

# Аппаратное обеспечение IoT/CPS

## Лекция 5

А. А. Подшивалов  
[apodshivalov@miem.hse.ru](mailto:apodshivalov@miem.hse.ru)

# Модели сетевого взаимодействия

Модель OSI

Приложений

Представления

Сеансовый

Транспортный

Сетевой

Канальный

Физический

# Модели сетевого взаимодействия

Модель OSI

Приложений

Представления

Сеансовый

Транспортный

Сетевой

Канальный

Физический

Модель TCP/IP

Приложений

TCP, UDP

IP (v4, v6)

Канальный

# Модели сетевого взаимодействия

Модель OSI

Приложений

Представления

Сеансовый

Транспортный

Сетевой

Канальный

Физический

Модель TCP/IP

Приложений

TCP, UDP

IP (v4, v6)

Канальный

IETF для IoT

CoAP

UDP

IPv6

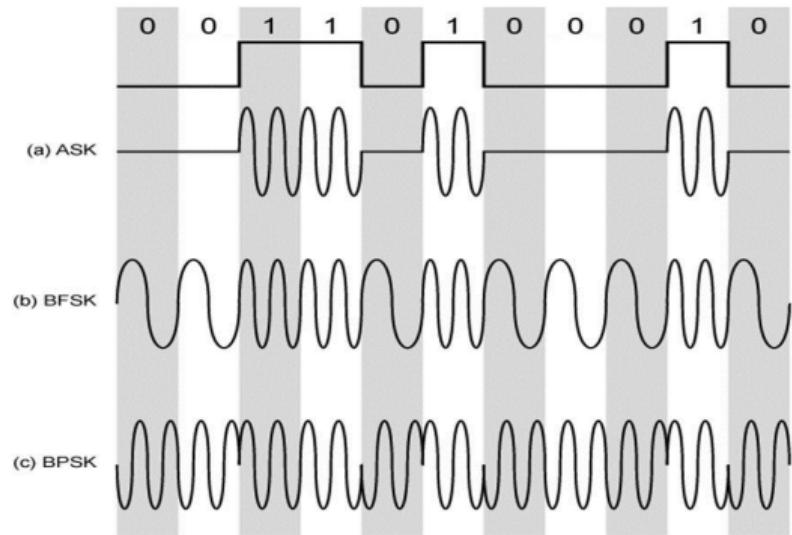
6LoWPAN

IEEE 802.15.4

# Основы цифровой радиосвязи и фундаментальные ограничения

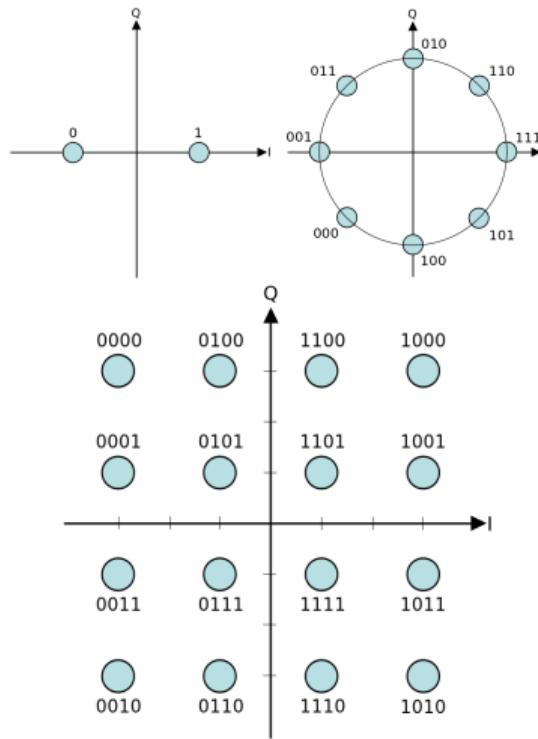
# Модуляция радиосигнала

- ▶ Изменение параметров несущего сигнала в зависимости от модулирующего сигнала
  - ▶ Амплитудная (AM)
  - ▶ Частотная (FM)
  - ▶ Фазовая (PM)
- ▶ Цифровая манипуляция
  - ▶ ASK — Amplitude shifted keying
  - ▶ FSK — Frequency shifted keying
  - ▶ PSK — Phase shifted keying
  - ▶ ...



# Цифровая манипуляция

- Передаем одним символом несколько бит
  - n-PSK
  - QAM
- OFDM — одновременно передается несколько поднесущих
- DSSS
  - Одному биту («символу») соответствует целая последовательность 0 и 1 («chips») в передаваемых данных (PSK или FSK)
  - CDMA
- CSS — Chirp Spread Spectrum



# Предел Шеннона

- Теорема Шеннона-Хартли

$$C = B \log_2 \left( 1 + \frac{S}{N} \right),$$

где:

- $C$  (capacity) — максимальная пропускная способность канала, бит/с
- $B$  (bandwidth) — полоса пропускания канала, Гц
- $S$  (signal) — полная мощность сигнала, Вт
- $N$  (noise) — мощность шума, Вт
- $\frac{S}{N}$  — отношение сигнал/шум, SNR
- При  $\frac{S}{N} \gg 1$ :

$$C = B \log_2 \left( 1 + \frac{S}{N} \right) \approx B \log_2 \frac{S}{N} = \frac{\ln 10}{\ln 2} B \log_{10} \frac{S}{N} \approx 3,32 \times B \times \log_{10} \frac{S}{N} = 0,332 \times B \times SNR^{[dB]}$$

