DOI: 10.58254/viti.6.2024.01.5

УДК 621.396

Артюх С. Г. ORCID: 0000-0003-2142-1552 (ВІТІ ім. Героїв Крут)
д-р техн. наук, професор Жук О. В. ORCID: 0000-0002-3546-1507 (НУОУ)
канд. техн. наук, доцент Симоненко О. А. ORCID: 0000-0001-8511-2017 (ВІТІ ім. Героїв Крут)
Марченко П. А. ORCID: 0009-0006-7261-6316 (НТУУ "КПІ ім. Ігоря Сікорського")

МОДЕЛІ ТА МЕТОДИ ВИЯВЛЕННЯ ВТОРГНЕНЬ У БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ ВІЙСЬКАМИ

Безпроводові сенсорні мережі є важливим елементом сучасних військових операцій, що забезпечують моніторинг та передачу даних у реальному часі. Однак ці мережі вразливі до фізичних і кібератак через обмеженість ресурсу, відсутність фізичного контролю над сенсорами та викликами, що пов'язані з використання безпроводових каналів зв'язку. Метою статті є проведення порівняльного аналізу моделей та методів виявлення вторгнень у безпроводових сенсорних мережах тактичної ланки управління військами.

Аналіз охоплює централізовані та децентралізовані підходи до управління безпекою з акцентом на моделі виявлення, що базуються на сигнатурах, аномаліях та специфікаціях. Також у статті розкрито можливості використання гібридних методів, що комбінують переваги вищезазначених підходів. Для порівняння ефективності моделей використовувалися загальнодоступні набори даних (KDD, NSL-KDD, WSN-DS) та синтетичні набори даних отриманих з використанням мережевих симуляторів. Результати показують, що централізовані моделі більш ефективні для малих мереж, але створюють навантаження на базову станцію, що може спричиняти затримки при виявленні атак. Децентралізовані моделі знижують навантаження та підвищують швидкість реагування на атаки, проте також мають свої недоліки. У статті зазначено, що жоден з існуючих методів не забезпечує повного захисту, тому комбінування підходів є найбільш ефективним рішенням.

Моделі та методи виявлення вторгнень на основі аномалій класифікуються залежно від їх функціональних можливостей: на основі статистики, на основі інтелектуального аналізу даних, на основі машинного навчання та на основі штучного інтелекту. Використання штучних нейронних мереж і машинного навчання значно покращує точність виявлення аномалій, але такі системи вимагають великих обчислювальних ресурсів та складні в налаштуванні.

Основний аналітичний висновок статті полягає в необхідності створення гібридної системи виявлення вторгнень з використанням штучних нейронних мереж і машинного навчання, яка поєднує централізовані та децентралізовані методи з урахуванням специфічних загроз для безпроводових сенсорних мереж тактичної ланки управління військами.

Напрямом подальших досліджень слід вважати розроблення функціональної моделі системи виявлення вторгнень для підсистеми безпеки у безпроводових сенсорних мережах тактичної ланки управління військами.

Ключові слова: *безпроводові сенсорні мережі, виявлення вторгнень, управління безпекою, тактична ланка управління, нейронні мережі, виявлення аномалії.*

S. Artiukh, O. Zhuk, O. Simonenko, P. Marchenko Models and methods of intrusion detection in wireless sensor networks of the tactical level of troop control

Wireless sensor networks are an important element of modern military operations, providing real-time monitoring and data transmission. However, these networks are vulnerable to both physical and cyber attacks due to limited resources, lack of physical control over the sensors, and challenges associated with using wireless communication channels. The aim of the article is to conduct a comparative analysis of models and methods for intrusion detection in tactical command-level wireless sensor networks.

The analysis covers centralized and decentralized security management approaches with a focus on detection models based on signatures, anomalies, and specifications. The article also explores the potential of using hybrid methods that combine the advantages of the aforementioned approaches. Publicly available datasets (KDD, NSL-KDD, WSN-DS) and synthetic datasets generated using network simulators were used to compare the effectiveness of the models. The results show that centralized models are more effective for small networks but create a load on the base station, which can cause delays in attack detection. Decentralized models reduce the load and improve the speed of response to attacks, but they also have their drawbacks. The article notes that none of the existing methods provide complete protection, so a combination of approaches is the most effective solution.

Anomaly-based intrusion detection models and methods are classified according to their functional capabilities: statistics-based, data mining-based, machine learning-based, and artificial intelligence-based. The use of artificial neural networks and machine learning significantly improves the accuracy of anomaly detection, but such systems require large computational resources and are complex to configure.

The main analytical conclusion of the article is the need to create a hybrid intrusion detection system using artificial neural networks and machine learning, which combines centralized and decentralized methods while considering specific threats to tactical command-level wireless sensor networks.

Future research should focus on developing a functional model of an intrusion detection system for the security subsystem in tactical command-level wireless sensor networks.

Keywords: *wireless sensor networks, intrusion detection, security management, tactical control link, artificial neural networks, signature analysis, cryptographic methods, anomaly detection.*

Постановка завдання. Безпроводові сенсорні мережі (*Wireless Sensor Networks*) є різновидом розподілених мереж, що складаються з вузлів (сенсорів), з інтегрованими функціями моніторингу параметрів навколишнього середовища, обробки і передачі даних.

У безпроводових сенсорних мережах (БСМ) тактичної ланки управління військами існують специфічні вразливості, а саме:

− необхідність компромісного використання бездротових каналів зв'язку (дає змогу зловмиснику створювати активні та пасивні завади, здійснювати перехоплення й аналіз мережевого трафіку, спотворювати або знищувати пакети на найбільш завантажених каналах);

− відсутність фізичного контролю сенсорів (дає змогу зловмиснику отримати фізичний доступ до компонентів БСМ завдяки чому є змога підміни, захоплення або знищення вузлів).

− динамічні умови побудови топології, децентралізованого управління та процесів масштабування (ускладнюють процедуру сертифікації, реалізацію систем виявлення вторгнень, тощо);

− обмеженість ресурсів вузлів (ускладнюють реалізацію надійних механізмів безпеки та впровадження стійких криптографічних алгоритмів).

Наявність зазначених особливостей створює низку передумов для реалізації фізичних і кібернетичних атак на БСМ та висуває вимоги до розроблення ефективних підходів виявлення вторгнень, з урахуванням особливостей динаміки середовища функціонування мереж такого типу.

Вторгнення – це несанкціонований доступ до інформації, зміна інформації, скидання частини пакетів і перенаправлення на наступні вузли мережі. Захист від зовнішніх атак містить застосування криптографічних методів: шифрування інформації, використання цифрового підпису та ін. Водночас, криптографічні методи не мають змоги забезпечити захист від впливу противника за наявності скомпрометованих або захоплених вузлів. Для захисту від внутрішніх атак передбачається використання моделей та методів виявлення вторгнень у безпроводових сенсорних мережах [1].

Аналіз останніх досліджень і публікацій. У роботі [2] проведено дослідження енергоефективних методів виявлення вторгнень у БСМ, проведено їх класифікації та розглянуто різні підходи до управління безпекою мережі. Проте автори не проводять аналіз типів атак та на яких рівнях моделі Open Systems Interconnection (OSI) функціонують такі методи. Водночас у статті [3] проведено аналіз вразливостей, основних і додаткових вимог з безпеки БСМ та запропоновано класифікацію атак (характер дій, рівень моделі відкритих систем, мета впливу, об'єкт управління, позиціонування відносно мережі, тип атакуючого пристрою). Запропоновано класифікацію та проведено аналіз існуючих атак у безпроводових сенсорних мережах тактичної ланки управління військами, що дає змогу досліджувати моделі та методи виявлення вторгнень.

У роботах [4, 5, 6] проведено аналіз методів і моделей виявлення вторгнень для БСМ за останнє десятиліття, проте не враховано інтеграцію штучних нейронних мереж в галузі. Слід зазначити, що у [7] автори аналізують сучасні підходи, що ґрунтуються на штучних імунних системах, штучних нейронних мережах та генетичних алгоритмах стосовно виявлення атак певних типів, а саме: відмови в обслуговуванні, витоки інформації та аномалії мережі. Водночас інші атаки, зокрема на БСМ тактичної ланки управління військами не розглядаються.

Метою роботи є проведення порівняльного аналізу моделей та методів виявлення вторгнень у безпроводових сенсорних мережах тактичної ланки управління військами, їх основних переваг і недоліків для удосконалення підсистеми управління безпекою у таких мережах.

Виклад основного матеріалу дослідження. Виявлення вторгнень може здійснюватися в умовах централізованого або децентралізованого управління [2].

При централізованому управлінні всі дані з вузлів збираються та передаються до центрального вузла або базової станції (БС) для подальшої обробки та виявлення аномалій. Тобто всі сенсори виконують функції збору інформації, а процес аналізу, прийняття рішень та виявлення вторгнень здійснюється на рівні БС.

