ІНТЕГРАЦІЯ WIRELESS SENSOR NETWORKS В INTERNET OF THINGS ТА ОСНОВНІ НАПРЯМКИ БЕЗПЕКИ

Удинська А.Р., ст.гр. ТКРм-20, ФКІТАЕР,
anna.udynska.fkitaer@donntu.edu.ua
Донецький національний технічний університет, м. Покровськ, Україна

Інтеграція бездротових сенсорних мереж (WSN) в IoT - це не просто припущення, оскільки ряд великих технологічних компаній підтримують і розвивають свою інфраструктуру IoT на основі WSN. Важливим є питання, як вузли датчиків повинні надавати свої послуги при підключенні WSN до Інтернету; або безпосередньо, або через базову станцію. «Об'єкт», підключений до Інтернету, має бути доступний для пошуку та адресації через Інтернет, але ця конкретна конфігурація може не підходити для певних сценаріїв. У деяких конкретних сценаріях, наприклад, в системах SCADA сенсорний вузол не повинен надавати свої послуги безпосередньо, а в інших сценаріях сенсорний вузол повинен бути повністю інтегрований в Інтернет.

Існують різні підходи до інтеграції WSN в IoT в залежності від вимог програми та розгорнутою інфраструктури WSN:

–повністю незалежна від інтернету, де WSN має власний протокол і вузли датчиків взаємодіють через централізований пристрій, який називається базовою станцією. Будь-який запит, що надходить з Інтернет-хосту, проходить через базову станцію, яка збирає і утримує всі дані з вузлів датчиків. Якщо базова станція діє в якості шлюзу прикладного рівня, то інтернет-хости і вузли датчиків можуть звертатися один до одного і обмінюватися інформацією без створення прямого з'єднання. WSN як і раніше не залежить від інтернету, всі запити проходять через шлюз.

–вузли датчиків впроваджують стек TCP / IP (або сумісний набір протоколів, такий як 6LoWPAN), так що будь-який інтернет-хост може мати з ними прямий зв'язок і навпаки. Вузли датчиків можуть більше не використовувати певні протоколи WSN.

–існує ще один заснований на топології інтеграційний підхід, при якому рівень інтеграції залежить від фактичного розташування вузлів, вузлами можуть бути подвійні датчики (базові станції), розташовані в корені WSN, або повноцінні магістральні пристрої, що дозволяють вузлам датчиків отримувати доступ в Інтернет в режимі точки доступу.

Еволюція IoT бере свій початок в конвергенції бездротових технологій, досягнень MEMS і цифрової електроніки, де в результаті мініатюрні пристрої, здатні відчувати і обчислювати, спілкуються по бездротовому зв'язку. Однак наявність IP-зв'язку не означає, що кожен вузол датчика повинен бути безпосередньо підключений до Інтернету.

Існує безліч проблем, які повинні бути ретельно продумані, і однією з таких проблем є безпека. З триваючим впровадженням IP-мереж додатки

IoT вже стали мішенню для атак, масштаби і витонченість яких будуть продовжувати рости. Взаємопов'язаний характер пристроїв Інтернету речей означає, що кожен погано захищений пристрій, підключений до мережі, потенційно впливає на безпеку і відмовостійкість Інтернету в усьому світі. Найслабша ланка визначає загальний рівень безпеки всієї інфраструктури. Ця проблема посилюється іншими міркуваннями, такими як масове розгортання однорідних пристроїв IoT, здатність деяких пристроїв автоматично підключатися до інших пристроїв і можливість розміщення цих пристроїв в небезпечних середовищах. Інтернет речей ставить нові завдання перед безпекою. Необхідно розвивати більш розумні системи безпеки, які включають кероване виявлення загроз, виявлення аномалій і прогнозний аналіз[1].

Існують різні проблеми при розробці рішень безпеки в IoT, наприклад, через пропускну здатність мережі, неоднорідність пристроїв, обмеження ресурсів, ненадійні канали зв'язку і розподілений характер.

У традиційних мережах TCP / IP безпека побудована на захисті конфіденційності, цілісності та доступності мережевих даних. Це робить систему надійною і захищає систему від зловмисних атак, які можуть привести до збоїв в роботі систем і розкриття інформації. Для Інтернету речей потрібні багатогранні рішення безпеки, в яких зв'язок захищений за допомогою служб конфіденційності, цілісності і автентифікації; мережа повинна бути захищена від вторгнень і збоїв. Вузол датчика, як в WSN, висуває додаткові вимоги до захисту і конфіденційності користувачів в залежності від сценарію застосування.

