УДК 004.7 **doi: 10.26906/SUNZ.2021.2.078**

А. А. Коваленко[1], Р. О. Ярошевич[1], О. І. Баленко[2]

[1] Харківський національний університет радіоелектроніки, Харків, Україна
[2] Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

INTERNET OF THINGS: ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА МЕТОДИ ПОКРАЩЕННЯ

Анотація. Новий виток технічного розвитку цивілізації, в переході до автоматизації не тільки процесів на виробничих підприємствах, але і процесів, що протікають в повсякденному житті кожної людини, полягає у використанні великої кількості невеликих малопотужних з обчислювальної та енергетичної точки зору пристроїв для виконання однотипних простих завдань. Така технологія закладена в основі узагальненої назви «Інтернет речей» (IoT). Кінцева мета якої – дозволити об'єктам навколо нас ефективно відчувати наше середовище, легко взаємодіяти і врешті-решт створити для нас кращий світ. З огляду на це, дозволяючи пристроям обмінюватися даними, коли вони не належним чином захищені, Інтернет відкриває їм ряд значних вразливих місць. Поряд з усіма перевагами і можливостями нових технологій виробники компонентів системи «Інтернет речей» не приділяють належної уваги проблемам інформаційної безпеки, які виникають при повсякденному використанні як окремих компонентів системи, так і цілого апаратно-програмного комплексу. Основна причина відмова виробників впроваджувати компоненти безпеки – це великі обчислювальні витрати, а отже, велика витрата електричної енергії, що має дуже важлива для апаратури, що працює від автономного джерела живлення. До того ж це призводить до подорожчання системи «Інтернет речей». Це дослідження зосереджене на розгляданні загроз і вразливостях безпеки на кожному рівні архітектури IoT та існуючих технологій доступу, їх слабкі сторони, а також пропонуються рішення для поліпшення загальної безпеки системи за допомогою локального шлюзу IoT.

Ключові слова: Інтернет речей; інформаційна безпека; трирівнева архітектура; шлюз.

Вступ

Internet of Things (Інтернет речей) – мережа фізичних або віртуальних унікальних ідентифікаторів, підключених безпосередньо або частково до Інтернету, які здатні ефективно передавати дані за допомогою збору та обміну інформацією, без необхідності взаємодії людини з людиною або людини з комп'ютером. Сьогодні технології Інтернету речей активно впроваджуються в усі сфери життя суспільства, дозволяючи використовувати різні пристрої, не обов'язково фізичні, для створення конкретних рішень, здатних полегшити життя людства. Пристрої стають здатними чути, бачити, думати, в деяких випадках діяти. Для правильної і ефективної роботи пристрою повинні коректно спілкуватися і координувати свої дії з іншими для того, щоб приймати ті чи інші рішення. Технології розподілених обчислень, вбудовані датчики, сучасні бездротові технології дозволяють Інтернету речей виконувати поставлені завдання.

Однією з головних проблем IoT є забезпечення інформаційної безпеки. Традиційні заходи безпеки і дотримання конфіденційності не можуть бути застосовані до технологій IoT, зокрема, через їх обмежену обчислювальну здатність. Окрім того, велика кількість підключених пристроїв створює проблему масштабованості. Тому необхідно обов'язково забезпечити дотримання безпеки, конфіденційність і моделі довіри, які підходять для контексту IoT. Основна ціль дослідження присвячена аналізу проблем забезпечення інформаційної безпеки IoT. Для вирішення цього було прийнято проаналізувати:

- багаторівневу структуру IoT;
- проблеми забезпечення безпеки на кожному з рівнів прийнятої структури IoT;
- дослідження забезпечення інформаційної безпеки IoT.

Архітектура

Розробка успішних програм IoT включає в себе завдання забезпечення мобільності: при переміщенні IoT пристрою змінюється IP-адреса, отже, необхідна налагоджена робота протоколів маршрутизації; надійності (система повинна бути дуже надійною і швидкою в плані збору і передачі даних і прийняття рішень), масштабованості, тобто можливості розширення користувачів мережі. Концепція Інтернету речей передбачає, що до мережі буде підключено мільйони пристроїв. Також серед завдань необхідно відзначити забезпечення управління та доступності: відстеження збоїв, конфігурації і продуктивності такої великої кількості пристроїв, за що відповідають відповідні протоколи управління. Крім того необхідно забезпечити сумісність в мережі: гетерогенні пристрої та протоколи повинні бути в змозі працювати один з одним з урахуванням збереження безпеки і конфіденційності.

