УДК 004.056.55:004.312.2 **doi: 10.26906/SUNZ.2026.1.224**

Я. В. Чертанов, А. А. Коваленко, В. В. Філіппов

Харківський національний університет радіоелектроніки, Харків, Україна

ПІДХІД ДО ВИБОРУ ПРОТОКОЛУ ТА АРХІТЕКТУРИ АВТОНОМНОЇ ДІЛЯНКИ ГРАНИЧНОГО ШАРУ IOT

Анотація. Актуальність. Стрімке зростання масштабів Інтернету речей (IoT) та потреб у моніторингу, автоматизації й оптимізації процесів у промисловості, логістиці, енергетиці, транспорті та смарт-технологіях зумовлює підвищений інтерес до ефективної організації мережних протоколів. Вибір протоколів передачі даних і архітектури мережі визначає продуктивність, енергоефективність, масштабованість та надійність IoT-систем, що робить цю тематику ключовою для сучасних досліджень і практичного впровадження. **Об'єкт дослідження:** протоколи та архітектури організації мережних протоколів Інтернету речей. **Мета статті:** аналіз і порівняння ефективності протоколів MQTT, CoAP, AMQP, XMPP та DDS, а також централізованої, децентралізованої та гібридної архітектур IoT для визначення задовільних рішень щодо побудови продуктивних і надійних систем Інтернету речей. **Результати дослідження.** У роботі проведено аналіз протоколів IoT за ключовими метриками: затримкою передачі, енергоефективністю та масштабованістю. Встановлено, що протоколи CoAP і DDS забезпечують найменші затримки, тоді як MQTT і COAP демонструють найкращу масштабованість. Протокол CoAP виявився найбільш енергоефективним, а AMQP і XMPP – показали підвищені витрати ресурсів. Оцінка архітектур IoT показала, що централізована архітектура забезпечує простоту керування, але має низьку стійкість до відмов, децентралізована – високу надійність і масштабованість, гібридна – збалансовані показники затримки, продуктивності й стійкості. Запропоновано комбінований підхід, що поєднує використання CoAP і MQTT у гібридній архітектурі для підвищення ефективності та адаптивності IoT-систем. **Висновки.** Сучасні протоколи і архітектури IoT мають різну ефективність залежно від умов застосування. Отримані результати можуть бути використані для побудови енергоефективних, масштабованих і надійних IoT-рішень у системах розумного моніторингу, автоматизації та безпеки. Сфера використання отриманих результатів: промислові та побутові IoT-системи, мережі моніторингу, автоматизовані системи керування, смарт-міста.

Ключові слова: Інтернет речей; протоколи IoT; MQTT; CoAP; AMQP; DDS; XMPP; архітектура IoT; централізована архітектура; децентралізована архітектура; гібридна архітектура; енергоефективність; масштабованість.

Вступ

Постановка проблеми. Інтернет речей (IoT) є одним із ключових напрямків сучасних мережних технологій, що забезпечує з'єднання пристроїв, систем і сенсорів для обміну даними у режимі реального часу. Актуальність цієї технології зумовлена стрімким зростанням потреб у моніторингу, автоматизації та оптимізації процесів у таких сферах, як промисловість, охорона здоров'я, «розумні міста», логістика та побутова техніка [1–3]. Ефективна організація мережних протоколів є основою стабільного та швидкого функціонування систем на базі IoT, забезпечуючи злагоджену взаємодію між пристроями. Організації протоколів для IoT включають різнорівневі архітектурні підходи, орієнтовані на зменшення затримок передачі даних, оптимізацію споживання енергії та забезпечення надійності з'єднань. Архітектури мереж IoT зазвичай організовані на основі відповідних потреб. Від вибору архітектури залежить можливість ефективно контролювати систему, витримувати збої вузлів або масштабувати системи на базі IoT. Таким чином, розвиток протоколів і архітектур організації мережних протоколів є фундаментальним для стабільного та безпечного функціонування IoT, відкриваючи можливості для інновацій у сучасних галузях [4, 5].

Аналіз останніх досліджень і публікацій. У роботах [1, 6, 7] описано поєднання протоколу MQTT для забезпечення передачі даних у системах з обмеженими ресурсами та протоколу CoAP для реалізації надійного зв'язку у вузькосмугових мережах. Дослідження показують, що використання цих протоколів у різних умовах дозволяє досягти значного підвищення продуктивності завдяки оптимізації енергоспоживання та мінімізації затримок.

