Надёжность IoT в нелицензируемом диапазоне. Доказываем на примере LoRaWAN

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

Некоторых потенциальных клиентов до сих пор беспокоит вопрос надёжности и безопасности передачи данных на общедоступных частотах. В данной статье наглядно объясняется, почему эти опасения беспочвенны.

Введение

В настоящее время в большинстве развитых стран в дополнение к сетям мобильной связи активно строятся сети Интернета вещей (IoT) класса LPWAN (Low Power Wide Access Network), работающие на нелицензируемых (т.е. общедоступных) радиочастотах. В Российской Федерации для этих целей выделен диапазон 868 МГц (частоты 864...869,2 МГц) [1], в котором уже построены сети как общемирового стандарта LoRaWAN (Long Range Wide Access Network), так и локальных спецификаций, например «Стриж» и «Вавиот».

Несмотря на миллионы уже подключённых к LPWAN-сетям устройств по всей планете, некоторых потенциальных клиентов до сих пор беспокоит вопрос надёжности и безопасности передачи данных на общедоступных частотах. Попробуем развеять сомнения на примере сети стандарта LoRaWAN, построенной в Российской Федерации АО «ЭР-Телеком Холдинг».

Нелицензируемость – не синоним вседозволенности

Нередко приходится слышать мнение, что системы связи в общедоступных диапазонах частот не могут обеспечивать уверенную связь уже только потому, что любой желающий может вывести в эфир генератор ватт эдак на 20 и «положить» всё вокруг. На самом деле, в нелицензируемых диапазонах для средств радиоэлектронной связи (РЭС) действуют даже более строгие правила, чем в лицензируемых. В частности, в полосе 868 МГц согласно решению ГКРЧ [2] ограничены, во-первых, излучаемая мощность (на большинстве каналов – не более 25 мВт), во-вторых, время нахождения в эфире (как правило, не более 1%). И наказание за нарушения указанных величин точно такие же, как и за несанкционированное вещание на лицензируемых частотах.

Так что любые системы гражданского назначения вне зависимости от способа выделения спектра – по стандартным процедурам (лицензионный) или по упрощённым (нелицензионный) – могут пострадать от преднамеренных радиопомех. Однако это в равной мере незаконно, и способы борьбы с такими помехами известны и одинаково доступны всем пользователям радиоспектра.

В то же время, разумеется, даже работающие по закону устройства могут создавать помехи своему окружению. Рассмотрим, как с этим борется стандарт LoRaWAN [3].