Існуюча архітектура Інтернету з її TCP/IP-протоколами не може впоратися з такою великою мережею, як IoT. Тому виникає необхідність в новій відкритій архітектурі, яка може відправляти звіти про безпеку, якість і клас послуг, які надаються передачі даних (QoS), разом з тим підтримуючи існуючі мережні додатки та використовуючи відкриті протоколи. Інтернет речей не може бути впроваджений без належних гарантій безпеки. Отже, захист даних і приватність є ключовими завданнями для IoT.

Для подальшого розвитку IoT запропонована багаторівнева архітектур безпеки[1].

Результати досліджень

1. Багаторівнева структура IoT. Структуру IoT можна розділити на три рівні – рівень сприйняття, мережний рівень та прикладний рівень (рис. 1).

Рис. 1. Трирівнева архітектура IoT

Рівень сприйняття – рівень пристроїв IoT, що надає кожному об'єкту фізичне значення. Він складається з датчиків даних різних видів, таких, як RFID-мітки, IR датчики або інші мережі датчиків, які можуть зчитувати температуру об'єкта, вологість, швидкість, місце розташування і т.д [2]. Цей рівень збирає корисну інформацію про об'єкти від датчиків, з'єднаних з ними, і перетворює цю інформацію в цифрові сигнали, які потім передаються до архітектури мережі для подальшої обробки. Завдання рівня сприйняття отримати надійне зчитування інформації про об'єкт, в будь-якому місці і в будь-який час. Мережний рівень –забезпечує повсюдний доступ, обробку, зберігання та передачу інформації за допомогою WiFi, Bluetooth, WiMaX, Zigbee, GSM, 3G і т.д., використовуючи протоколи IPv4, IPv6 , MQTT, DDS і т.д. Мережний рівень складається з рівня доступу (мобільні мережі зв'язку), і основного рівня обміну (Інтернет, мережі наступного покоління NGN, віртуальні приватні мережі).

Прикладний рівень аналізує і обробляє отриману контактну інформацію для прийняття правильного рішення і контролю за управлінням, додатками і послугами, використовуючи такі технології, як хмарні обчислення, глобальні обчислення, гарантуючи прямий доступ до бази даних для того, щоб помістити в неї всю необхідну інформацію. Використовуючи Intelligent Processing Equipment (обладнання інтелектуальної обробки), інформація обробляється, а потім виконується повністю автоматизована дія на основі результатів обробки цієї інформації.

Слід зазначити, що в деяких роботах розглядається більш, ніж трирівнева архітектурі IoT. В роботі [1] прийнята шестирівнева архітектура IoT включає, окрім цих трьох рівнів, рівень кодування, рівень додатків та бізнес-рівень. Де, наприклад, рівень кодування – ідентифікує об'єкт інтересу (основа Інтернету Речей). Цей рівень призначає кожному об'єкту свій унікальний ідентифікатор (ID), що дозволяє легко розрізняти об'єкти.

2. Проблеми інформаційної безпеки на рівнях структури IoT. Проблеми безпеки на рівні сприйняття включає фізичні захоплення сенсорних вузлів, захоплення вузла шлюзу, витік інформації сенсора, загрози цілісності даних, виснаження енергозабезпечення, загрози перевантаження, атаки типу DoS (відмова в обслуговуванні), загрози маршрутизації встановленням в мережу нелегітимних сенсорів, і загрози копіювання вузла [2].