У децентралізованих моделях обробка даних і виявлення аномалій здійснюється на рівні сенсорних вузлів, що знижує навантаження на центральний вузол і зменшує кількість переданих даних. Кожен сенсорний вузол або група вузлів мають свої програмні засоби, які здійснюють локальне виявлення вторгнень і лише при виявленні атаки передають інформацію на вищий рівень до голови кластера (ГК) і БС.

Сьогодні існує декілька загальнодоступних еталонних наборів даних (DARPA, KDD, NSL-KDD та WSN-DS та інші), що використовуються для перевірки ефективності виявлення вторгнень. Також для якісного моделювання поведінки БСМ за звичайного сценарію та сценарію атаки дослідники створюють власний набір даних за допомогою мережевих симуляторів NS2, NS3, OMNeT, Cooja, TOSSIM тощо.

За функціональністю моделі та методи виявлення вторгнень класифікуються за такими групами: на основі сигнатур, на основі аномалій, на основі специфікації та гібридні [6].

Класифікація моделей та методи виявлення вторгнень для БСМ тактичної ланки управління військами з урахуванням методів машинного навчання та штучних нейронних мереж наведена на рисунку 1.

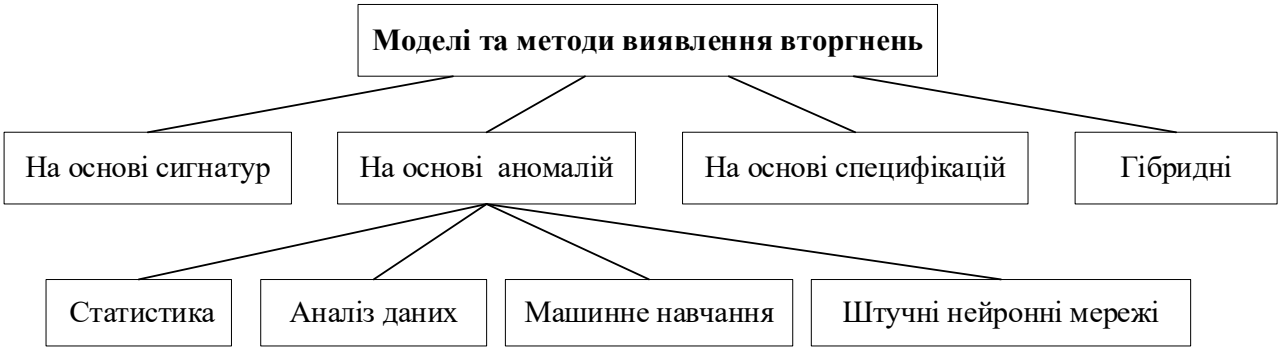

Рис. 1**.** Класифікація моделей та методів виявлення вторгнень для БСМ тактичної ланки управління військами

Моделі та методи виявлення вторгнень на основі сигнатур реалізуються шляхом порівняння моніторингових даних із базою даних сигнатур відомих загроз. Сигнатури можуть містити специфічні шаблони, що відображають відомі методи атак або зловмисну поведінку (шкідливі пакети даних або небезпечні послідовності команд).

Модель системи виявлення вторгнень (СВВ), що використовує набір еволюційно виведених правил для виявлення вторгнень у БСМ запропонована у роботі [8] на основі генетичного мережевого програмування (ГМП). Цей метод використовується для генерації правил виявлення вторгнень та контролю кількості цих правил та дає змогу удосконалювати правила, адаптуючись до змін у мережевій поведінці та нових типів атак. Правила вибираються на основі їх підтримки, достовірності та важливості (виміряної за допомогою статистики χ^2).

Тільки ті правила, які задовольняють певні порогові значення, вважаються важливими та зберігаються в наборі правил.

Для оцінювання та відбору правил автори використовують модифіковану відстань Жаккара, щоб виміряти схожість між правилами та між наборами правил. Мета запропонованого підходу полягає в тому, щоб мінімізувати відстань між правилами в одному наборі (зменшити редундантність) і максимізувати відстань між правилами в різних наборах (підвищити розрізнювальну здатність між нормальною поведінкою та вторгненнями).

Переваги: висока точність виявлення вторгнень шляхом точного налаштування параметрів системи, адаптивність до нових типів атак, можливість постійно оновлювати і вдосконалювати набір правил виявлення.

Недоліки: складність реалізації та налаштування, збільшені обчислювальні витрати, залежність ефективності роботи правил від повноти та точності вхідних даних.

Опис децентралізованої моделі СВВ для БСМ, що використовує фільтри Блума (ФБ) для зменшення розміру коду сигнатури атаки за допомогою хеш-функцій наведений у [9]. Створені сигнатури атак проходять через хеш-функції та поділяються за розміром на дві категорії, а потім відмічаються у відповідних масивах ФБ. Сигнатури розміром до 33 байт обробляються на мережевому рівні, а більші – на прикладному рівні. При передачі пакетів через мережу на кожному вузлі відбувається перевірка та порівняння з існуючими сигнатурами атак у масивах ФБ.

Переваги: енергоефективність, швидке виявлення атаки та оперативне реагування на потенційні загрози, гнучкість і адаптивність налаштування.

Недоліки: потреба в детальному налаштуванні та управлінні, ризик хибних спрацьовувань, проблеми з динамічним оновленням і видаленням сигнатур.

Для виявлення атак типу "вибіркової передачі" та "чорної діри" запропоновано метод на основі правил для побудови СВВ БСМ. Сигнатури атак зберігаються в БС з метою зниження енергоспоживання на сенсорних вузлах [10].

Принцип виявлення вторгнень базується на використанні контрольних пакетів (КП), які відправляються від ГК до БС на початку кожного сеансу зв'язку. Контрольний пакет містить інформацію про ГК та ідентифікатори вузлів-членів кластера. Для виявлення атак використовуються такі правила:

Затримки. *ЯКЩО* з вузла не надходять *КП* до БС до встановленого часу*, ТО* атака – "чорна діра".

Підмножини ідентифікаторів. *ЯКЩО* в КП відсутні ідентифікатори деяких членів кластеру*, ТО* атака – "вибіркова передача".

Переваги: простота управління та налаштування політики безпеки, мінімізація енергоспоживання сенсорних вузлів, висока швидкість реагування на інциденти БС.

Недоліки: високі вимоги до ресурсів БС та підвищенні ризики безпеки або компрометації БС, складність масштабованості.

Ієрархічна модель для виявлення аномальних вузлів у БСМ, що базується на використанні нечіткої логіки та правил "подія-умова-дія" була запропонована у [11]. Зазначена модель передбачає багаторівневу структуру, яка включає локальне виявлення на рівні вузлів кластера (ВК), групове виявлення на рівні кластерних агрегаторів (КА) та кластерне виявлення на рівні ГК.

Кожен ВК збирає дані про середовище та виконує локальний процес виявлення аномалій за допомогою нечіткої логіки. Для аналізу використовуються тимчасові семантичні кореляції. Кожен ВК зберігає короткострокову історію зібраних даних, які використовуються для побудови моделі ковзного вікна часу.

КА збирає локальні рішення від своїх сенсорних вузлів та використовує просторові багатовимірні кореляції для прийняття більш точного групового рішення.

ГК збирає групові рішення від ВК та використовує як просторово-часові атрибути (ПЧА) так і багатовимірні атрибути (БВА) кореляції для прийняття остаточного рішення щодо наявності аномальних вузлів.

Переваги: енергоефективність, зниження навантаження на центральний вузол через багаторівневу структуру СВВ, висока точність виявлення аномальних вузлів та зниження кількості хибних спрацьовувань.

Недоліки: складність налаштування та обслуговування, залежність від точності налаштувань правил та якості вхідних даних надісланих сенсорам, проблеми з динамічним оновленням і видаленням сигнатур.

У таблиці 1 наведено порівняльний аналіз методів і моделей виявлення вторгнень на основі сигнатур.

Таблиця 1

Методи та моделі виявлення вторгнень на основі сигнатур

Автор	Підхід	Атаки	Метод	Набір даних	Рівні OSI
Nannan et al. [8]	Централізований	Виснаження /Exhaustion Затоплення/ Flooding Шкідливе ПЗ/Malware Визначення топології/Homing Відмова в обслуговуванні/DoS	ГМП, відстань Жаккара	NSL-KDD	Канальний Мережевий Транспортний Прикладний
Cho et al. [9]	Децентралізований	Відмова в обслуговуванні/DoS	фільтри Блума	NS2	Прикладний
Hidoussi et al. [10]	Централізований	Чорна діра /Black Hole Вибіркова передача/Selective Forwarding	Правила затримки та підмножини ідентифікаторів	NS2	Мережевий
Berjab et al. [11]	Децентралізований	Відмова в обслуговуванні/DoS Десинхронізації/ Desynchronization	ПЧА БВА	NSL-KDD	Прикладний

Моделі та методи на основі сигнатур є надійним і точним інструментом для захисту від відомих атак, але їх ефективність залежить від актуальності бази сигнатур. Дані методи менш ефективні для боротьби з новими або складними атаками. Тому для підвищення ефективності виявлення потрібно їх використовувати в поєднанні з іншими методами, такими як евристичні або поведінкові аналізи.

