DOI: https://doi.org/10.36910/6775-2524-0560-2025-60-37
УДК 004.056.5:004.738.5:004.032.4
Артюх Сергій Григорович, ад'юнкт
http://orcid.org/0000-0003-2142-1552
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна

МЕТОД ВИЯВЛЕННЯ ВТОРГНЕНЬ У БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ НА ОСНОВІ ПРАВИЛ СПЕЦИФІКАЦІЇ ТА ШТУЧНОЇ НЕЙРОННОЇ МЕРЕЖІ

Артюх С. Г. Метод виявлення вторгнень у безпроводових сенсорних мережах на основі правил специфікації та штучної нейронної мережі. Використано ймовірнісну (стохастичну) стратегію моніторингу, засновану на байєсівській рівновазі Неша, що дало змогу агентам ВВ автоматично оптимізувати свою поведінку залежно від поточного рівня загроз і власних ресурсів, а також динамічно змінювати свої стратегії, забезпечуючи гнучкість й адаптивність системи до змін у поведінці зловмисних вузлів. Розроблено правила специфікації, які базуються на комбінуванні показників сенсорних вузлів, що впливають на якість передачі інформації. Стан вузлів відстежується агентами виявлення вторгнень, які пасивно моніторять мережу. Використано багатошарову нейронну мережу для динамічного оновлення порогових значень показників сенсорних вузлів у базі даних правил специфікацій, що використовуються агентами виявлення вторгнень. Розроблено та формалізовано метод виявлення вторгнень у безпроводових сенсорних мережах завдяки поєднанню ймовірнісної стратегії моніторингу агентами виявлення вторгнень стану сенсорного вузла на основі рівноваги Неша, правил специфікації комбінування показників сенсорних вузлів та детектування аномальної вузлів з використанням багатошарової нейронної мережі дало змогу адаптивно відстежувати аномалії та виявляти атаки мережевого рівня, запобігаючи небезпечному впливу зловмисних вузлів завдяки їх блокуванню.
Ключові слова: безпроводові сенсорні мережі, виявлення вторгнень, правила специфікації, штучний інтелект, нейронна мережа, машинне навчання, теорія ігор, метрики, рівновага Неша, база даних, кібербезпека.

Artiukh S. A method for detecting intrusions in wireless sensor networks based on specification rules and an artificial neural network. A probabilistic (stochastic) monitoring strategy based on Nash's Bayesian equilibrium was used, which allowed BB agents to automatically optimize their behavior depending on the current threat level and their own resources, as well as dynamically change their strategies, ensuring the flexibility and adaptability of the system to changes in the behavior of malicious nodes. Specification rules have been developed based on a combination of sensor node indicators that affect the quality of information transmission. The status of nodes is tracked by intrusion detection agents that passively monitor the network. A multilayer neural network is used to dynamically update the threshold values of sensor node indicators in the specification rule database used by intrusion detection agents. A method for detecting intrusions in wireless sensor networks has been developed and formalized by combining a probabilistic strategy for monitoring the status of a sensor node by intrusion detection agents based on Nash equilibrium, rules for combining sensor node indicators, and detection of anomalous nodes using a multilayer neural network. This made it possible to adaptively track anomalies and detect network-level attacks, preventing the dangerous influence of malicious nodes by blocking them.
Keywords: wireless sensor networks, intrusion detection, specification rules, artificial intelligence, neural network, machine learning, game theory, metrics, Nash equilibrium, database, cybersecurity.

Постановка проблеми. Безпроводові сенсорні мережі (БСМ) є розподіленою системою, що самоорганізується та складається з великої кількості невеликих за розмірами вузлів, об'єднаних між собою безпроводовим зв'язком. Завдяки здатності до ретрансляції повідомлень між різними елементами, БСМ можуть застосовуватися для низки специфічних завдань, а саме: моніторинг розташування противника, його кількості та характеру дій; збір розвідувальної інформації на місцевості; використання в системах наведення інтелектуальних снарядів; визначення положення необхідних об'єктів (подій); забезпечення захисту своїх підрозділів; моніторинг державного кордону в будь-якій місцевості та за будь-яких умов [1].

Разом з тим, БСМ характеризуються низкою обмежень щодо обчислювальних ресурсів вузлів, ширини смуги пропускання каналу зв'язку, малим об'ємом пам'яті для зберігання даних, часу автономної роботи вузлів, пов'язаною з ємністю батареї, а також специфікою їх випадкового розташуванням на місцевості.

Перелічені особливості значною мірою підвищують вразливість БСМ до різних типів атак [2]. Сенсорні вузли можуть бути легко скомпрометовані зловмисником, що дає змогу отримати йому контроль над пристроями, втручатись в їх роботу та фальсифікувати дані тощо.

Традиційні методи забезпечення безпеки, розроблені для проводових мереж, такі як міжмережеві екрани, системи шифрування та аутентифікації, виявляються малоефективними у БСМ через обмеженість ресурсів. Слід зазначити, що криптографічні підходи для захисту БСМ мають суттєві недоліки пов'язані з високими енерговитратами та нездатністю захищатись від внутрішні загрози [3, 4]. Тому виникає потреба у створенні спеціалізованих механізмів виявлення вторгнень, адаптованих до специфіки БСМ, що мають мінімальні витрати енергії та

обчислювальних ресурсів.

Аналіз останніх досліджень і публікацій. Ієрархічна система виявлення вторгнень (ВВ) на основі набору правил для ідентифікації зловмисних вузлів і запису детальної інформації про них в ієрархічну таблицю ізоляції, запропонована в [5]. Всі вузли в мережі управляються головами кластера (ГК), які надсилають всі сповіщення про виявлення вторгнень до основного голови кластера для їх агрегації та подальшої передачі до базової станції (БС). Недоліком зазначеної ієрархічна система ВВ є те, що основне навантаження щодо аналізу та ізоляції атак зосереджене на ГК, що може призвести до їх швидкого виснаження. Функції ГК залишаються незмінними протягом усього часу роботи мережі, що знижую загальну тривалість життя мережі та підвищує ймовірність відмови.

Децентралізовані кооперативні системи виявлення вторгнень, що розглянуті в [6, 7], використовують звичайні сенсорні вузли для аналізу трафіку мережі. Кожен вузол моніторить поведінку потенційно зловмисних вузлів, застосовуючи набір специфікаційних правил. Недоліком таких систем є загальний час життя БСМ пов'язаний з великими енерговитратами при виконанні моніторингу та синхронізації розподілених по мережі агентів виявлення вторгнень.

Система ВВ на основі аномалій, яка використовує розподілений SVM-класифікатор для виявлення зловмисних сенсорних вузлів, запропонована в [8]. Недоліком такої системи є великі обчислювальні витрати на реалізацію функціонування моделі SVM-класифікатора. Система виявлення вторгнень на основі аномалій, що використовує інформацію про сенсорні вузли (записи в таблицях маршрутизації, індикація рівня сигналу, розклад сну/пробудження тощо) для виявлення зловмисних вузлів, запропонована в [9]. Однак, недоліком системи ВВ є його високі обчислювальні витрати, що призводить до швидкого виснаження ресурсів БСМ.

Для ефективного виявлення атак на маршрутизацію, атак воронки, чорної діри та тунелювання у [10, 11] запропоновано використання систем ВВ на основі правил специфікації. Разом з тим недоліком таких систем є потреба регулярного оновлення бази правил специфікації. Також гібридні методи виявлення вторгнень на основі правил специфікації та аномалій, що досягають високої точності та швидкості виявлення широкого спектру атак, запропоновані в [12, 13]. Основним недоліком цих методів є їх високі обчислювальні витрати та споживання енергії, що мають негативний вплив на загальний термін роботи БСМ.

У [14] запропоновано систему виявлення вторгнень на основі теорії ігор, що використовує взаємне оцінювання вузлів і введення механізму ізоляції. Кожен вузол має перебувати в коректному стані функціонування (брати участь в маршрутизації та передачі даних між вузлами мережі), що визначає його репутацію. В разі втрати репутації вузлу призначається статус зловмисного, що призводить до тимчасового блокування функціонування вузла в мережі. Недоліком системи ВВ на основі теорії ігор є виявлення тільки атак типу чорна діра та можливість повернення вузла до зловмисної роботи після відновлення своєї репутації по завершенню блокування.

Метод децентралізованого виявлення вторгнень в мережі Vehicular Ad-hoc Network (VANET) запропонований у [15]. Такий метод використовує стратегію динамічної гри при якій гравець у кожному раунді копіює дії свого суперника з попереднього раунду. Спостереження за станом сенсорних вузлів здійснюється сусідніми вузлами та зазначена інформація передається до ГК. Для оцінювання репутації кожного вузла використовується теорія Демпстера–Шейфера, що дає змогу виявляти вторгнення за умови часткової невизначеності або суперечливості інформації на основі колективних спостережень. Проте при цьому метод генерується великий обсяг трафіку пов'язаного з виявлення вторгнень, та вимагає від усіх елементів мережі приймати участь моніторингу зловмисних вузлів.