- При  $\frac{S}{N} \ll 1$ :

$$C = B \log_2 \left( 1 + \frac{S}{N} \right) \approx B \frac{1}{\ln 2} \frac{S}{N} \approx 1,44 \frac{S}{N_0},$$

где  $N_0$  — спектральная плотность шума,  $N = BN_0$

- Термовой шум:  $N = k_B T B$ , где  $k_B = 1,380649 \times 10^{-23}$  Дж  $\times$  К — постоянная Больцмана,  $T$  — температура (в градусах Кельвина)

# Формула Фрииса

- Выражает мощность сигнала на приемнике в зависимости от расстояния (free-space pathloss)

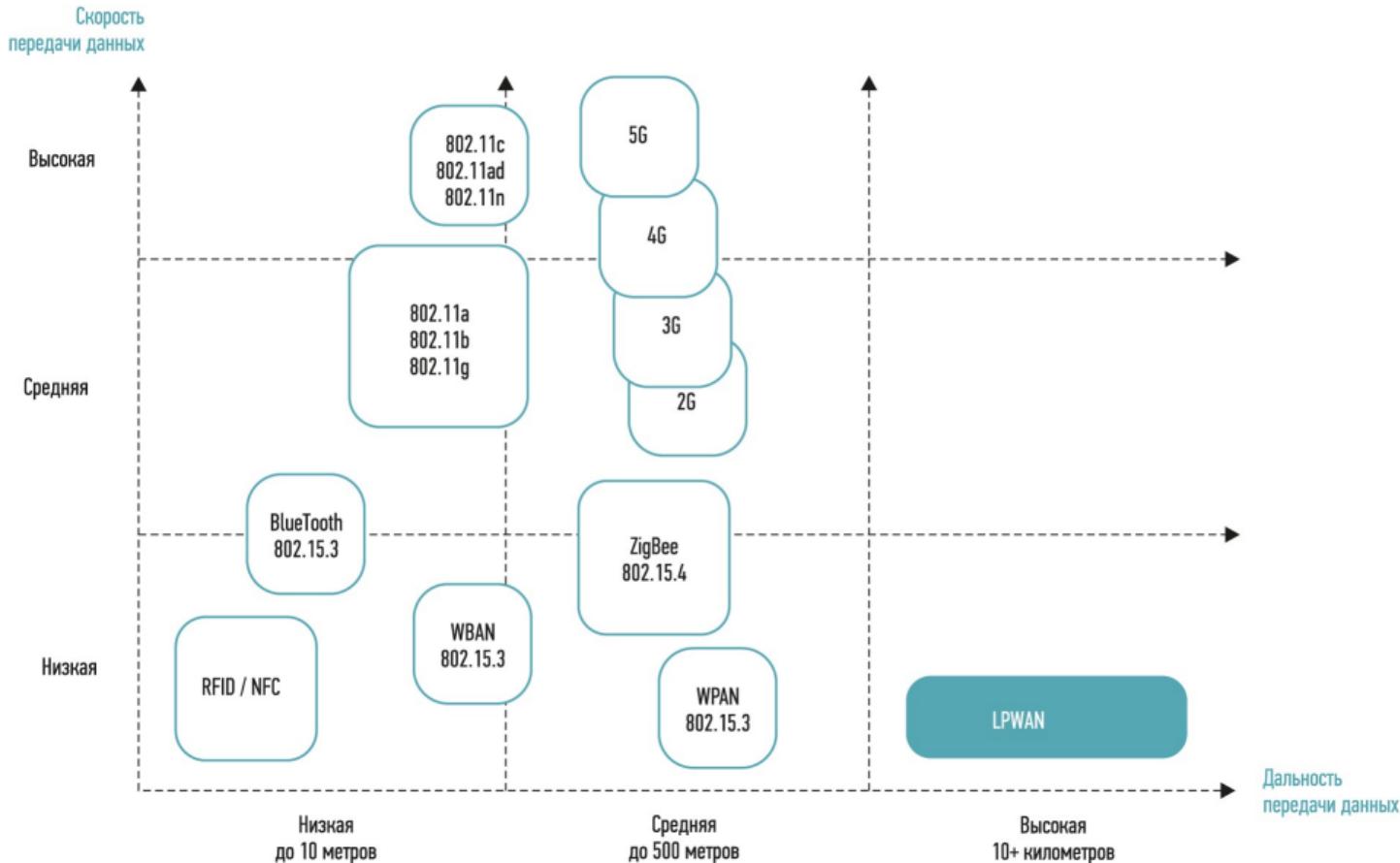
$$\frac{P_r}{P_t} = G_r G_t \left( \frac{\lambda}{4\pi R} \right)^2,$$

где:

- $P_r, P_t$  (power) — мощность сигнала на приемнике (receiver) и передатчике (transmitter)
- $G_r, G_t$  (gain) — коэффициент усиления антенн приемника и передатчика
- $R$  — расстояние между приемником и передатчиком
- $\lambda$  — длина волны
- Она же в дБ:

$$P_r^{[dBm]} = P_t^{[dBm]} + G_t^{[dBi]} + G_r^{[dBi]} + 20 \log_{10} \frac{\lambda}{4\pi R}$$

