УДК 621.382

ПРОБЛЕМИ АНАЛІЗУ ТРАФІКУ В МЕРЕЖІ IOT З ТЕХНОЛОГІЄЮ LI-FI

[1]Бушинський Д.А., [2]Романов А.О.

[1]*Навчально-науковий інститут телекомунікаційних систем*
КПІ ім. Ігоря Сікорського, Україна
[2]*Національний Авіаційний Університет*
E-mail: dbushynskyi2002@gmail.com, anton3329@gmail.com

CHALLENGES OF TRAFFIC ANALYSIS IN IOT NETWORK WITH LI-FI TECHNOLOGY

Suggestions for improving the security of the interaction of Internet of Things and Li-Fi technologies by classifying and analyzing network traffic.

Сучасні комунікаційні системи та мережі інтернету речей продовжують зростати, знаходячи застосування у всіх сферах людської діяльності. Ідея IoT значно покращила якість сучасного життя ці рішення суттєво змінили перспективи технологій. Задіяно різні галузі, включаючи промисловість, охорону здоров'я, будинки, автомобільну промисловість, спорт, розваги та багато інших. Це досягається завдяки широкомасштабному розгортанню сенсорних вузлів або Sensor Nodes (SN) або інтелектуальних пристроїв із можливістю вимірювання та звітування [4]. Однак це залучення викликає серйозні проблеми, оскільки через мережу потрібно пройти багато трафіку. Таким чином, різні класи мережевого трафіку; наприклад, ті, що генеруються за допомогою голосу, фінансових транзакцій, безпілотних автомобілів, SN та інших, є критичними для відповідних секторів і потребують швидкого проходження або фільтрації через проблеми безпеки. Розвиток IoT призводить до експоненціального збільшення розумних пристроїв і датчиків які генерують величезну та різнорідну кількість мережевих даних. Таким чином, вимоги до різних додатків в інтернеті речей швидко зростають, що призводить до попиту на більш точну класифікацію мережевого трафіку.

Пристрої потребують швидшої, безпечної та енергоефективної передачі даних. Зокрема, ми бачимо зростаючу потребу в гарантованій пропускній здатності з низькою затримкою в поєднанні з позиціонуванням не лише в повсякденному житті, доповненій реальності, але й у контролі промислових процесів у реальному часі. Комунікаційні та мережеві технології Li-Fi можуть надати ефективний і недорогий канал для повсюдного зв'язку в мережах IoT [2]. Він може забезпечити покращену швидкість передачі даних із низьким енергоспоживанням [7]. На відміну від радіочастотних хвиль, які використовуються Wi-Fi, світло не може проникати крізь стіни та двері. Це робить його більш безпечним і полегшує контроль, хто може підключатися до мережі [1]. Очевидно, що майбутнє Інтернету речей значною мірою залежить від його взаємодії з технологією Light Fidelity.

Однак у таких системах традиційні методи керування мережею для моніторингу та аналізу даних стикаються з деякими проблемами, наприклад, з точністю та ефективною обробкою великих даних у режимі реального часу. Машинне навчання або Machine Learning (далі - ML) ефективно використовується для полегшення аналітики та виявлення аномалії у системах великих даних для розпізнавання прихованих і складних закономірностей. Дослідники в області мереж застосовують моделі ML для програм моніторингу та аналізу мережевого трафіку або Network Traffic Monitoring and Analysis (NTMA), наприклад, класифікації та прогнозування трафіку.

Застосування ML в NTMA забезпечує підвищення якості функціонування та безпеки мереж IoT. Регулярний моніторинг трафіку, створеного з систем IoT, важливий для їх належного функціонування та виявлення шкідливих дій [5]. Одним із таких видів діяльності є класифікація пристроїв IoT у мережевому трафіку [3]. Це дозволяє адміністратору відстежувати діяльність девайсів, що може бути корисним для належної реалізації якості обслуговування, виявлення шкідливих пристроїв тощо.

Для забезпечення належного контролю мережевого трафіку, дослідимо чотири ключові завдання в NTMA, зображені на рис. 1:

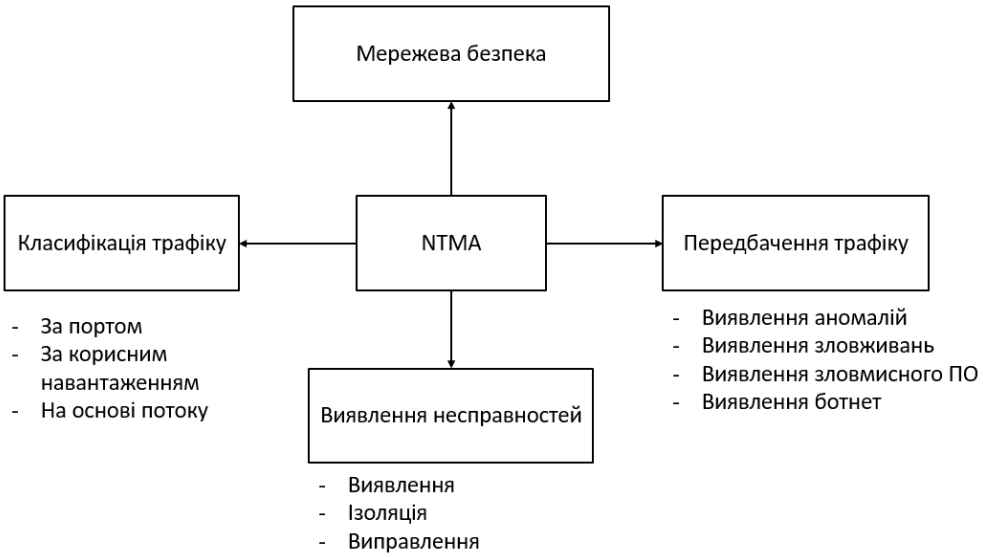

Рис. 1. Ключові завдання NTMA.

Методи машинного навчання, особливо алгоритми глибокого навчання або Deep Learning (DL), є одними з найпопулярніших методів обробки даних мережевого трафіку. Це пояснюється тим фактом, що сучасні комунікаційні системи та мережі IoT, мають відмінні характеристики, які відповідають алгоритмам DL. Ці особливості включають генерацію великих даних, складність, масштабність, зростаючу кількість протоколів у таких мережах тощо. Аналітичний підхід до великих даних можна використовувати для керування даними NTMA на основі машинного навчання. Підхід великих даних можна використовувати для класифікації трафіку атак у програмно-конфігурованої мережах або Software-defined Networking (SDN). Контроллер

SDN забезпечить обслуговування трафіку відповідно до політики, яка встановлена оператором мережі. Прибравши площину управління з мережевого обладнання, контролер реалізує централізовану систему керування, спрощує автоматичне керування мережею [8].

Традиційні методи для NTMA мають свої проблеми, наприклад, вони є неточними або сильно залежить від людського фактору. На відміну від традиційних методів, методи на основі DL мають наступні переваги [3]:

- Моделі DL не потребують значних людських зусиль, можуть використовувати різні репрезентативні шари та ефективні алгоритми для вилучення аномалій із величезних обсягів даних трафіку без розробки функцій. Ця перевага моделей дуже ефективна для методів NTMA, оскільки більшість даних керування мережею є немаркованими або напівмаркованими.

- Алгоритми здатні працювати з часово-просторовими даними, фіксуючи пов'язані залежності. Більшість даних про керування мережею, зібраних як набори даних часових рядів, можна аналізувати моделями DL з високою точністю.

- Крім того, нові парадигми машинного навчання, напр. федеративне навчання в основному розроблено для розподіленого впровадження методів глибокого навчання. Впровадження моделей DL за допомогою нових парадигм ML дозволяє навчати свою модель окремо на кожній машині.

Проведений аналіз проблем мережі IoT викликані великою кількістю генерованого трафіку. Окреслено способи контролю мережевих даних за допомогою NTMA. Досліджено впровадження машинного навчання для підвищення безпеки використання технології Li-Fi в мережах інтернет речей.

Література

1. Petrosino A., Striccoli, D., Romanov, O., Boggia, G., Grieco, L.A. Light Fidelity for Internet of Things: A survey. //Optical Switching and Networking// 2023, 48, 100732, https://www.sciencedirect.com/science/article/abs/pii/S1573427723000036
2. Enabled by Li-Fi Technology [Електронний ресурс] / S. P. Nazir, T. Mohammad, M. Ahmad: https://www.researchgate.net/publication/337388262_IoT_Enabled_by_Li-Fi_Technology.
3. Deep learning for Network Traffic Monitoring and Analysis / A. Shahraki, A. Mahmoud https://www.researchgate.net/publication/349056451_Deep_learning_for_Network_Traffic_Monitoring_and_Analysis_NTMA_A_survey.
4. The rise of traffic classification in IoT networks [Електронний ресурс] / Hamid Tahaei: https://www.sciencedirect.com/science/article/abs/pii/S1084804520300126.
5. IoT Network Traffic Classification Using Machine Learning Algorithms [Електронний ресурс] / K. Rakesh, S. Mayank: https://ieeexplore.ieee.org/abstract/document/9590566.
6. Toward Designing a Li-Fi-Based Hierarchical IoT Architecture [Електронний ресурс] / L. Albraheem, A. Aljaser – Режим доступу до ресурсу: https://ieeexplore.ieee.org/abstract/document/8413064.
7. Enhancing LiFi for next-generation Internet of things [Електронний ресурс] / J. Linnartz, E. Cunha – Доступу до ресурсу: https://link.springer.com/article/10.1186/s13638-022-02168-6.
8. Романов О.І., Свид І.В., Корнієнко Н.І., Романов А.О. Управління оптичною мережею контролером SDN на базі ONOS//Радіотехніка, № 210, 2022, С.184-192, DOI:10.30837/rt.2022.3.210.16.