

АНАЛІЗ ТЕХНОЛОГІЙ ТА СТАНДАРТІВ ЗВ'ЯЗКУ ДЛЯ МЕРЕЖІ ІОТ

Domracheva K.O., Dovzhenko N.M., Dmitrenko V.V. Analysis of technologies and connection standards for the iot network

The Internet of Things has become the basis of digital transformation and automation, the development of new business proposals and the improvement of our lifestyle, work and entertainment. Choosing the right type of connection is an inevitable part of any IoT project. Standards, technologies and platforms focused on the IoT ecosystem are developing at a very fast pace. The Internet of Things allows things to communicate and coordinate a solution for many different types of applications, including healthcare, home automation, disaster recovery, industry automation, etc. It is expected that in the future it will only increase the number of applications. The article provides an overview of existing standards and protocols IoT. An overview of the differences between IoT technologies is presented and Considered, for which applications each technology is best suited. There are many current IoT issues, including mobility, reliability, scalability, and many others. Despite the volume of work in the areas of mobility, scalability and management, enterprises continue to suffer from problems.

Keywords: international standards, network, technology, protocol, applications, speed, energy, provision.

Домрачева К.О., Довженко Н.М., Дмитренко В.В. Аналіз технологій та стандартів зв'язку для мережі ІОТ

У статті представлено огляд існуючих стандартів та протоколів ІОТ. Розглянуто стандарти, розроблені Internet Engineering Task Force (IETF), Інститутом інженерів з електротехніки та електроніки (IEEE), Міжнародним союзом електрозв'язку (МСЕ) та іншими організаціями зі стандартизації. Зроблено огляд відмінностей між технологіями ІОТ та розглянуто для яких додатків кожна технологія найкраще підходить. Крім того, зроблено огляд поточних проблем ІОТ та подальші можливості дослідження.

Ключові слова: міжнародні стандарти, мережа, технологія, протокол, додатки, швидкість, енергія, забезпечення.

Домрачева Е.А., Довженко Н.Н., Дмитренко В.В. Анализ технологий и стандартов связи для сети ИОТ

В статье представлен обзор существующих стандартов и протоколов IoT. Рассмотрены стандарты, разработанные Internet Engineering Task Force (IETF), Институтом инженеров по электротехнике и электронике (IEEE), Международным союзом электросвязи (МСЭ) и другими организациями по стандартизации. Сделано обзор различий между технологиями IoT и рассмотрены для каких приложений каждая технология лучше подходит. Кроме того, сделан обзор поточной проблем IoT и дальнейшие возможности исследования.

Ключевые слова: международные стандарты, сеть, технология, протокол, приложения, скорость, энергия, обеспечение.

Вступ

«Інтернет речей» або internet of things, ІОТ охоплює широкий спектр галузей та варіантів використання, які масштабуються від одного обмеженого пристрою до масштабного кроссплатформенного розгортання вбудованих технологій, що підключаються в режимі реального часу [1-7].

Все це об'єднує велику кількість старих та нових протоколів зв'язку, які дозволяють пристроям і серверам спілкуватися один з одним новими, більш взаємопов'язаними способами.

Стандарти, технології та платформи, орієнтовані на екосистему ІОТ розвиваються в дуже швидкому темпі. Інтернет речей дозволяє речам спілкуватися і координувати рішення для безліч різних типів додатків, включаючи охорону здоров'я, домашню автоматизацію, аварійне відновлення, автоматизація промисловості та ін. Очікується, що в майбутньому він буде тільки розширювати число додатків.

ІоТ-екосистема, як показано на рис. 1, складається з семирівневої моделі: ринок, придбання, приєднання, інтеграція, аналіз, додатки та послуги.

На нижньому рівні може бути інтелектуальна мережа, підключений будинок та ін. Другий рівень складається з датчиків та інтелектуальних пристроїв, які можна розглядати як ядро програми. Тип та розподіл датчиків варіюється в залежності від бажаних додатків. Прикладами таких датчиків є датчики температури, вологості, лічильники електроенергії або камери. Третій рівень складається з взаємопов'язаного шару, який полегшує передачу даних датчика в центр обробки даних. Там дані об'єднуються з іншими відомими наборами даних, такими як географічні дані, дані про населення або економічні дані. Крім того, об'єднані дані вивчаються з використанням методів машинного навчання та інтелектуального аналізу даних. Для забезпечення таких великих розподілених додатків необхідне програмне забезпечення для спільної роботи і комунікації. Такі парадигми включають програмно-конфігуровану мережу (SDN), сервісно-орієнтовану архітектуру (SOA) та ін.. Нарешті, верхній рівень складається з послуг, як управління енергією, управління охороною здоров'я, освіта, транспорт та ін.

