

DOI: <https://doi.org/10.36910/6775-2524-0560-2026-64-15>

УДК 621.396.96:621.391.822

Ентін Ігор Іванович, аспірант

<https://orcid.org/0009-0004-5545-7814>

Вінницький національний технічний університет, м. Вінниця, Україна

РОЗРОБКА МЕТОДУ ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ BLE СИСТЕМИ ЗВ'ЯЗКУ НА ОСНОВІ СТИБКОПОДІБНОЇ ЗМІНИ ЧАСТОТИ

Ентін І. І. Розробка методу підвищення завадостійкості BLE системи зв'язку на основі стрибкоподібної зміни частоти. Об'єктом дослідження є методи стрибкоподібної перебудови частоти (frequency hopping) у бездротових мережах Bluetooth Low Energy (BLE), зокрема порівняння традиційних випадкових, адаптивних, хаотичних та запропонованого оптимізованого хаотичного алгоритму. Актуальність дослідження зумовлена необхідністю мінімізації перешкод у спектрі, забезпечення надійного зв'язку між вузлами BLE та сумісності з Wi-Fi сигналами в умовах високого рівня шумів. У роботі розглядаються різні алгоритми частотного перестрибування, включно з класичними псевдовипадковими генераторами, логістичною картою як простим хаотичним генератором та оптимізацією параметра оновлення для зменшення перешкод і виключення самоінтерференції. Запропонований метод здатен адаптуватися до змін у радіочастотному середовищі, забезпечуючи високу якість зв'язку та безпеку передачі. Основні результати включають моделювання впливу різних алгоритмів на коефіцієнт перешкод та успішність підключення вузлів BLE в умовах співіснування з Wi-Fi сигналами. Запропонований оптимізований хаотичний метод демонструє найкраще співвідношення між зменшенням перешкод, високою ефективністю підключення та мінімальними часовими затратами на вибір каналу порівняно з іншими методами. Визначено також особливості обчислювальної складності різних генераторів псевдовипадкових чисел, зокрема Мерсенн-Твістера та логістичної карти. Інноваційність підходу полягає у використанні теорії хаосу для генерації адаптивних, непередбачуваних послідовностей частотних стрибків із оптимізацією параметрів, що дозволяє зменшити взаємні перешкоди між BLE-вузлами і підвищити сумісність із Wi-Fi.

Ключові слова: стрибкоподібна перебудова частоти, хаотичне перестрибування, адаптивний алгоритм, бездротовий зв'язок, логістична карта, псевдовипадковий генератор, безпека передачі, частотне рознесення.

Entin I. Development of a method to enhance the interference immunity of a BLE communication system based on frequency hopping. The object of the study is frequency hopping methods in Bluetooth Low Energy (BLE) wireless networks, specifically comparing traditional random, adaptive, and chaotic algorithms with a proposed optimized chaotic algorithm. The relevance of the study stems from the need to minimize spectral interference, ensure reliable communication between BLE nodes, and maintain compatibility with Wi-Fi signals in high-noise environments. The paper examines various frequency-hopping algorithms, including classical pseudorandom generators, the logistic map as a simple chaotic generator, and the optimization of the update parameter to reduce interference and eliminate self-interference. The proposed method is capable of adapting to changes in the radio-frequency environment, ensuring high communication quality and transmission security. The key results include modeling the impact of various algorithms on the interference ratio and the connection success rate of BLE nodes in environments where they coexist with Wi-Fi signals. The proposed optimized chaotic method demonstrates the best balance between interference reduction, high connection efficiency, and minimal time overhead for channel selection compared to other methods. Additionally, the computational complexity characteristics of various pseudorandom number generators—specifically the Mersenne Twister and the logistic map—have been determined. The innovative nature of the approach lies in the use of chaos theory to generate adaptive, unpredictable frequency-hopping sequences with parameter optimization, which reduces mutual interference between BLE nodes and improves compatibility with Wi-Fi.

Keywords: frequency hopping, chaotic hopping, adaptive algorithm, wireless communication, logistic map, pseudorandom generator, transmission security, frequency diversity.

Вступ

У сучасних бездротових мережах надзвичайно актуальним є завдання забезпечення ефективного співіснування різних типів пристроїв, зокрема Wi-Fi та Bluetooth, які працюють у спільному частотному діапазоні 2,4 ГГц. Зі зростанням кількості носимих пристроїв, систем "розумного дому", медичних та IoT-застосувань, проблема взаємних перешкод між цими технологіями стає дедалі гострішою. Перешкоди з боку сигналів Wi-Fi можуть суттєво знижувати якість з'єднання Bluetooth, що призводить до втрат даних, зниження швидкості передачі та загального погіршення продуктивності системи.

Одним з ефективних способів зменшення перешкод є використання алгоритмів стрибкоподібної перебудови частоти (FHSS), які дозволяють Bluetooth-пристроєм динамічно змінювати робочі канали для уникнення конфліктів з іншими сигналами. Існує кілька типів таких методів — випадкові, хаотичні, адаптивні — кожен із яких має свої переваги та обмеження щодо продуктивності та обчислювальної складності.

У цьому дослідженні розглянуто новий оптимізований метод хаотичної стрибкоподібної перебудови частоти, який дозволяє досягти високої стійкості до перешкод, забезпечити високу ймовірність успішного підключення та зменшити затримки вибору каналів. Проведено

моделювання різних сценаріїв взаємодії Wi-Fi і Bluetooth сигналів із використанням моделей AWGN, логістичної карти, ГПЧГ Мерсенна та методів Монте-Карло для кількісного аналізу ефективності запропонованого підходу.

У роботі [1] розглядається компроміс між пропускнуою здатністю та надійністю з'єднання в Bluetooth Low Energy (BLE). Автори розробляють математичну модель, що дозволяє кількісно оцінити вплив параметрів частотного перестрибування та повторної передачі даних на продуктивність системи. Вони демонструють, що збільшення надійності через повторні передачі призводить до зниження ефективного каналу передачі. Такий підхід є цінним для розробників енергозберігаючих мереж, де важливо підтримувати баланс між енергоефективністю і якістю обслуговування.

У роботі [2] представлено емпіричне моделювання ко-канальної інтерференції в BLE на основі даних реальних вимірювань. Дослідження фокусуються на вивченні впливу пристроїв Wi-Fi, що працюють на суміжних частотах. Авторами було встановлено, що інтерференція значно знижує ефективність BLE, особливо при високій щільності трафіку. Робота є важливою, оскільки підкреслює необхідність розробки більш адаптивних схем частотного перестрибування для уникнення конфліктів у спектрі.

У дослідженні [3] запропоновано швидку схему адаптивного перестрибування по частотах (Fast AFH), яка динамічно реагує на зміни навколишнього радіооточення. Запропонований алгоритм базується на швидкій оцінці якості каналу та виключенні каналів із високим рівнем завад. Експерименти показали суттєве зменшення втрат пакетів при збереженні високої пропускнуої здатності, що свідчить про ефективність запропонованого підходу в умовах високої інтерференції.

У роботі [4] автори розглядають схему перестрибування, яка враховує наявність Wi-Fi мереж, зокрема у переповненому частотному середовищі. Метод передбачає активне сканування спектра і уникнення каналів, зайнятих Wi-Fi. Такий підхід дозволяє підвищити стабільність BLE-з'єднань у міських умовах та приміщеннях з великою кількістю пристроїв.