В іншому дослідженні [4] було проведено порівняльний аналіз архітектур організації мережі IoT, таких як централізована, децентралізована та гібридна. Централізована архітектура ефективно працює з невеликою кількістю пристроїв завдяки центральному вузлу контролю даних. У той час децентралізовані архітектури, реалізовані із застосуванням протоколів AMQP (Advanced Message Queuing Protocol) та DDS (Data Distribution Service), забезпечують підвищену надійність і стійкість мережі завдяки рівномірному розподілу обчислювальних задач. Гібридні системи, що комбінують ці два підходи, демонструють високу ефективність у великих динамічних мережах за рахунок адаптації до навантажень у реальному часі [8]. Застосування таких архітектур у дослідженнях показує їх значні переваги для забезпечення обміну даними в IoT-системах із різними вимогами до ресурсів. У складних динамічних умовах вони дозволяють досягти стабільного функціонування завдяки поєднанню високої швидкодії та низьких затрат енергії [6, 8]. Такі результати є важливими для розвитку систем моніторингу, автоматизації та оптимізації процесів у різних сферах застосування Інтернету речей.

Метою роботи є дослідження ефективності, аналіз і порівняння протоколів MQTT, CoAP, AMQP, XMPP та DDS, а також централізованої, децентралізованої і гібридної архітектур організації

мережних протоколів для IoT. Стаття спрямована на оцінку переваг і обмежень кожного протоколу та архітектури і визначенні задовільних рішень для ефективного та продуктивного функціонування систем на базі IoT. Значна увага приділена застосуванню протоколів у різних середовищах, що дозволяє обґрунтувати їх доцільність для конкретних завдань, таких як розподілене збирання даних, автоматизований моніторинг та енергоефективний контроль пристроїв, що дозволить доповнити наявні теоретичні та практичні напрацювання у сфері IoT.

Теоретичний матеріал

Message Queuing Telemetry Transport (MQTT) являє собою легкий протокол обміну повідомленнями, призначений для передачі даних у системах на базі IoT, де обмежені ресурси та нестабільна мережа. Протокол працює за схемою «публікація-підписка» із центральним сервером – брокером, який отримує повідомлення від клієнтів-публікаторів і пересилає їх клієнтам-підписникам на основі заданих тем (рис. 1). Завдяки простій структурі протокол є енергоефективним і мінімізує навантаження на мережу [6,7]. Протокол MQTT підтримує різні рівні надійності, що дозволяють контролювати доставку даних від простого надсилання до гарантованої доставки повідомлень. Ця гнучкість та масштабованість дозволяють використовувати протокол MQTT як у локальних мережах, так і в хмарних сервісах, забезпечуючи ефективну роботу навіть у великих IoT-системах [8]. Проте MQTT має деякі недоліки. Робота протоколу залежить від брокера, що створює потенційну точку відмови. Для забезпечення безпеки передачі даних необхідно використовувати додаткове шифрування, наприклад, механізми TLS/SSL, оскільки вбудованих механізмів захисту немає [2,9]. Крім того, MQTT обмежений використанням лише стеку протоколів TCP/IP і менш ефективний для передачі великих обсягів даних, оскільки оптимізований для коротких повідомлень. Незважаючи на ці обмеження, завдяки своїй простоті, надійності та енергоефективності MQTT залишається одним із найпопулярніших протоколів для побудови систем на базі IoT та передачі даних між пристроями.

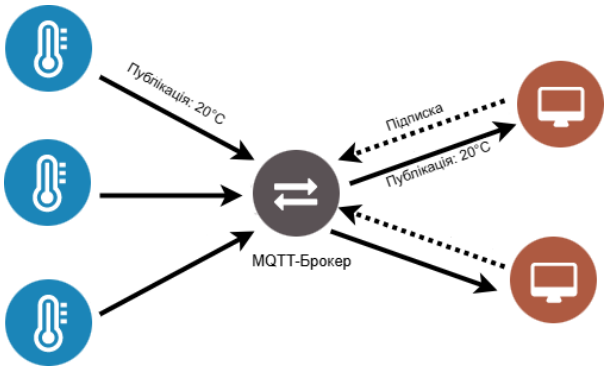


Рис. 1. Схема взаємодії компонентів в IoT при використанні протоколу MQTT

Constrained Application Protocol (CoAP) – це протокол передачі даних, розроблений для пристроїв із обмеженими обчислювальними ресурсами у системах на базі IoT. Протокол CoAP базується на схемі «клієнт-сервер» (рис. 2) і працює поверх протоколу User Datagram Protocol (UDP), що дає змогу забезпечити високу швидкість передачі даних із мінімальними затримками. Завдяки своїй компактності та простій структурі, CoAP ідеально підходить для малопотужних пристроїв і нестабільних мереж із низькою пропускною здатністю. Протокол CoAP підтримує можливість шифрування і обміну невеликими повідомленнями у форматі, що спрощує передачу даних у енергоефективний спосіб [5]. Додатково протокол використовує REST-подібну архітектуру, де команди взаємодіють із ресурсами серверів, що дозволяє ефективно організовувати обмін даними. Перевагами CoAP є його енергоефективність, гнучкість у роботі з невеликими обсягами даних та низькі вимоги до пропускної здатності мережі. Використання протоколу UDP забезпечує швидку передачу, що особливо важливо для пристроїв з короткочасними з'єднаннями. Однак внаслідок роботи на основі протоколу UDP, CoAP не забезпечує гарантованої доставки повідомлень і вимагає додаткових механізмів для забезпечення надійності [2, 7]. Іншим недоліком є обмежена масштабованість у порівнянні з іншими протоколами, такими як MQTT. Проте завдяки простоті, швидкості та відповідності специфікам обмежених пристроїв, протокол CoAP є ефективним рішенням для систем на базі IoT, де критично важливими є низьке енергоспоживання і мінімальні затримки при обміні даними.