Ієрархічний структуру системи ВВ для мереж Mobile Ad hoc Network (MANET), в якій функції моніторингу покладаються на ГК запропоновано у [16]. Взаємодія між ГК та сенсорними вузлами мережі моделюється як некооперативна байєсівська гра між двома гравцями, а ймовірнісні стратегії моніторингу формуються на основі рівноваги Неша. Проте основними недоліками цієї системи ВВ є можливість детектування тільки DoS атак та додаткові витрати ресурсів пов'язані з процедурою вибору ГК.

Разом з тим зазначений підхід щодо використання ймовірнісної стратегії моніторингу на основі рівноваги Неша доцільно використати для протидії більшої кількості атак мережевого рівня у БСМ.

Метою статті є розроблення методу виявлення вторгнень у безпроводових сенсорних

мережах на основі запропонованих специфікаційних правил комбінування показників сенсорних вузлів та багатошарової нейронної мережі детектування аномалій з використання імовірнісних стратегії моніторингу на основі теорії ігор для підвищення точності виявлення атак мережевого рівня та попередження виснаження ресурсів сенсорних вузлів.

Виклад основного матеріалу дослідження. Розглянемо ієрархічну гетерогенну кластерну БСМ, яка складається з трьох визначених рівнів: сенсорних вузлів, голови кластерів та базової станції. Всі сенсорні вузли мережі групуються в кластери та здійснюють передачу даних безпосередньо до свого ГК. Порівняно із сенсорними вузлами ГК мають збільшені обчислювальну потужність, запас енергії та дальність передачі сигналу. Голова кластеру координує діяльність сенсорних вузлів, приймає рішення щодо їх безпеки, агрегує, аналізує та передає узагальнену інформацію до БС. Централізоване управління всією мережею на основі аналізу та обробки даних здійснює БС (найпотужніший елемент мережі з необмеженим або значно більшим запасом енергії, підключений до зовнішніх інформаційних систем або інтернету), забезпечуючи масштабованість і стійкість всієї мережі (рис. 1).

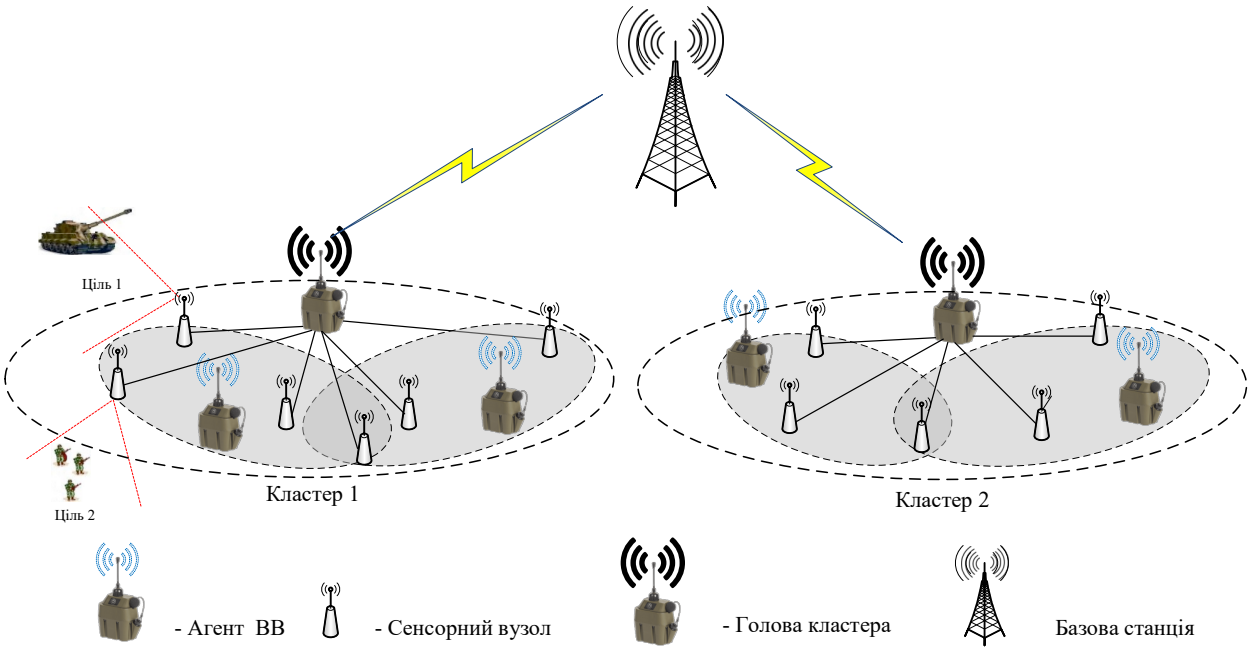


Рис. 1 Ієрархічна гетерогенна кластерна безпроводова сенсорна мережа.

У БСМ, наведеній на рис. 1, використовується сенсорні вузли типу T_1 виконують лише операцію збору первинних даних із зовнішнього середовища (температура, вологість, тиск, рівень освітленості тощо) та характеризуються низьким енергоспоживанням, обмеженими обчислювальними можливостями. Ці вузли передають дані безпосередньо ГК та не беруть участі у процесах виявлення вторгнень.

Вузли другого типу T_2 на додаток до операції збору даних здійснюють моніторинг стану сенсорних вузлів T_1, та мають більшу дальність передачі даних, підвищену обчислювальну потужність і як наслідок збільшене енергоспоживання. Слід зазначити, що вузли типу T_2 можуть перебувати в активному або пасивному режимах роботи . В активному режимі вузли типу T_2 можуть виконувати функції голови кластеру або агентів виявлення вторгнень та здійснювати операцію аналізу поведінки інших сенсорних вузлів мережі. Агенти ВВ проводять пасивний моніторинг, який впливає на його енергоефективність під час виявлення аномалій та атак у кластерних БСМ. Водночас, у межах свого кластера агент ВВ спостерігає за станом сенсорних вузлів T_1, не ініціює жодних запитів до них та не впливає на протокол передачі даних, залишаючись невидимим для мережі до моменту виявлення зловмисної активності.

Опишемо процес виявлення вторгнень на рівні сенсорних вузлів, наведеного на структурній схемі (рис. 2). Моніторинг агентом ВВ стану сенсорного вузла T_1 моделюється як некооперативна (*гравці не можуть об'єднуватись*) байєсівська (*вводиться ймовірність вибору гравцем тієї чи іншої стратегії*) гра з неповною інформативністю (*гравці мають вірування про невідоме, описані*

через розподіл імовірностей) між агентом ВВ та сенсорним вузлом (*двома конкуруючими гравцями*).

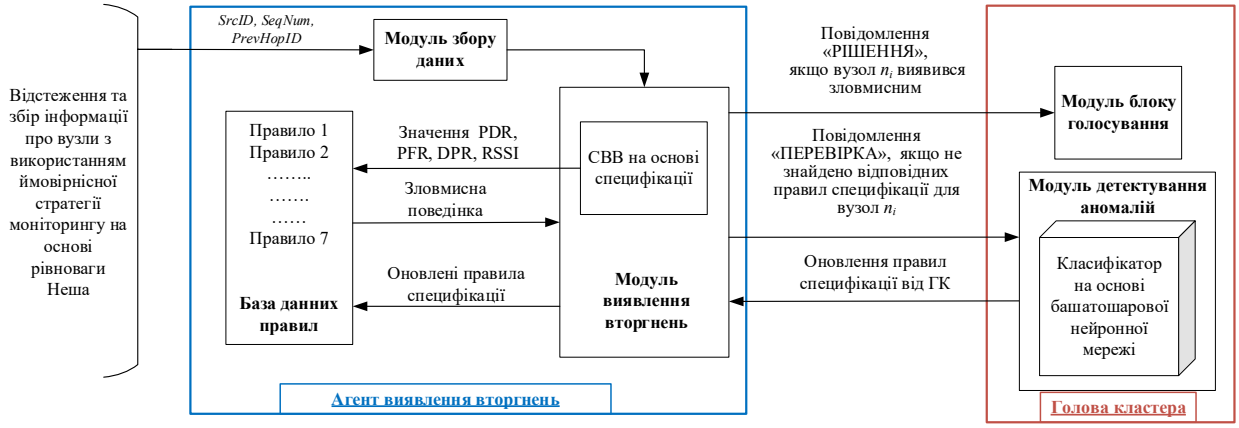


Рис. 2 – Структурна схема виявлення вторгнень на рівні сенсорних вузлів.