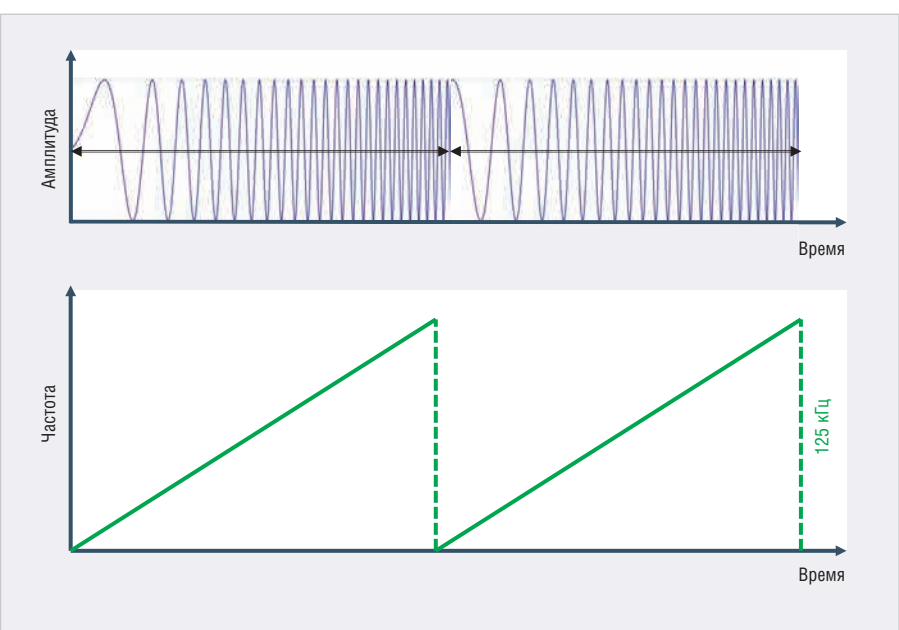

Рис. 1. Немодулированный сигнал LoRaWAN

Защита от внешних помех

Радиопротокол LoRaWAN использует импульсы линейно-частотной модуляции (ЛЧМ) или в англоязычном варианте – CSS (Chirp Spread Spectrum) (см. рис.1). В отличие от систем XNB (Extra Narrow Band) типа Sigfox, «Стрижа» и «Вавиота», использующих для связи узкую полосу в 100 Гц и фазовую модуляцию, данные в сетях LoRaWAN передаются датчиками в полосе шириной 125 кГц (т.е. более чем в 1000 раз шире).

Каждое устройство стандарта LoRaWAN излучает сигнал с изменяющейся частотой. Модуляция же LoRaWAN заключается в «обрыве» цикла на одной из промежуточных частот (см. рис. 2а) и новом его начале, именно это и кодирует передаваемый символ. Всего существуют 128 возможных различных частот «обрыва» цикла в каждом частотном канале (шириной, напомню, 125 кГц), а значит, один ЛЧМ-импульс кодирует 7 бит данных.

Поскольку частота сигнала LoRaWAN меняется в диапазоне 125 кГц, то узкополосная помеха практически не оказывает влияния на успешность декодирования сигнала LoRaWAN, чего нельзя сказать о системах XNB, сигнал которых может быть полностью уничтожен помехой шириной уже в несколько десятков герц. Ещё одно преимущество, вытекающее из особенности модуляции LoRaWAN, – устойчивая работа на движущихся объектах (поездах, автомобилях и т.п.), так как доплеровский сдвиг частоты заметно не влияет на успешность передачи сигнала.

