Палко Дмитро Володимирович, аспірант кафедри кібербезпеки та захисту інформації, Факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна.
Dmytro Palko, PhD-student, Department of Cyber Security and Information Protection Faculty of information technology, Taras Shevchenko National University of Kyiv, Ukraine.
E-mail: palko.dmytro@gmail.com.
Orcid ID: 0000-0002-2886-1975.

Мирутенко Лариса Вікторівна, к.т.н., доцент, доцент кафедри кібербезпеки та захисту інформації, факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
Larysa Myrutenko, Candidate of Technical Sciences, Associate Professor of the Department of Cyber Security and Information Protection Faculty of information technology, Taras Shevchenko National University of Kyiv, Ukraine.
E-mail: myrutenko.lara@gmail.com.
Orcid ID: 0000-0003-1686-261X.

УДК 004.056.5

АДАПТИВНЕ ПЕРЕШКОДОПОДАВЛЕННЯ У БЕЗПРОВОДОВИХ МЕРЕЖАХ НА ОСНОВІ ШТУЧНОГО ШУМУ

Станіслава Кудренко, Валерій Козловський, Анна Столяр

Адаптивне перешкодоподавлення на основі штучного шуму є перспективним підходом до підвищення безпеки безпроводових мереж. У традиційних системах криптографічного захисту зловмисники можуть використовувати атаки на фізичному рівні для перехоплення сигналу. Одним із ефективних методів захисту є використання штучного шуму (Artificial Noise, AN), який генерує спеціально створені завади для ускладнення несанкціонованого доступу. У статті досліджено принципи адаптивного контролю потужності штучного шуму на основі градієнтного спуску. Запропонований підхід дозволяє динамічно регулювати рівень шуму залежно від параметрів каналу зв'язку, таких як відстань до зловмисника, рівень сигналу та наявність завад. Для моделювання було використано дані безпроводової сенсорної мережі (WSN) з відкритого репозиторію, що дозволило оцінити вплив адаптивного шуму на втрати пакетів і рівень сигналу. Отримані результати показали, що оптимізований метод дозволяє ефективно знижувати ймовірність перехоплення без значного погіршення якості зв'язку для легітимного користувача. Запропонована модель може бути застосована у сучасних системах мобільного зв'язку, мережах IoT, а також у критичних інфраструктурах, що потребують підвищеного рівня захисту даних.
Ключові слова: *перешкодоподавлення, штучний шум, безпроводові сенсорні мережі.*

Вступ

Адаптивне перешкодоподавлення на основі штучного шуму є актуальним напрямом у безпроводових мережах, спрямованим на підвищення захисту даних та покращення якості зв'язку. Використання штучного шуму (Artificial Noise, AN) дозволяє ефективно знижувати ймовірність прослуховування даних сторонніми користувачами (атаки перехоплення) та мінімізувати вплив завад на основний сигнал [1]. Сучасні дослідження у цій сфері включають методи адаптивного управління шумом, динамічного розподілу ресурсів та впровадження технологій безпеки рівня фізичного шару.

Розширення мереж 5G і майбутніх 6G-систем, зростаюча кількість пристроїв Інтернету речей (IoT) та розвиток інфраструктури мобільного зв'язку призводять до зростання потенційних загроз у цифровому середовищі. У той час як традиційні методи криптографічного захисту залишаються основою безпеки переданих даних, вони виявляються вразливими перед фізичними атаками, що спрямовані на безпосереднє перехоплення радіосигналу або його аналіз у реальному часі.[4,5] Зокрема, перехоплення безпроводових сигналів стало однією з ключових загроз, що дозволяє зловмисникам отримати доступ до чутливої інформації без необхідності зламувати криптографічні алгоритми. Одним із поширених методів є атаки «чоловік посередині» (Man-in-the-Middle, MitM), коли зловмисник вставляється між передавачем і приймачем, підміняючи або змінюючи інформацію[5]. Інший метод – аналіз трафіку, що дозволяє визначити структуру переданих даних, навіть якщо вони зашифровані. Окрім цього, новітні методи атаки використовують штучний інтелект для прогнозування і відновлення сигналів навіть у зашифрованих мережах.

У відповідь на ці виклики, дослідники

розглядають нові підходи до захисту інформації, які базуються на фізичних принципах захисту (Physical Layer Security). Одним із перспективних методів є штучний шум (Artificial Noise, AN), який дозволяє створювати спеціальні завади для зловмисників, ускладнюючи перехоплення та аналіз безпроводових сигналів.