Для попередження виснаження ресурсів сенсорних вузлів (T_1), агенти ВВ (T_2) потребують оптимізації обсягу даних, які вони передають ГК. Надлишковий трафік, пов'язаний із процесами виявлення вторгнень, також може призводити до перевантаження мережі. Для вирішення зазначеної проблеми запропоновано використати ймовірнісний моніторинг агентами ВВ стану сенсорного вузла, що ґрунтується на рівновазі Неша, фундаментальному понятті в теорії ігор, коли жоден гравець не має вигоди змінювати свою стратегію в односторонньому порядку, якщо інші гравці не змінюють своїх [17].

Взаємодія між агентом ВВ (T_2) та сенсорним вузлом T_1 може бути представлена динамічною байєсівською грою, де один із гравців P_i є потенційним зловмисним вузлом, а інший гравець P_j є агентом ВВ. Інформацією про стан сенсорного вузла θ_{Pi} є невідомою для агента ВВ, який перебуває в стані θ_{Pj} (де j – кількість агентів ВВ). Якщо θ_{Pi}=1 (або 0), тоді сенсорний вузол є нормальним (або зловмисним).

Відповідно до теорії ігор припустимо, що сенсорний вузол може діяти за стратегією S_{Pi}. У зловмисному випадку вузол діє за двома стратегіями {*Атакувати, Не атакувати*}, а нормальний вузол – лише за однією {*Не атакувати*}. Вважатимемо, що агент ВВ завжди є нормальним (θ_{Pj}=1) і діє тільки за двома стратегіями S_{Pj} {*Моніторити, Не моніторити*}. Оскільки агент ВВ не має змоги перевірити стан сенсорного вузлом, то взаємодія між ними моделюється як байєсівська гра з неповною інформативністю:

$$G= \langle \Pi, S, U \rangle, \quad (1)$$

де $\Pi=\{P_i, P_j\}$ — множина взаємодіючих вузлів;

$S= S_{Pi} \times S_{Pj}$ — простір стратегій;

$U= U_{Pi} \times U_{Pj}$ — функція корисність сенсорного вузла та агента ВВ, яка залежать від їх стратегій S.

Припустимо $N =\{n_1, n_2, \dots, n_k\}$ – множина сенсорних вузлів у заданому кластері, а вузол $n_i \in N(1 \le i \le k)$ з активом ω_{n_i}, який позначає важливість сенсорного вузла в кластері, з погляду функціонування мережі, цілісності даних, ступеня участі у маршрутизації (агрегація даних, пересилання пакетів та кількості взаємодіючих з ним сенсорних вузлів) та потенційних втрат у разі його зловмисних дій

Показник правильних спрацьовувань (True positive Rate – TPR) та показник хибних спрацьовувань (False Positive Rate – FPR) агента ВВ позначимо через α та γ, відповідно, де $\alpha, \gamma \in [0,1]$. Витрати ресурсів пов'язані з реалізацією атаки позначимо через C_{a_i} та відповідно – здійснення моніторингу сенсорного вузла C_{m_i}. Зробимо припущення, що $C_{a_i}, C_{m_i} \ll \omega_{n_i}$, інакше у зловмисника і агента ВВ не буде жодного вигідного стимулу атакувати і захищати вузол n_i.

У таблиці 1 і таблиці 2 наведені матриці корисності, що відповідають взаємодії між агентом ВВ і вузлом n_i, коли стан сенсорного вузла n_i є зловмисним або нормальним.

Таблиця 1. Матриця корисності для зловмисного вузла

Стратегії	*Моніторити*	*Не моніторити*
Атакувати	$(1-2\alpha)\omega_{n_i} - C_{a_i}$; $(2\alpha-1)\omega_{n_i} - C_{m_i}$	$\omega_{n_i} - C_{a_i}$; $-\omega_{n_i}$
Не атакувати	0; $-\gamma\omega_{n_i} - C_{m_i}$	0; 0

Таблиця 2. Матриця корисності для нормального вузла

Стратегії	*Моніторити*	*Не моніторити*
Не атакувати	0; $-\gamma\omega_{n_i} - C_{m_i}$	0; 0

Сутність наведених матриць, полягає в тому, щоб дати змогу агенту ВВ максимізувати ймовірність успішного виявлення зловмисного вузла та водночас мінімізувати зловмисному вузлу ймовірність свого виявлення.

Для опису послідовності реалізацій зазначених стратегій (табл. 1, 2) доцільно використати дерево рішень (рис. 3), де сенсорному вузлу n_i на початку гри присвоюється значення апріорної зловмисності (p_o), що є загальною попередньою, відомою інформацією як агенту ВВ так і сенсорному вузлу n_i [16].

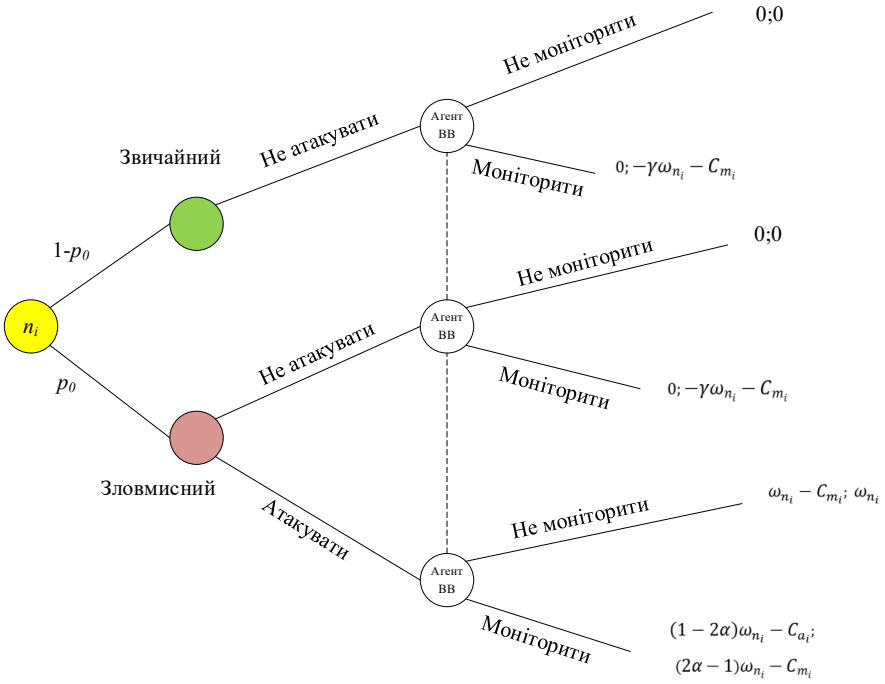


Рис. 3 – Дерево рішень реалізації стратегій в байєсівській грі між сенсорним вузлом та агентом ВВ

Припустимо, що зловмисний вузол реалізує чисту (детерміновану) стратегію *Атакувати*, то функції корисності агента ВВ під час реалізації стратегій *Моніторити* і *Не моніторити* відповідно становлять:

$$U_{\text{агент}}(\text{Моніторити}) = p_o\left((2\alpha-1)\omega_{n_i} - C_{m_i}\right) - (1-p_o)\left(\gamma\omega_{n_i} + C_{m_i}\right), \quad (2)$$

$$U_{\text{агент}}(\text{Не моніторити}) = -p_o\omega_{n_i}, \quad (3)$$

Функція $U_{\text{агент}}(\text{Моніторити})$ характеризує успішне виявлення атаки агентом ВВ завдяки моніторингу дій зловмисного вузла та запобігання його шкідливого впливу на мережу(кластер). Функція корисності $U_{\text{агент}}(\text{Не моніторити})$ характеризує витрати ресурсів агентом ВВ у випадку, коли шкідливий вузол здійснює атаку, а агент ВВ не виконує жодної дій.

Припустимо, що агент ВВ реалізує детерміновану стратегію *Моніторити*, то функції

корисності зловмисного вузла n_i під час реалізації стратегій *Атакувати* та *Не атакувати* відповідно становлять:

$$U_{n_i}(\text{Атакувати}) = p_o\left((1-2\alpha)\omega_{n_i} - C_{a_i}\right), \tag{4}$$

$$U_{n_i}(\text{Не атакувати}) = 0. \tag{5}$$

Функція $U_{n_i}(\text{Атакувати})$ характеризує витрати ресурсів на реалізацію атаки зловмисним вузлом n_i, а функція $U_{n_i}(\text{Не атакувати})$ характеризує витрати ресурсів, у випадку коли він не виконує жодних.