Моделі та методи виявлення вторгнень на основі аномалій реалізуються шляхом порівняння поточних дій і станів мережі з моделлю нормальної поведінки для виявлення відхилень, що можуть свідчити про можливе вторгнення або іншу аномалію. Зазначені моделі та методи класифікуються залежно від їх функціональних можливостей: на основі статистики, на основі інтелектуального аналізу даних, на основі машинного навчання та на основі штучного інтелекту.

Процес виявлення вторгнень починається зі збору даних з сенсорних вузлів, зокрема датчиків температури, вологості, тиску, рівня вібрацій, трафіку та енергоспоживання. Зібрані дані очищуються і нормалізуються для видалення шуму та заповнення пропущених значень. На основі оброблених даних створюється модель нормальної поведінки вузла. Поточні дані постійно порівнюються з цією моделлю для виявлення значних відхилень, що можуть свідчити про аномалії.

Методи та моделі виявлення на основі статистики спрямовані на виявлення вторгнень через аналіз статистичних відхилень у поведінці БСМ. Ці методи базуються на зборі великих

обсягів даних про нормальну функціонування діяльність системи, після чого створюються математичні моделі, що відображають її стандартні характеристики, такі як середнє значення, стандартне відхилення, дисперсія та інші статистичних моделей (логістична регресія, авторегресія). Під час моніторингу поточної активності системи виявляються значні відхилення від цих характеристик, що вказують на можливі аномалії та потенційні загрози.

Так у [12] запропоновано модель СВВ для БСМ, що використовує статистичний інструмент бінарної логістичної регресії (БЛР) для аналізу зібраних даних з вузлів (кількість отриманих та відправлених пакетів даних, кількість перенаправлених та втрачених пакетів).

На основі результатів аналізу БЛР система класифікує активність сенсора зловмисною якщо ймовірність зловмисної активності перевищує певний поріг.

Переваги: енергоефективність, можливість виявлення нових типів атак та висока точність виявлення відомих атак, можливість адаптації та змін налаштування для конкретних потреб і специфікацій мережі.

Недоліки: залежить від якості та репрезентативності тренувальних даних, складність визначення оптимальних порогів для класифікації, неспроможність виявляти атаки, що імітують нормальну поведінку мережі.

Статистичний метод виявлення атак "створення завад" в БСМ з використанням техніки контролю статистичного процесу на основі моделі експоненційно зваженого ковзного середнього (Exponentially Weighted Moving Average, EWMA) запропоновано у [13].

Основною ідеєю є використання моделі EWMA для моніторингу значення часу між прибуттями пакетів і виявлення випадків, коли його середнє значення відхиляється від норми, що може вказувати на створення завад зловмисником.

Визначення EWMA в момент часу *t* здійснюється за виразом [13]:

$$z(t) = \lambda \cdot x(t) + (1 - \lambda) \cdot z(t - 1),$$

де $x(t)$ – спостережуване значення в момент часу *t*; λ – коефіцієнт згладжування, який визначає вагу останніх спостережень відносно попередніх.

Переваги: енергоефективність, легкість імплементації та інтеграції в існуючі СВВ, швидкість виявлення аномалій.

Недоліки: низька ефективність у мережах з високою змінністю трафіку або в мережах, що характеризуються частими змінами топології, слабка адаптивність до складних та поліморфних атак, можливість виявлення тільки атак пов'язаних із створенням завад.

Модель СВВ для БСМ, що використовує теорію ігор та авторегресивну модель (АРМ) для ефективного передбачення атак і мінімізації споживання енергії запропоновано [14]. Система моделює взаємодію між атакуючими та СВВ як гру з двома гравцями, де кожен учасник намагається максимізувати свою вигоду: атакуючий – успішно виконати атаку, а СВВ – ефективно запобігти атаці. Модель ураховує можливі стратегії обох сторін та використовує концепцію змішаної рівноваги Неша для визначення оптимальних стратегій захисту. Такий підхід дозволяє системі адаптуватися до різних стратегій атак і вибирати найефективнішу стратегію оборони з урахуванням енерговитрат.

Система використовує АРМ для аналізу історичних даних про атаки і передбачення часу та цілей наступних атак. АРМ дає змогу ідентифікувати закономірності в поведінці атакуючих, базуючись на попередніх атаках і передбачати майбутні атаки.

Авторегресивна модель порядку p (кількість попередніх значень, що використовуються для передбачення поточного значення) формалізується за виразом [14]:

$$X_t = \phi_1 X_{t-1} + \phi_2 X_{t-2} + \cdots + \phi_p X_{t-p} + \varepsilon_t,$$

де X_t – поточне значення часового ряду в час *t*; $\phi_1, \phi_2, \ldots, \phi_p$ – параметри моделі, які визначають вплив попередніх значень на поточне значення; ε_t – термін шуму або помилки

в час t (серія некорельованих випадкових змінних з нульовим середнім і постійною дисперсією).

Переваги: висока ефективність виявлення вторгнень, енергоефективність, можливість адаптуватися до нових або еволюційних загроз.

Недоліки: складність реалізації та інтеграції моделі, залежність від вибору та налаштування параметрів, залежність від якості та обсягу попередньо отриманих даних, потреба в постійному оновленні.

Для виявлення атаки типу "воронки" у БСМ використовується геостатистична модель розподіленого моніторингу (ГМРМ) [15]. Принцип виявлення вторгнень полягає в тому, що вузли навколо воронки втрачають енергію швидше, ніж інші вузли, оскільки маршрути через атакуючий вузол використовуються частіше. Це призводить до формування "енергетичної кризи" навколо атакуючого вузла. Використання ГМРМ дає змогу БС оцінити ризик атаки в кожному кластері на основі змін у залишковій енергії та інших метрик, що містять геолокаційні дані вузлів.

Швидкість відмови для вузла j в регіоні i у час описується формулою

$$z(t_{ij};\ x_{ij}) = z_0 \exp(-\beta x_{ij} + W_i),$$

де t_{ij}; x_{ij} – вектор асоційованих коваріат (наприклад, залишкова енергія); W_i – термін, що відображає варіабельність між регіонами (фрагільність регіону); z_0 – початковий рівень безпеки.

Переваги: висока точність ідентифікації атак "воронки", гнучкість налаштування та масштабованість, швидкість реагування на вторгнення.

Недоліки: складність налаштування та оновлення, залежність від якості та обсягу попередньо отриманих даних, високі вимоги до обчислювальних ресурсів.

Узагальнена стохастична мережа Петрі (Generalized Stochastic Petri Nets, GSPN) використовується для визначення позиції розгортання спеціальних вузлів-інспекторів (BI), що аналізують трафік у кластері та надсилають попередження до ГК у разі виявлення аномальної поведінки [16].

Модель використовує статичний і динамічний підходи до розміщення BI. При статичному підході BI розміщуються на стратегічних позиціях у топології мережі, а при динамічному – BI періодично обираються серед звичайних вузлів кожного атомарного кластера.

Переваги: гнучкість налаштування, адаптивність, масштабованість, швидкість виявлення аномалій у поведінці вузлів.

Недоліки: підвищена складність управління та координація динамічного вибору BI, менша ефективність проти нових або модифікованих атак, великі енергозатрати BI.

У таблиці 2 наведено порівняльний аналіз методів та моделей виявлення вторгнень на основі статистики.

Таблиця 2

Методи та моделі виявлення вторгнень на основі статистики

Автор	Підхід	Атаки	Метод	Набір даних	Рівні OSI
Ioannou et al. [12]	Децентралізований	Чорна діра /Black Hole Вибіркова передача/Selective Forwarding	БЛР	Cooja	Мережевий
Osanaiye et al. [13]	Децентралізований	Створення завад/Jamming	EWMA	CRAWDA	Фізичний
Han et al. [14]	Централізований	Шкідливе ПЗ/Malware	APM	MAT Lab	Прикладний
Shafiei et al. [15]	Децентралізований	Воронка/Sinkhole	ГМРМ	OMNeT++	Мережевий
Ballarini et al. [16]	Децентралізований	Відмова в обслуговуванні/DoS	GSPN	NS2	Прикладний

Моделі та методи виявлення вторгнень на основі статистики в якості переваги мають можливості моніторингу та аналізу мережевого трафіку з великою адаптивністю та

масштабованістю. В якості недоліка можливе використання зловмисних вузлів з метою перенавчання статистичних алгоритмів для неправильного визначення їх нормальної поведінки.

Методи та моделі виявлення вторгнень на основі інтелектуального аналізу даних (Data Mining) використовують алгоритми обробки даних такі як кластеризація, класифікація, асоціація, аналіз послідовностей і прогнозування, які ефективно виявляють приховані патерни та аномалії при великих обсягах зібраної інформації з сенсорних вузлів.

