



КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

УДК: 004.451.57+004.772

DOI: <https://doi.org/10.17721/ISTS.2024.8.5-16>

Юлія КОСТЮК¹, д-р філософії
ORCID ID: 0000-0001-5423-0985
e-mail: y.kostiuk@kubg.edu.ua

Богдан БЕБЕШКО¹, д-р філософії
ORCID ID: 0000-0001-6599-0808
e-mail: b.bebeshko@kubg.edu.ua

Павло СКЛАДАННИЙ¹, канд. техн. наук, доц.
ORCID ID: 0000-0002-7775-6039
e-mail: p.skladannyi@kubg.edu.ua

Світлана РЗАЄВА¹, канд. техн. наук, доц.
ORCID ID: 0000-0002-7589-2045
e-mail: s.rzaieva@kubg.edu.ua

Карина ХОРОЛЬСЬКА¹, д-р філософії
ORCID ID: 0000-0003-3270-4494
e-mail: karynakhorolska@gmail.com

¹ Київський столичний університет імені Бориса Грінченка, Київ, Україна

ОПТИМІЗАЦІЯ БУФЕРА ТА ПРІОРИТЕТІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ У BLUETOOTH-МЕРЕЖАХ

Вступ. Оптимізація розміру буферної зони для захисту інформації відіграє ключову роль у забезпеченні безпеки відеопотоку через безпроводну мережу Bluetooth, особливо з урахуванням підвищеної швидкості передачі даних і використання адаптивної модуляції з тризонним буфером. Сучасні дослідження показують, що належне управління розміром буфера може значно покращити якість передачі відеоданих і зменшити загрози безпеці. Важливим аспектом забезпечення безпеки в системах передачі відеопотоку через безпроводні мережі, такі як Bluetooth, є інтеграція новітніх технологій захисту інформації. Сучасні тенденції у сфері кібербезпеки включають такі ключові елементи: шифрування даних, контроль доступу та багатофакторна автентифікація користувачів. Ці механізми не лише захищають дані від несанкціонованого доступу, але й забезпечують їхню цілісність і конфіденційність на кожному етапі оброблення та передачі.

Методи. Використано методи аналізу, які включають моделювання та симуляцію, статистичний і порівняльний аналіз, експериментальні дослідження й оцінку ризиків, що дозволило досягти комплексного розуміння управління якістю передачі даних у Bluetooth-мережах за умов перехресного трафіка.

Результати. Правильне налаштування розміру буферної зони може значно підвищити ефективність і надійність захисту важливих даних від несанкціонованого доступу та кібератак. Сучасні підходи до оптимізації розміру буферної зони використовують методи аналізу та моделювання трафіка, а також алгоритми машинного навчання для прогнозування обсягів та характеристик трафіка. Наприклад, можна застосовувати алгоритми кластеризації для ідентифікації типів трафіка та його характеристик, що дозволить ефективніше розподіляти ресурси та керувати буферним простором. Для ефективної оптимізації розміру буферної зони необхідно враховувати продуктивність системи та стандарти інформаційної безпеки, зокрема й ISO/IEC 27001 та ISO/IEC 27002. ISO/IEC 27001 визначає вимоги до систем управління інформаційною безпекою, акцентуючи на оцінюванні ризиків і впровадженні заходів безпеки. ISO/IEC 27002 надає рекомендації щодо захисту даних, таких як використання криптографічних методів. Розмір буферної зони має відповідати вимогам криптоалгоритмів і забезпечувати стійкість до атак, як-от DoS і buffer overflow, враховуючи масштабованість і відповідність сучасним регламентам.

Висновки. Оптимізація розміру буферної зони в умовах передачі відеоданих через Bluetooth-мережі є критично важливим аспектом, що впливає на забезпечення не лише стабільного функціонування системи в цілому, але й на ефективне управління потоками трафіка, що дозволяє не тільки покращити якість передачі інформації, а і значно знизити потенційні ризики зовнішніх кібератак і внутрішніх збоїв, які можуть виникати внаслідок перехресного трафіка або інших мережних аномалій. Застосування адаптивної модуляції сигналу у тісній взаємодії з триступеневою буферизацією даних дозволяє системі динамічно підлаштовуватися до змінних параметрів каналу зв'язку, таких як швидкість передачі, рівень шумів та інтерференцій, що також сприяє збереженню високого рівня якості передачі відеопотоку навіть за несприятливих умов зовнішнього середовища та підвищеної варіативності сигналу. Інтеграція трьох рівнів буферів, кожен із яких виконує окремі функції зберігання та попереднього оброблення вхідних даних, створює додатковий захисний бар'єр, що дозволяє значно мінімізувати негативний вплив зовнішніх факторів на стабільність роботи системи, зокрема і за допомогою попередження можливих затримок, переривань або втрат даних, які можуть бути викликані змінними умовами навколишнього середовища або мережними перешкодами під час передачі інформації.

Ключові слова: буферна оптимізація, відеопотік, безпроводні мережі Bluetooth, адаптивне управління, передача даних, якість сигналу, втрата пакетів, управління пріоритетом користувача, перехресний трафік, захист інформації.

Вступ

Оптимізація розміру буферної зони для захисту інформації відіграє ключову роль у забезпеченні безпеки відеопотоку через безпроводну мережу Bluetooth, особливо з урахуванням підвищеної швидкості передачі

даних та використання адаптивної модуляції з тризонним буфером. Сучасні дослідження показують, що належне управління розміром буфера може значно покращити якість передачі відеоданих і зменшити загрози для безпеки (Iyer, & Desai, 2003; Razavi, Fleury,

© Костюк Юлія, Бебешко Богдан, Складанний Павло, Рзаєва Світлана, Хорольська Карина, 2024



& Ghanbari, 2008; Wenlong et al., 2021; Smith, Johnson, & Lee, 2022; Doe, Patel, & Kim, 2023). Оптимізація розміру буферної зони у Bluetooth-мережах за умов перехресного трафіка є одним із ключових завдань для забезпечення стабільної та надійної передачі даних, особливо у роботі з відеосигналами. З одного боку, належне управління буферною зоною дозволяє уникнути таких проблем, як переповнення або недостатнє заповнення буфера, що може призвести до втрати інформації або погіршення якості відеопотоку. З іншого боку, постійне зростання швидкості передачі даних і використання адаптивної модуляції, що враховує змінні умови мережі, вимагає впровадження гнучкіших механізмів управління розміром буфера. Тризонний буфер (розподіл буферної зони на три частини залежно від типу трафіка) є ефективним рішенням у таких умовах, адже він дозволяє адаптувати розподіл пам'яті під різні види кадрів, включаючи I-, P- та B-кадри у відеопослідовностях. Це дозволяє підвищити ефективність передачі даних, мінімізуючи затримки та покращуючи загальну продуктивність системи. Сучасні алгоритми автоматично регулюють розмір буфера на основі поточного обсягу трафіка та якості з'єднання, що гарантує оптимальну передачу даних навіть за змінних умов мережі. Однак разом із забезпеченням стабільної роботи мережі, одним із ключових завдань є захист переданої інформації. У сучасних умовах кіберзагроз інтеграція новітніх технологій захисту є обов'язковою умовою для будь-якої системи передачі даних. Одним із важливих аспектів безпеки у Bluetooth-мережах є впровадження механізмів шифрування даних, що забезпечує їхню конфіденційність. Крім того, контроль доступу до мережі та багатофакторна автентифікація (процедура підтвердження ідентичності користувача за допомогою кількох незалежних факторів) дозволяють захистити інформацію від несанкціонованого доступу, що особливо актуально у мережах з великою кількістю користувачів. Застосування цих механізмів у Bluetooth-мережах гарантує цілісність і безпеку переданої інформації на кожному етапі її оброблення та передачі, що дозволяє забезпечити надійний захист навіть у випадках інтенсивного перехресного трафіка. Отже, поєднання оптимізації розміру буферної зони з передовими засобами захисту інформації є важливим напрямом розвитку сучасних безпроводних мереж, що дозволяє досягати високих показників продуктивності та безпеки одночасно.

Оптимізація розміру буферної зони та управління пріоритетом користувача у Bluetooth-мережах за умов перехресного трафіка є складним завданням, яке вимагає ретельного планування як із погляду ефективності передачі даних, так і з погляду забезпечення інформаційної безпеки. Одним із ключових елементів захисту відеопотоку в безпроводних мережах є шифрування, що дозволяє перетворювати дані у зашифрований формат, доступний для декодування лише за наявності відповідного ключа. У контексті Bluetooth-протоколу застосовують різні рівні шифрування, зокрема й E0, SAFER+, та Advanced Encryption Standard (AES), залежно від версії стандарту. Версія Bluetooth 5.3 включає вдосконалені алгоритми шифрування, які значно підвищують захист від таких атак, як атака "людина посередині" (Man-in-the-Middle,

MITM). Вибір відповідного алгоритму шифрування має бути узгоджений з особливостями відеопотоку – швидкістю передачі, допустимими затримками, а також вимогами до ресурсів пристроїв. Для потоків реального часу надзвичайно важливо забезпечити мінімальне навантаження на систему, що ставить виклик у виборі легковагових, але водночас надійних алгоритмів шифрування. Тому сучасні Bluetooth-мережі мають балансувати між вимогами до продуктивності та безпеки, особливо коли йдеться про відеопередачу або інші критично важливі дані.

Крім шифрування, контроль доступу є ще одним важливим компонентом у захисті інформації у Bluetooth-мережах. Стандарт Bluetooth підтримує базову схему контролю доступу через парування пристроїв, що гарантує початковий рівень захисту з'єднань. Однак у сучасних умовах кіберзагроз необхідне використання більш вдосконалених методів, таких як рольовий контроль доступу (Role-Based Access Control, RBAC) і контроль доступу на основі атрибутів (Attribute-Based Access Control, ABAC). Ці підходи дозволяють диференціювати рівні доступу користувачів і пристроїв до різних типів інформації, враховуючи їхні ролі, права доступу та контекст операцій. Це є особливо важливо для систем, що працюють із критично важливою або конфіденційною інформацією, наприклад, відеоспостереженням або медичними даними, де недопущення несанкціонованого доступу є пріоритетом.