У [5] досліджено загальні принципи адаптивного частотного перестрибування в бездротових мережах. Автори підкреслюють важливість динамічного моніторингу стану каналів та пропонують класифікацію методів AFH. Хоча робота не зосереджена виключно на BLE, вона закладає теоретичне підґрунтя для розробки ефективних стратегій перестрибування.

Дослідження [6] аналізує ефективність методів зменшення інтерференції в умовах повільного асинхронного перестрибування по частотах у Bluetooth. Автори показують, що інтелектуальні алгоритми вибору частот можуть суттєво знизити рівень завад навіть без глобальної синхронізації, що важливо для BLE, який часто працює у гетерогенному середовищі.

Нарешті, в [7] запропоновано eAFH — алгоритм інформованого частотного перестрибування, який використовує історію якості каналів для прогнозування та ухилення від «поганих» частот. Такий підхід дозволяє не лише зменшити втрати пакетів, а й зменшити затримки у мережі. Робота має практичне значення для BLE-сенсорних мереж у розумному будинку, де потрібна стабільність з'єднання.

Матеріали та методи

Bluetooth і Wi-Fi — це поширені бездротові технології, що широко використовуються в побутовій електроніці та функціонують у спільному ISM-діапазоні частот 2,4 ГГц. Незважаючи на спільний частотний простір, вони мають різні методи передачі даних: Bluetooth застосовує щільний (слотовий) підхід для зменшення енергоспоживання, тоді як Wi-Fi передає дані безперервно. Це призводить до взаємних перешкод, оскільки сигнали Wi-Fi можуть сприйматися як шум для приймачів Bluetooth, і навпаки.

Інтернет-речей (IoT) шлюзи та концентратори зазвичай підтримують кілька бездротових стандартів, включно з Wi-Fi, Zigbee, Thread та Bluetooth, щоб взаємодіяти з широким спектром пристроїв. Проте через спільне використання діапазону 2,4 ГГц може виникати зниження продуктивності, коли кілька радіомодулів працюють одночасно. Використання механізмів співіснування з Wi-Fi дозволяє зменшити рівень взаємних завад і покращити сумісну роботу різних протоколів[1].

Співіснування у діапазоні 2,4 ГГц забезпечує одночасну роботу технологій, таких як Wi-Fi, Bluetooth, Zigbee та Thread, без істотного впливу одна на одну. Завадостійкість важлива, оскільки конфлікти між сигналами можуть спричиняти зниження чутливості приймачів і підвищене енергоспоживання через повторні спроби передавання. Однак забезпечити ефективне співіснування

стає складніше в умовах сучасних шлюзів, які використовують потужніші передавачі, більшу пропускну здатність і до чотирьох одночасно активних радіомодулів у тому самому діапазоні. Це вимагає впровадження додаткових заходів для стабільної бездротової взаємодії[2].

На рисунку 1 представлено частотний розподіл ISM-діапазону 2,4 ГГц: Wi-Fi займає три неперекривні канали шириною 20 МГц, тоді як Bluetooth використовує 40 каналів BLE із кроком 2 МГц.

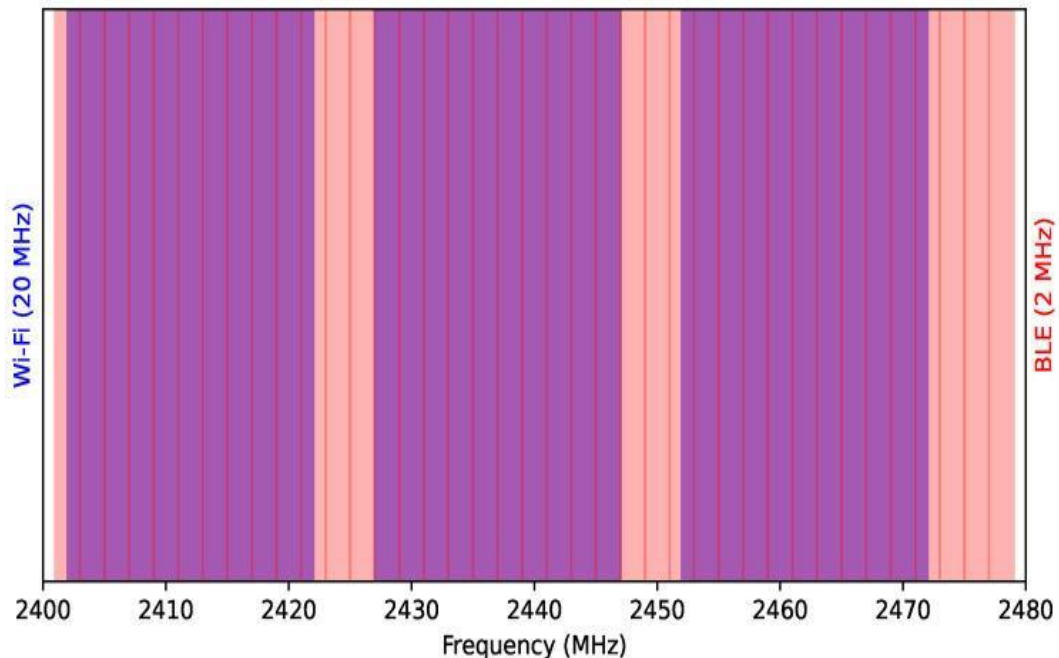


Рис. 1. Частотний план для діапазону ISM 2,4 ГГц.

Канал Wi-Fi має ширину 20 МГц, тоді як один канал BLE займає лише 2 МГц. Це означає, що в межах одного Wi-Fi-каналу може вміститися приблизно десять BLE-каналів. Із 40 Bluetooth-каналів, які використовуються в технології FHSS (стрибоподібна перебудова частоти), 10 (тобто 25%) можуть збігатися з частотою поточного Wi-Fi-каналу, як показано на рисунку 1.

Наприклад, якщо пристрій одночасно працює з Wi-Fi і Bluetooth — як під час дзвінка через Wi-Fi із використанням Bluetooth-гарнітури — можливе накладання сигналів. Якщо канал Bluetooth збігається з активною передачею пакета Wi-Fi, це може пошкодити Wi-Fi-пакет. У разі кількох таких помилок Wi-Fi-з'єднання автоматично знизить швидкість передачі, що збільшить тривалість передачі пакета та зменшить загальну пропускну здатність. Імовірність того, що пакет зазнає подальшої колізії, становить 25%. Якщо це станеться, пропускну здатність Wi-Fi ще більше погіршиться. Так само, у випадку пошкодження Bluetooth-пакета сигналом Wi-Fi, Bluetooth-передавач перейде на інший канал і повторить спробу (за умови асинхронної передачі), що також призводить до втрати ефективності[3].

Ефективне співіснування Bluetooth і Wi-Fi у межах ISM-діапазону 2,4 ГГц вимагає ретельного планування та впровадження спеціальних механізмів, спрямованих на зниження взаємних перешкод і забезпечення максимально можливої продуктивності бездротового з'єднання[4].

Вибір каналу

Правильний вибір каналу є критично важливим для забезпечення стабільного та якісного з'єднання Bluetooth Low Energy (BLE). З метою підвищення надійності зв'язку та зменшення впливу перешкод було розроблено низку алгоритмів, що оптимізують процес вибору каналу. Під час призначення частоти передачі для BLE сигналу, обрана несуча може або перетинатися з активним Wi-Fi-сигналом, або бути спрямована на менш зашумлений канал — залежно від певних критеріїв, які будуть розглянуті далі. Деякі з каналів можуть залишатися відносно вільними, навіть за наявності інтерференції між BLE та Wi-Fi, як це ілюструє рисунок 2.