В IPv6 досить IP-адрес для з'єднання мільярдів «речей», щоб сформувати новий світ Інтернету речей, але чи будуть ці речі досить захищені, щоб гарантувати індивідуальні права на конфіденційність і захистити системи від зловмисних атак?

Криптографічні алгоритми повинні бути високоефективними, з низьким енергоспоживанням, особливо для пристроїв з батарейним або пасивним живленням. У багатьох практичних додатках шлюз повинен відправляти періодичні керуючі повідомлення, сповіщення і конфіденційні дані на все носимі пристрої, де для шифрування широкомовних повідомлень потрібен загальний секретний ключ.

Криптографія з симетричним ключем, така як AES, забезпечує швидке і легке шифрування / дешифрування на таких інтелектуальних пристроях, а їх вбудоване обладнання також підтримує його. Однак коли ця кількість підключених пристроїв стає великою, обмін симетричними ключами стає неможливим, і потреба в ефективному протоколі створення масштабованого ключа стає критичною.

Інший підхід полягає в розподілі ключів за допомогою криптографії з асиметричним ключем, але він вимагає великих обчислювальних витрат - це основна проблема для пристроїв з обмеженими ресурсами. Тому традиційні методи безпеки не можуть бути застосовані через неоднорідність датчиків

(вбудованих або переносних), обмеженості ресурсів і системної архітектури.

Пристрої будуть розумними тільки в тому випадку, якщо вони будуть включати в себе технології, що забезпечують безпеку і конфіденційність. Погано захищені пристрої IoT можуть служити точками входу для кібератак, дозволяючи зловмисникам перепрограмувати пристрій або викликати його несправність. Більш того, унікальність криптографічних реалізацій полягає в тому, що вони також потребують захисту від фізичного втручання, активного або пасивного. Це означає, що контрзаходи повинні бути включені в процес проектування. Безпека в IoT повинна забезпечувати секретність і цілісність зв'язку, а також автентичність повідомлень, якими обмінюються.

З точки зору кінцевого користувача, неможливо легко модифікувати такі інтелектуальні пристрої - система безпеки повинна бути попередньо вбудована в систему. Інтеграція датчиків в Інтернет повинна забезпечувати функціональну сумісність, прозорість і гнучкість. Однак вузли датчиків за своєю природою мають обмежені ресурси - невеликі батареї, як правило, є основними джерелами енергії для цих вузлів датчиків з вимогою працювати протягом більш тривалого часу. Отже, енергоефективність стає важливим фактором крім питань безпеки та конфіденційності.

Для безпечного зв'язку E2E в WSN і IoT використовуються різні підходи, які можна розділити на наступні основні напрямки[2]:

– централізовані підходи;

– розширення та оптимізація на основі протоколів;

– альтернативні архітектури подання інформації;

– рішення, що вимагають наявності спеціальних апаратних модулів.

Також важливо розуміти методи атак, щоб раціоналізувати механізми безпеки в протоколах зв'язку. Деякі атаки відносно Інтернету речей:

– Прослуховування: процес прослуховування поточного зв'язку, що також є попередньою умовою для запуску наступних атак. В бездротовому зв'язку всі мають загальний доступ до середовища, тому для запуску потрібно менше зусиль у порівнянні з дротовим зв'язком.

– Імперсонація: зловмисник прикидається законним суб'єктом, наприклад, відтворює загальне повідомлення, щоб обійти вищезгадані цілі безпеки.

– Атака MITM: Атака «людина посередині» має місце, коли зловмисний об'єкт знаходиться на мережевому шляху двох справжніх об'єктів.

– DoS-атака: націлена на доступність системи, що пропонує послуги, досягається за рахунок виснажливого споживання ресурсів, щоб пропоновані послуги стали недоступні законним суб'єктам.

Традиційні методи безпеки не можуть бути застосовані через неоднорідність датчиків, низьких ресурсів і системну архітектуру систем на основі

IoT. Будь-яке несанкціоноване використання даних може обмежити використання додатків на базі IoT. Щоб зменшити ці загрози безпеки і конфіденційності, необхідна потужна інфраструктура мережевої безпеки. Однорангова аутентифікація і наскрізний захист даних є важливими вимогами для запобігання перехоплення конфіденційних даних або зловмисного запуску шкідливих завдань.

Деякі інші напрямки безпеки, які потребують уваги[3]:

–Забезпечення ідентифікації пристрою і механізмів його аутентифікації. Пристрої Інтернету речей можуть не мати необхідної обчислювальної потужності, пам'яті або сховища для підтримки поточних протоколів аутентифікації. Отже, аутентифікація і авторизація потребуватимуть відповідного реінжинірингу, щоб пристосуватися до нового підключеному світу Інтернету речей.

