УДК 004.056.55:004.738.5
DOI https://doi.org/10.32782/2663-5941/2025.4.1/12

Сокол Г.В.
Національний технічний університет
«Харківський політехнічний інститут»

Ковда Є.О.
Національний технічний університет
«Харківський політехнічний інститут»

МЕТОД ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНИХ ВУЗЛІВ НА MAC-РІВНІ

У статті розглянуто новий метод виявлення несанкціонованих вузлів у бездротових мережах на рівні управління доступом до середовища (MAC-рівень). Актуальність проблеми зумовлена поширеністю атак типу spoofing, flooding та MAC-імперсонування, які здатні порушити цілісність, конфіденційність та доступність мережевих ресурсів. Запропонований підхід ґрунтується на поведінковому аналізі активності мережевих вузлів із використанням баєсівських моделей та частинкової фільтрації. Метод дозволяє у реальному часі оцінювати ймовірність аномальної поведінки окремого вузла, адаптуватися до змін у мережевому середовищі та формувати профіль типового навантаження для подальшого виявлення відхилень.

Побудована математична модель враховує частоту звернень вузлів до середовища передачі та дозволяє використовувати апостеріорні оцінки для виявлення потенційно небезпечної активності. Особливу увагу приділено оптимізації системи на основі функції втрат, що враховує як хибнопозитивні, так і хибнонегативні спрацювання. Алгоритм передбачає формування гнучкого порогового значення для прийняття рішень, що дозволяє балансувати між чутливістю та точністю.

Імітаційне моделювання, проведене на прикладі 50 вузлів, засвідчило високу ефективність методу: точність класифікації склала 90 %, із незначним відсотком помилок. Метод не вимагає зовнішніх баз знань чи централізованого контролю, що забезпечує його сумісність із обмеженими обчислювальними ресурсами та практичну доцільність у середовищах IoT та Ad-Hoc мережах.

Таким чином, запропонований підхід демонструє високу надійність у виявленні несанкціонованих вузлів, гнучкість до змін мережевої топології та можливість інтеграції в існуючі бездротові протоколи зв'язку.

Ключові слова: *бездротові мережі, MAC-рівень, несанкціонований доступ, аномалії мережевої активності, баєсівське моделювання, частинкова фільтрація, поведінковий аналіз, виявлення вузлів, інтернет речей, система виявлення вторгнень.*

Постановка проблеми. У сучасних бездротових телекомунікаційних мережах рівень управління доступом до середовища (MAC-рівень) залишається одним із найбільш вразливих до зловмисних впливів. Атаки типу spoofing, flooding та MAC-імперсонування здатні серйозно порушити нормальне функціонування мережі, створити загрозу конфіденційності, цілісності та доступності інформації, а також знизити загальну продуктивність системи. Особливо небезпечною є поява несанкціонованих вузлів, які маскуються під легітимних користувачів і можуть непомітно здійснювати небажані або шкідливі дії.

У цьому контексті актуальним є завдання розробки методів виявлення таких вузлів на основі аналізу їхньої поведінки. Одним із перспективних підходів є використання математичних моделей, які дозволяють виявляти відхилення від типового профілю активності у межах MAC-рівня. У даній роботі запропоновано метод виявлення аномалій, що базується на поєднанні баєсівських моделей для оцінки ймовірності активності вузлів із методами стохастичної фільтрації, які забезпечують адаптивне оновлення оцінок у режимі реального часу. Такий підхід дозволяє реалізувати ефективну систему контролю безпеки, здатну виявляти

потенційно небезпечні вузли навіть за відсутності додаткових криптографічних механізмів або централізованого моніторингу.

Останні дослідження у сфері інформаційної безпеки показують зростаючий інтерес до поведінкових методів виявлення аномалій, які ґрунтуються на статистичному аналізі активності вузлів. Серед таких підходів особливої уваги заслуговують байєсівські моделі, що забезпечують гнучке представлення невизначеностей і дозволяють адаптуватися до нових умов на основі накопичених даних. У поєднанні з алгоритмами фільтрації, ці методи створюють передумови для побудови ефективних систем виявлення несанкціонованих дій без потреби у зовнішніх джерелах знань або централізованих базах шаблонів атак.

Аналіз останніх досліджень і публікацій. У сучасних дослідженнях, присвячених виявленню несанкціонованих вузлів у бездротових мережах, активно розробляються різноманітні підходи з використанням засобів машинного навчання, статистичного аналізу, фільтрації та штучного інтелекту.

