УДК 004.052.2+004.056 DOI: 10.31673/2412-4338.2025.013623

Соколов Володимир Юрійович
Київський столичний університет імені Бориса Грінченка, м. Київ
ORCID 0000-0002-9349-7946

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ БЕЗПРОВОДОВИХ СИСТЕМ ДО АТАК ГЛУШІННЯ

***Анотація**: Забезпечення стійкості безпроводових систем до атак глушіння є критично важливим завданням у сучасних умовах активного розвитку технологій безпроводового зв'язку. Атаки глушіння порушують роботу безпроводових мереж, спричиняючи втрату пакетів даних та зниження якості з'єднання. Такі атаки можуть мати різні цілі, включаючи порушення зв'язку, саботаж державних і корпоративних систем, отримання несанкціонованого доступу, шпигунство та підтримку кібервійни. Зловмисники можуть використовувати потужні передавачі, програмно-визначені радіостанції та інші засоби для створення перешкод у певних частотних діапазонах. У статті представлено результати експериментальних досліджень впливу атак глушіння на безпроводові мережі стандартів ZigBee, BLE і Wi-Fi. Проведено тестування стійкості зазначених технологій до перешкод, з використанням SDR-пристроїв для моніторингу спектру та оцінки ефективності атак. Аналіз отриманих даних показав, що втрати пакетів у ZigBee-мережах можуть досягати 80%, що значно впливає на швидкість оновлення датчиків. Для BLE-мереж досліджено залежність помилок передачі від потужності сигналу та швидкості передачі даних, що дозволило визначити оптимальні параметри захисту від атак. Зокрема, для зменшення впливу атак глушіння запропоновано підхід, який включає зміну частотного діапазону передачі, використання алгоритмів навчання з підкріпленням для адаптивного вибору параметрів зв'язку, а також використання технології для перенаправлення сигналів завад. Крім того, перспективним напрямком є застосування розумних методів зменшення завад у MIMO системах, які дозволяють протидіяти глушінню без попереднього знання характеристик завадного сигналу. Таким чином, дослідження підтвердило, що захист безпроводових систем від атак глушіння може бути досягнутий шляхом впровадження адаптивних механізмів управління, динамічного перерозподілу ресурсів зв'язку та застосування інтелектуальних методів аналізу сигналів. Використання зазначених підходів сприятиме підвищенню надійності безпроводових мереж та забезпеченню їх безпечного функціонування в умовах можливих загроз.*

***Ключові слова:** глушіння, перешкоди, ZigBee, BLE, Wi-Fi, програмно-визначене радіо, генератор шуму, HackRF One, інтернет речей, безпілотний літальний апарат.*

Sokolov Volodymyr
Borys Grinchenko Kyiv Metropolitan University, Kyiv
ORCID 0000-0002-9349-7946

ENSURING RESILIENCE OF WIRELESS SYSTEMS TO JAMMING ATTACKS

***Abstract**: Ensuring the resistance of wireless systems to jamming attacks is a critical task in today's rapidly developing wireless communication technologies. Jamming attacks disrupt wireless networks, causing the loss of data packets and degradation of connection quality. Such attacks can have various purposes, including disrupting communications, sabotaging government and corporate systems, gaining unauthorized access, espionage, and supporting cyberwarfare. Attackers can use powerful transmitters, software-defined radios, and other means to create interference in certain frequency bands. The article presents the results of experimental studies of the impact of jamming attacks on wireless networks of the ZigBee, BLE, and Wi-Fi standards. The resistance of these technologies to interference was tested using SDR devices to monitor the spectrum and evaluate the effectiveness of the attacks. The analysis of the data obtained showed that packet loss in ZigBee networks can reach 80%, which significantly affects the speed of sensor updates. For BLE networks, the dependence of transmission errors on signal strength and data rate was investigated, which*

allowed us to determine the optimal parameters of protection against attacks. In particular, to reduce the impact of jamming attacks, an approach is proposed that includes changing the frequency range of transmission, using reinforcement learning algorithms for the adaptive selection of communication parameters, and using technology to redirect interference signals. In addition, a promising direction is the use of smart interference reduction methods in MIMO systems that allow counteracting jamming without prior knowledge of the characteristics of the interfering signal. Thus, the study confirmed that the protection of wireless systems from jamming attacks can be achieved by implementing adaptive control mechanisms, dynamic redistribution of communication resources, and the use of intelligent signal analysis methods. The use of these approaches will help improve the reliability of wireless networks and ensure their safe operation in the face of possible threats.

***Keywords**: jamming, interference, ZigBee, BLE, Wi-Fi, software-defined radio, noise generator, HackRF One, Internet of Things, unmanned aerial vehicle.*

1. Вступ. Атака глушіння (jamming attack) – це один з варіантів атаки на відмову в обслуговуванні, яка порушує безпроводовий зв’язок, переповнюючи мережу шкідливими сигналами або шумом. Мета такої атаки залежить від наміру зловмисника. Але в будь-якому разі, основна задача глушіння безпроводового зв’язку – порушити або заблокувати радіосигнали, що досягається шляхом передачі шуму або завад у тому ж діапазоні частот, що й цільова система зв’язку, фактично роблячи її непридатною для використання. Його можна використовувати для порушення зв’язку, саботажу державних і корпоративних систем (в тому числі, й на підприємствах критичної інфраструктури, хоча використання безпроводового зв’язку на таких об’єктах зазвичай обмежене), перехоплення чи маніпулювання даними, отримання несанкціонованого доступу, завдавання фінансової чи репутаційної шкоди або підтримки кібервійни та шпигунства. Зловмисники зазвичай використовують потужні радіосигнали, фальшиві передавачі або програмно-визначені радіостанції ‘software-defined radio’ (SDR), щоб втручатися в роботу мережі.