– захист вихідної конфігурації і ініціалізації пристроїв від злому, крадіжки та інших форм злому протягом усього терміну служби, який у багатьох випадках може становити роки;

– застосування географічного положення та рівнів конфіденційності до даних;

– посилення інших методів, орієнтованих на мережу, таких як система доменних імен (DNS) з DNSSEC і DHCP, для запобігання атак;

– прийняття інших протоколів, більш стійких до затримок або перехідним з'єднанням (наприклад, мережі з затримкою);

– зв'язок і канали передачі даних повинні бути захищені, щоб дозволити пристроям відправляти і збирати дані до систем збору даних і від них. Хоча не всі кінцеві точки IoT можуть мати двосторонній зв'язок, використання SMS (автоматично або через адміністратора) дозволяє забезпечити безпечний зв'язок з пристроєм, коли необхідно вжити заходів.

Література

1. Круз Л. Интернет вещей и информационная безопасность: защита информации // Инсайд. 2013. № 6. С. 60–61.

2. Ивлиев С. Н. Предварительный анализ технической защищенности системы дистанционного образования (на материале Мордовского государственного университета) // Интеграция образования. 2012. № 4 (69). С. 27–31.

3. Ивлиев С. Н. Решение вопросов технической защиты информации в системе дистанционного образования Мордовского государственного университета // Отраслевые аспекты технических наук. 2012. № 6 (18). С. 13–16.

Анотація

Загальне бачення інтелектуальних систем сьогодні, за великим рахунком, асоціюється з однією єдиною концепцією - Інтернетом речей (IoT), де вся фізична інфраструктура пов'язана з інтелектуальними технологіями моніторингу та зв'язку за допомогою використання бездротових датчиків. У такій інтелектуальній динамічній системі датчики

підключаються для передачі корисної інформації та інструкцій з управління через розподілені сенсорні мережі. Бездротові датчики мають просте розгортання і кращу гнучкість пристроїв на відміну від дротової установки. З швидким технологічним розвитком датчиків, бездротові сенсорні мережі (WSN) стануть ключовою технологією для Інтернету речей (IoT) і безцінним ресурсом для реалізації бачення парадигми IoT. Також важливо розглянути питання про те, чи повинні датчики WSN бути повністю інтегровані в IoT чи ні. Нові проблеми в області безпеки виникають, коли датчики інтегровані в IoT. Питання безпеки необхідно розглядати в глобальній перспективі, а не тільки на місцевому рівні. У цій статті представлений огляд інтеграції датчиків в IoT, деякі основні проблеми безпеки, а також ряд напрямків безпеки, які можна використовувати для захисту своїх даних в Інтернеті.

Аннотация

Общее видение интеллектуальных систем сегодня, по большому счету, ассоциируется с одной единственной концепцией - Интернетом вещей (IoT), где вся физическая инфраструктура связана с интеллектуальными технологиями мониторинга и связи посредством использования беспроводных датчиков. В такой интеллектуальной динамической системе датчики подключаются для передачи полезной информации и инструкций по управлению через распределенные сенсорные сети. Беспроводные датчики имеют простое развертывание и лучшую гибкость устройств в отличие от проводной установки. С быстрым технологическим развитием датчиков, беспроводные сенсорные сети (WSN) станут ключевой технологией для Интернета вещей (IoT) и бесценным ресурсом для реализации видения парадигмы IoT. Также важно рассмотреть вопрос о том, должны датчики WSN быть полностью интегрированы в IoT или нет. Новые проблемы в области безопасности возникают, когда датчики интегрированы в IoT. Вопрос безопасности необходимо рассматривать в глобальной перспективе, а не только на местном уровне. В этой статье представлен обзор интеграции датчиков в IoT, некоторые основные проблемы безопасности, а также ряд направлений безопасности, которые можно использовать для защиты своих данных в Интернете.

Abstract

The common vision of intelligent systems today, by and large, is associated with one single concept - the Internet of Things (IoT), where the entire physical infrastructure is connected with intelligent monitoring and communication technologies through the use of wireless sensors. In such an intelligent dynamic system, sensors are connected to transmit useful information and control instructions via distributed sensor networks. Wireless sensors are easy to deploy and have better device flexibility than wired installations. With the rapid technological development of sensors, wireless sensor networks (WSNs) will become a key technology for the Internet of Things (IoT) and an invaluable resource for realizing the vision of the IoT paradigm. It is also important to consider whether WSN sensors should be fully integrated into the IoT or not. New security challenges arise when sensors are integrated into the IoT. Security needs to be viewed from a global perspective, not just at the local level. This article provides an overview of sensor integration in the IoT, some of the main security issues, and a number of security areas that you can use to protect your data online.