Застосування глибоких нейронних мереж для виявлення атак у бездротових сенсорних мережах демонструє високу точність класифікації та здатність до узагальнення нових типів аномалій [1]. Проте такі методи потребують великих обсягів навчальних даних і значних обчислювальних ресурсів, що ускладнює їх впровадження у пристрої з обмеженою енергією.

Алгоритми машинного навчання, зокрема дерева рішень, метод опорних векторів і випадкові ліси, активно застосовуються для класифікації мережевого трафіку та аномалій [2]. Їхньою перевагою є висока швидкодія та гнучкість, однак результати сильно залежать від якості вибору ознак.

Наївні баєсівські класифікатори також використовуються для виявлення несанкціонованих вузлів завдяки своїй простоті та здатності працювати в режимі реального часу [3]. Їх головним обмеженням є припущення незалежності між ознаками, що не завжди справджується в реальних мережах.

Байєсівські мережі в поєднанні з фільтраційними методами, такими як частинковий фільтр або фільтр Калмана, дозволяють точно оцінювати поведінкові параметри вузлів на основі історичних та поточних спостережень [4]. Ці методи забезпечують адаптивність до змін, але вимагають точного математичного налаштування.

Методи цифрової обробки сигналів застосовуються для ідентифікації несанкціонованих передавачів за фізичними характеристиками сигналу [5]. Такі рішення добре підходять для низькорівневого контролю, але чутливі до шумів і варіацій середовища.

Алгоритми кластеризації, наприклад, k-means або DBSCAN, використовуються для виявлення груп вузлів, які демонструють відхилену поведінку [6]. Вони дозволяють виявляти аномалії без потреби мати навчальні зразки, однак їх ефективність залежить від гіперпараметрів та вибору відстаней.

Рекурентні нейронні мережі застосовуються для аналізу послідовностей активності вузлів у часі, дозволяючи виявляти довготривалі залежності [7]. Основним обмеженням є складність та ресурсоємність навчання.

Методи підкріплювального навчання дозволяють системам з досвідом вдосконалювати стратегії виявлення шляхом самонавчання на основі нагород і штрафів [8]. Цей підхід є перспективним, однак потребує великої кількості ітерацій для досягнення прийнятного рівня продуктивності.

Інтеграція статистичних методів із класичними алгоритмами машинного навчання забезпечує компроміс між інтерпретованістю та ефективністю виявлення [9]. Такі моделі краще піддаються аналізу, однак не завжди досягають точності глибокого навчання.

Гібридні підходи, які поєднують сигнатурний аналіз та виявлення аномалій, дозволяють водночас виявляти відомі атаки та адаптуватися до нових загроз [10]. Їх головним недоліком є висока складність реалізації та інтеграції різних модулів.

У роботі [11] досліджено методи виявлення вторгнень у бездротових сенсорних мережах. Автори запропонували розподілену систему виявлення (DIDS), яка використовує характеристики мережевої активності (мощність сигналу, аномалії в буфері приймача, сліди пакетів тощо) для фіксації атак типу flooding і spoofing. Модель перевірено у симуляторі OPNET, що показало високу ефективність протидії DoS-атакам. Перевагою є динамічна адаптація до змін мережевого середовища, однак реалізація вимагає глибокого доступу до параметрів обладнання.

У публікації [12] розглянуто загальні принципи побудови превентивних і реактивних систем безпеки для традиційних та Ad-Hoc мереж. У роботі ідентифіковано вразливості на рівні багатокрокової маршрутизації, наведено класифікацію атак, запропоновано підходи до побудови систем раннього виявлення. Основна перевага – міжмережевий підхід, недолік – відсутність формальної моделі виявлення.

У статті [13] зроблено акцент на сучасних методах аутентифікації в бездротових мережах. Проаналізовано математичні та метрологічні основи надійності засобів ідентифікації, їх вплив на загальну безвідмовність телекомунікаційної системи. Робота цінна з погляду нормативної точності, але не орієнтована на динамічні мережі чи мобільні вузли.

Загалом, аналіз опрацьованих джерел свідчить про різноманіття підходів до виявлення несанкціонованих вузлів, що базуються як на класичних статистичних методах, так і на сучасних технологіях штучного інтелекту, з перспективами подальшої інтеграції в реальні мережеві системи.

Постановка завдання. Метою даної роботи є розробка і дослідження методу виявлення несанкціонованих вузлів у бездротових мережах на основі аналізу динаміки активності на MAC-рівні. Основна увага зосереджена на побудові математичної моделі, що дозволяє формувати поведінковий профіль кожного вузла, оцінювати ступінь відхилення поточної поведінки від очікуваної та виявляти аномалії із заданою чутливістю. Для реалізації поставленої мети у роботі використано баєсівський підхід до моделювання активності, методи частинкової фільтрації для онлайн-оцінювання параметрів, а також формалізовано критерії ухвалення рішень у вигляді функції втрат із ваговими коефіцієнтами для контролю хибних спрацювань.

