УДК 004.7

Пирч О.В., асистент,
Коробко Р.М., здобувач,
Панько Р.М., здобувач,
Державний університет «Хмельницький національний університет»

ОСОБЛИВОСТІ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ МАЛОЇ ІНТЕНСИВНОСТІ

Сучасні системи моніторингу безпеки мереж здебільшого орієнтовані на аналіз великих обсягів трафіку, адже у переважній більшості досліджень з виявлення аномалій опрацьовуються саме великі масиви мережевого трафіку: терабайти логів, довгі часові ряди, та багатогодинні сесії., де статистичні закономірності чітко виражені. Такий підхід традиційно формується навколо хмарних інфраструктур, великих корпоративних мереж або дата-центрів. Однак у випадках малої інтенсивності передавання даних, зокрема у сегментах IoT, промислових мережах або малих корпоративних інфраструктурах, класичні методи виявлення аномалій втрачають ефективність через нестачу даних і високу варіативність поведінкових характеристик. Саме там аномалії ховаються найкраще. У тих поодиноких пакетах важче знайти закономірність, але у той же час і легше непомітно приховати атаку.

Ключовими особливостями та проблемами аналізу трафіку малої інтенсивності є нестача статистично значущих значень, нерегулярність трафіку, домінування «квазіаномалій», та проблема високої чутливості алгоритмів. Коли активність низька, це призводить до того що кількість пакетів недостатня для побудови надійної моделі. У класичних методах (наприклад, сигнатурних або статистичних IDS) це призводить до високої похибки і неможливості формування репрезентативного профілю системи. У таких умовах кожен пакет стає важливим, і система повинна працювати з мінімальним набором інформації, не втрачаючи контексту.

Варто підкреслити, що потоки малої інтенсивності не мають чітких ритмів, що означає що пакети можуть надходити рідко, неформально, і без стабільного інтервалу. Це ускладнює побудову часових моделей і зменшує ефективність методів, що покладаються на регулярність (LSTM, ARIMA тощо). Інколи поведінка пристрою змінюється просто тому, що він працює в іншому режимі, і система, яка є досить чутлива о будь-яких змін, може сприйняти це як атаку і відповідним чином підкреслити це у системі безпека, що є false-positive відповіддю і може призупинити роботу системи поки ця проблема не буде вирішеною, що у свою чергу може завдати збитків компанії.

У трафіку малої інтенсивності з’являється багато подій, які формально відхиляються від норми, але не є шкідливими. Прикладами таких подій може бути повторна ініціалізація пристрою, коли працівник використовує

систему з іншого девайсу не завершивши сеанс на іншому пристрої, зміна інтервалу передачі даних, або ж короткотривала нестабільність мережі, яка може вплинути на те як трафік приймається, і може бути також сприйнята як аномальна зміна трафіку.

Для подолання цих проблем запропоновано використовувати комбіновані методи машинного навчання, зокрема автоенкодери для реконструкції нормальної поведінки та непараметричні алгоритми кластеризації (DBSCAN, k-NN) для виділення потенційно аномальних зразків. Крім того, ефективним виявився підхід із динамічним формуванням часових вікон, що враховує реальну активність мережевих вузлів, а не лише фіксовані інтервали часу. Аналіз особливостей трафіку малої інтенсивності засвідчує, що традиційні IDS-моделі не є ефективними для таких умов. Для підвищення якості виявлення аномалій необхідно застосовувати адаптивні підходи машинного навчання, здатні працювати з обмеженими та нестабільними даними.

Поєднання автоенкодерів, непараметричних алгоритмів та динамічної сегментації даних утворює модель, що успішно працює з неповними та нерегулярними потоками; знижує рівень false-positive спрацьовувань; виявляє як одиничні, так і групові аномалії; зберігає адаптивність у середовищах, де поведінка нормального трафіку змінюється. Усе це створює основу для побудови ефективних систем захисту в малих мережах, де тиша й повільні ритми трафіку не повинні вводити в оману: саме там найдовше ховається загроза.

Практична цінність дослідження полягає у можливості впровадження запропонованого методу в системи моніторингу безпеки корпоративних мереж, інфраструктури інтернету речей, промислові сегменти та віддалені вузли, де обсяг трафіку є обмеженим і нестійким. Запропонований підхід забезпечує підвищену точність виявлення аномалій за умов малої інтенсивності передавання даних, що дозволяє значно зменшити ризики непомічених атак, прихованих мережевих взаємодій та несанкціонованого доступу. Завдяки адаптивності та здатності працювати з мінімальними вибірками метод може бути використаний для зміцнення кіберзахисту у критично важливих інформаційних середовищах та інфраструктурах, де традиційні IDS-рішення втрачають ефективність.

Список використаних джерел:

1. Stephanie N. Anomaly Detection in Network Traffic Using Advanced Machine Learning Techniques. URL https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10833631

2. Félix I.V. Analysis of network traffic features for anomaly detection. URL https://www.researchgate.net/publication/269420763_Analysis_of_network_traffic_features_for_anomaly_detection