IoT приймає інформацію від великої кількості пристроїв, збирає великий масив даних різних форматів від безлічі джерел з неоднорідними характеристиками. В результаті цього на мережному рівні мають місце більш складні проблеми безпеки. До них відносяться можливі проблеми масштабованості мережі, викликані малопередбачуваним обсягом передачі даних від великого числа вузлів, що призводять до можливості здійснення атак DoS, DDoS, також несанкціонований доступ, перехоплення даних, конфіденційність, цілісність, віруси, експлойти, тощо. Окрема увага приділяється вразливостям програмного забезпечення (software vulnerabilities), що призводить до порушення безпеки після впровадження.

Причинами програмної вразливості можуть бути помилки розробників складного багатошарового програмного забезпечення (ПО), помилки ядра програми, застосування незахищеного коду, необроблених масивів з можливістю їх переповнення зловмисником, помилки в обробці Big Data, помилки БД, відсутність належної індексації або закріплення запитів БД, web-уразливості, недостатня продуктивність або масштабованість ПО, помилки розподіленої роботи додатків, а також віртуальних платформ і хмар. Слід зазначити складність ПО в IoT, викликану великою різноманітністю використовуваних апаратних платформ і операційних систем. Для проектування ПО необхідно емулювати поведінка приладів IoT, тобто створити імітатор зовнішнього середовища для серверів. Унаслідок обмежень в приладах (енергозабезпечення, продуктивність процесора, пам'ять) в IoT стоїть складне завдання уникнути сильного розбіжності між емулятором і приладом [2].

Крім порушення інформаційної безпеки традиційних мереж зв'язку додатки IoT стикаються з додатковими проблемами безпеки на прикладному рівні – при використанні хмарних обчисленнях, обробці інформації, забезпеченні прав на інтелектуальну власність, захист приватності та ін.

3. Методи підвищення захисту. Виходячи з усього вищесказаного та враховуючи вимоги до безпеки інформаційних систем, можна зробити висновок, що існують різні підходи для визначення та запобігання загроз. На основі розглянутої структури, а також з урахуванням тенденцій розвитку технології «Інтернет речей» можна запропонувати наступні методи підвищення захищеності архітектури.

Одним із рішень для покращення захисту структури – це використання шлюзів IoT, який буде розміщуватися на мережному рівні. Оскільки можливості і потреби пристроїв збільшуються, їх часто неможливо отримати спілкуючись безпосередньо з системами. Деякі датчики і контролери не підтримують енергоємні протоколи, такі як Wi-Fi або Bluetooth, і всі вони підключаються до безлічі громадських і приватних мереж (рис. 2).

Шлюз Інтернету речей виконує кілька важливих функцій: від переведення протоколів до шифрування, обробки, управління і фільтрації даних, за рахунок оптимізації продуктивності системи за допомогою зібраних ними операційних даних, які обробляються в режимі реального часу.

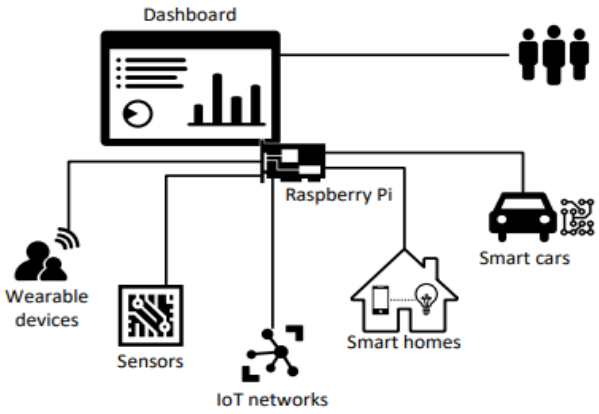

Рис. 2. «Хмара» на базі домашньої системи[4]

Шлюзи IoT можуть виконувати:

- висока масштабованість – вони можуть брати інтелектуальні дані з центру обробки даних або хмари і передавати їх до мережі;
- зниження витрат – кінцеві пристрої не обов'язково повинні мати таку високу обчислювальну потужність, пам'ять або сховище, оскільки шлюз робить все це за них[3];
- зниження витрат на зв'язок – менша кількість повідомлень M2M означає меншу мережу і (WAN) трафік;
- зниження ризиків – шлюзи можуть ізолювати непрацюючі пристрої і датчики до того, як вони вийдуть із ладу.

