

АРХІТЕКТУРА ДЛЯ РОЗПОДІЛЬНИХ ПРОГРАМ В ІОТ СИСТЕМИ

Міхаль О.П., Ляшенко О.С., Переходнов С.В.
Харківський університет радіоелектроніки, Харків, Україна

Надзвичайне зростання використання Інтернету речей (ІоТ) вплинуло на весь світ, змінивши спосіб повсякденного життя. Як і будь-які інші технології та засоби, мережі на базі Інтернету речей також потребують надійності та захисту. Існуючі методи та моделі обробки та передачі даних в таких системах не враховують усіх цілей надійності та безпеки. Для вирішення питань надійності роботи ІоТ систем, потрібно побудувати моделі та методи, які зможуть усунути недоліки та загрози функціонування відповідних систем. В якості можливого рішення було обрано використання теорії клітинних автоматів, яка дозволяє вирішувати питання класифікації та контролю елементів відповідної системи.

Метою доповіді є побудова архітектури для розподілених програм, які побудовані на використанні клітинних автоматів для забезпечення надійності ІоТ систем. В роботі розглянуто наступні питання: побудова моделей які дозволять оптимізувати роботу ІоТ систем та створення методів надійної обробки даних в компонентах системи. В архітектурі використовується полегшені криптоалгоритми [1].

Принципи клітинних автоматів застосовуються для генерації випадкових чисел, щоб досягти більшої безпеки та випадковості. Подвійне шифрування забезпечує багаторівневий захист даних на етапах завантаження та зберігання даних. Надання шифрування на основі динамічних сеансових ключів гарантує безпеку методу.

Також забезпечується безпечний обмін даними, взаємну автентифікацію між взаємодіючими об'єктами, швидке виконання, автентифікацію користувача та цілісність повідомлень. Пристрій ІоТ, підключений до вузла шлюзу, має успішно завершити етап реєстрації. Згодом, кожного разу, коли відбувається передача даних між пристроєм і вузлом шлюзу, виконується фаза взаємної автентифікації. Блокчейн-мережа, яка використовується на крайньому рівні, забезпечує автентифікацію вузлів-учасників і, отже, запобігає ненавмисній модифікації даних.

Запропонована архітектура виявляється ефективною з точки зору пропускну здатності, часу виконання та стійкості до різноманітних атак на безпеку.

Список літератури

1. Журіло О. Аналіз криптографічних примітивів в мережах ІоТ / О. Журіло, К. Комарець, О. Ляшенко // Проблеми інформатизації: тези доповідей восьмої міжнародної науково-технічної конференції, 26-27.11.2020. – Черкаси: ЧДТУ; Х.: НТУ «ХПІ»; Баку: ВА ЗС АР; Бельсько-Бяла: УТІГН; ДП «ПД ПКНДІ АП», 2020, Т. 1: секції 1-3. – С. 108.