Аспекты безопасной передачи данных в сетях IoT и их практическая реализация в LoRaWAN

Андрей Экономов (andrei.n.ekonomov@domru.ru)

В статье рассмотрены алгоритмы обеспечения безопасности данных на примере сети Интернета вещей LoRaWAN: авторизация, генерация ключей шифрования и осуществление надёжного хранения идентификаторов устройств.

Введение

В настоящее время сети Интернета вещей (Internet of Things, IoT) типа LPWAN (Low Power Wide Area Network) активно строятся по всему миру, однако вопрос безопасности передаваемых по ним данных и сигналов управления до сих пор остаётся открытым как для потенциальных клиентов, так и для телекоммуникационных специалистов.

Рассмотрим общие принципы защиты данных в сетях IoT на примере сети стандарта LoRaWAN (LongRange Wide Access Network), построенной в Российской Федерации АО «ЭР-Телеком Холдинг». Именно технология LoRaWAN сейчас является драйвером развития направления IoT во всём мире [1] и используется в качестве основного инструмента для управления критически важной инфраструктурой, транспортом, производством, здравоохранением, муниципальным и сельским хозяйством более чем в 100 странах мира.

Защита данных в любой сети Интернета вещей, независимо от конкретного стандарта или технологии, должна соответствовать следующим критериям:

- end-to-end конфиденциальность пользовательских данных на уровне приложения;
- взаимная идентификация абонентского устройства и сети;
- проверка целостности данных при передаче на радиоинтерфейсе;
- конфиденциальность сигнальной информации (управляющих команд);
- безопасное хранение идентификаторов абонентского устройства и его полномочий;
- оперативное устранение найденных уязвимостей в ПО компонентов сети и абонентских терминалов;
- возможность использования отечественных средств криптографической защиты информации (СКЗИ) для критической инфраструктуры.

Кроме того, стоит отметить необходимость защиты от атак серверов (операторских, управляющих сетью, и клиентских, на которых запускаются приложения обработки пользовательских данных), однако данный вопрос является слишком объёмным и рассмотреть его в рамках статьи не представляется возможным.

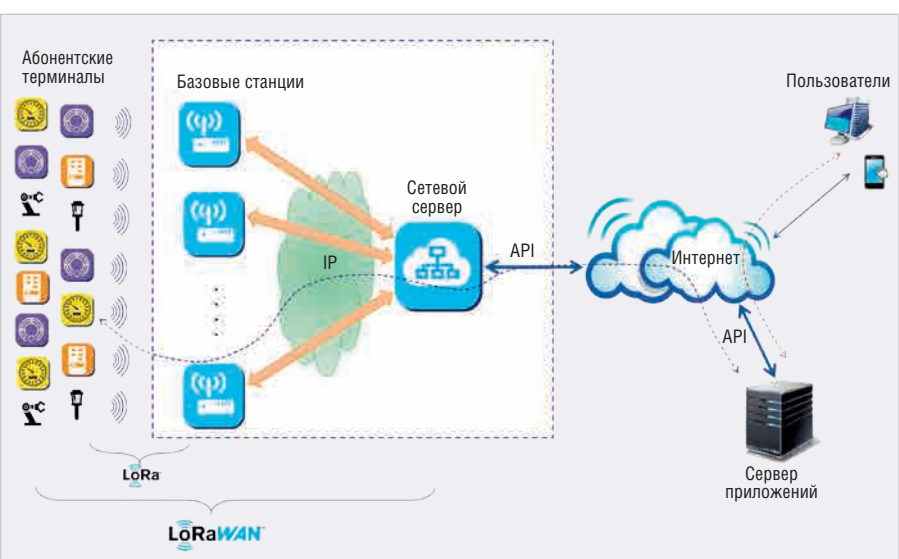


Рис. 1. Архитектура сети LoRaWAN

Описание архитектуры сети IoT на примере LoRaWAN

Сеть LoRaWAN состоит из следующих элементов (см. рис. 1): абонентские терминалы, базовые станции (шлюзы), сетевой сервер и серверы приложений.