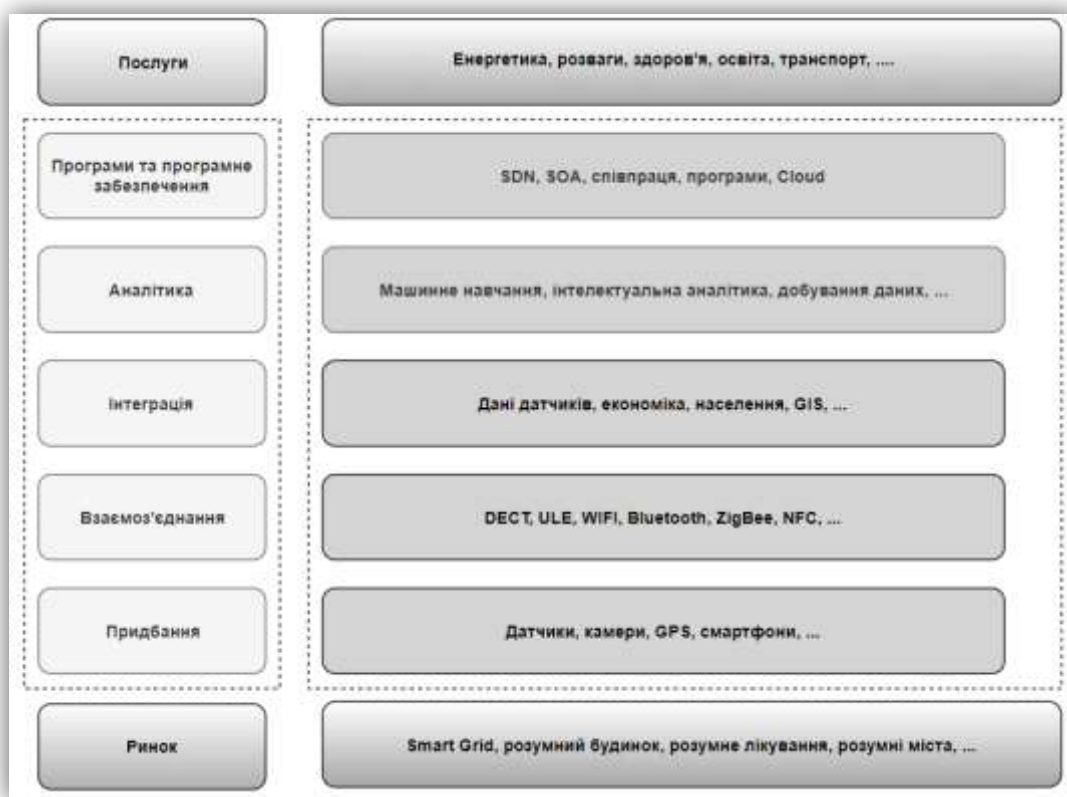


Рис.1. Екосистема Internet of Things

Стандарти, що охоплюють п'ять рівнів (програми, аналітика, інтеграція, взаємоз'єднання, придбання), були запропоновані декількома організаціями по стандартизації. Найвідоміші серед них IEEE, IETF і MCE. IEEE в основному працює з каналом передачі даних, IETF працює в мережах, а кілька організацій працюють над сесіями, безпекою та управлінням.

Ці стандарти включають протоколи зв'язку, маршрутизації, мережевого та сеансового рівнів, розроблених для задоволення вимог ІоТ.

Система ІоТ має трирівневу архітектуру: пристрої, шлюзи та системи даних. Дані переміщуються між цими рівнями через чотири типи каналів передачі.

1. Пристрій до пристрою (D2D) - прямиий контакт між двома смарт-об'єктами, коли вони миттєво обмінюються інформацією без посередників. Наприклад, промислові роботи і датчики безпосередньо пов'язані один з одним, щоб координувати свої дії і виконувати дії з

компонентами більш ефективно. Цей тип з'єднання поки не дуже поширений, тому що більшість пристроїв не здатні обробляти такі процеси.