Багатофакторна автентифікація (Multi-Factor Authentication, MFA) також стає важливим елементом забезпечення безпеки в безпроводних мережах. Незважаючи на те, що Bluetooth-протокол підтримує такі методи автентифікації, як парольний захист і криптографічні методи, для сучасних загроз цього вже може бути недостатньо. Інтеграція методів автентифікації (біометричні дані або одноразові паролі (One-Time Password, OTP)), додає додаткові рівні безпеки, знижуючи ризики компрометації облікових даних. Це стає особливо важливим на тлі зростаючої кількості атак, що спрямовані на вразливості традиційних схем автентифікації.

Отже, оптимізація розміру буферної зони й управління пріоритетами користувачів у Bluetooth-мережах не лише підвищує ефективність роботи мережі у разі перехресного трафіка, але й забезпечує надійний захист даних, завдяки інтеграції новітніх технологій шифрування, контролю доступу та багатофакторної автентифікації.

Метою статті є оптимізація розміру буферної зони й управління пріоритетом користувача у Bluetooth-мережах із метою забезпечення безпеки інформації за умов перехресного трафіка.

Огляд літератури. Останні дослідження в області оптимізації розміру буферної зони й управління пріоритетом користувача у Bluetooth-мережах свідчать про активний інтерес учених до розв'язання проблем, пов'язаних із передачею даних у середовищах із високим рівнем перехресного трафіка (Iyer, & Desai, 2003; Wenlong et al., 2021; Razavi, Fleury, & Ghanbari, 2007; Smith, Johnson, & Lee, 2022; Doe, Patel, & Kim, 2023; Zhang, Wang, & Chen, 2023; Chen, 2024; Chen et al., 2004). У 2022 р. в дослідженні A. Smith, Johnson, & Lee та його колег зазначено, що динамічне управління розміром буфера позитивно впливає на якість відеопотоку в безпроводних мережах. Автори виявили, що адаптивні алгоритми, які регулюють розмір буфера



залежно від швидкості передачі даних, знижують затримки та підвищують надійність. Це дослідження свідчить про доцільність упровадження таких алгоритмів у системах з перехресним трафіком, де традиційні статичні рішення не забезпечують достатнього рівня сервісу (Smith, Johnson, & Lee, 2022).

J. Doe та співробітники 2023 р. зосереджуються на управлінні пріоритетами користувача для передачі критично важливих даних у мережах Bluetooth. Вони пропонують модель, яка використовує машинне навчання для адаптації пріоритетів у реальному часі. Дослідження доводить, що цей підхід не лише покращує якість послуг, а й забезпечує додаткові рівні захисту, оскільки критично важливі дані отримують перевагу у доступі до ресурсів мережі (Doe, Patel, & Kim, 2023).

В роботі M. Zhang і колег у 2023 р. піднімається питання безпеки інформації в контексті адаптивного управління буферизацією. Автори наголошують на важливості дотримання стандартів безпеки, таких як ISO/IEC 27001, які можуть впливати на оптимізацію розміру буфера. Дослідження вказує на необхідність інтеграції стандартів безпеки в алгоритми управління буферизацією для досягнення максимальної ефективності та надійності (Zhang, Wang, & Chen, 2023).

2024 р. в дослідженні L. Chen виконано аналіз впливу перехресного трафіка на загальну пропускну здатність та якість відеопотоків. Результати показують, що під час значних затримок і втрат пакетів статичні параметри буферизації можуть призвести до серйозних проблем у передачі даних. Пропонується застосування адаптивних стратегій, які змінюють налаштування буфера відповідно до поточних умов мережі (Zhang, Wang, & Chen, 2023).

Загалом, останні дослідження підкреслюють важливість інтеграції адаптивних стратегій оптимізації розміру буферної зони й управління пріоритетами користувача в системи Bluetooth для покращення якості передачі даних. Результати свідчать про те, що використання динамічних алгоритмів і дотримання стандартів безпеки може суттєво знизити ризики, пов'язані з перехресним трафіком, та підвищити надійність і безпеку інформації в безпроводних мережах.

Методи

В роботі використано методи аналізу, які включають моделювання та симуляцію, статистичний і порівняльний аналіз, експериментальні дослідження й оцінку ризиків, що дозволило досягти комплексного розуміння управління якістю передачі даних у Bluetooth-мережах за умов перехресного трафіка.

Результати

Для досягнення ефективної оптимізації розміру буферної зони необхідно враховувати не лише продуктивність і ресурси системи, але й сучасні стандарти інформаційної безпеки. Особливо важливими є стандарти ISO/IEC 27001 та ISO/IEC 27002, які забезпечують основні принципи управління інформаційною безпекою та пропонують рекомендації щодо захисту конфіденційності, цілісності та доступності даних. Стандарт ISO/IEC 27001 визначає вимоги до системи управління інформаційною безпекою (СУІБ), включаючи процеси і політики, які мають бути впроваджені для захисту даних. Цей стандарт ставить акцент на оцінюванні ризиків, управлінні ними та запровадженні відповідних заходів безпеки. Оптимізація розміру буферної зони має враховувати ці аспекти, оскільки належна розробка та підтримка буферних механізмів напряду впливає на запобігання ризикам витоку чи пошкодження даних під

час їх оброблення або передачі. ISO/IEC 27002, у свою чергу, надає практичні рекомендації щодо заходів захисту, які можна застосовувати на різних етапах управління інформацією. Наприклад, для захисту конфіденційності та цілісності даних, що зберігаються або передаються, пропонується використовувати криптографічні методи, наприклад, шифрування або цифрові підписи. Це означає, що розмір буферної зони має відповідати вимогам криптографічних алгоритмів, які застосовують для захисту даних, оскільки недостатній або надмірний буфер може негативно вплинути на швидкість оброблення та забезпечення надійності цих алгоритмів (Iyer, & Desai, 2003; Razavi, Fleury, & Ghanbari, 2008; Wenlong et al., 2021; Smith, Johnson, & Lee, 2022; Doe, Patel, & Kim, 2023; Криворучко, Костюк, Ю. В., & Десятко, 2024).

Крім цього, відповідно до вимог стандартів, розмір буферної зони має бути достатнім для оброблення запитів у межах захищеного середовища, що враховує стратегії захисту від атак типу "відмова в обслуговуванні" (DoS) або втручання в буферний простір із метою компрометації системи (buffer overflow). Для таких атак важливо забезпечити наявність заходів контролю доступу та розподілу пам'яті, що мінімізує вразливості у буферній зоні та забезпечує стабільність і безпеку операцій. До того ж у сучасних умовах, із зростанням обсягів даних, що обробляються, все більшого значення набуває питання масштабованості й адаптивності буферної зони. Використання методів шифрування та захисту інформації має інтегруватися з можливостями автоматичного налаштування розміру буфера залежно від навантаження на систему й обсягу даних, що передаються. Це особливо важливо для хмарних технологій, де безпека даних та їхня конфіденційність повинні бути гарантовані на різних етапах передачі та зберігання, а також відповідати нормам захисту персональних даних, таким як Загальний регламент щодо захисту даних (GDPR) для Європейського Союзу. Отже, оптимізація розміру буферної зони повинна бути не лише технічним рішенням, але й відповідати сучасним вимогам інформаційної безпеки, враховуючи і стандарти ISO/IEC, й інші актуальні регламенти, що регулюють захист конфіденційних даних у цифровому середовищі (Razavi, Fleury, & Ghanbari, 2007; Smith, Johnson, & Lee, 2022; Chen, 2024; Chen et al., 2004; Kryvoruchko et al., 2024; Костюк, Ю. В., & Костюк Є. В., 2024; Scheiter et al., 2003).

У зв'язку з постійним розвитком технологій і загрозами безпеці, важливо постійно оновлювати методи оптимізації розміру буферної зони та вдосконалювати підходи до захисту інформації. Дослідження в цій сфері сприяє розробці нових технік і стратегій, які дозволять забезпечити найвищий рівень кібербезпеки та захисту інформації у суб'єктів господарювання. Зокрема, оптимізація розміру буферної зони, що забезпечує ефективне оброблення даних під час передачі в умовах змінного трафіка, є складним завданням, яке вимагає комплексного підходу та врахування різноманітних факторів, що впливають на безпеку й ефективність системи. Наприклад, у контексті Bluetooth-мереж, які є вразливими до перехресного трафіка, важливим є управління пріоритетом користувача (User Priority, UP). Це дозволяє віддавати перевагу певним типам трафіка, особливо мультимедійним даним, які є критично важливими для користувачів. Зазначимо, що впровадження сучасних моделей, таких як CQDDR (Channel



Quality Driven Data Rate), що адаптує швидкість передачі даних залежно від якості каналу, дозволяє підвищити надійність зв'язку. Використання сучасних методів аналізу та моделювання трафіка, таких як моделі AWGN (Additive White Gaussian Noise), дає змогу оцінити вплив шуму на якість передачі даних, що є особливо важливим в умовах нестабільності сигналу. Такі моделі сприяють оптимізації розмірів буферних зон, що, у свою чергу, покращує управління даними та зменшує ймовірність втрат пакетів. Отже, інтеграція різних підходів і технологій стає важливим етапом у досягненні високого рівня захисту інформації в Bluetooth-мережах (Zhang, Wang, & Chen, 2023; Костюк та ін., 2024; Rzaieva et al., 2024). З огляду на це в рамках оптимізації розміру буферної зони й управління пріоритетом користувача, варто зазначити, що комплексний аналіз трафіка та впровадження адаптивних механізмів управління можуть суттєво покращити якість обслуговування в умовах перехресного трафіка, що є критично важливим для забезпечення надійності та безпеки інформаційних систем у сучасному цифровому середовищі.