Абонентский терминал – обобщающее наименование для сенсоров, датчиков, счётчиков, актуаторов и радиомодулей IoT, устанавливаемых на стороне пользователя.

Базовая станция (БС) выполняет функции сопряжения и взаимодействия радиосети с абонентским терминалом и концентрации нагрузки с группы терминалов. Совокупность базовых станций оператора обеспечивает территорию радиопокрытия сети и прозрачную двунаправленную передачу данных между конечными устройствами и сетевым сервером.

Сетевой сервер – программно-аппаратный комплекс, управляющий радиосетью, контролирующий её и выполняющий маршрутизацию пакетов данных от абонентских терминалов до соответствующих серверов приложений.

Управление радиосетью состоит в том, что сетевой сервер сети LoRaWAN выбирает БС для передачи сообщений в направлении «вниз» (downlink), принимает решения о необходимости изменения скорости передачи данных для каждого терминала, мощности передатчика, контролирует заряд батарей конечных устройств, шифрует данные и т.п.

Контроль радиосети включает функции мониторинга, сбора статистики и аварийного информирования.

Каждый пакет данных, отправляемый абонентским терминалом, имеет в своём составе уникальный идентификатор DevAddr, а на сетевом сервере хранится запись о соответствии DevAddr и URL-сервера приложений, которому предназначена информация от терминала (датчика). На основании этого соответствия сетевой сервер выполняет маршрутизацию пакета до сервера приложений, где происходит его дальнейшая обработка приложением клиента.

Сервер приложений – платформа, производящая обработку данных, получаемых от терминалов и направляемых к ним. Помимо работы с данными, сервер приложения может управлять терминалами с уровня приложения (например, переводить их в режим работы другого класса, управлять опцией адаптивной передачи данных, мультикаста и т.п.). Сервер приложений может находиться на территории оператора, на территории клиента или в одном из «облачных» сервисов.