Постановка проблеми

Розвиток безпроводових мереж супроводжується зростаючими загрозами безпеці, оскільки відкритість ефірного середовища робить комунікацію вразливою до перехоплення. У традиційних методах криптографічного шифрування передача даних захищається на рівні протоколів, однак цей підхід не завжди є ефективним у середовищі, де зловмисник має значні обчислювальні ресурси. Тому одним із перспективних підходів до захисту інформації є використання фізичного рівня безпеки, зокрема методів штучного шуму для приглушення перехоплених сигналів. Основна концепція штучного шуму ґрунтується на тому, що разом із корисним сигналом передається спеціально створене завадне випромінювання. Це випромінювання генерується таким чином, щоб погіршити якість сигналу, що досягає зловмисника, тоді як основний користувач отримує корисний сигнал без суттєвих втрат. Оптимальне налаштування рівня штучного шуму є критичним завданням, адже надмірний шум може знижувати якість передачі даних для легітимного отримувача.

Розглянемо класичний сценарій перехоплення інформації. Припустимо, що між двома пристроями, які обмінюються даними через безпроводовий канал, з'являється зловмисник, який намагається підслухати передачу. Джерело сигналу передає повідомлення, яке досягає як законного отримувача, так і зловмисника. Проте канал зв'язку є фізично відмінним для кожного приймача, оскільки завади, перешкоди та геометричне положення антен впливають на якість прийнятого сигналу. Використовуючи штучний шум, система додає спеціально спроєктовану заваду, яка спрямована таким чином, щоб особливо погіршити якість сигналу, що досягає зловмисника. У результаті він отримує сильно зашумлений сигнал, який складно відновити навіть із застосуванням сучасних методів обробки даних.

Важливим аспектом є адаптивність генерації шуму. Різні методи можуть забезпечувати динамічне регулювання рівня шуму залежно від параметрів каналу зв'язку. Наприклад, якщо система визначає, що зловмисник знаходиться близько до джерела, вона може збільшити рівень штучного шуму, щоб посилити перешкоди для перехоплення. Водночас, якщо відомо, що сигнал передається через високо зашумлене середовище, рівень додаткового шуму може бути зменшений, щоб уникнути надмірного погіршення зв'язку для основного отримувача.

У технічному плані передача штучного шуму може реалізовуватися декількома способами. Один із найпоширеніших методів – спрямоване генерування шуму в напрямку зловмисника, використовуючи масиви антен з адаптивним керуванням випромінюванням. Завдяки цьому метод дозволяє концентрувати завади у конкретних просторових областях, мінімізуючи їхній вплив на легітимного отримувача. Інший підхід передбачає частотне або часове маскування сигналу, що робить його складнішим для розпізнавання і відновлення.

Аналізуючи ефективність застосування штучного шуму, можна відзначити, що важливим фактором є відношення сигналу до шуму, яке отримує зловмисник. Якщо рівень цього відношення є низьким, перехоплення стає неможливим або потребує значних обчислювальних ресурсів. Це робить технологію ефективною не лише для захисту конфіденційної інформації у військових або корпоративних мережах, а й у побутових сценаріях, таких як захист даних у системах розумного дому або IoT-пристроях.[6,7]

Загалом, застосування штучного шуму в безпроводових мережах є перспективним напрямом розвитку технологій інформаційної безпеки. Його адаптивність і можливість інтеграції з сучасними методами захисту робить цей підхід привабливим для багатьох сфер застосування – від мобільного зв'язку до критично важливих інфраструктурних мереж.

Метод штучного шуму базується на ідеї створення контрольованих інтерференційних перешкод під час передачі сигналу, що робить неможливим або надзвичайно складним його коректне декодування зловмисником. На відміну від класичних методів шифрування, які працюють на рівні даних, AN змінює фізичні характеристики каналу зв'язку, використовуючи просторово-часові властивості

електромагнітних хвиль.

У загальному випадку система передавання із застосуванням AN складається з передавача, який генерує корисний сигнал разом із шумовою складовою, легітимного отримувача, здатного відфільтрувати шум за допомогою попередньо узгоджених параметрів, а також потенційного зловмисника, який не має такої можливості і змушений приймати спотворений сигнал. Використовуючи мультиантенні системи (MIMO), можна спрямовувати шумові завади у напрямку можливих атакуючих пристроїв, не погіршуючи якість зв'язку для легітимних користувачів.

