УДК 535.8

Обеспечение ключевого транспорта в квантовых сетях при их интеграции с системами интернета вещей

Сантьев А.А.
Научный руководитель – к. ф.-м. н. Егоров В. И.
Национальный исследовательский Университет ИТМО

Введение. Технология квантового распределения ключей призвана заменить современные ассиметричные криптографические алгоритмы, которые будут уязвимыми при появлении более эффективного квантового компьютера, а также потенциально позволят обновлять ключи чаще и в автоматическом режиме. В связи с этим возникает необходимость разработки архитектуры безопасности систем интернета вещей, в основе которой обеспечение безопасности цифровых сервисов реализуется с использованием симметричных ключей, транспорт которых в системе обеспечивается с использованием технологии квантового распределения ключей. В связи с этим в работе рассматривается проблематика обеспечения ключевого транспорта в системах интернета вещей, в которых конфиденциальность и целостность обеспечивается с использованием симметричных криптографических примитивов и технологии квантового распределения ключей.

Основная часть. При построении квантовых сетей для преодоления ограничения по дальности функционирования сетей квантовой рассылки ключей (КРК) используется подход на основе доверенных промежуточных опорных узлов, позволяющий формировать квантово-защищенные ключи между опорными узлами сети на основе квантовых ключей. Таким образом, защита данных в квантовых сетях может обеспечиваться не только квантовыми ключами, но и квантовзащищенным ключами. Квантовые сети на основе данного принципа получили широкое развитие, особенно в Китиае и России, однако разработчики квантовых сетей находятся в поиске возможных подходов к реализации цифровых сервисов, безопасность которых основывается криптографическими примитивами, использующими квантовые или квантово-защищенные ключи.

В настоящий момент можно говорить об отсутствии комплексного представления о том, какой должна быть архитектура полноценных платформенных сервисов, в которых защита предоставляемых цифровых сервисов основана на применении технологии квантового распределения ключей. В мировой научной литературе встречаются примеры работ, которые описывают перспективы применения волоконно-оптических систем КРК для обеспечения безопасности данных в системах интернета вещей [1-3]. Следует отметить, что данные работы в большинстве своем носят обзорных характер. Важно отметить, что схемы квантовой цифровой подписи, квантового криптографического обязательства, квантового криптографического доказательства с нулевым разглашением исследуются как отдельные квантовые криптографические примитивы, однако на данным момент вопрос их интеграции в возможную архитектуру безопасности систем интернета вещей в мировом сообществе не был рассмотрен.

Данная работа направлена на разработку архитектуры ключевого транспорта в системах интернета вещей на основе симметричных криптографических алгоритмов с применением технологии квантового распределения ключей, позволяющей обеспечивать защищенную реализацию необходимых для функционирования систем интернета вещей цифровых сервисов без использования инфраструктуры открытого ключа, основывающейся на ассиметричных криптографических алгоритмах. На сегодняшний день данная задача не решена, особенно в контексте особенностей российских требований к безопасности. Интеграция данной разработки в реальные системы интернета вещей поспособствует изменению парадигмы обеспечения безопасности информации в системах интернета вещей, что, в свою очередь, позволит обеспечивать безопасность информации в системах интернета

вещей вне зависимости от вычислительных возможностей злоумышленника. Предлагаемая архитектура безопасности интернета вещей будет основана на изначально устойчивой к различным видам воздействий вне зависимости от изменения вычислительных способностей нарушителя, что способствует достижению информационно-теоретической стойкости архитектуры безопасности.

Разработка принципов ключевого транспорта осуществлялась с учетом организации систем интернета вещей по принципу цифровой платформы, что позволит в рамках единой информационной среды обеспечить алгоритмизированное взаимодействие значимого количества пользователей, имеющих различные роли (уровень привилегий в системе, статус доверия). В рамках платформенного подхода предлагается объединить целый набор криптографических примитивов, основанных на принципах симметричной криптографии, учесть особенности доставки квантовых и квантово-защищенных ключей с использованием технологии КРК различным пользователям системы и ее подсистемам, отвечающим за реализацию криптографических примитивов, получение, хранение и выдачу квантовых и квантово-защищенных ключей, а также сформировать схему последовательности для протокола взаимодействия пользователей системы и ее отдельных подсистем. Использование платформенного подхода позволит снизить транзакционные издержки при взаимодействии различных пользователей, что является одним из основных факторов, влияющих на перспективы внедрения технологии КРК в системы интернета вещей.

Выводы. Результаты предлагаемой работы поспособствуют масштабированию технологии квантового распределения ключей. Внедрение предложенных в рамках работы решений ускорит доведение технологии квантового распределения ключей до масштабного применения в системах интернета вещей, что в свою очередь позволит обеспечить безопасность систем интернета вещей, а как следствие возможность масштабирования и всецелого применения данных систем, даже с учетом возможных угроз от появления полноценных квантовых компьютеров.

Список использованных источников:

1. Alekha Parimal Bhatt, Anand Sharma, Quantum Cryptography for Internet of Things Securitya, Journal of Electronic Science and Technology, Volume 17, Issue 3, 2019, Pages 213-220

2. M. S. Rahman and M. Hossam-E-Haider, "Quantum IoT: A Quantum Approach in IoT Security Maintenance," 2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST), 2019, pp. 269-272

3. S. K. Routray, M. K. Jha, L. Sharma, R. Nyamangoudar, A. Javali and S. Sarkar, "Quantum cryptography for IoT: APerspective," 2017 International Conference on IoT and Application (ICIOT), 2017, pp. 1-4