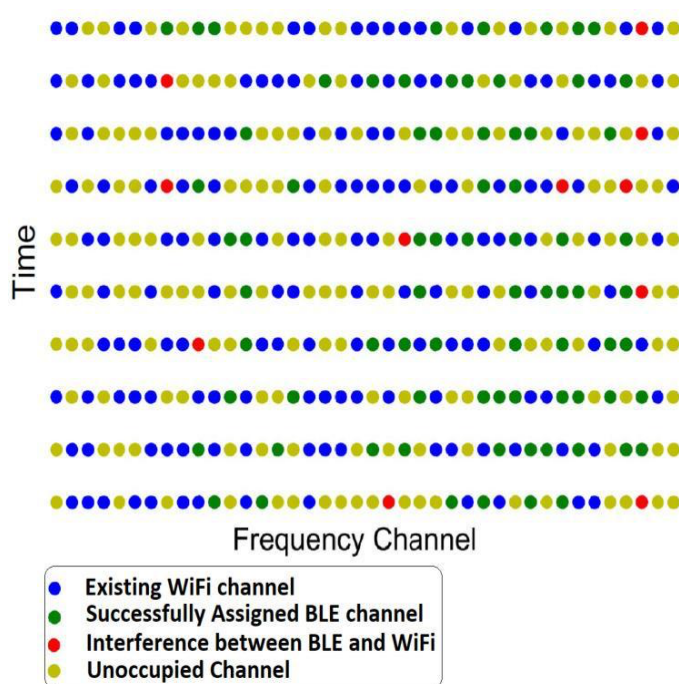


Рис. 2. Перехідна зміна частоти BLE може співіснувати з Wi-Fi.

Алгоритми вибору каналу в Bluetooth Low Energy (BLE) поділяються на три основні типи: фіксовані, динамічні та адаптивні. Фіксоване призначення каналу є найпростішим варіантом, однак воно часто неефективне в умовах сильних радіоперешкод. Натомість динамічні та адаптивні алгоритми здатні реагувати на зміну рівня завад у реальному часі, що забезпечує вищу якість з'єднання та більшу надійність. У численних дослідженнях проведено глибокий аналіз ефективності різних підходів до вибору каналу з урахуванням таких параметрів, як стабільність зв'язку, надійність та енергоспоживання. Результати свідчать, що обраний алгоритм значною мірою впливає на загальну продуктивність Bluetooth LE-з'єднання[5].

Для зменшення впливу завад і зниження ризику колізій Bluetooth LE застосовує механізм стрибкоподібної перебудови частоти (FHSS), який розподіляє передавання сигналів по різних частотах. Такий підхід значно зменшує ймовірність накладання сигналів та втрати даних.

Випадкова перестроювання частоти

Випадкова перебудова частоти — це метод, який покликаний підвищити захищеність і завадостійкість бездротового зв'язку шляхом уникнення фіксованого використання частот. Суть цього підходу полягає у швидкому та випадковому перемиканні між різними радіочастотами під час передавання сигналу.

Головна ідея випадкової зміни частоти полягає в тому, що постійне перемикання частот унеможливорює тривале блокування зв'язку або перехоплення даних. Така технологія активно використовується у військових системах зв'язку та інших критично важливих сферах, де потрібен надійний і захищений бездротовий канал.

У традиційних системах стрибкоподібної перебудови частоти вибір частот зазвичай ґрунтується на заздалегідь визначених псевдовипадкових послідовностях. Проте через їхню фіксованість ці послідовності не здатні підлаштовуватись під поточні умови радіоефіру. У результаті це може спричиняти частотні конфлікти та перевантаження каналів, що негативно впливає на якість зв'язку та пропускну здатність.

Нехай f_{base} позначає базову частоту BLE-сигналу, а f_{sets} — набір частотних зміщень. Тоді допустимий набір частот для реалізації випадкової перебудови визначається як множина: $F = \{f_{base} + f_{sets}\}$ де знак «+» означає об'єднання значень. У BLE цей набір зазвичай обмежений до 37 каналів.

У кожному часовому інтервалі система випадково обирає одну з частот із множини F , на яку й здійснюється наступний стрибок. Випадковість забезпечується генератором псевдовипадкових чисел (ГПВЧ), який генерує індекси для вибору частоти з F .

Позначимо N — загальна кількість часових інтервалів, тоді $h_n \in F$ представляє частоту, що використовується у n -му інтервалі, де $1 \leq n \leq N$. Відповідно, послідовність частот визначається як $h_1, h_2, \dots, h_N$ [6]:

$$h_n = f_{base} + f_{offset(n)} \quad 1$$

Позначимо $g(n)$ як генератор псевдовипадкових чисел (ГПВЧ), що для кожного часового інтервалу n відображає значення з діапазону $1, \dots, |F|$ на певну частоту з множини F .

Щоб запобігти можливості прогнозування частотної послідовності потенційними злоумисниками, псевдовипадкове відображення має бути криптографічно стійким і непередбачуваним. Серед поширених варіантів генераторів частот для таких задач використовуються, зокрема, лінійний конгруентний генератор (LCG) та генератор з обертанням Мерсенна (Mersenne Twister).

Хоча обидва генератори здатні створювати послідовності псевдовипадкових чисел, між ними існують помітні відмінності, зокрема у швидкості генерації, довжині періоду, рівні випадковості та рівні безпеки.

LCG є простим та високопродуктивним методом генерації псевдовипадкових чисел, що працює на основі лінійного рекурентного рівняння. Його базова формула має такий вигляд[6]:

$$x_{n+1} = (ax_n + c) \bmod m \quad 2$$

У цьому контексті x_n позначає n -те згенероване число, де a — множник, c — доданок, m — модуль, а операція $\bmod$ означає взяття за модулем. Лінійні конгруентні генератори (LCG) відзначаються простотою реалізації та малими вимогами до пам'яті. Проте вони мають серйозні обмеження, зокрема низьку ентропію та передбачуваність, що може зробити послідовність стрибків частоти вразливою до атак.

На противагу цьому, генератор псевдовипадкових чисел Мерсенна Твістер (Mersenne Twister) є набагато складнішим і забезпечує вищу безпеку. Він ґрунтується на скрученому генералізованому зсувному регістрі зворотного зв'язку (Twisted Generalized Feedback Shift Register) і здатен створювати довгі послідовності 32-бітних чисел. Завдяки своїй складній структурі, Mersenne Twister забезпечує кращу статистичну випадковість і менш вразливий до передбачення, ніж LCG. Разом із цим, він потребує більше пам'яті та обчислювальних ресурсів, але компенсує це надзвичайно великим періодом і високою якістю генерації випадкових значень.

У цьому дослідженні Mersenne Twister використовується для моделювання частотного вибору в сигналах BLE.

