. Зеленим позначено кількість добре обслужених сесій, червоним – кількість сесій з незадовільними результатами.

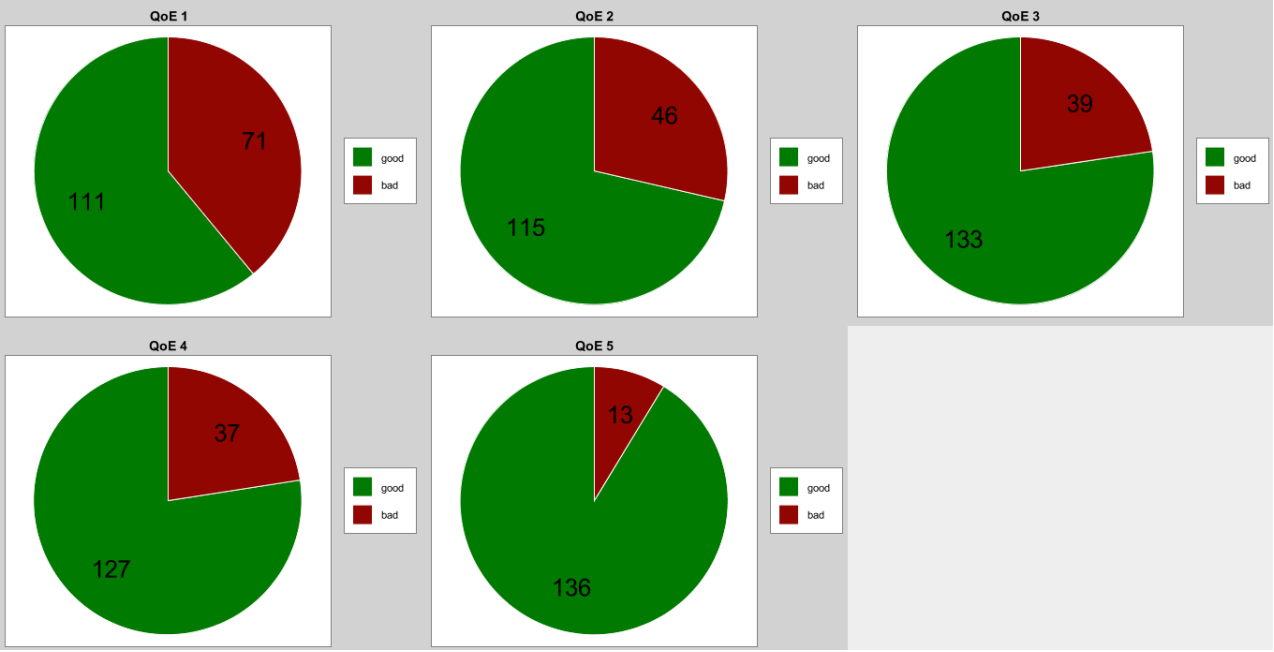


Рис. 3.5. Забезпечення якості сервісів по оцінках в мережі

Для відображення загального результату проходимо по всіх сесіях та звіряємо результати обробки пакетів за одну ітерацію. Загальний середній час очікування на обробку всіх сесій на кожному інтерфейсі в мережі згідно оцінки QoE зображено на графіку на рис. 3.6.

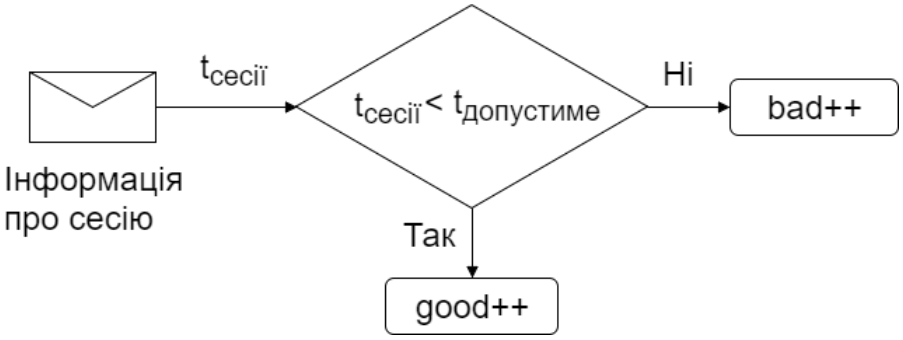


Рис. 3.6. Схема прийняття рішень для побудови QoE діаграм

У роботі показано детальний розгляд структури та зв’язків програми моделювання мережі написаної за допомогою мови програмування Java. Загальний принцип роботи моделювання даної мережі зображено на рис. 3.7.

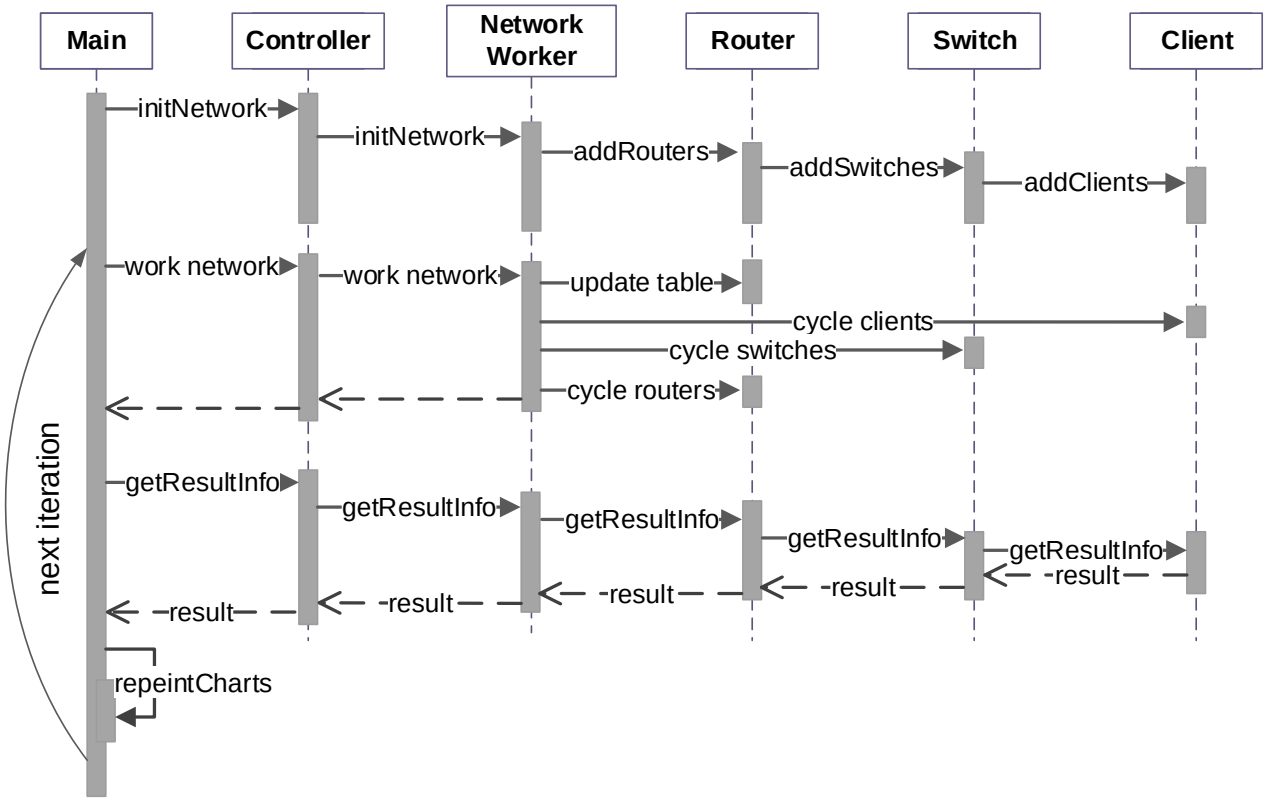


Рис. 3.7. Загальний алгоритм роботи мережі [179]

Як було сказано раніше, спочатку проводиться ініціалізація мережі і всіх залежностей. В класі *Main* для цього викликається метод *initNetwork()*, який в свою чергу через контролер (назва класу в програмі, не те ж саме що контролер в мережі SDN) викликає такий самий метод об’єкту, який відповідає за роботу мережі. В останньому реалізовано можливості для додання маршрутизаторів, додання комутаторів та відповідної кількості абонентів. Можливість для видалення елементів мережі. Ініціалізація та обрахунок IP – адрес для використовуваних мереж. IP – адреси збираються у відповідні пули, які розсилаються маршрутизаторам. Останні в свою чергу виконують функції DHCP сервера в відповідних мережах. При доданні нового абонента, йому виділяється вільна IP – адреса з пулу, якщо така існує, інакше інформуємо, що

немає можливості додання нового абонента. Також при додаванні будь-якого вузла, йому присвоюється випадковий унікальний номер MAC адреси. Всі номери реєструються в спеціальній колекції, тому при запиті на нову MAC адресу, генерується нова і перевіряється її унікальність. Це зроблено для додаткової гарантії того, що в мережі не буде двох елементів з однаковою MAC адресою. Проте імовірність такого випадку є дуже малою.

Також тут встановлюються швидкості для всіх інтерфейсів. Значення за замовчуванням виставлені – 100 Мбіт/с для локальних мереж, та 1000 Мбіт/с для глобальних мереж (між маршрутизаторами).

Після цього в класі *Main* створюються графіки та програма переходить до безкінечного циклу. В цьому циклі викликається метод *workNetwork(),* який покроково викликає відповідні методи для маршрутизаторів, комутаторів та клієнтів. Спочатку збираємо пакети з інтерфейсів та обробляємо їх. Тут відбувається сортування на кожному вузлі з відповідним активним методом (традиційним або пропонованим). Після цього викликаємо покроково надсилання пакетів. Такий порядок необхідно для того, щоб змоделювати роботу мережі за одну секунду. Основною причиною є виконання всього в одному потоці. Тому, якщо б відбувалася обробка і відразу надсилання – ми б мали некоректні дані, адже за одну секунду такого моделювання пакети могли б мігрувати від абонента відразу на маршрутизатор або навпаки.

Моделювання роботи мережі вирішено виконувати в одному потоці для спрощення розробки та взаємодії між елементами мережі. Адже при багатопотоковому виконанні немає гарантії що ці потоки будуть обробляти пакети з однаковою швидкістю.

Далі збирається статистика роботи мережі по активних сесіях та завантаженості мережі і оновлюються відповідні графіки. Після цього все повторюється.

Реалізація роботи клієнтів

Розглянемо клас клієнта та залежні від нього класи на рис. 3.8.

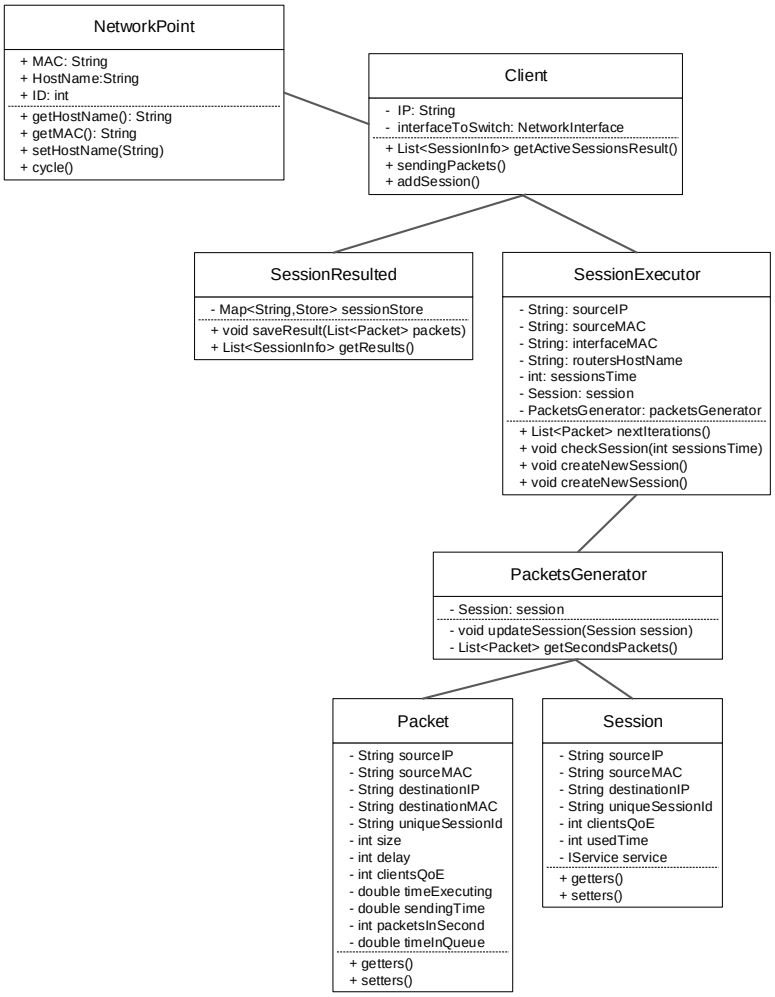


Рис. 3.8. Uml діаграма класу клієнта та залежних від нього класів

Клієнт розширює абстрактний клас NetworkPoint. Даний абстрактний клас має такі поля як IP – адреса, MAC – адреса та ID вузла. Також відповідні методи для їх отримання та встановлення. Також в даному абстрактному класі перевантажено метод *toString()*. В звичайному варіанті його реалізації з класу *Object* він показує інформацію по адресу пам’яті об’єкта, що для нас користі ніякої не дає. Тому потрібно переоприділити його, вказавши що ми хочемо виводити. Переоприділимо цей метод, щоб він повертав стрічку з такою інформацією:

```
HostName + "{" +
        "MAC='" + MAC + '\'' +
'}';
```

В такому випадку ми виводитимемо інформацію з використанням назви вузла (хоста) та його MAC – адреси у фігурних дужках.

Кожен клієнт встановлює свою IP – адресу, MAC – адресу та інтерфейс до комутатора, який його обслуговує. Даний інтерфейс символізує лінк від абонента до інтернет провайдера. Кожен клієнт має методи для генерування пакетів та сесій. Також кожен клієнт має додаткові класи, для збору інформації та статистики по отриманих послугах.

В даних класах проводиться виділення окремих сесій, адже при випадковому генеруванні кінцевого отримувача є можливість, що до одного абонента може згенеруватися декілька сесій. Після розділення сесій ми знаходимо середній час пакетів за секунду, кількість отриманих пакетів та розмір отриманих пакетів для кожної сесії. Кожен клієнт також має відповідні методи для збору з них даної статистики, які викликаються обслуговуючими їх комутаторами. Клас *NetworkPoint*, як було сказано раніше, є абстрактним, клас клієнта його наслідує та добавляє свої методи та поля. Клас *Packet* представляє собою сутність пакета з необхідними полями (не всіма, деякі додані, деякі упущені з ціллю спрощення реалізації програми). При генеруванні пакетів кожної секунди абонент генерує колекцію цих класів (*Packet*) з відповідними змінними полями – розміру одного пакету (у колекції кожен пакет має свій розмір). При надсиланні пакетів абоненти просто відправляють всі згенеровані пакети з даної колекції комутатору.

Клас *PacketsGenerator* генерує пакети кожної секунди, згідно кількості яка прописана для певного сервісу. *SessionExecutor* обслуговує всі сесії абонента.

Кожен абонент може мати декілька активних сесій. Тому при генеруванні пакетів обробка цих сесій буде поступовою. Модель реалізовано так, що кожен абонент в будь-який момент часу має мати активну сесію. Якщо сесія закінчиться, то створиться нова з спеціально спочатку згенерованим часом користування даною сесією, видом використовуваної послуги та кінцевим адресатом даної послуги (Destination IP address). Для покращення дослідження

передавання пакетів мережею, обрано, що кожна послуга буде генеруватися тільки до якоїсь іншої мережі. Що змусить пакети оброблятися маршрутизаторами. Іншими словами усі послуги які генеруються ніколи не будуть в одній локальній мережі. Даний випадок нас не цікавить, адже обслуговування таких послуг закінчується на найближчому комутаторі і ніяких проблем з часом надсилання тут виникнути не може.

Клас *SessionResulted* призначений для обробки і знаходження результатів з отриманих клієнтом пакетів. Цей процес складається також з декількох етапів. Для початку додається інформацію по отриманих пакетах до цього класу. Потім в циклі перебираються всі отримані пакети та розділяєються по сесіях. Також для кожної такої сесії зчитується результати з пакетів – їх кількість, час на надсилання мережею, та час очікування на обслуговування кожного пакета.

Клас *Session* містить в собі інформацію про актуальну сесію. Час використання, тип сервісу, IP адреси тощо. Кожного разу при створенні нової сесії, створюється новий об’єкт даної сесії з відповідними параметрами. При користуванні сесією ці параметри просто зчитуються та не генеруються кожного разу.

Список класів які представляють сервіси наведено на рис. 3.9. Тут наведено загальний інтерфейс для сервісу. Даний інтерфейс реалізується в абстрактному класі *Service*. В цьому класі додано загальні методи для отримання даних по послузі. Кожен вид послуги представлено окремим класом.

Ці класи наслідують абстрактний клас *Service* та додають свої значення параметрів, згідно таблиці яка була подана раніше. Тепер за такої архітектури ми можемо спростити процес роботи з згенерованою послугою. В такому випадку, коли всі послуги реалізовують однаковий інтерфейс, можуть обслуговуватися однаково. Тобто вони мають однакові методи, які описані в інтерфейсі. Це дає змогу нам обслуговувати усі послуги однаково, і не має різниці який це вид. Просто під час роботи значення параметрів автоматично

будуть підставлятися ті, які нам потрібно. Розподіл ймовірностей використання послуг в мережі було подано раніше у відповідній таблиці.

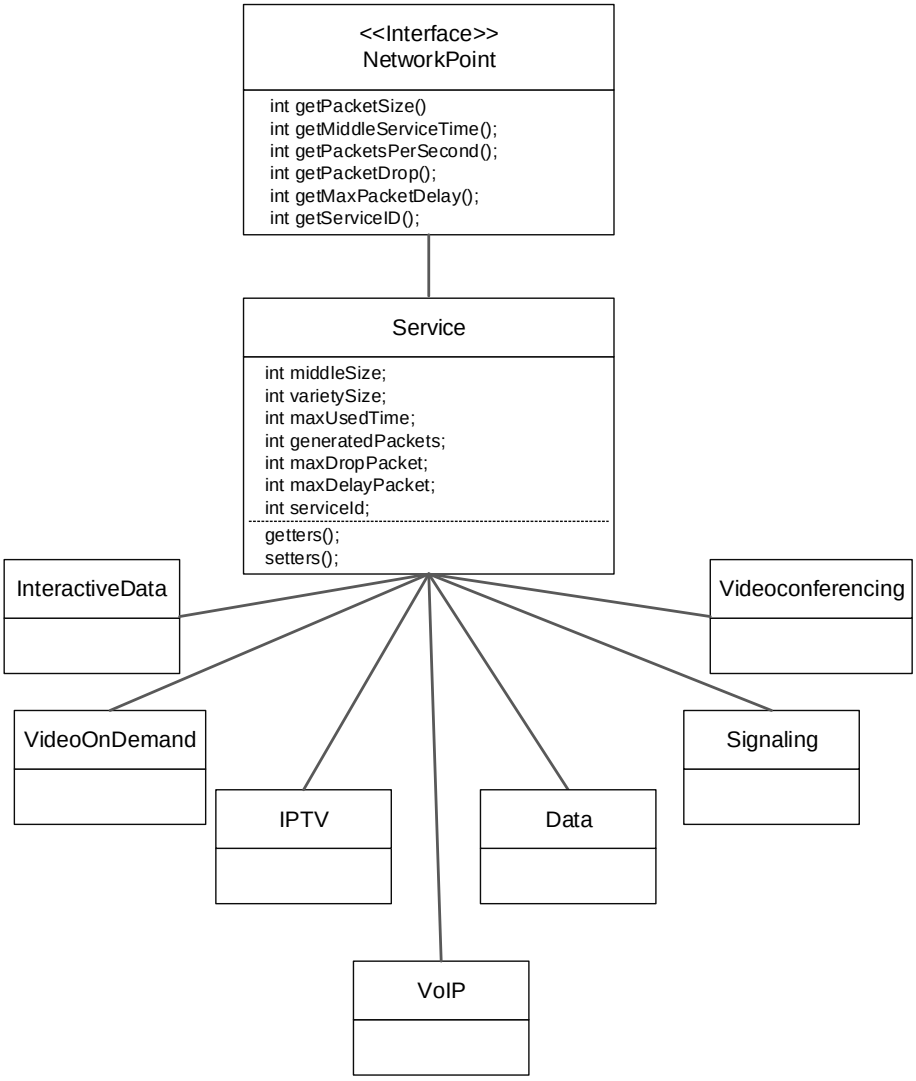


Рис. 3.9. Види сервісів в мережі

Реалізація роботи комутаторів

Далі розглянемо роботу комутаторів та залежних від них класів. Клас *Switch* (Комутатор) подано на рис.3.10. Він так само, як і клієнт розширює абстрактний клас *NetworkPoint* (точка мережі) та має аналогічні методи для встановлення і отримання IP – адреси, MAC – адреси та назви хосту. Також для даного класу так само діє перевизначений метод *toString()* (класу *Object* , який є батьківським для всіх класів в даній мові програмування). Даний метод аналогічно повертає стрічку з назвою хосту та MAC адресою.

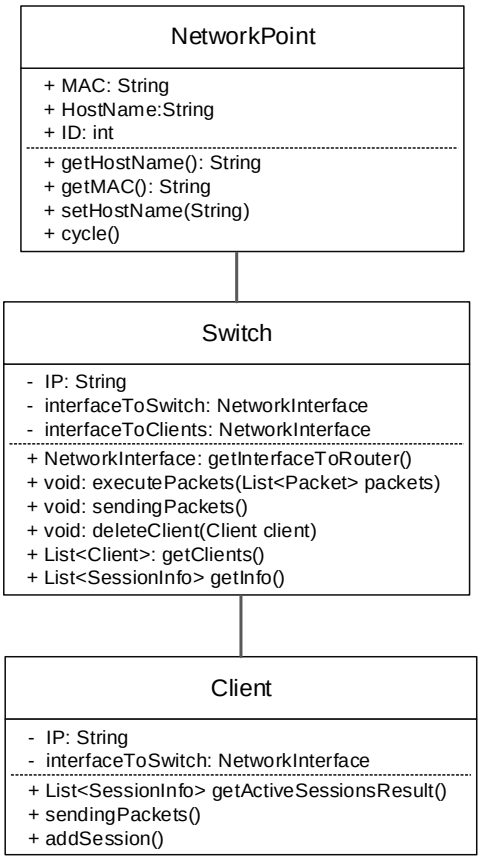


Рис. 3.10. Клас комутатора

Додатково в класі комутатора створюються методи для обробки клієнтів. Також тут вводиться окрема карта, яка символізує ARP – таблицю. Призначення даної таблиці зберігати MAC адреси та відповідні їм порти і інтерфейси, кудою до них можна доступитися. Це дає змогу обслуговувати локальні сесії.

Також введено додатковий метод для обробки отриманих з мережі пакетів. Усі пакети з мережі збираються в одну колекцію, далі при обробці ця колекція сортується згідно активного методу (традиційного або пропонованого) та обробляються у встановленому порядку. При комутації пакетів спочатку перевіряється чи адресатом є дана локальна мережа, якщо так то відправляється на відповідний порт комутатора з ARP – таблиці. Якщо кінцевою адресою є якась інша віддалена мережа – пакет відправляється далі маршрутизатору для подальшої обробки. Метод *sendingPackets()* призначений для безпосередньої

відправки оброблених пакетів. Також наявні методи для збору інформації по активних сесіях із обслуговуваних комутатором клієнтів. Даний метод викликається маршрутизатором для подальшого збору інформації.

Методи *GetClients()* та *DeliteClient(Client client)* призначені для отримання загального списку активних клієнтів та для видалення обраного клієнта з мережі. Кожен клас комутатора містить інтерфейси до маршрутизатора та до абонентів. Усі активні клієнти зберігаються локально у колекції. Тому при обробці клієнтів відбувається звичайний перебір цієї колекції.

Усі комутатори обслуговуються маршрутизаторами.

Реалізація роботи маршрутизаторів

Клас маршрутизатора і залежні від нього класи подано на рис. 3.11. Маршрутизатор, як і попередні розглянуті елементи, розширює базовий стандартний абстрактний клас. Тому містить аналогічний базовий функціонал – такий як отримання та призначення IP – адреси, MAC – адреси та назви хоста. Також наявний метод який повертає стрічку-представлення даного елемента – назва хоста та його MAC – адреса. Усі маршрутизатори містять в собі колекцію комутаторів, яких вони обслуговують. При роботі маршрутизатора, усі комутатори обслуговуються при переборі даної колекції.

Наявні методи для додавання комутаторів та видалення комутаторів. Аналогічно в цих методах відбувається їх додавання до локальної колекції для обробки, або видалення з неї. Кожен маршрутизатор містить додаткові колекції локальних та глобальних інтерфейсів.

З врахуванням нового рівня обробки пакетів в даному класі з’являються необхідні для цього елементи:

– Таблиці маршрутизації та методи для їх надсилання та оновлення;

– Метод для переключення використовуваного сортування (традиційного або пропонованого);

– Метод для збору інформації по завантаженості усіх його портів, як локальних так і глобальних;

– Метод для збору інформації з підпорядкованих комутаторів;

– Метод для отримання колекції підпорядкованих комутаторів;

– Методи для додання та видалення комутаторів;

Та інші допоміжні приватні методи.

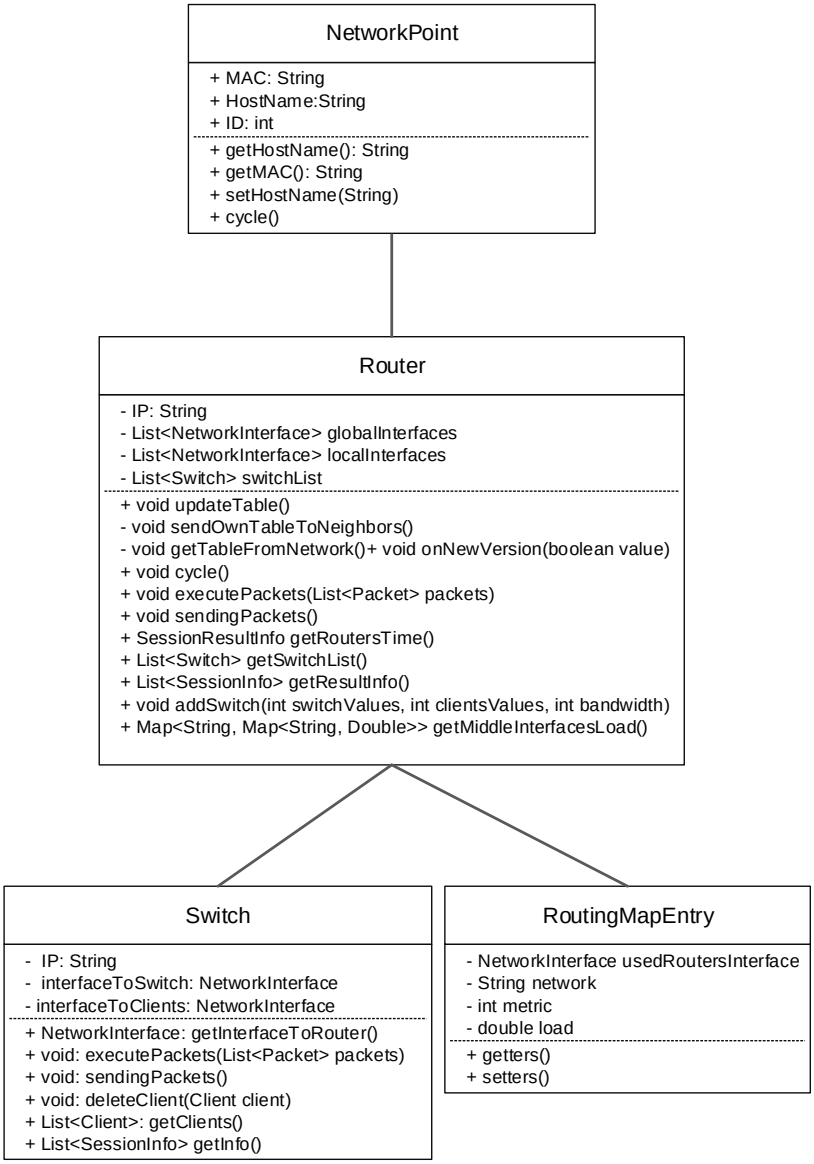


Рис. 3.11. Клас маршрутизатора

Робота такого маршрутизатора відрізняється від роботи комутатора введенням додаткової логіки.

Спочатку відбувається процес оновлення таблиць маршрутизації. Сюди входять методи для відправлення власної таблиці сусідам, отримання таблиць

від сусідів та обробки даних таблиць і зведення у єдину таблицю, згідно якої буде відбуватися процес маршрутизації.

Процес обробки декількох таблиць і зведення до однієї буде розглядатися пізніше. Після оновлення таблиць маршрутизації починається безпосередня обробка отриманих пакетів. Для цього пакети збираються з усіх локальних та глобальних інтерфейсів до єдиної колекції за допомогою методу *getPacketsForRouter().* Після цього дана колекція сортується згідно активного методу обслуговування (традиційного або пропонованого). Далі відбувається обробка згідно таблиць маршрутизації. Для цього перебираємо колекцію сортованих пакетів та обробляємо кожен пакет окремо. Для обробки обрано алгоритм швидкого надсилання *Fast forward*. В даному випадку зчитуються лише заголовок пакету з адресами для маршрутизації. Перевірка чексуми не відбувається (як у випадку використання методу *Store and forward* де для кожного пакету обчислюється чексума та звіряється з полем CRC, якщо співпадає – пакет відправляється далі, інакше відкидається і відбувається повторна передача цього пакету). Даний варіант має кращу швидкодію.

Зчитавши адресні дані з пакета при ітерації колекції аналізується мережа призначення. Для цього викливається допоміжний метод для отримання з IP – адреси вузла призначення IP – адреси його підмережі. Далі шукаємо дану підмережу в таблиці маршрутизації. Якщо пошуки були неуспішними, пакет має відправлятися на маршрутизатор за замовчуванням (default getaway). Алгоритм маршрутизації зображено на рис. 3.12. Після обробки усіх пакетів викликається метод для безпосереднього надсилання пакетів мережею.

Для спрощення і надання можливості легкого переключення між режимами обслуговування (традиційним і пропонованим) створено два компаратори (спеціальний клас мови програмування Java для порівняння об’єктів). Так як це дві реалізації одного класу, ми маємо можливість підставляти будь-яку з них в методи, де використовується їх базовий клас.

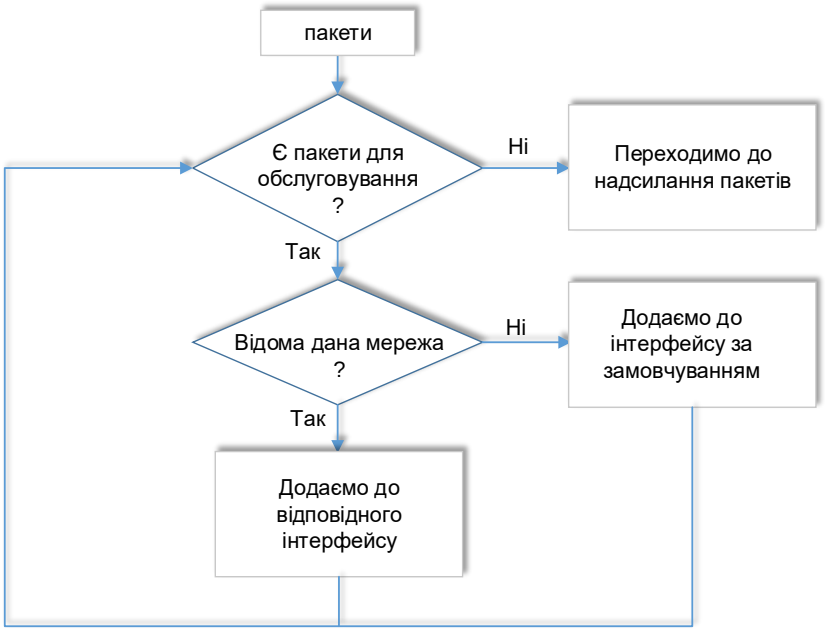


Рис. 3.12. Алгоритм маршрутизації пакетів

Тому для зміни алгоритму обслуговування створено спеціальний метод, який приймає змінну типу boolean (true або false). І в залежності від значення цієї змінної ми «включаємо» та «виключаємо» роботу нового методу. Робити це можна в будь-який час, будь-яку кількість разів в ручну або за допомогою реалізації інтелектуальної логіки управління на основі алгоритмів машинного навчання. Для цього викликається даний метод з основного класу, в якому працює безкінечний цикл, що символізує роботу мережі та займається збором і відображенням статистики і інформації.

3.3. Введення білінгової системи для реалізації запропонованого методу управління якістю послуг

При переході до режиму обслуговування абонентів згідно оцінок QoE стандартна абонентська плата за користування буде нераціональною. Адже в такому випадку всі абоненти платять однаково і відрізняється лише тариф, тобто надана абоненту швидкість. Для забезпечення коректної оплати за користування послугами пропонується оплата безпосередньо за використані

сесії (послуги). В такому випадку немає різниці, яка в абонента швидкість, якщо він замовить послугу з оцінкою «х» - мережа, якщо є змога, обслужить дану сесію з відповідною оплатою та якістю. Оплата може проводитися в такому випадку декількома способами. Основною перевагою такого методу є легка зміна коефіцієнтів оплати. Перед створенням сесії абонент буде обирати собі якість, з якою він хоче її отримати. Сервер, який обслуговуватиме білінг, в свою чергу згенерує оплату за дану сесію. В загальному рівень оплати залежить від завантаженості мережі. Якщо ресурсів для нових сесій є достатньо (мережа не навантажена) то і рівень оплати буде нижчим, адже обслуговування нової сесії не створить ніяких проблем. Проте коли розглядати мережу в години найбільшого навантаження – вартість буде набагато більшою. В такому випадку для забезпечення відповідного рівня, наприклад, для оцінки «5» (найкращої), мережі необхідно буде переконфігуровуватися. Традиційну мережу також можна покращити введенням білінгу за послуги. Для цього серверу який забезпечує білінг необхідно буде знати актуальний стан завантаженості мережі. Забезпечити це можна простим збором статистики з кожного маршрутизатора. Проте в такому випадку статистичні дані зазнаватимуть затримки – відправка мережею до серверу білінгу. Для вирішення даної проблеми пропонується приймати рішення не відразу після запиту клієнта на послугу, а через певний час, необхідний для прийняття актуального стану мережі. Так як всі нові сесії будуть проходити цю процедуру, то варіант, коли при очікуванні генеруватимуться якісь нові послуги відпадає. Організація потоків даних в телекомунікаційних структурах вимагає нових підходів до управління у зв’язку із лавиноподібним збільшення комутаційних правил та трудомісткості управління мережною інфраструктурою. Традиційний підхід до вирішення проблеми мережних взаємодій припускає послідовну обробку одиниць передачі, зокрема пакетів, на кожному рівні еталонної моделі мережної взаємодії ISO/OSI. Одним їх напрямів “модернізації” класичного підходу до організації мережної

архітектури є створення програмно-конфігурованих мереж, що використовують протокол OpenFlow. Час на встановлення консистентності мережі в такому випадку буде мінімальним, адже кожен маршрутизатор матиме окремий виділений сигнальний канал до контролера. Контролером також забезпечуватимуться білінг, маршрутизація та збір статистики.

Алгоритм прийняття рішення, чи є можливість обслуговувати даний запит зображено на рис. 3.13.

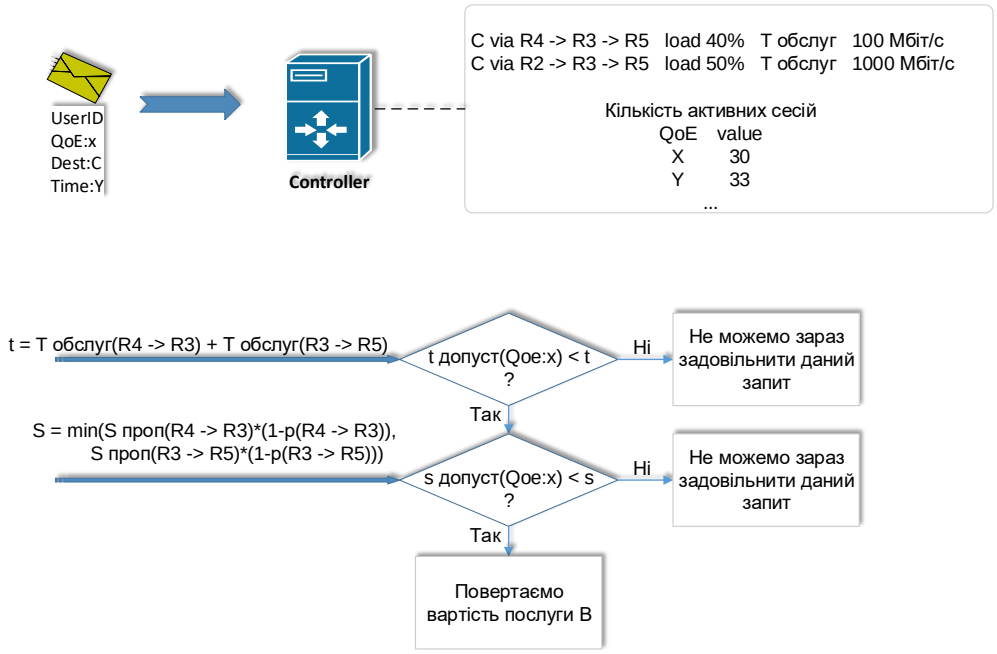


Рис. 3.13. Алгоритм прийняття рішення для нового запиту [179]

де, t – загальний час обслуговування пакетів обраної послуги та QoE оцінки на шляху від відправника до отримувача, $T_{обслуг}$ – час обслуговування пакетів обраної послуги та оцінки на певному лінку, S – розмір вільного ресурсу шляху, який обирається з мінімального значення шляху. Розраховується для одного лінка так: множимо пропускну здатність на вільний ресурс (1 – завантаженість) лінка та порівнюємо отриманий результат з необхідним ресурсом для обраної послуги та оцінки. Якщо отриманий ресурс дозволяє обслужити дану послугу – вертаємо білінг. Інакше переходимо до наступного маршруту і все знову. Якщо більше маршрутів немає – вертаємо відмову в обслуговуванні.

3.4. Алгоритм маршрутизації потоків з балансуванням навантаження в інтенційно-орієнтованих мережах

Як було сказано раніше, таблиця маршрутизації містить декілька маршрутів до кожної мережі, звісно, якщо такі існують. Метою цього є можливість покращити процес обслуговування послуг в мережі. На сьогоднішній день майже всі мережі є мультисервісними. Кожен вид послуги має свої параметри та показники «якісності» сприйняття мережевого обслуговування. Насамперед мережевий трафік ділиться на два види: чутливий до затримок та нечутливий до затримок. Відповідно на транспортному рівні моделі OSI вони забезпечуються відповідними протоколами. Послуги, які потребують обслуговування в реальному часі зазвичай обслуговуються за допомогою протоколу UDP. Послуги, які вимагають гарантоване надсилання пакетів – TCP. UDP— один із протоколів в стеку TCP/IP. Від протоколу TCP він відрізняється тим, що працює без встановлення з'єднання. UDP — це один з найпростіших протоколів транспортного рівня моделі OSI, котрий виконує обмін повідомленнями (датаграмами — англ. datagram) без підтвердження та гарантії доставки. При використанні протоколу UDP відповідальність за обробку помилок і повторну передачу даних покладена на протокол рівнем вище. Але попри всі недоліки, протокол UDP є ефективним для серверів, що надсилають невеликі відповіді великій кількості клієнтів. Для послуг, які обслуговуються протоколом UDP, втрачені пакети не надсилаються повторно.

Виходячи з цих даних, пропонується розділити обслуговування мережевого трафіку згідно використовуваного транспортного протоколу. Наприклад, коли є декілька маршрутів від мережі A до мережі B, трафік реального часу передавати шляхом, який забезпечить найменшу затримку. А трафік, який вимагає гарантованого надсилання і є менш вибагливим до затримок – найменш завантаженим маршрутом. Приклад вибору маршруту зображено на рис. 3.14.

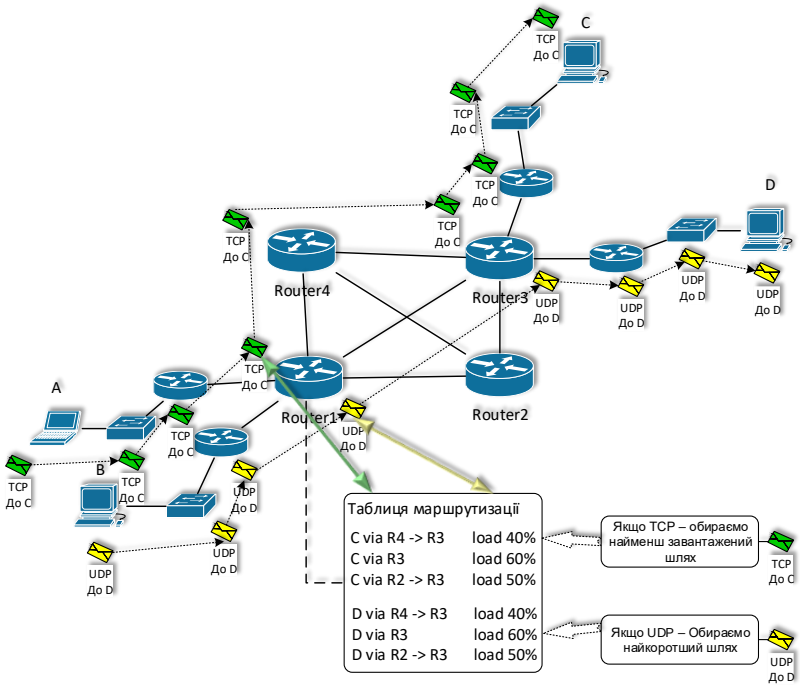


Рис. 3.14. Прийняття рішення для маршрутизації пакетів згідно використовуваного протоколу транспортного рівня

Також пропонується реалізувати інтелектуального балансувальника, який розділяв би завантаження одного порта на всю мережу. Алгоритм роботи балансувальника зображено на рис. 3.15.

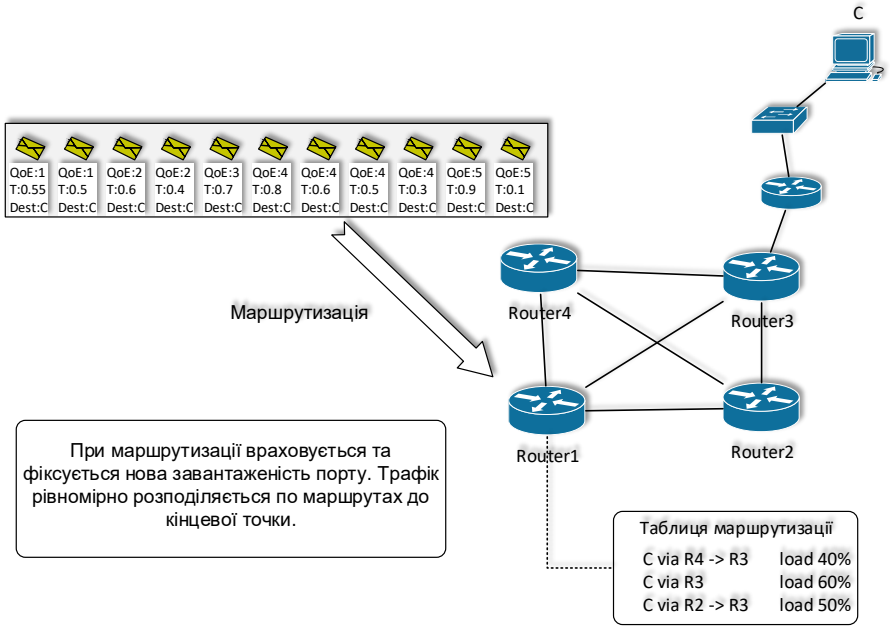


Рис. 3.15. Алгоритм роботи балансувальника в мережі

При маршрутизації пакетів беремо до уваги завантаженість маршруту, яка при доданні нових пакетів змінюється. При досягненні зміни в, наприклад 20% від початкової завантаженості (може бути виставлена з підбором найкращого значення), переключаємося на інший маршрут (якщо такий є) і так циклічно при досягненні дельти завантаженості на кожному маршруті.

3.5. Принцип функціонування нового методу клієнт-орієнтованого управління якістю в традиційних та програмно-конфігурованих IBN мережах

В традиційних мережах обслуговування відбувається почергово, згідно порядку в якому прийшли пакети (рис. 3.16).

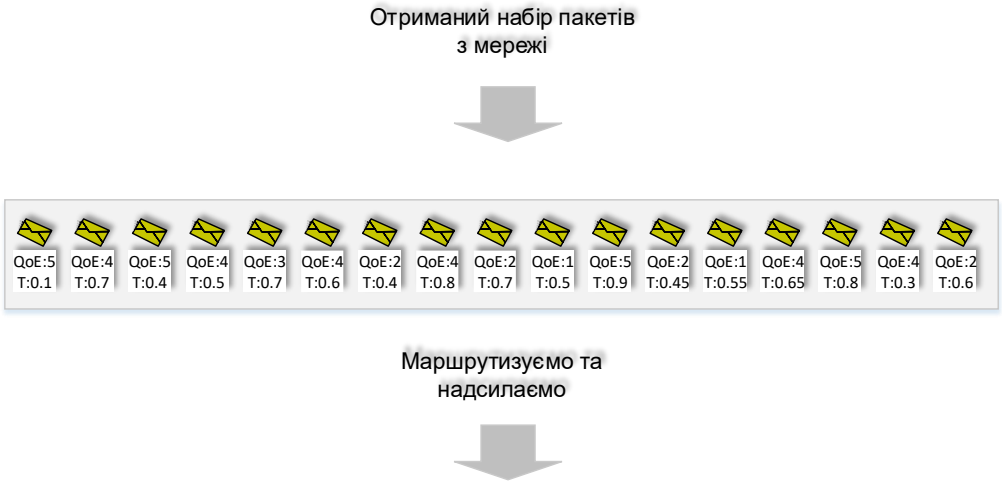


Рис. 3.16. Традиційний метод сортування пакетів

Черги на очікування обслуговування будуть формуватися лише при збільшенні інтенсивності надсилання, або збільшенні абонентів. В першому випадку покращувати щось немає сенсу, адже усі пакети будуть обслужені без затримок. Пропонований метод буде ефективним при утворенні черг на обслуговування. Пропонується чекати певний час пакетів для формування черги. Якби черга була на кількість пакетів, міг би бути варіант, що на нові пакети, при вільній мережі, черга буде чекати довго, що призведе до фатальних затримок. У випадку очікування певного часу ця проблема відпадає. Головним

моментом є той, що при великій черзі, час очікування набору черги буде меншим ніж час обробки всіх пакетів. Основною ідеєю є сортування пакетів в черзі на обслуговування за певними параметрами.

В такому варіанті не враховуються бажані абонентські оцінки рівня обслуговування. Пропонується сортування за таким принципом: найшвидше будуть обслуговуватися пакети з найвищою оцінкою та з найменшим часом, що залишився на надсилання. Алгоритм сортування пакетів зображено на рис. 3.17.

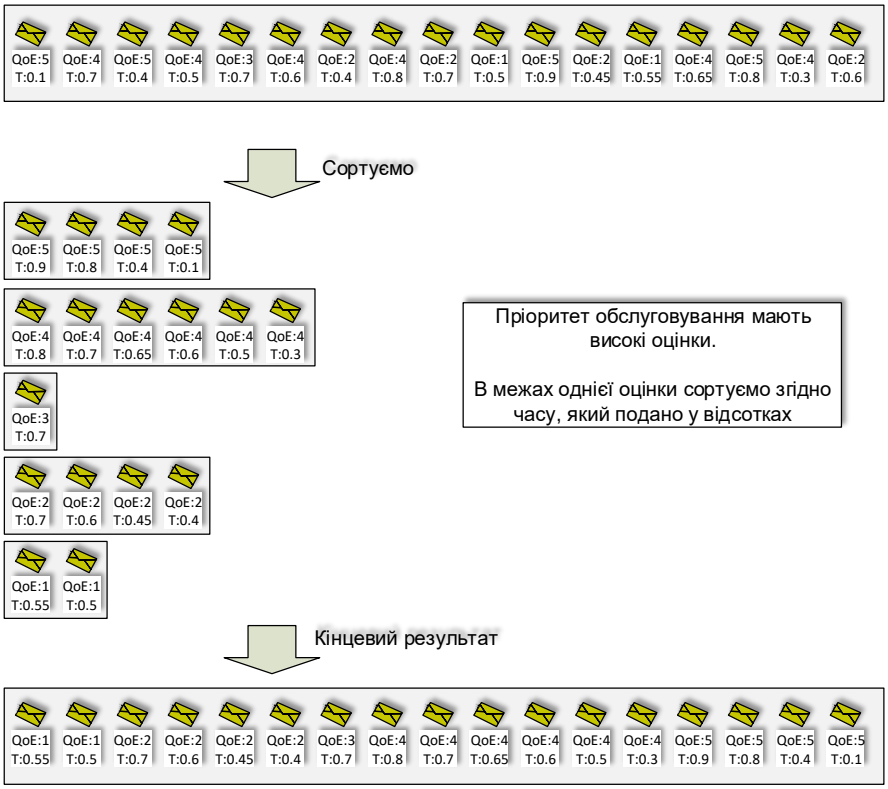


Рис. 3.17. Пропонований клієнт-орієнтований метод сортування пакетів [179]

Цей час для кожного виду послуг є свій. Пропонується маркувати пакети додатковим полем для часу на надсилання мережею. Найкращим місцем для впровадження даного поля – замість поля TTL (Time to live,). Загальна ідея залишиться та ж сама (пакет може існувати в мережі обмежений період часу, вичерпання якого ініціює відкидання даного пакету). Проте для нашого методу він дасть додаткову можливість забезпечення відповідного порядку на обслуговування. Кожен маршрутизатор в процесі надсилання відніматиме від

даного поля час, затрачений на його обслуговування. Для поєднання різних видів послуг даний час при сортуванні пропонується обраховувати у відсотковому еквіваленті. В такому випадку послуги відповідної оцінки будуть мати відповідну пріоритетність обслуговування.

Від звичайного сортування даний метод відрізняється можливістю сортування не за видом сервісу, а за відповідною оцінкою та введенням додаткової можливості керування трафіком згідно часу, що залишився на існування пакету. Остання можливість дає нам змогу зберегти пакети, у яких залишилося мало часу на надсилання, поставивши в чергу їх на перше місце.

В даному випадку, якщо обслужити пакет, в якого залишився мінімальний час на надсилання, швидше пакету, в якого часу ще достатньо – для другого якість суттєво не погіршиться. Але в такому випадку ми можемо уникнути відкидання першого пакету. Також час очікування даним пакетом (з оцінкою 5 та мінімальним часом на надсилання) набору черги буде меншим, ніж якби ми обслуговували пакети в даному порядку без сортування. В останньому варіанті даний пакет вже не отримує обслуговування. Даний алгоритм обслуговування можна покращити в SDN мережах. Так як дана мережа може вести статистику по кожній сесії, в процесі сортування можна враховувати ще один фактор – кількість відкидань пакетів певної сесії. Кожен вид сервісу має своє значення нормальної кількості можливих відкидань пакетів. Тому у випадку коли в нас два однакових пакети різних сесій з однаковим малим часом на надсилання будуть обслужені в правильному порядку – спочатку пакет, кількість відкидань для сесії якого є більшим, потім інший. Це в свою чергу додатково покращить показники якості обслуговування сесій в мережі.

3.6. Покращення якості обслуговування в умовах ведення IBN контролера

Традиційні мережі мають обмежені можливості для покращення методів обслуговування пакетів в мережі. Настає момент коли покращити якість обслуговування більше неможливо. В такому випадку пропонується

поступовий перехід до мережі SDN. При експлуатації мережі, час від часу мережеве обладнання виходить з ладу і найкращим рішенням є заміна на вузли з підтримкою обох методів обслуговування. З часом мережа дійде до того, що будуть з'являтися окремі сегменти, які можна буде обслуговувати лише контролером. В кінцевому результаті вся мережа перейде на нове обладнання. Введення контролера для реалізації IBN зображено на рис. 3.18.

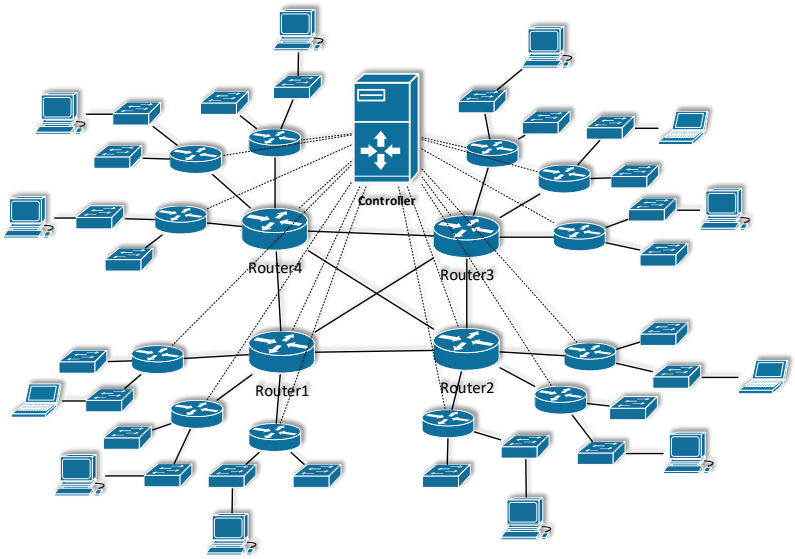


Рис. 3.18. Введення контролера в мережу

Контролер забезпечує багато переваг. Наприклад, контролер здійснює маршрутизацію і розповсюдження таблиць, замість маршрутизаторів. В цьому випадку мережа стає чутливою до змін топології та завантаженості. Час відгуку стає мінімальним, що дає змогу майже миттєво приймати рішення. Це стосується маршрутизації та забезпечення білінгу. Контролер збирає статистику з вузлів мережі. Завдяки чому при запиту на встановлення нової сесії не потрібно буде чекати певний час для коректного встановлення білінгу, що в свою чергу покращує показник задоволення абонента.

Також завдяки цьому покращується робота балансувальника та алгоритму вибору маршруту. Відбувається це все завдяки тому, що статистика по мережі є найновішою. Тобто, якщо якийсь віддалений вузол вийде з ладу, контролер буде знати це в найближчій ітерації мережі.

Розповсюдження таблиць маршрутизації контролером покращує зразу декілька параметрів. По-перше, час встановлення консистентності такої мережі буде мінімальним, адже кожен маршрутизатор матиме сигнальний канал до контролера. По-друге, мережа звільняється від лишньої сигнальної інформації, що поширювалася в мережі. В традиційних мережах, таблиця маршрутизації передається від кожного маршрутизатора до його сусідів, де порівнюється та обробляється. В даному розділі розглянуто основні моменти структури додатку моделювання роботи мережі. Запропоновано алгоритми та методи маршрутизації, білінгу, балансування в мультисервісних мережах. Розглянуто процес моделювання роботи мережі розробленою програмою.

3.7. Дослідження ефективності використання методу адаптивного клієнт-орієнтованого управління якістю послуг в IBN мережі

Загальний вигляд інтерфейсу імітаційної моделі показано на рис. 3.19.

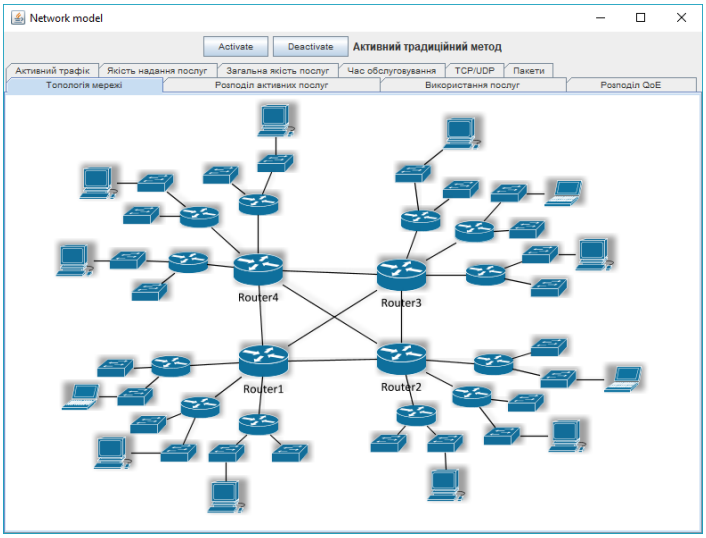


Рис. 3.19. Інтерфейс імітаційної моделі досліджуваної інфокомунікаційної мережі [179]

Дана програма має графічний інтерфейс для користувачів, за допомогою якого можна переключати методи обслуговування та отримувати результати. Програма складається з двох кнопок та десяти вкладок. Кнопки відповідають за

методи обслуговування. Activate – увімкнути новий метод обслуговування, Deactivate – перемкнути на стандартний метод. Поряд з кнопками виводиться інформація, який метод в даний момент активний. Далі розміщені вкладки такі як: топологія мережі; розподіл активних послуг; використання послуг; розподіл QoE; активний трафік; якість надання послуг; загальна якість послуг; час обслуговування; TCP/UDP; пакети.

Вкладки даної програми можна умовно поділити на два види – основні та додаткові. До додаткових вкладок можна віднести ті, які відображають статистику мережі, яка не залежить від використовуваного методу обслуговування пакетів в мережі. Тобто при зміні даного методу, інформація на даних вкладках залишатиметься незмінною. Вони подані для відображення детальнішої статистики роботи мережі. Дані вкладки розглянемо без перемикання методу обслуговування пакетів.

До основних вкладок відносяться ті, дані яких будуть змінюватися при перемиканні методу обслуговування пакетів в мережі. Вони мають найбільшу інформаційну цінність, тому що дають змогу порівняти ефективність функціонування методів обслуговування пакетів. На основі даних поданих на цих вкладках проведемо порівняльний аналіз двох методів – «традиційного» та запропонованого. Розглядати результати роботи мережі, подані на цих вкладках, будемо з перемиканням методу обслуговування.

Розпочнемо з додаткових вкладок.

Вкладка *«Топологія мережі»* містить зображення топології мережі, яка досліджується, дана вкладка була зображена на рис. 3.19. Інформація подана для кращого розуміння та наочного відображення досліджуваної мережі.

Вкладка *«Розподіл активних послуг»* містить кругову діаграму, яка відображає у відсотковому співвідношенні активні в мережі в даний момент використовувані послуги, зображення подано на рис. 3.20. Завдяки цьому графіку ми знаємо співвідношення активних послуг, що обслуговуються в

даний момент в мережі. До основних видів послуг, згідно даної діаграми, належать: відеоконференції, IPTV, звичайні дані, та голосовий зв'язок.

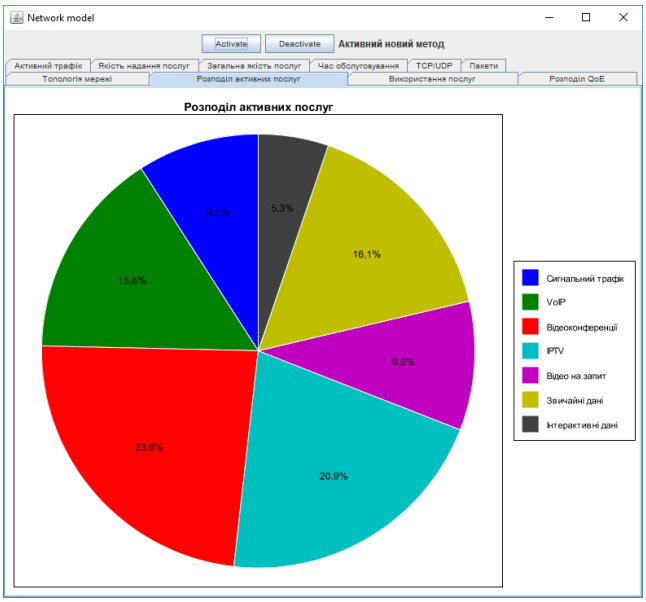


Рис. 3.20. Розподіл активних послуг у відсотковому співвідношенні

Наступна вкладка *«Використання послуг»* розширює інформацію про використовувані послуги. Тут подано графік використання послуг відносно часу моделювання, згідно якого ми маємо інформацію не лише на даний момент, а й впродовж моделювання. Даний графік зображено на рис.3.21.

Рис. 3.21. Розподіл послуг мережі відносно часу моделювання

На даному графіку, відповідно до діаграми, поданої на рис. 3.21., відображено кількість активних сесій кожного виду послуг. Тобто, якщо на рис.3.20. «відеоконференції» мали найбільший відсоток використання, то на цьому графіку дана послуга буде мати найбільшу кількість сесій. Цінністю даного графіку є можливість аналізувати, які види послуг обслуговувалися мережею, протягом певного часу.

Вкладка *«Розподіл QoE»* містить кругову діаграму, яка відображає у відсотковому співвідношенні, оцінки послуг, які зараз обслуговуються. Дану діаграму зображено на рис. 3.22.

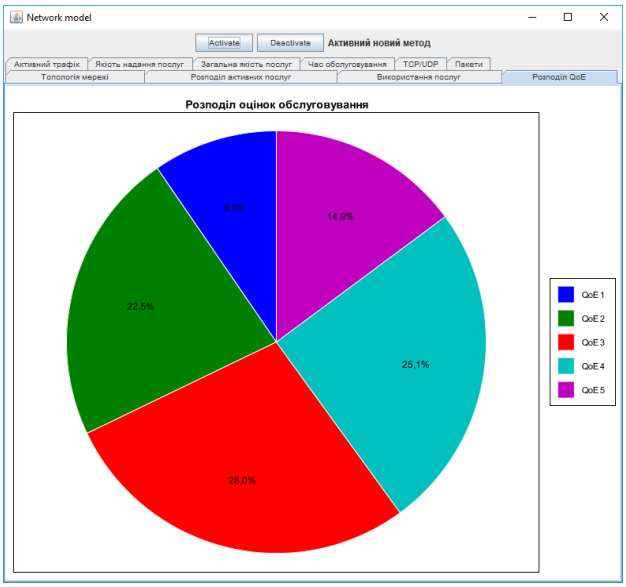


Рис. 3.22. Відсоткове співвідношення оцінок, обслуговуваних мережею

На даній діаграмі відображено розподіл активних оцінок, які клієнти обирають для своїх послуг, у відсотковому співвідношенні. Відповідно до даної діаграми, в мережі найменше послуг з оцінкою «1», та найбільше послуг з оцінкою «3». За допомогою даної діаграми ми можемо бачити, співвідношення оцінок сесій, що зараз обслуговуються мережею.

Вкладка *«Активний трафік»* відображає інформацію згідно трафіку обслуговуваних послуг в мережі. Тут подано графік відношення кількості трафіку в Мбіт до ітерації мережі. Даний графік зображено на рис. 3.23. На даній вкладці розміщено декілька графіків. Згідно легенди, вони відповідають

за кожен вид можливих послуг мережі, та один окремий – для загального трафіку. За допомогою даного графіку ми можемо отримати результати генерованого трафіку по кожному виду послуг. Загальний трафік відповідає сумі трафіків усіх послуг мережі.

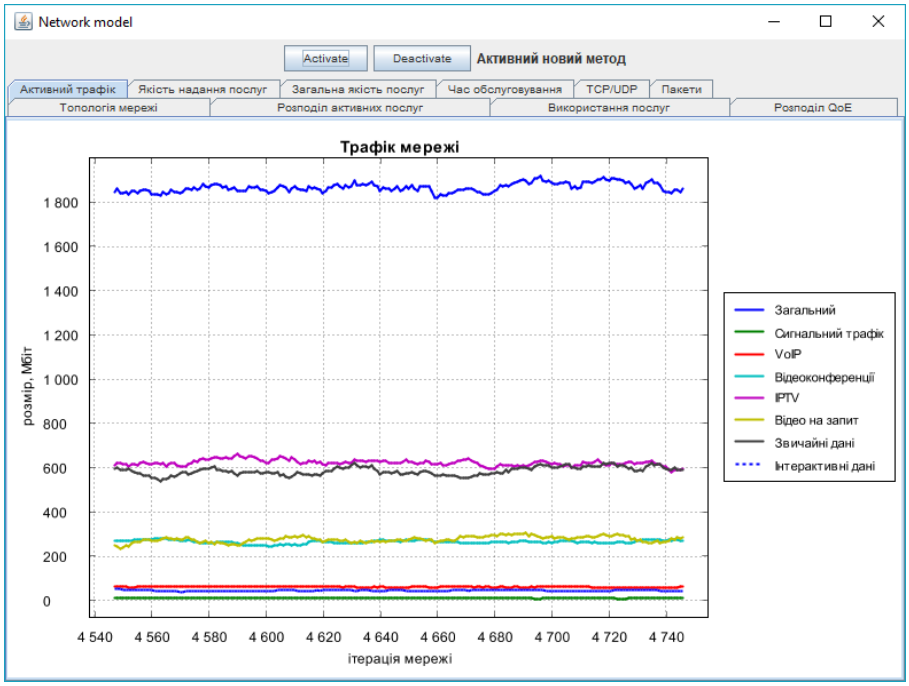


Рис. 3.23. Трафік мультисервісної мережі

Згідно розподілу послуг, поданого на рис. 3.23., чим популярнішою є послуга – тим більше трафіку буде даного виду. Також тут потрібно враховувати середній розмір пакетів кожного виду послуг. Тут відображається статистика зібрана по всій мережі.

Далі розглянемо вкладку *«Пакети»*. Тут, відповідно до назви, відображено графік зміни кількості обслуговуваних пакетів в мережі. Приклад зображено на рис. 3.24. Завдяки цьому графіку ми маємо інформацію про кількість пакетів, що обслуговувалися даною мережею за відповідний проміжок часу. Наступні вкладки розглянемо в поєднанні з двома методами обслуговування пакетів в мережі. Завдяки чому зможемо зробити висновки ефективності запропонованого методу.

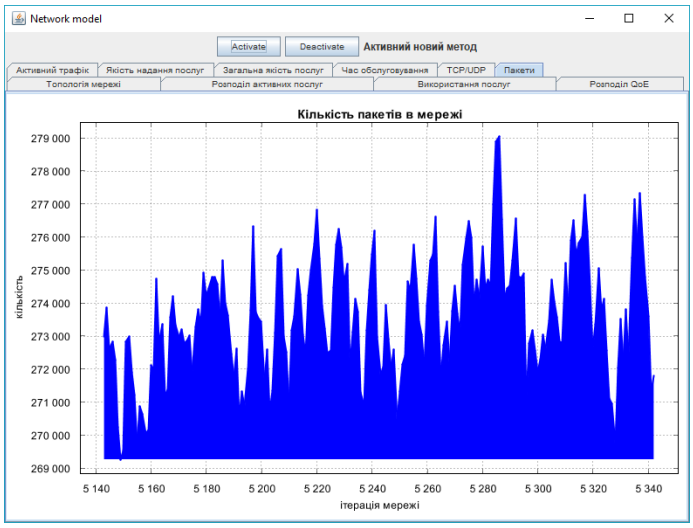


Рис. 3.24. Графік обслуговуваних пакетів в мережі

Вкладка *«Якість надання послуг»* містить інформацію про результати надання послуг для абонентів мережею. Також тут в правому нижньому куті показано виграш у разах – у скільки разів активний метод кращий від попереднього. На першому етапі моделювання (поки ще не змінювався метод обслуговування пакетів в мережі тут буде відображатися відношення добре обслужених сесій до погано обслужених сесій). Дані діаграми будуються на основі інформації, зібраної від отриманих клієнтами пакетів. Кожен вид послуг має свій еталонний час затримки надсилання пакетів. При використанні нового методу згруповані на оцінки QoE, кожній послузі, відповідно до оцінки вказано час затримки. Чим більша оцінка – тим меншу затримку повинні зазнавати пакети в процесі обслуговування. Відповідно оцінка «1» матиме найбільший час обслуговування, а оцінка «5» - найменший час обслуговування. При побудові діаграм ми перебираємо усі отримані сесії, та порівнюємо з «еталонним» часом для даної послуги та даної оцінки. Якщо час менший за допустимий – послугу надано мережею добре, інакше послугу надано погано.

Вкладка *«Загальна якість послуг»* розширює інформацію з попередньої вкладки. Вона відображає ту ж інформацію, тільки не на даний момент, а протягом певного проміжку моделювання. Максимальне значення для графіків

на даній вкладці «1», мінімальне «0». Чим більше значення – тим краще відношення добре обслужених сесій до погано обслужених.

Вкладка *«Час обслуговування»* подає інформацію про час обслуговування для кожного виду послуги та кожної оцінки даної послуги. В загальному результаті 35 графіків. Також, як і в попередній вкладці, тут показано виграш у разах, відносно попереднього активного методу обслуговування пакетів в мережі. Для цього виділено дві групи сесій мережі – чутливі до затримок та нечутливі до затримок. До першої групи ми відносимо сесії з транспортним протоколом UDP з оцінками 3, 4 та 5, так як для даний вид трафіку необхідно обслужити якнайшвидше. До нечутливих відносимо решту видів сесій: усі сесії з транспортним протоколом TCP, та оцінки 1 та 2. Спочатку розглянемо при ввімкнутому традиційному методі. Результат зображено на рис. 3.25.

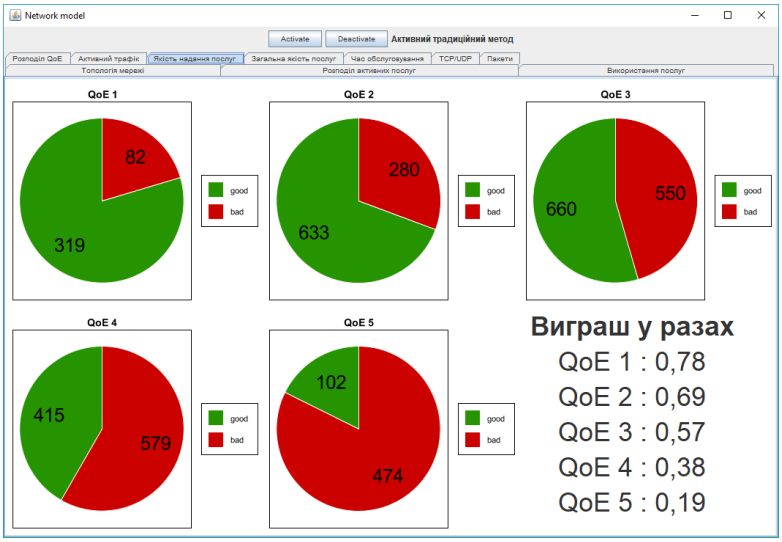


Рис. 3.25. Якість обслуговування пакетів в мережі при традиційному методі

З даного рисунку бачимо, що найкраще обслуговуються сесії оцінки «1». Зі збільшенням даної оцінки якість надання послуг падає. Для найвищої оцінки кількість сесій, що успішно обслуговуються мережею є мінімальною.

Дані результати отримуємо з того, що при традиційному методі пакети не сортуються та обробляються відповідно порядку, в якому прийшли на обслуговування. Тобто мережа не може гарантувати відповідної якості

обслуговування сесії для обраної оцінки. Порядок обслуговування матиме хаотичний характер для послуг різних оцінок. Даний результат подано на рис.3.26.

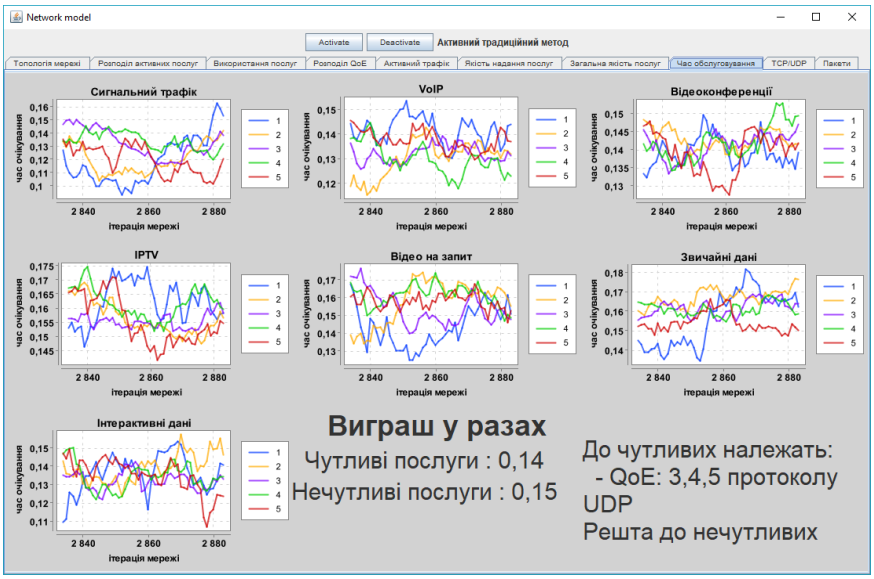


Рис. 3.26. Середній час очікування для кожної сесії відповідної оцінки при традиційному методі

Активуємо пропонований метод обслуговування пакетів в мережі, натиснувши для цього кнопку «Activate». Про успішний перехід свідчить зміна напису з активним методом обслуговування пакетів в мережі. Тепер розглянемо ті ж графіки знову. Згідно рис. 3.28, при новому методі обслуговування пакетів в мережі, ми значно покращуємо якість для сесій з вищими оцінками. Так якість обслуговування сесій покращилася : з оцінкою «5» у 5,17 разів; з оцінкою «4» у 2,30 разів; з оцінкою «3» у 1,15 разів.

Проте, повинен зберігатися закон збереження – коли ми покращуємо якість обслуговування одних послуг, ми погіршуємо якість обслуговування інших послуг. Відповідно якість погіршується для сесій: з оцінкою «2» у 0,3 0 разів; з оцінкою «1» у 0,23 разів. Згідно кругових діаграм майже всі сесії з оцінкою «5» отримали хорошу якість обслуговування. Також якість обслуговування покращилася для оцінок «4» та «3».

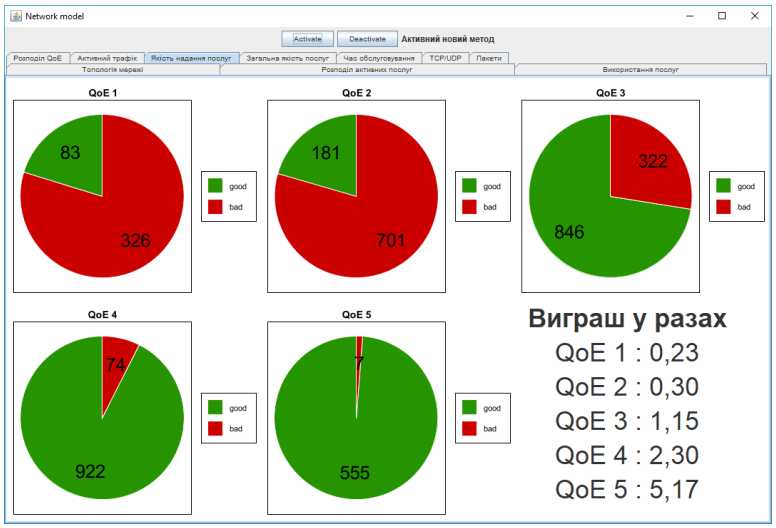


Рис. 3.27. Якість обслуговування пакетів в мережі при використанні пропонованого методу

Основна ідея, що для абонентів, які користуються послугами з оцінками «1» та «2» встановлено дуже низьку оплату. Користувачі не потребують найкращої якості та погоджуються, з тим, що їхні сесії зазнаватимуть тривалої затримки та повторних надсилань. Протилежно для абонентів, які потребують найкращої якості обслуговування (наприклад запланована ділова бесіда чи відеоконференція, комфортна гра в онлайн ігри та інші) пропонуються вищі оцінки. Для них оплата відходить на другий план, основне – якість даної сесії.

Зміну якості можна спостерігати на рис. 3.28, на якому явно видно зміни якості надання послуг.

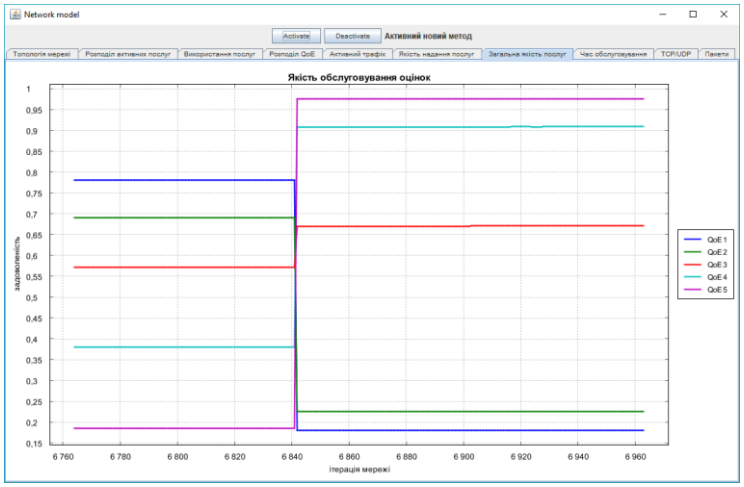


Рис. 3.28. Зміна якості обслуговування послуг різних оцінок QoE [179]

Відповідно до змін якості обслуговування послуг різних оцінок QoE змінилися і середній їх час обслуговування. Даний графік показано на рис. 3.29.

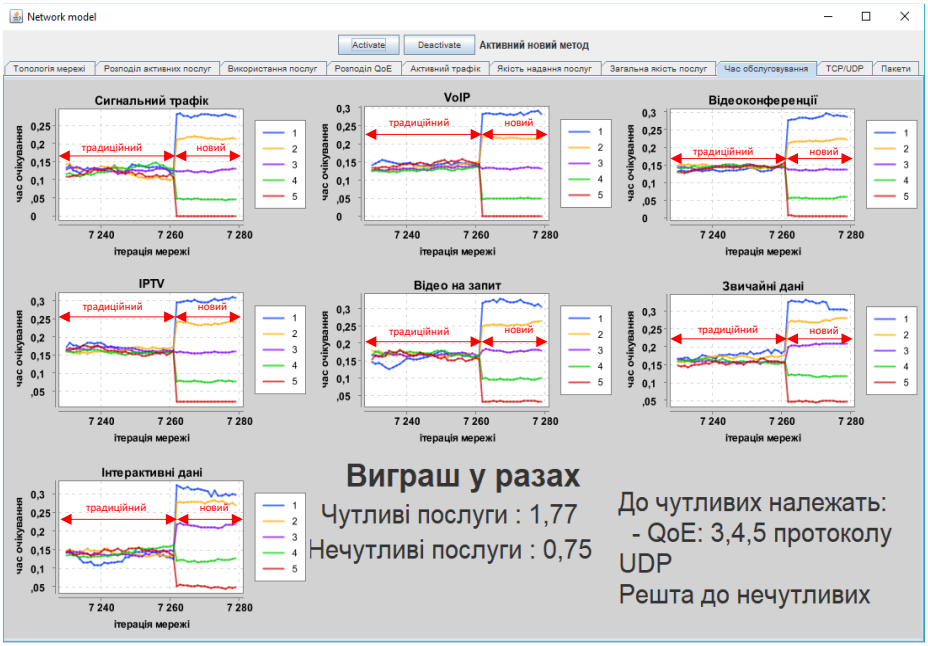


Рис. 3.29. Середній час очікування для кожної сесії відповідної оцінки при використанні пропонованого методу [179]

З даного графіку добре видно зміни при переході з традиційного методу обслуговування на пропонований. Середній час очікування обслуговування для кожної послуги змінився відносно поданого раніше виграшу. Для оцінок «5», «4» та «3» він зменшився. Для оцінок «1» та «2» - збільшився. Тепер обслуговування пакетів не є хаотичним. В такому режимі мережа може забезпечити відповідне обслуговування для високих оцінок. Також варто зауважити на зміни середнього часу обслуговування для чутливих та нечутливих сесій. Даний результат детальніше подано на рис. 3.29. Для чутливих сесій ми маємо покращення обслуговування в 1,77 рази. Проте для нечутливого трафіку ми маємо погіршення в 0,75 разів.

На даній вкладці *«TCP/UDP»* відображається середній час обслуговування для послуг, які використовують два види транспортних протоколів – TCP та UDP. На рис. 3.30. від початку ітерації до 10220 зображено середній час при

використанні традиційного методу обслуговування пакетів в мережі, після 10220 ітерації використовується пропонований метод. При переключенні з традиційного методу обслуговування на пропонований ми спостерігаємо зміну середнього часу обслуговування.

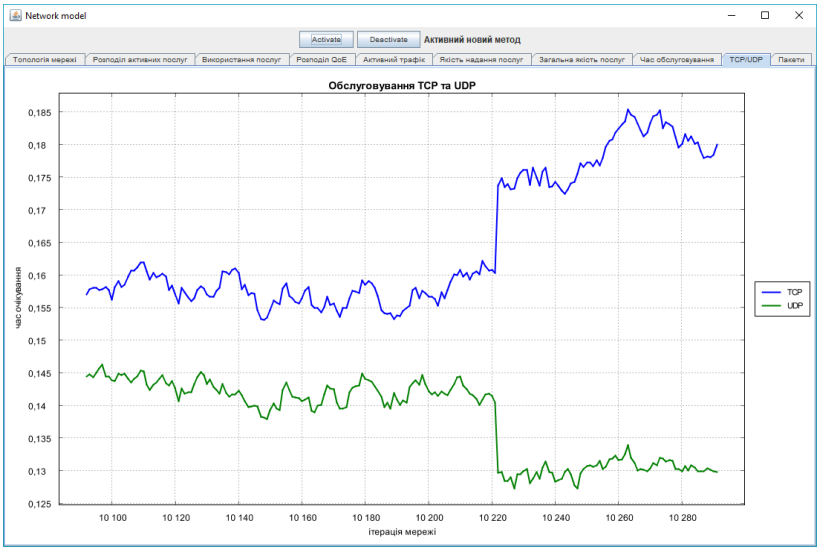


Рис. 3.30. Середній час обслуговування послуг з TCP/UDP при використанні пропонованого методу

Сесії, які використовують транспортний протокол TCP зазнають збільшення середнього часу обслуговування. Сесії, які використовують транспортний протокол UDP зазнають покращення.

Основною ідеєю таких змін є те, що TCP трафік може мати більший час на надсилання, та в разі відкидань пакетів їх повторне надсилання. Проте UDP трафік чутливий до затримки і не передається повторно при відкиданні.

3.8. Структурно-функціональна схема розробленої імітаційної моделі концептуальної IBN мережі з інтелектуальною логікою управління

Насправді моделювання впливу контекстних параметрів на задоволеність споживачів та їх відображення за єдиною шкалою якості QoE є складним процесом, який зумовлений наявністю великої кількості об’єктивних та суб’єктивних факторів. Деякі з цих факторів можна виміряти, а інші -

приховати та впливати опосередковано. У цьому випадку ці фактори часто розглядаються або окремо, або їх відображення в різних масштабах. Еволюційний розвиток соціально-економічних процесів та інформаційних технологій накладає деякі обмеження на актуальність QoE моделей управління якістю надання послуг. Питання про врахування нестаціонарності потреб та очікувань споживачів інформаційно-телекомунікаційних послуг при оцінці QoE є відкритим в наукових дослідженнях .Таким чином, через зміщення акценту на технічних питаннях до питань бізнесу та необхідності врахування домінуючого характеру якісних, невизначених та нечітких факторів при формуванні думки щодо рівня якості мережевих послуг, використання методів інтелектуального аналізу даних виправданий та доцільний у роботі.

Попередні результати отримано при моделюванні традиційної мережі, з введенням контролера, який:

– надає білінг абонентам;

– збирає статистику роботи мережі;

– збирає статистику якості обслуговування абонентів.

До основних мінусів використання традиційних мереж є:

– слабка інтеграція з білінговою системою;

– повільна реакція на зміну топології мережі;

– повільна реакція (або взагалі відсутня) на завантаження мережі, яка залежить від системних адміністраторів;

– немає змоги «вести» сесії в контролері.

Майже усі проблеми пов'язані з часом встановлення консистентності мережі у своїх аспектах. Розглянемо проблеми традиційних мереж при прийнятті рішення щодо маршрутизації з використанням пропонованого методу (балансувальника). Нагадаємо, що пропонується зберігати не лише найкращий маршрут до певної мережі, а усі можливі (без петель) та відповідного завантаження даного маршруту. Це завантаження виставляється, як найбільше завантаження на усіх переходах. Плюси даного методу – ми

розділяємо завантаження мережі на декілька інтерфейсів та розділяємо, за змоги, шляхи обслуговування трафіку UDP та TCP. Основною проблемою використання даного методу в традиційних мережах є час встановлення консистентності. Так як рішення має прийматися відразу, мережа може пропустити пікову зміну трафіку. Зокрема рішення прийматиметься, що на даному шляху завантаженість та, що виставлена в таблиці маршрутизації, проте за час, поки сигнальна інформація надійде до даного маршрутизатора завантаженість шляху може зрости, що викличе відповідні проблеми (перевантаженість шляху – буферизація пакетів, відкидання та повторне надсилання). Керуванням процесом обслуговуваного трафіку в мережі показано на рис.3.31. Кружечками показано час, коли приймається рішення. Відповідно в такому випадку мережа може «пропустити» зміни в завантаженості, та приймати не найкращі рішення.

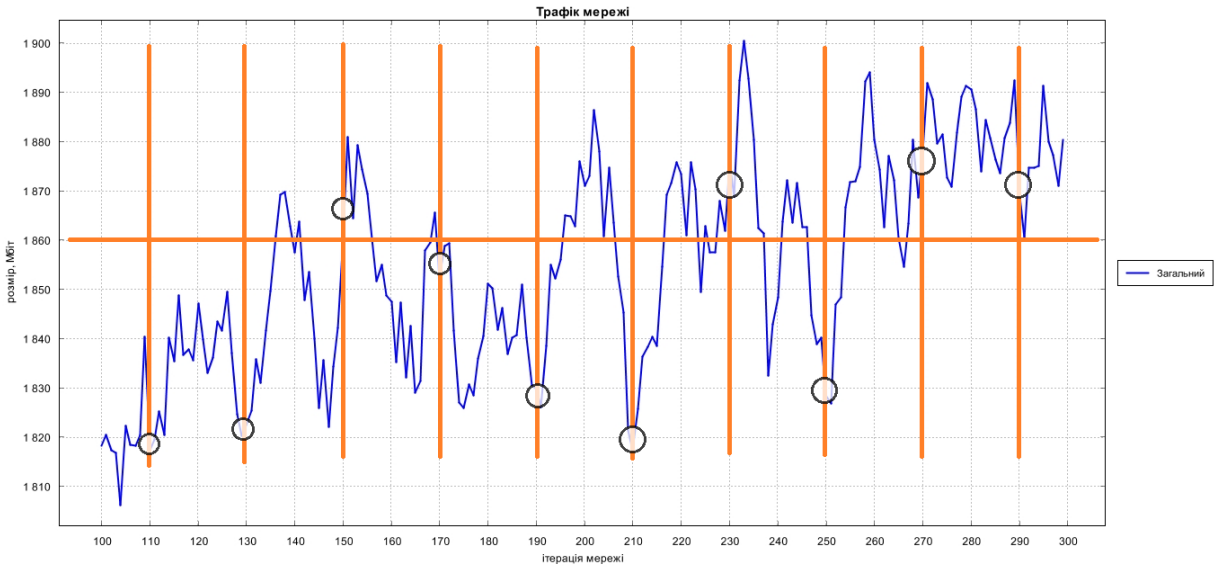


Рис. 3.31. Точки прийняття рішення про зміну конфігурації мережі IBN

Усі згадані проблеми вирішуються при переході до мереж нового покоління. В яких IBN контролер збирає статистику з кожного вузла. Для встановлення консистентності інформації необхідно мінімальний час, що в свою чергу покращує роботу балансувальника (більше не буде випадків

«пропусків» піків), дає змогу «вести» сесії (можливість відкидання дозволеної кількості пакетів в процесі надсилання, за необхідності), робить мережу чутливою до змін топології та інші.

Подальший розвиток запропонованого методу здійснюється в напрямку використання алгоритмів машинного навчання та методів формування статистичних вибірок, що характеризують параметри мережі з відомими оцінками якості QoE користувачів. Використання алгоритмів машинного навчання дають змогу швидше реагувати на несприятливі поєднання значень показників якості і попереджати ситуації, коли користувач незадоволений якістю отриманих сервісів для адаптивного прогнозування моменту переконфігурації мережі шляхом наперед сформованих правил для контролера мережі щодо процесу передавання інформаційних потоків. Структурно-функціональна схема розробленої імітаційної моделі концептуальної IBN з інтелектуальною логікою управління показано на рис. 3.32.

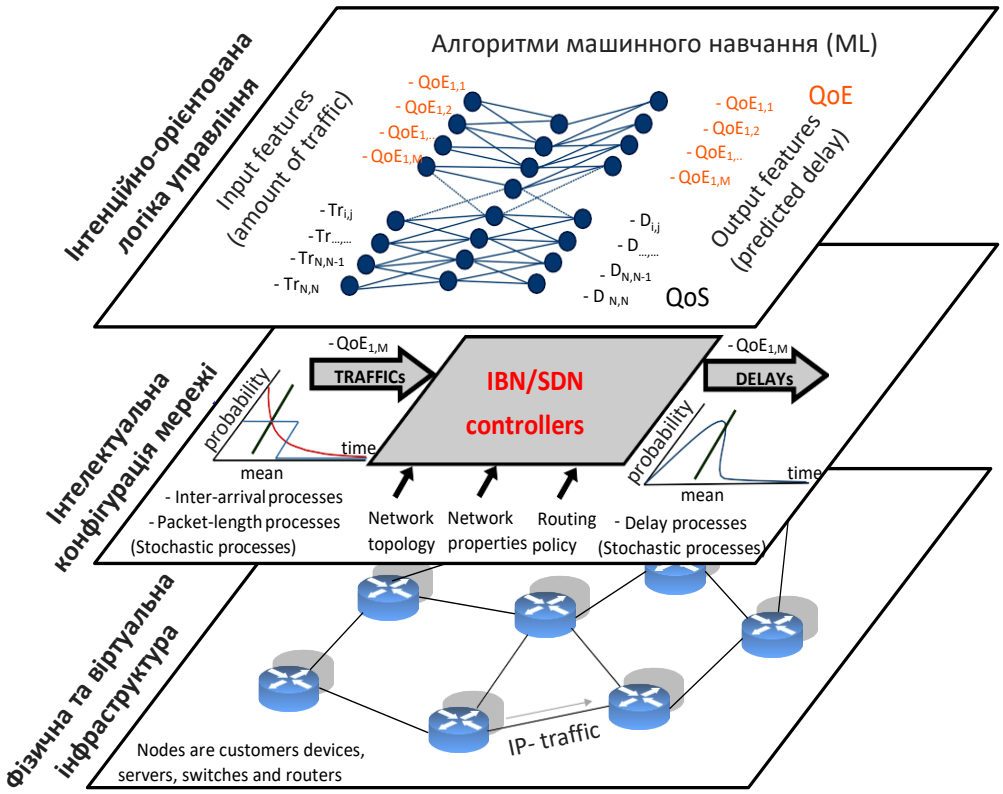


Рис. 3.32. Структурно-функціональна схема розробленої імітаційної моделі концептуальної IBN з інтелектуальною логікою управління [179]

На рис. 3.33. показано схему прогнозування рівня задоволеності користувача за оцінкою QoE для виявлення моментів переконфігурації IBN мережі та зменшення часу переконфігурації.

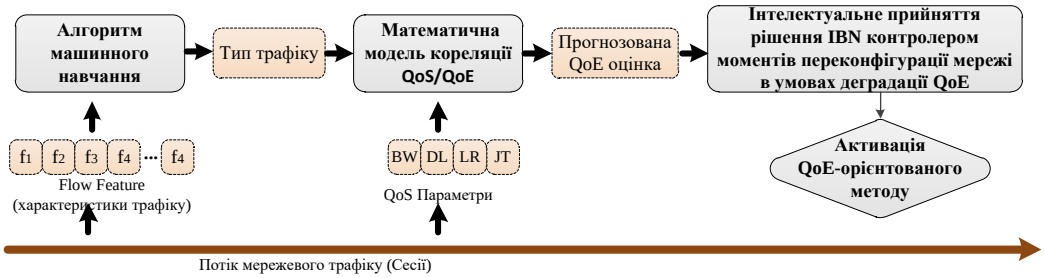


Рис. 3.33. Схема прогнозування моментів погіршення QoE

Інтелектуальна система моніторингу нормованого критерію якості обслуговування користувача згідно вище запропонованої схеми показано на рис. 3.34. В результаті моделювання встановлено, що використання запропонованої схеми управління дає змогу забезпечити швидше відновлення рівня якості сприйняття в умовах його погіршення.

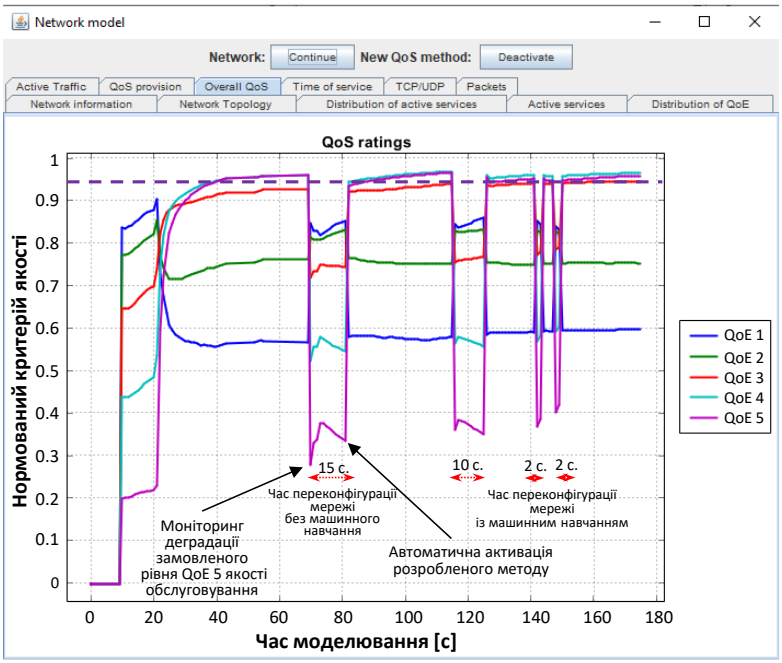


Рис. 3.34. Інтелектуальна система моніторингу якості мережі за критерієм QoE

Таким чином, у майбутньому автоматизація мережі на основі контролерів та алгоритмів машинного навчання, що підтримується технологією SDN/IBN

може покращити ефективність цифрового бізнесу. У майбутньому інформаційні технології IBN дадуть змогу автоматизувати управління всіма мережевими доменами, включаючи містечка, філії, глобальну мережу, Інтернет речей, 5G та великі дані, забезпечуючи значно новий рівень автоматизації, підвищуючи ефективність обслуговування, швидкість запуску інновацій та надійність мережевої інфраструктури.

Для ефективного впровадження централізованого управління мережею необхідно врахувати деякі цікаві аспекти, які слід включити на початку планування, щоб не зробити мережу небезпечною або недоступною, наприклад:

– Доступність контролера - головний аспект, який слід враховувати. Сильний взаємозв'язок між мережевими пристроями та контролером може бути проблемою, коли правила потрібно змінювати. Більше того, якщо мережі розроблені з урахуванням лише одного централізованого контролера, це може бути "єдиною точкою відмови". Розподілений підхід може бути застосований для забезпечення доступності та запобігання потенційним небажаним збоям. Крім того, для забезпечення надійності можна використовувати спеціальне рішення щодо резервування чи резервного копіювання. Захищеність та цілісність програмно-визначених мереж залишається важливим питанням враховуючи, що контролер є єдиною точкою несправності. Таким чином, для вирішення цієї проблеми можна адаптуватися до використання еластичної розподіленої архітектури контролера, яка функціонує шляхом логічної централізації площини управління, яка фізично розподілена, і вирішує такі проблеми, як масштабованість та надійність мереж. При дисбалансах навантаження, мережевий потік починає демонструвати випадкові тенденції, тому є сенс перенести комутатор із сильно завантаженого контролера на слабо завантажений. Хоча це не означає, що зловмисник не зможе повторити свою атаку на площину управління, але це безумовно забезпечує більшу безпеку.

