Авдалян А.А. Уязвимости в протоколах LORAWAN: можно ли взломать IOT-сети в умных городах? // Международный журнал информационных технологий и энергоэффективности.– 2025. –Т. 10 № 4(54) с. 74–77

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056.5

УЯЗВИМОСТИ В ПРОТОКОЛАХ LORAWAN: МОЖНО ЛИ ВЗЛОМАТЬ IOT-СЕТИ В УМНЫХ ГОРОДАХ?

Авдалян А.А.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: sharmanka228@gmail.com

LoRaWAN — это один из самых популярных протоколов связи для Интернета вещей (IoT), особенно в умных городах, где используется для управления инфраструктурой, мониторинга окружающей среды и автоматизации городских процессов. Однако, несмотря на свою энергоэффективность и дальность передачи данных, LoRaWAN имеет ряд уязвимостей, которые могут быть использованы злоумышленниками. В статье рассматриваются основные угрозы безопасности, такие как атаки на шифрование, подмена узлов и перехват данных, а также возможные способы защиты, включая усиленную аутентификацию, безопасное управление ключами и сегментацию сети.

Ключевые слова: LoRaWAN, IoT, умные города, безопасность, перехват данных, кибератаки, аутентификация, криптография.

VULNERABILITIES IN LORAWAN PROTOCOLS: IS IT POSSIBLE TO HACK RIOT NETWORKS IN SMART CITIES?

Avdalyan A.A.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: sharmanka228@gmail.com

LoRaWAN is one of the most popular communication protocols for the Internet of Things (IoT), especially in smart cities, where it is used for infrastructure management, environmental monitoring, and urban process automation. However, despite its energy efficiency and long-range data transmission, LoRaWAN has several vulnerabilities that attackers can exploit. This article examines the main security threats, such as encryption attacks, node spoofing, and data interception, as well as possible protection methods, including enhanced authentication, secure key management, and network segmentation.

Keywords: LoRaWAN, IoT, smart cities, security, data interception, cyberattacks, authentication, cryptography.

Введение

С развитием технологий Интернета вещей (IoT) появляется всё больше новых возможностей для создания умных городов. Одним из ключевых элементов таких городов является использование протоколов связи, которые обеспечивают взаимодействие устройств и систем на больших расстояниях с минимальным потреблением энергии. Одним из таких протоколов является LoRaWAN (Long Range Wide Area Network), который используется для организации беспроводных IoT-сетей. LoRaWAN позволяет подключать множество устройств, таких как датчики, контроллеры, системы мониторинга, и обеспечивать их работу

на больших расстояниях с использованием небольшой мощности. Это делает его идеальным решением для умных городов, где требуется управление многочисленными объектами и сервисами, такими как уличное освещение, системы видеонаблюдения, мониторинг качества воздуха и водоснабжения.

Однако, как и любая технология, LoRaWAN не защищён от уязвимостей, которые могут быть использованы злоумышленниками. В условиях умных городов, где в сеть подключены критически важные системы, безопасность IoT-сетей имеет первостепенное значение. Уязвимости в протоколах LoRaWAN могут стать причиной масштабных атак на инфраструктуру города, включая перехват данных, подмену команд управления или нарушение работы ключевых сервисов. В данной статье рассматриваются основные угрозы, связанные с использованием LoRaWAN в умных городах, а также предлагаются методы защиты, которые помогут минимизировать риски и повысить уровень безопасности таких сетей.

Уязвимости в протоколах LoRaWAN: можно ли взломать IoT-сети в умных городах?

С развитием Интернета вещей (IoT) технологии беспроводной связи становятся всё более востребованными. Одним из ключевых протоколов для передачи данных на большие расстояния с минимальным энергопотреблением является LoRaWAN (Long Range Wide Area Network). Этот протокол широко применяется в умных городах для управления освещением, мониторинга окружающей среды, автоматизации коммунальных услуг и других критически важных задач. Однако, как и любая технология, LoRaWAN не является полностью защищённым, и злоумышленники могут использовать его уязвимости для атак на инфраструктуру IoT-сетей.

Одной из главных проблем безопасности LoRaWAN является его криптографическая защита. Хотя в основе протокола лежат механизмы шифрования AES-128, многие реализации страдают от слабого управления ключами. В случае компрометации ключей злоумышленник может расшифровать передаваемые данные, а также подменять сообщения, что может привести к нарушению работы критически важных систем. Например, если злоумышленник перехватит и подменит команды управления уличным освещением, он может вызвать сбой в системе, создавая хаос в городе.

Другой распространённой уязвимостью LoRaWAN является подмена узлов сети. Аутентификация устройств в LoRaWAN-сетях может быть реализована неправильно или с недостаточной степенью защиты, что позволяет злоумышленникам внедрять поддельные устройства в сеть. Это открывает возможности для атак типа "человек посередине" (MITM), когда злоумышленник перехватывает трафик между устройствами и сетью, изменяя или перенаправляя передаваемые данные. В результате можно не только контролировать работу IoT-устройств, но и манипулировать информацией, что особенно опасно в сфере здравоохранения, транспорта и управления городской инфраструктурой.