2. **Пристрій до шлюзу** - зв'язок між датчиками та вузлами шлюзу. Шлюзи є більш потужними обчислювальними пристроями, ніж датчики. Вони виконують дві основні функції: об'єднують дані з датчиків і направляють їх у відповідну систему даних; аналізують дані і, якщо будуть виявлені які-небудь проблеми, повертають їх назад на пристрій. Існують різні протоколи шлюзу IoT, які можуть краще підходити до того чи іншого рішення в залежності від обчислювальних можливостей шлюзу, пропускну здатності та надійності мережі, частоти генерації даних та їх якості.

3. **Шлюз до систем даних** - передача даних від шлюзу до відповідної системи даних. Щоб визначити, який протокол використовувати, потрібно проаналізувати трафік даних (частота пакетів та перевантажень, вимоги безпеки та кількість потрібних паралельних з'єднань).

4. **Між системами даних** - передача інформації всередині центрів обробки даних або хмар. Протоколи для цього типу з'єднання повинні бути простими в розгортанні та інтеграції з існуючими додатками, мати високу доступність, ємність і надійне відновлення після збою.

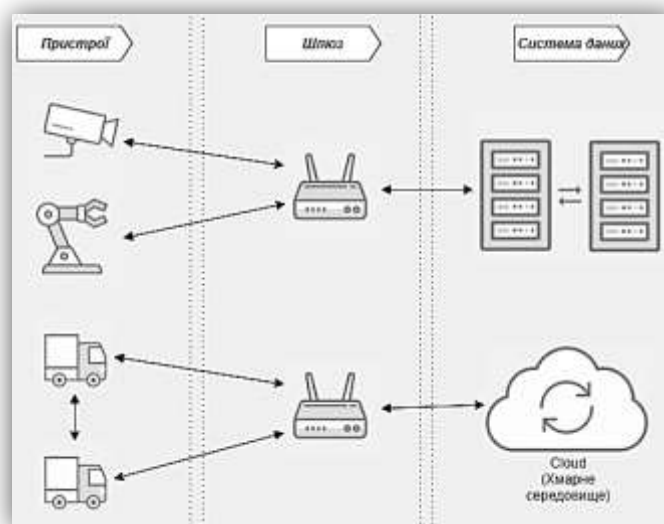


Рис.2 Архітектура IoT системи

Мережі поділяються на категорії залежно від відстані, яку вони надають.

1. **Наномережа** - це набір невеликих пристроїв (розміром не більше декількох мікрометрів), які виконують дуже прості завдання, такі як розпізнавання, обчислення, зберігання та виконують функцію аттенюатора. Такі системи застосовуються в біометричних, військових та інших нанотехнологіях.

2. **NFC** (Near-Field Communication) - низькошвидкісна мережа для підключення електронних пристроїв на відстані до 4 см один від одного. Можливими додатками є безконтактні платіжні системи, документи, що засвідчують особу, чи картки-ключі.

3. **BAN** (Body Area Network) - мережа для підключення переносних обчислювальних пристроїв, які можна носити або закріпленими на тілі, або поруч з тілом в різних положеннях, або вбудованими в тіло (імплантати).

4. **PAN** (персональна мережа) - мережа для зв'язку пристроїв в радіусі приблизно однієї або декількох кімнат.

5. **LAN** (Local Area Network) - мережа, що охоплює територію однієї будівлі.

6. **CAN** (Campus / Corporate Area Network) - мережа, яка об'єднує невеликі локальні мережі в межах обмежених географічною зоною (підприємства, університету).

7. **MAN** (Metropolitan Area Network) - велика мережа для певного мегаполісу, що працює на основі технології мікрохвильової передачі.

8. **WAN** (глобальна мережа) - мережа, яка існує у великому географічному регіоні і об'єднує різні невеликі мережі, в тому числі локальні мережі та мережі MAN.

В цілому до мереж IoT висувається багато вимог:

- Можливість підключення великої кількості різномірних елементів;
- Висока надійність;
- Передача даних в режимі реального часу з мінімальними затримками;
- Можливість захистити всі потоки даних;
- Можливість налаштування додатків;
- Моніторинг та управління трафіком на рівні пристрою;
- Економічна ефективність для великої кількості зв'язаних об'єктів.

