УДК 004.056.5

В. М. Ковальчук

Т. Г. Кирилащук

АНАЛІЗ ВИТОКУ КОНТЕКСТОЇ ІНФОРМАЦІЇ В ЗАШИФРОВАНОМУ ТРАФІКУ IOT-ПРИСТРОЇВ ЗА ДОПОМОГОЮ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Вінницький національний технічний університет

Анотація

У роботі досліджується проблема витоку метаданих через аналіз паттернів зашифрованого трафіку пристроїв Інтернету речей. Розглянуто можливість ідентифікації станів пристроїв на основі розміру пакетів та частоти їх відправлення. Запропоновано використання алгоритмів машинного навчання для виявлення контекстної інформації без дешифрування вмісту пакетів.

Ключові слова: кібербезпека; IoT; зашифрований трафік; метадані; машинне навчання; витік інформації.

ANALYSIS OF CONTEXTUAL INFORMATION LEAKAGE IN ENCRYPTED IOT TRAFFIC USING MACHINE LEARNING METHODS

Abstract

The paper investigates the issue of metadata leakage through the analysis of encrypted traffic patterns in IoT devices. The possibility of identifying device states based on packet size and transmission frequency is considered. The use of machine learning algorithms to extract contextual information without decrypting packet content is proposed.

Keywords: cybersecurity; IoT; encrypted traffic; metadata; machine learning; information leakage.

Вступ

Сучасна практика широкого застосування технологій шифрування, таких як HTTPS або TLS, у галузі Інтернету речей (IoT) сприяє створенню хибного уявлення про абсолютну захищеність передачі даних. Тим не менш, навіть за умов використання високонадійних криптографічних протоколів, мережевий трафік залишається вразливим до можливості його аналізу. Зловмисники, досліджуючи метадані, зокрема розмір передач пакетів та часові інтервали між ними, здатні реконструювати інформацію про активність користувача та отримувати контекстуальні дані, не розшифровуючи сам зміст переданих повідомлень.

Актуальність даної проблематики зумовлена швидким інтегруванням IoT-пристроїв у повсякденну діяльність, що, своєю чергою, сприяло зростанню використання шифрування трафіку як основного методу забезпечення конфіденційності.

Основна мета дослідження полягає у всебічному аналізі вразливостей IoT-пристроїв щодо витоку контекстної інформації через доступні метадані зашифрованого трафіку.

Результати досліджень

1. Специфікація ознак для класифікації трафіку

Головним критерієм для аналізу є розподіл довжин пакетів, оскільки саме специфіка функціонування пристроїв визначає обсяги формованих повідомлень. Наприклад, пакет розміром 150 байт може сигналізувати про виконання команди відкриття розумного замка, тоді як пакет на 100 байт – про його закриття. Крім постійної довжини повідомлень, ключову роль відіграють часові інтервали між пакетами, які відображають апаратні затримки мікроконтролера під час обробки сенсорних даних. Аналіз статистичних характеристик цих інтервалів, таких як середнє значення, дисперсія і стандартне відхилення, дозволяє алгоритмам машинного навчання ефективно розпізнавати роботу різних моделей пристроїв, навіть якщо їх функціональні можливості мають багато спільного.

Однією з основних груп характеристик є параметри, що визначають спрямованість і обсяг потоку даних, які враховують співвідношення між кількістю вхідних і вихідних пакетів упродовж певного періоду спостереження. З огляду на те, що переважна більшість IoT-пристроїв функціонує за подійною моделлю, аналіз характеристик типу Burst (епізодичних "вибухів" пакетів) стає інструментом, який дозволяє виявляти моменти активації цих пристроїв навіть на фоні загального трафіку. Кожна серія пакетів має притаманну їй тривалість і частоту, що забезпечує можливість класифікації стану системи з високою точністю, навіть у тому випадку, якщо вміст пакетів захищений протоколами на кшталт HTTPS або TLS.

Заключний етап специфікації передбачає аналіз ентропії корисного навантаження, що у зашифрованому трафіку наближається до одиничного значення. Одночасно структура метаданих зберігає свою передбачуваність та детермінованість. Ця стабільність метаданих виступає ключовою основою для навчання алгоритмів машинного навчання, таких як Random Forest або K-Nearest Neighbors. Такі алгоритми здатні виявляти закономірності витоку контекстної інформації у режимі реального часу.