# Фундаментальные ограничения и реальные технологии



# Два класса технологий IoT

- ▶ LPWAN, Low-power Wide Area Network
  - ▶ Скорость передачи не важна (сотни, редко тысячи бит/с), требуется большая зона покрытия
  - ▶ UNB-сети (Sigfox, NB-Fi и подобные), LoRa/LoRaWAN, в некоторой степени — NB-IoT
  - ▶ Частотный диапазон Sub 1-GHz (433 или 868/915 МГц)
- ▶ LR-WPAN, Low-rate Wireless Personal Area Network
  - ▶ Скорость передачи относительно мала (до 250 кбит/с)
  - ▶ IEEE 802.15.4, BLE, IEEE 802.11ah
  - ▶ Частотный диапазон ISM (2,4 ГГц) или Sub 1-GHz
- ▶ «Вне зачета» — традиционные беспроводные технологии: WiFi (IEEE 802.11), Bluetooth, Bluetooth Low Energy, сотовая связь



**Мокнет одинокая свинья** @Mos\_art1 · Apr 7



В истребителе главное — мотор. Обычно авиаписарчуки тут заводят свою заклепидорскую волынку про воздушное и водяное охлаждение, какие плюсы и минусы: это всё х~~у~~йня.

Двигатели делятся на:

- серийные.
- перспективные.
- экспериментальные.

6

2

43

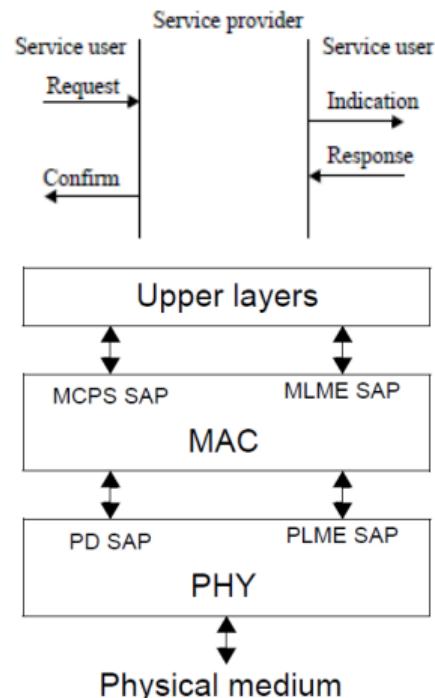
Конкретные примеры: WPAN и mesh-сети

# Канальный уровень

- ▶ Формирование кадров (MPDU)
- ▶ MAC — Medium Access Control, управление доступом к среде передачи
  - ▶ Очередность доступа, особенно в случае TDMA
  - ▶ Разрешение коллизий
  - ▶ Адресация
- ▶ LLC — Logical Link Control, управление связью
  - ▶ Установление и разрыв соединения
  - ▶ Подтверждение передачи, повторная отправка кадров
- ▶ Защита информации

# Стандарт IEEE 802.15.4

- ▶ Описывает физический (PHY) и MAC-уровни беспроводных персональных сетей (WPAN, wireless personal-area network) и интерфейсы между ними
- ▶ Несколько разных вариантов PHY, скорость передачи данных от 10 до 1000 кбит/с, размер пакета — 127 байт
  - ▶ GFSK, 50 кбит/с, 868/915 МГц; типичная чувствительность приемника (CC1310) — -110 дБм
  - ▶ Q-PSK DSSS, 250 кбит/с, 2,4 ГГц; типичная чувствительность приемника (CC2630) — -100 дБм



# MAC-уровень 802.15.4

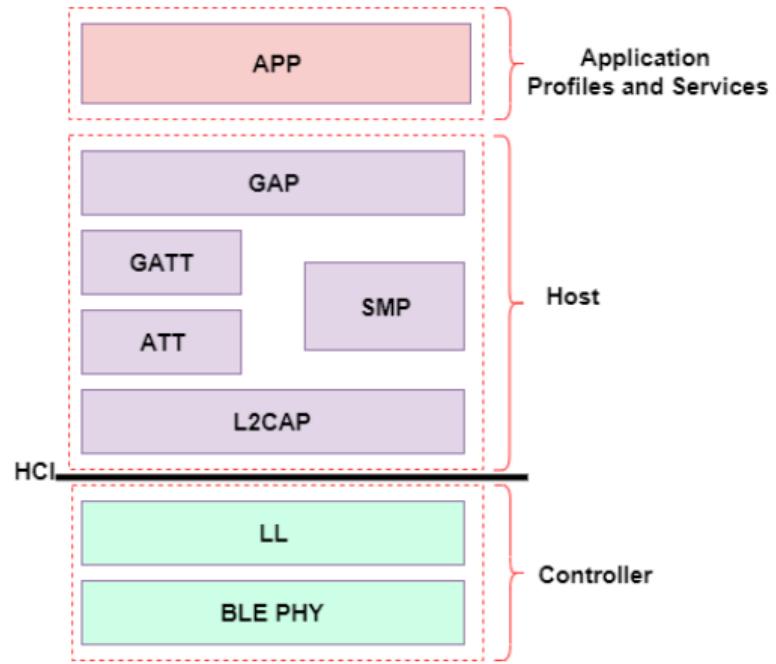
- ▶ Структура кадров, различные их типы (beacon, data frame, acknowledgement, MAC command)
- ▶ Алгоритмы доступа к каналу
- ▶ Адресация с помощью 6- и 2-байтовых адресов (6-байтовый адрес — это EUI-48)
- ▶ Топология сети — «звезда» или mesh
- ▶ Ассоциация и деассоциация
- ▶ Подтверждение приема данных
- ▶ Защита информации