За умови $U_{\text{агент}}(\text{Моніторити}) > U_{\text{агент}}(\text{Не моніторити})$, агент ВВ буде реалізовувати детерміновану стратегію *Моніторити*, у випадку коли зловмисний вузол реалізовує детерміновану стратегію *Атакувати*. Однак, у випадку якщо агент ВВ буде реалізовувати детерміновану стратегію *Моніторити*, природною реакцією зловмисного вузла буде реалізація детермінованої стратегії *Не атакувати.* Зазначене вище свідчить про те що зловмисний вузол може змінювати свою стратегію, що порушує рівновагою Неша у байєсівській грі за умови $p_o > \frac{\gamma\omega_{n_i}+C_{m_i}}{(2\alpha+\gamma)\omega_{n_i}}$

За умови $U_{\text{агент}}(\text{Моніторити}) < U_{\text{агент}}(\text{Не моніторити})$, агент ВВ буде реалізовувати детерміновану стратегію *Не моніторити*, незалежно від стратегії зловмисного вузла при $p_o < \frac{\gamma\omega_{n_i}+C_{m_i}}{(2\alpha+\gamma)\omega_{n_i}}$, що відповідає детермінованою рівновагою Неша у байєсівській грі.

Якщо зловмисний вузол буде реалізовувати детерміновану стратегію *Не атакувати*, то домінуючою стратегією агент ВВ буде *Не моніторити*, незалежно від значення p_o. У випадку, якщо агент ВВ буде реалізовувати детерміновану стратегію *Не моніторити*, природною реакцією зловмисного вузла буде – *Атакувати*. Таким чином агенту ВВ доцільно не моніторити поки зловмисний вузол не атакує, водночас для зловмисного вузла доцільно атакувати, щойно агент ВВ перестає моніторити.

Результати аналізу комбінування детермінованих стратегій зловмисного вузла та агент ВВ свідчать про те що не виконуються умови рівноваги Неша у байєсівській грі. Проте будь-яка некооперативна гра, що містить кінцеву множину гравців і стратегій, завжди має змішану (стохастичну) рівновагу Неша [17].

Припустимо зловмисний вузол реалізовує детерміновану стратегію *Атакувати* з ймовірністю p, тоді функція корисності агента СВВ, який реалізовує детерміновану стратегію *Моніторити* становить:

$$U_{\text{агент}}(\text{Моніторити}) = pp_o\left((2\alpha-1)\omega_{n_i} - C_{m_i}\right) - (1-p)p_o\left(\gamma\omega_{n_i} + C_{m_i}\right) - \\ -(1-p_o)\left(\gamma\omega_{n_i} + C_{m_i}\right), \tag{6}$$

Водночас функція корисності агента ВВ, який реалізовує стратегію *Не моніторити* становить:

$$U_{\text{агент}}(\text{Не моніторити}) = -pp_o\omega_{n_i}, \tag{7}$$

Разом з тим, функція корисності зловмисного вузла, що реалізовує детерміновані стратегії *Атакувати* та *Не атакувати*, коли агент ВВ реалізовує стратегію *Моніторити* з ймовірністю q відповідно становить :

$$U_{n_i}(\text{ Моніторити}) = p_o\left(q\left((1-2\alpha)\omega_{n_i} - C_{a_i}\right) + (1-q)\left(\omega_{n_i} - C_{a_i}\right)\right), \tag{8}$$

$$U_{n_i}(\text{Не моніторити}) = 0, \tag{9}$$

За умови $U_{\text{агент}}(\text{Моніторити}) = U_{\text{агент}}(\text{Не моніторити})$, для реалізації зловмисним вузлом стратегії *Атакувати* відповідає рівновазі Неша у байєсівській грі, ймовірність визначається за виразом:

$$p = \frac{\gamma\omega_{n_i}+C_{m_i}}{(2\alpha+\gamma)\omega_{n_i}p_o}, \tag{10}$$

Аналогічно, за умови $U_{n_i}(\text{Атакувати}) = U_{n_i}(\text{Не атакувати})$, ймовірність агента ВВ реалізувати стратегію *Моніторити* за рівновагою Неша у байєсівській грі визначається за виразом:

$$q = \frac{\omega_{n_i} - C_{a_i}}{2\alpha\omega_{n_i}}, \tag{11}$$

Оскільки при $p_o > \frac{\gamma\omega_{n_i} + C_{m_i}}{(2\alpha+\gamma)\omega_{n_i}}$ не існує детермінованої рівноваги Неша, але існує стохастична рівновага Неша у байєсівській грі, яка відповідає комбінації стратегій *Атакувати* з імовірністю p, якщо зловмисний вузол, *Не атакувати* коли – нормальний та *Моніторити* з ймовірністю q, p_o.

Оскільки в запропонованій моделі байєсівської гри попереднім є визначення ймовірності p_o зловмисного вузла, то представимо взаємодію між агентом ВВ і сенсорним вузлом як багатоетапну некооперативну гру, де переконання щодо зловмисності вузла n_i на i-му етапі гри оновлюється з використанням правила Байєса:

$$p_{P_j}\left(\theta_{P_i}|d_i(t), d_i(t-1)\right) = \frac{p_{P_j}\left(\theta_{P_i}|d_i(t-1)\right)P\left(d_i(t)|\theta_{P_i}, d_i(t-1)\right)}{\sum_{\tilde{\theta}_{P_i}} p_{P_j}\left(\tilde{\theta}_{P_i}|d_i(t-1)\right)P\left(d_i(t)|\tilde{\theta}_{P_i}, d_i(t-1)\right)}, \tag{12}$$

де $p_{P_j}\left(\theta_{P_i}|d_i(t-1)\right)$ – ймовірність спостереження агентом ВВ P_j стану вузла n_i за умови виконаної дії $d_i(t-1)$на попередьому етапі;

$P\left(d_i(t)|\theta_{P_i}, d_i(t-1)\right)$ – ймовірністю того, що вузол n_i виконує дію $d_i(t)$ на t-му етапі, враховуючи його визначений стан θ_{P_i} і попередню дію $d_i(t-1)$ на попередньому етапі;

$p_{P_j}\left(\tilde{\theta}_{P_i}|d_i(t-1)\right)$ ймовірність спостереження агентом ВВ P_j будь-якого стану $\tilde{\theta}_{P_i}$ вузла n_i за умови виконаної дії $d_i(t-1)$на попередньому етапі.

Умовну ймовірність, визначену наведеним вище правилом Байєса, можна обчислити за допомогою таких рівнянь:

$$P\left(d_i(t) = \text{Атакувати}|\theta_{P_i} = 1, d_i(t-1)\right) = p\alpha + (1-p)\gamma, \tag{13}$$

$$P\left(d_i(t) = \text{Не атакувати}|\theta_{P_i} = 1, d_i(t-1)\right) = p(1-\alpha) + (1-p)(1-\gamma), \tag{14}$$

$$P\left(d_i(t) = \text{Атакувати}|\theta_{P_i} = 0, d_i(t-1)\right) = \gamma, \tag{15}$$

$$P\left(d_i(t) = \text{Не атакувати}|\theta_{P_i} = 0, d_i(t-1)\right) = 1-\gamma \tag{16}$$

Стохастична рівновага Неша дає змогу одночасно забезпечити агентам ВВ непередбачуваність під час моніторингу сенсорних вузлів у кластері та оптимальність витрат ресурсів, що доповнює процес виявлення вторгнень у БСМ.

Для виявлення зловмисних вузлів в кластері агент ВВ доцільно використати набір правил специфікації, заснованих на значеннях показників *PDR*, *DPR*, *PFR* і *RSSI* вузлів (набір метрик), що характеризують їх обчислювальні ресурси та службовий трафік.

1. Коефіцієнт втрат пакетів *PDR* (Packet Drop Rate) – це частка переданих від вузла пакетів, які не отримані іншими вузлами (T_1 або T_2) у часовому вікні Δt. Він визначається за виразом [18]:

$$PDR = \frac{N_{\text{втр}}}{N_{\text{втр}} + N_{\text{прий}}}, \tag{17}$$

де $N_{\text{втр}}$ – кількість втрачених пакетів у часовому вікні Δt;

$N_{\text{прий}}$ – кількість прийнятих пакетів вузлом T_1.

Для обліку втрат пакетів, кожен переданий пакет від вузла T_1 має містити ідентифікатор джерела (*SrcID*), що дає змогу агенту диференціювати потоки від різних сенсорних вузлів, та порядковий номер пакета (*SeqNum*), що збільшується при кожній новій передачі.

Обчислення *PDR* здійснюється агентом у ковзному часовому вікні Δt завдяки аналізу порядкових номерів пакетів (*SeqNum)* отриманих від T_1. Якщо у потоці номерів *SeqNum* виявлено пропуски, вони накопичуються у лічильнику втрат з визначенням їх загальної кількості по завершенні часового інтервалу.

