



GoodWAN – реализация новых возможностей Интернета вещей

АЛЕКСАНДР ШЕПТОВЕЦКИЙ, ТЕХНИЧЕСКИЙ ДИРЕКТОР

Обзор LPWAN технологий

Ключевые преимущества LPWAN – это «дешево» и «просто»:

- Большая дальность (дешевая сеть)
- Большой срок службы батареи (просто в эксплуатации)
- Дешевые конечные устройства

Два основных варианта реализации LPWAN сети

- Лицензионный диапазон частот (повышенная мощность, относительно высокая скорость, нет помех).
- Безлицензионный диапазон частот (низкая мощность, низкая скорость, ограничение рабочего цикла передатчика, возможны помехи от других игроков).

Работающие технологии LPWAN сетей

- NB-IoT – эволюция сотовой связи
- SigFox (Стриж, BAWIOT в России) – UNB безлицензионный LPWAN
- LoRa – широкополосный безлицензионный LPWAN
- Другое

* В последнее время появилось много вариантов «light» LPWAN технологий, использующих NB канал – MIOTY, Аура 360, SNB и др. В этих технологиях как правило совмещается SDR-радио на базовой станции и современные NB радио-чипы на КУ и используют свои протоколы синхронизации. По чувствительности они минимум на 15-20 dB уступают классическому LPWAN.

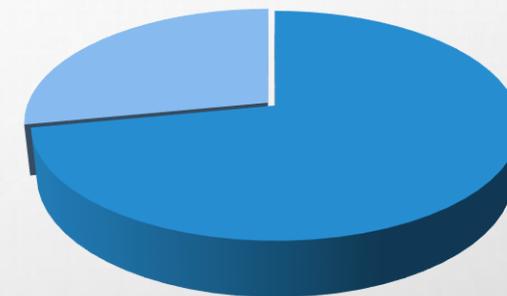
Преимущества и недостатки безлицензионного LPWAN в сравнении с NB-IoT

Преимущества

1. Стоимость конечного оборудования ниже
2. Стоимость разворачивания и обслуживания сети ниже
3. Срок службы батарейки больше

Недостатки

1. Маленький объем сообщения
2. Низкая скорость и высокая задержка
3. Не предназначены для потоковых данных
4. Ограниченные возможности обратного канала связи



■ NB-IoT ■ Безлицензионный LPWAN

Безлицензионные решения имеет смысл применять только в области где их эффективность оправдана и заведомо выше решений на основе сотовых систем связи

Место безлицензионного LPWAN на рынке IoT

Ниша безлицензионного LPWAN

1. Сделать дешевле КУ и сеть
 2. Работать там, где нет сотовой связи
 3. Сделать частное локальное решение
 4. Уменьшить или обнулить абонентскую плату
 5. Создавать специализированные сети одного решения (например сеть для ЖКХ или сельского хозяйства)
- Эти задачи решает классические безлицензионные LPWAN решения – LoRaWAN и SigFox

Можно ли продвинуться дальше и повысить эффективность LPWAN?

- Уменьшение стоимости ку и сети дает возможность появиться совершенно новым кейсам применений - Голубым Океанам Интернета вещей.
- Основное условие – это должны быть кейсы миллионники.
- Интеллектуальная собственность создания нового LPWAN решения исчисляется миллионами \$ и, при низкой стоимости КУ (порядка \$30), может окупиться только при больших тиражах.

Формула эффективного LPWAN - массовые кейсы, простые и дешевые устройства, безопасная сеть.

