УДК 004.738.5:004.77:004.056
А. Станько, доктор філософії; С. Козак; С. Кульчицький
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАХИЩЕНА ТЕЛЕМЕТРІЯ В IOT: ПОРІВНЯЛЬНИЙ АНАЛІЗ MQTT OVER TLS, HTTPS ТА COAP/DTLS ДЛЯ ДОМАШНІХ І ПРОМИСЛОВИХ ЗАСТОСУВАНЬ

UDC 004.738.5:004.77:004.056
A. Stanko, PhD.; S. Kozak; S. Kulchytskyi

SECURE TELEMETRY IN THE IOT: A COMPARATIVE ANALYSIS OF MQTT OVER TLS, HTTPS AND COAP/DTLS FOR HOME AND INDUSTRIAL APPLICATIONS

Захищена телеметрія є критичною для IoT, оскільки вимірювання (температура, енергоспоживання, вібрація, стани виконавчих механізмів) впливають на автоматизовані рішення та безпеку. У домашніх сценаріях зазвичай домінують вимоги простоти інтеграції й стабільності в Wi-Fi мережах, тоді як у промислових (IIoT) – прогнозованість затримок, відмовостійкість, керованість доступу та узгодженість із політиками ІБ підприємства. У роботі розглянуто три підходи до захищеної доставки телеметрії: MQTT over TLS, HTTPS і CoAP/DTLS, із фокусом на практичну придатність у двох середовищах.

MQTT over TLS поєднує модель publish/subscribe з брокером, що спрощує масштабування під багато споживачів даних та підтримує QoS для подій і тривог [1]. TLS забезпечує конфіденційність, цілісність і автентифікацію каналу, однак додає накладні витрати на встановлення сесії й потребує організованого життєвого циклу сертифікатів. У «розумному домі» MQTT/TLS є практичним для безперервної телеметрії та автоматизацій, особливо за наявності локального брокера/шлюзу. В IIoT він доцільний у централізованих архітектурах збору, але вимагає суворих ACL, сегментації та моніторингу доступів.

HTTPS (HTTP поверх TLS) є зручним завдяки універсальній підтримці веб-екосистемою та простій інтеграції з API, мобільними застосунками й хмарними сервісами. Це робить його придатним для пакетної телеметрії, керувальних запитів, конфігурацій і службових операцій. Водночас модель запит/відповідь і службові накладні витрати можуть бути неефективними для дуже частих коротких повідомлень із сенсорів, особливо на обмежених вузлах. Тому в домі HTTPS часто виступає «найпростішим транспортом» для інтеграцій, а в IIoT – радше протоколом інтеграційного рівня, ніж «польовим» протоколом.

CoAP/DTLS орієнтований на обмежені пристрої: працює поверх UDP, має компактні повідомлення та REST-подібну модель, що знижує витрати на передачу й обробку [2]. DTLS додає криптографічний захист для датаграм, однак може ускладнювати роботу через NAT/фаєрволи і потребує коректно налаштованих проксі/шлюзів для взаємодії з IT-контуром. У домашньому середовищі CoAP/DTLS доцільний для батарейних сенсорів і низькопотужних сегментів (через шлюз), а в IIoT – для щільних сенсорних мереж, де критичні мінімальні накладні витрати й стійкість до втрат пакетів.

Вибір протоколу доцільно здійснювати за критеріями: накладні витрати на захищену сесію, ефективність для малих повідомлень, енергоспоживання, керованість ключів/сертифікатів, вимоги до QoS, а також архітектурні ризики (зокрема роль брокера як потенційної точки концентрації). Узагальнено, MQTT over TLS є оптимальним для подієвої/потокової телеметрії з багатьма підписниками та QoS; HTTPS – для інтеграцій і керування в веб-інфраструктурі; CoAP/DTLS – для обмежених вузлів і низькопотужних мереж, де важлива «легкість» протоколу [1–3].

Література

1. OASIS. (2019). MQTT Version 5.0. OASIS Standard.
2. Shelby, Z., Hartke, K., & Bormann, C. (2014). The Constrained Application Protocol (CoAP) (RFC 7252). IETF.
3. Dizdarević, J., Carpio, F., Jukan, A., & Masip-Bruin, X. (2018). A survey of communication protocols for Internet of Things and related challenges of fog and cloud computing integration. ACM Computing Surveys, 51(6).