Виклад основного матеріалу. *Математична модель поведінки вузлів.*

Для виявлення несанкціонованої або аномальної активності на рівні MAC необхідно побудувати математичну модель нормальної поведінки вузлів у мережі. Така модель має враховувати, як часто кожен вузол звертається до середовища передачі даних, тобто ініціює доступ або здійснює передачу інформації.

Для формалізації активності вузлів введемо наступні позначення. Нехай N – загальна кількість вузлів у мережі. Тоді $x_i(t)$ – показник активності вузла i у момент часу t, де: $x_i(t)=1$, якщо вузол передає або намагається передати дані, $x_i(t)=0$, якщо вузол неактивний у цей момент. У свою чергу вектор стану мережі у момент часу t, який описує активність усіх вузлів мережі, має вигляд

$$X(t)=\left[x_1(t),x_2(t),\ldots,x_t(t)\right]. \qquad (1)$$

Для моделювання ймовірнісної поведінки окремого вузла використовується біноміальна модель, що є окремим випадком баєсівської мережі. Вона дозволяє описати, з якою ймовірністю вузол буде активним у певний момент часу. Така модель виглядає наступним чином:

$$P\left(x_i(t)\theta_i\right)=\theta_i^{x_i(t)}\left(1-\theta_i\right)^{1-x_i(t)}, \qquad (2)$$

де: $\theta_i\in[0,1]$ – параметр, який описує ймовірність того, що вузол i буде активним у довільний момент часу, $x_i(t)$ – фактичний стан активності вузла у час t.

Сутність наведеної формули (2) полягає в тому, що якщо $x_i(t)=1$, тобто вузол у даний момент часу є активним, то ймовірність цієї події дорівнює θ_i. Натомість, якщо $x_i(t)=0$, тобто вузол не проявляє жодної активності, ймовірність такої події становить $1-\theta_i$. Таким чином, поведінку кожного вузла можна повністю охарактеризувати одним параметром θ_i, який описує середню частоту його активності у мережі.

Оскільки параметр θ_i зазвичай невідомий наперед, його можна оцінити на основі зібраної історії спостережень за певний проміжок часу T. Для цього застосовується метод максимальної правдоподібності (Maximum Likelihood Estimation):

$$\hat{\theta}_i=\frac{1}{T}\sum_{t=1}^{T}x_i(t). \qquad (3)$$

Іншими словами, $\hat{\theta}_i$ – це середня частота активності вузла i протягом останніх T моментів часу. Такий підхід дозволяє сформувати профіль «нормальної» поведінки кожного вузла на основі реального трафіку, що спостерігається в мережі.

Таким чином було сформульовано основу для подальшого аналізу аномалій: якщо поведінка вузла починає суттєво відрізнятися від оціненого параметра $\hat{\theta}_i$, це може вказувати на спробу несанкціонованого доступу або атаку на MAC-рівні.

Аномалія як відхилення від апостеріорної ймовірності.

Одним із ключових етапів у процесі виявлення несанкціонованих або аномальних вузлів є аналіз їхньої поведінки в динаміці, зокрема оцінка того, наскільки поточна активність відхиляється від типового профілю. Для цього використовується баєсівський підхід, що дозволяє уточнювати ймовірність активності вузла з урахуванням нових спостережень.

Апостеріорна ймовірність параметра активності θ_i при наявній історії спостережень за вузлом $x_i^{1:t}$ обчислюється за формулою:

$$P\left(\theta_i|x_i^{1:t}\right)=\frac{P\left(x_i^{1:t}|\theta_i\right)\cdot P\left(\theta_i\right)}{P\left(x_i^{1:t}\right)}. \quad (4)$$

У цій формулі $x_i^{1:t}$ позначає послідовність значень активності вузла i від початкового моменту часу до моменту t, $P\left(\theta_i\right)$ – апріорне припущення про параметр активності, а $P\left(x_i^{1:t}|\theta_i\right)$ – ймовірність отриманої історії за умови фіксованого значення параметра θ_i. Знаменник $P\left(x_i^{1:t}\right)$ виконує роль нормалізаційної константи, що гарантує коректність результату з точки зору ймовірнісного простору.