GoodWAN в поисках Голубого Океана Интернета вещей

Возможности открыть для себя совершенно новые рынки требует
точного позиционирования на основной бизнес задаче

1. Умение отказаться от всего лишнего
2. Применение новых эффективных технологий
3. Максимальное снижению стоимости решений

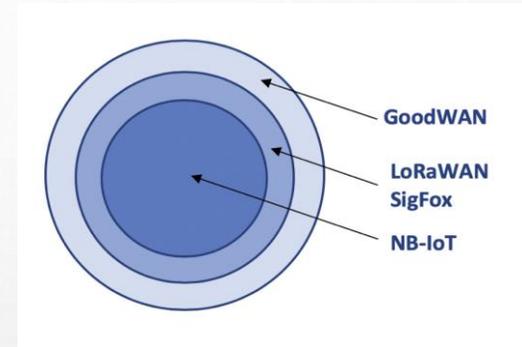
GoodWAN, три шага для открытия Голубого Океана Интернета Вещей:

1. Отказ от универсальности сети в пользу специализации на конечном наборе самых массовых кейсов применений , максимальная отстройка от NB-IoT решений
2. Минимизация стоимости устройств и их эксплуатации в сети
3. Максимально высокие требования к ключевым техническим характеристикам сети - площади покрытия, пропускной способности и безопасности

Три кита технологии GoodWAN

1. Энергоэффективный протокол (максимальная энергетика информационного бита)
2. Профессиональный радиоканал (дальность, чувствительность, помехозащищенность)
3. Идеальная безопасность (динамическая иммитовставка, динамический адрес в сети)

- **Технология GoodWAN – заточена для эффективной работы с большим объемом очень дешевых датчиков и устройств**



Технические особенности GoodWAN

GoodWAN – это LPWAN технология для создания «Голубых Океанов» на рынке Интернета вещей.

1. Объединение UNB и LoRa каналов (UNB в up-канале - высокая пропускная способность, LoRa в down-канале – симметричная дальность без увеличения мощности).
 2. Использование специального высококачественного профессионального приемника шлюза с большим динамическим диапазоном работы и устойчивого к помехам и интермодуляции.
 3. Специальный протокол физического уровня с высокой энергетикой информационного бита (максимально допустимо низкая скорость передачи при максимально короткой длине посылки в эфире для каждого кейса применений).
 4. Использование FSK UNB модуляции в радиоканале для обеспечения работы на движущихся объектах без заметной потери дальности.
 5. Необходимый уровень защиты канала (код целостности и подлинности сообщения и шифрование данных с использованием двух независимых ключей, передача ключей по воздуху, в том числе в одностороннем канале).
 6. Применение динамических ключей шифрования и динамического кодирования ID устройств.
 7. Использование только одностороннего канала в самых дешевых и массовых кейсах применений без потери качества и безопасности.
 8. Дешевые, но функциональные корпуса.
- ***Мы постарались объединить все лучшее технические решения, чтобы безлицензионный LPWAN нашел свою эффективную нишу и помогал открывать новые рынки IoT.***

Дальность LPWAN

При прочих равных условиях

1. Предельная площадь покрытия радиосистемы прямо пропорциональна энергии бита информации и обратно пропорциональна затуханию сигнала и шумам в канале, и практически не зависит от типа модуляции сигнала.

ОГРАНИЧЕНИЕ ШЕННОНА

$$S = W \cdot \log_2(1 + N_s/N_0)$$

$$N_s = N_{s0}/(K \cdot L^2)$$

$$L^2 = (N_{s0} \cdot W/S)/(N_0 \cdot K) \cdot (S/W)/(2^{(S/W)} - 1)$$

$$\text{ПРИ } S/W \leq 1, (S/W)/(2^{(S/W)} - 1) = 1 \div 1,4$$

$$L^2 \approx Q/(N_0 \cdot K)$$

N_0 и N_s - средняя спектральная мощность шума и полезного сигнала на входе приёмника.

