УДК 004.7:004.9

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ ПРОТОКОЛІВ MQTT ТА HTTP У IOT-СИСТЕМАХ

Сайко В.В.
vsa.st01@outlook.com
Черкаський державний фаховий бізнес-коледж
Люта М. В.
м. Черкаси, Україна

Сучасний етап розвитку інформаційних технологій характеризується стрімкою цифровізацією та впровадженням систем Інтернету речей (IoT) у промисловість, енергетику та побутову сферу. Як показують дослідження сучасних тенденцій у галузі інформаційних технологій, ефективність таких систем критично залежить від стабільності обміну даними між кінцевими вузлами та центральними серверами. Вузли моніторингу часто будуються на базі малопотужних мікроконтролерів (ESP32 чи STM32), тож вибір мережевого протоколу стає визначальним фактором їхньої надійності та автономності.

Протокол HTTP є найпопулярнішим методом передачі даних у веб-середовищі. Але його значний недолік – високі накладні витрати. Кожен запит вимагає встановлення нового TCP з'єднання або підтримки механізму сесій, а обсяг текстових заголовків запитів може складати до 800 байтів навіть при передачі одного числового значення [1]. В мережах з сотнями пристроїв це призводить до навантаження на канали зв'язку, що зменшує автономність роботи пристроїв.

Альтернативнм рішенням є протокол MQTT (Message Queuing Telemetry Transport), який з самого початку розроблявся для умов з низькою пропускною здатністю. Замість моделі «запит-відповідь» в HTTP, MQTT використовує модель «видавець-підписник». Взаємодія проходить через брокер – центральний вузол, який керує потоками повідомлень. Така модель дозволяє пристроям більшу частину часу перебувати в режимі очікування, це дуже важливо для енергоефективності [2]. Одна з найбільших переваг MQTT – його бінарна структура. Заголовок пакета має розмір 2 байти, що в рази менше, ніж у

звичайного HTTP-заголовка. Порівняння показує, що при відправці повідомлення обсягом 10 байтів, загальний пакет даних у MQTT буде в 10–12 разів меншим, ніж у HTTP.

Для стабільного моніторингу в реальних умовах MQTT покладається на QoS (Quality of Service). Рівень «QoS 1» гарантує доставку повідомлення хоча б один раз, що важливо для точного збору телеметрії. Важливим моментом є контроль технічного стану самих IoT-пристроїв. Тут MQTT пропонує свій механізм «Last Will and Testament». Коли пристрій раптово втрачає зв'язок через розряд батареї або технічний збій, брокер розсилає повідомлення про його відключення всім учасникам мережі. Щоб реалізувати такий функціонал в протоколі HTTP потрібно постійно опитувати пристрій (polling), створюючи надлишковий трафік та неефективні витрати енергії [3].

Ще одним важливим пунктом є безпека передачі даних. В HTTP, кожен запит може виконувати ресурсоємну процедуру TLS-рукостискання (handshake), в свою чергу MQTT встановлює зашифроване з’єднання один раз і підтримує його тривалий час. Протокол MQTT значну перевагу з архітектурою «Zero Trust» (нульової довіри). Брокер реалізує чітке розмежування мережі, де кожен датчик має права доступу лише до відповідних топіків, що робить неможливим подальше просування зловмисника у разі компрометації одного з вузлів. HTTP передає складні токени авторизації у кожному заголовку, що збільшує обсяг трафіку, навантаження на пристрій та вразливість до атак типу DoS через обмеженість ресурсів.

Отже, протокол MQTT є набагато ефективнішим за HTTP для систем IoT, яким потрібна висока стабільність та енергоефективність. Його використання зменшує обсяг трафіку на 80-90%, забезпечує гарантовану і захищену доставку повідомлень, збільшує автономність та дає можливість контролювати стан пристроїв у реальному часі.

Список використаних джерел:

1. RFC 7230: hypertext transfer protocol (HTTP/1.1): message syntax and routing. IETF Datatracker. URL: https://datatracker.ietf.org/doc/html/rfc7230 (дата звернення: 24.03.2026).
2. MQTT version 3.1.1. OASIS standard. URL: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html (дата звернення: 24.03.2026).
3. IoT fundamentals: networking technologies, protocols, and use cases for the internet of things. Cisco Press: Source for Cisco Technology. URL: https://www.ciscopress.com/store/iot-fundamentals-networking-technologies-protocols-9781587144561 (дата звернення: 24.03.2026).

УДК 004.8:336.7

ВИЯВЛЕННЯ ФІНАНСОВОГО ШАХРАЙСТВА У ЦИФРОВИХ ПЛАТІЖНИХ СИСТЕМАХ ІЗ ВИКОРИСТАННЯМ СУЧАСНИХ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Печерський Є.В.
yegor.141231@gmail.com
Черкаський державний фаховий бізнес-коледж
Марченко С. В.
м.Черкаси, Україна

Інтенсивна цифровізація фінансових сервісів, розвиток електронної комерції та мобільних платіжних платформ спричинили суттєве збільшення обсягів транзакційних потоків і водночас ускладнення шахрайських схем. Сучасні фінансові екосистеми характеризуються високою динамікою поведінкових патернів користувачів, мережевою природою взаємодій та значною нерівномірністю розподілу класів. За таких умов традиційні підходи на основі правил та класичні статистичні методи демонструють обмежену здатність до адаптації й своєчасного виявлення нових типів фінансових загроз.

Останні дослідження показують, що ефективність протидії шахрайству визначається не лише точністю класифікації транзакцій, але й здатністю систем аналізувати часову еволюцію фінансових взаємодій, враховувати мережеву