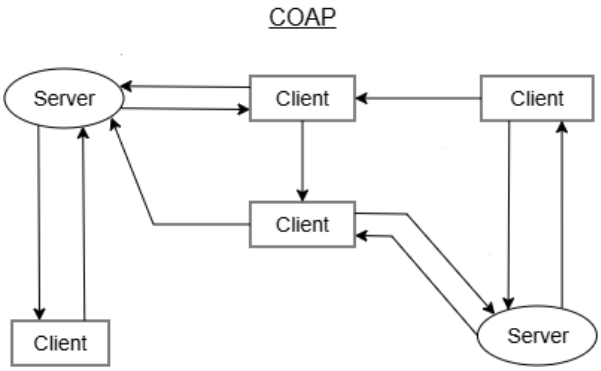


Рис. 2. Схема взаємодії компонентів в IoT при використанні протоколу COAP

Advanced Message Queuing Protocol (AMQP) є уніфікованим протоколом обміну повідомленнями, призначений для забезпечення надійної та впорядкованої передачі даних між компонентами системи. Протокол AMQP побудований по схемі «публікація-підписка», де центральну роль відіграє брокер повідомлень, який відповідає за прийом, зберігання та доставку даних. Протокол підтримує функціональність черг повідомлень, що дозволяє забезпечувати стійкість до збоїв та ефективне управління потоками даних (рис. 3). AMQP працює поверх протоколу Transmission Control Protocol (TCP), що гарантує надійність та цілісність переданих даних, а його стандартизація дозволяє інтегрувати рішення в системи різного масштабу. Перевагами протоколу AMQP є надійність доставки даних завдяки механі-

зму підтвердження повідомлень та можливість управління чергами для балансування навантаження. Протокол підтримує складну маршрутизацію повідомлень, пріоритезацію та контроль доступу, що робить його ефективним для великих та критичних систем [6,7]. Однак ці можливості супроводжуються значними обчислювальними витратами, що обмежує використання AMQP у пристроях з недостатніми ресурсами. Крім того, порівняно з простими протоколами, такими як MQTT або CoAP, AMQP вимагає більше пропускної спроможності мережі та затрат енергії. Незважаючи на ці обмеження, завдяки своїй гнучкості, надійності та підтримці складних сценаріїв передачі даних, протокол AMQP активно використовується для побудови масштабованих і стабільних систем у сучасних рішеннях IoT [6, 8].

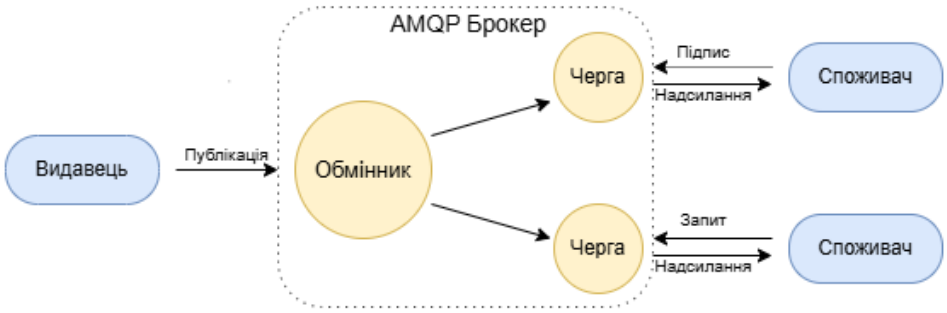


Рис. 3. Схема взаємодії компонентів в IoT при використанні протоколу AMQP

Data Distribution Service (DDS) є протоколом обміну даними, що розроблений для розподілених систем із жорсткими вимогами до швидкості та надійності. Протокол працює за схемою «публікація-підписка» дозволяє учасникам обмінюватися даними асинхронно, без прямого зв'язку між ними. Протокол DDS підтримує налаштування параметрів Quality of Service (QoS), які визначають надійність, затримки та пріоритетність передачі даних, що робить його універсальним для застосувань, таких як промисловий IoT, автономні системи та управління критично важливими інфраструктурами [3,9]. Протокол забезпечує автоматичне виявлення вузлів у мережі, ефективне використання пропускної здатності завдяки фільтрації даних і підтримує як гарантовану, так і оптимальну доставку. Основними перевагами DDS є гнучкість, висока надійність і підтримка роботи в реальному часі, що дозволяє створювати масштабовані системи для складних сценаріїв. Проте його впровадження може бути ускладнене через підвищені вимоги до обчислювальних ресурсів, що обмежує використання у пристроях з недостатніми ресурсами. Завдяки децентралізованій архітектурі та можливостям налаштування QoS, протокол DDS є переважно рішенням для середовищ із високою інтенсивністю взаємодії між пристроями та вимогами до надійності й низьких затримок [3,7].

