УДК 621.396.6:004.7

АНАЛІЗ ТА МОДЕЛЮВАННЯ IOT-ТРАФІКУ

Сидоренко В.С., Агеєв Д.В.
e-mail: vladyslav.sydorenko.cpe@nure.ua
Харківський національний університет радіоелектроніки,
каф. ІКІ ім.В.В. Поповського
м. Харків, Україна

This paper examines the characteristics of IoT traffic, focusing on its modeling and analysis. A generator tool was developed to generate synthetic traffic. Machine learning methods, such as Random Forest and KNN, were applied to classify devices and detect traffic types. The study proving the effectiveness of entropy-based analysis for IoT security enhancement.

Вступ. Розвиток Інтернету речей (IoT) суттєво змінює структуру інтернет-трафіку, створюючи нові виклики у сфері мережевого моніторингу та безпеки. Згідно з прогнозами International Data Corporation, до 2030 року кількість IoT-пристроїв досягне 51,6 мільярда, а загальний обсяг створюваних даних складе 79,4 зетабайти. Це викликає зростання обсягу трафіку, що передається мережею. IoT-пристрої мають обмежені обчислювальні ресурси, саме тому виникає необхідність у розробці методів моніторингу та аналізу IoT-трафіку, що дозволяють підвищити ефективність проектування та управління IoT мереж.

Метою дослідження є характеристика IoT-трафіку, розробка та тестування методів його моделювання. Основні завдання:

- розробити генератор трафіку для моделювання IoT-мереж;
- провести аналіз ентропії мережевого трафіку та дослідити його поведінку під різними умовами;
- застосувати методи машинного навчання для класифікації IoT-пристроїв.

Дослідження базується на емпіричних вимірюваннях IoT-трафіку, його аналізі за допомогою статистичних методів та моделюванні штучного трафіку. Було використано такі методи:

- моделювання трафіку: розробка генератора для імітації роботи IoT-пристроїв;
- визначення статистичних характеристик мережевого трафіку;
- методи машинного навчання: застосування алгоритмів Random Forest, KNN та SVM для класифікації пристроїв.

Для вивчення характеристик IoT-трафіку було створено генератор, який дозволяє емулювати роботу IoT-пристроїв у великих масштабах. Генератор працює на рівні пакетів та може імітувати трафік із заданими параметрами:

- період передачі даних,
- розмір пакету,

- використані протоколи.

Тестові сценарії включали моделювання різних пристроїв у мережі розумного дому: розумні лампи, камери, хаби та розетки. Також було проведено експерименти з генерацією аномального трафіку, зокрема DoS, DDoS та сканування портів.

Проведене дослідження дало такі результати:

1) Розподіл трафіку між пристроями:

- камера генерує найбільший обсяг даних (33,5 МБ/день);
- хаб – 10,9 МБ/день;
- лампа та розетки – 0,56–0,58 МБ/день.

2) Виявлено закономірності активності пристроїв:

- у періоди активності (ON) трафік зростає в 4-5 разів у порівнянні з періодами неактивності (OFF);
- під час DDoS-атак трафік зростає у 10 разів.

3) Точність класифікації IoT-пристроїв за допомогою машинного навчання:

- Random Forest – 94,74%;
- KNN – 92,77%;
- Decision Tree – 71,79%.

Висновки. Дослідження підтвердило можливість ефективного аналізу та класифікації IoT-трафіку за допомогою аналізу ентропії та машинного навчання. Розроблений генератор трафіку IoTTGen дозволяє відтворювати реальні сценарії роботи IoT-пристроїв та проводити тестування методів кібербезпеки.

Перспективним напрямком подальших досліджень є оптимізація методів детекції трафіку за допомогою глибокого навчання.

Список використаних джерел:

1. Rydning J. Worldwide IDC Global DataSphere Forecast, 2023-2027: It's a Distributed, Diverse, and Dynamic (3D) DataSphere // IDC Market Forecast. – 2023. – №. US50554523. URL: Worldwide IDC Global DataSphere Forecast, 2023-2027: It's a Distributed, Diverse, and Dynamic (3D) DataSphere

2. Bello, O., Zeadally, S. (2013). Communication Issues in the Internet of Things (IoT). In: Chilamkurti, N., Zeadally, S., Chaouchi, H. (eds) Next-Generation Wireless Technologies. Computer Communications and Networks. Springer, London. https://doi.org/10.1007/978-1-4471-5164-7_10

3. Bereziński, Przemysław, Bartosz Jasiul, and Marcin Szpyrka. "An Entropy-Based Network Anomaly Detection Method" *Entropy* 2015. Vol. 17, No. 4. pp. 2367-2408.DOI: https://doi.org/10.3390/e17042367