Стійкість безпроводових систем (в тому числі ZigBee, BLE, Wi-Fi тощо) до атак глушіння може бути значно підвищена за рахунок поєднання адаптивного управління, теоретико-ігрових підходів, динамічних архітектур захисту і передових методів машинного навчання. А так як забезпечення стійкості безпроводових систем до атак типу «глушіння» має вирішальне значення для підтримання безпечного та надійного зв’язку, то для протидії таким атакам в даній статті розглянуті методи глушіння та їхній вплив на безпроводові мережі різних стандартів. Розповсюдження безпроводових технологій обумовлює актуальність і необхідність проведення досліджень в цьому напрямку.

2. Аналіз літературних даних і постановка проблеми. Стратегії протидії завадам використовують різні методи для підтримки стабільності зв'язку та стійкості до атак завад. Безмодельне адаптивне управління використовує алгоритм прогностичної компенсації для забезпечення стабільності системи, незважаючи на завади, зберігаючи помилки відстеження стохастично стабільними [1]. Так в [2] розглядається підхід до багатошарових динамічних ігор, який застосовує байєсівську ігрову модель Стакельберга для оптимізації стратегій управління проти втрат пакетів і зовнішніх збурень. Такий підхід разом із архітектура захисту від рухомих цілей підвищує стійкість шляхом динамічної зміни різних характеристик (тип модуляції та частота каналу) при використанні подвійних каналів зв’язку [3]. Для специфічних систем можна використовувати, наприклад, придушення завад MIMO, яке розглядає завади як шум і використовує придушення завад і попереднє кодування передачі для підтримки зв’язку в системах MIMO-OFDM, як показано в [4]. Найсучаснішим є інтелектуальний захист від завад з глибоким навчанням, який використовує навчання з підкріпленням [5]. Існують також більш специфічні технології, наприклад, Ambient Backscatter, яка дозволяє передавачам перенаправляти сигнали завад для передачі даних або збору енергії, використовуючи навчання з підкріпленням для оптимізації роботи в умовах завад [6].

З точки зору передових технологій також є актуальним розумне зменшення завад в MU-MIMO, яке використовує алгоритми оптимізації для оцінки та протидії завадам без необхідності попереднього знання характеристик цих завад, що значно полегшує відновлення даних [7]. Таким чином глибинне навчання для зменшення завад інтегрує змагальне машинне навчання в когнітивний передавач, вводячи в оману зловмисників шляхом «неправильних» дій для підвищення пропускної здатності [8].

3. Мета і задачі дослідження. Метою дослідження є експериментальна перевірка впливу атак глушіння на безпроводові мережі різних стандартів.

Для досягнення поставленої мети вирішено такі завдання:

– розроблено методи глушіння і реалізовано їх за допомогою апаратного забезпечення;

– побудовані експериментальні катали безпроводового зв'язку;

– досліджено стійкість трьох технологій (ZigBee, BLE і Wi-Fi) до радіозавад.

4. Стійкість безпроводових мереж до атак глушіння. У військовому та оборонному контексті безпроводові перешкоди використовуються, щоб порушити зв'язок, радари чи системи наведення противника, перешкоджаючи його координації. Для забезпечення безпеки та конфіденційності глушіння може запобігти несанкціонованому спілкуванню чи прослуховуванню в конфіденційних зонах, таких як державні чи приватні установи. Крім того правоохоронні органи можуть використовувати його, щоб вивести з ладу вибухові пристрої з дистанційним керуванням або припинити спілкування підозрюваних під час операцій, в тому числі для санкціанованого контролю натовпу та порушення спілкування між протестувальниками або великими групами в певних ситуаціях. Крім того, перешкоди використовуються під час тестування та досліджень для оцінки стійкості безпроводових систем. Також слід зазначити, що глушіння часто є у багатьох країнах незаконним.

4.1. Експериментальне дослідження стійкості ZigBee мережі до атак глушіння

Експеримент базується на атаці глушіння на датчик ZigBee. Пакети приймаються сніфером, який підраховує кількість успішно доставлених пакетів та пакетів з помилками. SDR Nuand bladeRF 2.0 micro xA9 [9] та SDR Console ver. 3.2 [10] для моніторингу спектру. Сигнал регулярно передається кожні (16,2±1,0) секунди, тому кількість втрачених пакетів можна легко підрахувати. В якості тестового пристрою було обрано модуль ZigBee Tuya [11].Оскільки датчики ZigBee передають сигнал у певні моменти часу, глушіння таких сигналів є досить передбачуваним завданням. Збір даних здійснюється за допомогою USB-ключа Texas Instruments CC2531 [12] разом з програмним забезпеченням SmartRF Packet Sniffer ver. 1 [13]. Оскільки пакети від різних датчиків можуть надходити одночасно, всі пакети без зазначення адреси будуть відфільтровані. Успішно прийняті пакети та пакети з помилками зберігаються. Експеримент повторювався для кожного випадку з п'ятьма вимірами протягом 10 хвилин. Після цього результати були усереднені в табл. 1.