Реалізація випадкової стрибкоподібної зміни частоти для визначення частоти передачі BLE-сигналів може бути здійснена відповідно до рисунку 3.

```

Input: frequencies from 0 to 39, communication attempts  $N = 40,000$ .
Output: Assigned map of Bluetooth signals.
Define  $M_s = 40$ ;
for each  $M$  in  $M_s$  do
    Generate a random  $M$ -dimensional vector  $x$  of floats between 0 and 1;
    for each row  $i$  in hop_sequence do
        for each column  $j$  in hop_sequence do
            Choose a random frequency from frequencies with replacement and
            assign it to hop_sequence[i, j];
            Update  $x[j]$  by calling the function random_hopping;
        end
    end
    for each row  $i$  in interference_map do
        for each column  $j$  in interference_map do
            if frequencies[j] == hop_sequence[i, k] then
                interference_map[i, j] = 1;
            end
        end
    end
end
end
    
```

Рис. 3. Моделювання стрибкоподібної зміни частоти BLE та оцінка продуктивності. /

Хаотичне перестрибування частоти

Хаотична стрибкоподібна перебудова частоти — це підхід, який запроваджує елементи хаосу у схему зміни частоти з метою підвищення рівня безпеки бездротового зв'язку. У цьому методі використовується хаотична карта для формування послідовності перестрибування, за якою визначається частотний канал для кожної передачі.

Хаотична функція в контексті перебудови частоти — це математичний механізм, що створює нестабільну, змінну послідовність частот. На відміну від традиційних псевдовипадкових генераторів, хаотичні послідовності постійно змінюються у відповідь на умови радіооточення, що дозволяє їм краще адаптуватися до перешкод. Завдяки цьому пристрої BLE можуть періодично повертатися до раніше використаних каналів, покращуючи розподіл передач і зменшуючи ймовірність стабільного конфлікту з іншими сигналами.

Для реалізації хаотичного перестрибування частот можуть застосовуватись різні математичні карти, зокрема логістична карта, карта Енона або система Лоренца. Кожна з них має свої унікальні властивості і генерує різні типи хаотичних послідовностей. Порівняння цих підходів до хаотичної перебудови частот наведено в таблиці 1.

Таблиця 1. Порівняння методів хаотичної стрибкоподібної зміни частоти./ Table 1. Comparison of chaotic frequency hopping methods.

Техніка	Переваги	Недоліки	Складність
Логістична карта	Легко впровадити	Чутливість до початкових умов	Низький
Мапа Енона	Високий ступінь випадковості	Складний у впровадженні	Помірний
Система Лоренца	Дуже складна поведінка	Важко впровадити	Високий
Гібридні методи	Високий ступінь випадковості та безпеки	Складний у впровадженні	Високий

Загалом, застосування хаотичної перебудови частоти може стати ефективним засобом підвищення захищеності бездротового зв'язку. Водночас цей підхід може ускладнити реалізацію системи та збільшити її загальну складність. Тому перед впровадженням такого рішення важливо ретельно оцінити його переваги й потенційні недоліки. Одним із перспективних варіантів є логістична карта — проста за структурою хаотична функція, здатна ефективно генерувати псевдовипадкові послідовності, що робить її придатною для використання в бездротових системах, які впроваджують хаотичне перестрибування частот.

Логістична карта є прикладом математичної функції, яка демонструє, як складна хаотична динаміка може виникнути з простих нелінійних рівнянь. Вона описується наступною формулою[6]:

$$x_{n+1} = r \cdot x_n \cdot (1 - x_n) \quad 3$$

Тут x_n — це значення функції на n -му кроці часу, а r — параметр керування, який визначає інтенсивність або швидкість змін. Для певних значень параметра r , логістична карта проявляє хаотичну поведінку, формуючи непередбачувану та неперіодичну послідовність x_n .

Щоб інтегрувати логістичну карту в механізм стрибкоподібної перебудови частоти, необхідно зіставити отримані значення x_n із частотним діапазоном, у межах якого здійснюється перемикання. Це реалізується шляхом визначення множини допустимих частот $F = \{f_1, f_2, \dots, f_m\}$ де m — кількість доступних каналів. Значення x_n тоді відображається на відповідний канал із цієї множини за допомогою спеціального перетворення:[6]

$$h_n = (x_n) = f_{\lfloor (x_n \times (m-1)) + 1 \rfloor} \quad 4$$

Тут h_n позначає частоту, вибрану на n -му часовому кроці, а f — це функція, яка округлює значення $(x_n \times (m-1)) + 1$ до найближчого меншого цілого числа.

Хаотичне перестрибування частоти на основі логістичної карти відрізняється високою гнучкістю та здатністю адаптуватися, оскільки послідовність зміни частот формується з урахуванням поточного стану бездротового середовища. Через хаотичну природу логістичної карти ця послідовність є непередбачуваною для потенційних злоумисників, що робить цей метод значно безпечнішим порівняно з традиційними схемами перестрибування.

Реалізація хаотичного перестроювання частоти за допомогою логістичної карти для вибору частот сигналів BLE може бути виконана за рисунком 4.

```

Input:  $n\_channels$ : number of channels.
 $n\_slots$ : number of slots per channel.
 $n\_signals$ : number of Bluetooth signals.
 $r$ : parameter for logistic map.
Output: Assigned map of Bluetooth signals.

 $interference\_map \leftarrow$  random  $n\_channels \times n\_slots$  array;
 $x \leftarrow$  random number between 0 and 1;
 $channel\_sequence \leftarrow$  empty list;
for  $i \leftarrow 1$  to  $n\_slots \times n\_signals$  do
     $x \leftarrow logistic\_map(x, r)$ ;
     $channel\_index \leftarrow$  integer part of  $x \times n\_channels$ ;
    append  $channel\_index$  to  $channel\_sequence$ ;
end
 $assigned\_map \leftarrow$   $n\_channels \times n\_slots$  array filled with zeroes;
for  $i \leftarrow 1$  to  $n\_signals$  do
     $start\_slot \leftarrow$  random integer between 0 and  $n\_slots - 1$ ;
    for  $j \leftarrow 1$  to  $n\_slots$  do
         $slot\_index \leftarrow (start\_slot + j - 1) \bmod n\_slots$ ;
        if  $assigned\_map[channel\_sequence[(i - 1) \times n\_slots + j]][slot\_index] == 0$ 
            then
                 $assigned\_map[channel\_sequence[(i - 1) \times n\_slots + j]][slot\_index] \leftarrow i$ ;
            end
        else
             $assigned\_map[channel\_sequence[(i - 1) \times n\_slots + j]][slot\_index] \leftarrow$ 
                -1;
        end
    end
end
    
```

Рис. 4. Призначення сигналу Bluetooth з використанням хаотичної стрибкоподібної зміни частоти.

Логістична карта володіє низкою властивостей, які роблять її корисною в різних сферах. Зокрема, вона здатна генерувати псевдовипадкові числа, що широко застосовується у криптографії та інших галузях, де важлива випадковість.

У випадку хаотичного перестрибування частоти логістична карта може служити джерелом псевдовипадкових послідовностей, що визначають порядок зміни частот. Використання унікальної початкової умови для кожної передачі дозволяє створювати послідовності, які виглядають випадковими та непередбачуваними, що ускладнює злоумисникам можливість перехоплення сигналу.

Водночас логістична карта має і певні обмеження. Зокрема, вона дуже чутлива до початкових умов — незначні зміни на старті можуть призвести до кардинально різних результатів. Крім того, карта здатна демонструвати біфуркації з подвоєнням періоду, що ускладнює передбачення її поведінки.

