Internet of Things Protocols

Marceau Coupechoux

24 Feb. 2021

Introduction

- It seems that the term "Internet of Things" has been first coined in 1999 by Kevin Ashton, a cofounder of the RFID lab in MIT and who was working on the supply chain of Procter and Gamble.
- At first, IoT referred to RFID technology but expanded then to sensor networks, near field communications, body area networks, machine to machine communications, personal area networks, etc.
- There a profusion of standards and technologies for IoT. Some fixed and short range tech : RFID, Bluetooth, Zigbee, WiFi. Some long range low power tech : Sigfox, LoRa, Weightless, Ingenu. Some cellular tech : EC-GSM, LTE-M, NB-IoT.
- This presentation focuses on Sigfox, LoRa and NB-IoT.

Section 1

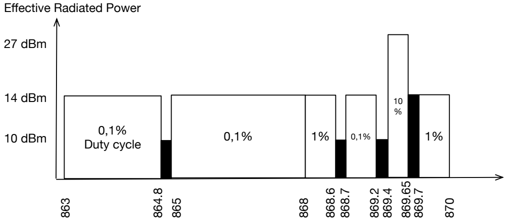
LPWAN

LPWAN characteristics I

- Long range (several kms)
- Low power consumption (battery life of several years)
- Low cost (less than 10 euros or even 1 euro for end points)
- Low data rates (few kbps)
- Targeted applications : smart meters, smart grids, smart cities (traffic control, lighting, wastes, parking, etc), healthcare, intelligent transport systems, smart buildings, smart homes, body area networks, future industry, security, agriculture, environment (air quality, water quality monitoring).
- Traffic characteristics : essentially on the uplink direction, downlink may be used for ack, configuration messages, system updates commands. Very short messages (GPS coordinates : 6 Bytes, temperature reporting : 2 Bytes, etc).
- Radio technologies are UNB (Sigfox, Telensa, Nwave, Weightless) and Spread Spectrum (LoRa, Ingenu).

Spectrum Aspects I

- The ERC Recommendation that applies for LPWAN is ERC/REC 70-03 (see also ETSI EN 300 220-1)
- Possible unlicensed bands are 169, 433, 863, 870 and 915 MHz. Every band has its own limitations in terms of available bandwidth, maximum ERP (effective radiated power), and/or duty cycle.
- The 863-870 MHz offers good tradeoffs in terms of range and antenna size. There are several subbands with different maximum ERP and/or duty cycles.
- In the range 869.4-869.65 MHz, maximum ERP is 27 dBm with a duty cycle of 10%. In the rest of the band, maximum is 24 dBm with a duty cycle of 0.1% or 1%.



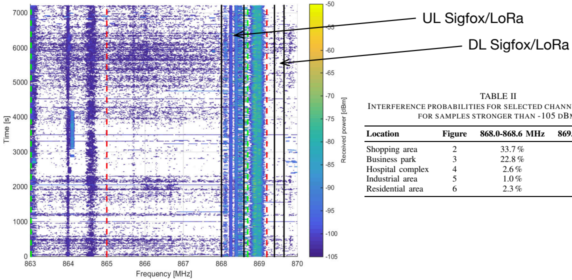
Spectrum Aspects II

- Sigfox and LoRa use ISM bands : 868 MHz in Europe+Middle East (ERC/REC 70-03), 902 MHz in US (FCC Part 15). Sub-1Ghz bands are preferred for better propagation conditions. Too low frequencies requires large antennas (e.g. 169 MHz).
- ISM bands advantages : free spectrum, available worldwide, already used by many technologies (Bluetooth, WiFi, etc), low carrier frequencies available (good propagation)
- ISM drawbacks : strict restrictions on transmit powers and duty cycles (even for base stations), possibly high interference and no QoS guarantee
- Example in Europe (ERC/REC 70-03) :
  - Uplink in 868.00-868.60 MHz : max tx power is 14 dBm, duty cycle<1%
    1% duty cycle = 36 s of activity per h = 6 messages per h (transmission of a message is approximately 6 s in Sigfox)
  - Downlink in 869.40-869.65 MHz : max tx power is 27 dBm, duty cycle<10%

Spectrum Aspects III

[Lauridsen'17, Vejlgaard'17]

- Measurements of the spectrum activity in the 868 MHz ISM band in Aalborg.
- UL may be highly interfered by smart meters, RFIDs, wireless audio, etc.
- Outdoor (resp. indoor) coverage can be reduced by 5-10% (resp. 20-50%).
- Failure rate may increase to 50-60% for LoRa and Sigfox.

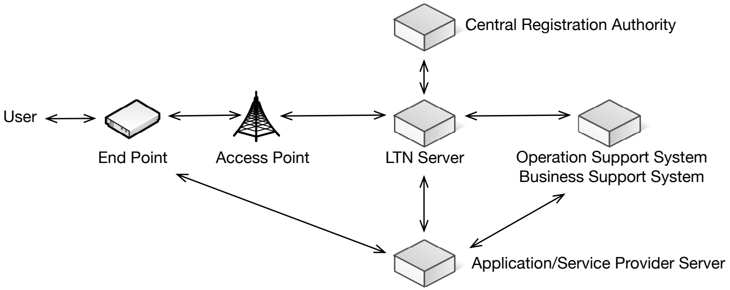


Shopping area Aalborg downtown

TABLE II
INTERFERENCE PROBABILITIES FOR SELECTED CHANNELS. MODELED FOR SAMPLES STRONGER THAN -105 dBm.

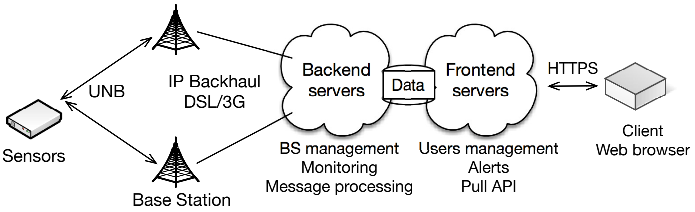
Location	Figure	868.0-868.6 MHz	869.4-869.65 MHz
Shopping area	2	33.7 %	0.9 %
Business park	3	22.8 %	58.2 %
Hospital complex	4	2.6 %	6.3 %
Industrial area	5	1.0 %	0 %
Residential area	6	2.3 %	0.1 %

ETSI Architecture for LPWAN



- LTN Server : message processing, network management
- CRA : provides unique device IDs and secret key to manufacturers
- OSS/BSS : operation and maintenance
- Application provider server : user and data management

Sigfox : Architecture I



- All messages are processes in the backend servers.
- Sensors can send/receive to/from multiple BSs.

Sigfox : Ultra Narrow Band

- Principle : Every transmission is done over a band much smaller than the system bandwidth (typically with 1/100 ratio). While typical narrowband systems use bandwidth of few kHz, UNB transmissions use few hundred Hz. Sigfox uses 100 Hz channels.
- Advantages : 1) the channel is characterized by flat fading, which simplifies analysis and receiver design, 2) receiver sensitivity is improved because of the low noise power, which allows for large coverage ranges, 3) many communications can be multiplexed in frequency domain.
- Drawbacks : 1) data rates are very low (100 bps for Sigfox uplink), 2) there is an uncertainty on the carrier frequency at both transmitter and receiver.
- Note : Quartz crystals are used for oscillators. They are known to drift because of temperature or imperfect components. They are characterized by their precision, e.g., a 20 ppm oscillator in frequency $f_c = 869$ MHz may drift by $\Delta f_c = f_c * 20/1e6 = 17.4$ kHz, which is much higher than the signal bandwidth. There are techniques like TCXO that can improve the precision but they are expensive. It is thus more difficult/expansive to have predefined frequency channels.

