УДК 004.056:004.738.5

В. І. Селезньов

КРИПТОГРАФІЧНІ МЕХАНІЗМИ ЗАХИСТУ ПРОТОКОЛУ MQTT В IOT-СИСТЕМАХ

Вінницький національний технічний університет

Анотація

У роботі проаналізовано основні криптографічні механізми захисту протоколу MQTT у системах Інтернету речей. Розглянуто актуальні вектори атак на MQTT-комунікації, особливості використання TLS та застосування малоресурсної криптографії для пристроїв з обмеженими апаратними ресурсами. Окрему увагу приділено алгоритму ASCON та проблемі управління криптографічними ключами в MQTT-мережах.

Ключові слова: MQTT, Інтернет речей, малоресурсна криптографія, TLS, ASCON, IoT-безпека.

Abstract

These theses analyze the main cryptographic protection mechanisms for the MQTT protocol in Internet of Things systems. Current attack vectors against MQTT communications, TLS applicability, and the use of lightweight cryptography for resource-constrained devices are considered. Particular attention is paid to the ASCON algorithm and the problem of cryptographic key management in MQTT networks.

Keywords: MQTT, Internet of Things, lightweight cryptography, TLS, ASCON, IoT security.

Вступ

Протокол MQTT (Message Queuing Telemetry Transport) є одним із найбільш поширених протоколів передачі телеметричних даних у системах Інтернету речей. Популярність MQTT пояснюється невеликим службовим навантаженням, мінімальним розміром заголовка та використанням моделі publish/subscribe [1]. Протокол широко застосовується у smart-пристроях, системах моніторингу, Industrial IoT та сенсорних мережах. Водночас базова специфікація MQTT не містить обов'язкових механізмів криптографічного захисту, через що безпека значною мірою переноситься на транспортний або прикладний рівень.

Проблема ускладнюється апаратними особливостями більшості IoT-вузлів. Значна частина пристроїв використовує малопотужні мікроконтролери з обмеженим обсягом оперативної пам'яті та низьким енергоспоживанням. У таких умовах використання класичних криптографічних протоколів створює додаткове навантаження на процесор, пам'ять і канал передачі даних [2]. Метою роботи є аналіз сучасних механізмів криптографічного захисту MQTT та визначення особливостей їх застосування для різних класів IoT-пристроїв.

Результати дослідження

Однією з основних проблем MQTT є відсутність шифрування за замовчуванням при використанні стандартного порту 1883. Це дозволяє виконувати перехоплення трафіку, replay-атаки, підміну повідомлень та несанкціоновану підписку на MQTT-топіки з використанням wildcard-символів [2]. Брокер повідомлень є єдиною точкою концентрації всього трафіку мережі, що робить його першочерговою ціллю для зловмисника. У промислових IoT-системах компрометація телеметричних даних може впливати не лише на інформаційну безпеку, а й безпосередньо на функціонування технологічних процесів, що суттєво підвищує критичність захисту на цьому рівні.

Найбільш поширеним механізмом захисту MQTT-комунікацій є використання TLS. Протокол TLS забезпечує шифрування транспортного каналу та автентифікацію брокера, а у випадку mutual TLS – також автентифікацію клієнта. Використання TLS 1.3 дозволило зменшити накладні витрати порівняно з TLS 1.2 завдяки скороченню процедури встановлення з'єднання з 2-RTT до 1-RTT та виключенню застарілих шифронаборів. На платформах типу ESP32 або STM32 застосування TLS є практи-

чно доцільним, однак для 8-бітних мікроконтролерів або пристроїв із малим обсягом RAM реалізація повного TLS-стеку часто є технічно надлишковою або неможливою без спеціалізованих криптоспівпроцесорів [3].

У зв'язку з цим для IoT-систем активно розвивається напрям малоресурсної криптографії. Основною метою таких алгоритмів є забезпечення криптографічного захисту при мінімальних витратах апаратних ресурсів. Одним із найбільш відомих рішень є алгоритм ASCON, який у 2023 році був стандартизований NIST як переможець Lightweight Cryptography Standardization Process [4]. Алгоритм підтримує режим authenticated encryption with associated data (AEAD), що дозволяє одночасно забезпечити конфіденційність і цілісність повідомлення, та характеризується компактною програмною реалізацією, що робить його придатним для широкого класу IoT-платформ.