– Масштабованість мережі також залежить від контролера, який потенційно може стати вузьким місцем. Якщо на контролер доставляється

занадто багато пакетів, мережа може мати проблеми з продуктивністю. Це означає, що важливо враховувати розподіл площини управління, щоб уникнути цих небажаних проблем.

– Також важлива безпека. Контролер - це компонент з критичним знанням мережі, саме ця особливість піддає контролер можливим атакам та загрозам. Крім того, канали між контролером і комутаторами можуть бути вразливими. Відповідно до специфікації OpenFlow, можна використовувати захищений зв’язок через протокол TLS, але його використання залежить від структури мережі, тому слід використовувати інтелектуальні DPI системи, систему моніторингу та аналізу мережевого трафіку, що дають змогу автоматизовано виявляти атаки та аномалії трафіку. Розроблення нової інтелектуальної DPI системи для IBN мереж розглянуто у розділі 4.

На основі дослідження ми довели, що майбутня мережа на основі намірів з використанням контролерів IBN/SDN може стати важливим кроком у розвитку мережевих технологій, допомагаючи компаніям оптимізувати мережеві операції та збільшувати доступність. Очевидно, що перехід на нову технологію потребуватиме часу, але можна очікувати, що концепція IBN поступово замінить традиційний підхід і буде впроваджуватися у зростаючу кількість корпоративних мереж.

Висновок до розділу 3

1. У цьому розділі роботи встановлено, що сервіси, які з'являються в майбутніх мережах, вимагають нових QoE-орієнтованих бізнес-моделей, які повинні використовуватися постачальниками послуг в пропонованому договорі зі своїми клієнтами.

2. У роботі пропонується підхід до забезпечення задоволеності клієнта, який відповідає якості обслуговування, з урахуванням очікувань клієнта, що пред'являються до QoE вимогам. Такий підхід добре вписується в концепцію мережі IBN, яка здатна розраховувати поведінку додатків і клієнтів, навчання і

реконфігурацію в процесі експлуатації, з метою мінімізації експлуатаційних витрат, поліпшення QoE, надійності і безпеки мережевих процесів. Розроблена методика заснована на нових алгоритмах маршрутизації потоку даних з системою балансування навантаження і білінгу. Використання білінгової системи дасть змогу клієнтам адаптивно замовити необхідну якість обслуговування для оцінки від 1 до 5 через персональні онлайн-офіси за певною ціною і отримати високу якість обслуговування в умовах високого навантаження мережі.

3. Розроблено імітаційну модель IBN з можливістю перемикання між двома методами обслуговування (традиційним і клієнт-орієнтованим). Перевагою цієї моделі є можливість пошуку нових рішень шляхом інтеграції алгоритмів в ядро мережі. Результати моделювання показують, що в порівнянні з традиційним методом SLA, пропонований метод ELA забезпечує необхідні наміри користувача до якості замовлених послуг. Використовуючи цей метод, провайдер зможе зробити свою мережу орієнтованою на клієнта. А також, за рахунок поліпшення QoS пріоритетних послуг, можна вивільнити мережеві ресурси, які використовувалися неефективно, для підключення нових клієнтів.

4. Використовуючи цей метод при побудові майбутньої мережі IBN, провайдер зможе автоматизувати багато рутинних речей, скоротивши витрати на обслуговуючий персонал. Основні завдання конфігурації і підтримки мережі, які виконуються системними адміністраторами, перейдуть до централізованого мережного елемента IBN контролера.

РОЗДІЛ 4. ІНТЕЛЕКТУАЛЬНА СИСТЕМА МОНІТОРИНГУ ТА АНАЛІЗУ ТРАФІКУ ДЛЯ АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ АНОМАЛІЇ І ЗАПОБІГАННЯ АТАК В ІНТЕНЦІЙНО-ОРІЄНТОВАНИХ МЕРЕЖАХ

4.1. Розроблення інтелектуальної DPI системи моніторингу та аналізу трафіку для автоматизованого виявлення аномалії і запобігання атак в інтенційно-орієнтованих мережах

Виявлення мережевих аномалій в даний час є одним із активно розвиваючих напрямків дослідження в галузі забезпечення кібербезпеки [186-188]. Це пов’язано з тим, що аномалії в більшості випадків є початковою стадією мережевих атак, що може мати як негативні нематеріальні наслідки, так і фінансові втрати для організацій. Розуміння природи аномалій мережевого трафіку є важливим завданням, як для традиційних інфокомунікаційних мереж, так і для майбутніх автоматизованих інтенційно-орієнтованих мереж. Незалежно від того, є ці аномалії шкідливими, важливо проаналізувати їх з двох причин:

– аномалії можуть спричинити перевантаження мережі та збільшити використання ресурсів мережевих вузлів;

– деякі аномалії не обов'язково впливають на мережу, але вони можуть мати серйозний вплив на якість надання сервісу кінцевому користувачеві.

Істотною проблемою виявлення аномалій є те, що форми аномалій можуть змінюватися залежно від причин їх появи, зокрема, створювані від простіших DoS-атак до неправильних конфігурацій адміністратора. Відмова в обслуговуванні, зловмисний контроль, зловмисна робота, сканування, шпигунство та неправильне налаштування – це такі атаки та аномалії, які можуть призвести до виходу з ладу всієї мережевої інфраструктури.

Виявлення та класифікація аномалій передбачає постійний процес моніторингу подій в інформаційних системах та мережах, саме для цього

використовуються більшість систем DPI. На сьогодні існуючі рішення для виявлення мережевих аномалій перешкоджають розробці єдиного універсального механізму виявлення раніше невідомих типів атак. DPI - це комерційні продукти, які дозволяють аналізувати трафік на наявність аномалій та загроз у реальному часі. Проте обмежувальними факторами використання таких систем є висока вартість і закрита архітектура, що ускладнює їх адаптацію до організаційної інфраструктури. Також згідно проведеного аналізу у підрозділі 1.4.4, встановлено, що існуючі DPI системи вимагають нових інтелектуальних методів виявлення аномалій та атак для забезпечення необхідного рівня якості обслуговування та безпеки в перспективних інтенційно-орієнтованих мережах [189]. Саме тому, у роботі пропонується розробити власну унікальну програмно-орієнтовану систему DPI, з можливістю в ній розгортати свої унікальні методи управління трафіком, виявлення аномалій, розпізнавання та блокування мережевих атак, що детально описуються у наступних підрозділах [190-194].

4.1.1. Структурно-функціональна схема інтелектуальної DPI системи моніторингу та аналізу трафіку

У даному підрозділі роботи розглянуто функціональність розробленої універсальної програмної системи класу DPI, як одного із важливих інструментів, що дає можливість отримувати надійні, актуальні дані про активність користувачів мережі і управляти трафіком в пропонованій концепції IBN. Запропоновані у роботі рішення на основі DPI дають змогу отримувати повну картину використання ресурсів мережі, виявляти абонентів, які споживають великі обсяги трафіку, а також ефективно управляти трафіком в режимі реального часу, що допомагає автоматизовано створювати або оптимізувати сервісні пропозиції, підвищувати якість послуг, управляти сервісними політиками і забезпечувати захист мережі і її користувачів. Попередньо зібрані статистичні дані, що надаються розробленою системою DPI

у вигляді звітів, здатні надати серйозну допомогу при автоматизованому пошуку несправностей, прогнозуванні обсягу трафіку в наступний момент часу і відповідно якісному проведенні регулювання інформаційними потоками. У свою чергу це дає змогу грамотно планувати розвиток самої IBN мережі та забезпечувати адаптивне надання сервісів з використанням існуючих алгоритмів машинного навчання. В результаті завдання моніторингу, безпеки, управління, пріоритезації трафіку і оптимізації загального навантаження на мережеву інфраструктуру стає вкрай важливою не тільки для корпоративного сектора, а й для операторів мобільного та фіксованого зв'язку. Поточні тенденції в сфері послуг інтернет-контенту вказують, що вимоги для управління трафіком непередбачувані. Тому постачальники послуг, зокрема оператори мобільного зв’язку 4G/5G повинні реалізовувати нові DPI-рішення (рис.4.1), де програмне забезпечення може бути оновлено для підтримки нових вимог до управління і контролю трафіку в міру необхідності.

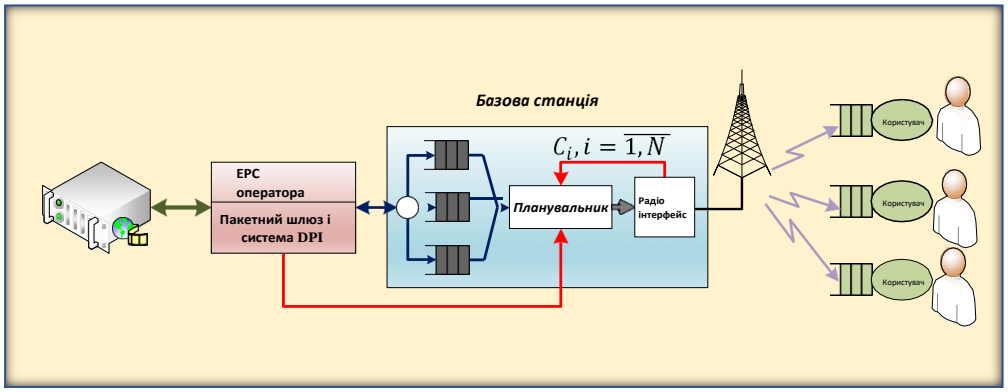


Рис. 4.1. Розташування DPI системи для оператора мобільного зв’язку 4G/5G

Один з основних методів, використовуваних в розробленій DPI-платформі є повірка сигнатур протоколів і додатків. Під сигнатурою розуміється шаблон опису даних, який вибирається для унікальної ідентифікації пов'язаного з ним програми/протоколу. Розроблена DPI-платформа зберігає бібліотеку сигнатур, яка поповнюється при появі нових версій або додатків. Крім сигнатурного методу також використовується аналіз мережевого трафіку, який теж може мати специфічні для кожного з додатків і протоколів характеристики (розмір

корисного навантаження, кількість і розміри пакетів у відповідь на запит, позиція фіксованих рядків або байт всередині пакету і т.д.). В розробленому арсеналі DPI є методи, засновані на статистичному і поведінковому характері потоку даних і інші евристичні методи. Зрозуміло, що вилучення інформації з пакета і її аналіз вимагають значних обчислювальних ресурсів, а одна з основних вимог до DPI-платформ для інтенційно-орієнтованих мереж - виконувати сканування пакетів на швидкості каналу передачі даних та гнучкість розгортання на різних сегментах мережі, що показано на рис.4.2.

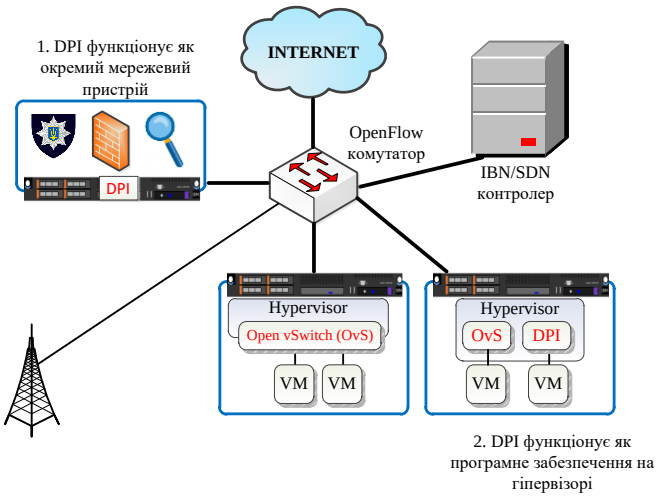


Рис. 4.2. Гнучкість розгортання розробленої програмної DPI системи для IBN

Найбільш складною частиною існуючих DPI-систем є підсистема аналізу трафіку, адже трафік реальних мереж дуже різноманітний, складається з безлічі протоколів та додатків, що у свою чергу для прийняття правильного розпізнавання інформаційних протоколів вимагає розробки нових DPI-систем, які повинні базуватися на комплексних методах аналізу трафіку. Таким чином, використання та дослідження існуючих методів аналізу трафіку, що проводилися в даній роботі, таких як сигнатурний аналіз, числовий аналіз, поведінковий та еврістичний аналіз, аналіз стану протоколу, аналіз зразка, дали змогу розробити на їх основі ефективні алгоритми розпізнавання основних інформаційних протоколів. Також, для детального вивчення принципів роботи протоколів використовувалися програми Wireshark та HexEditorNeo та існуюча

протокольна специфікація. На основі отриманих знань у роботі створенні алгоритми розпізнавання одних із основних протоколів DNS, RTP, HTTP, TLS, BitTorrent, uTP та програмно імплементовані в розроблену систему DPI. У роботі вважається, що автоматизоване розпізнавання інформаційних протоколів серед вхідного трафіку є першою фазою констатування факту легітимності трафіку, оскільки невідомий трафік в IBN мережах вказуватиме на можливість несанкціонованого доступу чи аномалії трафіку, який потребує блокування або більш детального аналізу. Другою фазою констатування факту легітимності трафіку є використання удосконаленого методу виявлення аномалій мережевого трафіку та атак на основі використання фрактального аналізу інформаційних потоків за критерієм Херста та статистичних характеристик (середнього значення, середнього квадратичного відхилення, і стандартного відхилення трафіку). Детальний принцип роботи пропонованого методу розглядається у розділі 4.5.

На основі вищезазначених міркувань розроблено нову програмну систему DPI для дослідження ефективності запропонованих рішень, щодо контролю потоків інформаційних протоколів та виявлення аномалій за допомогою критерію параметра Херста. Ядро системи реалізоване за допомогою середовища розробки Microsoft Visual Studio 2013. Графічний інтерфейс розроблений з використанням фреймворку Qt 5.6.2. Функції захоплення пакетів з мережевих інтерфейсів та управління трафіком реалізовані за допомогою бібліотеки WinSock 2.2. Для написання робочої програми була використана мова програмування C ++ [190]. Структурна схема розробленої програмної системи DPI показана на рис. 4.3.

Основний принцип роботи розробленої DPI полягає в тому, що пакети інформаційних протоколів від кожного абонента мережі проходять через 2 етапи - навчання і виявлення. Етап навчання триває заданий час, і після його закінчення система буде володіти таблицею значень, що містять в собі

інформативні ознаки для цього абонента по конкретних інформаційних протоколах.

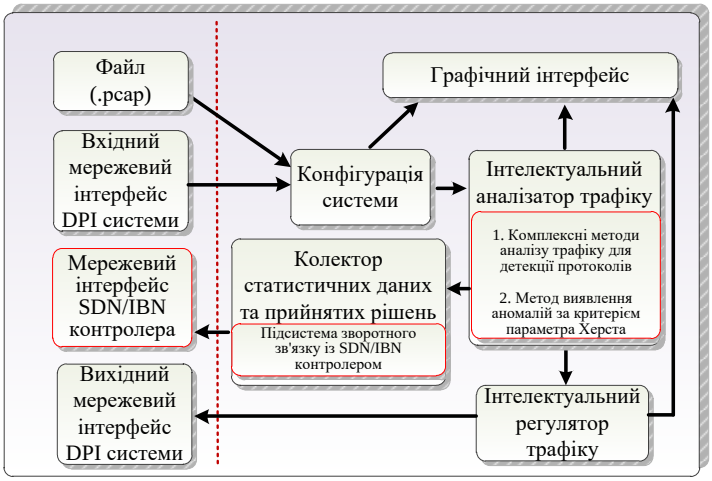


Рис. 4.3. Структурно-функціональна схема інтелектуальної DPI системи моніторингу та аналізу трафіку для автоматизованого виявлення аномалії і запобігання атак в інтенційно-орієнтованих мережах [190]

Навчання відбувається в умовах відсутності будь-яких аномалій та атак в мережі з метою надання достовірної інформації, що відповідають за так званні еталоні значення трафіку по яких відбуватиметься їх порівняння. Перейшовши на етап виявлення, система буде порівнювати розрахунки в режимі реального часу функціонування за певні інтервали із еталонними значеннями в таблиці отриманих в процесі навчання. Після чого робитимуться висновки про наявність аномальної активності. Для кожного абонента ведеться своя таблиця і для кожного ж абонента є свої етапи навчання і виявлення. Сама система володіє гнучкістю точки зору розгортання. Розроблена система DPI створена у вигляді програмного забезпечення, що встановлюється на серверах та аналізує трафік вибраного інтерфейсу та відповідно до заданих параметрів здійснює управління потоком даних.

В якості основних логічних компонентів розроблювальної системи виступають інтелектуальний аналізатор, колектор статистичних даних та прийняття рішень, а також інтелектуальний регулятор трафіку.

Інтелектуальний аналізатор займається перехопленням трафіку, отриманням цифрових значень із заголовків пакетів, та детекцію протоколів щодо певного класу трафіку, в свою чергу має зв'язок із колектором даних для отримання статистичних даних еталонних значень. Базується також на можливості використання алгоритмів машинного навчання, що детально показано у роботі [191]. Після чого аналізатор вирішує, що робити з трафіком далі. Для цього йому необхідно зрозуміти, чи є абонент новим або раніше він був у полі зору системи. Якщо абонент новий, то для нього система переходить на етап навчання, тобто заводиться нова порожня таблиця еталонних значень і починається її заповнення. Якщо абонент вже є в базі системи, то аналізатору необхідно зрозуміти, на якому етапі він знаходиться. Якщо на етапі навчання, то необхідно продовжити писати в існуючу таблицю. Якщо абонент знаходиться на етапі виявлення, то подальші дії передаються до регулятора трафіку.

Колектор статистичних даних та прийняття рішень займається сортуванням трафіку по абонентам і передачею значень для подальшої обробки аналізатором. Зокрема колектор даних DPI має логічну підсистему зв’язку із SDN/IBN контролером через мережевий інтерфейс пристрою, використовуючи протокол OpenFlow.

*Регулятор трафік*у, оперуючи значеннями, отриманими від аналізатора, порівнює їх зі значеннями з таблиць (отриманими на етапі навчання) і робить висновки про наявність чи відсутність аномалії чи атаки. Якщо аномалія виявлена - застосовується дія. Дією може бути якась санкція (наприклад, обмеження трафіку для абонента) або ж пасивна поведінка (оповіщення системного адміністратора про потенційну проблему). Другорядні компоненти DPI системи характеризуються модульним принципом побудови і складаються із таких частин: модуля зчитування даних з вхідного інтерфейсу; модуля розбору заголовків мережевого та транспортного рівнів; модуля детектора

протоколів; таблиці сесій для детектора протоколів; модуля збору статистики; графічного інтерфейсу користувача.

Вхідним інтерфейсом для програми може бути будь-який інтерфейс, з якого надходять пакети. Найпоширенішими інтерфейсами є файл і інтерфейс мережевої карти.

Призначенням модуля розбору заголовків мережевого та транспортного рівнів є аналіз заголовків відповідних рівнів і розділення групового потоку на менші потоки що належать одному абоненту. При наявності складних інкапсуляцій, тунелювання, компресії заголовків мережевого та транспортного рівнів OSI, потрібно спочатку вийняти первинні дані, які надсилалися від одного абонента до іншого. Згодом потік від одного абонента поділяється на елементарні потоки – потоки, які піддаються аналізу (наприклад 1 TCP сесія, або декілька пов’язаних UDP - сесій). Коли виділені елементарні потоки, потрібно провести розпізнавання протоколів – визначення типу протоколу. DPI-системи повинні виконувати це завдання з дуже високим рівнем точності, бо помилка розпізнавання може призвести до того, що користувач буде неправильно обслужений, або не обслужений взагалі. Таблиця сесій для детектора протоколу зберігає результат розпізнавання. Оскільки встановлена TCP чи UDP сесія, ініційована певним додатком продовжує існувати по певному сокеті, то є доцільним один раз здійснити розпізнавання протоколу і занести результат в таблицю сесій, а при надходженні кожного наступного пакету лише шукати запис в таблиці сесій. Таблицю сесій доцільно реалізовувати у вигляді дерева або хеш-таблиці, для того щоб мінімізувати час пошуку потрібного запису. При цьому в таблиці повинна зберігатися інформація про те, до якого протоколу відноситься даний пакет, а також за потреби певна статистична інформація, що потрібна протягом сесії. Ключем в таблиці є структура, що містить такі поля: IP-адресу джерела та призначання; порт джерела та призначення; протокол (TCP або UDP).

Призначенням модуля збору статистики є визначення параметрів трафіку, як загального, так і по кожному конкретному протоколу, реєстрація невідомого трафіку, або ж трафіку, при аналізі якого відбулися помилки. Розроблений графічний інтерфейс DPI системи дає змогу системному адміністратору взаємодіяти з програмою і отримувати ті відомості, які йому цікаві.

4.1.2. Алгоритми захоплення, аналізу та розпізнавання інформаційних потоків

Алгоритм роботи аналізатора трафіку.

Розглянемо загальний алгоритм роботи програми-аналізатора (рис. 4.4). Пакети з вхідного інтерфейсу подаються на модуль аналізу заголовків мережевого та транспортного рівнів, який формує ключ для таблиці сесій. Після цього здійснюється пошук по ключу в таблиці сесій і якщо запис не знайдено, то відбувається визначення протоколу детектором. Всі відомості про пакет зібрані в результаті обробки кожним модулем аналізуються модулем збору статистики. Результуюча інформація подається користувачу у вигляді таблиць та графіків.

Рис. 4.4. Загальний алгоритм роботи аналізатора трафіку [191]

Алгоритми зчитування даних з вхідного інтерфейсу

Вхідними інтерфейсами програми-аналізатора мережевого трафіку є мережева карта комп'ютера та pcap-файл. При використанні мережевої карти в якості вхідного інтерфейсу зчитування пакетів проводиться в режимі реального

часу з використанням бібліотеки WinPcap. В цьому випадку необхідно лише правильно підключити бібліотеку і викликати інтерфейсні функції.

Читання з файлу є складнішим, ніж читання з мережевого інтерфейсу. Пакети записуються в pcap-файл в той момент, коли приходять, тоді, як читання з файлу відбувається з приблизно сталою швидкістю. Звичайне читання з файлу призводить до спотворення статистичних результатів, адже не враховує час запису пакетів в файл. Для того, щоб результати не відрізнялися при читанні з двох інтерфейсів потрібний додатковий алгоритм, щоб моменти початку аналізу кожного наступного пакету були фіксованими (рис. 4.5)

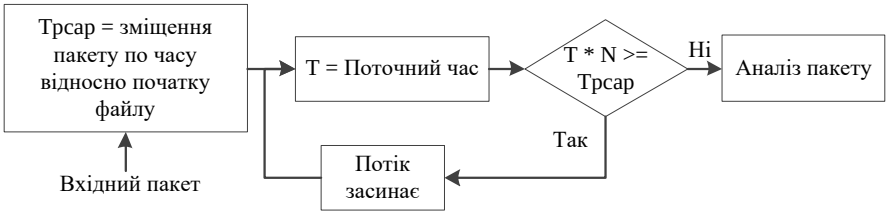


Рис. 4.5. Алгоритм читання пакетів з файлу [191]

Згідно алгоритму, робочий потік починає обробляти пакет, якщо час роботи програми в поточний момент часу є в N разів меншим, ніж часова позначка пакету в файлі. В протилежному випадку, потік почекає і перевірить умову знову.

Розробка детектора протоколів.

Без детектора протоколів програма-аналізатор не спроможна робити практично нічого, адже функцією детектора є розрізнення протоколів і аплікацій для подальшого збору статистики. Історично склалося, що в мережі Інтернет існують велика різноманітність протоколів, на кожен з яких необхідно розробити окремий алгоритм розпізнавання. Велика частина протоколів не є стандартизованою, а розробка протоколів в кращому випадку ведеться відповідно до документів RFC (Request for comments), що ускладнює розробку детекторів протоколів, адже RFC в багатьох випадках – це лише рекомендації.

Розпізнавання протоколів ускладнюється тим, що більшість компаній, розробляючи протоколи для своїх приватних цілей не розголошують деталей реалізації протоколу, а в вільному доступі, в кращому випадку, є лише презентації, в яких описані всі переваги використання даного протоколу. Дуже часто документ-опис протоколу є доступний лише для працівників компанії-розробника. Якщо протокол не описаний, розробник повинен сам дослідити принципи його роботи, адже тільки тоді, коли буде відомо, як відбувається процес взаємодій між мережевими пристроями, яка структура і параметри пакетів, можна написати детектор, який буде мати високу швидкодію і малу ймовірність помилки.

Набір полів формує унікальність конкретного протоколу і, за рахунок цього можна написати детектор протоколів. Проте, в умовах високошвидкісного трафіку до алгоритмів розпізнавання протоколів існують жорсткі вимоги по швидкодії, адже програма мусить обробляти великі обсяги даних і створювати мінімальну затримку передачі. Алгоритми розпізнавання мають бути водночас простими, а з іншого боку надійними, щоб ймовірність помилкового спрацювання детектора була мінімальною, зокрема, що є актуальним для реалізації програмно-конфігурованих інтенційно-орієнтованих мереж. Алгоритм розпізнавання в розробленій DPI системі базується на двох видах, зокрема:

– Послідовний (рис.4.6) – використовується для низькошвидкісних потоків даних. Кожен з алгоритмів розпізнавання виконується, коли закінчилося виконання попереднього алгоритму. Використовується один процесорний потік.

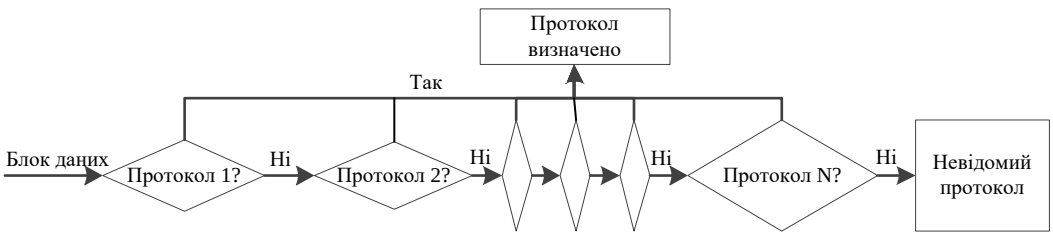


Рис. 4.6. Послідовний алгоритм розпізнавання

– Паралельний (рис. 4.7) – для високошвидкісних потоків даних. При цьому алгоритми розпізнавання виконуються паралельно, кожен в своєму процесорному потоці. Коли кожен з потоків закінчив виконання свого алгоритму, якщо протокол визначено одним із алгоритмів, то виконання припиняється, якщо ні, кожному потоку надається для виконання новий алгоритм.

Рис. 4.7. Паралельний алгоритм розпізнавання

4.1.3. Алгоритми розпізнавання протоколу DNS

Протокол DNS та алгоритм його розпізнавання.

Отже, DNS-пакети завжди присутні серед мережевого трафіку. Тому варто додати в систему аналізу трафіку алгоритм обробки DNS-протколу. Розпізнавання DNS полягає у співставленні структури вхідного пакету і структури DNS-пакету. Отже, знаючи структуру полів DNS-пакету можна зробити детектор, який буде відкидати пакети з неможливими значеннями полів. Якщо пакет пройде всі перевірки – це DNS.

Алгоритм роботи детектора DNS-протоколу зображений на рис. 4.8. Незважаючи на складність блок-схеми алгоритм повинен працювати швидко, адже не виконується ніяких складних операцій, крім перевірок вмісту полів. Послідовність дій алгоритму наступна:

1) Перевірка порта. Для DNS-протоколу зарезервованими є UDP та TCP порти з номером 53. Хоча в більшості випадків DNS-пакети передаються по UDP, та підтримка роботи по TCP є однією основних з вимог до DNS-сервера.

2) Перевіряємо поля кількість запитів та кількість відповідей. Якщо тип повідомлення запит, то поле відповідей буде пусте, якщо тип – відповідь, то поле запитів буде пусте.

3) Робимо стільки ітерацій, скільки запитів/відповідей, зменшуючи на кожній ітерації кількість запитів/відповідей на 1. При досягненні значення 0 відбувається вихід з циклу і прийняття рішення. На кожній ітерації здійснюємо розбір імені домену, тобто зчитуємо вказівники та переходимо по значеннях, яке вони вказують. Вихід за межі пакету означає, що це не DNS. Нульовий вказівник означає закінчення імені домену. Тип запиту та клас запиту для таких пакетів має становити 0x0001.

4) Якщо тип пакету – відповідь, потрібно зчитати довжину даних ресурсу і перейти по вказівнику.

5) Коли змінна кількість запитів/відповідей досягає значення 0, приймається рішення, що даний пакет DNS.

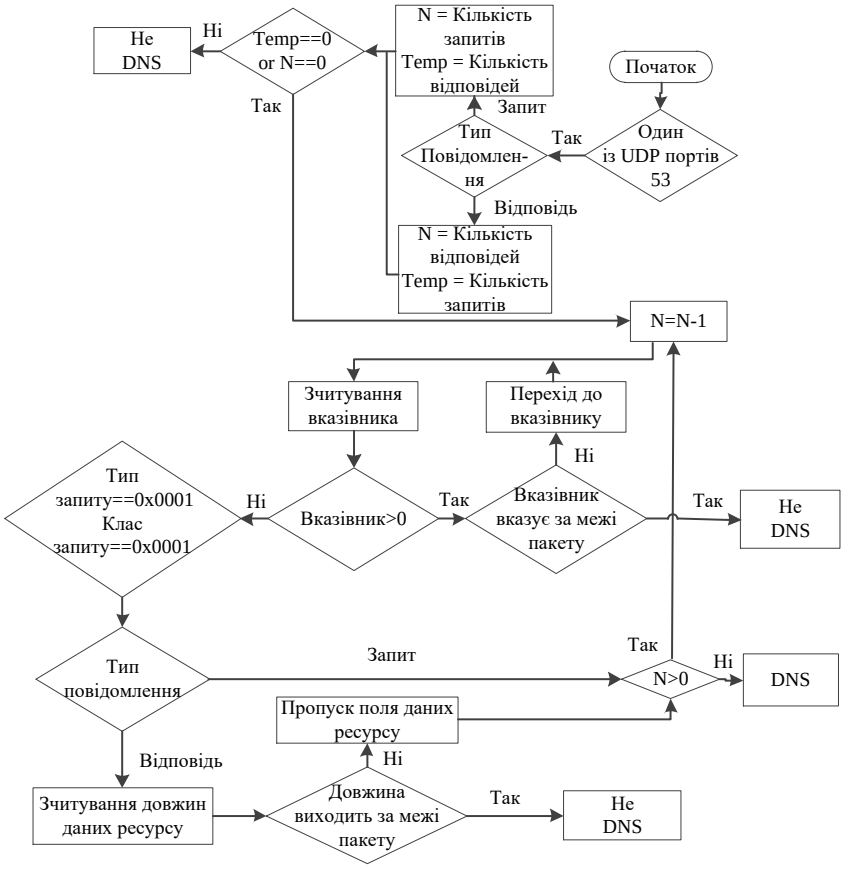


Рис. 4.8. Алгоритм роботи детектора DNS-протоколу [191]

4.1.4. Алгоритм розпізнавання протоколу RTP

Протокол RTP переносить в своєму заголовку дані, необхідні для збирання аудіо або відео в приймальному вузлі, а також дані про тип кодування інформації (JPEG, MPEG і т. д.). У заголовку даного протоколу передаються часова мітка і номер пакета. Ці параметри дають змогу при мінімальних затримках визначити порядок і момент декодування кожного пакету, а також інтерполювати втрачені пакети. RTP не має стандартного зарезервованого номера порту. Протокол RTP має заголовок змінної довжини. Мінімальна довжина заголовку становить 12 байт [195]. Оскільки RTP-заголовок не має чітко виражених полів окрім поля версії, то неможливо використати класичний аналіз зразка. Натомість проблема розпізнавання протоколу RTP легко вирішується з використанням поведінкового аналізу протоколу, дивлячись на значення окремих полів протоколу. Проте поведінковий аналіз, на відміну від сигнатурного завжди вимагає більше пам’яті, адже постає необхідність збереження заголовка пакета. Для кожного UDP – пакету потрібно здійснити 2 прості перевірки: версія повинна бути не меншою за 2, і довжина має бути достатньою для розбору заголовка. Ця перевірка дасть змогу відфільтрувати більш ніж половину UDP – пакетів. Алгоритм розпізнавання RTP пакету зображений на рис. 4.9.

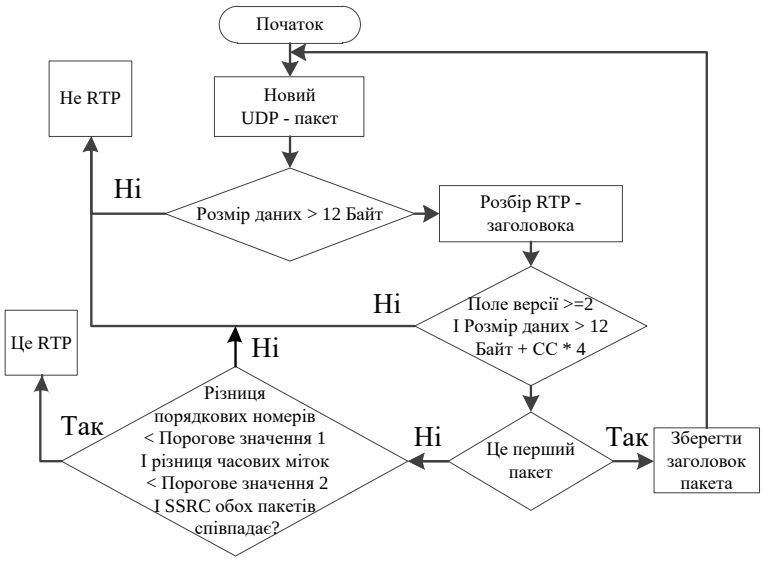


Рис. 4.9. Алгоритм роботи детектора RTP

Заголовок пакета і відомості про пакет, що пройшов просту перевірку, зберігається в детекторі. Коли надійшло два пакети (або за потреби більше), проводиться аналіз 3-х полів:

– Різниця порядкових номерів пакетів повинна бути невеликою. Порогове значення варто вибирати залежно від ймовірності втрати пакетів. Чим більша ймовірність втрати, тим більший поріг варто вибирати, проте при цьому зростає ймовірність помилки;

– Різниця часових міток (семплів) має бути меншою, ніж певне порогове значення, яке залежить від типу трафіку (аудіо/відео) та різниці порядкових номерів. Тому, якщо відомими є параметри потоку, можна оцінити максимально можливе значення цього поля. Якщо ж параметри потоку є невідомими, варто використати значення за замовчуванням;

– SSRC всіх пакетів має бути однаковим.

4.1.5. Алгоритм розпізнавання протоколів HTTP та TLS

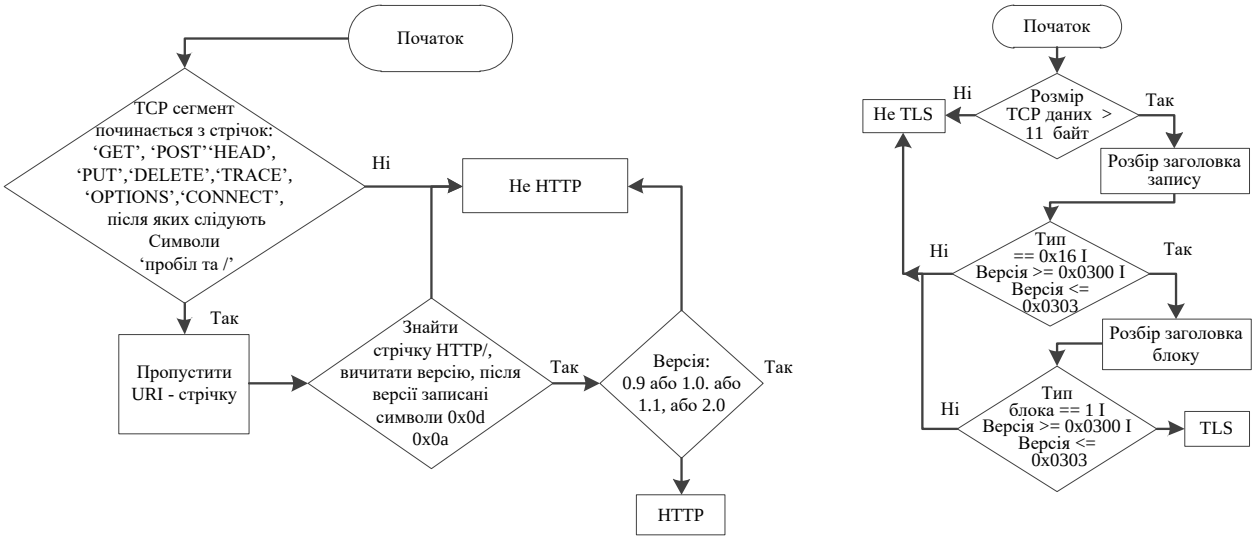
HTTP – це протокол передачі даних прикладного рівня, є основним протоколом для отримання інформації з веб-сайтів. Протокол HTTP використовує клієнт-серверну технологію: клієнт, що відправляє запит, є ініціатором з'єднання, сервер, який отримує запит, опрацьовує запит і відправляє клієнту результат [196].

Оскільки протокол HTTP має чітко визначену структуру, то його неважко детектувати. HTTP сесія починається з того, що клієнт надсилає до сервера один із відомих запитів, тобто TCP – сегмент повинен починатися однією з команд, після якого має записуватися URI-адреса і версія (рис. 4.10а).

Розпізнавання протоколу TLS проводиться по першому пакету, який надсилається від клієнта до сервера. Цей пакет містить заголовок запису розміром 5 байт, після якого йде 6-байтний заголовок блоку (рис. 4.10б).

Отже розмір TCP пакета має бути не меншим 11 байт, версії, вказані в заголовках мають відповідати актуальним версія протоколу, а тип запису і

блока відповідно мають бути рівними 0x16 (TLS handshake) та 0x01 (TLS client handshake).



а) б)

Рис. 4.10. Алгоритм розпізнавання протоколу HTTP – а), протоколу TLS – б)

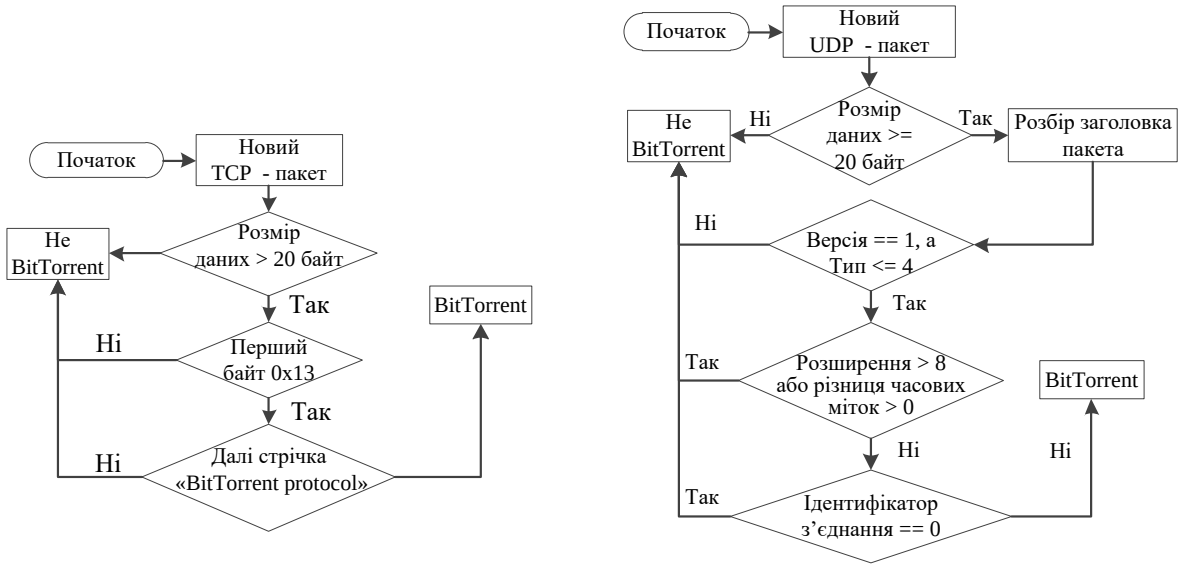
4.1.6. Алгоритм розпізнавання протоколів BitTorrent та uTorrent

BitTorrent та uTorrent Transport Protocol(uTP) на даний час є основними протоколами для передачі файлів в піринговых мережах. При передачі файли розбиваються на невеликі частини і в такому вигляді передаються. Торрент-клієнт скачує всі частини і потім збирає файл. Він працює по TCP і має дуже виражену структуру пакету, адже в першому байті заголовку міститься довжина імені протоколу. В цьому полі вказується число 0x13, а після нього записана текстова стрічка довжиною 19 байт, яка містить текст «BitTorrent protocol» [197]. Алгоритм розпізнавання протоколу зображено на рис. 4.11а.

Недоліком протоколу BitTorrent є те, що він працює по TCP, а отже торрент-трафік буде сповільнювати роботу інших додатків, таких, як браузер, поштовий клієнт, тощо, які є значно важливішими для користувача.

Протокол uTP є альтернативою протоколу BitTorrent. Він працює по UDP, внаслідок чого, торрент трафік буде передаватися з меншим пріоритетом, ніж TCP-трафік. Разом із тим передача даних по uTP є ефективнішою, через

менший обсяг службового трафіку [199]. Розпізнавання uTP сесії варто проводити по першому пакету в такій послідовності дій: спочатку необхідно перевірити, чи розмір даних є більшим або рівним 20 байтам. Потім розібрати заголовок, перевірити версію і значення типу. Оскільки перший пакет в сесії ще не може мати встановленого поля різниці часових міток, то в ньому має міститися 0. Ідентифікатор з'єднання не має бути рівним 0, а поле розширення не може містити значення більшого, ніж 8. Алгоритм розпізнавання протоколу uTP зображено на рис. 4.11б.



а) б)

Рис. 4.11. Алгоритм розпізнавання протоколу BitTorrent–а) та протоколу uTP–б)

4.1.7. Алгоритм збору статистики та визначення навантаження інформаційними потоками

Збір статистики проводиться з використанням елементарної структури даних (Stat), екземпляр якої використовується для збору статистики по одному з протоколів. Поля структури такі: загальна кількість байт (N); кількість байт після останнього перерахунку пропускної здатності (n); час останнього перерахунку пропускної здатності (T); останнє значення пропускної здатності (Thr). Для збору статистики по всіх протоколах використовується масив структур Stat, розмір якого дорівнює кількості протоколів, які обробляються

плюс 2, оскільки потрібно зберігати загальну статистику і статистику по невідомому трафіку. Крім того, для кожного абонента необхідно зберігати окремий масив структур Stat. Розглянемо роботу алгоритму збору статистики (рис. 4.12а).

Вхідними даними для системи збору статистики є сокет, тип протоколу, або невідомий тип і сокет. Відповідно до цього вибирається структура статистики Stat, в якій оновлюємо значення полів N, n структури Stat відповідно до значення L. Розрахунок пропускної здатності здійснюється в момент часу, що відповідає періоду оновлення графіків.

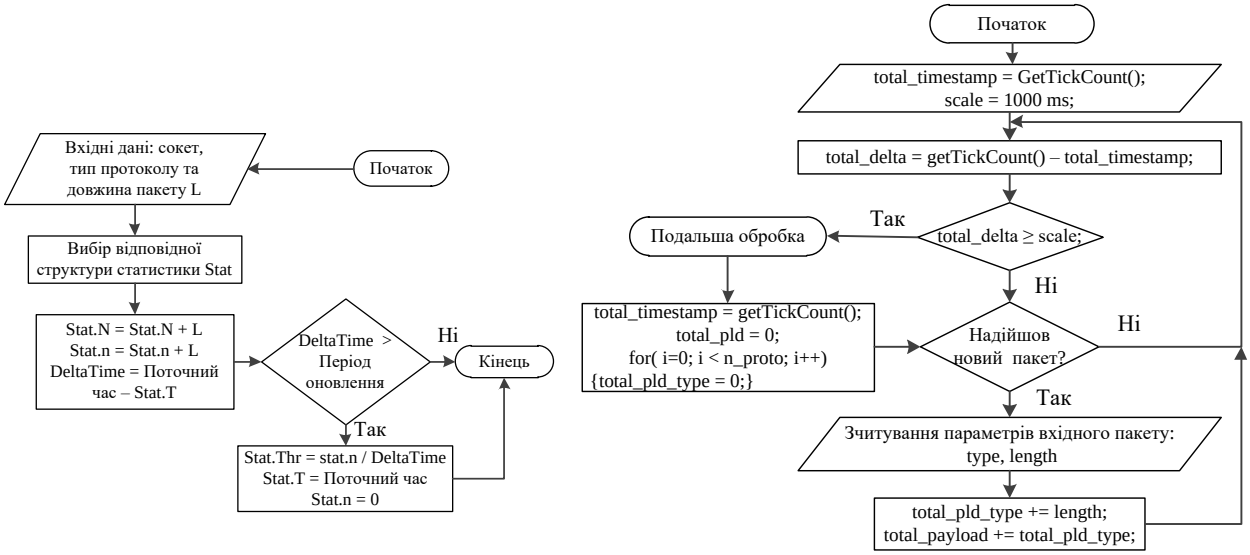


Рис.4.12. Алгоритм збору статистики – а) та визначення навантаження інформаційними потоками – б) [191]

Дана модель реалізовує регулювання інформаційного потоку по протоколах. Винесення рішення про блокування, обмеження, або надання пріоритету виноситься в залежності від типу протоколу та навантаження, яке ним створюється. Для визначення швидкості вхідного потоку застосовується наступний алгоритм визначення навантаження інформаційними потоками. Алгоритм виконується протягом всього часу роботи програми і використовується для вимірювання навантаження вхідних потоків. Кожен сокет

розглядається як окремий потік даних. Для кожного потоку даних реєструється кількість вхідних даних у байтах за одиницю часу. На початку роботи алгоритму реєструється час роботи програми, та задається ціна поділки часової шкали 1000 мс. Далі алгоритм переходить до виконання кроку 1.

Крок 1. Знаходимо різницю у часі між початком роботи програми та реальним часом , якщо ця різниця більша, або ж рівна ціні поділки (scale), то переходимо до кроку 2. Якщо ж різниця у часі менша за ціну поділки, тоді переходимо до кроку 3.

Крок 2. Миттєві значення навантажень передаються іншому потоку програми, який відповідає за регулювання потоку, глобальні часові мітці присвоюється значення реального часу і миттєві значення навантажень встановлюються рівними нулю. Переходимо до кроку 3.

Крок 3. Перевіряємо чи прийшов на вхід інтерфейсу новий пакет , якщо ні, то повертаємось до попереднього кроку. У випадку, якщо прийшов новий пакет, то виконується крок 4, в протилежному випадку – крок 1.

Крок 4. Зчитуємо тип пакету та його довжину у байтах. Сумуємо навантаження по конкретному типу. Переходимо до кроку 1.

В загальному випадку визначення навантаження конкретним типом трафіку можна виразити наступною формулою:

$$C_{П} = \sum_{i=0}^{n} C_{П_i}, \tag{4.1}$$

де n – кількість потоків одного типу, $C_{П_i}$ - навантаження створене одним потоком певного типу.

Загальне навантаження на один інтерфейс розраховується за формулою:

$$C = \sum_{i=0}^{N} C_i, \tag{4.2}$$

де N – кількість типів навантаження на один інтерфейс, C_i - навантаження створене одним типом трафіку.

4.2. Експериментальне дослідження процесу функціонування аналізатора трафіку DPI системи

4.2.1. Основні функції аналізатора трафіку розроблювальної DPI системи

До функцій програмної моделі належить:

1) Аналіз вмісту пакетів і класифікація абонентського трафіку по протоколах.

2) Ведення статистики та розрахунок для кожного з протоколів таких статистичних параметрів:

– Загальний обсяг трафіку по конкретному протоколу;

– Математичне очікування кількості трафіку за одиницю часу по протоколу;

– Дисперсія кількості трафіку;

– Стандартне відхилення кількості трафіку;

– Середня довжина пакету по протоколу;

– Середня частота надходження пакетів;

3) Відображення у вигляді графіка емпіричного значення густини розподілу ймовірності кількості трафіку

4) Можливість перегляду як загальної, так і статистики окремого абонента.

5) Можливість аналізу даних з pcap-файлу в режимі реального часу, або ж в прискореному режимі зі збереженням адекватності миттєвих результатів пропускної здатності.

6) Можливість аналізу даних, перехоплених з мережевої карти.

Програма складається з 3 основних заголовкових файлів:

– cWorker.h – містить клас для розбору пакетів і збору статистики;

– Detectors.h – містить набір класів детекторів і функцію, яка здійснює виклик кожного з них та обробку результатів;

– cUserInterface.h – містить клас, що використовує засоби бібліотеки Qt для створення графічного інтерфейсу з користувачем.

Програма побудована згідно принципів об’єктно-орієнтованого програмування і легко піддається масштабуванню. Наприклад, для добавлення нового детектора, потрібно лише створити функцію, або клас нового детектора, що реалізує стандартний інтерфейс.

Система працює в двох потоках:

– *Робочий потік*. Його функцією є аналіз вхідного пакету починаючи з канального і закінчуючи прикладним рівнем. Цей потік проводить аналіз заголовків мережевого та транспортного рівнів, здійснює виклик детекторів, та збір статистики. При потребі можна збільшити кількість робочих потоків, що призведе до збільшення швидкості аналізу вхідних пакетів за рахунок паралелізації обчислень;

– *Потік оновлення екрану*. Його функцією є періодичне оновлення графіків і статистичних показників при спрацюванні таймера.

Оновлення екрану включає в себе наступне:

– Зчитування статистики, зібраної робочим потоком і розрахунок пропускної здатності кожного з протоколів і користувачів;

– Перерахунок статистичних параметрів кожного з протоколів;

– Перебудова графіків та текстових полів.

Оновлення екрану проводиться з частотою 1 раз/секунду при читанні з мережевої карти. При читанні файлу оновлення екрану проводиться в N разів швидше, де N – швидкість читання з файлу, задана користувачем, за рахунок чого значення, отримані при різних швидкостях читання з файлу не відрізняються.

Користувацький інтерфейс моделі (рис. 4.13) – вікно, яке умовно можна поділити на 2 частини:

– Область відображення результатів, на якій відбувається відображення графіків та статистичних параметрів;

– Область налаштувань, на якій розміщені засоби для вибору вхідного інтерфейсу, керуючі кнопки, та поле з відображенням історії дій користувача.

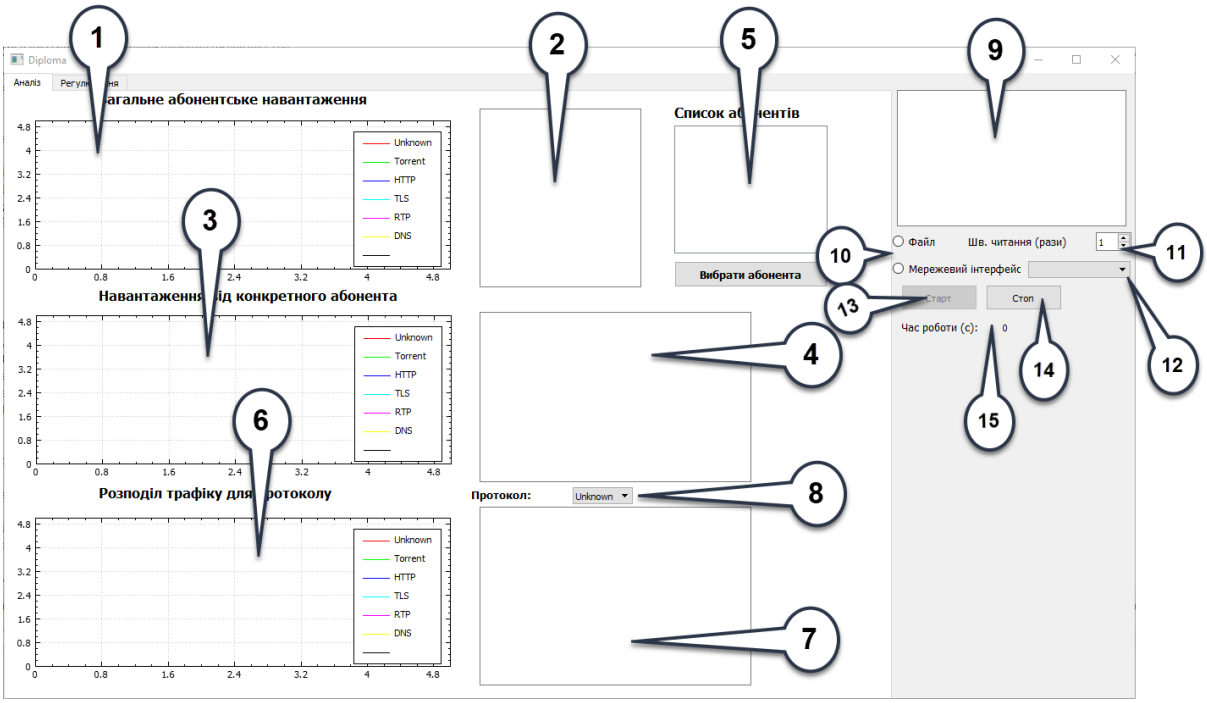


Рис. 4.13. Загальний вигляд вікна програми

Розглянемо детально кожний з елементів програмної моделі:

1) Графік загального абонентського навантаження показує як вхідний потік поділяється по протоколах в кожний момент часу;

2) Поле відображення статистики загального абонентського навантаження;

3) Графік навантаження від одного абонента;

4) Поле відображення статистики навантаження від одного абонента;

5) Поле вибору абонента зі списку. Дозволяє відслідковувати навантаження конкретного абонента. При виборі абонента відбувається перебудова графіка (3) і поля (4) ;

6) Графік густини розподілу ймовірності навантаження;

7) Поле відображення статистичних параметрів трафіку протоколу;

8) Меню вибору протоколу для відображення статистичних параметрів. Здійснює керування графіком (6) та полем (7) ;

9) Вікно історії;

10) Вибір вхідного інтерфейсу. Можливість читання з файлу, або з мережевої карти;

11) Вибір швидкості читання з файлу. При значенні 1 читання з файлу відбувається в режимі реального часу, при більших значеннях швидкість читання є в задану кількість разів більшою, ніж в режимі реального часу;

12) Вибір мережевого інтерфейсу з якого відбуватиметься зчитування пакетів;

13) Кнопка «Старт» – призводить до запуску робочого потоку і запуск таймера для оновлення екрану. Є неактивною, якщо не вибраний файл, або ж не вибраний мережевий інтерфейс;

14) Кнопка «Стоп» – призводить до зупинки таймера оновлення екрану і до завершення роботи робочого потоку;

15) Поле відображення часу роботи програми.

Для генерування абонентського навантаження використовувалися 5 комп'ютерів. На всіх комп'ютерах одночасно було запущено перехоплення пакетів програмою і протягом 5 хвилин проводилися наступні дії: Перегляд веб-сайтів; Слухання музики онлайн; Перегляд відео в YouTube; Скачування фільму з використанням торрент клієнта; Редагування онлайн-документа; Перегляд електронної пошти; Перегляд RTP-відео.

Отримано 5 pcap-файлів, які хронологічно об'єднані в один файл за допомогою програми Wireshark. Результуючий файл можна використовуватися в якості агрегованого трафіку від абонентів оператора.

4.2.2. Дослідження процесу функціонування аналізатора трафіку

Дослідження проводилося протягом 300 секунд, протягом яких проаналізовано 1Гб вхідного трафіку.

Після 170 секунд роботи моделі зафіксовані результати у вигляді знімків екрану. В цей момент часу загальний трафік являє собою сукупний трафік п'яти абонентів. Графік загального навантаження та навантаження від одного абонента зображені на рис. 4.14.

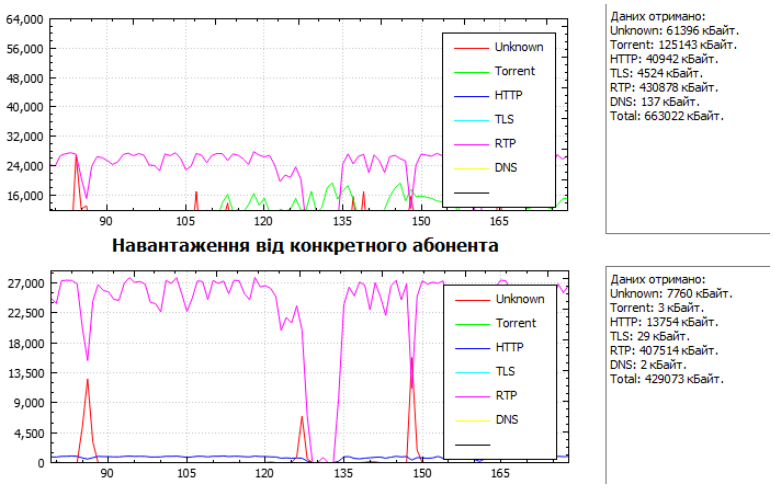


Рис. 4.14. Графіки загального абонентського навантаження та навантаження від першого абонента

Перший абонент дивиться відео високої якості по протоколу RTP і є абонентом, який в цей момент генерує найбільше навантаження. В момент часу t = 130 протягом 5 секунд немає RTP-навантаження, що відповідає моменту зупинки відео, або відтворення буферизованого відео. Другий абонент періодично генерує трафік невідомого протоколу.Третій абонент ввімкнув торрент-клієнт для скачування короткого фільму. Оскільки торрент-клієнт створює зразу багато TCP-з'єднань, спостерігається значний обсяг трафіку. Четвертий абонент відкриває сторінки в мережі Інтернет, а п'ятий абонент переглядає JPEG відео з веб-камери.

Графіки навантаження від 2-5 абонентів зображені на рис. 4.15.

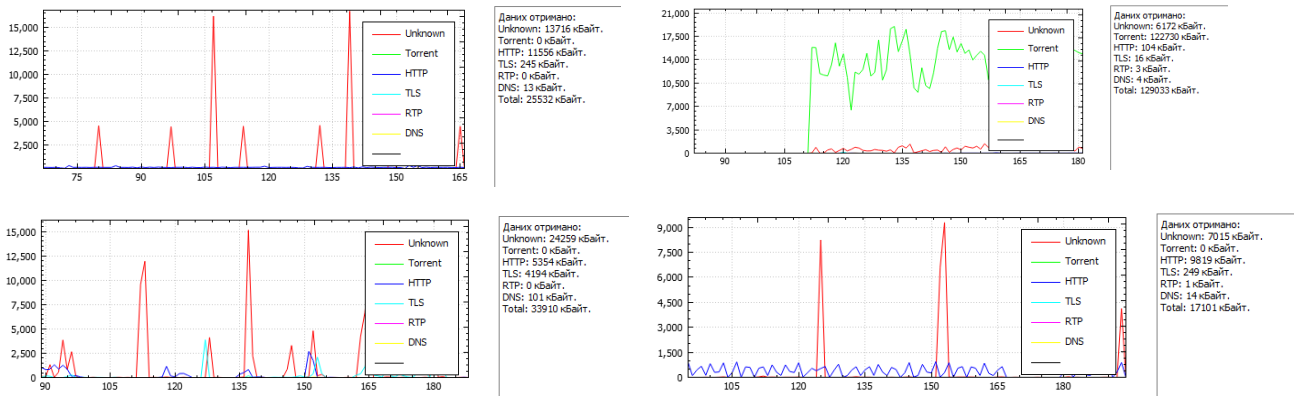


Рис. 4.15. Графіки навантаження від абонентів 2,3,4 та 5

За 5 хвилин моделювання програма зібрала статистику розподілу трафіку по протоколах, яка наведена в таблиці 4.1:

Таблиця 4.1

Результати моделювання: розподіл трафіку по протоколах

Протокол	Обсяг трафіку (Мб)
RTP	448,091
Torrent	447,648
TLS	56,491
HTTP	51,217
DNS	0,206
Невідомий	93,578
Загальний трафік	1086,392

На основі миттєвих значень навантаження побудовано графіки залежності ймовірності появи певного обсягу навантаження протоколу. Загальне навантаження (рис. 4.16а) за візуальним представленням схоже на нормальний закон розподілу, через виражену симетричність розподілу.

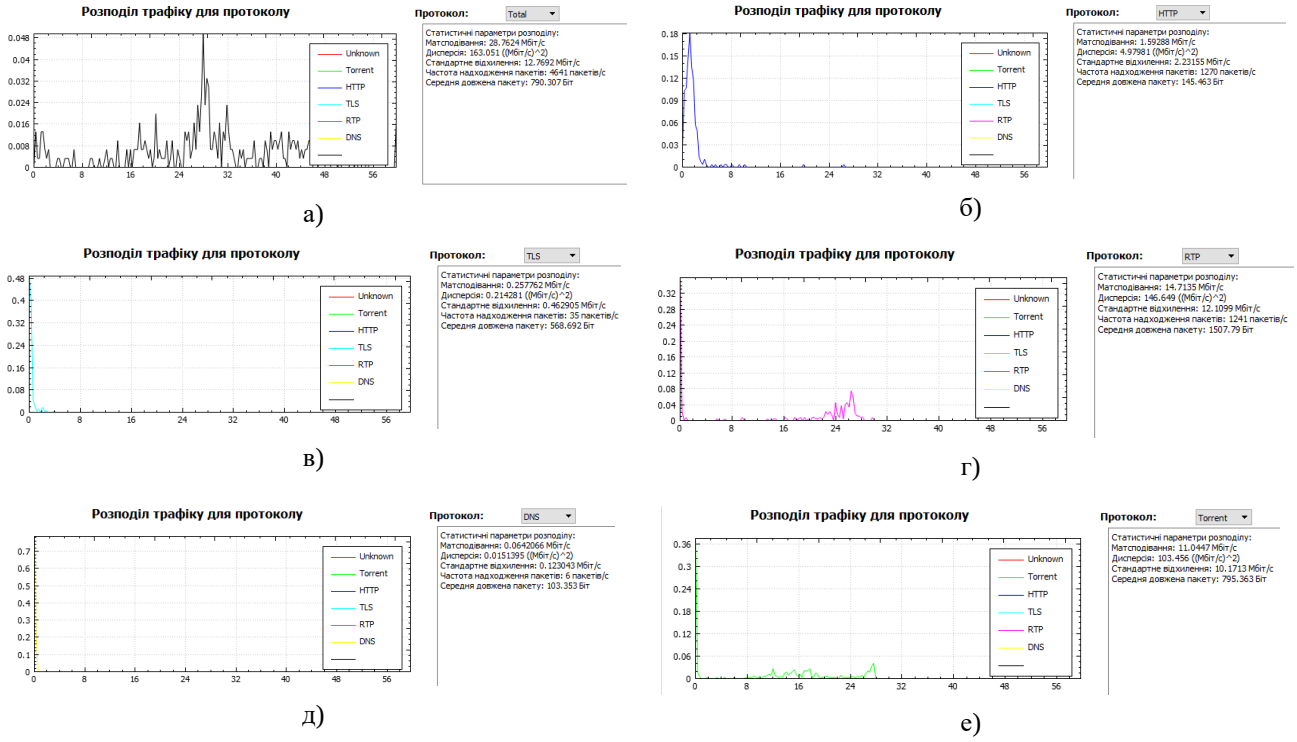


Рис. 4.16. Розподіл загального трафіку – а) та розподіли трафіку протоколів : HTTP– б), TLS – в), RTP – г), DNS – д), торрент-групи– е) [192]

Графіки ймовірності надходження певного обсягу навантаження та статистичні параметри для протоколів наведені на рис 4.16б – 4.16е.

Невелике значення математичного сподівання характерне для протоколу HTTP, адже абонененти, що переглядають веб-сторінки генерують невелике навантаження і воно по свому характеру є нерівномірним, адже сторінка завантажується і після цього очікує наступного запита від клієнта.

Закон розподілу навантаження TLS-протоколу є дуже подібним до HTTP. Відношення математичного сподівання до стандартного відхилення є близьким за значенням для TLS та HTTP трафіку.

Закон розподілу RTP-трафіку має такі параметри: математичне сподівання 14,7 та стандартне відхилення 12,1, що свідчить про те, що частину часу абонент перегладав відео високої якості, а частину часу не переглядав нічого.

Хоч DNS-трафік є завжди присутнім у будь-якій мережі, та він займає малу частину смуги пропускання оператора. DNS-пакети мають малу довжину. Моделювання показало, що середня довжина пакету становить 104 байти, а середня частота надходження пакетів – лише 6 пакетів/с.

Закон розподілу торрент-трафіку вказує на те, що протягом моделювання частину часу в мережі був присутній значний обсяг торрент трафіку, а частину часу його практично не було. Торрент займає велику частину смуги пропускання оператора і передача здійснюється пакетами з досить великим розміром – майже 800 байт.

Система аналізу трафіку є основною складовою частиною DPI-системи. Але сам по собі аналіз трафіку не принесе прибутку оператору. Потрібні активні дії направлені на контроль мережевого трафіку. Систему аналізу трафіку потрібно використовувати разом із системою контролю та регулювання трафіку, так, що вихідні дані системи аналізу є вхідними для системи контролю та регулювання. Система аналізу трафіку на основі різних критеріїв повинна визначити що відбувається з трафіком в даний момент часу і спрогнозувати ймовірний обсяг трафіку через деякий момент часу.

Для системи регулювання трафіку важливими є декілька параметрів трафіку протоколу:

– Поведінка трафіку: рівномірний, чи стрибкоподібний;

– зростання чи зменшення миттєвого значення навантаження;

– ймовірність появи певної величини навантаження в наступний момент часу.

Поведінка трафіку описується дисперсією. Якщо дисперсія є великою, то трафік буде стрибкоподібним, інакше рівномірним.

Для прогнозування обсягу трафіку слід аналізувати зміну математичного сподівання (М) та дисперсії (Д) протягом певного часу.

Математичного сподівання трафіку дозволяє оцінити, яке значення навантаження планується в наступний момент часу, а дослідження параметра дисперсії дозволяє оцінити можливе відхилення обсягу трафіку від математичного сподівання. Таким чином прогнозування обсягу трафіку в наступний момент часу – це імовірнісний процес, який залежить від багатьох факторів: часу доби, дня року, протоколу, конкретного абонента. Збір і аналіз статистичних даних дозволяє DPI-системі навчатися і внаслідок цього з більшою точністю здійснювати прогнозування обсягу трафіку в наступний момент часу і відповідно якісно здійснювати регулювання трафіку.

4.3. Експериментальне дослідження процесу функціонування регулятора трафіку DPI системи

4.3.1. Основні функції регулятора трафіку розроблювальної DPI системи

Робоче вікно другого етапу моделі містить: елементи управління потоком трафіку, засоби візуалізації стану каналу та меню вибору джерела захоплення пакетів і виглядає наступним чином:

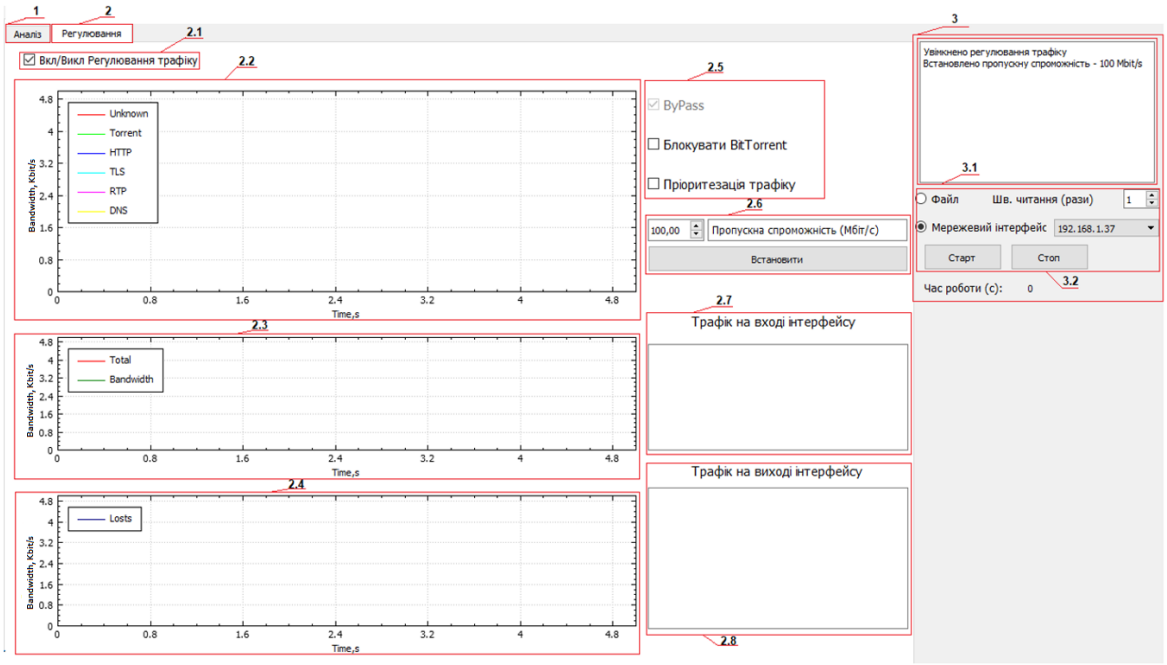


Рис.4.17. Графічний інтерфейс розроблювальної системи DPI

На рис. 4.17. зображено робоче вікно імітаційної моделі. Оскільки робота розділена на 2 етапи (аналіз трафіку та регулювання трафіку), то вікно програми також розділено на дві вкладки. Дані отримані в результаті виконання аналізу трафіку (першого етапу) є вхідними даними роботи програми регулювання трафіку(другого етапу).

Елементи інтерфейсу моделі позначені на рис.4.17:

1. Вкладка аналізу трафіку;

2. Вкладка регулювання трафіку:

2.1 Кнопка увімкнення, або для вимкнення регулювання;

2.2 Графік на якому відображається вхідний трафік по протоколах. У лівому верхньому кутку даного графіку відображена легенда. Навантаження кожного протоколу відображається кривою відповідного кольору на графіку. Червоним кольором відображається невідоме навантаження (навантаження яке не вдалось визначити аналізатором);

2.3 Графік на якому відображається загальне навантаження та поточне навантаження на інтерфейс. На даному графіку червоною кривою

відображається загальне навантаження на інтерфейс, а зеленою відображається смуга пропускання конкретного інтерфейсу;

2.4 Графік на якому відображаються загальні втрати;

2.5 Кнопки , які визначають режими роботи програми;

2.6 Вікно встановлення пропускної здатності інтерфейсу;

2.7 Статистика вхідного трафіку на певному інтерфейсі;

2.8 Статистика вихідного трафіку на певному інтерфейсі;

3.1 Журнал подій;

3.2 Меню вибору джерела захоплення мережевих пакетів.

Для початку роботи з даною програмною DPI системою слід задати джерело захоплення пакетів: файл , або ж мережевий інтерфейс. При читанні пакетів із файлу відкривається провідник де слід вибрати файл формату .pcap. У випадку читання із мережевого інтерфейсу програма сканує всі доступні їй мережеві інтерфейси та відображає їх у стрічці вибору мережевого інтерфейсу. Далі для роботи можливості регулювання трафіку потрібно встановити галочку у вікні 2.1 та в меню встановлення пропускної здатності встановити пропускну здатність каналу та натиснути кнопку «Старт».

Дана DPI система може працювати у декількох режимах регулювання:

1) *ByPass* – при роботі даного режиму усі інші режими вимкнені і програма не здійснює ніякого впливу на вхідний та вихідний трафік. Здійснюється лише вивід графіків та відображення статистики. Режим ByPass використовується для цілей моніторингу стану інтерфейсу та встановлений по замовчуванню.

2) *Блокування* – при роботі даного режиму увесь трафік, що був розпізнаний як «шкідливий» блокується і не проходить через інтерфейс. Даний режим доцільно використовувати тоді, коли «шкідливий» трафік займає велику частку від загальної пропускної здатності і через це абоненти, які користуються іншими послугами, такими як відео або аудіо зв’язок не отримують належної якості обслуговування.

Алгоритм роботи регулятора показано на рис.4.18.

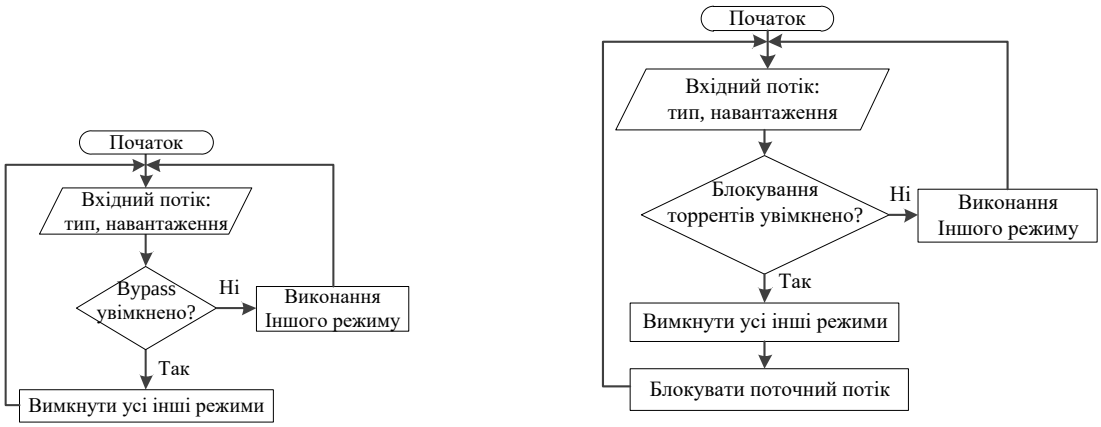


Рис.4.18. Алгоритм роботи моделі у режимі «ByPass» – а) та алгоритм роботи моделі у режимі « Блокування торрентів » – б)

3) *Пріоритезація трафіку* – при роботі даного режиму «шкідливий» трафік не блокується повністю. Пріоритет надається даним реального часу. Тобто «шкідливий» трафік блокується лише у тому випадку, коли його проходження призводить до втрати даних реального часу в іншому випадку трафік не блокується. Даний режим застосовується у випадках, коли навантаження шкідливого трафіку на інтерфейс незначне, але може призвести до погіршення якості обслуговування трафіку. Алгоритм роботи показано на рис.4.19.

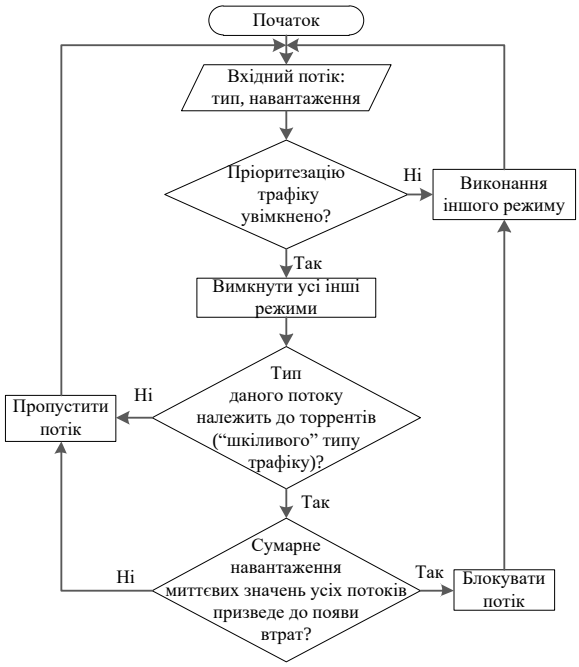


Рис. 4.19. Алгоритм роботи моделі у режимі «Пріоритезація трафіку»

Вибір режиму роботи системи дає змогу збільшити гнучкість каналу передачі та змінювати його поведінку не лише в залежності від його завантаження, але й від типу даних що передаються.

4.3.2. Дослідження процесу функціонування регулятора трафіку DPI системи

Для демонстрації роботи програми у режимі захоплення пакетів із мережевої карти увімкнемо регулювання трафіку, встановимо пропускну здатність інтерфейсу на рівні 5 Мбіт/с , виберемо режим читання із мережевого інтерфейсу та натиснемо кнопку «Старт». За замовчуванням дана модель працює у режимі ByPass. Відкриємо у браузері декілька сайтів, щоб побачити створене навантаження на інтерфейс. Як видно графіку навантаження по протоколах більшість навантаження створюється невідомими типами трафіку, TLS та DNS трафіком. Із графіку загального навантаження видно, що середнє навантаження на даному відрізку часу менше 400 Кбіт/с, що говорить про те, що навантаження, яке створюється одним користувачем є значно меншим ніж смуга пропускання і таких показників не достатньо для аналізу розроблених методів регулювання трафіку.

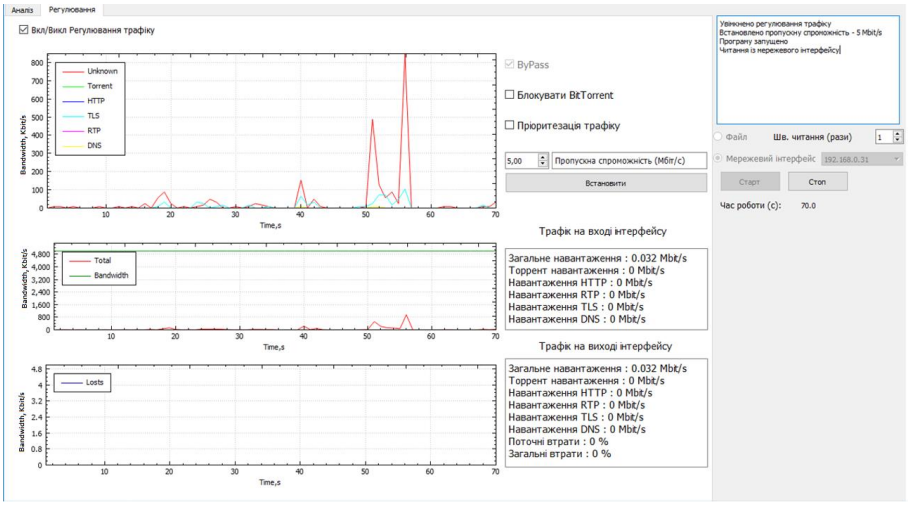


Рис.4.20. Робота DPI при захопленні пакетів із мережевої карти

Тому для подальшого аналізу використовується режим захоплення пакетів із файлу у якому містяться захоплені мережеві пакети від багатьох абонентів та різноманітність протоколів та створюваних ними навантажень достатня для проведення аналізу доцільності розроблених методів.

Для демонстрації роботи програми у режимі захоплення пакетів із файлу, встановимо пропускну здатність інтерфейсу на рівні 40 Мбіт/с.

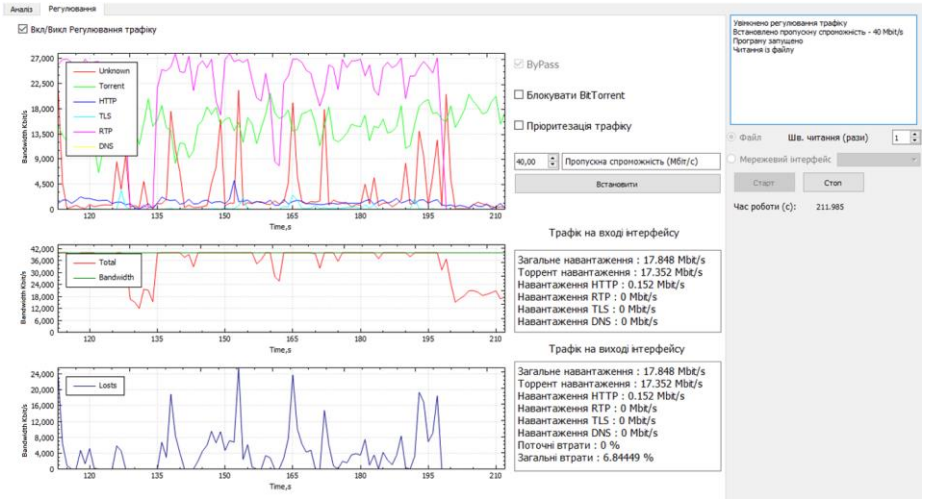


Рис.4.21. Робота моделі при захопленні пакетів із файлу [193]

Як видно із рисунку у режимі читання із файлу є достатня кількість навантаження різними протоколами. Більшість навантаження створюється такими протоколами як : RTP (~21 Мбіт/с), BitTorrent (~16 Мбіт/с), HTTP (~2 Мбіт/с), TLS(~0.5 Мбіт/с) та іншим видом навантаженням. Як видно із графіку втрат у даному випадку присутні значні втрати на рівні 6,8 % від загальних. З отриманих результатів можна зробити висновок, що файл підходить для проведення подальших дослідів та демонстрації роботи моделі у різних режимах.

4.4. Метод виявлення аномалій мережевого трафіку та атак для майбутніх інтенційно-орієнтованих інфокомунікаційних мереж

У роботі удосконалено метод виявлення аномалій мережевого трафіку, який відрізняється від відомих формуванням набору інформативних ознак, що характеризують нормальну та аномальну поведінку інфокомунікаційної системи на основі оцінки параметра Херста із можливістю самонавчання, що дало змогу за короткий проміжок часу з високим ступенем точності автоматизовано виявляти та блокувати складні атаки різних типів в традиційних та майбутніх інтенційно-орієнтованих мережах. Ідейним підґрунтям використання параметра Херста стало те, що в процесі дослідження

характеристик інформаційних потоків можна знайти унікальний взаємозв'язок між певним протоколом по якому передається трафік та характерного для нього параметра Херста. Зокрема шляхом проведення ряду контрольних вимірювань і заповнення у специфічному вигляді таблиці по кожному трафіку користувача можна в подальших спостереженнях робити висновки про нормальність чи аномальність трафіку, ґрунтуючись на віддаленості отриманих фактичних значень параметра Херста, від значень еталонного трафіку без аномалії, які наперед є навченими та встановленими в таблиці користувача. У зв'язку із простотою та високою швидкістю обрахунку для визначення параметра Херста трафіку використано R/S методику. Її суть полягає в наступному.

Визначається середнє значення інтенсивності надходження пакетів вхідного трафіку $X_k\left(k=1..N\right)$:

$$M_N = \frac{1}{N}\sum_{k=1}^{N} X_k \tag{4.3}$$

Визначається дисперсія інтенсивності надходження пакетів вхідного трафіку $X_k\left(k=1..N\right)$:

$$S_N^2 = \frac{1}{N}\sum_{k=1}^{N}\left(X_k - M\right)^2 . \tag{4.4}$$

Для оцінювання розмаху значень інтенсивності надходження пакетів запропоновано використати інтегральне відхилення, яке являє собою поінтервальне визначення відхилення суми j значень інтенсивності мультисервісного трафіку від j середніх значень інтенсивності.

Визначається інтегральне відхилення:

$$D_j = \sum_{k=1}^{j} X_k - jM,\ \mathrm{j}\in[1;\mathrm{N}] . \tag{4.5}$$

Відповідно, утворюється масив даних, для якого визначається розмах як різниця між максимальним та мінімальним значенням інтегрального відхилення.

Визначається рознесення інтегрального відхилення інтенсивності трафіку:

$$R_N = \max_{1 \le j \le N} D_j - \min_{1 \le j \le N} D_j . \tag{4.6}$$

Зі співвідношення:

$$\frac{R}{S} \approx \left(\frac{N}{2}\right)^H \tag{4.7}$$

визначається параметр Херста H для профілю вхідного трафіку:

$$H = \frac{\log\left(\frac{R_N}{S_N}\right)}{\log\left(\frac{N}{2}\right)} . \tag{4.8}$$

Вимірювання параметра Херста відбуваються із певним встановленим вікном моніторингу, зокрема отримані значення записуються у таблиці користувачів кожних 3, 15 та 60 сек. Вікно спостереження не обмежується лише в межах 60 секунд, а може бути і більшим. Проте в умовах зростання вікна спостереження процес виявлення аномалій буде довшим.

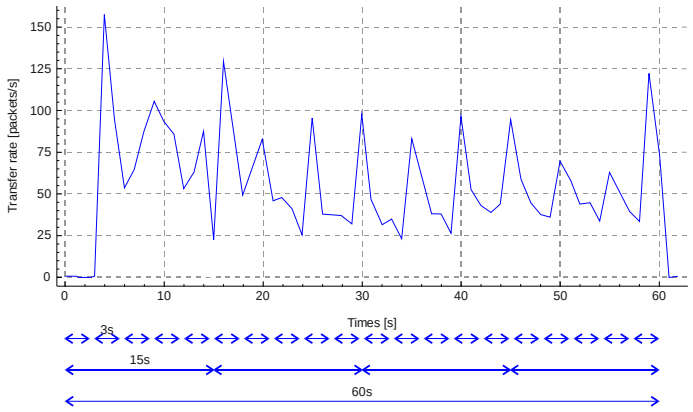


Рис.4.22. Приклад моніторингу трафіку з різним вікном спостереження [190]

Важливою частиною методу є концепція зберігання довідкових значень в таблицях. У таблицях передбачається зберігати дані, отримані після застосування математичної формули визначення параметра Херста. Кожен користувач ідентифікований DPI системою наприклад за IP-адресою містить свою таблицю моніторингу значень інформативних ознак трафіку згідно визначеного критерію Херста. Таблиці вважаються простроченими, якщо пристрій не отримує дані від абонента протягом заданого часу очікування. У

таблиці абонента зберігається його IP-адреса, час створення таблиці, а також інші значення, які не змінюються під час функціонування системи моніторингу. Крім того, в таблиці користувача зберігаються дані з 3-х різних вікон моніторингу (20 рядків 3-х секундного вікна, 4 рядка 15-секундного вікна і 1 рядок хвилинного вікна). У таблиці 4.2 наведено приклад таблиці абонента, заповненої в результаті роботи на етапі навчання.

Таблиця 4.2

Приклад таблиці користувача для DPI (вікно моніторингу 3 секунди)

IP.addr=XX.XX.XX.XX			**Another.data**		
Int., s.	**H1**	**H2**	**H3**	**H4**	**Hn**
Window.size=3sec.					
1-3	$H_{1\text{-}3}1$	$H_{1\text{-}3}2$	$H_{1\text{-}3}3$	$H_{1\text{-}3}4$	$H_{1\text{-}3}n$
…-…	…	…	…	…	…
58-60	$H_{58\text{-}60}1$	$H_{58\text{-}60}2$	$H_{58\text{-}60}3$	$H_{58\text{-}60}4$	$H_{58\text{-}60}n$
$H_{avg(3sec)}$	$H_{avg\ 1}$	$H_{avg\ 2}$	$H_{avg\ 3}$	$H_{avg\ 4}$	$H_{avg\ n}$
$SN_{(3sec)}$	$SN_{(3sec)}1$	$SN_{(3sec)}1$	$SN_{(3sec)}1$	$SN_{(3sec)}1$	$S_{(3sec)}1$

Таблиця 4.3

Приклад таблиці користувача для DPI(вікно моніторингу 15 секунд)

IP.addr=XX.XX.XX.XX			**Another.data**		
Int., s.	**H1**	**H2**	**H3**	**H4**	**Hn**
Window.size=15sec.					
1-15	$H_{1\text{-}15}1$	$H_{1\text{-}15}2$	$H_{1\text{-}15}3$	$H_{1\text{-}15}4$	$H_{1\text{-}15}n$
16-30	$H_{16\text{-}30}1$	$H_{16\text{-}30}2$	$H_{16\text{-}30}3$	$H_{16\text{-}30}4$	$H_{16\text{-}30}n$
31-45	$H_{31\text{-}45}1$	$H_{31\text{-}45}2$	$H_{31\text{-}45}3$	$H_{31\text{-}45}4$	$H_{31\text{-}45}n$
46-60	$H_{46\text{-}60}1$	$H_{46\text{-}60}2$	$H_{46\text{-}60}3$	$H_{46\text{-}60}4$	$H_{46\text{-}60}n$
$H_{avg(15sec)}$	$H_{avg\ 1}$	$H_{avg\ 2}$	$H_{avg\ 3}$	$H_{avg\ 4}$	$H_{avg\ n}$
S_N (15sec)	S_N (15sec)1	S_N (15sec)1	S_N (15sec)1	S_N (15sec)1	S_N (15sec)1

Таблиця 4.4

Приклад таблиці користувача для DPI (вікно моніторингу 60 секунд)

IP.addr=XX.XX.XX.XX			**Another.data**		
Int., s.	**H1**	**H2**	**H3**	**H4**	**Hn**
Window.size=60sec.					
1-60	$H_{1\text{-}3}1$	$H_{1\text{-}3}2$	$H_{1\text{-}3}3$	$H_{1\text{-}3}4$	$H_{1\text{-}3}n$
$H_{avg(60sec)}$	$H_{avg\ 1}$	$H_{avg\ 2}$	$H_{avg\ 3}$	$H_{avg\ 4}$	$H_{avg\ n}$

Як видно з прикладу таблиці користувачів в кінці кожного блоку записується середнє значення для кожного контрольованого об'єкта. Якщо вікно моніторингу дорівнює 60 секундам, то ці значення не враховуються (не обов'язково). Стандартне відхилення також враховується і записується в таблицю. Стандартне відхилення враховується для вікон моніторингу тривалістю 3 і 15 секунд. Сенс використання 3 різних типів вікон моніторингу полягає в тому, щоб на етапі виявлення мати більш точні дані для алгоритму.

Для кожного вікна спостереження визначається дисперсія S_N та середнє значення M_N параметра Херста. Після чого робиться висновок про присутність у трафіку аномалії шляхом їх порівняння із еталонним трафіком. Для прикладу, якщо трафік еталонного трафіку володіє наближеним нормальним розподілом для порівняння відхилень значень параметра Херста можна використати правило “трьох сигм”.

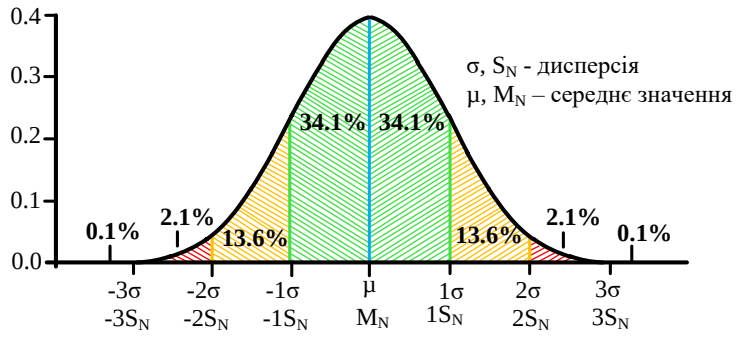
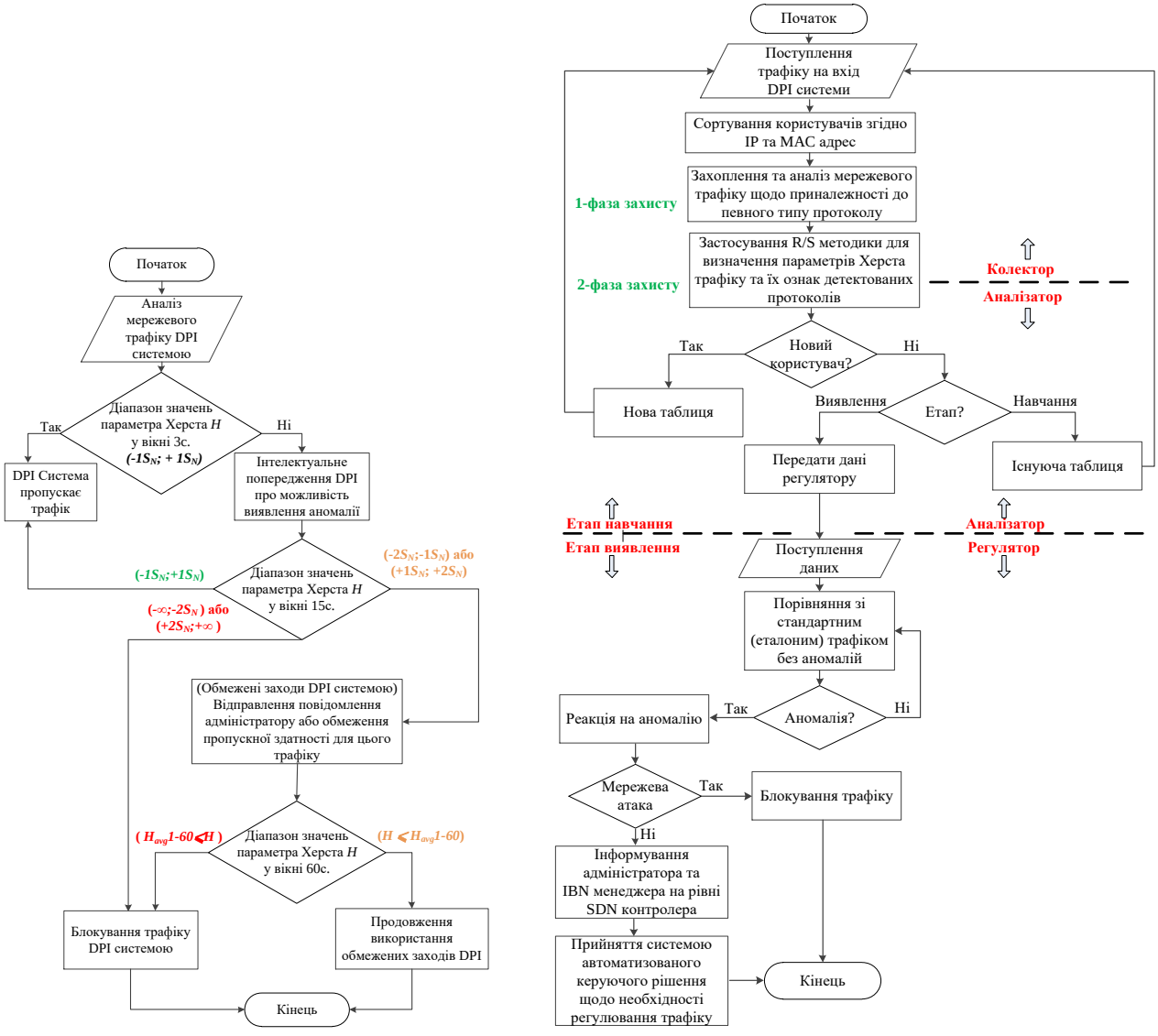


Рис.4.23. Правило “трьох сигм”

У цьому випадку представляється логічним запропонувати використовувати віддаленість від діапазону*(-1 S_N;+1 S_N)* як критерій аномалії трафіку. Таким чином, значення трафіку в діапазонах *(-∞;-1S_N)* або *(1S_N;+∞)* можна вважати аномальними. Якщо умова виконується у вікні протягом 3 секунд, то все вважається в порядку. Якщо в 3-секундному вікні умова не виконується (значення *H* виходять за межі нормального діапазону), система має підстави вважати, що існує аномалія. Однак система буде чекати значення 15-секундного вікна і порівнюватиме його з таблицями, розрахованими на етапі

навчання. Якщо на 15-секундному вікні немає аномалії, це вважається нормою, і ніяких дій не вживається. Якщо і тут є аномалія, необхідно з'ясувати, наскільки величина відхиляється від умовної норми. Якщо діапазон відхилень лежить у *(+1 S_N;+2 S_N)* або *(-2 S_N;-1 S_N)*, будуть вжиті обмежувальні заходи, і система буде продовжувати чекати значення хвилинного вікна.



а) б)

Рис. 4.24. Блок схема алгоритму виявлення аномалій для компонента DPI системи, що відповідає за регулювання трафіку– а) та блок-схема автоматизованого методу напів-контрольованого виявлення аномалії і запобігання атак на основі оцінки критерію Херста інформативних ознак трафіку– б) [190]

Якщо діапазон становить $(+2\ S_N;+\infty)$ або $(-\infty;-2\ S_N)$, система негайно вживатиме обмежувальних заходів. У хвилинному вікні можна отримати лише одне значення, тому в цьому вікні як критерій буде використано просте порівняння значень H для $H \leqslant Havg_{1\text{-}60}$. Якщо дана умова виконується, трафік вважається нормальним, якщо не виконується, трафік є аномальним.

Як видно з алгоритму, при виявленні аномалії в самому маленькому вікні моніторингу (3 секунди), система позначить це значення як підозріле, але не зробить ніяких дій (так як не можна з повною впевненістю сказати, що трафік аномальний, враховуючи характер "сплесковості" мережевого трафіку), можливо, це всього лише "точкова" аномалія. Якщо аномальна поведінка зберігається у вікні моніторингу протягом 15 секунд, то будуть вжиті відповідні заходи (обмежувальні або заборонні). Якщо аномальна поведінка також зберігається у вікні хвилинного моніторингу, то вже будуть прийняті заборонні заходи (блокування трафіку). Слід зазначити, що застосування заходів можливе лише в "серійному режимі". В іншому випадку DPI система пасивно інформує адміністратора про проблему (повідомлення в syslog, електронна пошта і т.д. або автоматично обмежує пропускну здатність цього трафіку для забезпечення QoS в режимі реального часу).