Таблиця 1

Результати по загублених пакетах

Глушіння	Втрачені пакети, %		
	Помилка	Загублено	Разом
Без глушіння	6,5	4,3	10,8±6,2
nRF24L01 + nRF24L01	11,4	80,5	91,9±2,7
Portapack FM tone	22,7	62,7	85,4±3,0
Portapack CW sweep	7,0	89,2	96,2±3,0
Portapack Rand CW	13,5	79,5	93,0±3,5
Portapack Rand FSK	13,0	80,5	93,5±3,0
ADF435x	8,1	87,0	95,1±2,2

З результатів експерименту видно, що навіть без атаки втрачається близько 11% пакетів. Під час атаки максимальний результат втрат пакетів припадає на CW розгортку. Таким чином, близько 80% всіх пакетів втрачається через завади, незалежно від типу генерації шуму. Втрата такої кількості пакетів датчиків збільшує час їх оновлення майже в десять разів.

Кожен з генераторів шуму має свої рівні генерації. Наприклад, для Portapack H2 HackRF One у програмі Jammer [14] використовує відносні рівні сигналу. Для визначення рівня підсилення було зроблено два виміри при мінімальному і максимальному рівнях сигналу. Припускаючи, що підсилення відбувається рівномірно по всьому діапазону, можна заповнити кожен з рівнів підсилення. Виберемо чотири рівні для кожного пристрою, як показано в табл. 2. Для nRF24L01+ і ADF435x використовуються значення вбудованих регістрів.

Таблиця 2

Регулювання рівня сигналу на генераторах шуму

Рівень	Генератор шуму					
	nRF24L01 + nRF24L01		Portapack		ADF435x	
	Рівень підсилювача потужності	Коефіцієнт підсилення, дБмВт	Приріст рівень	Коефіцієнт підсилення, дБмВт	R4B0 регістр	Коефіцієнт підсилення, дБмВт
Мінімальний	RF24_PA_MIN	0	0	0	0×24	0
Низький	RF24_PA_LOW	+6	15	+3	0×2C	+3
Високий	RF24_PA_HIGH	+12	31	+6	0×34	+6
Максимальний	RF24_PA_MAX	+18	47	+9	0×3C	+9

Для зручності порівняння в таблиці наведено нормалізовані значення. За результатами вимірювань побудовано графік на рис. 1.

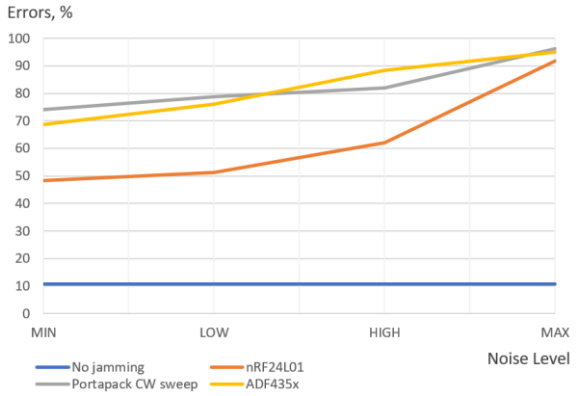

Рис. 1. Залежність кількості помилок від рівня шуму

На графіку видно, що кількість помилок дещо зростає для Portapack і ADF435x, а для nRF24L01+ вона збільшилася на 43,5%. Одним із способів економії енергії може бути передача завади у запланований час передачі. Наприклад, у нашому випадку передача відбувається приблизно раз на 16 секунд, тому заваду можна вмикати лише на час передачі. У цьому випадку визначається момент першої та другої передач, і відраховується час включення завади мінус 6%. Процес повторюється для кожного наступного інтервалу. Єдиним способом боротьби буде збільшення інтервалу між сеансами передачі та рандомізація інтервалів. Навіть якщо кількість датчиків велика, але вони передають короткі сигнали, то один і той самий пристрій може заглушити одразу кілька датчиків [15].

4.2. Експериментальне дослідження стійкості BLE мережі до атак глушіння

В даному дослідженні була використана схема, в якій в якості жертв виступають пристрої BTE Beacon. Активний зловмисник реалізований на мікросхемі Nordic Semiconductor (NS) nRF24L01+ з підсилювачами потужності та низького рівня шуму [16]. Сніффер пакетів налаштований на отримання пакетів від Beacons. Сніффер побудований на базі мікросхеми

Texas Instruments (TI) CC2541 [17]. В якості контрольного пристрою використано аналізатор спектру на базі SDR bladeRf [18]. Сучасні маяки працюють за технологією BLE (Bluetooth 4.2 і вище). Формати повідомлень, що передаються, відрізняються (наприклад, довжина пакета для iBeacon складає 30 байт, Eddystone – 31, AltBeacon – 37) [19, 20], але на даний момент вже доступні пристрої, які можуть працювати з різними форматами одночасно [21]. Обладнання працює в одному частотному діапазоні і за однаковими специфікаціями, тому ми можемо використовувати один і той самий метод глушіння для всіх пристроїв цього типу.