И последнее: модуляция и канальное кодирование LoRaWAN (допол-

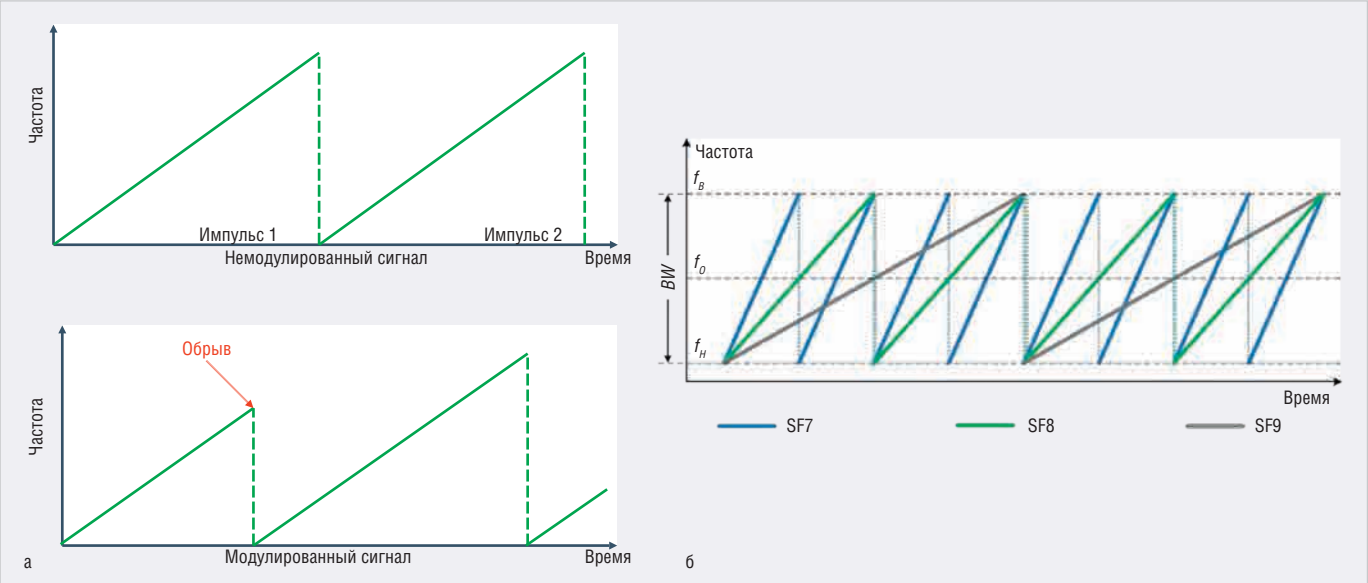

Рис. 2. Модулированный сигнал LoRaWAN в сравнении с немодулированным

нение пользовательских данных контрольными битами с целью успешного восстановления сообщения в случае потери его части, не путать с шифрованием) позволяют осуществлять приём полезной информации даже при отрицательных значениях отношения сигнал/шум (SNR до –20 дБ).

Борьба с внутренними коллизиями

С целью экономии заряда батарей абонентских устройств и ёмкости сети датчики LoRaWAN выходят в эфир на одном из восьми частотных каналов без предварительной синхронизации с сетью (в отличие от, скажем, GSM, где каждому абоненту сеть выделяет на время разговора персональный таймслот на определённом частотном канале). Это создаёт вероятность внутрисетевых «коллизий»: а вдруг две двери откроются одновременно и соответствующие сенсоры выйдут в эфир в один и тот же момент на одном частотном канале? Примет ли сеть сигнал от них, или они заглушат друг друга, или один заглушит другой? Давайте разбираться.

Стандартом LoRaWAN [3] определены так называемые Spreading Factors (SF), или «коэффициенты расширения спектра». Спецификацией [4] их предусмотрено всего шесть – от SF7 до SF12. SF – это «скорость» изменения частоты в ЛЧМ-импульсе: чем выше SF, тем медленней меняется частота (см. рис. 2б). Изменение SF на единицу означает увеличение длительности импульса в 2 раза. Для SF7 и полосы 125 кГц длительность импульса минимальна и составляет 1,024 мс.

Чем выше SF, тем медленней передаются данные, но тем выше способность системы распознать их без ошибок. SF каждому абонентскому устройству назначает сетевой сервер (NS – Network Server) по алгоритму ADR (Adaptive Data Rate – адаптивная скорость передачи данных) на основании измерений отношения сигнал-шум (SNR), выполненных базовой станцией. Если абонентские терминалы находятся в разных радиоусловиях относительно базовой станции (например, одно – рядом с БС, другое – далеко, или одно – у окна квартиры, второе – за капитальной стеной), то передавать данные они будут с разными SF. При этом они не будут друг с другом интерферировать даже в случае наложения сигналов друг на друга по времени на одном частотном канале. Магия? Вовсе нет, ведь в силу разной скорости изменения частоты у передатчиков с разными SF такие устройства будут представлять друг для друга лишь узкополосную помеху, что, как уже было сказано выше, легко компенсируется канальным кодированием.

А что будет, если базовая станция примет одновременные сообщения от двух устройств с одинаковым SF? Да, будет коллизия, и либо одно, либо оба сообщения будут потеряны в результате интерференции. Однако это произойдёт только на ОДНОЙ базовой станции, в то время как сигнал от каждого абонентского LoRaWAN в профессионально спланированной и грамотно построенной сети принимают минимум три БС (именно такое количество базовых станций необходимо для корректной работы опции геолокации методом TDoA (Time Difference of Arrival)). И если на одной БС возникнет коллизия, то приём сообщения успешно пройдёт через другие базовые станции. В сетевом сервере LoRaWAN даже существует специальный таймер (длительностью 250 мс), чтобы дождаться, пока сообщение от определённого абонентского устройства будет получено всеми возможными БС, с целью выбрать среди них наилучшую (с точки зрения SNR) на случай, если потребуется отправка сообщения от сети к датчику (подтверждение приёма или MAC-команда).