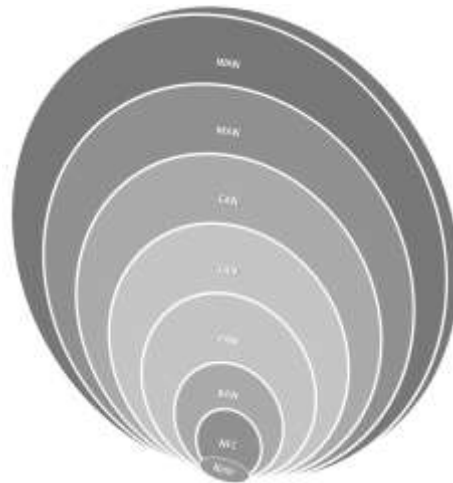


Рис.3. Категорії мереж

Особливості бездротових протоколів, стандартів і технологій для IoT

Стільникова технологія є основою мереж мобільного зв'язку. Але вона також підходить для додатків IoT, які повинні працювати на великих відстанях. Вони можуть скористатися можливостями стільникового зв'язку, такими як GSM, 3G, 4G (і 5G найближчим часом).

Технологія здатна передавати великі обсяги даних, але енергоспоживання і витрати також високі. Таким чином, це може бути ідеальним рішенням для проектів, які відправляють невеликі обсяги інформації. Стандарти GSM / GPRS / EDGE (2G), UMTS / HSPA (3G), LTE (4G). Використовувані частоти: 900/1800/1900/2100 МГц. Радіус дії: 35 км (GSM); 200 км (HSPA). Швидкість передачі даних: 35-170 кбіт / с (GPRS), 120-384 кбіт / с (EDGE), 384 кбіт / с-2 Мбіт / с (UMTS), 600 кбіт / с-10 Мбіт / с (HSPA), 3-10 Мбіт / с (LTE).

Long Term Evolution for Machines (LTE-M) (тип зв'язку LTE-Machine) - сімейство технологій на основі стандартів, які підтримують декілька категорій, таких як Cat-1 і CatM1, придатних для IoT.

LTE-M - це глобальна технологія з низьким енергоспоживанням, яка підтримує IoT за рахунок більш низької складності пристрою і забезпечує розширене покриття, дозволяючи при цьому повторно використовувати встановлену базу LTE. Це забезпечує термін служби батареї до 10 і більше років для широкого спектра випадків використання, при цьому вартість модемів знижується до 20-25% від існуючих модемів EGPRS. Мережі LTE-M будуть співіснувати з мобільними мережами 2G, 3G і 4G і користуватися всіма функціями безпеки та конфіденційності мобільних мереж, такими як підтримка конфіденційності ідентифікаторів користувачів, аутентифікація об'єкта, конфіденційність, цілісність даних та ідентифікація мобільного обладнання.

EC-GSM-IoT (розширене покриття-GSM-IoT) - забезпечує нові можливості існуючих стільникових мереж для додатків IoT LPWA (малої потужності). EC-GSM-IoT можна

активувати за допомогою нового програмного забезпечення, розгорнутого на дуже великій площі GSM, що забезпечує ще більший радіус дії для обслуговування пристроїв IoT.

EC-GSM-IoT - це заснована на стандартах технологія малої потужності для глобальної мережі. Технологія заснована на eGPRS і розроблена як стільникова система з високою пропускну здатністю, великою дальністю, низьким енергоспоживанням та низькою складністю для IoT-зв'язку. Оптимізація, зроблена в EC-GSM-IoT, може бути зроблена як оновлення програмного забезпечення для існуючих мереж GSM. Термін служби батареї до 10 років може підтримуватися для широкого спектра випадків використання.

Bluetooth - це технологія зв'язку малого радіусу дії, вбудована в більшість смартфонів та мобільні пристрої, що є основною перевагою для персональних продуктів.

Bluetooth добре відомий мобільним користувачам. Але не так давно з'явився новий важливий протокол для додатків IoT - Bluetooth Low-Energy (BLE) або Bluetooth Smart. Ця технологія є реальною основою для IoT, оскільки вона масштабована та гнучка для всіх ринкових інновацій. Крім того, він призначений для зниження енергоспоживання. Це дуже активно використовується в автомобільній мережі. Він має невелику затримку в рази менше звичайних стандартів Bluetooth.

Працює на частоті 2,4 ГГц. Діапазон дії 50-150 м (Smart / BLE). Швидкість передачі даних:

1 Мбіт / с (Smart / BLE).

Wi-Fi - це технологія бездротового підключення пристроїв. Вона дозволяє використовувати високу швидкість передачі даних та здатна обробляти великі обсяги даних.

Це найпопулярніший тип підключення в локальній мережі.

Стандарт заснований на IEEE 802.11. Частоти: 2,4 ГГц і 5 ГГц. Радіус дії близько 50 м.

