УДК 004.056.55

РАЗРАБОТКА ОТКАЗОУСТОЙЧИВОГО ПРОТОКОЛА АУТЕНТИФИКАЦИИ УСТРОЙСТВ В СИСТЕМЕ ИНТЕРНЕТА ВЕЩЕЙ

Чапасов П. К. (Университет ИТМО)
Научный руководитель - Голованов А. А.
(Университет ИТМО)

Введение. Интернет вещей (Internet of Things, IoT) — это инфраструктура взаимосвязанных сущностей, систем и информационных ресурсов, а также служб, позволяющих обрабатывать информацию о физическом и виртуальном мире и реагировать на нее [1]. Развитие технологий Интернета вещей приводит к значительному росту числа подключенных устройств, взаимодействующих в распределённых и часто недоверенных сетевых средах [2]. При этом устройства IoT, как правило, обладают ограниченными вычислительными, энергетическими ресурсами и объемом памяти, что делает нецелесообразным применение ресурсозатратных механизмов аутентификации [3]. Дополнительной проблемой является необходимость обеспечения устойчивости системы к отказам отдельных узлов, сетевым сбоям и компрометации участников. В существующих решениях часто наблюдается зависимость от центральных доверенных компонентов или применение неоптимальных по расходу ресурсов подходов. В связи с этим актуальной задачей является разработка протоколов аутентификации, сочетающих криптографическую стойкость, эффективность и отказоустойчивость.

Основная часть. В работе предлагается протокол аутентификации устройств, ориентированный на применение в IoT-системах с динамически изменяемым составом участников. Протокол основан на использовании асимметрической криптосистемы на эллиптических кривых, применяемой для формирования и проверки электронных подписей сообщений участников. В ходе выполнения протокола осуществляется взаимная аутентификация сторон и согласование общего секретного материала с использованием эфемерного протокола Диффи—Хеллмана [4].

Ключевой особенностью предлагаемого подхода является возможность аутентификации нового устройства через любой уже доверенный узел сети без необходимости обращения к центральному серверу после этапа первоначальной регистрации. В результате взаимной аутентификации новый участник получает актуальный общий секретный материал сети, который автоматически обновляется у всех участников. Динамическое обновление ключевого материала обеспечивает как прямую, так и обратную криптографическую секретность, исключая возможность расшифрования ранее переданных или последующих сообщений скомпрометированными узлами.

После согласования общего секрета участники используют симметрическое шифрование для защиты прикладного взаимодействия, в частности в рамках протокола OSCORE [5]. Такой подход позволяет существенно снизить вычислительную нагрузку и энергопотребление на устройствах по сравнению с использованием асимметрических механизмов для каждого обмена сообщениями, что делает протокол применимым для чувствительных к ресурсоемким вычислениям IoT-устройств.

Предложенный протокол обеспечивает отказоустойчивость сети за счёт отсутствия единой точки отказа: каждый узел хранит собственный сертификат и набор доверенных параметров, что позволяет сети функционировать и добавлять новых участников даже при недоступности центральных компонентов инфраструктуры.

Дополнительно предусмотрена возможность выполнения расширенной аутентификации для разграничения доступа к отдельным чувствительным ресурсам и сервисам, что позволяет использовать предложенный подход в системах с различными уровнями доверия между участниками.

Выводы. В результате работы разработан отказоустойчивый протокол аутентификации устройств для систем Интернета вещей, обеспечивающий взаимную аутентификацию участников, безопасное распределение ключевого материала в системе, независимость от постоянной доступности центральных компонентов и устойчивость к компрометации отдельных узлов.

Список использованных источников:

1. ГОСТ Р 71777-2024 (ИСО/МЭК 20924:2024) "Национальный стандарт Российской Федерации. Информационные технологии. Интернет вещей. Термины и определения" от 01.02.2025;
2. State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally // IoT Analytics [Электронный ресурс]. – URL: https://iot-analytics.com/number-connected-iot-devices/ (дата обращения: 17.11.2025);
3. Протокол защищенного обмена для индустриальных систем (CRISP 1.0) // РусКрипто [Электронный ресурс]. – URL: https://ruscrypto.ru/resource/archive/rc2019/files/13_Shemyakina.pdf (дата обращения: 17.11.2025);
4. Rescorla E. Diffie-Hellman key agreement method (RFC 2631) //The Internet Society. – 1999;
5. Selander G. et al. RFC 8613: Object Security for Constrained RESTful Environments (OSCORE). – 2019.

Автор _____ Чапасов П. К.

Научный руководитель _____ Голованов А. А.