Аномальна поведінка вузла визначається як суттєве відхилення його апостеріорної оцінки $P\left(\theta_i|x_i^{1:t}\right)$ від усередненої оцінки $\hat{\theta}_i$, яка була отримана на основі історичних спостережень. У випадку, коли модуль різниці між цими двома оцінками перевищує певне граничне значення ε, тобто:

$$\left|P\left(\theta_i|x_i^{1:t}\right)-\hat{\theta}_i\right|>\varepsilon, \quad (5)$$

вузол вважається підозрілим і таким, що потенційно демонструє аномальну або несанкціоновану активність. Цей підхід дозволяє формально і кількісно виявляти відхилення від очікуваної поведінки, не потребуючи жорстких правил або порогів, які могли б бути неефективними у змінних умовах мережі.

Модель фільтрації.

Для забезпечення високої точності оцінювання динамічної активності вузлів у реальному часі доцільно використовувати стохастичні методи фільтрації. У рамках цієї роботи запропоновано застосування алгоритму частинкової фільтрації (англ. Particle Filter), який є ефективним інструментом для наближеної баєсівської оцінки у випадках, коли аналітичне обчислення апостеріорної ймовірності є складним або неможливим.

Суть частинкової фільтрації полягає в апраксимації функції розподілу ймовірностей за допомогою скінченої множини випадкових зразків, або так званих частинок. Кожна частинка представляє можливе значення оцінюваного параметра – у нашому випадку це параметр активності вузла $\theta_i(t)$. Для початку роботи алгоритму виконується ініціалізація множини частинок: випадковим чином генеруються M значень $\theta_i^{(1)},\theta_i^{(2)},\ldots,\theta_i^{(M)}$, які задають початкову апроксимацію розподілу.

Далі, для кожної частинки обчислюється вага, яка відображає правдоподібність поточного спостереження $x_i(t)$, за умови, що істинним є відповідне значення параметра активності. Ваги оновлюються рекурсивно, з урахуванням попередньої ваги та ймовірності нового спостереження. Формально, оновлення ваги $w_i^{(j)}(t)$ для j-тої частинки на момент часу t описується виразом:

$$w_i^{(j)}(t)\propto P\left(x_i(t)|\theta_i^{(j)}(t-1)\right)\cdot w_i^{(j)}(t-1). \quad (6)$$

Цей підхід дозволяє адаптувати оцінювання параметра в режимі онлайн, оскільки з кожним новим спостереженням вага частинок перераховується відповідно до актуального стану вузла.

На основі оновлених ваг обчислюється поточна оцінка параметра активності $\hat{\theta}_i(t)$ як зважене середнє всіх частинок:

$$\hat{\theta}_i(t)=\sum_{j=1}^{M}w_i^{(j)}(t)\cdot\theta_i^{(j)}(t). \quad (7)$$

Це значення є найкращою доступною апроксимацією істинного параметра активності вузла з урахуванням усієї наявної інформації до моменту часу t.

Однак із часом розподіл ваг може ставати надто «розмитим» – більшість ваг стають близькими до нуля, тоді як кілька частинок мають непропорційно високі значення. Такий ефект називається дегенерацією вибірки й істотно знижує ефективність фільтрації. Для подолання цієї проблеми застосовується процедура ресемплінгу, під час якої виконується перегенерація множини частинок відповідно до їхніх ваг. У результаті отримується нова вибірка, яка краще відображає поточний розподіл ймовірностей і дозволяє зберегти точність оцінювання в подальшому.

Таким чином, частинковий фільтр забезпечує гнучку та адаптивну модель оцінки динамічного параметра активності вузла, що є ключовим для вчасного виявлення аномальних змін у поведінці, характерних для несанкціонованого доступу на MAC-рівні.

Функція втрат і оптимізації.

Побудова ефективної системи виявлення несанкціонованих вузлів на MAC-рівні неможлива без чіткої математичної постановки задачі оптимізації. Основною метою є мінімізація загальної кількості помилкових рішень, які система може прийняти під час класифікації вузлів як нормальних або аномальних. У даному контексті враховуються два основні типи помилок: хибнопозитивні спрацювання (False Positives, FP), коли нормальний вузол помилково розпізнається як загрозливий, та хибнонегативні спрацювання (False Negatives, FN), коли аномальний або несанкціонований вузол залишається непоміченим.