Адаптивна стрибкоподібна перебудова частоти

Адаптивна перебудова частоти — це метод, який використовується в бездротових системах для динамічного коригування послідовності змін частоти з урахуванням рівня перешкод та шуму в каналі. Основна ідея полягає у моніторингу якості каналу та адаптації стрибків частоти для уникнення смуг із високим рівнем завад або шуму.

Зазвичай адаптивна стрибкоподібна зміна частоти включає кілька етапів. Спершу здійснюється оцінка якості каналу, наприклад, шляхом вимірювання співвідношення

сигнал/перешкода плюс шум (SINR) або інших метрик. Після ідентифікації проблемних частотних діапазонів формується нова послідовність перестрибувань, яка уникає цих каналів. Це можна зробити випадковим вибором нової послідовності або за допомогою спеціального алгоритму генерації. Оновлена послідовність застосовується у системі для подальших передач, при цьому моніторинг якості каналу продовжується з метою подальшої адаптації.

Перевагою адаптивного стрибкоподібного перемикавання є покращення надійності та продуктивності бездротового зв'язку в умовах завад і шуму. Крім того, цей метод підвищує безпеку, ускладнюючи зломисникам перехоплення сигналу. Використання логістичної карти може спростити реалізацію адаптивної зміни частоти, генеруючи псевдовипадкові послідовності, які обходять проблемні канали. Однак впровадження цього підходу потребує додаткових апаратних та програмних ресурсів, що може збільшити складність і вартість системи.

Завдяки здатності динамічно коригувати послідовність частотних стрибків залежно від рівня перешкод і шуму, адаптивна стрибкоподібна перебудова частоти стає все більш популярною у бездротових технологіях. Існує кілька методів адаптації, серед яких:

Метод на основі порогового значення: встановлюється поріг для рівня шуму або перешкод, і послідовність змін частоти оновлюється, якщо виміряні показники перевищують цей поріг. Перевага — простота реалізації та низькі вимоги до обчислювальних ресурсів. Недолік — обмежена ефективність при різних умовах шуму та завад.

Метод на основі навчання: використовуються алгоритми машинного навчання для аналізу структури шуму і перешкод у каналі та відповідної адаптації частотних перестрибувань. Перевага — висока гнучкість і здатність покращувати продуктивність із часом. Недолік — високі обчислювальні витрати, які можуть бути неприйнятними для деяких систем.

Розподілений метод: кожен вузол мережі самостійно оцінює якість каналу та обмінюється інформацією з іншими вузлами для узгодження послідовності перестрибувань. Цей підхід підвищує надійність і адаптивність у динамічних умовах, але збільшує потребу у координації і комунікації, що ускладнює систему.

Гібридний метод: поєднує кілька підходів, наприклад, методи на основі порогових значень і навчання, щоб максимально підвищити продуктивність і адаптивність. Водночас він потребує значних ресурсів і є складнішим у реалізації.

Вибір конкретного методу залежить від вимог і обмежень конкретної бездротової системи. Для простих мереж із низьким рівнем завад підійдуть методи на основі порогів, тоді як у складних середовищах з високою завадозахищеністю доцільнішими будуть методи навчання або розподілені підходи. Гібридні рішення можуть запропонувати найкращі результати, але потребують більших обчислювальних ресурсів і складнішої реалізації[7].

Запропонований метод

Запропонований метод хаотичної стрибкоподібної зміни частоти базується на оптимізації коефіцієнта оновлення g з метою мінімізації перешкод і досягнення нульової самоперешкоди між вузлами BLE, що використовують стрибкоподібну зміну частоти. Робота методу може здійснюватися таким чином:

- 1) Визначається набір N частот для перебудови, які застосовуватимуться вузлами BLE.
- 2) Ініціалізується коефіцієнт оновлення g випадковим значенням у межах від 3,6 до 4,0.
- 3) Для кожного вузла BLE генерується хаотична послідовність на основі логістичної карти з поточним значенням g . Ця послідовність визначає порядок вибору частот для стрибків вузла.
- 4) Обчислюється матриця інтерференції I розміром $N \times N$, де $I_{ij} = 1$, якщо частота i створює перешкоду для частоти j , і $I_{ij} = 0$ у протилежному випадку.
- 5) Для кожного вузла BLE визначаються перешкоди, які він спричиняє іншим вузлам, з використанням матриці I . Якщо виявляється, що вузол створює самоперешкоду, його хаотична послідовність коригується шляхом вибору інших частот.
- 6) Значення g оновлюється за допомогою оптимізаційного алгоритму, наприклад, градієнтного спуску або імітації відпаду, з метою мінімізації загальної інтерференції між вузлами. Кроки 3–6 повторюються, доки не досягається мінімальний рівень перешкод та відсутність самоперешкод.

Цей підхід застосовує теорію хаосу для генерації випадкових, непередбачуваних послідовностей стрибків частоти для кожного вузла BLE, що запобігає утворенню передбачуваних шаблонів і знижує рівень взаємних перешкод. Завдяки оптимізації коефіцієнта g хаотична поведінка

системи налаштовується таким чином, щоб мінімізувати інтерференцію та забезпечити відсутність самоперешкод. Проте реалізація цього методу може вимагати значних обчислювальних ресурсів і бути складнішою за традиційні способи стрибкоподібної зміни частоти. Схему алгоритму наведено на рисунку 5.