В исследовании [5], проведённом компаниями MachineQ и Semtech, установлено, что восемь восьмиканальных БС LoRaWAN за сутки в состоянии принять 1 млн сообщений от абонентских устройств. А если надо больше? Ответ простой: увеличивать количество базовых станций. Ведь в отличие от сотовых систем связи, БС LoRaWAN не ведут постоянного вещания пилотных (как в LTE) или широковещательных (как в GSM) сигналов, так что установка новых базовых станций не приводит к повышению внутрисетевой интерференции. Основную часть времени БС LoRaWAN работают на приём, а режим передачи включается лишь в редких случаях отправки команды управления или подтверждения приёма на абонентское устройство. Также для покрытия помещений можно использовать репитер LoRaWAN (его спецификация на момент написания этого материала находится на финальном утверждении в техническом комитете LoRa Alliance). Репитер позволит улучшить

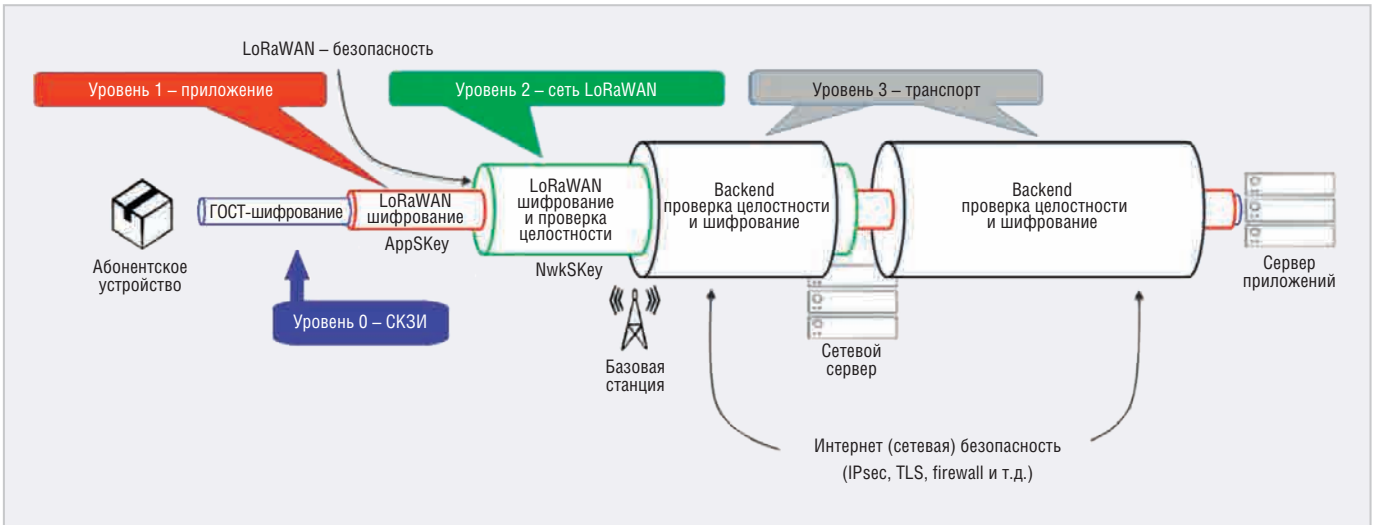

Рис. 3. Общая схема безопасности данных в сети LoRaWAN, дополненная уровнем СКЗИ (средства криптографической защиты информации)

(т.е. уменьшить номер) SF для сообщений, отправляемых indoor-датчиками, что снизит вероятность коллизий (ведь, как было указано выше, сообщения с низким SF передаются многократно быстрее, чем сообщения с высоким SF).

Что касается безопасности передаваемых в сетях LoRaWAN сообщений (см. рис. 3), то в сетях рассматриваемого стандарта используется многоуровневая система шифрации пользовательской информации и проверки целостности данных с широчайшими возможностями кастомизации. Это позволяет построить систему с наивысшим уровнем защиты, в том числе для использования в КИИ (критическая информационная инфраструктура) [6]. Этот вопрос был подробно рассмотрен в материале [7].