# 6LoWPAN

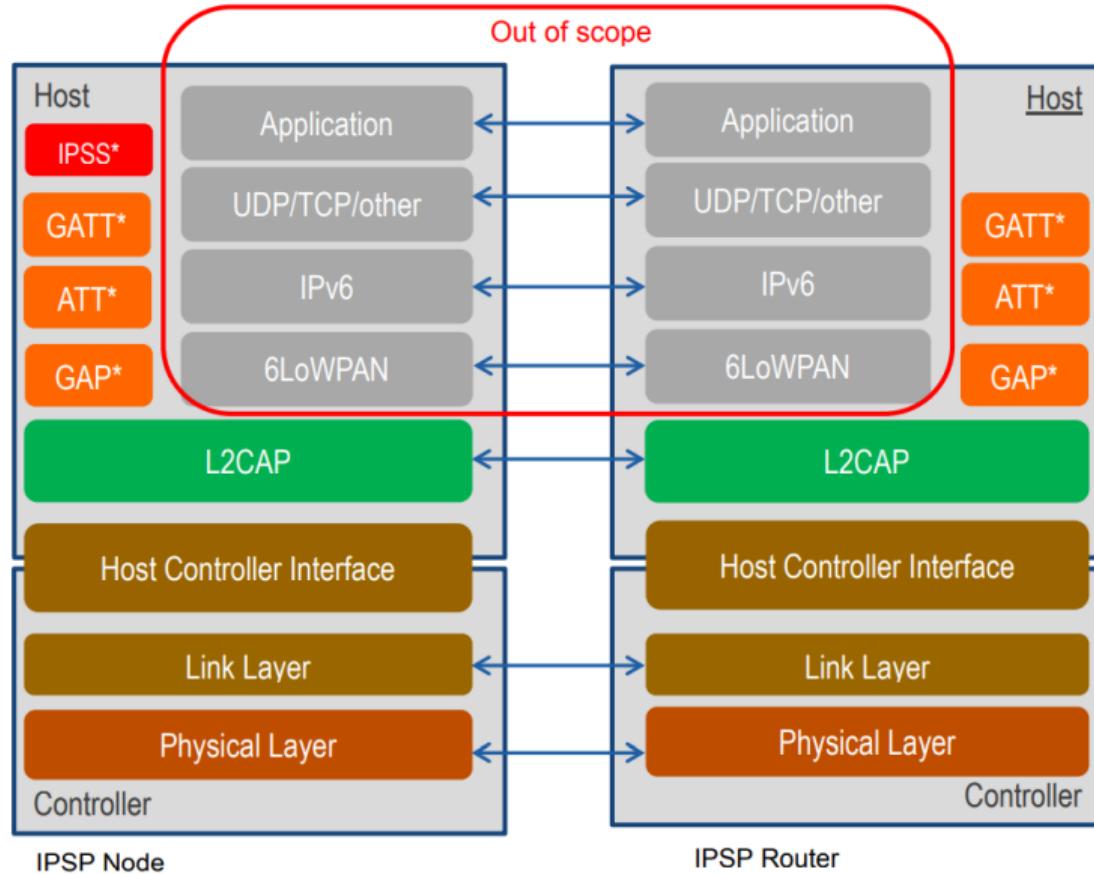
- ▶ Стандарт передачи пакетов IPv6 в сетях IEEE 802.15.4, IPv6 over Low-Power Wireless Personal Area Networks (RFC 4944)
- ▶ Сжатие заголовков (обновлено в RFC 6282)
- ▶ Фрагментация пакетов
- ▶ Маршрутизация, два основных подхода:
  - ▶ mesh-under (LOAD, LOADng — принят как стандарт ITU-T G.9903)
  - ▶ route-over, каждый узел может выступать IP-маршрутизатором (RPL, RFC 6550 — стандарт IETF)
- ▶ Автоматическое конфигурирование адресов (с помощью ICMPv6)

# Bluetooth Low Energy

- ▶ Стандарт для небольших персональных сетей
- ▶ 40 каналов в диапазоне 2,4 ГГц, расстояние между соседними каналами 2 МГц, модуляция GFSK, 1 Мбит/с
- ▶ Ведущее и ведомое устройство обмениваются данными с некоторой периодичностью
- ▶ L2CAP — Logical Link Control and Adaptation Protocol, одна из функций — фрагментация пакетов



# 6LoWPAN поверх BLE



# Защита информации в радиосети

# Угрозы в радиосети



- ▶ Кто угодно может слушать эфир на любой частоте
- ▶ В лицензионном диапазоне любой желающий может передавать в эфир что угодно, пока не придет Роскомнадзор
- ▶ В безлицензионном диапазоне любой желающий может передавать в эфир что хочет
- ▶ Большинство IoT-систем работает в безлицензионных диапазонах (433 МГц, 868 МГц, 2,4 ГГц)
- ▶ Угрозы (далеко не исчерпывающий список)
  - ▶ Перехват данных
  - ▶ Передача фальсифицированных данных
  - ▶ Косвенное определение состояния устройства

# Наивный протокол

Адрес отправителя	Адрес получателя	Служебные поля	Данные	CRC
-------------------	------------------	----------------	--------	-----

- ▶ Целостность пакета проверяется контрольной суммой (CRC)
- ▶ Данные не зашифрованы
- ▶ Кто угодно может прочитать данные
- ▶ Кто угодно может сфальсифицировать данные

# Наивный протокол + шифрование

Адрес отправителя	Адрес получателя	Служебные поля	Данные (AES-128)	CRC
-------------------	------------------	----------------	------------------	-----

- Целостность пакета проверяется контрольной суммой (CRC)
- Данные зашифрованы, например, AES-128
- Посторонний не может прочитать данные
- Посторонний не может сфальсифицировать данные

# Подмена данных MAC-уровня

Подмена отправителя	Подмена получателя	Подмена MAC	Данные (AES-128)	CRC'
---------------------	--------------------	-------------	------------------	------

- ▶ Получаем из эфира чужой пакет
- ▶ Меняем что угодно, кроме зашифрованных данных
- ▶ Пересчитываем контрольную сумму
- ▶ Те же данные, но от другого отправителя, или к другому получателю, или...