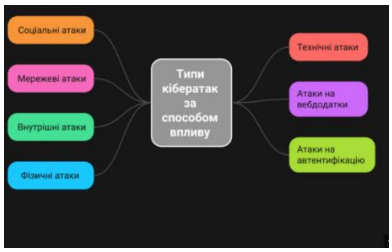

Рисунок 1 – Концептуальна модель витоку контекстної інформації через аналіз метаданих зашифрованого трафіку IoT-пристроїв [1]

На схемі, поданій на рисунку 1, продемонстровано практичну реалізацію атаки типу «аналіз трафіку». У цьому випадку об'єктом спостереження виступають не самі зашифровані дані пакетів, а їхні зовнішні характеристики. Наприклад, у контексті смарт-замка можна помітити певну закономірність: подія відкриття дверей супроводжується передачею пакета обсягом 150 байт, а подія закриття – пакетом розміром 100 байт. Це підтверджує теорію, що навіть за застосування протоколів шифрування, таких як HTTPS чи TLS, предсказувана поведінка IoT-пристроїв створює можливості для зловмисників дистанційно відслідковувати особисті дії користувача та визначати його час перебування вдома. Таким чином, метадані трафіку фактично стають своєрідним «прихованим каналом», що нівелює переваги сучасного шифрування і підкреслює важливість використання додаткових методів обфускації даних.

2. Використання методів змагального навчання для обходу аналізу

Ефективний захист конфіденційності в Інтернеті речей можна забезпечити за допомогою методів змагального машинного навчання, які спрямовані на введення класифікаторів зловмисника в оману. Суть методу полягає у створенні змін у мережевому трафіку, які примушують модель розпізнавання неправильно інтерпретувати поточний стан пристрою. Для цього підходу зазвичай застосовують генеративно-змагальні мережі (GAN), де одна підмережа розробляє оптимальні шаблони маскування, а інша перевіряє здатність розрізняти оригінальний трафік і модифікований. У системі існує дві нейронні мережі:

1. Генератор

2. Дискримінатор – є найважливішим інструментом під час вирішення задач класифікації. На відміну від інших методів, дискримінантний аналіз дозволяє дослідникy спрогнозувати, до якого класу належить новий об’єкт [2].

За даними спеціалістів Cisco, ключовим методом ідентифікації пристроїв без порушення конфіденційності є технологія SPLT (Sequence of Packet Lengths and Times), яка перетворює послідовність розмірів пакетів та інтервалів їх прибуття у математичний вектор для класифікації.

Маніпуляції зосереджуються на ключових параметрах, які технологія Cisco SPLT використовує для ідентифікації пристроїв. Зокрема, генерований алгоритм штучно змінює послідовність довжин мережевих пакетів та часові інтервали між ними, перетворюючи статичний цифровий "відбиток" пристрою на хаотичний шум.

Висновки

Шифрування трафіку забезпечує захист самого вмісту даних, проте метадані IoT-пристроїв залишаються вразливими. Дослідження свідчать, що шляхом аналізу розмірів пакетів і часових проміжків між ними можна визначити дії користувача навіть без необхідності розшифровування переданої інформації. Технологія Cisco SPLT ілюструє можливість класифікації станів пристроїв, ґрунтуючись на векторних шаблонах трафіку. Це створює загрозу витоку контекстної інформації, яка стосується особистого життя користувачів. Для посилення захисту пропонуються методи, засновані на використанні змагального навчання за допомогою нейронних мереж типу GAN. Додавання шумів та зміна характеристик пакетів допомагають ефективно приховувати реальну активність пристроїв від систем моніторингу й аналізу трафіку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Типи кібератак – 4 класифікації кібератак. Datami. URL: https://datami.ee/ua/blog/types-of-cyberattacks-4-classifications-of-cyber-threats/ (дата звернення: 15.02.2026).
2. 5.1 Сутність і завдання дискримінантного аналізу. Бізнес-аналітика багатовимірних процесів. URL: http://ebooks.git-elt.hneu.edu.ua/babap/5-1-id5-1.html (дата звернення: 15.02.2026).

Вікторія Михайлівна Ковальчук – студентка групи 2КІТС-24б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: viktoriakovalchuk999@gmail.com;

Науковий керівник: Тетяна Генадіївна Кирилащук – асистент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: kgt0998@gmail.com;

Viktoriia M. Kovalchuk – student of the 2KITS-24b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: viktoriakovalchuk999@gmail.com;

Scientific Supervisor: Tetiana H. Kyrylashchuk – assistant of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: kgt0998@gmail.com.