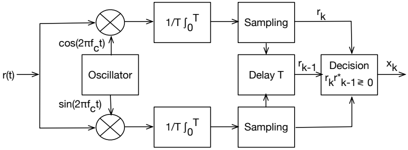
Sigfox : DBPSK on the Uplink I

- Motivation :
  - For long range communications, a robust modulation is required (while high data rate is not a primary concern). Low order modulation are thus good candidates.
  - The demodulation of classical PSK signals is done coherently, i.e., with the knowledge of a phase reference. For short burst communications, obtaining this phase reference is difficult in practice.
- DBPSK is a modulation that is simpler to implement than classical BPSK since it does not require the estimation of the carrier phase : it is sometimes presented as a *non-coherent* scheme. It results however in higher BER.
- In DBPSK, the transmitted bit is encoded in the phase difference between two successive symbols. The transmitted signal at k-th signaling interval is

$$s_k(t) = \Re\{g(t)e^{j\theta_k}e^{j2\pi f_c t}\},$$

where $g(t)$ is the signal pulse shape,
$\theta_k = \theta_{k-1}$ if the k-th transmitted bit is $x_k = 0$ and
$\theta_k = \theta_{k-1} + \pi$ if $x_k = 1$.

Sigfox : DBPSK on the Uplink II

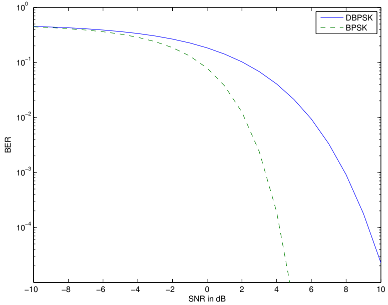


- Optimum DBPSK detector requires the exact knowledge of the carrier frequency f_c. After demodulation (multiplication by $e^{j2\pi f_c t}$, integration and sampling), the received sample is $r_k = \sqrt{E_b}e^{j\theta_k+\phi} + n_k$, where ϕ is a random phase and n_k is noise. Now :

$$r_k r_{k-1}^* = E_b e^{j(\theta_k - \theta_{k-1})} + \tilde{n}_k$$

  which does not depend on ϕ (if ϕ is constant across multiple symbol intervals). Note : in coherent communications, ϕ is known to the receiver. An error occurs if $r_k r_{k-1}^* < 0$ while $x_k = 0$.
- Optimum DBPSK achieves a BER of $P_e = \frac{1}{2}e^{-\gamma_b}$ (AWGN channel), a bit less than 3 dB loss compared to $P_e = Q(\sqrt{2\gamma_b})$ for BPSK.

Sigfox : DBPSK on the Uplink III



- A SNR of 8 dB is required to achieve a BER of 10^{-3}.

Sigfox : R-FDMA I

- Motivation :
  - Maintaining synchronization and orthogonal transmissions costs a lot of overhead in traditional wireless networks.
  - Contention-free MAC protocols are inefficient in case of low throughput, bursty, sporadic traffic and would lead to waste of resources.
  - Having fixed frequency channels is hardly feasible at very low cost (≈ 1 € for Sigfox radio chipset) because of the lack of precision of oscillators wrt to the very narrow band of the transmitted signal bandwidth.
- R-FDMA : every node randomly chooses a carrier frequency continuously in the system bandwidth. Several transmissions may overlap in the frequency as well as in the time domain. R-FDMA is basically a un-slotted Aloha in time-frequency domain.
- To combat collisions, R-FDMA allows for r repetitions of the same packet.

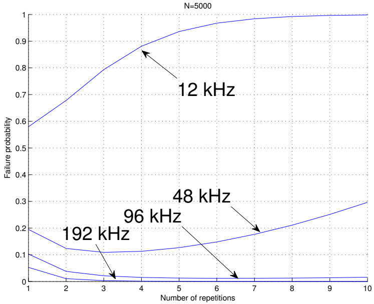
Sigfox : R-FDMA II

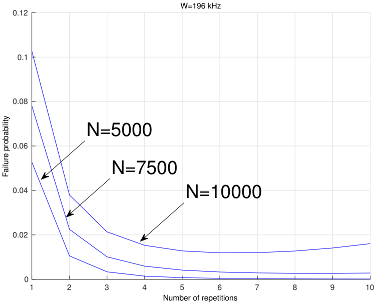
- Payload is between 0 and 12 Bytes, overhead is about 14 Bytes (preamble, id, hash code, CRC), data rate is 100 bps, $\delta_f = 300$ Hz, $\lambda = 6/3600$ messages/s.

Preamble	Synchro	Device ID	Payload	Auth.	FCS
4 bytes	2 bytes	4 bytes	0...12 bytes	var	2 bytes

- At very low system bandwidth, repetitions do not help. At high system bandwidth, repetitions are good up to a high value (but delay increases). At intermediate bandwidth, there is an optimal number of repetitions.
- Sigfox uses 3 repetitions and $W = 196$ kHz, with a target failure probability of 1%, the system can support approximately 7500 users per cell, or 1 million messages per day.

Sigfox : R-FDMA III





Sigfox : R-FDMA IV

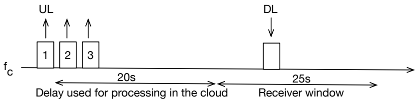
- UL frame structure :

Preamble	Synchro	Device ID	Payload	Auth.	FCS
4 bytes	2 bytes	4 bytes	0...12 bytes	var	2 bytes

- Device ID : Every device has a unique 32 bit ID allocated by a central registration authority to device manufacturers.
- Every device has a 128 bit long secret key used to authenticate every message.

Sigfox : Downlink Operation I

- Downlink operation : DL transmission is requested by the device, there is a 20 s delay before the response. The DL message is transmitted within a window of 25 s.



  Processing delay is used to transmit the UL message to the cloud and to process the demand.
  Receiver window allows for scheduling of DL messages.
  DL frequency is uniquely determined by the related UL frequency.

- DL header size is 8 Bytes :

Preamble	Synchro	flags	FCS	Auth.	Error codes	Payload
32 bits	13 bits	2 bits	8 bits	16 bits	var	var.

Sigfox : Downlink Operation II

- There is also a possibility of a slow drift of the carrier frequency so that $f(t) = f_c + \alpha(t)$ due to oscillator imperfections. For a 100 Hz signal, the drift can be of the order 2 Hz/s [Lacharte17]. The device should be able to cope with this issue.
- Assuming 12 bytes of overhead and a data rate of 600 bps, 10% of max duty cycle translates in 225 messages per hour. Sigfox announces a guarantee of 4 messages per day per device, so that 1350 devices can be served per cell.