# Добавляем имитовставку (MIC)

Адрес отправителя	Адрес получателя	Служебные поля	Данные (AES-128)	MIC
-------------------	------------------	----------------	------------------	-----

- ▶ Шифрование всего пакета слишком ресурсоемко
- ▶ Вместо (или вместе с) контрольной суммы используем MIC (Message Integrity Code, имитовставка) — зависящую от ключа одностороннюю хеш-функцию
- ▶ AES-CMAC и другие подобные алгоритмы

# Определение состояния устройства

Адрес отправителя	Адрес получателя	Служебные поля	Данные (AES-128)	MIC
-------------------	------------------	----------------	------------------	-----

- ▶ Шифрование AES-ECB: каждый раз один и тот же ключ
- ▶ Зашифрованный блок меняется, только если меняются исходные данные
- ▶ Даже не расшифровывая блок данных, можно понять, изменились ли они
- ▶ Если показания водосчетчика не менялись уже неделю — в квартире никого нет

# Добавляем «соль»

Адрес отправителя	Адрес получателя	Служебные поля	Данные+«соль» (AES-128)	MIC
-------------------	------------------	----------------	-------------------------	-----

- ▶ 2 или 4 случайных байта
- ▶ При приеме и расшифровке «соль» отбрасывается
- ▶ Одни и те же данные, но разная «соль» — разные зашифрованные блоки

# Атака повтором

Адрес отправителя	Адрес получателя	Служебные поля	Данные+«соль» (AES-128)	MIC
-------------------	------------------	----------------	-------------------------	-----

- ▶ Прослушиваем эфир, записываем нужный пакет
- ▶ В нужный нам момент времени воспроизводим его
- ▶ Пример: охранная сигнализация, датчик вскрытия окна

# Защита от атаки повтором

Адрес отправителя	Адрес получателя	Служебные поля	CTR	Данные (AES-CTR)	MIC
-------------------	------------------	----------------	-----	------------------	-----

- ▶ Добавляем счетчик или nonce (number used once)
- ▶ Счетчик может только возрастать, nonce не должен повторяться
- ▶ Сброс счетчика в 0 — отдельная и редкая процедура

# Активная атака повтором

Адрес отправителя	Адрес получателя	Служебные поля	CTR	Данные (AES-CTR)	MIC
-------------------	------------------	----------------	-----	------------------	-----

- ▶ Записываем пакет с номером  $n$  и одновременно «глушим» его на приемнике
- ▶ Записываем пакет с номером  $n + 1$  и одновременно «глушим» его на приемнике
- ▶ Воспроизводим пакет с номером  $n$  (пользователь считает, что это — пакет с номером  $n + 1$ )
- ▶ Затем воспроизводим пакет с номером  $n + 1$

Конкретные примеры: LPWAN

# LPWAN: Диапазон 868 МГц в России

## Приложение 12 к Решению ГКРЧ № 18-46-03-1 от 11 сентября 2018 года

*Неспециализированные (любого назначения) устройства — устройства малого радиуса общего применения, включая устройства дистанционного управления и передачи телеметрии, телеуправления, сигнализации, передачи данных и других подобных передач*

- ▶ 864,0 — 865,0 МГц — мощность до 25 мВт, рабочий цикл до 0,1% или LBT (listen before talk), запрещено использование на территории аэропортов
- ▶ 866,0 — 868,0 МГц — мощность до 25 мВт, рабочий цикл до 1% или LBT, запрещено использование на территории аэропортов, спектральная плотность мощности до 1000 мВт/МГц
- ▶ 868,7 — 869,2 МГц — мощность до 100 мВт, рабочий цикл до 10% или LBT, использование без ограничений

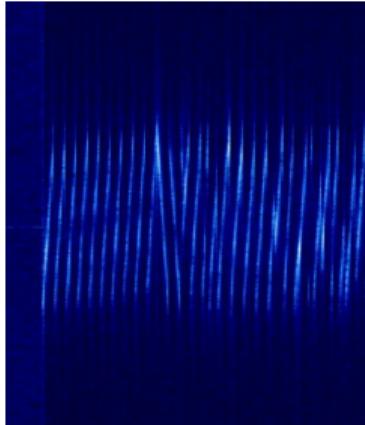
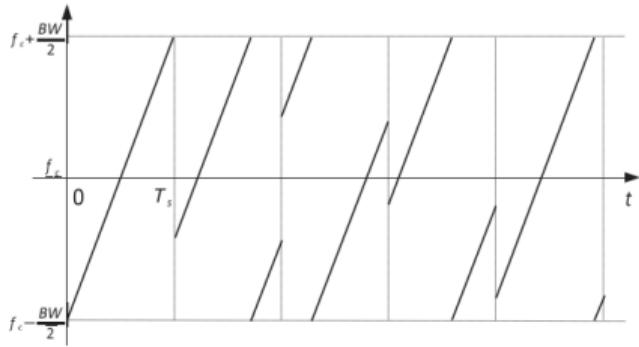
# LPWAN: Sigfox и аналоги