Для кількісної оцінки загальних втрат у системі введено функцію втрат (loss function), яка дозволяє формалізувати компроміс між двома типами помилок. Функція має вигляд:

$$L = \alpha \cdot FP + \beta \cdot FN, \quad (8)$$

де параметри α та β є ваговими коефіцієнтами, що відображають відносну важливість кожного типу помилки. Наприклад, якщо в конкретному середовищі більш критичними є хибнонегативні рішення, які дозволяють атакуючим вузлам залишатися в мережі, то значення β має бути вищим за α. У випадках, коли хибнопозитивні рішення можуть призвести до зайвого виключення коректних пристроїв, перевага надається більшому значенню α.

Оптимізація системи виявлення аномалій полягає у виборі такого порогового значення μ, яке мінімізує значення функції втрат L. Тобто, необхідно знайти оптимальний компроміс між чутливістю та специфічністю системи. Залежно від складності моделі та характеру вхідних даних, для розв'язання цієї задачі можуть бути використані різні методи оптимізації, зокрема градієнтні методи, які дозволяють знаходити екстремуми диференційованих функцій, або байєсівська оптимізація, яка ефективна у випадках, коли функція втрат є неявною, нелінійною або має шум.

Таким чином, запропонований підхід до формалізації критеріїв якості виявлення дозволяє адаптувати систему до конкретних вимог користувача або середовища, забезпечуючи збалансовану роботу між точністю та надійністю.

Метод виявлення несанкціонованого вузла.

Побудований у роботі математичний апарат дозволяє сформулювати практичний метод (рис. 1), який може бути реалізований у системах моніторингу та керування доступом на рівні MAC. Його призначення – виявляти вузли, чия поведінка суттєво відхиляється від очікуваної, і тим самим ідентифікувати потенційно несанкціоновані або шкідливі пристрої.

На першому етапі для кожного вузла в мережі ініціалізується індивідуальна байєсівська модель, яка враховує історію його активності та дозволяє сформувати початкову оцінку параметра ймовірності доступу до середовища – $\hat{\theta}_i$. Надалі, у процесі функціонування мережі, для кожного вузла в реальному часі обчислюється актуальне значення оціненого параметра активності $\theta_i(t)$, використовуючи метод частинкової фільтрації або інший відповідний інструмент.

Ключовим кроком у процесі виявлення є порівняння оцінки $\theta_i(t)$, з історичним середнім значенням $\hat{\theta}_i$.

$$D_i(t) = \left| P\left(\theta_i | x_i^{1:t}\right) - \hat{\theta}_i \right|. \quad (9)$$

Якщо величина $D_i(t)$ перевищує заздалегідь визначений поріг μ, вважається, що вузол демонструє аномальну активність, яка не відповідає його типовому профілю. У такому випадку фіксується інцидент потенційного порушення правил доступу до середовища.

З метою уникнення реакцій на поодинокі флуктуації або тимчасові збурення, алгоритм реалізує принцип накопичення підозрілих відхилень. Якщо відхилення $D_i(t) > \mu$ спостерігається у вузла багаторазово або із заданою частотою протягом контрольного інтервалу, такий вузол заноситься до умовного «чорного списку» як підозрюваний

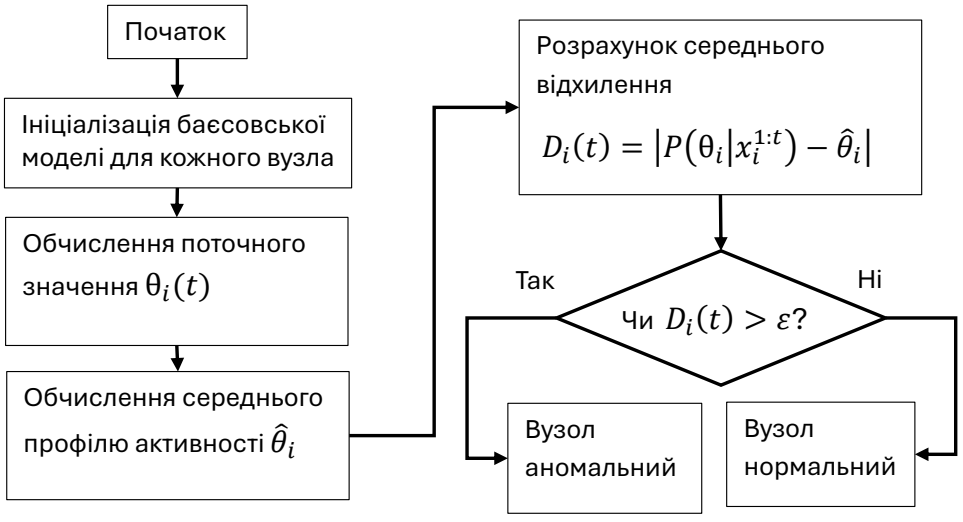

Рис. 1. Метод виявлення аномальних вузлів

у несанкціонованій поведінці. Надалі можлива ізоляція цього вузла, обмеження його доступу або подальше аналізування адміністраторами мережі.