Швидкість передачі даних 150-200 Мбіт / с, максимум 600 Мбіт / с.

ZigBee 3.0 - це бездротова мережа з низьким енергоспоживанням і низькою швидкістю передачі даних, яка використовується в основному в промислових умовах.

Альянс Zigbee навіть створив універсальну мову для Інтернету речей - Dotdot, який дозволяє інтелектуальним об'єктам безпечно працювати в будь-якій мережі та легко розуміти один одного.

Це один з найбільш часто використовуваних стандартів в IoT, призначений для зв'язку в розумних будинках, пультах дистанційного керування та системи охорони здоров'я.

ZigBee Pro пропонує більше можливостей, включаючи безпеку з використанням обміну симетричними ключами, масштабованість з використанням стохастичного призначення адрес та стандартно високої якості завдяки ефективному багато-до-одного механізму маршрутизації.

Працює на частоті 2,4 ГГц, радіус дії 10-100м зі швидкістю передачі даних: 250 кбіт / с.

NB-Fi - відкритий протокол бездротової передачі даних малого об'єму на великих відстанях при низьких витратах енергії LPWAN. Призначений для побудови розподілених мереж телеметрії, межмашинної взаємодії та інтернету речей.

В основі стандарту NB-Fi покладено використання Ultra Narrow Band (UNB) фазоманіпульованих сигналів, які в поєднанні з перешкодостійким кодуванням дозволяють досягати дуже високих значень чутливості прийому (до мінус 150 дБм), при цьому сумарна смуга частот для одночасної передачі великої кількості каналів є досить вузькою. Це дозволяє забезпечувати зв'язок з пристроями на дуже великих відстанях від 10 км (місто) до 50 км (пряма видимість) при швидкості передачі від 0.3 кбіт / с до 50 Кбіт / с на канал шириною 100 Гц.

NB-Fi дозволений для вільного і безкоштовного використання при реалізації передачі на частоті 868 МГц та обмеженні потужності до 25 мВт на дальність ~ 120 метрів.

Мережа NB-Fi використовує топологію «зірка», де кожен пристрій безпосередньо взаємодіє з базовою станцією.

LoRaWAN (Long Range Wide Area Network) - оптимізований протокол для глобальних мереж, який призначений для підтримки величезних мереж (наприклад, розумних міст) з

мільйонами пристроїв з низьким енергоспоживанням. Він підтримує резервування, низьку вартість, низьке енергоспоживання та збір енергії.

LoRaWAN може забезпечити недорогий мобільний та безпечний двосторонній зв'язок в різних галузях промисловості. Радіус дії 2-5 км (міська зона), 15 км (приміська зона). Швидкість передачі даних 0,3-50 кбіт/с.

NB-IoT (вузькосмуговий IoT) - технологія, стандартизована 3GPP, яка призначена для підключення до цифрових мереж зв'язку широкого спектра автономних пристроїв. Наприклад, медичних датчиків, лічильників споживання ресурсів, пристроїв розумного будинку та ін. NB-IoT мережа може бути розгорнута як на обладнанні стільникових мереж LTE, так і окремо, в тому числі поверх GSM.

NB-IoT характеризується гнучким управлінням енергоспоживанням пристроїв (аж до 10 років в мережі від батареї ємністю 5 Вт ч), величезною ємністю мережі (десятки-сотні тисяч підключених пристроїв на одну базову станцію), низькою вартістю пристроїв, оптимізованою для поліпшення чутливості модуляції сигналу.

SigFox – технологія для створення бездротових мереж для підключення об'єктів з низьким енергоспоживанням, таких як лічильники електроенергії та розумних годинників, які повинні постійно включатися та передавати невеликі обсяги даних. Sigfox використовує диференціальну двійкову фазову маніпуляцію (DBPSK) та гаусову частотну маніпуляцію (GFSK), яка забезпечує зв'язок з використанням промислової смуги частот ISM, яка використовує 868 МГц в Європі та 902 МГц в США. Технологія використовує широко поширений сигнал, який вільно проходить крізь тверді об'єкти та потребує мало енергії. Існуючий стандарт зв'язку Sigfox підтримує до 140 повідомлень в день, кожне з яких може нести корисне навантаження в 12 октетів зі швидкістю передачі даних до 100 байтів в секунду.