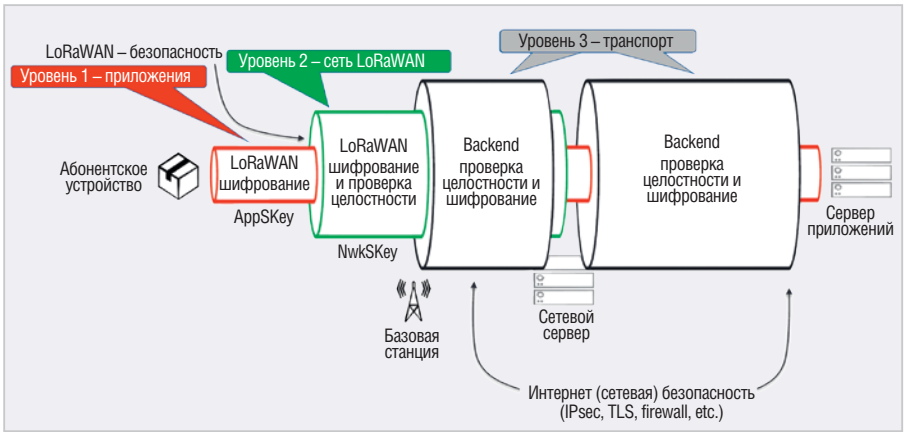


Рис. 2. Общая схема безопасности данных в сети LoRaWAN

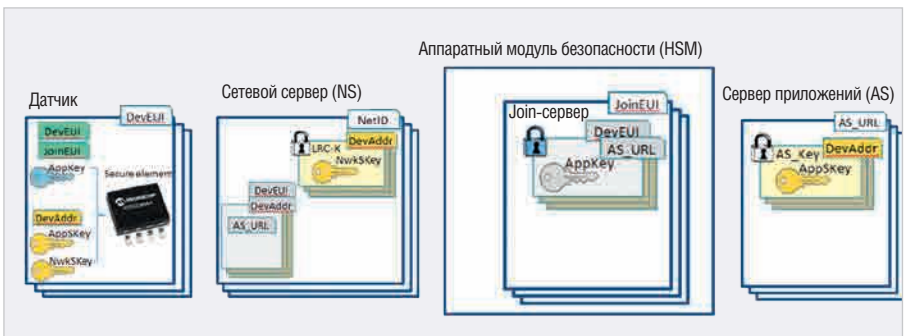


Рис. 3. Схема хранения ключей шифрования

Обеспечение безопасности передаваемых данных

В сети IoT LoRaWAN используется многоуровневая система безопасности передачи данных (см. рис. 2).

1-й уровень. AES-шифрование на уровне приложения (end-to-end, т.е. между абонентским терминалом и сервером приложений) с помощью 128-битного переменного сессионного ключа Application session key (AppSKey). Данный ключ шифрования хранится в абонентском терминале и на сервере приложений и недоступен оператору сети (доступ к AppSKey есть только у клиента – владельца сервера приложений). Формирование сессионного ключа происходит параллельно в абонентском терминале и на стороне сети во время процедуры активации терминала; через эфир AppSKey не передаётся.

2-й уровень. AES-шифрование и проверка целостности сообщений на сетевом уровне (между абонентским терминалом и сетевым сервером) с помощью 128-битного переменного сессионного ключа Network session key (NwkSKey). Данный уровень шифрования используется для защиты передаваемых сигнальных команд на MAC-уровне, а также для вычисления MIC (Message Integrity Code) с целью проверки целостности данных, передаваемых по радиоинтерфейсу. NwkSKey хранится в абонентском терминале и на сетевом сервере и недоступен клиенту (доступ к NwkSKey есть только у оператора сети – владельца сетевого сервера). Формирование сессионного ключа NwkSKey также происходит параллельно в абонентском терминале и на стороне сети во время процедуры активации терминала; через эфир NwkSKey не передаётся.

3-й уровень. Стандартные методы аутентификации и шифрования интернет-протокола (IPsec, TLS и т.п.) при передаче данных по транспортной сети между узлами сети (базовая станция, сетевой сервер, Join-сервер (см. далее), сервер приложений).

По команде приложения или сетевого сервера в любой момент возможен переход на новую сессию с генерацией нового комплекта ключей шифрования, что делает бесполезными старые ключи шифрования. Кроме того, имеется возможность установки периодической генерации нового комплекта ключей NwkSKey и AppSKey.

В версии стандарта LoRaWAN V1.0.x [2] формирование сессионных ключей на стороне сети производится на сетевом сервере (NS), однако в версии V1.1 [3] для этих целей определяется выделенный сервер (так называемый Join-сервер) (см. рис. 3), который может быть дополнительно защищён отдельным аппаратным модулем безопасности HSM (Hardware Security Module). В этом случае для безопасной передачи сгенерированных сессионных ключей между серверами, а также хранения их на сетевом сервере и сервере приложений внедряются дополнительные ключи: AS_Key для ключа AppSKey и LRC_K для ключа NwkSKey. На абонентском устройстве ключи шифрования опционально могут защищаться специальным аппаратным элементом безопасности Secure Element (например, микроконтроллером Microchip ATECC608A), что исключит их компрометацию в случае физического воздействия на терминал.

Внедрение аппаратных средств защиты в сети и на терминале делает бесполезными попытки перехвата сессионных ключей при передаче их между серверами и взлома серверов или абонентских устройств с целью извлечения сессионных ключей.

Рассмотренные мероприятия создают также условия для защищённого роуминга данных (безопасной авторизации датчиков в гостевой сети и защищённой передачи данных домашнему серверу приложений из гостевой сети).

В целях дополнительной защиты процесса генерации сессионных ключей Join-сервер может быть физически вынесен на территорию клиента или производителя устройств (см. рис. 4). В этом случае даже сотрудники оператора не смогут получить доступ к сессионным и корневым ключам шифрования абонентского терминала.