Sigfox : Uplink Coverage I

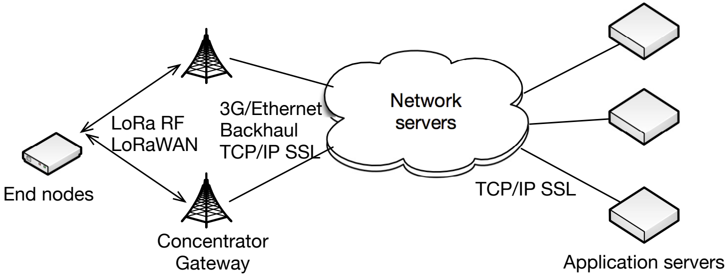
- Noise level : $N_{dBm} = 10\log_{10}(N_0 W) + NF = -150$ dBm for $N_0 = -174$ dBm/Hz, $W = 100$ Hz and $NF = 4$ dB.
- Target SNR is around 8 dB (for a BER of 10^{-3})
- Rx sensitivity : $S = N_{dBm} + SNR = -142$ dBm
- EIRP is bounded by the regulation : $P_{tx} = 14 + 2.15 = 16.15$ dBm
- Gains : typical antenna gain at the BS is $G_r = 6$ dBi (provides a benefit on the uplink but does not allow to increase the ERP on the downlink). Antenna diversity gain : $G_d = 3$ dB. $G = G_r + G_d$.
- Losses : cable losses $L_c = 3$ dB. Penetration loss for indoor propagation : $L_p = 18$ dB. $L = L_c + L_p$.
- Margin : shadowing standard deviation $\sigma = 7$ dB. Shadowing margin is $M_s = 9$ dB for $P_{out} = 0.9$. Jake's formula : $P_{out} = Q(K_s/\sigma)$, where K_s is the shadowing margin and σ is in dB.

Sigfox : Uplink Coverage II

- In absence of shadowing and penetration loss :
  $MAPL1 = P_{tx} + G - L - S = 164$ dB
  (order of magnitude presented in the literature).
- With shadowing and penetration loss : $MAPL2 = P_{tx} + G - L - M_s - S = 137$ dB.
- Hata model valid for 150-1500 MHz can be applied with $f = 868$ MHz, $h_B = 30$ m, $h_m = 1$ m, Urban Environment large cities, we obtain $R_1 = 11$ km for MAPL1 and $R_2 = 1.88$ km for MAPL2.
- Hata model for rural areas provides : $R_1 = 70$ km and $R_2 = 12$ km.

LoRa : Architecture

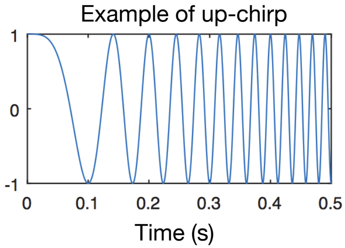
- Gateways receive and forward to/from network servers. There is no association of end nodes to gateways. It is up to the network servers to select the right gateway for downlink.
- Network servers include all the intelligence : manage radio parameters, remove duplicate messages, send ACKs.



LoRa : Physical layer I

- LoRa physical layer is proprietary and is partly described in patents originally owned by Cycleo in 2008 and acquired in 2012 by Semtech.
- LoRa uses Chirp Spread Spectrum (CSS) a technique developed in the 50's and used by sonars and radars.
- It is a spread spectrum modulation, i.e., $BT >> 1$, where B is the signal bandwidth and T is the symbol duration (vs narrowband signals for which $BT \approx 1$).
- Information bits are encoded in symbols also called **chirps** of duration T_s.
- A chirp is a constant amplitude sinusoid whose frequency varies linearly with time. If the frequency is increasing, we have an **up-chirp**, otherwise a **down-chirp**.

LoRa : Physical layer II



LoRa : Physical layer III

- There are N different possible chirps. We define the spreading factor as : $SF = \log_2(N)$, this is the number of bits carried by a chirp.
- Chirp duration T_s is sub-divided in N segments (or **chips**) of equal duration $\frac{1}{B}$, so that :

$$N = 2^{SF} = BT_s$$

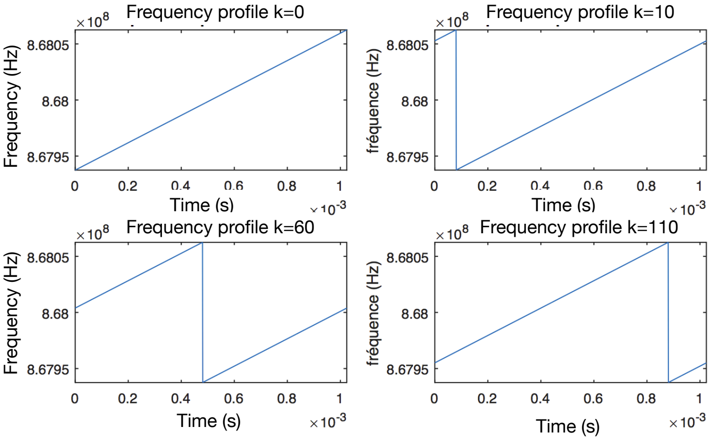
- Chirps are distinguished by their frequency profile : from a **raw-chirp**, other chirps are obtained by cyclic translation of k chips of the frequency.
- The raw chirp ($k = 0$) has a frequency varying from $f_0 = f_c - \frac{B}{2}$ to $f_1 = f_c + \frac{B}{2}$:

$$f_{tx}^{(0)}(t) = \frac{B}{T_s}(t - t_0) + f_0 = f_c + \frac{B}{T_s}(t - t_0) - \frac{B}{2}$$

  where t_0 is the chirp start time and f_c is the carrier frequency.
- The k-th chirp is now :

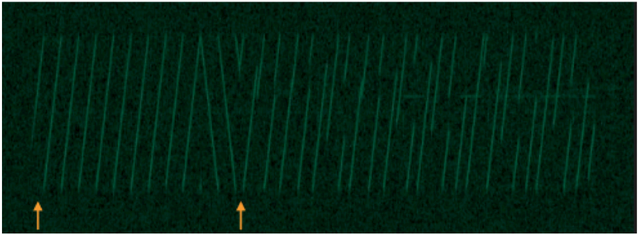
$$f_{tx}^{(k)}(t) = \begin{cases} f_c + \frac{B}{T_s}(t - (t_0 + \frac{k}{B})) + \frac{B}{2} & \text{si } t_0 \leq t \leq t_0 + \dfrac{k}{B} \\ f_c + \frac{B}{T_s}(t - (t_0 + \frac{k}{B})) - \frac{B}{2} & \text{si } t_0 + \frac{k}{B} \leq t \leq t_0 + T_s \end{cases}$$

LoRa : Physical layer IV



LoRa : Physical layer V

- Example of LoRa frame (from M. Knight. "Decoding the LoRa PHY", 2016).
- The preamble is made of a sequence of raw-chirps followed by 2 down-chirps, it is used for synchronization.