Таким чином, запропонований алгоритм забезпечує не лише чутливе виявлення аномалій, а й враховує стійкість до хибнопозитивних реакцій завдяки механізму адаптивного порівняння і накопичення подій.

Експериментальні результати.

Для перевірки ефективності запропонованого методу виявлення несанкціонованих вузлів на рівні MAC було проведено імітаційний експеримент у середовищі, що моделює роботу бездротової мережі з 50 вузлами. У моделі передбачалося, що частина вузлів веде себе нормально, дотримуючись типової активності, у той час як деякі вузли імітують зловмисну поведінку через надмірну частоту доступу до середовища.

У рамках експериментального моделювання була розглянута мережа, яка складалася з 50 вузлів. Із загальної кількості пристроїв 10 % (тобто 5 вузлів) були змодельовані як атакуючі (таблиця 1). Їх поведінка характеризувалася високою частотою спроб доступу до середовища передачі – ймовірність активності таких вузлів варіювалася в межах від 0.7 до 0.9. Решта 90 % вузлів (45 пристроїв) демонстрували нормальну мережеву поведінку, для якої характерна значно нижча інтенсивність взаємодії – ймовірність активності знаходилась у діапазоні від 0.1 до 0.3.

Тривалість спостереження за кожним вузлом становила 100 часових інтервалів, що дозволило сформувати як історичні, так і поточні профілі активності. Для виявлення аномалій використовувалося поточне значення оціненого параметра активності $\theta_i(t)$, обчислене як середнє за останні 10 моментів часу. Критерій фіксації відхилення від нормальної поведінки був реалізований у вигляді порогової умови: якщо абсолютне відхилення поточного значення від історичного профілю перевищувало граничне значення $\mu = 0.25$, то така поведінка вважалася підозрілою.

У процесі моделювання для кожного вузла було проведено оцінку ключових параметрів, необхідних для подальшого аналізу його поведінки. Зокрема, розраховувалося середнє значення активності $\hat{\theta}_i$, яке характеризує загальну частоту звернень вузла до середовища доступу

Таблиця.1

Оцінка активності та класифікація вузлів

Вузол	Тип	θ̂	θ(t)	Виявлено як	Вузол	Тип	θ̂	θ(t)	Виявлено як
1	Атакуючий	0,84	0,9	Нормальний	**26**	Нормальний	0,21	0,2	Нормальний
2	Атакуючий	0,76	0,3	Аномальний	**27**	Нормальний	0,1	0	Нормальний
3	Атакуючий	0,85	1	Нормальний	**28**	Нормальний	0,21	0,2	Нормальний
4	Атакуючий	0,77	0,6	Нормальний	**29**	Нормальний	0,17	0,1	Нормальний
5	Атакуючий	0,65	0,8	Нормальний	**30**	Нормальний	0,18	0,1	Нормальний
6	Нормальний	0,12	0,1	Нормальний	**31**	Нормальний	0,21	0,3	Нормальний
7	Нормальний	0,26	0,3	Нормальний	**32**	Нормальний	0,1	0,1	Нормальний
8	Нормальний	0,25	0,2	Нормальний	**33**	Нормальний	0,17	0,1	Нормальний
9	Нормальний	0,19	0,3	Нормальний	**34**	Нормальний	0,25	0,3	Нормальний
10	Нормальний	0,14	0,2	Нормальний	**35**	Нормальний	0,1	0	Нормальний
11	Нормальний	0,19	0,1	Нормальний	**36**	Нормальний	0,21	0,2	Нормальний
12	Нормальний	0,13	0,1	Нормальний	**37**	Нормальний	0,13	0,2	Нормальний
13	Нормальний	0,22	0,4	Нормальний	**38**	Нормальний	0,12	0,1	Нормальний
14	Нормальний	0,24	0,4	Нормальний	**39**	Нормальний	0,27	0,2	Нормальний
15	Нормальний	0,21	0,2	Нормальний	**40**	Нормальний	0,27	0,2	Нормальний
16	Нормальний	0,09	0	Нормальний	**41**	Нормальний	0,23	0,3	Нормальний
17	Нормальний	0,27	0,4	Нормальний	**42**	Нормальний	0,12	0,2	Нормальний
18	Нормальний	0,28	0,2	Нормальний	**43**	Нормальний	0,12	0	Нормальний
19	Нормальний	0,1	0	Нормальний	**44**	Нормальний	0,19	0,4	Нормальний
20	Нормальний	0,12	0	Нормальний	**45**	Нормальний	0,12	0	Нормальний
21	Нормальний	0,16	0	Нормальний	**46**	Нормальний	0,15	0,1	Нормальний
22	Нормальний	0,18	0,2	Нормальний	**47**	Нормальний	0,2	0,2	Нормальний
23	Нормальний	0,15	0,1	Нормальний	**48**	Нормальний	0,12	0,3	Нормальний
24	Нормальний	0,17	0,1	Нормальний	**49**	Нормальний	0,32	0,6	Аномальний
25	Нормальний	0,21	0,1	Нормальний	**50**	Нормальний	0,13	0	Нормальний

