Анализ методов сетевой безопасности в LPWAN сетях

М. Н. Сторожук[1], Р. В. Киричек[2]
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича
[1]maxstor@bk,ru, [2]kiricheck.sut@mail.ru

***Аннотация*. Сети LPWAN используются для обслуживания важных объектов критической инфраструктуры, для которых информационная безопасность имеет особое значение. Шифрование - эффективный способ предотвратить несанкционированный доступ к каналу связи. Каждая из технологий построения сетей LPWAN имеет свои особенности и отличительные особенности. В докладе представлен краткий обзор наиболее популярных в России сетей LPWAN и используемых в них методов шифрования.**

Ключевые слова: Интернет вещей; беспроводные сети; шифрование; безопасность

I. Введение

Сети LPWAN используются, в том числе, и для обслуживания объектов критической инфраструктуры, для которых защита информации имеет особое значение. Эффективным способом для предотвращения несанкционированного доступа к каналу связи является шифрование. Это обеспечивает конфиденциальность и целостность передаваемой информации. На данный момент существует несколько технологий построения LPWAN сетей. Каждая из них имеет свои особенности и отличительные черты. В докладе предлагается краткий обзор наиболее востребованных в России LPWAN сетей и методов шифрования, используемых в них.

II. Сеть LoRaWAN

Одной из самых популярных моделей для построения LPWAN сетей является технология LoRaWAN, разработанная американской компанией Semtech. В ней используется AES-CMAC алгоритм шифрования, описанный в рекомендации RFC4493, для оригинальной аутентификации и защиты целостности. AES-CCM используется алгоритм, описанный в рекомендации IEEE 802.15.4-2011 [1].

Это выглядит, как многоуровневая система безопасности передачи данных:

Уровень 1. AES-шифрование на уровне приложения (между абонентским терминалом и сервером приложений) с помощью 128-битного переменного сессионного ключа AppSKey. Данный ключ хранится в абонентском терминале и на сервере приложений и не доступен оператору сети. Доступ к AppSKey есть только у клиента – владельца сервера приложений.

Уровень 2. AES-шифрование и проверка целостности сообщений на сетевом уровне (между абонентским терминалом и сетевым сервером) с помощью 128-битного переменного сессионного ключа NwkSKey. Этот ключ хранится в абонентском терминале и на сетевом сервере и не доступен клиенту. Доступ к NwkSKey есть только у оператора сети – владельца сетевого сервера.

Уровень 3. 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, сервер приложений).

Несмотря на то, что в нашей стране не требуется обязательная сертификация средств шифрования при передаче сообщений, не составляющих государственную тайну (Извещение по вопросу использования несертифицированных средств кодирования (шифрования), при передаче сообщений в информационно-телекоммуникационной сети «Интернет», ФСБ России 18.07.2016) по требованию заказчика используемые в стандарте LoRaWAN уровни шифрования AES-128, могут быть дополнены одним из стандартизованных в России алгоритмов, входящих в семейство ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012, или алгоритмом «Кузнечик» (согласно ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015). Для этого предлагается при производстве абонентских терминалов LoRaWAN устанавливать в них дополнительный микроконтроллер, сертифицированный ФСБ России на отсутствие не декларируемых возможностей и соответствующий требованиям, которые предъявляются к шифровальным средствам класса КС3 (дистанционное банковское обслуживание, электронный документооборот в государственном секторе и т. д.). Таким микроконтроллером может быть, например, микропроцессор отечественного производства MIK51SC72D, сертифицированный ФСБ России, имеющий небольшие размеры (14 кв. мм) и малое энергопотребление [2].

Протокол XNB

XNB – отечественная разработка компании «Современные радио технологии». Данные шифруются по ГОСТ, XTEA или AES. Шифрование по ГОСТу дает возможность использования протокола на объектах критической инфраструктуры.

Протокол **NB-Fi**

Протокол **NB-Fi** был разработан российской компанией **WAVIoT** (ООО «Телематические Решения») для функционирования в широком спектре радиочастот, в том числе в свободном от лицензирования спектре радиочастот [3]. В качестве схем шифрования и выработки имитовставки для двух-ключевой схемы используются режимы CTR и OMAC на основе блочного шифра «Магма» с ключом шифрования длиной 256 бит (данные алгоритмы и схемы определены в **ГОСТ Р 34.12-2015** и **ГОСТ Р 34.13-2015**). Для обеспечения конфиденциальности и целостности пакетов транспортного уровня протокола **NB-Fi** используется схема аутентифицированного шифрования с дополнительными данными [4]. Криптографический анализ протокола показал ряд его уязвимостей.

Протокол **OpenUNB**

Протокол **OpenUNB** также является отечественной разработкой за авторством рабочей группы Сколтеха по интернету вещей. В нем заложены алгоритмы шифрования ГОСТ Р 34.12-2015 и FIPS PUB 197(Advanced Encryption Standard). Полезная нагрузка пакета выбирается для согласования с размерами шифроблоков данных блочных алгоритмов, что не всегда будет являться достоинством.

0Z от Sigfox

Sigfox – французский разработчик и провайдер IoT-устройств, запустил в России промышленную сеть интернета вещей **0Z**. Технология использует шифрование AES с HMACs с закрытым ключом, который встроен в прибор, плюс некоторый порядковый номер [5].

III. Выводы

После рассмотрения представленных протоколов становится понятно, что они используют для шифрования стандарты AES, «Магма» и «Кузнечик» в различных вариациях. Протоколы, использующие российские ГОСТы, применимы для построения промышленных сетей интернета вещей в России, а также для объектов критической инфраструктуры (XNB, OpenUNB, NB-FI). Сети, использующие зарубежные стандарты шифрования, применимы только для гражданской и коммерческой эксплуатации (LoRaWAN, Sigfox).

Список литературы

[1] ООО «Вега-Абсолют» [Электронный ресурс]: URL: https://habr.com/ru/post/462353/.

[2] Андрей Экономов. Сеть LoRaWan: безопасность обеспечивается [Электронный ресурс]: Журнал ИКС, научный журнал. URL: https://www.iksmedia.ru/articles/5573226-Set-LoRaWAN-bezopasnost-obespechiva.html(дата обращения 1.02.2021).

[3] Nb-Fi [Электронный ресурс] // Википедия : свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/NB-Fi (дата обращения 1.02.2021).

[4] Безопасность и криптозащита протокола NB_Fi [Электронный ресурс]: URL: https://waviot.ru/technology/nb-fi-security/ (дата обращения 1.02.2021).

[5] Кумаритова Д.Л., Киричек Р.В. «Обзор и сравнительный анализ технологий LPWAN сетей» // Информационные технологии и телекоммуникации. 2016. Т.4. № 4. С. 33-48.