У дослідженні, що стосується відеопослідовності MPEG-2 з роздільною здатністю SIF (Standard Input Format), встановлено, що частота 25 кадрів на секунду та специфікація структури групи зображень (Group of Pictures, GOP), що включає $N = 12$ та $M = 3$, суттєво впливають на відносні розміри I -, P - та біпредиктивних B -кадрів. У цьому контексті N визначає кількість кадрів, що проходять між двома I -кадрами, тоді як M вказує на кількість кадрів, що з'являються перед наступним ключовим кадром, який може бути або I -кадром або P -кадром. Наприклад, коли $M = 3$, це означає, що перед кожним ключовим опорним кадром з'являються три інші кадри. Фактичний аналіз показав, що усереднення даних за GOP призводить до незначних змін у загальному зображенні, в той час як статичне співвідношення 6:3:2 для розмірів I -, P - та B -кадрів виявилось досить ефективним. Однак зауважимо, що відносний розмір P -кадрів і B -кадрів може варіюватися залежно від розміру I -кадрів, що вказує на необхідність адаптації методів оптимізації буферної зони й управління пріоритетом користувача в умовах перехресного трафіка. Зокрема й управління пріоритетом користувача (User Priority, UP) має важливе значення у контексті Bluetooth-мереж, оскільки дозволяє оптимізувати передачу даних, забезпечуючи пріоритет для мультимедійних потоків, які є критично важливими для користувачів. Використання адаптивних стратегій, що ґрунтуються на аналізі відносних розмірів кадрів, може покращити ефективність застосування буферної зони, запобігаючи затримкам у передачі даних під час пікових навантажень у мережі. Тому інтеграція знань про структуру кадрів MPEG-2, специфіку GOP та управління пріоритетами користувачів у Bluetooth-мережах може привести до значного покращення захисту інформації в умовах перехресного трафіка, що особливо важливо у сучасному цифровому середовищі, де зростає обсяг мультимедійних даних. Отже, реалізація комплексного підходу, що включає методи моделювання й адаптивного управління трафіком, є ключовим фактором у забезпеченні високої якості обслуговування та безпеки передачі даних.

Розглядаючи статичне співвідношення розмірів 6:3:2 між різними типами кадрів, доцільно звернути увагу на структуру групи зображень (Group of Pictures, GOP), що складається з параметрів $N = 12$ та $M = 3$. У цій структурі частота появи типів кадрів, зокрема I -,

P - та B -кадрів, перебуває у співвідношенні 1:3:8, що вказує на відносні пропорції їхньої присутності в потоці даних. З метою визначення оптимальних розмірів буферних зон, можна застосувати просте перемноження цих трьох співвідношень, що призведе до загального співвідношення 6:9:16 для буферних зон. Це співвідношення, у свою чергу, дозволяє здійснити ефективний розподіл пакетів у загальному буфері, місткість якого становить 50 пакетів, що дає змогу організувати їх у зонах відповідно до вищезгаданого співвідношення. В результаті такого розподілу, перша зона буде містити 25 пакетів, друга – 15, а третя – 10 пакетів, що забезпечує належну оптимізацію використання буферної зони й управління пріоритетом користувача (User Priority, UP). Це важливо, оскільки ефективне управління пріоритетами в умовах перехресного трафіка в Bluetooth-мережах дозволяє не тільки зберегти якість передачі даних, але й підвищити рівень захисту інформації. Оптимізація розміру буферної зони вимагає комплексного підходу, що включає аналіз структур кадрів, адаптацію їхніх пропорцій до специфіки даних, а також використання методів управління пріоритетами. Це, у свою чергу, сприяє покращенню якості обслуговування та забезпеченню безпеки інформаційних потоків у Bluetooth-мережах, де підвищена ймовірність виникнення перехресного трафіка може негативно вплинути на ефективність передачі даних. Отже, реалізація вказаних методів є критично важливою для успішного функціонування систем захисту інформації у сучасних умовах.

Розподіл зон у контексті оптимізації розміру буферної зони було скориговано за допомогою лінійного фільтра прогнозування P -порядку (Linear Predictive Filter, LPF), що дозволяє отримувати точніші дані про співвідношення між різними типами кадрів, які передають у Bluetooth-мережах. Причому фільтр восьмого порядку забезпечує надзвичайно малу різницю між прогнозованими та фактичними співвідношеннями, що свідчить про його високу ефективність у моделюванні потоку даних. Значення коефіцієнтів, отримані за допомогою фільтра P -порядку, визначено з урахуванням співвідношення між I -кадрами та P -кадрами, а також між P - та B -кадрами. I -кадри (інформаційні кадри) слугують ключовими точками у стисненні відео, оскільки містять повну інформацію про зображення, тоді як P -кадри (прогнозовані кадри) та B -кадри (біпредиктивні кадри) покладаються на дані з I -кадрів для забезпечення зменшення обсягу даних, що передаються. Отже, завдяки застосуванню методів лінійного прогнозування, стає можливим більш точне управління пріоритетами користувача (User Priority, UP) у системах Bluetooth, що в умовах перехресного трафіка є критично важливим для підтримання високої якості передачі даних і захисту інформації. Оптимізація розподілу зон і коригування співвідношення між різними типами кадрів не лише покращують ефективність використання буферної зони, але й підвищують рівень безпеки, що є важливим аспектом у сучасних умовах загроз кібербезпеці. Отже, реалізація таких методів, як лінійне прогнозування, в межах управління буферними зонами дозволяє забезпечити ефективніший контроль за трафіком, що, у свою чергу, сприяє безперебійному функціонуванню Bluetooth-мереж і захисту інформаційних потоків від можливих загроз. Це підкреслює важливість комплексного підходу до проблеми оптимізації безпеки інформації в умовах, що швидко змінюються, з урахуванням новітніх технологій



і стратегій. Лінійний фільтр прогнозування P -порядку представлено так:

$$X(m+1) = \sum_{k=1}^P w_k \cdot X(m-k+1), \quad (1)$$

де $X(m+1)$ – прогнозоване значення відношення, оцінене на основі попередніх значень P попередніх значень для вибірки m , тоді як w_k – це вагові коефіцієнти P адаптивних фільтрів, індексовані по k . Вагові коефіцієнти оцінюються за допомогою

$$w(m+1) = w(m) + \frac{e(m) \cdot X(m)}{\|X(m)\|^2}, \quad (2)$$

де W – вектор-стовпець довжини P вагових коефіцієнтів, X – вектор-стовпець довжини P вимірювань відношень у часі:

$$X(m) = [X(m), X(m-1), \dots, X(m-P+1)]^T, \quad (3)$$

тут T – транспонування вектора, змінна $e(m)$ відображає похибку між вимірним і прогнозованим значенням відношення. Систему ініціалізовано відношенням 6:3:2, яке раніше згадувалося як підходяще для відносних розмірів I-, P- і B-кадрів.

У сучасному стандарті MPEG-2 як I-кадри, так і P-кадри можуть містити внутрішньокеровані макроблоки, крім макроблоків предиктивного типу і SKIP, що не оновлюють відповідні макроблоки з попереднього кадру. Оскільки відповідні макроблоки в наступних кадрах залежать від цих макроблоків до приходу наступного I-кадру, важливо, щоб вони були доставлені

до декодера без пошкоджень (Iyer, & Desai, 2003; Wang et al., 2021; Chen, 2024; Костюк та ін., 2024; Chen et al., 2004; Криворучко, Костюк, Ю. В., & Десятко, 2024; Костюк, Ю. В., & Костюк, Є. В., 2024; Scheiter et al., 2003; Костюк та ін., 2024; Rzaieva et al., 2024). У сучасному алгоритмі буферної зони 2, для визначення розподілу внутрішньокерованих макроблоків, вибирається кожні M P-кадрів, де M є константою, що визначає частоту оновлення політики захисту. Політика захисту пакетів, яка застосовується до P-кадрів у зоні 2 буфера, коригується на основі розподілу макроблоків і поширюється на наступні M P-кадрів, що дозволяє адаптивно змінювати захисні механізми залежно від поточних характеристик потоку даних. Протягом виконання цієї політики кожен наступний кадр знову перевіряється на відповідність установленим правилам безпеки, що гарантує безперервний контроль якості захисту. Розмір $M = 100$ обрано з огляду на припущення, що характеристики відеопотоку залишаються стабільними та постійними протягом цього інтервалу часу, що дозволяє оптимізувати процес кодування та забезпечити ефективний контроль якості передачі даних. На рис. 1 зображено отриманий розподіл P-кадрів, який згруповано за десятьма категоріями, що використовуються в поточному алгоритмі, причому для демонстрації результатів у цьому прикладі застосовано 1000 P-кадрів замість стандартних 100, що дозволило детальніше відобразити закономірності в поведінці кадрів.

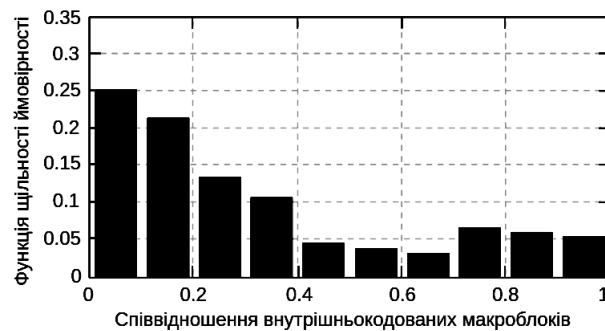


Рис. 1. Розподіл співвідношень внутрішньокерованих макроблоків P-кадрів

Функцію відображення, яка була отримана в результаті дослідження, зображено на рис. 2 для двох різних варіантів місткостей буферної зони 2. Вона квантується відповідно до накопиченої кількості пакетів, що відображені на горизонтальній осі, що дозволяє точно вимірювати взаємозалежність між заповненням

буфера та кількістю пакетів. Застосування цієї функції дає можливість лінійно коригувати кількість захищених пакетів P-кадрів залежно від поточного рівня заповнення буферної зони 2, що підвищує адаптивність системи в умовах змінного навантаження на мережу.