Рис. 2. Порівняння середніх і поточних значень активності вузлів з порогом виявлення

протягом усього періоду спостереження. Одночасно із цим визначалося поточне значення параметра активності $\theta_i(t)$, обчислене як середнє за останні десять часових інтервалів. Це дозволяло виявляти короткотривалі, але значущі відхилення у поведінці вузлів.

Для кожного вузла також обчислювалося абсолютне відхилення $D_i(t) = \left| P\left(\theta_i | x_i^{1:t}\right) - \hat{\theta}_i \right|$, яке слугувало індикатором аномальності. Якщо значення цього відхилення перевищувало заздалегідь визначене порогове значення μ, поведінка вузла вважалася підозрілою.

Таким чином, механізм прийняття рішення базувався на оцінці динамічної узгодженості між поточним та історичним профілем активності кожного вузла.

Згідно з результатами експерименту, запропонований підхід продемонстрував високу ефективність. Загальна точність класифікації склала 90.0 %, що підтверджує здатність моделі до надійного розмежування нормальної та аномальної поведінки. Частка хибнопозитивних спрацювань становила 2.0 %: у цих випадках нормальні вузли були помилково ідентифіковані як аномальні. У той самий час частка хибнонегативних спрацювань склала 8.0 %, тобто деякі атакуючі вузли не були виявлені системою.

На рисунку нижче подано графік порівняння оцінених середніх значень активності вузлів $\hat{\theta}_i$ та їх поточних значень $\theta_i(t)$. Червона пунктирна лінія позначає порогове значення ε, що використовувалося для фіксації аномалії.

Отримані результати свідчать про збалансованість методу, який забезпечує високу точність при помірному рівні помилкових рішень. Завдяки адаптивному механізму оцінювання активності, система демонструє хорошу чутливість до відхилень і водночас зберігає стійкість до випадкових флуктуацій у поведінці нормальних вузлів.

Наведені дані підтверджують, що метод виявлення на основі баєсівської моделі та оцінки активності дозволяє ефективно ідентифікувати зловмисну поведінку в мережі.

Висновки. У результаті проведеного дослідження було розроблено ефективний метод виявлення несанкціонованих вузлів на MAC-рівні, який ґрунтується на аналізі відхилень у поведінці пристроїв без необхідності використання додаткового апаратного забезпечення. Запропонований підхід поєднує у собі баєсівське моделювання й адаптивну фільтрацію, що дозволяє здійснювати динамічну оцінку параметрів активності кожного вузла в реальному часі.

Гнучкість методу забезпечується завдяки здатності до самонавчання на основі історичних даних та оновлення оцінок при зміні мережевого середовища. Це робить запропоновану модель особливо корисною в умовах нестабільного трафіку або змінної топології. Крім того, обрані алгоритмічні рішення дозволяють забезпечити сумісність з широким спектром існуючих протоколів канального рівня, таких як IEEE 802.11 або IEEE 802.15.4, що відкриває можливості для практичного впровадження у бездротові мережі різного призначення – від локальних IoT-систем до великих корпоративних інфраструктур.

Таким чином, метод демонструє як високу ефективність виявлення, так і практичну доцільність у сучасних телекомунікаційних системах з обмеженими ресурсами.