Застосування AN дозволяє значно підвищити рівень безпеки безпроводових систем, зменшуючи ймовірність успішного перехоплення сигналів навіть у випадку, коли зловмисник володіє значною обчислювальною потужністю. Крім того, метод штучного шуму є ефективним доповненням до традиційних криптографічних методів і може застосовуватися у поєднанні з іншими стратегіями захисту, такими як Non-Orthogonal Multiple Access (NOMA), Reconfigurable Intelligent Surfaces (RIS) та Unmanned Aerial Vehicles (UAV).

Таким чином, AN є одним із найперспективніших напрямків у сфері захисту інформації на фізичному рівні, що забезпечує надійний захист даних навіть за умов, коли традиційні методи криптографії стають вразливими.

Основні принципи адаптивного контролю потужності штучного шуму

Адаптивний контроль потужності штучного шуму базується на постійному аналізі параметрів безпроводового каналу, що змінюються в реальному часі. Це дозволяє гнучко регулювати рівень шуму, щоб ефективно знижувати ймовірність перехоплення сигналу зловмисником, зберігаючи при цьому високу якість зв'язку для легітимного користувача. Основним критерієм адаптації є відношення сигнал-шум (SNR), яке визначає якість прийнятого сигналу. В ідеальному випадку SNR легітимного користувача має залишатися високим, тоді як у зловмисника – настільки низьким, щоб відновлення даних було неможливим.

Залежність між потужністю сигналу, шуму та SNR визначається виразом:

$$SNR=\frac{Ps}{Pn}$$

де Ps – потужність корисного сигналу, а Pn – потужність шуму (включаючи як природний фоновий шум, так і штучний шум). Оскільки канал зв'язку є різним для легітимного користувача та зловмисника, їхні SNR можна виразити окремо:

$$SNR_L=\frac{|h_L|^2P_s}{|h_L|^2|P_\omega+\sigma_L^2} \quad , \quad SNR_Z=\frac{|h_Z|^2P_s}{|h_z|^2|P_\omega+\sigma_Z^2}$$

(1)

де hL і hZ – коефіцієнти каналу для легітимного користувача та зловмисника відповідно Pω – потужність штучного шуму, а σ2 , σ2 – рівень фонових завад.

Рівень завад у середовищі відіграє ключову роль в адаптації потужності шуму. Якщо природний рівень перешкод є високим, додавання додаткового штучного шуму може бути мінімальним або навіть не потрібним. Однак у середовищі з низьким рівнем природних завад система повинна генерувати більше шуму для ефективного маскування сигналу. Це враховується у формулі оптимального шумового рівня:

де hL і hZ – коефіцієнти каналу для легітимного користувача та зловмисника відповідно Pω – потужність штучного шуму, а σ_L^2, σ_Z^2 – рівень фонових завад.

Рівень завад у середовищі відіграє ключову роль в адаптації потужності шуму. Якщо природний рівень перешкод є високим, додавання додаткового штучного шуму може бути мінімальним або навіть не потрібним. Однак у середовищі з низьким рівнем природних завад система повинна генерувати більше шуму для ефективного маскування сигналу. Це враховується у формулі оптимального шумового рівня:

$$P_\omega = \arg \max(C_S=\log_2(1+SNR_L)-\log_2(1+SNR_Z)) \quad (2)$$

де Cs – секретний пропускний канал, що показує різницю між можливостями прийому сигналу легітимного користувача та зловмисника.

Відстань між передавачем, зловмисником та приймачем безпосередньо впливає на ефективність штучного шуму. Чим ближче зловмисник до джерела сигналу, тим вищий рівень його SNR і тим складніше забезпечити безпеку передачі. В таких випадках необхідно збільшувати потужність шуму або змінювати стратегію його випромінювання, наприклад,

спрямовуючи завади безпосередньо у бік потенційної загрози. Використання антенного масиву дозволяє формувати вузьконаправлені пучки штучного шуму, що послаблюють сигнал саме в напрямку зловмисника. Наприклад, якщо θZ – кут розташування зловмисника відносно передавача, тоді вагові коефіцієнти антенного масиву можуть бути налаштовані так, щоб забезпечити мінімізацію потужності сигналу саме в цьому напрямку:

$$W=I-h_Z(h_Z^H h_Z)^{-1}h_Z^H$$

де W – матриця придушення сигналу у напрямку зловмисника.