В якості сніффера пакетів використовувався модуль TI CC2541 (існує дві модифікації цього модуля) [17]. Встановлення прошивки для снiфінгу вимагає використання TI CC-Debugger, який, у свою чергу, вимагає оновлення рідної прошивки [22]. Результати снiфінгу можуть бути збережені у вигляді послідовності пакетів, які доступні для подальшого аналізу в програмному забезпеченні SmartRF Packet Sniffer [23]. В якості атакуючого пристрою використовується модуль NS nRF24L01+ [16], який працює в більш широкому діапазоні, ніж потрібно для глушіння BLE. Крім того, не потрібно глушити всі сорок каналів, які передбачені специфікацією, а лише три канали: 37-й (2,402 ГГц), 38-й (2,426 ГГц) і 39-й (2,480 ГГц). Доступні дві модульні модифікації цього зловмисника.

Для реалізації атакуючої сторони було використано проект, описаний в [9]. Модуль Arduino Nano використовується для управління модулем NS nRF24L01+. Зловмисник може працювати автономно із зовнішнім джерелом живлення. Зовнішнє управління для нього не потрібне. На відміну від запропонованого проекту, використовується лише один передавальний модуль. Перед відправкою кожного пакета модуль необхідно повторно ініціалізувати. В результаті кількість пакетів у каналі зменшилася більш ніж у шість разів через час на повторну ініціалізацію. В експерименті використовувався лише 38-й (0×26) канал.

В якості аналізатора спектра використано багатофункціональний SDR Nuand bladeRF [18, 24]. Для отримання спектрограм використовується SDR Console (ver. 3.2, build 2731) [25] з драйвером для цього типу SDR [26]. Дані з аналізатора спектра є коригувальними, але не використовуються для характеристики успішності атаки. Експеримент проводився всередині будівлі. Передавач і приймачі були розташовані на висоті однієї довжини хвилі (~12,5 см) від підлоги і в дальньому полі, що становить мінімум 60 см. За допомогою програми Beacon Simulator для телефонів Android [27] визначено чотири радіомаяки, що знаходяться в зоні досяжності. Такі ж пакети отримані в програмі SmartRF Packet Sniffer [13].

Щоб оцінити межі робочого рівня сигналу жертв, візьмемо модель траєкторії втрат:

$$P_{\text{RX}} = P_{\text{TX}} - 10\,\gamma \lg\left(\frac{r}{r_0}\right) - L_0, \qquad (1)$$

де P_{TX} – потужність передачі, дБмВт; γ – експонента втрат на шляху; r – довжина шляху; r_0 – опорна відстань, $r_0 = 1$ м для мікростільника; L_0 – нормальна випадкова величина [28].

Для нашого експерименту візьмемо середнє значення коефіцієнта втрату $\gamma = 5$ (для приміщень він вибирається в діапазоні від 4 до 6) і довжину шляху $r = 10$ м. Максимальний рівень сигналу передавача $P_{\text{TX max}} = 4$ дБмВт і приймача $P_{\text{RX max}} = -66$ дБмВт [29], тому $L_0 = 10$ дБмВт. Таким чином, пристрої знаходяться в діапазоні від мінус 66 до мінус 100 дБмВт. Спектр сигналу відстежувався для контролю і підтримки незмінності умов експерименту. Миттєвий спектр сигналу в точці прийому було отримано для мінімальної, середньої (рис. 2) та максимальної потужності передавача.

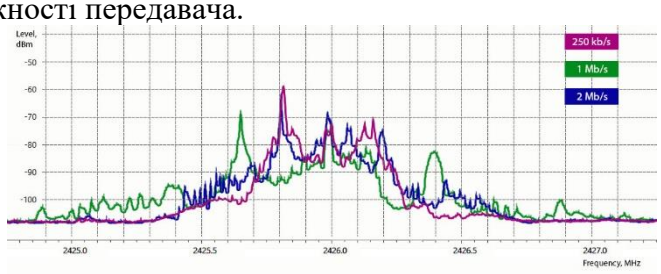

Рис. 2. Потужність передачі спектра $P_{\text{TX}} = -18$ дБмВт для різних швидкостей передачі

З графіків видно, що чим більша швидкість передачі, тим ширшим стає спектр. Це, в свою чергу, призводить до меншої концентрації енергії в каналі BLE, а отже, до зменшення кількості помилок.

Експерименти проводилися для різних рівнів сигналу (0, –6, –12, –18 і –36 дБмВт) і різних швидкостей передачі даних (250 кбіт/с, 1 Мбіт/с і 2 Мбіт/с). Для кожної комбінації експеримент було повторено п’ять разів. Було відправлено 960 пакетів, в результаті чого було проаналізовано кількість отриманих і втрачених пакетів. Отримані пакети були двох типів: цілі та з однією помилкою (CRC дозволяє ідентифікувати такі пакети). Для оцінки результатів використовувався показник Packet Error Rate (PER) як відношення кількості цілих пакетів до загальної кількості відправлених пакетів. Закономірність майже лінійна, як показано на рис. 3.

