УДК 004.056

ОРГАНІЗАЦІЯ ЗАХИСТУ ВІД АТАК НА РІВНІ ПРОТОКОЛІВ IOT

Месевра О. О.
github853@gmail.com
Черкаський державний фаховий бізнес-коледж
Ратайчук П. Є.
м. Черкаси, Україна

Стрімкий розвиток та глобальне впровадження технологій Інтернету речей (IoT) у сучасні інфраструктурні рішення, починаючи від систем «розумного дому» і закінчуючи масштабними комплексами промислового Інтернету речей (IoT), вимагає розробки та впровадження принципово нових, надійних механізмів безпеки. Архітектура таких систем має свої специфічні особливості побудови: більшість кінцевих вузлів характеризуються вкрай обмеженими обчислювальними ресурсами, малим обсягом оперативної пам'яті та низьким рівнем енергоспоживання. Через ці апаратні обмеження використання традиційних, ресурсоємних мережевих протоколів та важких криптографічних алгоритмів стає неефективним або взагалі неможливим.

Саме тому основними стандартизованими протоколами прикладного рівня для взаємодії IoT-пристроїв на сьогодні є MQTT (Message Queuing Telemetry Transport) та CoAP (Constrained Application Protocol). Протокол MQTT функціонує на базі архітектури «публікація-підписка» (Publish-Subscribe) і використовує центральний вузол зв'язку – брокер, що дозволяє асинхронно обмінюватися повідомленнями між пристроями. Своєю чергою, протокол CoAP побудований за REST-архітектурою і працює поверх протоколу UDP, що мінімізує накладні витрати на встановлення з'єднання та робить його ідеальним для нестабільних мереж. Однак, незважаючи на їхню високу ефективність та оптимізованість для роботи в умовах обмежених ресурсів, базові специфікації цих протоколів часто не мають вбудованих суворих механізмів шифрування за замовчуванням, що робить їх вразливими до широкого спектра мережевих атак.

Актуальність даного дослідження зумовлена гострою необхідністю детального аналізу та класифікації векторів кібератак на рівні прикладних

протоколів IoT для подальшої розробки комплексних та дієвих систем захисту. Особливої уваги під час проєктування безпечних IoT-мереж потребують атаки типу відмови в обслуговуванні (DoS/DDoS), перехоплення та модифікації даних (Man-in-the-Middle), а також атаки, що базуються на повторній передачі повідомлень (Replay-атаки).

Теоретичний аналіз показує, що атака типу відмови в обслуговуванні (DoS) у середовищі MQTT найчастіше реалізується шляхом генерації зловмисником надлишкової кількості запитів на підключення до брокера (Connection Flooding) або масової публікації повідомлень у певні топіки. Це призводить до критичного вичерпання ресурсів брокера (завантаження процесора, переповнення оперативної пам'яті), внаслідок чого він втрачає здатність обробляти легітимні запити від авторизованих сенсорів чи контролерів. Виявити таку аномалію можливо за допомогою систем моніторингу мережі, які фіксують різке зростання кількості вхідних пакетів із певних IP-адрес, а також стрімке збільшення затримки відповіді сервера.

Не менш небезпечними є атаки типу Man-in-the-Middle (MITM). Оскільки базові версії MQTT та CoAP можуть передавати дані у відкритому вигляді (Plaintext), зловмисник, що знаходиться в одній мережі з пристроями, здатний перехоплювати телеметрію. MITM-атаки дозволяють зловмиснику не лише пасивно читати конфіденційні дані, а й активно модифікувати їх перед доставкою брокеру або клієнту, що може призвести до хибного спрацьовування виконавчих механізмів в IoT-системі.

Replay-атаки (повторна передача повідомлень) спрямовані на перехоплення валідних, вже сформованих пакетів управління та їхню подальшу багаторазову відправку в мережу. Зловмисник імітує дії авторизованого клієнта, що є критичною вразливістю для систем, де не реалізовано належне шифрування, не використовуються часові мітки (timestamps) або унікальні ідентифікатори сесій. Визначення та виявлення цих загроз передбачає глибокий інспекційний аналіз мережевого трафіку (Deep Packet Inspection), пошук дубльованих

послідовностей пакетів та моніторинг аномалій у часових інтервалах надходження повідомлень.

