Аппаратное обеспечение IoT/CPS
Лекция 7

А. А. Подшивалов
apodshivalov@miem.hse.ru

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), зона покрытия — до десятков метров, интересно энергосбережение
  - 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

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

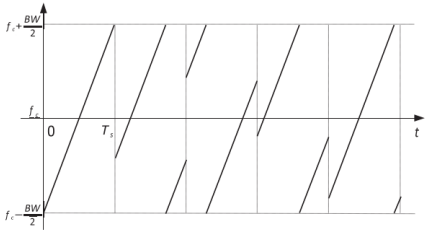
- 864,0 — 865,0 МГц — мощность до 25 мВт, рабочий цикл до 0,1% или LBT (listen before talk), запрещено использование на территории аэропортов
- 866,0 — 868,0 МГц — мощность до 25 мВт, рабочий цикл до 1% или LBT, запрещено использование на территории аэропортов, спектральная плотность мощности до 1000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

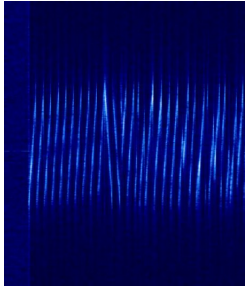
LPWAN: Sigfox и аналоги

- 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 MAC-уровня (в РФ частично стандартизирован в ГОСТ Р 70036-2022)

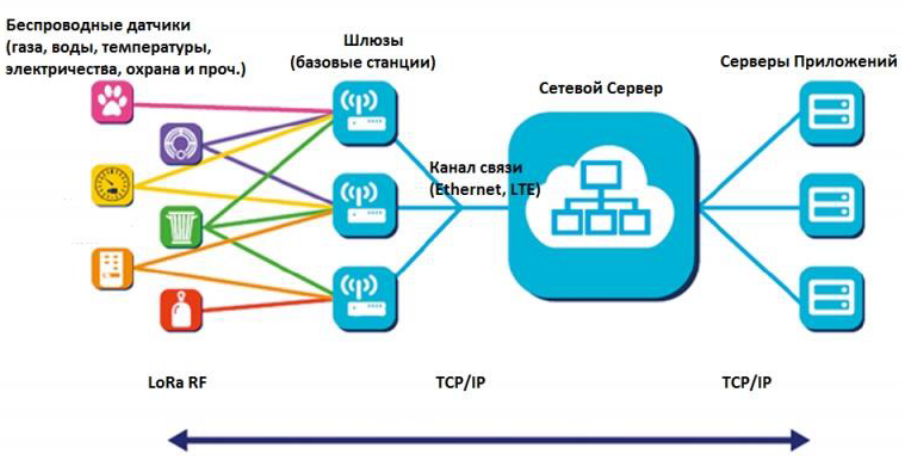
Модуляция LoRa

- 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



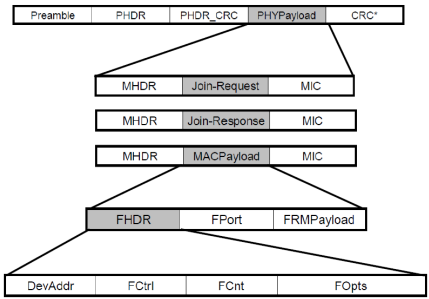
Шлюз LoRaWAN

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

https://github.com/Lora-net/packet_forwarder

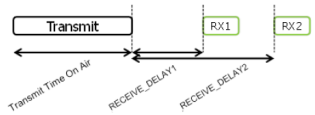
Шлюз LoRaWAN

Структура кадра LoRaWAN



- Преамбула — 12 чирпов
- PHDR — заголовок для PHY с параметрами модуляции
- CRC — контрольная сумма, используется только для uplink
- MHDR — заголовок MAC-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

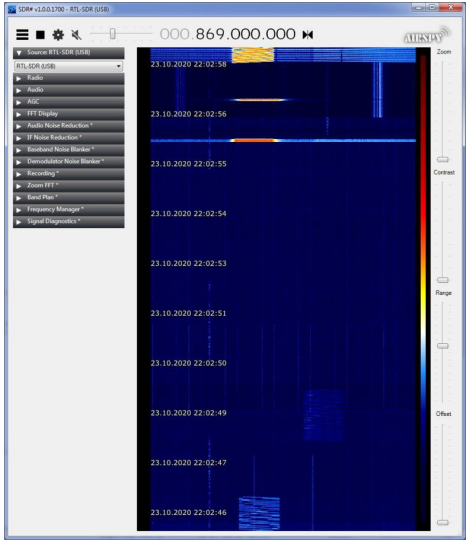
Частотный план LoRaWAN

- 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

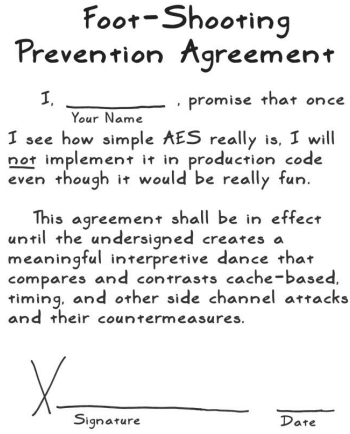
- Шифрование данных, защита от подмены служебных полей (AES-CMAC), защита от атаки повтором (AES-CTR)
- Активация — обнуление счетчика кадров и выработка двух ключей (Network Session Key, Application Session Key)
- ABP — Activation by Personalisation
  - Сессионные ключи «вшиты» в устройство, счетчик 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 **псевдо**случайных 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

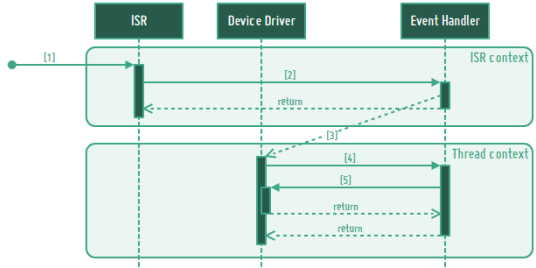
- Источники «настоящих» случайных чисел обычно медленные
- Удобно получить одно случайное число и использовать его, как *seed* для PRNG
- Источники случайности приемлемого качества:
  - Действия пользователя в интерактивной системе
  - Микрошум на «висящем в воздухе» входе АЦП
  - Шум в радиоэфире
  - 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)
- GNRC — собственный сетевой стек Riot (IPv6, UDP, статус реализации TCP — «экспериментальный», альтернативная реализация LoraWAN)
- NimBLE — реализация стека BLE (портирована из ОС Mynewt)
- Semtech LoRaMAC — «эталонная» реализация LoRaWAN и ее адаптация для Riot

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