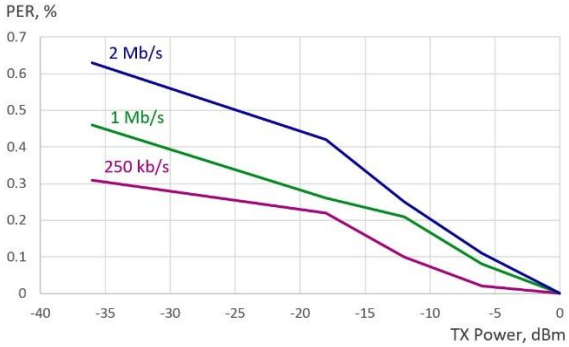

Рис. 3. Залежність PER від потужності передавача та швидкості передачі даних

Перелом графіка відбувається для різних швидкостей передачі даних в діапазоні мінус (20..10) дБмВт. Чим менший переданий пакет, тим пізніше відбувається цей злам. Процес є переривчастим, оскільки пакети з одиничними помилками можуть бути виявлені та виправлені.

Крім того, ми можемо побудувати патерн від пакетів з однією помилкою до втрачених пакетів (рис. 4).

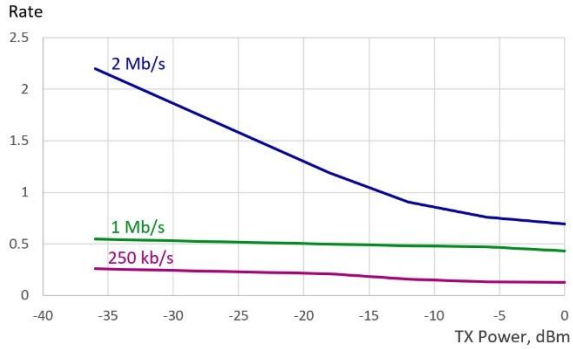

Рис. 4. Співвідношення пакетів з однією помилкою до втрачених пакетів

Зі зменшенням швидкості передачі графік не змінюється, лише для швидкості передачі 2 Мбіт/с, при збільшенні потужності завади більше ніж мінус 12 дБмВт відношення одиночних помилкових пакетів до втрачених стає майже постійним. Як видно з наведених вище графіків, завадостійкість дозволяє майже повністю заглушити передачу інформаційних пакетів. Оскільки для передачі даних з датчиків використовується протокол ZigBee, то одним із способів забезпечення стабільності роботи мережі може бути дублювання на різних частотах або використання гетерогенної безпроводової мережі з пропрієтарними протоколами передачі даних [30, 31].

4.3. Експериментальне дослідження стійкості Wi-Fi мережі до атак вузькосмугового глушіння

Дослідження проводилося на малонавантаженій мережі. Для емуляції трафіку використовувалися 32-байтові ехо-відповіді протоколу ICMP, згенеровані мережевою утилітою *ping*. В якості тестового каналу було обрано 11-й канал Wi-Fi, шириною 22 МГц і середньою частотою 2462 МГц. У даному дослідженні використовувалася схема, в якій точка доступу Wi-Fi була побудована на Raspberry Pi моделі B ver. 2 в якості жертв [32].

Для перевірки працездатності тестової точки доступу використовується програма Wifi Analyzer [33] для ОС Android. Для формування різних перешкод було обрано два методи: апаратний генератор вузькосмугового шуму і SDR для широкосмугового зв'язку. Генератор шуму на базі ADF435x [34] з Pololu Wixel та OLED SSD1306 [35]. Контроль генерованих завад здійснюється за допомогою SDR Nuand bladeRF 2.0 micro xA9 [9] та SDR Console ver. 3.2 [10]. Клієнт побудований на базі мережевої карти Intel Wi-Fi 6E AX211 160 МГц.

В експерименті час доставки шкідливого пакета без завад визначався як базовий, а потім вводилися завади з шириною спектра 300 кГц для частот, що відповідають 10-му, 11-му та 12-му Wi-Fi каналам. Результати наведено в табл. 3.

Таблиця 3

Середній час та кількість помилок при отриманні ICMP-пакетів

Параметр	Частота, МГц			
	без	2457,0±0,3 (10-й канал)	2462,0±0,3 (11-й канал)	2467,0±0,3 (12-й канал)
Час доставки, мс	7,35±1,13	674,39±106,23	8,64±0,70	666,34±137,36
Похибки, %	0	11	0	6

Вузькосмугова завада на 11-му каналі дещо збільшує час проходження сигналу в межах похибки вимірювання, оскільки в середині спектра відсутня одна піднесуча, яка перекривається завадою [36]. При генерації на 10-му і 12-му каналах середній час різко зростає на порядок, і починають з'являтися похибки до 11%. Така поведінка пояснюється перекриттям мінус 21 і 21 пілотної піднесучих і вузькосмугової інтерференції. Оскільки ширина спектра завади становить 300 кГц, а ширина пілотної піднесучої 312,5 кГц, і середня частота двох спектрів відрізняється на 104,2 кГц, завада перекриває пілотний спектр на 65%.