LoRaWAN также подвержен атакам на уровень физического доступа. Поскольку сеть работает на неконтролируемых частотах (например, 868 МГц в Европе и 915 МГц в США), её можно заглушить при помощи мощных помеховых сигналов. Это позволяет злоумышленникам нарушить связь между IoT-устройствами и базовыми станциями, временно выводя сеть из строя. Такая атака может быть использована для дестабилизации работы

умного города, например, отключения датчиков контроля качества воздуха или систем умного парковочного мониторинга[1].

Помимо атак на физическом уровне, LoRaWAN подвержен анализу сетевого трафика. Несмотря на наличие шифрования, метаданные пакетов, такие как время передачи, частота и идентификаторы устройств, остаются видимыми. Анализируя эти данные, злоумышленники могут определить поведение устройств, их расположение и даже прогнозировать возможные события в сети. Например, если атакующий выявит закономерности в передаче данных датчиков системы полива в умном городе, он сможет предсказать, когда включаются и выключаются определённые зоны орошения, а затем использовать эту информацию для дальнейших атак[2].

Одним из способов защиты от атак на LoRaWAN является использование усиленной аутентификации устройств. В стандартных настройках LoRaWAN применяется метод аутентификации с фиксированными ключами, что делает систему уязвимой в случае их утечки. Более безопасным решением является внедрение механизма динамического управления ключами, который регулярно обновляет ключи шифрования, минимизируя риск компрометации[3].

Другим важным шагом в защите LoRaWAN является правильное управление сетью. Сегментация сети, при которой различные группы IoT-устройств работают в отдельных логических сегментах, позволяет изолировать компрометированные устройства и предотвращает распространение атак. Кроме того, использование механизмов обнаружения аномалий, таких как анализ поведения трафика и машинное обучение, позволяет оперативно выявлять подозрительную активность в сети[4].

Дополнительную защиту можно обеспечить за счёт использования VPN или защищённых туннелей для передачи данных между LoRaWAN-шлюзами и серверами. Это исключает возможность перехвата данных в канале связи и предотвращает атаки на уровень управления сетью. Кроме того, настройка правильных параметров мощности передатчика и частотных каналов снижает вероятность успешных атак, основанных на помехах и глушении сигнала[5].

В условиях быстрого роста IoT-сетей и внедрения LoRaWAN в инфраструктуру умных городов вопросы безопасности становятся всё более актуальными. Несмотря на энергоэффективность и дальность передачи данных, уязвимости в этом протоколе делают его потенциальной мишенью для злоумышленников. Без надлежащих мер защиты хакеры могут получить доступ к критически важным системам, перехватывать данные и даже дестабилизировать работу городской инфраструктуры.

Заключение

LoRaWAN играет важную роль в развитии умных городов, позволяя автоматизировать широкий спектр задач, от управления коммунальными услугами до мониторинга состояния окружающей среды. Однако его уязвимости делают IoT-сети потенциально уязвимыми для атак, которые могут привести к утечке данных, сбоям в работе городской инфраструктуры и финансовым потерям.

Для минимизации рисков необходимо применять комплексный подход к защите LoRaWAN-сетей. Использование динамических ключей шифрования, многофакторной аутентификации и сетевой сегментации значительно снижает вероятность успешных атак.

Внедрение механизмов обнаружения аномалий и мониторинга трафика также помогает оперативно выявлять попытки взлома.

По мере развития технологий LoRaWAN киберугрозы будут эволюционировать, и защита этих сетей должна оставаться приоритетом для разработчиков и администраторов IoT-инфраструктуры. Только комплексный подход к безопасности поможет обеспечить надёжность IoT-сетей и предотвратить возможные атаки в умных городах будущего.

Список литературы

1. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей. – 2018.
2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
3. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
4. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348.
5. Волкогонов В. Н. и др. Применение физически неклонируемых функций для выполнения аутентификации в среде интернета вещей //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2021. – С. 409-414.

References

1. Kotenko I. V. and others. A human-machine interaction model based on touchscreens for monitoring the security of computer networks. – 2018.
2. Minyaev A. A. Method of evaluating the effectiveness of the information protection system of geographically distributed personal data information systems //Actual problems of infotelec communications in science and education (APINO 2020), 2020, pp. 716-719.
3. Lesnova E. M., Pestov I. E. Development of an error detection and correction method for a distributed information network based on big data //Regional Informatics and information security. - 2018. pp. 236-240.
4. Gorban S. A., Krasov A.V., Tsvetkov A. Yu. Assessment of the effectiveness of access rights control mechanisms in Linux OS //Actual problems of infotelec communications in science and education (APINO 2023). – 2023. – pp. 345-348.
5. Volkogonov V. N. et al. The use of physically non-cloned functions to perform authentication in the Internet of Things environment //Actual problems of infotelec communications in science and education. - 2021. – pp. 409-414.