У випадках, коли використання повного TLS-захисту є недоцільним, шифрування може виконуватись безпосередньо на рівні MQTT payload. Для цього можуть використовуватись ASCON-128, ChaCha20-Poly1305 та інші малоресурсні алгоритми [5]. Для забезпечення цілісності окремих повідомлень без повного шифрування застосовуються MAC-коди та хеш-функції. Такий підхід дозволяє гнучко налаштовувати рівень захисту залежно від можливостей конкретного пристрою та вимог системи.

Окремою проблемою залишається управління криптографічними ключами в масштабованих MQTT-мережах. Використання статичних Pre-Shared Keys спрощує реалізацію, однак унеможливлює властивість forward secrecy та створює труднощі при оновленні ключів і масштабуванні мережі. У сучасних дослідженнях пропонуються малоресурсні протоколи обміну ключами, орієнтовані на IoT-пристрої з обмеженими обчислювальними можливостями. Зокрема, Kaganurmath et al. запропонували протокол DLKS-MQTT, що використовує nonce-значення для протидії replay-атакам при встановленні сеансових ключів без повноцінного асиметричного обміну на стороні клієнта [6].

Висновки

Протокол MQTT не містить вбудованих механізмів криптографічного захисту, тому безпечна передача даних у IoT-системах потребує використання додаткових засобів шифрування та автентифікації. Для IoT-пристроїв із достатніми апаратними ресурсами ефективним рішенням є використання TLS 1.3 та mutual TLS, тоді як для пристроїв з обмеженими апаратними ресурсами більш доцільним є застосування малоресурсної криптографії та шифрування на рівні MQTT payload.

Стандартизація алгоритму ASCON з боку NIST підтверджує актуальність використання малоресурсної криптографії в IoT-системах. Для MQTT-середовища перспективним є поєднання TLS-захисту та малоресурсних алгоритмів шифрування залежно від апаратних можливостей пристроїв. Окремою проблемою залишається безпечне управління криптографічними ключами в масштабованих IoT-мережах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. MQTT Version 5.0. OASIS Standard. 2019. URL: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html (дата звернення: 16.05.2026).

2. Bashir A., Hussain Mir A. Securing Communication in MQTT enabled Internet of Things with Lightweight security protocol. *EAI Endorsed Transactions on Internet of Things*. 2018. Т. 3, № 12. С. 154390. URL: https://doi.org/10.4108/eai.6-4-2018.154390 (дата звернення: 16.05.2026).

3. Winarno A., Sari R. F. A Novel Secure End-to-End IoT Communication Scheme Using Lightweight Cryptography Based on Block Cipher. *Applied Sciences*. 2022. Т. 12, № 17. С. 8817. URL: https://doi.org/10.3390/app12178817 (дата звернення: 15.05.2026).

4. National Institute of Standards and Technology. Lightweight Cryptography Standardization Process: NIST Selects Ascon. 2023. URL: https://csrc.nist.gov/Projects/lightweight-cryptography (дата звернення: 15.05.2026).

5. Thakor V. A., Razzaque M. A., Khandaker M. R. A. Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. *IEEE Access*. 2021. Т. 9. С. 28177–28193. URL: https://doi.org/10.1109/access.2021.3052867 (дата звернення: 15.05.2026).

6. Kaganurmath S., Cholli N. G., Anala M. R. DLKS-MQTT: A Lightweight Key Sharing Protocol for Secure IoT Communications. *Engineering, Technology & Applied Science Research*. 2025. Т. 15, № 2. С. 21532–21538. URL: https://doi.org/10.48084/etasr.10216 (дата звернення: 15.05.2026).

Селезньов Віталій Ігорович — асистент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: seleznov.vitalii@gmail.com

Seleznov Vitalii — Assistant of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, email: seleznov.vitalii@gmail.com