4.4. Експериментальне дослідження стійкості Wi-Fi мережі до атак широкосмугового глушіння

Активний зловмисник реалізований на SDR HackRF One [37] з розширенням Portapack H2 та програмним забезпеченням Jammer [14]. Клієнт і аналізатор спектра використовуються ті ж самі, що і в попередньому експерименті. Генератор Portapack Jammer дозволяє генерувати кілька типів модуляції у вибраному каналі Wi-Fi з різною частотою дискретизації (від 10 Гц до 100 кГц).

Для кожного типу модуляції та частоти було проведено двадцять вимірювань. Кожне вимірювання складалося з 100 ICMP-пакетів. Зафіксовано час проходження пакетів та кількість втрачених пакетів. Середній час проходження пакетів з урахуванням середньоквадратичного відхилення наведено в табл. 4, а графік – на рис. 5.

Таблиця 4

Середній час отримання ICMP-пакетів

Частота, Гц	Середній час доставки посилки, мс			
	FM tone	CW sweep	Rand CW	Rand FSK
10	127.91±15.51	174.27±15.15	117.33±16.59	178.85±28.13
10^2	110.66±18.07	93.61±15.37	133.52±19.26	147.62±14.20
10^3	94.83±17.05	104.52±20.63	133.54±24.74	92.00±9.51
10^4	136.64±18.61	132.47±11.39	129.66±14.72	130.76±14.34
10^5	95.51±13.61	311.20±30.75	155.20±14.49	151.38±17.52

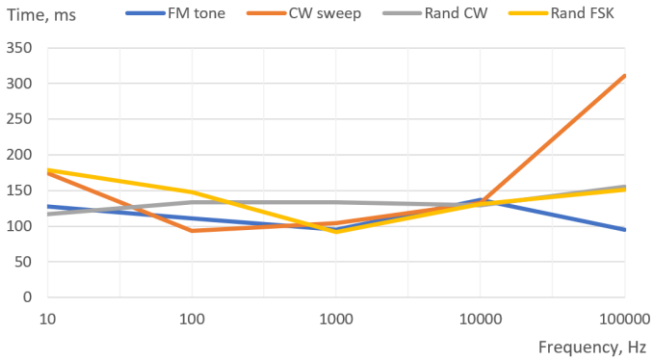

Рис. 5. Залежність середнього часу проходження ICMP-пакету від типу модуляції та частоти

Як видно з рис. 5.10, найбільш підходящою комбінацією для створення завад є CW розгортка на частоті 10 кГц. Крива помилок, показана на рис. 6, дає інші результати: найбільша кількість помилок виникає при випадковій генерації сигналу на частоті 10 Гц.

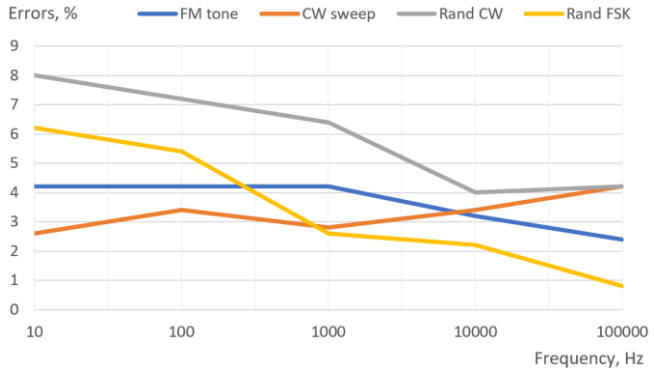

Рис. 6. Залежність кількості помилок від типу модуляції та частоти

Як видно з експерименту, повністю зупинити передачу даних через безпроводову мережу не вдалося, але вдалося зменшити її пропускну здатність [38].

5. Обговорення результатів дослідження

Збільшення рівня сигналу завад може бути непомітним для користувача до певного моменту, коли кількість помилок в системі починає лавиноподібно зростати. Це призводить до збільшення кількості втрачених пакетів і генерування нового трафіку через ретрансляцію. Однак додатковий трафік також піддається впливу завад, тому корисна швидкість передачі даних знижується ще більше. Слід зазначити, що для низьких швидкостей передачі даних співвідношення пакетів з однією помилкою до втрачених пакетів є постійним [32].

Для точок доступу, які працюють у декількох діапазонах, глушіння впливає на продуктивність системи лише частково. Коли атака починається, відбувається різке погіршення якості зв'язку і зависання сигналу, при цьому помітно, що точка доступу і клієнт переходять в інший діапазон. При переході з діапазону 2,4 до 5 ГГц максимальна відстань впевненого прийому зменшується, але повністю придушити роботу такої системи вкрай складно. Крім того, захист від атак глушіння вимагає впровадження таких заходів безпеки, як скачкоподібна зміна частоти, моніторинг сигналів, системи виявлення вторгнень та запобігання вторгненням для виявлення та усунення перешкод у режимі реального часу. Такі системи доступні лише для обмеженої кількості корпоративних користувачів, але відкриті хот-споти та домашні мережі є надзвичайно вразливими до атак глушіння.