Модель СВВ для ідентифікації атаки "чорної діри" на основі аналізу поведінки вузлів мережі з метою ідентифікації їх аномальної поведінки запропоновано у [17]. Виявлення вторгнень базується на обробці даних за допомогою алгоритму кластеризації K-means та алгоритму класифікації J-48 для побудови дерева рішень. Спочатку набір даних з нормальною поведінкою вузлів піддається кластеризації та визначаються вузли з подібними поведінковими (функціональними) характеристиками. Наступним кроком є застосування алгоритму J-48 для побудови дерева рішень, яке допомагає класифікувати вузли на нормальні або зловмисні залежно від їх поведінки. Вибір атрибуту в J-48 (зиск інформації) проводиться за виразом [17]:

$$IG(S,A) = H(S) - \sum_{t\epsilon T} \frac{|S_t|}{|S|} H(S_t),$$

де $IG(S,A)$ – зиск інформації від атрибута A для множини S; $H(S)$ – ентропія множини S; T – множина всіх можливих значень атрибута A; S_t – підмножина S для якої атрибут A має значення t.

Переваги: висока точність ідентифікації атаки "чорної діри" та можливість їх раннього виявлення, адаптація до нових загроз завдяки можливості перенавчання моделі.

Недоліки: потреба значних обчислювальних ресурсів, залежність точності виявлення від вибору параметрів, потреба в затратах часу на навчання та оптимізацію.

Модель виявлення аномалій на основі кластеризації K-медоїдів для ідентифікації атаки "чорної діри" та атаки "вибіркової передачі" у БСМ розроблена у [18]. Вона працює за принципом моніторингу та аналізу мережевих параметрів вузлів. Використовуючи алгоритм K-медоїдів, вузли з подібними характеристиками групуються в кластери та обирається медоїд у кластері завдяки мінімізації суми попарних відстаней між точками в кластері.

Для кожного кластера обчислюються порогові значення для різних параметрів (наприклад, обсяг трафіку або затримка пакетів) та у разі перевищення порогу визначається аномальну поведінка вузла.

Переваги: висока точність та швидкість виявлення атак "вибіркової передачі" та "чорної діри", простота реалізації та стійкість до шуму.

Недоліки: обмежена масштабованість, залежність ефективності виявлення від початкового вибору медоїдів та налаштувань порогових значень.

Для виявлення атак "воронки" та "виснаження" запропоновано модель СВВ, що забезпечує дворівневе виявлення вторгнень, де локальні агенти швидко виявляють аномалії, а центральний агент проводить глибший аналіз для підтвердження вторгнень [19]. Локальний агент встановлюється в кожному вузлі та виконують менш складні функції виявлення аномалій. Вони збирають дані моніторингу та інформацію про маршрути. Центральний агент, що встановлюється на БС, аналізує отримані дані від локальних агентів та виконує їх класифікацію алгоритмом дерева рішень.

Переваги: ефективність проти відомих та нових атак, висока швидкість реагування та точність виявлення, зменшена кількість помилкових спрацювань, можливість збалансувати навантаження на обчислювальні та енергетичні ресурси вузлів мережі.

Недоліки: складність налаштування, залежність від якості набору даних, потенційна вразливість БС до DoS атак, потенційна проблема масштабування.

Для виявлення атаки "затоплення" використовується алгоритм класифікації K-найближчих сусідів (K-Nearest Neighbor, KNN), що реалізується моделлю СВВ, архітектура якої складається з модуля бездротового мережевого інтерфейсу, модуля зберігання даних, модуля аналізу та судження, а також модуля реагування на вторгнення [20].

Кожен вузол представляється як багатовимірний вектор ознак, що містить різні параметри поведінки вузла. Система визначає K-найближчих сусідів для кожного вузла та аналізує, до якої категорії (нормальні або аномальні) належить більшість цих сусідів. На основі аналізу відстані між вузлом та його найближчими сусідами визначається порогове значення, при перевищені якого СВВ класифікує вузол як аномальний і може вжити заходів щодо ізоляції вузла або сповіщення адміністратора мережі про вторгнення.

Переваги: адаптивність до змін у поведінці мережі, простота імплементації (реалізації та інтеграції) в БСМ, висока ефективність виявлення аномалій.

Недоліки: потреба зберігання великих обсягів даних в пам'яті вузла, залежність від вибору параметрів та незбалансованих даних, потреба в значних обчислювальних ресурсах.

У таблиці 3 наведено порівняльний аналіз методів і моделей виявлення вторгнень на основі інтелектуального аналізу даних.

Таблиця 3

Методи та моделі виявлення вторгнень на основі аналізу даних

Автор	Підхід	Атаки	Метод	Набір даних	Рівні OSI
Kaur et al. [17]	Централізований	Чорна діра /Black Hole	K-means, J48	NS2	Мережевий
Ahmad et al. [18]	Централізований	Чорна діра /Black Hole Вибіркова передача/Selective Forwarding	K-медоїдів	NS2	Мережевий
Coppolino et al. [19]	Централізований	Воронка/Sinkhole Виснаження/Exhaustion	Дерево рішень	NS3	Канальний Мережевий
Li et al. [20]	Централізований	Затоплення/ Flooding	KNN	NSL-KDD	Транспортний

Моделі та методи виявлення вторгнень на основі інтелектуального аналізу даних, дозволяють ідентифікувати нові та складні атаки, здійснювати проактивний захист та можуть адаптуватися до змін у поведінці мережі. В якості недоліків можна зазначити велику обчислювальну складність та залежність від навчальних даних і вибору параметрів, які потрібно враховувати в процесі виявлення вторгнень.

Моделі та методи виявлення аномалій на основі машинного навчання орієнтовані на побудову моделей, які можуть генерувати точні прогнози або виявляти закономірності в наявних наборах даних. Їх головною метою є розробка алгоритмів і моделей, що здатні генерувати нові набори даних, прогнозувати або приймати рішення.

Модель СВВ, що ґрунтується на використанні архітектури з локальними агентами (ЛА) та центральним агентом (ЦА), доповнену застосуванням порогових метрик разом із деревами рішень для класифікації та виявлення атак типу "воронки" представлено у [21].

ЛА встановлюється на сенсорному вузлі та сповіщає ЦА про можливе вторгнення в мережу. ЛА спостерігає за певними характеристиками трафіку та інших змінних (кількість, частота та тип пакетів) мережі та визначає аномалії на основі порогових значень за допомогою методики експоненціального ковзного середнього (Exponential Moving Average, EMA).

Методика EMA використовується для згладжування даних та визначення напрямку їх зміни протягом певного часу. Значення EMA в момент часу *t* визначається за виразом;

$$EMA_t = \alpha \cdot M_t + (1 - \alpha) \cdot EMA_{t-1},$$

де M_t – поточне спостережуване значення параметра в момент t, EMA_{t-1} – значення EMA в попередній момент часу, $\alpha = \frac{2}{N+1}$ – коефіцієнт згладжування, N – кількість періодів.

ЦА діє як координатор між всіма ЛА і виконує більш складний аналіз отриманих сповіщень. За допомогою дерева рішень ЦА класифікує поведінку мережі як нормальну або аномальну, засновану на зібраних даних. Це дає змогу ідентифікувати більш складні атаки, які можуть не бути виявлені на рівні ЛА.

Переваги: здатність до самонавчання, високий рівень гнучкості та масштабованості системи, висока ефективність виявлення складних атак.

Недоліки: залежність ефективності від якості даних, потреба в обчислювальних ресурсах, ризик підвищення хибних спрацювань пов'язаних з перенавчання моделі.

Модель СВВ запропонована у [22] базується на комбінації кооперативної теорії ігор та нечіткого Q-навчання, що використовується для моделювання взаємодії між гравцями (атаковані вузли, БС, зловмисник). Кожен гравець обирає свою стратегію для досягнення максимальної вигоди. Для вузлів та БС стратегії спрямовані на виявлення та запобігання атакам, а для зловмисника – успішна реалізація атаки. Модель використовує спеціалізовані функції вигоди для моделювання наслідків різних комбінацій стратегій.

Для оптимізації процесу прийняття рішень використовується нечітке Q-навчання, що дає змогу адаптуватися до змін у середовищі мережі та ефективно вибирати стратегії для максимізації вигоди [22]:

$$Q(s,a) \leftarrow Q(s,a) + a[r + \gamma \max_{a'} Q(s',a') - Q(s,a)],$$

де a – дія або швидкість навчання; a' – наступна можлива дія $Q(s,a)$ – значення Q-функції для стану s та дії; r – винагорода за дію a у стані s; γ – коефіцієнт дисконтування, що відображає важливість майбутніх винагород; s' – наступний стан після виконання дії a.