- ▶ UNB — Ultra-Narrow Band; Sigfox, Стриж, Waviot, NB-Fi, Феникс...
- ▶ Скорость передачи — 50/100/200 бит/с, модуляция FSK или PSK
- ▶ Очень узкая полоса (50–200 Гц)
- ▶ Сложная БС, проблемы с организацией нисходящего канала
- ▶ Закрытый протокол МАС-уровня (в РФ частично стандартизирован в ГОСТ Р 70036-2022)

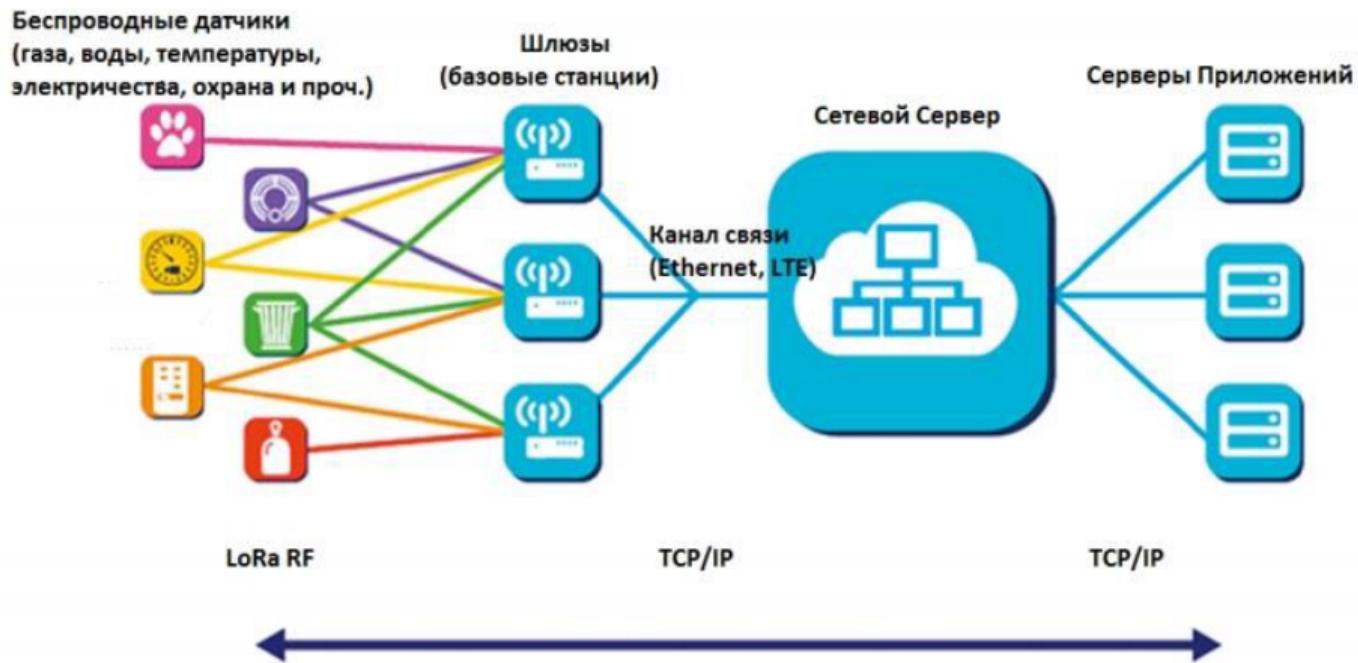


# Модуляция LoRa

- ▶ Линейно-частотная модуляция (CSS, Chirp Spread Spectrum)
- ▶ Модуляция — «излом» чирпа в некоторый момент
  - ▶ SF — коэффициент расширения спектра, «наклон» чирпа и количество бит/чирп
  - ▶ Ширина полосы (от 7,81 до 250 кГц)
  - ▶ ECC — error-correcting code (4/5, 4/6, 4/7, 4/8)
- ▶ Ортогональность различных SF
- ▶ Очень высокая чувствительность приемника (от -136 до -118 дБм в зависимости от скорости передачи данных — от 300 бит/с до 10 кбит/с)



# LPWAN: LoRaWAN



# Шлюз LoRaWAN

- ▶ Внутри модем SX1301/SX1302
- ▶ Принимает все пакеты на 8 частотных каналах одновременно, пересыпает их сетевому серверу
- ▶ По запросу сетевого сервера — передает данные оконечным устройствам

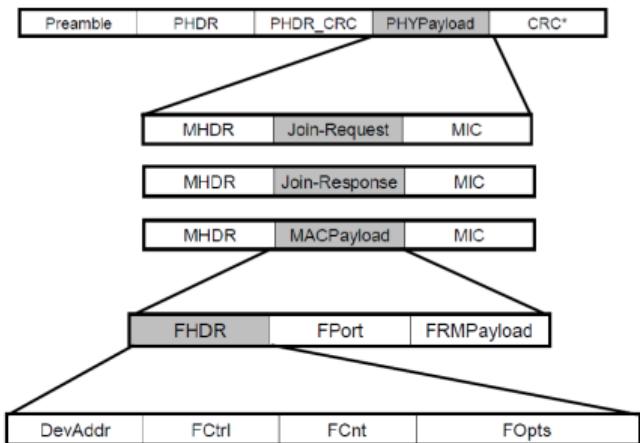


[https://github.com/Lora-net/packet\\_forwarder](https://github.com/Lora-net/packet_forwarder)