Блок-схема автоматизованого методу напів-контрольованого виявлення аномалії і запобігання атак на основі оцінки критерію Херста інформативних ознак трафіку для розроблювальної DPI системи показано на рис.4.24б.

4.5. Експериментальний стенд реальної корпоративної мережі для порівняння ефективності функціонування існуючої DPI системи із запропонованою інтелектуальною DPI

У роботі проведено порівняння розробленої інтелектуальної програмної DPI системи із існуючою для комерційного застосування системою DPI SolarWinds, яка також включає у себе функції виявлення мережних аномалій, контролю трафіку, детектування інформаційних протоколів та розпізнавання

атак. Для цього розроблено експериментальний стенд реальної мережі (рис.4.25), що складається із: кінцевих пристрої (камера IoT, ноутбук та комп'ютер), що генерують законний (легітимний) трафік, генератора нелегітимного трафіку (мережева атака) є звичайний комп'ютер у корпоративній мережі, мережевих пристрої в корпоративній мережі (комутатор і маршрутизатор), об'єкта атаки - стандартного веб-сервера в Інтернеті, та встановленого на окремих серверах перед маршрутизатором програмне забезпечення двох DPI систем із віддзеркаленням вхідного трафіку.

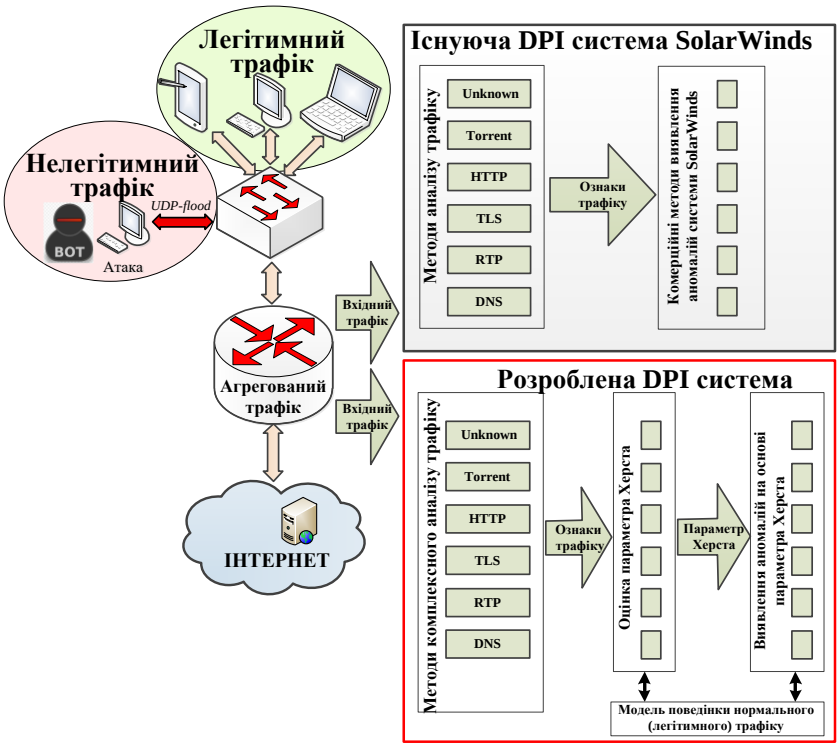


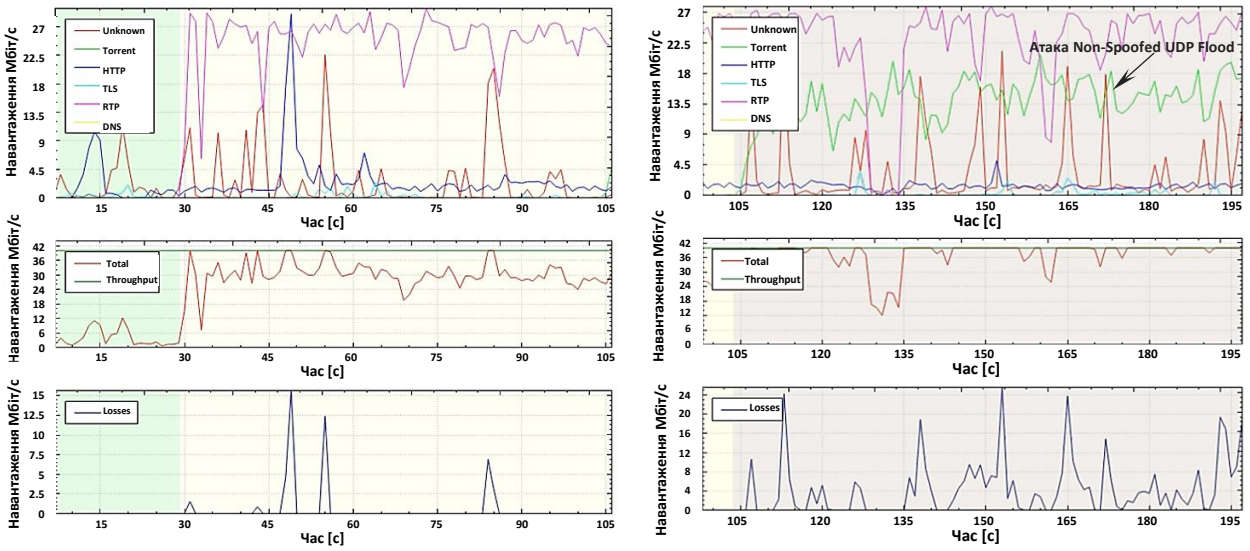
Рис. 4.25. Експериментальний стенд реальної корпоративної мережі для порівняння ефективності функціонування існуючою DPI системи із запропонованою [190]

Для подальшого аналізу та порівняння систем використовується режим захоплення файлів (файл. pcap) для захоплення мережевих пакетів від усіх абонентів, включаючи нелегітимний трафік та різноманітність створюваних ними протоколів. Захопивши пакети, можна дослідити однаковий сукупний трафік для двох систем, щоб отримати точні результати для порівняння. Щоб

продемонструвати систему в режимі захоплення пакетів з файлу, встановлено пропускні здатності інтерфейсів на рівні 40 Мбіт/с. Більшість законних трафіків створюються такими протоколами, як RTP, Torrent, HTTP, TLS та іншими типами. Для генерації нелегітимного трафіку використано атаку типу (*Non-Spoofed UDP Flood*). Відмінність від *UDP Flood* полягає в тому, що UDP пакети генеруються з реальних IP-адрес ботами, що істотно ускладнює виявлення цих видів атак, особливо якщо боти генерують трафік через NAT, за яким знаходяться легітимні користувачі [199]. Так само, як і звичайний UDP Flood, цей вид атак спрямований на вичерпання системних ресурсів і заповнення каналу "непотрібним" трафіком. Такій атаці піддався відомий ігровий сервер MMORPG Albion Online [200]. Фільтрувати UDP трафік під час такої атаки - досить складне завдання, тому більшість операторів та систем пропонують тільки одне рішення - блокування трафіку, що в свою чергу є небажаним, оскільки може призвести до помилкового блокування легітимного трафіку, що передається протоколом UDP.

Першим етапом експерименту є моніторинг завантаженості каналу мережі існуючою DPI SolarWinds та пропонованою DPI системами в умовах передавання лише законного трафіку. Обидві системи показали однакові результати використання пропускної здатності (рис. 9а). Як бачимо з рис. 9а (область зеленого кольору) на початковому етапі, навантаження на інтерфейс незначне і коливається на рівні 2 Мбіт/с, а рівень втрат – 0% від загального навантаження. Цей період часу показує завантаженість каналу в умовах низьких навантаженнях, створюваними такими протоколами, як HTTP, TLS та невідомим трафіком. При подальшому моніторингу внаслідок появи трафіку RTP протоколу, спостерігається зростання навантаження на інтерфейс до 38 Мбіт/с із загальною втратою даних – 1,8% від сумарного вхідного трафіку у Мбіт/с (область жовтого кольору рис. 9а). Слід зазначити, що втрати на певних періодах спостереження спричинені сплесковістю трафіку і не є постійними.

Другим етапом експерименту є моніторинг пропускної здатності в процесі передавання легітимного та нелегітимного трафіку (атаки класу UDP Floods) за допомогою існуючої системи DPI SolarWinds. Система SolarWinds DPI виявляє Non-Spoofed UDP Flood атаку як легітимний трафік uTP, що теж передається протоколом UDP. Моніторинг пропускної здатності під час передавання трафіку атаки за допомогою графічного інтерфейсу системи DPI показано на рис. 4.26а. Як бачимо з рис. 4.26б, це призводить до значних втрат інших видів трафіку, таких як RTP та HTTP, рівень загальних втрат збільшився до 7,2%, а максимальний відсоток поточних втрат склав 48%, також характер втрат із стрибкоподібного змінився на постійний. Це свідчить про те, що щосекунди втрачається до 48% корисного навантаження. Такі втрати неприпустимі для проведення, наприклад, відеоконференцій, IP-телефонії або комфортного серфінгу в Інтернеті.



а) б)

Рис.4.26. Моніторинг пропускної здатності каналу під час передавання законного трафіку за допомогою існуючої DPI SolarWinds та запропонованої системи DPI – а), моніторинг пропускної здатності каналу під час передавання легітимного та нелегітимного трафіку (Non-Spoofed UDP Flood) за допомогою системи SolarWinds DPI – б) [190]

Третім етапом експерименту є моніторинг пропускної здатності в процесі передавання легітимного та нелегітимного трафіку (атаки класу UDP Floods) за допомогою запропонованої системи DPI. Зокрема для кожної групи тестових даних DPI системою знайдено діапазон $(-3S_N; +3S_N)$ відхилення критерію Херста та оцінено статистичну значимість відмінностей середніх значень від еталонного (модель поведінки нормального легітимного трафіку). Використовуючи запропоновану систему, у 3-секундному вікні моніторингу створювана атака розпізнається як протокол uTP із підозрою на аномалію. Оскільки оцінений параметр Херста не знаходиться в межах $(-1S_N;+1S_N)$, що показано на рис. 4.27а та згідно запропонованого алгоритму на рис. 4.24, будуть вжиті обмежувальні заходи. У цьому випадку дані, що мають вищий пріоритет, передаються першими. Під час роботи режиму пріоритетності трафіку "шкідливий" трафік передається тоді, коли це не погіршує якість інших послуг.

На рис. 4.27б червоним кольором позначені області, де навантаження незначне. Для оператора це означає простій каналу, тому для запобігання простою в дані моменти часу, передається розпізнаний протокол uTP, як торрент трафік, проте розроблена DPI система ще не повністю провела аналіз щодо виявлення аномалії по даному трафіку. У даному випадку забезпечується достатній рівень QoS для послуг з високим пріоритетом, але дані торрентів повністю не блокуються. Із використанням даного режиму, при навантаженні 52.52 Мбіт/с, рівень загальних втрат складав 2%, а максимальні поточні втрати 19% (рис. 4.27б). Але, згідно із запропонованим алгоритмом виявлення аномалії, після моніторингу 3-х секундного вікна система буде чекати на отримані значення 15-секундного вікна моніторингу та порівнювати параметр Херста із таблицями, розрахованими на етапі навчання. Оскільки обчислюваний параметр Херста для 15 секундного вікна моніторингу знаходиться в межах $(+1S_N; +2S_N)$ (рис.4.27в), то відповідно до алгоритму рис. 4.24б, якщо діапазон відхилень лежить в межах $(+1S_N; +2S_N)$ будуть вжиті обмежувальні заходи, і система буде продовжувати чекати значення хвилинного вікна. Побудова графіку для вікна хвилинного моніторингу не має

сенсу, оскільки значення існує в одній копії, і як критерій аномальності буде використано просте порівняння значень *H* для *Havg1-60*⩽*H*. З рис. 4.27в видно, що для цього експерименту $H_{avg1-60}$ = *0,403* та *H* = *0,599*, при якому можна вважати, що трафік є аномальним відносно контрольних значень *0,403<0,599*. Після чого система автоматично заблокувала аномальний трафік, що дало змогу звільнити пропускну здатність системи та покращити параметри якості обслуговування.

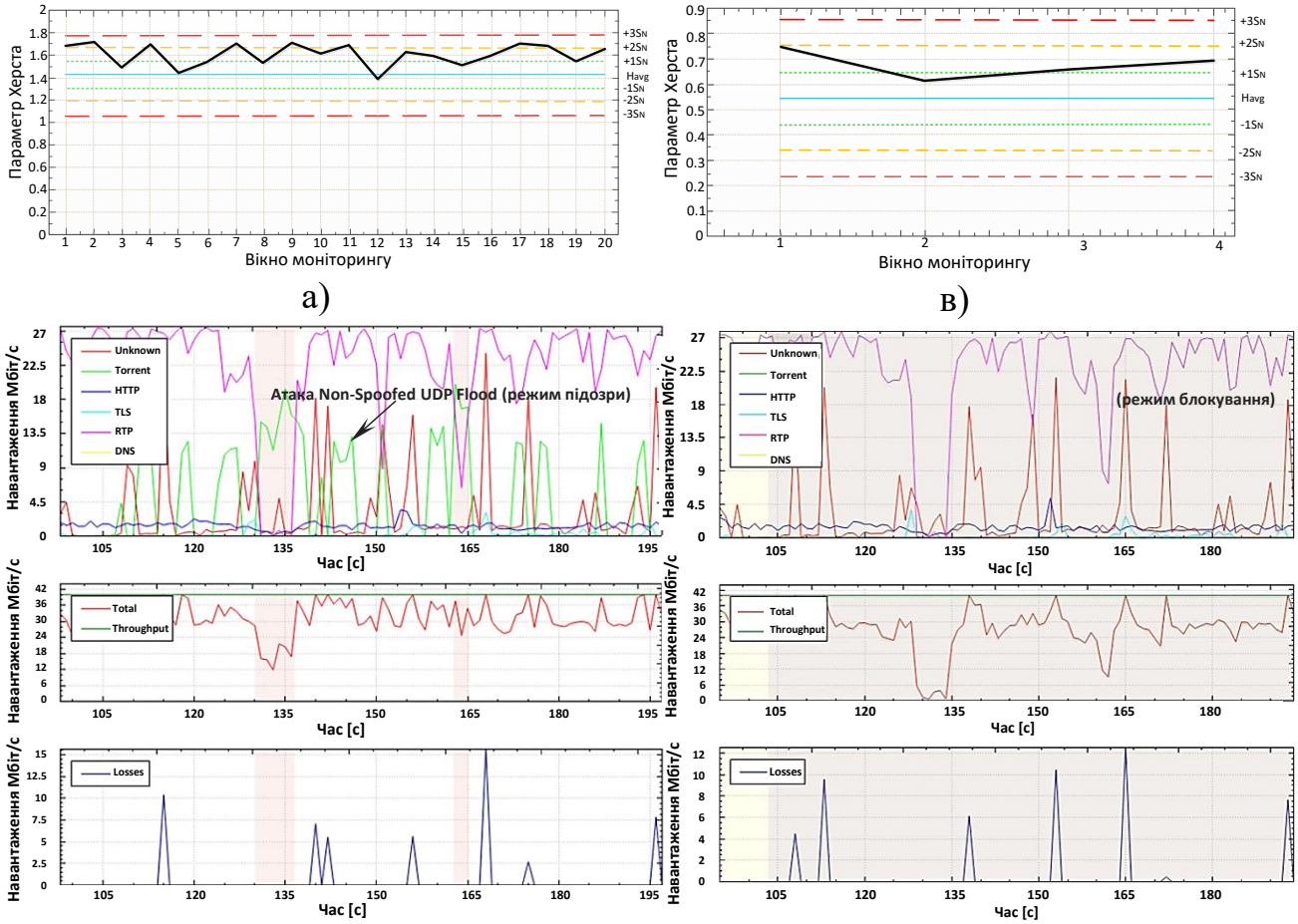


Рис. 4.27. Зміна параметра Херста для класу підозри на "аномалію" у 3-х секундному вікні моніторингу – а), моніторинг пропускної здатності каналу під час передавання легітимного та нелегітимного трафіку за допомогою розробленої системи DPI (режим підозри) – б), зміна параметра Херста у 15-ти секундному вікні моніторингу – в), моніторинг пропускної здатності каналу під час передавання легітимного та нелегітимного трафіку за допомогою розробленої системи DPI (режим блокування) – г) [190]

На рис. 4.27в показано, в якому із вікон моніторингу значення аномального трафіку перевищили поріг і в якому діапазоні вони потрапили за допомогою запропонованої системи. Моніторинг пропускної здатності під час передавання законного та нелегітимного трафіку із використанням запропонованої системи DPI після блокування аномалії показано на рис. 4.27г. В результаті блокування розпізнаної атаки максимальна втрата даних становить 16%, а рівень загальних втрат при загальному вхідному навантаженні на інтерфейс 53,736 Мбіт/с зменшився від 7,2% до 2% у порівнянні із системою DPI SolarWinds (рис. 10г).

Запропонована система має знання класу "норма" для більшості існуючих протоколів, таких як DNS, HTTP, RTP, Torrent та TLS. А розроблена програмна система DPI може виявляти атаки, такі як: SYN Flood, фрагментація HTTP, UDP Flood, DNS Flood, Media Data Flood, Non-Spoofed UDP Flood.

Запропонована система DPI апробована та впроваджена в корпоративній мережі інфраструктури Національного університету "Львівська політехніка". Це дозволило налаштувати першу лінію захисту від мережевих атак з урахуванням виявлених випадків та джерел загроз, які раніше не враховувались у стандартних засобах захисту, що збільшує швидкість реагування на виникаючі загрози та рівень кібербезпеки організації в цілому.

Створені програмні компоненти запропонованої системи DPI підвищують ефективність використання стандартних систем виявлення та запобігання вторгненню шляхом виявлення та врахування нових нестандартних факторів та залежностей. Використання розробленої системи в комунікаційній інфраструктурі дає змогу з достатнім ступенем точності оцінити присутність аномалій трафіку та забезпечити блокування або фільтрацію небажаних інформаційних потоків.

Висновок до розділу 4

1. У даному розділі роботи для підвищення рівня мережевої безпеки в інтенційно-орієнтованих мережах розроблено унікальну систему моніторингу

та аналізу мережевого трафіку, яка базується на гармонійному поєднанні переваг методів сигнатурного, статистичного та фрактального аналізу інформативних ознак щодо детектування інформаційних протоколів та ранжування прихованих властивостей аномального трафіку.

2. Для вирішення проблеми виявлення мережевих аномалій та розпізнавання атак запропоновано метод формування набору інформативних ознак, що формалізують нормальну та аномальну поведінку системи на основі оцінки параметра Херста мережевого трафіку.

3. Встановлено, що розроблені програмні компоненти запропонованої системи підвищують ефективність використання стандартних систем виявлення та запобігання вторгненню шляхом виявлення та врахування нових нестандартних факторів та залежностей. Експериментальним шляхом доведено, що використання розробленої системи в комунікаційній інфраструктурі дало змогу з достатнім ступенем точності оцінити присутність аномалій трафіку та забезпечити блокування або фільтрацію небажаних інформаційних потоків у порівнянні із відомими рішеннями.

4. Встановивши в ключових точках мережі DPI-системи, адміністратори мережі отримують можливість виявляти і обмежувати співробітників, які споживають великий обсяг трафіку особистого характеру, і користувачів, які порушують корпоративні політики використання мережі і доступу в Інтернет, ефективно управляти пріоритезацією трафіку, забезпечуючи зменшення навантаження і підвищення доступності каналів, гарантуючи надійне функціонування критично важливих додатків і сервісів, наприклад, IP-телефонії. Розроблена DPI забезпечує кращу візуалізацію даних, керованість, додаткові можливості створення послуг, підвищення їх експлуатаційної та комерційної ефективності, що є важливим для інтенційно-орієнтованих мереж.

РОЗДІЛ 5. МЕТОДОЛОГІЯ АДАПТИВНОГО СТРУКТУРНО-ФУНКЦІОНАЛЬНОГО СИНТЕЗУ ГЕТЕРОГЕННОЇ ІНТЕНЦІЙНО-ОРІЄНТОВАНОЇ ІНФРАСТРУКТУРИ

5.1. Розроблення методів розподілу радіоресурсів та балансування навантаження в інтенційно-орієнтованій мережі 4G/5G для адаптивного надання сервісів Інтернету речей

У зв'язку із тим, що запропонована методологія синтезу інфокомунікаційної мережі повинна базуватися на таких принципах, як ієрархічність та декомпозиція об'єкту дослідження; узгодження цілей та координації управління; потокового аналізу і моделювання процесів; оптимального, адаптивного та інтенційно-орієнтованого управління, особливу увагу у процесі синтезу гетерогенної IBN мережі для адаптивного надання сервісів присвячено рівню радіодоступу мереж 2G-5G (рис.5.1). Зокрема, для врахування мінливих намірів користувачів щодо якості обслуговування у роботі удосконалено існуючі методи оптимального вибору технології та формування структури рівня радіодоступу, розроблено нові методи планування, розподілу та оптимізації частотно-часових ресурсів.

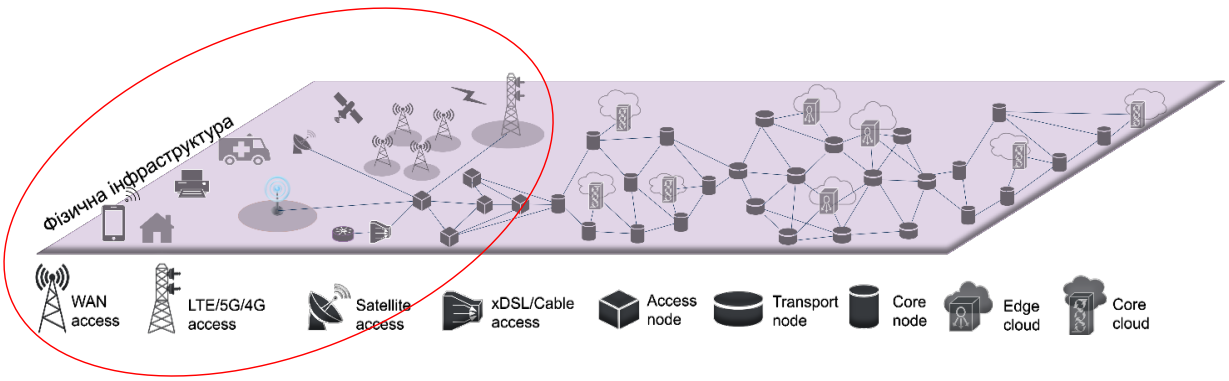


Рис. 5.1. Синтез рівня радіодоступу гетерогенної IBN мережі

В умовах поступового впровадження сервісів IoT на мережі оператора мобільного зв'язку одною із основних ідей в межах концепції IBN є адаптування якості сервісів IoT згідно намірів кінцевих користувачів. Таким

чином, механізми адаптивної пріоритезації трафіку та мехінзми балансування навантаження в мережах 4-го та 5-го покоління для систем IoT є одним з найважливіших аспектів, від якого в подальшому буде залежати розвиток Інтернету речей у світі.

Зокрема, основою для розгортання та адаптивного надання сервісів IoT пропонується використати технологію LTE, яка успішно експлуатується не тільки для мереж 4G, а також згідно розглянутих у першому розділі прогнозів провідних компаній виробників LTE обладнання та наукових вчених буде ядром для розвитку майбутніх мереж 5G/6G. Одним із ефективних шляхів підвищення продуктивності та покращення основних параметрів якості обслуговування (QoS) в мережах, що базуються на технології є застосування принципів оптимального розподілу мережевих ресурсів. Використання рішень щодо розподілу мережевих ресурсів дає змогу ефективно реагувати на зміну стану та умов функціонування безпровідної мережі, які можуть спричинятись, наприклад, виходом з ладу або перевантаженням її елементів, коливаннями трафіку, що надходить у мережу, динамікою зміни сигнально-завадової обстановки тощо. Функції розподілу мережевих ресурсів у технології LTE покладені на систему управління радіоресурсами (Radio Resource Management, RRM) [201], а саме на планувальника (scheduler), який відповідальний за планування ресурсів для станцій користувачів (Users Equipment, UE) та пристроїв IoT.

До таких ресурсів, насамперед, належать символи (часовий ресурс) і частотні піднесучі (частотний ресурс). Найменшою структурною одиницею радіоресурсу, яку можна виділити тій чи іншій станції користувача, є ресурсний блок (Resource Block, RB) [202]. Необхідно зауважити, що рішення RRM про виділення мережевих ресурсів передусім ґрунтується на вимогах до QoS, а при впровадженні сервісів IoT появляється необхідність у нових механізмах пріоритезації трафіку та управління якістю обслуговування в мережах LTE для забезпечення гарантованого E2E QoS. Тому завдання розподілу частотно-

часових ресурсів у гетерогенній мобільній мережі LTE/IoT повинна бути сформульована як завдання розподілу RB між UE мережі та IoT пристроїв, залежно від заявлених вимог до пропускної здатності та параметрів QoS [203].

5.1.1. Побудова інтенційно-орієнтованої гетерогенної мережі 4G/5G для розгортання сервісів IoT

У технології LTE, механізми планування ресурсів низхідного та висхідного каналу зв'язку не визначені стандартом, залишаючи право вибору за виробниками обладнання базових станцій eNodeB [5-7]. Для мінімальних змін технології LTE та відповідних затрат на обладнання пропонується ввести в архітектуру IBN/IoT контролер. Даний контролер відповідатиме за механізми планування ресурсів низхідного та висхідного каналів для IoT пристроїв та дасть змогу операторам мережі залишити існуючі базові станції eNodeB без змін. Контролер - це окрема серверна машина, на якій встановлено програмне забезпечення, що відповідає за планування ресурсів IoT-трафіку (планувальник). Можна встановити цей контролер поблизу базової станції LTE або розгорнути у хмарі з можливістю оренди та збільшення продуктивності сервера. Реалізація побудови залежить від прогнозованої кількості пристроїв IoT, підключених до базової станції. Значне зростання кількості підключених пристроїв вимагає потужної серверної машини для швидкої роботи контролера IoT. Проте проектантам мережі для надання сервісів IoT необхідно окремо виділити вузькосмуговий спектр 200 кГц, оскільки немає необхідності у високій пропускній здатності за рахунок передавання малих об'ємів даних. У разі потреби надання високих швидкостей, пропонується передавати дані у спектрі LTE. На рис.5.2 запропоновано удосконалену архітектуру мережі мобільного зв'язку 4G/5G на основі технології LTE для впровадження сервісів IoT [204]. Згідно наведеної у другому розділі концептуальної моделі гетерогенної мережі IBN, EPC ядро мережі LTE може бути повністю віртуалізоване на серверних машинах використовуючи для цього технологію

віртуалізації мережевих функцій NFV, а у поєднанні із використанням програмно-конфігурованої радіосистеми SDR та централізованого головного контролера SDN/IBN дасть змогу забезпечити основний принцип програмованості, що вимагається для концепції гетерогенної IBN мережі.

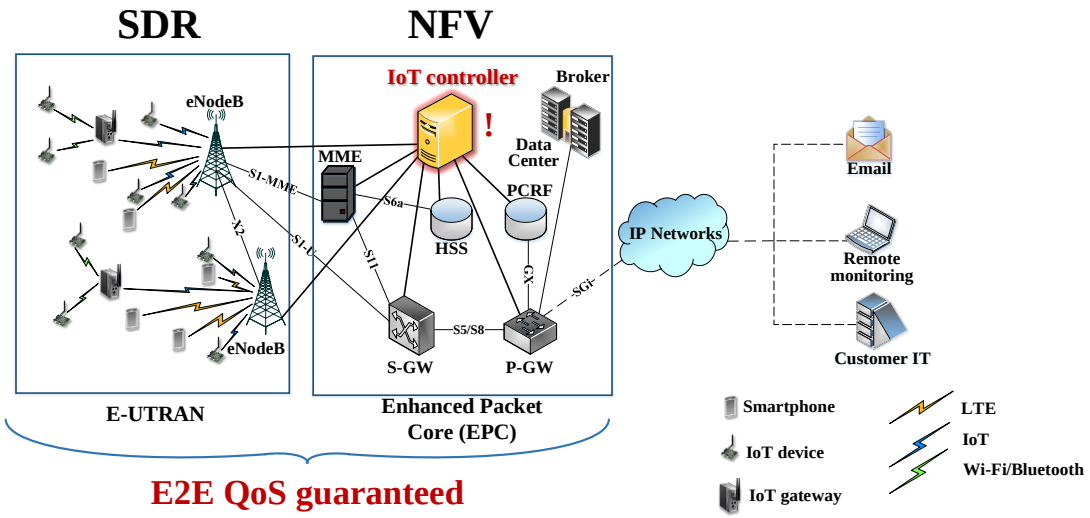


Рис. 5.2. Архітектура інтенційно-орієнтованої гетерогенної мережі 5G LTE/IoT

Відмінною особливістю мереж LTE є відмова від повторного використання частот. Тобто абоненти в усіх комірках передають і приймають дані в одних і тих же смугах частот в один і той же час, що є причиною виникнення міжкоміркової інтерференції (Inter-Cell Interference або ICI). Найбільш гостро ця проблема зачіпає тих абонентів та IoT пристроїв, які знаходяться на краю комірки. Якщо дві сусідні базові станції виділяють своїм IoT пристроям під передавання даних ресурсні блоки в одній і тій же смузі частот і в один і той же час, то можна з певною часткою ймовірності стверджувати, що ці пристрої будуть заважати один одному. Проблема найбільш ефективного використання частотного-часових ресурсів мережі хвилює всіх операторів, які надають послуги на основі мереж 4G/5G.

У даній роботі розглядаються методи зменшення впливу міжкоміркової інтерференції і збільшення відношення сигнал/шум на кордонах комірок на основі статистичних даних про радіоумови IoT пристрою (користувача) (SINR -

Signal to Noise plus Interfetence Ratio) і з використанням динамічних підходів до координації інтерференції по інтерфейсу X2 при виділенні вузькосмугового спектру IoT в спектрі LTE. На рис. 5.3. запропоновано в процесі планування покриття мереж виділяти IoT спектр на кінці спектру LTE (рис.5.3а), на початку спектру LTE (рис.5.3 б) та всередині спектру LTE (рис.5.3в).

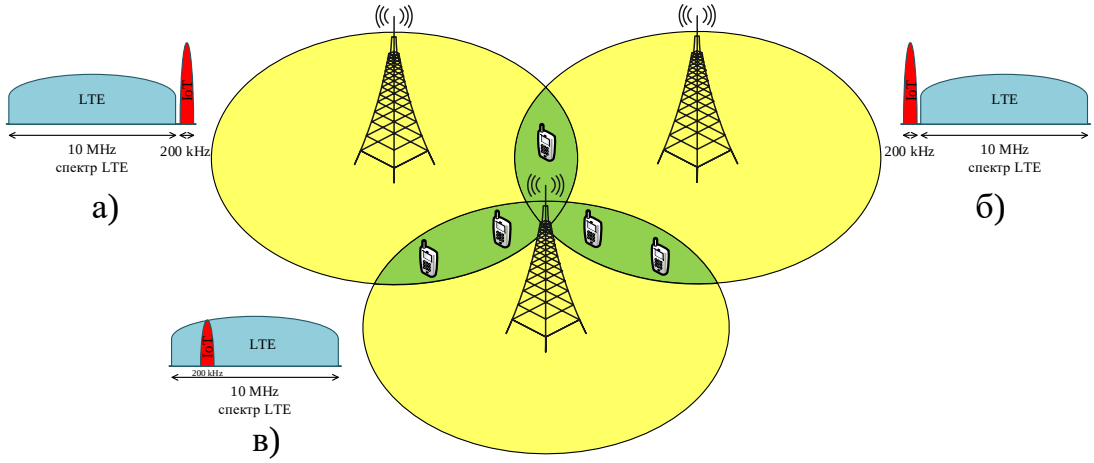


Рис. 5.3 Спосіб виділення вузькосмугового спектру IoT в спектрі LTE

Метод координації міжкоміркової інтерференції заснований на тому, що сусідні базові станції передають по X2 інтерфейсу інформацію про свою завантаженність у вигляді Overload, тобто рішення при розподілі ресурсів приймається на підставі попередньо зібраної статистичної інформації. Таким чином, базові станції фактично мають можливість домовитися між собою хто з них який піддіапазон (subband) і в який момент часу буде використовувати.

Такий алгоритм розподілу ресурсів дозволяє збільшити пропускну здатність системи, за рахунок збільшення відношення сигнал/шум для абонентів та пристроїв IoT, що знаходяться на кордоні комірок, і як наслідок оптимального використання схеми модуляції і кодування.

Простий спосіб, за допомогою якого UE або IoT може вибрати відповідне значення індикатора показника якості каналу (CQI), базується на значеннях частоти блокових помилок (Block Error Rate, BLER). UE або IoT на основі виміряної якості прийнятого сигналу згідно зі значенням CQI проводить вибір

відповідної схеми модуляції та кодування, яка забезпечує BLER≤10%. Список схем модуляції та кодових швидкостей зі значеннями CQI, що підтримуються в стандарті 3GPP LTE [205], наведено в таблиці 5.1.

Таблиця 5.1

Відповідність сигнально-кодової конструкції значенню CQI

Індекс показника якості каналу	Модуляція	Швидкість кодування	Спектральна ефективність	Відношення сигнал/шум
1	QPSK	0.0762	0.1523	-6.7
2	QPSK	0.1172	0.2344	-4.7
3	QPSK	0.1885	0.3770	-2.3
4	QPSK	0.3008	0.6016	0.2
5	QPSK	0.4385	0.8770	2.4
6	QPSK	0.5879	1.1758	4.3
7	16QAM	0.3691	1.4766	5.9
8	16QAM	0.4785	1.9141	8.1
9	16QAM	0.6016	2.4063	10.3
10	64QAM	0.4551	2.7305	11.7
11	64QAM	0.5537	3.3223	14.1
12	64QAM	0.6504	3.9023	16.3
13	64QAM	0.7539	4.5234	18.7
14	64QAM	0.8525	5.1152	21.0
15	64QAM	0.9258	5.5547	22.7

5.1.2. Метод інтенційно-орієнтованого розподілу радіоресурсів в мережах 4G/5G для адаптивного надання сервісів IoT

У роботі вперше розроблено метод розподілу частотно-часових ресурсів низхідного та висхідного каналу зв’язку гетерогенної мережі LTE/NB-IoT, який, на відміну від відомих, враховує наміри користувачів щодо рівня якості надання сервісів Інтернету речей та проводить адаптивне інтелектуальне планування процесом виділення радіоресурсів на основі аналізу пріоритетності даних, зокрема у вузькосмуговому NB-IoT спектрі, що дало змогу забезпечити необхідну інтенційно-орієнтовану якість обслуговування із кінця в кінець. Далі у роботі надається більш детальний опис розробленого методу.

Визначення класу, до якого належить той чи інший трафік UE пропонуємо проводити на основі параметру QCI (QoS Class Identifier). Параметр QCI може приймати один із дев'яти станів, кожен з яких, відповідно, асоціюється з певним видом сервісу (ToS), а відтак і з видом каналу передачі, швидкістю, коефіцієнтом помилок та затримкою. QCI є міткою у пакеті IPv6 "ID каналу". Для сервісів IoT запропоновано метод пріоритезації трафіку, який базується на основі критерію допустимих затримок та середньої кількості відмов в обслуговуванні. Згідно таблиці 5.2 запропоновано 4 класи сервісів IoT з різними вимогами до QoS. QCI_{IoT} є міткою у пакеті IPv6, значення якого записується у полі ToS.

Таблиця 5.2

Характеристики QCI_{IoT}

QCI_{IoT}	Тип	Пріоритет	Допустима затримка $T_з$, мс	Допустима кількість відмов в обслуговуванні, $P_в$%	Клас послуг сервісів IoT
1	Гарантований час передавання даних (GBR_{IoT}) трафік реального часу	1	10	0,01	L1
2		2	20	0,1	L2
3	Гарантований час передавання даних (GBR_{IoT}) трафік нереального часу	3	1000	5	L3
4	Негарантований час передавання даних (Non-GBR_{IoT}) трафік нереального часу	4	$t_{невизначене}$	$P_{невизначене}$	L4

На рис.5.4 показано процедуру оптимального використання схеми модуляції і кодування для забезпечення QoS на фізичному рівні. Після чого

механізм планування пропускної здатності використовується LTE та IoT планувальниками для виділення UE та IoT пристрою ресурсу з необхідною швидкістю передавання для забезпечення E2E QoS.

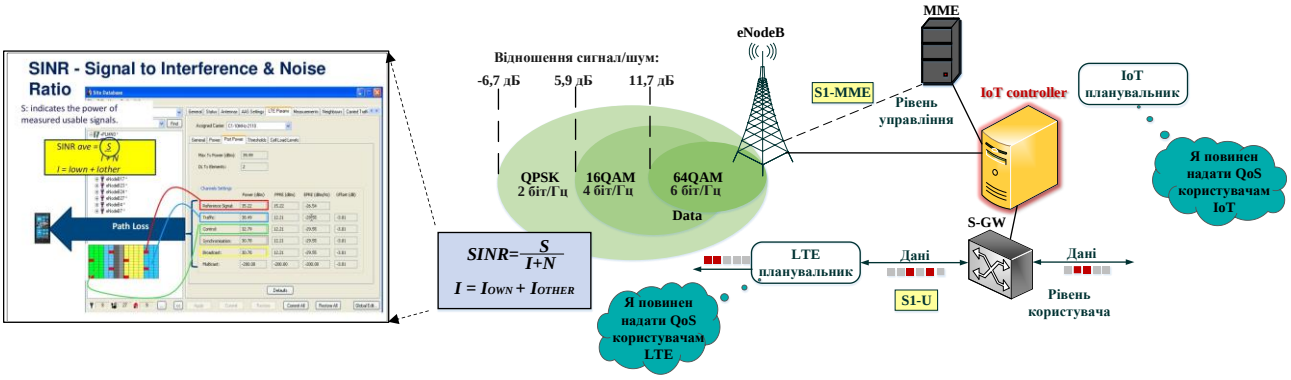


Рис. 5.4. Механізм планування пропускної здатності LTE та IoT планувальниками для виділення UE та IoT пристрою ресурсу для забезпечення E2E QoS згідно встановлених пріоритетів

Запропонована функціональна структура та взаємодія між базовою станцією, контролером IoT та пристроєм IoT показані на рис.5.5.

Ця структура складається з чотирьох рівнів, перелічених нижче:

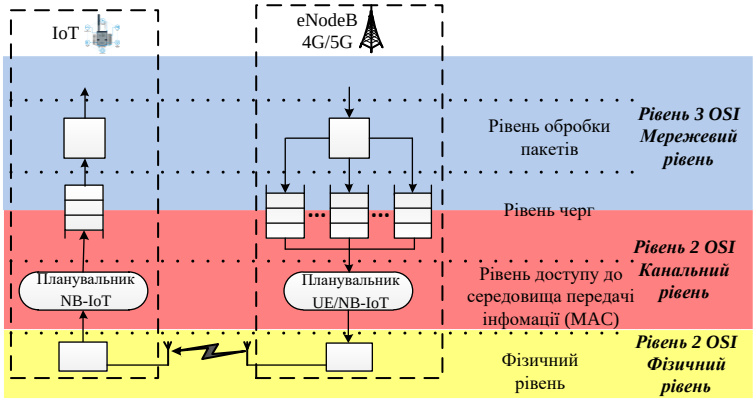
1. Рівень оброблення пакетів.

2. Рівень черги для передавання даних по безпровідному каналу зв'язку.

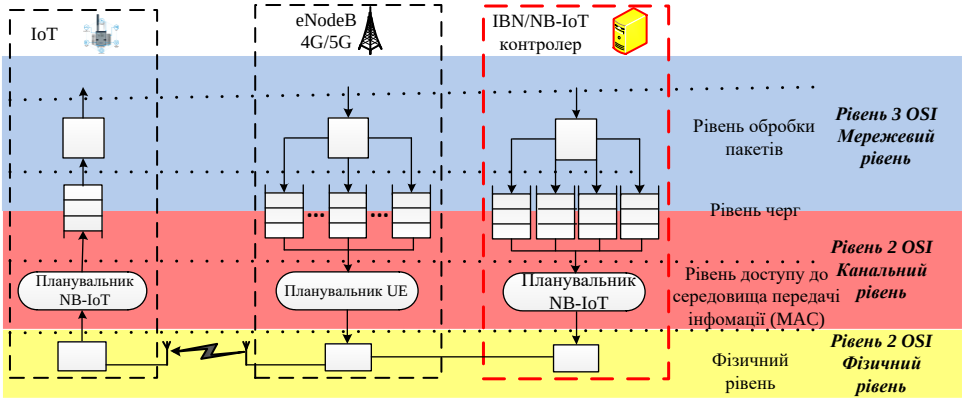
3. Рівень доступу до середовища передавання даних.

4. Фізичний рівень.

Наведемо приклад передавання даних від моменту його отримання на базовій станції eNodeB, до моменту його появи на мережевому рівні користувацького пристрою чи IoT пристрою. З транспортної EPC мережі оператора пакет потрапляє на рівень оброблення пакетів, даний рівень проводить стиснення заголовків пакетів транспортного і мережевого рівня, для зменшення обсягу переданих даних по безпровідному каналу та визначає сигнальні дані пакету IoT пристрою в його черзі нижчого рівня.



а)



б)

Рис. 5.5 Класична вузькосмугова архітектура NB-IoT розгорнута в межах базової станції 4G/5G, що взаємодіє з пристроєм IoT – а), запропонована архітектура NB-IoT, що взаємодіє між базовою станцією 4G/5G, контролером IoT та IoT пристроєм – б) [206]

Нижче знаходиться рівень черг для передавання даних по безпровідному каналу зв'язку. На даному рівні для кожного IoT пристрою, підключеного до базової станції, розташована черга (буфер) для даних. Рівень черг є проміжним між рівнями оброблення пакетів і канального рівня, що виконує роль тимчасового сховища даних в процесі передавання даних по безпровідному каналу. Обслуговуванням черг займається нижчий рівень: рівень доступу до середовища передавання (Medium Access Control або MAC) [207].

Рівень доступу до середовища передавання даних виконує основну функцію для системи в цілому, зокрема на основі інформації від рівня

фізичного середовища і вищого рівня базової станції проводить розподіл ресурсів безпровідного каналу і забезпечує надійність передавання даних. Даним процесом розподілу займається планувальник ресурсів безпровідного каналу, встановлений на базовій станції eNodeB в традиційній реалізації NB-IoT (в англомовній літературі використовується позначення Media Access Channel Scheduler або MAC Scheduler) [208]. У нашому випадку NB-IoT планувальник знаходиться на окремому контролері IBN/NB-IoT. Планувальник в кожному субкадрі здійснює розподіл ресурсів радіоканалу (ресурсних блоків) у відповідність з деяким алгоритмом (зокрема у роботі пропонуються унікальні алгоритми управління розумною чергою). Важливо відзначити, що планувальник не виділяє ресурси абонентам, у яких немає даних в даному субкадрі. У кожному кадрі формується карта розподілу ресурсних блоків, яка буде передана на фізичний рівень. Таким чином, роботу алгоритму планування можна представити у вигляді розподілу часток каналу 200 кГц між пристроями IoT різного пріоритету.

Сформована карта розподілу ресурсних блоків буде передана на рівень фізичного середовища, який забезпечить передавання даних з рівня черг у виділені частотно-часові ресурси. Надалі, при коректній роботі всіх описаних рівнів базової станції пакет буде доставлений по безпровідному каналі на призначений для користувача чи IoT пристрій та пройшовши стек в зворотному порядку, стане доступний на мережевому рівні користувацького пристрою.

Найбільш ефективним результатом щодо забезпечення необхідного рівня якості обслуговування в технології LTE може бути досягнуто шляхом розв’язання задачі розподілу частотних і часових ресурсів у низхідному та висхідному каналі зв’язку. Найменшим елементом у частотно-часовій області кадру IoT є ресурсний блок, який складається з 12 згрупованих частотних піднесучих. Ресурсний блок займає 180 кГц у частотній і 0,5 мс у часовій області. Конфігурацію RB у частотно-часовій області ілюструє рис.5.4-5.5 Кількість піднесучих OFDM або SC-FDMA символів в одному ресурсному

блоці залежить від відстані між піднесучими, а також від значення циклічного префікса (Cyclic Prefix, CP). Необхідний спектр для IoT становить 180 кГц. В залежності від рівня QoS виділяється необхідна кількість ресурсних блоків.

Таким чином, запропоновано розподіляти ресурси в низхідному і висхідному каналах IoT, використовуючи запропоновані алгоритми управління "розумною чергою", зокрема для каналу вниз показано на рис.5.6. Детальний принцип роботи алгоритмів управління чергою розглядатимуться у підрозділі 5.1.4. Для цього у роботі здійснено модифікацію логічних каналів управління з метою гнучкого управління QoS на канальному рівні. Зокрема, додатково введено нові канали, які передають сигнальну інформацію про блок ресурсів для конкретного сенсора IoT з його пріоритетом і унікальним ідентифікатором пристрою. На відміну від відомих рішень, ці канали дають змогу виділити один ресурсний блок для передавання невеликого повідомлення від датчика IoT і забезпечити мінімальну затримку 0,5 мс в кадрі. Ці затримки особливо важливі для тактичних даних IoT в реальному часі, які забезпечити в традиційній NB-IoT є неможливо.

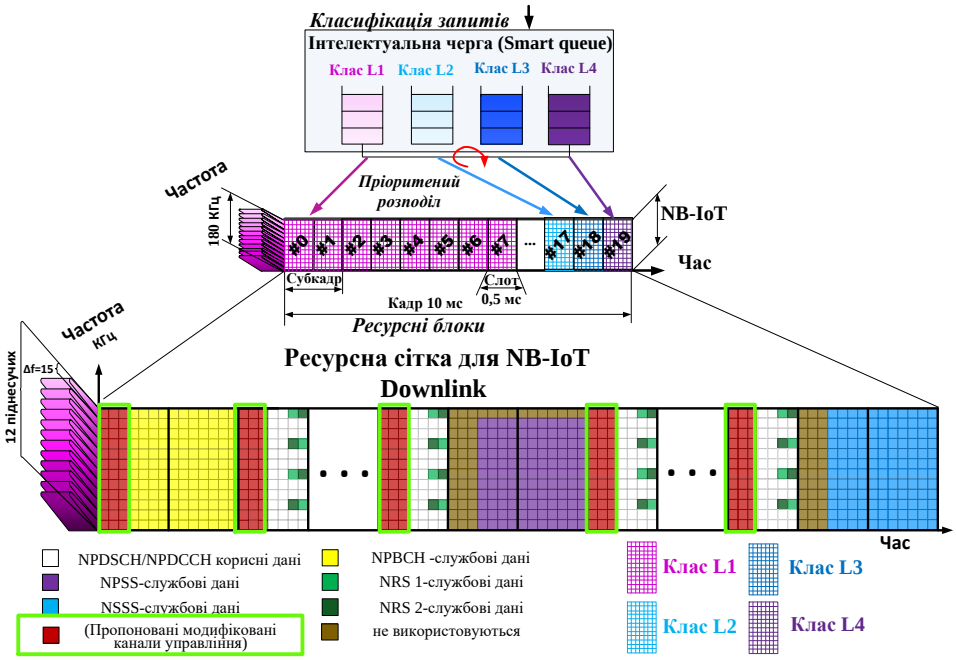


Рис.5.6. Ресурсна сітка NB-IoT для низхідного каналу зв’язку [206]

При передачі по низхідній лінії зв'язку на фізичному рівні NB-IoT використовуються наступні сигналізаційні канали:

– Вузькосмугова фізична передача даних спільного каналу (NPDSCH);

– Управління вузькосмуговим фізичним каналом управління низхідної лінії зв'язку (NPDCCH);

– Система передачі інформації вузькосмугового каналу фізичного мовлення (NPBCH).

Кожен кадр починається з передачі каналу NPBCH, який може приймати нульовий підкадр. Кожен 5-й субкадр передається сигналом NPSS, тоді як останній субкадр кожного парного кадру передається сигналом вузькосмугового вторинного сигналу синхронізації (NSSS). Канали NPDSCH або NPDCCH розміщуються у решті вільних підкадрів.

Базова станція в мережах NB-IoT може працювати з однією або двома антенами (антенні порти R2000 та R2001). Ці порти передають опорні сигнали, специфічні для NB-IoT. Якщо ресурс каналу для NB-IoT виділяється в смузі пропускання активної мережі LTE, тоді опорні сигнали широкосмугової мережі NRS1 і NRS2 також передаються в ресурсному блоці (RB). При розміщенні символів каналу NPDSCH на лівій стороні зарезервовано 1–3 символи OFDM для передачі каналу управління PDCCH широкосмугової мережі LTE (2 символи OFDM на рис.5.6).

У роботі проведено модифікацію для контрольних каналів, які складаються з LTE PDCCH, каналів опорних сигналів, специфічних для комірок LTE, та інтелектуальних каналів управління узгодженості черг на контролері IoT, що взаємодіють із кінцевим пристроєм IoT. Канал управління також передає інформацію контролеру про використання ресурсів. Ці канали управління пропонуються для гнучкості управління QoS на рівні зв'язку, який передає сигналізаційну інформацію про блок ресурсів для конкретного повідомлення датчика IoT з його пріоритетом та унікальним ідентифікатором пристрою. На відміну від відомих рішень, ці канали дозволяють виділити один

блок ресурсів для передачі невеликого повідомлення від датчика IoT і забезпечити його передавання з мінімальною затримкою 0,5 мс у кадрі. Сигнальні канали показані червоним кольором у зеленій рамці на рис.5.6.

Далі розглядається вузькосмуговий фізичний спільний канал висхідної лінії зв'язку та вузькосмуговий фізичний канал управління висхідною лінією, показаний на рис.5.7:

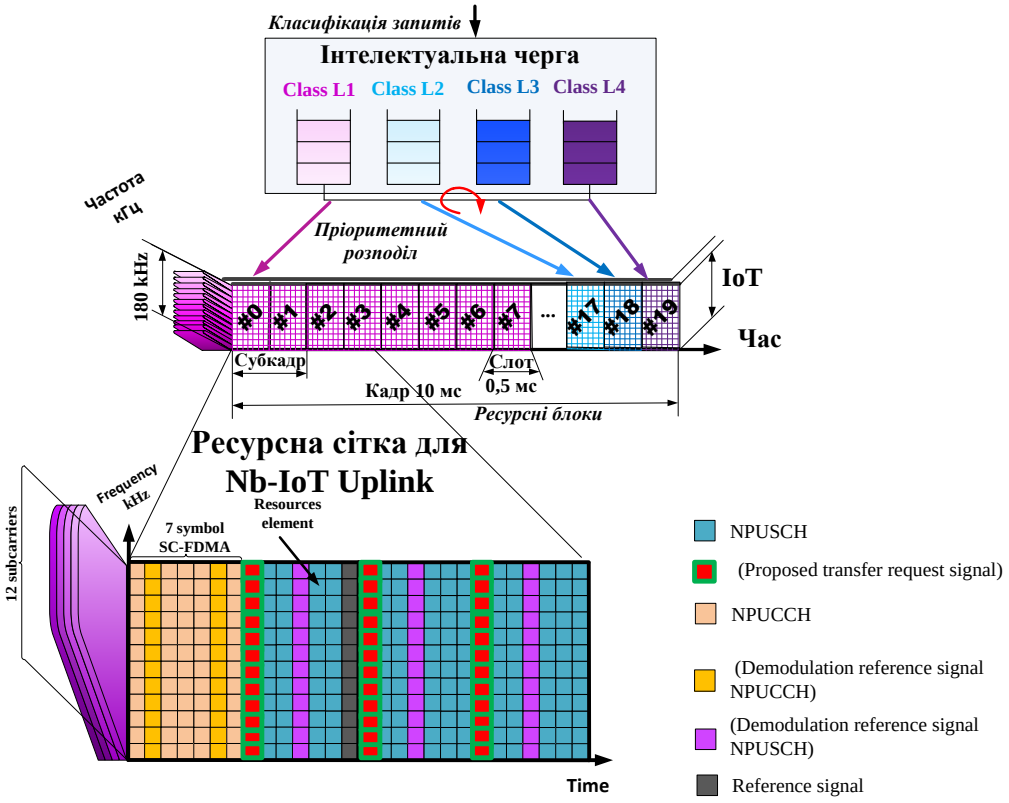


Рис.5.7. Ресурсна сітка NB-IoT для низхідного каналу зв’язку [206]

– Вузькосмуговий фізичний спільний канал висхідної лінії зв'язку (NPUSCH) - це фізичний канал, який використовується для передачі даних висхідної лінії зв'язку пристроєм IoT. Він також може нести інформацію управління висхідною лінією. Цей канал є аналогом каналу PDSCH у висхідній лінії зв'язку.

– Вузькосмуговий фізичний канал висхідної лінії зв'язку (NPUCCH) - це фізичний канал керування висхідною лінією зв'язку (PUCCH), який забезпечує

різноманітну сигналізацію управління. Ця сигналізація відома як запит планування, підтвердження даних низхідній лінії зв'язку (ACK)/негативне підтвердження (NACK) та інформація про індикатор якості каналу (CQI). Зокрема у роботі введено новий сигнал запиту на передачу для зв'язку з контролером IoT, що показано червоним кольором на рис.5.7.

UE NB-IoT (обладнання користувача) можуть передавати реагуючий зворотний зв'язок HARQ через вузькосмуговий фізичний спільний канал висхідної лінії зв'язку (NPUSCH) або вузькосмуговий фізичний канал управління висхідною лінією зв'язку (NPUCCH). Надано варіанти визначення фізичних структур NPUCCH та NPUSCH та мультиплексування користувачів по висхідній лінії зв'язку (UL).

5.1.3. Метод балансування навантаження в інтенційно-орієнтованій мережі LTE/NB-IoT

Одним із способів, пропонованих у роботі є забезпечення необхідної якості обслуговування на основі використання засобів моніторингу мережі. Використання централізованого моніторингу дає змогу визначити пріоритетні напрямки розвитку цілої мережі. Визначивши стан мережі рівня радіодоступу можна знайти і передбачити вузькі місця при обслуговуванні користувачів та IoT пристроїв. Моніторинг дасть змогу не тільки знайти фактори, які знижують продуктивність мережі, але і стане поштовхом до пошуку алгоритмів і методів їх вирішення.

У роботі запропоновано метод балансування навантаження з врахуванням пріоритетів даних на основі зібраної статистики системи моніторингу ресурсів LTE/NB-IoT [209]. Суть даного методу полягає у забезпеченні якості обслуговування пріоритетного трафіку IoT в умовах недостатності необхідних частотно-часових ресурсів в межах основної комірки обслуговування. У такому випадку, пропонується з допомогою системи моніторингу ресурсів, за яку відповідає нововведений IoT контролер в архітектуру LTE, перенаправляти

трафік IoT реального часу класу L1 на обслуговування альтернативної (додаткової) базової станції eNodeB (рис.5.8).

Пристрій	Переносник	Примітка
-//-		**Хендовер**
-//-		**Можливі підключення**
		LTE
		IoT
max min		**Рівень завантаженості ресурсної сітки**
		Макрокомірка: Всередині приміщення - немає; Поза приміщенням: > 10 Вт; Радіус дії: кілометри
		Пікокомірка: Всередині приміщення: 100-250 мВТ; Поза приміщенням: 1-5 мВТ; Радіус дії: десятки метрів
		Фемтокомірка: Всередині приміщення: 10-100 мВТ; Поза приміщенням: 0,2-1 мВТ; Радіус дії: десятки метрів

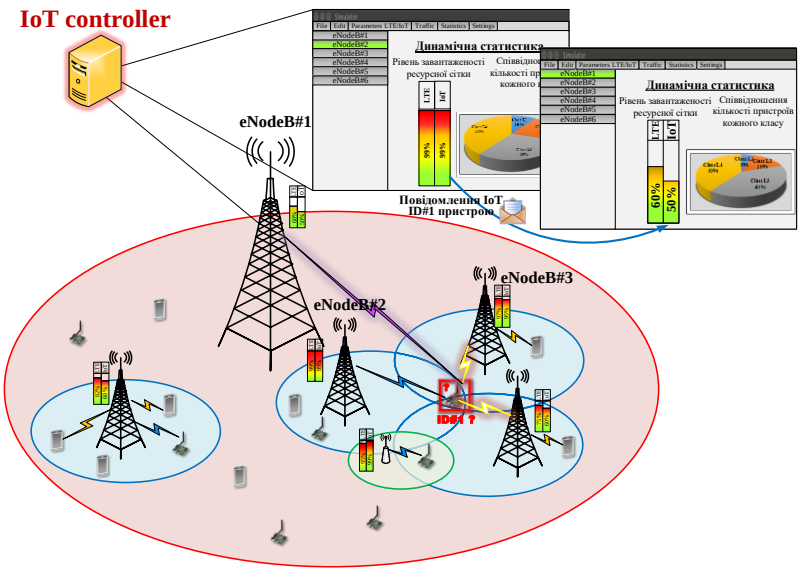


Рис.5.8. Принцип роботи методу балансування навантаження з врахуванням пріоритетів даних на основі зібраної статистики системи моніторингу ресурсів LTE/IoT

Процедура взаємодії елементів мережі LTE/IoT при передаванні повідомлення класу L1 показано на рис.5.9.

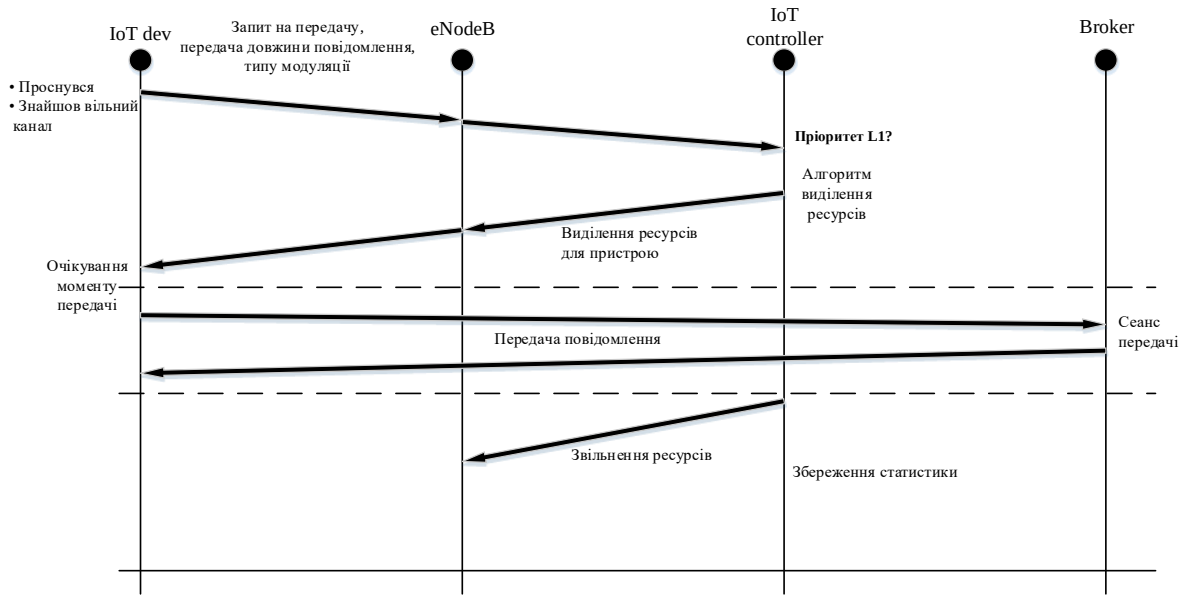


Рис.5.9. Процедура взаємодії елементів мережі LTE/IoT при передаванні повідомлення класу L1 [206]

IoT пристрій «проснувся», зчитав інформацію з сенсорів, створив повідомлення і відправив запит на передачу, в якому міститься розмір повідомлення і тип модуляції, який визначений на основі рівня сигналу. IoT контролер аналізує запит і виділяє на базовій станції ресурси для передачі. IoT пристрій отримує відповідь, очікує свого моменту передачі і передає повідомлення. Після передачі повідомлення IoT контролер звільняє ресурси на базовій станції і зберігає статистику.

Таким чином, у роботі набув подальшого розвитку метод балансування навантаження в мережі LTE/NB-IoT, який, на відміну від відомих, в умовах недостатності необхідних ресурсів для обслуговування критично-важливих IoT даних в межах основної базової станції, дав змогу на основі розробленої централізованої системи моніторингу частотно-часових ресурсів та аналізу пріоритету забезпечити ультранадійний зв'язок з низькими затримками шляхом перенаправлення на обслуговування менш завантаженої альтернативної базової станції.

5.1.4. Розроблення алгоритмів управління “розумною чергою” на основі методів пріоритезації та балансування IoT трафіку в інтенційно-орієнтованих мережах 4G/5G

Запропонована 4G/5G мережа повинна забезпечити необхідну якість обслуговування для різних сервісів. Основним методом гарантування якості обслуговування є використання каналів зв’язку з високою пропускною здатністю. Проте, це водночас є і найдорожчим методом. Суть інших методів полягає у пріоритетному наданні ресурсів мережі трафіку “чутливих протоколів” за рахунок протоколів, яким не потрібна висока якість обслуговування. В мережах 4G/5G слід використовувати “розумну чергу”, у якій пріоритет залежить від типу сервісу. Різні типи сервісів вимагають різної пріоритезації [210]. Тобто з розвитком сервісів IoT одне з основних завдань в

концепції IBN є адаптування якості сервісу (QoS) згідно з вимогами конкретного виду сервісу конкретного користувача.

При реалізації послуг з використанням мобільної мережі необхідно враховувати не тільки пріоритет, увагу слід акцентувати і на затримці, швидкості передачі запиту на виконання, а також гарантії виконання. Що стосується останнього, то при реалізації обміну даних між пристроями важливим є погодження параметрів якості обслуговування, яке повинно здійснюватися на двох кінцях передачі з метою оптимального і своєчасного виконання запитів до відповідного пристрою. При реалізації обслуговування повинні бути сформовані певні буфери пам'яті, які служитимуть в якості черги на рівні планування радіоресурсів. У роботі запропоновано алгоритми управління "розумною чергою" на основі запропонованого методу пріоритезації IoT трафіку в гетерогенній мобільній мережі.

Тип гарантований час передавання даних (GBR_{IoT}) трафік реального часу:

Для IoT класу L1

При запуску алгоритму базова станція очікує на запит на передавання даних (блок 1). Після цього проходить аналіз пріоритету пристрою, з якого відбуватиметься передавання. Встановлюється, що пріоритет пристрою є L1 (найвищий). Проводиться аналіз черги та ресурсів мережі для здійснення передавання даних (блок 2). Якщо є наявні ресурси, то здійснюється конфігурація базової станції (блок 3) і відправляються сигналізаційні дані та запит на передавання до IoT пристрою (блок 4). Після успішної передачі відбувається збереження статистики (блок 12) для подальшого прогнозування активності IoT пристрою. В протилежному випадку перевіряється можливість звільнення ресурсів за рахунок пристроїв класу L3 (блок 7). Якщо можна звільнити ресурси, то IoT device класу L3 відтерміновується та реорганізовується черга (блок 8), та переходимо із блоку 6 у блок 3. Якщо наявних ресурсів недостатньо, відбувається пошук альтернативних базових

станцій (блок 5), в яких є вільні ресурси для передавання даних. Якщо існує така базова станція (блок 6), то резервуються ресурси в спектрі частот для IoT сервісів (блок 7) та конфігурується альтернативна базова станція (блок 8). Відправляються сигналізаційні дані та запит на передавання до IoT пристрою (блок 9). Після успішної передачі відбувається збереження статистики (блок 12). У випадку, якщо ресурсів в спектрі для IoT сервісів на альтернативній базовій станції недостатньо, здійснюється передача обслуговування з'єднання в загальний канал зв'язку (блок 10). Відправляються сигналізаційні дані та запит на передавання до IoT пристрою (блок 11) і він обслуговується як абонент мобільної мережі. Після успішної передачі відбувається збереження статистики (блок 12). Завершується робота алгоритму (блок 13). Блок-схема алгоритм роботи відображена на рис. 5.10а.

Для IoT класу L2

При запуску алгоритму базова станція eNodeB очікує на запит встановлення з'єднання (блок 1). Після оброблення всіх запитів проводиться аналіз класу пристроїв, які підключилися та трафіку, який вони будуть передавати. Всі під'єднані пристрої заносяться в чергу, відповідно до класів, яким вони належать (по пріоритетах). На основі отриманих даних перевіряється доступність ресурсів для передавання трафіку від пристроїв класу L2(блок 2). Якщо ресурсів достатньо, то застосовується алгоритм для L1 (блок 3). Якщо ресурсів не вистачає, то аналізується черга і визначається час відтермінування передавання (блок 4). Перевіряється доступність ресурсів в межах допустимої затримки для даного класу (блок 5). У випадку доступності ресурсів для передавання трафіку на протязі допустимого часу затримки вносимо IoT пристрій в чергу та переходимо до алгоритму для L1 (блок 6→3). В протилежному випадку перевіряється можливість звільнення ресурсів за рахунок пристроїв класу L3 (блок 7). Якщо можна звільнити ресурси, то IoT пристрій класу L3 відтерміновується та реорганізовується черга (блок 8) та переходимо із блоку 6 у блок 3. Якщо ресурси неможливо звільнити, то

проводиться пошук альтернативних базових станцій (блок 9). Далі виконується перевірка того, чи можна здійснити передавання трафіку в межах допустимої затримки при використанні альтернативної базової станції (блок 10). Якщо можна, то відбувається резервування ресурсів на альтернативній базовій станції та конфігурація альтернативної базової станції (блок 11-12). Після цього відбувається налаштування IoT пристроїв для роботи з альтернативною базовою станцією (блок 13). Далі відбувається збереження статистики для подальшого прогнозування (блок 14). Якщо не можна, то у власній черзі резервується доступний ресурс (блок 15). Далі конфігурується базова станція (блок 16). А також конфігурується IoT пристрій для передавання через деякий час (блок 17). Далі відбувається збереження статистики для подальшого прогнозування (блок 14). Вкінці відбувається повернення на початок алгоритму (блок 18). Блок-схема алгоритм роботи відображена на рис.5.10б.

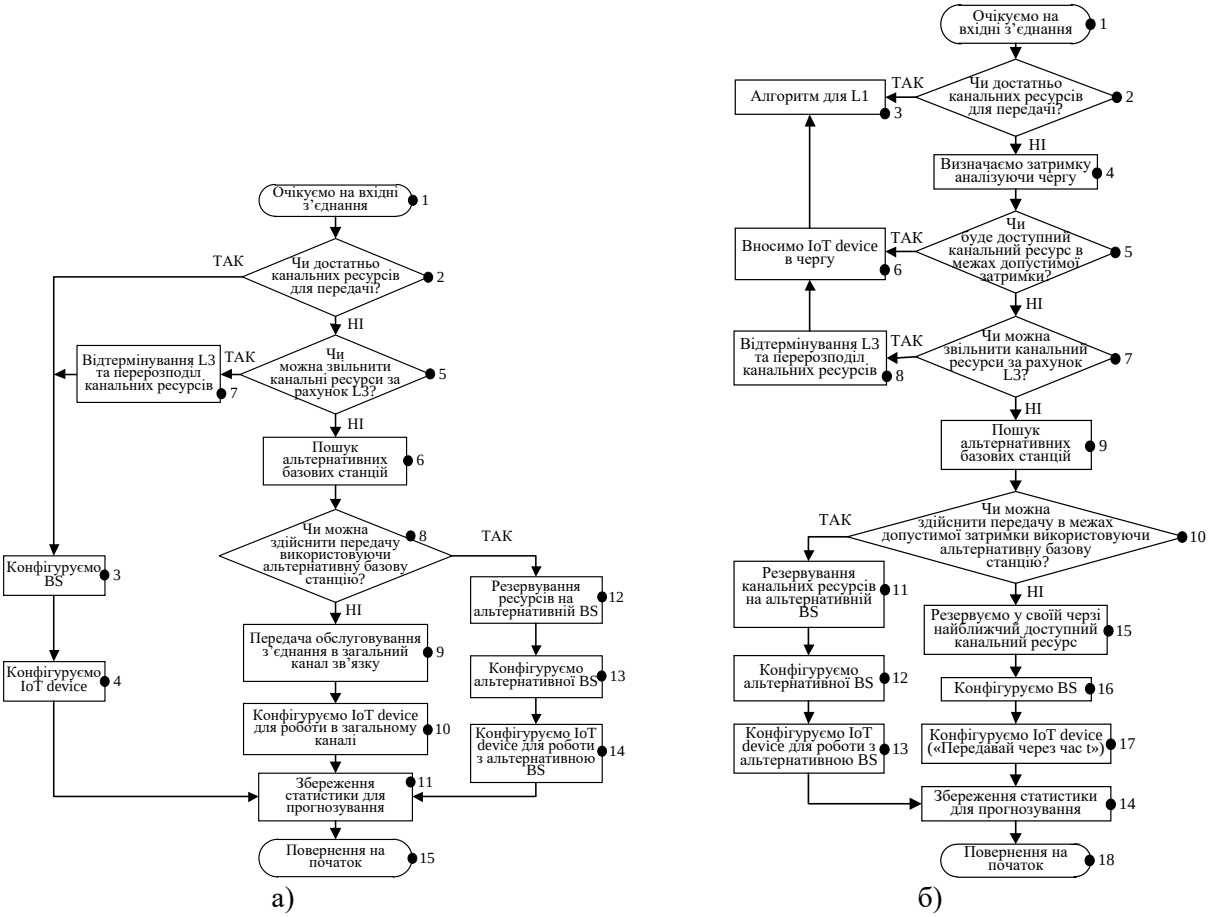


Рис.5.10. Блок-схема алгоритму управління "розумною чергою" для IoT класу L1 – а) та L2 – б)

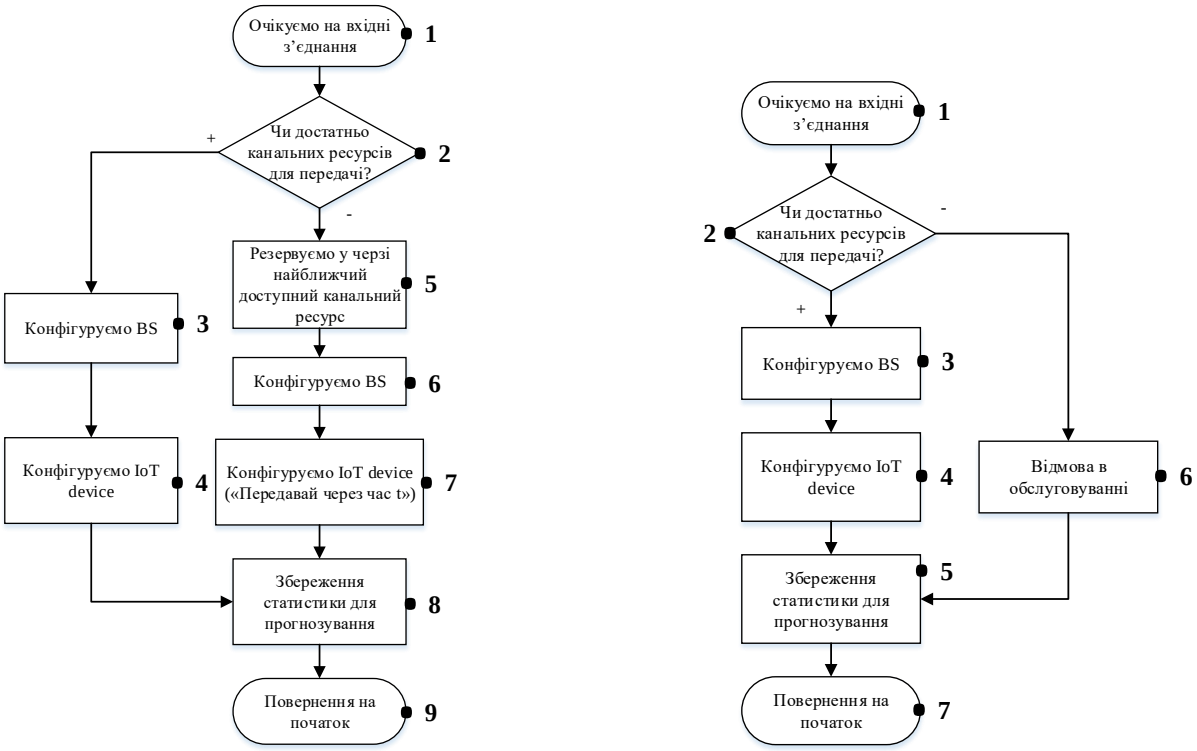
Тип негарантований час передавання даних (Non-GRB$_{IoT}$) трафік не реального часу:

Для IoT класу L3

При запуску алгоритму базова станція очікує на запит на передавання даних (блок 1). Встановлюється, що пріоритет пристрою є L3. Проводиться аналіз черги та ресурсів мережі для здійснення передавання даних (блок 2). Якщо є наявні ресурси, то здійснюється конфігурація базової станції (блок 3) і відправляються сигналізаційні дані та запит на передавання до IoT пристрою (блок 4). Після успішної передачі відбувається збереження статистики (блок 8) для подальшого прогнозування активності IoT пристрою. Якщо наявних ресурсів недостатньо, то проводиться аналіз черги та відбувається резервування ресурсів у найближчий момент часу (блок 5). Конфігурується базова станція для передавання даних (блок 6), визначається час затримки t, через який відбудеться передавання. Відправляються сигналізаційні дані, час затримки t та запит на передавання до IoT пристрою (блок 7). Після успішної передачі відбувається збереження статистики (блок 8). Робота алгоритму завершується (блок 9). Блок-схема алгоритму роботи відображена на рис.5.11а.

Для IoT класу L4

При запуску алгоритму базова станція очікує на запит на передавання даних (блок 1). Встановлюється, що пріоритет пристрою є L4. Проводиться аналіз черги та ресурсів мережі для здійснення передавання даних (блок 2). Якщо є наявні ресурси, то здійснюється конфігурація базової станції (блок 3) і відправляються сигналізаційні дані та запит на передавання до IoT пристрою (блок 4). Після успішної передачі відбувається збереження статистики (блок 5) для подальшого прогнозування активності IoT пристрою. Якщо наявних ресурсів недостатньо, то передавання даних не відбувається. Пристрій отримує відмову в обслуговуванні (блок 6). Відбувається збереження статистики про неуспішне передавання (блок 5). Робота алгоритму завершується (блок 7). Блок-схема алгоритму роботи відображена на рис. 5.11б.



а) б)

Рис.5.11. Блок-схема алгоритму управління "розумною чергою" для IoT класу L3 – а) та L4 – б) [206]

5.1.5. Моделювання та дослідження ефективності запропонованих рішень на основі розробленої імітаційної моделі мережі LTE/NB-IoT

Для дослідження ефективності запропонованих рішень розроблено імітаційну модель гетерогенної мобільної мережі LTE/NB-IoT. Дана модель реалізована у вигляді java симулятора дискретних подій, для цього використано Discrete-Event Simulation and Modelling in Java DESMO-J (DESMO-J), що включає такі функціональні класові блоки, як черги, генерація випадкових чисел та різних статистичних розподілів [211].

Спрощена структурно-функціональна схема моделі, відображена на рис. 5.12, де червоним кольором показано нововведенні блоки, реалізовані у вигляді додаткових програмних надбудов.

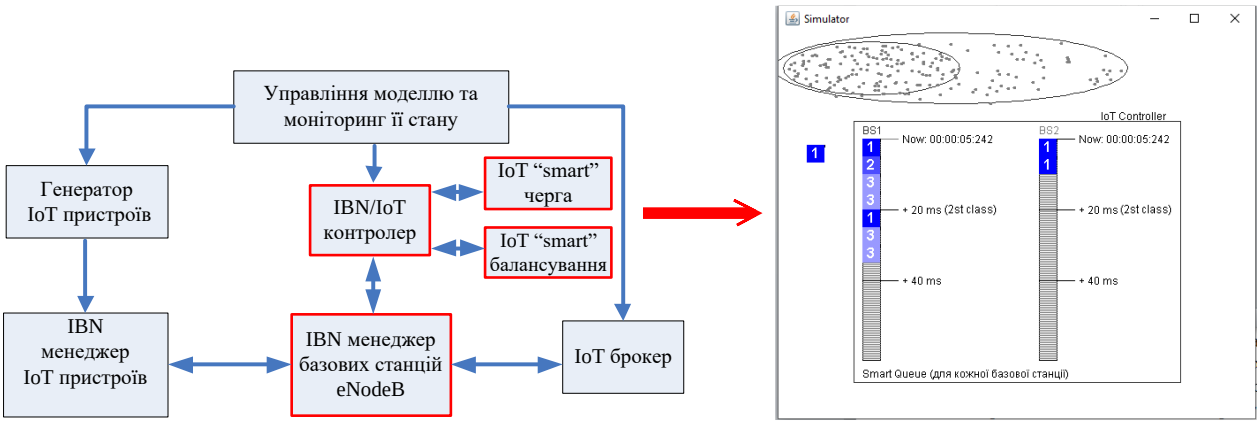


Рис. 5.12. Структурно-функціональна схема імітаційної моделі мережі LTE/IoT

Основними елементами моделі, які відповідають реальним компонентам мережі є:

IoT пристрій – являється кінцевим пристроєм мережі із встановленим пріоритетом QoS згідно запропонованого у другому розділі ELA договору, основними функціями якого є формування повідомлення, відправлення запиту на виділення каналу для передавання даних, відправлення повідомлення, приймання повідомлення відповіді, планування наступної процедури передавання даних.

IBN/IoT контролер – забезпечує моніторинг стану канальних ресурсів базових станцій для передавання повідомлень, виділення необхідних канальних ресурсів для конкретних IoT пристроїв, перерозподіл канальних ресурсів між кінцевими пристроями. Забезпечує збір, опрацювання та аналіз статистичних. даних підключень .

Базова станція eNodeB – здійснює перевірку цілісності повідомлення, забезпечує взаємодію між IoT пристроями, IoT контролером та IoT брокером. Містить в собі масив канальних ресурсів, які IoT-контролер виділяє для передавання даних за різними пристроями.

IoT брокер – здійснює зберігання даних, які надсилають IoT пристрої, аналізує їх та виконує певні, раніше визначені операції (відправлення, обробка, збереження та ін.).

IoT пристрій генерує інформаційне повідомлення і відправляє запит на отримання канального ресурсу для обслуговування базовою станцією eNodeB. В запиті також міститься розмір інформаційного повідомлення і вид модуляції. Базова станція перевіряє цілісність запиту і перенаправляє його на IoT контролер. IoT контролер аналізує запит і стан масиву канальних ресурсів поточної базової станції.

Якщо канальні ресурси забезпечують обслуговування в межах допустимої затримки, то вони закріплюються за IoT пристроєм. IoT контролер відправляє відповідь з номером канальних ресурсів на поточну базову станцію. Базова станція перенаправляє відповідь на IoT пристрій, який аналізує відповідь і очікує на свій канальний ресурс, в якому і буде передавати інформаційне повідомлення через базову станцію на IoT брокер. Останній зберігає інформацію, передану в повідомленні. Якщо немає вільних канальних ресурсів, то запит обслуговується згідно вище описаних алгоритмів.

Дослідження запропонованих рішень з використанням імітаційного моделювання

Основні вхідні дані для моделі:

– кількість IoT пристроїв - 2000;

– кількість ресурсних блоків у вузькосмуговому спектрі 200 кГц;

– види модуляції: BPSK, QPSK, 16QAM, 64QAM;

– середня довжина повідомлення від IoT пристроїв в залежності від обраної модуляції: 10 ресурсних блоків;

– середнє навантаження, ρ_i, де i=1,2,3,4,5 що враховується для контролера IoT, зокрема ρ_1 =0.12, ρ_2 =0.18, ρ_3 =0.5, ρ_4 =0.75, ρ_5 =1;

– співвідношення розподілу IoT пристроїв по класах: R_L1=10%, R_L2=20%, R_L3 = 30% та R_L4 = 40%;

– допустимі затримки для кожного класу пристроїв: D_L1 = 10мс, D_L2=20 мс, D_L3=$T_{з.допустима}$, D_L4=$T_{з.допустима.}$;

– типи тривалості затримок: поширення сигналу по безпровідному каналі, часу оброблення сигналу на базовій станції, поширення сигналу по провідному середовищі, час оброблення IoT контролером, IoT пристроєм та час очікування передавання даних.

Тривалість передавання даних IoT пристроїв із кінця в кінець визначається за формулою 5.1.

$$T_{з.E2E} = 3 \cdot t_{пош.сигн.безпров.} + 3 \cdot t_{обр.BS.} + 3 \cdot t_{пош.сигн.пров.} + t_{обр.IoTконтр.} + t_{обр.IoTпристр.} + t_{очікув.передаваня} \quad (5.1)$$

де $t_{пош.сигн.безпров.}$ затримка поширення сигналу по безпровідному каналі; $t_{обр.BS.}$ затримка оброблення сигналу на базовій станції; $t_{пош.сигн.пров.}$ затримка поширення сигналу по провідному середовищі; $Tt_{обр.IoTконтр.}$ затримка оброблення IoT контролером; $t_{обр.IoTпристр.}$ затримка оброблення IoT пристроєм та затримка очікування передавання даних $t_{очікув.передаваня}$.

Етапи моделювання:

Моделювання проводиться у три етапи:

Перший етап (I) полягає у дослідженні E2E QoS при обслуговуванні потоку вхідних запитів за принципами існуючого методу *(Proportional Fair Scheduling)*. *Другий етап* (II) полягає у дослідженні E2E QoS при обслуговуванні потоку вхідних запитів згідно запропонованого методу пріоритезації трафіку IoT *(P.IoT)*.

Третій етап (III) полягає у дослідженні E2E QoS при обслуговуванні потоку вхідних запитів при одночасній реалізації методів пріоритезації трафіку *(P.IoT)* та балансуванні навантаження *(LB.IoT)*.

Протягом однієї секунди моделювання передається 100 кадрів тривалістю 10 мс, 1 кадр містить 20 ресурсних блоків (слотів) тривалістю 0,5 мс, відповідно за одну секунду передається 2000 ресурсних блоків однією EnodeB.

Одночасна робота методу пріоритезації IoT трафіку і методу балансування навантаження забезпечує зменшення середньої затримки E2E для пристроїв, які

передають дані в режимі реального часу (L1, L2), за рахунок збільшення середньої затримки передавання для пристроїв, які не чутливі до затримки (L3, L4) (рис. 5.13а). Відсоток відмов у обслуговуванні для пріоритетних пристроїв при застосуванні запропонованих методів на рис.5.13б.

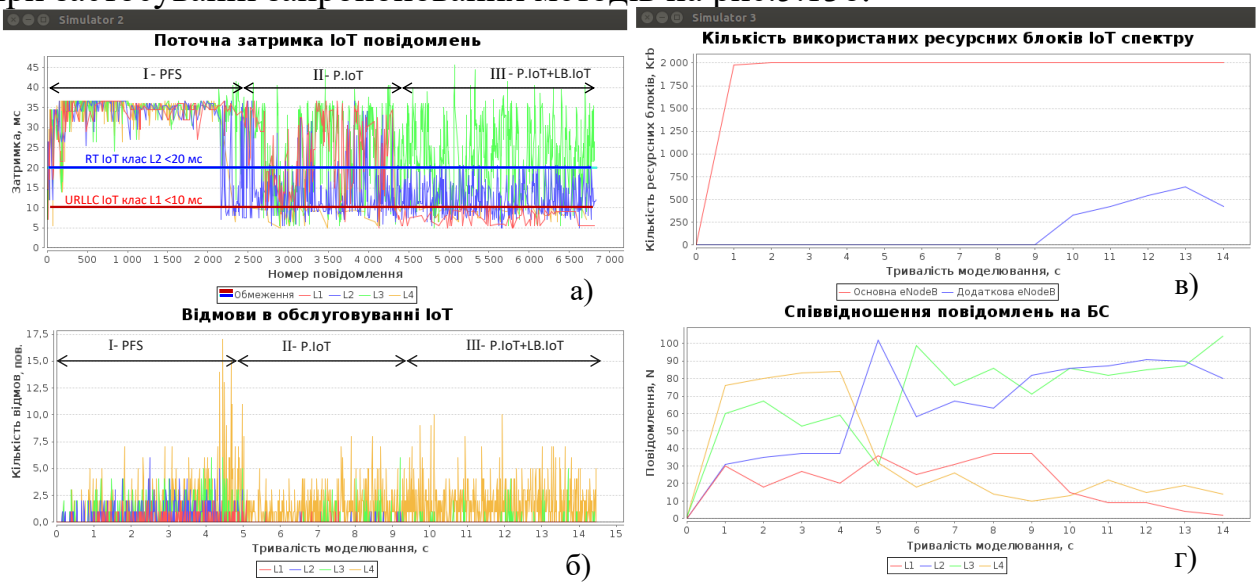


Рис.5.13. Поточна затримка в процесі передавання IoT повідомлень – а), кількість відмов – б), кількість використаних ресурсних блоків IoT спектру – в) та співвідношення кількості переданих повідомлень різних пріоритетів – г)

На даному етапі моделювання одночасно працює метод пріоритезації IoT трафіку і метод балансування навантаження. За рахунок цього, при перевантаженні поточної базової станції, частина пріоритетних пристроїв передається на обслуговування іншій базовій станції, як показано на рис. 5.13в.

На основі імітаційного моделювання встановлено, що методи пріоритезації IoT трафіку та балансування навантаження, дають змогу зменшити середню затримку передавання повідомлень реального часу з кінця в кінець на 68,8% в гетерогенній мережі LTE/NB-IoT (рис.5.14б). При використанні механізму пріоритезації, зменшити кількість відмов у обслуговуванні на 58% для класу L1 та 76% для L2 у порівнянні з існуючими методами в умовах високого навантаження (рис.5.14в).

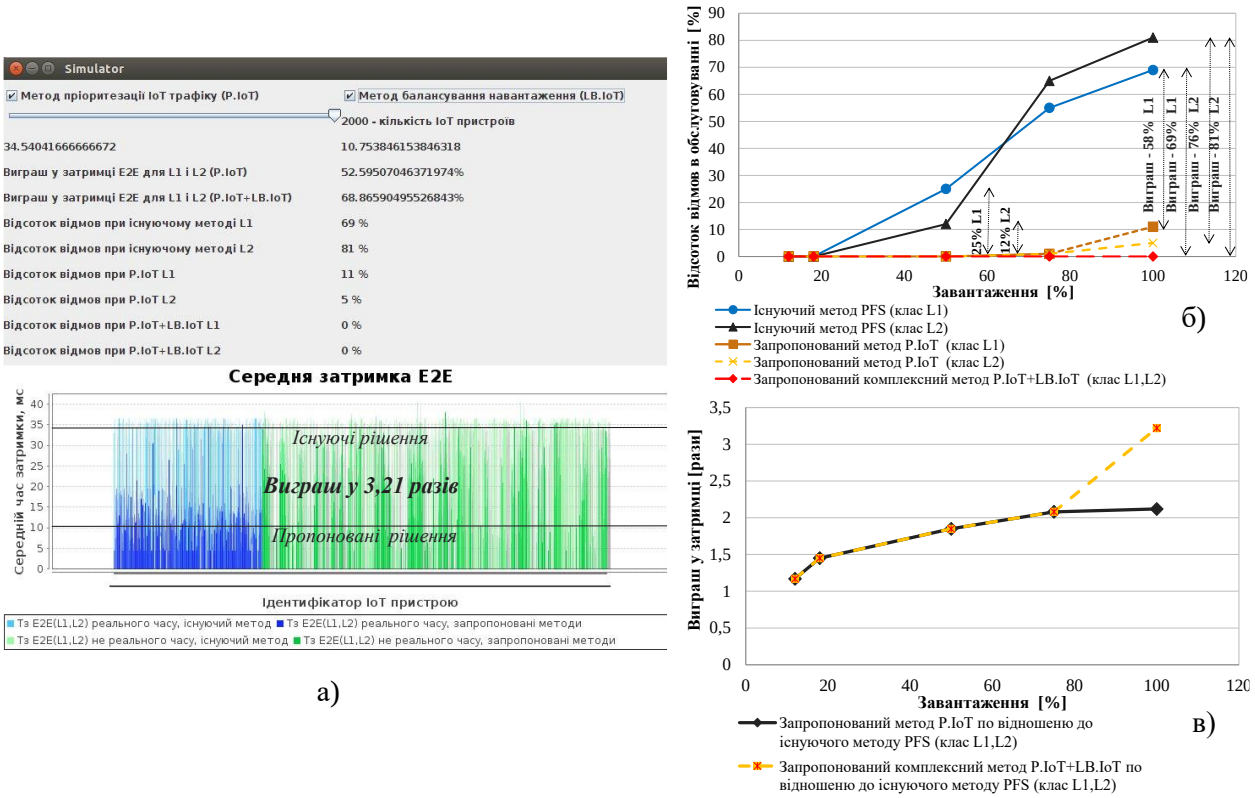


Рис.5.14. Графічний інтерфейс імітаційної моделі результатів порівняння ефективності пропонованих рішень – а), оцінка ефективності запропонованих методів у порівняні із відомим PFS методом за критерієм “відмов в обслуговуванні” для пріоритетних IoT пристроїв (класів L1, L2) – б) та “затримки обслуговування” – в) в умовах різного завантаження IoT контролера

У випадку одночасного використання запропонованих рішень досягається мінімальна кількість відмов для сервісів IoT класу L1 та L2 в умовах недовантаженості альтернативних базових станцій [206].

5.2. Розроблення адаптивного інтенційно-орієнтованого методу розподілу ресурсів та формування структури рівня радіодоступу 4G/5G

Для синтезу рівня радіодоступу сучасних мереж нового покоління розроблено адаптивний інтенційно-орієнтований метод розподілу ресурсів та формування структури рівня радіодоступу 4G/5G, який відрізняється від відомих урахуванням локалізації групи інтенційно-орієнтованого

користувацького навантаження та аналізом замовлених QoE оцінок щодо забезпечення необхідного рівня якості сприйняття сервісу, що дало змогу ефективніше використовувати наявні енергетичні та частотно-часові ресурси із забезпеченням замовленої якості обслуговування. Далі у роботі розглядається більш детальний опис розробленого методу.

Планування багаторівневих мереж мобільного зв'язку є більш складним у порівнянні із однорівневими мережами [20]. Необхідно окремо враховувати щільність базових станцій кожного рівня і потім визначати суперпозицію усіх рівнів при розрахунку параметрів для кінцевих користувачів. При плануванні класичним (стаціонарним) методом така гетерогенна мережа не буде ефективною за рахунок неоднорідності навантаження на різних територіях. Тому потрібно використати такий спосіб планування мережі, який враховував би доцільність і оптимальність розміщення базових станцій в залежності від локалізації навантаження, забезпечуючи при цьому високу енергоефективність мережі шляхом переведення в неактивний режим базових станцій, які не використовуються для обслуговування користувачів. У випадку гетерогенних мереж найкращим методом є інтеграція множини малих комірок в існуючу структуру мережі радіодоступу. Такий метод забезпечить високу якість надання послуг у місцях щільного скупчення користувацького навантаження та дозволить розвантажити існуючу мережу.

5.2.1. Побудова багаторівневої інтенційно-орієнтованої мережі 4G/5G для загального користування

У роботі запропонована архітектура гетерогенної IBN мережі, що складається із 4 рівнів показано на рис. 5.15.

Рівень контролера – реалізує функції керування мережею і реалізований у вигляді програмно-керованого ядра SDN/IBN, що використовує хмарне середовище для зберігання і обробки даних про мережу. Даний рівень володіє програмними і апаратними засобами, що забезпечують локалізацію абонента,

визначення його швидкості і напрямку руху, розрахунок значень порогової потужності і коефіцієнта SINR та інші необхідні обчислення. До його функцій відносять: адаптивну зміну структури і частотного планування рівня радіодоступу в залежності від вхідного навантаження; системгий аналіз стану мережі і параметрів якості обслуговування; безперервний аналіз синальзаційних даних, що отримуються від нижчих рівнів – вектор зміни відстані до БС для кожного користувача, загальну кількість активних користувачів мережі; формування і зміна карти навантаження; розподіл абонентів по структурі рівня радіодоступу; обробка і збереження даних, отриманих від нижчих рівнів; керування процесом агрегації та регулювання енергоспоживання мережі.

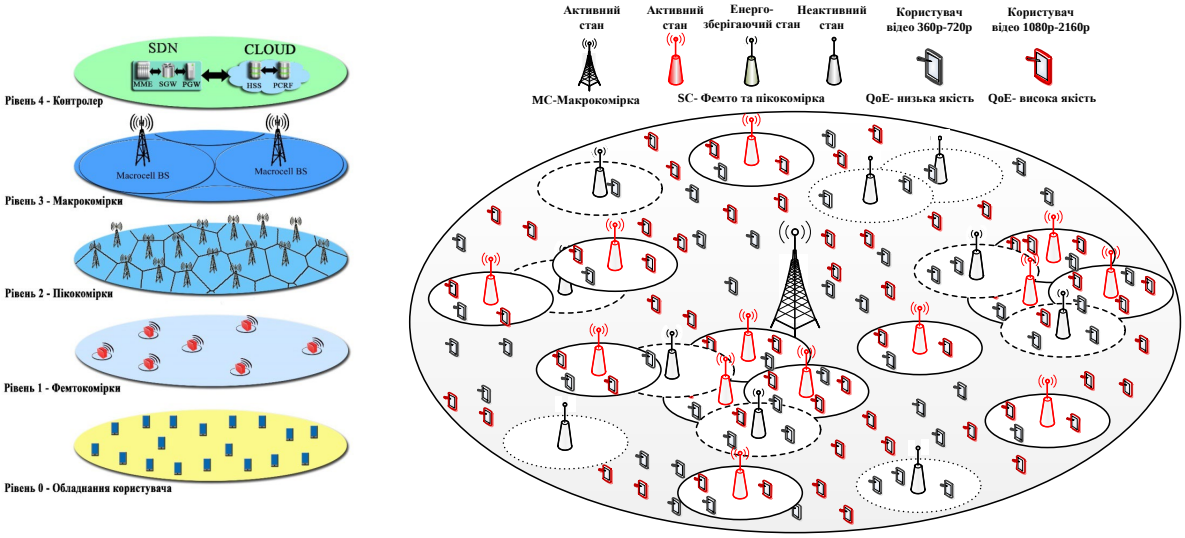


Рис.5.15. Архітектура програмо-конфігурованої гетерогенної мережі з використанням малих комірок з нерегулярною структурою [212]

Рівень макрокомірок – призначений для обслуговування рухомих абонентів, які не можуть бути на обслуговуванні в комірок нижчого рівня. Крім того, макрокомірка є шлюзом через який комірки нижчого рівня підключені до мережі. Радіус дії може досягати 1-2км.

Рівень пікокомірок – адаптивно в режимі функціонування змінюють стани залежно від навантаження і обслуговують абонентів з високими вимогами до трафіку. Радіус дії становить 100-200 м. В даному випадку володітиме двома

станами: Idle – BS прослуховує середовище, надсилає Broadcast_ID, визначає вектор зміни відстані до БС – та Active – станція працює в нормальному режимі, містить інформацію про допустимі {Fi} та поточні {Si} користувачі. Обслуговує малорухомих коритсувачів (низький вектор руху), які мвиманають високих вимог обслуговування (високий QoS_class, QoE-5). Під'єднана до базової станції вищого рівня за допомогою оптично-волоконного кабелю.

Рівень фемтокомірок – динамічно розгортаються в місцях великого скупчення користувачів і виконують аналогічні функції, що комірки 2 рівня.

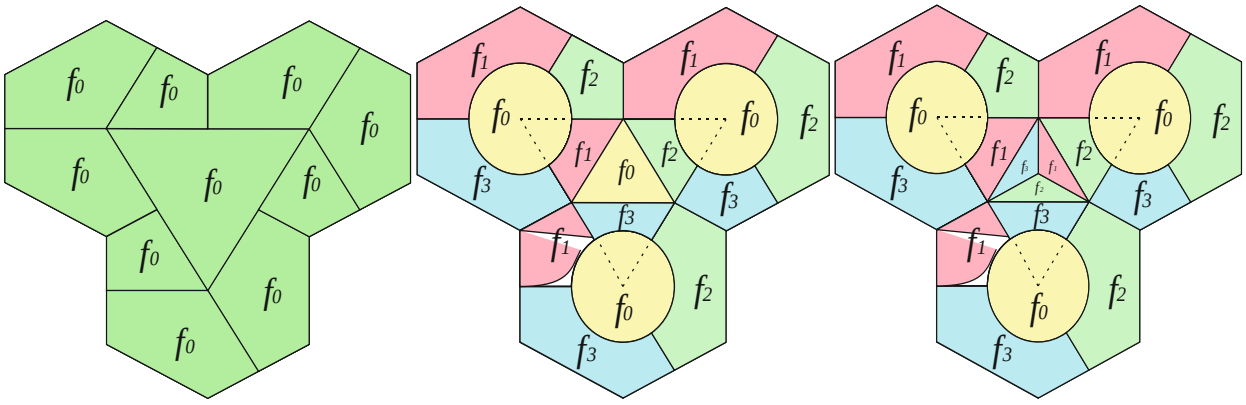
Рівень користувачів – володіє атрибутами QoS_class, надсилає CSI, $P_{пор.}$, SINR, QoE on request.