N_{s0} - средняя спектральная мощность полезного сигнала на выходе передатчика

S - максимальная скорость в канале связи

W - ширина канала

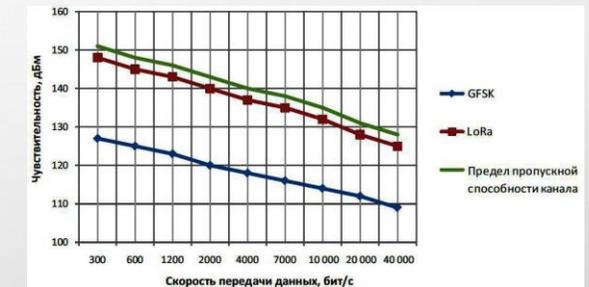
L - Максимальное расстояние между приемником и передатчиком

K - усредненный коэффициент затухания сигнала в пространстве

L - расстояние между передатчиком и приемником.

K - усредненный коэффициент затухания сигнала в пространстве

$Q = N_{s0} \cdot W/S$ - энергия одного бита передатчика



2. Дальность работы LPWAN систем критично зависит от высоты подъема антенны шлюза, и это не потому, что земля закругляется. В городе чаще всего сигнал приходит на приемник отразившись от стен ближайших домов. Поднимая приемник, Вы увеличиваете эффективную площадь отраженного сигнала, которую она видит.

- Увеличение скорости в 2 раза - в 2 раза уменьшает площадь покрытия шлюза для любых видов модуляции как UNB, так и LoRa.
- Увеличение высоты подъема антенны в 2 раза - в 2 раза увеличивает площадь покрытия шлюза

Длина посылки, энергоэффективность бита

Энергоэффективность – обеспечение большой дальности за счет вложения максимальной энергии в каждый бит с одновременным максимальным сокращением длины посылки для увеличения срока работы от одной батарейки и пропускной способности сети.

Минимальная структура LPWAN сообщения

- | | |
|----------------------------------|------------|
| • Преамбула | 4 байт |
| • Адрес устройства в сети | 4 байта |
| • Информация пользователя | 0-12 байт* |
| • CRC | 2 байта |
| • Иммитовставка | 2 байта |
| • Динамическая вставка / счетчик | 2 байта |
| • Служебная информация | 0-4 байта |
| • Помехозащищенное кодирование | x2* |

Преимущества коротких сообщений

- Возможно увеличение дальности за счет уменьшения скорости передачи
- Больше срок службы батарейки
- Больше пропускная способность системы
- Больше помехозащищенность сообщения

Полезная информация в эфире (LoRa, SigFox) значительно удлиняется. Для простого датчика, например температуры, полезная информация составляет 6 байт, но в эфире передается не менее 24 байт.

- *Безлицензионный LPWAN не предназначен для передачи потоковых данных*
- *Ресурс датчика - порядка 50 000 сообщений от одной литиевой батарейки 2 000 мАЧ*

Пропускная способность

Пропускная способность сети ограничена в первую очередь вероятностью коллизий в up-канале.

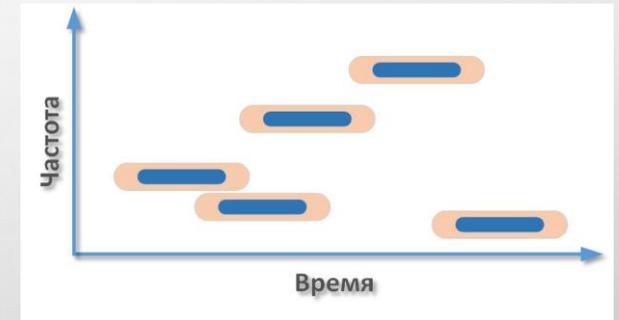
Для сетей LoRaWAN, вероятность коллизии при небольшой загрузке сети: $k=3600 * p * n_f / t_p / 2$ (где n_f – количество каналов, p - вероятность наложения, t_p – длительность посылки).

Пропускная способность стандартного 8-канального LoRaWAN шлюза с $sf=12$ и длиной посылки 1,2 секунды, ограничена 2300 сообщениями в час при 10% вероятности потери сообщения и если более слабый сигнал подавляет более сильный.

В UNB системах понятие канала передатчика размыто, КУ выходит в эфир в полосе приема шлюза на случайной частоте.