Несмотря на то что в РФ не требуется обязательная сертификация средств кодирования (шифрования)

Рис. 4. Возможные сценарии размещения Join-сервера

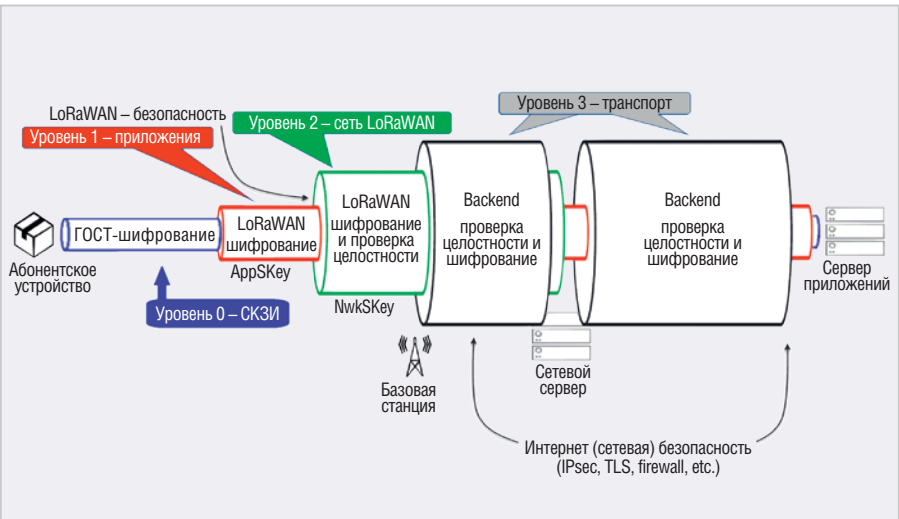


Рис. 5. Схема внедрения СКЗИ в структуру шифрования данных сетей LoRaWAN

при передаче сообщений, не составляющих государственную тайну [4], по требованию заказчика используемые в стандарте LoRaWAN уровни шифрования AES-128 могут быть дополнены одним из стандартизованных в РФ алгоритмов, входящих в семейство ГОСТ Р 34.10-2012 [5], ГОСТ Р 34.11-2012 [6], или алгоритмом «Кузнечик» (согласно ГОСТ Р 34.12-2015 [7] и ГОСТ Р 34.13-2015 [8]). Для этого при производстве абонентских терминалов LoRaWAN предлагается устанавливать в них дополнительный микроконтроллер СКЗИ, сертифицированный ФСБ России и соответствующий требованиям, предъявляемым к шифровальным средствам класса КС3 (дистанционное банковское обслуживание, электронный документооборот в государственном секторе и т.д.). В качестве такого микроконтроллера могут быть использованы, например, микропроцессоры отечественного производства «Микрон MIK51SC72D» или «Микрон MIK51AD144D», сертифицированные ФСТЭК и ФСБ России, имеющие небольшие размеры (около 14 мм^2) и малое энергопотребление.

Схема безопасности данных в сети LoRaWAN с дополнительным уровнем СКЗИ представлена на рисунке 5.

Ключ шифрования уровня СКЗИ, например SubSKey (согласно ГОСТ Р 34.12-2015 [7]), прошивается в абонентский терминал LoRaWAN при производстве, так же как и корневой ключ уровней шифрования 1–2 LoRaWAN, или внедряется в терминал вместе с микроконтроллером СКЗИ при введении терминала в эксплуатацию (путём использования специального слота). Дешифрация данных уровня СКЗИ производится на территории заказчика сервером приложений после дешифрации уровня приложения сессионным ключом AppSKey. Ключ шифрования SubSKey передаётся клиенту вместе с датчиком непосредственно производителем абонентского терминала и недоступен сотрудникам оператора сети LoRaWAN.