5.2.2. Метод частотного планування та диференціація трафіку згідно QoE вимог в інтенційно-орієнтованій мережі 4G/5G

Оскільки, абонентське навантаження локалізоване нерівномірно, тому розміщувати базові станції необхідно також нерівномірно. В місцях, де більша густота абонентського навантаження, має бути більша щільність розміщення базових станцій і навпаки. Вирішенням цієї проблеми може стати стохастична геометрія. Згідно запропонованої архітектури розбиття площі покриття рівня 2 між базовими станціями пропонуємо здійснювати використовуючи метод Вороного [215]. Суть методу полягає в розбитті площини так, що кожна область розбиття складається з множини точок, кожна з яких є ближча до певного об'єкта, ніж до іншого.

Згідно запропонованої архітектури мережі радіуси дії малих комірок є набагато меншими за радіус дії макро базових станцій, отже,малих комірок буде значно більше на одиницю площі. Оскільки сучасні способи частотного плануванні не розраховані на використання у гетерогенних мережах, то внаслідок збільшення малих комірок зростає кількість інтенференцій. Тому, виникає потреба у пошуках нових методів частотного планування, які б мінімізували кількість інтенференцій на всіх рівнях. Розглянемо класичний

спосіб покриття території гексагональними комірками, який успішно застосовується на сучасних мобільних мережах (рис.5.16). Якщо провести уявні лінії з центрів трьох сусідніх макрокомірок таким, то утвориться трикутник, який слугуватиме місцем розташування малих комірок. Для того, щоб мінімізувати кількість інтенференцій на краях макрокомірок, пропонуємо в середині утвореного «трикутника» утворити ще один «трикутник» таким чином, що в межах великого «трикутника» зміщення частот відбувається проти годинникової стрілки на одну позицію відносно макрокомірки, а в межах малого «трикутника» буде використовуватися та сам частота, що й у ближній зоні макрокомірок (рис. 5.16 б) або ж цей «трикутний» буде розділений та три рівні частини в кожній з яких використовуватиметься частота оберненого сектору (рис. 5.16 в).

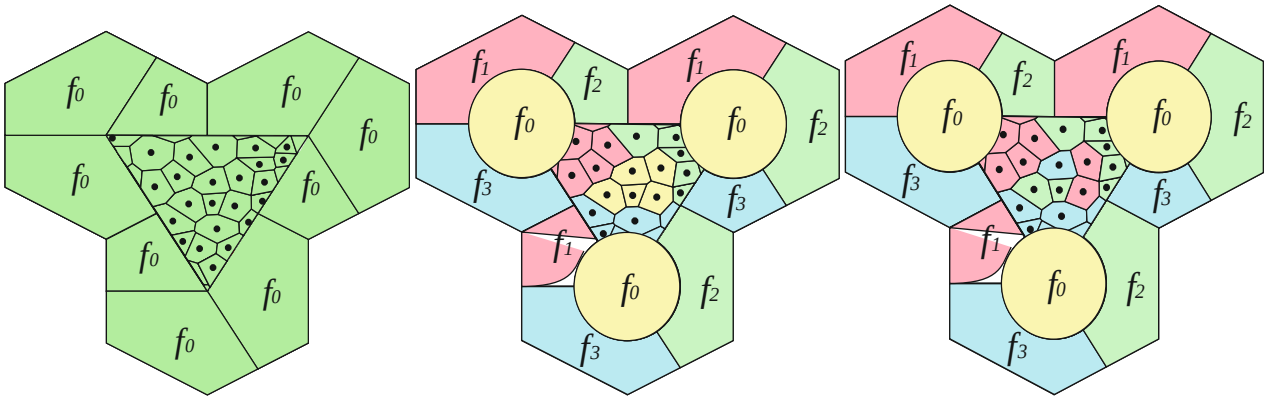


а) б) в)

Рис. 5.16. Розподіл частот для ефективного впровадження «малих комірок» в існуючу мережу. (f_i– смуга частот, в даній області) [172]

Такий розподіл забезпечить ефективніше, в порівнянні з існуючими, повторне використання частот. Утворені в результаті таких маніпуляцій «трикутники» слугуватимуть місцем для розташування малих комірок згідно способу розміщення базових станцій на основі діаграм Вороного. Такий підхід дозволяє визначити в якому місці потрібно ставити базову станцію певного

типу та на якій частоті вона функціонуватиме (рис. 5.17б). Це дасть змогу уникнути встановлення зайвих базових станцій та зменшити рівень інтерференцій.



а) б) в)

Рис. 5.17. Накладання ідеалізованого розподіленого спектру на нерегулярну структуру

Такий частотний поділ дозволить більш раціонально використовувати частотні ресурси мережі в порівнянні з існуючими методами та збільшити спектральну ефективність мережі в цілому. Спектральна ефективність в загальному випадку визначається відношенням пропускної здатності C, яку необхідно забезпечити, до добутку необхідної ширини спектру ΔF і площі покриття S:

$$S_{ef} = \frac{C}{\Delta F \cdot S} \tag{5.2}$$

Пропускна здатність каналу, яку необхідно забезпечити для кожного користувача згідно вимог QoE, визначається за теоремою Шеннона з врахуванням співвідношення між рівнями сигналу і шуму (SINR):

$$C_i = \Delta F \cdot log_2(1 + SINR_i) \tag{5.3}$$

Кожен користувач володіє інформацією про рівень прийнятого та переданого на базову станцію сигналу. Тому спектральна ефективність мережі

із нерегулярною структурою малих комірок залежатиме лише від радіусу дії базової станції певного рівня та значення SINR.

$$S_{ef_i} = \frac{\sum_i \log_2(1 + SINR_i)}{S} \tag{5.4}$$

Якщо врахувати, що смуги f_0, f_1, f_2 та f_3 (рис. 5.17 б,в) рівні між собою, то при використанні нового методу частотного планування доступна для абонента смуга частот збільшиться майже в 3 рази, а, відповідно, спектральна ефективність зростатиме пропорційно до кількості абонентів, які знаходяться в межах триграника утвореного базовими станціями регулярного покриття. В процесі оброблення потоків даних контролер проводить їх класифікацію відповідно до вимог щодо замовленої якості обслуговування згідно оцінок QoE. Основними елементами, які керуватимуть процесом пріоритезації трафіку на цьому рівні є PCRF (Policy and Charging Rules Function) та PCEF (Policy and Charging Enforcement Function) [216].

Для того, щоб забезпечити дотримання параметрів QoS сервісів у роботі інформаційні потоки класифікуються на дві групи: потоки з гарантованою мінімальною швидкістю передачі (Minimum Guaranteed Bit Rate, GBR) і потоки без гарантій по швидкості передачі даних (Non-GBR). Потоки цього типу мають задане значення мінімальної швидкості передачі, яке встановлюється під час процедур створення потоку або його зміни. При цьому, можлива передача даних з більшою швидкістю, ніж мінімально встановлена, якщо є вільні ресурси на радіо каналі. Також може бути встановлено обмеження на максимальну швидкість передачі даних (Maximum Bit Rate, MBR). Потоки такого типу використовуються, наприклад, при передачі VoIP трафіку. Non-GBR потоки. Потоки даного типу не гарантують ніякої мінімальної швидкості передачі даних. Визначення класу, до якого належить той чи інший трафік пропонуємо проводити на основі відомого параметру QCI (*QoS Class Identifier*).Параметр QCI може приймати один із дев’яти станів (таблиця 5.3), кожен з яких,

відповідно, асоціюється з певним видом сервісу (ToS), а відтак і з видом каналу передачі, швидкістю, коефіцієнтом помилок та затримкою. QCI є міткою у пакеті IPv4 "ID каналу"(рис.5.18).

Таблиця 5.3

Визначення класу QoS згідно модифікованого обслуговування

QoS клас	**QCI**	**Тип каналу**	**Приклад сервісу / Необхідна пропускна здатність**	**Тип трафіку**	**Затримка**	**Коеф. помилок**	**Обслуговування** (макро-MC, фемто-SC)
QoS клас (max)	2	З гарантованою швидкістю передачі (GBR)	Відео дзвінки (2 Мбіт/с)	Розмовний	100 мс; 200 мс; 400 мс;	10^{-3} 10^{-4} 10^{-5}	MC MC+SC
	3		Онлайн ігри (1 Мбіт/с)	Інтерактивний	2 с;	$< 10^{-9}$	
	4		Потокове відео (5-20 Мбіт/с)	Потокові дані	< 1 с;	10^{-5} 10^{-6} 10^{-7} 10^{-8}	
	7		Інтерактивні ігри (512 Кбіт/с)	Інтерактивний	2 с;	$< 10^{-9}$	
QoS клас (min)	1	З не гарантованою швидкістю передачі (NGBR)	Телефонні дзвінки (64 Кбіт/с)	Розмовний	100 мс; 200 мс; 400 мс;	10^{-3} 10^{-4} 10^{-5}	MC
	5		IMS сигналізація (30 Кбіт/с)	"Фоновий"	N/A	$< 10^{-9}$	
	6		Сервіси, що базуються на використанні TCP(e-mail, web) (128 Кбіт/с)				
	8						
	9						

Використання адаптивної пріоритезації трафіку для задоволення вимог QoE дасть змогу для абонентів, які користуються мобільними додатками різних типів одночасно, при необхідності, використати різні канали передавання, які підпорядковані базовим станціям різних рівнів, а відтак забезпечити швидкісний широкосмуговий доступ для кожного абонента, або ж використати об`єднаний канал GBR & NGBR, який дозволить якісно та з мінімальними

параметрами затримками обслужити великий об`єм даних, який генеруватимуть абоненти. Пріоритезація також дасть можливість розвантажити канали з низькою швидкістю передачі, що підпорядковані макро базовій станції, шляхом визначення пріоритету і направлення на обслуговування "об`ємних" абонентів на рівні фемто базової станції.

Запропонований підхід дасть змогу створити чіткий, впорядкований алгоритм обслуговування різнотипних сервісних запитів на відповідних рівнях. Як результат, ця впорядкованість сприятиме максимізації якості надання сервісів та збільшенню числа користувачів такої мережі, а це, в свою чергу, спричинить загальне зростання прибутків компанії.

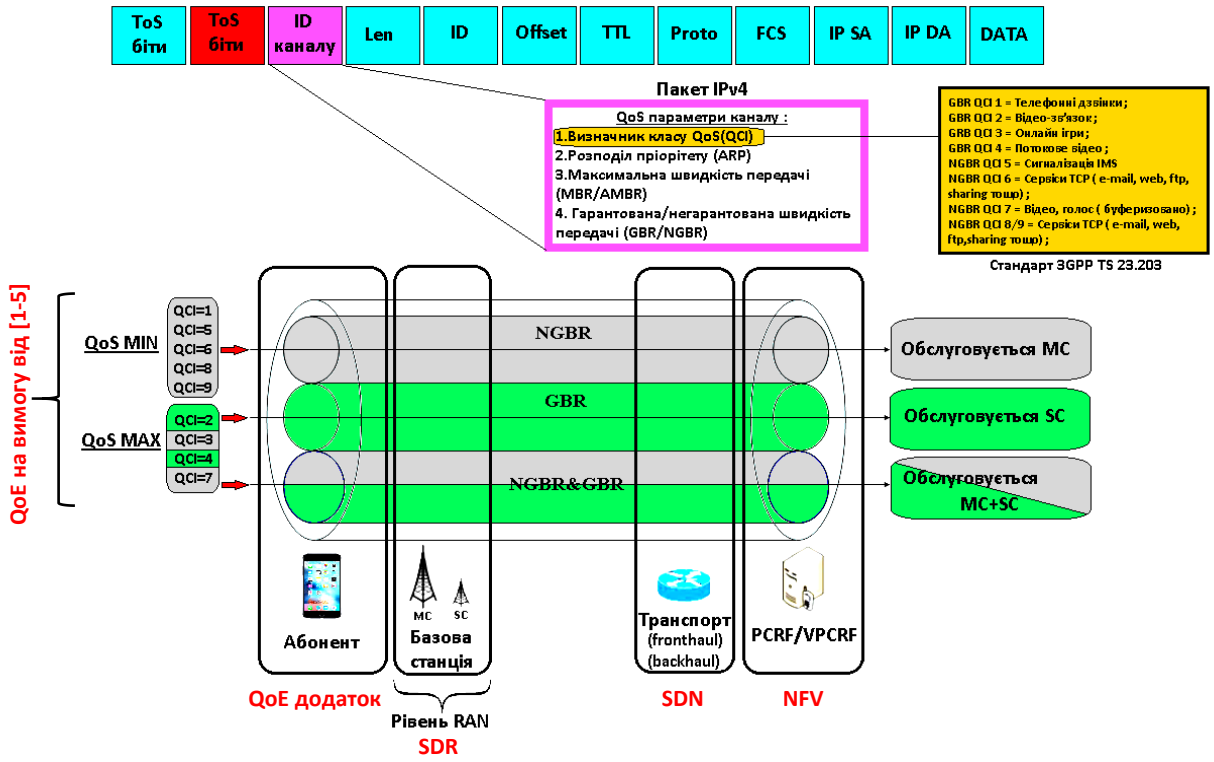


Рис.5.18. Присвоєння QCI, вибір каналу та передача [172]

Канал GBR & NGBR утворюється в результаті агрегації частот до абонента від MC та SC одночасно [217]. Рішення про агрегацію приймається на рівні контролера. Умовно кажучи, IBN/SDN контролер об’єднує дві базові станції в одну віртуальну, тим самим здійснюючи агрегацію частот до абонента. Для

прикладу, нехай абонент обслуговується макро базовою станцією, яка може забезпечити пропускну здатність 20 Мбіт/с. Однак, абоненту цієї пропускної здатності для певного індивідуального обслуговування недостатньо, тобто користувач вимагає високої QoE недостатньо. В такому випадку контролер приймає рішення про підключення даного абонента додатково до станції нижчого рівня, яка може забезпечити абоненту 50 Мбіт/с. Як результат відбувається агрегація частотного спектру згідно описаного вище методу, а абонент зможе отримати пропускну здатність 70 Мбіт/с.

5.2.3. Математична модель оптимізаційної задачі розподілу ресурсів та формування енергоефективної структури рівня радіодоступу 4G/5G

Для планування багаторівневих гетерогенних мереж мобільного зв'язку потрібно використати такий спосіб планування мережі, який враховував би доцільність і оптимальність розміщення базових станцій в залежності від локалізації навантаження, типу замовлених послуг GBR та NGBR та QoE оцінки користувачів забезпечуючи при цьому високу енергоефективність мережі шляхом переведення в неактивний режим базових станцій, які не використовуються для обслуговування користувачів .

Щоб визначити навантаження, яке вносить відповідний користувач GBR або NGBR за наявності доступних радіоресурсів формалізуємо спочатку модель SINR. У гетерогенному середовищі миттєвий SINR кінцевого користувача j з комірки i для виділеного ресурсного блоку (RB) r всередині підкадру формулюється як,

$$SINR_{i,j,r}(\tau) = \frac{P_{i,r}^{tx}(\tau) \cdot |h_{i,j,r}|^2}{\sum_{\forall k \in M, k \neq i} P_{k.r}^{tx} \cdot |h_{k,j,r}|^2 + F_r \cdot N_0}, \quad (5.4)$$

де, $P_{i,r}^{tx}$ та $h_{i,j,r}$ визначає потужність передачі i^{th} комірки та коефіцієнт підсилення каналу між коміркою i та користувачем j для RB r, відповідно. $\sum_{\forall k \in M, k \neq i} P_{k.r}^{tx} \cdot |h_{k,j,r}|^2$ - це перешкоди від усіх інших комірок, крім обслуговуючої комірки, для користувача j (оскільки частота повторного

використання дорівнює 1), N_0 - спектральна густина потужності шуму та $F_r \cdot$ - ширина каналу виділених ресурсних блоків RB для певного типу сервісу. Якщо $\overline{SINR}_{i,j}(t)$ визначає середнє значення SINR усіх RB в момент часу t в межах підкадру (тобто $\tau \in (t-l,t)$), де l тривалість у секундах. Тоді досягнута спектральна ефективність користувача j з і-ї комірки по всіх підкадрах буде $\eta_{i,j}(t)$, і є логарифмом середнього SINR, тобто $\log_2(1+\overline{SINR}_{i,j}(t))$ згідно теореми Шеннона [21].

Навантаження, створюване користувачами GBR, є відношенням кількості ресурсів, які вони займають, до загальної кількості доступних ресурсів у мережі. Для цього спочатку визначається загальне навантаження, спричинене користувачами GBR на комірку i, тобто $D_{GBR,i}$ та визначається як $\sum_{\forall j \in GBR} I_{i,j}(t) \cdot d^j_{GBR}(t)$ - показник асоціації, він дорівнює 1, якщо користувач j підключений до i-ї BS у момент часу t, інакше дорівнює 0. $d^j_{GBR}(t)$ - вимога до швидкості j-го користувача GBR у момент часу t згідно замовлених QoE оцінок. У комірці $i, \omega^j_{GBR,used}(t)$ визначає кількість використаних частотно-часових ресурсів (ресурсних блоків RB) в момент часу t. Частка використовуваних RB користувачем GBR j, що обслуговується коміркою i, становить,

$$\omega^{i,j}_{GBR,used}(t) = \frac{I_{i,j}(t) \cdot d^j_{GBR}(t)}{\min(F_r \cdot \eta_{i,j}(t), C^{i,j}_{BH}(t))}. \tag{5.5}$$

Звідси випливає, що ємність мережі радіодоступу 4G/5G обмежена доступними RB і спектральною ефективністю і-ої комірки. Навантаження i-ої комірки користувачами GBR j (тобто $\rho^{i,j}_{GBR}(t)$) - це відношення кількості зайнятих ресурсів до кількості доступних ресурсів і подається як,

$$\rho^{i,j}_{GBR}(t) = \frac{\omega^{i,j}_{GBR,useed}(t)}{\min(\omega^i_{AC}(t)\omega^{i,j}_{BH}(t))}, \tag{5.6}$$

де $\omega^i_{AC}(t)$ - кількість доступних RB в комірці i та $\omega^{i,j}_{BH}(t)$ - кількість доступних RB в гетерогенній мережі доступу для користувача j, та формується як

$\left\lceil \frac{C_{BH}^{i}(t)}{F_r \cdot \eta_{i.j}(t)} \right\rceil$, де $\lceil \ \rceil$ - це мінімальне ціле число, $C_{BH}^{i}(t)$ - пропускна здатність комірки *i* в момент часу t. Відповідно, якщо швидкість передавання даних, що підтримується коміркою *i* є великою, а спектральна ефективність низька, це диктує загальний стан мережі з обмеженими перешкодами, коли користувацькі ресурси в мережі доступу обмежують швидкість користувача ($\omega_{AC}^{i}(t) < \omega_{BH}^{i,j}(t)$).

Використовуючи рівняння 5.6 загальне навантаження GBR для BS *i* в момент часу *t* становить $\sum_{\forall j \in N_{GBR}} I_{i,j}(t) \cdot \rho_{GBR}^{i,j}(t)$. Отже, середнє навантаження через користувачів GBR становить,

$$\overline{\rho}_{GBR}(t) = \frac{\sum_{\forall i \in M} \rho_{GBR.i}(t)}{|M|}. \tag{5.7}$$

Для визначення справедливості розподілу навантаження користувача між комірками використаємо вираз [218]

$$\xi(t) = \frac{\left(\sum_{\forall i \in M} \rho_{GBR.i}(t)\right)^2}{|M| \cdot \sum_{\forall i \in M} \left(\rho_{GBR.i}(t)\right)^2}, \tag{5.8}$$

де $\xi(t)$ коливається від $\left[\frac{1}{|M|}, 1\right]$ чим він більший, тим збалансованішим буде розподіл користувачів між БС.

Для користувачів NGBR метою є вибрати цільову комірку, яка максимізує результуюче використання мережі. Це означає, наскільки ефективно мережеві ресурси можуть бути використані для підвищення досяжних показників усіх користувачів NGBR. Оскільки функція корисності користувача U_j NGBR *j* з комірки *i* є монотонно зростаючою функцією досяжної швидкості передачі даних, яку можна обчислити у випадку пропорційного справедливого планування, подібного до [219,220], як:

$$R_{i.j}(t) = \eta_{i,j}(t) \cdot BW \cdot \left\lfloor \frac{\overline{\omega}_{net}^{i,j}(t)}{|N_{NGBR}^{i}|} \right\rfloor, \tag{5.9}$$

де $\lfloor \ \rfloor$ - максимальне ціле число і $\overline{\omega}_{net}^{i,j}(t)$- загальні доступні RB для користувача NGBR j в момент часу t та визначається, як $\omega_{net}^{i,j}(t) - \omega_{GBR,used}^{i}(t)$, $\cdot | N_{NGBR}^{i} |$ - кількість користувачів NGBR, що обслуговуються BS i.

Максимізація справедливості для користувачів GBR хоча і вирівнює використання ресурсів серед комірок, але така асоціація не знає про стан каналу користувачів. Таким чином, це погіршує загальну продуктивність мережі, оскільки користувач може бути пов'язаний із BS що забезпечує слабкий рівень сигналу, що призводить до нижчої спектральної ефективності. Метою повинно бути врахування розподілу споживання ресурсів між різними eNodeB, а також фактичних ресурсів, споживаних eNodeB в мережі. Пізніше фіксується стан каналу користувачів, оскільки користувачеві GBR (з вимогами щодо фіксованої швидкості для забезпечення певного рівня QoE) із кращим індексом якості каналу CQI виділяється менша кількість частотно-часових ресурсів, щоб задовольнити свою швидкість порівняно з користувачем GBR з поганим каналом. Таким чином, коли відбувається передавання користувачами інших eNodeB, це не тільки змінює розподіл споживання ресурсів між різними eNodeB, але це також впливає на ресурси, споживані різними eNodeB в мережі.

Відповідно цільова функція задачі ефективного розподілу радіоресурсів для групи GBR, формалізується у вигляді:

$$\max_{I_{i,j}(t)} \xi(t) \cdot (1 - \overline{\rho}_{GBR}(t)), such\ that\ ; \tag{5.10}$$

$$\sum_{\forall i \in M} I_{i,j}(t) \cdot \min(R_{i,j}(t), C_{BH}^{i,j}(t)) \geq d_{GBR}^{j}(t), \forall j \in N_{GBR}\ ; \tag{5.11}$$

$$\sum_{\forall j \in N_{GBR}} I_{i,j}(t) \cdot \omega_{GBR,used}^{i,j}(t)) \leq \min(\omega_{AC}^{i}(t), \omega_{BH}^{i}(t)), \forall i \in M\ ; \tag{5.12}$$

$$\sum_{i \in M} I_{i,j}(t) = 1, \forall j \in N_{GBR}\ . \tag{5.13}$$

Цільова функція задачі розподілу радіоресурсів для групи GBR, формалізується у вигляді,

$$\max_{I_{i,j}(t)} \sum_{\forall i \in M} \sum_{\forall j \in N_{NGBR}} U_j(I_{i,j}(t) \cdot R_{i,j}(t)), such\ that; \quad (5.14)$$

$$\sum_{\forall i \in M} I_{i,j}(t) = 1, \forall j \in N_{NGBR}. \quad (5.15)$$

Рівняння 5.10 та рівняння 5.14 визначає цілі передачі відповідно для користувачів GBR та NGBR. Це означає вибрати матрицю асоціації користувачів $I_{i,j}(t)$ $\forall i \in M$ і $j \in N$, яка максимізує вищезазначені цільові функції. Для користувачів GBR критерієм є вибір цільової комірки, яка рівномірно розподіляє користувачів по мережі, мінімізуючи середнє навантаження мережі. Рівняння 5.11 та 5.12 означає обмеження швидкості та обмеження доступних ресурсів для користувачів GBR та комірок ($i \in M$) відповідно. Рівняння 5.13 та 5.15 визначають обмеження асоціації для користувачів GBR та NGBR відповідно.

На основі вище сформульованого завдання розподілу ресурсів необхідно також врахувати можливість підвищення енергоефективності мережі шляхом динамічного формування структури рівня радіодоступу. У запропонованій моделі енергозберігаючий стан БС визначається в залежності від кількості UE, які вимагають високошвидкісного трафіку даних (наприклад відео з високою роздільною здатність, оцінка користувача QoE-5), і кількості UE, які існують у зонах перекриття, які зазвичай охоплюються розглянутою BS та сусідніми BS. Якщо всі UE, які вимагають високошвидкісного трафіку даних під покриттям БС, можуть бути покриті сусідніми БС, розглянута БС може бути переведена в режим сну або в режим вимкнення для економії енергії, і навпаки по мірі зростання вмикати базові станції.

Загальне енергоспоживання рівнем радіодоступу мережі 4G/5G визначається як [222]:

$$P_{total5G} = \sum_{j=0}^{k-1} P(j)_{MC} + \sum_{j=0}^{m-1} P(j)_{SC}\ , \quad (5.16)$$

де $P(j)_{MC}$ - енергоспоживання $MCBS_j$ *j-ї* макрокомірки, *k*-кількість БС макрорівня в мережі 5G, $P(j)_{SC}$ - енергоспоживання $SCBS_j$ *j-ї* базової станції фемтокомірки та пікокомірки, *m*-кількість БС фемто та пікорівня в мережі 5G.

Припускається, що всі UE користувачі *n*, які знаходяться в зоні покриття BS_j можуть обслуговуватись. Встановлення зв'язку між $MCBS_j, SCBS_j$ та *UE* позначається як $a_{j,i}$, і, і його значення визначається згідно рівнянні (5.17), де $MCBS_j(0 \le j < k-1)$ і $SCBS_j(0 \le j < m-1)$.

$$a_{j,i} = \begin{cases} 1, if\ u_i\ is\ connected\ with\ BS_j \\ 0, otherwise\ ,(0 \le j < m+1, 0 \le i < n) \end{cases} . \qquad (5.17)$$

Попит на певний тип трафіку даних користувачем UE позначається як d_j, і його значення визначається як:

$$d_i = \begin{cases} 1, if\ u_i\ reqruired\ data\ service \\ 0, otherwise\ (0 \le i < n) \end{cases} . \qquad (5.18)$$

Тип та якість необхідного трафіку даних UE позначається як r_i і значення його визначається як:

$$r_i = \begin{cases} 1, if\ u_i\ reqruired\ high\ rate\ data\ service\ QoE_{high}, (0 \le i < n) \\ 0, f\ u_i\ reqruired\ low\ rate\ data\ service\ \ QoE_{low} \end{cases} . \qquad (5.19)$$

У рівнянні (5.20) ω_j пов'язане з тим, чи знаходиться BS_j у активному стані чи ні, а e_j пов'язано з тим, чи знаходиться BS_j у сплячому стані чи ні, у рівнянні (6):

$$\omega_j = \begin{cases} 1, if\ B_j\ is\ in\ on\ state\ ,(0 \le j < m+1) \\ 0, otherwise \end{cases} ; \qquad (5.20)$$

$$e_j = \begin{cases} 1, if\ B_j\ is\ in\ sleep\ state\ ,(0 \le j < m) \\ 0, otherwise \end{cases} . \qquad (5.21)$$

Використовуючи наведені вище рівняння, отримується енергоспоживання малих комірок $SCBS_j$, *P(j)*, як:

$$P(j)_{SC} = \omega_j \times (1-e_j) \times (P_{SC}^f + \rho_{SC} \times P_{SC}^{tx}(j)) + e_j \times (1-\omega_j) \times P_{SC}^e, \quad (5.22)$$

де, якщо $SCBS_j$ перебуває у стані включення, споживання енергії обчислюється як сума фіксованого споживання енергії P_{SC}^f та енергоспоживання $P_{SC}^{tx}(j)$, що залежить від навантаження малої комірки ρ_{SC}. Якщо $SCBS_j$ перебуває в режимі сну, тоді для розрахунку використовується споживання енергії для стану сну P_{SC}^e та енергоспоживання. Залежного від навантаження, енергоспоживання $P_{SC}^{tx}(j)$ визначається, як:

$$P_{SC}^{tx}(j) = P_{SC}^{tx,\max} \times \sum_{i=0}^{n-1} \left(d_i \times a_{j.i} \times \frac{(r_i \times C_{QoEh} + (1-r_i) \times C_{QoEl})}{C_{SC}^{\max}} \right), \quad (5.23)$$

де $C_{SC}^{\max}$ максимальна пропускна здатність малої комірки, C_{QoEh} пропускна здатність необхідна для обслуговування користувачів із високою якістю обслуговування, наприклад відео з високою роздільною здатністю, оцінка користувача QoE становить 5), C_{QoEl} пропускна здатність необхідна для обслуговування користувачів із низькою якістю обслуговування, наприклад відео з низькою роздільною здатність, оцінка користувача QoE становить 2).

Аналогічно, енергоспоживання P_{MC} для макрокомірок $MCBS_j$, отримується, як у рівнянні (5.24), як сума фіксованого енергоспоживання P_{MC}^f та енергоспоживання, залежного від навантаження [223].

$$P_{MC} = P_{MC}^f + \rho_{MC} \times P_{MC}^{tx}, \quad (5.24)$$

де P_{MC}^{tx} визначається так, як у рівнянні (5.25):

$$P_{MC}^{tx} = P_{MC}^{tx,\max} \times \sum_{i=0}^{n-1} \left(d_i \times a_{j,i} \times \frac{(r_i \times C_{QoEh} + (1-r_i) \times C_{QoEl})}{C_{MC}^{\max}} \right), \quad (5.25)$$

де $C_{PC}^{\max}$ максимальна пропускна здатність макрокомірки.

Передбачається, що максимальне споживання енергії $SCBS_j$ становить $P_{SC}^{\max}$, і, отже, споживана потужність $SCBS_j$ повинна бути меншою або дорівнює $P_{SC}^{\max}$:

$$P(j)_{small} \le P_{SC}^{\max}, (0 \le j \le m-1). \quad (5.26)$$

Аналогічним чином передбачається, що максимальне споживання енергії $MCBS_j$ становить $P_{MC}^{\max}$, і, отже, енергоспоживання $MCBS_j$ має бути меншим або рівним $P_{MC}^{\max}$:

$$P_{MC} \le P_{MC}^{\max}. \quad (5.27)$$

Якщо SBS j увімкнено, UE i може мати зв'язок з SBS j. Однак, якщо SBS j не перебуває у стані, UE i не може мати з'єднання з SBS j. Ці відносини обмежуються наступним чином:

$$a_{j,i} \le \omega_j. \quad (5.28)$$

Тип необхідного трафіку даних UE i визначається як 1 або 0, залежно від типу необхідної послуги передачі даних, і це менше або дорівнює існуванню попиту на трафік даних UE i:

$$r_i \le d_j. \quad (5.29)$$

Оскільки UE i може мати щонайбільше одне з'єднання або з $MCBS_j$, або з будь-якими $SCBS_j$ в межах $MCBS_j$, обмеження виражається наступним чином:

$$\sum_{j=0}^{m} a_{j,i} \le 1. \quad (5.30)$$

Оскільки $SCBS_j$ може перебувати в одному із станів увімкнення, сну та вимкнення, сума ω_j для увімкненого стану та e_j для вимкненого стану повинна бути меншою або дорівнювати 1:

$$\omega_j + e_j \le 1, (0 \le j \le m-1). \quad (5.31)$$

Максимальна кількість UE в $MCBS_j$ дорівнює n, максимальна кількість $SCBS_j$ в $MCBS_j$ дорівнює m, кількість $MCBS_j$ дорівнює k=1, і вони обмежуються наступним чином:

$$0 \le i < n, 0 \le j < m+1. \quad (5.32)$$

Використовуючи вищезазначені обмеження, проблему оптимізації запропонованої схеми енергозбереження формулюється наступним чином:

$$\min P_{total5G}. \tag{5.33}$$

Задача оптимізації, визначена в цій роботі, є змішаним цілочисельним лінійним програмуванням, оскільки деякі змінні в пропонованій оптимізації обмежуються дискретними цілими значеннями.

5.2.4. Блок-схеми інтенційно-орієнтованого методу розподілу ресурсів та формування структури рівня радіодоступу 4G/5G

Для розв'язання вище сформульованого завдання ефективного розподілу радіоресурсів з врахуванням QoE вимог користувачів у роботі запропоновано у вигляді блок схем інтенційно-орієнтований метод розподілу ресурсів та формування структури рівня радіодоступу 4G/5G, що програмно автоматизується у імітаційній моделі використовуючи при цьому готові програмні класи, що розв'язують цілочисельні задачі лінійного та нелінійного програмування. Розроблений метод в основному базується на трьох основних етапах. На першому етапі IBN/SDN контролер мережі на основі обміну сигналізаційними даними між базовими станціями і користувачами збирає статистику стосовно просторово-часової локалізації абонентського навантаження з метою створення певної карти навантаження на певній території покриття. Розглядається також можливість користувачів з допомогою мобільного додатку замовляти в оператора мережі певний рівень якості обслуговування у вигляді QoE оцінки. На другому етапі методу відбувається системний аналіз зібраних QoE вимог користувачів та отриманої інформації стосовно локалізації навантаження для прийняття рішення щодо інтенційно-орієнтованого обслуговування абонентів. На третьому етапі проводиться автоматизоване рішеннящодо модифікації та формування (якщо не була створена до цього моменту) структури рівня радіодоступу на основі інтуїтивної логіки управління контролера SDN/IBN мережі.

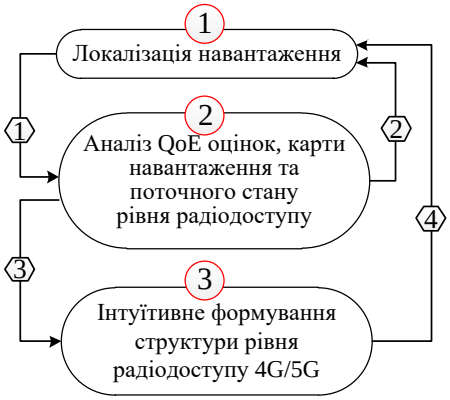


Рис. 5. 19. Загальна блок схема інтенційно-орієнтованого методу розподілу ресурсів та формування структури рівня радіодоступу 4G/5G [221]

Розглянемо детально принцип роботи даного методу. Усі користувачі IBN мережі на першому етапі підключаються до макрокомірки $M(S)=\{MC_1, MC_2....MC_i\}$. Кожен користувач описуються наступними атрибутами мережі: порогова потужність ($P_{пор.}$) випромінювання від користувача до БС; SINR; QoS_class послуг GBR/NGBR та замовленою QoE оцінкою щодо якості обслуговування. На основі даних атрибутів абонентський пристрій UE формує запит на обслуговування ($QoE_{onrequest}$), який відсилається по каналу «вверх» до БС. Малі комірки, які знаходяться в режимі енергозбереження характеризуються вимкненим каналом «вниз» (Downlink), увімкнутим є тільки канал «вверх». Базова станція макрорівня отримавши інформацію від користувачів, дає вказівку через канал UL малим коміркам SC^N, SC^{N-1}, визначити Channel State Information (CSI), а саме вектор зміни відстані до БС шляхом зміни потужності сигналу (ΔP_{UL_UEi}), після чого для кожної малої комірки формується матриця «допустимих користувачів» $\{K\}$, які містять статистику по усіх користувачах, що потенційно можуть бути обслужені конкретною БС. Формування карти навантаження проводиться з допомогою контролера SDN/IBN, який здійснює аналіз матриць $\{K_i\}\{S_i\}$, де ($\{K_i\}$-матриця користувацьких пристроїв, які потенційно можуть бути обслужені базовою станцією, $\{S_i\}$-матриця UE, які вже обслуговуються базовою станцією та

«відкидання» користувачів, які не можуть бути обслужені через невідповідність параметрів якості радіоканалу [221].

$$K_i = [UE_{reserv}, UE_{reserv}, ..., UE_{reserv}], S_i = [UE_{current}, UE_{current}, ..., UE_{current}], \quad (5.34)$$

де UE_{reserv} - користувацький пристрій, що знаходиться в радіусі дії комірок SC^N, SC^{N-1} та потенційно може бути нею обслужений, $UE_{current}$ - користувацький пристрій, що обслуговується в даний момент SC^N, SC^{N-1}.

У результаті чого для кожної базової станції рівня SC^N, SC^{N-1} формуються матриці {*K*'}, що містять інформацію про користувачів, яких необхідно обслужити конкретною базовою станцією. Керуюча інформація надсилається на нижчий рівень і формується загальна карта поточного навантаження R_i.

$$R_i = \sum K_i + \sum S_i . \quad (5.35)$$

Для кожної з малих комірок утворюється своя матриця користувачів {K'}(5.36), які потенційно повинні бути обслужені конкретною БС.

$$K'_i = K_i - \sum UE_{notserviced} . \quad (5.36)$$

$UE_{notserviced}$ - абонентський пристрій, який не може бути обслужений конкретною БС, у зв'язку із невідповідністю параметрів низхідного каналу або мобільності користувача.

На основі керуючої інформації щодо аналізу стану мережі та карти поточного навантаження формується матриця {R'}(5.37), яка містить в собі інформацію про стан користувачів, що вже є на обслуговуванні структурою рівня радіодоступу та інформацію про абонентів, що потенційно повинні бути обслужені конкретною базовою станцією.

$$R'_i = \sum K'_i + \sum S_i \quad (5.37)$$

Роботу другого етапу блок-схеми методу, що відповідає за аналіз стану рівня радіодоступу є одним із основних та показано на рис. 5.20б. Згідно якого контролер вирішує як надати сервіс користувачу *UE* із певною оцінкою QoE в

межах кожної базової станції, що йому доступна. Вибір проводиться на основі трьох правил:

1) Якщо користувач UE характеризується високим значенням вектора зміни відстані до базової станції, то обслуговування здійснюватиметься макрокоміркою MC_{Dl}. Аналогічно макрокоміркою будуть обслуговуватися користувачі, що вимагають будь-який інший *QoS_class,* зокрема таких що вимагають низького рівня QoE, якщо немає можливості їх підключення до альтернативної SC малої комірки.

2) Якщо користувач UE характеризується низьким значенням вектора зміни відстані до БС та високими вимогами до трафіку *QoS_classmax*, що відповідає оцінкам $QoE_{4,5}$ і підключення його до активних структурних елементів рівня радіодоступу не спричинить перенавантаження, то SDN/IBN контролер підключить його до відповідної малої комірки SC із паралельною агрегацією каналів макрокомірки MC_{Dl}. Таким чином шляхом агрегації частот забезпечується краща якість обслуговування. В результаті чого відбувається перевірка матриць *{Ki}* і *{Si}*, щоб з'ясувати чи є необхідність у зміні структури рівня радіодоступу 4G/5G шляхом переведення малих комірок в неактивний стан для зменшення енергоспоживання мережі. При виникненні такої необхідності контроль переноситься на третій блок, якщо немає, то перебудовується поточна карта навантаження і контроль переноситься на перший етап блок-схеми загального методу..

3) Якщо користувач UE характеризується низьким значенням вектора зміни відстані до БС та високими вимогами до трафіку *QoS_classmax,* що відповідає оцінкам $QoE_{4,5}$ і немає можливості підключення його до активних структурних елементів рівня радіодоступу виноситься рішення про застосування додаткових малих комірок та керування передається на третій етап загальної блок-схеми методу.

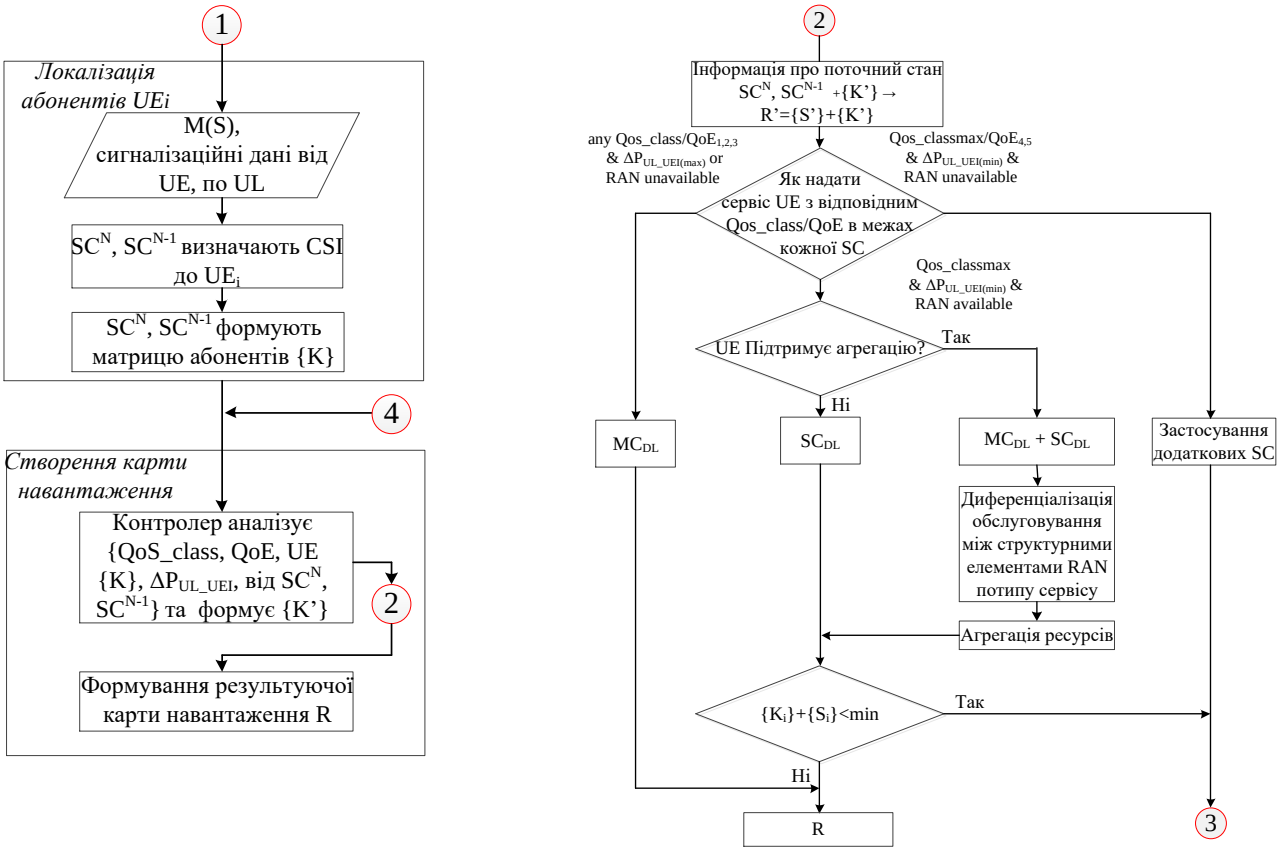
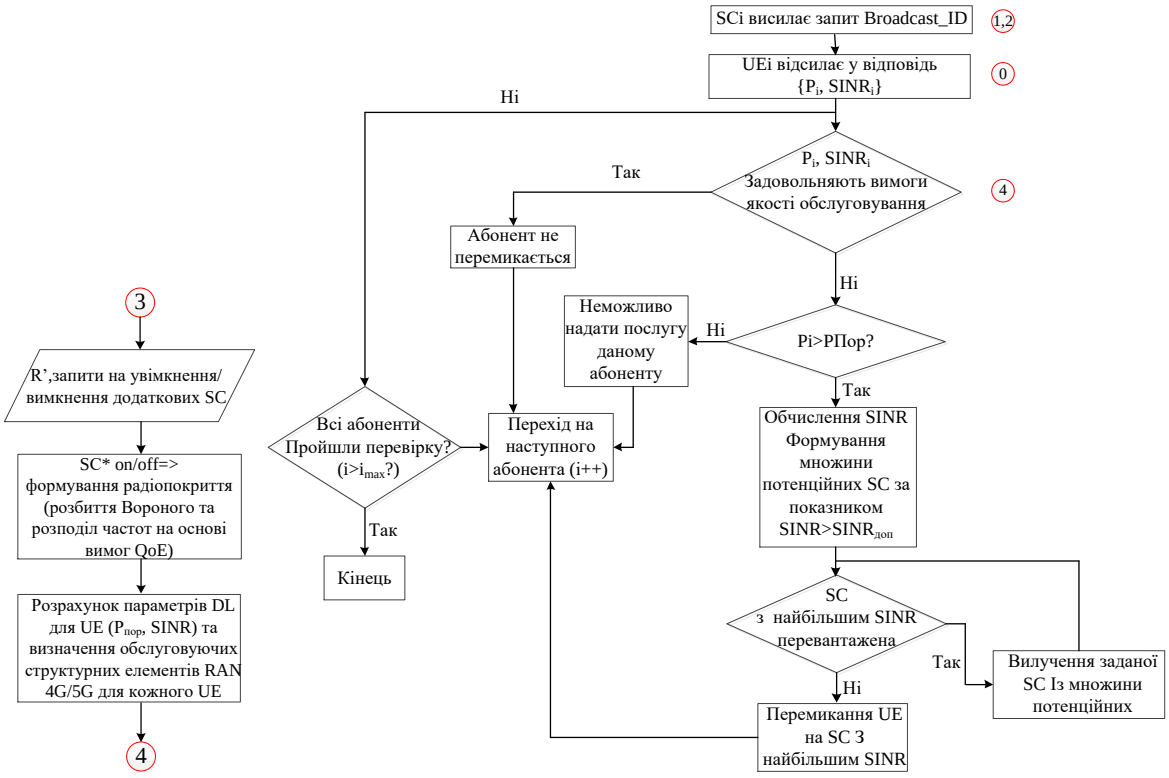


Рис. 5.20. Алгоритм локалізації користувачів та створення карти навантаження – а) та алгоритм аналіз стану RAN – б) [11]

Отримавши необхідну інформацію про користувачів UE_i, що мають бути обслужені конкретною базовою станцією та матрицю $\{Si\}$, що містить інформацію про активних користувачів малих комірок і використовуючи дані про розміщення базових станцій та зону їх покриття, контролер вирішує котрі саме БС та їх кількість потрібні для обслуговування поточного навантаження. В результаті чого відбувається перебудова структури мережі рівня радіодоступу (рис.5.21а). Далі проводиться визначення та перевірка параметрів DL для користувачів *UE* та індентифікації обслуговуючих структурних елементів рівня радіодоступу для кожного UE_i згідно алгоритму представленого на рис. 5.21б.

Кожна із малих комірок SC формує множину користувачів, для яких значення прийнятого рівня потужності сигналу більше деякого порогового значення $P_{пор.}$ Для цього кожна комірка *SC* посилає широкомовний ехо-запит, що містить ідентифікатор даної *SC* до всіх користувачів в зоні своєї дії. Кожен

користувач *UE*, отримавши запит відповідає на нього вказавши значення потужності прийнятого сигналу, інтерференційних завад і шумів в тому ж діапазоні *(P_i, $SINR_i$)*. Після чого виміряні дані передаються до SDN/IBN контролера.



а) б)

Рис. 5.21 Принцип роботи третього етапу методу – а) та розрахунок параметрів DL для *UE* та визначення обслуговуючих структурних елементів рівня радіодоступу для кожного *UE* – б)

Контролер порівнює отримані значення потужності з пороговим і відкидає тих користувачів, у яких прийняте значення менше від порогового – цих користувачів неможливо обслуговувати, оскільки жодна з комірок не має достатньої потужності для цього. Тоді для кожного абонента з отриманої множини формується множина SC, для яких параметр SINR є більшим за допустиме значення. Ці SC формують множину потенційних, які могли б обслуговувати користувача. Після цього вибирається SC з найбільшим значенням SINR з набору потенційних SC і перевіряється, чи не

перевантажений він. Якщо обрана SC перевантажена, вона видаляється з набору потенційних SC і процес повторюється до тих пір, поки не буде обрано SC, яка може обслуговувати користувачів. Потім контролер дає користувачеві вказівку перейти до обраної SC. Якщо всі малі комірки є перевантаженими, то користувач буде обслуговуватися макрокомірками. Потім система повертається до виконання кроку 3 (виконання блоку створення карти).

5.2.5. Розроблення імітаційної моделі інтенційно-орієнтованої гетерогенної мережі мобільного зв'язку 4G/5G

З метою оцінки ефективності запропонованих рішень в процесі синтезу радіодоступу та оптимізації мережі за критерієм замовленої якості обслуговування користувачів розроблено імітаційну модель інтенційно-орієнтованої гетерогенної мережі 4G/5G, яка, на відміну від існуючих засобів моделювання, враховує основні технічні параметри функціонування стандарту LTE для створення реальних умов дослідження та автоматизує у вигляді програмного коду запропонований метод інтенційно-орієнтованого управління частотно-часовими ресурсами та формування структури рівня радіодоступу. Основною перевагою розробленої моделі є використання системно-об'єктного підходу проектування функціональних блоків мережі мобільного зв'язку на основі відомих LTE стандартів, що дало змогу адекватно формалізувати опис системи як єдине ціле, надавши повну інформацію про структуру, функціонування і поводження окремих елементів системи.

Імітаційна модель мережі мобільного зв'язку складається із трьох базових станцій макрорівня. Вони утворюють регулярну структуру мобільної мережі. На робочому полі моделі не показано всієї зони дії макрокомірок, оскільки цікавою для дослідження є величина навантаження на сектор базової станції (60^0). Центри макростанцій утворюють трикутник. В цьому трикутнику розміщені малі комірки SC двох рівнів. Місцезнаходження пікокомірок і фемтокомірок встановлено відповідно до розробленого методу. Якщо є потенційне навантаження, вони вмикаються, коли навантаження на них немає,

вони вимикаються і зникають із робочого поля. Ввімкнення і вимкнення фемтокоміркок призводить до зміни структури рівня радіодоступу. Робоче поле моделі представлено на рис. 5.22.

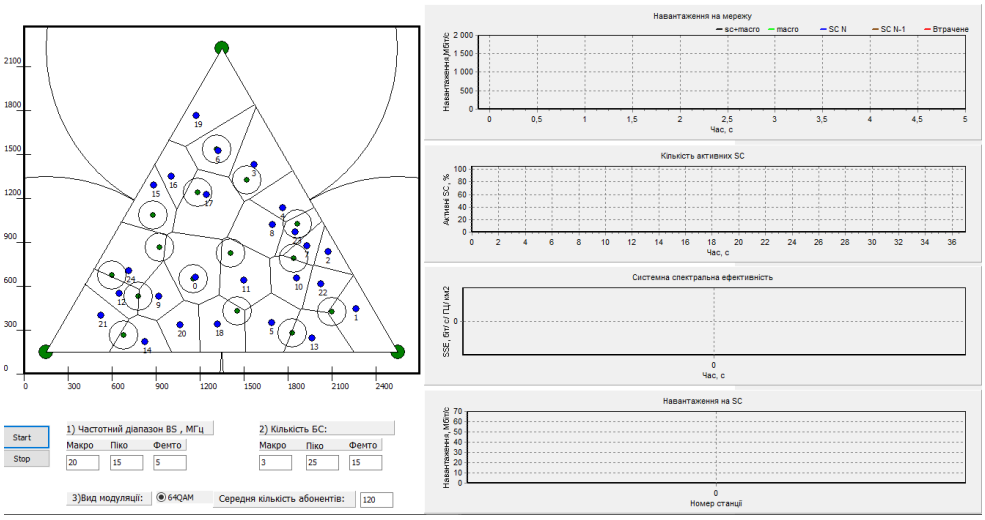


Рис.5.22. Робоче поле моделі

Виходячи зі швидкості абонента і генерованої ним трафіку, абонент буде обслуговуватися або базовою станцією одного рівня, або декількома станціями різного рівня (з агрегацією спектра).

Для генерування трафіку і моделювання швидкості руху абонента використовуються генератори, засновані на єдиних і логнормального законах розподілу, які в сукупності дають можливість отримати сценарії поведінки абонента поблизу реальних мереж мобільного зв'язку. При цьому переміщення абонента в моделі є Квазіпостійним. Це означає, що абонент буде рухатися з постійною швидкістю протягом деякого часу, після чого йому буде присвоєно нове значення швидкості руху. Напрямок руху розраховується за кількома сценаріями, розробленими в моделі:

1. Мінімальне навантаження на мережу. Рух абонентів є випадковим. Абоненти доволі рівномірно розподілені по модельованій території покриття.

2. Зростання потенційного навантаження від абонентів. Досягається збільшенням кількості абонентів і їх рухом із деяким тяжінням до центру моделі.

3. Функціонування мережі в години найбільшого навантаження.

4. Поступове зменшення навантаження на мережу. Поступово зменшується кількість користувачів, вони рухаються від центра моделі. Подальший напрямок мобільності – випадковий.

Індивідуальною особливістю користувача є ймовірність його активності. Зробимо припущення, що абоненти з ймовірністю P генерують трафік (активні абоненти) і з ймовірністю (1 - P) не генерують ніякого навантаження (пасивні абоненти). Всі вхідні параметри моделювання наведені у таблицях 5.4 та 5.5. Тестування роботи мережі та аналіз її показників проводились протягом 12 годин.

Таблиця 5.4

Параметри моделювання інтенційно-орієнтованої мережі 5G

Параметри базових станцій			
	MC	SC^N	SC^{N-1}
Потужність випромінювання	46 дБп	23-30 дБп	до 23 дБп
Частотний діапазон	20 МГц	15 МГц	5 МГц
Режим передачі	MIMO	SISO	SISO
Радіус дії	1.2 км	200-300 м	50 м
Модуляція	QPSK-64QAM	QPSK-64QAM	QPSK-64QAM
Кількість антен	4x4	4x4	4x4
Кількість базових станцій	3	25	15
Параметри абонентів			
Активність	Абонент активний з ймовірністю *p* і пасивний з ймовірністю (1-p). $p \in (0.5 , 0.9)$		
Навантаження Y	Випадкове, рівномірний закон розподілу $y \in (0,20)$		
Кількість ітерацій N, протягом яких параметри абонента є сталими	*N* – випадкова рівномірно розподілена величина. $N \in [1 , 20]$.		
Розподіл абонентів по території.	Є дві групи абонентів: а)Абоненти рівномірно розподілені по території. Існують протягом всього часу моделювання. б)Додаткові абоненти -- для моделювання скупчення абонентського навантаження. Група абонентів з'являється, існує певний проміжок часу та зникає.		
Середня кількість абонентів	120		

Генерація навантаження абонентами відбувається в декілька етапів: Генеруємо сесію та обираємо її параметри такі як час користування сесією, вид сервісу, бажана оцінка QoE (від 1 до 5); Генеруємо трафік для сесії поки вона не завершиться; Після завершення генеруємо новий трафік з новими параметрами.

Таблиця 5.5

Параметри моделювання QoE намірів користувачів

Тип сервісу	Відсотковий еквівалент,%	Пропускна здатність для сервісу, Мбіт/с	QoE для відео контенту
Перегляд відео 480p	30	0.1-2	QoE<3
Перегляд відео 720p	15	2-3	QoE<(3-3.5)
Перегляд відео 1080p	5	3-7	QoE<(3.5-4.5)
Перегляд відео 1140p	5	7-11	QoE<(4.5-4.8)
Перегляд відео 2160p	5	11-14	QoE (4.8 -5)
Відео конференція	20	5	-
Перегляд web-ресурсів	22	2	-
E-mail	21	0.5	-
IP-телефонія	2	1	-

В імітаційній моделі кожна базова станція містить в собі список користувачів, список активних та пасивних користувачів, ідентифікатор назви вузла та таблицю розподілу навантаження. Також базова станція має відповідні методи для створення обчислення зони, в якій знаходиться користувач []. Це необхідно для подальшого алгоритму, який буде полягати в аналізі зони в якій знаходиться користувач і необхідних йому ресурсів. Відбувається обчислення кількості активних абонентів в різних зонах базової станції. Кожної ітерації генеровані дані абоненти відправляють до відповідного базової станції, який їх обслуговує. Після зчитування даних, йде аналіз ресурсів мережі та можливих вільних ресурсів. Базова станція в запропонованій моделі дозволяє здійснювати розподіл зі шириною каналу від 0.2 до 20 МГц. Максимальне значення корисної швидкості для центральної і граничної площі комірки буде залежати від коефіцієнта розподілу ресурсів. В розробленій моделі саме цей коефіцієнт буде визначатись динамічним способом.

Таблиця 5.6

Можлива пропускна здатність в 5G

CQI	Ширина каналу, МГц							
	0,2	1,4	3	5	10	15	20	100
	Корисна швидкість, Мбіт/с							
1	0,022	0,246	0,6413	1,0801	2,1769	3,2738	4,3707	21,853
2	0,034	0,379	0,9866	1,6616	3,3491	5,0366	6,7241	33,620
3	0,056	0,609	1,5868	2,6724	5,3865	8,1006	10,8146	54,073
4	0,089	0,973	2,5323	4,2648	8,5961	12,9273	17,2586	86,292
5	0,130	1,418	3,6916	6,2172	12,531	18,8454	25,1594	125,79
6	0,174	1,901	4,9496	8,3358	16,801	25,2671	33,7327	168,66
7	0,219	2,388	6,2157	10,468	21,099	31,7307	42,362	211,80
8	0,284	3,096	8,0574	13,569	27,351	41,1324	54,9137	274,56
9	0,357	3,892	10,129	17,059	34,384	51,7094	69,0344	345,17
10	0,405	4,416	11,494	19,357	39,017	58,6767	78,3361	391,68
11	0,493	5,374	13,985	23,553	47,473	71,3942	95,3145	476,57
12	0,579	6,312	16,427	27,666	55,762	83,8598	111,956	559,78
13	0,671	7,317	19,041	32,069	64,638	97,2069	129,775	648,87
14	0,759	8,274	21,533	36,265	73,0947	109,9243	146,754	733,770
15	0,8249	8,9853	23,383	39,3805	79,3743	119,368	159,3618	796,808

Через те, що відношення сигнал шум в центральній зоні комірки і в граничній зоні комірки відрізняються, то можлива пропускна здатність в цих зонах буде відрізнятись Для кореляції максимального значення пропускної здатності на границях комірки, використаємо антену типу 4x4, що дозволить в 2 рази збільшити можливе максимальне значення. При перегляді розподілу користувачів на території базової станції потрібно звернути увагу на кількість користувачів в центральній і граничній площах базової станції [224]. Для коректування моделі можна добавити користувачів вручну в потрібну площу базової станції. На рис. 5.23 спостерігаємо розподіл абонентів на території дії базової станції. Можна зауважити, що концентрація абонентів в центрі комірки набагато більша за концентрацію абонентів на границях комірки.

На рис.5.24 спостерігаємо розподіл активних абонентів на території центральної площі комірки і граничної площі комірки в залежності від відповідного часового інтервалу. В даній симуляції кількість користувачів в

центральні площі комірки знаходиться в межах 20 користувачів, а для граничної зони комірки кількість абонентів знаходиться в межах 3-4 користувача.

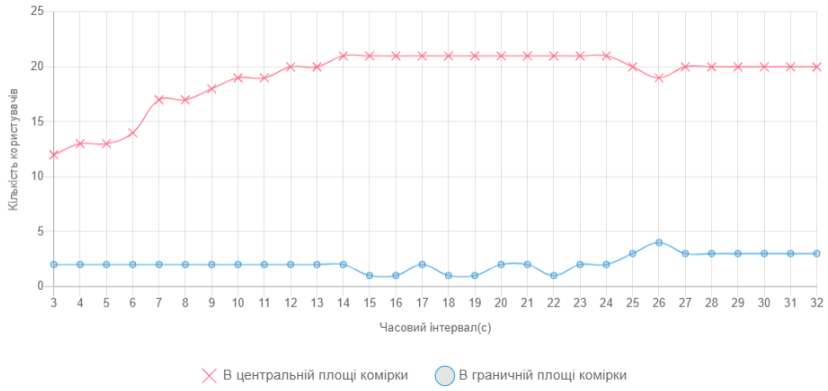


Рис.5.23. Розподіл абонентів на території дії базової станції відповідно до зон базової станції

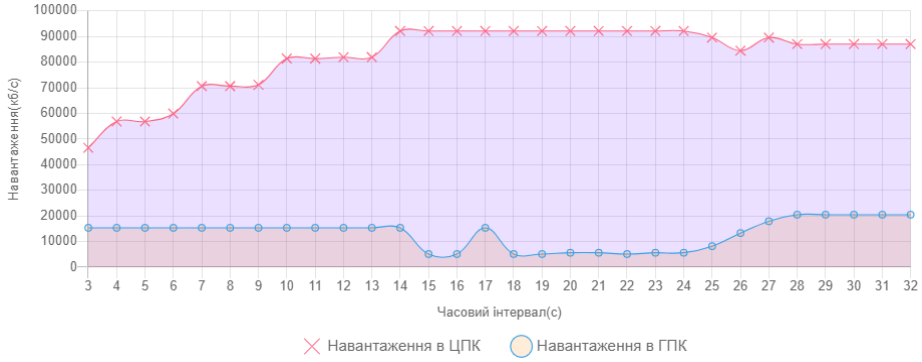


Рис.5.24. Динаміка навантаження в центральній і граничній площах комірки

5.2.6. Моделювання та дослідження ефективності запропонованого методу на основі розробленої імітаційної моделі мережі

На основі вхідних даних імітаційної моделі оцінено ефективність запропонованого методу інтенційно-орієнтованого управління частотно-часовими ресурсами та формування структури рівня радіодоступу. Зокрема, з рис.5.25 випливає, що навантаження коливається в часі, але має певну тенденцію до зростання і спаду, відносно якої оновлюється структура рівня радіодоступу. При збільшенні навантаження з 200 до 600 Мбіт/с зросла частка

активних малих комірок SC з 20 % до 55%, відповідно і збільшилась спектральна ефективність мережі з 1,55 до 4 біт/с/Гц/км^2 (рис. 5.26). Разом із тим при зменшенні інтенсивності трафіку в період часу t=(40000, 43000) з 600 до 350 Мбіт/с кількість активних базових станцій зменшилася з 60 % до 20%. В моменти часу t = 400 і t = 42500 навантаження становить 250 і 380 Мбіт/с відповідно, але при цьому є однакова частка активних базових станцій (20%). Це пояснюється тим, що в другому випадку абоненти є більш скупчені навколо окремих базових станцій.

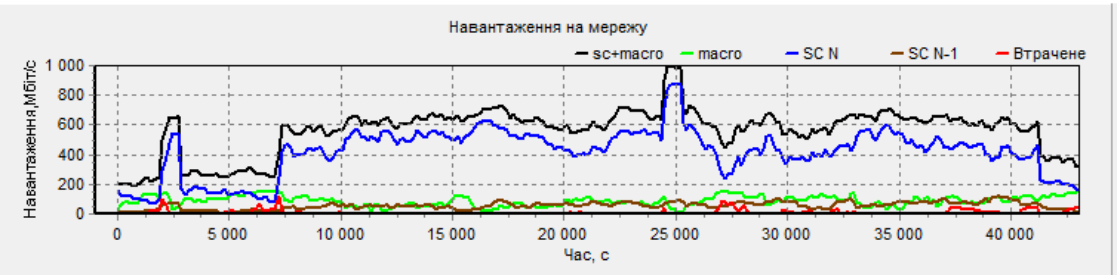


Рис.5.25. Результати моделювання: навантаження на мережу [172]

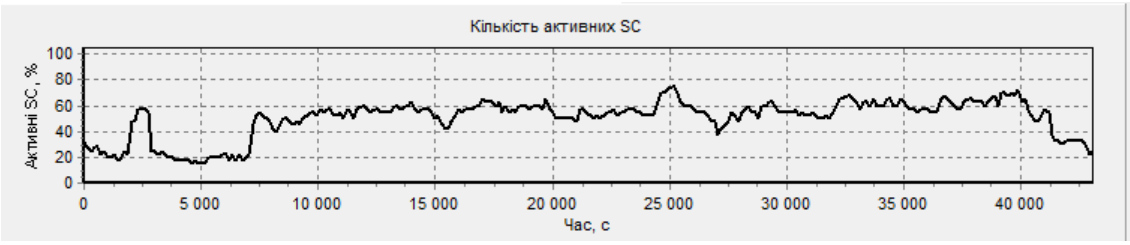
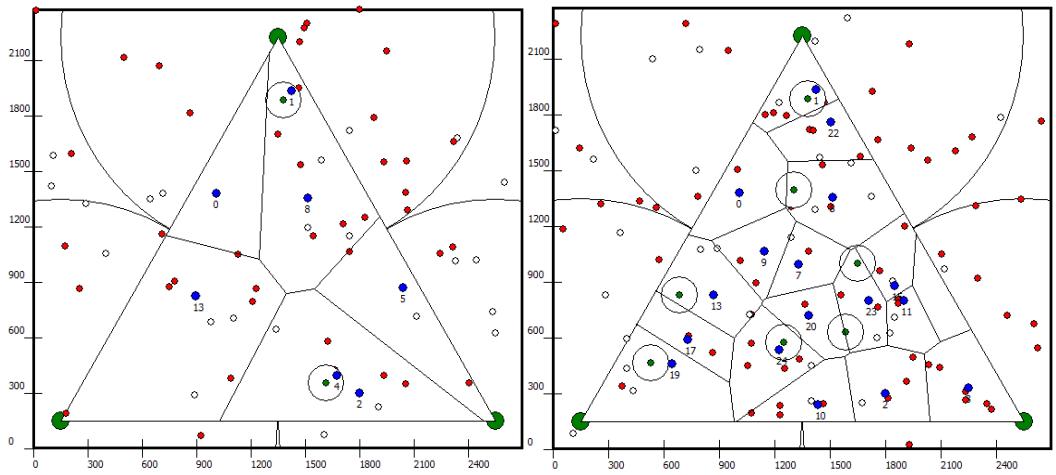


Рис.5.26.Результати моделювання: частка ввімкнених SC

Рис.5.27. Результати моделювання: системна спектральна ефективність

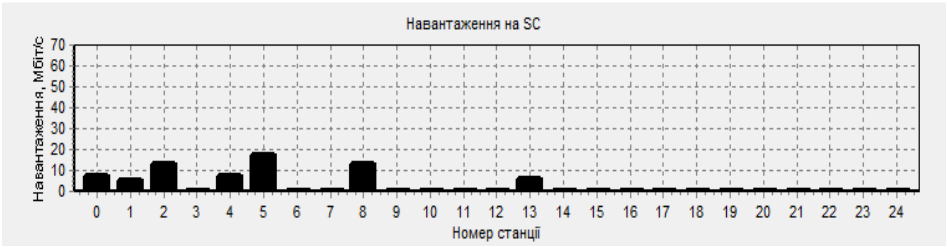
Отже, мережа з адаптивною структурою рівня радіодоступу володіє значно більшою гнучкістю в порівнянні з статичною структурою (рис.5.28). При невеликому абонентському навантаженні більшість малих комірок SC є вимкненими, відповідно кращими є показники роботи мережі по

енергоефективності і взаємній інтерференції SC. При великому навантаженні структура рівня радіодоступу стає більш деталізованою, а при ввімкненні всіх SC має такі ж параметри, як мережа зі статичною структурою.

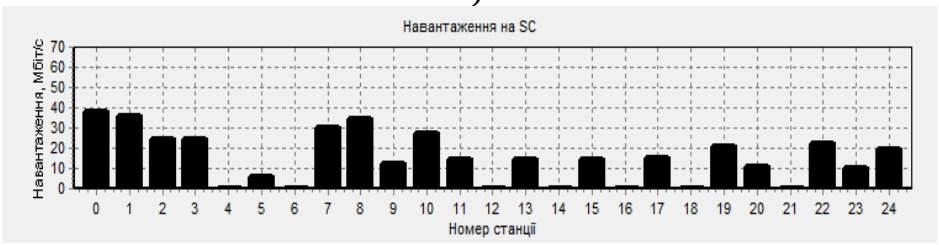


а) б)

Рис.5.28. Структура рівня радіодоступу для двох моментів часу: а) низький рівень навантаження; б) високий рівень навантаження [221]



а)

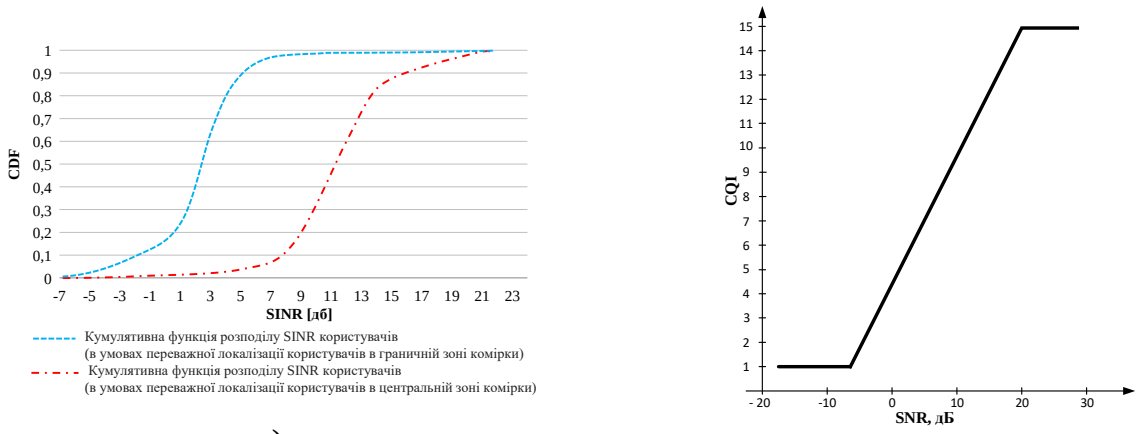


б)

Рис.5.29. Навантаження на конкретну SC для двох моментів часу – а) низький рівень навантаження та – б) високий рівень навантаження

Для порівняння та оцінки ефективності впровадження нового методу із відомими, використано критерій ймовірність того, що користувач отримає певну пропускну здатність каналу. Для цього у роботі використано кумулятивну функцію розподілу (cumulative distribution function), CDF ймовірності виділення середньої пропускної здатності для одного користувача

в умовах використання різних методів розподілу радіоресурсів. На основі імітаційної моделі проведено порівняння кумулятивних функції розподілу пропускних здатностей користувачів при використанні існуючих методів розподілу ресурсів RR (Round Robin), PF(Proportional Fairness) та із використанням запропонованого інтенційно-орієнтованого методу, по відношенню до еталонної кумулятивної функції розподілу пропускних здатностей користувачів сформованої на основі їх замовлених QoE оцінок, які характеризують певний рівень якості обслуговування (зокрема виділення необхідної пропускної здатності для перегляду відеосервісу у замовленій якості). Відповідно, ефективнішим буде цей метод розподілу ресурсів, кумулятивна функція якого наближається до еталонної. Порівняння проводилось для двох випадків локалізації користувачів: в умовах переважної локалізації в граничній зоні комірки (низькі значення SINR рис.5.30а) та в центральній зоні комірки (високі значення SINR рис. 5.30а).



а) б)

Рис.5.30. Кумулятивна функція розподілу SINR в умовах різної локалізації користувачів – а) та співвідношення SINR та CQI рівня – б) (в умовах використання запропонованого та існуючих методів розподілу радіоресурсів)

В результаті порівняння встановлено, що запропонований інтенційно-орієнтований метод дає змогу забезпечити кращу адаптивність розподілу ресурсів щодо забезпечення замовленої якості обслуговування у порівнянні із відомими. Зокрема, запропонований метод проводить раціональний розподіл

ресурсів аналізуючи оцінки користувачів QoE, шляхом розв'язання завдання гнучкого перерозподілу частотно-часових ресурсів між різними вимогами користувачів адаптуючи функцію до еталонної, що показано на рис.5.31.

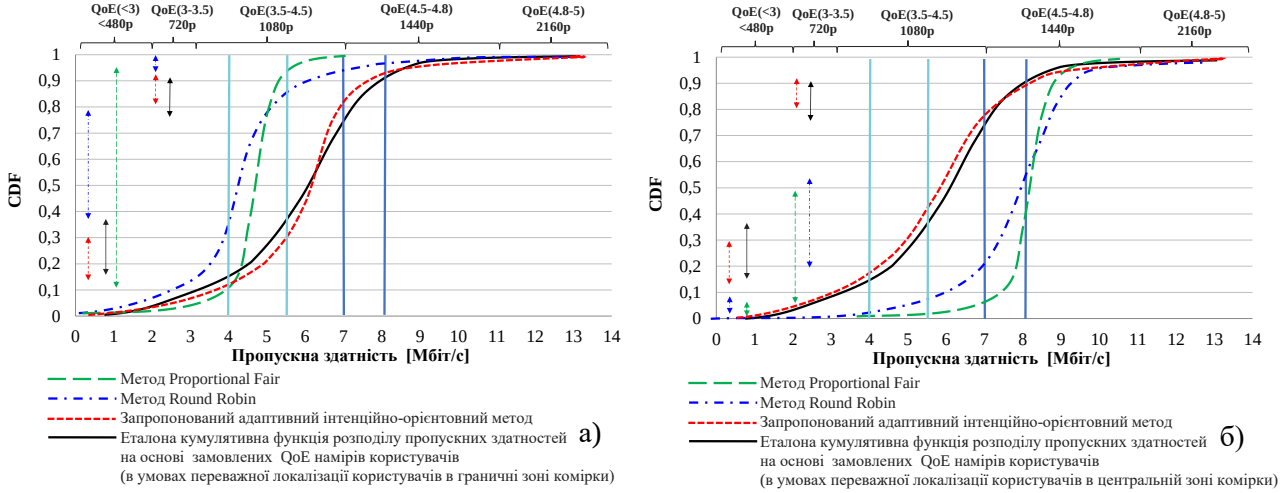


Рис.5.31. Порівняння кумулятивних функції розподілу пропускних здатностей користувачів в умовах різної локалізації користувачів при низьких SINR – а) та високих SINR – б) (в умовах використання запропонованого та існуючих методів розподілу радіоресурсів)

Також у роботі проведено дослідження можливості використання запропонованого методу для адаптивного формування структури рівня радіодоступу 4G/5G з метою зменшення енергоспоживання IBN мережі рівнем радіодоступу. Зокрема пропонується, коли базові станції не обслуговують жодного користувача слід їх переводити у режим енергозбереження і тим самим формувати структуру RAN (Radio Access Network), яка буде підлаштовуватися під потреби користувачів, тобто параметри рівня радіодоступу будуть адаптивно змінюватися залежно від замовленого рівня якості обслуговування [225,226]. Для повноцінного підвищення енергоефективності IBN мережі необхідно аналогічну процедуру забезпечити як на рівні серверів в процесі організації віртуальних машин VM, так і на рівні мережі (енергоефективна QoE-маршрутизація, розділ 2), при цьому використовуючи мінімальну кількість мережевих вузлів із забезпеченням вимог щодо замовленої якості обслуговування користувачів (рис.5.32).

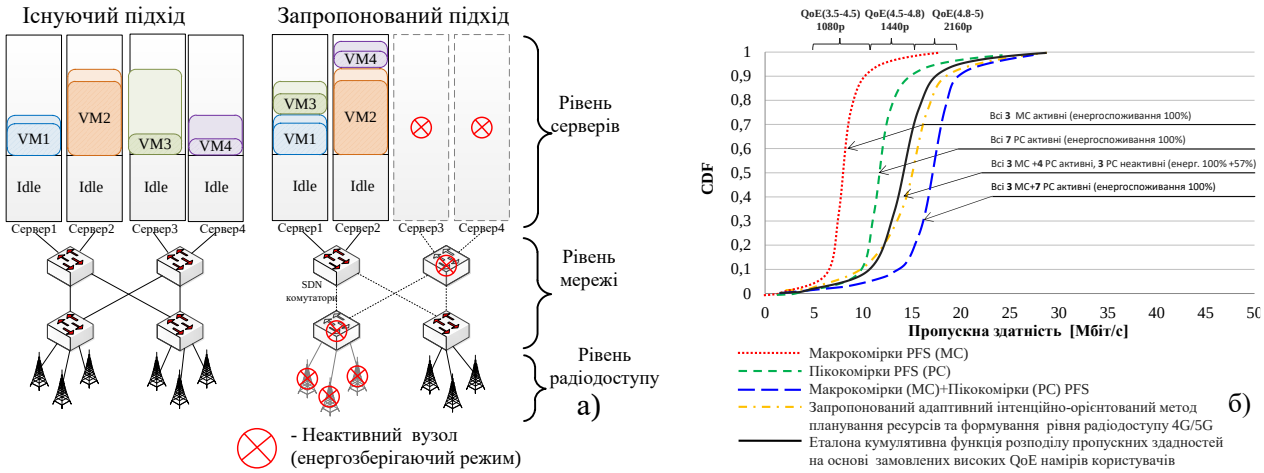


Рис.5.32. Принцип методу розподілу ресурсів та формування структури рівня радіодоступу в IBN для підвищення енергоефективності мережі – а), порівняння кумулятивних функції розподілу пропускних здатностей користувачів в умовах різної кількості активних базових станцій – б) (в умовах використання запропонованого та існуючих методів розподілу радіоресурсів)

Для кількісної оцінки ефективності використання розробленого методу розподілу ресурсів в мережах 4G/5G у роботі сформовано критерій якості обслуговування користувачів Q, який також може бути використаний для операторів мобільного зв'язку в процесі оптимізації мережі:

$$Q = \frac{\sum_{QoE=1}^{5} \sum_{i=1}^{Наб_{\cdot QoE}} Y_{iQoE_{поточна}} \left(P_{ціна\,QoE.поточна} \right)}{\sum_{QoE=1}^{5} \sum_{i=1}^{Наб_{\cdot QoE}} Y_{i_{QoE.потреб}} \left(P_{ціна\,k.max} \right)}, \tag{5.38}$$

де $Y_{iQoE_{поточна}}$ – пропускна здатність, що надана i-му абоненту QoE-ї категорії, $P_{ціна\,QoE.поточна}$ – ціна сервісу абонента в залежності від швидкості, яка йому надана, $P_{ціна\,k.max}$ – максимально можлива ціна сервісу абонента, $Y_{i_{QoE.потреб}}$ – швидкість, яку потребує i-й абонент для QoE-ї категорії.

$$Y_{iQoE_{поточна}} = (N_{RB} \cdot m \cdot n \cdot MIMO \cdot Kod_{RATE} \cdot \log 2(Modul)) \cdot S \tag{5.39}$$

де (S) відсоток корисних даних в кадрі ($S=0.75$), число виділених ресурсних блоків (N_{RB}) на протязі секунди, кількість ресурсних елементів ($m=12$ –

кількість піднесучих, *n=7* – кількість символів), кількість антен, швидкість коду Kod_{RATE}, позиційність модуляції *log2(Modul).*

Нормоване значення критерію *Q* змінюється від 0 до 1, де вище значення означає кращу якість обслуговування та розраховується як середнє значення для кожної зони із 9 комірок (від 1 до 16), що характеризують певний рівень індикатора якості каналу CQI в умовах використання різної ширини каналу від 0.2 до 20 МГц (рис.5.33).

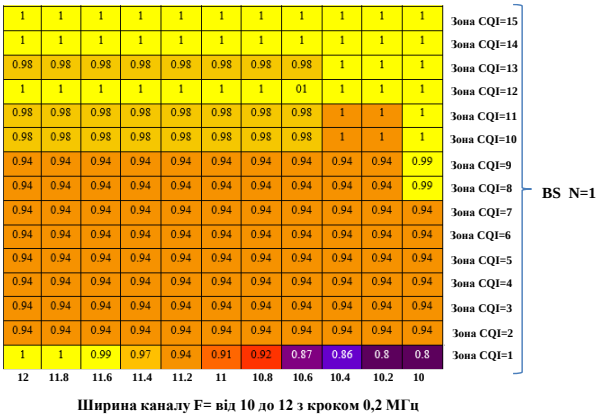
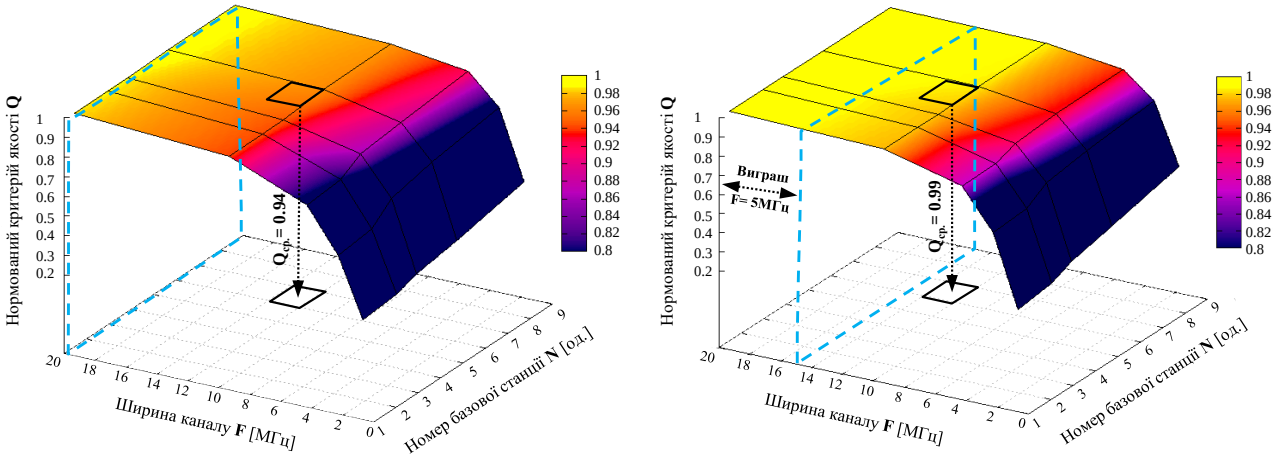


Рис.5.33. Принцип оцінки середнього значення нормованого критерію якості Q для користувачів, що розподілені по різних зонах CQI однієї базової станції (BS) в залежності від зміни ширини каналу F



а) б)

Рис.5.34. Традиційні методи управління ресурсами (оцінка критерія якості *Q*) – а) та пропоновані методи управління ресурсами (оцінка критерія якості *Q*)– б)

На рис. 5.34а показано, що для забезпечення високого рівня замовленої якості обслуговування у мережі із 9 базових станцій, що відповідає значенню Q=1, оператору мережі необхідно мати ширину каналу 20 МГц із існуючими методами розподілу радіоресурсів, та 15 МГц із запропонованим (рис. 5.34б). Таким чином, на основі проведеного дослідження встановлено, що розроблений адаптивний інтенційно-орієнтований метод розподілу ресурсів та формування структури рівня радіодоступу мереж 4G/5G дав змогу ефективніше на 25 % використовувати наявні частотно-часові ресурси та зменшити на 8,7% енергоспоживання мережі рівня радіодоступу (рис.5.32б) для забезпечення замовленої якості обслуговування користувачів у порівнянні із традиційними методами. І навпаки, в умовах використання однакової ширини каналу забезпечується краща якість обслуговування згідно вимог користувачів при використані запропонованого методу. Підтвердженням цього є отриманий результат показаний на рис. 5.34, зокрема, у базовій станції під номером №7 при різних варіантах використання ширини каналу (від 12 до 14 мГц) середній показник нормованого критерію якості обслуговування користувачів становить Q=0.94 (рис.5.34а) в умовах використання традиційного методу розподілу ресурсів, де при цьому самому сценарію моделювання при використанні запропонованого методу середній показник нормованого критерію якості обслуговування користувачів становить Q=0.99 (рис.5.34б).

5.3. Синтез гетерогенної інтенційно-орієнтованої мережі для організації віртуальних сегментованих мереж різного призначення

Важливим останнім етапом синтезу гетерогенної інтенційно-орієнтованої мережі є розроблення методу наскрізної віртуалізації ресурсів інформаційно-комунікаційної інфраструктури. Використання даного підходу для національних операторів мереж дасть змогу автоматично розгортати в межах однієї інфраструктури мережі різного призначення та забезпечити адаптивну якість надання послуг певній групі бізнес-користувачів. Віртуалізація

програмно-конфігурованого вузла інформаційної інфраструктури згідно запропонованої концепції IBN передбачає створення двох або більше віртуальних аналогів в межах фізичного обладнання, зокрема для рівня радіодоступу, транспорту та серверів (базових станцій A_i, комутаторів/маршрутизаторів B_i та серверів C_i).

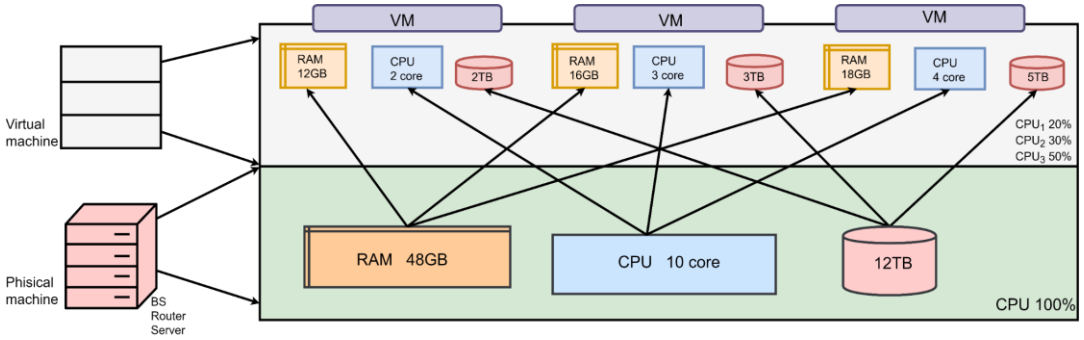
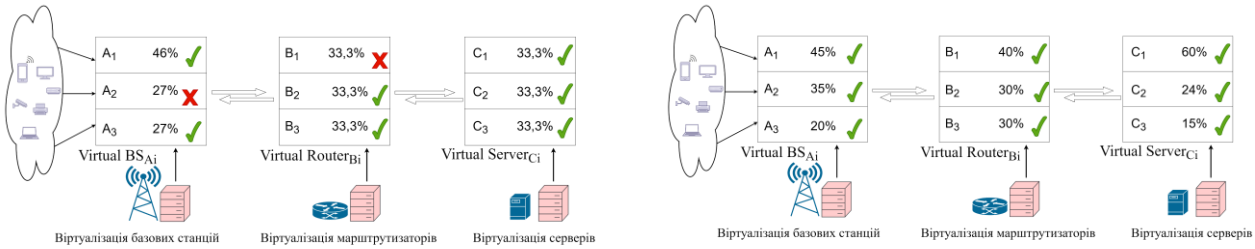


Рис.5.35. Спрощена схема віртуалізації елементів мережі з динамічним розподілом ресурсів

Кожен із розгорнутих віртуальних сегментів призначений для індивідуального обслуговування інформаційних потоків з необхідним рівнем QoS згідно сформульованих мінливих вимог користувачів, шляхом міжрівневого узгодження пулу обчислювальних ресурсів CPU, RAM, Buffer Capacity мережевих пристроїв [228]. Під обчислювальними ресурсами розуміються апаратні ресурси серверної машини, на якій з допомогою технології NFV організовується функціональність певного мережевого елемента (базових станцій, комутаторів/маршрутизаторів та серверів). Продуктивність віртуальної машини залежить від обсягу виділених фізичних ресурсів, зокрема чим більше ресурсів виділено для віртуальної машини тим більша буде швидкість оброблення даних. У роботі запропоновано структурно-функціональну модель вузла IBN мережі з динамічною віртуалізацією обчислювальних ресурсів, яка дає змогу описати процес віртуалізації базових станцій, маршрутизаторів, серверів в мережах наступного за оптимізацією заданого рівня параметрів для визначених типів сервісу з набором властивих їм

вимог до забезпечення QoS та QoE [230]. Статичний та динамічний розподіл ресурсів мережевої інфраструктури за допомогою технологій віртуалізації показано на рис. 5.36.



а) б)

Рис.5.36. Існуючий статичний розподіл ресурсів мережевої інфраструктури за допомогою віртуалізації – а) та запропонований динамічний розподіл ресурсів мережевої інфраструктури – б)

Новизною такого підходу синтезу концептуальної мережі IBN з допомогою технології віртуалізації є те, що у централізований IBN/SDN контролер мережі вводиться головний блок менеджера управління ресурсами. Даний блок розробляється з метою забезпечення адаптивного розгортання сегментованих мереж різного призначення та різної продуктивності в межах однієї фізичної інфраструктури, враховуючи при цьому вимоги щодо якості надання послуг.

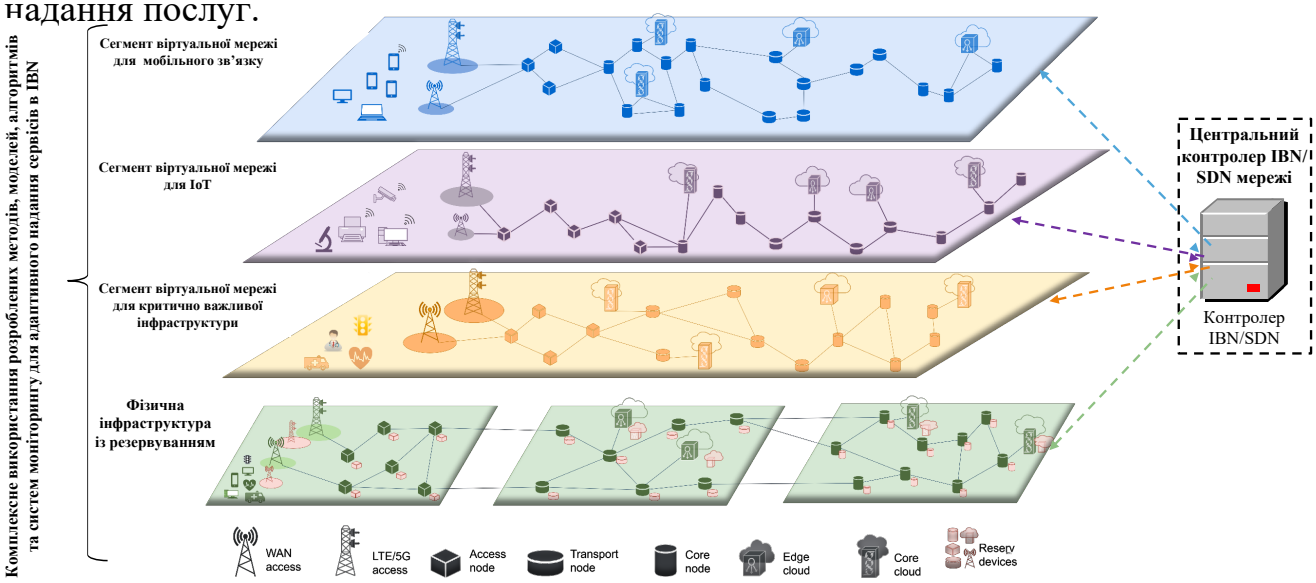


Рис.5.37. Архітектура синтезованої інтенційно-орієнтованої гетерогенної мережі з віртуалізацією ресурсів

Таким чином, на основі розроблених у попередніх розділах роботи нових методів управління якістю надання послуг, розподілом ресурсів, енергоефективністю мережі, захищеністю передавання даних та наскрізної віртуалізації ресурсів, вперше запропоновано ***методологію синтезу гетерогенної інтенційно-орієнтованої мережі***, згідно якої можна інтелектуально виділяти зв'язки між структурно-функціональними елементами мережі, які можуть не тільки автоматизовано перебудовуватись з різною продуктивністю, але й виникати заново, вишукуючи шляхи найбільш адекватного пристосування до мінливих вимог користувачів щодо адаптивного надання сервісів.

Далі у роботі розглянуто більш детально процес віртуалізації мережевої інфраструктури з використанням теорії масового обслуговування та засобів середовища моделювання SimEvents програмної системи Matlab.

5.3.1. Метод адаптивного управління структурно-функціональними параметрами вузлів IBN інфраструктури в умовах динамічної віртуалізації ресурсів

У роботі запропоновано структурно-функціональну модель вузла мережі (з статичною та динамічною віртуалізацією обчислювальних ресурсів [230], яка дозволяє описати процес динамічної віртуалізації базових станцій, маршрутизаторів, серверів в мережах наступного за оптимізацією заданого рівня параметрів для визначених типів сервісу з набором властивих їм вимог до забезпечення QoS та підвищити надійність мережі. При такому проектуванні підвищується стійкість мережі до кібер атак, оскільки в умовах атаки на віртуалізований мережевий пристрій відбудеться перевантаження лише віртуальної машини, що обробляє замасковану під потік атаку. Розглянемо процес функціонування запропонованої моделі пристрою з віртуалізацією ресурсів (рис.5.38).

На рис. 5.38 для прикладу показано процес адаптивного управління обчислювальними ресурсами мережевого пристрою за критерієм середнього часу затримки пакетів від завантаження віртуальних маршрутизаторів в умовах статичного та динамічного виділення ресурсів.

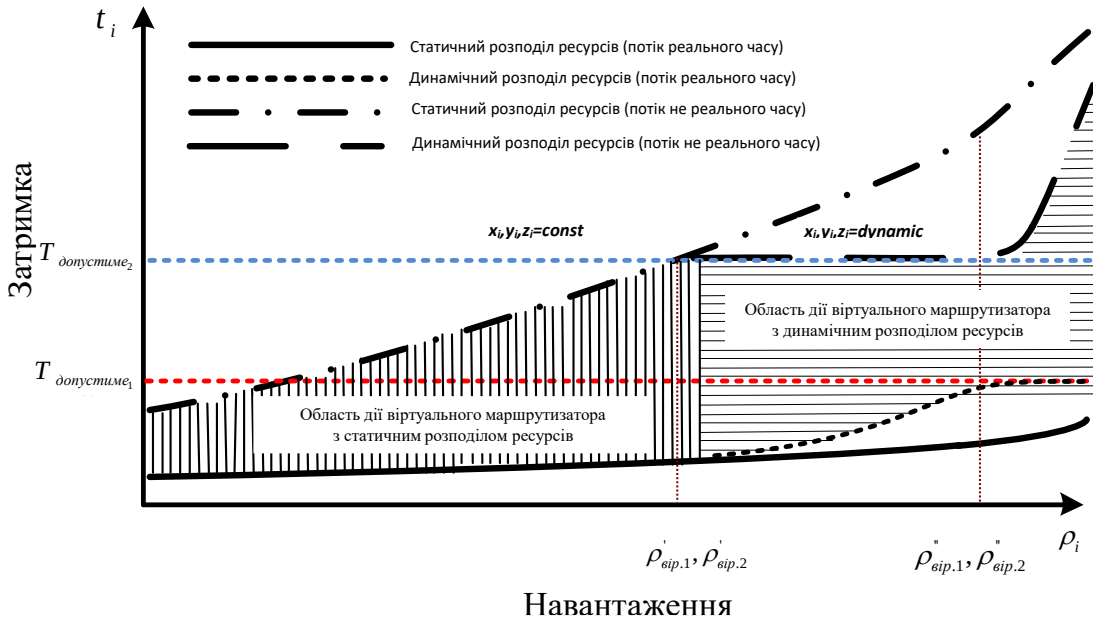


Рис.5.38 Процес адаптивної віртуалізації вузла (маршрутизатора) за оптимізацією затримки обслуговування послуг в умовах статичного та динамічного розподілу обчислювальних ресурсів [231]

Відповідно для простоти формалізації трафік можна розділити на два класи $K = 2$. Припустимо, що затримка для пакетів першого класу (чутливого до затримок) t_1 у віртуальному вузлі не повинна перевищувати допустиме значення $T_{допустиме_1}$, відповідно умова дотримання необхідного рівня якості обслуговування за критерієм затримки $(t_1 \le T_{допустиме_1})$. Затримка пакетів для другого класу t_2 (трафіку не чутливого до затримок) не повинна перевищувати $T_{допустиме_2}$, відповідно умова гарантованого рівня QoS у віртуальному вузлі призначеного для нечутливого до затримок виглядатиме, як $(t_2 \le T_{допустиме_2})$. Тоді в умовах низького навантаження $(\rho_{i1} \le \rho'_{вір.1}), (\rho_{i2} \le \rho'_{вір.2})$ на віртуальні вузли першого та другого класу в i - й момент часу при статичному розподілі

обчислювальних ресурсів, задовольняються всі вимоги щодо якості обслуговування потоків всіх пріоритетів. При високому навантаженні $(\rho'_{вір.1} \le \rho_{i1} \le \rho''_{вір.1}), (\rho'_{вір.2} \le \rho_{i2} \le \rho''_{вір.2})$ в певні моменти часу виникають ситуації коли $(t_2 \ge T_{допустиме_2})$ та $(t_1 \ge T_{допустиме_1})$. В такому разі потрібно застосовувати динамічний розподіл ресурсів, що дасть змогу покращити параметри QoS. Шляхом моніторингу QoS проводиться перерахунок параметрів обчислювальних ресурсів CPU, RAM, Buffer capacity мережевого пристрою, з метою їх адаптивного розподілу між класовими віртуальними вузлами [29].