Вероятность коллизии при небольшой загрузке сети: $K=3600 * P * F_B / F_K / 4$ (где P - вероятность наложения, F_B - ширина канала приемника, F_K – ширина спектра передатчика, T_p – длительность посылки)

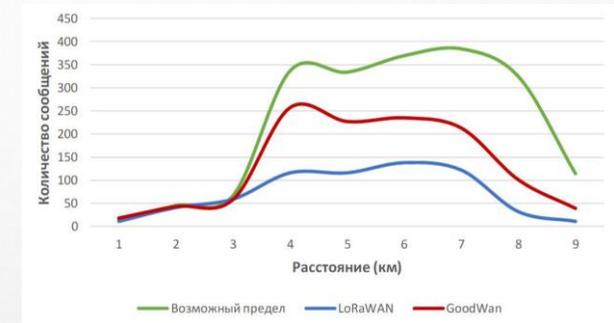
Для GoodWAN расчётное значение пропускной способности up-канала шлюза с полосой 192 кГц и длиной посылки 1,6 секунды, соответствует 54 000 сообщениям в час. У SigFox, Стрижа и Waviot, это значение будет еще больше за счет использования фазовой модуляции в канале.



- **Пропускная способность UNB канала более, чем на порядок превышает пропускную способность LoRaWAN**
- **Увеличение пропускной способности за счет увеличения скорости приводит к пропорциональному уменьшению площади покрытия шлюза**

Вероятность доставки, повторы и пропуски сообщений

- В любых радиосетях всегда существует вероятность потери отдельного сообщения.
- Асинхронный характер передачи сообщений предполагает не нулевую вероятность их коллизий в эфире.
- Доставка сообщения с получением квитанции в LPWAN сетях фактически не возможна из-за особенностей работы обратного канала.
- SigFox применяет тоекратный повтор каждого сообщения в эфире
- GoodWAN разделяет весь информационный поток от КУ на два типа сообщений – «мониторинг состояния» и «важное сообщение». «Мониторинг состояния» передается с помощью одной посылки, а доставка «важного сообщения» обеспечивается за счет нескольких повторов посылок (до 5 повторов).
- Сеть GoodWAN строится исходя из вероятности потери одного не критичного сообщения 10^{-1} и обеспечивает вероятность потерь для критичных сообщений 10^{-5} .
- *Сравнение площадей out-door покрытия в реальных городских условиях для различных типов LPWAN систем проще всего оценивать в вероятности пропуска сообщения в зависимости от расстояния*



Количество переданных и принятых сообщений в зависимости от расстояния до шлюза в реальной городской застройке для out-door покрытия.

Динамический диапазон

Реальная дальность прямого канала определяется качеством приемника шлюза по нескольким параметрам одновременно: чувствительность, динамический диапазон, избирательность, интермодуляция, собственные шумы.

Почему необходим высокий динамический диапазон для UNB систем

- Объявлена высокая чувствительность у ведущих производителей (LoRa -137 dBm, SigFox, Стриж -145 dBm, Waviot -153 dBm)
- Если в UNB используется классический SDR приемник с 16 разрядным АЦП на входе, то рабочий диапазон составляет 12-13 разрядов (2-3 младших бита надо отдать на шумы, а один старший оставить на переполнение) или 75 dB диапазона по мощности. При чувствительности -145 dBm, это ограничивает максимальную мощность сигнала на входе приемника -70 dBm.
- Такую мощность создает 100 мВт передатчик в прямой видимости от шлюза на расстоянии 2,5 км

Результат

- Близко расположенные передатчики выводят приемник шлюза из линейного режима!
- Если приемник шлюза с динамическим диапазоном 75 dB принимает сигнал от КУ в прямой видимости 100 метров с излучаемой мощностью 100 мВт, то его чувствительность фактически ограничена -120 dBm!
- ***UNB приемник должен одновременно принимать сильные и слабые сигналы в диапазоне не менее 110 dB и иметь как минимум 24 разрядное АЦП на входе.***