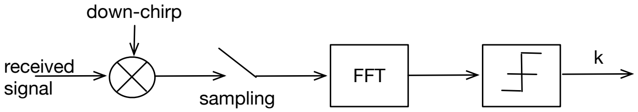
Preamble Payload

LoRa : Physical layer VI

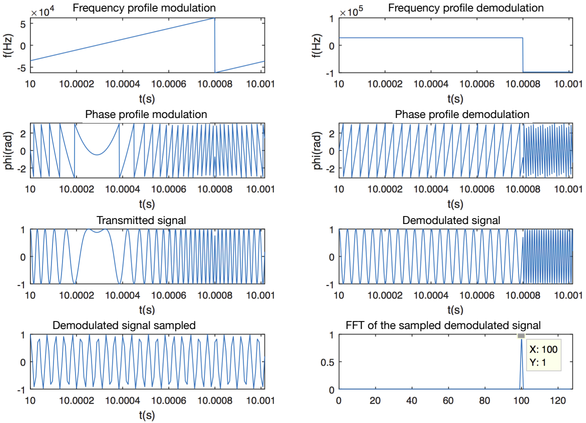
- Decoding follows the following steps : 1) received chirps are multiplied by a raw dow-chirp ; 2) the signal is sampled at B Hz ; 3) a FFT is performed ; 4) k is deduced.
- Down-chirp equation : $f_{dc}(t) = f_d - \frac{B}{T_s}(t - t_0) + \frac{B}{2}$
- Received signal after multiplication by the down-chirp :

$$f_{rx}^{(k)}(t) = \begin{cases} f_c + f_d - \frac{k}{T_s} + B & \text{si } t_0 \leq t \leq t_0 + \frac{k}{B} \\ f_c + f_d - \frac{k}{T_s} & \text{si } t_0 + \frac{k}{B} \leq t \leq t_0 + T_s \end{cases}$$

- After multiplication by the down-chirp, we obtain two frequencies that differ from B Hz, so that the sampled signal becomes : $f_{rx\_B}^{(k)}(t) = f_c + f_d - \frac{k}{T_s}$

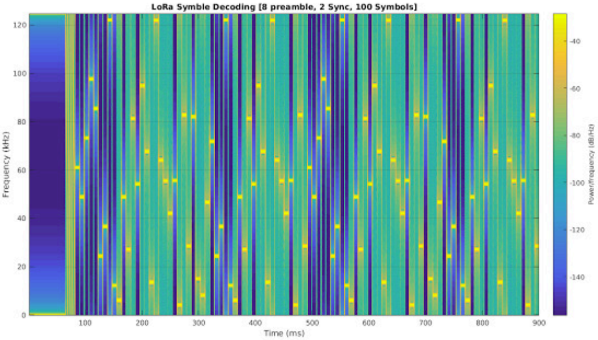


LoRa : Physical layer VII



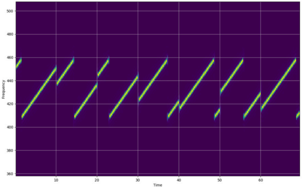
LoRa : Physical layer VIII

- Example of spectrogram (from S. Ghoslya, "All about LoRa").

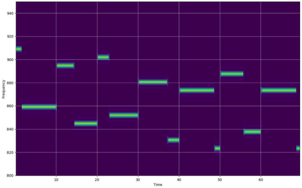


LoRa : Physical layer IX

- Another example of spectrogram before and after multiplication by the downchirp.



Spectrogram of the message



Spectrogram after multiplication by the raw chirp

LoRa : Physical layer X

- LoRa PHY characteristics : $B \in \{125, 250, 500\}$ kHz, $SF \in \{7, 8, ...12\}$.
- Recall that : $N = 2^{SF} = BT_s$
- Symbol rate is $R_s = \frac{1}{T_s} = \frac{B}{2^{SF}}$. Bit rate is : $R_b = SF\frac{B}{2^{SF}}$.
- For a given B : the higher SF, the lower the bit rate. For a given SF : the higher the bandwidth, the higher the bit rate.
- There is a trade-off between coverage and data rate. NB : coding rate is not taken into account here (between 1/2 and 4/5).
- Maximum payload size is 222 Bytes.

Table – R_b in kbps

B(kHz)\SF	7	8	9	10	11	12
125	6,8	3,9	2,2	1,2	0,7	0,4
250	13,7	7,8	4,4	2,4	1,3	0,7
500	27,3	15,6	8,8	4,9	2,7	1,5

LoRa : Physical layer XI

Orthogonality :

- According to the US patent on LoRa physical layer (Semtech), transmissions with different SF on the same frequency channel are orthogonal, except the combinations in this table :

TABLE 1

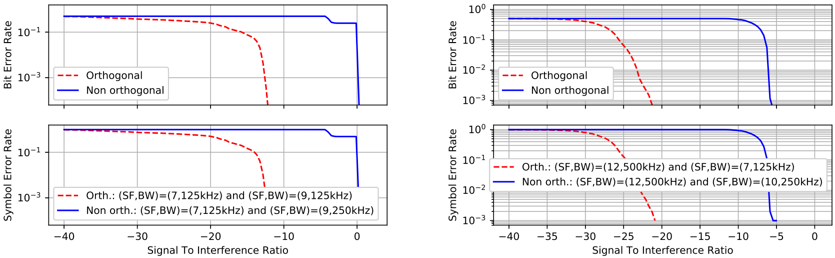
non-orthogonal ('X') combinations of LoRa channels characterized by spreading factor (SF) and bandwidth (BW) in kHz

SF		07	08	09	10	11	12	07	08	09	10	11	12	07	08	09	10	11	12
	BW	125	125	125	125	125	125	250	250	250	250	250	250	500	500	500	500	500	500
07	125	x								x								x	
08	125		x								x								x
09	125			x								x							
10	125				x								x						
11	125					x													
12	125						x												
07	250							x								x			
08	250								x								x		
09	250	x								x								x	
10	250		x								x								x
11	250			x								x							
12	250				x								x						
07	500													x					
08	500														x				
09	500							x								x			
10	500								x								x		
11	500	x								x								x	
12	500		x								x								x

- In fact, there is no evidence for that, and recent experiments have shown that orthogonality does not hold on the same channel [Makhaylov'17].

LoRa : Physical layer XII

Some home-made simulations (useful and interference signals are synchronized) :



- Orthogonal interferers are rejected at typical SIR values.
- Higher SF are more robust.

NB : LoRa PHY simulations have been performed by T. Feltin (X3A) and B. Nguyen (Telecom Paris - RIO)

LoRa : Uplink Coverage I

Coverage vs. data rate tradeoff in LoRa (from [Georgious'16]) :

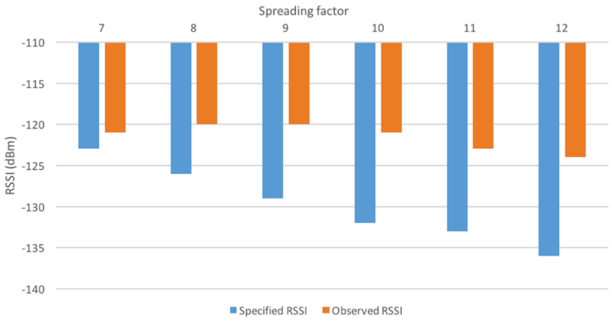
LoRa Characteristics of a 25 byte Message at BW = 125 kHz

SF	bit-rate kb/s	Packet air-time ms	Transmits per hour	Receiver Sensitivity	SNR q_{SF} dBm	Range km
7	5.47	36.6	98	-123 dBm	-6	0-2
8	3.13	64	56	-126	-9	2-4
9	1.76	113	31	-129	-12	4-6
10	0.98	204	17	-132	- 15	6-8
11	0.54	372	9	-134.5	-17.5	8-10
12	0.29	682	5	-137	-20	10+

LoRa : Uplink Coverage II

[Augustin'16]

- LoRa tests in Palaiseau (suburban environment).
- Receiver sensitivity measured vs Semtec specifications (and previous calculation) :



LoRa : Uplink Coverage III

With $SF = 12$ only location C (at 2300 m) provides an acceptable packet delivery ratio.