У роботі запропоновано умову адаптивного управління обчислювальними ресурсами структурно-функціонального мережевого вузла з віртуалізацією ресурсів для забезпечення необхідної якості обслуговування інформаційних послуг. Забезпечити динамічний характер процесу управління обчислювальними ресурсами в межах запропонованого підходу віртуалізації мережевої інфраструктури можливо шляхом введення керуючих змінних $<a_i, b_i, c_i>$, $<x_i, y_i, z_i>$, $<k_i, l_i, m_i>$, які відповідають за частку виділених обчислювальних ресурсів із загального пулу в процесі віртуалізації i - го віртуального вузла (базової станції, маршрутизатора, сервера). Згідно фізичного змісту $<a_i, b_i, c_i>$, $<x_i, y_i, z_i>$, $<k_i, l_i, m_i>$ мають місце наступні умови:

$$\begin{cases} a_i, b_i, c_i \in \{0,1\} \rightleftarrows Virtual_{BS}, \ де \ \sum_{i=1}^{n} x_i = 1, \sum_{i=1}^{n} y_i = 1, \sum_{i=1}^{n} z_i = 1 \\ x_i, y_i, z_i \in \{0,1\} \rightleftarrows Virtual_R, \ де \ \sum_{i=1}^{n} a_i = 1, \sum_{i=1}^{n} b_i = 1, \sum_{i=1}^{n} c_i = 1 \\ k_i, l_i, m_i \in \{0,1\} \rightleftarrows Virtual_S, \ де \ \sum_{i=1}^{n} k_i = 1, \sum_{i=1}^{n} l_i = 1, \sum_{i=1}^{n} m_i = 1 \end{cases} \quad (5.40)$$

де a_i, x_i, k_i описує Buffer capacity, b_i, y_i, l_i – CPU, c_i, z_i, m_i – RAM, n – кількість віртуальних вузлів.

Сума довжин віртуальних черг, процесорної ємності та оперативної памяті віртуальних вузлів у критичному випадку не може перевищувати загального розміру буфера, процесора та оперативної пам’яті фізичного вузла без віртуалізації.

$$\begin{cases} \sum_{i=1}^{n} a_i \cdot q_{черги_i} \le Q_{буф\,BS}, \sum_{i=1}^{n} x_i \cdot q_{черги_i} \le Q_{буф\,R}, \sum_{i=1}^{n} k_i \cdot q_{черги_i} \le Q_{буф_S}, \\ \sum_{i=1}^{n} b_i \cdot q_{черги_i} \le CPU_{BS}, \sum_{i=1}^{n} y_i \cdot q_{черги_i} \le CPU_R, \sum_{i=1}^{n} l_i \cdot q_{черги_i} \le CPU_S, \\ \sum_{i=1}^{n} c_i \cdot q_{черги_i} \le RAM_{BS}, \sum_{i=1}^{n} z_i \cdot q_{черги_i} \le RAM_R, \sum_{i=1}^{n} m_i \cdot q_{черги_i} \le RAM_S, \end{cases} \quad (5.41)$$

де $q_{черги_i}$ – довжина віртуальних черг; $Q_{буф}$ –обсяг буферної пам'яті; CPU_i – частота процесора i-го віртуального вузла; CPU – номінальна частота процесора фізичного вузла; CPU_i – частота процесора i-го віртуального вузла; RAM – оперативна пам'ять фізичного вузла; RAM_i – оперативна пам'ять i-го віртуального вузла.

$$\begin{cases} t_{поточне_i} \le T_{допустиме_i} \\ p_{поточне_i} \le P_{допустиме_i} \\ dt_{поточне_i} \le dT_{допустиме_i} \end{cases} \Rightarrow \begin{cases} a_i \cdot RAM_i + x_i \cdot RAM_i + k_i \cdot RAM_i, \in RAM \\ b_i \cdot CPU_i + y_i \cdot CPU_i + l_i \cdot CPU_i, \in CPU \\ c_i \cdot q_{черги\,i} + z_i \cdot q_{черги\,i} + m_i \cdot q_{черги\,i}, \in q_{черги\,i} \end{cases} \quad (5.42)$$

де $t_{поточне_i}$ – поточна затримка буферизації потоку в i-ому віртуальному вузлі; $T_{допустиме_i}$ – допустима затримка потоку в i-ому віртуальному буфері вузла згідно встановлених рекомендації; $p_{поточне_i}$ – імовірність відкидання даних в буфері i-го віртуального вузла; $P_{допустиме_i}$ – допустимі втрати потоку у i-ому віртуальному буфері вузла згідно встановлених рекомендацій; $dt_{поточне_i}$, – поточний джитер буферизації потоку в i-ому віртуальному вузлі; $dT_{допустиме_i}$ – допустимий джитер потоку у i-ому віртуальному буфері вузла згідно встановлених рекомендацій.

В результаті, при подальшому збільшенні навантаження $(\rho'_{вір.1} \le \rho_{i1} \le \rho''_{вір.1}), (\rho'_{вір.2} \le \rho_{i2} \le \rho''_{вір.2})$ на вузол мережі в умовах динамічного розподілу ресурсів в певні моменти часу, середня затримка даних послуг нереального часу фіксується і відповідає висунутим вимогам $(t_2 = T_{допустиме_2})$, на відміну від статичного ресурсного розподілу, коли не дотримуються вимоги щодо затримки даного потоку. При цьому збільшується затримка послуг реального

часу t_1, проте $(t_1 \le T_{допустиме_1})$. В умовах високого навантаження на мережевий пристрій, коли $(\rho_{i1} \ge \rho^{"}_{вір.1}),(\rho_{i2} \ge \rho^{"}_{вір.2})$ аналогічно проводиться перерозподіл ресурсів між віртуальними вузлами класового обслуговування з метою не допустити виходу за межі норм середнього часу перебування першого класу послуг реального часу $(t_1 \le T_{допустиме_1})$, проте в таких умовах зростає затримка послуг нереального часу, як правило не погіршуючи якість сприйняття послуг кінцевими користувачами.

5.3.2. Моделювання процесу синтезу гетерогенної інтенційно-орієнтованої мережі для організації віртуальних сегментованих мереж різного призначення

Мережевий вузол з віртуалізацією згідно теорії систем масового обслуговування (СМО) можна зобразити за допомогою каскадного включення буферної пам'яті, обслуговуючих пристроїв та менеджера ресурсів (гіпервізора) [232]. Втрати продуктивності на обслуговування гіпервізора є невисокі, проте для розроблення аналітичної моделі віртуалізованого мережевого пристрою необхідно врахувати вплив віртуалізації на продуктивність системи в залаженості від використовуваної технології віртуалізації в процесі проектування корпоративних мереж. Відповідно у роботі вперше запропоновано використати коефіцієнт впливу віртуалізації на продуктивність системи - κ. Поведінка трафіку мультисервісної IP-мережі характеризується різними законами розподілу і тому при віртуалізації мережевого пристрою кожен віртуальний вузол працює із своїм класом послуг, кожен з яких описується відповідною функцією розподілу інтервалів між подіями (пакетів, запитами) та функцією розподілу тривалості обслуговування.

Зокрема у роботах [230-232] розроблено імітаційну модель маршрутизатора за допомогою компонент SimEvents програмної системи Matlab. Для реалізації дискретно-подієвого моделювання в середовищі Simulink

використовується компонента SimEvents. За допомогою SimEvents можна моделювати і проектувати розподілені системи управління, апаратні конфігурації, мережі передачі і збору інформації.

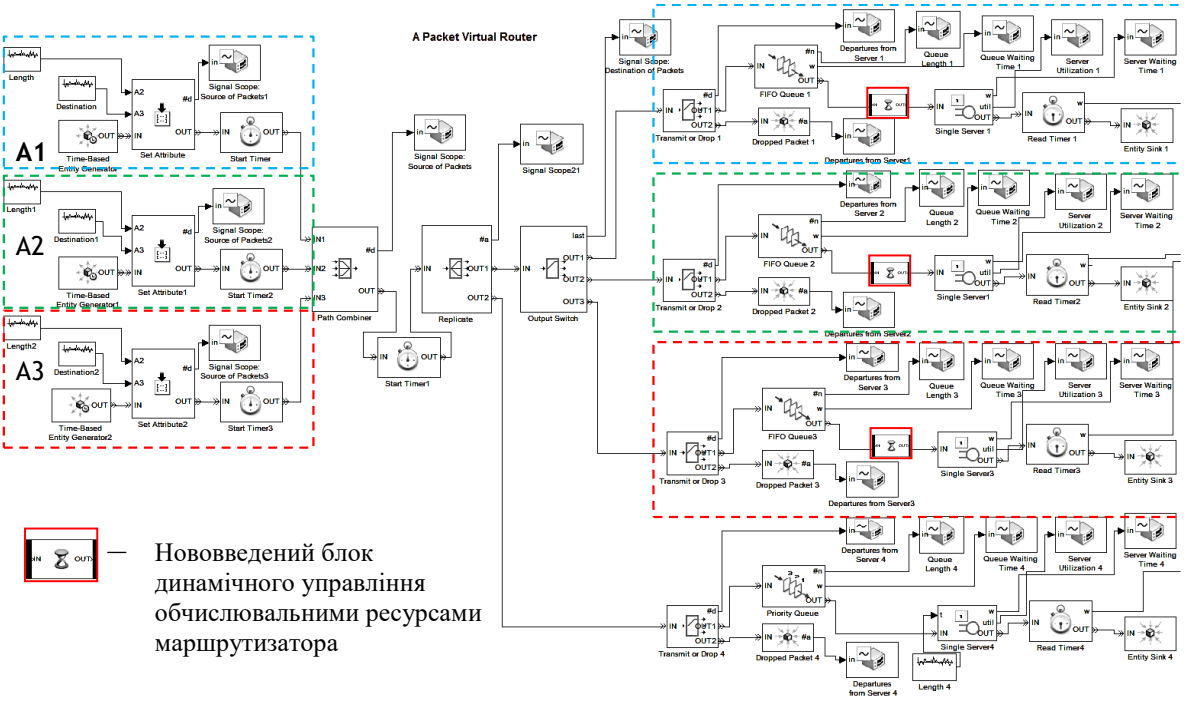


Рис.5.39. Схема моделі пакетного маршрутизатора з динамічною віртуалізацією ресурсів (1,2,3) та без віртуалізації з пріоритетною обробкою черг

В роботі наведено програмні коди для блоків *Schedule priority flow delay*, що відповідають за аналіз пріоритеів вхідних пакетів та їх розподіл по затримках пакетів. Порівняння тривалостей обслуговування пакетів в маршрутизаторі з використанням пріоритетів та із статичною віртуалізацією ресурсів мережевого пристрою показано на рис.5.40а.

Як бачимо у порівнянні з пріоритетним обслуговуванням пакетів, для статичної віртуалізації при голосовому потоці результат по затримці буде гіршим, оскільки під час пріоритетного обслуговування найвищим пріоритетом володіють пакети голосу та підлягають першочерговому обслуговуванню. Відповідно трафік даних та відео в певні моменти часу перевищують свої допустимі норми затримок і є значно більшими у порівнянні зі тривалістю

обслуговування пакетів, яка забезпечується статичною віртуалізацією. Таким чином провівши моделювання та дослідження, встановлено, що жодна з описаних систем не гарантує достатню якість обслуговування потоків.

Наступним пунктом дослідження є порівняння результатів затримки пакетів послуг системи з динамічним розподілом ресурсів маршрутизатора (організація трьох віртуальних маршрутизаторів) та обслуговуванням пакетів за порядком пріоритетної черги PQ в одному стандартному маршрутизаторі (рис.5.40б).

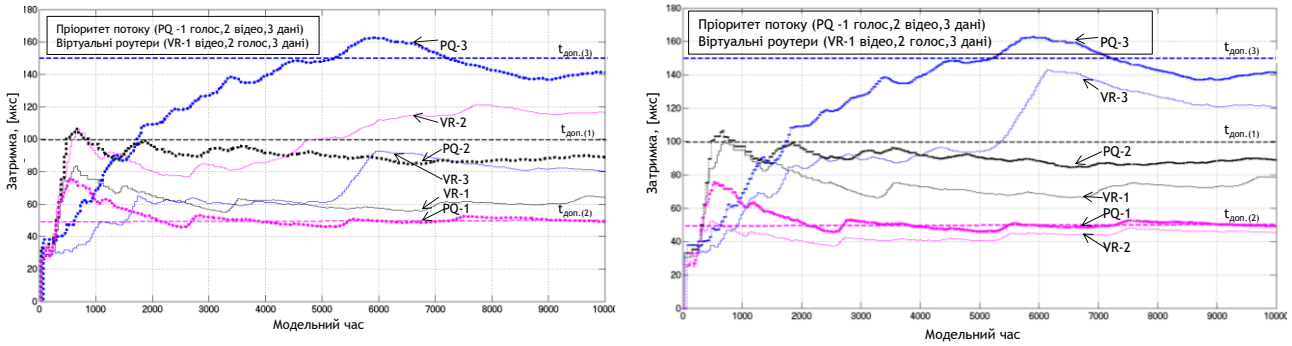


Рис.5.40. Порівняння тривалостей обслуговування пакетів в маршрутизаторі з пріоритезацією та з статичною віртуалізацією ресурсів мережевого пристрою – а) та з динамічною віртуалізацією ресурсів мережевого пристрою – б) [231]

Провівши моделювання, встановлено що система пріоритетного обслуговування інформаційних послуг не здатна забезпечити усім потокам гарантованого рівня QoS за критерієм мінімальної затримки та є менш ефективною у порівнянні із системою динамічної віртуалізації обчислювальних ресурсів мережевого пристрою.

У роботі проведено моделювання процесу синтезу гетерогенної інтенційно-орієнтованої мережі для організації віртуальних сегментованих мереж різного призначення шляхом узгодженості ефективності функціонування рівня радіодоступу, транспорту та серверного обслуговування за критерієм наскрізної затримки передавання даних. Новизною такого підходу синтезу концептуальної мережі IBN з допомогою технології віртуалізації є те, що у

моделі (рис.5.41.) розроблено блоки BS IBN Manager, Switch/router IBN Manager, server IBN Manager та головний IBN Manager, що відповідає за централізований IBN/SDN контролер мережі та виконує функції інтелектуального менеджера наскрізного узгодженого управління ресурсами. Даний блок розробляється з метою забезпечення адаптивного розгортання сегментованих мереж різного призначення та різної продуктивності в межах однієї фізичної інфраструктури, враховуючи при цьому вимоги щодо якості надання послуг.

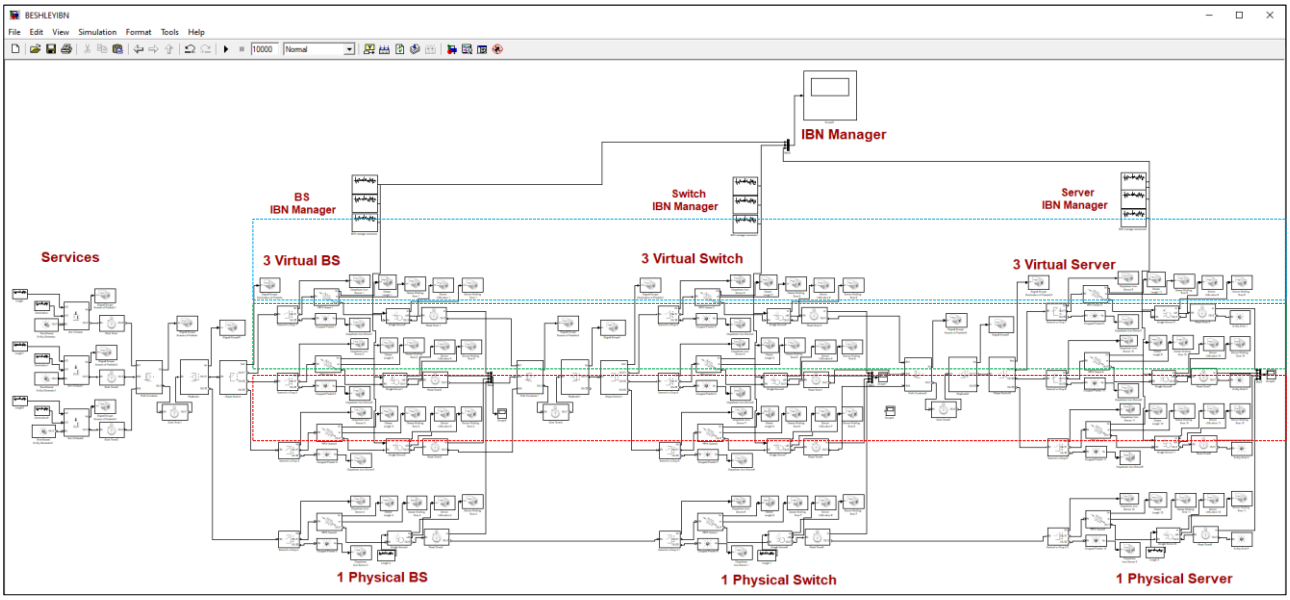


Рис.5.41. Структурно-функціональна схема імітаційної моделі гетерогенної віртуалізованої IBN мережі

Зокрема, встановлено, що в умовах статичної віртуалізації ресурсів кожній віртуальній машині надається однакова кількість ресурсів, що свою чергу може призвести до того, що коли на віртуальний вузол поступить трафік з високою інтенсивністю можуть виникнути значні затримки та втрати пакетів при обмежені кількості виділених фізичних ресурсів [92]. У роботі розглянуто різні ситуації, коли на віртуальну інфраструктуру (віртуальну машину) надходить трафік з низькою інтенсивністю, середньою та високою. Як видно з рис. 5.42 віртуальний сегмент A1, який відповідає за критично важливі сервіси Інтернету

речей не справляється із обслуговування вхідного навантаженням за критерієм забезпечення наскрізної затримки передавання даних в умовах статичного розподілу фізичних ресурсів між віртуальними машинами.

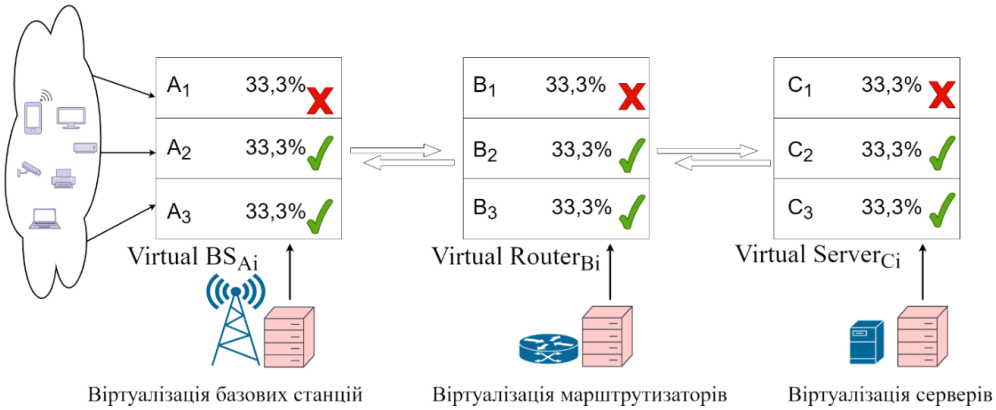


Рис. 5.42. Розподіл ресурсів мережевої інфраструктури за допомогою статичної віртуалізації при високому навантаженні

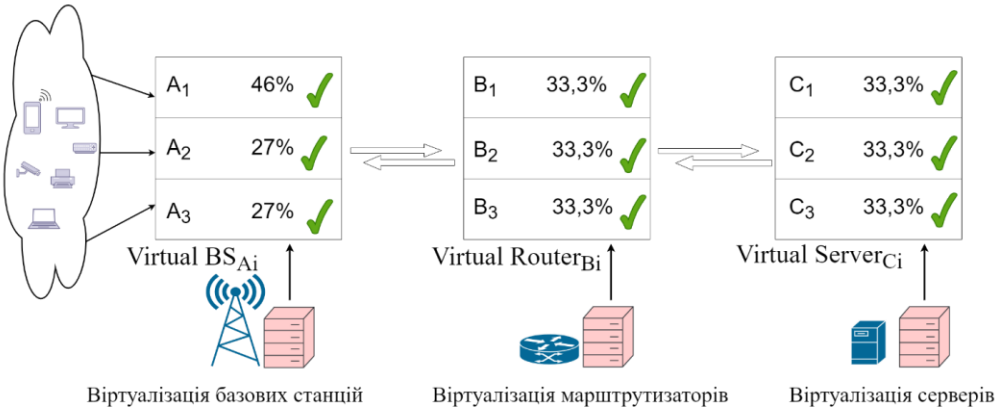
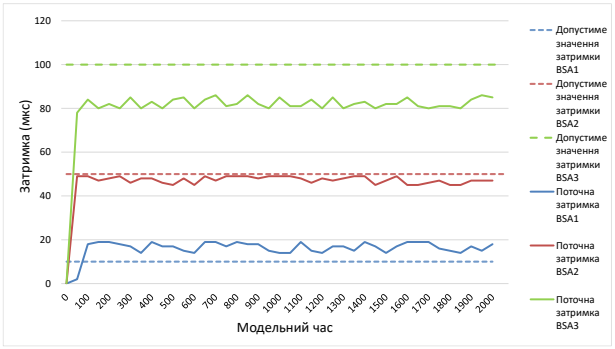
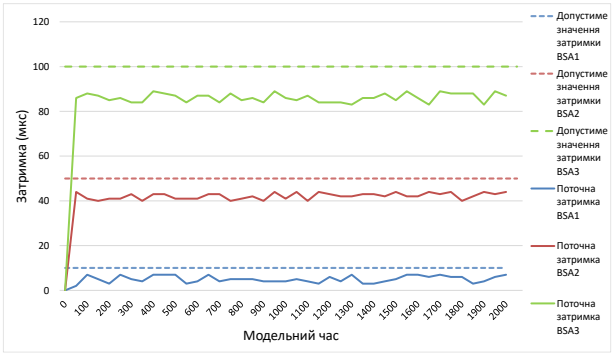


Рис.5.43. Розподіл ресурсів мережевої інфраструктури за допомогою динамічної віртуалізації при низькому навантаженні

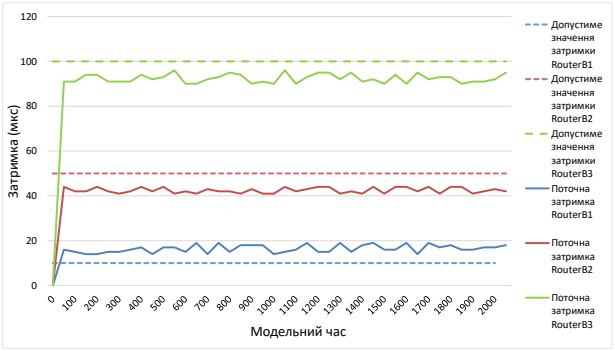
Також на графіках на рис.5.44 (а, б, в) зображено приклади графіків тривалості оброблення даних віртуального обслуговуючого пристрою на різних рівнях з яких видно, коли трафік, який відповідає за потік пакетів виходить за межі допустимого значення. Отже, відбуваються погіршення якості обслуговування абонентів, затримки та втрати даних.



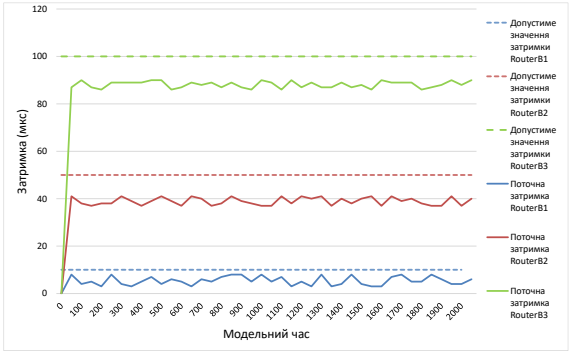
а



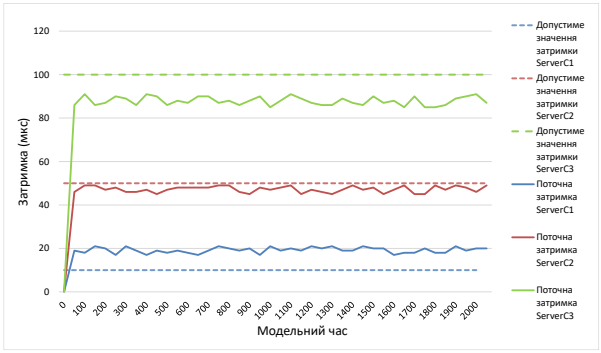
г



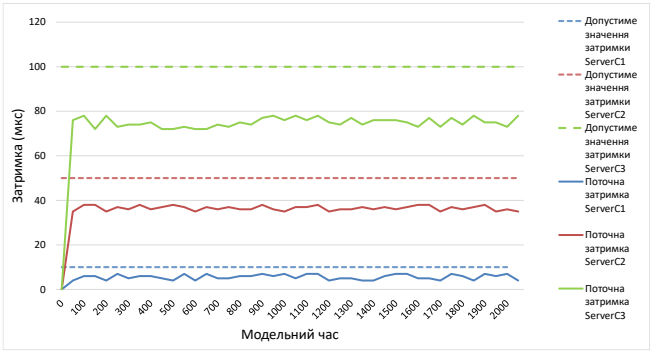
б



д



в



е

Рис.5.44. Тривалість оброблення даних віртуалізованих машин на рівні базових станцій (а), маршрутизаторів(б) та серверів (в) при високому навантаженні з існуючою статичною віртуалізацією ресурсів та на рівні базових станцій (г), маршрутизаторів(д) та серверів (е) при високому навантаженні з пропонованою динамічною віртуалізацією ресурсів

Як видно з результатів, застосування статичної віртуалізації мережевого пристрою не здатна повністю забезпечити гарантованого рівня QoS усім присутнім потокам в мережі за критерієм затримки. У випадку перевищення допустимої затримки потоками у вузлі, вважається, що сервіс зазнає

погіршення якості обслуговування за критерієм мінімальної затримки. Для того щоб оптимізувати роботу, вирішено використати динамічний розподіл ресурсів, який дає змогу управляти ресурсами гнучкіше у дані моменти часу, враховуючи вхідне навантаження.

На сьогоднішній час немає технології, яка б в процесі передавання даних динамічно змінювала б ресурси віртуальної машини без втрати даних за декілька секунд. Тобто потрібно зупинити фізичну машину, перерозподілити ресурси і наново запустити. Такий тимчасовий простій в мережі напряму відобразиться на трафіку та якості обслуговування абонентів. Також в мережі є ситуації, коли обладнання виходять з ладу. Це можуть бути як просто базові станції, так і великі сервери. Під час цього можуть втрачатись важливі дані, погіршується доступність до ресурсів мережі та відповідно втрачається довіра абонентів. Щоб не було значних втрат пропонується зробити так звану резервну «сплячу» фізичну машину, яка сконфігурована аналогічно як і активна. Оскільки Big Date (головний контролер IBN, який частково виконує функці гіпервізора) збирає дані по загальному навантаженню, можна передбачати коли віртуальні машини перевантажуються і потрібна динамічна зміна ресурсів. Для того щоб зробити практичну реалізацію, яка напрямлена для вирішення проблеми ми пропонуємо зробити «резервну фізичну мережу» (рис.5.45). Коли пристрій виходить з ладу, чи потрібно перерозподілити ресурси на віртуальній машині, саме тоді використовується резервна мережа.

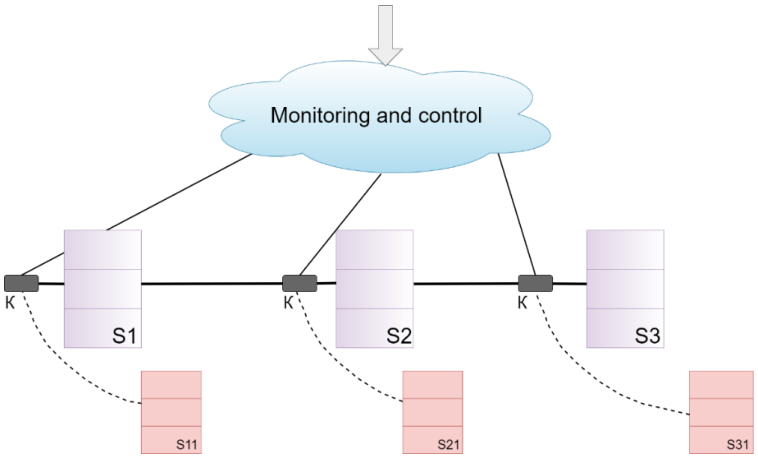


Рис.5.45. Схема фрагменту мережі з віртуалізацією та резервуванням

З допомогою концентратора на вхід поступає один потік трафіку і на виході розпаралелює на два порти. На момент перерозподілу ресурсів концентратор перекриває порт до активної машини, в той момент скріпт-файлом на «сплячу» машину надсилаються дані, які програмно активують машину з певними структурно-функціональними параметрами і машина розгортається згідно мінливого навантаження чи вимог групи користувачів. Тоді концентратор блокує порт, який з'єднаний з активною машиною і весь трафік поступає на «сплячу» машину, яка стає активною в той же самий момент часу. Коли почнеться ще один пік навантаження для динамічного перерозподілення ресурсів Big Data знову надсилає скрипт-файл на «сплячу» в той момент машину, яка розгортається згідно заданих потреб [233]. Тоді концентратор повторює свої функції, а саме: блокує порт, який з'єднаний з активною машиною і весь трафік поступає на «сплячу» машину, яка стає активною в той момент з потрібним розподілом ресурсів.

5.3.3. Систематизація та узагальнення результатів розробленої методології синтезу гетерогенної інтенційно-орієнтованої мережі

Узагальнюючи отримані результати в процесі синтезу мережі встановлено, що прикладна частина методології являє собою інформаційну IBN технологію адаптивного управління параметрами та розподілом трафіку мережі. На основі запропонованої методології, яка включає в собі розроблені нові принципи, моделі, методи та алгоритми вирішується проблема взаємодії технічних і програмних засобів при реалізації інтелектуального управління інфраструктурою мережі, розподілом трафіку, мережевою безпекою, організації збору, обробки та передавання інформації. Загальна схема проведеного системного аналізу складних гетерогенних інфокомунікаційних систем в процесі синтезу інтенційно-орієнтованих мереж показано на рис.5.46.

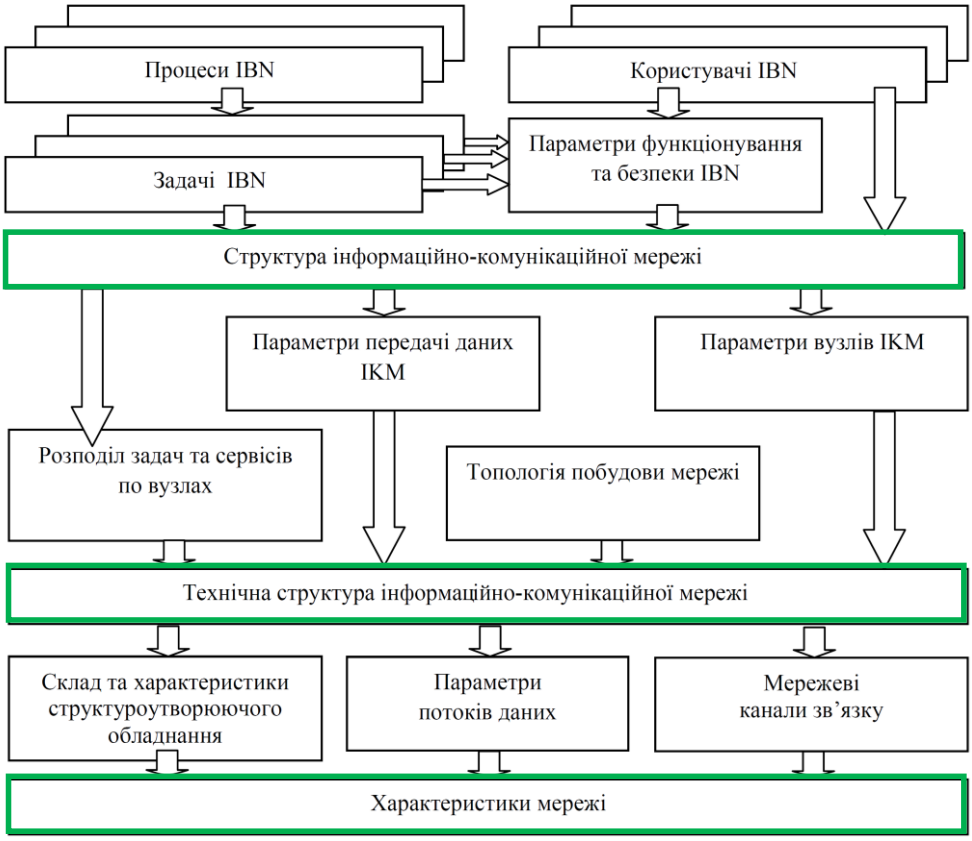


Рис.5.46. Загальна схема проведеного системного аналізу складних гетерогенних інфокомунікаційних систем в процесі синтезу інтенційно-орієнтованих мереж

В результаті проведеного аналізу та розроблених нових рішень побудовано архітектуру запропонованої синтезованої гетерогенної IBN мережі, яка умовно складається з шести горизонтальних площин [234]: площина доступу, площина ядра, площина управління та площина штучного інтелекту, площина користувачів, а також однієї вертикальної площини інтелектуального моніторингу та управління інфраструктурою (рис.5.47).

Площина користувачів відповідає за індивідуалізацію обслуговування клієнтів шляхом врахування замовлених QoE оцінок, що дає змогу кінцевим користувачам сервісів опосередковано впливати на функціональну конфігурацію мережі, а з допомогою машинного навчання підкласу площини штучного інтелекту реагувати на несприятливі поєднання значень показників

якості і попереджати ситуації, коли користувач незадоволений якістю отриманих сервісів для адаптивного прогнозування моменту переконфігурації мережі.

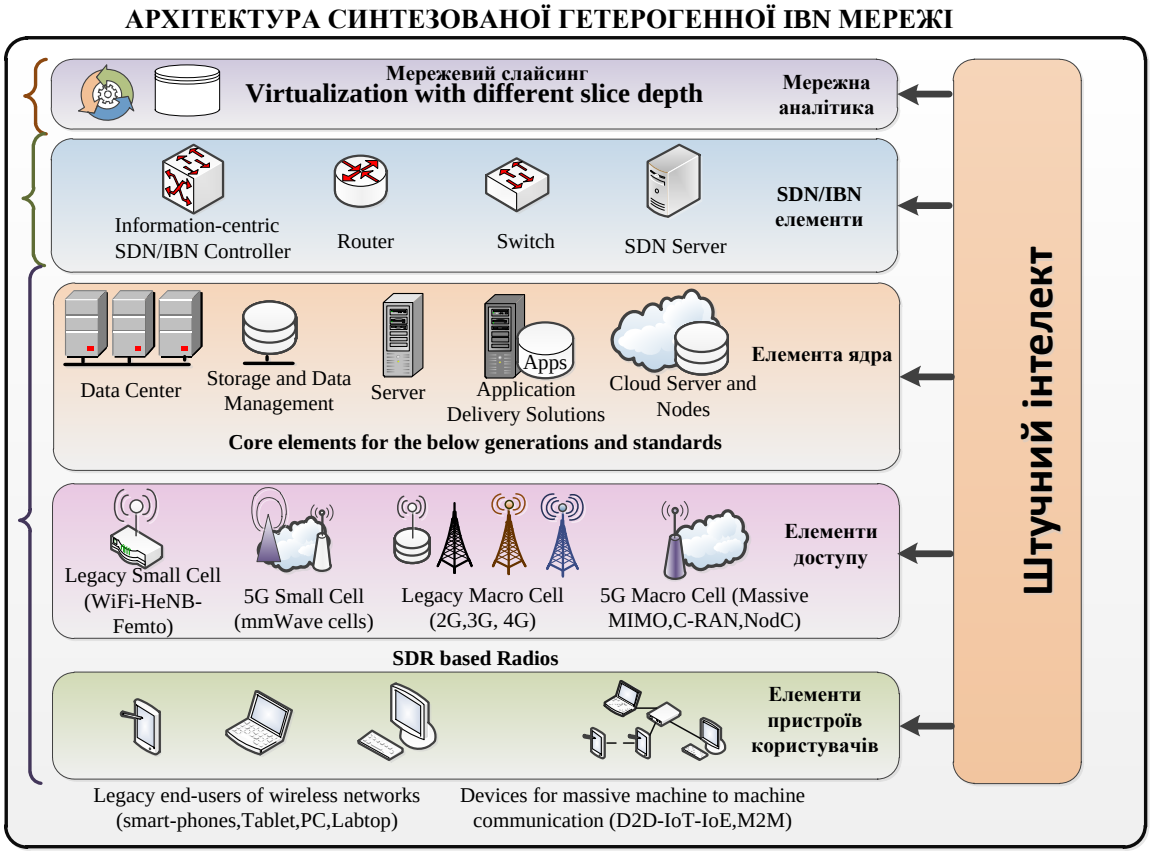


Рис.5.47. Багаторівнева архітектура синтезованої гетерогенної IBN мережі в межах концепції Future Network [235]

Площина доступу відповідає за безпосереднє надання сервісів кінцевим користувачам з використанням фізичної мережної інфраструктури фіксованого та мобільного абонентського доступу. До функцій даної площини відноситься передавання сигналів у фізичних каналах зв'язку, зокрема обробка сигналів, кодування даних, модуляція, тощо. Конфігурація фізичної мережної інфраструктури визначається шляхом синхронізації параметрів фізичних пристроїв із їх віртуалізованими абстракціями [236].

Площина ядра охоплює основні аспекти процесу передавання пакетного трафіку в гетерогенній мережі. Вона охоплює сервісні шлюзи, маршрутизатори

та комутатори, а також відповідає за агрегацію трафіку, управління мобільністю користувачів, функціональні можливості AAA (Authentication, Authorization and Accounting – аутентифікація, авторизація та білінг. Важливим компонентом даної площини є віртуалізація мережних функцій (NFV), зокрема: віртуалізація мережних пристроїв, віртуалізація канальних ресурсів та віртуалізація композитних сервісів. На основі технології NFV синтезується віртуальна абстракція фізичної мережної інфраструктури, конфігурація якої синхронізується із конфігурацією фізичної мережної інфраструктури [237-239].

Площина управління відповідає за прийняття рішень в режимі реального часу стосовно основних параметрів функціонування гетерогенної мережі. В основі даної площини є контролер IBN/SDN, який виконує функції управління ресурсами, управління мобільністю користувачів, балансування навантаження, контроль розгортання мережі для клієнт-орієнтованого надання сервісів, маршрутизацію інформаційних потоків та наскрізний контроль за забезпеченням об’єктивних та суб’єктивних параметрів якості сервісу (E2E QoS-QoE)[240-243]. На основі усіх вищезгаданих чинників, IBN/SDN контролер адаптивно визначає конфігурацію віртуальної гетерогенної мережної інфраструктури для клієнт-орієнтованого надання сервісів кінцевим користувачам.

Площина мережної аналітики складається з високопродуктивних серверів і баз даних, які використовуються для збирання та аналізу великих даних з усіх рівнів функціонування гетерогенної мережі IBN мережі. Запропонована система мережної аналітики функціонує на основі крос-рівневого асинхронного збору даних про основні параметри та характеристики функціонування мережних елементів із прив’язкою до часових та територіальних метаданих. Система дає змогу збирати будь-які дані у текстовій, числовій та графічній формі. Дана особливість відкриває великі можливості для операторів з точки зору налаштувань системи моніторингу DPI відповідно до їх вимог у цільовій області розгортання мережі та надання сервісів. Крім того, дана система дає

змогу знизити кількість службової інформації в каналах зв’язку оператора за рахунок невеликого обсягу переданих даних. В кінцевому результаті на даному рівні аналізуються рішення про динамічну віртуалізацію мережевої інфраструктури для організації логічно ізольованих сегментованих мереж певного призначення [244].

Вертикальна площина штучного інтелекту відповідає за формування бази знань про основні параметри та характеристики функціонування гетерогенної інтенційно-орієнтованої мережної інфраструктури з використанням інтелектуальних алгоритмів машинного навчання. На даному рівні використовується інформація отримана із системи моніторингу мережі, зокрема дані про якість зв’язку та задоволеність рівнем сервісу з боку кінцевих користувачів, інформація про завантаженість мережних вузлів, несправність елементів фізичної інфраструктури, а також довготривала статистика поведінки кінцевих користувачів та характеристики функціонування гетерогенної мережної інфраструктури. Отримана інформація передається на площину управління, де використовується для прийняття більш ефективних рішень, які б враховували попередній досвід системи та відповідно формують правила для головного контролера мережі.

На сьогоднішній час цифровий розвиток передбачає виконання комплексу завдань, що позитивно вплинуть на економіку, бізнес, суспільство та життєдіяльність країни в цілому на основі розгортання новітніх цифрових інфраструктур [245]. Цифрові інфраструктури це комплекс технологій, продуктів та процесів, що забезпечують обчислювальні, телекомунікаційні та мережеві можливості на цифровій основі. Цифрові інфраструктури є основою цифрової економіки. Майбутня концепція розвитку цифрової економіки та суспільства на основі інтеграції трендових інформаційно-комунікаційних технологій та використання запропонованої методології синтезу IBN показано на рис.5.48.

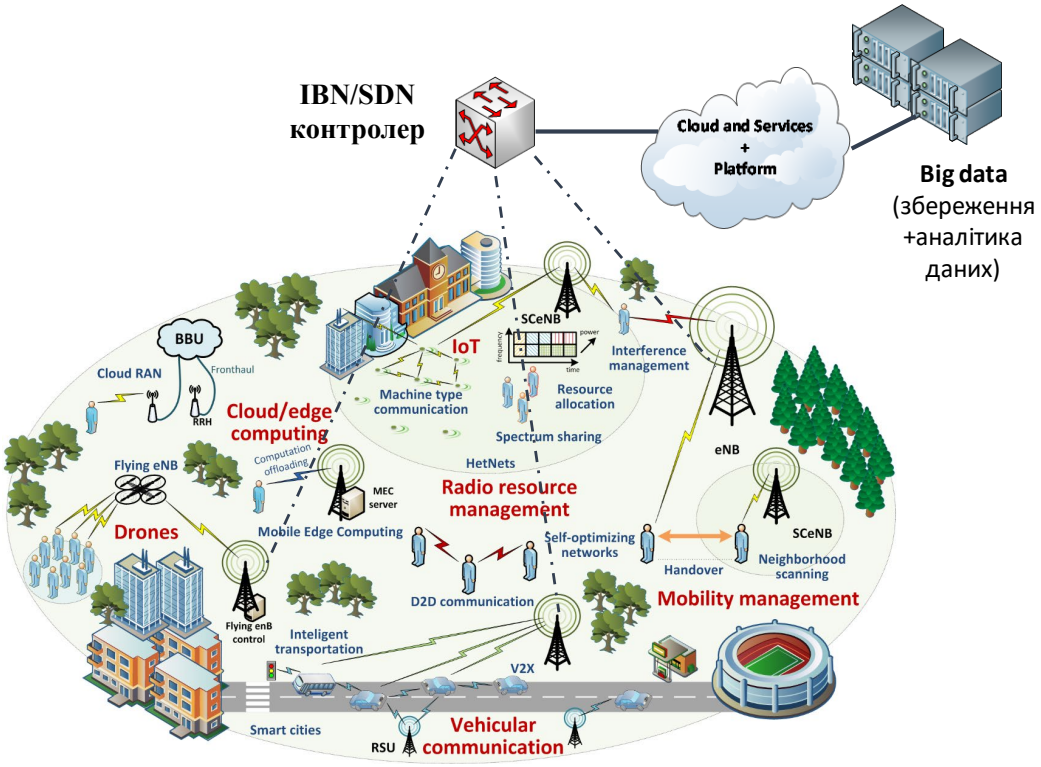


Рис 5.48. Майбутня концепція розвитку цифрової економіки та суспільства на основі інтеграції трендових інформаційно-комунікаційних технологій та використання запропонованої методології синтезу IBN

Таким чином, впровадження інтенційно-орієнтованих мереж для повсюдного компютингу дасть змогу забезпечити прискорений сценарій цифрового розвитку, як найбільш релевантного питання для світу та України з точки зору викликів, потреб та можливостей.

5.4. Висновки до 5-го розділу

1. У цьому розділі роботи розглядаються основні аспекти синтезу рівня радіодоступу гетерогенної IBN мережі для адаптивного надання сервісів. Зокрема, для врахування мінливих намірів користувачів щодо якості обслуговування удосконалено існуючі методи формування структури рівня радіодоступу 4G/5G, розроблено нові методи планування, розподілу та оптимізації частотно-часових ресурсів.

2. Зокрема на основі проведеного дослідження доведено, що запропонований адаптивний інтенційно-орієнтований метод розподілу ресурсів та формування структури рівня радіодоступу мереж 4G/5G дав змогу ефективніше на 25 % використовувати наявні частотно-часові ресурси та зменшити на 8,7% енергоспоживання мережі рівня радіодоступу для забезпечення замовленої якості обслуговування користувачів у порівнянні із традиційними методами.

3. Комплексне використання розроблених методів пріоритезації IoT трафіку та балансування навантаження, дають змогу зменшити середню затримку передавання повідомлень реального часу з кінця в кінець до 3 разів, при цьому роблячи систему NB-IoT придатною для забезпечення ультра надійного зв'язку з низькими затримками, що є важливим для розвитку інтенційно-орієнтованих мереж 5G.

4. Для дослідження ефективності застосування віртуалізації мережевої інфраструктури проведено ряд досліджень стосовно адаптивного розподілу ресурсів на рівні базових станції, маршрутизатора та сервера. Дослідження проведено в умовах різного навантаження на різні компоненти мережі, що дало змогу оцінити затримку на віртуальних вузлах та збалансувати ресурси для забезпечення наскрізної затримки обслуговування в межах допустимого. Запропоновано концептуальну модель мережевої інфраструктури з реалізацією адаптивної віртуалізації ресурсів шляхом використання системи моніторингу навантаження, скрипт файлів розгортання віртуальних машин різної продуктивності, контролера мережі в Big Data та резервного обладнання мережі.

5. Запропоновано методологію синтезу гетерогенної інтенційно-орієнтованої мережі, згідно якої можна інтелектуально виділяти зв’язки між структурно-функціональними елементами мережі, які можуть не тільки автоматизовано перебудовуватись з різною продуктивністю, але й виникати заново, вишукуючи шляхи найбільш адекватного пристосування до мінливих вимог користувачів щодо адаптивного надання сервісів за певними критеріями якості обслуговування.

РОЗДІЛ 6. ПРАКТИЧНА РЕАЛІЗАЦІЯ ІНТЕНЦІЙНО-ОРІЄНТОВАНОЇ МЕРЕЖІ КОРПОРАТИВНОГО СЕГМЕНТУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ SDN ТА АВТОМАТИЗАЦІЇ ЗАПРОПОНОВАНИХ УПРАВЛІНСЬКИХ РІШЕНЬ

6.1. Розробка прототипу корпоративного сегменту енергоефективної інтенційно-орієнтованої мережі на базі мікроконтролерних платформ

У роботі розроблено прототип енергоефективної IBN мережі на основі мікроконтролерних платформ з віртуалізацією мережевих функцій SDN, що дало змогу шляхом реалізації запропонованих рішень підвищити гнучкість управління мережею, зменшити енергоспоживання та забезпечити необхідну якість надання критично важливих сервісів Інтернету речей в корпоративних мережах, що підтверджено актами впровадження [246].

Інтуїтивна логіка управління ресурсами мережі забезпечується шляхом програмної імплементації запропонованих рішень енергоефективної QoE маршрутизації на контролері SDN, яка може адаптувати свою конфігурацію відповідно до вимог цільових програм IoT. Технічно платформа складається з набору недорогих та енергоефективних одноплатних комп'ютерів, які пов'язані між собою в мережі з програмною конфігурацією. Запропонований комутатор SDN розгортається на мікроконтролерній платформі Raspberry Pi 3 за допомогою програмного забезпечення Open vSwitch (OvS), тоді як контролер Floodlight розгортається на платформі Orange Pi Prime. Для даного IBN прототипу розроблено унікальну систему моніторингу якості функціонування мережі за критерієм затримки передавання даних IoT. Особливістю системи моніторингу є використання методу наскрізного вимірювання затримки передавання даних шляхом додавання часової мітки до метаданих заголовків пакету, що дає змогу в режимі реального часу визначати час оброблення пакету кожним компонентом мережі та в умовах перевищення норм сповіщати про

прийняття необхідних управлінських рішень. Для забезпечення згідно намірів користувачів необхідного рівня QoS/QoE для критично важливих додатків на базі розробленої платформи реалізовано централізовану потокову модель QoE маршрутизації (розділ 2.3). Розроблена платформа характеризується високою автономністю та адаптивністю з точки зору забезпечення вимог користувачів. Підтвердженням цього є проведення реальних експериментальних досліджень. У наступних підрозділах розглянуто більш детально процес розробки прототипу корпоративного сегменту енергоефективної інтенційно-орієнтованої мережі на базі мікроконтролерних платформ.

6.1.1. Структурно-функціональна схема інтенційно-орієнтованої SDN/IoT мережі на базі мікроконтролерів

У роботі розроблено прототип енергоефективної інтенційно-орієнтованої мережі побудованої на базі мікроконтролерних платформ Raspberry Pi 3 Model B та віртуалізації функцій компонентів технології SDN (програмно-конфігурованих мереж). Структурно-функціональна схема інтенційно-орієнтованої SDN/IoT мережі на базі мікроконтролерів показано на рис.6.1.

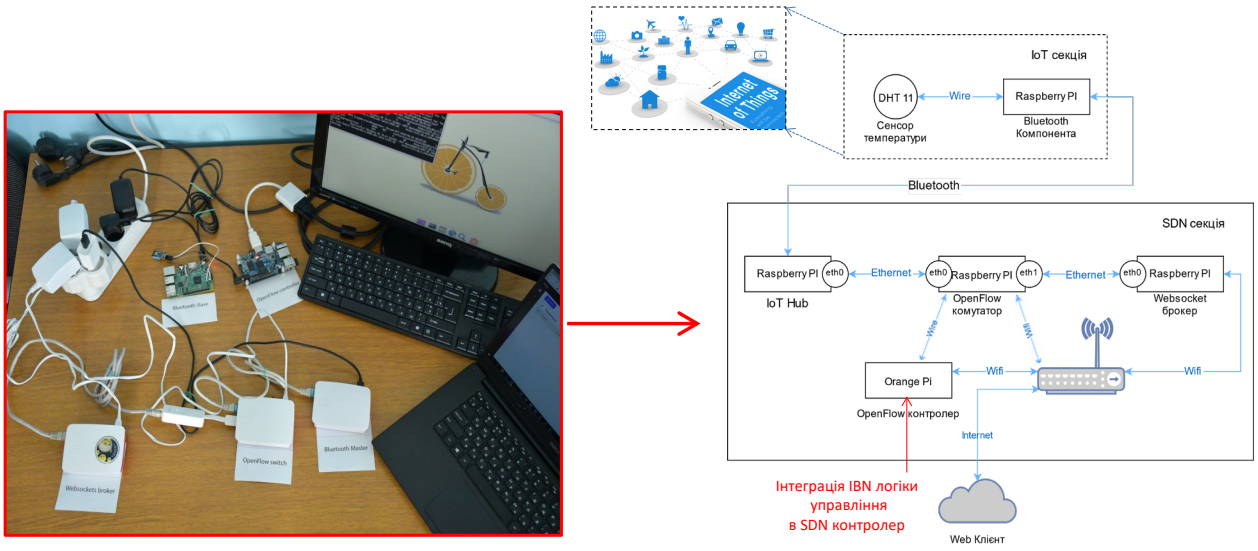


Рис.6.1. Структурно-функціональна схема прототипу інтенційно-орієнтованої SDN/IoT мережі побудованої на основі мікроконтролерів та віртуалізацій мережевих функцій [247]

Схема прототипу складається з двох основних частин, зокрема IoT та SDN секції. Між собою ці секції спілкуються через інтерфейс Bluetooth. Доступ до даної моделі реалізовано через інтернет, за допомогою веб-додатку.

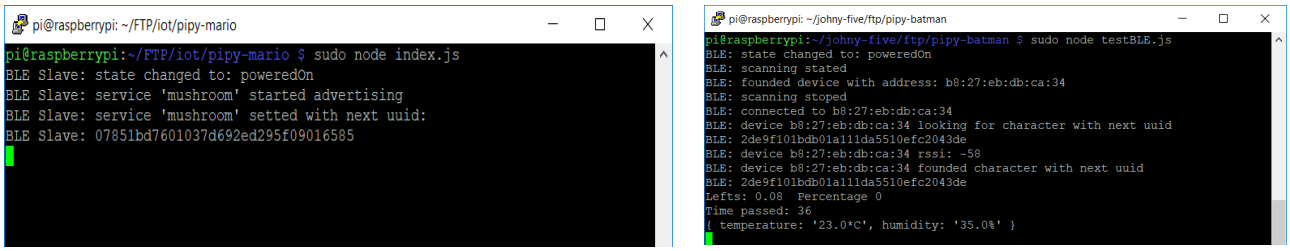
Секція IoT. У роботі зроблено припущення, що критично важливою послугою IoT в даній платформі є передача даних про температуру і вологість. Для цієї мети використовується простий датчик температури DHT11 [52]. DHT11 забезпечує зчитування температури навколишнього середовища від 0 °C до + 50 ° C з точністю ± 2 ° C [53]. Цей датчик підключається до Raspberry Pi, який діє як передавач від датчика через Bluetooth Low Energy (BLE). Разом з датчиком компонент Bluetooth в секції IoT збирає дані. Розроблений прототип для наочності отримує дані тільки з одного датчика Однак в практичному застосуванні кількість датчиків і виконавчих механізмів зазвичай досягає десятків або навіть сотень модулів. Для зручності всі ці модулі будуть взаємодіяти через безпровідні інтерфейси, такі як Bluetooth, Zigbee, Z-Wave, Wi-Fi, NFC, мобільні мережі і т.д., а їх агрегацію продовжить проміжний брокер, який вже буде контролювати доступ і надавати інтерфейс для доступу в Інтернет речей.

Для даної моделі необхідно, щоб один із пристроїв був в ролі slave пристрою, і інший в ролі master пристрою. Кінцевий модуль буде slave пристроєм, а брокер буде master. Пристрій в ролі slave повинен мати новий сервіс, котрий буде у своєму складі мати характеристику про дані із сенсора температури. Відповідно master визначатиме цей сервіс, знаходитиме дану характеристику і буде відправляти запит на отримання даних. Slave при запиті до даної характеристики в цей момент отримуватиме дані з сенсора DHT11.

За допомогою бібліотеки bleno котра дає зручний інтерфейс на мові програмування JavaScript, написано програму, яка автоматично створює новий Bluetooth сервіс для зчитування даних з сенсора. Тому для розробленого IBN прототипу реалізовано програму, котра створює сервіс для отримання даних з

сенсора. Після запуску даної програми у терміналі можна побачити що сервіс запущений і очікує на запит (рис.6.2а).

Тепер необхідно підготувати master пристрою. Для цього також використано Raspberry Pi. Для того щоб зробити master пристрій використано бібліотеку Noble написану також на JavaScript. Відповідно знаючи адресу Bluetooth Slave пристрою, котрий містить сенсор температури, можна здійснити пошук пристрою з відповідною адресою, котра відповідає за температуру. Результат виконаної програми при успішному знаходженні шуканого пристрою з відповідним сервісом показано на рис. 6.2б.



а) б)

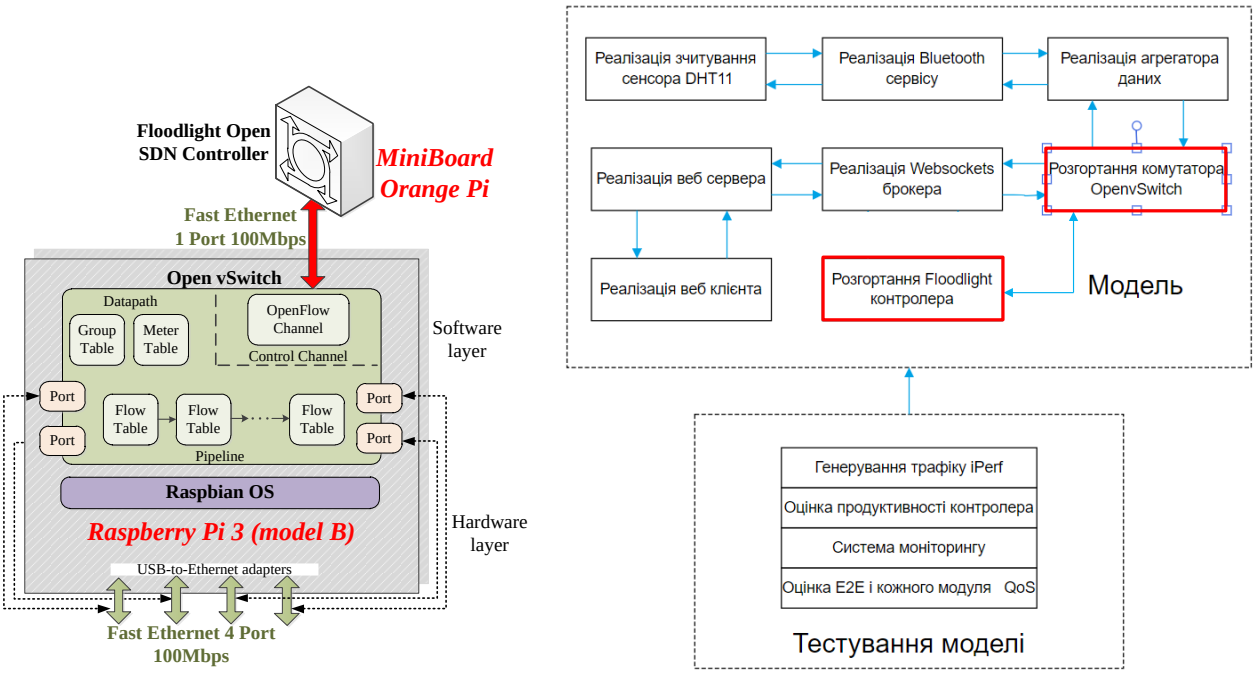
Рис.6.2. Вікно результату успішного знаходження шуканого Bluetooth slave пристрою – а) та вимірювання даних через Bluetooth slave – б)

Відповідно пристрій Bluetooth Master має доступ до отримання температури зі сенсора на іншому пристрої, які можна надсилати у Інтернет при запиті. IoT Hub виконаний у вигляді Raspberry Pi. IoT Hub агрегує дані з декількох IoT компонентів, спілкуючись через BLE. Завдяки проміжному IoT Hub дані можуть отримуватись із сенсорів.

SDN секція. SDN частина в цій архітектурі складається з 3-х основних компонентів: Комутатор Openflow, брокер WebSockets і контролер Openflow. У роботі розроблено 5-портовий SDN комутатор на основі Raspberry pi 3 та програмне забезпечення Open vSwitch (OvS). Комутатор OpenFlow у вигляді Raspberry Pi діє як віртуальний комутатор на основі OvS. OvS - це високоякісний багаторівневий віртуальний комутатор з ліцензією Apache 2.0 з відкритим вихідним кодом. Основним призначенням OvS є надання комутатора

для апаратно-віртуалізованих середовищ для підтримки безлічі протоколів і стандартів, які використовуються в інфокомунікаційних мережах. Прототип SDN комутатора і контролера на базі одноплатних комп'ютерів (Raspberry Pi 3 і Orange Pi Prime) показано на рис. 6.3а.

Блок-схема етапів реалізації прототипу мережі показано на рис.6.3б. Кожен із цих блоків це окремо написані програми та розроблені програмно-апаратні рішення для інтеграції в одну систему (програмні коди додаються у додатку).



а) б)

Рис.6.3. Структурно-функціональна схема прототипу SDN комутатора і контролера розгорнутих на основі мікроконтролерних платформ – а) та етапи реалізації прототипу – б)

Розроблений комутатор містить в собі таблицю маршрутизації FlowTable. Так як комутатор тільки що створений, таблиця по замовчуванню є пустою.

Так як перший пристрій підключено до порта eht0, а другий до порта eth1, достатньо зробити два простих правила маршрутизації:

1) при поступленні пакету на порт eth0, відправляти до порта eth1;

2) при поступленні пакету на порт eth1, відправляти до порта eth0.

Кожне правило маршрутизації повинне також включати в собі такий параметр як пріоритет (priority). Саме по пріоритету комутатор буде обирати найбільш оптимальний маршрут і відповідно обробляти пакет до заданого маршруту. Чим вище значення priority, відповідно тим вищий пріоритет. Добавити правило маршрутизації котре буде перенаправляти всі поступленні пакети із порта eth0 на порт eth1 можна за допомогою команди $ ovs-vsctl add-flow mybridge priority=500,in_port=1,actions=output:2 []. На рис. 6.4 показано базову настройку Open vSwitch FlowTable для розробленого прототипу мережі.

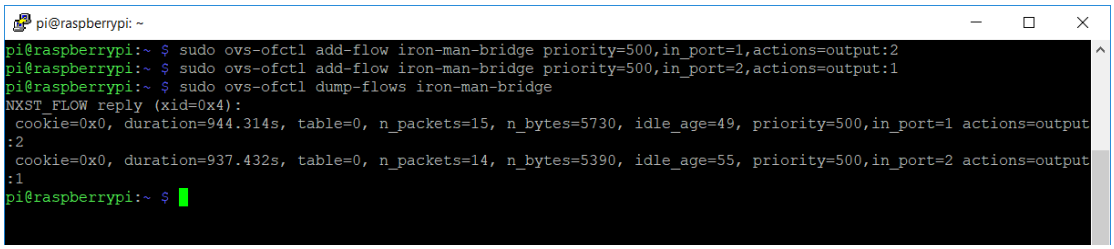
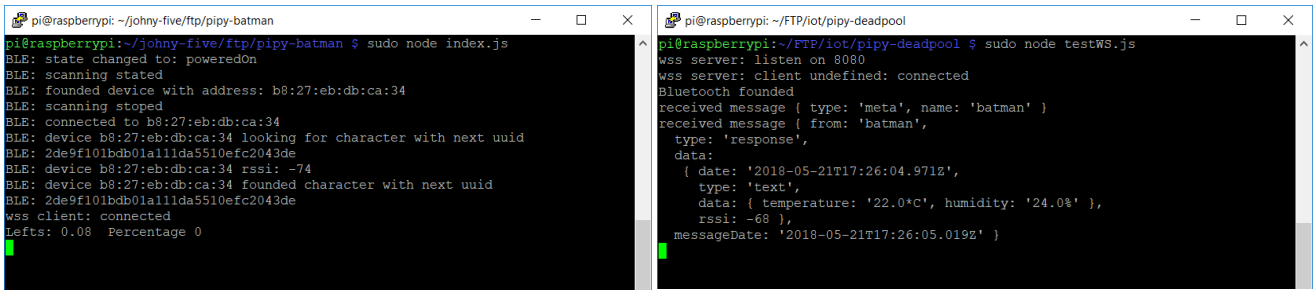


Рис.6.4. Налаштування правил маршрутизації на Open vSwitch

Відповідно після цього, спробувавши доступитись з одного хоста до іншого, котрі підключені до даного комутатора, результат буде успішним. Проте для пересилання даних між двома хостами, однієї команди ping недостатньо. Для спілкування між сервісами в режимі реального часу (не в режимі запит відповідь) було обрано протокол WebSocket. WebSocket — це протокол, що призначений для обміну інформацією між браузером та веб-сервером в режимі реального часу. Він забезпечує двонаправлений повнодуплексний канал зв'язку через один TCP-сокет. Відповідно на брокері необхідно запустити програму, котра підніматиме WebSocket сервер, котрий при підключенні очікуваного клієнта, відсилатиме запит на отримання даних від сенсора температури. Bluetooth Master цього разу виступає в ролі Master пристрою для Slave сенсора, і клієнтом WebSocket для брокера. Результат при успішному з’єднанні до обох пристроїв Bluetooth Master показано на рис.6.5а. У свою чергу брокер отримує дані з сенсора температури(рис. 6.5б).



а) б)

Рис. 6.5. Bluetooth Master приєднався успішно до WebSocket сервера – а) та брокер отримав дані з сенсора температури – б)

При виборі контролера OpenFlow для цієї платформи були розглянуті в першу чергу контролери з мінімальними системними вимогами, оскільки для контролера SDN планується використовувати енергоефективний та недорогий одноплатний комп'ютер. Відповідно, використано плату Orange Pi Prime, яка має чотири процесорних ядра та два гігабайти оперативної пам'яті, ресурсів яких достатньо для SDN контролера Floodlight [249]. У даному прототипі, це контрольна точка, звідки відбувається моніторинг даної мережі, управління потоку даних, а також балансування навантаження (load balancing), автоматичне масштабування (auto scaling), та інші переваги SDN. Даний контролер не є єдиною точкою падіння (single point of failure) [250-254].

6.1.2. Система моніторингу якості функціонування реалізованого прототипу в IBN мереж за критерієм затримки передавання даних

У роботі розроблено систему моніторингу якості функціонування реалізованого прототипу інтенційно-орієнтованої мережі за критерієм наскрізної затримки передавання даних, що є одним із ключових параметрів моніторингу якості надання сервісів реального часу критично-важливої інфраструктури. Особливістю системи є використання розробленого унікального методу наскрізного вимірювання затримки передавання даних шляхом додавання часової мітки до метаданих заголовків пакету (рис.6.6), що дає змогу визначати час оброблення пакету кожним компонентом мережі та в

умовах перевищення норм автоматизовано сповіщати про прийняття необхідних інтуїтивних керуючих рішень [247].

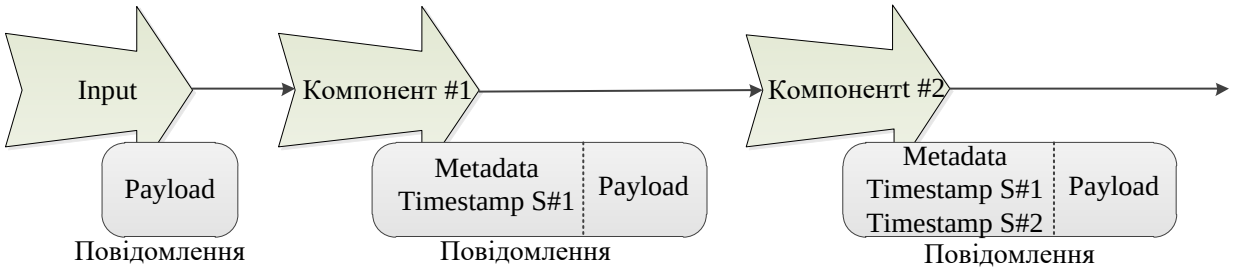


Рис. 6.6. Принцип методу вимірювання затримки

Даний метод вимагає, щоб часові параметри на всіх компонентах були максимально синхронізованими для точних розрахунків. Для цього на кожному компоненті прототипу мережі, що працюють на базі ОС Linux використано команду ntpdate, яка може встановити системний час по протоколу NTP (Network Time Protocol) з точністю до однієї мікросекунди [254]. Таким чином, коли всі компоненти знаходяться у внутрішній мережі, включаючи брокера, виміряна похибка затримки знаходиться в межах однієї мікросекунди. Якщо брокер знаходиться у зовнішній мережі, важко забезпечити високу точність оцінки затримки, похибка може змінюватися до декількох мілісекунд.

Алгоритм роботи методу є наступним:

– Перші n = 10 повідомлень отримуються зі всіма часовими мітками $timestamp_m$, де змінною $timestamp$ вказується позначка часу, m – компонент прототипу мережі (контролер SDN, комутатор SDN, брокер, датчик, тобто.).

– Обчислюється затримка між всім компонентами мережі за формулою:

$$delay_{m2-m1} = timestamp_{m2} - timestamp_{m1} \tag{6.1}$$

– Обчислюється порогове значення кожної затримки за формулою:

$$threshold_{m2-m1} = (\frac{1}{n}\sum_{i}^{n=10} delay_{m2-m1_i}) \cdot 1.20 \tag{6.2}$$

де 1.20 – максимальне зміщення від середньої затримки

– Обчислюється сумарна порогова затримка :

$$threshold_{sum} = \sum threshold_{m2-m1} \tag{6.3}$$

– Далі повідомлення надсилаються тільки з початковою часовою міткою, для визначення загальної затримки

– Якщо загальна затримка перевищує допустиму, наступні повідомлення надсилаються з часовими мітками, і затримка контролюється на кожному модулі. Система автоматично прийме рішення для уникнення затримки.

– Після здійснення оптимізації, повернутись до першого кроку.

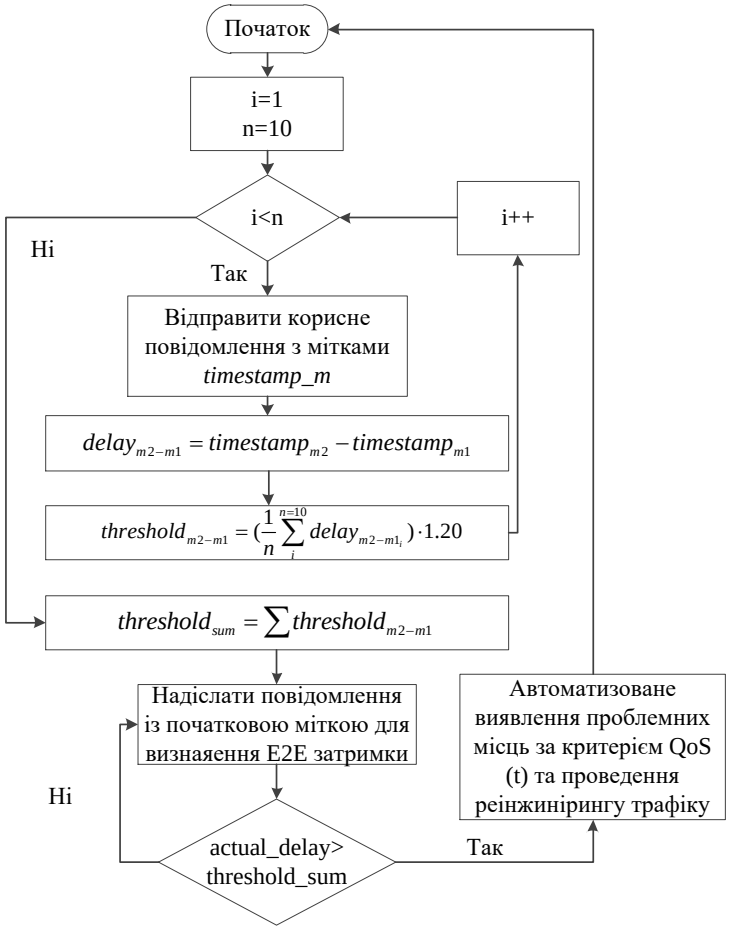
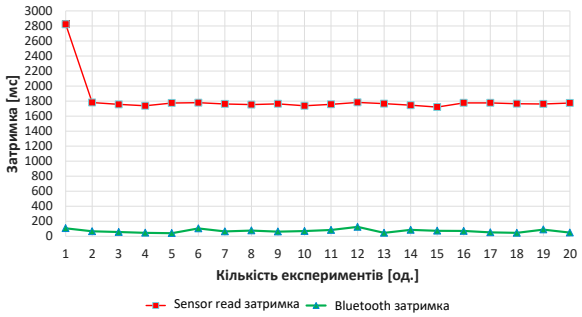


Рис.6.7. Алгоритм вимірювання затримки для розробленого прототипу мережі

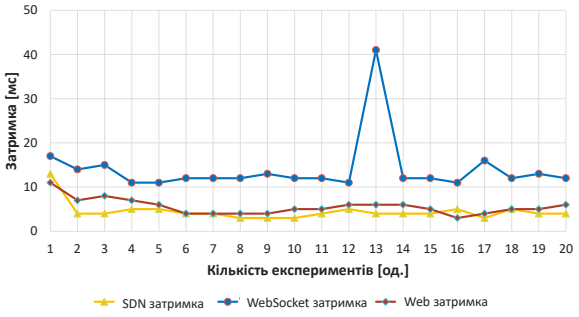
В процесі аналізу тестової моделі слід пам’ятати, що дана програмно-конфігурована мережа, є найпростішим її варіантом, котра має тільки один комутатор, котрий з’єднує між собою два хоста. Інтернет речей реалізовано у вигляді простого сенсора температури і вологості, котрий за допомогою

Bluetooth пересилає тільки два параметри, значення вологості і значення температури, тобто малу кількість даних. Веб-клієнт реалізовано у двох варіантах: веб-сервер і веб-клієнт знаходяться у внутрішній мережі (edge computing), веб-сервер розміщено віддалено на одному із безкоштовних веб-хостингів (cloud computing), а клієнт підключений через мобільну мережу 4G.

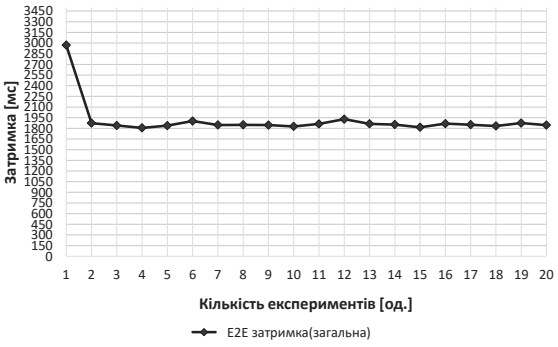
На кожному компоненті розробленого прототипу мережі при поступленні пакету даних, модуль добавляв метадані до цього пакету. Одним із параметрів метаданих є час затримки. Тобто кожен модуль на своєму рівні вимірював час затримки. Для аналізу затримки було здійснено 20 експериментів. Під одним експериментом розуміється створення запиту з веб клієнту, і отримання відповіді на веб-клієнті. Існують такі затримки рис.6.8: Sensor read latency, Bluetooth latency, SDN latency, WebSocket latency, Web latency, E2E Total.



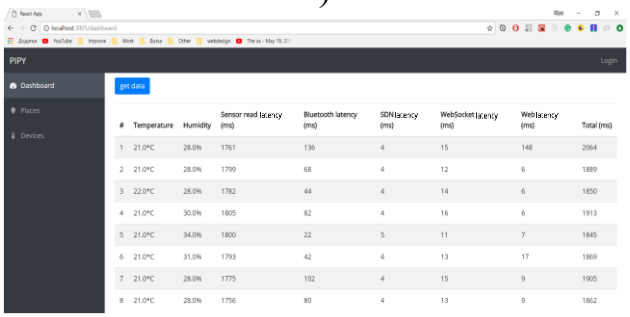
а)



б)



в)



г)

Рис.6.8. Результати вимірювання затримки передавання даних внесених кожним компонентом розробленого прототипу мережі

Sensor read latency – затримка на надіслання запиту та отримання даних зі сенсора в мілісекундах. В даній моделі це є DTH11 – сенсор температури і

вологості. Raspberry Pi через інтерфейс GPIO отримує ці дані. Значення цієї затримки для 20 експериментів показано на рис. 6.8а. Середнє значення цієї затримки - 1814,4 мс. Стандартне відхилення - 238 мс. Як видно з графіка дане значення є доволі постійним, крім першого запиту.

Bluetooth latency – затримка на надсилання запиту та отримання даних через Bluetooth інтерфейс в мілісекундах. Об'єм даних зі сенсора в запиті займає приблизно 200 байт. Значення цієї затримки для 20 експериментів показано на рис.6.8а. Середнє значення цієї затримки - 71,2 мс. Стандартне відхилення - 22,9 мс. Дане значення є не стійким, і сильно варіюється.

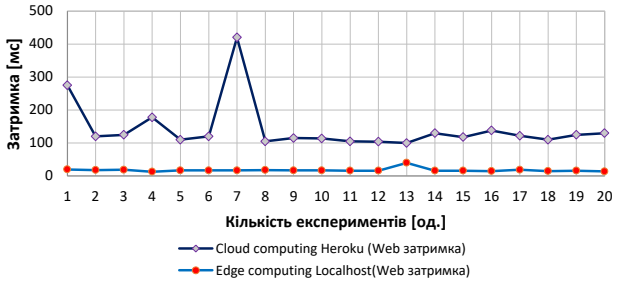
SDN latency – затримка на roundtrip проходження даних через віртуальний комутатор Open vSwitch та контролер SDN. Raspberry Pi з'єднаний з іншим Raspberry Pi через проміжний Raspberry Pi котрий є віртуальним комутатором. Комутатор з'єднує два хости через ethernet порти. Raspberry Pi підтримує 100 Base Ethernet, тобто швидкість передачі через цей порт максимальна 100 Мбіт/секунду. Віртуальний комутатор при отримані пакету на один із портів, знаходить яку дію має він здійснити з даним пакетом з FlowTable. В даному комутаторі тільки два значення в таблиці маршрутизації.. Значення цієї затримки для 20 експериментів показано на рис. 6.8б. Середнє значення цієї затримки - 4,5 мс. Стандартне відхилення - 2,1 мс. Дане значення є стійким, і не сильно варіюється, тільки при першому запиті, є замітна більша затримка, що відбувається при першочерговому зверненні до контролера SDN. Значення середньої затримки -1,4 мс, та стандартне відхилення – 0,15 мс.

WebSocket latency – затримка на надсилання запиту від веб-сервера до брокера і отримання відповіді. Брокер і веб-сервер спілкуються по протоколу WebSocket. Затримка вимірювалась вже при встановленому з'єднанні. Необхідно врахувати що у даному експерименті веб-сервер знаходиться у локальній мережі (edge computing). Об'єм даних повідомлення також становить приблизно 1 Кбайт. Значення цієї затримки для 20 експериментів показано на рис. 6.8б. Середнє значення цієї затримки - 14,05 мс. Стандартне відхилення -

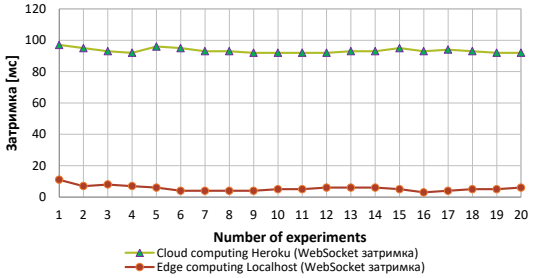
6,6 мс. Дане значення є доволі стійким, і слабо варіюється, проте інколи з різних причин може бути значно довша затримка.

Web latency – затримка на roundtrip створення запиту веб-клієнтом та отримання відповіді від веб-сервера в мілісекундах. Запит виконується по протоколу HTTP, і отримується відповідь в розміром в 1 Кбайт. Необхідно врахувати що як і веб-клієнт, так і веб-сервер знаходяться у одній внутрішній мережі. Значення цієї затримки для 20 експериментів показано на рис. 6.8б Середнє значення цієї затримки - 5,55 мс. Стандартне відхилення - 1,8 мс. Дане значення не є стійким.

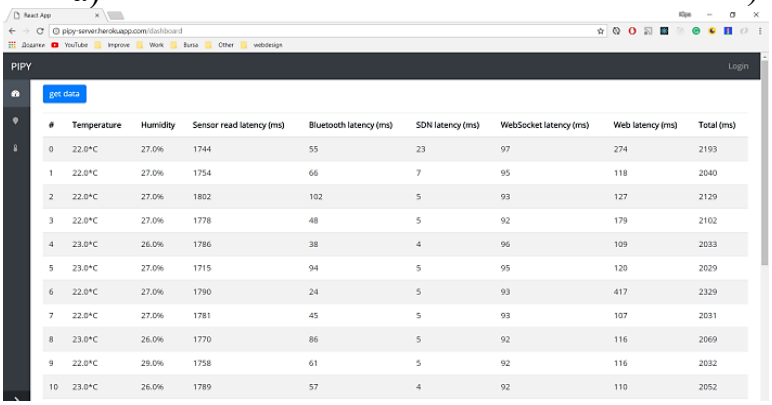
Отже, якщо просумувати ці всі затримки, для попередніх експериментів, отримаємо наступний графік (рис. 6.8в) сумарної затримки, тобто затримка, від моменту, як користувач на веб-клієнтів натиснув кнопку для запиту даних, до отримання їх у таблиці на веб-клієнті. Середнє значення сумарної затримки - 1909,6 мс, а стандартне відхилення – 251,4 мс. Проте як видно з графіка, вже після першого запиту, значення затримки було доволі стабільним. Проте в даній моделі веб-клієнт і веб-сервер знаходились у внутрішній мережі.



а)



б)



в)

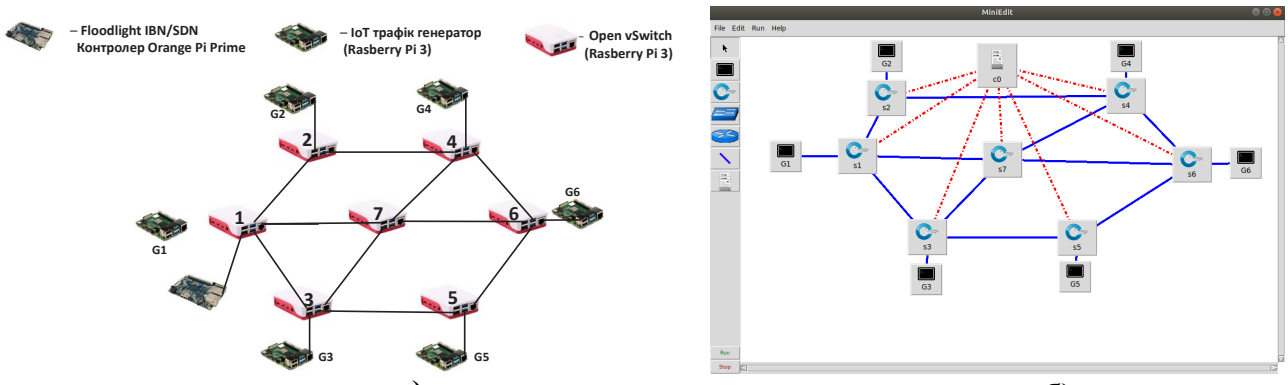
Рис. 6.9.Порівняння затримок при Edge та Cloud Computing

Тому, щоб це перевірити, веб-сервер було розгорнуто на віддаленому веб - хостингу Heroku (cloud computing). На рис. 6.9 показано розгорнуту версію на віддаленому хостингу. Як видно з рисунка, всі затримки зберегли приблизно однакові значення, крім затримки Web latency. Справжній клієнт буде доступатись з інтернету до віддаленого сервера. В результаті буде більша затримка.

6.1.3. Дослідження ефективності QoE маршрутизації на базі розробленого прототипу інтенційно-орієнтованої мережі

У цій частині роботи описується реалізація запропонованої моделі QoE маршрутизації, детальний принцип роботи, якої описано в розділі 2.

Для експериментального дослідження та оцінки ефективності у роботі імплементовано у вигляді програмного коду логіку запропонованої моделі QoE-маршрутизації для контролера Floodlight, а також побудовано топологію SDN мережі спочатку в середовищі Mininet, а після успішного тестування реалізовано на реальному обладнанні з використанням мікроконтролерних платформ. Ця топологія складається з 7 Open vSwitches, 1 контролера Floodlight SDN та 6 генераторів трафіку IoT, (G1, G2, G3, G4, G5 і G6). Експериментальна схема дослідження показана на рис.6.10.



а) **б)**

Рис.6.10.Експериментальна схема дослідження QoE-маршрутизації на реальному обладнані – а), у середовищі Mininet – б) [255]

Пропускна здатність каналу між усіма вузлами для всіх портів встановлена рівною 100 Мбіт/с. Під час експерименту трафік IoT генерувався в мережі за допомогою мультисервісної системи генерації трафіку, запропонованої в роботі [164]. Матриця вимог C_{ij} до пропускної здатності зв'язку між вузлами наведена нижче в Мбіт/с.

$C_{ij} =$

	1	2	3	4	5	6
1	0	12,5	16,5	5	9	7
2	11	0	12,5	20	14	13
3	5	16,5	0	21	12,6	5
4	10	14,5	12	0	13	11
5	8	18	6	8	0	15
6	12	8	9	15	5	0

Вузол № 7 є проміжним (він представляє рівень агрегації), тому жодні пристрої IoT до нього не підключені. Відповідно до матриці вимог сформовано перелік потоків для всіх категорій трафіку. Набір абонентів та послуги IoT, які вони використовують, генеруються для пропускної здатності каналу 100 Мбіт/с. Список потоків для 9 користувачів наведено в таблиці 6.1 (C – пропускна здатність каналу зв'язку, Мбіт/с; C_P – пріоритет користувачів IoT, Q – інтегральний критерій якості користувачів).

Кожен абонент використовує певний набір послуг IoT. У разі порожньої комірки на перетині стовпця та рядка, ця послуга повинна розглядатися як та, яка не гарантує якості послуги, якщо користувач користується нею. Усі інші послуги IoT мають вимоги до пропускної здатності та параметри обслуговування для конкретного користувача, що забезпечується угодою про обслуговування між абонентом та оператором мережі. Як видно з таблиці 6.1, кожному абонентові присвоюється пріоритет у межах відповідного діапазону пріоритетів для певного виду послуги. Ця процедура виконується для кожної пари серверів, що використовуються для генерації навантаження абонентів.

Наступним кроком було обчислення відносних пріоритетів потоків IoT, беручи до уваги класифікацію категорій послуг, запропонованої у розділі 2.

До першої категорії послуг належать (критично важливі сервіси IoT), які передаються в режимі реального часу, надзвичайно чутливі до затримки пакетів, належать такі: автоматизований екстрений виклик IoT (A), моніторинг температури критично важливих об'єктів (B), IoVT відео в реальному часі (C).

Таблиця вимог користувачів щодо якості надання сервісів IoT, що задається для логіки SDN контролера наведено в таблиці 6.1.

Таблиця 6.1

Таблиця вимог користувачів щодо якості надання сервісів IoT

IoT послуги	Клас	Пара-метри	Користувачі								
			1	2	3	4	5	6	7	8	9
Автоматизований екстрений виклик IoT (A)	Реальний час	*C*	0,17	0,19	0,16	0,19	0,18	0,18	-	-	-
		Cp	5	10	15	20	25	30	-	-	-
		Q	0,25	0,22	0,22	0,21	0,21	0,21	----	----	----
Моніторинг температури (B)	Реальний час	*C*	1,25	1,01	1,17	1,25	1,17	1,27	1,11	1,09	1,44
		Cp	260	265	270	275	280	285	290	295	300
		P_{IoT_k}	0,188	0,187	0,186	0,185	0,184	0,183	0,182	0,181	0,18
Відео IoVT (C)	Реальний час	*C*	1,91	2,09	2,13	2,21	2,15	2,17	1,95	2,33	2,42
		Cp	515	520	525	530	535	540	545	550	555
		Q	0,148	0,147	0,146	0,145	0,144	0,143	0,142	0,141	0,42
IoT-оповіщення (Photo/text/Email) (D)	Не реальний час	*C*	1,59	1,60	1,54	1,80	1,68	1,53	1,90	1,46	1,81
		Cp	770	775	780	785	790	795	800	805	810
		Q	0,428	0,427	0,426	0,425	0,424	0,423	0,422	0,421	0,42
VoD IoVT (E)	Не реальний час	*C*	2,06	2,22	1,71	1,84	2,15	2,13	1,97	2,16	2,14
		P	1025	1030	1035	1040	1045	1050	1055	1060	1065
		Q	0,58	0,57	0,56	0,55	0,54	0,53	0,52	0,51	0,5
IoT відео (720p60) (F)	Не реальний час	*C*	5,56	5,57	3,99	5,50	5,72	5,72	5,50	-	-
		Cp	1280	1285	1290	1295	1300	1305	1310	-	-
		Q	0,88	0,87	0,86	0,85	0,84	0,83	0,82	----	----
IoT відео (1080p60) (G)	Не реальний час	*C*	9,96	9,90	9,48	10,63	10,06	10,49	8,30	12,98	9,82
		Cp	1540	1545	1550	1555	1560	1565	1570	1575	1580
		Q	0,98	0,97	0,96	0,95	0,94	0,93	0,92	0,91	0,9

У роботі вирішено провести порівняння запропонованої моделі маршрутизації із моделюю (DMCQR, deterministic multiconstrained centralized QoS routing), представленої у роботі [142]. На основі проведено аналізу у 1

розділі, встановлено, що дана модель маршрутизації DMCQR в межах наукових досліджень стосовно багатокритеріальної маршрутизації потоків даних для програмно-конфігурованих мереж вважається одним із кращих.

Для перевірки ефективності запропонованих рішень стосовно гарантування необхідної якості обслуговування для критично важливих послуг IoT в умовах високого навантаження в мережі використаний сервіс реального часу IoVT (Internet of Video Things), що транслює відео з сервера G6. Мережа заповнена IoT-трафіком відповідно до вимог, наведених вище у матриці, що генерується мультисервісними генераторами трафіку IoT G1-G6, підключеними до 6 комутатора OVS. Згідно функціонування моделі маршрутизації DMCQR мережа була заповнена фоновим мультисервісним трафіком, що генерується пристроями IoT. Усі оптимальні шляхи для потоків та їх вимоги щодо пропускної здатності наведено в таблиці 6.2.

Таблиця 6.2

Оптимальні шляхи передавання фонового IoT трафіку між різними хостами визначенні на основі маршрутизації DMCQR

Потік між хостами	Шлях	Пропускна здатність, Мбіт/с	Потік між хостами	Шлях	Пропускна здатність, Мбіт/с
G1→G2	1-2	12,5	G4→G1	4-7-1	10
G1→G3	1-3	16,5	G4→G2	4-2	14,5
G1→G4	1-7-4	5	G4→G3	4-7-3	12
G1→G5	1-7-6-5	9	**G4→G5**	**4-6-5**	**13**
G1→G6	1-7-6	7	**G4→G6**	**4-6**	**11**
G2→G1	2-1	11	G5→G1	5-3-1	8
G2→G3	2-1-3	12,5	**G5→G2**	**5-6-4-2**	**18**
G2→G4	2-4	20	G5→G3	5-3	6
G2→G5	**2-4-6-5**	**14**	**G5→G4**	**5-6-4**	**8**
G2→G6	2-1-7-6	13	G5→G6	5-6	15
G3→G1	3-1	5	G6→G1	6-7-1	12
G3→G2	3-1-2	16,5	**G6→G2**	**6-4-2**	**12**
G3→G4	3-7-4	21	G6→G3	6-7-3	9
G3→G5	3-5	12,6	**G6→G4**	**6-4**	**15**
G3→G6	3-7-6	5	G6→G5	6-5	5

Наступним кроком було створення навантаження лише за допомогою IoVT-відео сервісу реального часу від генератора трафіку IoT G6. Згідно методу маршрутизації DMCQR визначено оптимальні шляхи для передавання даного потоку до кінцевих користувачів, що знаходяться на кожному із генераторів G1 – G5. Канали зв'язку та пропускна здатність необхідна для цих потоків, які задіяні в процесі передавання по оптимальних шляхах наведені в таблиці 6.3

Таблиця 6.3

Оптимальні шляхи передавання трафіку IoVT-відео сервісу реального часу від хоста (генератора) трафіку IoT G6 до G1 – G5 визначенні на основі маршрутизації DMCQR

Потік	Необхідна пропускна здатність, Мбіт/с	Шлях
G6→G1	19.36	6-7-1
G6→G2	17.45	6-7-1-2
G6→G3	9.13	6-5-3
G6→G4	**9.05**	**6-4**
G6→G5	1.91	6-5

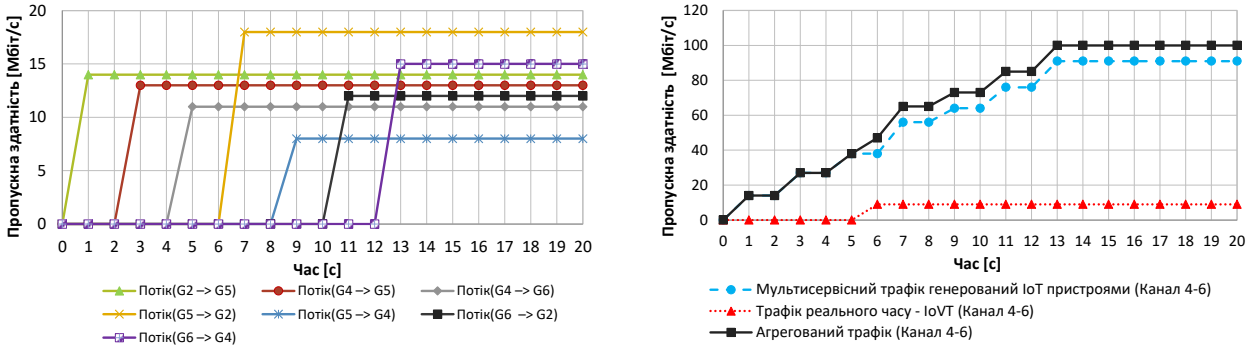
Модуль, що відповідає за моніторинг мережі може використовувати OpenFlow для надсилання HTTP-запитів, щоб отримати пропускну здатність в реальному часі.

В результаті маршрутизації згідно моделі DMCQR в мережі сталося незбалансоване завантаження ланок. Особливу увагу слід звернути на канал між комутаторами 4-6, який має значні затримки і високу ймовірність втрати пакетів через недостатню пропускну здатність каналу. Канали 5-6 і 6-7 знаходяться в стані близькому до перевантаження з високою ймовірністю затримок для потоку реального часу IoVT. Крім того, немає альтернативних шляхів передачі з достатньою пропускною здатністю для потоку 9.05 Мбіт/с з G6 на G4 хости. Тому, відповідно до підходу DMCQR, оптимальним шляхом для потоків IoVT 9.05 Мбіт/с з G6 в G4 за критерієм QoS є шлях 6-4.

Проведемо детальний аналіз потоків IoT, що призводять до перевантаження ланки 4-6 за моделлю DMCQR. Сумарне навантаження від IoT

трафіку згідно таблиць 6.2 та 6.3 розраховано наступним чином та показано на рис. 6.11.

$$f_{(G_2 \to G_5)} = F_3 + B_2 + F_4 + D_2 + D_7 = 3.99 + 1.01 + 5.5 + 1.6 + 1.9 = 14 \ [Мбіт/с]$$
$$f_{(G_4 \to G_5)} = F_2 + C_5 + D_5 + A_2 + D_9 + D_2 = 5.57 + 2.15 + 1.68 + 0.19 + 1.81 + 1.6 = 13 \ [Мбіт/с]$$
$$f_{(G_4 \to G_6)} = G_7 + A_2 + A_3 + C_6 + A_6 = 8.3 + 0.19 + 0.16 + 2.17 + 0.18 = 11 \ [Мбіт/с]$$
$$f_{(G_5 \to G_2)} = G_8 + C_9 + B_8 + B_3 + A_5 = 12.98 + 2.42 + 1.09 + 0.16 + 1.17 + 0.18 = 18 \ [Мбіт/с]$$
$$f_{(G_5 \to G_4)} = F_7 + A_3 + B_8 + B_4 = 5.5 + 0.16 + 1.09 + 1.25 = 8 \ [Мбіт/с]$$
$$f_{(G_6 \to G_2)} = G_6 + B_3 + A_6 + A_3 = 10.49 + 1.17 + 0.18 + 0.16 = 12 \ [Мбіт/с]$$
$$f_{(G_6 \to G_4)} = G_4 + F_3 + A_2 + A_4 = 10.63 + 3.99 + 0.19 + 0.19 = 15 \ [Мбіт/с]$$



а) б)

Рис. 6.11 Навантаження в каналі 4-6 створюваного фоновим IoT трафіком– а) та навантаження в каналі 4-6 створюваного фоновим IoT трафіком та додатковим трафіком реального часу IoVT – б) [255]

Загальне навантаження від сервісу реального часу IoVT, що генерується генератором трафіку IoT G6 відповідно до таблиць 6.2 і 6.3, розраховується наступним чином.

$$f_{(G_6 \to G_1)} = C_1 + C_2 + C_3 + C_4 + C_5 + C_6 + C_7 + C_8 =$$
$$= 1.91 + 2.09 + 2.13 + 2.21 + 2.15 + 2.17 + 1.95 + 2.33 + 2.42 = 19.36 \ [Мбіт/с]$$
$$f_{(G_6 \to G_2)} = C_2 + C_3 + C_4 + C_5 + C_6 + C_7 + C_8 =$$
$$= 2.09 + 2.13 + 2.21 + 2.15 + 2.17 + 1.95 + 2.33 + 2.42 = 17.45 \ [Мбіт/с]$$
$$f_{(G_6 \to G_3)} = C_4 + C_6 + C_8 + C_9 = 2.21 + 2.17 + 2.33 + 2.42 = 9.13 \ [Мбіт/с]$$
$$f_{(G_6 \to G_4)} = C_3 + C_6 + C_7 + C_8 = 2.13 + 2.17 + 2.33 + 2.42 = 9.05 \ [Мбіт/с]$$
$$f_{(G_6 \to G_5)} = C_1 = 1.91 \ [Мбіт/с]$$

За результатами аналізу видно, що навантаження створене в каналі 4-6 від мультисервісного трафіку включає в себе потоки IoT в реальному часі

(автоматичний аварійний виклик IoT (A), моніторинг температури (B), IoVT (C) в реальному часі) для яких, необхідно також забезпечити допустиму затримку E2E. Затримка E2E потоків IoT, що проходять по каналу, може бути визначена згідно формули.

$$D_{E2E} = \sum_{(i,j)\in E} d_{ij}. \tag{6.4}$$

У роботі оцінено затримку E2E для фонового мультисервісного IoT-трафіку, що проходить по перевантаженому каналу 4-6, в такий спосіб.