# Шлюз LoRaWAN

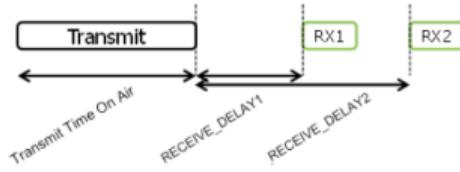


# Структура кадра LoRaWAN



- ▶ Преамбула — 12 чирпов
- ▶ PHDR — заголовок для РНУ с параметрами модуляции
- ▶ CRC — контрольная сумма, используется только для uplink
- ▶ MHDR — заголовок МАС-уровня, 1 байт с типом сообщения и версией протокола
- ▶ MIC — Message Integrity Code, AES-CMAC с использованием ключа сети (Network Session Key)
- ▶ Payload, «полезная нагрузка» AES-128 с помощью ключа приложения (Application Session Key)
- ▶ FCnt — frame counter, счетчик кадров

# Классы устройств LoRaWAN



- ▶ После передачи данных устройство готово к приему данных
- ▶ Сеть должна ответить либо в первом «окне приема», либо во втором
  - ▶ RX1 — частота и параметры модуляции зависят от частоты и модуляции, использованной при uplink
  - ▶ RX2 — частота и параметры модуляции фиксированы (по умолчанию — в региональных параметрах, могут быть изменены командой от сети устройству)
- ▶ Класс B (Beacon) — дополнительные «окна приема» по расписанию
- ▶ Класс C (Continuous) — всегда готово к приему данных на RX2

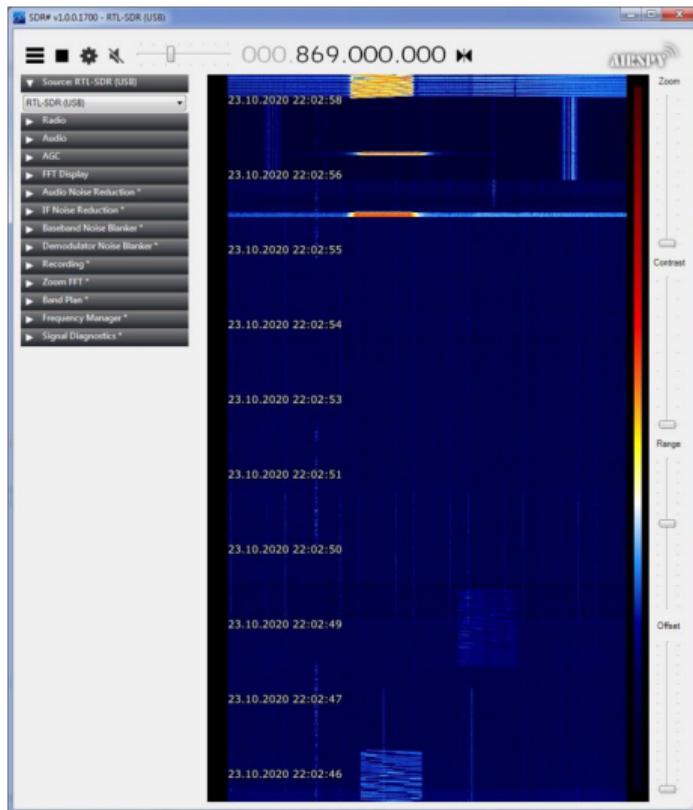
# Частотный план LoRaWAN

- ▶ Regional Parameters — приложение к стандарту
  - ▶ Используемые частоты (обязательные каналы для Join)
  - ▶ Виды модуляции
  - ▶ Продолжительность RECEIVE\_DELAY, JOIN\_ACCEPT\_DELAY
  - ▶ Параметры RX1 и RX2
  - ▶ Размер payload
- ▶ Дополнительные каналы сообщает сетевой сервер (вместе с JoinAccept)

# Частотный план LoRaWAN — RU864 и EU868

- ▶ Для РФ определен частотный план RU864, сильно отличающийся от EU868
- ▶ EU868
  - ▶ Три обязательных канала: 868,10, 868,30, 868,50 МГц, ширина полосы 125 кГц
  - ▶ До 5 дополнительных каналов
  - ▶ RX2 — на частоте 869,525 кГц, DR0 (SF12, 125 кГц)
- ▶ RU864
  - ▶ Два обязательных канала: 868,90, 869,10 МГц, ширина полосы 125 кГц
  - ▶ До 6 дополнительных каналов, обычно выбираются в диапазоне 864-865 МГц, с 2018 года можно использовать 866-868 МГц
  - ▶ RX2 — на частоте 869,10 кГц (совпадает с одним из обязательных каналов), DR0 (SF12, 125 кГц)

# Обмен в сети LoRaWAN



- ▶ Частота — по горизонтальной оси, время — по вертикальной («водопад»)
- ▶ Цвет — мощность принятого сигнала
- ▶ Видно оба обязательных канала
- ▶ Внизу — обмен с малым DR, ответ в RX2 через 2 с
- ▶ Вверху — обмен с большим DR, ответ в RX1 через 1 с