Захист від атак типу глушіння вимагає поєднання технічних та операційних заходів: регулярного відстеження рівня сигналу, аналізу шаблонів мережевого трафіку та виявлення аномалій, застосування скачкоподібної зміни частоти, безперервного моніторингу сигналів

для виявлення наявності сигналів перешкод, спеціалізованого обладнання або програмного забезпечення для виявлення та локалізації джерела перешкод [38].

6. Висновки

У роботі були підготовлений тестовий макет з трьома різними типами генераторів шуму для різних безпроводових стандартів. За результатами експерименту для ZigBee були отримані значення кількості помилок, які показують, що під час передачі пакетів втрачається близько 11%. При спрямованому кількість втрачених пакетів може сягати 95%, що призводить до неможливості використання мережі за призначенням. Для BLE при менш ніж 0,7% успішно доставлених пакетів неможливо говорити про успішну роботу навіть некритичного обладнання. З відношення кількості пакетів з однією помилкою до кількості втрачених пакетів видно, що переломний момент на графіку настає при рівні сигналу мінус 12 дБмВт для швидкості передачі 2 Мбіт/с. Для Wi-Fi експериментів із завадами видно, що використання широкосмугових завад не завжди дає кращий результат, ніж вузькосмугових. При використанні вузькосмугових завад з накладенням пілотної піднесучої кількість втрачених пакетів склала 11%, а середній час доставки ICMP-пакету збільшився на порядок. При 15–20% помилок зв’язок з точкою доступу повністю обривався. Якщо точка доступу підтримує можливість переходу на іншу частоту або навіть в інший частотний діапазон, то зв'язок переривається на півхвилини. Широкосмугові перешкоди знижують пропускну здатність приблизно в 19 разів, а втрата пакетів становить в середньому 4%.

В наступних роботах планується шукати залежність між довжиною пакету та кількістю помилок.

Список використаної літератури

1. Qiu X., Wang, Y., Xie X., Zhang H. Resilient Model-Free Adaptive Control for Cyber-Physical Systems Against Jamming Attack. Neurocomputing. 2020. Vol. 413. P. 422–430. DOI: 10.1016/j.neucom.2020.04.043.

2. Zhao L., Xu H., Zhang J., Yang H. Resilient Control for Wireless Cyber–Physical Systems Subject to Jamming Attacks: A Cross-Layer Dynamic Game Approach. IEEE Transactions on Cybernetics. 2020. Vol. 52. P. 2599–2608. DOI: 10.1109/TCYB.2020.3006095.

3. Alshawi A., Satam P., Almoualem F., Hariri S. Effective Wireless Communication Architecture for Resisting Jamming Attacks. IEEE Access. 2020. Vol. 8. P. 176691–176703. DOI: 10.1109/ACCESS.2020.3027325.

4. Yan Q., Zeng H., Jiang T., Li M., Lou W., Hou Y. (2016). Jamming Resilient Communication Using MIMO Interference Cancellation. IEEE Transactions on Information Forensics and Security, 11, P. 1486–1499. DOI: 10.1109/TIFS.2016.2535906.

5. Cao K., Zhengkong H. (2023). Intelligent Anti-Jamming Methods for Wireless Networks. 8th International Conference on Intelligent Computing and Signal Processing (ICSP). 2023. P. 670–674. DOI: 10.1109/ICSP58490.2023.10248518.

6. Van Huynh N., Nguyen D., Hoang D., Dutkiewicz E., Mueck M. Ambient Backscatter: A Novel Method to Defend Jamming Attacks for Wireless Networks. IEEE Wireless Communications Letters. 2020. Vol. 9. P. 175–178. DOI: 10.1109/LWC.2019.2947417.

7. Marti G., Kölle T., Studer C. Mitigating Smart Jammers in Multi-User MIMO. IEEE Transactions on Signal Processing. 2022. Vol. 71. P. 756–771. DOI: 10.1109/TSP.2023.3246226.

8. Erpek T., Sagduyu Y., Shi Y. Deep Learning for Launching and Mitigating Wireless Jamming Attacks. IEEE Transactions on Cognitive Communications and Networking. 2018. Vol. 5. P. 2–14. DOI: 10.1109/TCCN.2018.2884910.

9. Szymaniak J. BladeRF Windows Install Guide. Installing BladeRF Software with MatLab and Simulink Support. 2016. https://www.nuand.com/bladeRF-doc/guides/bladeRF_windows_installer.html

10. SDR-Radio. SDR Console. 2022. https://www.sdr-radio.com/download

11. Tuya. ZTU Module Datasheet. 2022. https://developer.tuya.com/en/docs/iot/ztu-module-datasheet?id=Ka45nl4ywgabp

12. Texas Instruments. A USB-Enabled System-On-Chip Solution for 2.4-GHz IEEE 802.15.4 and ZigBee Applications. 2010. https://www.ti.com/lit/ds/symlink/cc2531.pdf

13. Texas Instruments. SmartRF Packet Sniffer. User's Manual. 2014. https://www.ti.com/lit/ug/swru187g/swru187g.pdf

14. Ried E. Portapack-mayhem. 2022. https://github.com/eried/portapack-mayhem/wiki/Jammer

15. Sokolov V., Skladannyi P., Korshun N. ZigBee Network Resistance to Jamming Attacks. IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics. 2023. P. 161–165. DOI: 10.1109/UkrMiCo61577.2023.10380360.