Extensible Messaging and Presence Protocol (XMPP) є гнучким протоколом обміну повідомленнями та даними, розробленим для передачі структурованої інформації у реальному часі. Спочатку протокол XMPP був створений для систем миттєвого обміну повідомленнями, але завдяки своїй архітектурі він знайшов широке застосування у різних галузях, включно з IoT [7,9]. Протокол базується на архітектурі клієнт-сервер і використовує протокол TCP для надійної та безпечної передачі даних (рис. 4). Однією з ключових особливостей протоколу XMPP є його здатність працювати у децентралізованих системах завдяки підтримці федеративної мережі, де різні сервери взаємодіють між собою для обміну повідомленнями та присутністю. XMPP пропонує численні переваги, серед яких універсальність, розширюваність завдяки XML-структурі та можливість використання у системах, що потребують обміну даними у реальному часі. Завдяки своїй гнучкості протокол підтримує не лише передачу текстових повідомлень, а й мультимедійних даних, керування пристроями та повідомлення про стан присутності, що є важливим для IoT-додатків. Проте використання XML робить протокол XMPP надлишковим порівняно з простими протоколами, такими як MQTT чи CoAP, що обмежує його ефективність у пристроях з обмеженими ресурсами [5, 6]. Крім того, постійна підтримка з'єднання збільшує енергоспоживання, що є критичним для енергоефективних IoT-систем. Незважаючи на ці обмеження, протокол XMPP залишається надійним і універсальним рішенням не тільки для IoT, а й для багатьох інших областей, зокрема систем миттєвого обміну повідомленнями, онлайн-спілкування та корпоративних платформ [3, 8].

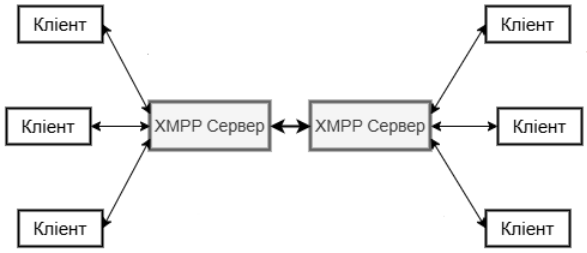


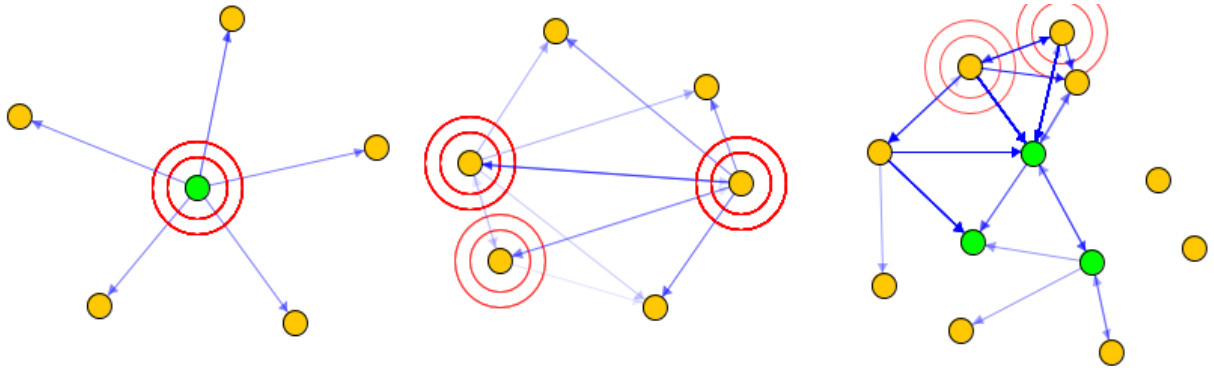
Рис. 4. Схема взаємодії компонентів в IoT при використанні протоколу XMPP

Централізована архітектура є найбільш простою, де всі пристрої підключені до одного центрального вузла (рис. 5, а), що відповідає за обробку даних та координацію системи. Такий підхід забезпечує легке управління та моніторинг усіх процесів, а також високу ефективність передачі даних у реальному часі [4].

Проте централізована архітектура має недолік у вигляді єдиної точки відмови: вихід центрального вузла з ладу призводить до зупинки всієї системи [2, 7]. Децентралізована архітектура розподіляє функції керування та обробки даних між кількома вузлами (рис. 5, б), що взаємодіють автономно. Такий підхід має підвищену стійкість до збоїв, оскільки вихід одного вузла не паралізує всю мережу.