Переваги: адаптивність, висока точність та ефективність виявлення, ефективне використання ресурсів, можливість виявлення потенційних загроз (проактивне виявлення).

Недоліки: складність реалізації та налаштування, потенційна складність масштабування, потреба зберігання великої кількості даних про попередні взаємодії та вибори стратегій.

Метод виявлення вторгнень на основі глибокого навчання з використанням архітектури багатошарового автоматичного кодера (Stacked Denoising Autoencoder, SDA) дає змогу ідентифікувати атаки, аналізуючи та класифікуючи характеристики місцеположення разом із топологічними індексами [23].

Різниця потужності сигналу (RSSI) між неатакованими та атакованими вузлами визначається за виразом:

$$RSSIDIFF_{ij} = RSSI_{N,ij} - RSSI_{A,ij},$$

де $RSSI_{N,ij}$ та $RSSI_{A,ij}$ – потужність сигналу між вузлом-маяком i та невідомим вузлом j в неатакованих та атакованих сценаріях відповідно.

Архітектура SDA використовується для здобуття корисних характеристик із сировинних даних через послідовні шари автоенкодерів, що призначені для відновлення вхідного сигналу на виході.

Переваги: висока точність класифікації та виявлення складних атак, зменшене навантаження на вузли, здатність до самонавчання.

Недоліки: необхідність великої кількості даних та витрати певного часу для навчання, залежність від якості даних, потреба в значних обчислювальних ресурсах.

Для виявлення атак "чорної діри "та "затоплення", запропоновано метод, що поєднує алгоритм нечіткої кластеризації c-means, однокласового методу опорних векторів (Support Vector Machine, SVM) і процедури ковзного вікна [24].

Алгоритм нечіткої кластеризації c-means використовується для розділення даних моніторингу на кластери, що представляють нормальні та аномальні стани сенсорних даних. Мета такого алгоритму визначити центри кластерів та призначити кожному виміру даних ступінь приналежності до кожного кластера. Алгоритм мінімізує цільову функцію:

$$J(U,V) = \sum_{i=1}^{n}\sum_{j=1}^{c} u_{ij}^{m}||x_i - v_j||^2,$$

де n – кількість точок даних, c – кількість кластерів, u_{ij} – ступінь приналежності i-ої точки до j-го кластера, m – параметр, що визначає рівень нечіткості кластеризації, x_i – i-та точка даних, v_j – центр j-го кластера.

Однокласова SVM використовується для ідентифікації нових даних, що відхиляються від нормального шаблону поведінки, який був навчений моделлю. Це досягається максимізацією відстані між даними та походженням у просторі ознак, трансформованому завдяки ядра. Рішення моделі може бути представлене так:

$$f(x) = sign(\sum_{i=1}^{n} a_i K(x_i, x) - \rho),$$

де $K(x_i, x)$ – функція ядра між i-тим навчальним вектором і вектором, що тестується x, a_i –коефіцієнти, що визначаються під час навчання моделі, ρ – відступ від походження.

Процедура ковзного вікна використовується для аналізу часових залежностей між послідовними точками даних, щоб додатково оцінити підозрілий зразок даних.

Переваги: висока ефективність і точність розпізнавання аномалій, адаптивність і легкість впровадження, енергоефективність.

Недоліки: складність налаштування параметрів, висока залежність ефективності виявлення від вибірки даних, потреба у великих обсягах даних для регулярного оновлення моделі.

Модель СВВ на основі алгоритму SMOTE (Synthetic Minority Over-sampling Technique) , який проводить балансування набору даних KDDCup'99 шляхом створення синтетичних прикладів міноритарного класу (тобто класу, який має менше представництво у наборі даних) запропоновано в [25]. Для кожного зразка міноритарного класу визначається кількість його найближчих сусідів k, а потім вибирається один з цих сусідів і створюється новий синтетичний зразок шляхом інтерполяції між розглянутим зразком та вибраним сусідом. Після балансування датасету за допомогою SMOTE використовується алгоритм випадкового лісу для класифікації зразків.

Переваги: масштабованість та висока швидкість обробки даних при великій кількісті вузлів, здатність моделі точно класифікувати рідкісні типи атак, малий ризик перенавчання.

Недоліки: великі енергозатрати через складність обчислень потреба у великих обсягах даних для регулярного оновлення моделі, залежність від налаштування параметрів.

У таблиці 4 наведено порівняльний аналіз методів і моделей виявлення вторгнень на основі машинного навчання.

Таблиця 4

Методи та моделі виявлення вторгнень на машинного навчання

Автор	Підхід	Атаки	Метод	Набір даних	Рівні OSI
Garofalo et al. [21]	Децентралізований	Воронка/Sinkhole	EMA	NS3	Мережевий
Shamshirband et al. [22]	Децентралізований	Відмова в обслуговуванні/DoS	нечітке Q-навчання	NS2, WSN-DS	Прикладний

Автор	Підхід	Атаки	Метод	Набір даних	Рівні OSI
Wang et al. [23]	Централізований	Сивілли/Sybil Нерівномірність доступу/Unfairness Тунелювання/Wormhole Колізії/Collision	SDA	NS2	Канальний Мережевий
Qu et al. [24]	Централізований	Чорна діра/Black Hole Затоплення/Flooding	c-means SVM	OMNeT++	Мережевий Транспортний
Tan et al. [25]	Централізований	Виснаження /Exhaustion Затоплення/ Flooding Шкідливе ПЗ/Malware Відмова в обслуговуванні/DoS	SMOTE Випадковий ліс	KDD Cup'99	Прикладний Мережевий Транспортний

Методи та моделі на основі машинного навчання дають змогу виявляти відомі та невідомі атаки за допомогою аналізу великих обсягів даних та ідентифікації аномалій у поведінці мережі. Перевагами методів є адаптивність, висока точність та можливість роботи в реальному часі. Як недолік слід зазначити наявність чутливості до шуму, складність обчислення та необхідність специфічного налаштування особливо в умовах обмежених ресурсів.

Для виявлення атак у реальному часі для зменшеним втручання людини використовують **методи виявлення вторгнень на основі штучних нейронних мереж**, що імітують алгоритми роботи людського мозку, використовуючи нейрони та їх взаємозв'язки.

Модель СВВ, що використовує метаевристичні алгоритми вовчої зграї та еволюційних систем для оптимізації нейронної мережі досліджено в [26]. Алгоритм вовчої зграї оптимізує ваги і параметри нейронної мережі для підвищення точності та ефективності виявлення аномалій. Він моделює соціальну структуру і полювання сірих вовків, використовуючи лідерів (альфа, бета, дельта) для керівництва пошуком оптимальних рішень в просторі рішень. Алгоритм еволюційних систем використовується для покращення процесу виявлення аномалій шляхом адаптації нейронної мережі до змін у даних і умовах роботи мережі. Він використовує принципи еволюції для ефективного пошуку в просторі параметрів, адаптуючи і вдосконалюючи модель нейронної мережі.

Визначення відстані D між вовком (поточним рішенням) та здобиччю (оптимальним рішенням) здійснюється за виразом:

$$D = |C \cdot X_p(t) - X(t)|,$$

де $X_p(t)$ – позиція здобичі (оптимального рішення) на ітерації t, $X(t)$ – позиція вовка, C – коефіцієнт, що визначає вплив здобичі на рух вовка.

Переваги: висока точність виявлення аномалій та потенційних атак, адаптивність до змін у поведінці мережі, масштабованість, ефективність у режимі реального часу завдяки швидкому навчанню нейронної мережі.

Недоліки: значні вимоги до обчислювальних ресурсів, складність налаштування, залежність ефективності виявлення та ризик перенавчання від якості та актуальності даних.

Модель СВВ у БСМ на основі ройового інтелекту (Swarm Intelligence for Wireless sensor networks Cybersecurity, SIWC), містить три основні рівні: сенсорів, безпеки та прийняття рішень [27].

Рівень сенсорів (Sensor Layer) складається з різних вузлів (датчиків), що періодично вимірюють набір критичних параметрів (кількість колізій, швидкість передачі пакетів тощо) у своєму радіусі дії та відповідають за збір та передачу даних до рівня безпеки.

Рівень безпеки (Security Layer) складається з вузлів-захисників, що відповідають за виявлення аномальних поведінок безпеки та атак у кластері. Кожен вузол-захисник є ГК і використовує метод оцінювання максимальної правдоподібності для визначення рівня безпеки свого кластера. Цей метод тренується за допомогою алгоритму ройового інтелекту для пошуку найкращих значень, що підвищують ймовірність виявлення атак.

Найвищий рівень прийняття рішень (Decision Layer) розгортається на рівні БС мережі, яка отримує повідомлення про загрози від ГК та вживає відповідних заходів, таких як пом'якшення атаки або вимкнення атакованого вузла.

Переваги: адаптивність до нових видів атак, висока швидкість виявлення та реагування на вторгнення, масштабованість, мала потреба в обчислювальних ресурсах.

