УДК 004.056

Ткаченко В.В.
Маліновський В.І.

АНАЛІЗ МЕТОДІВ ОРГАНІЗАЦІЇ І КОНТРОЛЮ ЗАХИСТУ З'ЄДНАНЬ КІНЦЕВИХ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

Вінницький національний технічний університет, Вінниця, Україна

Анотація

У роботі проведено аналіз методів моніторингу захищеності з'єднань кінцевих пристроїв Інтернету речей (IoT). Розглянуто основні загрози на рівнях архітектури IoT: атаки типу «людина посередині», підміна даних і відмова в обслуговуванні. Проаналізовано підходи до забезпечення конфіденційності, цілісності та доступності даних: криптографічне шифрування, протоколи автентифікації та методи виявлення аномалій на основі машинного навчання. Наведено порівняльний аналіз методів за ефективністю, ресурсними вимогами та покриттям вимог безпеки. Визначено перспективи розвитку інтелектуального моніторингу IoT-мереж.

Ключові слова: Інтернет речей; безпека IoT; моніторинг з'єднань; виявлення аномалій; машинне навчання; шифрування даних; конфіденційність; цілісність; доступність.

Abstract

This paper analyzes methods for monitoring the security of connections of Internet of Things (IoT) end devices. The main threats across IoT architecture layers are reviewed, including man-in-the-middle attacks, data substitution, and denial of service. Approaches to ensuring confidentiality, integrity, and availability of data are analyzed, including cryptographic encryption, authentication protocols, and machine learning-based anomaly detection. A comparative analysis of methods is provided according to efficiency, resource requirements, and security coverage. Prospects for intelligent IoT security monitoring are identified.

Keywords: Internet of Things; IoT security; connection monitoring; anomaly detection; machine learning; data encryption; confidentiality; integrity; availability.

Вступ

Інтернет речей (IoT) охоплює дедалі ширше коло пристроїв – від побутової техніки та носимої електроніки до промислових сенсорів і медичного обладнання. Якщо ранні прогнози передбачали понад 30 млрд підключених IoT-пристроїв до 2025 року [1], то реальна кількість у 2025 році склала близько 21 млрд, а до 2030-го очікується понад 40 млрд [2]. Разом із масштабом зростає і кількість атак, що робить захист з'єднань кінцевих пристроїв критично важливим завданням.

Захист IoT-систем спирається на три ключові властивості: конфіденційність (захист від несанкціонованого доступу до даних), цілісність (незмінність даних при передачі) та доступність (безперервне функціонування сервісів). Порушення будь-якої з них несе серйозні ризики – в охороні здоров'я, промисловій автоматизації та управлінні інфраструктурою [3].

Метою даної роботи є аналіз та систематизація методів організації і контролю захисту з'єднань для підвищення захищеності комунікацій пристроїв Інтернету речей. Для досягнення мети вирішуються такі завдання: огляд основних протоколів і загроз безпеці IoT-з'єднань; аналіз криптографічних методів захисту; дослідження підходів до виявлення аномалій; порівняльна оцінка методів.

Результати дослідження

IoT-системи мають трирівневу архітектуру: граничний рівень (Edge) – кінцеві пристрої та сенсори; центральний рівень (Core/Platform) – обробка та маршрутизація даних; рівень представлення (Enterprise/Representation) – корпоративні застосунки та хмарні сервіси [1; 3]. Ключовим з точки зору кібербезпеки є рівень Edge – саме тут підключаються кінцеві пристрої, працюють протоколи IoT і відбуваються атаки на інтерфейси. Переважна більшість кінцевих IoT-пристроїв функціонує на радіоінтерфейсах (Bluetooth, ZigBee, LoRa, LTE), що суттєво розширює поверхню атак і робить захист з'єднань на рівні Edge критично важливим завданням [3].

Для з'єднань кінцевих пристроїв IoT використовується широкий спектр протоколів передачі даних: MQTT, CoAP, AMQP, HTTP/HTTPS – для обміну повідомленнями; LoRa/LoRaWAN, LwM2M, LpWAN – для мереж великого радіусу дії з малим енергоспоживанням; ZigBee, Z-Wave, Bluetooth/BLE, NFC – для мереж малої дальності; WiFi/WiMAX, LTE – для широкосмугового доступу; RFID – для ідентифікації та відстеження [3]. Більшість цих протоколів первісно не проєктувалась із урахуванням

вимог безпеки: MQTT за замовчуванням не шифрує трафік, ZigBee і Bluetooth мають задокументовані вразливості у процедурах з'єднання (pairing). CoAP та LwM2M підтримують захист через DTLS, але налаштування шифрування залишається на розсуд розробника. Відтак безпека з'єднань кінцевих пристроїв визначається не лише вибором протоколу, а й коректністю його захищеного налаштування [3].

На граничному рівні (Edge) поширені атаки «людина посередині» (MitM), підробка ідентичності (spoofing) та атаки відтворення (replay attacks). Вони дозволяють перехоплювати команди керування пристроями та дані сенсорів. DDoS-атаки є особливо небезпечними для мереж із великою кількістю вузлів – вони виснажують ресурси пристроїв і порушують доступність сервісів [3].