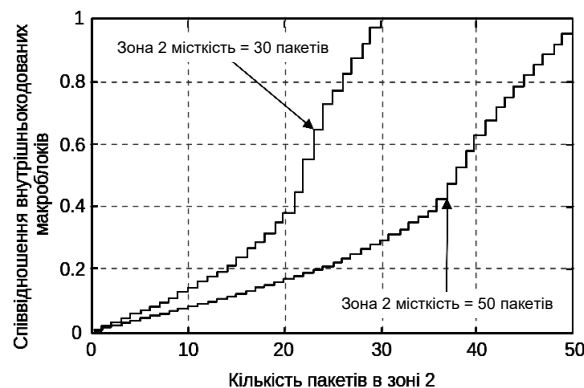


Рис. 2. Функція картографування захисту, яка заснована на двох різних буферах зони 2



Для визначення рівня захисту в зоні 2, місткість якої становить 50 пакетів, захисту підлягають лише ті Р-кадри, які містять більше ніж 62,4 % внутрішньо-

кодованих макроблоків, за умови, що в буфері перебуває не менше 40 пакетів.

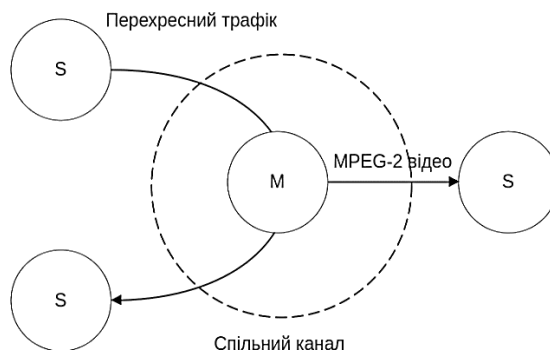


Рис. 3. Bluetooth-піконет із перехресним трафіком

У кожний момент часу, коли стає відомою поточна кількість пакетів у зоні 2 та співвідношення внутрішньокодovаних макроблоків у відповідному кадрі, система може оперативно прийняти рішення щодо необхідності захисту цього кадру. Формування функції відображення, яка показує взаємозв'язок між ймовірністю захисту та кількістю пакетів, відбувається за допомогою набору з десяти ймовірностей, як проілюстровано на рис. 2, де вони проєктуються на пропускну здатність буферної зони 2. Наприклад, у співвідношенні внутрішньокодovаних макроблоків 0,1 відповідна ймовірність захисту дорівнює приблизно 0,25, що означає виділення 13 пакетів ($0,25 \times 50$) для

захисту в буфері місткістю 50 пакетів. Подібні розрахунки здійснюються для наступної точки, де співвідношення макроблоків становить 0,2, а сукупна ймовірність зростає до 0,46 ($0,25+0,21$), що також продемонстровано на графіку рис. 2.

На рис. 3 показано конфігурацію моделювання, в якій відеопотік формату MPEG-2 передається з головного Bluetooth-вузла на підлеглий вузол S1, в той час як цей підлеглий виконує роль джерела трафіка для вузла S3. Важливо зазначити, що між підлеглими вузлами відсутня пряма комунікація, у зв'язку з чим головний вузол забезпечує створення окремих черг для кожної лінії зв'язку, що видно з рис. 4.

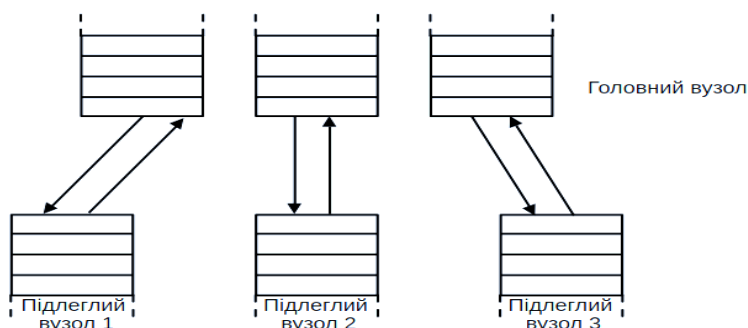


Рис. 4. Модель буфера для Bluetooth

Стандарт Bluetooth, хоч і не окреслює конкретної дисципліни обслуговування черг, за замовчуванням імплементує 1-обмежене циклічне планування, яке, як продемонстровано в численних наукових дослідженнях (Iyer, & Desai, 2003; Razavi, Fleury, & Ghanbari, 2008; Wenlong et al., 2021; Razavi, Fleury, & Ghanbari, 2007; Chen et al., 2004; Kryvoruchko et al., 2024), показує значну ефективність у сценаріях із високими навантаженнями, порівняно з дисципліною вичерпної черги. Це особливо актуально для середовищ, де інтенсивний трафік може призводити до затримок, що негативно впливають на загальну якість обслуговування. У зв'язку із цим, балансування навантаження та мінімізація затримок стають критично важливими для підтримки оптимального рівня якості сервісу, що, у свою чергу, особливо важливо в контексті сучасних мультимедійних додатків, таких як відеоконференції та потокове відео, які вимагають мінімальної затримки та високої пропускну здатності. З метою досягнення цих цілей необхідно приділяти особливу увагу аналізу різних метрик, що забезпечують моніторинг заторів у мережах Bluetooth. До таких метрик належать не лише традиційні показники втрат пакетів, але й параметри, що стосуються перехресного трафіка, який виникає, коли кілька джерел даних активно генерують трафік, а також самоперевантаження, що спостерігається, коли джерело трафіка генерує обсяги даних, які перевищують пропускну здатність каналу.

У процесі передачі інформації в мережах Bluetooth під час пікових навантажень виникають численні проблеми, які потребують уваги, зокрема й недостатня продуктивність процесорного блока мережного



пристрою, обмежена пропускна здатність вихідного інтерфейсу, а також зміни топології мережі, що відбуваються у процесі експлуатації та призводять до нерівномірного розподілу навантаження між центральними пристроями. У таких складних умовах оптимізація розміру буферної зони стає надзвичайно важливою для забезпечення стабільної передачі даних, оскільки неадекватний розмір буфера може призвести до втрат пакетів і збільшення затримок у передачі. Важливим аспектом цього процесу є адаптивне управління пріоритетом користувача, яке може суттєво зменшити затримки і покращити якість відеопотоку, що передається, що особливо актуально для мультимедійних додатків, які вимагають високої швидкості та надійності. Для досягнення цих цілей розроблення інтелектуальних алгоритмів, які враховують зміну трафіка і завантаження мережі, стає важливим аспектом забезпечення безперебійної передачі даних в умовах перехресного трафіка. Отже, ефективна оптимізація розміру буферної зони, разом із раціональним управлінням пріоритетами користувачів, здатна значно покращити якість передачі інформації та підвищити рівень безпеки даних у Bluetooth-мережах. Для моделювання процесу управління довжиною буферної черги пропонується використовувати диференціальні рівняння, оскільки цей підхід дозволяє дослідити динаміку зміни розміру буфера залежно від умов передачі даних, таких як швидкість передачі та затримки в мережі. Застосування диференціальних рівнянь у цій сфері може виявити оптимальні параметри управління буферизацією, що свою чергу, забезпечить ефективнішу передачу інформації, особливо в умовах перехресного трафіка. Це зменшить імовірність втрат даних і підвищить якість відеопотоку, що є критично важливим для безпечного обміну інформацією в Bluetooth-мережах.

$$y'(t) + \alpha p(t)y^2(t) = \beta R^{-1}(1 - p(t)), \quad (4)$$

де $y'(t)$ – швидкість передачі даних (пакети/с); $p(t)$ – функція ймовірності втрати пакетів; R – затримка (одиниця часу); α – параметр мультиплікативного зменшення розміру вікна передачі даних у разі втрати пакета; β – параметр адитивного збільшення розміру вікна за відсутності втрати пакетів.

У контексті оптимізації розміру буферної зони й управління пріоритетом користувача для захисту інформації в Bluetooth-мережах за умов перехресного трафіка важливе значення має рівняння Ріккати, яке, попри відсутність аналітичних розв'язків у квадратурах у загальному випадку, виступає потужним інструментом для опису критичних аспектів, таких як швидкість передачі даних, імовірність втрати пакетів, затримка та параметри управління вікном передачі. Це рівняння здатне враховувати динамічні зміни в мережній топології, які можуть суттєво впливати на загальну продуктивність системи, що є особливо важливим у контексті перехресного трафіка, де зміни можуть бути різкими та непередбачуваними. З метою отримання розв'язків цього рівняння в практичних застосуваннях пропонується використовувати чисельний метод Рунге – Кутти, який забезпечує високу точність обчислень у разі варіювання значень параметрів моделі. Використання цього методу є доцільним, оскільки в процесі моделювання трафіка бездротової мережі важливо врахувати можливість зміни топології, або, як ще кажуть, реконфігурації

мережі, що може відбуватися в реальному часі через різні фактори, такі як переміщення пристроїв, зміни навантаження або збої в роботі обладнання.

