Басистий В. А., магістрант
Чешун О. В., здобувач
Чешун В. М., к.т.н., доцент
Хмельницький національний університет

ОРГАНІЗАЦІЯ КОМУТАЦІЙНИХ ПІДКЛЮЧЕНЬ МІКРОКОМП'ЮТЕРІВ В КОМЛЕКСІ МОНІТОРИНГУ І АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ ІОТ

Системи IoT відіграють все більшу роль в різних сферах життєдіяльності людини, але мають значний недолік – вразливість до кібератак [1]. Більшість пристроїв і систем IoT не здатні виконувати завдання захисту, зокрема, здійснювати моніторинг мережевого трафіку. Це пояснюється їхніми обмеженими ресурсами: низькою обчислювальною потужністю, невеликим обсягом пам'яті та обмеженою енергетичною ємністю. Через ці фактори встановлення засобів для постійного моніторингу та аналізу даних безпосередньо на IoT-пристроях стає неможливим.

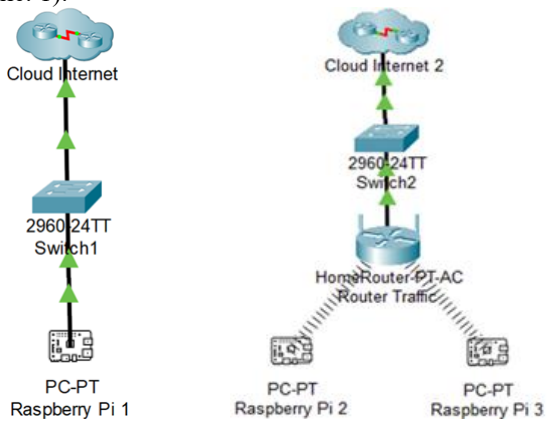
Внаслідок таких обмежень завдання з моніторингу часто передаються на централізовані сервери або хмарні платформи, які мають достатньо ресурсів для обробки великих обсягів даних [2]. Однак, безперервне передавання даних від великої кількості пристроїв до сервера може спричинити перевантаження мережі, а обробка даних на централізованих серверах може бути недостатньо швидкою для IoT-систем, які потребують миттєвої реакції на загрози.

В [3] авторами запропоноване рішення для створення комплексу моніторингу і аналізу мережевого трафіку IoT на одноплатних мікрокомп'ютерах.

Базовим елементом комплексу є мікрокомп'ютер Raspberry Pi (можлива реалізація на інших одноплатних мікрокомп'ютерах), на якому розгортається програма моніторингу. Для розробки програмної складової комплексу було обрано мову програмування Python з бібліотеками Psutil, Scapy, Pandas, що дає можливість отримувати детальну інформацію про активні процеси та підключені пристрої.

Сховищем інформації виступає сервер, який дозволяє користувачу збирати окремі пакети за стандартним протоколом від певного пристрою або від всіх одночасно. Аналіз проводиться на комп'ютері користувача без використання ресурсу основного пристрою.

Комплекс передбачає можливість підключень на основі кабельних з'єднань і через маршрутизатор з бездротовою точкою доступу (рис. 1).



а) б)

Рис. 1 – Організація комутаційних підключень в системі моніторингу:
а) кабельне; б) з бездротовою точкою доступу

У випадку, коли немає можливості реалізувати безпровідне підключення, є можливість підключити IoT-пристрій через кабель (рис. 1.а). Використавши такий варіант підключення можна забезпечити надійний і стабільний зв'язок, який не обмежується перешкодами, але це робить підключення пристроїв обмеженим через кількість портів комутатора.

Бездротове підключення (рис. 1.б) вимагає використання маршрутизатора з функцією бездротової точки доступу для підключення до Інтернету. Цей варіант підключення надає можливість підключати велику кількість пристроїв, з високою швидкістю, тому воно є найкращим і обмежується тільки специфічним обладнанням і швидкістю передачі даних пристроїв.

Список використаних джерел:

1. Метод виявлення DDOS атак на IOT мережі / Нічепорук А.О. та ін. Вісник Хмельницького національного університету, Технічні науки. 2020. №1 (281). С.184-191.
2. Засоби моніторингу мережі в IoT інфраструктурі з гібридною архітектурою / Каплунов А. В., Гайдай А. Р., Гер В. М., Нікольський С. С. Телекомунікаційні та інформаційні технології. 2023. № 2(79). С.22-32.
3. Басистий В.А., Чешун О.В., Чешун В.М. Комлекс моніторингу і аналізу мережевого трафіку IOT на одноплатних мікрокомп'ютерах. Тези доповідей XXVII Всеукраїнської НПК «Могилянські читання – 2024», Технічні науки. С.103-108.