Система моніторингу периметра об'єкта критичної інфраструктури

УДК 004.056

Олександр Галущенко[1], Володимир Лужецький[2]

Вінницький національний технічний університет,
[1]mamr3379@gmail.com, [2]v.luzhetskyi@vntu.edu.ua

Захист об'єктів критичної інфраструктури набуває особливої актуальності в теперішній час. Тому значна увага приділяється створенню систем забезпечення кібербезпеки, що призначені для запобігання, своєчасного виявлення та протидії загрозам безпеці об'єктам критичної інфраструктури з використанням кіберпростору; усунення умов, що їм сприяють, та причин їх виникнення.

Процес забезпечення безпеки великих за площею об'єктів критичної інфраструктури (великі промислові об'єкти, електростанції, морські порти та ін.)базується на використанні комплексу технічних систем і заходів, метою яких є виявлення та попередження несанкціонованого проникнення в заборонену зону. Ці системи мають забезпечувати багатофакторний контроль ближніх та дальніх рубежів.

У доповіді розглядається система моніторингу периметра об'єкта критичної інфраструктури, яка використовує особливості Wi-Fi технології бездротової мережі з пристроями на основі сімейства стандартів IEEE 802.11.

Використання бездротових технологій надає багато переваг і забезпечує гнучкість в побудові бізнес-процесів. Особливо це стосується управління рухомими об'єктами, складської логістики та об'єктів, де неможливо або складно організувати дротову мережу.

Основна задача моніторингу полягає у:

- визначенні координат пристроїв з модулями Wi-Fi, що працюють як точка доступу;
- визначенні часу їх появи в зоні, що підлягає моніторингу;
- створення історії їх переміщень.

Для розв'язання даної задачі потрібно знати координати всіх точок доступу на планеті та здійснювати моніторинг радіоефіру навколо об'єкта критичної інфраструктури.

Будь-який мережевий пристрій має свій унікальний ідентифікатор у вигляді MAC-адреси. Теоретично існує понад 281 трильйон унікальних MAC-адрес. Ця кількість дозволяє забезпечити унікальність ідентифікаторів для всіх мережевих пристроїв у світі. Глобальна система моніторингу створює базу координат всіх пристроїв на планеті та здійснює їх прив'язку до карти.

Метод визначення координат пристроїв передбачає реалізацію таких дій. Створюється віртуальне середовище, в якому кожна віртуальна машина формує унікальний набір характеристик (fingerprinting), який ніколи більше не буде застосовуватися. До геопровайдерів надсилається запит виду: «Я увімкнувся, бачу тільки один пристрій з MAC-адресою ****, скажи, де я». Якщо надходить відповідь з координатами пристрою за MAC-адресою ****, то дані записуються в базу і віртуальна машина змінює свої характеристики для наступного запиту. Якщо

відповіді немає, то псевдовипадковим чином формується наступна MAC-адреса і робиться запит. Це виконується до тих пір, поки не буде отримано відповідь.

Будь-який пристрій, що працює в стандарті IEEE 802.11, обмінюється технічною інформацією з іншими пристроями, які розташовані поруч. Це необхідно для визначення завантаженості каналів і перемикання самих точок доступу на менш завантажені канали. Ще цей механізм використовується для більш точної геолокації. Мобільний пристрій, який хоче визначити свою геолокацію, збирає отримані дані: MAC-адресу точки доступу Wi-Fi, SID та LAC базових станцій операторів мобільного зв'язку, рівень сигналу в точці вимірювання та передає ці дані геопровайдеру. Геопрвайдер повертає координати розташування пристроїв, що бачить пристрій, якому потрібно визначити свої координати.

Для створення глобальної системи моніторингу використано хмару AMAZON AWS, 1500 орендованих серверів з 36 одночасно працюючими потоками. Така система забезпечує можливість здійснювати моніторинг всіх MAC-адрес на планеті кожні 24 години. Завдяки чому можна відстежувати переміщення пристроїв з однієї локації в іншу.

Локальна система моніторингу здійснює моніторинг радіоефіру навколо об’єкта критичної інфраструктури використовуючи дані, отримані від глобальної системи моніторингу, та від вимірювального комплексу. Дані від глобальної системи моніторингу запитуються шляхом виділення певної зони на карті. Результатом виконання запиту є набір координат, які доступні для оброблення в межах зазначеної зони.

Для моніторингу радіоефіру використовуються нерухомі та рухомі вимірювальні пристрої. Це забезпечує побудову радіоефірної карти місцевості навколо об’єкта критичної інфраструктури. Аналіз такої карти дає можливість виявити:

- аномальні пристрої, власники яких шукають підходи до території, що охороняється, але не потрапляють у поле зору камер відео спостереження;
- однакові пристрої біля різних об’єктів критичної інфраструктури;
- різні пристрої, що раніше підключалися до точки доступу з одним ім'ям мережі.

Таким чином, поєднання цих двох систем моніторингу дозволяє своєчасно виявляти:

- осіб, які проводять негласне спостереження за об'єктами критичної інфраструктури або за працівниками;
- спроби злому Wi-Fi мереж та перехоплення трафіку клієнтів цих мереж;
- спроби сканування мережі критичної інформаційної інфраструктури хакерами та місця фізичного розташування хакера при підключенні до мережі Wi-Fi;
- переміщення осіб у темний час доби в зонах поганої видимості камер відеоспостереження.