Информационная Безопасность

Источники угроз LPWAN

1. Легкость доступа к физическому каналу передачи данных (ISM диапазон, большой радиус действия, доступность оборудования)
2. Открытые стандарты
3. Ограничения в объеме передаваемой информации
4. Крайне ограниченные возможности обратного канала
5. Открытое ID конечного устройства



Методы защиты физического уровня LPWAN

1. Помехоустойчивое кодирование
2. Проверка целостности (CRC)
3. Иммитовставка (цифровая подпись)
4. Защита от повторов
5. Шифрование информации
6. Смена ключей по воздуху
7. *Динамическое кодирование адреса

Динамическое кодирование

Открытая передача адреса в сети – основной элемент снижающий безопасность LPWAN систем.

Для большого класса КУ сам факт передачи сигнала от конкретного устройства может нести в себе достаточно информации для злоумышленника, например - охранные датчики, по активности которых в эфире можно определить сам факт их срабатывания.



- Существуют системы, в основном военные, которые синхронизируют смену ключей шифрования и свой адрес в сети по времени.
- Основной проблемой такого типа систем является необходимость постоянной точной синхронизации часов передатчика с часами приемника.
- Решение GoodWAN позволяет каждые 4 минуты изменять ключ иммитовставки и сам адрес КУ в сети, необходимая синхронизация часов сервера сети с часами КУ возможна по времени прихода регулярных сообщений ur-канала по часам принявшего это сообщение шлюза.

- **Динамическое кодирование на физическом уровне – реальная возможность сделать LPWAN действительно безопасным.**

Недооцененный односторонний канал

Для определенного и достаточно массового класса устройств, где нет необходимости ими управлять – нет необходимости в обратном канале.

Большинство современных систем радиохраны большого радиуса действия работает по одностороннему каналу и обеспечивает при этом все высокие требования к системам профессиональной охраны объектов.

GoodWAN в своих решениях для создания наиболее массовых и дешевых устройств активно использует одностороннюю технологию без ухудшения надежности и безопасности работы системы.

Дополнительные особенности.

Односторонний канал GoodWAN это:

- Постоянный контроль канала связи
- Высокая пропускная способность сети
- Обеспечение требований безопасности
- Возможность передача ключей по воздуху
- Дешевые конечные устройства

- Классификация сообщений на «регулярные» (вероятность пропаданий до 10%) и редкие «важные» события (вероятностью пропуска не хуже 10^{-5}), передаваемые с пяти-кратным повтором
- Контроль канала за счет передачи контрольных сообщений
- Запрет на передачу потоковых данных
- Запрет на обновление прошивки по воздуху по LPWAN каналу

- **Односторонний канал – самый эффективный элемент безлицензионной LPWAN системы.**