На рівні Core/Platform та Enterprise загрозу становлять SQL-ін'єкції, вразливості API та слабка перевірка TLS-сертифікатів. Мобільні застосунки, що взаємодіють із IoT-сенсорами, нерідко є додатковою точкою входу через недостатню автентифікацію [3].

Окрему загрозу становить фізична незахищеність кінцевих пристроїв на рівні Edge: зловмисник може підключитися до вузла у незахищеному середовищі і замінити прошивку або вбудувати шкідливий код [1; 3].

Аналіз основних методів захисту з'єднань кінцевих пристроїв IoT

Симетричне шифрування AES-256 є де-факто стандартом для захисту IoT-трафіку між пристроєм і хмарою. У роботі [4] реалізовано наскрізне шифрування на базі AES-256 у режимі ECB: дані шифруються безпосередньо на IoT-станції до передачі через стільникову мережу. Це унеможливлює читання трафіку навіть при перехопленні MITM. Середня затримка шифрування склала 451 мс – прийнятно для більшості сценаріїв моніторингу. Практичні тести показали стійкість до brute-force, MITM, phishing та DoS [4].

Проте AES незастосовний безпосередньо до ресурсообмежених пристроїв через багатораундове розгортання ключів і складні перетворення. Для таких випадків розроблено AEAD-підхід (Authentication, Encryption and Anomaly Detection) [5]. Шифрування медичних і сенсорних даних побудовано на XOR-кодуванні: час шифрування 0,12 мс проти 0,25 мс у AES і 0,45 мс у RSA. Час дешифрування – 0,10 мс. При цьому конфіденційність забезпечується кодуванням із побітовими зсувами і XOR з бінарним ключем [5].

Автентифікація у AEAD поєднує однонаправлені хеш-функції, XOR і біометрію – зчитування відбитка пальця через нечіткий екстрактор. Це забезпечує захист від вгадування пароля та атак привілейованих інсайдерів. Обчислювальна вартість протоколу – 0,815 мс, тоді як конкурентні рішення потребують 6,7-11,2 мс [5]. Така різниця є критичною для ресурсообмежених вузлів, де витрати на автентифікацію безпосередньо впливають на час відгуку.

Шифрування захищає дані у транзиті, але не виявляє, коли пристрій сам поводиться аномально – надсилає незвичну кількість пакетів, встановлює з'єднання з незнайомими адресами або раптово змінює частоту опитування сенсорів. Саме для цього потрібне виявлення аномалій [1].

Аномалії поділяються на три типи: пунктові (відхилення окремої точки), контекстуальні (відхилення залежно від контексту) та колективні (відхилення групи) [1]. Методи виявлення охоплюють геометричні, статистичні та ML/DL-підходи, що обираються залежно від характеру даних і вимог до затримки.

Серед ML-алгоритмів широко застосовуються KNN, SVM, Random Forest та наївний байєсів класифікатор [3]. SVM добре працює на незбалансованих наборах, де аномалій значно менше за норму. LSTM-мережі ефективно обробляють часові ряди мережевого трафіку, виявляючи зміни у патернах комунікацій, характерні для різних типів атак [3].

У підході AEAD [5] кластеризація K-means спочатку групує медичні дані сенсорів, потім KNN ідентифікує аномальні екземпляри на основі дистанцій і міток класів. SVM без урахування аномалій досяг точності 85,51%; із аномальними зразками – 71,76%. Це демонструє, що ігнорування аномалій суттєво погіршує якість класифікації і підтверджує необхідність їхнього включення до навчальної вибірки [5].

Онлайн-алгоритми обробляють потоки трафіку безперервно – без накопичення повного набору даних. Це єдиний прийнятний варіант для роботи в реальному часі на ресурсообмежених пристроях. Офлайн-методи точніші, але вимагають значно більше пам'яті та обчислювальних ресурсів [1].

Виявити аномалію – лише половина задачі. Потрібна інфраструктура, яка збирає метрики з усіх пристроїв, агрегує їх і реагує на порушення без участі людини [6].

Prometheus збирає метрики у форматі часових рядів через pull-модель; потужна мова запитів PromQL дозволяє виявляти аномальні тренди в з'єднаннях. Програмна платформа моніторингу інфраструктури Zabbix забезпечує комплексний збір метрик та контроль стану мережевих пристроїв і IoT-вузлів. Snort, Suricata і Zeek аналізують мережевий трафік у реальному часі – сигнатурний аналіз у поєднанні з ML дозволяє виявляти атаки, які не мають відомих сигнатур [6]. Для ресурсообмежених

кінцевих пристроїв ключовою технологією є Edge Computing із протоколами MQTT, CoAP і LwM2M: локальна попередня обробка знижує мережеве навантаження і затримки [6].