Недоліки: складність налаштування, потреба в регулярних оновленнях та підтримці, залежність точності від параметрів та якості набору даних.

Для виявлення атаки "чорної діри" модель СВВ поєднує алгоритм мурашиних колоній (Ant Colony Optimization, ACO) та алгоритм рою частинок (Particle Swarm Optimization, PSO) [28]. Кожна частинка розміщуються в пошуковому просторі та має вектори положення та швидкості. Вона оцінює своє поточне положення за допомогою функції пристосування, що визначає, наскільки добре дане положення задовольняє критерії виявлення атак. Це може містити аналіз шаблонів трафіку, часових інтервалів між пакетами та інших властивостей даних.

Кожна частинка запам'ятовує найкраще знайдене нею положення та визначає найкраще положення серед усіх частинок у рої. Положення частинки i в час t+1 оновлюється на основі її нової швидкості $v_i^{(t+1)}$:

$$x_i^{(t+1)} = x_i^{(t)} + v_i^{(t+1)},$$

де $x_i^{(t)}$ – положення частинки i в час t.

Частинки, які консистентно показують високі значення функції пристосування в потенційно аномальних областях, можуть вказувати на наявність вторгнення.

Переваги: висока точність виявлення атаки "чорної діри", масштабованість, адаптивність.

Недоліки: складність реалізації через необхідність інтеграції хеш-таблиць та управління роєм частинок, залежність від параметрів та якості набору даних, потреба в обчислювальних ресурсах.

Модель СВВ, що реалізується на синтезі алгоритмів adaboost, зграї (косяка) риб та культурного обміну для свого навчання використовує набір даних NSL-KDD [29]. Алгоритм adaboost інтегрує багато слабких класифікаторів у сильний, стабільний та адаптивний класифікатор. Ієрархічна структура допомагає відсіювати більшість нормальних даних на перших рівнях, залишаючи для подальшого аналізу лише потенційно аномальні дані.

Для виявлення зловживань використовується нейронна мережа зворотного поширення помилок, оптимізована за допомогою алгоритму культурного обміну та зграї (косяка) риб. Вихідний сигнал нейронної мережі для k-го нейрону вихідного шару, обчислюється за виразом:

$$O_k = f(\sum_{j=1}^{l} H_j w_{jk} - b_k),$$

де H_j – вихідний сигнал j-го нейрона прихованого шару, w_{jk} – вага між j-м нейроном прихованого шару та k -м нейроном вихідного шару.

Переваги: висока адаптивність та масштабованість, зниження навантаження на обчислювальні та енергетичні ресурси вузлів, комплексність і точність системи.

Недоліки: складність налаштування та інтеграції, затрати часу на тренування та оптимізацію моделі, залежність ефективності від якості набору даних.

Метод виявлення вторгнень запропонований у [30] базується на поєднанні алгоритму спектральної кластеризації та множини глибоких нейронних мереж. Спочатку застосовується алгоритм спектральної кластеризації для поділу набору даних на кластери на основі схожості даних. Потім кожен кластер обробляється окремою нейронною мережею із використанням декількох шарів автоенкодерів для попереднього навчання глибокої нейронної мережі. Після чого виконується дрібна настройка з учителем для кінцевого завдання класифікації, що дає змогу моделі вчитися на особливостях кожного кластера.

Переваги: висока ефективність, адаптивність до змін у поведінці мережевого трафіку, можливість виявлення нових типів атак, малі затрати часу на тренування і тестування моделі.

Недоліки: потреба у великому наборі даних для тренування, складність налаштування параметрів, потреба в значних обчислювальних ресурсах, велика залежність ефективності від якості кластеризації.

У таблиці 5 наведено порівняльний аналіз методів та моделей на основі штучних нейронних мереж.

Таблиця 5

Методи та моделі виявлення вторгнень на основі штучних нейронних мереж

Автор	Підхід	Атаки	Метод	Набір даних	Рівні OSI
Mansouri et al. [26]	Централізований	Воронка/Sinkhole Відмова в обслуговуванні/DoS Сивілли/Sybil Визначення топології /Homing	алгоритми вовчої зграї та еволюційних систем	NS3	Канальний Мережевий Прикладний
Bitam et al. [27]	Децентралізований	Відмова в обслуговуванні/DoS Сивілли/Sybil Тунелювання/Wormhole Виснаження/Exhaustion	SIWC	NS3	Канальний Мережевий Прикладний
Nithiyanandam et al. [28]	Централізований	Воронка/Sinkhole	ACO, PSO	NS2	Мережевий
Sun et al. [29]	Децентралізований	Виснаження /Exhaustion Затоплення/ Flooding Шкідливе ПЗ/Malware Відмова в обслуговуванні/DoS	алгоритми adaboost, зграї риб та культурного обміну	NSL-KDD	Канальний Мережевий Транспортний Прикладний
Ma et al. [30]	Централізований	Виснаження /Exhaustion Затоплення/ Flooding Шкідливе ПЗ/Malware Визначення топології /Homing Відмова в обслуговуванні/DoS	спектральна кластеризація та множина глибоких нейронних мереж	NSL-KDD	Канальний Мережевий Транспортний Прикладний

Моделі та методи виявлення вторгнень на основі штучних нейронних мереж, мають високу точність, адаптивність та ефективність роботи у реальному часі при використанні метаевристичних алгоритмів вовчої зграї, ройового інтелекту і мурашиної колонії. Недоліками таких методів є складність налаштування, високі вимоги до ресурсів і ризик перенавчання.

Моделі та методу виявлення вторгнень на основі специфікацій використовують чітко визначені правила і моделі, що описують допустимі форми поведінки системи. Основу такого підходу є детальне розроблення специфікацій, що відображають всі етапи створення цих правил від мережевих протоколів до файлових операцій для моніторингу та аналізу системної активності. Під час роботи СВВ постійно перевіряє системні операції на відповідність встановленим специфікаціям, що дає змогу ідентифікувати аномалії, які свідчать про вторгнення [6].

Шляхом аналізу поведінки кожного вузла та порівнянні його з встановленими нормами модель СВВ використовує специфікацію на основі правил для виявлення аномалій у мережі [31].

Для цього використовується список аудиту (*A_List*), який містить інформацію про кількість відправлених, отриманих, переспрямованих та повторно відправлених пакетів для кожного вузла.

$$A\_List = \{Node\_ID, A\_snt, A\_rec, A\_fwd, A\_rtm\},$$

де *Node_ID* – ідентифікатор вузла, *A_snt* – кількість відправлених пакетів, *A_rec* – кількість отриманих пакетів, *A_fwd* – кількість переспрямованих пакетів, *A_rtm* – кількість повторно відправлених пакетів.

На основі цих даних формується список прапорців (*F_List*), що вказує на відхилення поведінки вузла від норми:

$$F\_List = \{Node\_ID, F\_snt, F\_rec, F\_fwd, F\_rtm\},$$

де *F_snt, F_rec, F_fwd, F_rtm* – прапорці, що можуть приймати одне з трьох значень: *N (miN)* – якщо значення менше мінімального порогу; *X* (*maX*) – якщо значення більше максимального порогу; *L* – якщо значення знаходиться в межах норми (*normaL*).

На основі *F_List* визначається рівень підозрілості вузла в списку *ML_List*:

$$ML\_List = \{Node\_ID, Maliciousness\_Level\},$$

де *Maliciousness_Level* – рівень підозрілості може бути одним з трьох значень: *Hig* (високий) – якщо кількість L менше або дорівнює двом; *Med* (середній) – якщо кількість L дорівнює трьом; *Low* (низький) – якщо поведінка вузла не відповідає жодному з вищезазначених критеріїв.

Переваги: висока точність виявлення вторгнень з низьким рівнем помилкових спрацювань, зниження навантаження на окремі вузли мережі.

Недоліки: потреба в постійному оновленні правил, збільшення службового трафіку між вузлами, вразливість до складних атак, складність виявлення нових типів атак, залежність від налаштування порогових значень та інших параметрів.

Гібридні моделі та методи виявлення вторгнень використовує переваги підходу, заснованого на сигнатурах, аномаліях і специфікаціях. Гібридний підхід підвищує точність до виявлення вторгнень, але збільшує складність реалізації [6].

Гібридний метод виявлення вторгнень, що полягає в комбінації різних методів виявлення на кожному з рівнів мережі запропоновано в [32].

На рівні вузлів використовується метод виявлення на основі специфікацій із встановленням певних правил для кожного типу атаки. На рівні ГК здійснюється виявлення аномалій на основі алгоритму бінарної класифікації SVM.

На рівні БС (високий рівень) використовує механізм голосування для прийняття остаточного рішення щодо підозрілих вузлів на основі звітів від ГК.

Переваги: ефективність та точність ідентифікації різних типів атак, можливість оптимізації обробки даних і розподілу навантаження, енергоефективність, адаптивність.

Недоліки: складність реалізації та налаштування, залежність ефективності від правильності налаштування параметрів, можливість затримки в реакції на атаки.