$D_{E2E(G_2 \to G_5)} = d_{24} + d_{46} + d_{65} = 24.5 + 200 + 35.6 = 260.1$ [*мс*]

$D_{E2E(G_4 \to G_5)} = d_{46} + d_{65} = 200 + 35.6 = 235.6$ [*мс*]

$D_{E2E(G_4 \to G_6)} = d_{46} = 200$ [*мс*]

$D_{E2E(G_5 \to G_2)} = d_{56} + d_{64} + d_{42} = 35.6 + 200 + 24.5 = 260.1$ [*мс*]

$D_{E2E(G_5 \to G_4)} = d_{56} + d_{64} = 35.6 + 200 = 235.6$ [*мс*]

$D_{E2E(G_6 \to G_2)} = d_{64} + d_{42} = 200 + 24.5 = 224.5$ [*мс*]

$D_{E2E(G_6 \to G_4)} = d_{64} = 200$ [*мс*]

У роботі також оцінено затримку E2E для потоків IoVT в реальному часі, що генеруються з G6, в такий спосіб.

$D_{E2E(G_6 \to G_1)} = d_{67} + d_{71} = 34.4 + 35.6 = 70$ [*мс*]

$D_{E2E(G_6 \to G_2)} = d_{67} + d_{71} + d_{12} = 34.4 + 35.6 + 27 = 97$ [*мс*]

$D_{E2E(G_6 \to G_3)} = d_{65} + d_{53} = 35.6 + 11.2 = 46.8$ [*мс*]

$D_{E2E(G_6 \to G_4)} = d_{64} = 200$ [*мс*]

$D_{E2E(G_6 \to G_5)} = d_{65} = 35.6$ [*мс*]

Згідно запропонованого методу адаптивної маршрутизації для запобігання перевантажень на каналі 4-6, проведено перерозподіл ресурсів, зокрема для інформаційних потоків IoT нереального часу оптимальним шляхом в мережі є 4-7-3-5 $f_{(G_4 \to G_5)_{unrealtime}} = F_2 + D_5 + D_9 + D_2 = 5.57 + 1.68 + 1.81 + 1.6 = 10.66$ [*Мбіт / с*], а також шлях 4-6-5 для потоків реального часу $f_{(G_4 \to G_5)_{realtime}} = C_5 + A_2 = 2.15 + 0.19 = 2.34$ [*Мбіт / с*], що генеруються з хоста G4 на G5. У роботі оцінено затримку E2E потоків IoT, що проходять через

перевантажений канал 4-6 в умовах використання запропонованого методу маршрутизації.

Затримка E2E для фонового мультисервісного IoT трафіку визначається наступним чином.

$$D_{E2E(G_2 \to G_5)} = d_{24} + d_{46} + d_{65} = 24.5 + 29.5 + 26 = 80 \ [мс]$$

$$D_{E2E(G_4 \to G_5)} = d_{46} + d_{65} = 29.5 + 26 = 55.5 \ [мс]$$

$$D_{E2E(G_4 \to G_6)} = d_{46} = 29.5 \ [мс]$$

$$D_{E2E(G_5 \to G_2)} = d_{56} + d_{64} + d_{42} = 26 + 29.5 + 24.5 = 80 \ [мс]$$

$$D_{E2E(G_5 \to G_4)} = d_{56} + d_{64} = 26 + 29.5 = 55.5 \ [мс]$$

$$D_{E2E(G_6 \to G_2)} = d_{64} + d_{42} = 29.5 + 24.5 = 54 \ [мс]$$

$$D_{E2E(G_6 \to G_4)} = d_{64} = 29.5 \ [мс]$$

Затримка E2E для потоків IoVT в реальному часі, що генеруються з G6, виглядає наступним чином.

$$D_{E2E(G_6 \to G_1)} = d_{67} + d_{71} = 34.4 + 35.6 = 70 \ [мс]$$

$$D_{E2E(G_6 \to G_2)} = d_{67} + d_{71} + d_{12} = 34.4 + 35.6 + 27 = 97 \ [мс]$$

$$D_{E2E(G_6 \to G_3)} = d_{65} + d_{53} = 26 + 13 = 39 \ [мс]$$

$$D_{E2E(G_6 \to G_4)} = d_{64} = 29.5 \ [мс]$$

$$D_{E2E(G_6 \to G_5)} = d_{65} = 26 \ [мс]$$

У процесі дослідження та порівняння відомої моделі маршрутизації DMCQR із запропонованою, досягнуто кращої збалансованості завантаження канальних ресурсів мережі за рахунок раціонального вибору шляхів для різнорідного трафіку (рис. 6.12б) та зменшено до 3 разів середню затримку обслуговування потоків реального часу з кінця в кінець для яких при використанні маршрутизації DMCQR не виконувались допустимі норми затримки (рис. 6.12в).

В цілому, вищенаведені результати показують, що запропонований метод маршрутизації потоків забезпечує необхідну якість обслуговування E2E для всіх критично важливих додатків IoT, на відміну методу маршрутизації DMCQR, розробленої авторами в роботі [32].

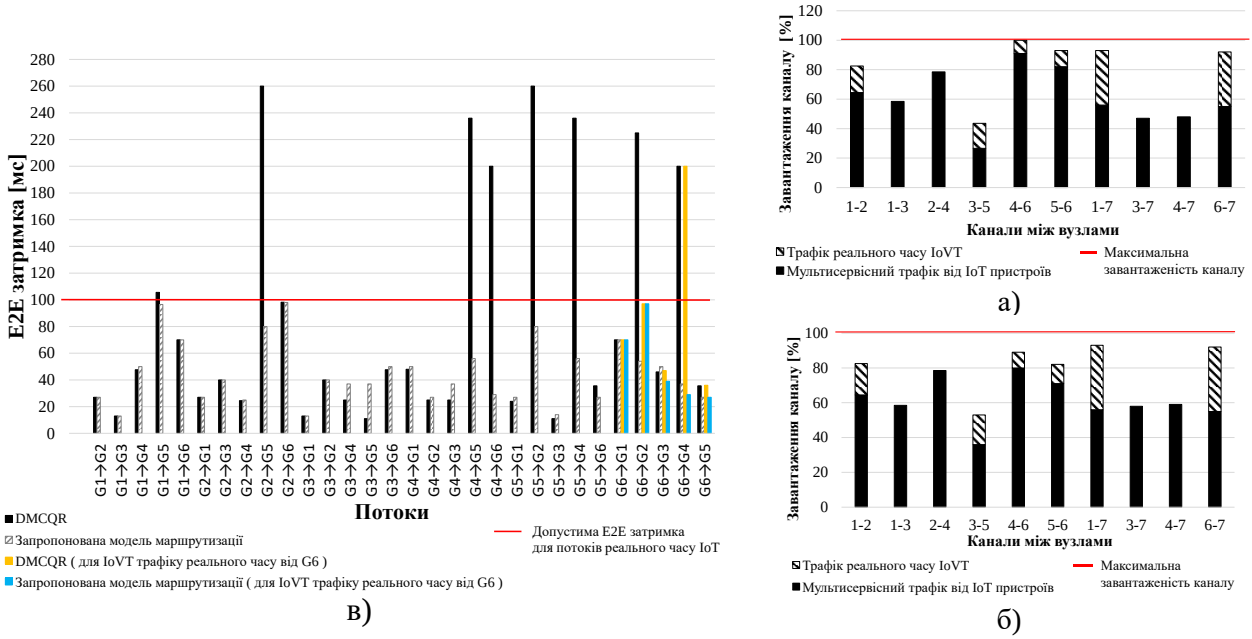


Рис.6.12. Завантаженість каналів в умовах використання DMCQR – а), завантаженість каналів в умовах використання запропонованої маршрутизації – б), порівняння моделей маршрутизації за критерієм затримки передавання даних – в) [255]

Згідно з дослідженням [256] споживання енергії Raspberry Pi 3 становить E = 8,1 [кДж/год]. Загальне споживання енергії розробленого прототипу мережі на день розраховується наступним чином:

$$E_{Network} = \sum_{i=i+1}^{24} (E \cdot n)_i \left[\text{kJ/h}\right], \tag{6.5}$$

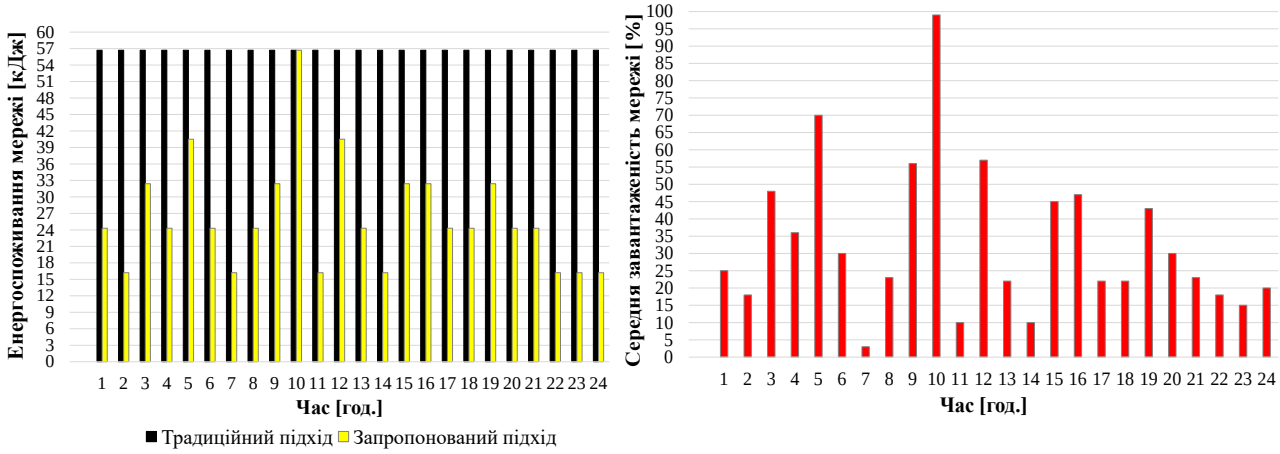
де n - кількість активних комутаторів SDN на основі Raspberry Pi, E енергоспоживання одного комутатора SDN.

Енергозбереження розраховується наступним чином:

$$K_{energy\ saving} = (1 - \frac{E_{network_{with\ our\ solution}}}{E_{network_{without\ our\ solution}}}) \cdot 100 \tag{6.6}$$

У роботі використано реальний експериментальний стенд прототипу SDN для дослідження ефективності QoE маршрутизації стосовно мінімізації енергоспоживання мережі. Для даного дослідження у мережі генерувалось різне навантаження протягом 24 годин протягом якого відбувалась активація та

деактивація комутаторів . Експериментальні результати показують, що загальне споживання енергетичної мережі без нашого рішення становить $E_{network_{without\ our\ solution}} = 1361[\text{kJ/h}]$ та із нашим $E_{network_{with\ our\ solution}} = 632[\text{kJ/h}]$.



а) б)

Рис.6.13. Результати експериментального дослідження процесу оптимізації рівня енергоспоживання інтенційно-орієнтованої мережі в умовах використання традиційного та запропонованого підходу – а) в залежності від завантаженості мережі – б) [247]

Таким чином встановлено, що в умовах низької інтенсивності загального трафіку (рис. 6.13б) досягається зменшення енергоспоживання мережі до 53,56% (рис. 6.13а).

6.2. Розробка прототипу корпоративного сегменту інтенційно-орієнтованої мережі на базі апаратних SDN комутаторів ZODIAC FX/GX

У попередньому підрозділі роботи було досліджено базову структуру програмно-конфігурованих мереж для Інтернету речей на базі одноплатних комп’ютерів з інтенційно-орієнтованою логікою управління. При дослідженні структури прототипу, виявлено ряд переваг поєднання згаданих технологій SDN/IoT. Після базової структури, у роботі описується процес розробки на основі цих же технологій більш прикладної задачі, зокрема для якісного

надання критично-важливого сервісу IoVT (відеопотоку реального часу). Враховуючи ряд потреб, котрі можуть виникнути на практиці, архітектуру даної системи було розроблено таким чином, щоб у подальшому без додаткових проблем масштабувати дану систему, а саме можливості у підключенні декількох відеокамер та користувачів без погіршення QoS. Для цього на розробленому прототипі мережі проведено реалізацію інтуїтивного міжсерверного балансування навантаження в умовах деградації QoS, а також аналіз зображення у реальному часі. Враховуючи, що дана система розроблена для критично-важливого сервісу, у ній також реалізовано зворотній проксі, котрий оптимізує трафік, шифрує пакети, балансує навантаження, захищає від розподілених атак на відмову. Реалізований зворотній проксі базується на певних аспектах DPI системи пропонованої у розділі 4.

Ключовим елементом для можливості масштабування пропонованої інтенційно-орієнтованої мережі вносить OpenFlow контролер та апаратний SDN комутатор Zodiac FX [257], який на відміну від розгорнутого віртуального комутатора на Raspberry забезпечує кращу продуктивність та більш гнучкіші можливості процесу передавання.

Дану систему було проаналізовано на ряд атрибутів якості, згідно стандарту ISO/IEC 25010, серед яких функціональна придатність, надійність, ефективність роботи, корисність, безпека, сумісність, технічне обслуговування та переносність.

6.2.1. Адаптивний вибір оптимального сервера обслуговування та реалізація балансування навантаження на базі розробленого прототипу із використанням SDN комутатора ZODIAC FX

Вся IBN система побудована на основі одноплатних комп’ютерів – RaspberryPi. У якості SDN є комутатор Zodiac FX котрим управляє і моніторить контролер OpenFlow на базі Ryu фреймворка. Доступ до відеопотоку відбувається через інтернет за допомогою веб-додатку, котрий знаходиться на

хостингу firebase, та доступний за посиланням. Так як сама система працює без шифрування, у системі реалізовано зворотній проксі, котрий шифрує і стискає дані. Зворотній проксі реалізовано за допомогою Ngnix. Також передбачено що система буде сильно навантажуватись, тому у створеній системі є два відеосервіси, і балансування навантаження між ними відбувається на зворотньому проксі. Зворотній проксі також обмежує кількість активних з'єднань для блокування різного роду атак на відмову. Кінцева структурна схема реалізованого прототипу зображена на рис.6.14.

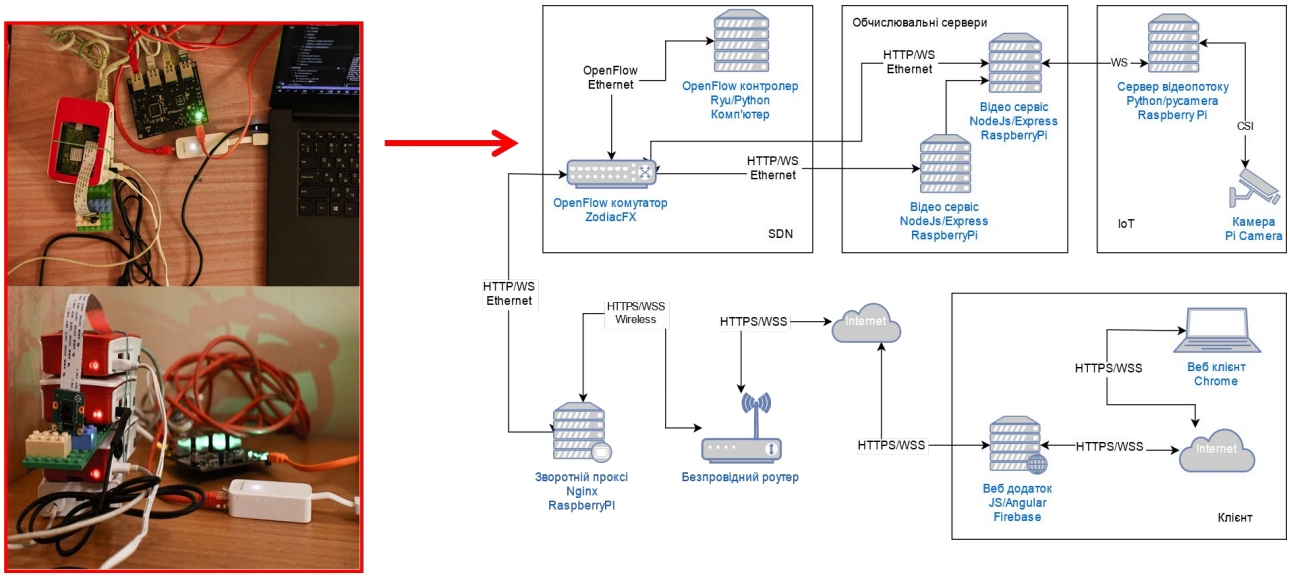
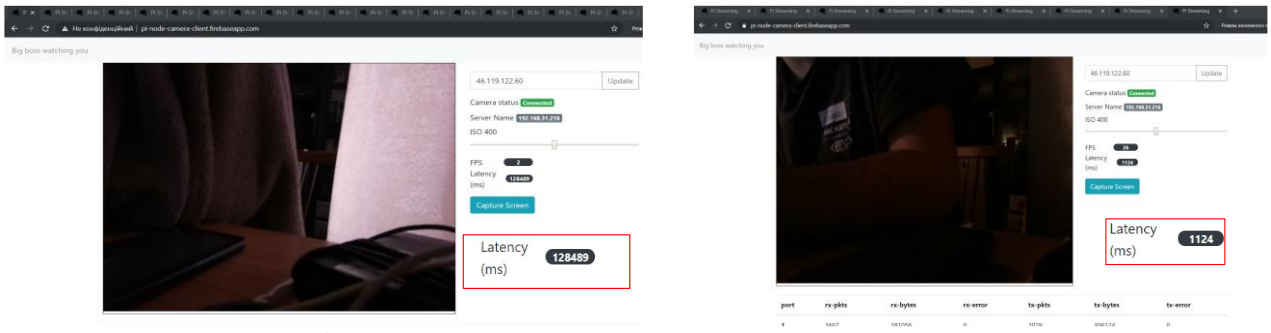


Рис.6.14. Структурна схема системи відеопотоку реального часу на базі програмно-конфігурованих мережах

Так як в першу чергу система використовується кінцевими користувачами за допомогою веб-додатку, всі подальші випробування, тестування та заміри будуть проводитись через веб-додаток. Даний веб-додаток розвернутий на безкоштовному хостингу з найдешевшим тарифним планом на Firebase від Google.

Необхідно провести тестування даної системи, скільки активних користувачів одночасно може користуватись системою. Для цього достатньо у анонімному вікні у веб-браузері Chrome відкрити необхідну кількість вкладок. Для першого тесту буде перевірено роботу з 20 активними з'єднаннями.

Результат тесту показано на рис. 6.15. Як видно, що затримка різко піднялась до неприйнятних показників (128489 мс), і значення кадрів на секунду дуже низьке, що не уможливлює використання даної системи.



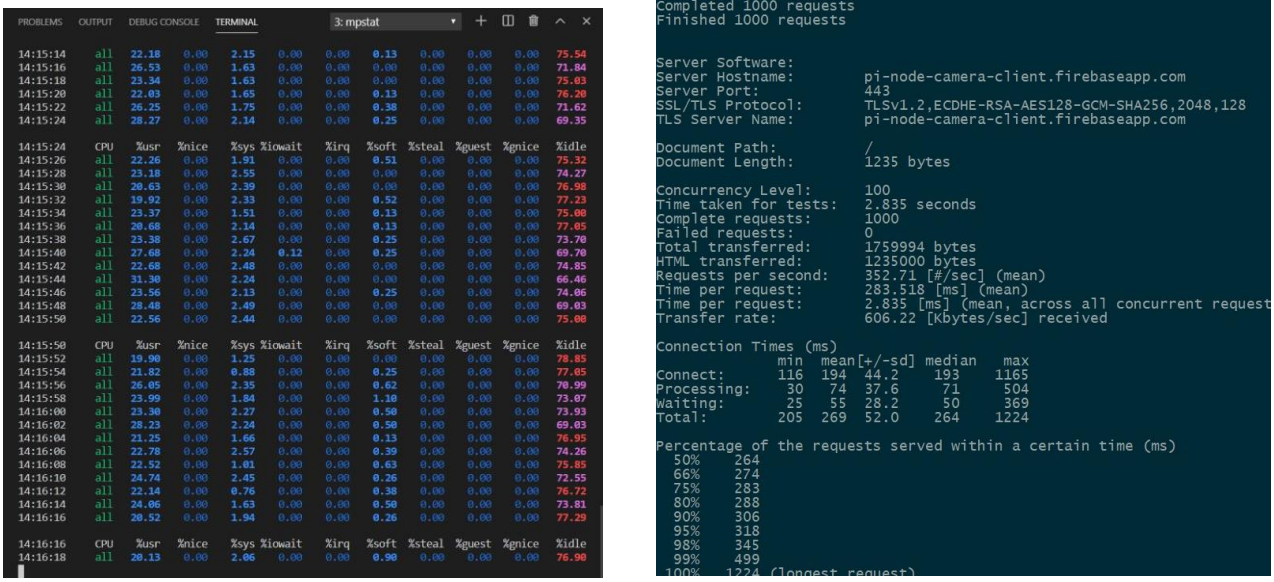
а) б)

Рис. 6.15. Тестування в умовах 20 активних підключень без балансування навантаження – а) та із запропонованим методом вибору сервера обслуговування – б)

Реалізація запропонованого механізму балансування завантаження має на меті оптимізувати використання ресурсів, максимізувати пропускну здатність, мінімізувати час відгуку та уникнути перевантаження. У даній системі на зворотному проксі реалізовано балансування навантаження. Адже коли клієнти будуть доступатись до системи, на вході проксі також відразу буде розвантажувати систему між серверами. Так як зворотній проксі розроблено за допомогою сервера Ngnix, завдання по балансуванню навантаження на себе також візьме Ngnix [258]. У Ngnix реалізовано функціональність для підтримки балансування навантаження. Логіка балансування полягає у виявленні моментів погіршення параметрів QoS.

Після проведення аналогічного тестування у роботі використано балансування навантаження для 10 активних користувачів (рис.6.15б). У цьому випадку затримка коливається трішки більше секунди (1124 мс), проте для користування є цілком прийнятним. Таким чином у роботі доведено ефективність запропонованого підходу щодо адаптивного вибору сервера обслуговування з точки зору забезпечення якості обслуговування користувачів.

Разом з цим паралельно також порівнювалось навантаження на систему, на котрій запущенг відеосервіс. Використовуючи mpstat - команду Unix-подібних операційних систем для отримання статистики пов’язаної з процесором, було проведено аналіз навантаження системи (у даному випадку RaspberryPi). На рис. 6.16а подано результат виконання даної функції. Як видно що кількість активних з’єднань в прийнятних межах, не збільшують навантаження на систему.



а) б)

Рис. 6.16. Статистика навантаження відеосервісу Mpsta – а) та результат тестування навантаження програмою ab – б)

Також варто провести тестування для веб-додатку, скільки може обробити запитів одночасно. Для цього було використано утиліту – ab. ab - Apache HTTP серверна команда для проведення тестування навантажень на сервер, через створення декількох паралельних запитів. Для проведення було використано стандартні налаштування бібліотеки, 1000 запитів, по 100 запитів паралельно. Результати подано на рис. 6.16б. Як видно, що середній час на встановлення

з’єднання було 193 мс, обробка запиту – 71 мс, очікування 50 мс і сумарно 264 мс. Подані дані показано для здійснення https запиту на веб-додаток.

Передача відеопотоку здійснюється через протокол WSS [259]. Для отримання даних про з’єднання через протокол WSS, використано програму Telerik Fiddler. Fiddler - це програма, котра перехоплює всі запити, дозволяє їх модифікувати, видаляти та досліджувати. Також дана програма вміє розшифровувати трафік зашифрований по SSL та TSL. Коли користувач вперше потрапляє на веб-додаток, він спочатку завантажує статичні файли для веб-сторінки HTML, CSS, JS, а далі здійснює запит на з’єднання з відеопотоком. Сумарний час складає 15 секунд, і об’єм всіх ресурсів 510 Кбайт для веб-додатку. Дані подані на рис.6.17.

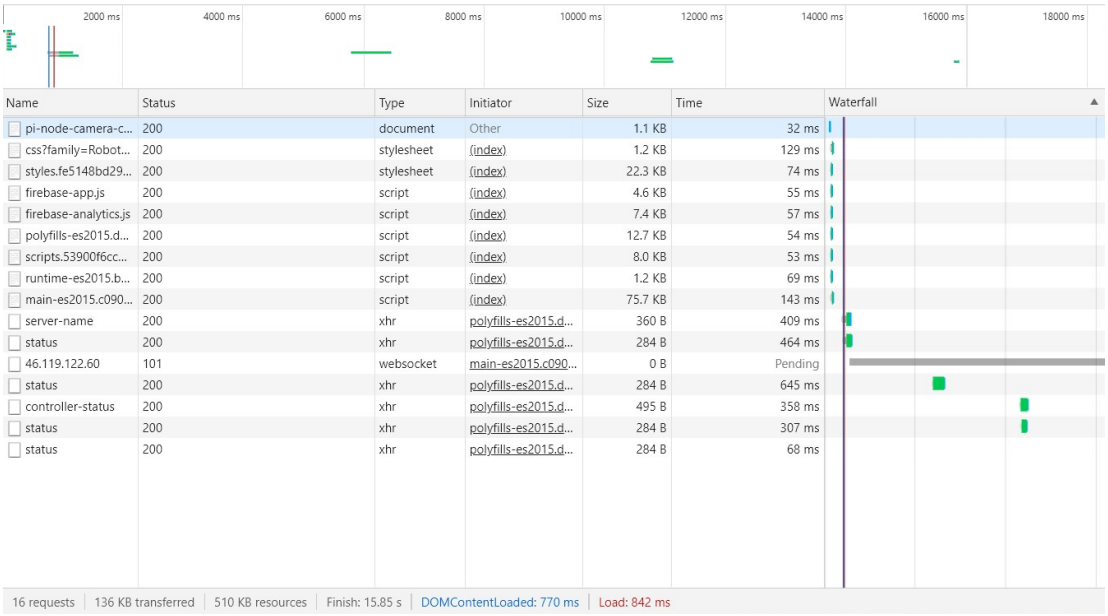


Рис. 6.17. Ресурси для веб-додатку

При спілкуванні через WSS, відео передається пакетами. Розмір кожного пакета складає приблизно 1.5 Кбайт, а затримка між кожним пакета 30-100 мс (рис. 6.18).

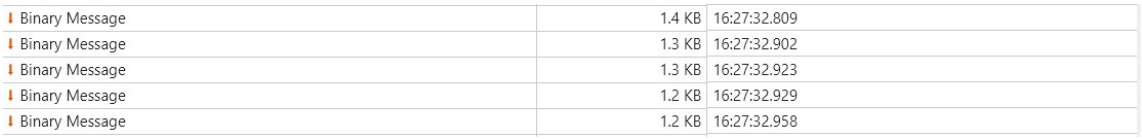


Рис. 6.18 Пакети по WSS

Також проведено аналіз затримок у порівнянні з’єднання локально та через інтернет у веб-додатку, та аналогічно для 1-го та 10-и підключень. На рис.6.19 показано графік затримок у веб-додатку. Дана затримка показує час проходження пакету від сервера відеопотоку до веб-додатку. У результаті можна сказати, що при підключенні 10 клієнтів, створюється незначна загальна затримка (в діапазоні 10-50 мс), що також властиве і у випадку при підключенні через локальний веб-додаток так і через інтернет. Локальний веб-додаток на відміну від інтернет веб-додатку, не потребує проходження через проміжні з’єднання, відповідно складає меншу затримку, згідно графіку можна приблизно оцінити дану затримку в діапазоні 150-250 мс.

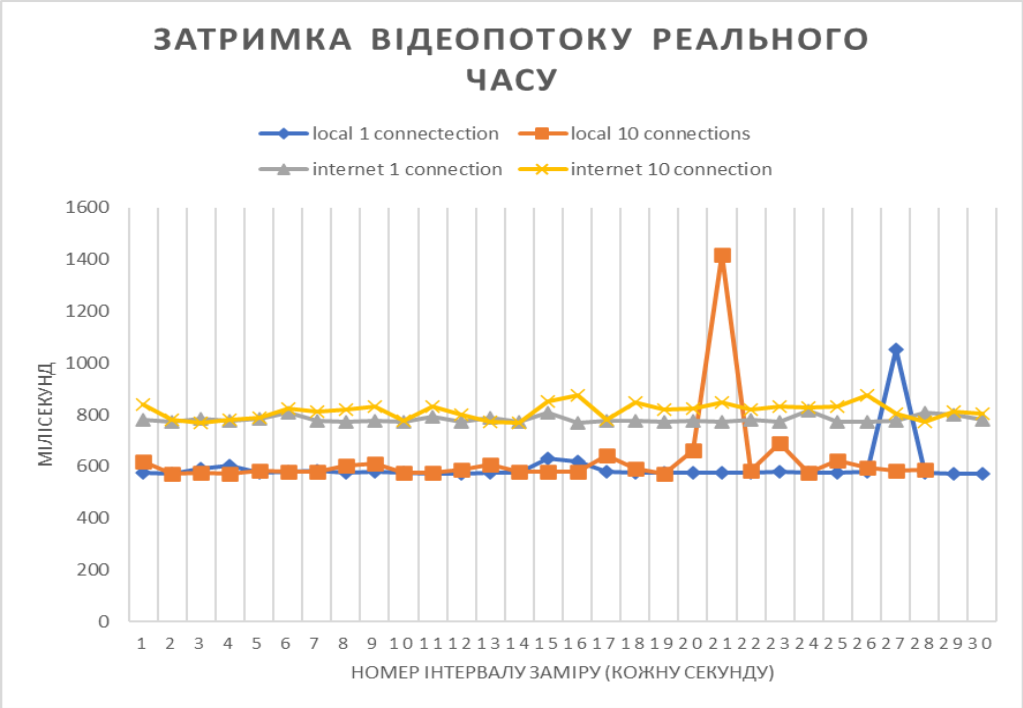


Рис. 6.19. Затримка відеопотоку реального часу

У архітектурі даної системи є зворотній проксі, котрий використовує для цього Nginx із модифікованою логікою. Одним із способів захисту від даних атак, що пропонується у роботі є обмеження кількості підключених одночасно з’єднань з однієї IP адреси. Було обрано обмеження у 5 з’єднань.

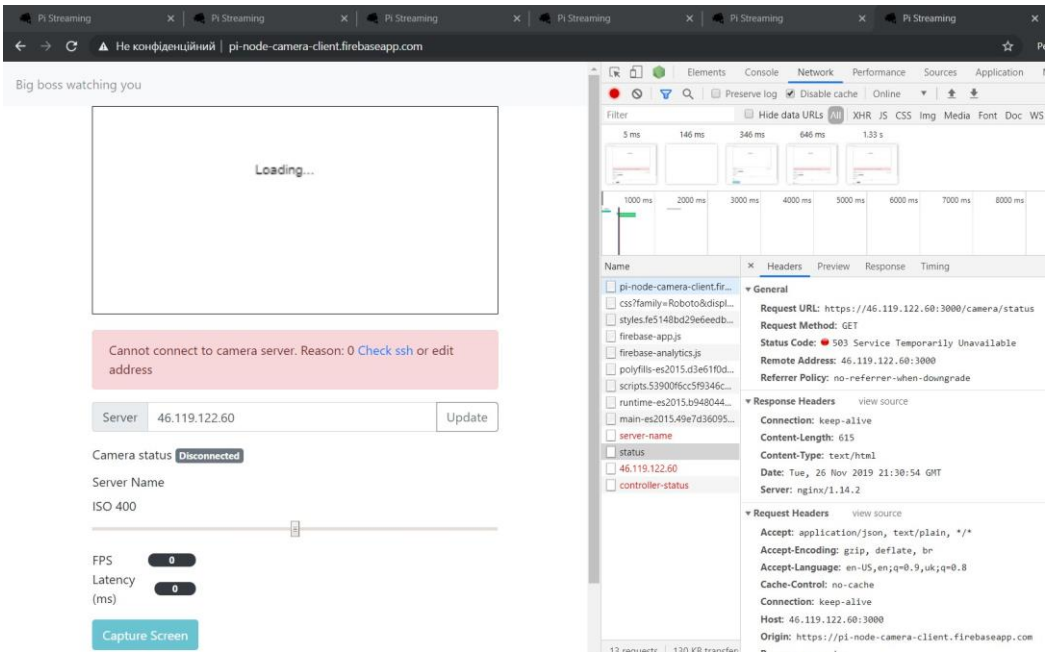


Рис. 6.20. Захист від DDOS атаки

Після налаштування Nginx, на рис.6.20. видно що після підключення 6 вкладок у веб-браузері, на останній вкладці, буде видно що з’єднання не встановлено, і як видно, що від сервера прийшла відповідь 503 помилка, котра вказує що сервіс тимчасово не доступний.

6.2.2. Практична реалізація QoE системи моніторингу та маршрутизації в SDN мережі, що базується на комутаторах ZODIAC GX та контролера ONOS

У роботі на основі апаратних SDN комутаторів ZODIAC GX [260] побудовано прототип інтенціно-орієнтованої мережі, в межах якого успішно реалізовано метод клієнт-орієнтованого управління якістю обслуговування, який, на відміну від існуючих для вибору маршруту передавання даних базується на метриці порогового значення критерію QoE. Для цього впершу чергу було реалізовано моніторингову QoE систему, яка дає змогу на основі QoS аналізу стану мережі виявляти вузькі місця в SDN мережі та автоматизовано встановлювати маршрут передавання даних для покращення

показника якості сприйняття послуги в умовах його деградації шляхом переконфігурування мережі. Це досягається за допомогою ONOS контролера SDN та реалізації додаткової функціональності поверх нього, щоб змінити шлях передавання трафіку на альтернативний, коли QoE опускається нижче заданого порогу.

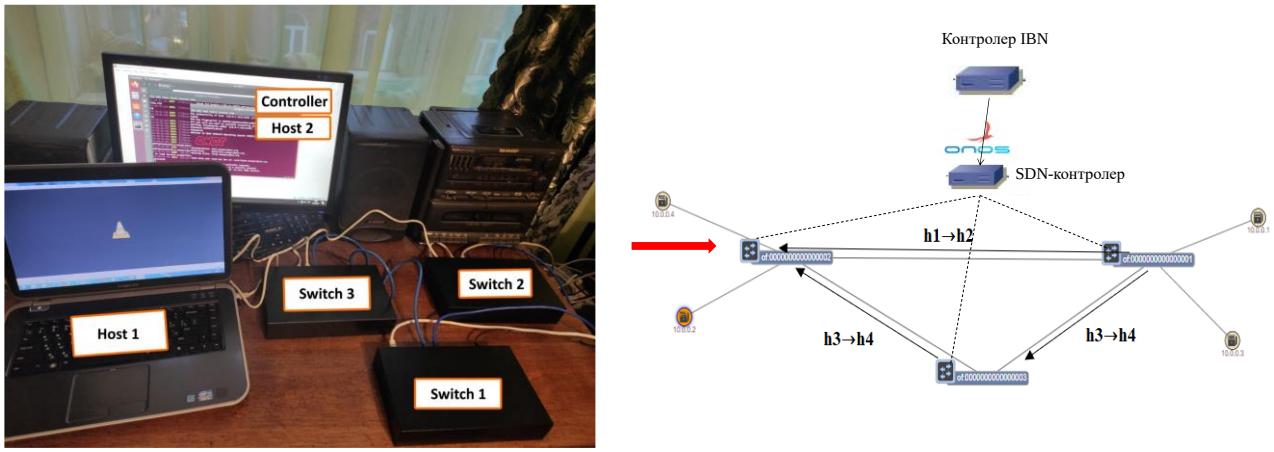
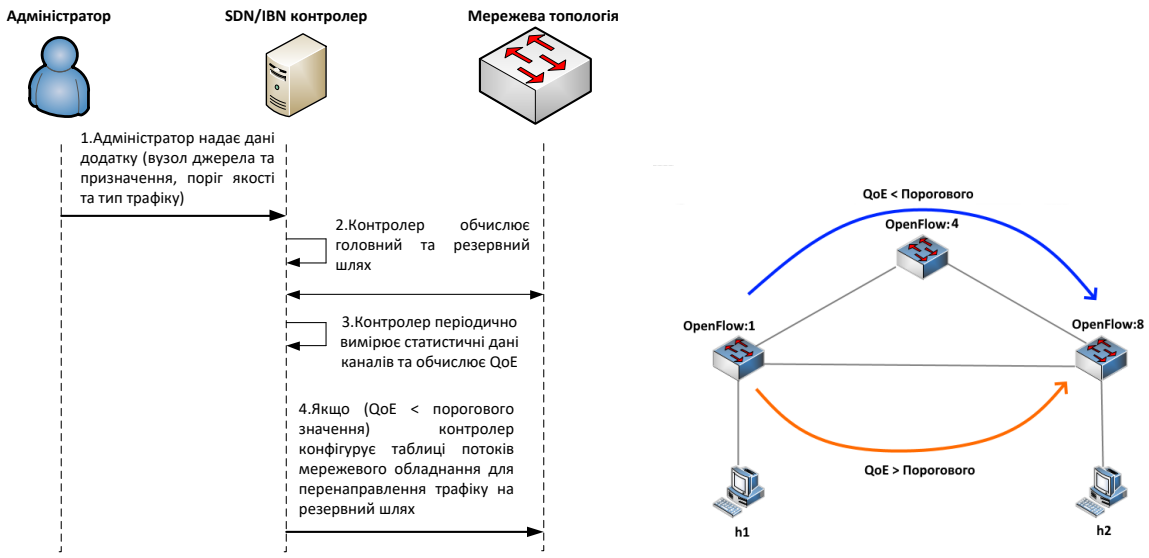


Рис. 6.21. Прототип корпоративного сегменту інтенційно-орієнтованої мережі побудованого на базі апаратних SDN комутаторів ZODIAC GX та ONOS контролера IBN

Підхід, який використовується для того, щоб забезпечити збереження QoE на задовільних рівнях, це періодичний моніторинг та оцінка якості на основі їх статистичних даних. Зокрема, програма обчислює найкоротший шлях між вихідним та кінцевим хостами, який буде як основний шлях передачі, а також другий найкоротший шлях (якщо такий існує), який буде резервним у випадку незадовільної якості обслуговування в процесі передавання відеопотоку реального часу. Потім починається процес моніторингу якості; контролер IBN/SDN періодично збирає статистику з комутаторів (різні статистичні дані для кожного типу програми) і використовує їх для обчислення QoE рівня за 5-бальною шкалою. Якщо передбачуване значення нижче вказаного порогу, тоді автоматично встановлюються відповідні правила для перенаправлення трафіку на альтернативний шлях. Процес роботи, описаний вище, графічно показаний на рис. 6.22.



а) б)

Рис. 6.22. Принцип роботи QoE системи моніторингу – а) та топологія досліджуваної мережі –б [261]

Кожного разу, коли контролеру потрібно виміряти затримку, він створює пакет із конкретною MAC-адресою джерела - зокрема 00: 00: 00: 00: 00: 09 - і надсилає його кожному комутатору в мережі (за винятком вихідного комутатора) до вихідного інтерфейсу, так що наступний комутатор отримує його. Детальний принцип вимірювання затримки описано у розділі 2.4. Кожен комутатор (за винятком вхідного комутатора, оскільки у нього немає попереднього комутатора для прийому пакету) налаштований з відповідним правилом потоку для пересилання контролеру будь-якого пакету з конкретною MAC-адресою. Різниця між часом, коли комутатор отримує пакет, і часом, коли попередній комутатор надіслав пакет, полягає у затримці певної лінії зв'язку. Додавання затримок усіх каналів зв’язку шляху призводить до затримки шляху. Кожен комутатор налаштований за правилом такого формату:

priority=1000,dl_src=00:00:00:00:00:09 actions=CONTROLLER:65535

На основі даного дослідження написано Python скріпт, який працює на контролері ONOS.

```
received_time = time.time() * 1000 - start_time

#measure T1
if event.connection.dpid == src_dpid:
  OWD1=0.5*(received_time - sent_time1)
  #print "OWD1: ", OWD1, "ms"

#measure T2
elif event.connection.dpid == dst_dpid:
  OWD2=0.5*(received_time - sent_time1)
  #print "OWD2: ", OWD2, "ms"
```

а)

```
received_time = time.time() * 1000 - start_time

if packet.type==0x5577 and event.connection.dpid==dst_dpid:
  c=packet.find('ethernet').payload
  d,=struct.unpack('!I', c)
  print "delay:", received_time - d - OWD1-OWD2, "ms"
```

б)

Рис.6.23. Обчислення параметрів Ts1 та Ts2 – а), обчислення значення затримки – б)

```
INFO:openflow.of_01:[00-00-00-00-00-01 1] connected
ConnectionUp:  00-00-00-00-00-01
INFO:openflow.of_01:[00-01-00-00-00-01 2] connected
ConnectionUp:  00-01-00-00-00-01
delay: 17.6373291016 ms
delay: 10.1243896484 ms
delay: 10.1201171875 ms
delay: 11.1755371094 ms
delay: 11.6986083984 ms
delay: 12.6079101562 ms
delay: 11.0582275391 ms
delay: 10.1243896484 ms
```

Рис.6.24. Результат вимірювання затримки скріптом

На рис. 6.24 зображено виміряну затримку між s1 та s2, при заданій затримці каналу зв’язку 10 мс.

Також на рис. 6.25 описано процес вимірювання затримки на топології мережі.

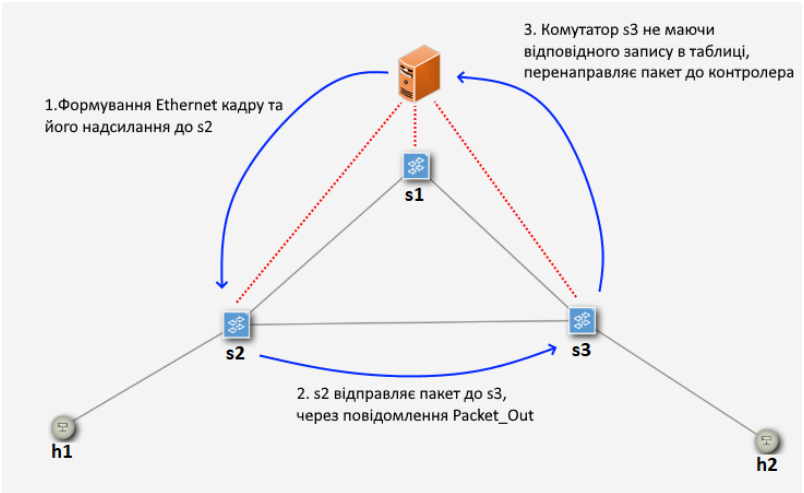


Рис. 6.25. Процес вимірювання затримки у мережі [261]

Для обчислення втрат пакетів та враховуючи, що відеотрафік передається UDP-пакетами, контролер SDN періодично контролює кількість UDP-пакетів, відправлених від відправника (h1), і кількість UDP-пакетів, отриманих приймачем (h2), і обчислює їх різницю, поділену на кількість відправлених пакетів.

Для реалізації моніторингу втрат пакетів, вхідні та вихідні комутатори налаштовані так, щоб пересилати контролеру - крім заздалегідь визначеного вихідного інтерфейсу на наступний вузол - будь-який отриманий ними пакет UDP (вхід отримує UDP-пакети від хоста відправника та вихід із попереднього вузла шляху). У свою чергу, контролер підраховує загальну кількість вхідних та вихідних пакетів UDP шляху та може визначити втрату пакетів. Вхідний і вихідний комутатори налаштовуються за допомогою правил наступного формату:

priority=1000,udp,in_port=x actions=CONTROLLER:65535,output:y

Наприклад, відповідними правилами для OpenFlow:1 та OpenFlow:8 є:

OF1: priority=1000,udp,in_port=1 actions=CONTROLLER:65535,output:3

OF8: priority=1000,udp,in_port=3 actions=CONTROLLER:65535,output:2

Принцип обчислення втрат пакетів наступний, контролер отримує статистичні дані про втрати пакетів комутаторів s2 та s3. За отриманою статистикою переданих та прийнятих пакетів на відповідних комутаторах контролер обчислює загальну кількість втрачених пакетів за формулою 6.7.

$$packetLoss(report) = input\_pkts - output\_pkts \quad (6.7)$$

Процес вимірювання втрат пакетів відбувається наступним чином, у мережі з вище вказаною топологією, штучно вводяться втрати каналу зв`язку на ділянці шляху s2→s3, втрати пакетів рівні 10%. Тоді h1 через утиліту ping відправляє пакети до h2. Далі IBN контролер відправляє запит на статистичні дані від комутаторів і обчислює процент втрат пакетів.

```
ConnectionUp:  00-00-00-00-00-01
INFO:openflow.of_01:[00-01-00-00-00-01 2] connected
ConnectionUp:  00-01-00-00-00-01
[2020-12-7]11.37.55 Path Loss Rate = 0.0 %
[2020-12-7]11.37.56 Path Loss Rate = 0.0 %
[2020-12-7]11.37.57 Path Loss Rate = 0.0 %
[2020-12-7]11.37.58 Path Loss Rate = 0.0 %
[2020-12-7]11.37.59 Path Loss Rate = 0.0 %
[2020-12-7]11.38.00 Path Loss Rate = 0.0 %
[2020-12-7]11.38.01 Path Loss Rate = 0.0 %
[2020-12-7]11.38.02 Path Loss Rate = 12.5 %
[2020-12-7]11.38.03 Path Loss Rate = 11.1111111111 %
[2020-12-7]11.38.04 Path Loss Rate = 10.0 %
[2020-12-7]11.38.05 Path Loss Rate = 9.09090909091 %
[2020-12-7]11.38.06 Path Loss Rate = 8.33333333333 %
[2020-12-7]11.38.07 Path Loss Rate = 7.69230769231 %
[2020-12-7]11.38.08 Path Loss Rate = 7.14285714286 %
[2020-12-7]11.38.09 Path Loss Rate = 6.66666666667 %
[2020-12-7]11.38.10 Path Loss Rate = 6.25 %
[2020-12-7]11.38.11 Path Loss Rate = 5.88235294118 %
[2020-12-7]11.38.12 Path Loss Rate = 5.55555555556 %
[2020-12-7]11.38.13 Path Loss Rate = 10.5263157895 %
[2020-12-7]11.38.14 Path Loss Rate = 10.0 %
[2020-12-7]11.38.15 Path Loss Rate = 10.0 %
```

Рис.6.26. Результат вимірювання втрат пакетів

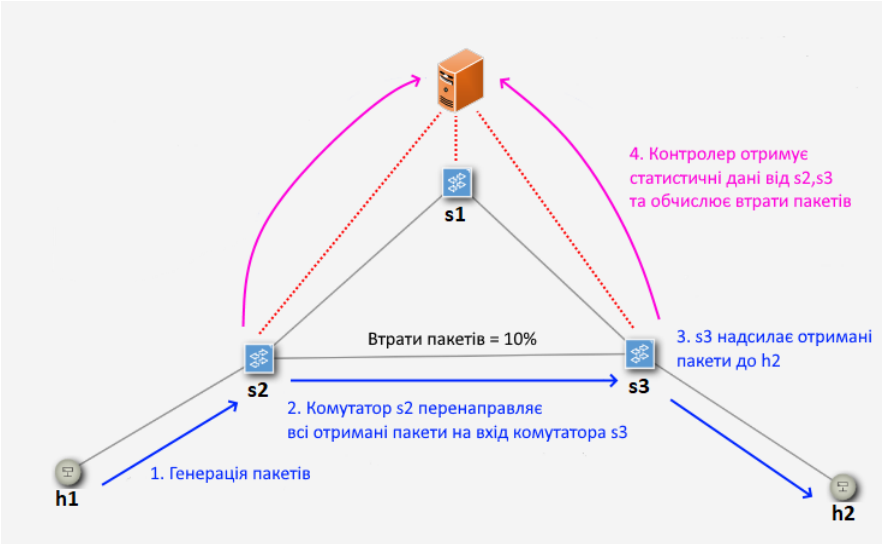


Рис. 6.27. Метод вимірювання втрат пакетів [261]

Для того, щоб обчислити бітрейт, команда ffmpeg –i [VIDEO_PATH] –hide_banner виконується через код Java, і вихідні дані аналізуються, поки не буде здійснено доступ до значення бітрейту. Для того, щоб обчислити частоту кадрів, команда –i [VIDEO_PATH] –hide_banner виконується за допомогою коду Java, і вихідні дані аналізуються, поки не буде отримано доступ до значення частоти кадрів. Результати QoE моніторингової системи показано на рис.6.28 - 6.30.

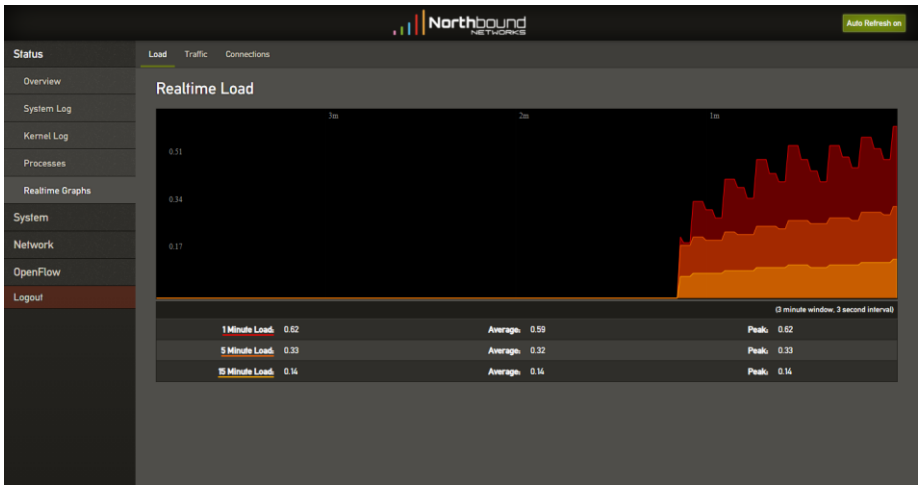


Рис.6.28. Моніторинг завантаженості комутатора ZODIAC GX

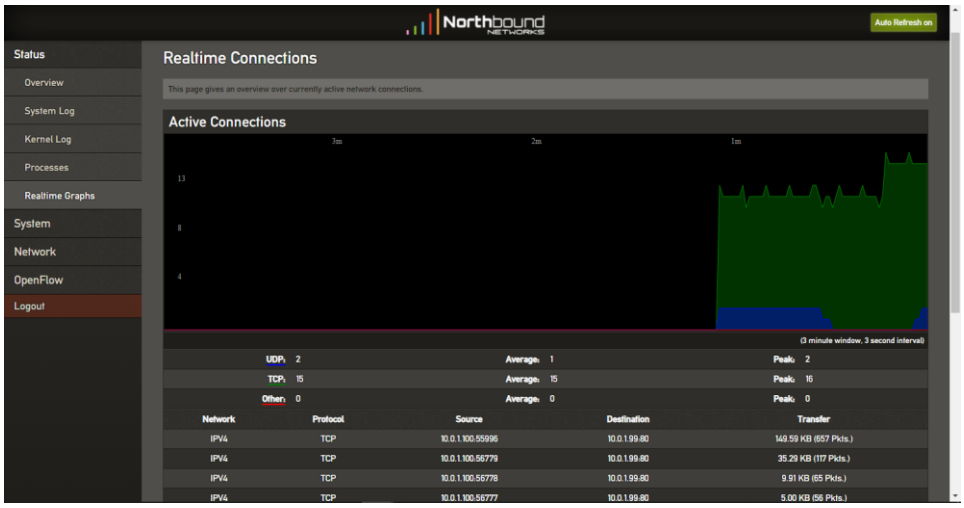


Рис.6.29. Моніторинг трафіку по протоколах в комутаторі ZODIAC GX

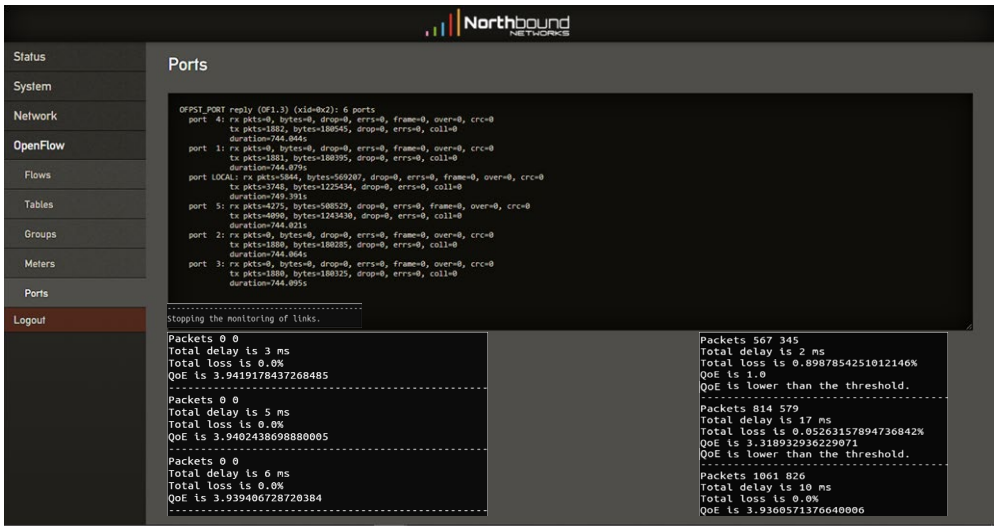
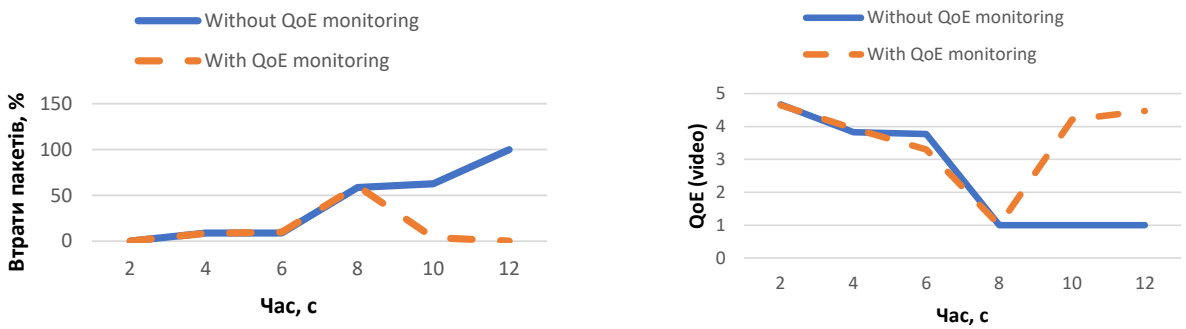


Рис.6.30. Моніторинг QoE рівня та фіксації його деградації [261]

У роботі проведено дослідження розробленої QoE системи моніторингу та маршрутизації потоків, зокрема дослідження проведено з потоковою передачею відео реального часу. Експеримент проводився протягом 12 секунд, сам трафік генерується між хостами h1 і h2. Кожні 4 секунди параметри каналів зв'язку погіршувались через введення штучних втрат пакетів. При порівнянні результатів, видно, що запропонована система моніторингу може зменшити кількість втрат пакетів і, як правило, поліпшити якість обслуговування у випадку потокового відео та відповідно забезпечити кращу якість сприйняття послуги для кінцевих користувачів (рис.6.31).



а) б)

Рис.6.31. Порівняння втрат пакетів – а) та рівня QoE – б) в процесі передавання відеопотоку без запропонованої системи моніторингу та із розробленою QoE системою моніторингу [261]

На основі проведеного дослідження встановлено, що без запропонованої системи моніторингу контролер не реагує на погіршення оцінки якості відео, що призводить до незадовільної якості обслуговування. Доведено ефективність використання розробленої QoE моніторингової системи, згідно якої у умовах виявлення погіршення рівня QoE відеопотоку в каналі зв’язку проводиться перенаправленням трафіку на альтернативний шлях передавання шляхом автоматизації процесів запропонованої QoE маршрутизації.

6.3. Розробка прототипу мобільного та операторського додатку для адаптивного клієнт-орієнтованого надання послуг в гетерогенній IBN мережі

Розроблення засобів зворотного зв'язку між клієнтом і оператором щодо адаптації рівня якості надання сервісів чи їх намірів в умовах мінливих вимог користувачів є одним із важливих та невирішених на сьогоднішній час завдань для повноцінної реалізації концепції інтенційно-орієнтованої мережі. Саме тому у роботі пропонується практична реалізація такого засобу, зокрема розроблено прототип мобільного та операторського додатку для адаптивного клієнт-орієнтованого надання послуг в гетерогенній інтенційно-орієнтованій мережі. Концептуальна модель гетерогенної мережі IBN з використанням пропонованого мобільного та операторського додатку показана на рис. 6.32

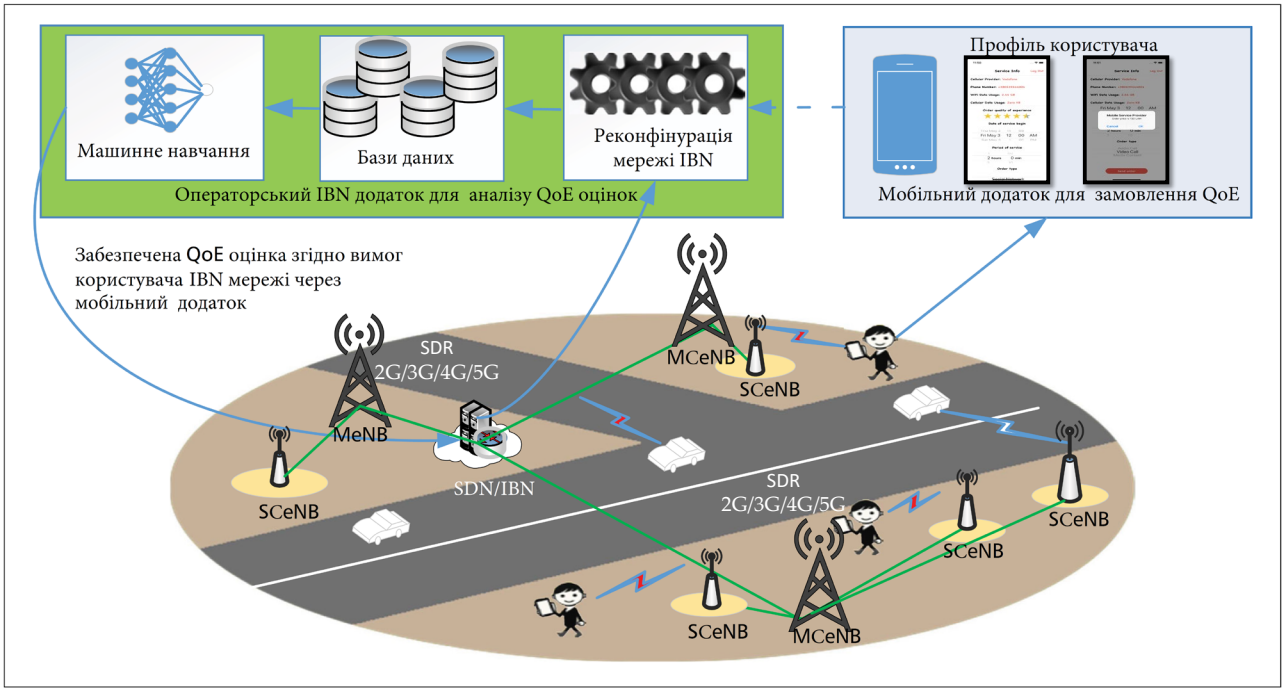


Рис. 6.32. Концептуальна модель гетерогенної мережі IBN із QoE додатком

Використання даного підходу дасть змогу операторам мережі забезпечити індивідуалізацію обслуговування користувачів з певним рівнем якості надання сервісів шляхом аналізу їх QoE оцінок (замовлених через розроблений мобільний додаток) та із допомогою алгоритмів машинного навчання реагувати

на несприятливі поєднання значень показників якості і попереджати ситуації, коли користувач незадоволений якістю отриманих сервісів для адаптивного прогнозування моменту переконфігурації мережі.

Для розробки даного QoE мобільного додатку використано:

1. Платформу розробки мобільних та веб-застосунків Firebase;

2. Середовище розробки xCode;

3. Емулятор мобільного пристрою iOS Simulator.

На рис. 6.33 зображено функціональні можливості мобільного додатку.

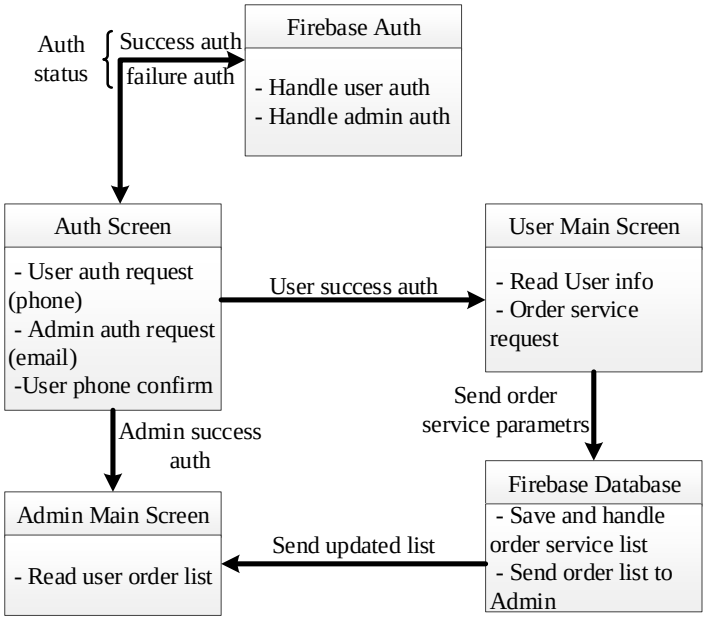


Рис. 6.33. UML-діаграма мобільного додатку Mobile-Service-Provider

Початковим екраном після запуску додатку є “*Authorization Screen*”, він призначений для аутентифікації, як адміністратора мережі IBN чи звичайного користувача. Основними функціями даного блоку є:

– *User authorization request* - Запит на авторизацію звичайного користувача;

– *Admin authorization request* - Запит на авторизацію адміністратора;

– *User phone confirmation code* - Підтвердження номеру звичайного користувача за допомогою коду який буде надіслано на мобільний номер після авторизації через Firebase Auth.

При авторизації дані користувача (мобільний телефон) чи дані адміністратора (електронна пошта та пароль) відсилаються в службу “Firebase Auth” яка має можливість виконувати такі функції даного блоку:

– *Handle user authorization credential* - обробляти дані користувача та підтверджувати чи відхиляти авторизацію;

– *Handle admin authorization credential* - обробляти дані адміністратора та підтверджувати чи відхиляти авторизацію.

Далі при успішній авторизації користувача, відкривається “User Main Screen” блок який має такий набір функцій:

– *Read user info* - користувач може переглядати інформацію по своєму аккаунту;

– *Order service request* - зробити запит на надання послуг по замовленню.

Якщо користувач зробив запит на надання послуг, виконується надсилання даних в базу даних служби *“Firebase Database”,* даний блок виконує такі функції:

– *Save and handle order serivce* - дані обробляються та зберігаються в базі даних яка формує список запитів;

– *Send order list to admin menu* - дана функція автоматично при любих змінах в базі даних відсилає оновлений список запитів до адміністратора.

– *Read user order list* - адміністратор може переглядати список запитів від користувачів та відштовхуючись від цього при потребі редагувати дані запити через доступ до Firebase.

Платформа Firebase потрібна для використання двох сервісів, які вона надає, таких як *Firebase Auth ma Firebase Database*.

Firebase Auth — це служба, яка може аутентифікувати користувачів, використовуючи лише код на стороні клієнта. Він підтримує соціальні логін-провайдери Facebook, GitHub, Twitter і Google (і Google Play Games). Крім того, вона включає в себе систему управління користувачами, за допомогою якої розробники можуть увімкнути автентифікацію користувача за допомогою входу з електронної пошти та пароля, що зберігаються в Firebase.

Firebase Database надає в режимі реального часу базу даних та сервер як службу. Ця служба надає розробникам застосунків API, який дозволяє синхронізувати дані застосунків між клієнтами та зберігати їх у хмарі Firebase.

6.3.1. Можливості клієнтської частини мобільного програмного забезпечення

Для створення мобільного додатку на платформу iOS використано середовище розробки xCode та мову програмування Swift.

При відкриванні додатку користувач мобільного додатку попадає на екран аутентифікації. У користувача є два типи аутентифікації, через мобільний телефон, що використовується для звичайних користувачів, які хочуть замовити послугу мобільного зв'язку та через електронну пошту, що використовується адміністратором для перегляду списку замовлень через додаток. Для прикладу розглянемо аутентифікацію клієнта в розробленому додатку, який матиме можливість замовити послугу мобільного зв'язку.

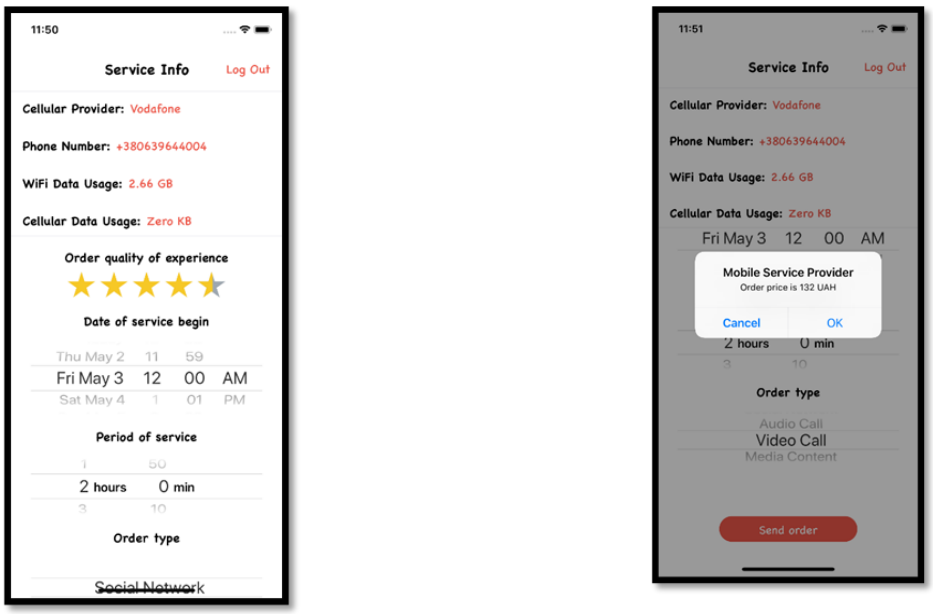
Користувачу потрібно ввести власний мобільний номер до якого буде прив'язаний його аккаунт в додатку за допомогою служби Firebase Auth.

Формат номеру телефону має мати такий вигляд "+380XXXXXXXXX". Далі користувач при натиску на кнопку "Sign In" переходить на браузерне вікно де служба Firebase Auth перевіряє автоматично чи за допомогою перевірки, що реальна людина пробує авторизуватись в додаток. При успішній перевірці служби Firebase Auth, користувачу відкривається вікно підтвердження мобільного номеру на який надіслали код підтвердження для аутентифікації.

Користувачу потрібно ввести код підтвердження в поле вводу та натиснути кнопку "OK", якщо код введено правильний, користувачу відкривається екран з власною короткою інформацією та інтерфейсом для замовлення послуг мобільного зв'язку. В навігаційному меню зображено заголовок екрану та кнопку "Log Out" яка дає змогу користувачеві вийти з свого аккаунту в додатку.

На екрані головного меню в верхньому блоці відображається інформація користувача: (Мобільний провайдер, Номер телефону, Кількість використаного трафіку через “Wi-Fi”, Кількість використаного трафіку через мобільні дані (2G-4,5G).

Користувач має можливість задати параметри по яких буде надаватись послуга: оцінка QoE, що характеризує рівень якості надання послуг; дату коли почати надавати дану послугу; період надання даної послуги; тип сервісу для якої будуть надаватись послуги.



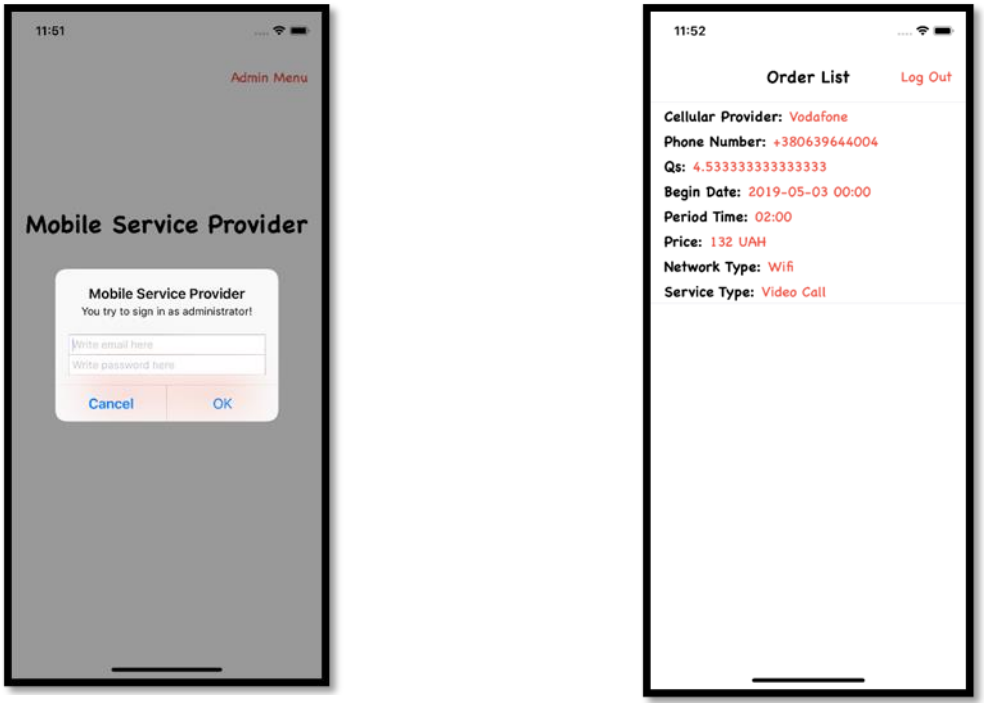
а) б)

Рис. 6.34. Вікно підтвердження замовлення – а) та екран головного меню зі зміненими параметрами замовлення послуги – б)

На рис. 6.34а. показано стан додатку при прокручуванні вниз блоку з замовленням послуги по певних критеріях які вибрав користувач. Також тут розташована кнопка “Send order”, яка відкриває користувачеві вікно з підтвердження даного замовлення. У вікні відображається ціна даного замовлення, користувач має можливість відмінити запит на отримання даної послуги чи підтвердити її за допомогою кнопок “Cancel” та “OK” (рис.6.34б).

6.3.2. Можливості операторської частини мобільного програмного забезпечення

Оператору мобільного зв'язку чи адміністратору для того, щоб аутентифікуватись в додатку потрібно натиснути на кнопку "Admin menu" яка відкриє вікно з полями для аутентифікації адміністратора.



а) б)

Рис. 6.35. Головний екран адміністратора зі списком замовлень послуг – а) та вікно аутентифікації адміністратора - б)

Адміністратор аутентифікується використовуючи електронну пошту та пароль створений для нього. Користувач має можливість відхилити аутентифікацію як адміністратор чи підтвердити її за допомогою кнопок "Cancel" та "OK". В концепції IBN функції системного адміністратора виконує інтелектуальний контролер, який вміє перетворювати певні наміри в набір команд для реалізації автоматизованого управління. Якщо користувач успішно аутентифікувався як адміністратор відкривається головний екран адміністратора. Так само як і звичайний користувач адміністратор має можливість вийти з свого аккаунту за допомогою кнопки "Log Out".

Також на екрані відображається список усіх замовлень користувачів посортований по даті початку надання послуг покращення мобільного зв’язку.

Кожне замовлення відображається з такими параметрами: Назва провайдера; Мобільний номер замовника послуги; QoE (якість надання послуг); Дата початку надання послуг; Період надання послуг; Ціна даної послуги; Тип з’єднання користувача в момент замовлення послуги; Тип контенту для якої будуть надаватись послуги.

6.3.3. Можливості хмарного сервісу для обробки даних з мобільного програмного забезпечення

На даній платформі створено проект Mobile Service Provider, який в подальшому застосований як сервіс аутентифікації користувача в мобільному додатку та як хмарна база даних працює в режимі реального часу. Даний додаток створюється з метою можливості операторів мобільного зв’язку доступатись до даних у яких зберігається інформація від користувачів про запит на вимогу певної послуги з необхідним рівнем сприйняття послуги. Які оператори попередньо проаналізувавши повинні забезпечити надання даної послуги згідно виставленого тарифу згідно яких формується запит. А мобільні користувачі у свою чергу доступатися до даних запитів з можливістю перегляду суми оплати надання послуги. Також налаштовані методи аутентифікації користувача в мобільному додатку за допомогою служби Firabase Auth. За допомогою служби Firebase Auth ми можем получити доступ до списку користувачів мобільного додатку та типу аутентифікації користувача.

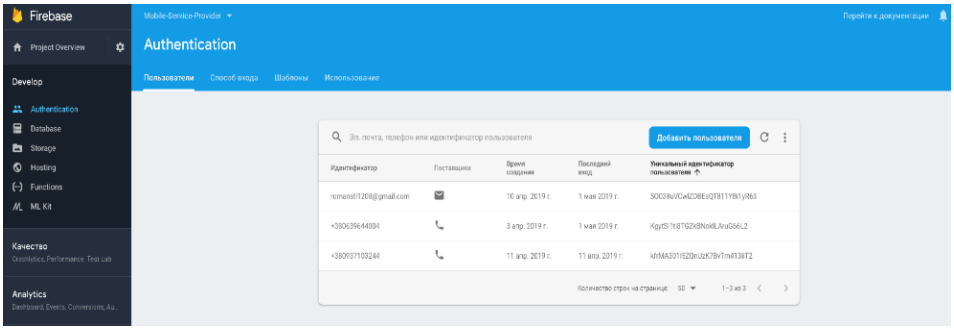


Рис. 6.36 Список користувачів мобільного додатку

При використанні служби Firebase Database [262] можна аналізувати та редагувати дані які були отримані з мобільного додатку. Дана можливість є корисною для операторів мобільного зв’язку.

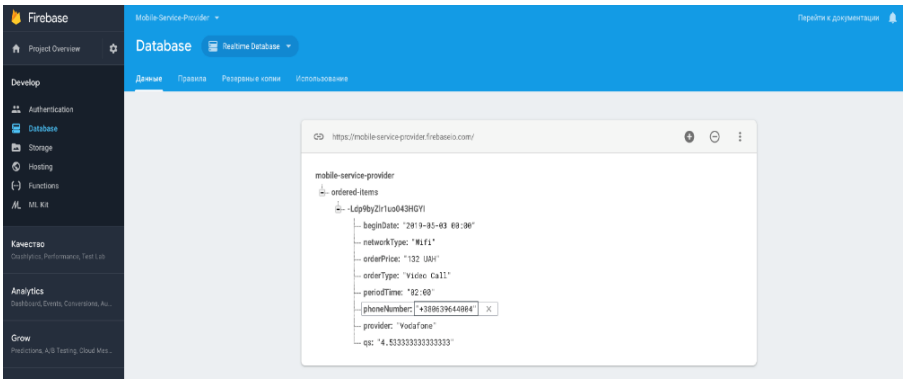


Рис. 6.37. Інтерфейс бази даних в службі Firebase Database

На рис. 6.37 зображено інтерфейс бази даних, за допомогою мобільного додатку в базі даних створюється об’єкт під назвою “ordered-items”, який в подальшому використовується, як список замовлень користувачів при наданні послуг в гетерогенній мережі. Кожне замовлення послуг зі сторони мобільного додатку отримує свій універсальний ідентифікатор в базі даних. Даний ідентифікатор слугує об’єктом, який містить в собі набір параметрів отриманих від користувача додатку.

6.3.4. Алгоритм спільного управління ресурсами гетерогенної IBN мережі з використанням Big Data та розробленого QoE додатку

Для надання послуг користувачеві по замовлених параметрах, потрібно виділяти користувача в певний період часу як пріоритетний (на період надання замовлених послуг). В певні періоди часу мережа може мати надмірне навантаження яке може впливати на якість надання даних послуг, розроблено алгоритм який буде забезпечувати надання даних послуг для користувача.

На рис. 6.38 представлено алгоритм роботи, що дає змогу ефективно управляти ресурсами гетерогенної мережі для надання замовлених послуг з необхідним рівнем якості сприйняття послуг [263].

Забезпечення замовленого QoE користувача в гетерогенній мережі досягається шляхом застосування 4-х способів управління процесом обслуговування абонентів.

1. Пошук альтернативної радіо технології безпровідного зв'язку SDR/2G/3G/4G/5G) з необхідними ресурсами для задоволення необхідного QoE.

2. Аналіз наданих ресурсів для активних сесій (які обслуговуються за стандартним рішенням та відносяться до не пріоритетних користувачів) поточної технології та мінімізація ресурсів до надання допустимого значення якості.

3. Переключення не пріоритетних користувачів на альтернативні технології, для яких плавно забезпечується отримана якість аналогічно до наданої в поточній радіотехнології з метою вивільнення ресурсів поточної технології для пріоритетних користувачів, що використовують запропонований додаток з можливість замовлення бажаної послуги з відповідним рівнем якості сприйняття.

4. Тимчасове відключення не пріоритетних користувачів, які використовують значну кількість ресурсів поточної технології з метою вивільнення ресурсів для пріоритетних користувачів, що використовують запропонований додаток з можливість замовлення бажаної послуги з відповідним рівнем якості сприйняття.

Робота алгоритму розпочинається із запису вхідних даних у БД. До вхідних даних належать запити на обслуговування згідно замовленої якості з допомогою розробленого мобільного додатку, а також дані про стан гетерогенної мережі (активні сесії для кожної технології).

Після запису статистичних даних переходимо до їх аналізу та порівняння з максимально допустимими значеннями для кожної з технологій. За допомогою аналізу даних, оцінюються критичні точки в мережі, та приймаються рішення

про підключення пріоритетних запитів та мінімізацію наданих ресурсів непріоритетних активних сесій, що поступають в конкретний момент часу.

У випадку завантаження гетерогенної мережі проводиться детальний аналіз NP (Network Parametrs) активних сесій та запитів, що поступили [264]. Далі обчислюються вільні ресурси в гетерогенній мережі та порівнюються із необхідною кількістю ресурсів для обслуговування вхідних запитів. Якщо є необхідна кількість ресурсів, тоді відбувається перерозподіл та балансування навантаження в гетерогенній мережі [265-267], кожному з користувачів які замовили послугу надсилаються дані з оптимальною БС, яка може його обслужити. В іншому випадку, аналізується пріоритетність активних сесій та вхідних запитів. Непріоритетні сесії та запити відкидаються та будуть опрацьовані пізніше, а пріоритетні запити обслуговуються із необхідною якістю обслуговування. Після цього через час Δt алгоритм виконується знову.

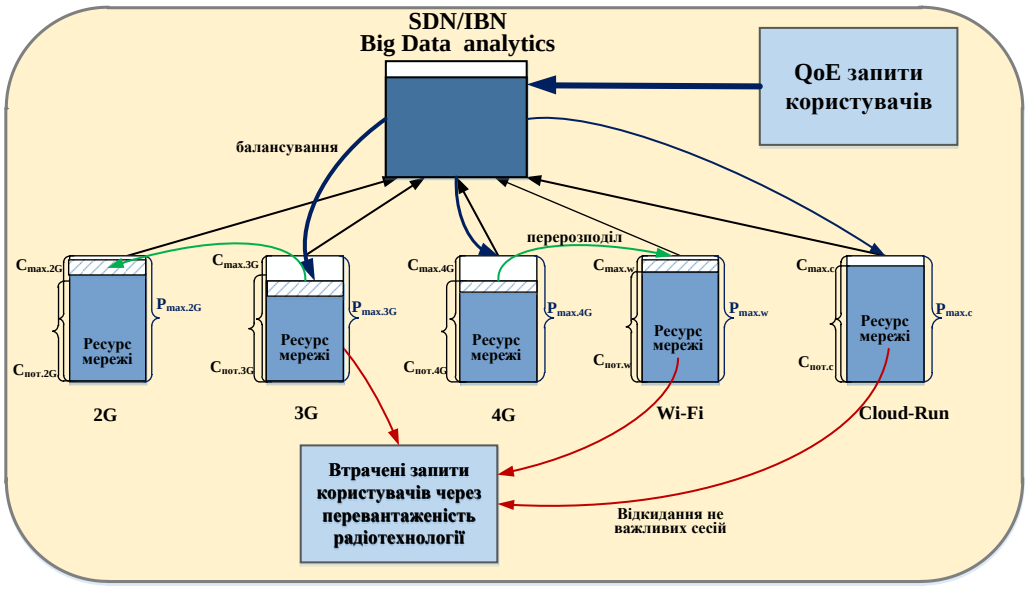
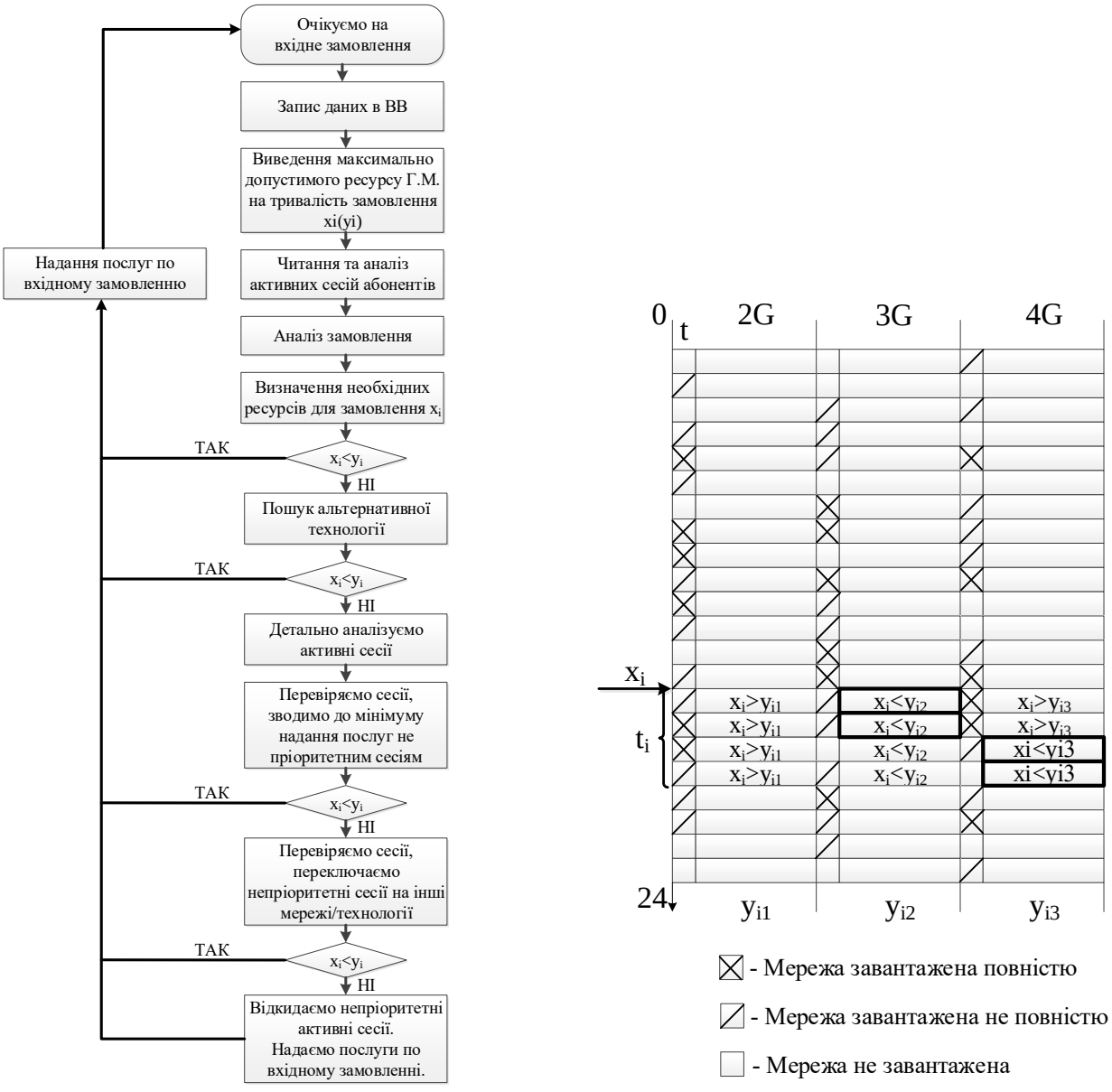


Рис. 6.38. Алгоритм роботи гетерогенної мережі з використання Big Data та розробленого мобільного додатку

Даний алгоритм розглядає користувачів як пріоритетних, тих хто використовує мобільне програмне забезпечення для замовлення послуг з певними параметрами та тривалістю виконання даної послуги. Інші користувачі позначаються як не пріоритетні, при сильному навантаженні на мережу та

недостачі ресурсів для надання послуг пріоритетним сесіям, непріоритетним активним сесіям може бути зведено до мінімуму надання послуг (не помітні втрати для сесії), переключення непріоритетної активної сесії на іншу технологію, наприклад з 4G на 3G при умові мінімальних втрат для сесії чи відкидання сесії і опрацювання пізніше.



а) б)

Рис. 6.39. Алгоритм роботи гетерогенної мережі з використання Big Data та розробленого мобільного додатку – а) та управління ресурсами для забезпечення замовленого QoE – б)

Користувачі, які зробили замовлення послуги через мобільне програмне забезпечення також вказують тривалість надання даної послуги, цей параметр є важливою складовою правильного функціонування гетерогенної мережі, тому що на даний проміжок часу (Ti) потрібно аналізувати стан мережі та приймати рішення для задовільнення якості надання послуг. На рис. 6.39б розглянуто один з варіантів функціонування гетерогенної мережі. Користувач зробив замовлення на надання послуг по заданим параметрам (вимогам), на рис. 6.39б зображено параметр X_i який відповідає за необхідну кількість ресурсів для задовільнення замовлення користувача та тривалість дії даного замовлення (T_i). Кожна колонка на рис. 6.39б відповідає за певну технологію (2G,3G,4G) [268-270], в певний момент часу кожна технологія має максимально допустиму кількість ресурсів (Y_{i1},Y_{i2},Y_{i3}) та різну завантаженість на мережу відповідно.

У випадку зображеному на рис. 6.39б ми можемо спостерігати, що необхідна кількість ресурсів для користувача, що зробив замовлення не підходить для використання технології 2G тому ми її автоматично відкидаємо. Далі ми можемо спостерігати що протягом замовленого проміжку часу надання послуг, дані постійно аналізуються та приймаються рішення щодо вимог даного замовлення. Ми можемо спостерігати що на певний період часу ми не можемо надати пріоритетному користувачеві використовувати технологію 4G так як вона є перезавантаженою, але в цей самий момент при аналізі визначається, що користувачеві для надання необхідних ресурсів ми можемо використати технологію 3G та при потребі коли навантаження на мережу з технологією 4G впаде, переключити користувача. У випадку якщо мережа з технологією 3G не підходила для надання необхідних ресурсів, система приймала рішення про переключення/відключення непріоритетних користувачів для зменшення завантаженості мережі з технологією 4G та надання необхідних ресурсів для пріоритетних користувачів. Система дає змогу надавати пріоритетним користувачам максимально допустиму кількість ресурсів по їхнім вимогам, при

певних ситуаціях система аналізує дані та шукає оптимальне рішення як для пріоритетних користувачів так і для не пріоритетних.

Збільшення або зменшення пропускної здатності каналів вузлів не впливало на працездатність і результативність алгоритмів. Зі збільшенням обсягів ресурсів однаково збільшувалося число заявок і, як наслідок, кількість підключених плеєрів глядачів для всіх досліджуваних алгоритмів.

6.3.5. Експериментальне дослідження ефективності запропонованого алгоритму управління ресурсами в гетерогенній IBN мережі мобільного зв'язку

Для проведення експериментального дослідження роботи алгоритму, який надає послуги по замовленню користувача згенеровано 1000 запитів з мобільного додатку, які в подальшому обробляються. Відповідно в один момент часу поступило 20 запитів з різними вимогами щодо замовленої якості обслуговування проаналізувавши базу даних Big Data у середовищі Firebase Database.

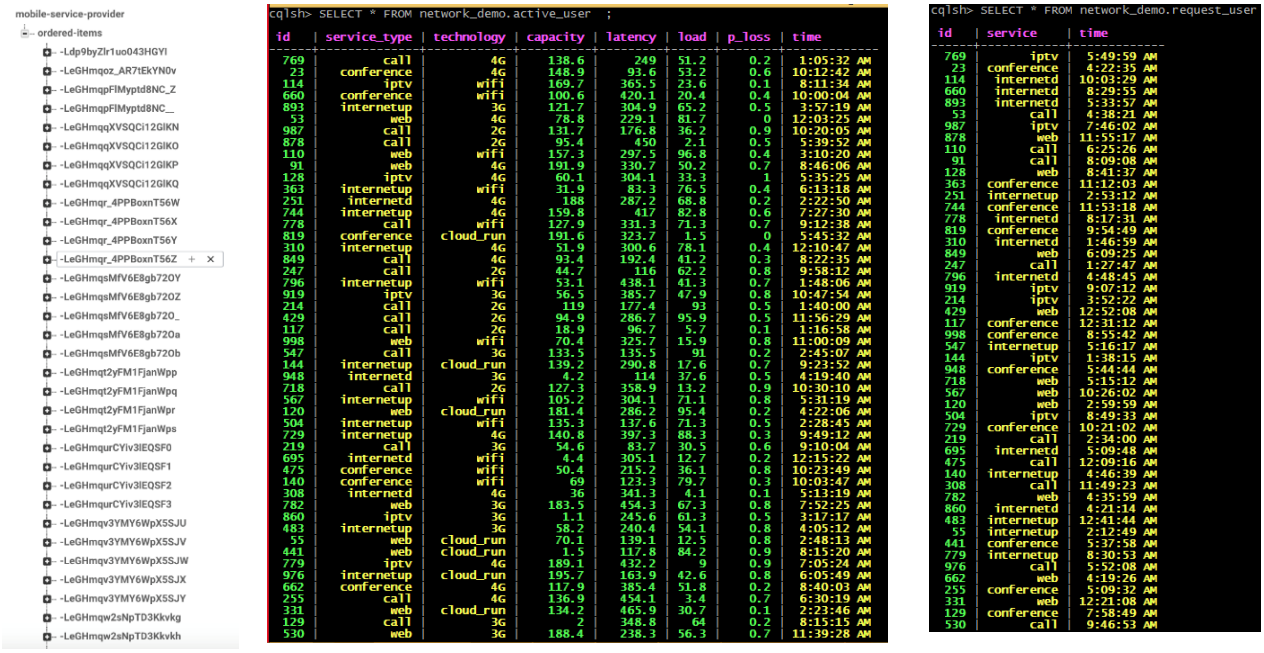
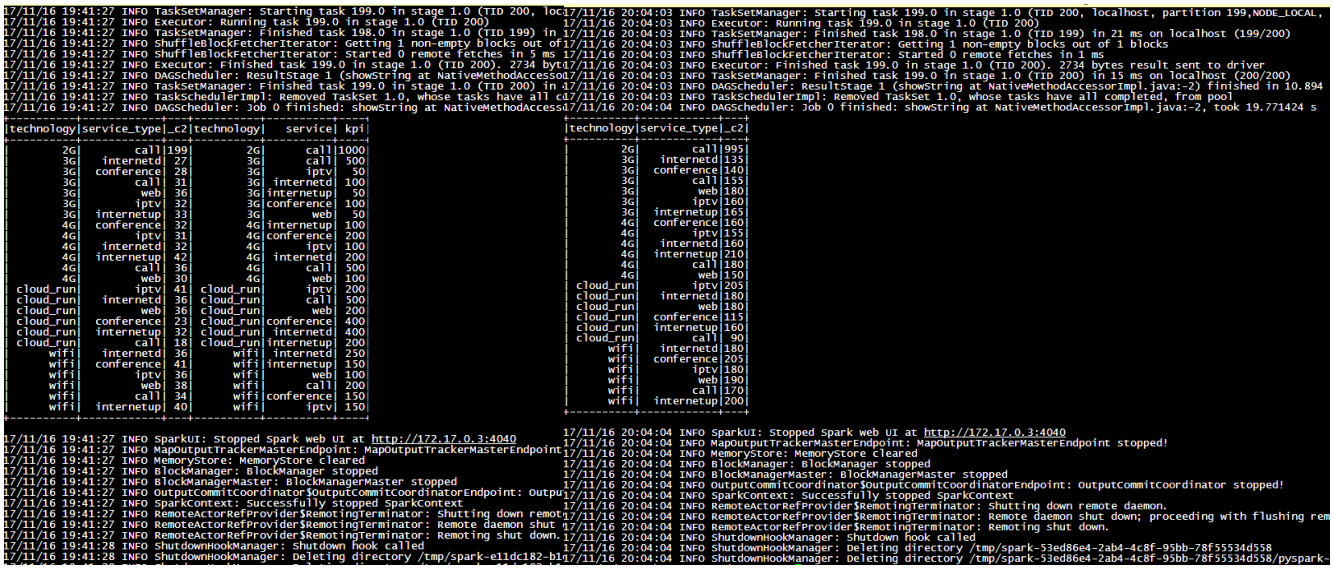


Рис. 6.40. 1000 згенерованих запитів в базі даних Firebase



а) б)

Рис.6.41. Експериментальні результати розробленої мобільної системи для аналізу великих даних: виведення максимально доступного та поточного ресурсу гетерогенної мережі – а), активні сеанси в години пік– б).

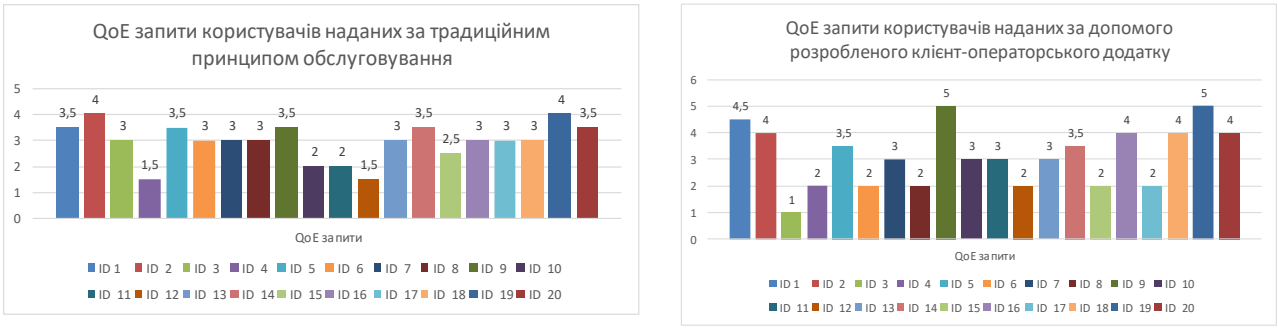
Для порівняння ефективності використання даного підходу від традиційного взято перші 20 запитів з бази даних. У роботі розглядається оцінка QoE від 1 до 5, для забезпечення необхідної якості по даній шкалі безпровідні технології в гетерогенному середовищі повинні мати необхідні ресурси.

