БЕЗПЕКА WI-FI МЕРЕЖ З ВИКОРИСТАННЯМ ЕЛЕМЕНТІВ НЕЧІТКОЇ ЛОГІКИ

Василенко Т.О., Завгородній Я.О.

Кафедра комп'ютерної радіоінженерії та систем технічного захисту інформації,
Харківський національний університет радіоелектроніки,
Україна

E-mail: tetiana.vasylenko@nure.ua
yaroslav.zavhorodnii@nure.ua

Abstract

The paper provides a description of the algorithm for the operation of an intrusion detection system in a Wi-Fi network using fuzzy logic. This algorithm makes it possible to make decisions about the presence of a potential security threat while taking into account various or rapidly changing conditions that traditional intrusion detection systems do not consider. Parameters such as current operating conditions, signal strength, number of failed authentications, level of anomalous traffic, number of connected clients, signal strength variance, and frequency of probe requests can be analyzed. The proposed algorithm for analyzing the state of a Wi-Fi network based on fuzzy logic enables more adequate decision-making regarding network anomalies. The use of fuzzy logic allows decisions to be adjusted depending on changes in the network's operating conditions. The system can operate either in automatic mode (making decisions autonomously) or with the assistance of an operator (an expert who, after analyzing the obtained results, makes decisions manually depending on the situation).

Наразі бездротові мережі є надзвичайно актуальними та відіграють важливу роль у житті людей. Багато компаній успішно застосовують бездротові локальні мережі для керування виробничими процесами, лікарні розгортають бездротові мережі з метою підвищення ефективності роботи та зручності. Базовим стандартом для бездротових локальних мереж є IEEE 802.11, різні версії якого регламентують передавання даних у діапазонах 2,4 і 5 ГГц, що детальніше розглянуто в [1, 2]. Дальність зв'язку, як правило, не перевищує 200 м.

Оскільки пристрої стандарту 802.11 обмінюються даними через радіоефір, будь-яка інша станція, що використовує цей діапазон, також може приймати ці дані. Для забезпечення хоча б мінімального рівня безпеки бездротової мережі застосовують механізми шифрування, засновані на алгоритмах WPA та WPA2 (Wi-Fi Protected Access) [3], а також системи виявлення вторгнень IDS [3].

Стандартні методи забезпечення безпеки, що базуються на чітких правилах і в більшості націлені на технології провідних мереж виявляються недостатньо ефективними в динамічності параметрів безпроводової мережі. Тому актуальною задачею є розробка алгоритму аналізу станів безпровідної мережі, що зможе врахувати всі особливості саме безпровідної мережі Wi-Fi. Для вирішення цієї задачі запропоновано використати математичний апарат нечіткої логіки.

Для оцінювання рівня безпеки безпровідних Wi-Fi мереж запропоновано використати декілька параметрів, що характеризують як фізичні характеристики безпровідної мережі, так і особливості її функціонування. Такими параметрами є: рівень сигналу, кількість невдалих автентифікацій, частка аномального трафіку, кількість активних клієнтів, дисперсія RSSI та частота надсилання probe-запитів. До кожного параметру було створено функції належності для опису нечітких лінгвістичних змінних використовуються трапецієподібні функції належності, які добре підходять для змін реальних параметрів Wi-Fi мереж. Функції належності такого виду спрощують побудову правил нечіткої логіки для безпровідних мереж.

Для створення системи безпеки безпровідної Wi-Fi мережі було використано шість вхідних параметрів. Щоб врахувати всі можливі комбінації, потрібно створити 729 правил (6 параметрів × 3 терми = 3^6=729). Реальна система захисту має врахувати всі ці правила, і якщо в процесі функціонування системи будуть додаватися нові параметри, то кількість правил буде зростати відповідно. Але вручну створити таку модель є досить об'ємним завданням, і щоб не перевантажувати систему, але презентувати її ефективність, в рамках даної роботи було створено спрощену базу правил (16

правил), де реакція системи визначається факторами які найбільше впливають на ризики мережі. Наприклад, якщо система показує, що трафік є аномальний, то майже неможливо, скільки користувачів або який рівень сигналу, то ризик все одно буде високим. Або якщо кількість невдалих автентифікацій високий і одночасно велика кількість probe-запитів, це майже завжди говорить про наявність атаки.

Процедура обробки запропонованого алгоритму має наступну послідовність.

1. На першому етапі здійснюється збір даних. В реальному часі система захисту отримує дані з точки доступу, або використовуючи спеціалізоване програмне забезпечення, що аналізує середовище передачі даних.

2. Другий етап аналізу полягає в тому, що всім шести вхідним параметрам і одному вихідному задаються функції належності, що складаються з лінгвістичних термів. В нашому випадку це трапецієподібні функції, які оцінюють параметр від 0 до1.

3. Третій етап процедури обробки пов'язаний з створенням бази правил. В даній роботі правила створювалися використовуючи трьох експертів та статистичний аналіз роботи безпровідних Wi-Fi мереж середньої величини. Сформована база правил містить 16 правил, що мають формат типу: «ЯКЩО–ТО».