Выводы

Обозначенные ранее критерии безопасной передачи данных в сети IoT стандарта LoRaWAN реализуются следующими способами:

- AES-шифрование с помощью сессионного ключа AppSKey;
- процесс авторизации терминала при первичном подключении к сети (или по специальной команде о повторе авторизации);
- вычисление MIC-кода на основе сессионного ключа NwkSKey;
- AES-шифрование MAC-команд с помощью сессионного ключа NwkSKey;
- внедрение аппаратного элемента безопасности Secure Element в абонентский терминал и защита HSM-модулем Join-сервера;
- дистанционная смена ПО абонентских терминалов через эфир с помощью специфицированного LoRaAlliance-механизма FUOTA (Firmware Upgrade Over The Air) [9] и установка обновлений на сетевой сервер и сервер приложений;
- внедрение дополнительного «нулевого» уровня end-to-end-шифрования по сертифицированным ФСБ РФ алгоритмам.

Литература

1. LoRaWAN Members Meeting, Tokyo, 2018.
2. LoRaWAN™ Specification, version V1.0.3, 2018.
3. LoRaWAN™ 1.1 Specification, 2018.
4. Извещение по вопросу использования несертифицированных средств кодирования (шифрования) при передаче сообщений в информационно-телекоммуникационной сети Интернет. ФСБ РФ, 2016.
5. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
6. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.
7. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры.
8. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров.
9. LoRa Alliance, FUOTA Process Summary Technical Re 1 commendation TR002 v1.0.0, 2019.

НОВОСТИ МИРА

НТЦ «Модуль» запускает в серийное производство NaviMatrix

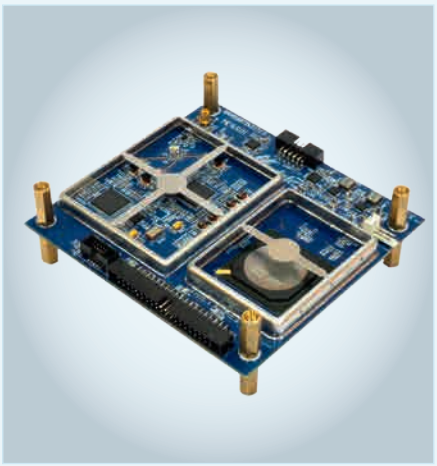
Научно-технический центр «Модуль», ведущий российский разработчик микроэлектронных компонентов, представляет готовый к серийному выпуску встраиваемый модуль высокоточного спутникового трёхчастотного навигационного приёмника МС149.01, который будет продвигаться на рынке под брендом NaviMatrix.

Приёмник выполняет обработку спутниковых навигационных сигналов в дифференциально-фазовом режиме и позволяет достигать сантиметровой точности при определении координат в динамике или миллиметровой в статике.

Устройство построено на базе отечественного навигационного процессора К1888ВС018 собственной разработки НТЦ «Модуль». По своим характеристикам приёмник приближается к зарубежным аналогам и может конкурировать с ведущими отечественными разработками, что подтверждают сравнительные экспериментальные замеры.

NaviMatrix МС149.01 представляет «элиту» высокоточного навигационного оборудования: он работает в трёх частотных диапазонах и принимает сигналы глобальных навигационных спутниковых систем GPS и ГЛОНАСС. Устройство достаточно компактное и энергоэффективное, поэтому может быть интегрировано в самый широкий круг аппаратных комплексов, где требуются высокоточные местоопределения. Навигационный модуль совместим с библиотекой высокоточной навигации RTKLib.

Новая разработка НТЦ «Модуль» найдёт применение в высокоточной навигационной аппаратуре потребителей. Устройство актуально в таких отраслях, как автомобильный и ж/д транспорт, автоматизированные датчики и сети для обнаружения деформации конструкций, точное земледелие, геодезия, робототехника, системы беспилотного транспорта и т.д.



Навигационный модуль функционирует в широком диапазоне температур –40…+70°С. Особое значение данная разработка приобретает в связи с программами импортозамещения и задачами обеспечения независимости от импортной продукции.

Презентация приёмника состоялась на XIII Международном навигационном форуме.

Пресс-служба НТЦ «Модуль»