Отже, для досягнення оптимального вибору структури мережі необхідно задати оцінку ефективності передачі даних, що включає не лише аналіз основних показників, а й виявлення ключових аспектів, які впливають на якість обслуговування. Це може включати, наприклад, визначення оптимального розміру буферної зони, що дозволить зменшити ймовірність втрат даних під час передачі, а також налаштування параметрів управління пріоритетами, які, своєю чергою, можуть суттєво покращити загальний користувацький досвід під час використання мультимедійних сервісів, таких як потокове відео або відеоконференції. З огляду на це, об'єднання розглянутих аспектів підкреслює важливість комплексного підходу до дослідження й оптимізації мережі, що є критично важливим для забезпечення високої якості передачі даних і безпеки інформації в умовах перехресного трафіка. Використання рівняння Ріккати в комбінації з чисельними методами, такими як метод Рунге – Кутти, а також оцінювання ефективності передачі даних сприяють виробленню оптимальних рішень у сфері управління мережними ресурсами, що у свою чергу, покращує ефективність обслуговування користувачів і підвищує загальний рівень безпеки інформації у Bluetooth-мережах. Для цієї мети підходить співвідношення

$$E = \frac{W_k}{W_k + W_s}, \quad (5)$$

де W_k – кількість переданих корисних даних; W_s – кількість службової інформації. Цей підхід дозволяє забезпечити ефективнішу передачу даних у бездротових мережах, з урахуванням змін топології та оптимізації структури мережі.

Обсяг службового трафіка можна представити як функцію частоти реконфігурації мережі F_r і кількість вузлів nV_i у кластері V_0 :

$$W_s = f(F_r, V_0), \quad (6)$$

Тому для зменшення службового трафіка в мережі частота реконфігурацій за заданим проміжком часу ΔT та кількість кластерів мережі повинні бути зведені до мінімуму. Тоді оптимальний розмір мережі можна охарактеризувати за допомогою коефіцієнта k :

$$k = \frac{F_r \cdot V_0}{\Delta T}, \quad k \rightarrow \min, \quad (7)$$

Для перевірки отриманої моделі достатньо порівняти величину модельного трафіка зі значеннями, вибраними як еталон. Зручним інструментом для розв'язання цієї задачі може бути показник конкордації $p(t_k)$ модельних і еталонних значень трафіка на заданому часовому інтервалі:

$$p(t_k) = \frac{2 \cdot m(t_k) \cdot M(t_k)}{m(t_k)^2 + M(t_k)^2}, \quad (8)$$

де t_k – k -й момент часу контролю трафіка; $m(t_k)$ – математичне сподівання еталонного трафіка; $M(t_k)$ – математичне сподівання модельного трафіка.

У процесі оптимізації розміру буферної зони й управління пріоритетом користувача для захисту інформації в Bluetooth-мережах за умов перехресного трафіка важливо зазначити, що ефективність передачі



даних визначають відношенням між кількістю корисних і службових даних, що суттєво впливає на зменшення ймовірності втрат даних і підвищення якості відеопотоку. З метою досягнення зазначених цілей, пропонується мінімізувати частоту реконфігурацій мережі та кількість кластерів, оскільки саме ці фактори мають вирішальний вплив на обсяг службового трафіка, що генерується за передачі даних. Оптимальний розмір мережі можна охарактеризувати за допомогою спеціального коефіцієнта, який залежить від частоти реконфігурацій, кількості вузлів у кластері та заданого проміжку часу. Цей коефіцієнт дозволяє точніше налаштовувати параметри мережі для забезпечення високої продуктивності та стабільності у передачі даних. Для верифікації моделі, що описує вказану систему, необхідно порівняти модельний трафік з еталонними значеннями, що дає змогу оцінити її точність через показник конкордації. Отже, реалізація зазначених заходів забезпечує не лише надійність, а і якість обміну інформацією у Bluetooth-мережах, що є критично важливим для безпечної передачі даних у середовищі, де існує ризик перехресного трафіка. Використання статистичних методів для оцінювання ефективності передачі, а також обґрунтоване управління структурою мережі сприяє покращенню загального користувацького досвіду, зменшуючи ймовірність затримок і втрат даних, які можуть негативно вплинути на діяльність користувачів. Тому в межах дослідження оптимізації мережі варто враховувати цілий ряд факторів, включаючи не лише технічні параметри, а й вимоги до якості обслуговування, що також вплине на розроблення більш ефективних методів управління даними в умовах перехресного трафіка. Отже, комплексний підхід до аналізу й оптимізації системи може суттєво підвищити надійність і безпеку інформаційних потоків у Bluetooth-мережах, що є важливим аспектом у сучасному інформаційному середовищі.

У роботах (Wenlong et al., 2021; Razavi, Fleury, & Ghanbari, 2007; Smith, Johnson, & Lee, 2022; Doe, Patel, & Kim, 2023; Zhang, Wang, & Chen, 2023; Chen, 2024; Костюк та ін., 2024; Tahir et al., 2021) запропоновано динамічний метод контролю перевантаження, заснований на адаптивному регулюванні швидкості вхідних пакетів залежно від рівня втрат: якщо втрати залишаються нижчими за 5 %, швидкість передачі збільшується, а якщо рівень втрат перевищує 15 %, швидкість знижується. Проте за умови досягнення 10 % втрат, спостерігається значне погіршення якості відео, що є критичним для інтерактивних застосунків. У роботах (Chen et al., 2004; Ramana et al., 2009; Rzaieva et al., 2024; Костюк та ін., 2024) досліджувалася також затримка пакетів як індикатор перевантаження, що виявилось точнішим показником, ніж втрата пакетів, особливо для Bluetooth-зв'язків. Однак використання цього показника як зворотного зв'язку для контролю перевантаження спричиняло коливання якості відео та затримки пакетів, що призводило до нестабільності в роботі мережі. Сучасні дослідження у цій сфері зосереджено на вдосконаленні алгоритмів адаптивного управління трафіком, з урахуванням інтелектуальні механізми прогнозування заторів і використання машинного навчання для оптимізації розподілу ресурсів у мережах Bluetooth. Це дозволяє забезпечити не лише стабільну продуктивність, але й адаптацію системи до зміни умов навантаження в реальному часі, що є важливим кроком у напрямку

підвищення ефективності роботи сучасних безпроводних мереж, особливо в умовах інтенсивного мультимедійного трафіка.

З іншого боку, буфер здатний відстежувати зміни і в прямому, і в перехресному трафіку. У дослідженні (Smith, Johnson, & Lee, 2022; Doe, Patel, & Kim, 2023; Zhang, Wang, & Chen, 2023; Chen, 2024; Chen et al., 2004; Костюк та ін., 2024) також підтверджено, що моніторинг заповненості буферів значно зменшує затримку та покращує PSNR у разі застосування контролю перевантажень. Графік швидкості відео-трафіка демонструє фіксований перехресний трафік із постійною швидкістю передачі даних (CBR) на рівні 200 кбіт/с і розмір пакета 800 Б. Важливо зазначити, що це означає ефективну швидкість передачі даних 400 кбіт/с через спільний канал, оскільки трафік із постійною швидкістю проходить через два переходи до місця призначення (Chen et al., 2004; Kryvoruchko et al., 2024; Костюк та ін., 2024; Scheiter et al., 2003; Костюк та ін., 2024). Крім того, розмір пакета призводить до неоптимального використання пропускну здатності каналу. Джерелом відеотрафіка є 40-секундний MPEG2 CIF новинний кліп (з помірним рухом) із частотою кадрів 25 кадрів/с та структурою GOP $N = 12$ та $M = 3$, з повністю заповненими пакетами. Коли швидкість даних перетинає поріг близько 1,6 Мбіт/с, заповненість буферів різко зростає, оскільки швидкість насичення Bluetooth-з'єднання 2,1 Мбіт/с наближається до максимальної. Аналогічно, у разі фіксованої швидкості джерела MPEG2 на рівні 1,25 Мбіт/с, спостерігається різке збільшення заповнення буфера, коли швидкість CBR наближається до максимальної пропускну здатності каналу.

Оптимізація розміру буферної зони дозволяє уникнути перевантаження буфера, яке може призвести до втрати пакетів або зниження якості відеопотоку. Неправильно налаштована буферна зона може або занадто швидко заповнитися, що призведе до переповнення і втрати даних, або залишатися надто малою, що призведе до затримок і нестабільності в передачі. Збалансований розмір буфера дає змогу ефективно управляти потоками даних, забезпечуючи стабільний рівень якості сервісу і мінімізуючи вплив на затримки передачі, що є критично важливим для відеопотоків у реальному часі. У мережах Bluetooth застосовують адаптивну модуляцію, яка дозволяє змінювати швидкість передачі даних залежно від умов мережі, таких як інтерференція, віддаленість пристроїв або наявність перехресного трафіка. Використання тризонного буфера дозволяє розподілити вхідний потік даних на три зони (напр., низького, середнього та високого пріоритету), що забезпечує кращий контроль над трафіком. Кожна зона буфера обробляє потоки даних із різними характеристиками та вимогами до затримки і втрат. Це підвищує ефективність захисту, оскільки дані різних типів обробляються відповідно до їхнього пріоритету та чутливості до втрат і затримок. Одним із ключових завдань буферизації в Bluetooth-мережах є захист від загроз, пов'язаних із переповненням буфера та втратою критично важливих даних. Буферна зона може стати мішенню для атак типу Denial-of-Service (DoS) або Buffer Overflow, коли злоумисник намагається перевантажити систему, що призводить до відмови в обслуговуванні або викрадення даних. Оптимізований буфер з адаптивною модуляцією може динамічно коригуватися залежно від загроз або змін у трафіку, що дозволяє підтримувати



захист даних на високому рівні навіть під час атак. Сучасні алгоритми оптимізації буфера можуть використовувати зворотний зв'язок від приймача для адаптації розміру буферної зони в реальному часі. Це важливо в умовах змінних мережних параметрів, коли швидкість передачі даних та якість сигналу можуть значно коливатися. Якщо система виявляє збільшення затримки або втрат пакетів, вона може відповідно змінити розмір буфера, щоб запобігти подальшим проблемам. Такий підхід підвищує гнучкість і ефективність системи захисту відеопотоку. За підвищеної швидкості передачі даних, характерній для сучасних Bluetooth-мереж, буфер виконує функцію згладжування пікових навантажень і мінімізації втрат пакетів. Завдяки правильному налаштуванню буфера, відеодані можуть передаватися з мінімальними втратами, що є важливим для підтримки високої якості відеопотоку, особливо під час відеоконференцій або потокового передавання мультимедіа в режимі реального часу.