4. На четвертому етапі відбувається агрегація правил. Тобто обчислюються всі правила і перевіряється наскільки вони відповідають поточному стану безпроводової мережі. Обчислювання реалізується з допомогою нечіткої логіки, розраховуючи мінімуми функцій належності, так як даний метод є класичним для типу системи Mamdani, що була використана в роботі.

5. Після перетворення ознак у нечіткі лінгвістичні змінні та їх розрахунки, здійснюється комплексна оцінка всіх параметрів. Суть цього етапу полягає в тому, що всі множини правил, які виявилися вище 0 об'єднуються в одну спільну функцію, що характеризує ступінь ризику безпроводової мережі за допомогою операції максимум. Якщо декілька з правил показали високий рівень ризику безпеці безпроводової мережі, що мають різні рівні ризику, ми об'єднуємо їх. Об'єднання реалізується використанням найбільших значень в кожній точці. В результаті отримуємо криву, що характеризує поточний стан безпроводової мережі.

6. Після комплексної оцінки всіх параметрів необхідно провести дію дефазифікації (перетворення лінгвістичної змінної в числову). В даній роботі для дефазифікації було використано метод «центру ваги». Такий метод полягає в наступному: отриманий результат значення ступеня ризику безпровідної мережі розглядається як плоску фігуру, і знаходження конкретного числа ризику відбувається знаходження координати центру площі (математичного сподівання), тобто точку, де б отримана фігура «врівноважилася», якщо б її поклали на вісь.

7. На основі числа, що отримане після процедури дефазифікації, система визначає стан безпеки безпроводової мережі відповідно до:

- 0–0.25 — низький ризик (нормальна робота),
- 0.25–0.55 — середній ризик (посилене спостереження),
- 0.55–0.75 — високий ризик (запис події в журнал),
- >0.75 — критичний ризик (автоматичне блокування або сповіщення адміністратора).

8. На останньому етапі відбувається прийняття результуючого рішення системи безпеки. Рішення залежить від рівня ризику, що буде визначено системою на поточний момент:

I. При визначенні системою результату «Низький ризик» означає, що робота мережі відбувається в штатному режимі без жодних підозрілих активностей, тобто всі параметри мережі знаходяться в межах допустимих значень. В такому випадку система продовжує звичайне функціонування та періодично робить записи в журнал про стан мережі (RSSI, кількість клієнтів, трафік). Більше ніяких додаткових дій не проводиться, щоб не перевантажувати систему захисту.

Наприклад якщо рівень сигналу є стабільним, причому кількість клієнтів відповідає нормі, для поточного часу і дня тижня, а невдалі автентифікації є поодинокі і трафік передається без аномалій.

II. При «Середньому ризик» система безпровідного захисту фіксує деякі відхилення в аналізованих показниках, але їх відхилення не значне. В такому випадку можливі збої зв'язку безпроводової мережі, випадкові повтори автентифікації або нестабільність сигналу. Це говорить про те, що ймовірність атаки не висока, але все одно мережа потребує контролю. В такому випадку система починає підвищений моніторинг мережі: частіше отримує дані від мережі (наприклад, якщо в штатному режимі дані надходять до системи захисту кожну хвилину, а зараз починає отримувати кожні 10 секунд); починає записувати в журнал розширений список параметрів (probe-запити, аномалії

трафіку); проводиться аналіз сусідніх точок доступу (на випадок реалізації атаки фальшива точка доступу). Також система може обмежити швидкість обміну даних для деяких підозрілих клієнтів, або запросити від них повторну автентифікацію. При такому рівні ризику адміністратор отримує повідомлення, про стан мережі.

Наприклад якщо система захисту зафіксувала зниження сигналу у деяких абонентів та незначне зростання кількості probe-запитів, але без втрати зв'язку.

III.Коли визначається «Високий ризик» це означає що система безпровідного захисту зафіксувала ознаки проведення атаки (підозрілий клієнт, підбір паролю або нехарактерний трафік). В такій ситуації робиться запис у журнал безпеки, де записується час, MAC-адрес, та інші параметри сигналу. Система надсилає повідомлення адміністратору з поміткою «УВАГА», може блокувати підозрілих абонентів а також передає сигнал системі виявлення вторгнень для виконання порівняння сигнатур з базою даних вже відомих атак.

Наприклад, абонент або декілька абонентів проявляють підозрілу активність: змінюється рівень сигналу, відбуваються помилки автентифікації, а трафік не типовий для абоненту – це з великою долею ймовірності може свідчити про початок атаки man-in-the-middle («людина посередині»).

IV. При «Критичному ризику» в мережі відбувається активність, що однозначно вказує на проведенні активних дій атаки на безпровідну мережу Wi-Fi: перехоплення каналу зв'язку, фальшива точка доступу, масові запити автентифікації або різке збільшення probe-запитів. При такій агресивній активності система безпеки реагує відразу, блокуючи агресивну активність, можливе повне блокування трафіку в окремому сегменті, а вже після блокування сповіщає адміністратора про небезпеку. Також робиться запис у журнал безпеки, що містить всі поточні параметри.