До методів підвищення захищеності архітектури на рівні сприйняття можна віднести:

- уніфікація кодування – розробка єдиного для всіх пристроїв протоколу кодування інформації, у 1-й черзі використовується технологія RFID, де використовуються європейські та японські стандарти [3];
- коди корекції – допомагають уникнути колізій, які виникають при одночасному зчитуванні інформації з багатьох безпровідних пристроїв;
- захист конфіденційності RFID;
- протоколи аутентифікації пристроїв – як правило, реалізовані у вигляді парольної схеми;
- шифрування інформації, що передається мережею, використання простих симетричних алгоритмів;
- протоколи безпечної маршрутизації, а також управління передачею між пристроями на сьогоднішній момент будуються на використанні сертифікатів достовірностей, наприклад X.509 та ін.;
- уніфікація протоколу передачі даних – складається з визначення формату представлення даних: XML, JSON або ін.

На останньому рівні розгляду аспектів безпеки, пов’язаних із веб-сервісами та хмарними обчисленнями. Так як ці елементи не мають явної специфіки щодо середовища «Інтернет речей», увагу на них акцентувати не будемо.

Висновки

Стрімкий розвиток в практичному плані концепції Інтернету речей, викликане широким поширенням безпровідних технологій та міжмашинним обміном, розвитком технологій хмарних обчислень і початком переходу на IPv6. Однак використання IoT у багатьох областях обмежено складними проблеми в сфері забезпечення інформаційної безпеки. В даній роботі виконано аналіз багаторівневої архітектури IoT, а саме: рівень сприйняття, мережний рівень та прикладний рівень. Проаналізовано проблеми забезпечення безпеки на кожному з рівнів прийнятої структури та запропоновано методи визначення та запобігання загроз середовища «Інтернет речей».

СПИСОК ЛІТЕРАТУРИ

1. «Интернет Вещей: концепция, приложения и задачи» [Електронний ресурс] – Режим доступу до ресурсу https://cyberleninka.ru/article/n/internet-veschey-kontseptsiya-prilozheniya-i-zadachi/viewer.
2. «ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНТЕРНЕТ ВЕЩЕЙ: ОБЗОР» [Електронний ресурс] – Режим доступу до ресурсу https://cyberleninka.ru/article/n/problemy-bezopasnosti-internet-veschey-obzor/viewer.
3. «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ ИНТЕРНЕТ ВЕЩЕЙ» [Електронний ресурс] – Режим доступу до ресурсу https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-sisteme-internet-veschey/viewer.
4. «INTERNET OF THINGS SECURITY PROBLEMS» [Електронний ресурс] – Режим доступу до ресурсу https://www.researchgate.net/publication/331318204_Internet_of_Things_Security_Problems

Received (Надійшла) 22.01.2021
Accepted for publication (Прийнята до друку) 31.03.2021

Internet of things: problems of information security and methods of improvement

Andriy Kovalenko, Roman Yaroshevich, Oleksii Balenko

Abstract. A new round of technical development of civilization, in the transition to automation of not only processes in industrial enterprises, but also processes occurring in everyday life, is to use a large number of small low-power from a computational and energy point of view devices to perform simple tasks. This technology is the basis of the generalized name "Internet of Things" (IoT). Its ultimate goal is to allow the objects around us to effectively feel our environment, interact easily, and ultimately create a better world for us. Because of this, by allowing devices to communicate when they are not properly protected, the Internet opens up a number of significant vulnerabilities. Along with all the advantages and capabilities of new technologies, manufacturers of Internet of Things components do not pay due attention to the problems of information security that arise in the daily use of individual components of the system and the whole hardware and software complex. The main reason for the failure of manufacturers to implement safety components is the high computational costs and, consequently, the high consumption of electrical energy, which is very important for equipment running on a stand-alone power supply. In addition, it leads to more expensive Internet of Things. This study focuses on addressing security threats and vulnerabilities at each level of the IoT architecture and existing access technologies, their weaknesses, and offers solutions to improve the overall security of the system through a local IoT gateway.

Keywords: Internet of Things; informational security; three-level architecture; sluice.