Крім того, децентралізація забезпечує хорошу масштабованість, особливо у великих системах, де навантаження рівномірно розподіляється [4, 8]. Недоліком є складність управління для забезпечення координації вузлів і узгодженості даних потрібні додаткові механізми.

Гібридна архітектура поєднує у собі централізовані та децентралізовані принципи, балансуючи між контролем і гнучкістю. Центральний вузол виконує функцію керування, тоді як частина обчислювальних задач розподіляється між периферійними вузлами (рис. 5, в). Це дозволяє зменшити навантаження на основний сервер та підвищити стійкість системи [4,7]. Гібридна архітектура гнучка та масштабована, але вимагає точного налаштування для оптимальної роботи.



а б в

Рис. 5. Види архітектур: а – централізована; б – децентралізована; в – гібридна

Дослідження ефективності мережних протоколів та архітектур IoT

Ефективність протоколів передачі даних залежить від таких критеріїв, як швидкість передачі, енергоефективність, масштабованість та безпека. У сучасних розподілених системах протоколи мають забезпечувати оптимальне використання мережних ресурсів, гарантуючи при цьому стабільну роботу навіть у нестабільних середовищах. Швидкість передачі визначає здатність протоколу ефективно обробляти великий обсяг даних при мінімальних затримках. Енергоефективність є ключовим фактором для пристроїв із обмеженими ресурсами. Масштабованість дозволяє системі ефективно працювати зі збільшенням кількості вузлів чи обсягів даних. Безпека протоколу гарантує захист інформації від несанкціонованого доступу, що є критично важливим для підприємницької діяльності.

Для дослідження ефективності протоколів були використані інструменти Cooja операційної системи Contiki та PerfTest у RabbitMQ. Cooja використовувалася для моделювання протоколів MQTT, CoAP, XMPP та DDS, а PerfTest – для протоколу AMQP. Ці інструменти дозволили отримати інформацію про затримку передачі між пристроями IoT, енергоефективність та масштабованість протоколів. Збір даних для кожного протоколу проводилося у однакових умовах.

Архітектура централізована, наявний один сервер/брокер, змінна кількість клієнтських вузлів. В якості вузлів використовувалися Tmote Sky – платформа для IoT мереж з низьким енергоспоживанням.

У ході дослідження ефективності передачі (рис. 6) найкращі результати продемонстрували протоколи CoAP та DDS, із затримкою в діапазоні від 170 до 270 мс. Для DDS було налаштовано параметри QoS, оптимізовані для швидкої передачі даних через протокол UDP, який також лежить в основі CoAP. Натомість протоколи MQTT, AMQP та XMPP, що працюють на базі TCP, показали схожі результати із затримкою в межах 670–780 мс, що значно перевищує показники CoAP і DDS.

Енергоефективність вузла залежить від часу, витраченого на передачу та отримання даних, навантаження на процесор, а також тривалості перебування в режимі сну. За результатами вимірювань (рис. 7), протокол CoAP продемонстрував найкращі показники енергоспоживання. Протоколи XMPP та MQTT виявили вищу енергопотребу, демонструючи схожі тенденції зростання, тоді як результати протоколів DDS і XMPP були близькими.

Налаштування QoS у протоколах MQTT та DDS суттєво впливає на ефективність передачі даних та енергоспоживання. Зокрема, оптимізація DDS для швидкої передачі інформації спричинила значне зростання енергопотреби вузлів.

Зростання затримки у протоколах на основі UDP є вищим, ніж у аналогічних, але основаних на протоколі TCP, що обмежує їх здатність до масштабування.

Водночас енергоспоживання пристроїв системи на базі IoT визначає тривалість автономної роботи, і зі збільшенням кількості вузлів значне зростання енергопотреби може ускладнити додавання нових пристроїв до мережі.