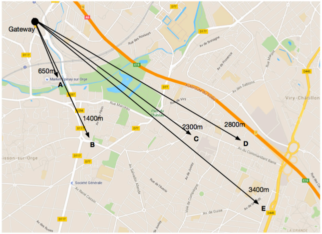
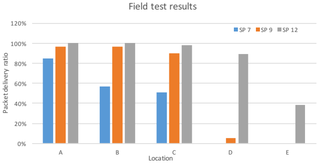


Figure 6. Map of LoRa field test.



LoRaWAN : the MAC layer I

There are three classes of end devices :

- Class A "All" : battery powered devices, no downlink latency constraint
- Class B "Beacon" : battery powered devices, controlled downlink latency
- Class C "Continuous" : devices that can afford to continuously listen to the downlink channel, no latency on the downlink.

LoRaWAN : the MAC layer II

Class A MAC layer :

- Devices change channel in a pseudo-random fashion for every transmission.
- In the 868 MHz band in Europe, devices must support 3 channels.
- They have to respect the maximum duty-cycle. If a transmission lasts T s on a channel with duty cycle d, the device should be off on that channel during T_{off} s, s.t.

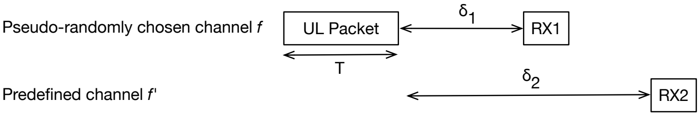
$$\frac{T}{T + T_{off}} \leq d$$

The device adapts its channel hopping sequence to the channel availability.

LoRaWAN : the MAC layer III

Uplink transmissions :

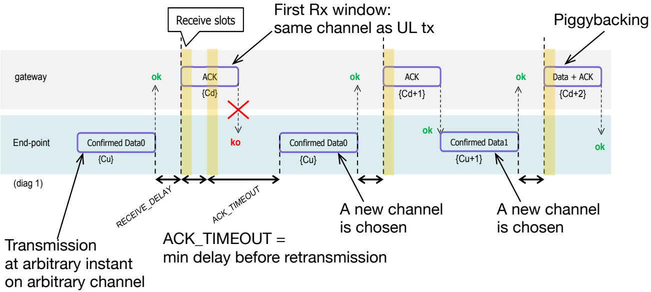
- After an uplink transmission, the device opens 2 short receive windows after delays δ_1 and δ_2 (typically 1 and 2 s).
- The first window uses the same channel. If a message is decoded and is intended for the transmitting device, the second window is ignored.
- The second window uses a predefined fixed downlink channel with higher duty cycle (10%) and frame is transmitted at the lowest available data rate.
- A device cannot send a new message before receiving a downlink message or the end of the second window.
- Receive windows are long enough to be able to detect a preamble.



LoRaWAN : the MAC layer IV

ARQ :

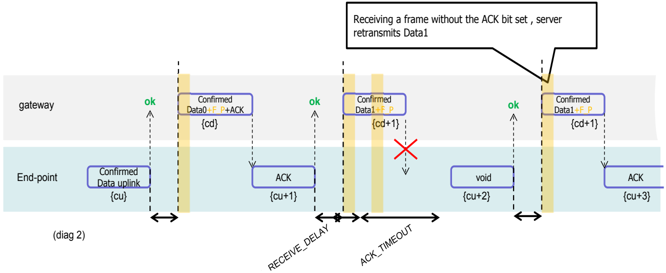
- *Unconfirmed data* does not require ACK.
- ACK for *confirmed data* is triggered by the message type on the UL. ACK is sent during one of the receive windows. NACK is implicit. ACK_TIMETOUT is a random backoff. After a maximum number of retransmissions is reached, the data rate may be lowered for another round of retransmissions.



LoRaWAN : the MAC layer V

DL pending data :

- A Frame Pending bit informs the device that the network has several frames pending for it.



LoRaWAN : the MAC layer VI

Adaptive data rate :

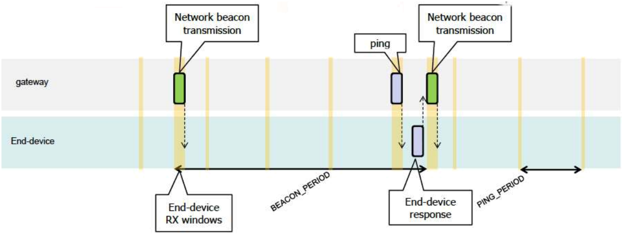
- Data rate and output power are adaptive. The network controls the data rate based on UL SNR measurements by sending DL control messages.
- The device also validates periodically that UL frames are correctly received. After N UL messages without any response, the device requests an ACK from the network. In case there is no response, the data rate is lowered step by step. A very similar mechanism is implemented in WiFi.
- DL data rates in receive windows depends on the corresponding UL data rate.

LoRaWAN : the MAC layer VII

Class B MAC layer :

- Class B devices are available for reception at predictable time instants.
- The gateway periodically (every 128 s) transmits on a fixed frequency channel a beacon, which is a timing reference.
- Devices open reception windows (ping slots) at periodic time instants after the beacon transmission.
- The network may initiate DL transmission during ping slots.

LoRaWAN : the MAC layer VIII

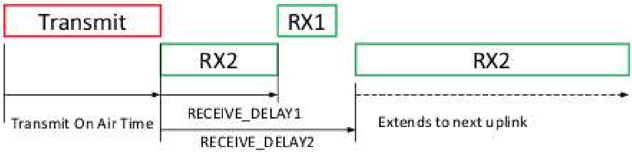


- The device chooses a data rate and a ping slot periodicity (bw 1 and 128 s) based on the beacon received power and its battery life.
- The duration between the beacon and the first ping slot is pseudo-random (and known by both the device and the gateway).
- All gateways of a given network are time synchronized.
- When a device moves and detects a new gateway, it should inform the network.

LoRaWAN : the MAC layer IX

Class C MAC layer :

- Devices always listen to the second receive window (recall : on a predefined frequency channel), except when they transmit or receive on the first receive window.



LoRaWAN : MAC performance I

We consider only Class A devices. We adopt the pure Aloha model with infinite population (the number of devices is large).
Assumptions :

- There N devices, each one generates a load λ_u.
- There are F frequency channels.
- We ignore orthogonality between the SF.
- The proportion of devices with DR i is p_i.
- The packet duration for DR i is T_i.
- We assume an unacknowledged mode.