Управління пріоритетом користувача та захист інформації в умовах відсутності та наявності перехресного трафіка є невід'ємною частиною стратегії забезпечення безпеки відеопотоку через безпроводну мережу Bluetooth. Сучасні технології та підходи до управління безпекою вимагають уваги до динамічних умов мережного середовища та постійного розвитку загроз. З одного боку, в умовах відсутності перехресного трафіка, управління пріоритетом користувача може бути спрощеним, оскільки мережа має більшу пропускну здатність і менші ймовірності конфліктів ресурсів. Проте це не означає, що заходами безпеки можна знехтувати. Навпаки, навіть за відсутності перешкод, важливо забезпечити конфіденційність даних і захист від можливих атак. З іншого боку, у присутності перехресного трафіка управління пріоритетом користувача стає складнішим завданням. Це вимагає розроблення алгоритмів і механізмів, які дозволять ефективно реагувати на зміни у мережному середовищі та на рівні перешкод. Сучасні рішення включають інтелектуальне призначення пріоритетів, адаптивне керування ресурсами та застосування розумних алгоритмів буферизації. Усі ці заходи спрямовані на забезпечення безпеки відеопотоку через безпроводну мережу Bluetooth із підвищеною швидкістю передачі даних за допомогою адаптивної модуляції з тризонним буфером (Ramana, et al., 2009; Rzaieva et al., 2024; Костюк та ін., 2024; Chia, & Beg, 2003). Розвиток і вдосконалення таких стратегій стають ключовими у забезпеченні надійності й конфіденційності передачі відеоданих в сучасному цифровому середовищі.

Під час аналізу ділянок без коригування буферів, встановлено статичні межі між зонами відповідно до співвідношення розмірів 6:3:2, де застосовано лінійну функцію відображення UP (пріоритет користувачів), замість нелінійної функції. Водночас для областей із коригуванням буфера зони були встановлені відповідно до фактичного співвідношення розмірів між типами кадрів, усередненого за послідовністю (Smith, Johnson, & Lee, 2022; Doe, Patel, & Kim, 2023; Zhang, Wang, & Chen, 2023; Криворучко, Костюк, Ю. В., & Десятко, 2024; Костюк, Ю. В., & Костюк, Є. В., 2024; Scheiter et al., 2003). Аналіз показав, що у разі статичного графіка меж зони справджується менша загальна пропускна здатність, оскільки захищається занадто багато пакетів, що може призвести до більшої втрати пакетів через переповнення буфера для певних типів перехресного трафіка. З іншого боку, якщо

політика відсутності коригування буфера була застосована до налаштувань меж контрольованої зони, то це могло б призвести до припливу пакетів Р-кадрів із вищою швидкістю передачі даних, збільшення кількості пакетів із помилками і, як наслідок, до зниження якості отриманого відео. Отже, регулювання буфера впливає на якість передачі даних і безпеку інформації, а оптимізація цього процесу важлива для забезпечення ефективної захищеності й надійності мережі.

Варто зазначити, що загальна пропускна здатність у статичних межах зони менша, ніж у разі регулювання буфера та встановлення контрольованої межі. Це означає, що захищається занадто багато пакетів, що може призвести до втрати пакетів через переповнення буфера для певних типів перехресного трафіка. З іншого боку, відсутність коригування буфера може призвести до припливу пакетів Р-кадрів із вищою швидкістю передачі даних, що також збільшує кількість пакетів із помилками та знижує якість отриманого відео.

Перехресний трафік застосовують відповідно до сценарію, тоді як послідовність новинних кліпів формує відеопотік MPEG2. У контексті цього дослідження використано як одностаціонарну, так і двостаціонарну моделі шуму. Під час першої серії симуляцій перехресний трафік був статичним CBR зі швидкістю 200 кбіт/с та розміром пакета 800 Б, а транспортним протоколом для CBR було обрано UDP. PSNR використовують як об'єктивну метрику для оцінювання якості відео, з рівнем близько 40 дБ, що вважається відмінним для мобільного зв'язку, та рівні нижче 25 дБ, які ймовірно є непридатними для перегляду. Для детальнішого порівняння якості відео у бездротовому зв'язку можна звернутися до джерел (Chen et al., 2004; Криворучко, Костюк, Ю. В., & Десятко, 2024; Rzaieva et al., 2024). Початкова модель шуму в каналі використовувала одностаціонарну модель. Застосовано як динамічну зміну меж зони, так і регулювання буфера зони 2. Коли всі пакети захищено на радіочастотному каналі, спостерігається помітне покращення якості відео, яке виявляється і як загальний рівень PSNR, і як флуктуація якості. Падіння якості пов'язане з втратою пакетів через переповнення буфера. Початковий сплеск якості прийому відео на рівні 40 дБ пояснюється відсутністю активації джерела CBR до закінчення цього періоду. Хоча візуально складніше розрізнити початковий сплеск якості прийому відео, узагальнені результати демонструють перевагу UP (пріоритет користувачів) з адаптивною модуляцією.

В межах оптимізації розміру буферної зони й управління пріоритетом користувача для захисту інформації в Bluetooth-мережах за умов перехресного трафіка важливо звернути увагу на аспекти, пов'язані з моделями шуму каналу. Однією з таких моделей є AWGN (Additive White Gaussian Noise), яка використовується для оцінювання впливу шуму на передачу даних у каналах зв'язку. Ця модель дозволяє краще зрозуміти складність умов передачі, зокрема і в умовах змінного трафіка. Для точнішого опису умов передачі даних було проведено оновлення моделі шуму, що дало змогу перейти до двостаціонарної моделі. Це уможливило детальний аналіз, зокрема і порівняння з моделлю CQDDR (Channel Quality Driven Data Rate). CQDDR адаптує швидкість передачі даних залежно від якості каналу, забезпечуючи ефективну передачу в умовах змінного трафіка. У застосуванні схеми UP (User Priority), важливого аспекту управління,



відзначено, що якість відеопотоку протягом часу не зазнає різких змін, що є критично важливим для споживачів мультимедійного контенту. Виявлено, що падіння якості через втрату пакетів є серйознішим порівняно з одностадійним каналом AWGN. Це свідчить про складні умови функціонування Bluetooth-мережі, особливо за високих рівнів шуму і швидкості передачі 3 Мбіт/с, коли спостерігається значне падіння якості відео, що підкреслює необхідність адаптивного управління параметрами передачі. Хоча модель CQDDR забезпечує покращення порівняно з політикою єдиної швидкості передачі, середня якість відео в цій схемі залишається нижчою, ніж у схемі UP. Це підкреслює важливість адаптивної модуляції з керуванням буфером, оскільки вона здатна забезпечити вищу якість відео, зменшуючи втрати пакетів, які виникають через радіочастотні перешкоди під час передачі даних. У моделі з двома станами втрати пакетів на швидкості 3 Мбіт/с зростають через збільшення ймовірності помилок у каналі, що підтверджує важливість ретельного управління трафіком. З огляду на ці фактори, для передачі відео схема UP виявилася вигіднішою, оскільки вона ефективно враховує вміст пакетів і умови трафіка, підвищуючи загальну якість обслуговування. Використання адаптивної модуляції в комбінації зі схемою UP забезпечує баланс між різними вимогами, що дозволяє вибрати оптимальний підхід для різних сценаріїв передачі даних. Отже, підходи до управління якістю передачі у Bluetooth-мережах за умов перехресного трафіка потребують комплексного аналізу й інтеграції різних моделей, що дозволить підвищити надійність та ефективність обміну інформацією. Важливим є акцент на адаптивних стратегіях, які забезпечують безпеку та якість мультимедійних сервісів у бездротових мережах, що є критично важливим у сучасному інформаційному середовищі (Iyer, & Desai, 2003; Wenlong et al., 2021; Doe, Patel, & Kim, 2023; Zhang, Wang, & Chen, 2023; Костюк, Ю. В., & Костюк Є. В., 2024).

Щодо заповненості буферів під час симуляції перехресного трафіка CBR, виявлено, що з використанням схеми UP заповненість буфера вирівнюється до постійного рівня протягом 6 с, перевищуючи 50-пакетну місткість буфера на більш як 10 пакетів. За загальної швидкості 2 Мбіт/с та SNR на рівні 16 дБ втрата пакетів через радіочастотні перешкоди мінімальна, однак, захищені пакети також можуть бути втрачені через близькість до місткості буфера. Нарешті, навіть за передачі всіх пакетів на найвищій швидкості без UP ризик втрати пакетів через переповнення буфера відсутній, проте втрата пакетів усе ще відбувається через радіочастотні перешкоди. Отже, для ефективного управління трафіком і забезпечення найвищої якості відео варто розглядати використання UP з адаптивною модуляцією, яка дозволяє вирівняти ці дві протилежності та забезпечити оптимальну продуктивність системи (Zhang, Wang, & Chen, 2023; Chen, 2024; Костюк та ін., 2024; Chen et al., 2004; Костюк, Ю. В., & Костюк Є. В., 2024).