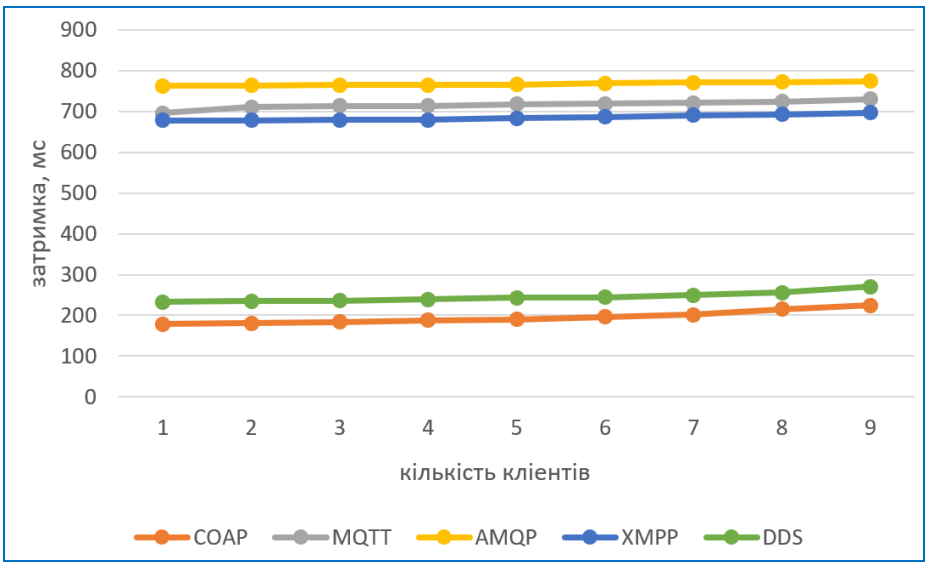


Рис. 6. Графік залежності затримки від кількості клієнтів для різних протоколів

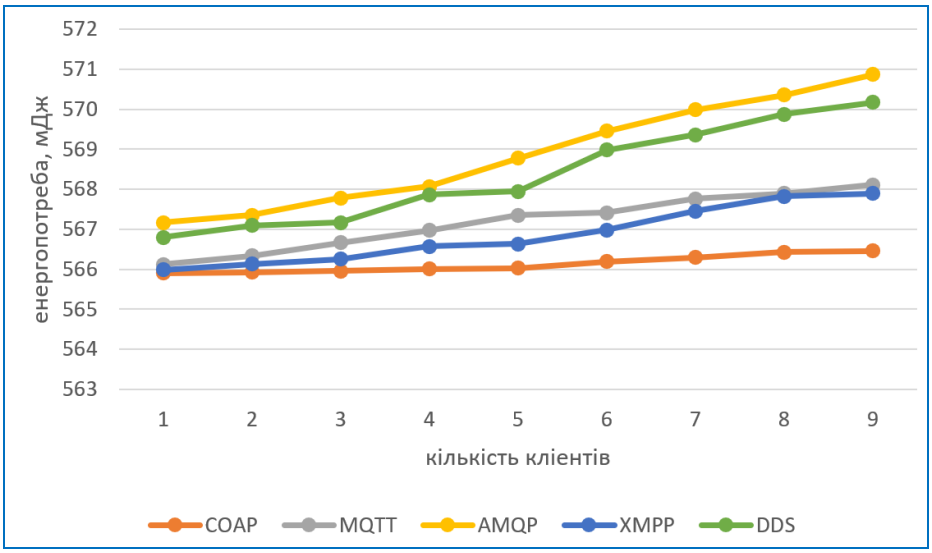


Рис. 7. Графік залежності енергопотреби від кількості клієнтів для різних протоколів

Найкращими за масштабованістю є протоколи MQTT та DDS завдяки їхній гнучкості у налаштуваннях. CoAP демонструє найвищу енергоефективність, однак зі збільшенням мережі його ефективність передачі повідомлень суттєво знижується. Але протоколи XMPP та AMQP мають високі показники енергоспоживання і недостатню гнучкість у налаштуванні швидкості передачі даних, через що вони поступаються протоколам MQTT, DDS та CoAP у здатності до масштабування.

Ефективність архітектур IoT залежить від ефективності управління, стійкості до відмов, масштабованості та затримок передачі. Ефективність управління визначає рівень можливої координації вузлів. Стійкість до відмов гарантує роботу системи навіть при виході з ладу окремих компонентів, що критично важливо для надійності.

Масштабованість дозволяє системі адаптуватися до зростання кількості пристроїв та даних, підтримуючи стабільну продуктивність. Затримки передачі впливають на швидкість реакції, яка може змінюватися з кількістю запитів до вузлів. У результаті дослідження можна дійти висновку, що централізована архітектура забезпечила чіткий контроль через центральний сервер, що спрощує управління та обробку даних, але обмежує стійкість до відмов і масштабованість, створюючи ризик перевантаження та високих затримок у великих системах.

Децентралізована архітектура розподіляє обробку між вузлами, що підвищує автономність, стійкість і дозволяє масштабувати мережу, але може призводити до зростання затримок у великих системах через складність координації між вузлами.

Гібридна архітектура комбінує переваги обох видів, поєднуючи часткову автономність вузлів із централізованим контролем, що підвищує стійкість і забезпечує помірну масштабованість та затримки передачі, збалансовуючи навантаження на систему.

Аналіз результатів дослідження показав цікаву різницю в ефективності протоколів та архітектур. Протоколи CoAP та DDS показали низькі затримки, які мали значну тенденцію росту при збільшені кількості пристроїв в IoT мережі, тоді як MQTT, XMPP та AMQP показали високу, але стабільну затримку.