LoRaWAN : MAC performance II

Analysis :

- The load generated on a channel by DR i is $\lambda_i = \frac{p_i N \lambda_u}{F}$.
- A packet from DR j is successfully transmitted at t if for all i, there is no packet transmission in the interval $[t - T_i; t + T_j]$. The success probability is thus :

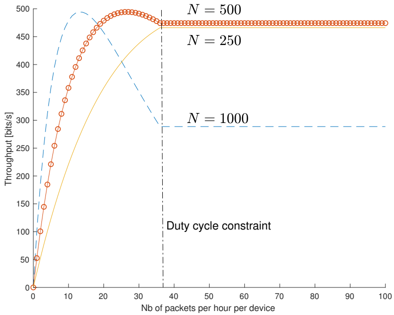
$$P^j_{succ} = \prod_i exp\left(-\lambda_i(T_i + T_j)\right) = exp\left(-\sum_i \lambda_i(T_i + T_j)\right)$$

- The overall normalized throughput is now :

$$S = F \sum_j \lambda_j T_j exp\left(-\sum_i \lambda_i(T_i + T_j)\right)$$

LoRaWAN : MAC performance III

Assumptions : $L = 50$ Bytes, $p = [0.28\ 0.2\ 0.14\ 0.1\ 0.08\ 0.19]$, $DR = [0.4\ 0.7\ 1.2\ 2.2\ 3.9\ 6.8]$ kbps, duty cycle is 1%, $F = 3$.
NB : The load is constrained by the packets with longer time duration, i.e., with smallest data rate. Here : $L/DR_{min} = 1$ s ; so that devices cannot send more than 36 packets per hour with a duty cycle of 1%.



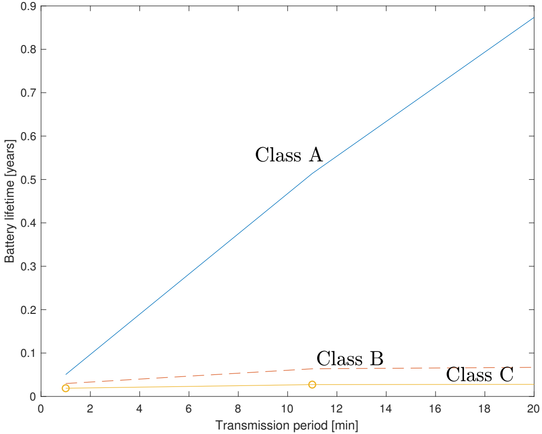
LoRaWAN : Battery considerations

- Batteries are characterized by their capacity (in Ah, typically from 100 to 2500 mAh), shape (AA, AAA, cell coin, etc), voltage (from 1.2V to 9V typically for radio modules), chemistry (lithium, Alkaline, Nickel Metal Hybrid, lead-acid), rechargeable or not, internal discharge rate, etc.
- Class A : Average current between two transmissions is computed as follows :

$$I = \frac{1}{T} \sum_i I_i T_i$$

  where T is the period, I_i is the current drawn during T_i in state i. State i may be either Transmit, Receive or Sleep (or other intermediate states as shown in [Casals'17]).
- Battery lifetime (ignoring self-discharge) is : $L = \frac{C}{I}$, where C is the battery capacity.

LoRaWAN : Battery considerations



Section 2

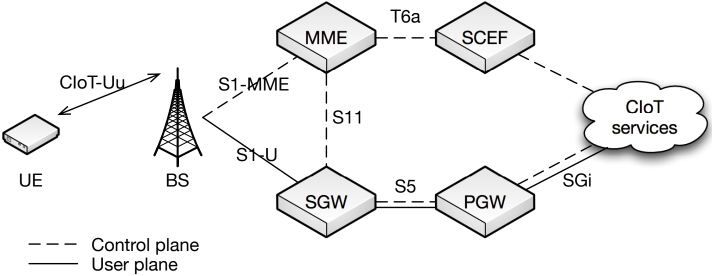
NB-IoT

Introduction

- NB-IoT is like a simplified FDD LTE system designed for non-delay sensitive machine-type communications.
- Resource organization, channels, MAC layer are similar to LTE but many features have been removed (like handover, D2D, carrier aggregation, measurements, etc).
- No QoS guarantee : NB-IoT cannot be used for delay-sensitive data.
- NB-IoT is deployed in licensed frequencies and occupies a bandwidth of 180 kHz.
- 60 kbps in UL, 30 kbps in DL, no duty cycle constraint.
- NB-IoT will be the technology adopted by 5G standards for IoT communications.

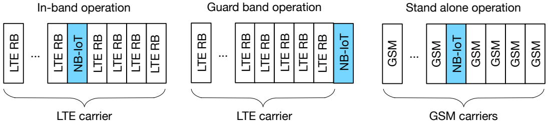
Architecture

- The Service Capability Exposure Function (SCEF) is for the delivery of non-IP data packets over the control plane. The user data is carried by control messages. This path is used by sensors with proprietary stacks that do not implement the TCP/IP suite.



Operation Modes

- Stand alone operation : A GSM channel (200 kHz) is refarmed.
- Guard band operation : NB-IoT is deployed in unused sub-carriers located in the guard band of a LTE system.
- In-band operation : Some Resource Blocks of a LTE system are dedicated to NB-IoT. Only a restricted list of RBs can be allocated to NB-IoT (in particular RBs including LTE synchronization signals are excluded). Coexistence with LTE should be managed (e.g. with reference signals and control channels).

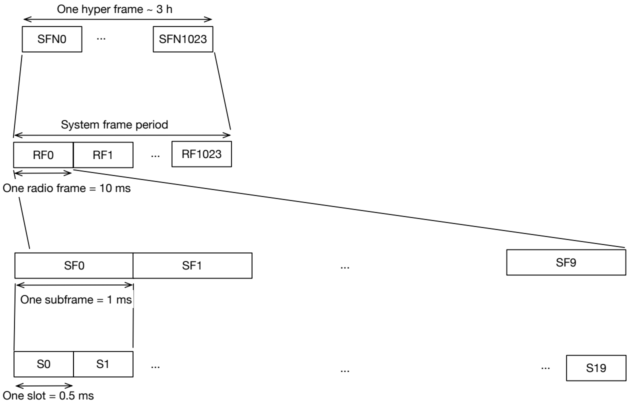


- Coexistence : SA>guard band>inband. Simplicty : inband>guard band>SA.
- Frequency bands are in the lower range of existing LTE bands (from 700 to 1900 MHz). Duplexing mode is FDD half duplex : UEs either transmit or receive and there is at least 1 ms gap between Tx and Rx.

