УДК 004.738

ПРОТОКОЛ МНОЖИННОЇ АВТЕНТИФІКАЦІЇ, ЯК ОСНОВА БЕЗПЕЧНОГО ОБМІНУ ІНФОРМАЦІЄЮ НА БАЗІ ІНТЕРНЕТУ РЕЧЕЙ

Б.В. Сіндєєв, студент
Київський національний університет технологій та дизайну
Г.М. Мельник, кандидат технічних наук, доцент
Київський національний університет технологій та дизайну
О.З. Колиско, кандидат технічних наук, доцент
Київський національний університет технологій та дизайну

Ключові слова: протокол, Інтернет речей, автентифікація, безпека, обмін, ключ, інформація.

В останні роки швидкий прогрес технологій спричинив значний прорив як у мережевій індустрії, так і в комунікаційній інфраструктурі, що запровадило сучасну мережеву концепцію під назвою Інтернет речей (IoT) у сферу мереж і технологій [1]. Крім того, важливою проблемою є те, що IoT затвердив свою позицію в поточному комунікаційному ландшафті, демонструючи помітну важливість і ефективність у сприянні підключенню широкого спектру елементів і пристроїв [2]. Спеціалізована категорія мереж, відома як мережі з низьким енергоспоживанням і втратами (LLN), була ідентифікована в комунікаційній інфраструктурі Інтернету речей [3]. Використання LLN можна розглядати як ефективне в проектуванні та розвитку інфраструктури й бізнес-пристроїв. У розгалуженому домені, охопленому IoT, представлені мережі з низьким енергоспоживанням і втратами, що включають пристрої з обмеженими ресурсами, такі як датчики та мітки радіочастотної ідентифікації (RFID) [4].

Процедура маршрутизації для мережевих елементів, що володіють обмеженими ресурсами в мережах з низьким енергоспоживанням і мережах з втратами, потребує протоколу, здатного ефективно працювати в існуючих обмеженнях, та відповідати необхідним критеріям. IoT стикається з багатьма проблемами безпеки, які можна розділити на дві окремі групи: фундаментальні аспекти безпеки, які має забезпечувати IoT, і конкретні проблеми безпеки на кожному рівні структури IoT. Два фактори створюють проблеми безпеки в мережі:

Природа передової мережевої технології – використання легких алгоритмів шифрування та дешифрування, відомих завдяки спрощеним операціям і реалізації. Використання стандартизованих протоколів що використовується для зменшення обсягу даних, якими вузли мережі обмінюються один з одним.

Проблеми, безпеки та конфіденційності мережевих компонентів, вирішуються на етапі впровадження безпечного зв'язку в IoT.Значні обсяги даних передаються в мережі Інтернету речей, що викликає занепокоєння щодо конфіденційності даних. Маємо велику кількість пристроїв, що ускладнює їх ідентифікацію, оцінку та моніторинг для забезпечення відповідності політиці безпеки. Оскільки передача даних

відбувається через незахищений канал, є можливість перехоплення даних, зібраних з датчиків. Крім того, зловмисники можуть зімітувати вузли користувача, вузли датчиків або вузли шлюзу. Тому, щоб забезпечити безпеку зв'язку в мережі, яка передбачає зв'язок між промисловими користувачами та датчиками, а також зв'язок від датчиків через вузли шлюзу, життєво важливо розробити протоколи зв'язку відповідно до конкретних вимог цих компонентів. Також важливо встановити взаємну автентифікацію як важливий захід безпеки.

Протокол множинної автентифікації сприяє покращенню політики безпеки й захисту вузлів Інтернету речей. Основними задачами є:

1. Удосконалення системи симетричного шифрування. Використовуючи переваги безпеки протоколу ECDH, є можливість реалізовати механізм, завдяки якому сторони зв'язку можуть генерувати необхідний симетричний ключ. Цей ключ використовується для шифрування повідомлень, якими обмінюються в процесі протоколу, і використовується замість фіксованого симетричного ключа, вибраного мережею.

2. Реалізація процесу узгодження ключа на основі протоколу ECDH. Протокол безпеки генерує ключ захищеного сеансу для взаємодіючих об'єктів після безпечного завершення процесу протоколу за умов взаємної автентифікації для об'єктів, що зв'язуються.

3. Багаторазові механізми автентифікації на основі протоколу ECDH. Під час процесу протоколу приватні параметри вузлів зв'язку та протокол ECDH використовуються для реалізації ефективного механізму автентифікації

4. Низька обчислювальна вартість операцій процесу протоколу. Усвідомлюючи, що вузли з функціями низького споживання енергії сприяють роботі мережі, протокол не тільки зберігає свої функції безпеки, але й суттєво скорочує час обчислень, необхідний для його роботи.

Список використаних джерел

1. Karner Michael, Hillebrand Joachim. Going to the Edge: Bringing Artificial Intelligence and Internet of Things Together. 2024. DOI: 10.1007/978-3-031-54049-3_1.

2. Zeng Weihao, Xu Xinyu, Zhang Qianyun, Shi Jiting, Qin Zhijin, Guan, Zhenyu. A Secure and Efficient Distributed Semantic Communication System for Heterogeneous Internet of Things Devices. 2024. DOI: 10.48550/arXiv.2407.14140.

3. Remya S, Pillai Manu, Arjun C, Subbareddy Somula, Cho Yong. Enhancing Security in LLNs using a Hybrid Trust-Based Intrusion Detection System for RPL. *IEEE Access*. 2024. PP. 1-1. DOI: 10.1109/ACCESS.2024.3391918.

4. Zhang WenHua, Xu Lei, Liu HongGang. Application Research of RFID Information in the Era of Internet of Things. 2020. DOI: 10.1007/978-981-33-4601-7_23.