2. Коефіцієнт пересилання пакетів *PFR* (Packet Forwarding Rate) – визначає частку транзитних пакетів, які сенсорний вузол T_1 переадресовує далі за маршрутом. Він визначається за виразом [18]:

$$PFR = \frac{N_{\text{транз}}}{N_{\text{фіксован}}}, \tag{18}$$

де $N_{\text{транз}}$ – кількість транзитних пакетів, які вузол T_1 мав би переслати у часовому вікні Δt;

$N_{\text{фіксован}}$ – кількість пакетів, які агент ВВ фактично зафіксував у ефірі від вузла T_1.

Агент ВВ аналізує пакети та записує до переліку ідентифікатор попереднього вузла *PrevHopID* та номер пакета *SeqNum* і протягом проміжку часу τ відстежує ретрансляцію цього пакету вузлом T_1. У випадку зафіксованої ретрансляції – лічильник $N_{\text{транз}}$ збільшує значення на 1 і запис в таблиці видаляється. Якщо час τ сплив без ретрансляції – збільшується значення $N_{\text{фіксован}}$ на 1. Наприкінці кожного вікна Δt значення *PFR* обчислюється для кожного сусіднього вузла T_1, а лічильники обнуляються для нового циклу спостереження.

3. Коефіцієнт дублювання пакетів *DPR* (Duplicate Packet Rate) визначає частку пакетів, що передані повторно від одного й того самого вузла в межах часового вікна Δt та визначається за виразом [19]:

$$DPR = \frac{N_{\text{дубл}}}{N_{\text{заг}}}, \tag{19}$$

де $N_{\text{дубл}}$ – кількість дубльованих пакетів;

$N_{\text{заг}}$ – загальна кількість отриманих пакетів від вузла за час Δt.

Для кожного прийнятого пакета агент ВВ реєструє пару *SrcID, SeqNum* та перевіряє її на наявність запису в локальному переліку. У разі наявності запису зазначеної пари лічильник $N_{\text{дубл}}$ збільшується на 1.

4. Показник рівня отриманого сигналу *RSSI* (Received Signal Strength Indicator) – це числовий параметр, що характеризує потужність радіосигналу, прийнятого радіоприймачем сенсорного вузла під час отримання кожного пакета даних. *RSSI* автоматично вимірюється агентом ВВ без додаткової взаємодії з вузлами T_1 та використовується для оцінювання якості зв'язку між вузлами у БСМ. Цей показник визначається за виразом [20]:

$$RSSI = P_0 - 10\beta * lg\left(\frac{d}{d_0}\right), \tag{20}$$

де d – відстань від пристрою до передавача;

d_0 – відстань від пристрою до точки, на якій виконувався вимірювання потужності сигналу P_0 (еталонна відстань);

P_0 – потужність сигналу пристрою, виміряна на одиничній відстані d_0 від пристрою, dBm;

β – коефіцієнт загасання сигналу при поширенні в середовищі.

Слід зазначити, що сенсорний вузол T_1 гетерогенних ієрархічних БСМ n_i (де i =1,.., k, а k – кількість вузлів у кластері) найбільш вразливі для атак мережевого рівня, що впливають на порушення конфіденційності, цілісності, доступності, автентифікації та виснаження ресурсів. До таких атак належать атака Сивілли, Hello флуд атака, атаки типу вибіркова передача, атака чорної діри, атака типу тунелювання, атака модифікації маршрутної інформації та атаки створення завад [2].

Для виявлення зазначених атак мережевого рівня розробимо правила специфікації для агентів ВВ, які базуються на формальних або неформальних описах правильного, очікуваного або допустимого функціонування системи, процесу чи пристрою [21]. Зазначені правила визначають, як має поводитись система або її компоненти у "нормальних" умовах, і використовуються для виявлення відхилень чи помилок:

Правило 1. ЯКЩО значення *PDR* на вузлі n_i перевищує порогове значення $\delta_{pdr_{SF}}$, ТО вузол n_i виконує атаку вибіркового передачі.

Правило 2. ЯКЩО значення *PDR* та *RSSI* вузла n_i перевищують порогові значення $\delta_{pdr_{BH}}$, та $\delta_{rssi_{BH}}$, ТО вузлом n_i виконується атака чорної діри.

Правило 3. ЯКЩО значення *RSSI* вузла n_i перевищує порогове значення $\delta_{rssi_{WH}}$, а значення *PDR* сусіднього вузла n_i перевищує $\delta_{pdr_{WH}}$, ТО вузол n_i вважається учасником атаки тунелювання.

Правило 4. ЯКЩО значення *DPR*, *PFR* та *RSSI* вузла n_i перевищують порогові значення $\delta_{dpr_{JAM}}$, $\delta_{pfr_{JAM}}$, та $\delta_{rssi_{JAM}}$ ТО вузол n_i вважається учасником атаки створення завад.

Правило 5. ЯКЩО Z-оцінка *RSSI* для вузла n_i перевищує порогове значення 2,5 $\delta_{rssi_{SYB}}$, ТО вузол n_i вважається учасником атаки Сивілли. [22] Z-оцінка обчислюється для RSSI вузла n_i за формулою:

$$Z = \frac{RSSI_{n_i} - \mu}{\sigma}, \tag{21}$$

де μ – середнє значення рівеня потужності прийнятих сигналів у кластері;

σ – середньоквадратичне значення *RSSI* всіх сусідніх вузлів у кластері.

Правило 6. ЯКЩО значення *PDR* та *RSSI* вузла n_i перевищує порогове значення $\delta_{rssi_{HELLO}}$ та $\delta_{pdr_{HELLO}}$, а значення *PFR* не перевищують порогові значення $\delta_{pfr_{HELLO}}$, ТО вузол n_i здійснює атаку Hello флуд.

Правило 7. ЯКЩО значення *PFR* та *DPR* вузла n_i перевищує порогове значення $\delta_{pfr_{SRI}}$ та $\delta_{dpr_{SRI}}$, а значення *PDR* не перевищує порогове значення $\delta_{pdr_{SRI}}$, ТО вузол n_i здійснює модифікацію маршрутної інформації.

Для виявлення атак мережевого рівня агент ВВ корелює значення показників *PDR*, *DPR*, *PFR* і *RSSI* сенсорних вузлів із набором правил специфікації, які зберігаються в його базі даних правил. Коли агент ВВ виявляє зловмисний вузол, він інформує ГК через повідомлення *«РІШЕННЯ»*. Повідомлення *«РІШЕННЯ»* містить тип виявленої атаки, ідентифікатори зловмисного сенсорного вузла та самого агента ВВ. Голова кластеру реєструє це повідомлення у своїй таблиці підозр та чекає на додаткові повідомлення від інших агентів ВВ для досягнення заданого порогу кворуму. Якщо досягнуто кворум ГК ізолює вузол T_1 на локальному рівні (видаляє його з топології, видаляє маршрути до нього, припиняє передачу даних через цей T_1 та додає його до локального чорного списку). Після цього ГК формує підсумковий пакет і надсилає його на БС для інформування щодо повного блокування зловмисного вузла.

Якщо локальні правила специфікацій не дали однозначного висновку щодо зловмисності сенсорного вузла, агент ВВ надсилає ГК повідомлення «*ПЕРЕВІРКА»* для верифікації й реагування на підозрілу активність сенсорних вузлів. Повідомлення «*ПЕРЕВІРКА»* містить множину показників (метрик)вузла (*PDR*, *PFR*, *DPR*, *RSSI*), ідентифікатор підозрюваного сенсорного вузла та самого агента ВВ. Таке повідомлення дає підставу ГК для прийняття рішення стосовно зловмисності вузла, особливо якщо на один і той самий вузол T_1 надходять декілька повідомлень *«ПЕРЕВІРКА»*, та ініціювати розширену процедуру аналізу, що містить такі етапи:

1. Голова кластера здійснює оцінювання множини підозрілих показників вузла на основі власної бази специфікаційних правил, що враховують особливості топології кластера та поточну статистику мережі. Якщо значення множини показників виходять за межі встановлених порогових значень або їхня комбінація вказує на потенційну атаку, ГК може одразу прийняти рішення про зловмисність вузла.