Наприклад, якщо трафік аномальний, велика кількість автентифікацій, а рівень сигналу різко зменшується може говорити про DOS, атаку з підміною точки доступу або сканування абонентів мережі.

Підсумовуючи все вище подане, можна узагальнити у вигляді табл. 1.

Таблиця 1. Результати вимірювання рівня сигналу

Рівень ризику	**Інтервал після дефазифікації**	**Дії**	**Тип реакції**
Низький	0 – 0,29	Моніторинг	Пасивна
Середній	0,3 – 0,59	Посилене спостереження, запис у журнал подій	Напівактивна
Високий	0,6 – 0,89	Реєстрація інциденту, обмеження трафіку	Активна
Критичний	0,9 – 1	Автоблокування, сповіщення	Агресивна

9. Як додаткова функція, але також дуже важлива, що реалізується вже після прийняття рішень – це зворотний зв'язок. Таке доповнення допомагає навчити систему захисту реакціям на атаки з якими вона вже зустрічалася, або корегувати функції належності або реакції системи захисту на якусь конкретну активність. Агресивним подіям система навчається в автоматичному режимі, а інші зміни вносить адміністратор після перегляду і аналізу журналу подій.

Структурна схема, що реалізує функції аналізу мережі з використанням нечіткої логіки, представлена на рисунку 1.

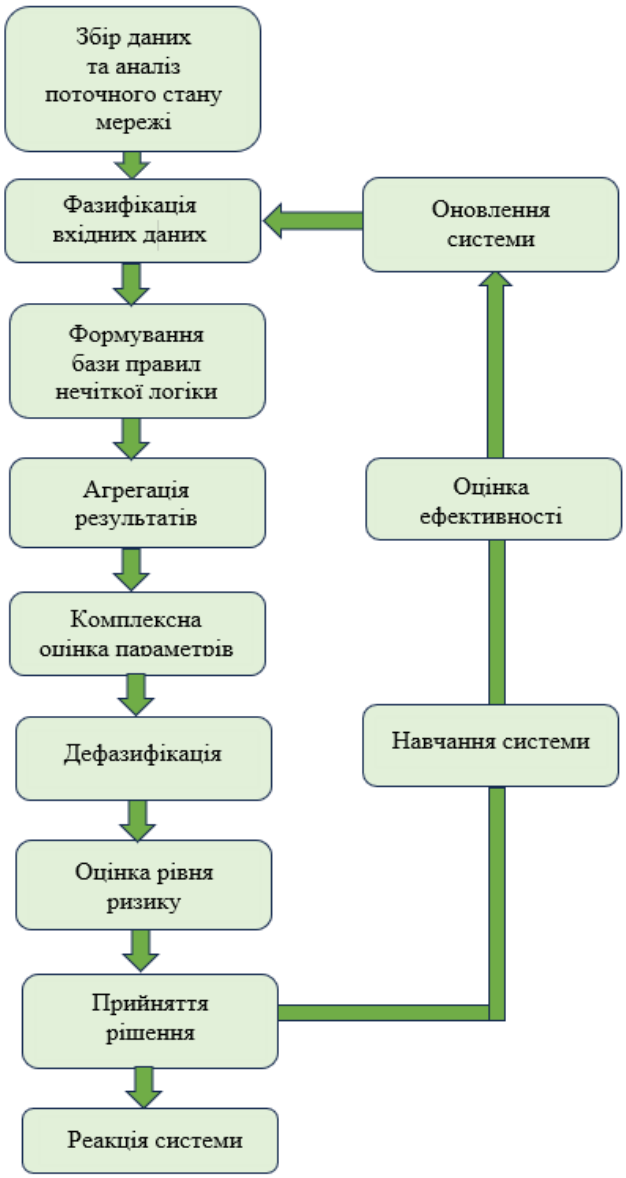

Рис. 1. Структурна схема, що реалізує функції аналізу мережі з використанням нечіткої логіки

Висновки

Запропонований у роботі алгоритм аналізу стану Wi-Fi мережі на основі нечіткої логіки дозволяє більш адекватно ухвалювати рішення щодо аномальності мережі. Використання нечіткої логіки дає змогу коригувати рішення залежно від змін умов функціонування мережі. Система може працювати як у автоматичному режимі (самостійно ухвалює рішення), так і за участю оператора (експерт, проаналізувавши отримані результати, ухвалює рішення самостійно залежно від ситуації).

Література

1. Gast M. S. 802.11 Wireless Networks: The Definitive Guide. Sebastopol CA, USA: O'Reilly Media, 2013.

2. O'Hara B., Petrick A. The IEEE 802.11 Handbook: A Designer's Companion. New York, NY, USA: IEEE Press, 2005.

3. Kuznetsov V. I., Shvachych H. H. Metody zabezpechennia bezpeky bezdrotovykh merezh IEEE 802.11 // Visnyk NTUU KPI. Informatyka, 2019.