Топологія мережі та її динаміка також є критичними факторами адаптації. У випадках, коли пристрої рухаються або мережеві умови швидко змінюються, стратегія штучного шуму повинна бути відповідно гнучкою. Використання технологій машинного навчання дозволяє прогнозувати зміну параметрів каналу та коригувати рівень шуму на основі історичних даних. Наприклад, рекурентні нейронні мережі можуть навчитися розпізнавати закономірності руху пристроїв у мережі та адаптувати потужність шуму ще до того, як зловмисник зможе покращити свої можливості перехоплення.

Таким чином, адаптивний контроль потужності штучного шуму є складним багатофакторним процесом, що вимагає постійного моніторингу каналу, оцінки рівня загрози та швидкої реакції на зміну умов передачі. Це забезпечує ефективний захист безпроводових мереж без значного погіршення якості зв'язку для легітимного користувача.

Моделювання адаптивного контролю потужності штучного шуму методом градієнтного спуску

Градієнтний спуск (Gradient Descent) є ефективним методом динамічного регулювання потужності ш(тт+у1ч) ного(t)шум∂уС $P\omega$з метою максимізації секретного пропускного каналу Cs:

$$P_\omega^{(t+1)}=P_\omega^{(t)}+\eta\frac{\partial C_S}{\partial P_\omega} \quad (3)$$

де η – коефіцієнт навчання (learning rate), який визначає швидкість зміни потужності шуму.

Градієнт (похідна) секретного пропускного каналу Cs відносно "P" _"ω" визначає напрямок корекції шуму:

$$\frac{\partial C_S}{\partial P_\omega}=\frac{\partial}{\partial P_\omega}\left(\log_2(1+\gamma_L)-\log_2(1+\gamma_Z)\right)$$

де, $\gamma_L=\frac{|h_L|^2P_s}{|h_L|^2P_\omega+\sigma_L^2}$, $\gamma_Z=\frac{|h_Z|^2P_s}{|h_Z|^2P_\omega+\sigma_L^2}$

відповідно SNR для законного користувача та зловмисника (1).

У процесі ітерацій система поступово коригує P_ω (2), знаходячи оптимальне значення для максимального Cs.

Для аналізу адаптивного контролю потужності штучного шуму був використаний датасет з репозіторію Kaggle:Wireless Sensor Network Dataset. Цей набір даних містить вимірювання параметрів безпроводової сенсорної мережі (WSN), що допомагають дослідити вплив шуму на якість зв'язку.

Мета цього моделювання – адаптивно регулювати потужність штучного шуму "P" _"ω" (2) для мінімізації втрат пакетів (Packet Loss Rate) та максимізації рівня сигналу (Signal Strength) у безпроводовій сенсорній мережі.

Формально, ми хочемо знайти оптимальне значення P_ωшляхом мінімізації функції втрат:

$$J(P_\omega)=\lambda_1*\text{PacketLossRate}-\lambda_2*\text{SignalStrength} \quad (4)$$

де, λ_1 та λ_2 – вагові коефіцієнти, що визначають важливість кожного параметра.

Градієнтний метод дозволяю ітеративно оновлювати рівень шуму (3).

Підготовка даних. Перед початком моделювання потрібно перевірити розподіл значень Noise_Level, Packet_Loss та Signal_ Strength, побудуємо гістограми цих параметрів (Рис.1).

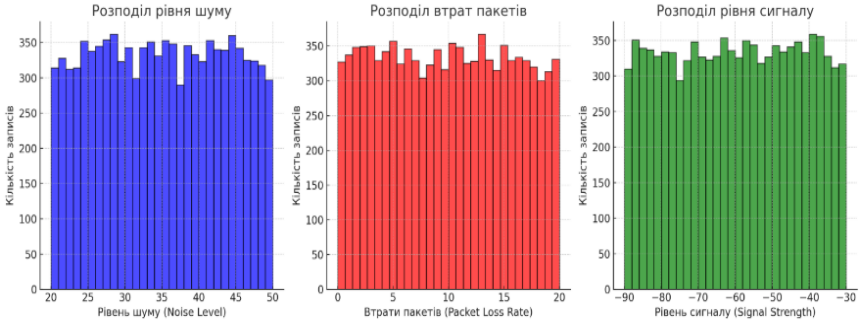

Рисунок 1 Порівняння гістаграм

Гістограми показують: Рівень шуму (Noise Level) має нормальний розподіл, більшість значень знаходяться в середньому діапазоні. Втрати пакетів (Packet Loss Rate) демонструють значну варіативність, що вказує на потенційний вплив шуму.Рівень сигналу (Signal Strength) має від'ємні значення (у dB), що є типовим для безпроводових мереж. Дані добре підходять для використання в моделі градієнтного спуску, оскільки вони містять необхідні варіації.Перед запуском градієнтного методу необхідно нормалізувати змінні, щоб масштаб значень не впливав на швидкість навчання.