У рамках подальшого практичного дослідження планується розробка та розгортання віртуального тестового середовища для моделювання вищезазначених векторів атак на протоколи MQTT та CoAP. Головним завданням практичної частини стане дослідження та фіксація ключових мережевих і системних параметрів. Зокрема, будуть аналізуватися такі метрики: затримка передачі повідомлень (Latency), відсоток втрат мережевих пакетів (Packet Loss Rate), загальна пропускна здатність каналу (Throughput), а також рівень навантаження на обчислювальні ресурси мережевих вузлів (використання CPU та RAM) під час штатної роботи та в умовах активної кібератаки. Для детального аналізу структури перехоплених пакетів та виявлення вразливостей застосовуватимуться спеціалізовані засоби мережевого моніторингу та аналізатори трафіку, такі як Wireshark.

Додатково планується дослідити ефективність впливу криптографічних протоколів TLS для MQTT та DTLS для CoAP на загальну продуктивність мережі. Буде проведено порівняльний аналіз швидкодії системи до та після впровадження механізмів парольної аутентифікації та списків контролю доступу (ACL), які виступають базовими методами протидії несанкціонованому доступу. Комплексний аналіз цих параметрів дозволить сформувати обґрунтовані рекомендації щодо організації безпеки в IoT-системах, збалансувавши рівень захисту з допустимими втратами продуктивності.

Список використаних джерел:

1. Banks A., Gupta R. MQTT Version 5.0. *OASIS Standard*. 2019. URL: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html (дата звернення: 25.02.2026).
2. Shelby Z., Hartke K., Bormann C. The Constrained Application Protocol (CoAP). *Internet Engineering Task Force (IETF), RFC 7252*. 2014. URL: https://datatracker.ietf.org/doc/html/rfc7252 (дата звернення: 01.03.2026).

3. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. *Internet Engineering Task Force (IETF), RFC 8446*. 2018. URL: https://datatracker.ietf.org/doc/html/rfc8446 (дата звернення: 02.03.2026).
4. Rescorla E., Tschofenig H., Modadugu N. Datagram Transport Layer Security Version 1.2. *Internet Engineering Task Force (IETF), RFC 6347*. 2012. URL: https://datatracker.ietf.org/doc/html/rfc6347 (дата звернення: 02.03.2026).
5. Eclipse Mosquitto: An open source MQTT broker. *Eclipse Foundation*. URL: https://mosquitto.org/ (дата звернення: 05.03.2026).
6. Docker Security. *Docker Documentation*. URL: https://docs.docker.com/engine/security/ (дата звернення: 06.03.2026).
7. Wireshark User's Guide. *Wireshark Foundation*. URL: https://www.wireshark.org/docs/wsug_html_chunked/ (дата звернення: 09.03.2026).

УДК 004.946

ВИКОРИСТАННЯ ДОПОВНЕНОЇ РЕАЛЬНОСТІ У МЕДИЦИНІ: ВІД ДІАГНОСТИКИ ДО ОПЕРАЦІЙ

Левандовський Д. О.
Levandovskijsenis2@gmail.com
Черкаський державний фаховий бізнес-коледж
Люта М. В.
м. Черкаси, Україна

Доповнена реальність (AR) є сучасною технологією, що поєднує реальне середовище з віртуальними об'єктами шляхом накладання цифрової інформації (зображень, 3D-моделей, тексту) в режимі реального часу [1]. У медичній галузі застосування AR відкриває нові можливості для підвищення точності діагностики, удосконалення підготовки медичного персоналу та оптимізації хірургічних втручань [2].

З огляду на зростання вимог до якості медичних послуг і безпеки пацієнтів, впровадження інноваційних технологій, зокрема доповненої реальності, набуває особливої актуальності [3].