Downlink I

Frame structure, Resource Block and Resource Element :

- Same definition as for LTE : 1 RB = 12 sc (15 kHz) $\times$ 7 OFDM symbol
- A new structure : the hyper frame (approx. 3 hours)



Downlink II

Downlink channels :

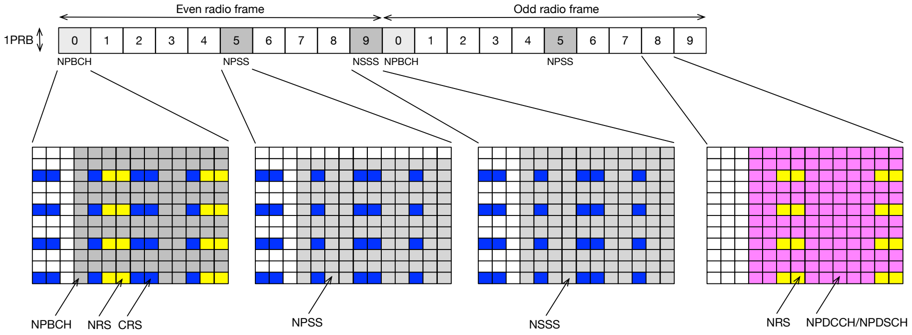
- NPSS and NSSS (Narrowband Primary and Secondary Synchronization Signals) :
    - They are used for frequency and time synchronization.
    - They provide the NCellID (504 possible values as in LTE).
    - The first 3 OFDM symbols are left free for the PDCCH of LTE.
    - Multiple OFDM symbols are used to compensate the lack of frequency resources (vs. LTE).
- NRS (Narrowband Reference Signals) :
    - They are used for channel estimation.
    - Their location depends on the NCellID.
    - LTE RS are also present in the in-band operation, but there is no overlap bw NRS and RS.

Downlink III

- NPBCH (Narrowband Physical Broadcast Channel) :
  - Carries the MIB (System Frame Number, Hyper Frame Number, value tag, access baring tag, operation mode, SIB1 scheduling).
  - A UE is not required to always decode all system informations. Changes in system informations are indicated by a value tag in the MIB and/or with a paging message.
  - TTI of 640 ms (iso 40 ms in LTE) with 8 repetitions for better coverage.
  - NPBCH, NPSS and NSSS are transmitted on a RB called the *anchor carrier*.

Downlink IV

Physical channels locations (assuming 4 antennas for LTE and 2 antennas for NB-IoT) :

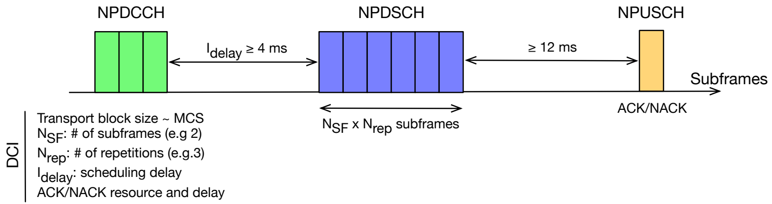


Downlink V

- NPDSCH (Narrowband Physical Shared Channel) :
  - Carries user data, SIBs, paging and dedicated signalling.
  - Modulation is QPSK (iso QPSK, 16-QAM, 64-QAM in LTE).
  - One or two antennas (transmit diversity) can be used (iso 9 TM in LTE including spatial multiplexing and MU-MIMO).
  - A single HARQ process (iso up to 8 in LTE), but ACK/NACK is not required.
  - Maximum transport block size is 680 bits (iso 70 000 bits in LTE without spatial multiplexing).
  - Repetitions allows to improve the coverage (up to 2048).

Downlink VI

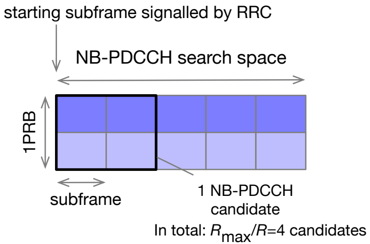
- NPDCCH (Narrowband Physical Downlink Control Channel) :
  - Carries control information (DCI) : UL and DL allocations, Paging scheduling
  - There is no specific subframes for the transmission of PDCCH, there are only predefined regions in which PDCCH can be transmitted, these regions are called *search spaces*.
  - UEs shall perform blind decoding by monitoring the search spaces and try to decode the PDCCH.
  - 4ms delay between allocation and data transmission on the DL (iso same subframe in LTE)



Downlink VII

Search space :

- Contrary to LTE, there is no static location for the NB-PDCCH in the radio frame.
- UEs have to monitor all possible predefined regions, called search spaces, where PDCCH can be located.
- Within a search space, blind decoding is performed by considering all possible aggregation and repetition levels.



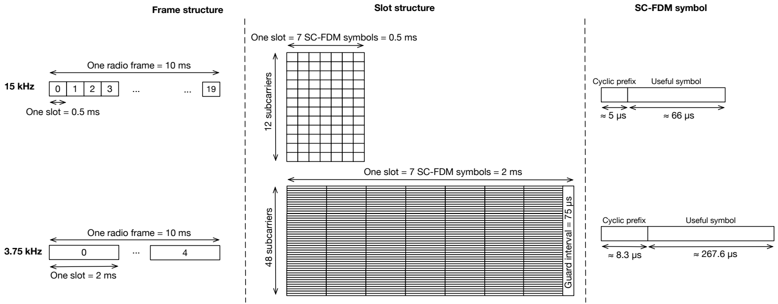
Aggregation Level is L=1 or 2 (# of half-PRB)
Repetition Level is R_{max} in {1,2,4,…,2048}
Repetition Number is R in {R_{max},R_{max}/2,R_{max}/4,R_{max}/8}
Example: R_{max}=8, R=2, L=2

With $R_{max} = 8$ (depends on the coverage class), only $L = 2$ is possible and $R \in \{8, 4, 2, 1\}$. For $R = 2$ there are 4 candidates. The periodicity of this search space is a multiple of R_{max}.

Uplink I

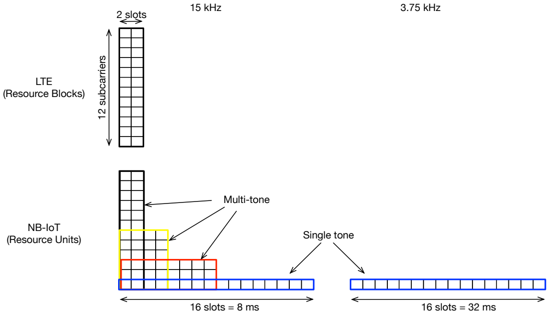
Resource organization :

- As in UL LTE, SC-FDMA is used but with 2 possible subcarrier spacings (15 kHz or 3.75 kHz).



Uplink II

- The smallest resource unit (for allocation) in LTE is 2 RBs (12 sc $\times$ 2 slots) ; In NB-IoT : 1 Resource Unit (RU) which is smaller and can span up to 16 slots.
- Short subcarrier spacing (3.75 kHz) and flexible number of allocated subcarriers are two features to improve the coverage of the system and allow the multiplexing of more users simultaneously.



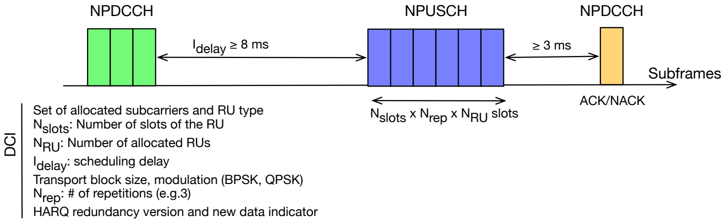
Uplink III

Uplink channels :

- DMRS (Demodulation Reference Signal) :
  - They are used for channel estimation.
  - There location depends on the RU type, the subcarrier spacing and information type (control or data). As in LTE, they are time-multiplexed with data sent on the PUSCH.