16. Chen H.-T., Lin P.-Y., Lin C.-Y. A Smart Roadside Parking System using Bluetooth Low Energy Beacons. Advances in Intelligent Systems and Computing. Springer International Publishing. 2019. P. 471–480. DOI: 10.1007/978-3-030-15035-8_44.

17. Hernández-Rojas D., Fernández-Caramés T., Fraga-Lamas P., Escudero C. Design and Practical Evaluation of a Family of Lightweight Protocols for Heterogeneous Sensing through BLE Beacons in IoT Telemetry Applications. Sensors. 2017. Vol. 18, no. 1. P. 57. DOI: 10.3390/s18010057.

18. Feasycom. FeasyBeacon 5Mart FSC-BP104 Bluetooth 5.0 Battery Powered Beacon Datasheet. Ver. 1.4. https://www.feasycom.net/Content/upload/pdf/201913049/FSC-BP104.pdf

19. Apple. Proximity Beacon Specification. Release R1. 2015. https://developer.apple.com/ibeacon/

20. Google. Eddystone. 2016. https://github.com/google/eddystone/tree/master/eddystone-uid

21. AltBeacon. Spec. 2019. https://github.com/AltBeacon/spec

22. Nordic Semiconductor. nRF24L01+. Single Chip 2.4 GHz Tranceiver. Preliminary Product Specification. Ver. 1.0. 2008. https://www.sparkfun.com/datasheets/Components/SMD/nRF24L01Pluss_Preliminary_Product_Specification_v1_0.pdf

23. Ler W. BLE-Jammer. 2020. https://github.com/lws803/BLE-jammer

24. Is Bluetooth Low Energy Jamming Possible with an SDR Like the HackRF on GNURadio? 2020. https://dsp.stackexchange.com/questions/70989/is-bluetooth-low-energy-jamming-possible-with-an-sdr-like-the-hackrf-on-gnuradio

25. Brown S. V3.2 Release Notes. 2022. https://forum.sdr-radio.com:4499/viewtopic.php?f=66&t=1722

26. Picod J.-M. SDRSharp-BladeRF. 2019. https://github.com/jmichelp/sdrsharp-bladerf

27. Hiribarren V. Generate Nearby Notifications using Beacon Simulator. 2017. https://workshop.alea.net/post/2017/10/nearby-notifications-simulator/

28. Klinglmayr J., Bergmair B., Klaffenböck M. A., Hörmann L. B., Pournaras E. Sustainable Consumerism via Context-Aware Shopping. International Journal of Distributed Systems and Technologies. 2017. Vol. 8, no. 4. P. 54–72. DOI: 10.4018/ijdst.2017100104.

29. Kontakt. Beacon Transmission Power, Range, and RSSI. 2020. https://support.kontakt.io/hc/en-gb/articles/4413258518930-Beacon-transmission-power-range-and-RSSI

30. Sokolov V., Kipchuk F., Skladannyi P., Zhyltsov O., Ageyev D. Method for Increasing the Various Sources Data Consistency for IoT Sensors. IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PICST). Oct. 10, 2022. P. 522–526. DOI: 10.1109/picst57299.2022.10238518.

31. Sokolov V., Skladannyi P., Astapenya V. Bluetooth Low-Energy Beacon Resistance to Jamming Attack. IEEE 13th International Conference on Electronics and Information Technologies. 2023. P. 270–274. DOI: 10.1109/ELIT61488.2023.10310815.

32. Kipchuk F., Sokolov V., Buriachok V., Kuzmenko L. Investigation of Availability of Wireless Access Points based on Embedded Systems, IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T). IEEE, Oct. 2019. P. 1–5. DOI: 10.1109/picst47496.2019.9061551.

33. Farproc. Wifi Analyzer. 2023. https://play.google.com/store/apps/details?id=com.farproc.wifi.analyzer

34. Analog Devices. Wideband Synthesizer with Integrated VCO Data Sheet ADF4350. 2016. https://www.analog.com/media/en/technical-documentation/data-sheets/ADF4350.pdf

35. Sokolov V., Skladannyi P., Platonenko A. Video Channel Suppression Method of Unmanned Aerial Vehicles. IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO). IEEE, 10 Oct. 2022. P. 473–477. DOI: 10.1109/elnano54667.2022.9927105.

36. Ward L. 802.11ac Technology Introduction. White Paper. 2012. https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_application/application_notes/1ma192/1MA192_7e_80211ac_technology.pdf

37. Great Scott Gadgets. HackRF. 2023. https://hackrf.readthedocs.io/_/downloads/en/latest/pdf/

38. Sokolov V., Skladannyi P., Astapenya V. Wi-Fi Interference Resistance to Jamming Attack. IEEE 5th International Conference on Advanced Information and Communication Technologies. 2023. P. 1–4. DOI: 10.1109/AICT61584.2023.10452687.