Выводы

Системы IoT, использующие нелицензионный спектр, могут быть спроектированы таким образом, чтобы обеспечить безопасную и приемлемую для достаточно ответственных приложений (вплоть до КИИ) вероятность доставки сообщения. Ограничения из-за количества устройств теоретически возможны, однако они возникают при плотностях размещения датчиков, существенно превышающих реально прогнозируемые ситуации, и в случае необходимости легко устраняются увеличением числа базовых станций и установкой репитеров, что подтверждает международный опыт [5].

Литература

1. Решение ГКРЧ № 07-20-03-001 от 07.05.2007 «О выделении полос радиочастот устройствам малого радиуса действия».
2. Решение ГКРЧ № 18-46-03-1 от 11.09.2018 «О выделении полос радиочастот, внесении изменений в решения ГКРЧ и продлении срока действия решений ГКРЧ».
3. LoRaWAN™ Specification, Version V1.0.3, 2018.
4. LoRaWAN™ 1.0.3 Regional Parameters, 2018.
5. *Ross Gilson, Michael Grudsky.* LoRaWAN Capacity Trial in Dense Urban Environment, 2018.
6. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.
7. *А.Н. Экономов.* «Аспекты безопасной передачи данных в сетях IoT и их практическая реализация в LoRaWAN». Современная электроника. 2019. № 5.

НОВОСТИ МИРА

18-я международная выставка «ChipEXPO–2020» пройдёт в Технопарке Инновационного центра «Сколково»

В 2020 году 18-я международная выставка по электронике, компонентам, оборудованию, технологиям «ChipEXPO–2020» пройдёт 15–17 сентября в Технопарке Инновационного центра «Сколково».

Центр «Сколково» является важнейшей новаторской площадкой России, на которой проходит много мероприятий технологической, инновационной и научной направленности.

С ноября 2019 года после открытия МЦД-1 и интеграции его с московским метро транспортная доступность «Сколково» составляет 17 минут. Выставка станет ещё более интересной и удобной для делового сотрудничества участников и посетителей благодаря тому, что Технопарк «Сколково» обладает самой современной инфраструктурой, которая позволяет проводить масштабные выставки, конференции, симпозиумы, подчёркивают организаторы.

Дополнительным плюсом для участников станет тот факт, что в «Сколково» работают около 1800 компаний-резидентов, часть из которых связана с электроникой и микроэлектроникой. Ряд этих компаний примут участие в проекте.

Как отметили организаторы выставки, в ноябре–декабре 2019 года принят ряд документов Минпромторга России и Госкорпорации «Ростех», устанавливающих основные концептуальные направления выставки «ChipEXPO–2020», тематику экспозиций, разделы деловой программы.

В настоящее время формируется деловая программа выставки, разрабатывается новое положение о конкурсе «Золотой Чип», оптимизируется количество и тематика номинаций конкурса и формируется экспертный совет для оценки поданных заявок и подведения итогов.

Организаторы мероприятия приглашают компании подать заявки на участие в «ChipEXPO–2020» и её деловой программе! Устроители всегда открыты к диалогу по разработке и предоставлению расширенного комплекса услуг, которые сделают участие в выставке ещё более эффективным.

Серия GENESYS™

TDK·Lambda

НОВОЕ ПОКОЛЕНИЕ
ПРОГРАММИРУЕМЫХ ИСТОЧНИКОВ ПИТАНИЯ

ГАРАНТИЯ 5 лет

- Выходные мощности: 1,5 / 1,7 / 2,7 / 3,4 и 5 кВт
- Выходное напряжение от 10 до 600 В
- Выходной ток от 2,6 до 500 А
- КПД до 92% на полной нагрузке
- Управление: LAN, USB, RS-232/485
- Вес менее 7,5 кг, высота модуля 1U для 19" стойки (модель на 1,5 кВт имеет размер ½ 19" стойки)
- GSP 10 кВт, GSP 15 кВт – готовые модули с завода-изготовителя, состоящие из ведущего модуля и одного или двух ведомых
- Полный заводской контроль качества и тестирование
- Привлекательная цена
- Управление: LAN, USB, RS-232/485, Modbus-TCP

PROSOFT®

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

(495) 234-0636
INFO@PROSOFT.RU

WWW.PROSOFT.RU