Аналіз заповненості буферів під час моделювання перехресного трафіка CBR вказує на те, що за швидкості передачі даних 3 Мбіт/с буфер усе ще залишається недозаповненим без загрози переповнення, що підтверджує залежність падіння якості відео на цій швидкості від втрати пакетів через радіочастотні перешкоди. Як для схеми адаптивної модуляції UP, так

і для схеми CQDDR спостерігається можливість втрати пакетів через переповнення буфера в умовах поганої пропускної здатності каналу. Проте схема CQDDR виявляє тенденцію вибирати вищу брутто-швидкість 3 Мбіт/с, що призводить до розрядження буфера, але збільшує ризик втрати більш важливих пакетів, таких як ключові кадри. Це пояснює нижчу якість відео, збереженого за допомогою схеми CQDDR. Для додаткового оцінювання впливу умов каналу значення BER для брутто-швидкості 3 Мбіт/с у поганому стані двоканальної моделі Гілберта – Елліотта змінювалися від $i \cdot 10^{-4}$, де $i = 1, 2, 3, 4, 5$, а інші параметри моделі залишалися незмінними. Для відео Newsclip середнє значення PSNR погіршується зі збільшенням BER, як можна було очікувати. Режим із швидкістю передачі даних 3 Мбіт/с виявляв більшу схильність до втрат пакетів через радіочастотні завади порівняно з режимом із швидкістю 2 Мбіт/с. Вища ефективність схеми адаптивної модуляції UP порівняно з CQDDR підтверджується на всьому спектрі значень BER (Костюк та ін., 2024; Chia, & Beg, 2003; Sabeen et al., 2021).

Моделювання впливу збільшення інтенсивності фонового трафіка CBR є важливим аспектом досліджень у сфері кібербезпеки та захисту інформації. У разі збільшення швидкості CBR спостерігається зближення якості переданого відео між схемами адаптивної модуляції UP і CQDDR. Це пояснюється зростанням ймовірності втрати пакетів через переповнення буфера у схемі UP, що особливо актуально для швидкості 2 Мбіт/с (Razavi, Fleury, & Ghanbari, 2007; Doe, Patel, & Kim, 2023; Костюк та ін., 2024; Scheiter et al., 2003; Костюк, & Костюк 2024; Ramana et al., 2009). Зменшення швидкості обслуговування буфера відправлення у зв'язку з наявністю CBR-пакетів призводить до відкидання більшої кількості пакетів, що призводить до швидкого погіршення якості відео. До того ж у процесі збільшення заповнення буфера менше пакетів може бути захищено схемою UP, що збільшує наближення продуктивності схеми UP до схеми CQDDR.

Результати порівняння показали, що менші втрати відбуваються через переповнення буфера за швидкості 2 Мбіт/с у присутності вебтрафіка. Додатково, результати для інших відеопослідовностей були включені для демонстрації універсальності отриманих результатів (Chen et al., 2004; Костюк, Ю. В., & Костюк Є. В., 2024; Scheiter et al., 2003; Костюк та ін., 2024). Порівняння також вказало на погіршення середнього PSNR у сценаріях з двома станами каналу, але залишило UP кращою за CQDDR щодо якості передачі відео.

Дослідження підтверджує, що адаптивні схеми мають перевагу перед фіксованими, особливо у випадках несприятливих умов передачі даних. Наприклад, нерівномірний захист у потоковому передаванні даних через Bluetooth приводить до покращення якості відео порівняно з фіксованими схемами. Такі дослідження дають підстави для вдосконалення методів захисту даних у різних умовах передачі.

Дискусія і висновки

Оптимізація розміру буферної зони у Bluetooth-мережах є важливою складовою забезпечення надійної і безперебійної передачі відеоданих, оскільки правильне налаштування буферних параметрів не тільки покращує загальну ефективність оброблення трафіка, але і знижує вразливість системи до зовнішніх загроз, таких як перехресний трафік або мережні атаки, спрямовані на порушення конфіденційності чи



доступності даних. Важливість цього процесу зумовлена тим, що він дозволяє запобігти перевантаженням мережних ресурсів, спричиненим великою кількістю одночасно переданих даних, що, своєю чергою, забезпечує підтримку безперервного потоку інформації без значних затримок або втрат даних.

Застосування технології адаптивної модуляції у контексті управління Bluetooth-мережами є особливо актуальним, оскільки цей метод дозволяє автоматично налаштовувати параметри модуляції залежно від поточних умов каналу зв'язку, таких як швидкість передачі, рівень шумів та інших можливих перешкод. Це дає змогу підтримувати стабільність і надійність передачі відеопотоків навіть за умов змінних параметрів середовища, в якому працює мережа. Здатність мережі динамічно адаптуватися до змінних умов, зокрема і в умовах підвищеної перехресної інтерференції, суттєво підвищує рівень безпеки переданої інформації, знижуючи ризики можливих атак, що можуть виникати через несанкціонований доступ до переданих даних.

Додаткову надійність у процесі передачі даних забезпечує тризонний буфер, який розподіляє потік інформації на три етапи зберігання та попереднього оброблення. Така багаторівнева структура дозволяє не тільки мінімізувати ризик затримок або втрат інформації, але й ефективно захистити систему від зовнішніх факторів, наприклад, від раптових змін у навантаженні на мережу або несприятливих умов передачі даних. Використання буферних механізмів із кількома рівнями захисту підвищує загальну стійкість системи до збоїв, спричинених інтерференцією або перехресними перешкодами, тим самим гарантує стабільну роботу мережі в умовах змінюваних параметрів каналу зв'язку та різного рівня трафіка.

Отже, інтеграція адаптивної модуляції сигналу з тризонним буфером дозволяє оптимізувати управління ресурсами у Bluetooth-мережах так, що передача відеоданих відбувається з максимально можливою якістю і мінімальними затримками, забезпечуючи водночас високий рівень захисту інформації навіть за умов значної варіативності параметрів каналу зв'язку, що особливо важливо у сучасних умовах активного використання бездротових мереж для передавання конфіденційної інформації.

Перспективою подальшого дослідження буде поглиблення впливу адаптивних методів управління трафіком у Bluetooth-мережах на ефективність передачі даних за умов високого навантаження та перехресного трафіка. Додатково до цього, важливим аспектом дослідження стане оцінювання впливу зовнішніх факторів, таких як радіочастотні інтерференції або зміни середовища, на продуктивність системи, а також пошук оптимальних рішень для мінімізації цих впливів.

Внесок авторів: Юлія Костюк – концептуалізація, методологія, аналіз джерел, підготування огляду літератури; Богдан Бебешко – збір емпіричних даних та їхня валідація; Павло Складанний – емпіричне дослідження, розробка рекомендацій, практичне застосування отриманих результатів, формулювання перспектив для подальших досліджень; Світлана Рзаєва – оцінка ефективності запропонованих рішень, аналіз ризиків; Карина Хорольська – формулювання загальних висновків.

Список використаних джерел

Костюк, Ю. В., & Костюк Є. В. (2024). Вдосконалені методи безпеки в 4G мережах з метою забезпечення ефективного захисту від атак на передачу даних. *Наука і техніка сьогодні*, 6(34), 789–807. [https://doi.org/10.52058/2786-6025-2024-7\(35\)-789-804](https://doi.org/10.52058/2786-6025-2024-7(35)-789-804)

Костюк, Ю. В., & Шапран, В. О. (2024). Технології виявлення аномальних подій та сигнатур в реальному часі. *Наука і техніка сьогодні*, 4(32), 1069–1084. [https://doi.org/10.52058/2786-6025-2024-4\(32\)-1069-1084](https://doi.org/10.52058/2786-6025-2024-4(32)-1069-1084)

Костюк, Ю. В., Бебешко, Б. Т., Крючкова, П. П., Литвинов, В. Д., Оксанич, І. Г., Складанний, П. М., & Хорольська, К. В. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. *Кибербезпека: освіта, наука, техніка*, 1(25), 229–252. <https://doi.org/10.28925/2663-4023.2024.25.229252>

Криворучко, О. І., Костюк, Ю. В., & Десято, А. (2024). Систематизація ознак несанкціонованого доступу до корпоративної інформації на основі застосування методів криптографічного захисту. *Ukrainian Scientific Journal of Information Security*, 30(1), 140–149.

Chen, L. (2024). Impact of cross-traffic on bandwidth and video quality in Bluetooth networks. *Telecommunications Systems*, 77(1), 67–82. <https://doi.org/10.1007/s11235-023-00789-6>

Chen, L.-J., Kapoor, R., Sanadidi, M. Y., Lee, R., & Gerla, M. (2004). Audio streaming over Bluetooth: An adaptive ARQ timeout approach. In *Proceedings of the Conference: 24th International Conference on Distributed Computing Systems Workshops (ICDCS 2004 Workshops)*, 23–24 March 2004 (pp. 196–201). Hachioji, Tokyo, Japan, 24.

Chia, C. H., & Beg, M. S. (2003). Realizing MPEG-4 video transmission over wireless Bluetooth link via HCL. *IEEE Transactions on Consumer Electronics*, 49(4), 1028–1034. <https://ieeexplore.ieee.org/document/1261191>

Doe, J., Patel, R., & Kim, S. (2023). User priority management for critical data transmission in Bluetooth networks. *International Journal of Network Management*, 33(4), e2178. <https://doi.org/10.1002/nem.2178>

Iyer, A., & Desai, U. (2003). A comparative study of video transfer over Bluetooth and 802.11 wireless MAC. In *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC '03)*, 3 (pp. 2053–2057). IEEE.

Razavi, R., Fleury, M., & Ghanbari, M. (2007). Low-delay video control in a personal area network for augmented reality. In *Proceedings of the 4th Visual Information Engineering* (pp. 1245–1300). The institution of engineering and technology.

Rzaieva, S., Rzaiev, D., Kostiuk, Y., Hulak, H., & Shcheblanin, O. (2024). Methods of modeling database system security. In *Proceedings of CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems* (pp. 384–390). CEUR Workshop Proceedings (CEUR-WS.org).

Razavi, R., Fleury, M., & Ghanbari, M. (2008). Power-constrained fuzzy logic control of video streaming over a wireless interconnect. *EURASIP Journal on Advances in Signal Processing*, 1–14. <https://doi.org/10.1155/2008/560749>

Scheiter, C., Steffen, R., Zeller, M., Knorr, R., Stabernack, B., & Wels, K.-W. (2003). A system for QoS-enabled MPEG-4 video transmission over Bluetooth for mobile applications. In *Proceedings of International Conference on Multimedia and Expo (ICME '03)*, 1 (pp. 789–792).