Дослідження енергоефективності протоколів MQTT, XMPP, DDS та AMQP показали середній рівень, але вони мають високу тенденцію росту енергопотреби вузлів при збільшені кількості пристроїв мережі. CoAP же показав найнижчий показник енергопотреби і тенденції її росту.

MQTT, DDS та CoAP мають найкращі можливості до масштабованості, тоді як XMPP та AMQP вказують на можливість підтримки меншої кількості пристроїв в мережі.

Централізована архітектура організації систем на базі IoT надає найкращий контроль над вузлами мережі, але страждає від підвищеної затримки та зниженої стійкості до відмов, тоді як децентралізована архітектура має кращу масштабованість, значну стійкість до відмов, але має складності у контролі над мережею.

Гібридна архітектура поєднує можливості обох видів, що робить її кращою за них, але вона є складнішою для налаштування.

Було детально проаналізовано протоколи та архітектури IoT, а також адаптовано до різних умов дослідження. Продуктивність обраних протоколів була перевірена за допомогою ключових метрик: ефективності передачі, енергоспоживання та масштабованості, що дозволило отримати детальну картину їх здатності працювати у реальних умовах. Для архітектур IoT було оцінено стійкість до відмов, енергоспоживання, масштабованість та затримку передачі, що є критично важливими характеристиками для забезпечення надійної роботи систем.

Висновки

В ході проведеного дослідження було ретельно підібрано умови для оцінки продуктивності сучасних протоколів та архітектур IoT. Продуктивність обраних протоколів була проаналізована за допомогою ключових метрик: ефективності передачі, енергоспоживання та масштабованості, що дозволило отримати детальну картину їх здатності працювати у приближених до реальних умовах. Для архітектур IoT було оцінено стійкість до відмов, енергоспоживання, масштабованість та затримку передачі, що є критично важливими характеристиками для забезпечення надійної роботи систем.

У результаті дослідження було запропоновано комбінований підхід використання протоколів CoAP та MQTT на гібридній архітектурі, що надає переваги у вигляді високої ефективності передачі протоколів з низьким енергоспоживанням вузлів мережі з додатковою можливістю налаштування і високою захищеністю мережі. Це рішення є ефективним для реальних застосувань у галузях розумного моніторингу, автоматизації та безпеки.

Протоколи CoAP, MQTT, AMQP, DDS та XMPP демонструють свою ефективність у задачах IoT, де ключовими факторами є швидкість передачі даних, надійність, масштабованість і енергоефективність. Завдяки низьким вимогам до обчислювальних ресурсів, CoAP є ідеальним для пристроїв з обмеженими ресурсами, таких як датчики та контролери. Однак його основним недоліком є орієнтація на прості запити й відповідь, що обмежує його можливості в складних системах з інтенсивним обміном даними. Протоколу MQTT притаманна легкість та адаптивність до різноманітних умов. Завдяки схемі «публікації-підписки», цей протокол добре працює у додатках з обмеженою пропускною здатністю мережі, що робить його надійним вибором для систем моніторингу або управління IoT. Однак, його можливості обмежуються відсутністю гарантії доставки при зміні QoS. AMQP забезпечує високий рівень надійності та безпеки передачі даних, що робить його гарним вибором у критично важливих системах. Проте значні обчислювальні витрати обмежують його використання у системах з обмеженими ресурсами. Крім того, складність протоколу у порівнянні з MQTT може ускладнити впровадження. Протокол DDS демонструє вражаючу продуктивність для систем з низькою затримкою і великим обсягом даних. Завдяки своїй гнучкості та здатності підтримувати динамічний обмін даними в реальному часі, DDS є ідеальним для високонавантажених систем, таких як автомобільні або авіаційні мережі. Однак, його складність та високі вимоги до ресурсів обмежують використання у простих IoT-рішеннях. XMPP забезпечує ефективну комунікацію в системах обміну миттєвими повідомленнями завдяки своїй гнучкій архітектурі та підтримці розширень.

Проте через орієнтацію на текстові повідомлення та відносно високу накладну вартість, він менш ефективний у випадках передачі сенсорних даних чи обміну великими обсягами інформації. Таким чином, вибір оптимального протоколу залежить від конкретних умов та завдань.

Для простих систем із низькими вимогами до ресурсів CoAP і MQTT залишаються надійними варіантами, тоді як AMQP та DDS забезпечують кращу надійність і продуктивність для складних і критично важливих задач.

Конфлікт інтересів

Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Використання засобів штучного інтелекту

Автори підтверджують, що не використовували технології штучного інтелекту при створенні представленої роботи.