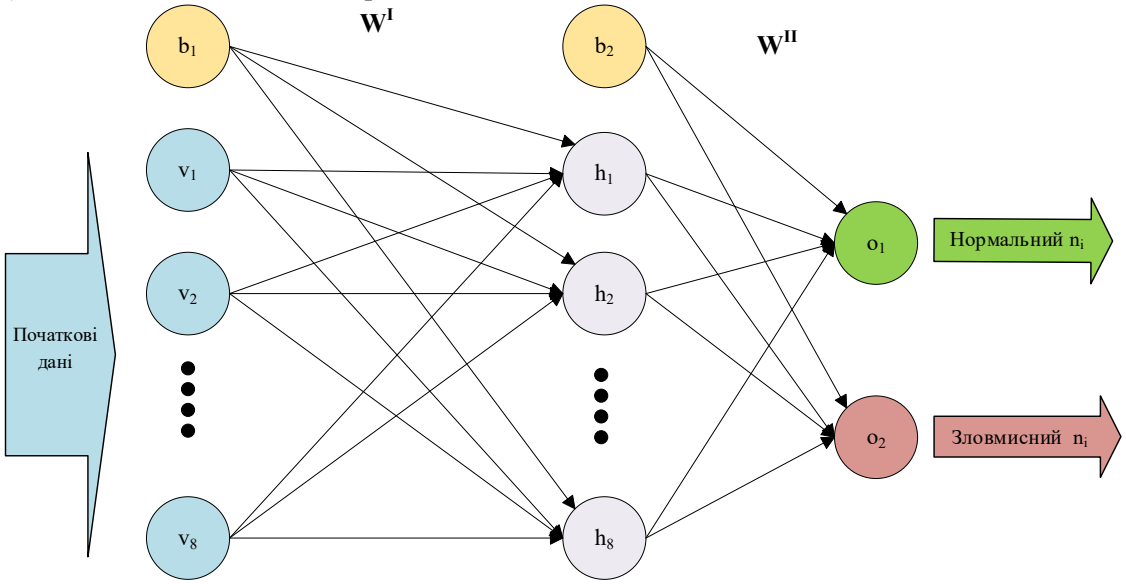
2. Якщо самостійний аналіз не дає змоги впевнено ідентифікувати атаку, ГК використовує класифікатор на основі нейронної мережі, навчений на ознаках типових атак. Вхідними даними для такого модуля є множина метрик вузла, а також агреговані показники інших вузлів. Якщо нейромережа дає змогу підтвердити наявність атаки, ГК діє аналогічно до випадку із досягнення порогу кворуму повідомлення *«РІШЕННЯ»* та ізолює зловмисний вузол T_1 та інформує про це БС.

3. Голова кластера формує пакет із оновленими порогами ($\delta_{pdr_{SF}}, \delta_{pdr_{BH}}, \delta_{rssi_{BH}}$та ін) на основі досвіду поточного раунду і розсилає всім агентам ВВ кластера оновлені правила специфікації через регулярні інтервали.

Таким чином, процедура взаємодії між агентами ВВ, головою кластера та базовою станцією забезпечує не лише енергоефективне та точне виявлення атак, а й динамічне вдосконалення локальних механізмів реагування через колективну експертизу зловмисності вузлів.

Важливою складовою процесу виявлення вторгнень є детектування аномалій з

використанням нейронної мережі. Модуль, що виконує зазначену функцію класифікує повідомлення *«ПЕРЕВІРКА»*, що пересилаються агентами ВВ, як нормальні або аномальні. Кожен ГК постійно навчає свій вбудований класифікатор на основі багатошарової нейронної мережі (БНМ), модель якого наведено на рис. 4.



Вхідний шар Прихований шар Вихідний шар

Рис. 4 – Модель класифікатора на основі нейронної мережі голови кластера

Для детектування аномалій обрано багатошаровий перцептрон (багатошарова нейронна мережа) оскільки має здатність моделювати складні нелінійні взаємозв'язки між ознаками вузлів, зберігаючи при цьому прийнятну обчислювальну складність та одночасно високу точність класифікації (вміння розпізнавати комбінації ознак, недоступні простим алгоритмам), стійкість до "шуму" у даних, швидке навчання, а також гнучкість масштабування архітектури моделі відповідно до наявних ресурсів [23].

Початковими даними для вхідного шару класифікатора на основі нейронної мережі ГК є ідентифікатор, рівень енергії, показники *PDR*, *PFR*, *RSSI*, *DPR* підозрілого сенсорного вузла, а також значення *PDR, RSSI* сусідніх вузлів у кластері. Рівень енергії додають у початкові дані, щоб дати нейронній мережі змогу врахувати багатовимірні (комбіновані) аномалії, зменшити хибні спрацювання та забезпечити кращу гнучкість детектора навіть у випадках, не описаних простими правилами.

Позначимо кількість нейронів БНМ у вхідному, прихованому та вихідному шарах як *n, h* та *o* відповідно. Вхідний і прихований шари складаються з однакової кількості нейронів ($v = h = 8$) [24], тоді як вихідний рівень складається з двох нейронів, що відповідають нормальному та зловмисному станам вузла ($o = 2$). Крім того, вхідний і прихований шари мають спеціальний додатковий нейрон зміщення (біас), для вхідних даних якої встановлено постійне значення +1. Завдяки біасу, нейронна мережа постійно додає до функції активації одиницю та класифікує дані навіть тоді, коли на всі входи нейронів вхідного і прихованого шарів подані нульові значення.

Вхідні дані для h-нейронів прихованого шару визначаються за виразом:

$$y_h = \sum_{v=1}^{8} x_v \, w_{vh}^{\mathrm{I}} + b_1 \qquad (22)$$

де v=(1,.., 8) – порядковий номер нейрона вхідного шару;

h=(1,.., 8) – порядковий номер нейрона прихованого шару;

x_v – початкові дані вхідного шару;

w_{vh} – ваговий коефіцієнт з'єднання між n-м нейроном вхідного шару та h-м нейроном прихованого шару;

b_1 – біас вхідного шару.

Кожен нейрон вхідного шару з'єднаний з усіма нейронами прихованого шару, що мають вбудовану активаційну функцію та перетворюють зважену суму вхідних даних y_h (6) завдяки сігмоїдній функції, що є гладкою та нелінійною, а її значення змінюється у межах від 0 до 1:

$$Y_h = \frac{1}{1+e^{-y_h}} \tag{23}$$

де y_h– зважена сума вхідних значень.

На вхід нейронів вихідного шару надходять пронормоване значення виразу (6) за функцією (7) від кожного нейрону *h* прихованого шару та його біаса.

Вхідні дані для о-нейронів вихідного шару визначаються за виразом:

$$Q_o = \sum_{h=1}^{8} Y_h \, w_{ho}^{\text{II}} + b_2 \tag{24}$$

де *o*=(1,2) – порядковий номер нейрона вихідного шару*;*

Y_h – нормовані дані прихованого шару;

w_{ho} – ваговий коефіцієнт з'єднання між *h*-м нейроном прихованого шару та *o*-м нейроном вихідного шару;

b_2 – біас прихованого шару.

Кожне з'єднання БНМ має пов'язане значення ваги, задане w_{nh}^{I} та w_{ho}^{II} які доцільно представити у вигляді вагових матриць:

$$\text{W}^{\text{I}} = \begin{vmatrix} w_{11}^{\text{I}} & \dots & w_{18}^{\text{I}} \\ \dots & \dots & \dots \\ w_{81}^{\text{I}} & \dots & w_{88}^{\text{I}} \end{vmatrix}, \quad \text{W}^{\text{II}} = \begin{vmatrix} w_{11}^{\text{II}} & \dots & w_{18}^{\text{II}} \\ w_{21}^{\text{II}} & \dots & w_{28}^{\text{II}} \end{vmatrix}. \tag{25}$$

Для навчання класифікатора на основі БНМ та коригування значень W^{I} та W^{II} доцільно використовувати алгоритм зворотного поширення помилки [24].

На рис. 5 наведено алгоритм виявлення вторгнень в безпроводовій сенсорній мережі, що використовує ймовірнісний моніторинг агентами ВВ стану сенсорного вузла на основі рівноваги Неша, правил специфікації комбінування показників сенсорних вузлів та детектування аномальної вузлів на основі багатошарової нейронної мережі.