Uplink IV

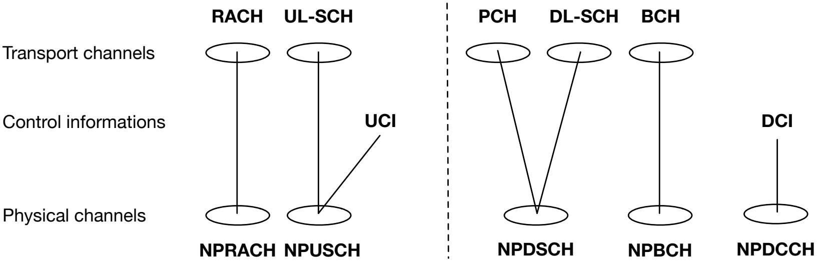
- NPUSH (Narrowband Physical Uplink Shared Channel) :
  - Carries user data and control information (no equivalent of PUCCH in LTE).
  - BPSK for control information, BPSK or QPSK for user data.
  - Single antenna transmissions (no MIMO).
  - Single HARQ process and ACK/NACK is required.
  - Maximum transport block size is 1000 bits.
  - Repetitions allows to improve the coverage (up to 128).
  - Single tone transmission : 1 subcarrier, Multi-tone : 3, 6 or 12 subcarriers.



Uplink V

- NPRACH (Narrowband Physical Random Access Channel) :
  - The procedure is always contention based (vs. contention based or free in LTE). It is similar to the LTE procedure.
  - Random access resources are periodic and are made of contiguous sets of subcarriers with subcarrier spacing of 3.75 kHz.
  - There 1 to 128 repetitions of the preambles and frequency hopping is applied.

Channel summary



Energy Management I

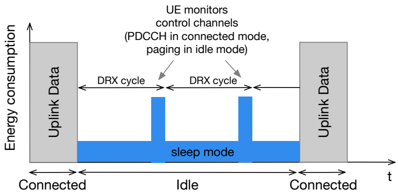
Radio Resource Control Modes :

- The UE can be either in RRC_Idle or RRC_Connected.
- In RRC_Idle, the UE only listens to paging messages. It must regularly switch to RRC_Connected to update its location. When data arrives, it must reconnect and switch to RRC_Connected. Re-connection implies control messages exchanges that take some time and consumes some energy.
- In RRC_Connected, the UE decodes all control channels with potentially commands for it. Energy consumption is much higher.

Energy Management II

Discontinuous Reception (DRX) :

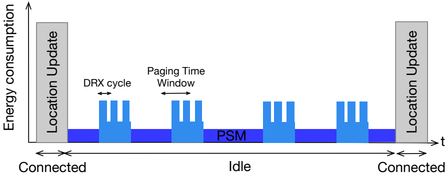
- The UE and the network negotiate when the device can sleep. The network may also broadcast cell specific parameters.
- During sleep periods, the UE is not reachable by the network. This implies some additional delay for DL transmissions. Sleep periods can be interrupted for UL data transfer.
- DRX is triggered by an inactivity timer. After another inactivity timer, the UE switches from short to long DRX cycles.
- DRX cycle is 3h at most (vs. 2.56 s in LTE).



Energy Management III

Power Saving Mode (PSM) :

- In PSM, the UE do not monitor pagings anymore and wakes up only for location updates. PSM duration is up to 413 days (R13). In PSM, the UE shuts its radio modem down, it is not reachable by the network : it is a *deep sleep* mode.
- The UE remains registered to the network, there is no need for reattachment when it becomes active again.
- Devices regularly receiving data from the network should favour DRX approach, while devices that send data with few network command can use PSM.



Conclusion

- Philosophy of NB-IoT design : remove from LTE all what is not strictly required, in particular all features related to high throughput and capacity (spatial multiplexing, multiple HARQ process, high order modulations, etc) ; adapt protocols to low complexity UEs (delays) ; improve coverage (repetitions) ; improve battery life.
- Important tradeoffs : coverage vs. battery life, reachability vs. battery life, data rate vs. coverage.

Acronyms I

ACK	Acknowledgment
API	Application Programming Interface
AWGN	Average White Gaussian Noise
BCH	Broadcast Channel
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
BS	Base Station
BSS	Business Support System
CIoT	Cellular IoT
CRA	Central Registration Authority
CRC	Cyclic Redundancy Code
CSS	Chirp Spread Spectrum
D2D	Device to Device
DBPSK	Differential Binary Phase Shift Keying
DCI	Downlink Control Information
DL	Downlink
DL-SCH	Downlink Shared Channel
DMRS	Demodulation Reference Signal
DRX	Discontinuous Reception
DSL	Digital Subscriber Line
EC-GSM	Extended Coverage GSM
ERP	Effective Radiated Power
FDD	Frequency Division Duplex
FFT	Fast Fourier Transform
GPS	Global Positioning System
HARQ	Hybrid Automatic Repeat on Request
IoT	Internet of Things
ISM	Industrial Scientific Medical
LPWAN	Low Power Wide Area Network

Acronyms II

LTE	Long Term Evolution
LTN	Low Throughput Network
MAC	Medium Access Control
MIB	Master Information Block
MIMO	Multiple Input Multiple Output
MME	Mobility Management Entity
MU-MIMO	Multi-User MIMO
NACK	Negative Acknowledgment
NB-IoT	Narrow Band IoT
NPBCH	Narrowband Physical Broadcast Channel
NPDCCH	Narrowband Physical Downlink Control Channel
NPDSCH	Narrowband Physical Downlink Shared Channel
NPRACH	Narrowband Physical Random Access Channel
NPSS	Narrowband Primary Synchronization Signal
NPSS	Narrowband Secondary Synchronization Signal
NPUSCH	narrowband Physical Uplink Shared Channel
NRS	Narrowband Reference Signal
OFDM	Orthogonal Frequency Division Multiplex
OFDMA	Orthogonal Frequency Division Multiple Access
OSS	Operation Support System
PCH	Paging Channel
PDCCH	Physical Downlink Control Channel
PGW	packet Gateway
PSK	Phase Shift Keying
PSM	Power Saving Mode
QAM	Qadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RACH	Random Access Channel

Acronyms III

RB	Resource Block
RE	Resource Element
R-FDMA	Random Frequency Division Multiple Access
RFID	Radio Frequency Identification
RRC	Radio Resource Control
RS	Reference Signal
RU	Resource Unit
SA	Stand Alone
SCEF	Service Capability Exposure Function
SC-FDMA	Single Carrier Frequency Division Multiple Access
SGW	Serving Gateway
SIB	System Information Block
SNR	Signal to Noise Ratio
TCXO	Temperature Compensated Crystal Oscillator
TM	Transmission Mode
TTI	Transmission Time Interval
UCI	Uplink Control Information
UE	User Equipment
UNB	Ultra Narrow Band
UL	Uplink
UL-SCH	Uplink Shared Channel