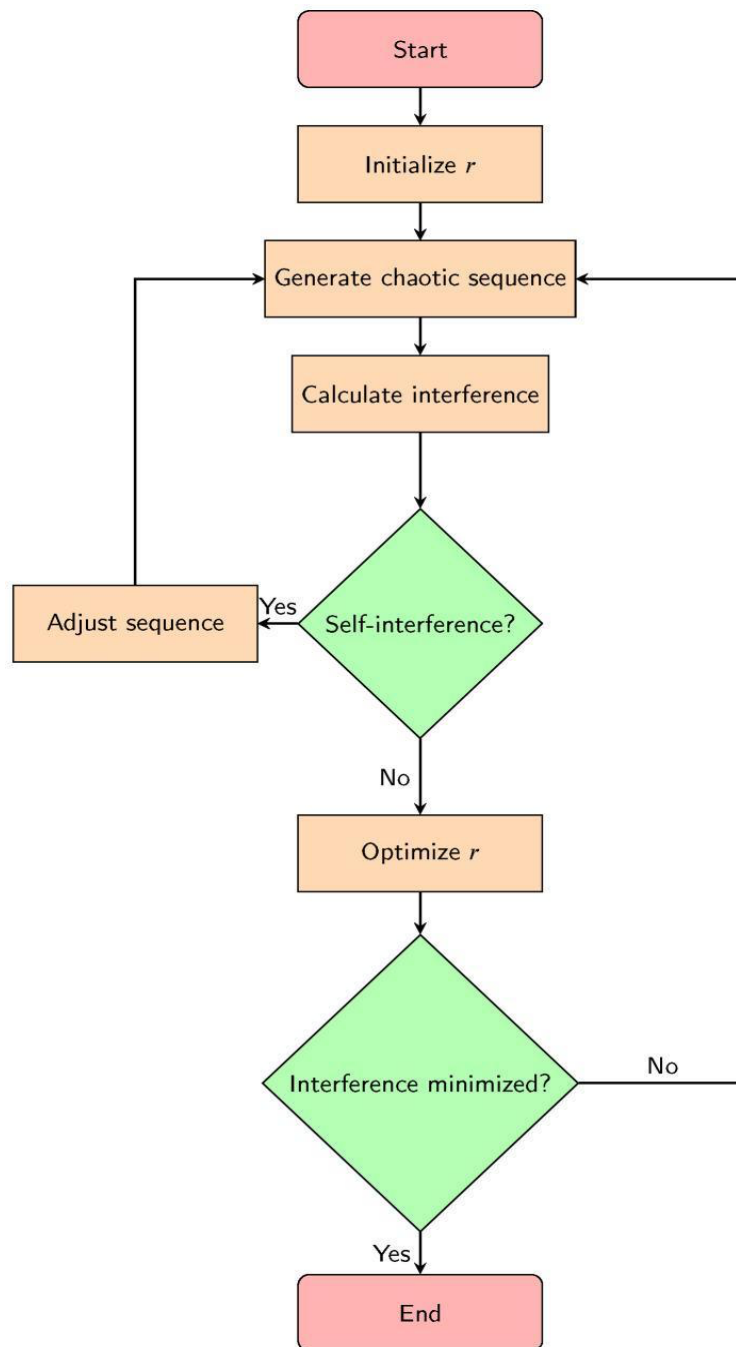


Рис. 5. Блок-схема запропонованого методу хаотичної стрибкоподібної зміни частоти.

Для порівняння чотирьох методів стрибкоподібної зміни частоти — випадкового, хаотичного, адаптивного та запропонованого — використовуються такі критерії:

Зменшення перешкод: Метод повинен ефективно знижувати рівень взаємних перешкод між вузлами, що здійснюють перебудову частоти.

Уникнення самоперешкод: Гарантується, що кожен вузол не створює перешкод самому собі під час стрибків.

Частотне рознесення: Метод має охоплювати широкий спектр частот, щоб уникнути перевантаження окремих каналів.

Синхронізація: Забезпечується координація між вузлами для запобігання колізіям при одночасних переходах.

Адаптивність: Спосіб повинен динамічно реагувати на зміни в навколишньому середовищі, наприклад, появу нових пристроїв або джерел завад.

Складність: Метод має бути максимально простим для реалізації та не вимагати значних ресурсів.

На основі цих критеріїв здійснено порівняння чотирьох методів, результати якого наведено в таблиці 2.

Таблиця 2. Порівняння методів стрибкоподібної зміни частоти./ Table 2. Comparison of frequency-hopping methods.

Критерії	Випадкове	Хаотичний	Адаптивний	Запропоновано
Зменшення перешкод	Помірний	Низький	Високий	Високий
Уникнення самоперешкод	Низький	Низький	Високий	Високий
Частотне рознесення	Помірний	Високий	Високий	Високий
Синхронізація	Низький	Низький	Помірний	Високий
Адаптивність	Низький	Низький	Високий	Високий
Складність	Помірний	Простий	Комплекс	Помірний

З таблиці 2 видно, що запропонований метод забезпечує найкращі показники за такими критеріями, як зменшення перешкод, уникнення власних перешкод, частотне рознесення, синхронізація та адаптивність, при цьому залишаючись відносно простим для впровадження. Хаотичний та адаптивний методи також демонструють високий рівень зменшення перешкод і частотного рознесення, але їхня реалізація може бути більш складною. Випадковий метод є найпростіший у виконанні, проте показує низькі результати щодо зменшення перешкод і частотного рознесення.

Результати та обговорення

Для імітації впливу перешкод Bluetooth на сигнали Wi-Fi моделювання обох сигналів виконувалося з урахуванням таких параметрів.

Спершу задавалися параметри моделювання сигналу Wi-Fi: кількість пакетів — 1000, кількість бітів у пакеті — 1000, а значення SNR (співвідношення сигнал/шум) варіювалося від 0 до 30 дБ. Несучі частоти Wi-Fi обиралися з трьох неперекриваючих каналів (2412, 2437, 2462 МГц), кожен з пропускну здатністю 20 МГц, при цьому для моделювання використовувалася перша несуча частота.

Далі сигнал Bluetooth моделювався із стрибкоподібною зміною несучої частоти в межах 10 доступних каналів, які можуть співіснувати з моделюваним сигналом Wi-Fi, що має пропускну здатність 2 МГц. Пакети Bluetooth передавалися через 1600 часових інтервалів на пакет.

Для оцінки впливу перешкод на бітову та пакетну помилки Wi-Fi використовували модель каналу AWGN та метод Монте-Карло, що дозволяє визначити коефіцієнти помилок при різних рівнях перешкод. Аналіз проводився як функція положення несучої частоти Bluetooth всередині смуги пропускання Wi-Fi, а також залежно від інтенсивності і тривалості перешкод відносно пакету Wi-Fi.

Величина вектора помилок (EVM) слугує показником точності демодуляції сигналу, відображаючи наскільки відхилення демодульованого сигналу від оригінального. Зазвичай EVM виражається у відсотках або в децибелах (дБ).

Високий рівень EVM свідчить про суттєві спотворення або помилки в демодульованому сигналі порівняно з оригіналом, що призводить до збільшення числа бітових помилок і погіршення

роботи системи. Низький показник EVM означає точне відтворення оригінального сигналу та високу якість зв'язку.

На рисунку 6 показано, як розташування несучої частоти Bluetooth у смузі пропускання Wi-Fi впливає на якість сигналу Wi-Fi з урахуванням показника EVM.

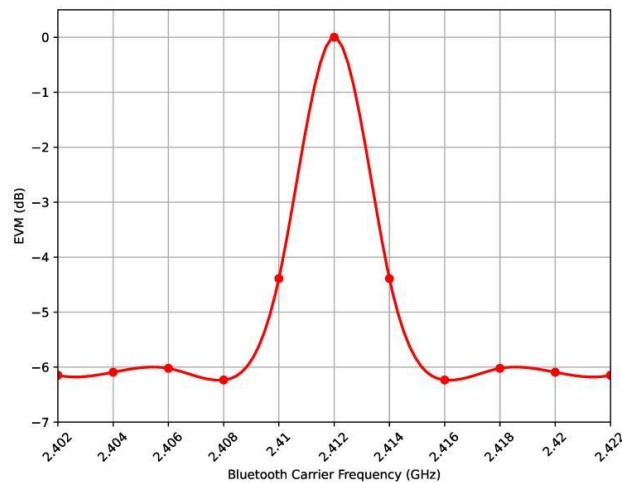


Рис. 6. Перехідна зміна частоти BLE може співіснувати з Wi-Fi.

Коли несуча частота сигналу BLE, який викликає перешкоди, близька до несучої частоти Wi-Fi, значення EVM зростає, і навпаки. Якщо несучі частоти BLE та Wi-Fi співпадають, EVM дорівнює 0 дБ, що свідчить про повну втрату пакетів Wi-Fi. Тому в подальших симуляціях перешкоди враховуються лише у випадках, коли несучі частоти сигналів BLE та Wi-Fi співпадають.