# Защита данных в LoraWAN

- ▶ Шифрование данных, защита от подмены служебных полей (AES-CMAC), защита от атаки повтором (AES-CTR)
- ▶ Активация — обнуление счетчика кадров и выработка двух ключей (Network Session Key, Application Session Key)
- ▶ ABP — Activation by Personalisation
  - ▶ Сессионные ключи «вшиты» в устройство, счетчик никогда не обнуляется
  - ▶ При компрометации ключей их невозможно сменить
  - ▶ 16-битный счетчик может переполниться
- ▶ OTAA — Over-the-air activation
  - ▶ Для получения сессионных ключей нужен обмен кадрами Join-Request и Join-Response, при этом обнуляются счетчики кадров
  - ▶ Нужен один «вшитый» в устройство ключ (Application Key)
  - ▶ При компрометации сессионных ключей их можно сменить (по инициативе как устройства, так и сервера сети)

# Процедура Join



Немного о криптографии и генераторах  
случайных чисел

# Три главных правила криптографии

1. Не изобретайте свой алгоритм
2. Если вам кажется, что авторы известных алгоритмов что-то сделали неправильно, но про это не написано у Брюса Шнайера — вам кажется
3. Ни при каких обстоятельствах не изобретайте свой алгоритм

## Foot-Shooting Prevention Agreement

I, \_\_\_\_\_, promise that once  
Your Name  
I see how simple AES really is, I will  
not implement it in production code  
even though it would be really fun.

This agreement shall be in effect  
until the undersigned creates a  
meaningful interpretive dance that  
compares and contrasts cache-based,  
timing, and other side channel attacks  
and their countermeasures.

X \_\_\_\_\_  
Signature \_\_\_\_\_ Date \_\_\_\_\_

# Средства операционной системы

- ▶ sys/crypto — алгоритмы шифрования
- ▶ sys/hashes — хеши, в том числе криптографические
- ▶ sys/random — генератор **псевдослучайных** чисел

# True random number generator

Настоящий генератор случайных чисел может быть только аппаратным:

- ▶ Подбрасывание монеты
- ▶ Вращение рулетки
- ▶ Физические процессы, корнями уходящие в квантовую механику
  - ▶ Дробовой шум
  - ▶ Туннелирование электронов

# Pseudo random number generator

- ▶ Сложная числовая функция, выдающая почти непредсказуемую последовательность чисел с очень большим периодом
- ▶ Если не сказано иного — всегда предполагайте псевдослучайность
- ▶ Последовательность определяется одним числом — *seed*
- ▶ При одном и том же *seed* — одна и та же последовательность
- ▶ *seed* должен быть *настоящим* случайным числом

# Инициализация PRNG

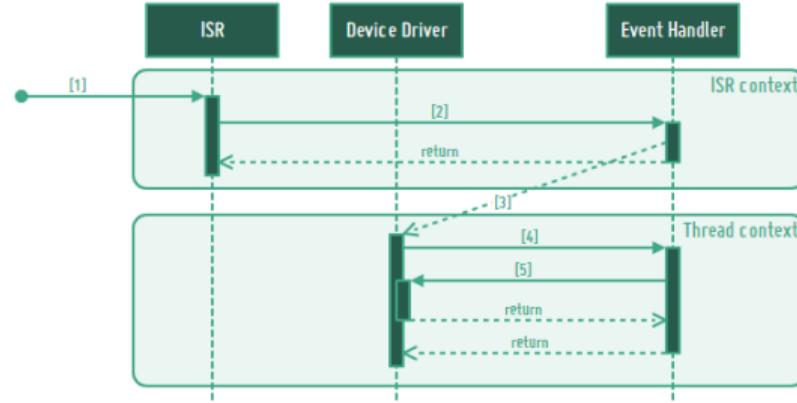
- ▶ Источники «настоящих» случайных чисел обычно медленные
- ▶ Удобно получить одно случайное число и использовать его, как *seed* для PRNG
- ▶ Источники случайности приемлемого качества:
  - ▶ Действия пользователя в интерактивной системе
  - ▶ Микрошум на «висящем в воздухе» входе АЦП
  - ▶ Шум в радиоэфире
  - ▶ Отклонения двух тактовых генераторов
- ▶ Источники случайности неприемлемого качества:
  - ▶ Время, прошедшее с момента старта системы
- ▶ Можно собрать много приемлемых случайных чисел и посчитать для них криптографический хеш

Сетевой стек ОС Riot

# Основные варианты

- ▶ lwIP — популярная реализация TCP/IP для встраиваемых систем (Ethernet, IPv4, TCP, UDP)
- ▶ Semtech LoRaMAC — «эталонная» реализация LoRaWAN и ее адаптация для Riot
- ▶ GNRC — собственный сетевой стек Riot (IPv6, UDP, статус реализации TCP — «экспериментальный»)
- ▶ NimBLE — реализация стека BLE (портирована из ОС Mynewt)

# Интерфейс netdev



```
const netdev_driver_t sx127x_driver = {
    .send = _send,
    .recv = _recv,
    .init = _init,
    .isr = _isr,
    .get = _get,
    .set = _set,
};
```

# Сетевой стек GNRC

- ▶ Каждый сетевой протокол обслуживается отдельным потоком
- ▶ В ходе обработки пакета он передается между уровнями с помощью средств IPC
- ▶ Пакет состоит из нескольких фрагментов (snips), это могут быть заголовки, фрагменты заголовков, данные...
- ▶ Для хранения данных используется «буфер пакетов» с собственным управлением памятью