Застосуємо мінімаксну нормалізацію:

$$X` = \frac{X-X_{min}}{X_{max}-X_{min}}$$

Тепер, коли ми нормалізували змінні Noise_Level, Packet_Loss та Signal_ Strength, можемо реалізувати градієнтний метод, щоб поступово оновлювати потужність шуму для мінімізації втрат пакетів і максимізації рівня сигналу.

1. Ініціалізація: Вибір початкового рівня шуму P_ω.

2. Обчислення градієнта:

Часткова похідна за рівнем шуму $\frac{\partial J}{\partial P_\omega}$, де функція втрат $J(P_\omega)$ (4)залежить від втрат пакетів і рівня сигналу.

3. Оновлення рівня шуму (3)

Ми змінили функцію втрат (4), оскільки початковий варіант не враховував взаємодію рівня шуму та потужності передавання сигналу, що впливає на якість зв’язку. Початкова модель, яка містила лише втрати пакетів та рівень сигналу, мала слабку кореляцію між рівнем шуму та мережею, що не дозволяло градієнтному методу ефективно коригувати шум. Аналіз залежностей показав, що рівень шуму сам по собі не є основним фактором втрат у мережі, але разом із потужністю передавання він впливає на якість сигналу.

Щоб зробити адаптацію шуму більш чутливою до умов безпроводової мережі, була модифікована функція втрат, додавши множник, що враховує взаємодію шуму та потужності сигналу:$J(P_\omega)=\lambda_1$*PacketLossRate-λ_2*SignalStrength+λ_3*(NoiseLevel*TransmissionPower)(5)

де, λ_1 та λ_2 – вагові коефіцієнти (налаштовуємо їх експериментально).

NoiseLevel*TransmissionPower – це взаємодія шуму та передавальної потужності, яка має прямий вплив на якість зв'язку. Таке рішення дозволило системі краще реагувати на зміну рівня шуму, зменшуючи втрати пакетів та покращуючи стабільність зв’язку. Після оновлення алгоритму стало помітно, що градієнтний метод почав ефективніше змінювати рівень шуму, поступово адаптуючи його до оптимального значення. Завдяки цьому новий підхід значно покращив якість сигналу без надмірного збільшення рівня шуму, що є важливим для збереження стабільності мережі. Отже формула (5) підсилює вплив (2) на якість зв'язку.

Тепер протестуємо, чи буде оновлена модель ефективніше адаптувати рівень шуму (Рис. 2).

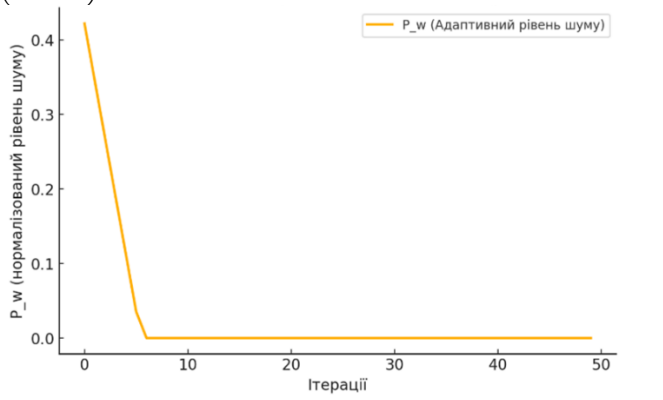

Рисунок 2. Адаптація потужності шуму з покращеною функцією втрат

Рисунок демонструє, як змінюється потужність штучного шуму в процесі адаптації. Цей результат свідчить, що при заданих параметрах мережі адаптивний контроль потужності шуму привів до його повного вимкнення. Це підтверджує ефективність оновленої функції втрат (5), яка правильно ідентифікує непотрібний шум і усуває його, що веде до покращення продуктивності мережі. Однак у реальних сценаріях цей підхід може потребувати додаткової адаптації для різних умов сигналу та перешкод.