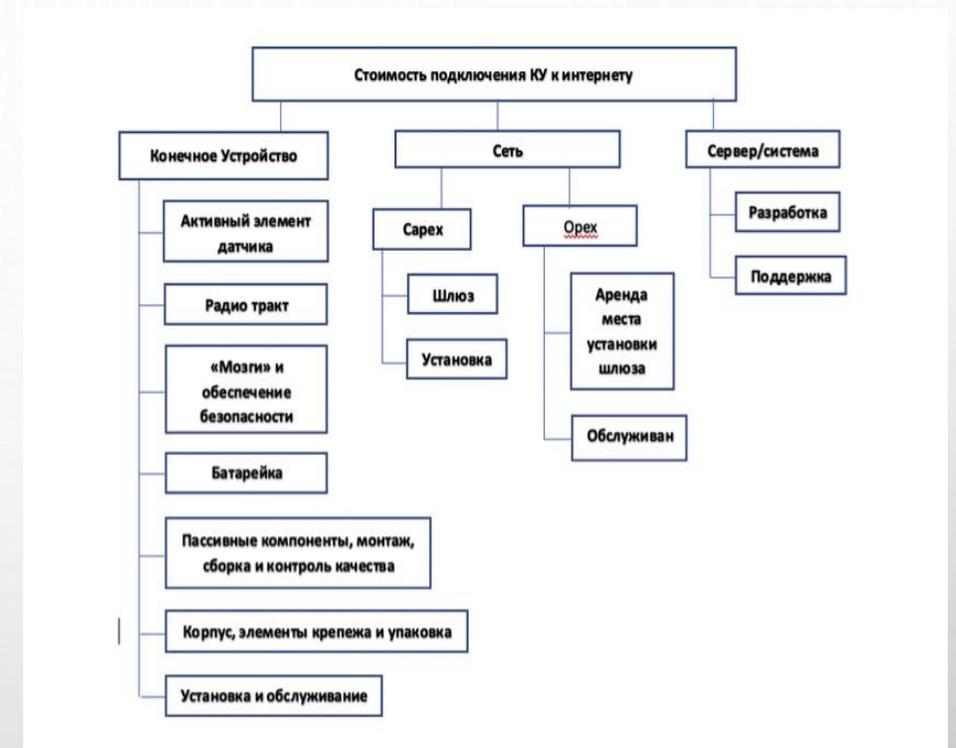
Экономика LPWAN

Структура стоимости

- Стоимость КУ \$35-100
- Стоимость шлюзов и сервера* \$300-2000
- Абонентская плата* \$0,5-10

Структура себестоимости при среднесерийном производстве (оценка для элементарного КУ)

- Себестоимость КУ \$10-25
 - Чувствительный элемент (датчик) \$1-4
 - Радиоканал \$2-4
 - Мозги (тактика работы, радиопrotocol, шифрование) \$3-4
 - Плата, сборка, контроль качества \$2-5
 - Батарейка, антенна \$1,5
 - Корпус \$1-2
 - Упаковка, инструкции, установочные элементы \$1-2
- Поддержание сети
 - Сарех \$1000
 - Орех \$800/мес
- Сервер ?
- Интеллектуальная стоимость ?
- Продвижение и продажи x2-3



- *Содержание сети за счет абонентской платы или включено в стоимость устройств

Дизайн конечных устройств

Требования к низкой стоимости устройств накладывает определенные ограничения на конструкцию и внешний дизайн конечных устройств.

Например, если для потребительской электроники внешний вид изделия имеет чуть ли не первостепенное значение, то для датчиков промышленного исполнения более важен класс защиты устройства:

Гаджеты и промышленные датчики – совершенно разные подходы к дизайну



- **Дизайн конечных устройств может быть очень разным – его определяет коммерческая задача.**

Кейсы - миллионники

- 1. Кнопка вызова или заказа**
 - Ритейл, умный дом, умный город, безопасность, сервисы
- 2. Датчик температуры**
 - Умный дом, умный город, лечебные учреждения, холодильники
- 3. PIR-датчик**
 - Безопасность, люки канализации, технологические помещения, шкафы, сейфы, ящики стола
- 4. Датчик угла наклона**
 - Безопасность, люки канализации, столбы, мачты, деревья
- 5. Датчик влажности почвы (тензиометрический)**
 - Сельское хозяйство
- 6. Датчик уровня жидкости**
 - МЧС – уровень водоемов и рек, подтопления, ЖКХ – подтопление подвалов, умный город – подтопление улиц
- 7. Инфракрасный датчик мусора**
 - ЖКХ
- 8. Радио-пломба бочки**
 - Логистика
- 9. Многое другое – Голубые Океаны Интернета вещей еще ждут своих решений**

Контроль открытия люка

Опытная зона контроля вскрытия люков в Москве.



Датчик – PIR, крепление на подлючнике

Передает keeralive раз в 6 часов из-под закрытого люка

Спасибо за внимание!



АЛЕКСАНДР ШЕПТОВЕЦКИЙ, ТЕХНИЧЕСКИЙ ДИРЕКТОР

SAU@GOODWAN.RU

+7 (499) 455 04 35