

ТЕХНОЛОГІЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ В ІОТ-СИСТЕМАХ

Згурська А.В.

e-mail: anastasiia.zghurska@nure.ua

Науковий керівник – д.т.н., доц. Чала О.В.

e-mail: oksana.chala@nure.ua

Харківський національний університет радіоелектроніки, каф. ІСТ
м. Харків, Україна

This paper explores the core data transmission and communication technologies utilized in modern Internet of Things (IoT) systems. It analyzes lightweight protocols such as MQTT and CoAP, alongside wireless communication standards including Wi-Fi, Bluetooth Low Energy (BLE), and LoRaWAN. The research highlights the critical balance between power consumption, data transfer rates, and range, particularly when implementing these technologies on popular embedded platforms and microcontrollers. Effective selection of communication architectures ensures the reliability, security, and scalability of distributed embedded IoT networks in real-time applications.

Швидке зростання Інтернету речей (Internet of Things, IoT) зробило технології передачі інформації ключовими для продуктивності, масштабованості та безпеки систем. Мільярди пристроїв з обмеженими ресурсами нині обмінюються даними через різноманітні дротові та бездротові мережі, генеруючи величезні потоки даних від периферії до хмари. Тому вибір та інтеграція відповідних технологій передачі є критично важливими для задоволення вимог додатків щодо затримки, надійності, енергоефективності та захисту конфіденційних даних.

Зв'язок в IoT зазвичай структурований у вигляді багаторівневих архітектур, які розділяють функції сприйняття, мережі та додатків. На рівні сприйняття датчики та виконавчі механізми генерують сирі дані, часто за суворих обмежень щодо потужності, пам'яті та обчислювальних можливостей. Зокрема, при реалізації кінцевих вузлів на базі мікроконтролерів (наприклад, архітектури STM32 або платформ Arduino), цей обмежений обсяг оперативної пам'яті створює жорсткі вимоги до низькорівневого програмування (C/C++). Це особливо критично під час оптимізації виділення пам'яті під мережеві буфери (наприклад, оптимізація розміру буферних масивів для обробки та передачі пакетів даних). Мережний рівень забезпечує підключення через короткодіючі мережі (наприклад, ZigBee, Bluetooth Low Energy (BLE), Wi-Fi), далекодіючі глобальні мережі з низьким енергоспоживанням (LPWAN, такі як NB-IoT, LoRa, Sigfox, Weightless) або стільникові системи 4G/5G. Прикладний рівень спирається на легкі протоколи обміну повідомленнями (MQTT, CoAP, AMQP, HTTP, DDS, XMPP, WebSockets) для доставки даних і команд між пристроями, шлюзами та

хмарними або периферійними службами. Парадигми периферійних і хмарних обчислень лежать в основі зберігання та великомасштабної аналітики, одночасно розвантажуючи обмежені кінцеві пристрої.

Бездротові технології, що використовуються в IoT, утворюють кілька основних класів, які відрізняються дальністю дії, швидкістю передачі даних, енергетичним профілем і частотним діапазоном. Короткодіючі рішення для персональних/локальних мереж, такі як IEEE 802.15.4 (ZigBee, 6LoWPAN), BLE, Wi-Fi та RFID/NFC, підтримують зв'язок усередині будівель з різними компромісами між пропускну здатністю, енергоспоживанням і вартістю. ZigBee та BLE орієнтовані на малопотужні сенсорні мережі з низькою швидкістю передачі даних, тоді як Wi-Fi пропонує вищу пропускну здатність за вищих витрат енергії. Технології LPWAN, включаючи NB-IoT, LoRa, Sigfox і Weightless, розширюють покриття на багато кілометрів, мінімізуючи енергоспоживання та складність пристроїв за рахунок низьких швидкостей передачі даних і невеликих обсягів корисного навантаження.