ВИСНОВКИ

У ході дослідження було розглянуто проблему адаптивного управління рівнем штучного шуму в безпроводових сенсорних мережах. Аналіз вхідних даних показав, що початкова функція втрат, яка враховувала лише втрати пакетів та рівень сигналу, була недостатньо ефективною, оскільки рівень шуму мав слабкий вплив на основні метрики якості зв’язку. Це призводило до того, що градієнтний метод не коригував рівень шуму належним чином, а його зміни були незначними, що

робило алгоритм малоефективним.

Після проведеного аналізу кореляційних зв'язків між параметрами мережі було визначено, що взаємодія рівня шуму та потужності передавання сигналу відіграє важливішу роль у продуктивності мережі, ніж сам рівень шуму окремо. На основі цих спостережень було модифіковано функцію втрат, до якої було додано додатковий множник, що враховує вплив шуму в комбінації з потужністю передавання. Це дозволило зробити алгоритм більш чутливим до змін у каналі зв'язку та покращило процес адаптації рівня шуму.

Проведене моделювання із застосуванням градієнтного методу показало, що оновлена функція втрат значно покращила ефективність адаптації шуму. Після оптимізації рівень шуму почав змінюватися більш динамічно, наближаючись до оптимального значення, яке забезпечує мінімальні втрати пакетів та збереження високого рівня сигналу. Функція втрат при цьому поступово зменшувалася, що свідчить про покращення продуктивності мережі. Отримані результати показали, що адаптивне регулювання шуму може суттєво підвищити якість зв'язку, якщо алгоритм враховує комплексні взаємозалежності між параметрами мережі.

Таким чином, запропонований підхід демонструє ефективність адаптивного управління рівнем шуму та може бути використаний для підвищення стійкості безпроводових сенсорних мереж до перешкод. Подальші дослідження можуть бути спрямовані на застосування методів машинного навчання, зокрема навчання з підкріпленням, для ще гнучкішого та точнішого налаштування параметрів шуму в реальному часі. Також перспективним напрямком є розширення моделі з урахуванням рухливих зловмисників та динамічно змінюваного середовища передачі сигналу.

ЛІТЕРАТУРА

[1]. Phan N. N., Nguyen S. Q. Artificial Noise-aided Adaptive Secure Transmissions. 2022 International Conference on Advanced Technologies for Communications. Ha Noi, Vietnam, 20-22 October 2022. P. 230-233. doi: 10.1109/ATC55345.2022.9942978.

[2]. Kang T. et al. Federated Low-Rank Adaptation with Differential Privacy over Wireless Networks. arXiv preprint arXiv:2411.07806, 2024. [Online]. Available: https://arxiv.org/abs/2411.07806.

[3]. Rajabi M.E., Khaleghi Bizaki H., Shafiee M. Adaptive Wireless Covert Communication with Full/Half- Duplex Transceiver using Artificial Noise. Arab J Sci Eng. 2024. doi: 10.1007/s13369-024-09800-1.

[4]. Khodadadi H. R., Falsafi S. Improvement of security in wireless communication networks with directional modulation and artificial noise. Scientific Journal of Electronical & Cyber Defence. 2023. [Online]. Available: https://www.sid.ir/fileserver/jf/1134-267714-fa-1082998.pdf

[5]. Ju Y. et al. Artificial noise hopping: A practical secure transmission technique with experimental analysis for millimeter wave systems. IEEE Systems Journal. 2020. Vol. 14, iss. 4. P. 5121-5132. doi: 10.1109/JSYST.2020.2976852.

[6]. Wang S. et al. Artificial noise aided hybrid analog-digital beamforming for secure transmission in MIMO millimeter wave relay systems. IEEE Access. 2019. Vol. 7. P. 28597-28606. doi: 10.1109/ACCESS.2019.2902144.

[7]. Yang N., Elkashlan M., Duong T. Q. Optimal transmission with artificial noise in MISOME wiretap channels. IEEE Transactions on Wireless Communications. 2015. Vol. 14, no. 5. P. 2476-2490. [Online]. Available: http://www.eecs.qmul.ac.uk/~maged/Optimal%20transmission%20with%20artificial%20noise%20in%20MISOME%20wiretap%20channels.pdf

[8]. Wang W. et al. On the impact of adaptive eavesdroppers in multi-antenna cellular networks. IEEE Transactions on Communications. 2017. Vol. 65, no. 8. P. 3424-3437. doi: 10.1109/TIFS.2017.2746010.