Список літератури

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2022). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 24(4), 2347–2404. https://doi.org/10.1109/COMST.2015.2444095

2. Choudhary, A., Khandal, V., Choudhary, R. et al. Internet of Things: a comprehensive overview, architectures, applications, simulation tools, challenges and future directions. Discover Internet of Things, 4, 16, 2024. https://link.springer.com/article/10.1007/s43926-024-00084-3
3. Domínguez-Bolaño, T., Campos, O., Barral, V., Escudero, C. J. An overview of IoT architectures, technologies, and existing open-source projects. arXiv preprint arXiv:2401.15441, 2024. https://doi.org/10.48550/arXiv.2401.15441
4. Ray, P. P. (2023). A review on architectures, protocols, and standards in Internet of Things. Internet of Things, 22, 100765. https://doi.org/10.1016/j.iot.2023.100765
5. Sobin C. C. A Survey on Architecture, Protocols and Challenges in IoT. Wireless Personal Communications, vol. 112, no. 3, 2020, pp. 1383–1429. https://doi.org/10.1007/s11277-020-07108-5
6. Larian, H., Larian, A., Sharifi, M., Movahednejad, H. Towards Web of Things Middleware: A Systematic Review. arXiv preprint arXiv:2208.04272, 2022. https://doi.org/10.48550/arXiv.2201.08456
7. Dauda, A., Mazhar, T., Malik, M. A. et al. A Survey on IoT Application Architectures. Sensors, 24(21), 6872, 2024. https://doi.org/10.3390/s24165320
8. Al-Yudidharma, A., Anwar, M. F., Pratama, R. A., et al. Messaging protocols and electronic platforms used in the Internet of Things for the purpose of building smart homes: A systematic literature review. Journal of Systems Architecture, 143, 102989, 2023. https://doi.org/10.1016/j.procs.2022.12.127
9. Al-Andoli M. N., Kumar K., Kumar A., Jaber M. M., Shah R. Dimensions of Internet of Things: Technological Taxonomy, Architecture, Applications and Open Challenges — A Systematic Review. Wireless Communications and Mobile Computing, 2022, Vol. 2022, 28 p. https://doi.org/10.1155/2022/9148373

Received (Надійшла) 06.12.2025
Accepted for publication (Прийнята до друку) 04.02.2026
Publication date (Дата публікації) 27.02.2026

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Чертанов Ярослав Валерійович – студент кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Yaroslav Chertanov – student of the Department of Electronic Computers, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine;
e-mail: yaroslav.chertanov@nure.ua; ORCID ID: https://orcid.org/0009-0008-4648-5871;

Коваленко Андрій Анатолійович – доктор технічних наук, професор, завідувач кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Andriy Kovalenko – Doctor of Technical Sciences, Professor, Head of the Department of Electronic Computers, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine;
e-mail: andriy.kovalenko@nure.ua; ORCID ID: https://orcid.org/0000-0002-2817-9036;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=56423229200.

Філіппов Владлен Валерійович – аспірант кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Vladlen Filippov – PhD student, Department of Electronic Computers, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine;
e-mail: vladlen.filippov@nure.ua; ORCID Author ID: http://orcid.org/0009-0004-2524-7840.

Approach for selecting the protocol and architecture of the autonomous section of the IoT edge layer

Yaroslav Chertanov, Andriy Kovalenko, Vladlen Filippov

Abstract. Relevance. The rapid growth of the Internet of Things (IoT) and the need for monitoring, automation, and optimization of processes in industry, logistics, energy, transportation, and smart technologies has led to increased interest in the effective organization of network protocols. The choice of data transmission protocols and network architecture determines the performance, energy efficiency, scalability, and reliability of IoT systems, making this topic key for modern research and practical implementation. **Object of study:** protocols and architectures for organizing Internet of Things network protocols. **Purpose of the article:** to analyze and compare the effectiveness of MQTT, CoAP, AMQP, XMPP, and DDS protocols, as well as centralized, decentralized, and hybrid IoT architectures to identify satisfactory solutions for building productive and reliable Internet of Things systems. **Research results.** The paper analyzes IoT protocols according to key metrics: transmission delay, energy efficiency, and scalability. It was found that CoAP and DDS protocols provide the lowest latency, while MQTT and COAP demonstrate the best scalability. The CoAP protocol proved to be the most energy-efficient, while AMQP and XMPP showed increased resource consumption. The evaluation of IoT architectures showed that centralized architecture provides ease of management but has low fault tolerance, decentralized architecture has high reliability and scalability, and hybrid architecture has balanced latency, performance, and fault tolerance. A combined approach is proposed that combines the use of CoAP and MQTT in a hybrid architecture to improve the efficiency and adaptability of IoT systems. **Conclusions.** Modern IoT protocols and architectures have different efficiencies depending on the conditions of use. The results obtained can be used to build energy-efficient, scalable, and reliable IoT solutions in smart monitoring, automation, and security systems. The scope of application of the results obtained: industrial and domestic IoT systems, monitoring networks, automated control systems, smart cities.

Keywords: Internet of Things; IoT protocols; MQTT; CoAP; AMQP; DDS; XMPP; IoT architecture; centralized architecture; decentralized architecture; hybrid architecture; energy efficiency; scalability.