Методи стрибкоподібної зміни частоти для сигналів BLE моделюються з метою мінімізації перешкод для Wi-Fi, а схема моделювання наведена на рисунку 7.

```

Input: frequencies from 0 to 39, communication attempts  $N = 40,000$ .
Output: A CSV file containing the performance measures.
Define  $M_s = 40$ ;
for each  $M$  in  $M_s$  do
    Generate a random  $M$ -dimensional vector  $x$  of floats between 0 and 1;
    for each row  $i$  in  $hop\_sequence$  do
        for each column  $j$  in  $hop\_sequence$  do
            Choose a random frequency from  $frequencies$  with replacement and
            assign it to  $hop\_sequence[i, j]$ ;
            Update  $x[j]$  by calling the function  $random\_hopping$ ;
        end
    end
    for each row  $i$  in  $interference\_map$  do
        for each column  $j$  in  $interference\_map$  do
            if  $frequencies[j] == hop\_sequence[i, k]$  then
                 $interference\_map[i, j] = 1$ ;
            end
        end
    end
    Write  $interference\_map$  to a CSV file "interference_map.csv";
    Calculate various performance measures such as the number of successful BLE
    signal transmissions, the number of BLE transmissions that interfere with an
    ongoing Wi-Fi communication, and the self-interference count;
    Store the performance measures in  $performance\_measures$ ;
end
Write the  $performance\_measures$  list to a CSV file;
    
```

Рис. 7. Моделювання стрибкоподібної зміни частоти BLE та оцінка продуктивності.

У цьому розділі порівнюються різні типи алгоритмів стрибкоподібної перебудови частоти, описані в попередніх розділах, із запропонованим алгоритмом. Порівняння здійснюється за показниками уникнення перешкод, коефіцієнтом успішності та обчислювальною складністю. В роботі представлено результати симуляцій для кількох методів: випадкового, хаотичного,

адаптивного випадкового, адаптивного хаотичного, а також запропонованої оптимізованої хаотичної техніки, яка демонструє кращі результати у зменшенні перешкод для Wi-Fi та забезпеченні високого рівня успішного підключення вузлів Bluetooth.

Моделювання проводилося у середовищі, яке враховує існуючі перешкоди від сигналів Wi-Fi і від вузлів Bluetooth. Було порівняно такі показники продуктивності, як загальний коефіцієнт перешкод, коефіцієнт успішних підключень і час обробки запиту при виборі каналу. Аналіз проводився для різної кількості вузлів Bluetooth, які здійснюють доступ.

Загальні коефіцієнти перешкод для різних методів стрибкоподібної перебудови частоти наведені на рисунку 8.

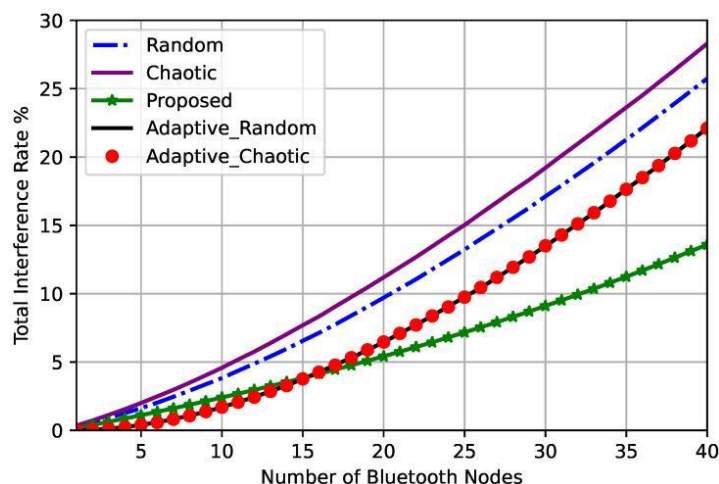


Рис. 8. Загальні коефіцієнти перешкод для різних методів стрибкоподібної зміни частоти.

Очевидно, що загальний рівень перешкод збільшується зі зростанням кількості вузлів Bluetooth, що одночасно отримують доступ, для всіх розглянутих методів стрибкоподібної перебудови частоти. Метод хаотичного стрибкоподібного перемикавання частоти продемонстрував найвищий рівень перешкод у порівнянні з іншими підходами, тоді як адаптивний метод мав нижчий рівень перешкод, ніж хаотичний і випадковий методи, як показано на рисунку 8. Водночас запропонований оптимізований метод хаотичного стрибкоподібного перемикавання частоти виявився злегка більш зашумленим порівняно з адаптивним методом при невеликій кількості вузлів Bluetooth. Проте, зі збільшенням кількості вузлів, наш метод показав суттєво менший рівень перешкод порівняно з адаптивним.

Загальний показник успішного підключення визначався як кількість вузлів Bluetooth, яким успішно призначалися частоти без створення перешкод для сигналів Wi-Fi. Порівняння цього показника для різних методів стрибкоподібної перебудови частоти наведено на рисунку 9.

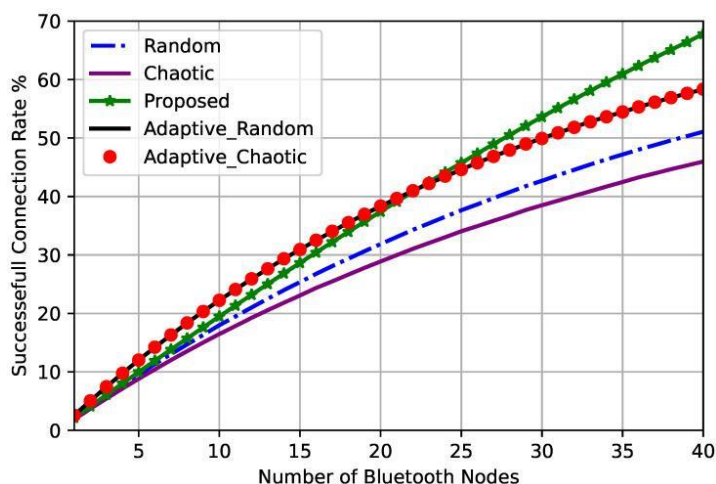


Рис. 9. Загальна кількість успішних з'єднань для різних методів стрибкоподібної зміни частоти.

Очевидно, що загальний коефіцієнт успішного підключення зростає зі збільшенням кількості Bluetooth-вузлів, що одночасно отримують доступ, для всіх розглянутих методів стрибкоподібної зміни частоти. Метод хаотичного стрибкоподібного перемикавання частоти показав найнижчий рівень успішних підключень порівняно з іншими методами, тоді як адаптивний метод мав кращі результати, ніж хаотичний та випадковий, як видно на рисунку 9. Проте запропонований оптимізований метод хаотичного перемикавання продемонстрував найвищу продуктивність серед усіх, включно з адаптивним, особливо при великій кількості вузлів Bluetooth. Однак при кількості вузлів до 20 він поступався адаптивному методу.

Генератори псевдовипадкових чисел Мерсенн-Твістера та логістична карта мають різну обчислювальну складність, яку можна оцінити за допомогою нотації Big O.

Генератор Мерсенн-Твістера має часову складність $O(N)$ для генерації N чисел, що пояснюється початковою ініціалізацією стану. Після цього кожне число генерується за сталий час, тому загальна складність лінійна. Логістична карта є нелінійною функцією, де поточне значення обчислюється на основі попереднього, і часова складність однієї ітерації становить $O(1)$, оскільки включає лише прості арифметичні операції.

Також вимірюється час виконання запиту для обробки вибору каналу. Порівняння цього показника для різних методів стрибкоподібної зміни частоти наведено на рисунку 10.