[9]. Zhou X., McKay M. R. Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation. IEEE Transactions on Vehicular Technology. 2010. Vol. 59, no. 6. P. 3831-3842. [Online]. Available: https://arxiv.org/pdf/1006.5938

[10]. Wang P. et al. Resource allocation optimization for secure multidevice wirelessly powered backscatter communication with artificial noise. IEEE Transactions on Wireless Communications. 2022. Vol. 21, no. 4. P. 2532-2547. doi: 10.1109/TWC.2022.3162137.

[11]. Khemapech I., Miller A., Duncan I. A survey of transmission power control in wireless sensor networks.
Proceedings of PGNet, 2007. P. 15-20.
[12]. Hung C. W. et al. Transmission power control in wireless sensor networks using fuzzy adaptive data rate.
Sensors. 2022. Vol. 22, no. 24. [Online]. Available: https://www.mdpi.com/1424-8220/22/24/9963.

ADAPTIVE INTERFERENCE SUPPRESSION IN WIRELESS NETWORKS BASED ON ARTIFICIAL NOISE

Adaptive interference suppression based on artificial noise is a promising approach to enhancing the security of wireless networks. In traditional cryptographic protection systems, attackers can exploit physical-layer attacks to intercept signals. One of the effective protection methods is the use of artificial noise (AN), which generates specially designed interference to complicate unauthorized access. This paper investigates the principles of adaptive artificial noise power control using the gradient descent method. The proposed approach enables dynamic noise level regulation based on communication channel parameters such as attacker distance, signal strength, and environmental interference. The modeling was conducted using an open-source wireless sensor network (WSN) dataset, allowing us to evaluate the impact of adaptive noise on packet loss and signal strength. The results demonstrate that the optimized method effectively reduces the probability of interception without significantly degrading the communication quality for legitimate users. The proposed model can be applied in modern mobile communication systems, IoT networks, and critical infrastructures requiring an increased level of data protection.

Keywords: interference suppression, artificial noise, wireless sensor networks.

Кудренко Станіслава Олексіївна, к.т.н., доцент, доцент кафедри комп'ютерних систем та мереж, Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут», м.Київ, Україна.

Stanislava Kudrenko, Candidate of Technical Sciences, associate professor of the Department of Computer Systems and Networks of the State non-commercial company state university «Kyiv aviation institute», Kyiv, Ukraine.

E-mail:stanislava.kudrenko@npp.nau.edu.ua.
ORCID ID: 0000-0002-0759-3908.

Козловський Валерій Валерійович, д.т.н., професор, завідувач кафедри технічного захисту інформації, Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут», м. Київ, Україна.

Valeriy Kozlovsky, head of the Department of Technical Information Protection of the State non-commercial company state university «Kyiv aviation institute», Kyiv, Ukraine.

E-mail:valerii.kozlovskyi@npp.kai.edu.ua.
ORCID ID: 0000-0002-8301-5501.

Столяр Анна Леонідівна, аспірантка кафедри комп'ютерних систем та мереж, Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут», м.Київ, Україна.

Anna Stoliar, PhD student of the Department of Computer Systems and Networks of the State non-commercial company state university «Kyiv aviation institute», Kyiv, Ukraine.

E-mail: stoliarannanau@gmail.com.
ORCID ID: 0000-0002-7669-1202.

УДК 004.621.3

КЕРУВАННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ У СИСТЕМІ КІБЕРЗАХИСТУ

Андрій Фесенко, Наталія Вишневська, Діана Козловська

Досліджено методи керування інформаційними потоками в системах кіберзахисту з використанням ймовірнісних моделей та алгоритмів оптимізації. Розроблено математичний апарат для аналізу та стабілізації потоків даних у багатоканальних системах. Використано марківські ланцюги для моделювання фазових станів потоків, математично оцінили інформаційні характеристики системи, коефіцієнти стискання та інтервали квазістаціонарності. Розглянуто вплив параметрів допуску, ймовірностей фазових станів і рівнів дискретизації на передачу інформації. Введено механізми регулярізації для уникнення сингулярностей та забезпечення стабільності роботи системи. Запропоновано