Математична модель моніторингу гетерогенних мереж описує IoT-систему як граф:

$$G \in \{V; E\}, \quad (1)$$

де V – множина вузлів {пристрої, сенсори, сервери}, E – множина з'язків між ними {фізичні або логічні канали}. Стан кожного вузла описується вектором-функцією метрик:

$$M_i(t) = f[CPU_i(t), MEM_i(t), NET_i(t), IO_i(t)], \quad (2)$$

де $M_i(t)$ – вектор-функція показників продуктивності вузла v_i у момент часу t; $CPU_i(t)$ – завантаження процесора (% використання); $MEM_i(t)$ – використання оперативної пам'яті; $NET_i(t)$ – мережевий трафік (вхідний/вихідний); $IO_i(t)$ – швидкість дискових операцій введення/виведення. Усі метрики нормалізуються до діапазону [0, 1] для уніфікованого аналізу. Аномалія виявляється або пороговою евристикою (перевищення граничного значення θ_k), або ML-моделлю – автоенкодером, що порівнює реальні метрики з прогнозованими [6].

Наскрізне шифрування є обов'язковою умовою: без нього зловмисник може перехопити та маніпулювати телеметрією під час передачі від IoT-станції до хмари [4]. Практичні тести показали пропускну здатність до 200 пакетів/с при смузі 2,7 кбіт/с [4]. Разом з тим одна з реальних загроз у каналах IoT – навмисне або автоматичне вимкнення шифрування: захист є високим, коли шифрування і автентифікація активовані, проте за їх відсутності він фактично зникає. Тому обов'язковою складовою є постійний моніторинг стану шифрування та автентифікації на кожному вузлі граничного рівня (Edge).

Таблиця 1 – Порівняльний аналіз методів організації та контролю захисту з'єднань IoT

Метод / підхід	Конфіден-ційність	Цілісність	Виявлення аномалій	Ресурсні вимоги
Контроль AES-256 шифрування [4]	Так	Частково	Ні	Середні
Контроль цілісності (XOR-кодування AEAD)[5]	Так	Так (з MAC)	Ні	Низькі
Машинне навчання (ML/DL) [3]	Ні	Ні	Так	Високі
Статистичний аналіз [1]	Ні	Ні	Частково	Низькі
Комплексний контроль AEAD (хеш+XOR+KNN) [5]	Так	Так	Так	Середні
Prometheus / Zabbix [6]	Частково	Так	Частково	Середні

Висновки

Аналіз показав, що жоден окремий метод не покриває всіх вимог CIA. AES-256 забезпечує конфіденційність, але непридатний для сильно ресурсообмежених вузлів. XOR-кодування з хешем дає прийнятний захист при мінімальних витратах. ML-методи (SVM, KNN, LSTM) ефективно виявляють аномалії, але потребують обчислювальних ресурсів граничного вузла або сервера.

Підхід AEAD [5] є найближчим до практичного балансу: автентифікація, XOR-шифрування та кластерно-класифікаційне виявлення аномалій в одному легковагому рішенні. Системи контролю реального часу (Prometheus, Snort) у поєднанні з Edge Computing формують ефективну інфраструктуру безпеки IoT. Перспективним напрямом є стандартизація захищеного налаштування протоколів IoT (MQTT over TLS, CoAP+DTLS, захищений LoRaWAN) та впровадження інтелектуального контролю з'єднань на граничному (Edge) рівні.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Марченко Р.М., Коваленко А.А., Знайдюк В.Г. Аналіз методів виявлення аномального трафіку в мережах IoT. Системи управління, навігації та зв'язку. 2024. № 1. С. 133-136. DOI: 10.26906/SUNZ.2024.1.133.
2. IoT Analytics. Number of connected IoT devices growing 14% to 21.1 billion globally in 2025. 2025. URL: https://iot-analytics.com/number-connected-iot-devices/ (дата звернення: 10.03.2026).
3. Mazhar T., Talpur D.B., Shloul T.A., Ghadi Y.Y., Haq I., Ullah I., Ouahada K., Hamam H. Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence. Brain Sciences. 2023. Vol. 13, No. 683. DOI: 10.3390/brainsci13040683.
4. Saleem K., Zinou M.F., Mohammad F., Ouni R., Elhendi A.Z., Almuhtadi J. End-to-end security enabled intelligent remote IoT monitoring system. Frontiers in Physics. 2024. Vol. 12, Article 1357209. DOI: 10.3389/fphy.2024.1357209.
5. Song L., Lan H., Du J., Wang K., Kang W. Application of intelligent Internet of Things technology in the security monitoring system of power Internet of Things network. Discover Internet of Things. 2025. Vol. 5, Article 44. DOI: 10.1007/s43926-025-00107-7.
6. Жебка В.В. Інформаційні технології моніторингу гетерогенних мереж в режимі реального часу. Кібербезпека: освіта, наука, техніка. 2025. № 3(27). С. 591-603. DOI: 10.28925/2663-4023.2025.27.787.

Ткаченко Владислав Вікторович – студент групи 2БС-22б, кафедра захисту інформації, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця.

Науковий керівник: ***Маліновський Вадим Ігорович*** – к.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця.

Vladyslav Tkachenko – student of group 2BS-22b, Department of Data Protection, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

Scientific supervisor: ***Malinovskyi Vadim Igorovich*** – PhD, Associate Professor, Department of Data Protection, Vinnytsia National Technical University, Vinnytsia.