Порівняльні аналізи підкреслюють, що жодна технологія не є універсально оптимальною; натомість вибір технології повинен відповідати моделям трафіку, необхідній якості обслуговування, щільності розгортання та цільовим показникам часу автономної роботи. Промисловий IoT і додатки управління в реальному часі створюють додаткове навантаження на технології передачі, поєднуючи у спільних мережах різномірний трафік – повідомлення систем жорсткого реального часу, чутливу до часу телеметрію та дані з доставкою за можливості (best-effort). Огляди показують, що детерміновані розширення Ethernet і мережі, чутливі до часу (TSN), а також функції ультранадійного зв'язку з низькою затримкою (URLLC) в 5G, є ключовими для забезпечення суворих часових гарантій, проте стандартизація та довіра до поведінки бездротових мереж у реальному часі залишаються відкритими питаннями.

Поверх каналних технологій, протоколи обміну повідомленнями прикладного рівня визначають, як інформація рухається в системах IoT. MQTT – це легкий протокол «видавець-підписник», який широко розповсюджений завдяки низьким накладним витратам, маршрутизації на основі тем та підтримці ненадійних мереж, що робить його придатним для пристроїв з обмеженими ресурсами та хмаро-орієнтованих архітектур. На практиці така архітектурна модель є високоефективною для систем автоматизації. Зокрема, при проєктуванні та функціональному моделюванні (наприклад, з використанням методології IDEF0 для побудови діаграм вузлів) комплексу «Розумний будинок», саме MQTT дозволяє забезпечити необхідну безперервну синхронізацію станів усіх пристроїв у реальному часі. CoAP використовує архітектурний стиль REST поверх UDP і адаптований до обмежених середовищ та проксіювання до HTTP, що забезпечує безшовну інтеграцію з веб-сервісами. HTTP, AMQP, DDS і XMPP задовольняють

більш складні потреби обміну повідомленнями, включаючи схему «запит-відповідь», потокову передачу та розповсюдження в реальному часі в промислових або мультимедійних середовищах.

Передача інформації в IoT піддається різноманітним загрозам через відкриті канали, різноманітні пристрої та велику площу для атак. Основні цілі безпеки включають конфіденційність, цілісність, автентифікацію, доступність та приватність в умовах обмежених ресурсів. Аналіз систем управління IoT виявляє вразливості на рівнях доступу, передачі та стабільності затримок; небезпечний контроль доступу, слабкий захист каналу та маніпуляції з часом можуть поставити під загрозу поведінку системи.

Окрім традиційної криптографії, нові схеми інтегрують компресійне зондування та методи на основі хаосу для одночасного стиснення, шифрування та вибіркового приховування критичної інформації. Методи на основі напівтензорного добутку компресійного зондування (STP-CS) можуть запропонувати багаторівневу реконструкцію, дозволяючи отримувачам з різними рівнями авторизації одержувати різні уявлення про ті самі передані дані, таким чином підтримуючи збереження приватності при передачі в сценаріях IoT. На системному рівні архітектури, що використовують хмарні фреймворки безпечної передачі даних, програмно-конфігуровані мережі (SDN) та ізоляцію мереж, спрямовані на максимальне використання надійних комунікаційних ресурсів при забезпеченні політик безпеки.

Аналіз показав, що ефективність IoT-систем залежить від балансу між енергоспоживанням і вибором протоколів. Реалізація на базі STM32 або Arduino потребує оптимізації пам'яті під мережеві буфери. Використання IDEF0 та MQTT забезпечує синхронізацію пристроїв «Розумного будинку» в реальному часі. Для захисту даних перспективним є застосування методів компресійного зондування.

Список використаних джерел:

1. Cirani S., Ferrari G., Picone M., Veltri L. Internet of Things: Architectures, Protocols and Standards. John Wiley & Sons, 2019. URL: <https://onlinelibrary.wiley.com/doi/book/10.1002/9781119359715>
2. Kumar N., Jamwal P. Analysis of Modern Communication Protocols for IoT applications. Karbala International Journal of Modern Science. 2021. Vol. 7, No. 3. P. 196–211. URL: <https://kijoms.uokerbala.edu.iq/home/vol7/iss4/14/>
3. Internet of Things: a comprehensive overview, architectures, applications, simulation tools, challenges and future directions / S. K. Sharma et al. Discover Internet of Things. 2024. Vol. 4, No. 1. Art. 9. URL: <https://link.springer.com/article/10.1007/s43926-024-00084-3>