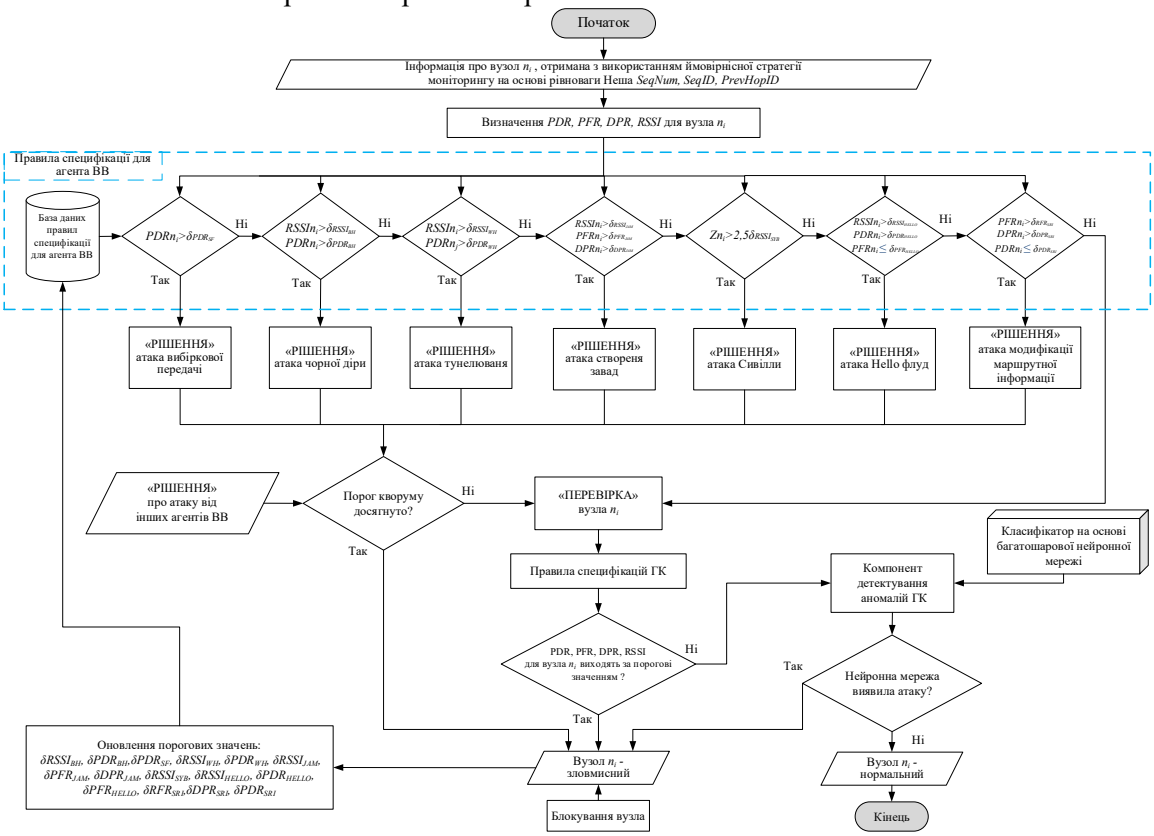


Рис. 5 – Алгоритм виявлення вторгнень беспроводовій сенсорній мережі

Висновки та перспективи подальшого дослідження. Для мінімізації витрат ресурсів і зменшення обсягу мережевого трафіку використано ймовірнісну (стохастичну) стратегію моніторингу, засновану на байєсівській рівновазі Неша. Завдяки цьому агенти ВВ автоматично оптимізують свою поведінку залежно від поточного рівня загроз і власних ресурсів та здатні динамічно змінювати свої стратегії, забезпечуючи гнучкість й адаптивність системи до змін у поведінці зловмисних вузлів.

Оскільки мережеві атаки суттєво впливають на функціонування ієрархічної гетерогенної БСМ, то для агентів ВВ розроблено правила специфікації, які базуються на комбінуванні лише тих показників сенсорних вузлів, що реально впливають на якість передачі інформації. Акцент зроблено на ролі агентів виявлення вторгнень, які пасивно моніторять мережу.

Використання простих статистичних метрик і процедур знижує обчислювальні витрати мережі, а впровадження багатошарової нейронної мережі дає змогу динамічно оновлювати порогові значення показників сенсорних вузлів у базі даних правил специфікацій для агентів ВВ, що забезпечує постійну адаптацію системи до мінливих умов середовища та поведінки мережі.

Поєднання ймовірнісної стратегії моніторингу агентами ВВ стану сенсорного вузла на основі рівноваги Неша, правил специфікації комбінування показників сенсорних вузлів та детектування аномальної вузлів з використанням багатошарової нейронної мережі дало змогу розробити метод виявлення вторгнень у безпроводових сенсорних мережах, який здатний адаптивно відстежувати аномалії та виявляти атаки мережевого рівня, запобігаючи небезпечному впливу зловмисних вузлів завдяки їх блокуванню.

Перспективами подальших досліджень слід вважати розроблення методики управління безпекою безпроводових сенсорних мереж прикладного призначення з використанням функціональної моделі підсистеми безпеки системи управління таких мереж та розробленого у цій статті методу виявлення вторгнення.

Список бібліографічного опису

1 Машталір В., Жук О., Міненко Л., Артюх С. Концептуальні підходи застосування бездротових сенсорних мереж арміями передових країн світу. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2023. Т. 47, № 2. С. 96–112. URL: https://doi.org/10.33099/2311-7249/2023-47-2-96-112 (дата звернення: 06.08.2025).

2. Артюх С., Жук О., Чернега В. Класифікація атак у безпроводових сенсорних мережах тактичної ланки управління військами. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2023. Т. 48, № 3. С. 11–19. URL: https://doi.org/10.33099/2311-7249/2023-48-3-11-19 (дата звернення: 06.08.2025).

3. Zhou L., Chao H.-C. Multimedia traffic security architecture for the internet of things. *IEEE Network*. 2011. Т. 25, № 3. С. 35–40. URL: https://doi.org/10.1109/mnet.2011.5772059 (дата звернення: 08.08.2025).

4. A survey on key management mechanisms for distributed Wireless Sensor Networks / M. A. Simplício та ін. *Computer Networks*. 2010. Т. 54, № 15. С. 2591–2612. URL: https://doi.org/10.1016/j.comnet.2010.04.010 (дата звернення: 08.08.2025).

5. Chen R.-C., Hsieh C.-F., Huang Y.-F. A new method for intrusion detection on hierarchical wireless sensor networks. *the 3rd International Conference*, м. Suwon, Korea, 15–16 січ. 2009 р. New York, New York, USA, 2009. URL: https://doi.org/10.1145/1516241.1516282 (дата звернення: 08.08.2025).

6. Cooperative Intrusion Detection in Wireless Sensor Networks / I. Krontiris та ін. *Lecture Notes in Computer Science*. Berlin, Heidelberg, 2009. С. 263–278. URL: https://doi.org/10.1007/978-3-642-00224-3_17 (дата звернення: 08.08.2025).

7. Decentralized intrusion detection in wireless sensor networks / A. P. R. da Silva та ін. *the 1st ACM international workshop*, м. Montreal, Quebec, Canada, 13 жовт. 2005 р. New York, New York, USA, 2005. URL: https://doi.org/10.1145/1089761.1089765 (дата звернення: 08.08.2025).

8. Quarter Sphere Based Distributed Anomaly Detection in Wireless Sensor Networks / S. Rajasegarar та ін. *2007 IEEE International Conference on Communications*, м. Glasgow, Scotland, 24–28 черв. 2007 р. 2007. URL: https://doi.org/10.1109/icc.2007.637 (дата звернення: 08.08.2025).

9. Bhuse V., Gupta A. Anomaly intrusion detection in wireless sensor networks. *Journal of High Speed Networks*. 2006. Т. 15, № 1. С. 33–51. URL: https://doi.org/10.3233/hsn-2006-276 (дата звернення: 08.08.2025).

10. I. Krontiris, T. Dimitriou and F. C. Freiling, Towards intrusion detection in wireless sensor networks. *In proceedings of the 13th European Wireless Conference*, 2007.

11. Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks / I. Krontiris та ін. *Algorithmic Aspects of Wireless Sensor Networks*. Berlin, Heidelberg. С. 150–161. URL: https://doi.org/10.1007/978-3-540-77871-4_14 (дата звернення: 08.08.2025).

12. A Global Hybrid Intrusion Detection System for Wireless Sensor Networks / Y. Maleh та ін. *Procedia Computer Science*. 2015. Т. 52. С. 1047–1052. URL: https://doi.org/10.1016/j.procs.2015.05.108 (дата звернення: 08.08.2025).

13. Hybrid Intrusion Detection System for enhancing the security of a cluster-based Wireless Sensor Network / K. Q. Yan та ін. *2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT 2010)*, м. Chengdu, China, 9–11 лип. 2010 р. 2010. URL: https://doi.org/10.1109/iccsit.2010.5563886 (дата звернення: 08.08.2025).