Smith, A., Johnson, B., & Lee, C. (2022). Dynamic buffer management for video streaming in wireless networks. *Journal of Wireless Communications and Networking*, 2022(15), 235–250. <https://doi.org/10.1007/s11276-022-03425-5>

Tahir, S., Aldabbagh, G. A., Bakhsh, S. T., & Said, A. M. (2021). Hybrid congestion sharing and route repairing protocol for Bluetooth networks. *WSEAS Transactions on Computers*, 49–55. <https://doi.org/10.37394/23205.2021.20.6>

Wenlong, W., Chunhua, Z., Zilong, C., & Shuai, L. (2021). Mobile node design of indoor positioning system based on Bluetooth and LoRa network. *Journal of Physics*, 1738(1), 1–4. <https://doi.org/10.1088/1742-6596/1738/1/012092>

Zhang, M., Wang, Y., & Chen, T. (2023). Security considerations in adaptive buffer management strategies. *Information Systems Security*, 32(2), 123–139. <https://doi.org/10.1080/15504816.2023.1234567>

References

Chen, L. (2024). Impact of cross-traffic on bandwidth and video quality in Bluetooth networks. *Telecommunications Systems*, 77(1), 67–82. <https://doi.org/10.1007/s11235-023-00789-6>

Chen, L.-J., Kapoor, R., Sanadidi, M. Y., Lee, R., & Gerla, M. (2004). Audio streaming over Bluetooth: An adaptive ARQ timeout approach. In *Proceedings of the Conference: 24th International Conference on Distributed Computing Systems Workshops (ICDCS 2004 Workshops)*, 23–24 March 2004 (pp. 196–201). Hachioji, Tokyo, Japan, 24.

Chia, C. H., & Beg, M. S. (2003). Realizing MPEG-4 video transmission over wireless Bluetooth link via HCL. *IEEE Transactions on Consumer Electronics*, 49(4), 1028–1034. <https://ieeexplore.ieee.org/document/1261191>

Doe, J., Patel, R., & Kim, S. (2023). User priority management for critical data transmission in Bluetooth networks. *International Journal of Network Management*, 33(4), e2178. <https://doi.org/10.1002/nem.2178>

Iyer, A., & Desai, U. (2003). A comparative study of video transfer over Bluetooth and 802.11 wireless MAC. In *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC '03)*, 3 (pp. 2053–2057). IEEE.

Kostiuk, Y. V., & Kostiuk, Y. V. (2024). Enhanced security methods in 4G networks to ensure effective protection against data transmission attacks. *Science and Technology Today*, 6(34), 789–807 [in Ukrainian]. [https://doi.org/10.52058/2786-6025-2024-7\(35\)-789-804](https://doi.org/10.52058/2786-6025-2024-7(35)-789-804)



Kostiuk, Y. V., & Shapran, V. O. (2024). *Technologies for detecting anomalous events and signatures in real-time*. *Science and Technology Today*, 4(32), 1069–1084 [in Ukrainian]. [https://doi.org/10.52058/2786-6025-2024-4\(32\)-1069-1084](https://doi.org/10.52058/2786-6025-2024-4(32)-1069-1084)

Kostiuk, Y. V., Bebesko, B. T., Kryuchkova, L. P., Lytvynov, V. D., Oksanych, I. H., Skladannyi, P. M., & Khorolska, K. V. (2024). Information protection and data exchange security in wireless mobile networks with authentication and key exchange protocols. *Cybersecurity: Education, Science, Technology*, 1(25), 229–252 [in Ukrainian]. <https://doi.org/10.28925/2663-4023.2024.25.229252>

Kryvoruchko, O. I., Kostiuk, Y. V., & Desiatko, A. (2024). Systematization of signs of unauthorized access to corporate information based on the application of cryptographic protection methods. *Ukrainian Scientific Journal of Information Security*, 30(1), 140–149 [in Ukrainian].

Razavi, R., Fleury, M., & Ghanbari, M. (2007). Low-delay video control in a personal area network for augmented reality. In *Proceedings of the 4th Visual Information Engineering* (pp. 1245–1300). The institution of engineering and technology.

Rzaieva, S., Rzaiev, D., Kostiuk, Y., Hulak, H., & Shcheblanin, O. (2024). Methods of modeling database system security. In *Proceedings of CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems* (pp. 384–390). CEUR Workshop Proceedings (CEUR-WS.org).

Razavi, R., Fleury, M., & Ghanbari, M. (2008). Power-constrained fuzzy logic control of video streaming over a wireless interconnect. *EURASIP Journal on Advances in Signal Processing*, 1–14. <https://doi.org/10.1155/2008/560749>

Scheiter, C., Steffen, R., Zeller, M., Knorr, R., Stabernack, B., & Wels, K.-W. (2003). A system for QoS-enabled MPEG-4 video transmission over Bluetooth for mobile applications. In *Proceedings of International Conference on Multimedia and Expo (ICME '03)*, 1 (pp. 789–792).

Smith, A., Johnson, B., & Lee, C. (2022). Dynamic buffer management for video streaming in wireless networks. *Journal of Wireless Communications and Networking*, 2022(15), 235–250. <https://doi.org/10.1007/s11276-022-03425-5>

Tahir, S., Aldabbagh, G. A., Bakhsh, S. T., & Said, A. M. (2021). Hybrid congestion sharing and route repairing protocol for Bluetooth networks. *WSEAS Transactions on Computers*, 49–55. <https://doi.org/10.37394/23205.2021.20.6>

Wenlong, W., Chunhua, Z., Zilong, C., & Shuai, L. (2021). Mobile node design of indoor positioning system based on Bluetooth and LoRa network. *Journal of Physics*, 1738(1), 1–4. <https://doi.org/10.1088/1742-6596/1738/1/012092>

Zhang, M., Wang, Y., & Chen, T. (2023). Security considerations in adaptive buffer management strategies. *Information Systems Security*, 32(2), 123–139. <https://doi.org/10.1080/15504816.2023.1234567>

Отримано редакцією журналу / Received: 17.09.24

Прорецензовано / Revised: 15.10.24

Схвалено до друку / Accepted: 30.11.24

Yuliia KOSTIUK¹, PhD
ORCID ID: 0000-0001-5423-0985
e-mail: y.kostiuk@kubg.edu.ua

Bohdan BEBESHKO¹, PhD
ORCID ID: 0000-0001-6599-0808
e-mail: b.bebeshko@kubg.edu.ua

Pavlo SKLADANNYI¹, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0002-7775-6039
e-mail: p.skladannyi@kubg.edu.ua

Svitlana RZAEVA¹, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0002-7589-2045
e-mail: s.rzaieva@kubg.edu.ua

Karyna KHOROLSKA¹, PhD
ORCID ID: 0000-0003-3270-4494
e-mail: karynakhorolska@gmail.com

¹ Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine

OPTIMIZATION OF BUFFER AND PRIORITIES FOR ENSURING SECURITY IN BLUETOOTH NETWORKS

Background. The optimization of buffer zone size for information protection plays a crucial role in ensuring the security of video streaming over Bluetooth wireless networks, particularly given the increased data transmission speeds and the use of adaptive modulation with a three-tier buffer. Recent studies show that proper management of buffer size can significantly enhance the quality of video data transmission and reduce security threats. An important aspect of ensuring security in video streaming systems over wireless networks like Bluetooth is the integration of cutting-edge information protection technologies. Modern trends in cybersecurity encompass key elements such as data encryption, access control, and multi-factor user authentication. These mechanisms not only protect data from unauthorized access but also ensure its integrity and confidentiality at every stage of processing and transmission.

Methods. The study employed analytical methods including modeling and simulation, statistical and comparative analysis, experimental research, and risk assessment, enabling a comprehensive understanding of data transmission quality management in Bluetooth networks under cross traffic conditions.

Results. Properly configuring the buffer zone size can significantly enhance the efficiency and reliability of protecting critical data from unauthorized access and cyberattacks. Modern approaches to buffer size optimization utilize traffic analysis and modeling methods, as well as machine learning algorithms to predict traffic volumes and characteristics. For instance, clustering algorithms can be employed to identify traffic types and characteristics, allowing for more efficient resource allocation and buffer space management. To effectively optimize the buffer zone size, it is essential to consider system performance and information security standards, including ISO/IEC 27001 and ISO/IEC 27002. ISO/IEC 27001 outlines requirements for information security management systems, emphasizing risk assessment and the implementation of security measures. ISO/IEC 27002 provides recommendations for data protection, such as the use of cryptographic methods. The buffer zone size must meet the requirements of cryptographic algorithms and ensure resilience against attacks such as DoS and buffer overflow, while also considering scalability and compliance with contemporary regulations.

Conclusions. Optimizing the buffer zone size in the context of video data transmission over Bluetooth networks is a critical aspect that affects not only the stable operation of the system as a whole but also the effective management of traffic flows, allowing for improvements in information transmission quality and significantly reducing potential risks from external cyberattacks and internal failures that may arise due to cross traffic or other network anomalies. The application of adaptive signal modulation in close interaction with three-tier data buffering enables the system to dynamically adjust to variable communication channel parameters, such as transmission speed, noise levels, and interference. This, in turn, helps maintain a high level of video stream quality even under adverse environmental conditions and increased signal variability. The integration of three buffer levels, each performing distinct storage and preprocessing functions for incoming data, creates an additional protective barrier that significantly minimizes the negative impact of external factors on system stability, particularly by preventing possible delays, interruptions, or data loss that may arise due to changing environmental conditions or network impediments during information transmission.

Keywords: buffer optimization, video streaming, Bluetooth wireless networks, adaptive management, data transmission, signal quality, packet loss, user priority management, cross traffic, information protection.

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; in the decision to publish the results.