Weightless - запатентований стандарт відкритих бездротових технологій для обміну даними між базовою станцією та тисячами пристроїв навколо неї (з використанням радіохвиль з довжиною хвилі в незайнятих телевізійних каналах передачі) з високим рівнем безпеки.

Спочатку було три опублікованих стандартів підключення Weightless Weightless-P, Weightless-N та Weightless-W. Weightless-N був першим стандартом, розробленим для підтримки IoT, який використовував TDMA зі стрибкоподібною перебудовою частоти для мінімізації завад. Він використовує ультратонкі смуги в смузі частот ISM нижче 1 ГГц. З іншого боку, Weightless-W надає ті ж функції, але використовує частоти телевізійного діапазону. Weightless (Weightless-P) став справжнім переможцем завдяки своїй двобічній вузькосмуговій технології, розробленій для роботи на глобальних ліцензованих і неліцензованих частотах ISM.

DDS (служба поширення даних) - це стандарт IoT для масштабованого та високопродуктивного зв'язку між комп'ютерами в режимі реального часу. Він був розроблений Object Management Group (OMG). DDS використовує архітектуру публікації/підписки і в основному використовується для зв'язку M2M.

DDS можливо розгорнути як на пристроях з невеликим розміром, так і в хмарі.

Стандарт DDS має два основних рівня:

- Data-Centric Publish-Subscribe (DCPS), який доставляє інформацію передплатникам;
- Рівень відновлення локальних даних (DLRL), який забезпечує інтерфейс для функцій DCPS.

Найвищими перевагами цього протоколу є висока якість обслуговування та надійність з використанням архітектури без посередників, яка підходить для IoT та M2M-зв'язку. Він пропонує 23 рівні якості обслуговування, які дозволяють пропонувати різні критерії якості, в тому числі: безпека, терміновість, пріоритет, довговічність, надійність та ін.

ANT - це запатентована технологія бездротової сенсорної мережі, в якій використовується стек протоколів бездротового зв'язку, що дозволяє здійснювати зв'язок між напівпровідниковими радіостанціями, що працюють в промисловому, науковому та

медичному розподілі радіочастотного спектру 2,4 ГГц (діапазон ISM). Представлення даних, сигналізація, аутентифікація та виявлення помилок.

EnOcean - це енергозберігаюча бездротова технологія, яка в основному використовується для автоматизації, але може використовуватися для інших додатків IoT (опалення, вентиляції та кондиціонування повітря та ін.). Основна ідея полягає в тому, щоб використовувати ефективно перетворення енергії руху або будь-якого типу енергії навколишнього середовища в корисну енергію за допомогою перетворювачів.

RPMA (довільний фазовий множинний доступ) - технологічна система зв'язку, яка використовує розширений спектр прямої послідовності (DSSS) з множинним доступом. Ця технологія LPWAN використовує неліцензований діапазон ISM 2,4 ГГц (промисловий, науковий та медичний). Ця технологія пропонує такі функції, як низьке енергоспоживання, окремий ширококомовний канал для швидких оновлень програмно-апаратних засобів та 128-розрядне шифрування AES для різних додатків IoT.

Технологія RPMA забезпечує швидкість завантаження 31 кбіт/с та швидкість передачі 15,6 кбіт/с. Вона схожа на NB-IoT, але з максимальною втратою зв'язку (MCL) 167 дБ, її сигнали досягають глибоко в будівлях та під землею. Ця технологія ідеально підходить для додатків IoT / M2M, оскільки пристрої здатні працювати більше 10 років без підзарядки. Це робить її ідеальною для пристроїв, які необхідно розміщувати в віддалених або в важкодоступних місцях, які не підключені до електромережі.

MQTT (message queuing telemetry transport)- це легкий протокол для відправки простих потоків даних від датчиків в додатки та проміжне програмне забезпечення.

Протокол працює поверх TCP / IP і включає в себе три компоненти: передплатник, видавець та брокер. Видавець збирає дані та відправляє їх передплатникам. Брокер тестує видавців і передплатників, перевіряє їх авторизацію та забезпечує безпеку.

MQTT підходить для невеликих, дешевих пристроїв з низьким обсягом пам'яті та низьким енергоспоживанням.

AMQP (Advanced Message Queuing Protocol) - це протокол прикладного рівня для середовищ проміжного програмного забезпечення, орієнтованих на повідомлення. Це схвалено як міжнародний стандарт.

Обробка протоколу складається із трьох компонентів, які слідують певним правилам.