Модель гібридної СВВ, що складається з двох основних модулів запропоновано в [33]. Модуль виявлення зловживань порівнює поведінку мережі з відомими моделями атак використовуючи заздалегідь визначені сигнатури атак або патерни. Модуль виявлення аномалій використовує нейронну мережу зворотного поширення помилок (Back Propagation Network, BPN), що дає змогу системі класифікувати поведінку як нормальну чи аномальну на основі навчених вагових коефіцієнтів та взаємодій між нейронами у мережі.

Рішення про вторгнення приймається на основі результатів обох модулів. Якщо модуль виявлення аномалій фіксує атаку, але модуль виявлення зловживань не виявляє атаку, система

вважає, що атаки не було, і це розцінюється як помилкове спрацьовування модуля виявлення аномалій. Якщо обидва модулі виявляють атаку, система підтверджує факт вторгнення і визначає клас атаки на основі результатів роботи модуля виявлення зловживань.

Переваги: висока точність виявлення, енергоефективність, адаптивність, можливість ідентифікації відомих та невідомих атак.

Недоліки: складність реалізації та налаштування, залежність ефективності виявлення від правильності налаштування параметрів, можливість затримки в реакції на атаки.

Багаторівневою гібридною модель СВВ, що використовує правила специфікації та нейронні мережі для ідентифікації зловмисних вузлів запропоновано в [34]. Система здійснює моніторинг на трьох рівнях: рівні вузла, ГК та БС.

На найнижчому рівні вузлів розміщено агентів СВВ, які здійснюють моніторинг діяльність сенсорів в кластері за допомогою набору специфікацій та правил. Ці правила базуються на таких параметрах, як частота отримання пакетів, частота пересилання пакетів, дублювання пакетів та індикатор сили сигналу. Взаємодія між СВВ і вузлом відбувається на основі теорії ігор з двома учасниками. СВВ адаптує свої стратегії моніторингу на основі Байєсівського рівноважного стану Неша (Bayesian Nash Equilibrium, BNE), що дає змогу мінімізувати обсяг введеного в мережу трафіку СВВ.

Гра визначається як $G = \{N, S, U\}$, де $N = \{P_i, P_j\}$ є множиною гравців, де P_i є потенційно зловмисним вузлом, а P_j – захисником (СВВ); $S = S_i \cdot S_j$ представляє простір стратегій гри, з S_i і S_j як просторами стратегій для P_i, і P_j відповідно; $U = U_i \cdot U_j$ – визначає простір виграшів, з $U_i \cdot$ і U_j як виграшами для P_i, і P_j.

На середньому рівні ГК виконують моніторинг інших ГК завдяки комбінації правил специфікації та легкої нейронної мережі, що дає змогу класифікувати дії інших ГК як нормальні або аномальні.

На найвищому рівні БС збирає інформацію від кількох ГК для виявлення зловмисних ГК. Якщо ГК виявляється зловмисним, він видаляється з мережі, а на його місце обирається новий ГК.

Переваги: висока точність і швидкість виявлення енергоефективність, масштабованість, адаптивність, мінімізація службового трафіку

Недоліки: складність розгортання та налаштування системи, залежність ефективність від точності встановлених параметрів складність управління та обслуговування

Гібридну модель СВВ поєднує підсистему виявлення на основі сигнатур та підсистему виявлення аномалій [35].

Підсистема виявлення на основі сигнатур призначена для ідентифікації відомих інтрузивних поведінок за допомогою сигнатур або визначених ознак цих поведінок. Алгоритм випадкового лісу генерує багато дерев рішень на основі підмножини навчальних даних та ознак, а потім використовує голосування більшості для прийняття рішення.

Підсистема виявлення аномалій базується на алгоритмі кластеризації E-DBSCAN (Enhanced Density-Based Spatial Clustering of Applications with Noise), що групує дані на основі їх щільності, ідентифікуючи області високої щільності, які відокремлені областями низької щільності. Важливим аспектом є використання ієрархічної та довіреної агрегації даних, що передбачає оцінку довіри між ГК та відповідними вузлами всередині кожного кластера.

Довіра до агрегатора T_{agg} визначається за виразом:

$$T_{agg} = \frac{\sum_{n=1}^{k}(T_n+1)\cdot W_n}{\sum_{n=1}^{k}(T_n+1)},$$

де T_n – довіра до вузла n у кластері з k сенсорів; W_n – призначена вага для кожного вузла на основі його довіри.

Переваги: висока точність виявлення, адаптивність, можливість виявляти відомі та невідомі атаки, ефективність управління потоками даних.

Недоліки: складність реалізації, налаштування та обслуговування, залежність від якості навчальних даних, значні вимоги до обчислювальних ресурсів.

У таблиці 6 наведено порівняльний аналіз гібридних методів та моделей виявлення вторгнень.

Таблиця 6

Гібридні методи та моделі виявлення вторгнень

Автор	Підхід	Атаки	Метод	Набір даних	Рівні OSI
Sedjelmaci et al. [32]	Децентралізо-ваний	Чорна діра/Black Hole Вибіркова передача/Selective Forwarding Hello флуд/HELLO flood Тунелювання/Wormhole	База специфіка-цій, SVM	TOSSIM	Мережевий
Yan et al. [33]	Децентралізо-ваний	Виснаження /Exhaustion Затоплення/ Flooding Шкідливе ПЗ/Malware Визначення топології /Homing Відмова в обслуговуванні/DoS	BPN База сигнатур	KDDCup'99	Канальний Мережевий Транспортний Прикладний
Subba et al. [34]	Децентралізо-ваний	Чорна діра/Black Hole Вибіркова передача/Selective Forwarding Тунелювання/Wormhole Відмова в обслуговуванні/DoS Сивілли/Sybil	BNE, База специфікацій легка нейронна мережа	NS2	Канальний Мережевий Транспортний Прикладний
Otoum et al. [35]	Централізований	Виснаження/Exhaustion Затоплення/Flooding Шкідливе ПЗ/Malware Визначення топології/Homing	Випадковий ліс E-DBSCAN	NS2	Канальний Мережевий Транспортний Прикладний

Гібридні моделі та методи виявлення вторгнень дають змогу комбінувати переваги вищезазначених методів (сигнатури, аномалії та специфікації) для підвищення точності та адаптивності. Вони вимагають значних зусиль для налаштування, управління та підтримки, мають велику обчислювальну складність.

Висновки. У статті проведено класифікацію та порівняльний аналіз моделей та методів виявлення вторгнень у безпроводових сенсорних мережах тактичної ланки управління військами, на основі підходу управління, протидії атакам та реалізації по рівнях моделі OSI. Результати порівняльного аналізу свідчать, що універсального методу, що задовольняє вимогам безпеки безпроводових сенсорних мереж не існує.

При централізованому підході управляння на єдиний вузол виявлення здійснюється більше навантаження та зростають витрати часу на ідентифікацію вторгнення. Але при децентралізованому підході модуль виявлення вторгнень розгортається на різних рівнях (вузол, ГК, БС), що вимагає більшого споживання енергії для обміну службовою інформацією.

Методи та моделі виявлення вторгнень на основі сигнатур, аномалій, специфікації дають змогу виявляти відомі та невідомі атаки, проте мають ряд недоліків та складнощів пов'язаних з первинним налаштуванням мережі. Водночас вибір гібридного підходу виправданий у випадках, коли потрібна висока точність та адаптивність до нових загроз.

Саме тому для підвищення ефективності виявлення в реальних умовах потрібно розробити гібридний метод, що поєднує різні моделі та методи виявлення вторгнень з автоматичним налаштуванням параметрів та адаптацією до змін у мережевому середовищі.

Напрямом подальших досліджень слід вважати розроблення функціональної моделі системи виявлення вторгнень для підсистеми безпеки у безпроводових сенсорних мережах тактичної ланки управління військами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Міночкін А. І., Романюк В. А., Шаціло П. В. Виявлення атак в мобільних радіомереж. *Збірник наукових праць № 1*. – Київ. ВІТІ НТУУ "КПІ". – 2005. – С. 102-111.

2. Ghosal A., Halder S. A survey on energy efficient intrusion detection in wireless sensor networks. *Journal of Ambient Intelligence and Smart Environments*. 2017. Vol. 9, no. 2. P. 239–261. URL: https://doi.org/10.3233/ais-170426 (date of access: 07.10.2024).

3. Артюх С.Г., Жук О.В., Чернега В.М. Класифікація атак у безпроводових сенсорних мережах тактичної ланки управління військами. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2023.Т. 48. № 3, 2023. С.11-19.

4. On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks / A. Abduvaliyev et al. *IEEE Communications Surveys & Tutorials*. 2013. Vol. 15, no. 3. P. 1223–1237. URL: https://doi.org/10.1109/surv.2012.121912.00006 (date of access: 08.10.2024)..