14. Estiri M., Khademzadeh A. A game-theoretical model for intrusion detection in wireless sensor networks. *2010 IEEE*

23rd Canadian Conference on Electrical and Computer Engineering - CCECE, м. Calgary, AB, Canada, 2–5 трав. 2010 р. 2010. URL: https://doi.org/10.1109/ccece.2010.5575157 (дата звернення: 08.08.2025).
15. Wahab O. A., Otrok H., Mourad A. A Dempster–Shafer Based Tit-for-Tat Strategy to Regulate the Cooperation in VANET Using QoS-OLSR Protocol. *Wireless Personal Communications*. 2013. Т. 75, № 3. С. 1635–1667. URL: https://doi.org/10.1007/s11277-013-1443-y (дата звернення: 08.08.2025).
16. Subba B., Biswas S., Karmakar S. Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation. *Engineering Science and Technology, an International Journal*. 2016. Т. 19, № 2. С. 782–799. URL: https://doi.org/10.1016/j.jestch.2015.11.001 (дата звернення: 08.08.2025).
17. Algorithmic Game Theory / ред.: N. Nisan та ін. Cambridge : Cambridge University Press, 2007. URL: https://doi.org/10.1017/cbo9780511800481 (дата звернення: 08.08.2025).
18. R. Baskar, P. C. K. Raja, C. Joseph, and M. Reji, "Node attribute behavior based intrusion detection inwireless networks", International Journal of Engineering and Technology, Vol. 5 (5), pp. 3692-3698,(2013)
19. Publish/Subscribe Protocol in Wireless Sensor Networks: Improved Reliability and Timeliness. *KSII Transactions on Internet and Information Systems*. 2018. Т. 12, № 4. URL: https://doi.org/10.3837/tiis.2018.04.008 (дата звернення: 08.08.2025).
20. A Simplified and High Accuracy Algorithm of RSSI-Based Localization Zoning for Children Tracking In-Out the School Buses Using Bluetooth Low Energy Beacon / S. Sakphrom та ін. *Informatics*. 2021. Т. 8, № 4. С. 65. URL: https://doi.org/10.3390/informatics8040065 (дата звернення: 08.08.2025).
21. Sebestyen G., Hangan A. Anomaly detection techniques in cyber-physical systems. *Acta Universitatis Sapientiae, Informatica*. 2017. Т. 9, № 2. С. 101–118. URL: https://doi.org/10.1515/ausi-2017-0007 (дата звернення: 08.08.2025).
22. Yaro A. S., Maly F., Prazak P. Outlier Detection in Time-Series Receive Signal Strength Observation Using Z-Score Method with Sn Scale Estimator for Indoor Localization. *Applied Sciences*. 2023. Т. 13, № 6. С. 3900. URL: https://doi.org/10.3390/app13063900 (дата звернення: 08.08.2025).
23. An Intrusion Detection Using Machine Learning Algorithm Multi-Layer Perceptron (MlP): A Classification Enhancement in Wireless Sensor Network (WSN) / G. V. Reddy та ін. *International Journal on Recent and Innovation Trends in ---Computing and Communication*. 2022. Т. 10, № 2s. С. 139–145. URL: https://doi.org/10.17762/ijritcc.v10i2s.5920 (дата звернення: 08.08.2025).

References

1. Mashtalir V.V., Zhuk O.V., Minenko L.M., Artiukh S.G. Conceptual approaches to the use of wireless sensor networks by the armies of the world's leading countries. Modern Information Technologies in the Sphere of Security and Defence. (2023) (2), p. 96-112.
2. Artiukh S.G, Zhuk O.V., Cherneha V.M. Classification of attacks in wireless sensor networks of the tactical command and control of troops. Modern Information Technologies in the Sphere of Security and Defence. (2023) (3), p. 11-19.
3. Zhou L., Chao H.-C. Multimedia traffic security architecture for the internet of things. *IEEE Network*. 2011. Vol. 25, no. 3. P. 35–40. URL: https://doi.org/10.1109/mnet.2011.5772059 (date of access: 08.08.2025).
4. A survey on key management mechanisms for distributed Wireless Sensor Networks / M. A. Simplício et al. *Computer Networks*. 2010. Vol. 54, no. 15. P. 2591–2612. URL: https://doi.org/10.1016/j.comnet.2010.04.010 (date of access: 08.08.2025).
5. Chen R.-C., Hsieh C.-F., Huang Y.-F. A new method for intrusion detection on hierarchical wireless sensor networks. *the 3rd International Conference*, Suwon, Korea, 15–16 January 2009. New York, New York, USA, 2009. URL: https://doi.org/10.1145/1516241.1516282 (date of access: 08.08.2025).
6. Cooperative Intrusion Detection in Wireless Sensor Networks / I. Krontiris et al. *Lecture Notes in Computer Science*. Berlin, Heidelberg, 2009. P. 263–278. URL: https://doi.org/10.1007/978-3-642-00224-3_17 (date of access: 08.08.2025).
7. Decentralized intrusion detection in wireless sensor networks / A. P. R. da Silva et al. *the 1st ACM international workshop*, Montreal, Quebec, Canada, 13 October 2005. New York, New York, USA, 2005. URL: https://doi.org/10.1145/1089761.1089765 (date of access: 08.08.2025).
8. Quarter Sphere Based Distributed Anomaly Detection in Wireless Sensor Networks / S. Rajasegarar et al. *2007 IEEE International Conference on Communications*, Glasgow, Scotland, 24–28 June 2007. 2007. URL: https://doi.org/10.1109/icc.2007.637 (date of access: 08.08.2025).
9. Bhuse V., Gupta A. Anomaly intrusion detection in wireless sensor networks. *Journal of High Speed Networks*. 2006. Vol. 15, no. 1. P. 33–51. URL: https://doi.org/10.3233/hsn-2006-276 (date of access: 08.08.2025).
10. I. Krontiris, T. Dimitriou and F. C. Freiling, Towards intrusion detection in wireless sensor networks. *In proceedings of the 13th European Wireless Conference*, 2007.
11. Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks / I. Krontiris et al. *Algorithmic Aspects of Wireless Sensor Networks*. Berlin, Heidelberg. P. 150–161. URL: https://doi.org/10.1007/978-3-540-77871-4_14 (date of access: 08.08.2025).
12. A Global Hybrid Intrusion Detection System for Wireless Sensor Networks / Y. Maleh et al. *Procedia Computer Science*. 2015. Vol. 52. P. 1047–1052. URL: https://doi.org/10.1016/j.procs.2015.05.108 (date of access: 08.08.2025).
13. 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: 08.08.2025).
14. Estiri M., Khademzadeh A. A game-theoretical model for intrusion detection in wireless sensor networks. *2010 IEEE 23rd Canadian Conference on Electrical and Computer Engineering - CCECE*, Calgary, AB, Canada, 2–5 May 2010. 2010. URL: https://doi.org/10.1109/ccece.2010.5575157 (date of access: 08.08.2025).
15. Wahab O. A., Otrok H., Mourad A. A Dempster–Shafer Based Tit-for-Tat Strategy to Regulate the Cooperation in VANET Using QoS-OLSR Protocol. *Wireless Personal Communications*. 2013. Vol. 75, no. 3. P. 1635–1667.

URL: https://doi.org/10.1007/s11277-013-1443-y (date of access: 08.08.2025).
16. Subba B., Biswas S., Karmakar S. Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation. *Engineering Science and Technology, an International Journal*. 2016. Vol. 19, no. 2. P. 782–799. URL: https://doi.org/10.1016/j.jestch.2015.11.001 (date of access: 08.08.2025).
17. Algorithmic Game Theory / ed. by N. Nisan et al. Cambridge : Cambridge University Press, 2007. URL: https://doi.org/10.1017/cbo9780511800481 (date of access: 08.08.2025).
18. R. Baskar, P. C. K. Raja, C. Joseph, and M. Reji, "Node attribute behavior based intrusion detection inwireless networks", International Journal of Engineering and Technology, Vol. 5 (5), pp. 3692-3698,(2013)
19. Publish/Subscribe Protocol in Wireless Sensor Networks: Improved Reliability and Timeliness. *KSII Transactions on Internet and Information Systems*. 2018. Vol. 12, no. 4. URL: https://doi.org/10.3837/tiis.2018.04.008 (date of access: 08.08.2025).
20. A Simplified and High Accuracy Algorithm of RSSI-Based Localization Zoning for Children Tracking In-Out the School Buses Using Bluetooth Low Energy Beacon / S. Sakphrom et al. *Informatics*. 2021. Vol. 8, no. 4. P. 65. URL: https://doi.org/10.3390/informatics8040065 (date of access: 08.08.2025).
21. Sebestyen G., Hangan A. Anomaly detection techniques in cyber-physical systems. *Acta Universitatis Sapientiae, Informatica*. 2017. Vol. 9, no. 2. P. 101–118. URL: https://doi.org/10.1515/ausi-2017-0007 (date of access: 08.08.2025).
22. Yaro A. S., Maly F., Prazak P. Outlier Detection in Time-Series Receive Signal Strength Observation Using Z-Score Method with Sn Scale Estimator for Indoor Localization. *Applied Sciences*. 2023. Vol. 13, no. 6. P. 3900. URL: https://doi.org/10.3390/app13063900 (date of access: 08.08.2025).
23. An Intrusion Detection Using Machine Learning Algorithm Multi-Layer Perceptron (MlP): A Classification Enhancement in Wireless Sensor Network (WSN) / G. V. Reddy et al. *International Journal on Recent and Innovation Trends in Computing and Communication*. 2022. Vol. 10, no. 2s. P. 139–145. URL: https://doi.org/10.17762/ijritcc.v10i2s.5920 (date of access: 08.08.2025).