1. Обмін - отримує повідомлення та розміщує їх в черзі
2. Черга повідомлень - зберігає повідомлення, поки вони не будуть безпечно оброблені клієнтським додатком
3. Прив'язка - встановлює зв'язок між першим та другим компонентами.

DASH7 - це новий протокол бездротового зв'язку, який використовується для активних RFID-пристроїв, працює на частоті ISM. Він в основному призначений для масштабованих мереж, з більш високою швидкістю передачі даних в порівнянні з традиційним ZigBee. Це недороге рішення, яке підтримує шифрування та адресацію IPv6.

GoodWAN - технологія що забезпечує передачу коротких, рідкісних, значимих повідомлень від економічних автономних датчиків, розташованих на великих відстанях один від одного. Створена для задач, в яких LTE-M та існуючі LPWAN мережі виявляються неефективними.

Головна особливість і основна перевага GoodWAN - це прямий канал (як у SigFox) з великою пропускну здатністю та високою завадозахищеністю і, одночасно, симетричний по дальності, простий в реалізації і дешевий зворотний канал (як у LoRa).

Для передачі в прямому каналі використовується UNB сигнал з частотною, а не фазовою модуляцією, як це реалізовано у SigFox, що значно покращує якість передачі інформації з рухомих об'єктів.

Цифрова обробка сигналу в базовій станції реалізована на спеціалізованому сигнальному процесорі, що зробило собівартість базової станції нижче конкурентів, без погіршення її характеристик та підвищило стійкість до «зависань» системи і знизило її енергоспоживання.

GoodWAN пропонує вирішення проблеми роумінгу рухомих об'єктів в мережі з безлічі просторово розподілених базових станцій, яка не має якісного рішення ні у SigFox, ні в протоколі LoRaWAN.

Проблеми IoT

Незважаючи на велику кількість стандартів IoT, успішне застосування IoT все ще залишається складним завданням через безліч проблем. Ці проблеми включають в себе: мобільність, надійність, масштабованість, управління, доступність, функціональну сумісність, витрати та забезпечення енергії.

Мобільність. IoT-пристрої повинні вільно переміщатися в середовищі і, отже, змінювати свої IP-адреси та підключатися до мереж в місцях їх розташування. Таким чином, протоколи маршрутизації, повинні бути реконструйовані кожен раз, коли вузол виходить з мережі або приєднується до мережі, що додає багато накладних витрат. Крім того, мобільність може привести до зміни постачальника послуг, що може додати ще один рівень складності через переривання обслуговування та зміни шлюзу.

Надійність. Для додатків аварійного реагування дуже важливо, щоб система працювала ідеально та поставляла всі свої специфікації правильно. Отже, в додатках IoT система повинна бути дуже надійною та швидко збирати дані, передавати їх та приймати рішення. Неправильні рішення можуть призвести до катастрофічних сценаріїв.

Масштабованість. Оскільки мільйони та трильйони пристроїв підключаються в одному додатку IoT, масштабованість стає проблемою, яку повинно вирішувати. Додатки IoT повинні бути терпимі до нових послуг та пристроїв, постійно підключаються до мережі і, отже, повинні бути розроблені для забезпечення розширюваних послуг та операцій.

Управління. Існують протоколи для віддаленого керування пристроями, але ці протоколи не можуть бути застосовані до всіх програм IoT. Провайдери повинні управляти несправностями, конфігураціями, обліком, продуктивністю та безпекою (FCAPS) їх взаємопов'язаних пристроїв.

Доступність. Наявність платформ IoT має гарантувати доступність як програмного, так і апаратного забезпечення для користувачів системи та передплатників сервісу. Наявність програмного забезпечення означає, що послуги надаються користувачам, навіть коли трапляються збої. Наявність обладнання означає, що до існуючих пристроїв легко отримати доступ що сумісний з різними протоколами. Крім того, ці протоколи повинні бути досить компактними, щоб бути вбудованими в обмежені пристрої IoT.

Сумісність означає, що гетерогенні пристрої та протоколи повинні мати можливість взаємодіяти з кожним іншим. Це складно через велику кількість різних платформ, що використовуються в системах IoT. Сумісність повинна здійснюватися як розробниками додатків, так і виробниками пристроїв, щоб забезпечити послуги незалежно від використовуваної клієнтом платформи або апаратного забезпечення.

Вартість та складність. Незважаючи на відносно дешеві ціни на пристрої IoT, такі як датчики та інтелектуальні перетворювачі, вони все ще коштують занадто дорого, щоб побудувати додаток IoT. Така складна інтеграція різних протоколів та стандартів робить IoT програми не доступні для загального користування. Зниження вартості та складності є величезною проблемою.