5. Alrajeh N. A., Khan S., Shams B. Intrusion Detection Systems in Wireless Sensor Networks: A Review. *International Journal of Distributed Sensor Networks*. 2013. Vol. 9, no. 5. P. 167575. URL: https://doi.org/10.1155/2013/167575 (date of access: 07.10.2024).

6. Osanaiye O. A., Alfa A. S., Hancke G. P. Denial of Service Defence for Resource Availability in Wireless Sensor Networks. *IEEE Access*. 2018. Vol. 6. P. 6975–7004. URL: https://doi.org/10.1109/access.2018.2793841 (date of access: 08.10.2024).

7. Alrajeh N. A., Lloret J. Intrusion Detection Systems Based on Artificial Intelligence Techniques in Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*. 2013. Vol. 9, no. 10. P. 351047. URL: https://doi.org/10.1155/2013/351047 (date of access: 08.10.2024).

8. Intrusion Detection System Based on Evolving Rules for Wireless Sensor Networks / N. Lu et al. *Journal of Sensors*. 2018. Vol. 2018. P. 1–8. URL: https://doi.org/10.1155/2018/5948146 (date of access: 08.10.2024).

9. A Partially Distributed Intrusion Detection System for Wireless Sensor Networks / E. Cho et al. *Sensors*. 2013. Vol. 13, no. 12. P. 15863–15879. URL: https://doi.org/10.3390/s131215863 (date of access: 08.10.2024).

10. Centralized IDS Based on Misuse Detection for Cluster-Based Wireless Sensors Networks / F. Hidoussi et al. *Wireless Personal Communications*. 2015. Vol. 85, no. 1. P. 207–224.

11. Hierarchical Abnormal-Node Detection Using Fuzzy Logic for ECA Rule-Based Wireless Sensor Networks / N. Berjab et al. *2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC)*, Taipei, Taiwan, 4–7 December 2018. 2018. URL: https://doi.org/10.1109/prdc.2018.00051 (date of access: 08.10.2024).

12. Ioannou C., Vassiliou V. An Intrusion Detection System for Constrained WSN and IoT Nodes Based on Binary Logistic Regression. *MSWIM '18: 21st ACM Int'l Conference on Modelling, Analysis and Simulation of Wireless and Mobile Systems*, Montreal QC Canada. New York, NY, USA, 2018. URL: https://doi.org/10.1145/3242102.3242145 (date of access: 08.10.2024).

13. Osanaiye O. A., Alfa A. S., Hancke G. P. Denial of Service Defence for Resource Availability in Wireless Sensor Networks. *IEEE Access*. 2018. Vol. 6. P. 6975–7004. URL: https://doi.org/10.1109/access.2018.2793841 (date of access: 08.10.2024).

14. Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model / L. Han et al. *Information Sciences*. 2019. Vol. 476. P. 491–504. URL: https://doi.org/10.1016/j.ins.2018.06.017 (date of access: 08.10.2024).

15. Detection and mitigation of sinkhole attacks in wireless sensor networks / H. Shafiei et al. *Journal of Computer and System Sciences*. 2014. Vol. 80, no. 3. P. 644–653. URL: https://doi.org/10.1016/j.jcss.2013.06.016 (date of access: 08.10.2024).

16. Ballarini P., Mokdad L., Monnet Q. Modeling tools for detecting DoS attacks in WSNs. *Security and Communication Networks*. 2013. Vol. 6, no. 4. P. 420–436.

17. Kaur G., Singh M. Detection of black hole in Wireless Sensor Network based on Data Mining. *2014 5th International Conference- Confluence The Next Generation Information Technology Summit*, Noida, India, 25–26 September 2014. 2014. URL: https://doi.org/10.1109/confluence.2014.6949343 (date of access: 08.10.2024).

18. Hybrid Anomaly Detection by Using Clustering for Wireless Sensor Network / B. Ahmad et al. *Wireless Personal Communications*. 2018. Vol. 106, no. 4. P. 1841–1853. URL: https://doi.org/10.1007/s11277-018-5721-6 (date of access: 08.10.2024).

19. Applying Data Mining Techniques to Intrusion Detection in Wireless Sensor Networks / L. Coppolino et al. *2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, COMPIEGNE, France, 28–30 October 2013. 2013.

20. A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network / W. Li et al. *Journal of Electrical and Computer Engineering*. 2014. Vol. 2014. P. 1–8. URL: https://doi.org/10.1155/2014/240217 (date of access: 08.10.2024).

21. Garofalo A., Di Sarno C., Formicola V. Enhancing Intrusion Detection in Wireless Sensor Networks through Decision Trees. *Lecture Notes in Computer Science*. Berlin, Heidelberg, 2013. P. 1–15. URL: https://doi.org/10.1007/978-3-642-38789-0_1 (date of access: 08.10.2024)..

22. Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks / S. Shamshirband et al. *Engineering Applications of Artificial Intelligence*. 2014. Vol. 32. P. 228–241. URL: https://doi.org/10.1016/j.engappai.2014.02.001 (date of access: 08.10.2024).

23. Wang H., Wen Y., Zhao D. Identifying localization attacks in wireless sensor networks using deep learning. *Journal of Intelligent & Fuzzy Systems*. 2018. Vol. 35, no. 2. P. 1339–1351. URL: https://doi.org/10.3233/jifs-169677 (date of access: 08.10.2024).

24. A Lightweight Intrusion Detection Method Based on Fuzzy Clustering Algorithm for Wireless Sensor Networks / H. Qu et al. *Advances in Fuzzy Systems*. 2018. Vol. 2018. P. 1–12. URL: https://doi.org/10.1155/2018/4071851 (date of access: 08.10.2024).

25. Wireless Sensor Networks Intrusion Detection Based on SMOTE and the Random Forest Algorithm / X. Tan et al. Sensors. 2019. Vol. 19, no. 1. P. 203. URL: https://doi.org/10.3390/s19010203 (date of access: 08.10.2024).

26. Mansouri A., Majidi B., Shamisa A. Metaheuristic neural networks for anomaly recognition in industrial sensor networks with packet latency and jitter for smart infrastructures. *International Journal of Computers and Applications*. 2018. P. 1–10. URL: https://doi.org/10.1080/1206212x.2018.1533613 (date of access: 08.10.2024).

27. Bitam S., Zeadally S., Mellouk A. Bio-inspired cybersecurity for wireless sensor networks. *IEEE Communications Magazine*. 2016. Vol. 54, no. 6. P. 68–74.

28. N. Nithiyanandam, P. Latha Parthiban, B. Rajalingam. Effectively Suppress the Attack of Sinkhole in Wireless Sensor Network using Enhanced Particle Swarm Optimization Technique. *International Journal of Pure and Applied Mathematics*, Vol. 118, No. 9, pp. 313-329, 2018.

29. An Integrated Intrusion Detection Model of Cluster-Based Wireless Sensor Network / X. Sun et al. *PLOS ONE*. 2015. Vol. 10, no. 10. P. e0139513. URL: https://doi.org/10.1371/journal.pone.0139513 (date of access: 08.10.2024).

30. A Hybrid Spectral Clustering and Deep Neural Network Ensemble Algorithm for Intrusion Detection in Sensor Networks / T. Ma et al. *Sensors*. 2016. Vol. 16, no. 10. P. 1701. URL: https://doi.org/10.3390/s16101701 (date of access: 08.10.2024).

31. A Hybrid Spectral Clustering and Deep Neural Network Ensemble Algorithm for Intrusion Detection in Sensor Networks / T. Ma et al. *Sensors*. 2016. Vol. 16, no. 10. P. 1701. URL: https://doi.org/10.3390/s16101701 (date of access: 08.10.2024).

32. Sedjelmaci H., Senouci S. M., Feham M. An efficient intrusion detection framework in cluster-based wireless sensor networks. *Security and Communication Networks*. 2013. Vol. 6, no. 10. P. 1211–1224. URL: https://doi.org/10.1002/sec.687 (date of access: 08.10.2024).

33. Hybrid Intrusion Detection System for enhancing the security of a cluster-based Wireless Sensor Network / K. Q. Yan et al. *2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT 2010)*, Chengdu, China, 9–11 July 2010. 2010. URL: https://doi.org/10.1109/iccsit.2010.5563886 (date of access: 08.10.2024).

34. Subba B., Biswas S., Karmakar S. A Game Theory Based Multi Layered Intrusion Detection Framework for Wireless Sensor Networks. *International Journal of Wireless Information Networks*. 2018. Vol. 25, no. 4. P. 399–421. URL: https://doi.org/10.1007/s10776-018-0403-6 (date of access: 08.10.2024).

35. Otoum S., Kantarci B., Mouftah H. T. Detection of Known and Unknown Intrusive Sensor Behavior in Critical Applications. *IEEE Sensors Letters*. 2017. Vol. 1, no. 5. P. 1–4. URL: https://doi.org/10.1109/lsens.2017.2752719 (date of access: 08.10.2024).