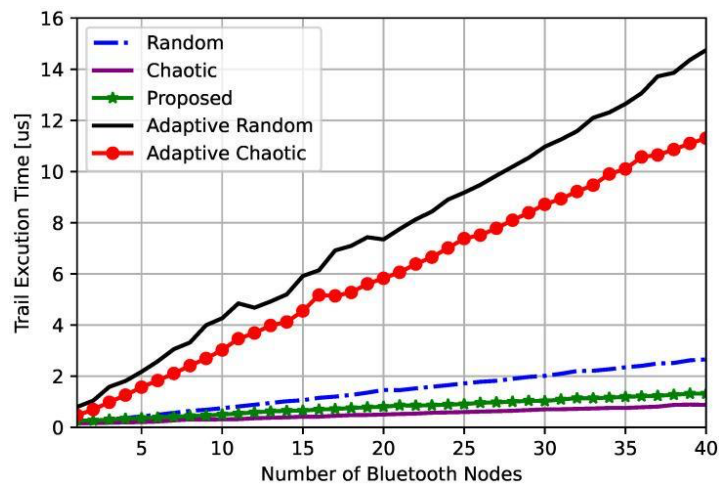


Рис. 10. Порівняння часу виконання проб для методів стрибкоподібної зміни частоти.

Дослідження показали, що метод хаотичної стрибкоподібної зміни частоти характеризується найкоротшим часом виконання, що свідчить про явну перевагу хаотичних підходів завдяки їх простоті, як показано на рисунку 8. Водночас адаптивні методи потребують значно більше часу на виконання, причому адаптивний випадковий метод виявився найповільнішим серед усіх. Запропонований метод демонструє час виконання, близький до традиційного хаотичного методу, і значно коротший, ніж у інших порівняних підходів.

В цілому, результати підтвердили, що оптимізований хаотичний метод стрибкоподібної зміни частоти забезпечує найкраще поєднання зменшення перешкод для Wi-Fi, високої ефективності підключення вузлів Bluetooth і мінімальних часових витрат на вибір каналу, що робить його ефективним рішенням для керування перешкодами у бездротових мережах.

Варто також відзначити, що адаптивні методи демонструють подібні показники щодо рівня перешкод і успішності підключень, при цьому адаптивний хаотичний метод значно швидший за адаптивний випадковий.

Висновки

У результаті проведеного моделювання та порівняння різних методів стрибкоподібної перебудови частоти для Bluetooth-пристроїв було встановлено, що запропонований оптимізований хаотичний метод забезпечує найкращий баланс між ключовими показниками ефективності. Він демонструє високу здатність до уникнення перешкод із боку Wi-Fi-сигналів, досягає високого рівня успішного підключення вузлів Bluetooth і водночас характеризується низькою обчислювальною складністю та мінімальним часом виконання.

У порівнянні з традиційними хаотичними, випадковими та адаптивними методами, запропонований підхід особливо ефективний у мережах з великою кількістю пристроїв, де значно знижує рівень колізій та підвищує надійність передачі даних. Було доведено, що логістична карта як генератор псевдовипадкових чисел має перевагу в простоті реалізації, що сприяє зменшенню затримок при виборі каналів.

Таким чином, запропонована методика може бути ефективно використана в системах бездротового зв'язку нового покоління для покращення якості передачі даних, підвищення енергетичної ефективності та забезпечення стабільної роботи в умовах високого рівня перешкод.

Список бібліографічного опису

1. Pang B. Modeling the Trade-off between Throughput and Reliability in a Bluetooth Low Energy Connection. / B. Pang, T. Claeys, H. Hallez, J. Boydens // V. Poirot, O. Landsiedel // arXiv. – 2021. – Режим доступу: – 2024. – Режим доступу: <https://doi.org/10.48550/arXiv.2405.01231>.
2. Ghafi H. K. Modeling of co-channel interference in bluetooth low energy based on measurement data. / H. K. Ghafi, C. Spindelberger, H. Arthaber // EURASIP Journal on Wireless Communications and Networking. – 2021. – Vol. 2021. – Art. 143. – DOI: <https://doi.org/10.1186/s13638-021-02005-2>.
3. Yoon Y. A Fast Adaptive Frequency Hopping Scheme Mitigating the Effect of Interference in Bluetooth Low Energy Networks. / Y. Yoon, C. Jung, J. Seo, J. Li, J. Kim, S. Jin, N. Silva, K. Han // Lecture Notes in Computer Science. – Cham : Springer, 2016. – P. 196–204. – DOI: https://doi.org/10.1007/978-3-319-49178-3_15.
4. So J. Interference-aware frequency hopping for Bluetooth in crowded Wi-Fi networks. / J. So, Y. Kim // Electronics Letters. – 2016. – Vol. 52, Iss. 17. – DOI: <https://doi.org/10.1049/el.2016.1773>.
5. Liang X.-h. On the Research of Adaptive Frequency Hopping in the Wireless Communication. / X.-h. Liang, L. Cheng // ICCSEE 2013 : proceedings. – 2013. – DOI: <https://doi.org/10.2991/iccsee.2013.522>.
6. Kim K. Interference Mitigation in Asynchronous Slow Frequency Hopping Bluetooth Networks. / K. Kim, G. L. Stüber // Wireless Personal Communications. – 2004. – Vol. 28. – P. 143–159. – DOI: <https://doi.org/10.1023/B:WIRE.0000021421.50247.f0>.
7. Poirot V. eAFH: Informed Exploration for Adaptive Frequency Hopping in Bluetooth Low Energy. arXiv. <https://doi.org/10.48550/arXiv.2112.03046>.

References

- 1) Pang, B., Claeys, T., Hallez, H. & Boydens, J. (2024). Modeling the Trade-off between Throughput and Reliability in a Bluetooth Low Energy Connection. arXiv. <https://doi.org/10.48550/arXiv.2405.01231>.
- 2) Ghafi, H. K., Spindelberger, C. & Arthaber, H. (2021). Modeling of co-channel interference in bluetooth low energy based on measurement data. EURASIP Journal on Wireless Communications and Networking, 2021: 143. <https://doi.org/10.1186/s13638-021-02005-2>.
- 3) Yoon, Y., Jung, C., Seo, J., Li, J., Kim, J., Jin, S., Silva, N. & Han, K. (2016). A Fast Adaptive Frequency Hopping Scheme Mitigating the Effect of Interference in Bluetooth Low Energy Networks. In Lecture Notes in Computer Science (pp. 196–204). Springer. https://doi.org/10.1007/978-3-319-49178-3_15.
- 4) So, J. & Kim, Y. (2016). Interference-aware frequency hopping for Bluetooth in crowded Wi-Fi networks. Electronics Letters, 52(17). <https://doi.org/10.1049/el.2016.1773>.
- 5) Liang, X.-h. & Cheng, L. (2013). On the Research of Adaptive Frequency Hopping in the Wireless Communication. ICCSEE 2013. <https://doi.org/10.2991/iccsee.2013.522>.
- 6) Kim, K. & Stüber, G. L. (2004). Interference Mitigation in Asynchronous Slow Frequency Hopping Bluetooth Networks. Wireless Personal Communications, 28, 143–159. <https://doi.org/10.1023/B:WIRE.0000021421.50247.f0>.
- 7) Poirot, V. & Landsiedel, O. (2021). eAFH: Informed Exploration for Adaptive Frequency Hopping in Bluetooth Low Energy. arXiv. <https://doi.org/10.48550/arXiv.2112.03046>.

Історія статті:

Отримано: 13.08.2026 Доопрацьовано: 26.08.2026 Прийнято до друку: 23.09.2026 Опубліковано: 29.09.2026