Список літератури:

1. Imrana Y., Xiang Y., Ali L., Abdul Rauf Z. A bidirectional LSTM deep learning approach for intrusion detection. Expert Systems with Applications. 2021. Vol. 185. Art. 115524. DOI: 10.1016/j.eswa.2021.115524
2. Aly M., Behiry M.H. Enhancing anomaly detection in IoT-driven factories using Logistic Boosting, Random Forest, and SVM: A comparative machine learning approach. *Scientific Reports.* 2025. Vol. 15. Art. 23694. DOI: 10.1038/s41598-025-08436-x
3. Phatcharathada B., Srisuradetchai P. Randomized Feature and Bootstrapped Naive Bayes Classification. *Applied System Innovation.* 2025. Vol. 8, No. 4, Article 94. DOI: 10.3390/asi8040094
4. Ahmad R., Alkhammash E.H. Online adaptive Kalman filtering for real-time anomaly detection in wireless sensor networks. *Sensors.* 2024. Vol. 24, no. 15: 5046. DOI: 10.3390/s24155046
5. Peng D., Xie K., Liu M. Application of Gray Wolf Particle Filter algorithm based on golden section in wireless sensor network mobile target tracking. *Electronics.* 2024. Vol. 13, no. 13: 2440. DOI: 10.3390/electronics13132440
6. Retiti Diop Emane C, Song S, Lee H, Choi D, Lim J, Bok K, Yoo J. Anomaly Detection Based on GCNs and DBSCAN in a Large-Scale Graph. *Electronics.* 2024. 13(13):2625. DOI: 10.3390/electronics13132625
7. Almomani I., Al Kasasbeh B., Al Akhras M. WSN DS: a dataset for intrusion detection systems in wireless sensor networks. Sensors. 2016. Vol. 2016. No. 1. Art. 4731953. DOI: 10.1155/2016/4731953
8. Gueriani A., Kheddar H., Mazari A. C. Deep reinforcement learning for intrusion detection in IoT: a survey. ArXiv preprint. 2024. Art. arXiv:2405.20038. DOI: 10.48550/arXiv.2405.20038
9. Mathonsi T., van Zyl T.L. Statistics and deep learning-based hybrid model for interpretable anomaly detection. *Neural Comput. Appl.* 2022. Vol. 37. P. 707-721. DOI: 10.1007/s00521-021-06697-x
10. Mohite R., Ouarbya L. Interpretable anomaly detection: a hybrid approach using rule-based and machine learning techniques. *Proc. IEEE I2CT.* Pune, India, 2024, pp. 1-10, doi: 10.1109/I2CT61223.2024.10543396.
11. Mahjabin T., Xiao Y., Sun G., Jiang W. A survey of distributed denial of service attacks, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks. 2017. Vol. 13. No. 12. Art. 1550147717741463. DOI: 10.1177/1550147717741463
12. Alansari Z., Anuar N. B., Kamsin A., Belgaum M. R. A systematic review of routing attacks detection in wireless sensor networks. PeerJ Computer Science. 2022. Vol. 8. Art. e1135. DOI: 10.7717/peerj-cs.1135
13. Kwon D. K., Yu S. J., Lee J. Y., Son S. H., Park Y. H. WSN SLAP: secure and lightweight mutual authentication protocol for wireless sensor networks. Sensors. 2021. Vol. 21. No. 3. Art. 936. DOI: 10.3390/s21030936

Sokol H.V., Kovda Ye.O. METHOD FOR DETECTION OF UNAUTHORIZED NODES AT THE MAS LEVEL

The article discusses a new method for detecting unauthorized nodes in wireless networks at the media access control (MAC) level. The relevance of the problem is due to the prevalence of attacks such as spoofing, flooding and MAC impersonation, which can violate the integrity, confidentiality and availability of network resources. The proposed approach is based on behavioral analysis of network node activity using Bayesian models and particle filtering. The method allows for real-time assessment of the probability of anomalous behavior of an individual node, adaptation to changes in the network environment and formation of a typical load profile for further detection of deviations. The constructed mathematical model takes into account the frequency of node access to the transmission medium and allows the use of a posteriori estimates to detect potentially dangerous activity. Special attention is paid to system optimization based on a loss function that takes into account both false positive and false negative responses. The algorithm involves the formation of a flexible threshold value for decision-making, which allows balancing between sensitivity and accuracy.

Simulation modeling, conducted on the example of 50 nodes, demonstrated the high efficiency of the method: the classification accuracy was 90%, with a small percentage of errors. The method does not require external knowledge bases or centralized control, which ensures its compatibility with limited computing resources and practical feasibility in IoT and Ad-Hoc network environments.

Thus, the proposed approach demonstrates high reliability in detecting unauthorized nodes, flexibility to changes in network topology and the possibility of integration into existing wireless communication protocols.

Key words: *wireless networks, MAC layer, unauthorized access, network activity anomalies, Bayesian modeling, particle filtering, behavioral analysis, node detection, Internet of Things, intrusion detection system.*

Дата надходження статті: 22.07.2025
Дата прийняття статті: 31.07.2025
Опубліковано: 27.10.2025