Якщо для запитуваної оцінки на послугу (X_i) в гетерогенному середовищі знайдеться необхідний ресурс, щоб задовольнити цю шкалу (Y_i), то абонент автоматично перейде на обслуговування цієї технології

Список запитів користувачів та їх QoE(Xi): ID 1 (4.5), ID 2 (5), ID 3 (1), ID 4 (2), ID 5 (4), ID 6 (2), ID 7 (3), ID 8 (2), ID 9 (5), ID 10 (3), ID 11 (3), ID 12 (2), ID 13 (3), ID 14 (4), ID 15 (2), ID 16 (4), ID 17 (2), ID 18 (4), ID 19 (5), ID 20 (4) показано на рис. 6.42.

Рис.6.42. Вибірка QoE запитів користувачів з бази даних Firebase Database

Список ресурсів які може надати мережа з використанням традиційного підходу (Yi трад) (3.5) показано на рис. 6.43.



а) б)

Рис.6.43. Аналіз можливостей надання QoE запитів користувачів без використанням розробленого мобільного додатку – а) та з використанням розробленого мобільного додатку – б)

Список ресурсів, які може надати конкретна безпровідна мережа (Yi QoE) з використанням підходу, який базується на даному алгоритмі, що аналізує параметри користувача по запитах: показано на рис. 6.41.

Розглянемо перший випадок з запитом ID 1. Користувач подав запит на надання послуг з QoE (4.5). При традиційному підході мережа 4G змогла надати користувачеві тільки QoE (3.5) так як на даний момент часу це був максимально допустимий вільний ресурс мережі. При використанні підходу, який керується даним алгоритмом мережа була проаналізована і для виконання бажань користувача проведено пошук альтернативної радіо технології 3G

безпровідного зв’язку з необхідними ресурсами для задоволення необхідного QoE (4.5) показано на рис. 6.44.

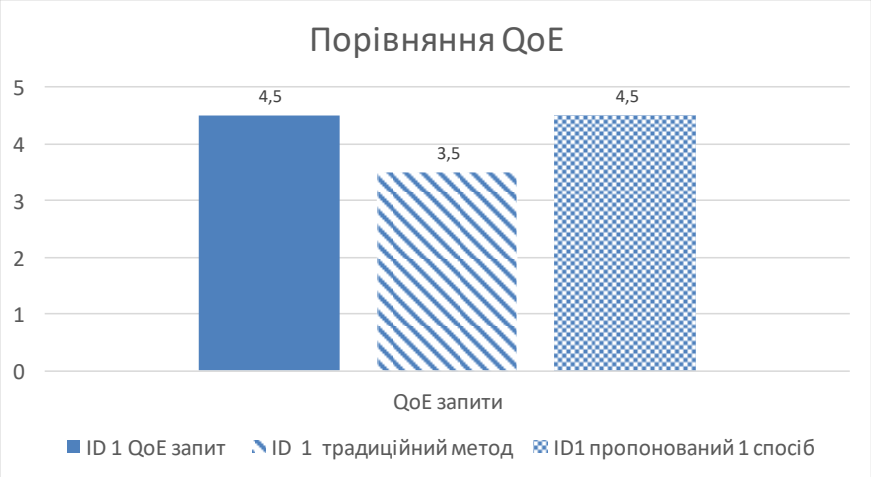


Рис.6.44. Порівняння можливостей надання QoE запиту користувача ID 1 за першим способом управління ресурсами

У другому випадку розглянемо запит ID 4. Користувач подав запит на надання послуг з QoE (2). При традиційному підході мережа змогла надати користувачеві тільки QoE (1.5) так як на даний момент часу це був максимально допустимий вільний ресурс мережі. При використанні підходу, який керується даним алгоритмом проведено аналіз наданих ресурсів для активних сесій (які обслуговуються за стандартним рішенням та відносяться до не пріоритетних користувачів) поточної технології та мінімізація ресурсів до надання допустимого значення якості, ми можемо спостерігати що традиційний підхід немає можливості оптимізації розділення ресурсів і інколи надає надлишкову кількість ресурсів користувачам, коли інші користувачі потребують даних ресурсів. У випадку використання даного алгоритму надлишкові ресурси розподіляються по іншим користувачам, в першу чергу для пріоритетних тобто запит ID 4 з QoE (2) наданий показано на рис.6.45.

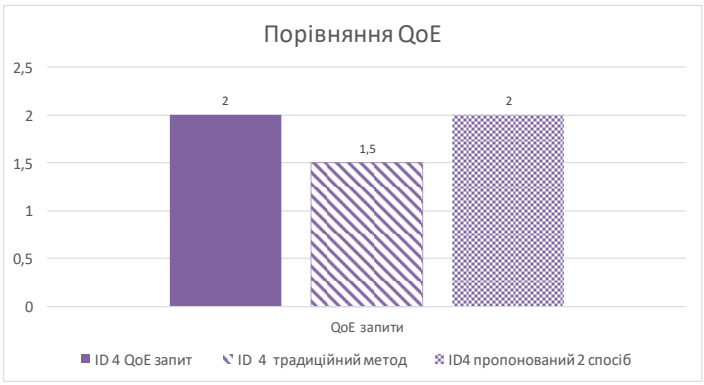


Рис.6.45. Аналіз можливостей надання QoE запитів користувачів з використання розробленого мобільного додатку

У третьому випадку розглянемо запит ID 9. Користувач подав запит на надання послуг з QoE (5). При традиційному підході мережа змогла надати користувачеві тільки QoE (3.5) так як на даний момент часу це був максимально допустимий вільний ресурс мережі. При використанні підходу який керується даним алгоритмом проведено переключення не пріоритетних користувачів на альтернативні технології, для яких плавно забезпечиться отримана якість аналогічно до наданої в поточній радіотехнології з метою вивільнення ресурсів поточної технології для пріоритетних користувачів, що використовують запропонований додаток з можливістю замовлення бажаної послуги з відповідним рівнем якості сприйняття. Запит ID 9 з QoE (5) після вивільнення ресурсів є успішно наданий показано на рис.6.46.

Рис.6.46. Аналіз можливостей надання QoE запитів користувачів з використання розробленого мобільного додатку

У четвертому випадку розглянемо запит ID 18. Користувач подав запит на надання послуг з QoE (4). При традиційному підході мережа змогла надати користувачеві тільки QoE (3) так як на даний момент часу це був максимально допустимий вільний ресурс мережі. При використанні підходу який керується даним алгоритмом проведено тимчасове відключення не пріоритетних користувачів, які використовують значну кількість ресурсів поточної технології з метою вивільнення ресурсів для пріоритетних користувачів, що використовують запропонований додаток з можливістю замовлення бажаної послуги з відповідним рівнем якості сприйняття. Запит ID 18 з QoE (4) після вивільнення ресурсів є успішно наданий показано на рис.6.47 .

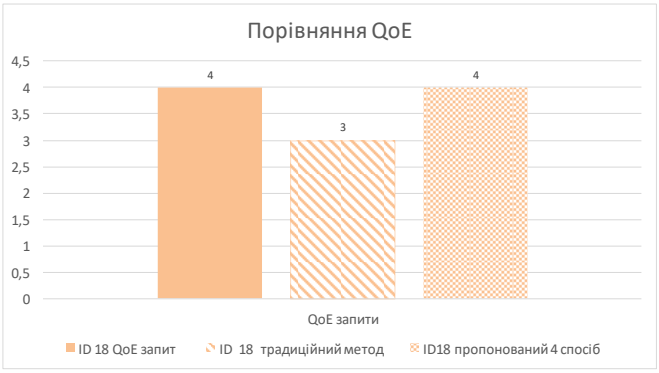


Рис. 6.47. Аналіз можливостей надання QoE запитів користувачів з використанням розробленого мобільного додатку

Як ми можемо спостерігати з даного дослідження при використанні алгоритму 3 користувачам не було надано бажаної якості надання послуг, так як по певних причинах ні один з 4 підходів не міг бути виконаний.

Отже, по отриманих запитах від користувачів використовуючи традиційний підхід мережа змогла задовольнити 5/20 користувачів тобто 25%.

У випадку використання підходу що базується на даному алгоритмі, який аналізує запити (бажання) користувачів, мережа змогла задовольнити 17/20 користувачів тобто 85%. На рис. 6.48а показано співвідношення задоволеності користувачів без використання пропонованого рішення (без розробленого мобільного додатку. На рис. 6.48б показано співвідношення задоволеності

користувачів з використання пропонованого рішення(з розробленим мобільним додатком)мобільного додатку.

а) б)

Рис. 6.48. Співвідношення задоволеності користувачів без використання пропонованого рішення (без розробленого мобільного додатку) – а) та з використання пропонованого рішення (з розробленим мобільним додатком) – б)

Важливим критерієм для якісного надання послуг мережі користувачам є оптимізація ресурсів мережі [271], тому що при традиційному підході [272] мережа могла різко понижувати QoE користувача по причині завантаженості мережі та недостатньої кількості вільних ресурсів. У випадку використання запропонованого алгоритму у мережі, проаналізовано всі активні сесії і при використанні описаних підходів не пріоритетним користувачам надається допустиме значення якості. Запропонований клієнт-операторський додаток, дасть змогу оператору з використанням Big Data проаналізувати вимоги користувача щодо замовленої якості обслуговування з метою створення майбутньої IBN мережі [273-280].

6.4. Висновки до 6-го розділу

1. Розроблено прототипи інтенційно-орієнтованої мережі на базі мікроконтролерних платформ, апаратних SDN комутаторів ZODIAC FX/GX та віртуалізації мережевих функцій компонентів технології SDN, в межах яких

реалізовано та оцінено ефективність запропонованих рішень щодо адаптивного клієнт-орієнтованого управління ресурсами та якістю обслуговування. Розроблено унікальну систему моніторингу якості функціонування реалізованих прототипів IBN мереж. Особливістю системи є використання розробленого методу наскрізного вимірювання затримки передавання даних з кінця в кінець для кожного компонента мережі шляхом додавання власної мітки часу до метаданих.

2. На основі експериментального дослідження в межах розробленого прототипу IBN мережі встановлено, що запропонована модель енергоефективної QoE-маршрутизації потоків даних у порівнянні із відомою концептуальною моделлю багатокритеріальної маршрутизації DMCQR, дала змогу досягти кращої збалансованості завантаження канальних ресурсів мережі за рахунок раціонального вибору шляхів для різнорідного трафіку та зменшити до 3 разів середню затримку обслуговування потоків реального часу з кінця в кінець для яких в умовах використання маршрутизації DMCQR не виконувались допустимі норми затримки, а також в умовах низької інтенсивності загального трафіку зменшити енергоспоживання мережі до 53,56%.

3. Проведено реалізацію інтуїтивного міжсерверного балансування навантаження в умовах деградації QoS, а також аналізу зображення відеопотоку у реальному часі на основі розробленого прототипу, що базується на мікроконтролерних платформах та апаратних SDN комутаторів ZODIAC FX.

4. Розроблена моніторингова QoE система для прототипу корпоративної IBN мережі, що базується на комутаторах ZODIAC GX та нововведеного контролера IBN, як надбудови над ONOS дала змогу виявляти вузькі місця в мережі та автоматизовано знайти маршрут передавання даних для покращення показника якості сприйняття послуги шляхом переконфігурування мережі.

5. Впроваджена система порівняна та оцінена, із стандартною системою маршрутизації як результат, нова система призвела до набагато менших втрат пакетів, ніж маршрутизація за замовчуванням, і, отже, до набагато вищої якості.

6. У роботі запропоновано клієнт-операторський додаток, який дасть змогу оператору з використанням Big Data проаналізувати вимоги користувача щодо замовленої якості обслуговування, а також оцінити можливості його обслуговування для вибору мережі доступу в гетерогенному безпровідному середовищі. Клієнтський додаток використовує тільки інформацію, доступну в мобільних пристроях, і не залежать від інформації, доступної в мережах, до яких прикріплені ці пристрої. Механізм прийняття рішень на основі замовлених послуг користувача за допомогою клієнтського додатку, запропонований у цій роботі, враховує ряд обмежень, включаючи характеристики мережі та моделі мобільності з точки зору швидкості руху користувача. У цьому розділі також пропонуються рішення для інтуїтивного управління мережами мобільності, що протиставляє інші пропозиції, використовуючи підхід, заснований на клієнтському додатку. У роботі пропонується метод, що підтримує мобільність для користувачів в гетерогенних середовищах, уникаючи проблеми надання якісних послуг по заданим вимогах. Результати включають зменшення кількості незадоволених користувачів мережі, що досягаються завдяки тому, що розроблений алгоритм використовуючи Big Data проводить аналіз замовлень від користувачів та приймає рішення відносно стану мережі, щодо надання бажаних послуг. Результати також включають в себе імітаційні моделі, реальні прототипи, а також тести, які можуть бути використані для розвитку майбутніх інтенційно-орієнтованих мережах. Запропоновані рішення в цій роботі в основному оцінюються за допомогою моделювання та розробки прототипу мобільного та операторського додатку. Аналітичні методи використовуються для доповнення деяких результатів моделювання та розробки прототипу.

ОСНОВНІ РЕЗУЛЬТАТИ ТА ВИСНОВКИ

В дисертаційній роботі вирішено наукову-прикладну проблему розроблення методології аналізу та синтезу складних гетерогенних інфокомунікаційних систем з метою створення нової програмно-конфігурованої інтенційно-орієнтованої мережі, яка постійно на основі мінливих вимог користувачів щодо якості надання сервісів та розгортання інфраструктури навчається, адаптується, автоматизується і захищається від потенційних кібератак шляхом використання нових методів розподілу ресурсів, інженерії трафіку, мережевої аналітики та існуючих алгоритмів машинного навчання.

Основні результати роботи полягають у наступному:

1. Проведено аналіз сучасного стану проблеми управління якістю надання сервісів в інформаційно-комунікаційних мережах. Встановлено, що з розвитком інфокомунікаційних систем вимоги користувачів і їх поведінка змінилися. Зокрема, для кінцевих бізнес-користувачів все більш важливим стає адаптивне надання сервісу, постійний зв’язок та індивідуалізація обслуговування. Визначено, що для отримання адаптивного рівня якості надання сервісів необхідно враховувати як технічні показники якості функціонування мережі, так і користувацьку оцінку якості надаваних сервісів, що, у свою чергу, вимагає розробки нових методів та моделей управління якістю сервісів в інфокомунікаційних мережах.

2. Формалізовано модель адаптивного управління перерозподілом ресурсів інфокомунікаційних мереж для реалізації концепції IBN. Запропоновано використати комплексний показник якості обслуговування користувачів сформованого у вигляді оцінки QoE, як основного критерію для адаптивного управління перерозподілом ресурсів в умовах зміни значимості бізнес-процесів в контексті реалізації концепції IBN. Розвинуто математичну модель визначення суб’єктивного рівня задоволеності користувача за оцінкою QoE в залежності від зміни об’єктивних показників якості обслуговування QoS, що забезпечуються в IBN/SDN мережі, зокрема для відео та аудіо сервісів реального часу. Формування математичної моделі QoS/QoE кореляції здійснено на основі проведення власних експериментальних досліджень.

3. Вперше запропоновано та реалізовано потокову модель енергоефективної QoE-маршрутизації для інтенційно-орієнтованих мереж. Новизною моделі є те, що для вибору оптимального шляху передавання даних використовується адаптивна QoE-орієнтована метрика маршруту, яка базується на розробленій математичній моделі кореляції нормалізованого значення замовленого рівня якості сприйняття сервісу та інтегрального адитивного критерію поточних показників якості обслуговування із врахуванням функціональних параметрів завантаженості мережевих вузлів. Що у результаті програмної реалізації на SDN/IBN контролері дало змогу підтримувати компроміс між бажаною інтенційно-орієнтованою якістю обслуговування користувачів, завантаженістю та енергоефективністю мережі шляхом переведення в енергозберігаючий режим незадіяних вузлів. У роботі запропоновано централізований моніторинг та управління мережевою структурою з допомогою удосконаленої логіки SDN контролера, що дало змогу на основі отриманої поточної статистики про стан мережі адаптивно приймати рішення щодо побудови оптимальної топології мережі за критеріями QoS/QoE та енергоспоживання. Удосконалено алгоритм вимірювання затримки передавання даних в програмно-конфігурованих мережах шляхом формування контролером пробних пакетів меншого розміру із різними пріоритетами, що дало можливість для низько пріоритетних потоків покращити точність моніторингу до 45% та зменшити до 22% сигналізаційне навантаження у порівнянні із відомими.

4. Розроблено метод адаптивного клієнт-орієнтованого управління якістю надання послуг для інтенційно-орієнтованих мереж. Новизна методу полягає в тому, що в умовах високого навантаження мережі для формування якості послуги враховується як об'єктивна оцінка часових мережевих характеристик, так і замовлені згідно намірів клієнтів суб'єктивні QoE оцінки, що дало змогу кінцевим користувачам сервісів опосередковано впливати на функціональну конфігурацію мережі, а з використанням алгоритмів машинного навчання для централізованої системи моніторингу та управління мережею реагувати на несприятливі поєднання значень показників якості і попереджати ситуації, коли

користувач незадоволений якістю отриманих сервісів для адаптивного прогнозування моменту переконфігурації мережі. Розроблено імітаційну модель мережі з можливістю перемикання між двома методами управління якістю обслуговування (традиційного та клієнт-орієнтованого). Перевагою даної моделі є можливість досліджувати нові рішення для майбутньої концепції інтенційно-орієнтованих мереж шляхом інтеграції унікальних алгоритмів у ядро мережі. Встановлено, що запропонований метод адаптивного клієнт-орієнтованого управління якістю послуг дає виграш в середньому від 2-5 разів за критерієм кількості користувачів, які вимагають високої якості сприйняття послуги.

5. Удосконалено метод виявлення аномалій мережевого трафіку та атак для майбутніх інтенційно-орієнтованих інфокомунікаційних мереж, який відрізняється від відомих способом формування набору інформативних ознак, що формалізують нормальну та аномальну поведінку системи на основі оцінки параметра Херста. Розроблено інтелектуальну DPI систему моніторингу та аналізу трафіку, яка дала змогу виявити складні атаки різного роду, зокрема таких як SYN Flood, фрагментація HTTP, UDP Flood, DNS Flood, Non-Spoofed UDP Flood та шляхом автоматизованого блокування виявленого шкідливого трафіку зменшити загальний рівень втрат на 5% у порівнянні із існуючою комерційною системою SolarWinds DPI. Новизною розроблювальної DPI системи є те, що вона базується на гармонійному поєднанні переваг методів сигнатурного, статистичного та фрактального аналізу інформативних ознак щодо детектування інформаційних протоколів і ранжування прихованих властивостей аномального трафіку.

6. На основі розробленої імітаційної моделі гетерогенної мережі LTE/NB-IoT встановлено, що комплексне використання розроблених методів пріоритезації IoT трафіку та балансування навантаження, дають змогу зменшити середню затримку повідомлень реального часу з кінця в кінець на 68,8% (або 3,21 рази), а також при використанні механізму пріоритезації, зменшити кількість відмов у обслуговуванні на 58% для класу L1 (трафік RT) та 76% для L2 (трафік URLLC) у порівнянні з існуючим методом

пропорційного розподілу ресурсів в умовах високого навантаження. У випадку одночасного використання запропонованих рішень досягається мінімальна кількість відмов для сервісів IoT класу L1 та L2 в умовах недовантаженості альтернативних базових станцій.

7. Розроблено адаптивний інтенційно-орієнтований метод розподілу ресурсів та формування структури рівня радіодоступу мереж 4G/5G. Новизна методу полягає у безпосередньому врахуванні просторово-часової локалізації абонентського навантаження та замовлених вимог бізнес-користувачів на основі аналізу їх QoE оцінок, що дало змогу для операторів мобільного зв'язку ефективніше на 25% використовувати наявні частотно-часові ресурси та зменшити на 8,7% енергоспоживання мережі рівня радіодоступу із гарантуванням замовленої якості обслуговування користувачів у порівнянні із відомими методами.

8. Розроблено імітаційну модель процесу функціонування інтенційно-орієнтованої гетерогенної мережі мобільного зв'язку. На основі імітаційної моделі оцінено ефективність запропонованого методу інтенційно-орієнтованого управління частотно-часовими ресурсами та формування структури рівня радіодоступу. Основною перевагою розробленої моделі є використання системно-об'єктного підходу проектування функціональних блоків мережі мобільного зв'язку на основі відомих LTE стандартів, що дало змогу адекватно формалізувати опис системи як єдине ціле, надавши повну інформацію про структуру, функціонування і поводження окремих елементів системи. Використання на практиці розробленої моделі операторами мобільного зв'язку дасть змогу досліджувати процес оптимізації мережі за критерієм замовленої якості обслуговування з урахуванням обмеженості спектральних та енергетичних ресурсів у порівнянні із відомими методами, як на етапі планування майбутньої інтенційно-орієнтованої мережі 5G, так і на етапі експлуатації існуючих 4G.

9. Запропоновано методологію синтезу гетерогенної інтенційно-орієнтованої мережі, згідно якої можна інтелектуально виділяти зв'язки між структурно-функціональними елементами мережі, які можуть не тільки

автоматизовано перебудовуватись з різною продуктивністю, але й виникати заново, вишукуючи шляхи найбільш адекватного пристосування до мінливих вимог користувачів щодо адаптивного надання сервісів. Новизною методології є те, що вона базується на розроблених у роботі нових методах адаптивного управління якістю надання послуг, енергоефективністю, захисту, розподілу та наскрізної віртуалізації ресурсів мережі.

10. Розроблено прототипи інтенційно-орієнтованої мережі на базі мікроконтролерних платформ, апаратних SDN комутаторів ZODIAC FX/GX та віртуалізації мережевих функцій компонентів технології SDN, в межах яких реалізовано та оцінено ефективність запропонованих рішень щодо адаптивного клієнт-орієнтованого управління ресурсами та якістю обслуговування. Розроблено унікальну систему моніторингу якості функціонування реалізованих прототипів IBN мереж. Особливістю системи є використання розробленого методу наскрізного вимірювання затримки передавання даних з кінця в кінець для кожного компонента мережі шляхом додавання власної мітки часу до метаданих.

На основі експериментального дослідження в межах розробленого прототипу IBN мережі встановлено, що запропонована модель енергоефективної QoE-маршрутизації потоків даних у порівнянні із відомою концептуальною моделлю багатокритеріальної маршрутизації DMCQR, дала змогу досягти кращої збалансованості завантаження канальних ресурсів мережі за рахунок раціонального вибору шляхів для різнорідного трафіка та зменшити до 3 разів середню затримку обслуговування потоків реального часу з кінця в кінець для яких в умовах використання маршрутизації DMCQR не виконувались допустимі норми затримки, а також в умовах низької інтенсивності загального трафіку зменшити енергоспоживання мережі до 53,56%. Підтвердженням цього є проведення експериментального дослідження та порівняння ефективності запропонованої моделі маршрутизації із централізованою детермінована багатокритеріальною QoS маршрутизацією запропоновану авторами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. В. В. Косенко та І. Ш. Невлюдов, *Моделі структурного синтезу для управління параметрами інфокомунікаційних мереж систем критичної інфраструктури*. Монографія ХНУРЕ, 2019.

2. J. J. Wilke and J. P. Kenny, "Opportunities and limitations of Quality-of-Service in Message Passing applications on adaptively routed Dragonfly and Fat Tree networks," *2020 IEEE International Conference on Cluster Computing (CLUSTER)*, 2020, pp. 109-118.

3. P. Daras et al, "Fundamental Limitations of Current Internet and the path to Future Internet," *White Paper, Future Internet Reference Architecture group, European Commission*, Dec. 2010 pp. 7-18.

4. A. Feldmann and J. Rexford, "IP network configuration for intradomain traffic engineering," in *IEEE Network*, vol. 15, no. 5, pp. 46-57.

5. S. Suman and A. Agrawal, “IP Traffic Management With Access Control List Using Cisco Packet Tracer”, *International Journal of Science, Engineering and Technology Research*, vol. 5, pp. 1556–1561, May 2016.

6. M. Kassim c “A Survey: Bandwidth Management in an IP Based Network”, *World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering*, vol. 6, no. 2, p. 8, 2012.

7. A. Kovalick, "Design Elements for Core IP Media Infrastructures," in *SMPTE Motion Imaging Journal*, vol. 125, no. 2, pp. 16-23, March 2016.

8. Minghai Xu, Zhengkun Mi, Xiaofang Feng and Wenke Xie, "Implementation techniques of IntServ/DiffServ integrated network," *International Conference on Communication Technology Proceedings, 2003. ICCT 2003.*, Beijing, China, 2003, pp. 231-234 vol.1.

9. Y. Bernet et al., "A Framework for Integrated Services Operation over DifIServ Networks", *RFC*, vol. 2998, November 2000.

10. R Braden, L Zbads, S. Berson, S. Herzog and S. Jamin, "Resource ReSerVation Protocol (RSVP) - Functional Specification", *RFC*, vol. 2205, September 1997.

11. N. Rouhana and E. Horlait, "Differentiated services and integrated services use of MPLS," *Proceedings ISCC 2000. Fifth IEEE Symposium on Computers and Communications*, Antibes-Juan Les Pins, France, 2000, pp. 194-199.

12. М. М. Климаш, О. В. Корецький, М. І. Бешлей, В. Б. Янишин, "Дослідження побудови технологічних ресурсів у конвергентній мережі на базі мобільного оператора для надання послуги Triple Play", *Вісник Національного університету "Львівська політехніка"*, серія "Радіоелектроніка та телекомунікації ", №. 705, с. 176–183, 2011.

13. B. Moon and H. Aghvami, "RSVP extensions for real-time services in wireless mobile networks," in *IEEE Communications Magazine*, vol. 39, no. 12, pp. 52-59, Dec. 2001.

14. A. Abella, V. Friderikos and H. Aghvami, "Differentiated services versus over-provisioned best-effort for pure-IP mobile networks," *4th International Workshop on Mobile and Wireless Communications Network*, Stockholm, Sweden, 2002, pp. 450-457

15. М. М. Климаш, М.І. Бешлей, І.О Кагало, Л.М. Готра, "Вдосконалення методів та алгоритмів управління інформаційними потоками в конвергентних телекомунікаційних мережах," *матеріали 4-ї Міжнародної науково-практичної конференції присвяченої 25-річчю заснування кафедри "Радіотехніки та інформаційні безпеки" Чернівецького національного університету ім. Юрія Федьковича"*, м. Чернівці, 2014, с.106-107.

16. M. Klymash, M. Beshley and O. Lavriv, "Model of Network Resources Management on the Basis of Services Priorities Association", *Proceedings of XIIth International conference The experience of designing and application of CAD Systems in microelectronics" CADSM'2013*, pp. 146-148, 24–27 February.

17. M. Beshley, M. Beshley, M. Seliuchenko, O. Lavriv, V. Chervenets, H. Kholiavka, et al., "Increasing the efficiency of real-time content delivery by improving the technology of priority assignment and processing of IP traffic", *Smart Computing Review*, vol. 5, no. 2, pp. 76-88, 2015.

18. M. Beshley, V. Romanchuk, M. Seliuchenko and A. Masiuk, "Investigation the modified priority queuing method based on virtualized network test bed", *The Experience of Designing and Application of CAD Systems in Microelectronics Lviv*, pp. 1-4, 2015.

19. T. Minagawa and T. Ikegami, "Double WFQ QoS scheduling based on flow number in diffserve network," *2010 The 12th International Conference on Advanced Communication Technology (ICACT)*, 2010, pp. 1365-1370.

20. H. Wang and H. Tianfield, "Energy-Aware Dynamic Virtual Machine Consolidation for Cloud Datacenters," in *IEEE Access*, vol. 6, pp. 15259-15273, 2018

21. X. -C. Xiao, X. -W. Zheng, Y. Wei and X. -C. Cui, "A Virtual Network Resource Allocation Model Based on Dynamic Resource Pricing," in *IEEE Access*, vol. 8, pp. 160414-160426, 2020.

22. S. Liu, C. Li, Z. Liu and Q. Zhang, "Virtual Machine Dynamic Deployment Scheme Based on Double-Cursor Mechanism," in *IEEE Access*, vol. 8, pp. 214481-214493, 2020.

23. Y. Himura and Y. Yasuda, "Static validation of network device configurations in virtualized multi-tenant datacenters," *2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013)*, 2013, pp. 160-168.

24. T. Samak and E. Al-Shaer, "Fuzzy Conflict Analysis for QoS Policy Parameters in DiffServ Networks," in *IEEE Transactions on Network and Service Management*, vol. 9, no. 4, pp. 459-472, December 201

25. O. Lemeshko, O. Yeremenko and A. M. Hailan, "Design of QoS-routing scheme under the timely delivery constraint," *2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)*, Lviv, 2017, pp. 97-99.

26. R. Stankiewicz and A. Jajszczyk, "Modular Model Based Performance Evaluation of a DiffServ Network Supporting Assured Forwarding PHB," *2008 IEEE International Conference on Communications*, 2008, pp. 208-213.

27. R. Yu, W. Zhong, S. Xie, Y. Zhang and Y. Zhang, "QoS Differential Scheduling in Cognitive-Radio-Based Smart Grid Networks: An Adaptive Dynamic Programming Approach," in *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, no. 2, pp. 435-443, Feb. 2016.

28. W. Zai-jian, Y. Dong and X. Wang, "A Dynamic Service Class Mapping Scheme for Different QoS Domains Using Flow Aggregation," in *IEEE Systems Journal*, vol. 9, no. 4, pp. 1299-1310, Dec. 2015.

29. X. Ma, Z. Zhang and S. Su, "Cost-aware Multi-Domain Virtual Data Center embedding," in *China Communications*, vol. 15, no. 12, pp. 190-207, Dec. 2018.

30. G. Liang and W. Li, “A Novel Industrial Control Architecture Based on Software-Defined Network”, *Measurement and Control*, vol. 51, p. 002029401878431, Jul. 2018.

31. I. Radu, "Integrating Software Defined Networks with Traditional Hardware Networks," *2018 International Conference on Communications (COMM)*, 2018, pp. 309-312.

32. P. Danielis et al, "Emulation of SDN-supported automation networks," *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, Luxembourg, 2015, pp. 1-8.

33. F. A. Lopes, M. Santos, R. Fidalgo and S. Fernandes, "A software engineering perspective on SDN programmability", *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1255-1272, 2nd Quart. 2016.

34. M. Hayes, B. Ng, A. Pekar and W. K. G. Seah, "Scalable Architecture for SDN Traffic Classification," *in IEEE Systems Journal*, vol. 12, no. 4, pp. 3203-3214, Dec. 2018.

35. W. Braun and M. Menth, "Software-defined networking using OpenFlow: Protocols applications and architectural design choices", *Future Internet*, vol. 6, no. 2, pp. 302-336, 2014.

36. M. Karakus and A. Durresi, "A survey: Control plane scalability issues and approaches in software-defined networking (SDN)", *Comput. Netw.*, vol. 112, pp. 279-293, Jan. 2017.

37. S. V. Krishna, A. Shrivastava and S. J. Wagh, "SDN in High Performance Computing for Scientific and Business Environment (SBE)," *2017 International Conference on Computational Intelligence in Data Science(ICCIDS)*, Chennai, 2017.

38. W. Wang, Q. Qi, X. Gong, Y. Hu and X. Que, "Autonomic QoS Management Mechanism in Software Defined Network," in *China Communications*, vol. 11, no. 7, pp. 13-23, July 2014.

39. H. Zhou *et al*., "Improving QoS in SDN with Lossless Multi-Domain Reconfigurations," *2015 IEEE 23rd International Symposium on Quality of Service (IWQoS)*, Portland, OR, 2015, pp. 77-78.

40. Ardiansyah, Y. Choi, M. R. K. Aziz and D. Choi, "Latency Minimization for Energy Internet Communications with SDN Virtualization Infrastructure," *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Beijing, China, 2019, pp. 1-7.

41. A. Lara, A. Kolasani, and B. Ramamurthy, "Network Innovation Using OpenFlow: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 493–512, First Qu. 2014.

42. V. Varadharajan et al, "A Policy-Based Security Architecture for Software-Defined Networks," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 897-912, April 2019.

43. I. Ahmad, S. Namal, M. Ylianttila and A. Gurtov, "Security in Software Defined Networks: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2317-2346, Fourthquarter 2015.

44. J. Wang, Q. Qi, J. Gong and J. Liao, "Mitigating the Oscillations Between Service Routing and SDN Traffic Engineering," in *IEEE Systems Journal*, vol. 12, no. 4, pp. 3426-3437, Dec. 2018.

45. S. Agarwal, M. Kodialam and T. V. Lakshman, "Traffic engineering in software defined networks", *Proc. IEEE INFOCOM*, pp. 2211-2219, 2013.

46. L. Davoli, L. Veltri, P. L. Ventre, G. Siracusano and S. Salsano, "Traffic Engineering with Segment Routing: SDN-Based Architectural Design and Open Source implementation", *Proc. Eur. Workshop Softw. Defined Netw.*, pp. 111-112, Sep. 2015.

47. S. Geissler, S. Herrnleben, R. Bauer, A. Grigorjew, T. Zinner and M. Jarschel, "The Power of Composition: Abstracting a Multi-Device SDN Data Path Through a Single API," in *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 722-735, June 2020.

48. M. Shin, K. Nam and H. Kim, "Software-defined networking (SDN): A reference architecture and open APIs," *2012 International Conference on ICT Convergence (ICTC)*, 2012, pp. 360-361.

49. H. Cui, Y. Zhu, Y. Yao, L. Yufeng and Y. Liu, "Design of intelligent capabilities in SDN," *2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE)*, 2014, pp. 1-5.

50. T. G. Nguyen et al, "SeArch: A Collaborative and Intelligent NIDS Architecture for SDN-Based Cloud IoT Networks," in *IEEE Access*, vol. 7, pp. 107678-107694, 2019.

51. Y. Yu *et al.*, "Fault Management in Software-Defined Networking: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 349-392.

52. A. Binsahaq, T. R. Sheltami and K. Salah, "A Survey on Autonomic Provisioning and Management of QoS in SDN Networks," in *IEEE Access*, vol. 7, pp. 73384-73435, 2019.

53. E. Pateromichelakis, M. Shariat, A. u. Quddus and R. Tafazolli, "On the Evolution of Multi-Cell Scheduling in 3GPP LTE / LTE-A," in *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 701-717, Second Quarter 2013.

54. N. Abu-Ali, A. M. Taha, M. Salah and H. Hassanein, "Uplink Scheduling in LTE and LTE-Advanced: Tutorial, Survey and Evaluation Framework," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1239-1265, 2014.

55. J. Zhang, M. Wang, M. Hua, T. Xia, W. Yang and X. You, "LTE on License-Exempt Spectrum," in *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 647-673, Firstquarter 2018.

56. A. Gupta and R. K. Jha, "A Survey of 5G Network: Architecture and Emerging Technologies," in *IEEE Access*, vol. 3, pp. 1206-1232, 2015.

57. M. Agiwal, A. Roy and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1617-1655, thirdquarter 2016.

58. C. Wang, J. Bian, J. Sun, W. Zhang and M. Zhang, "A Survey of 5G Channel Measurements and Models," in *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3142-3168, Fourthquarter 2018.

59. A. Shaikh and M. J. Kaur, "Comprehensive Survey of Massive MIMO for 5G Communications," *2019 Advances in Science and Engineering Technology International Conferences (ASET)*, 2019, pp. 1-5.

60. J. Liu, C. R. Lin and Y. Hu, "Joint Resource Allocation, User Association, and Power Control for 5G LTE-Based Heterogeneous Networks," in *IEEE Access*, vol. 8, pp. 122654-122672, 2020.

61. M. Klymash, H. Beshley, A. Masiuk and I. Strykhalyuk, "Concept for ensuring effective functioning of mobile communication system in heterogenous 5G infrastructure," *2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)*, 2017, pp. 272-274.

62. D. Benhaddou et al, "Coordinated Multipoint User Scheduling for 5G Cloud Radio Access Network," *2020 IEEE International Symposium on Systems Engineering (ISSE)*, 2020, pp. 1-7.

63. J. Han and K. Kwon, "I/Q Balance-Enhanced Wideband Receiver Front-End for 2G/3G/4G/5G NR Cellular Applications," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 67, no. 6, pp. 1881-1891, June 2020.

64. R. Zeqiri, F. Idrizi and H. Halimi, "Comparison of Algorithms and Technologies 2G, 3G, 4G and 5G," *2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, 2019, pp. 1-4.

65. P. Ahokangas *et al*., "Business Models for Local 5G Micro Operators," in *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 3, pp. 730-740, Sept. 2019.

66. M. R. Palattella *et al*., "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models," in *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 510-527, March 2016.

67. W. Ejaz and M. Ibnkahla, "Multiband Spectrum Sensing and Resource Allocation for IoT in Cognitive 5G Networks," in *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 150-163, Feb. 2018.

68. N. Gupta *et al*., "SDNFV 5G-IoT: A Framework for the Next Generation 5G enabled IoT," *2020 International Conference on Advances in Computing, Communication & Materials (ICACCM)*, 2020, pp. 289-294.

69. J. M. Khurpade, D. Rao and P. D. Sanghavi, "A Survey on IOT and 5G Network," *2018 International Conference on Smart City and Emerging Technology (ICSCET)*, 2018, pp. 1-3.

70. M. Fuentes *et al*., "5G New Radio Evaluation Against IMT-2020 Key Performance Indicators," in *IEEE Access*, vol. 8, pp. 110880-110896, 2020.

71. M. Benisha et al., "Requirements and challenges of 5G cellular systems," *2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*, 2016, pp. 251-254.

72. Hussein T. Mouftah; Melike Erol-Kantarci; Mubashir Husain Rehmani, "5G and D2D Communications at the Service of Smart Cities," in *Transportation and Power Grid in Smart Cities: Communication Networks and Services* , Wiley, 2019, pp.147-169.

73. D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Blockchain for 5G and beyond networks: A state of the art survey”, *Journal of Network and Computer Applications*, vol. 166, p. 102693, Sep. 2020.

74. M. J. Riaz, A. Sultan, M. Zahid, A. Javed, Y. Amin and J. Loo, "MIMO Antennas for Future 5G Communications," *2020 IEEE 23rd International Multitopic Conference (INMIC)*, 2020, pp. 1-4.

75. D. Zhai, R. Zhang, J. Du, Z. Ding and F. R. Yu, "Simultaneous Wireless Information and Power Transfer at 5G New Frequencies: Channel Measurement and Network Design," in *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 1, pp. 171-186, Jan. 2019.

76. M. O. Ojijo and O. E. Falowo, "A Survey on Slice Admission Control Strategies and Optimization Schemes in 5G Network," in *IEEE Access*, vol. 8, pp. 14977-14990, 2020.

77. R. F. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," in *IEEE Access*, vol. 8, pp. 99999-100009, 2020.

78. M. Chahbar, G. Diaz, A. Dandoush, C. Cérin and K. Ghoumid, "A Comprehensive Survey on the E2E 5G Network Slicing Model," in *IEEE Transactions on Network and Service Management*, vol. 18, no. 1, pp. 49-62, March 2021.

79. H. Cho, C. Lai, T. K. Shih and H. Chao, "Integration of SDR and SDN for 5G," in *IEEE Access*, vol. 2, pp. 1196-1204, 2014

80. S. Sun, M. Kadoch, L. Gong and B. Rong, "Integrating network function virtualization with SDR and SDN for 4G/5G networks," in *IEEE Network*, vol. 29, no. 3, pp. 54-59, May-June 2015.

81. J. S. Hsin *et al*., "Multi-RAT multi-connectivity active steering antenna technology for IoT, Wi-Fi, LTE, and 5G," *2020 IEEE Radio and Wireless Symposium (RWS)*, 2020, pp. 87-90.

82. F. Z. Yousaf, M. Bredel, S. Schaller and F. Schneider, "NFV and SDN—Key Technology Enablers for 5G Networks," in *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2468-2478, Nov. 2017.

83. W. Ma, J. Beltran, D. Pan and N. Pissinou, "Placing Traffic-Changing and Partially-Ordered NFV Middleboxes via SDN," in *IEEE Transactions on Network and Service Management*, vol. 16, no. 4, pp. 1303-1317, Dec. 2019.

84. A. Bradai, K. Singh, T. Ahmed and T. Rasheed, "Cellular software defined networking: a framework," in *IEEE Communications Magazine*, vol. 53, no. 6, pp. 36-43, June 2015.

85. J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca and J. Folgueira, "Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges," in *IEEE Communications Magazine*, vol. 55, no. 5, pp. 80-87, May 2017.

86. P. Caballero, A. Banchs, G. de Veciana, X. Costa-Pérez and A. Azcorra, "Network Slicing for Guaranteed Rate Services: Admission Control and Resource Allocation Games," in *IEEE Transactions on Wireless Communications*, vol. 17, no. 10, pp. 6419-6432, Oct. 2018.

87. “E2E Network Slicing - Key 5G technology: What is it? Why do we need it? How do we implement it?”, Network Manias. https://www.netmanias.com/en/?m=view&id=blog&no=8325 (accessed Apr. 25, 2020).

88. Boddepalli, Sai. “Performance Evaluation of v-eNodeB using Virtualized Radio Resource Management.” (2018).

89. R. Kokku, R. Mahindra, H. Zhang and S. Rangarajan, "Nvs: A Substrate for Virtualizing Wireless Resources in Cellular Networks", *IEEE/ACM Trans. Netw.*, vol. 20, no. 5, pp. 1333-1346, Oct. 2012

90. C. Liang and F. R. Yu, "Wireless Network Virtualization: A Survey, Some Research Issues and Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 358-380, Firstquarter 2015.

91. “How Has COVID-19 Impacted Last Mile Networks?”, Internet Society, Feb. 02, 2021. https://www.internetsociety.org/blog/2020/05/how-has-covid-19-impacted-last-mile-networks/ (accessed Apr. 25, 2021).

92. Z. Zhou, L. Tan, B. Gu, Y. Zhang and J. Wu, "Bandwidth Slicing in Software-Defined 5G: A Stackelberg Game Approach," in *IEEE Vehicular Technology Magazine*, vol. 13, no. 2, pp. 102-109, June 2018.

93. T. Hu, Z. Guo, P. Yi, T. Baker and J. Lan, "Multi-controller Based Software-Defined Networking: A Survey," in *IEEE Access*, vol. 6, pp. 15980-15996, 2018

94. M. Condoluci and T. Mahmoodi, "Softwarization and virtualization in 5G mobile networks: Benefits, trends and challenges", *Computer Networks*, vol. 146, pp. 65–84, Dec. 2018.

95. C.-W. Ahn and S.-H. Chung, "SDN-Based Mobile Data Offloading Scheme Using a Femtocell and Wi-Fi Networks”, *Mobile Information Systems*, vol. 2017, p. e5308949, Feb. 2017.

96. X. Duan, “Software-defined Networking enabled Resource Management and Security Provisioning in 5G Heterogeneous Networks", 2017, Accessed: Dec. 25, 2020. [Online]. Available: https://core.ac.uk/display/85003266.

97. J. Rizkallah and N. Akkari, "SDN-based vertical handover decision scheme for 5G networks," *2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)*, 2018, pp. 1-6.

98. C. Qiu, C. Zhao, F. Xu, and T. Yang, “Sleeping mode of multi-controller in green software-defined networkingϵ”, *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, p. 282, Dec. 2016.

99. A. Rafiq, A. Mehmood, T. Ahmed Khan, K. Abbas, M. Afaq, and W.-C. Song, “Intent-Based End-to-End Network Service Orchestration System for Multi-Platforms”, *Sustainability*, vol. 12, no. 7, Art. no. 7, Jan. 2020.

100. K. Abbas, M. Afaq, T. Ahmed Khan, A. Rafiq, and W.-C. Song, “Slicing the Core Network and Radio Access Network Domains through Intent-Based Networking for 5G Networks”, *Electronics*, vol. 9, no. 10, Art. no. 10, Oct. 2020.

101. E. Zeydan and Y. Turk, "Recent Advances in Intent-Based Networking: A Survey," *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 2020, pp. 1-5.

102. Y. Wei, M. Peng, and Y. Liu, “Intent-based networks for 6G: Insights and challenges”, *Digital Communications and Networks*, vol. 6, no. 3, pp. 270–280, Aug. 2020, doi: 10.1016/j.dcan.2020.07.001.

103. Release 15. Available online: https://www.3gpp.org/release-15 (accessed 20 March 2020).

104. Release 16. Available online: https://www.3gpp.org/release-16 (accessed 20 March 2020).

105. Release 17. Available online: https://www.3gpp.org/release-17 (accessed 20 March 2020).

106. Y. Miao, W. Li, D. Tian, M. S. Hossain and M. F. Alhamid, "Narrowband Internet of Things: Simulation and Modeling," in *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2304-2314, Aug. 2018.

107. A. P. Matz, J.-A. Fernandez-Prieto, J. Cañada-Bago, and U. Birkel, “A Systematic Analysis of Narrowband IoT Quality of Service”, *Sensors*, vol. 20, no. 6, Art. no. 6, Jan. 2020, doi: 10.3390/s20061636.

108. X. Chen, Z. Li, Y. Chen and X. Wang, "Performance Analysis and Uplink Scheduling for QoS-Aware NB-IoT Networks in Mobile Computing," in *IEEE Access*, vol. 7, pp. 44404-44415, 2019.

109. A. Hassebo, M. Obidat and M. Ali, "Four LTE uplink scheduling algorithms performance metrics: Delay, throughput, and fairness tradeoff," *2017*

IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), 2017, pp. 300-305.

110. A. S. Shafigh, P. Mertikopoulos and S. Glisic, "A novel dynamic network architecture model based on stochastic geometry and game theory," *2016 IEEE International Conference on Communications* , Kuala Lumpur, 2016, pp. 1-7.

111. M. Emara, H. ElSawy, S. Sorour, S. Al-Ghadhban, M. Alouini and T. Y. Al-Naffouri, "Stochastic geometry model for multi-channel fog radio access networks," *2017 15th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*, Paris, 2017, pp. 1-6.

112. T. Maksymyuk, M. Brych, V. Pelishok , "Stochastic Geometry Models for 5G Heterogeneous Mobile Networks," *Smart Computing Review*, vol. 5, №2, c. 89-101.

113. D. Sabella, M. Caretti and R. Fantini, "Energy saving schemes for self-backhauled Small Cells in LTE-Advanced networks," *2014 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, Istanbul, 2014, pp. 23-28.

114. R. Trestian et all, "Exploring energy consumption issues for multimedia streaming in LTE HetNet Small Cells," *2015 IEEE 40th Conference on Local Computer Networks (LCN)*, Clearwater Beach, FL, 2015, pp. 498-501.

115. R. Trestian, Q. Vien, P. Shah and G. Mapp, "Exploring energy consumption issues for multimedia streaming in LTE HetNet Small Cells," *2015 IEEE 40th Conference on Local Computer Networks (LCN)*, Clearwater Beach, FL, 2015, pp. 498-501.

116. H. Çelebi, N. Maxemchuk, Y. Li and İ. Güvenç, "Energy reduction in small cell networks by a random on/off strategy," *2013 IEEE Globecom Workshops (GC Wkshps)*, Atlanta, GA, 2013, pp. 176-181.

117. П. О. Гуськов, Т. А. Максимюк, and М. М. Климаш, "Метод динамічного формування структури рівня радіодоступу для мереж 5G", *Вісник*

Національного університету Львівська політехніка. Радіоелектроніка та телекомунікації, №818, с. 220–230, 2015.

118. A. Antonopoulos, E. Kartsakli, A. Bousia, L. Alonso and C. Verikoukis, "Energy-efficient infrastructure sharing in multi-operator mobile networks," in *IEEE Communications Magazine*, vol. 53, no. 5, pp. 242-249, May 2015.

119. M. Oikonomakou, A. Antonopoulos, L. Alonso and C. Verikoukis, "Cooperative Base Station Switching Off in Multi-Operator Shared Heterogeneous Network," *2015 IEEE Global Communications Conference (GLOBECOM)*, 2015, pp. 1-6.

120. S. Lee, S. Moon, and Y. Yi, "On Greening Cellular Networks by Sharing Base Stations: A Game-theoretic Approach", *9th EAI International Conference on Performance Evaluation Methodologies and Tools*, 2016, pp. 87–94.

121. M. W. Kang and Y. W. Chung, "An Efficient Energy Saving Scheme for Base Stations in 5G Networks with Separated Data and Control Planes Using Particle Swarm Optimization", *Energies*, vol. 10, no. 9, Art. no. 9, Sep. 2017.

122. A. A. Barakabitze *et al*., "QoE Management of Multimedia Streaming Services in Future Networks: A Tutorial and Survey," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 526-565, Firstquarter 2020.

123. Z. Xu and A. Zhang, "Network Traffic Type-Based Quality of Experience (QoE) Assessment for Universal Services", *Applied Sciences*, vol. 9, no. 19, Art. no. 19, Jan. 2019.

124. A. Wahab, N. Ahmad, and J. Schormans, "Statistical Error Propagation Affecting the Quality of Experience Evaluation in Video on Demand Applications", *Applied Sciences*, vol. 10, no. 10, Art. no. 10, Jan. 2020.

125. P. Trakas, F. Adelantado and C. Verikoukis, "QoE-Aware Resource Allocation for Profit Maximization Under User Satisfaction Guarantees in HetNets With Differentiated Services," in *IEEE Systems Journal*, vol. 13, no. 3, pp. 2664-2675, Sept. 2019.

126. В. А. Бачинский, В. Ш. Гиоргизова-Гай, “Выбор протокола динамической маршрутизации в корпоративной IP-сети”, *Систем. дослідж. та інформ. Технології,* № 1, С. 99-110, 2011.

127. I. Fiţigău and G. Toderean, "Network performance evaluation for RIP, OSPF and EIGRP routing protocols," *Proceedings of the International Conference on electronics, computers and artificial intelligence - ECAI-2013*, Pitesti, 2013, pp. 1-4.

128. S. G. Thorenoor, "Dynamic Routing Protocol Implementation Decision between EIGRP, OSPF and RIP Based on Technical Background Using OPNET Modeler," *2010 Second International Conference on Computer and Network Technology*, Bangkok, 2010, pp. 191-195.

129. К. Шевчук, С. Захарченко, “Метод вдосконалення одношляхових протоколів динамічної маршрутизації,” *Інформаційні технології та комп'ютерна інженерія,* № 2, 16-25, 2018.

130. Z. Hu, M. Beshley, V. Vitalii, S. Jun and T. Volodymyr, "Modified EIRGP Routing Protocol for Backbone Infrastructure of Wireless Multimedia Sensor Networks," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, Ukraine, 2020, pp. 894-899.

131. O. Lemeshko, O. Yeremenko and A. M. Hailan, "Design of QoS-routing scheme under the timely delivery constraint," *2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)*, Lviv, 2017, pp. 97-99.

132. O. Lemeshko, O. Yeremenko, M. Yevdokymenko, A. Shapovalova, A. Ilyashenko and B. Sleiman, "Traffic Engineering Fast ReRoute Model with Support of Policing," *2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON)*, Lviv, Ukraine, 2019, pp. 842-845.

133. O. Lemeshko, O. Yeremenko and A. M. Hailan, "Two-level method of fast ReRouting in software-defined networks," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 376-379.

134. O. Lemeshko and O. Yeremenko, “Enhanced method of fast re-routing with load balancing in software-defined networks”, *Journal of Electrical Engineering*, vol. 68, no. 6, pp. 444–454, Nov. 2017.

135. И. В. Стрелковская, И. Н. Соловская, “Особенности решения задач управления трафиком в телекоммуникационной сети,” *Наукові праці ОНАЗ ім. О. С. Попова*, № 2. С. 24-34, 2011.

136. И. В. Стрелковская, И. Н. Соловская, “Сравнительный анализ результатов решений задач многопутевой маршрутизации различными методами,” *Наукові праці ОНАЗ ім. О. С. Попова*, № 1, С. 56-64, 2014.

137. O. Lemeshko, O. Yeremenko, M. Yevdokymenko and A. M. Hailan, "Tensor Based Load Balancing under Self-Similar Traffic Properties with Guaranteed QoS," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, Ukraine, 2020, pp. 293-297.

138. U. Shende and V. Bagdi, "A Review on Traffic Engineering Techniques in Software Defined Networks," *2019 International Conference on Intelligent Sustainable Systems (ICISS)*, Palladam, Tamilnadu, India, 2019, pp. 503-506.

139. T. Kim and T. Nguyen-Duc, "OQR: On-demand QoS Routing without Traffic Engineering in Software Defined Networks," *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*, Montreal, QC, 2018, pp. 362-365.

140. Y. Yang, C. Yang, S. Chen, W. Cheng and F. Jiang, "Implementation of Network Traffic Monitor System with SDN," *2015 IEEE 39th Annual Computer Software and Applications Conference*, Taichung, 2015, pp. 631-634.

141. M. Afaq and Wang-Cheol Song, "sFlow-based resource utilization monitoring in clouds," *2016 18th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Kanazawa, 2016, pp. 1-3.

142. S. Zhu, Z. Sun, Y. Lu, L. Zhang, Y. Wei and G. Min, "Centralized QoS Routing Using Network Calculus for SDN-Based Streaming Media Networks," in *IEEE Access*, vol. 7, pp. 146566-146576, 2019

143. . Fu and F. Wu, “Investigation of multipath routing algorithms in software defined networking,” in *Proc. Int. Conf. Green Inform*., Aug. 2017, pp. 269-273.

144. A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: techniques, datasets and challenges”, *Cybersecurity*, vol. 2, no. 1, p. 20, Jul. 2019.

145. S. M and M. T. Roopa, “Inspection of Deep Packet Inspection in Real-time for Performance Testing: A Framework”, *International Journal of Engineering Research & Technology*, vol. 3, no. 27, Jul. 2018, Accessed: Apr. 26, 2021.

146. C. Feng, T. Li and D. Chana, "Multi-level Anomaly Detection in Industrial Control Systems via Package Signatures and LSTM Networks," *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2017, pp. 261-272.

147. T. Ergen and M. Kerpiççi, "A novel anomaly detection approach based on neural networks," *2018 26th Signal Processing and Communications Applications Conference (SIU)*, 2018, pp. 1-4.

148. Junyuan Shen and Jidong Wang, "Network intrusion detection by artificial immune system," *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, 2011, pp. 4716-4720.

149. Y. Liu, H. Yu, C. Gong, and Y. Chen, “A real time expert system for anomaly detection of aerators based on computer vision and surveillance cameras”, *Journal of Visual Communication and Image Representation*, vol. 68, p. 102767, Apr. 2020, doi: 10.1016/j.jvcir.2020.102767.

150. E. Nikolova and V. Jecheva, "Applications of Clustering Methods to Anomaly-Based Intrusion Detection Systems," *2015 8th International Conference on Database Theory and Application (DTA)*, 2015, pp. 37-41.

151. M. Solaimani, M. Iftekhar, L. Khan and B. Thuraisingham, "Statistical technique for online anomaly detection using Spark over heterogeneous data from multi-source VMware performance data," *2014 IEEE International Conference on Big Data (Big Data)*, 2014, pp. 1086-1094.

152. Y. Chae, “Representing Statistical Network-Based Anomaly Detection by Using Trust”, *Open Access Dissertations*, Jan. 2017.

153. P. Dymora and M. Mazurek, “Anomaly Detection in IoT Communication Network Based on Spectral Analysis and Hurst Exponent”, *Applied Sciences*, vol. 9, no. 24, Art. no. 24, Jan. 2019, doi: 10.3390/app9245319.

154. Савицька О. М., Салабай В. О., “Діджиталізація управління бізнесом підприємства в контексті розвитку Індустрії 4.0 в Україні,” *Бізнес, інновації, менеджмент: проблеми та перспективи: зб. тез доп. І Міжнародної наук.-практ. конф., 23 квіт. 2020 р. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка»*, 2020. – С. 62-63.

155. Ролик А.И0., “Модель управления перераспределением ресурсов информационно телекоммуникационной системы при изменении значимости бизнес-процессов,” *Автоматика. Автоматизация. Электротехнические комплексы и системы*, №2 (20), С. 73–82, 2007.

156. A. Singh, G. S. Aujla and R. S. Bali, "Intent-Based Network for Data Dissemination in Software-Defined Vehicular Edge Computing," in *IEEE Transactions on Intelligent Transportation Systems*, doi: 10.1109/TITS.2020.3002349.

157. В.В. Москаленко, С.В. Пімоненко, “Метод прогнозування рівня сприйняття якості обслуговування в інформаційно-телекомунікаційних системах,” *Автоматизированные системы управления и приборы автоматики*,” №172, с. 4 – 12, 2015.

158. “Принципи і методи системного аналізу - Аналіз інноваційної діяльності Підручники для студентів онлайн”. https://stud.com.ua/45001/investuvannya/printsipi_metodi_sistemnogo_analizu (accessed Apr. 26, 2020).

159. V. Chervenets, V. Romanchuk, H. Beshley and A. Khudyy, "QoS/QoE correlation modified model for QoE evaluation on video service," *2016 13th*

International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), 2016, pp. 664-666.

160. M. Beshley, M. Seliuchenko, O. Panchenko and A. Polishuk, "Adaptive flow routing model in SDN," *2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)*, Lviv, 2017, pp. 298-302.

161. V. Romanchuk, M. Beshley, A. Polishuk and M. Seliuchenko, "Method for processing multiservice traffic in network node based on adaptive management of buffer resource," *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, Ukraine, 2018, pp. 1118-1122.

162. K. Phemius and M. Bouet, "Monitoring latency with OpenFlow," *Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)*, Zurich, 2013, pp. 122-125.

163. R. B. Santos, T. R. Ribeiro and C. d. A. C. César, "A network monitor and controller using only OpenFlow," *2015 Latin American Network Operations and Management Symposium (LANOMS)*, Joao Pessoa, 2015, pp. 9-16.

164. S. Jun, K. Przystupa, M. Beshley, O. Kochan, H. Beshley, M. Klymash, J. Wang, D. Pieniak, “A Cost-Efficient Software Based Router and Traffic Generator for Simulation and Testing of IP Network,” *Electronics*, vol. 9, no. 1, pp. 40-1–40-24, Jan. 2020. doi: 10.3390/electronics9010040.

165. В. А. Вишняков та Б. А. Монич, “Модели и управление качеством программно-определяемых сетей”, *Проблемы инфокоммуникаций*, №1, С.42-47, 2019.

166. M. Seliuchenko, M. Beshley, O. Panchenko and M. Klymash, “Development of monitoring system for end-to-end packet delay measurement in software-defined networks,” *IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET’2016)*, Feb. 23-26, 2016, Lviv, Ukraine, pp. 667 – 670.

167. A. D. Khomonenko, V. G. Degtyarev and M. M. Khalil, "Analysing the efficiency of a cloud computing system with a WEB Interface by numerical calculation non-Markovian multichannel system with “cooling”," *2017 XX IEEE International Conference on Soft Computing and Measurements (SCM)*, 2017, pp. 120-123.

168. N. Chechina *et al.*, "Evaluating Scalable Distributed Erlang for Scalability and Reliability," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 28, no. 8, pp. 2244-2257, 1 Aug. 2017.

169. «Исследование и разработка методов построения сетей связи пятого поколения 5G, обеспечивающих выполнение требований концепции Тактильного Интернета», https://www.dissercat.com/content/issledovanie-i-razrabotka-metodov-postroeniya-setei-svyazi-pyatogo-pokoleniya-5g-obespechiva.

170. M. Firdhous, O. Ghazali and S. Hassan, "Modeling of cloud system using Erlang formulas," *The 17th Asia Pacific Conference on Communications*, 2011, pp. 411-416.

171. M. Jia, W. Liang, Z. Xu and M. Huang, "Cloudlet load balancing in wireless metropolitan area networks," *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, 2016, pp. 1-9.

172. М. М. Климаш, Т. А. Максимюк, М. І. Бешлей, *Методи та моделі побудови гетерогенних мереж мобільного зв’язку 4G/5G*. Львів, Україна: Видавництво "Львівська політехніка", 2020. ISBN: 978-966-941-552-3.

173. M. Beshley, M. Klymash, M. Hamal, Y. Shkoropad and A. Branytskyy, "Method for Estimating Service Delay in Edge and Cloud Computing Architecture," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, Ukraine, 2020, pp. 915-919.

174. I. Demydov, M. Klymash, M. Beshley, O. Shpur, “Features of the cloud services implementation in the national network segment of Ukraine,” *Information and telecommunication science*. K.: NTUU «KPI», No.1, pp. 31–38, 2016.

175. M. Klymash, I. Demydov, M. Beshley and O. Kostiv, "Structures Assessment of Data-Centers' Telecommunication Systems for Metadata Fixation," *2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Odessa, Ukraine, 2018, pp. 1-7.

176. М.М. Климаш, В.І. Романчук, М.І. Бешлей, А.О. Лунтовський, "Дослідження ефективності використання ресурсів навчально-наукового центру паралельних обчислень," *Міжнародна науково-технічна конференція (Сучасні інформаційно-телекомунікаційні технології)*, м. Київ, 2015, с. 61–63.

177. I. Demydov, N. Baydoun, M. Beshley, M. Klymash, O. Panchenko, "Development of basic concept of ICT platforms deployment strategy for social media marketing considering tectonic theory*," EUREKA: Physics and Engineering*, vol. 0, no.1, pp. 18–33, Jan. 2020.

178. E. Kapassa, M. Touloupou, A. Mavrogiorgou and D. Kyriazis, "5G & SLAs: Automated proposition and management of agreements towards QoS enforcement," *2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, 2018, pp. 1-5.

179. M. Beshley, P. Vesely, A. Prislupskiy, H. Beshley, M. Kyryk, V. Romanchuk, I. Kahalo, "Customer-Oriented Quality of Service Management Method for the Future Intent-Based Networking," *Applied Sciences*, vol. 10, no. 22, pp. 8223-1– 8223-38. Nov. 2020.

180. O. Panchenko, A. Polishuk, M. Seliuchenko and M. Beshley, "Method for adaptive client oriented management of quality of service in integrated SDN/CLOUD networks," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 452-455.

181. М.І. Бешлей, О.М. Панченко, І.В. Демидов, М.О Селюченко, "Метод динамічного управління якістю послуг в інтегрованій SDN/CLOUD мережі," *Фізико-технологічні проблеми, обробки та зберігання інформації в*

інфокомунікаційних системах: матеріали V Міжнародної науково-практичної конференції, м. Чернівці, 2016 р., с. 74 –75.

182. M. Janner, J. Fu, M. Zhang, and S. Levine, “When to Trust Your Model: Model-Based Policy Optimization”, *Advances in Neural Information Processing Systems*, vol. 32, 2019, Accessed: Apr. 26, 2021.

183. Y. Sun, X. Yuan, W. Liu and C. Sun, "Model-Based Reinforcement Learning via Proximal Policy Optimization," *2019 Chinese Automation Congress (CAC)*, 2019, pp. 4736-4740.

184. M. Varela, P. Zwickl, P. Reichl, M. Xie and H. Schulzrinne, "From Service Level Agreements (SLA) to Experience Level Agreements (ELA): The challenges of selling QoE to the user," *2015 IEEE International Conference on Communication Workshop (ICCW)*, 2015, pp. 1741-1746.

185. Z. Weiwei, G. Jian, G. Wenjie and C. Shaomin, "NetFlow-based network traffic monitoring," *2011 13th Asia-Pacific Network Operations and Management Symposium*, 2011, pp. 1-4.

186. D. He, S. Chan, X. Ni and M. Guizani, "Software-Defined-Networking-Enabled Traffic Anomaly Detection and Mitigation," in *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1890-1898, Dec. 2017.

187. J. Hong, C. Liu and M. Govindarasu, "Integrated Anomaly Detection for Cyber Security of the Substations," in *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1643-1653, July 2014.

188. J. Yang, C. Zhou, S. Yang, H. Xu and B. Hu, "Anomaly Detection Based on Zone Partition for Security Protection of Industrial Cyber-Physical Systems," in *IEEE Transactions on Industrial Electronics*, vol. 65, no. 5, pp. 4257-4267, May 2018.

189. D. Kao, "Using the Actionable Intelligence Approach for the DPI of Cybercrime Insider Investigation," *2020 22nd International Conference on Advanced Communication Technology (ICACT)*, 2020, pp. 1218-1224.

190. W. Song, M. Beshley, K. Przystupa, H. Beshley, O.Kochan, A.Pryslupskyi, D. Pieniak, J.Su, “A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection,” *Sensors*, vol. 20, no. 6, p. 1637-1–1637-41, March 2020.

191. H. Xu, K. Przystupa, C. Fang, O. Kochan, M. Beshley, A.Marciniak, “A combination strategy of feature selection based on an integrated optimization algorithm and weighted k-nearest neighbor to improve the performance of network intrusion detection,” *Electronics*, vol. 9, no. 8, pp. 1206-1–1206-22, July 2020.

192. M. Beshley, S. Toliupa, V. Pashkevych and R. Kolodiy, “Development of software system for network traffic analysis and intrusion detection,” *2018 International Conference Radio Electronics & Info Communications (UkrMiCo)*, Kiev, 2018, pp. 1-3.

193. Z. Cheng, M. Beshley, H. Beshley, O. Kochan and O. Urikova, "Development of Deep Packet Inspection System for Network Traffic Analysis and Intrusion Detection," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, Ukraine, 2020, pp. 877-881.

194. .І. Бешлей, М.М. Климаш, О.М. Панченко, Г.В. Бешлей, “Розроблення системи моніторингу та аналізу трафіку інформаційно телекомунікаційної мережі для виявлення аномалії і запобігання атак,” *І міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно телекомунікаційних систем” (PCSITS)*, м. Київ, 2018р., с. 201–203.

195. M. Laumer, P. Amon, A. Hutter and A. Kaup, "A compressed domain change detection algorithm for RTP streams in video surveillance applications," *2011 IEEE 13th International Workshop on Multimedia Signal Processing*, 2011, pp. 1-6.

196. M. Eslahi, M. S. Rohmad, H. Nilsaz, M. V. Naseri, N. M. Tahir and H. Hashim, "Periodicity classification of HTTP traffic to detect HTTP Botnets," *2015 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, 2015, pp. 119-123.

197. C. Çiflikli, A. Gezer, A. T. ÖzÖahin and Ö. Özkasap, "Comparison of Bittorrent packet traffic characteristics over IPv6 and IPv4," *2009 International Conference on Application of Information and Communication Technologies*, 2009, pp. 1-5.

198. C. Testa and D. Rossi, "On the impact of uTP on BitTorrent completion time," *2011 IEEE International Conference on Peer-to-Peer Computing*, 2011, pp. 314-317.

199. Glossary: Common DDoS Attack Types. Corero, 2019. https://www.corero.com/blog/glossary/

200. Albion. https://gcorelabs.com/ru/cases/albion/ (accessed Apr. 27, 2021).

201. С. В. Гаркуша та О. В. Гаркуша, “Розробка математичної моделі управління пропускною здатністю низхідного каналу зв’язку технології LTE, що використовує перший вид розподілу ресурсів”, *Вісник Національного університету Львівська політехніка. Радіоелектроніка та телекомунікації,* №. 818, pp. 211–219, 2015.

202. Y. Kim and S. Park, "Analytical Calculation of Spectrum Requirements for LTE-A Using the Probability Distribution on the Scheduled Resource Blocks," in *IEEE Communications Letters*, vol. 22, no. 3, pp. 602-605, March 2018.

203. P. Rengaraju, C. Lung, F. R. Yu and A. Srinivasan, "On QoE monitoring and E2E service assurance in 4G wireless networks," in *IEEE Wireless Communications*, vol. 19, no. 4, pp. 89-96, August 2012.

204. M. Klymash, H. Beshley, M. Seliuchenko and T. Maksymyuk, "Improving architecture of LTE mobile network for IoT services provisioning," *2017 2nd International Conference on Advanced Information and Communication Technologies (AICT)*, 2017, pp. 209-212.

205. L. A. Sonkusare and S. N. Dhage, "Analysis of LTE UE RF parameters for 3GPP specification," *2015 International Conference on Computers, Communications, and Systems (ICCCS)*, 2015, pp. 82-86.

206. M. Beshley, N. Kryvinska, M. Seliuchenko, H. Beshley, E. Shakshuki, A. Yasar, “End-to-End QoS “Smart Queue” Management Algorithms and Traffic Prioritization Mechanisms for Narrow-Band Internet of Things Services in 4G/5G Networks,” *Sensors*, vol. 20, no.8, pp.2324-1–2324-30, Apr. 2020.

207. I. I. Al-Shiab and R. E. Ahmed, "On fairness in LTE downlink MAC scheduling algorithms," *2015 International Conference on Information and Communication Technology Research (ICTRC)*, 2015, pp. 171-174.

208. A. H. Bui, C. T. Nguyen, T. C. Thang and A. T. Pham, "A Comprehensive Distributed Queue-Based Random Access Framework for mMTC in LTE/LTE-A Networks With Mixed-Type Traffic," in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 12, pp. 12107-12120, Dec. 2019.

209. М.М. Климаш, М.І. Бешлей, Ю.Д. Дещинський, О.М. Панченко, “Розробка методу балансування навантаження в SDN мережах на основі модифікованого протоколу STP,” *Комп’ютерні технології друкарства*, №2, с.с. 146–155, 2015

210. М.І. Бешлей, В.В. Червенець, І.В. Демидов, В.І. Романчук, О.М. Панченко, “Розвиток методів передавання даних реального часу шляхом вдосконалення процесів пріоритезації потоків у маршрутизаторах,” *Системи озброєння і військова техніка:- Х: Харк. ун-т Повітр. Сил ім. І. Кожедуба*, 5(142), с. 114 –123, 2016.

211. A. Koors, "Assessing Risk in Discrete Event Simulation by Generalized Deviation," *2013 8th EUROSIM Congress on Modelling and Simulation*, 2013, pp. 336-344.

212. І.О. Кагало, М.І. Бешлей, М.М. Климаш, О.М. Панченко, Г.В. Бешлей, “Адаптивне формування багаторівневої радіоструктури інтегрованих мереж LTE/Wi-Fi,” *Телекомунікаційні та інформаційні технології*, № 3(64), с. 24 –38, 2019.

213. П. О. Гуськов, А. С. Цуркан, О. М. Шпур, Б. А. Бугиль, and М. М. Климаш, “Модель мережі радіодоступу з використанням методу адаптивного

формування структури”, *Вісник Національного університету Львівська політехніка. Радіоелектроніка та телекомунікації*,№ 849, pp. 256–264, 2016.

214. I. Kahalo, H. Beshley, M.Beshley and O. Panchenko, “Enhancing QoS and energy efficiency of LTE/LTE-U/Wi-Fi integrated network based on adaptive technique for radio structure formation,” *in Proc. of IEEE 2019 UKRCON*, Kiev, 2019, pp. 1167–1170.

215. D. Gonzalez G. and J. Hamalainen, "Planning and Optimization of Cellular Networks through Centroidal Voronoi Tessellations," *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, 2015, pp. 1-2.

216. P. Mandal, "PCRF: On the blocking probability of LTE-A," *2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2020, pp. 1-4.

217. T. V. K. Buyakar, H. Agarwal, B. R. Tamma and A. A. Franklin, "Resource Allocation with Admission Control for GBR and Delay QoS in 5G Network Slices," *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, 2020, pp. 213-220.

218. Miaona Huang, Suili Feng and Jun Chen, "Dynamic association for load balancing in LTE multi-cell networks," *Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC)*, 2013, pp. 3465-3469.

219. H. Wang, L. Ding, P. Wu, Z. Pan, N. Liu and X. You, "QoS-Aware Load Balancing in 3GPP Long Term Evolution Multi-Cell Networks," *2011 IEEE International Conference on Communications (ICC)*, 2011, pp. 1-5

220. F. H. Khan and M. Portmann, “Joint QoS-control and handover optimization in backhaul aware SDN-based LTE networks”, Wireless Netw, vol. 26, no. 4, pp. 2707–2729, May 2020, doi: 10.1007/s11276-019-02021-7.

221. M. Klymash, O. Lavriv, T. Maksymyuk and M. Beshley, "State of the art and further development of information and communication systems," *2016*

International Conference Radio Electronics & Info Communications (UkrMiCo), Kiev, 2016, pp. 1-6.

222. S. Wenguang, V. Andrushchak, M. Kaidan, M. Beshley, O. Kochan, S. Jun, “Methodology for Calculating the Energy Consumption of Information Communication Systems,” *Technical Electrodynamics*, no. 4, pp. 80–88, July 2020

223. K. Przystupa, M. Beshley, M. Kaidan, V. Andrushchak, I. Demydov, O. Kochan, D. Pieniak, “Methodology and Software Tool for Energy Consumption Evaluation and Optimization in Multilayer Transport Optical Networks,” *Energies*, vol. 13, no. 23, pp. 6370-1–6370-21. Dec. 2020.

224. Г.В. Бешлей, М.О. Селюченко, І.А Берневек, С.І. Пущак, М.І. Бешлей, “Алгоритм кластеризації, агрегації та класифікації M2M пристроїв в гетерогенній мережі 4G/5G,” *Вісник Національного університету “Львівська політехніка”. Радіоелектроніка та телекомунікації*, № 874, с. 95–102, 2017.

225. M. Klymash, H. Beshley, M. Seliuchenko and M. Beshley, "Algorithm for clusterization, aggregation and prioritization of M2M devices in heterogeneous 4G/5G network," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 182-186.

226. H. Beshley, M. Klymash, M. Beshley and I. Kahalo, "Improving the Efficiency of LTE Spectral Resources Use by Introducing the New of M2M/IoT Multi-Service Gateway," *2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM)*, Polyana, Ukraine, 2019, pp. 114-117.

227. V. Romanchuk, M. Klymash, M. Beshley, O. Panchenko, A. Polishchuk, “Development of software-based router model with adaptive selection of algorithms for queues servicing,” *Technology audit and production reserves,* №3/2(41), pp. 46–55, 2018.

228. В.І. Романчук, М.І. Бешлей, А.М. Прислупський, Г.В. Бешлей, “Метод декомпозиції структури мережного пристрою з віртуалізацією ресурсів,” *Наукові записки Української академії друкарства*, №1(56), с. 31– 42. 2018.

229. М.В. Кайдан, М.І. Бешлей, Т.А. Максимюк, Б.М. Стрихалюк, Р.З. Матвіїв, “Теорія Кернера та фазові переходи для потоків у телекомунікаційних мережах,” *Вісник Національного університету “Львівська політехніка”*. Радіоелектроніка та телекомунікації, № 909, с. 29–34, 2018.

230. M. Beshley, V. Romanchuk, V. Chervenets and A. Masiuk, "Ensuring the quality of service flows in multiservice infrastructure based on network node virtualization," *2016 International Conference Radio Electronics & Info Communications (UkrMiCo)*, Kiev, 2016, pp. 1-3.

231. M. Klymash, V. Romanchuk, M. Beshley and P. Arthur, "Investigation and simulation of system for data flow processing in multiservice nodes using virtualization mechanisms," 2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON), Kiev, 2017, pp. 989-992.

232. М.І. Бешлей, В.В. Червенець, В.І. Романчук, А.В. Поліщук, “Модель віртуального маршрутизатора з статичною та динамічною реконфігурацією ресурсів,” *Міжнародна науково технічна конференція «Проблеми телекомунік аці» ПТ-2016: збірник матеріалів конференції* , м. Київ, 2016р., с. 140–142.

233. M. Seliuchenko, M. Kyryk, M. Beshley, M. Zhovtonoh, “Automated Recovery of Server Applications for SDN-Based Internet of Things,” *2019 IEEE 3nd International Conference on Advanced Information and Communication Technologies (AICT)*, Lviv, 2019, pp. 25-29.

234. M. Klymash, M. Beshley, “Perspective directions of development and research in the field of information and communication technologies,” *BA Magazine “Wissen im Markt”*, no. 3, pp. 31–37, 2019

235. М.М. Климаш, А.Р. Масюк, Г.В. Бешлей, М.І. Бешлей, “Концепція програмно конфігурованої гетерогенної мережі мобільного зв'язку на основі технологій SDN/NFV та SDR,” *Фізико-технологічні проблеми , обробки та*

зберігання інформації в інфокомунікаційних системах: матеріали V Міжнародної науково-практичної конференції, м. Чернівці, 2016 р., с. 35–36.

236. T. Maksymyuk, M. Beshley, M. Klymash, O. Petrenko and Y. Matsevityi, "Eavesdropping-resilient wireless communication system based on modified OFDM/QAM air interface," *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, Ukraine, 2018, pp. 1127-1130.

237. М.М. Климаш, В.І. Романчук, О.М. Панченко, М.І. Бешлей, А.В. Поліщук, "Розроблення програмного маршрутизатора з автоматичним розгортанням віртуальних вузлів," *Вісник Національного університету "Львівська політехніка". Радіоелектроніка та телекомунікації*, № 885, с. 22 – 30, 2017.

238. V. Romanchuk, M. Beshley, O. Panchenko and P. Arthur, "Design of software router with a modular structure and automatic deployment at virtual nodes," 2017 2nd International Conference on Advanced Information and Communication Technologies (AICT), Lviv, 2017, pp. 295-298.

239. H. Beshley, M. Beshley, T. Maksymyuk and I. Strykhalyuk, "Method of centralized resource allocation in virtualized small cells network with IoT overlay," in Proc. of IEEE 2018 TCSET, Lviv-Slavske, 2018, pp. 1147–1151.

240. M. Beshley, A.Pryslupskyi, O. Panchenko and H. Beshley, "SDN/Cloud Solutions for Intent-Based Networking," *2019 IEEE 3nd International Conference on Advanced Information and Communication Technologies (AICT)*, Lviv, 2019, pp. 95-98.

241. Beshley, A. Pryslupskyi, O. Panchenko and M. Seliuchenko, "Dynamic Switch Migration Method Based on QoE- Aware Priority Marking for Intent-Based Networking," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, Ukraine, 2020, pp. 864-868.

242. М.М. Климаш, М.В. Кайдан, М.І. Бешлей, А.В. Редька, “Оптимізація багатошарової структури транспортної мережі на основі технологій IP/MPLS/DWDM за допомогою методу діакоптики,” *Наукові записки Українського науково-дослідного інституту зв'язку*, № 3, с. 32–42, 2015.

243. M. Klymash, M. Seliuchenko, M. Beshley and S. Redchuk, "Increasing wavelengths utilization efficiency in OTNoDWDM network based on local resource distribution method," *2015 Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*, Kharkiv, 2015, pp. 157-160.

244. V. Romanchuk. M. Beshley, A. Prislupskiy, H. Beshley, O. Panchenko, “Method of multiservice infrastructure decomposition with network resource slicing for IoT,” *Internet of Things (IoT) and Engineering Applications (Canada),* vol. 3, no.1, pp. 22–23. May 2018.

245. М.М. Климаш, А.Б. Нажм, О.Л. Костів, І.В. Демидов, М.І. Бешлей, “Створення ефективних ІКТ-платформ електронного урядування інтерактивного типу: аналіз архітектури систем розповсюдження контенту,” *Наукові записки Українського науково-дослідного інституту зв'язку*, № 3, с. 31–45, 2019.

246. M. Beshley, *Development and testbed of software router for critical application*. Saarbrücken, Germany: LAP Lambert Academic Publishing, 2019. ISBN: 978-613-9-46367-1.

247. M. Beshley , N. Kryvinska, H. Beshley, O. Kochan and L. Barolli, "Measuring End-to-End Delay in Low Energy SDN IoT Platform," *Computers, Materials & Continua,* vol. 69, pp. 2021.

248. В.І Романчук, М.І. Бешлей, О.М. Панченко, А.В. Поліщук, “Метод узгодженого розв’язання завдань балансування різнопріоритетного навантаження між чергами мережевих пристроїв,” *Наукові записки Українського науково-дослідного інституту зв’язку*, №2(50), с. 48–57, 2018.

249. M. Beshley, M. Seliuchenko, O. Panchenko, O. Zyuzko and I. Kahalo, "Experimental performance analysis of software-defined network switch and controller," *in Proc. of IEEE 2018 TCSET*, Lviv-Slavske, 2018, pp. 282–286.

250. Z. Zhang, L. Ma, K. K. Leung, F. Le, S. Kompella and L. Tassiulas, "How Advantageous Is It? An Analytical Study of Controller-Assisted Path Construction in Distributed SDN," in *IEEE/ACM Transactions on Networking*, vol. 27, no. 4, pp. 1643-1656, Aug. 2019.

251. T. Das and M. Gurusamy, "Controller Placement for Resilient Network State Synchronization in Multi-Controller SDN," in *IEEE Communications Letters*, vol. 24, no. 6, pp. 1299-1303, June 2020.

252. S. Ejaz, Z. Iqbal, P. Azmat Shah, B. H. Bukhari, A. Ali and F. Aadil, "Traffic Load Balancing Using Software Defined Networking (SDN) Controller as Virtualized Network Function," in *IEEE Access*, vol. 7, pp. 46646-46658, 2019.

253. A. Pryslupskyi, O. Panchenko, M. Beshley and M. Seliuchenko, "Improvement of multiprotocol label switching network performance using software-defined controller," *in Proc. of IEEE 2019 CADSM*, Polyana, Ukraine 2019, pp. 106–109.

254. E. Mallada, X. Meng, M. Hack, L. Zhang and A. Tang, "Skewless network clock synchronization without discontinuity: convergence and performance," *IEEE/ACM Transactions on Networking*, vol. 23, no. 5, pp. 1619–1633, 2015.

255. M. Beshley , N. Kryvinska, H. Beshley, M. Medvetskyi and L. Barolli, "Centralized QoS Routing Model for Delay/Loss Sensitive Flows at the SDN-IoT Infrastructure," *Computers, Materials & Continua*. 2021.

256. М.М. Климаш, В.І. Романчук, М.І. Бешлей, “Розроблення макету мультисервісної мережі на базі програмно-апаратної платформи для забезпечення навчально-наукового процесу кафедри телекомунікацій,” *1st International Conference "Advanced Information and Communication Technologies"(AICT’2015)*, Lviv, 2015, pp. 175–178.

257. D. González, C. Mellado, K. Waltam and A. Lara, "Low-cost SDN Switch Comparison: Zodiac FX and Raspberry Pi," *2019 IV Jornadas Costarricenses de Investigación en Computación e Informática (JoCICI)*, 2019, pp. 1-5.

258. “nginx”. https://hub.docker.com/_/nginx (accessed Apr. 28, 2020).

259. Y. Cheng, B. Chen and Y. Lee, "Design and Performance Evaluation of Very Large-scale Optical Frame Switching Networks based on WSS for Future Data Centers," *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 2019, pp. 1-4.

260. N. Networks, “Zodiac GX - Zodiac GX Hardware Specifications”, Northbound Networks. https://northboundnetworks.com/pages/zodiac-gx-zodiac-gx-hardware-specifications (accessed Apr. 28, 2021).

261. M. Medvetskyi, M. Beshley and M. Klymash, "A Quality of Experience Management Method For Intent-Based Software-Defined Networks," *2021 IEEE 16th International Conference on the Experience of Designing and Application of CAD Systems (CADSM)*, 2021, pp. 59-62.

262. L. Goswami and P. Agrawal, "IOT based Diagnosing of Fault Detection in Power Line Transmission through GOOGLE Firebase database," *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, 2020, pp. 415-420.

263. М.І. Бешлей, М.О. Селюченко, П.О. Гуськов, А.Р. Масюк, “Підвищення ефективності роботи гетерогенних мереж методом динамічного перерозподілу ресурсів між різними безпроводовими технологіями,” *Міжнародна науково-технічна конференція «Сучасні інформаційно-телекомунікаційні технології»: матеріали науково-технічної конференції*, м. Київ, 2015 р., с. 49–50.

264. М.І. Бешлей, М.М. Климаш, А.Р. Масюк, “Розробка і дослідження імітаційної моделі безпровідної гетерогенної мережі,” *Міжнародна науково-технічна конференція «Проблеми телекомунікацій» ПТ-2016: збірник матеріалів конференції*, м. Київ, 2016 р., с. 70–72.

265. Masiuk, M. Beshley, O. Lavriv and Y. Deschynskiy, “Common radio resource management model for heterogeneous cellular networks,” *IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET’2016)*, Feb. 23-26, 2016, Lviv, Ukraine, pp. 661-663

266. H. Beshley, M. Kyryk, M. Beshley and O. Panchenko, "Method of Information Flows Engineering and Resource Distribution in 4G/5G Heterogeneous Network for M2M Service Provisioning," *2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)*, Lviv, 2018, pp. 229-233.

267. M. Klymash, H. Beshley, O. Panchenko and M. Beshley, "Method for optimal use of 4G/5G heterogeneous network resourses under M2M/IoT traffic growth conditions," *2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, 2017, pp. 1-5.

268. A. Biswas and V. R. Gupta, "Multiband Antenna Design for Smartphone Covering 2G, 3G, 4G and 5G NR frequencies," *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, 2019, pp. 84-87.

269. S. Ghauri and D. Feng, "Analysis of UWB coexistence with 2G/3G/4G Wireless Communication systems," *2012 Proceedings of International Conference on Modelling, Identification and Control*, 2012, pp. 1028-1033.

270. L. Tong, Z. Pei, Z. Yanyun and M. Dexiang, "The analysis of intermodulation interference for coexistence of different systems including 2G/3G/4G," *2014 XXXIth URSI General Assembly and Scientific Symposium (URSI GASS)*, 2014, pp. 1-4.

271. М.О. Селюченко, Г.В. Бешлей, А.Р. Масюк, М.І. Бешлей, “Багаторівневе управління ресурсами в гетерогенній мульти-операторській мережі,” *1st International Conference "Advanced Information and Communication Technologies"(AICT’2015)*, Lviv, 2015, pp. 125–128.

272. М.М. Климаш, В.І. Романчук, М.І. Бешлей, “Розроблення макету мультисервісної мережі на базі програмно-апаратної платформи для забезпечення навчально-наукового процесу кафедри телекомунікацій,” *1st International Conference "Advanced Information and Communication Technologies"(AICT’2015)*, Lviv, 2015, pp. 175–178.

273. L. Wang and D. T. Delaney, "QoE Oriented Cognitive Network Based on Machine Learning and SDN," *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, 2019, pp. 678-681.

274. T. Szyrkowiec *et al.*, "Automatic intent-based secure service creation through a multilayer SDN network orchestration," in *IEEE/OSA Journal of Optical Communications and Networking*, vol. 10, no. 4, pp. 289-297, April 2018ю

275. T. Subramanya, R. Riggio and T. Rasheed, "Intent-based mobile backhauling for 5G networks," *2016 12th International Conference on Network and Service Management (CNSM)*, 2016, pp. 348-352.

276. A. Campanella, "Intent Based Network Operations," *2019 Optical Fiber Communications Conference and Exhibition (OFC)*, 2019, pp. 1-3.

277. K. Abbas et al, "IBNSlicing: Intent-Based Network Slicing Framework for 5G Networks using Deep Learning," *2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 2020, pp. 19-24.

278. E. Zeydan and Y. Turk, "Recent Advances in Intent-Based Networking: A Survey," *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 2020, pp. 1-5.

279. F. Aklamanu, S. Randriamasy, E. Renault, I. Latif and A. Hebbar, "Intent-Based Real-Time 5G Cloud Service Provisioning," *2018 IEEE Globecom Workshops (GC Wkshps)*, 2018, pp. 1-6.

280. W. Chao and S. Horiuchi, "Intent-based cloud service management," *2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, 2018, pp. 1-5.

Додаток 1. Акти впровадження

"ЗАТВЕРДЖУЮ"
Директор
ТзОВ «ОСТВЕР СЕРВІСЕЗ»
_____ Купецька І. Б.
10. 01. 2021р.

АКТ

про використання результатів докторської дисертаційної роботи
Бешлей Миколи Івановича
«Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів»

Даний акт складений про те, що у ТзОВ «ОСТВЕР СЕРВІСЕЗ» використані результати дисертаційної роботи «Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів» представленої на здобуття наукового ступеня доктора технічних наук.

Зокрема, використано модель енергоефективної QoE-маршрутизації для інтенційно-орієнтованих мереж, яка для вибору оптимального маршруту передавання використовує адаптивну QoE-орієнтовану метрику шляху, що автоматизовано розраховується централізованим контролером мережі на основі розробленої математичної моделі кореляції нормалізованого значення замовленого рівня якості сприйняття сервісу та інтегрального адитивного критерію поточних показників якості обслуговування із врахування функціональних параметрів завантаженості мережевих вузлів, що дало змогу підтримувати компроміс між бажаною інтенційно-орієнтованою якістю обслуговування користувачів, завантаженістю та енергоефективністю мережі шляхом переведення в енергозберігаючий режим не задіяних вузлів.

Запропонована модель енергоефективної QoE-маршрутизації потоків даних у порівнянні із відомою концептуальною моделлю багатокритеріальної маршрутизації DMCQR (Deterministic Multiconstrained Centralized QoS Routing) для програмно-конфігурованих мереж, дала змогу досягти кращої збалансованості завантаження канальних ресурсів мережі за рахунок раціонального вибору шляхів передавання для різнорідного трафіка та зменшити до 3 разів середню затримку обслуговування потоків реального часу з кінця в кінець для яких при використанні маршрутизації DMCQR не виконувались допустимі норми затримки, а також в умовах низької інтенсивності загального трафіку зменшити енергоспоживання мережі до 53,56%.

Результати експериментальних досліджень, виконаних на виробничих потужностях ТзОВ «ОСТВЕР СЕРВІСЕЗ» в процесі тестування розробленого автором програмного забезпечення та спеціалізованих прикладних програмних інтерфейсів необхідних для реалізації інтенційно-орієнтованої мережі розгорнутої на платформі програмно-конфігурованих мереж SDN відповідають результатам досліджень, що представлені у дисертаційній роботі, похибка не перевищує 2%.

Результати дисертаційної роботи «Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів» використовувались на безоплатній основі за згодою автора.

Директор Купецька І. Б.

"ЗАТВЕРДЖУЮ"
Директор Львівської філії
(керуючої філії Західного макрорегіону)
ПАТ «Укртелеком» у м. Львові, кандидат технічних наук

_____ Андрухів Т.В.
_____ 2020 р.
79007, м. Львів, вул. Дорошенка, 43

АКТ

про впровадження результатів дисертаційної роботи **Бешлея Миколи Івановича** на тему «**Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів**» на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі

Даний акт складений про те, що в результаті спільних наукових досліджень в напрямку майбутньої трансформації та синтезу телекомунікаційної мережі у Львівській філії ПАТ «Укртелеком» була використана запропонована Бешлеєм М.І. методологія аналізу та синтезу складних гетерогенних телекомунікаційних систем з метою створення нової програмно-конфігурованої інтенційно-орієнтованої мережі, яка відрізняється від існуючих підходів багатоаспектним уявленням про структуру інфокомунікаційної системи як про цілісну централізовану програмовану мережну інфраструктуру, що складається з окремих підсистем та дало змогу інтелектуально виділяти зв'язки між структурно-функціональними елементами мережі, які можуть не тільки автоматизовано перебудовуватись з різною продуктивністю, але й виникати заново, вишукуючи шляхи найбільш адекватного пристосування до мінливих вимог користувачів для підвищення рівня адаптивності системи на основі розроблених методів управління якістю сприйняття сервісу, захищеності даних, енергоефективності та гнучкості використання ресурсів.

Підприємство підтверджує працездатність розроблених, методів, алгоритмів та засобів необхідних для трансформації існуючої мережі в напрямку побудови майбутньої інтенційно-орієнтованої телекомунікаційної мережі. Зокрема, протестовано та підтверджено на виробничих потужностях ПАТ «Укртелеком» ефективність використання розроблених автором Бешлеєм М.І.:

- адаптивного алгоритму вибору рівня технології граничних та хмарних обчислень для забезпечення необхідного рівня якості обслуговування сервісів в інтенційно-орієнтованій інфокомунікаційній мережі.
- алгоритму вибору мережі доступу в гетерогенному середовищі з використанням Big Data, який, на відміну від відомих, враховує та аналізує оцінки замовленої якості сприйняття послуги та дає змогу покращити якість обслуговування високопріоритених послуг на вимогу та збільшити прибуток оператора.
- прототипу мобільного та операторського додатку для адаптивного клієнт-орієнтованого надання послуг в гетерогенній телекомунікаційній мережі, що дає змогу отримувати користувачам замовлену якість обслуговування на основі зворотного зв'язку між оператором мережі.

Акт складений для пред'явлення до спеціалізованої вченої ради із захисту дисертацій і не є підставою для фінансових розрахунків.

Начальник відділу планування мереж Качан В.М.

«ЗАТВЕРДЖУЮ»
Директор
ТзОВ «Телекомунікаційна компанія»

_____ Пентак І.М.
“07” 10 2020 р.

АКТ
про використання результатів докторської дисертаційної роботи
Бешлея Миколи Івановича
«Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів»

Даний акт складений про те, що у ТзОВ «Телекомунікаційна компанія» використані результати дисертаційної роботи Бешлея М.І. «Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів», представленої на здобуття наукового ступеня доктора технічних наук. Зокрема, на телекомунікаційній мережі ТзОВ «Телекомунікаційна компанія» впроваджено метод адаптивного клієнт-орієнтованого управління якістю надання послуг для телекомунікаційних мереж, який, на відміну від відомих, в умовах високого навантаження мережі для формування якості послуги включає в себе як об'єктивну оцінку часових мережевих характеристик, так і замовлені згідно намірів суб'єктивні QoE (Quality of Experience) оцінки клієнтів, що дало змогу кінцевим користувачам сервісів опосередковано впливати на функціональну конфігурацію мережі, а з допомогою машинного навчання реагувати на несприятливі поєднання значень показників якості і попереджати ситуації, коли користувач незадоволений якістю отриманих сервісів для адаптивного прогнозування моменту переконфігурації мережі.

Для відділу управління та розвитку мережі представниками ТзОВ «Телекомунікаційна компанія» використано імітаційну модель інтенційно-орієнтованої телекомунікаційної мережі з можливістю перемикання між двома методами управління якістю обслуговування (традиційного та клієнт-орієнтованого). Перевагою даної моделі є можливість досліджувати нові рішення для майбутньої концепції інтенційно-орієнтованих мереж шляхом інтеграції унікальних алгоритмів у ядро мережі. Встановлено, що запропонований метод адаптивного клієнт-орієнтованого управління якістю послуг дає виграш в середньому від 2-5 разів за критерієм кількості користувачів, які вимагають високої якості сприйняття послуги.

Результати експериментальних досліджень, виконаних на виробничих потужностях ТзОВ «Телекомунікаційна компанія», відповідають результатам досліджень, що представлені у дисертаційній роботі, похибка не перевищує 2%.

Головний інженер Рубаха І.М.

"ЗАТВЕРДЖУЮ"
Директор
ТзОВ «МаксіТех»
_____ Заблоцький С.О.
"___" _____ 2020 р.

АКТ

про використання результатів докторської дисертаційної роботи
Бешлея Миколи Івановича
«Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів»

Даний акт складений про те, що у ТзОВ «МаксіТех» для підвищення рівня захищеності корпоративної інформаційної мережі використані результати дисертаційної роботи Бешлея М.І. «Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів», представленої на здобуття наукового ступеня доктора технічних наук, зокрема:

- інтелектуальну DPI (Deep Packet Inspection) систему моніторингу та аналізу мережевого трафіку, що дала змогу виявити складні атаки різного роду, зокрема таких як Non-Spoofed UDP Flood та шляхом автоматизованого блокування виявленого шкідливого трафіку зменшити загальний рівень втрат на 5% у порівнянні із існуючою комерційною системою SolarWinds DPI. Також, запропонована система надала можливість інтелектуально управляти, здійснювати діагностику інформаційної мережі та оцінювати функції і процедури електронних бізнес-процесів та їх взаємозв'язок, з метою раціонального управління мережними ресурсами, адаптованими до цілей розвитку підприємства;
- метод виявлення аномалій мережевого трафіку для систем моніторингу інформаційної мережі, який відрізняється від відомих формуванням набору інформативних ознак, що характеризують нормальну та аномальну поведінку інфокомунікаційної системи на основі оцінки параметра Херста із можливістю самонавчання, що дало змогу, за короткий проміжок часу, з високим ступенем точності, автоматизовано, виявляти та блокувати складні атаки різних типів в традиційних та майбутніх інтенційно-орієнтованих мережах.

Результати експериментальних досліджень, виконаних на виробничих потужностях ТзОВ «МаксіТех», відповідають результатам досліджень, що представлені у дисертаційній роботі, похибка не перевищує 3%.

Директор Заблоцький С.О.

"ЗАТВЕРДЖУЮ"
Заступник директора
ТОВ «ІнформКонсалт»

Матіїшин Л.З.
“ 24 ” 04 2020 р.

