Ячменьова С.О., здобувач,
Шелуха О.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

МЕТОДИ ЗАХИСТУ WI-FI-МЕРЕЖ ВІД СПУФІНГУ

Останні роки зростає кількість кібератак через відкриті точки доступу в мережі стандарту IEEE 802.11 (Wi-Fi). Зловмисники завдяки відкритому характеру середовища мають можливість виявляти MAC адреси інших пристроїв у мережі, що дає змогу здійснити спуфінг атаку, так звану як «Злий двійник» («Evil twin»). Задля протидії поданої проблеми безпеки використовуються спостереження та аналіз кадрів у підключенні, зокрема моніторинг за допомогою систем штучного інтелекту.

Стандарт IEEE 802.11 є одним із основних видів бездротового зв'язку, який часто використовується Wi-Fi-мережами через велику кількість мобільних пристроїв. Не зважаючи на низку переваг у використанні, описаний стандарт працює за допомогою радіоефіру і широкомовної природи фізичного рівня, що робить мережу вразливою до здійснення атак на безпечній відстані. Зокрема, виокремлюють атаки: спрямовані на різні рівні мережевої моделі OSI; рекогносцирування; доступності; посередника; спуфінг.

Атака спуфінгу, зокрема «Злий двійник», націлена на перепідключення користувачів до шахрайської точки доступу для витягання конфіденційної інформації. Цей тип атаки може використовувати бездротові системи з низьким рівнем захисту, що стає особливо небезпечним з урахуванням розвитку мікрочипів та Інтернету речей. Зловмисники можуть використовувати вразливі пристрої, такі як смарт-годинники, фітнес-браслети, кардіо системи, для отримання конфіденційної інформації. Кінцевий результат атаки полягає в перевантаженні мережі шляхом відправки завдань з високим пріоритетом і цілеспрямованому перехопленні доступу до інтернет-трафіку від ключових пристроїв клієнта [1].

На сьогоднішній день стандартними заходами для запобіганнями такого роду атаки є низка заходів, що включають забезпечення тактових відміток з'єднання, нагляд за підозрілою активністю у бездротовій мережі та забезпечення шифрованого доступу до підключення. Спостереження мережі стандарту IEEE 802.11 та моніторинг кадрів-маяків підключення використовують для визначення несанкціонованих точок доступу, що піддалися атаці чи підозрілій активності.

Моніторинг Wi-Fi зазвичай здійснюють за допомогою мережного аналізатора, налаштувавши фільтрацію по Mac-адресі і певному типу кадрів. Проте, варто зазначити, що процес контролю системи є складним та витратним, тому сьогодні актуальним є використання програм-оптимізаторів чи систем штучного інтелекту для полегшення поставленої задачі.

Можна виділити низку переваг використання штучного інтелекту для боротьби зі спуфінгом типу «Злий двійник» («Evil twin»), а саме: гнучкість та адаптація до змін в мережі; висока швидкість обробки; оптимальний аналіз мережі; доступність до системи знань; нескладний процес зміни даних.

У комплексі моніторингу підключень використовується алгоритм k-найближчих сусідів з використанням штучного інтелекту. Цей метод аналізує мережеві пакети, зберігає дані на основі часових рядів і визначає категорію пристроїв за рівнем сигналу від точки доступу. Основна мета алгоритму – створення моделі класифікації для нових зразків на основі їх подібності до найближчих зразків у наборі даних. Слід зазначити, що метод k-найближчих сусідів з використанням аналізу за допомогою штучного інтелекту, було протестовано і оцінено під час дослідження науковими працівниками «Львівської Політехніки» у 2023 році [2].

Отримані результати, а саме 100 % тестових випадків (більше 7 тисяч), було класифіковано правильно, що вказує, на те, що обраний метод аналізу даних дозволить значно підвищити безпеку інформаційно-комунікаційних системах державного та приватного рівнів [2].

Важливо відмітити деякі негативні сторони використання описаного методу аналізу даних, а саме: необхідність технічного забезпечення для повного функціонування системи, постійне навчання мережі штучного інтелекту, ризик неточності виявлення атаки.

Отже, у сучасному світі є реалізація ефективних методів з використанням штучного інтелекту в моніторингу кадрів для захисту в мереж стандарту IEEE 802.11 від кібератак типу «Злий двійник».

Таким чином, подальші дослідження будуть спрямовані на вдосконалення існуючих методів та систем протидії спуфінг-атак, розробку нових технологій для поліпшення моніторингу та покращення захисту від стороннього втручання в безпровідних мережах стандарту IEEE 802.11(Wi-Fi).

Список використаної літератури

1. Корольков Р.Ю. Сценарій атаки з використанням несанкціонованої точки доступу у мережах IEEE 802.11. Кібербезпека: освіта, наука, техніка. 3 (11), 2021, с. 144-154. – URL: https://doi.org/10.28925/2663-4023.2021.11.144154