Збір енергії все ще залишається проблемою в пристроях IoT через відсутність технологій збору енергії для таких невеликих пристроїв з обмеженими ресурсами. Живлення є критичною проблемою в IoT, оскільки ці пристрої повинні працювати декілька років без заміни батареї. Отже, збирати енергію з руху або будь-якого іншого джерела енергії та перетворювати її в накопичену енергію, що є критичною задачею для таких пристроїв.

Висновки

Інтернет речей став основою цифрової трансформації та автоматизації, розробки нових бізнес-пропозицій та поліпшення нашого способу життя, роботи та розваг. Вибір відповідного типу підключення є неминучою частиною будь-якого проекту IoT.

У цій статті представлено всебічний огляд протоколів, технологій та стандартів для IoT. Багато з цих протоколів мають були розроблені та стандартизовані IETF, IEEE, MCE та іншими організаціями, в той час як багато інших у розвитку.

Існує багато поточних проблем IoT, в тому числі: мобільність, надійність, масштабованість і багато інших. Незважаючи на обсяг роботи в області мобільності, масштабованості та управління, підприємства як і раніше страждають від проблем.

Список використаної літератури

1. Joe Decuir. Standards Architect, gy CSR Technology Councilor, Bluetooth Architecture Review Board IEEE Region 6 Northwest Area chair [Електронний ресурс] / Joe Decuir – Режим доступу до ресурсу: <https://californiaconsultants.org/wp-content/uploads/2014/05/CNSV-1205-Decuir.pdf>. (15.05.2019).

2. Sakovich N. Internet of Things (IoT) Protocols and Connectivity Options: An Overview [Електронний ресурс] / Natalia Sakovich. – 2018. – Режим доступу до ресурсу: <https://www.sam-solutions.com/blog/internet-of-things-iot-protocols-and-connectivity-options-an-overview/>. (22.05.2019г).

3. Gomez C. “Overview and evaluation of Bluetooth low energy: An emerging low-power wireless technology,” in Sensors / C. Gomez, J. Oller, J. Paradells. // vol. 12, no. 9. – 2012. – pp. 11734–11753.

4. Zigbee resource guide [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: http://www.nxtbook.com/nxtbooks/webcom/zigbee_rg2016/#/0. (15.05.2019).

5. LoRaWAN specification [Електронний ресурс] / [N. Sornin, M. Luis, T. Eirich та ін.] // LoRa Alliance. – 2015. – Режим доступу до ресурсу: <https://www.loraalliance.org/portals/0/specs/LoRaWAN%20Specification%201R0.pdf>. (28.04.2019).

6. Khaldoun Al Agha. Mobile and Wireless Networks / Khaldoun Al Agha, Guy Pujolle, Tara Ali Yahya. // Wiley. – 2016. – pp. 241.

7. Tara Salman. A Survey of Protocols and Standards for Internet of Things [Електронний ресурс] / Tara Salman, Raj Jain // arxiv. – 2019. – Режим доступу до ресурсу: <https://arxiv.org/ftp/arxiv/papers/1903/1903.11549.pdf>. (4.05.2019).

Автори статті

Домрачева Катерина Олексіївна – кандидат технічних наук, доцент кафедри телекомунікаційних систем та мереж, Державний університет телекомунікацій, Київ, Україна.

Довженко Надія Михайлівна – кандидат технічних наук, доцент кафедри інформаційної та кібернетичної безпеки, Державний університет телекомунікацій, Київ, Україна.

Дмитренко Володимир Віталійович – асистент кафедри телекомунікаційних систем та мереж, Державний університет телекомунікацій, Київ, Україна.

Authors of the article

Domracheva Kateryna Oleksiivna – candidate of Science (technic), Associate Professor of the Department of Telecommunication Systems and Networks, State University of Telecommunications, Kyiv, Ukraine.

Dovzhenko Nadiia Michailivna – candidate of Science (technic), Associate Professor of the Department of Information and Cybersecurity, State University of Telecommunications, Kyiv, Ukraine.

Dmitrenko Volodymyr Vitaliyovych - Assistant Professor, Department of Telecommunication Systems and Networks, State University of Telecommunications, Kyiv, Ukraine.

Дата надходження в редакцію: 24.06.2019 р.

Рецензент: д.т.н., доцент В.Ф. Заїка