АКТ

про використання результатів докторської дисертаційної роботи
Бешлея Миколи Івановича
«Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів»

Даний акт складений про те, що у ТОВ «ІнформКонсалт», для підвищення якості функціонування корпоративної мережі, використані результати дисертаційної роботи Бешлея М.І. «Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів», представленої на здобуття наукового ступеня доктора технічних наук, а саме:

- прототип корпоративного сегменту енергоефективної інтенційно-орієнтованої мережі побудованого на базі мікроконтролерних платформ та віртуалізації мережевих функцій компонентів технології SDN, впровадження якого дало змогу підвищити гнучкість управління мережею, зменшити енергоспоживання мережі та забезпечити необхідну якість надання сервісів, у тому числі і критично важливих IoT даних;
- систему моніторингу якості функціонування реалізованого прототипу інтенційно-орієнтованої мережі за критерієм наскрізної затримки передавання даних, що є одним із ключових параметрів моніторингу якості надання сервісів реального часу критично-важливої інфраструктури. Особливістю системи є використання розробленого Бешлеєм М.І. унікального методу наскрізного вимірювання затримки передавання даних шляхом додавання часової мітки до метаданих заголовків пакету, що дає змогу визначати час оброблення пакету кожним компонентом мережі та в умовах перевищення норм сповіщати про прийняття необхідних керуючих рішень.

Заступник директора Матіїшин Л.З.

«ЗАТВЕРДЖУЮ»
Директор
ТзОВ ВТФ «Контех»

_____ Смольницький Є.С.
"07" 10 2020 р.

АКТ

про використання результатів докторської дисертаційної роботи
Бешлея Миколи Івановича
«Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів»

Даний акт складений про те, що у ТзОВ ВТФ «Контех» для підвищення рівня захищеності корпоративної інформаційної мережі використані результати дисертаційної роботи Бешлея М.І. «Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів», представленої на здобуття наукового ступеня доктора технічних наук.

Зокрема представниками компанії ТзОВ ВТФ «Контех» за згодою автора Бешлея М.І. використано для внутрішньої корпоративної мережі інтелектуальну систему моніторингу та аналізу мережевого трафіку, що дала змогу виявити складні атаки різного роду, зокрема таких як Non-Spoofed UDP Flood та шляхом автоматизованого блокування виявленого шкідливого трафіку зменшити загальний рівень втрат на 5%. За допомогою розробленої автором Бешлеєм М.І, програмно-апаратної системи моніторингу (Deep Packet Inspection) системні адміністратори корпоративної мережі ТзОВ ВТФ «Контех» отримали змогу управляти швидкістю передавання окремих пакетів, піднявши її або, навпаки, зменшивши. Deep Packet Inspection дозволила автоматизовано фільтрувати додатки, що забивають Інтернет-канал, змінювати пріоритети передавання різних типів даних, наприклад, прискорюючи відкриття Інтернет сторінок за рахунок зменшення швидкості завантаження великих файлів.

Результати експериментальних досліджень, виконаних на виробничих потужностях ТзОВ ВТФ«Контех», відповідають результатам досліджень, що представлені у дисертаційній роботі, похибка не перевищує 3%.

Керівник відділу
обслуговування мереж Смольницький О.Є.

Науково-дослідний інститут інтелектуальних комп'ютерних систем

Research Institute of Intelligent Computer Systems

West Ukrainian National University
Ministry of Education and Science of Ukraine
Glushkov Institute of Cybernetics
National Academy of Sciences of Ukraine

3 Peremoga Square, Ternopil, 46009, Ukraine
Tel: +380 (352) 475050 ext.12234
Fax: +380 (352) 47-5053 (24 hrs)
http://ics.wunu.edu.ua/ ics@wunu.edu.ua

Західноукраїнський національний університет
Міністерство освіти і науки України
Інститут кібернетики ім. В.М. Глушкова
Національна академія наук України

пл. Перемоги 3, Тернопіль, 46009, Україна
Тел: +380 (352) 475050 внутр.12234
Факс: +380 (352) 47-5053 (24 год)
http://ics.wunu.edu.ua/ ics@wunu.edu.ua

№ _____ «10» 11 2020р.

АКТ
про використання результатів докторської дисертаційної роботи
Бешлея Миколи Івановича
«Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів»

Даний акт складений про те, що у Науково-дослідному інституті інтелектуальних комп'ютерних систем для побудови інтелектуальної інформаційної мережі надання сервісів Інтернету речей використані результати дисертаційної роботи Бешлея М.І. «Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів», представленої на здобуття наукового ступеня доктора технічних наук, а саме:

- прототип енергоефективної інтенційно-орієнтованої мережі побудованої на базі мікроконтролерних платформ Raspberry Pi 3 Model B та віртуалізації функцій компонентів технології SDN (програмно-конфігурованих мереж), впровадження якого дало змогу підвищити гнучкість управління мережею, зменшити енергоспоживання мережі та забезпечити необхідну якість надання критично важливих сервісів Інтернету речей;
- систему моніторингу якості надання IoT сервісів реального часу критично-важливої інфраструктури для розробленого прототипу мережі;
- алгоритм вимірювання затримки передавання даних в програмно-конфігурованих мережах шляхом формування SDN контролером пробних пакетів меншого розміру з різними пріоритетами, що дало можливість у високонавантажених каналах для низько пріоритетних потоків покращити точність моніторингу до 45% та зменшити до 22% сигналізаційне навантаження у порівнянні із відомими.

Акт складений для пред'явлення до спеціалізованої вченої ради із захисту дисертацій і не є підставою для фінансових розрахунків.

Директор
Науково-дослідного інституту
інтелектуальних комп'ютерних систем Кочан В.В.

«Затверджую»
Проректор з наукової роботи
Національного університету
«Львівська політехніка»
_____ д.т.н. І.В. Демидов
«___» _____ 2020 р.

АКТ

про використання результатів докторської дисертаційної роботи Бешлея Миколи Івановича «Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів».

Комісія у складі начальника науково-дослідної частини, к.т.н., Небесного Р.В., заступника начальника планово-фінансового відділу Чулой Т.М., завідувача кафедри телекомунікацій, д.т.н., проф. Климаша М.М., склала цей акт у тому, що у держбюджетних науково-дослідних роботах: «Методи побудови та моделі інформаційно-телекомунікаційної інфраструктури на основі SDN-технологій для систем електронного урядування» (ДБ/SDN), (№ держреєстрації 0115U000444, (2015-2016 рр.) – учасник); «Методи побудови гетерогенних інформаційно-комунікаційних систем для розгортання програмно-конфігурованих мереж 5G подвійного використання» (ДБ/5G), (№ держреєстрації 0117U004449, (2017–2018 рр.) – відповідальний виконавець); «Розроблення методів адаптивного управління радіочастотним ресурсом у мережах мобільного зв'язку LTE-U для розвитку стандартів 4G/5G в Україні» (ДБ/LTE-U), (№ держреєстрації 0117U007177, (2018–2019 рр.) – відповідальний виконавець)); «Розроблення новітньої децентралізованої мережі мобільного зв'язку на основі блокчейн-архітектури та штучного інтелекту для впровадження технологій 5G/6G в Україні» (ДБ/Блокчейн), (№ держреєстрації 0120U100674, (2020-2022 рр.) – відповідальний виконавець); «Розробка методів та уніфікованих програмно-апаратних засобів для розгортання енергоефективних інтенційно-орієнтованих інфокомунікаційних мереж подвійного призначення» (ДБ/IBN), (№ держреєстрації 0120U102201, (2020-2022 рр.) – керівник) використані наступні результати дисертаційної роботи Бешлея Миколи Івановича на тему «Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів»:

- методологія синтезу гетерогенної інтенційно-орієнтованої мережі;
- алгоритми вибору безпровідної мережі доступу в гетерогенному середовищі з використанням Big Data;
- методи розподілу ресурсів, балансування навантаження та формування структури рівня радіодоступу мереж 4G/5G;
- метод адаптивного клієнт-орієнтованого управління якістю надання послуг для IBN мереж та імітаційну модель IBN;
- систему моніторингу та аналізу трафіку для автоматизованого виявлення аномалії і запобігання атак в інфокомунікаційних мережах;
- прототипи програмно-конфігурованої мережі корпоративного сегменту.

Перелічені моделі, методи та алгоритми дають змогу провести синтез інтенційно-орієнтованих мереж для поетапної трансформації сучасних інфокомунікаційних мереж.

Члени комісії:

_____ Небесний Р.В.

_____ Чулой Т.В./

_____ Климащ М.М.

«Затверджую»
Проректор з наукової-педагогічної роботи
Національного університету
«Львівська політехніка»

_____ доц. О.Р. Давидчак
«16» 09 2020 р.

АКТ

про використання результатів докторської дисертаційної роботи Бешлея Миколи Івановича на тему «Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів», у навчальному процесі кафедри телекомунікацій.

Даний акт складений комісією у складі:

- д.т.н., Стрихалюка Б.М., директора Інституту телекомунікацій, радіоелектроніки та електронної техніки;
- д.т.н., доц., Кайдана М.В., декана магістратури Інституту телекомунікацій, радіоелектроніки та електронної техніки;
- д.т.н., проф. Климаша М.М., завідувача кафедри телекомунікацій.

проте, що в навчальному процесі кафедри телекомунікацій використано результати дисертаційної роботи Бешлея М.І. «Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів», а саме:

- розроблено новий розділ лекційного курсу з дисципліни «Проектування інформаційних систем», що стосується розроблення методології проектування програмно-конфігурованих мереж для студентів-бакалаврів спеціальності – 126 «Інформаційні системи та технології»;
- розроблено цикл лекцій та лабораторних робіт з дисципліни «Технології інформаційно-комунікаційних мереж», в якому студенти вивчають методи аналізу та синтезу програмно-конфігурованих мереж для студентів-бакалаврів спеціальності – 126 «Інформаційні системи та технології»;
- розроблено цикл лекцій та лабораторних робіт з дисципліни «Побудова та протоколи гетерогенних мереж мобільного зв'язку», в якому студенти вивчають методологію адаптивного структурно-функціонального синтезу гетерогенної інтенційно-орієнтованої мережі для студентів-магістрів спеціальності – 172 «Телекомунікації та радіотехніка».

Члени комісії:

_____ Стрихалюк Б.М.

_____ Кайдан М.В.

_____ Климаш М.М.

湖北工業大學
HUBEI UNIVERSITY OF TECHNOLOGY

Certificate of Implementation of the Results of the Thesis by Beshley Mykola

This certificate is made about the fact that as a result of joint scientific research in the direction of increasing the security level of the corporate information network in Hubei University of Technology, the results of the dissertation work of Beshley Mykola "Synthesis and implementation of intent-based infocommunication networks for adaptive services provision" were used.

The delegation from Hubei University of Technology used the intellectual DPI (Deep Packet Inspection) system of monitoring and analysis of network traffic developed by Beschle, which differs from the existing analogs DPI approach to intellectual decision-making management process of data transmission, based on a harmonious combination of the advantages of signature, statistical and fractal analysis of information signs to detect information protocols and ranking of the hidden properties of abnormal traffic. It provided a complete overview of the network resources utilization, identified subscribers consuming large volumes of traffic, effectively managed traffic and service policies in real time, automated creation or optimization of service offers, improving service quality and ensuring network and user protection.

The use of intelligent DPI network traffic monitoring and analysis in Hubei University of Technology's campus network has made it possible to detect and block complex attacks of various kinds, such as Non-Spoofed UDP Flood, while increasing the efficiency of bandwidth resources and reducing data loss for legitimate traffic.

Prof. Ye ZhiWei

March 30, 2021

地址：中国湖北省武汉市洪山区南李路28号 电话（传真）：+86-27-5975 0009 / 邮编：430068 / 网址：http://www.hbut.edu.cn/
Add: No.28 Nanli Road,Hongshan District,Wuhan,Hubei,P.R.China Tel (Fax): +86-27-5975 0009 / Zip Code: 430068 / http:www.hbut.edu.cn/

Додаток 2. Програмний код реалізації імітаційних моделей процесу функціонування мережі 4G/5G, LTE/NB-IoT та IBN

Базова Станція

```
public class BaseStation extends Event {
    private static Long idIncrementer = 0L;
    private Long id;
    MobileSystem mobileSystem;
    private List<Message> internalMessages = new ArrayList();
    private Message messageInProcess;
    ResourceArray resourceArray;
    long l1 = 0L;
    long l2 = 0L;
    long l3 = 0L;
    long l4 = 0L;

    public Long getId() {
        return this.id;
    }

    public BaseStation(MobileSystem mobileSystem) {
        Long var2 = idIncrementer;
        idIncrementer = idIncrementer + 1L;
        this.id = var2;
        this.mobileSystem = mobileSystem;
        this.resourceArray = new ResourceArray(mobileSystem, this);
    }

    public void execute(AbstractSimulator simulator) {
        Simulator sim = (Simulator)simulator;
        if (this.messageInProcess != null) {
            if (this.messageInProcess.getTypeMessage() == 1) {
                if (this.messageInProcess.getClassMessage() == 0) {
                    this.redirectDataMessageToBroker(simulator, this.messageInProcess);
                }
            } else if (this.messageInProcess.getTypeMessage() == 0) {
                if (this.messageInProcess.getClassMessage() == 0) {
                    this.requestNewDataConnection(simulator, this.messageInProcess);
                } else {
                    this.sendResponseToIotDevice(simulator, this.messageInProcess);
                }
            }

            if (!this.internalMessages.isEmpty()) {
                this.messageInProcess = (Message)this.internalMessages.remove(0);
                this.setTime(this.messageInProcess.getTime());
                sim.insert(this);
            } else {
                this.messageInProcess = null;
            }
        }


    }

    public void processMessageFromRadioInterface(AbstractSimulator simulator, Message message) {
        double time = 0.0D;
        time += 5.0E-4D;
        time += 2.0E-4D;
        this.processMessage(simulator, message, time);
    }

    public void processMessageFromPacketNetwork(AbstractSimulator simulator, Message message) {
        double time = 0.0D;
        time += 0.001D;
        time += 2.0E-4D;
        this.processMessage(simulator, message, time);
    }

    private void requestNewDataConnection(AbstractSimulator simulator, Message message) {
        this.setTime(message.getTime());
        Logger.log("Bs id=" + this.id + " redirected the request from IoT device id=" +
((ConnectionRequestSignallingMessage)message).getDeviceId() + " to controller at " + this.now());
        this.crc(message);
        this.mobileSystem.getIoTControler().requestNewDataConnection(simulator, message);
    }

    private void sendResponseToIotDevice(AbstractSimulator simulator, Message message) {
        Simulator sim = (Simulator)simulator;
        this.setTime(message.getTime());
        Logger.log("BS id=" + this.id + " redirected response from IoT controller to IoT device id=" +
((ConnectionRequestSignallingMessage)message).getDeviceId() + " at " + sim.now());

this.mobileSystem.getIOTDeviceById(((ConnectionRequestSignallingMessage)message).getDeviceId()).processingResponseMessage(sim
, message);
    }

    private void redirectDataMessageToBroker(AbstractSimulator simulator, Message message) {
        this.setTime(message.getTime());
        Logger.log("Bs id=" + this.id + " redirected the data message from IoT device id=" +
((DataMessage)message).getDeviceId() + " to Broker at " + this.now());
        this.crc(message);
        if (!((DataMessage)message).getUniversalChanel()) {
            switch(message.getDevicePriority()) {
            case 1:
                ++this.l1;
                break;
            case 2:
                ++this.l2;
                break;
            case 3:
```

```
                ++this.l3;
                break;
            case 4:
                ++this.l4;
            }
        }

        this.mobileSystem.getBroker().processMessage(simulator, message);
    }

    private void crc(Message message) {
    }

    public List<Long> getPriorityStatistic() {
        List<Long> list = new ArrayList();
        if (this.l3 > 200L - this.l1 - this.l2 - this.l4) {
            this.l3 = 200L - this.l1 - this.l2 - this.l4;
        }

        list.add(this.l1);
        list.add(this.l2);
        list.add(this.l3);
        list.add(this.l4);
        this.l1 = 0L;
        this.l2 = 0L;
        this.l3 = 0L;
        this.l4 = 0L;
        return list;
    }

    public ResourceArray getResourceArray() {
        return this.resourceArray;
    }

    void addMessage(Message message, Simulator simulator) {
    }
}
```

Брокер

```
public class Broker extends Event {
    int receivedMessagesCount = 0;
    MobileSystem mobileSystem;
    Map<Long, List<Double>> avergeDelaysForDevice = new HashMap();
    Map<Long, List<Double>> avergeDelaysForDeviceOnMethod = new HashMap();
    Map<Long, List<Double>> avergeDelaysForDeviceOnMethodAndBalans = new HashMap();
    int inert = 100;
    int inert1 = 100;
    Map<Message, Double> delayForMessage = new HashMap();

    public Broker() {
    }

    public Map getDelaysForMessage() {
        return this.delayForMessage;
    }

    public Map getAvergeDelaysForDevice() {
        return this.avergeDelaysForDevice;
    }

    public void processMessage(AbstractSimulator simulator, Message message) {
        Simulator sim = (Simulator)simulator;
        ++this.receivedMessagesCount;
        double time = message.getTime1() - message.getTimeRequest();
        if (time >= 0.0D) {
            this.delayForMessage.put(message, time);
            ArrayList list;
            boolean a;
            Iterator var8;
            Entry longListEntry;
            if (ResourceArray.balans && ResourceArray.algorithm) {
                if (this.inert != 0) {
                    --this.inert;
                    return;
                }

            Logger.log("[Broker] Packet delay is:" + String.valueOf(time));
        }
    }
}
```

IoT Контролер

```
public class IoTControler extends Event {
    MobileSystem mobileSystem;
    Message messageInProcess;
    private List<Message> paketIncomingBuffer = new ArrayList();

    IoTControler(MobileSystem mobileSystem) {
        this.mobileSystem = mobileSystem;
    }

    public void execute(AbstractSimulator simulator) {
        Simulator sim = (Simulator)simulator;
        if (this.messageInProcess != null && this.messageInProcess.getTypeMessage() == 0 &&
this.messageInProcess.getClassMessage() == 0) {
            this.newIotConnection(simulator, this.messageInProcess);
            if (!this.paketIncomingBuffer.isEmpty()) {
                this.messageInProcess = (Message)this.paketIncomingBuffer.remove(0);
                this.setTime(this.messageInProcess.getTime());
                sim.insert(this);
            } else {
                this.messageInProcess = null;
```

```
            }
        }

    }

    public void requestNewDataConnection(AbstractSimulator simulator, Message message) {
        Simulator sim = (Simulator)simulator;
        double delay = 0.0012000000000000001D;
        message.setTime(sim.now() + delay);
        if (this.messageInProcess == null) {
            this.messageInProcess = message;
            this.setTime(sim.now() + delay);
            simulator.insert(this);
        } else {
            this.paketIncomingBuffer.add(message);
        }

    }

    private void newIotConnection(AbstractSimulator simulator, Message message) {
        this.setTime(message.getTime());
        Logger.log("IoT controler received the request from IoT device id=" +
((ConnectionRequestSignallingMessage)message).getDeviceId() + " at " + this.now());
        ConnectionRequestSignallingMessage message1 = (ConnectionRequestSignallingMessage)message;
        this.mobileSystem.getBaseStationById(message1.getBaseStationId()).resourceArray.AddNewDev(simulator, message1);
        this.responseToIotDevice(message1, (Simulator)simulator);
    }

    public void responseToIotDevice(Message message, Simulator simulator) {
        Logger.log("IoT controler selected " + ((ConnectionRequestSignallingMessage)message).getCountResourseBlocks() + " RB
from " + ((ConnectionRequestSignallingMessage)message).getNumberResourseBlock() + " in BS " +
((ConnectionRequestSignallingMessage)message).getDestinationBaseStationId() + " and responded IoT dev id=" +
((ConnectionRequestSignallingMessage)message).getDeviceId() + " at " + this.now());
        message.setClassMessage((byte)1);
        message.calculateCRC();

this.mobileSystem.getBaseStationById(((ConnectionRequestSignallingMessage)message).getBaseStationId()).processMessageFromPack
etNetwork(simulator, message);
    }
}
```

IoT Пристрій

```
public class IOTDevice extends Event {
    private boolean send = false;
    private static Long idIncrementer = 0L;
    private Long id;
    private Long countLoss = 0L;
    MobileSystem mobileSystem;
    private DataMessage message;
    private int priority;
    private byte modulation = 10;
    private double time1 = 0.0045D;
    private double timeRequest = 0.0D;
    private int generatedTraffic = 0;
    private final Long DEFAULT_BASE_STATION_ID = 0L;
    private Long selectedBSId;

    public IOTDevice(MobileSystem mobileSystem, int Priority, byte modulation) {
        this.selectedBSId = this.DEFAULT_BASE_STATION_ID;
        Long var4;
        if (Priority != 3 && Priority != 4) {
            var4 = idIncrementer;
            idIncrementer = idIncrementer + 1L;
            this.id = var4;
        } else {
            var4 = idIncrementer;
            idIncrementer = idIncrementer + 1L;
            this.id = var4;
            this.id = this.id + 1000L;
        }

        var4 = idIncrementer;
        idIncrementer = idIncrementer + 1L;
        this.id = var4;
        this.mobileSystem = mobileSystem;
        this.priority = Priority;
        this.modulation = modulation;
    }

    public Long getId() {
        return this.id;
    }

    public int getPriority() {
        return this.priority;
    }

    private void requestConnection(AbstractSimulator simulator) {
        Logger.log("IoT device id=" + this.id + " send request data transmission to BS at " + this.now());
        Message connectionRequestSignallingMessage = new ConnectionRequestSignallingMessage(this.id, this.priority,
this.message.getLength(), this.DEFAULT_BASE_STATION_ID);
        connectionRequestSignallingMessage.setTimeRequest(this.now());
        this.calculateModulation();
        connectionRequestSignallingMessage.setModulation(this.modulation);
        connectionRequestSignallingMessage.calculateCRC();
        connectionRequestSignallingMessage.setTime(this.now());
        this.mobileSystem.getBaseStationById(this.DEFAULT_BASE_STATION_ID).processMessageFromRadioInterface(simulator,
connectionRequestSignallingMessage);
    }

    public void processingResponseMessage(AbstractSimulator simulator, Message message) {
        Simulator sim = (Simulator)simulator;
        double delay = 7.0E-4D;
        this.setTime(sim.now() + delay);
```

```
        this.setTime(delay + message.getTime());
        if (((ConnectionRequestSignallingMessage)message).getRefusal()) {
            Long var6 = this.countLoss;
            Long var7 = this.countLoss = this.countLoss + 1L;
            Logger.log("IoT device id=" + this.id + " reseived refual from IoT controler at " + this.now());
            double nextEventTime = this.now() + (double)(new Random()).nextInt(10);
            this.message = null;
            this.setTime(nextEventTime);
            simulator.insert(this);
        } else {
            if (((ConnectionRequestSignallingMessage)message).getUniversalChanel()) {
                this.message.setUniversalChanel();
            }

            Logger.log("IoT device id=" + this.id + " reseived response from IoT controler at " + this.now());
            this.crc(message);
            ConnectionRequestSignallingMessage response = (ConnectionRequestSignallingMessage)message;
            this.setTime(this.now() + 5.0E-4D * (double)response.getNumberResourseBlock());

            try {
                this.message.setTime1(this.time1 + this.message.getTimeRequest() + 5.0E-4D *
(double)response.getNumberResourseBlock());
            } catch (Exception var8) {
                return;
            }

            this.selectedBSId = response.getDestinationBaseStationId();
            if (!((ConnectionRequestSignallingMessage)message).getReorganisation()) {
                simulator.insert(this);
            } else {
                simulator.reloadEvent(this);
            }
    }

    private void sendDataMessage(AbstractSimulator simulator, Message message) {
        this.message.setTime(this.now());
        Logger.log("IoT device id=" + this.id + " send data message at " + this.now());
        this.mobileSystem.getBaseStationById(this.selectedBSId).processMessageFromRadioInterface(simulator, this.message);

    public void startSend() {
        this.send = true;
    }

    public void stopSend() {
        this.send = false;
    }
}
```

Мобільна система 4G/5G

```
public class MobileSystem implements MonitoringCapability {
    IoTControler ioTControler;
    Broker broker;
    private Map<Long, IOTDevice> iotDevices = new HashMap();
    private Map<Long, BaseStation> baseStations = new HashMap();
    private Simulator simulator;
    private MobileSystemArea mobileSystemArea;
    static final int MAX_DEVICE_FIRST_MESSAGE_DELAY = 10;

    public MobileSystemArea getMobileSystemArea() {
        return this.mobileSystemArea;
    }

    public Map getIotDevices() {
        return this.iotDevices;
    }

    public MobileSystem(MobileSystemArea mobileSystemArea) {
        this.mobileSystemArea = mobileSystemArea;
        this.createIOTDevices(20);
        this.createRadioAccessNetwork();
        this.ioTControler = new IoTControler(this);
        this.broker = new Broker();
    }

    public void start(Simulator simulator) {
        Iterator var2 = this.iotDevices.values().iterator();

        while(var2.hasNext()) {
            IOTDevice device = (IOTDevice)var2.next();
            simulator.insert(device);
        }

        var2 = this.baseStations.values().iterator();

        while(var2.hasNext()) {
            BaseStation baseStation1 = (BaseStation)var2.next();
            baseStation1.resourceArray.setTime(5.0E-4D);
            baseStation1.getResourceArray().setSimulator(simulator);
            simulator.insert(baseStation1.resourceArray);
        }

        simulator.doAllEvents();
    }

    private void createIOTDevices(int devicesNumber) {
        for(int i = 0; i < devicesNumber; ++i) {
            IOTDevice device;
            int j;
            for(j = 0; j < 10; ++j) {
                device = new IOTDevice(this, 1, (byte)42);
                device.setTime((double)(new Random()).nextInt(2000) * 0.0025D);
                this.iotDevices.put(device.getId(), device);
            }
```

```
            for(j = 0; j < 20; ++j) {
                device = new IOTDevice(this, 2, (byte)42);
                device.setTime((double)(new Random()).nextInt(2000) * 0.0025D);
                this.iotDevices.put(device.getId(), device);
            }

            for(j = 0; j < 30; ++j) {
                device = new IOTDevice(this, 3, (byte)42);
                device.setTime((double)(new Random()).nextInt(2000) * 0.0025D);
                this.iotDevices.put(device.getId(), device);
            }

            for(j = 0; j < 40; ++j) {
                device = new IOTDevice(this, 4, (byte)42);
                device.setTime((double)(new Random()).nextInt(2000) * 0.0025D);
                this.iotDevices.put(device.getId(), device);
            }
        }

    }

    private void createRadioAccessNetwork() {
        BaseStation baseStation = new BaseStation(this);
        baseStation.getResourceArray().setSimulator(this.simulator);
        this.baseStations.put(baseStation.getId(), baseStation);
        baseStation = new BaseStation(this);
        baseStation.getResourceArray().setSimulator(this.simulator);
        this.baseStations.put(baseStation.getId(), baseStation);
    }

    public double getTotalGeneratedLoad() {
        double totalGeneratedLoad = 0.0D;

        IOTDevice device;
        for(Iterator var3 = this.iotDevices.values().iterator(); var3.hasNext(); totalGeneratedLoad +=
(double)device.getGeneratedTraffic()) {
            device = (IOTDevice)var3.next();
        }

        return totalGeneratedLoad + (double)(new Random()).nextInt(100);
    }

    public Map getDelaysToMessage() {
        double totalGeneratedLoad = 0.0D;
        return this.broker.getDelaysForMessage();
    }

    public Map getAvergeDelaysForDevice() {
        if (ResourceArray.algorithm && ResourceArray.balans) {
            return this.broker.avergeDelaysForDeviceOnMethodAndBalans;
        } else {
            return ResourceArray.algorithm && !ResourceArray.balans ? this.broker.avergeDelaysForDeviceOnMethod :
this.broker.avergeDelaysForDevice;
        }
    }

    public Map getCountLoss() {
        Map<Integer, Long> map = new HashMap();
        Long lossL1 = 0L;
        Long lossL2 = 0L;
        Long lossL3 = 0L;
        Long lossL4 = 0L;
        Iterator var6 = this.iotDevices.entrySet().iterator();

        while(var6.hasNext()) {
            Entry<Long, IOTDevice> deviceEntry = (Entry)var6.next();
            switch(((IOTDevice)deviceEntry.getValue()).getPriority()) {
            case 1:
                lossL1 = lossL1 + ((IOTDevice)deviceEntry.getValue()).getCountLoss();
                break;
            case 2:
                lossL2 = lossL2 + ((IOTDevice)deviceEntry.getValue()).getCountLoss();
                break;
            case 3:
                lossL3 = lossL3 + ((IOTDevice)deviceEntry.getValue()).getCountLoss();
                break;
            case 4:
                lossL4 = lossL4 + ((IOTDevice)deviceEntry.getValue()).getCountLoss();
            }
        }

        map.put(1, lossL1);
        map.put(2, lossL2);
        map.put(3, lossL3);
        map.put(4, lossL4);
        return map;
    }

    public Map getLoadFromBaseStation() {
        Map<Long, Long> map = new HashMap();
        Iterator var2 = this.baseStations.entrySet().iterator();

        while(var2.hasNext()) {
            Entry<Long, BaseStation> baseStationEntry = (Entry)var2.next();
            map.put(baseStationEntry.getKey(),
((BaseStation)baseStationEntry.getValue()).resourceArray.getNumberOfResoursBlockUsed());
        }

        return map;
    }

    public List getPriorityStatistic() {
        return this.getBaseStationById(0L).getPriorityStatistic();
    }

    public IOTDevice getIOTDeviceById(Long id) {
```

```
        return (IOTDevice)this.iotDevices.get(id);
    }

    public BaseStation getBaseStationById(Long id) {
        return (BaseStation)this.baseStations.get(id);
    }

    public int getSizeMapBaseStation() {
        return this.baseStations.size();
    }

    public IoTControler getIoTControler() {
        return this.ioTControler;
    }

    public Broker getBroker() {
        return this.broker;
    }

    public long setNumberSendDevice(int i) {
        double j = (double)this.iotDevices.size();
        j /= 100.0D;
        j *= (double)i;

        for(Iterator var6 = this.iotDevices.entrySet().iterator(); var6.hasNext(); --j) {
            Entry<Long, IOTDevice> longIOTDeviceEntry = (Entry)var6.next();
            if (j > 0.0D) {
                ((IOTDevice)longIOTDeviceEntry.getValue()).startSend();
            } else {
                ((IOTDevice)longIOTDeviceEntry.getValue()).stopSend();
            }
        }

        return (long)j;
    }

    public void setSimulator(Simulator simulator) {
        this.simulator = simulator;
    }
}
```

Масив ресурсів

```
public class ResourceArray extends Event {
    private int tL1 = 4;
    private int tL2 = 14;
    private int tAllovable = 30;
    private Long numberOfResoursBlockUsed = 0L;
    public static boolean algorithm = false;
    public static boolean balans = false;
    private List<Long> resourseBlockPriorityList = new ArrayList();
    private List<Double> resourseBlockTimingList = new ArrayList();
    private List<Long> resourseBlockIdList = new ArrayList();
    private double delayFromControlerToDevice = 0.001900000000000002D;
    private double lastTimeInRa;
    private MobileSystem mobileSystem;
    private BaseStation baseStation;
    private Simulator simulator;
    Long numberResourseBlock;
    int countResourseBlocks;

    ResourceArray(MobileSystem mobileSystem, BaseStation baseStation) {
        this.lastTimeInRa = this.delayFromControlerToDevice * 2.0D;
        this.mobileSystem = null;
        this.baseStation = null;
        this.numberResourseBlock = 1L;
        this.countResourseBlocks = 1;
        this.mobileSystem = mobileSystem;
        this.baseStation = baseStation;
    }

    public void setSimulator(Simulator simulator) {
        this.simulator = simulator;
    }

    public void AddNewDev(AbstractSimulator simulator, ConnectionRequestSignallingMessage message) {
        this.simulator = (Simulator)simulator;
        if (!algorithm) {
            if ((double)this.resourseBlockTimingList.size() <= this.delayFromControlerToDevice / 5.0E-4D + 1.0D +
(double)this.tAllovable / 0.5D) {
                this.priority1(message);
            } else {
                message.setRefusal();
            }
        } else {
            switch(message.getDevicePriority()) {
            case 1:
                if ((double)this.resourseBlockTimingList.size() <= this.delayFromControlerToDevice / 5.0E-4D + 1.0D +
(double)this.tL1 / 0.5D) {
                    this.priority1(message);
                } else if (!this.optimisationResourse(message, 1)) {
                    if (balans) {
                        if (!this.otherBs(message)) {
                            this.universalChanet(message);
                        }
                    } else if ((double)this.resourseBlockTimingList.size() > this.delayFromControlerToDevice / 5.0E-4D + 1.0D
+ (double)this.tAllovable / 0.5D) {
                        message.setRefusal();
                    } else {
                        this.priority1(message);
                    }
                }
                break;
            case 2:
                if ((double)this.resourseBlockTimingList.size() <= this.delayFromControlerToDevice / 5.0E-4D + 1.0D +
```

```
(double)this.tL2 / 0.5D) {
                    this.priority1(message);
                } else if (!this.optimisationResourse(message, 2)) {
                    if (balans) {
                        if (!this.otherBs(message)) {
                            if ((double)this.resourseBlockTimingList.size() > this.delayFromControlerToDevice / 5.0E-4D +
1.0D + (double)this.tAllovable / 0.5D) {
                                message.setRefusal();
                            } else {
                                this.priority1(message);
                            }
                        }
                    } else if ((double)this.resourseBlockTimingList.size() > this.delayFromControlerToDevice / 5.0E-4D + 1.0D
+ (double)this.tAllovable / 0.5D) {
                        message.setRefusal();
                    } else {
                        this.priority1(message);
                    }
                }
                break;
            case 3:
                if ((double)this.resourseBlockTimingList.size() > this.delayFromControlerToDevice / 5.0E-4D + 1.0D +
(double)this.tAllovable / 0.5D) {
                    message.setRefusal();
                } else {
                    this.priority1(message);
                }
                break;
            case 4:
                if ((double)this.resourseBlockTimingList.size() <= this.delayFromControlerToDevice / 5.0E-4D + 1.0D +
(double)this.tL1 / 0.5D) {
                    this.priority1(message);
                } else {
                    message.setRefusal();
                }
            }
        }

    }        for(i = firstRB; i <= endRB; ++i) {
            if ((Long)this.resourseBlockPriorityList.get(i) == 3L) {
                if (counter == 0) {
                    firstRB = i;
                }

                ++counter;
                if (counter == message.getCountResourseBlocks()) {
                    endRB = i;
                    break;
                }
            } else {
                counter = 0;
            }
        }

        if (counter < message.getCountResourseBlocks()) {
            return false;
        } else {
            id = (Long)this.resourseBlockIdList.get(endRB);

            for(i = endRB + 1; i <= endRBDefault; ++i) {
                if (id != this.resourseBlockIdList.get(i)) {
                    endRB = i - 1;
                    break;

    public void execute(AbstractSimulator simulator) {
        super.execute(simulator);
        Simulator sim = (Simulator)simulator;
        if (!this.resourseBlockIdList.isEmpty()) {
            long id = (Long)this.resourseBlockIdList.get(0);
            if (this.resourseBlockIdList.size() == 1 || this.resourseBlockIdList.size() > 1 && id !=
(Long)this.resourseBlockIdList.get(1)) {
                RemoveProcessedElementTrigger a = new RemoveProcessedElementTrigger(this.mobileSystem.getMobileSystemArea());
                a.setBaseStation(this.baseStation);
                a.scheduleAnimation(simulator, (Event)null);
            }

            Long var7 = this.numberOfResoursBlockUsed;
            Long var6 = this.numberOfResoursBlockUsed = this.numberOfResoursBlockUsed + 1L;
            this.resourseBlockIdList.remove(0);
            this.resourseBlockTimingList.remove(0);
            this.resourseBlockPriorityList.remove(0);
        }

        this.setTime(sim.now() + 5.0E-4D);
        sim.insert(this);
    }

    public long getNumberOfResoursBlockUsed() {
        long c = this.numberOfResoursBlockUsed;
        this.numberOfResoursBlockUsed = 0L;
        if (c > 2000L) {
            c = 2000L;
        }

        return c;
    }
}
```

IBN QoE intents

Клієнт

```
public class Client extends NetworkPoint {
    private static int clientsId = 1;
    private String ip;
    private String routersHostName;
    private NetworkInterface interfaceToSwitch;
    private SessionExecutor sessionExecutor;
    private SessionResulted sessionsResult = new SessionResulted();

    String getIp() {
        return this.ip;
    }

    NetworkInterface getInterfaceToSwitch() {
        return this.interfaceToSwitch;
    }

    Client(String ip, NetworkInterface switchInterface, String routersHostName) {
        String CLIENT = "Client ";
        super.setHostName(CLIENT + clientsId++);
        this.routersHostName = routersHostName;
        this.ip = ip;
        this.interfaceToSwitch = new NetworkInterfaceImpl(this.getMAC());
        this.interfaceToSwitch.setNeighbors(switchInterface);
        this.addSession();
    }

    private void addSession() {
        this.sessionExecutor = new SessionExecutor(this.getIp(), this.getMAC(),
this.interfaceToSwitch.getNeighbors().getInterfaceMAC(), this.routersHostName);
    }

    public void cycle() {
        this.sessionsResult.saveResult(this.interfaceToSwitch.getPacketsFromNetwork());
        this.interfaceToSwitch.setPacketsToSend(this.sessionExecutor.nextIterations());
    }

    public void sendingPackets() {
        this.interfaceToSwitch.packetsSending();
    }

    List<SessionInfo> getActiveSessionsResult() {
        return this.sessionsResult.getResults();
    }
}
```

Контролер IBN мережі

```
public class NetworkController {
    private Map<String, RoutingMapEntry> networkRoutingMap = new HashMap();
    private List<Router> newRouters = new ArrayList();
    private List<Router> oldRouters = new ArrayList();
    private static Map<String, NetworkController.ControllerRow> networkMap = new HashMap();

    public NetworkController() {
    }

    public void updateTable() {
        this.addLocalNetwork(this.newRouters);
        this.addLocalNetwork(this.oldRouters);
        List<Map<String, RoutingMapEntry>> tableFromROuter = new ArrayList();
        Iterator var2 = this.newRouters.iterator();

        Router router;
        while(var2.hasNext()) {
            router = (Router)var2.next();
            tableFromROuter.add(router.getRoutingTable());
        }

        this.buildNetwork();
        var2 = this.newRouters.iterator();

        while(var2.hasNext()) {
            router = (Router)var2.next();
            router.updateRoutingTable(this.networkRoutingMap);
        }

    }

    public static int getBilling(Session session) {
        if (networkMap.get(IpCalculator.getNetworkAddress(session.getDestinationIP())) == null) {
            return 0;
        } else {
            getPaths(IpCalculator.getNetworkAddress(session.getSourceIP()),
IpCalculator.getNetworkAddress(session.getDestinationIP()));
```

```
            return 100;
        }
    }

    private static List<String> getPaths(String sNetwork, String dNetwork) {
        return null;
    }

    private void addLocalNetwork(List<Router> routers) {
        Iterator var2 = routers.iterator();

        while(var2.hasNext()) {
            Router router = (Router)var2.next();
            Map<String, NetworkInterface> routerLocalNetworks = router.getLocalNetwoks();
            Iterator var5 = routerLocalNetworks.entrySet().iterator();

            while(var5.hasNext()) {
                Entry<String, NetworkInterface> entry = (Entry)var5.next();
                if (networkMap.get(entry.getKey()) == null) {
                    networkMap.put(entry.getKey(), new NetworkController.ControllerRow(router,
(NetworkInterface)entry.getValue()));
                }
            }
        }

    }

    private void buildNetwork() {
    }

    public void addNewRouter(Router router) {
        this.newRouters.add(router);
    }

    public void addOldRouter(Router router) {
        this.oldRouters.add(router);
    }

    public List<Router> getOldRouters() {
        return this.oldRouters;
    }

    public void cycle() {
        Iterator var1 = this.newRouters.iterator();

        while(var1.hasNext()) {
            Router router = (Router)var1.next();
            router.cycle();
        }

    }

    public void sendingPackets() {
        Iterator var1 = this.newRouters.iterator();

        while(var1.hasNext()) {
            Router router = (Router)var1.next();
            router.sendingPackets();
        }

    }

    class ControllerRow {
        private NetworkInterface inter;
        private Router router;

        ControllerRow(Router router, NetworkInterface inter) {
            this.router = router;
            this.inter = inter;
        }

        public ControllerRow() {
        }

        public NetworkInterface getInter() {
            return this.inter;
        }

        public void setInter(NetworkInterface inter) {
            this.inter = inter;
        }

        public Router getRouter() {
            return this.router;
        }

        public void setRouter(Router router) {
            this.router = router;
        }

        public String toString() {
            return "ControllerRow{inter=" + this.inter + ", router=" + this.router.getHostName() + '}';
        }
```

```
    }
}
```

Маршрутизатор

```
public class Router extends NetworkPoint {
    private boolean newVersion = false;
    private static int routerID = 1;
    private static String ROUTER = "Router ";
    private int bandwidth;
    private Map<String, RoutingMapEntry> routingTable = new HashMap();
    private List<NetworkInterface> globalInterfaces = new ArrayList();
    private List<NetworkInterface> localInterfaces = new ArrayList();
    private Deque<IpPull> ipPullForSwitches;
    private List<Switch> switchList = new ArrayList();
    private NetworkInterface defaultInterface = new NetworkInterfaceImpl();
    private Map<String, NetworkInterface> localNetwoks = new HashMap();
    private static newVersionComparator newVersionComparator = new newVersionComparator();
    private static oldVersionComparator oldVersionComparator = new oldVersionComparator();
    public static Comparator<Packet> comparator;
    private static boolean executionVersion;
    private Map<String, Double> globalInterfaceLoad;
    private Map<String, Double> localInterfaceLoad;
    private ServicesSessionInfo servicesSessionInfo = new ServicesSessionInfo();

    public Router(Deque<IpPull> ipPullForSwitches) {
        super.setHostName(ROUTER + routerID++);
        this.ipPullForSwitches = ipPullForSwitches;
    }

    public void setBandwidthForGlobalInterfaces(int bandwidth) {
        this.bandwidth = bandwidth;
    }

    public NetworkInterface getGlobalInterface() {
        NetworkInterface networkInterface = new NetworkInterfaceImpl();
        networkInterface.setBandwidth(this.bandwidth);
        this.globalInterfaces.add(networkInterface);
        return networkInterface;
    }

    public Map<String, RoutingMapEntry> getRoutingTable() {
        return this.routingTable;
    }

    void updateRoutingTable(Map<String, RoutingMapEntry> routingTable) {
        this.routingTable = routingTable;
    }

    public void updateTable() {
        if (!this.newVersion) {
            this.sendOwnTableToNeighbors();
            this.getTableFromNetwork();
        }

    }

    private void sendOwnTableToNeighbors() {
        Map<String, RoutingMapEntry> tempTable = new HashMap();
        Iterator var2 = this.routingTable.entrySet().iterator();

        while(var2.hasNext()) {
            Entry<String, RoutingMapEntry> entrySet = (Entry)var2.next();
            RoutingMapEntry old = (RoutingMapEntry)entrySet.getValue();
            tempTable.put(entrySet.getKey(), this.addToMetric(old));
        }

        var2 = this.globalInterfaces.iterator();

        while(var2.hasNext()) {
            NetworkInterface networkInterface = (NetworkInterface)var2.next();
            networkInterface.routingTableSending(tempTable);
        }

    }

    private RoutingMapEntry addToMetric(RoutingMapEntry entry) {
        return new RoutingMapEntry(entry.getNetwork(), entry.getMetric() + 1, entry.getUsedRoutersInterface());
    }

    private void getTableFromNetwork() {
        Iterator var1 = this.globalInterfaces.iterator();

        while(var1.hasNext()) {
            NetworkInterface networkInterface = (NetworkInterface)var1.next();
            Map<String, RoutingMapEntry> tempTable = networkInterface.getRoutingMapEntriesFromNetwork();
            Iterator var4 = tempTable.entrySet().iterator();

            while(var4.hasNext()) {
                Entry<String, RoutingMapEntry> entrySet = (Entry)var4.next();
                String ip = (String)entrySet.getKey();
                RoutingMapEntry routingMapEntry = (RoutingMapEntry)entrySet.getValue();
                routingMapEntry.setUsedRoutersInterface(networkInterface);
                if (!this.routingTable.containsKey(ip)) {
```

```
                this.routingTable.put(ip, routingMapEntry);
            } else {
                this.routingTable.put(ip, this.getBetter((RoutingMapEntry)this.routingTable.get(ip), routingMapEntry));
            }
        }
    }

}

private RoutingMapEntry getBetter(RoutingMapEntry own, RoutingMapEntry other) {
    return own.getMetric() <= other.getMetric() ? own : other;
}

public Map<String, NetworkInterface> getLocalNetwoks() {
    return this.localNetwoks;
}

public static void changeVersion(boolean newVersion) {
    if (executionVersion != newVersion) {
        executionVersion = newVersion;
        comparator = (Comparator)(newVersion ? newVersionComparator : oldVersionComparator);
    }
}

public static boolean isNewVersion() {
    return executionVersion;
}

public void cycle() {
    this.executePackets(this.getPacketsForRouter());
}

private ArrayList<Packet> getPacketsForRouter() {
    ArrayList<Packet> packetsForExecuting = new ArrayList();
    Iterator var2 = this.globalInterfaces.iterator();

    NetworkInterface lInterface;
    while(var2.hasNext()) {
        lInterface = (NetworkInterface)var2.next();
        packetsForExecuting.addAll(lInterface.getPacketsFromNetwork());
    }

    var2 = this.localInterfaces.iterator();

    while(var2.hasNext()) {
        lInterface = (NetworkInterface)var2.next();
        packetsForExecuting.addAll(lInterface.getPacketsFromNetwork());
    }

    return packetsForExecuting;
}

private void executePackets(ArrayList<Packet> packets) {
    if (packets.size() != 0) {
        packets.sort(comparator);
        String network = "";
        NetworkInterface inter = this.defaultInterface;
        Iterator var4 = packets.iterator();

        while(var4.hasNext()) {
            Packet packet = (Packet)var4.next();
            if (packet.getDelay() > 0.0D) {
                if (!packet.getDestinationNetwork().equals(network)) {
                    network = packet.getDestinationNetwork();
                    RoutingMapEntry ent = (RoutingMapEntry)this.routingTable.get(packet.getDestinationNetwork());
                    if (ent != null) {
                        inter = ent.getUsedRoutersInterface();
                    }
                }

                inter.setPacketsToSend(packet);
            }
        }

    }
}

public void sendingPackets() {
    this.globalInterfaceLoad = new HashMap();
    this.localInterfaceLoad = new HashMap();
    Iterator var1 = this.globalInterfaces.iterator();

    NetworkInterface lInterface;
    while(var1.hasNext()) {
        lInterface = (NetworkInterface)var1.next();
        this.globalInterfaceLoad.put(lInterface.getInterfaceMAC(), lInterface.getLoadInfo());
        this.servicesSessionInfo.addValues(lInterface.packetsSending());
    }

    var1 = this.localInterfaces.iterator();

    while(var1.hasNext()) {
        lInterface = (NetworkInterface)var1.next();
        this.localInterfaceLoad.put(lInterface.getInterfaceMAC(), lInterface.getLoadInfo());
```

```
            this.servicesSessionInfo.addValues(lInterface.packetsSending());
        }

    }

    public SessionResultInfo getRoutersTime() {
        this.servicesSessionInfo.averageValues();
        return this.servicesSessionInfo.getInfo();
    }

    public void addSwitch(int switchValues, int clientsValues, int bandwidth) {
        for(int i = 0; i < switchValues; ++i) {
            if (this.ipPullForSwitches.size() == 0) {
                System.out.println("There aren't enough free network");
                return;
            }

            NetworkInterface interfaceToSwitch = new NetworkInterfaceImpl();
            interfaceToSwitch.setBandwidth(bandwidth);
            IpPull ipPull = (IpPull)this.ipPullForSwitches.pollFirst();
            this.localInterfaces.add(interfaceToSwitch);
            Switch swiitch = new Switch(interfaceToSwitch, ipPull);
            swiitch.getInterfaceToRouter().setBandwidth(bandwidth);
            interfaceToSwitch.setNeighbors(swiitch.getInterfaceToRouter());
            swiitch.addClients(clientsValues, this.getHostName());
            this.switchList.add(swiitch);
            String network = ipPull.getNetworkAddress();
            this.routingTable.put(network, new RoutingMapEntry(network, 0, interfaceToSwitch));
            this.localNetwoks.put(network, interfaceToSwitch);
        }

    }

    public List<Switch> getSwitchList() {
        return this.switchList;
    }

    public List<SessionInfo> getResultInfo() {
        List<SessionInfo> allSwitches = new ArrayList();
        Iterator var2 = this.switchList.iterator();

        while(var2.hasNext()) {
            Switch switcH = (Switch)var2.next();
            allSwitches.addAll(switcH.getInfo());
        }

        return allSwitches;
    }

    public Map<String, Map<String, Double>> getMiddleInterfacesLoad() {
        Map<String, Map<String, Double>> interfaceLoad = new HashMap();
        interfaceLoad.put("Global", this.globalInterfaceLoad);
        interfaceLoad.put("Local", this.localInterfaceLoad);
        return interfaceLoad;
    }

    static {
        comparator = oldVersionComparator;
        executionVersion = false;
    }
}
```

Комутатор

```
public class Switch extends NetworkPoint {
    private static int switchId = 1;
    private static final String SWITCH = "Switch ";
    private List<Client> clients = new ArrayList();
    private Map<String, NetworkInterface> arpTable = new HashMap();
    private IpPull ipPull;
    private NetworkInterface interfaceToRouter;
    private NetworkInterface interfaceToClients;

    public Switch(NetworkInterface routerInterface, IpPull ipPull) {
        super.setHostName("Switch " + switchId++);
        this.ipPull = ipPull;
        this.interfaceToClients = new NetworkInterfaceImpl(this.getMAC());
        this.interfaceToRouter = new NetworkInterfaceImpl(this.getMAC());
        this.interfaceToRouter.setNeighbors(routerInterface);
    }

    NetworkInterface getInterfaceToRouter() {
        return this.interfaceToRouter;
    }

    public void cycle() {
        ArrayList<Packet> tempPacketsList = this.interfaceToClients.getPacketsFromNetwork();
        this.executePackets(this.interfaceToRouter.getPacketsFromNetwork());
        tempPacketsList.sort(Router.comparator);
        this.executePackets(tempPacketsList);
    }

    private void executePackets(ArrayList<Packet> packets) {
        Iterator var2 = packets.iterator();
```

```
        while(var2.hasNext()) {
            Packet packet = (Packet)var2.next();
            NetworkInterface tempInterface = (NetworkInterface)this.arpTable.get(packet.getDestinationIP());
            if (tempInterface != null) {
                tempInterface.setPacketsFromNetwork(packet);
            } else {
                this.interfaceToRouter.setPacketsToSend(packet);
            }
        }

    }

    public void sendingPackets() {
        this.interfaceToRouter.packetsSending();
    }

    void addClients(int clientsValues, String routersHostName) {
        for(int i = 0; i < clientsValues; ++i) {
            String ip = this.ipPull.getIpAddress();
            if (ip.isEmpty()) {
                return;
            }

            Client client = new Client(ip, this.interfaceToClients, routersHostName);
            this.clients.add(client);
            this.arpTable.put(ip, client.getInterfaceToSwitch());
            IpCollector.addClientIpAddress(ip, routersHostName);
        }

    }

    void deleteSwitch() {
        Iterator var1 = this.clients.iterator();

        while(var1.hasNext()) {
            Client client = (Client)var1.next();
            this.deleteClient(client);
        }

    }

    public void deleteClient(Client client) {
        this.clients.remove(client);
        this.arpTable.remove(client.getIp());
        this.ipPull.returnIpAddress(client.getIp());
        MacGenerator.removeMac(client.getMAC());
        IpCollector.removeClientIp(client.getIp());
    }

    public List<Client> getClients() {
        return this.clients;
    }

    public List<SessionInfo> getInfo() {
        List<SessionInfo> allClient = new ArrayList();
        Iterator var2 = this.clients.iterator();

        while(var2.hasNext()) {
            Client client = (Client)var2.next();
            allClient.addAll(client.getActiveSessionsResult());
        }

        return allClient;
    }
}
```

Типи сервісів

```
public abstract class Service implements IService {
    public static final int SERVICES_VALUES = 7;
    public static final int SIGNALING_ID = 1;
    public static final int VOIP_ID = 2;
    public static final int VIDEOCONFERENCING_ID = 3;
    public static final int IPTV_ID = 4;
    public static final int VIDEO_ON_DEMAND_ID = 5;
    public static final int DATA_ID = 6;
    public static final int INTERACTIVE_DATA_ID = 7;
    protected static int DATA_generatedPackets = 99;
    protected static int INTERACTIVE_DATA_generatedPackets = 50;
    protected static int IPTV_generatedPackets = 80;
    protected static int SIGNALING_generatedPackets = 40;
    protected static int VIDEOCONFERENCING_generatedPackets = 50;
    protected static int VIDEO_ON_DEMAND_generatedPackets = 80;
    protected static int VOIP_generatedPackets = 60;
    protected static int DATA_maxUsedTime = 33;
    protected static int INTERACTIVE_DATA_maxUsedTime = 35;
    protected static int IPTV_maxUsedTime = 33;
    protected static int SIGNALING_maxUsedTime = 22;
    protected static int VIDEOCONFERENCING_maxUsedTime = 36;
    protected static int VIDEO_ON_DEMAND_maxUsedTime = 22;
    protected static int VOIP_maxUsedTime = 33;
    protected static int DATA_transport = 1;
    protected static int INTERACTIVE_DATA_transport = 1;
```

```
    protected static int IPTV_transport = 0;
    protected static int SIGNALING_transport = 0;
    protected static int VIDEOCONFERENCING_transport = 0;
    protected static int VIDEO_ON_DEMAND_transport = 1;
    protected static int VOIP_transport = 0;
    protected static int DATA_maxDelayPacket = 10;
    protected static int INTERACTIVE_DATA_maxDelayPacket = 10;
    protected static int IPTV_maxDelayPacket = 10;
    protected static int SIGNALING_maxDelayPacket = 10;
    protected static int VIDEOCONFERENCING_maxDelayPacket = 10;
    protected static int VIDEO_ON_DEMAND_maxDelayPacket = 10;
    protected static int VOIP_maxDelayPacket = 10;
    protected static int DATA_middleSize = 800;
    protected static int DATA_varietySize = 700;
    protected static int INTERACTIVE_DATA_middleSize = 350;
    protected static int INTERACTIVE_DATA_varietySize = 299;
    protected static int IPTV_middleSize = 800;
    protected static int IPTV_varietySize = 700;
    protected static int SIGNALING_middleSize = 64;
    protected static int SIGNALING_varietySize = 36;
    protected static int VIDEOCONFERENCING_middleSize = 600;
    protected static int VIDEOCONFERENCING_varietySize = 199;
    protected static int VIDEO_ON_DEMAND_middleSize = 800;
    protected static int VIDEO_ON_DEMAND_varietySize = 700;
    protected static int VOIP_middleSize = 100;
    protected static int VOIP_varietySize = 199;
    private int middleSize;
    private int varietySize;
    private int maxUsedTime;
    private int generatedPackets;
    private int transport;
    private int maxDelayPacket;
    private int serviceId;

    public Service(int middleSize, int varietySize, int maxUsedTime, int generatedPackets, int transport, int maxDelayPacket,
int serviceId) {
        this.middleSize = middleSize;
        this.varietySize = varietySize;
        this.maxUsedTime = maxUsedTime;
        this.generatedPackets = generatedPackets;
        this.transport = transport;
        this.maxDelayPacket = maxDelayPacket;
        this.serviceId = serviceId;
    }

    public int getServiceID() {
        return this.serviceId;
    }

    public int getPacketSize() {
        return this.middleSize + (int)(Math.random() * (double)this.varietySize);
    }

    public int getMiddleServiceTime() {
        return (int)(Math.random() * (double)this.maxUsedTime + 5.0D);
    }

    public int getPacketsPerSecond() {
        return this.generatedPackets;
    }

    public int getTransport() {
        return this.transport;
    }

    public int getMaxPacketDelay() {
        return this.maxDelayPacket;
    }

    public String toString() {
        return String.format("Service id = %d,%nPacket size = %d,%nService time = %d,%nPacket per second = %d,%nPacket's drop
= %d,%nPacket's delay = %d%n", this.getServiceID(), this.getPacketSize(), this.getMiddleServiceTime(),
this.getPacketsPerSecond(), this.getTransport(), this.getMaxPacketDelay());
    }
}
```

Процесор мережі

```
public class NetworkWorker implements ControllerInt {
    private static final String NEW_MASK = "255.255.240.0";
    private static final String OLD_MASK = "255.0.0.0";
    private static final String NETWORK = "10.0.0.0";
    private List<Switch> switches = new ArrayList();
    private List<Client> clients = new ArrayList();
    private NetworkController networkController = new NetworkController();
    private Deque<List<String>> pullForRouters = new ArrayDeque();
    private IpCalculator ipCalculator = new IpCalculator("10.0.0.0", "255.0.0.0", "255.255.240.0");
    public int allClients;
    private int iteration = 0;
    private GetMiddle getMiddle = new GetMiddle();

    public NetworkWorker() {
    }
```

```
public int getAllClients() {
    return this.allClients;
}

public void initNetwork(int clientPerSwitch, int switchesPerRouter) {
    this.pullForRouters = this.ipCalculator.getNetworkPull(12, 30);
    int switchBandwidth = 100;
    int routerBandwidth = 1000;
    this.addRouter(0, 0, switchBandwidth, routerBandwidth, false);
    this.addRouter(0, 0, switchBandwidth, routerBandwidth, false);
    this.addRouter(0, 0, switchBandwidth, routerBandwidth, false);
    this.addRouter(0, 0, switchBandwidth, routerBandwidth, false);
    this.addRouter(switchesPerRouter, clientPerSwitch, switchBandwidth, routerBandwidth, false);
    this.addRouter(switchesPerRouter, clientPerSwitch, switchBandwidth, routerBandwidth, false);
    this.addRouter(switchesPerRouter, clientPerSwitch, switchBandwidth, routerBandwidth, false);
    this.addRouter(switchesPerRouter, clientPerSwitch, switchBandwidth, routerBandwidth, false);
    this.addRouter(switchesPerRouter, clientPerSwitch, switchBandwidth, routerBandwidth, false);
    this.addRouter(switchesPerRouter, clientPerSwitch, switchBandwidth, routerBandwidth, false);
    this.addRouter(switchesPerRouter, clientPerSwitch, switchBandwidth, routerBandwidth, false);
    this.addRouter(switchesPerRouter, clientPerSwitch, switchBandwidth, routerBandwidth, false);
    this.addRouter(switchesPerRouter, clientPerSwitch, switchBandwidth, routerBandwidth, false);
    this.addRouter(switchesPerRouter, clientPerSwitch, switchBandwidth, routerBandwidth, false);
    this.addRouter(switchesPerRouter, clientPerSwitch, switchBandwidth, routerBandwidth, false);
    System.out.printf("All clients %d\n", this.allClients);
    List<Router> routers = this.networkController.getOldRouters();
    this.makeNeighbor((Router)routers.get(0), (Router)routers.get(1));
    this.makeNeighbor((Router)routers.get(0), (Router)routers.get(2));
    this.makeNeighbor((Router)routers.get(0), (Router)routers.get(3));
    this.makeNeighbor((Router)routers.get(1), (Router)routers.get(2));
    this.makeNeighbor((Router)routers.get(1), (Router)routers.get(3));
    this.makeNeighbor((Router)routers.get(2), (Router)routers.get(3));
    this.makeNeighbor((Router)routers.get(0), (Router)routers.get(4));
    this.makeNeighbor((Router)routers.get(0), (Router)routers.get(5));
    this.makeNeighbor((Router)routers.get(0), (Router)routers.get(6));
    this.makeNeighbor((Router)routers.get(1), (Router)routers.get(7));
    this.makeNeighbor((Router)routers.get(1), (Router)routers.get(8));
    this.makeNeighbor((Router)routers.get(1), (Router)routers.get(9));
    this.makeNeighbor((Router)routers.get(2), (Router)routers.get(10));
    this.makeNeighbor((Router)routers.get(2), (Router)routers.get(11));
    this.makeNeighbor((Router)routers.get(2), (Router)routers.get(12));
    this.makeNeighbor((Router)routers.get(3), (Router)routers.get(13));
    this.makeNeighbor((Router)routers.get(3), (Router)routers.get(14));
    this.makeNeighbor((Router)routers.get(3), (Router)routers.get(15));
    Iterator var6 = routers.iterator();

    while(var6.hasNext()) {
        Router router1 = (Router)var6.next();
        this.switches.addAll(router1.getSwitchList());
    }

    var6 = this.switches.iterator();

    while(var6.hasNext()) {
        Switch swwitch = (Switch)var6.next();
        this.clients.addAll(swwitch.getClients());
    }

    for(int i = 0; i < 10; ++i) {
        Iterator var11 = routers.iterator();

        while(var11.hasNext()) {
            Router router = (Router)var11.next();
            router.updateTable();
        }

        this.networkController.updateTable();
    }

}

private void makeNeighbor(Router router, Router neighbor) {
    NetworkInterface routerInterface = router.getGlobalInterface();
    NetworkInterface neighborInterface = neighbor.getGlobalInterface();
    routerInterface.setNeighbors(neighborInterface);
    neighborInterface.setNeighbors(routerInterface);
}

public void workNetwork() {
    List<Router> routers = this.networkController.getOldRouters();
    System.out.printf("Iterations : %d\n", this.iteration++);
    Iterator var2 = routers.iterator();

    Router router;
    while(var2.hasNext()) {
```

```
            }

        return this.getMiddle.getMiddle();
    }

    public Map<String, Map<String, Map<String, Double>>> getInterfacesLoad() {
        Map<String, Map<String, Map<String, Double>>> loadInfo = new HashMap();
        Iterator var2 = this.networkController.getOldRouters().iterator();

        while(var2.hasNext()) {
            Router router = (Router)var2.next();
            loadInfo.put(router.getHostName(), router.getMiddleInterfacesLoad());
        }

        return loadInfo;
    }
}
    private void updateNetworkInfo(SessionResultInfo sessionResultInfo) {
        this.ActiveServices.setText(this.formatForNetworkInfo("Active Services", sessionResultInfo.getServices()));
    }

    private void updateServiceValues() {
        for(int i = 1; i <= services; ++i) {
            this.serviceVal.updatePieSeries((String)servicesID.get(i), this.servicesValues[i - 1]);
        }

    }

    private void updateTimeOfSeries(SessionResultInfo sessionResultInfo, int iteration) {
        double[][] serviceTimeInfo = sessionResultInfo.getServiceTimeInfo();
        this.values = this.showResult.getCurrentData(serviceTimeInfo, this.values);
        this.time = this.showResult.getIteration(iteration, this.time);

        for(int i = 0; i < services; ++i) {
            XYChart chart = (XYChart)this.timeOfSeries.get(i);

            for(int j = 1; j <= QoS; ++j) {
                chart.updateXYSeries(String.valueOf(j), this.time, this.values[i][j - 1], (double[])null);
            }
        }

    }

    private void updateTrafficChart(int iteration) {
        this.timeForTraffic = this.showResult.getIteration(iteration, this.timeForTraffic);
        this.getTrafficSize();

        for(int i = 1; i <= services; ++i) {
            this.traffic.updateXYSeries((String)servicesID.get(i), this.timeForTraffic, this.serviceTraffic[i - 1],
(double[])null);
        }

        this.traffic.updateXYSeries("General", this.timeForTraffic, this.serviceTraffic[services], (double[])null);
    }

    private void updateQoEPie(List<SessionInfo> allServicesInfo, int iteration) {
        int[][] result = this.CompareTimeWithEtalone(allServicesInfo, iteration);

        for(int i = 0; i < QoS; ++i) {
            PieChart chart = (PieChart)this.pieCharts.get(i);
            chart.updatePieSeries("good", result[i][0]);
            chart.updatePieSeries("bad", result[i][1]);
            this.QoEs.updatePieSeries(String.format("QoE %d", i + 1), Math.round(this.QoEsValues[i]));
        }

    }

    private void updateTCPUDP(List<SessionInfo> allServicesInfo) {
        double[][] tcpAndUdp = this.getTCPudpTimes(allServicesInfo);
        this.tcpUdp.updateXYSeries("UDP", this.timeForTraffic, tcpAndUdp[0], (double[])null);
        this.tcpUdp.updateXYSeries("TCP", this.timeForTraffic, tcpAndUdp[1], (double[])null);
        this.packets.updateXYSeries("Packets", this.timeForTraffic, tcpAndUdp[2], (double[])null);
    }

    private void updateGoodToBad() {
        double[][] temp = new double[5][this.timeForTraffic.length];

        int i;
        for(i = 0; i < QoS; ++i) {
            System.arraycopy(this.GoodToBad[i], 1, temp[i], 0, this.timeForTraffic.length - 1);
            temp[i][this.timeForTraffic.length - 1] = this.goodToBadData[i];
        }

        this.GoodToBad = temp;
```

```
        for(i = 1; i <= QoS; ++i) {
            this.goodToBad.updateXYSeries("QoE " + i, this.timeForTraffic, this.GoodToBad[i - 1], (double[])null);
        }

    }

    private double[][] getTCPudpTimes(List<SessionInfo> allServicesInfo) {
        double[][] tempTimes = new double[3][this.timeForTraffic.length];
        double[] tempTraffic = new double[services + 1];
        int sessions = 0;
        int tcp = 0;
        int udp = 0;
        double tempTcpTime = 0.0D;
        double tempUdpTime = 0.0D;

        int var10001;
        SessionInfo info;
        for(Iterator var11 = allServicesInfo.iterator(); var11.hasNext(); tempTraffic[var10001] += info.getSize() * 8.0D) {
            info = (SessionInfo)var11.next();
            if (info.getTransport() == 0) {
                ++udp;
                tempUdpTime += info.getMiddleTime();
            } else {
                tempTcpTime += info.getMiddleTime();
                ++tcp;
            }

            sessions += info.getPackets();
            var10001 = services;
            tempTraffic[var10001] += info.getSize() * 8.0D;
            var10001 = info.getServiceID() - 1;
        }

        tempTcpTime /= (double)tcp;
        tempUdpTime /= (double)udp;
        this.iterationServicesTraffic = tempTraffic;
        System.arraycopy(this.tcpUDPdata[0], 1, tempTimes[0], 0, this.tcpUDPdata[0].length - 1);
        tempTimes[0][this.tcpUDPdata[0].length - 1] = tempUdpTime;
        System.arraycopy(this.tcpUDPdata[1], 1, tempTimes[1], 0, this.tcpUDPdata[1].length - 1);
        tempTimes[1][this.tcpUDPdata[1].length - 1] = tempTcpTime;
        System.arraycopy(this.tcpUDPdata[2], 1, tempTimes[2], 0, this.tcpUDPdata[2].length - 1);
        tempTimes[2][this.tcpUDPdata[2].length - 1] = (double)sessions;
        this.tcpUDPdata = tempTimes;
        return tempTimes;
    }


    private int[][] CompareTimeWithEtalone(List<SessionInfo> info, int iteration) {
        int[][] result = new int[5][2];
        int[] tempServices = new int[7];
        double[] tempQoEs = new double[5];
        double sensitiveTime = 0.0D;
        int sensitiveValues = 0;
        double unSensitiveTime = 0.0D;
        int unSensitiveValues = 0;
        Iterator var12 = info.iterator();

        while(var12.hasNext()) {
            SessionInfo sessionInfo = (SessionInfo)var12.next();
            ++tempServices[sessionInfo.getServiceID() - 1];
            int var10002;
            if (sessionInfo.getMiddleTime() <
(Double)((Map)this.etaloneTimes.get(sessionInfo.getServiceID())).get(sessionInfo.getClientsQoS())) {
                var10002 = result[sessionInfo.getClientsQoS() - 1][0]++;
            } else {
                var10002 = result[sessionInfo.getClientsQoS() - 1][1]++;
            }


    private void initServicesID() {
        servicesID.put(6, "Ordinary data");
        servicesID.put(7, "Interactive data");
        servicesID.put(4, "IPTV");
        servicesID.put(1, "Service traffic");
        servicesID.put(5, "Video on demand");
        servicesID.put(3, "Video conferences");
        servicesID.put(2, "VoIP");
    }



     private void initTime() {
         this.etaloneTimes.put(6, this.getTimeMap(new double[]{0.33D, 0.27D, 0.2D, 0.15D, 0.1D}));
         this.etaloneTimes.put(7, this.getTimeMap(new double[]{0.33D, 0.27D, 0.2D, 0.15D, 0.1D}));
```

```
        this.etaloneTimes.put(5, this.getTimeMap(new double[]{0.23D, 0.2D, 0.17D, 0.1025D, 0.04D}));
        this.etaloneTimes.put(4, this.getTimeMap(new double[]{0.21D, 0.195D, 0.17D, 0.1125D, 0.05D}));
        this.etaloneTimes.put(1, this.getTimeMap(new double[]{0.21D, 0.18D, 0.15D, 0.0875D, 0.025D}));
        this.etaloneTimes.put(3, this.getTimeMap(new double[]{0.21D, 0.18D, 0.16D, 0.0925D, 0.035D}));
        this.etaloneTimes.put(2, this.getTimeMap(new double[]{0.21D, 0.175D, 0.15D, 0.09D, 0.03D}));
        Map<Integer, Map<Integer, List<Integer>>> x = new HashMap();
        x.put(0, this.initBugraw());
        x.put(1, this.initBugraw());
        this.bugraw.put(0, x);
        x = new HashMap();
        x.put(0, this.initBugraw());
        x.put(1, this.initBugraw());
        this.bugraw.put(1, x);
        this.bugrawTime.put(0, 1.0D);
        this.bugrawTime.put(1, 1.0D);
        this.bugrawTimeName.put(0, "Sensitive services");
        this.bugrawTimeName.put(1, "Insensitive services");
    }

    private Map<Integer, List<Integer>> initBugraw() {
        Map<Integer, List<Integer>> temp = new HashMap();

        for(int i = 1; i < 6; ++i) {
            temp.put(i, new ArrayList());
        }

        return temp;
    }

    private Map<Integer, Double> getTimeMap(double[] time) {
        Map<Integer, Double> temp = new HashMap();

        for(int i = 0; i < time.length; ++i) {
            temp.put(i + 1, time[i]);
        }

        return temp;
    }

    static {
        QoS = ChoseQoS.QOS_VALUES;
        services = 7;
        newVersion = false;
        networkPause = false;
        chartsSize = 50;
        servicesID = new HashMap();
    }
}
```

Додаток 3. Програмний код реалізації QoE додатку

Клас, який забезпечує відображення та обробку даних на екрані “Меню користувача”

```
import UIKit
import FirebaseAuth
import FirebaseDatabase
import CoreTelephony
import Cosmos
import Reachability

class ServiceSetupVC: UIViewController {

    @IBOutlet weak var logOutBtn: UIButton!
    @IBOutlet weak var cellularProviderLbl: UILabel!
    @IBOutlet weak var phoneNumberLbl: UILabel!
    @IBOutlet weak var wifiUsageLbl: UILabel!
    @IBOutlet weak var cellularUsageLbl: UILabel!
    @IBOutlet weak var cosmosView: CosmosView!
    @IBOutlet weak var beginDatePicker: UIDatePicker!
    @IBOutlet weak var endDatePicker: UIDatePicker!
    @IBOutlet weak var orderTypePicker: UIPickerView!
    @IBOutlet weak var sendOrderBtn: UIButton!

    let orderTypeList = ["Social Network","Audio Call","Video Call", "Media Content"]

    let rootRef = Database.database().reference()
    var ref: DatabaseReference?

    override func viewDidLoad() {
        super.viewDidLoad()
        prepareUI()
        prepareDatabase()
    }

    override func viewWillAppear(_ animated: Bool) {
        prepareData()
    }
        private func prepareUI() {
        orderTypePicker.delegate = self
        orderTypePicker.dataSource = self
        sendOrderBtn.layer.cornerRadius = sendOrderBtn.bounds.height / 2
        sendOrderBtn.clipsToBounds = true
        beginDatePicker.minimumDate = Date()
        cosmosView.settings.updateOnTouch = true
        cosmosView.settings.fillMode = .precise
        cosmosView.settings.starSize = 40
        cosmosView.settings.starMargin = 5
        cosmosView.rating = 1
        cosmosView.didFinishTouchingCosmos = { rating in
    }

    private func prepareDatabase() {
        ref = rootRef.child("ordered-items")
    }
    private func prepareData() {
        let networkInfo = CTTelephonyNetworkInfo()
        if let carrier = networkInfo.serviceSubscriberCellularProviders?["0000000100000001"] {
            cellularProviderLbl.text = carrier.carrierName?.capitalized
        }

        if let number = Auth.auth().currentUser?.phoneNumber {
            phoneNumberLbl.text = number
        }
        wifiUsageLbl.text = SystemDataUsage.dataUsageString(from: SystemDataUsage.wifiCompelete)
        cellularUsageLbl.text = SystemDataUsage.dataUsageString(from: SystemDataUsage.wwanCompelete)
    }
    @IBAction func logOutAction(_ sender: Any) {
        let firebaseAuth = Auth.auth()
        do {
            try firebaseAuth.signOut()
            self.navigationController?.popViewController(animated: true)
        } catch let signOutError as NSError {
            print ("Error signing out: %@", signOutError)
```

```
        }
    }

    @IBAction func sendOrderAction(_ sender: UIButton) {
        guard let provider = cellularProviderLbl.text else { return }
        guard let userPhone = phoneNumberLbl.text else { return }
        let qs = "\(cosmosView.rating)"
        let formatter = DateFormatter()
        formatter.dateFormat = "yyyy-MM-dd HH:mm"
        let beginDateStr = formatter.string(from: beginDatePicker.date)
        formatter.dateFormat = "HH:mm"
        let periodDateStr = formatter.string(from: endDatePicker.date)
        let orderType = orderTypeList[orderTypePicker.selectedRow(inComponent: 0)]
        let orderedModel = OrderModel(provider: provider, phone: userPhone, qs: qs, beginDate: beginDateStr, period: periodDateStr, orderType:
orderType)
        showPriceAlert(orderedModel: orderedModel)


extension ServiceSetupVC {

    private func showPriceAlert(orderedModel: OrderModel) {
        let price = Int.random(in: 50...200)
        let message = "Order price is \(price) UAH"
        let alertVC = UIAlertController(title: "Mobile Service Provider", message: message, preferredStyle: .alert)
        let cancelAction = UIAlertAction(title: "Cancel", style: .cancel, handler: nil)
        let okAction = UIAlertAction(title: "OK", style: .default) { (action) in

            orderedModel.price = "\(price) UAH"
            orderedModel.networkType = self.getNetworkType() ?? ""
            let dic = orderedModel.toAnyObject()
            let orderEntity = self.ref?.childByAutoId()
            orderEntity?.setValue(dic)
        }

        alertVC.addAction(cancelAction)
        alertVC.addAction(okAction)
        present(alertVC, animated: true, completion: nil);
    }

    private func getNetworkType() -> String? {
        let reachability = Reachability()!
        do {
            try reachability.startNotifier()
            let status = reachability.connection
            if (status == .none) {
                return nil
            } else if (status == .wifi) {
                return "Wifi"
            } else if (status == .cellular) {
                let networkInfo = CTTelephonyNetworkInfo()
                let carrierType = networkInfo.currentRadioAccessTechnology
                switch carrierType {
                case CTRadioAccessTechnologyGPRS?,CTRadioAccessTechnologyEdge?,CTRadioAccessTechnologyCDMA1x?: return "2G"
                case
CTRadioAccessTechnologyWCDMA?,CTRadioAccessTechnologyHSDPA?,CTRadioAccessTechnologyHSUPA?,CTRadioAccessTechnologyCDM
AEVDORev0?,CTRadioAccessTechnologyCDMAEVDORevA?,CTRadioAccessTechnologyCDMAEVDORevB?,CTRadioAccessTechnologyeHRP
D?: return "3G"
                case CTRadioAccessTechnologyLTE?: return "LTE"
                default: return nil
                }
            } else {
                return nil
            }
        } catch {
            return nil
        }
    }
}
extension ServiceSetupVC: UIPickerViewDelegate, UIPickerViewDataSource {
    func numberOfComponents(in pickerView: UIPickerView) -> Int {
        return 1
    }

    func pickerView(_ pickerView: UIPickerView, numberOfRowsInComponent component: Int) -> Int {
        return orderTypeList.count
    }
```

```
    func pickerView(_ pickerView: UIPickerView, titleForRow row: Int, forComponent component: Int) -> String? {
        return orderTypeList[row]
    }
}
```

Клас, який забезпечує відображення та обробку даних на екрані “Меню адміністратора”

```
import UIKit
import FirebaseAuth
import FirebaseDatabase


class OrderListVC: UIViewController {


    @IBOutlet weak var orderTableView: UITableView! {
        didSet {
            orderTableView.delegate = self
            orderTableView.dataSource = self
            orderTableView.estimatedRowHeight = 211
            orderTableView.rowHeight = UITableView.automaticDimension
        }
    }

    let rootRef = Database.database().reference()
    var ref: DatabaseReference?

    var orderedList = [OrderModel]()

    override func viewDidLoad() {
        super.viewDidLoad()
        prepareDatabase()
    }

    private func prepareDatabase() {
        ref = rootRef.child("ordered-items")

        ref?.observe(DataEventType.value, with: { (snapshot) in
            guard let orderedItems = snapshot.value as? [String: AnyObject] else { return }
            var orderedList = [OrderModel]()
            for key in orderedItems.keys {
                guard let modelDic = orderedItems[key] as? [String: String] else { return }
                orderedList.append(OrderModel.toModelFrom(dic: modelDic))
            }

            orderedList = orderedList.sorted { (prev,next) in
                let dfmatter = DateFormatter()
                dfmatter.dateFormat = "yyyy-MM-dd HH:mm"
                let prevDate = dfmatter.date(from: prev.beginDate)
                let prevDateStamp: TimeInterval = prevDate!.timeIntervalSince1970
                let prevTimeStamp: Int = Int(prevDateStamp)

            self.orderedList = orderedList
            self.orderTableView.reloadData()
        })

    @IBAction func logOutAction(_ sender: Any) {
        let firebaseAuth = Auth.auth()
        do {
            try firebaseAuth.signOut()
            self.navigationController?.popViewController(animated: true)
        } catch let signOutError as NSError {
            print ("Error signing out: %@", signOutError)
        }

extension OrderListVC: UITableViewDelegate, UITableViewDataSource {

    func tableView(_ tableView: UITableView, numberOfRowsInSection section: Int) -> Int {
    func tableView(_ tableView: UITableView, cellForRowAt indexPath: IndexPath) -> UITableViewCell {
        guard let cell = tableView.dequeueReusableCell(withIdentifier: "OrderListCell") as? OrderListCell else { return UITableViewCell() }
        cell.setup(model: orderedList[indexPath.row])
        return cell
    }
}
```

Додаток 4. Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Наукові праці, у яких опубліковані основні результати дисертації

1. M. Beshley, *Development and testbed of software router for critical application*. Saarbrücken, Germany: LAP Lambert Academic Publishing, 2019. ISBN: 978-613-9-46367-1.

2. M. M. Климаш, T. A. Максимюк, M. I. Бешлей, *Методи та моделі побудови гетерогенних мереж мобільного зв'язку 4G/5G.* Львів, Україна: Видавництво "Львівська політехніка", 2020. ISBN: 978-966-941-552-3.

3. I. Demydov, N. Baydoun, M. Beshley, M. Klymash, O. Panchenko, "Development of basic concept of ICT platforms deployment strategy for social media marketing considering tectonic theory*," EUREKA: Physics and Engineering*, vol. 0, no.1, pp. 18–33, Jan. 2020. (Scopus Q2).

4. S. Jun, K. Przystupa, M. Beshley, O. Kochan, H. Beshley, M. Klymash, J. Wang, D. Pieniak, "A Cost-Efficient Software Based Router and Traffic Generator for Simulation and Testing of IP Network," *Electronics*, vol. 9, no. 1, pp. 40-1–40-24, Jan. 2020. (Scopus/Web of Science Q1).

5. W. Song, M. Beshley, K. Przystupa, H. Beshley, O. Kochan, A. Pryslupskyi, D. Pieniak, J. Su, "A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection," *Sensors*, vol. 20, no. 6, p. 1637-1–1637-41, March 2020. (Scopus/Web of Science Q1).

6. M. Beshley, N. Kryvinska, M. Seliuchenko, H. Beshley, E. Shakshuki, A. Yasar, "End-to-End QoS "Smart Queue" Management Algorithms and Traffic Prioritization Mechanisms for Narrow-Band Internet of Things Services in 4G/5G Networks," *Sensors*, vol. 20, no.8, pp.2324-1–2324-30, Apr. 2020. (Scopus/Web of Science Q1).

7. S. Wenguang, V. Andrushchak, M. Kaidan, M. Beshley, O. Kochan, S. Jun, "Methodology for Calculating the Energy Consumption of Information Communication Systems," *Technical Electrodynamics*, no. 4, pp. 80–88, July 2020. (Scopus Q3).

8. H. Xu, K. Przystupa, C. Fang, O. Kochan, M. Beshley, A. Marciniak, “A combination strategy of feature selection based on an integrated optimization algorithm and weighted k-nearest neighbor to improve the performance of network intrusion detection,” *Electronics,* vol. 9, no. 8, pp. 1206-1–1206-22, July 2020. (Scopus/Web of Science Q1).

9. M. Beshley, P. Vesely, A. Prislupskiy, H. Beshley, M. Kyryk, V. Romanchuk, I. Kahalo, “Customer-Oriented Quality of Service Management Method for the Future Intent-Based Networking,” *Applied Sciences*, vol. 10, no. 22, pp. 8223-1–8223-38. Nov. 2020. (Scopus/Web of Science Q1).

10. K. Przystupa, M. Beshley, M. Kaidan, V. Andrushchak, I. Demydov, O. Kochan, D. Pieniak, “Methodology and Software Tool for Energy Consumption Evaluation and Optimization in Multilayer Transport Optical Networks,” *Energies*, vol. 13, no. 23, pp. 6370-1–6370-21. Dec. 2020. (Scopus/Web of Science Q1).

11. V. Romanchuk. M. Beshley, A. Prislupskiy, H. Beshley, O. Panchenko, “Method of multiservice infrastructure decomposition with network resource slicing for IoT,” *Internet of Things (IoT) and Engineering Applications* (Canada), vol. 3, no.1, pp. 22–23. May 2018.

12. M. Klymash, M. Beshley, “Perspective directions of development and research in the field of information and communication technologies,” *BA Magazine “Wissen im Markt”*, no. 3, pp. 31–37, 2019.

13. М.М. Климаш, М.В. Кайдан, М.І. Бешлей, А.В. Редька, “Оптимізація багатошарової структури транспортної мережі на основі технологій IP/MPLS/DWDM за допомогою методу діакоптики,” *Наукові записки Українського науково-дослідного інституту зв'язку*, № 3, с. 32–42, 2015.

14. М.І. Бешлей, В.В. Червенець, І.В. Демидов, В.І. Романчук, О.М. Панченко, “Розвиток методів передавання даних реального часу шляхом вдосконалення процесів пріоритезації потоків у маршрутизаторах,” *Системи озброєння і військова техніка: наук. журнал - Х: Харк. ун-т Повітр. Сил ім. І. Кожедуба*, 5(142), с. 114 –123, 2016.

15. М.М. Климаш, М.І. Бешлей, Ю.Д. Дещинський, О.М. Панченко, “Розробка методу балансування навантаження в SDN мережах на основі

модифікованого протоколу STP," *Комп'ютерні технології друкарства*, №2, с. 146–155, 2015.

16. I. Demydov, M. Klymash, M. Beshley, O. Shpur, "Features of the cloud services implementation in the national network segment of Ukraine," *Information and telecommunication science. K.: NTUU «KPI»*, No.1, pp. 31–38, 2016.

17. М.М. Климаш, В.І. Романчук, О.М. Панченко, М.І. Бешлей, А.В. Поліщук, "Розроблення програмного маршрутизатора з автоматичним розгортанням віртуальних вузлів," *Вісник Національного університету "Львівська політехніка". Радіоелектроніка та телекомунікації,* № 885, с. 22 – 30, 2017.

18. Г.В. Бешлей, М.О. Селюченко, І.А Берневек, С.І. Пущак, М.І. Бешлей, "Алгоритм кластеризації, агрегації та класифікації M2M пристроїв в гетерогенній мережі 4G/5G," *Вісник Національного університету "Львівська політехніка". Радіоелектроніка та телекомунікації*, № 874, с. 95–102, 2017.

19. V. Romanchuk, M. Klymash, M. Beshley, O. Panchenko, A. Polishchuk, "Development of software-based router model with adaptive selection of algorithms for queues servicing," *Technology audit and production reserves,* №3/2(41), pp. 46–55, 2018.

20. В.І Романчук, М.І. Бешлей, О.М. Панченко, А.В. Поліщук, "Метод узгодженого розв'язання завдань балансування різнопріоритетного навантаження між чергами мережевих пристроїв," *Наукові записки Українського науково-дослідного інституту зв'язку*, №2(50), с. 48–57, 2018.

21. В.І. Романчук, М.І. Бешлей, А.М. Прислупський, Г.В. Бешлей, "Метод декомпозиції структури мережного пристрою з віртуалізацією ресурсів," *Наукові записки Української академії друкарства*, №1(56), с. 31– 42. 2018.

22. М.В. Кайдан, М.І. Бешлей, Т.А. Максимюк, Б.М. Стрихалюк, Р.З. Матвіїв, "Теорія Кернера та фазові переходи для потоків у телекомунікаційних мережах," *Вісник Національного університету "Львівська політехніка". Радіоелектроніка та телекомунікації*, № 909, с. 29–34, 2018.

23. І.О. Кагало, М.І. Бешлей, М.М. Климаш, О.М. Панченко, Г.В. Бешлей, "Адаптивне формування багаторівневої радіоструктури інтегрованих мереж

LTE/Wi-Fi,” *Телекомунікаційні та інформаційні технології*, № 3(64), с. 24 –38, 2019.

24. М.М. Климаш, А.Б. Нажм, О.Л. Костів, І.В. Демидов, М.І. Бешлей, “Створення ефективних ІКТ-платформ електронного урядування інтерактивного типу: аналіз архітектури систем розповсюдження контенту,” *Наукові записки Українського науково-дослідного інституту зв'язку*, № 3, с. 31– 45, 2019.

Наукові праці, які засвідчують апробацію матеріалів дисертації

25. M. Klymash, M. Seliuchenko, M. Beshley and S. Redchuk, "Increasing wavelengths utilization efficiency in OTNoDWDM network based on local resource distribution method," *2015 Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*, Kharkiv, 2015, pp. 157–160. (очна участь із доповіддю)

26. M. Klymash, O. Lavriv, T. Maksymyuk and M. Beshley, "State of the art and further development of information and communication systems," *2016 International Conference Radio Electronics & Info Communications (UkrMiCo)*, Kiev, 2016, pp. 1– 6. (заочна участь, доповідь співавтора)

27. M. Beshley, V. Romanchuk, V. Chervenets and A. Masiuk, "Ensuring the quality of service flows in multiservice infrastructure based on network node virtualization," *2016 International Conference Radio Electronics & Info Communications (UkrMiCo)*, Kiev, 2016, pp. 1–3. (очна участь із доповіддю)

28. M. Seliuchenko, M. Beshley, O. Panchenko and M. Klymash, “Development of monitoring system for end-to-end packet delay measurement in software-defined networks,” *IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET’2016)*, Lviv, 2016, pp. 667–670. (очна участь із доповіддю)

29. A. Masiuk, M. Beshley, O. Lavriv and Y. Deschynskiy, “Common radio resource management model for heterogeneous cellular networks,” *IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET’2016)*, Lviv, 2016, pp. 661–663. (заочна участь, доповідь співавтора)

30. O. Panchenko, A. Polishuk, M. Seliuchenko and M. Beshley, "Method for adaptive client oriented management of quality of service in integrated SDN/CLOUD networks," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 452–455. (очна участь із доповіддю)

31. M. Klymash, H. Beshley, M. Seliuchenko and M. Beshley, "Algorithm for clusterization, aggregation and prioritization of M2M devices in heterogeneous 4G/5G network," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 182–186. (очна участь із доповіддю)

32. M. Klymash, H. Beshley, O. Panchenko and M. Beshley, "Method for optimal use of 4G/5G heterogeneous network resourses under M2M/IoT traffic growth conditions," *2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Odessa, 2017, pp. 1–5. (заочна участь, доповідь співавтора)

33. V. Romanchuk, M. Beshley, O. Panchenko and P. Arthur, "Design of software router with a modular structure and automatic deployment at virtual nodes," *2017 2nd International Conference on Advanced Information and Communication Technologies (AICT)*, Lviv, 2017, pp. 295–298. (заочна участь, доповідь співавтора)

34. M. Klymash, V. Romanchuk, M. Beshley and P. Arthur, "Investigation and simulation of system for data flow processing in multiservice nodes using virtualization mechanisms," *2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON)*, Kiev, 2017, pp. 989–992. (очна участь із доповіддю)

35. M. Beshley, M. Seliuchenko, O. Panchenko and A. Polishuk, "Adaptive flow routing model in SDN," *2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)*, Lviv, 2017, pp. 298–302. (заочна участь, доповідь співавтора)

36. H. Beshley, M. Kyryk, M. Beshley and O. Panchenko, "Method of information flows engineering and resource distribution in 4G/5G heterogeneous

network for M2M service provisioning," *2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)*, Lviv, 2018, pp. 229–233. (очна участь із доповіддю)

37. V. Romanchuk, M. Beshley, A. Polishuk and M. Seliuchenko, "Method for processing multiservice traffic in network node based on adaptive management of buffer resource," *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2018, pp. 1118 –1122. (очна участь із доповіддю)

38. T. Maksymyuk, M. Beshley, M. Klymash, O. Petrenko and Y. Matsevityi, "Eavesdropping-resilient wireless communication system based on modified OFDM/QAM air interface," *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2018, pp. 1127–1130. (заочна участь, доповідь співавтора)

39. M. Beshley, M. Seliuchenko, O. Panchenko, O. Zyuzko and I. Kahalo, "Experimental performance analysis of software-defined network switch and controller," *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2018, pp. 282–286. (очна участь із доповіддю)

40. H. Beshley, M. Beshley, T. Maksymyuk and I. Strykhalyuk, "Method of centralized resource allocation in virtualized small cells network with IoT overlay," *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2018, pp. 1147–1151. (очна участь із доповіддю)

41. M. Klymash, I. Demydov, M. Beshley and O. Kostiv, "Structures assessment of data-centers telecommunication systems for metadata fixation," *2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Odessa, 2018, pp. 1–7. (заочна участь, доповідь співавтора)

42. M. Beshley, S. Toliupa, V. Pashkevych and R. Kolodiy, “Development of software system for network traffic analysis and intrusion detection,” *International*

Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Kiev, 2018, pp. 1–3. (очна участь із доповіддю)

43. M. Seliuchenko, M. Kyryk, M. Beshley, M. Zhovtonoh, “Automated Recovery of Server Applications for SDN-Based Internet of Things,” *International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo),* Lviv, 2019, pp. 25–29. (очна участь із доповіддю)

44. I. Kahalo, H. Beshley, M.Beshley and O. Panchenko, “Enhancing QoS and energy efficiency of LTE/LTE-U/Wi-Fi integrated network based on adaptive technique for radio structure formation,” *2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON),* Kiev, 2019, pp. 1167–1170. (заочна участь, доповідь співавтора)

45. M. Beshley, A. Pryslupskyi, O. Panchenko and H. Beshley, “SDN/Cloud solutions for intent-based networking,” *2019 IEEE 3nd International Conference on Advanced Information and Communication Technologies (AICT),* Lviv, 2019, pp. 95–98. (очна участь із доповіддю)

46. A. Pryslupskyi, O. Panchenko, M. Beshley and M. Seliuchenko, "Improvement of multiprotocol label switching network performance using software-defined controller," *2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM),* Polyana, Ukraine 2019, pp. 106 –109. (очна участь із доповіддю)

47. H. Beshley, M. Klymash, M. Beshley and I. Kahalo, "Improving the efficiency of LTE spectral resources use by introducing the new of M2M/IoT multi-service gateway," *2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM),* Polyana, Ukraine, 2019, pp.114 –117. (очна участь із доповіддю)

48. M. Beshley, A. Pryslupskyi, O. Panchenko and M. Seliuchenko, "Dynamic switch migration method based on QoE-aware priority marking for intent-based networking," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET),* Lviv-Slavske, 2020, pp. 864 –868. (очна участь із доповіддю)

49. Z. Cheng, M. Beshley, H. Beshley, O. Kochan and O. Urikova, "Development of deep packet inspection system for network traffic analysis and intrusion detection," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2020, pp. 877–881. (очна участь із доповіддю)

50. Z. Hu, M. Beshley, V. Vitalii, S. Jun and T. Volodymyr, "Modified EIRGP routing protocol for backbone infrastructure of wireless multimedia sensor networks," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2020, pp. 894–899. (очна участь із доповіддю)

51. M. Beshley, M. Klymash, M. Hamal, Y. Shkoropad and A. Branytskyy, "Method for estimating service delay in edge and cloud computing architecture," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2020, pp. 915–919. (очна участь із доповіддю)

52. М.О. Селюченко, Г.В. Бешлей, А.Р. Масюк, М.І. Бешлей, “Багаторівневе управління ресурсами в гетерогенній мульти-операторській мережі,” *1st International Conference "Advanced information and communication technologies"(AICT’2015),* Lviv, 2015, pp. 125–128. (очна участь із доповіддю)

53. М.М. Климаш, В.І. Романчук, М.І. Бешлей, “Розроблення макету мультисервісної мережі на базі програмно-апаратної платформи для забезпечення навчально-наукового процесу кафедри телекомунікацій,” *1st International Conference "Advanced information and communication technologies"(AICT’2015),* Lviv, 2015, pp. 175–178. (очна участь із доповіддю)

54. М.М. Климаш, В.І. Романчук, М.І. Бешлей, А.О. Лунтовський, “Дослідження ефективності використання ресурсів навчально-наукового центру паралельних обчислень,” *Міжнародна науково-технічна конференція (Сучасні інформаційно-телекомунікаційні технології)*, м. Київ, 2015, с. 61–63. (очна участь із доповіддю)

55. М.І. Бешлей, В.В. Червенець, В.І. Романчук, А.В. Поліщук, “Модель віртуального маршрутизатора з статичною та динамічною реконфігурацією

ресурсів,” *Міжнародна науковотехнічна конференція «Проблемивтелекомунікаці» ПТ-2016: збірник матеріалів конференції* , м. Київ, 2016р., с. 140 –142. (очна участь із доповіддю)

56. М.І. Бешлей, М.О. Селюченко, П.О. Гуськов, А.Р. Масюк, “Підвищення ефективності роботи гетерогенних мереж методом динамічного перерозподілу ресурсів між різними безпроводовими технологіями,” *Міжнародна науково-технічна конференція «Сучасні інформаційно-телекомунікаційні технології»: матеріали науково-технічної конференції,* м. Київ, 2015 р., с. 49–50. (заочна участь, доповідь співавтора)

57. М.І. Бешлей, М.М. Климаш, А.Р. Масюк, “Розробка і дослідження імітаційної моделі безпровідної гетерогенної мережі,” *Міжнародна науково-технічна конференція «Проблеми телекомунікацій» ПТ-2016: збірник матеріалів конференції*, м. Київ, 2016 р., с. 70–72. (заочна участь, доповідь співавтора)

58. М.І. Бешлей, О.М. Панченко, І.В. Демидов, М.О Селюченко, “Метод динамічного управління якістю послуг в інтегрованій SDN/CLOUD мережі,” *Фізико-технологічні проблеми, обробки та зберігання інформації в інфокомунікаційних системах: матеріали V Міжнародної науково-практичної конференції*, м. Чернівці, 2016 р., с. 74 –75. (очна участь із доповіддю)

59. М.М. Климаш, А.Р. Масюк, Г.В. Бешлей, М.І. Бешлей, “Концепція програмно конфігурованої гетерогенної мережі мобільного зв'язку на основі технологій SDN/NFV та SDR,” *Фізико-технологічні проблеми , обробки та зберігання інформації в інфокомунікаційних системах: матеріали V Міжнародної науково-практичної конференції,* м. Чернівці, 2016 р., с. 35–36. (заочна участь, доповідь співавтора)

60. М.І. Бешлей, М.М. Климаш, О.М. Панченко, Г.В. Бешлей, “Розроблення системи моніторингу та аналізу трафіку інформаційно телекомунікаційної мережі для виявлення аномалії і запобігання атак,” *І міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно телекомунікаційних систем”(PCSITS)*, м. Київ, 2018р.,с.201– 203. (заочна участь, доповідь співавтора)