



A REPORT ON « 5G NB-IoT »



Protocols for Wireless Sensor Network

SUBMITTED BY

*Yacine BENCHEHIDA 5ISS-B1
Hugo LE BELGUET 5ISS-B1
Sami BEYAH 5ISS-A2*

UNDER THE GUIDANCE OF

Prof. **Daniela DRAGOMIRESCU**

Academic Year: 2021-2022
October 16, 2021

Contents

Introduction.....	2
Physical Layer in NB-IoT	3
a) Generalities	3
b) Mode of Operations	3
i) Bandwidth.....	3
ii) Frequency Bands	4
c) Drive system.....	4
i) Downlink.....	4
ii) Uplink.....	5
d) Modulation	6
e) Datarate & Scope	6
f) Summary table of Physical layer	7
Channel Access and Mac Layer in NB-IoT	8
a) Physical Channels and Signals	8
i) Access protocols on Downlink.....	8
ii) Access protocols on Uplink.....	8
b) Collisions.....	9
Power consumption	10
a) The mechanism behind the power management of an NB-IoT device	10
b) Measurement of an NB-IoT power consumption.....	11
Security	13
Conclusion	15
References	16

Introduction

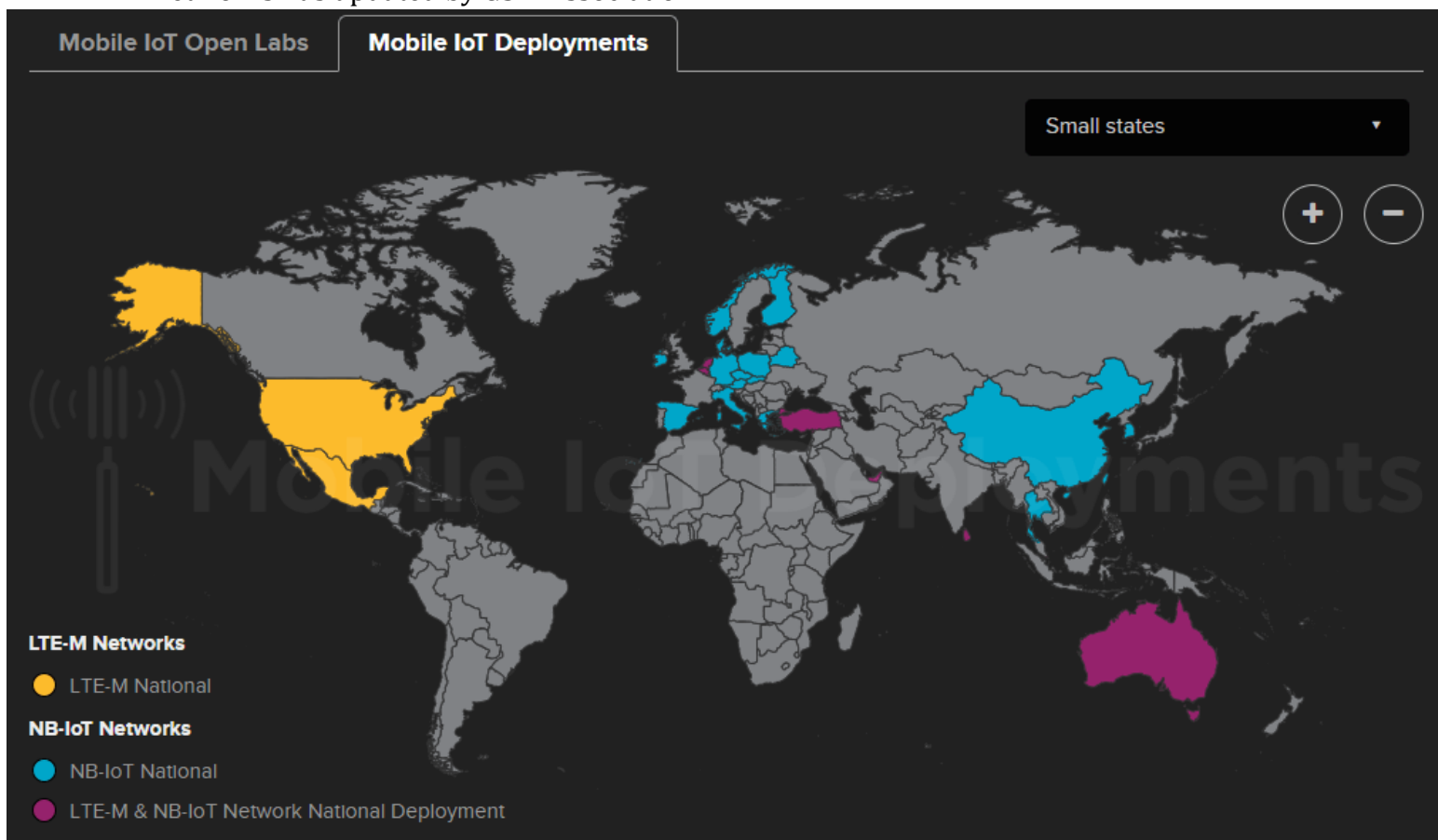
Narrowband Internet of Things (NB-IoT) is a new fast-growing wireless technology 3GPP cellular technology standard introduced in *Release 13* that addresses the LPWAN (Low Power Wide Area Network) requirements of the IoT. It's been classified as a 5G technology, standardised by 3GPP in 2016. It is a new 3GPP radio-access technology in the sense that it is not fully backward compatible with existing 3GPP devices.

It is fast emerging as the best-in-class leading LPWAN technology to enable a wide range of new IoT devices, including smart parking, utilities, wearables, and industrial solutions.

The main characterises of NB-IoT are:

- An excellent indoor coverage,
- A support of a massive number of connections,
- A cost efficiency,
- To support Massive Machine Type Communication (mMTC)
- To enable low-power, low-cost and low -data-rate communication ideal for IoT
- To optimise network architecture.

Below you can find a map that help you track the expansion of these low power wide area networks. It's updated by GSM Association.



Release 13 introduced a new UE category for NB-IoT: Cat. NB1

Physical Layer in NB-IoT

Physical Layer defines the physical operation of the NB-IoT device including receive sensitivity, channel rejection, output power, number of channels, chip modulation, and transmission rate specifications.

a) Generalities

NB-IoT adopts the same protocol stack as the legacy LTE. However, some design changes in both PHY and MAC layers were introduced to support the massive long-range connections with up to additional 20 dB MCL than in legacy technologies such as LTE, GSM, and GPRS. Those changes are described in what follow.

NB-IoT inherits from LTE most of its features as well as its essential channels and signals. However, the complexity of these channels and signals was reduced in order to respect the low-cost and low-power constraints of NB-IoT user equipment modules.

b) Mode of Operations

i) Bandwidth

The system was designed to occupy a frequency band of 180 kHz (corresponding to one resource block in the LTE system), and to handle a high number of repetitions to achieve long-range transmissions and deep indoor penetration.

NB-IoT has a channel bandwidth of 200 kHz but occupies only 180 kHz. This is equal to one resource block in LTE (1 RB). This bandwidth enables three modes of operation:

- **Standalone operation:** NB-IoT operates independently, for example on channels previously used for GSM. The GSM channel bandwidth of 200 kHz provides a 10 kHz guard buffer on both sides to neighbouring GSM channels.
- **Guard band operation:** NB-IoT utilizes resource blocks in the guard bands of an LTE channel
- **In-band operation:** NB-IoT re-uses frequencies which are not used by LTE inside the LTE channel bandwidth

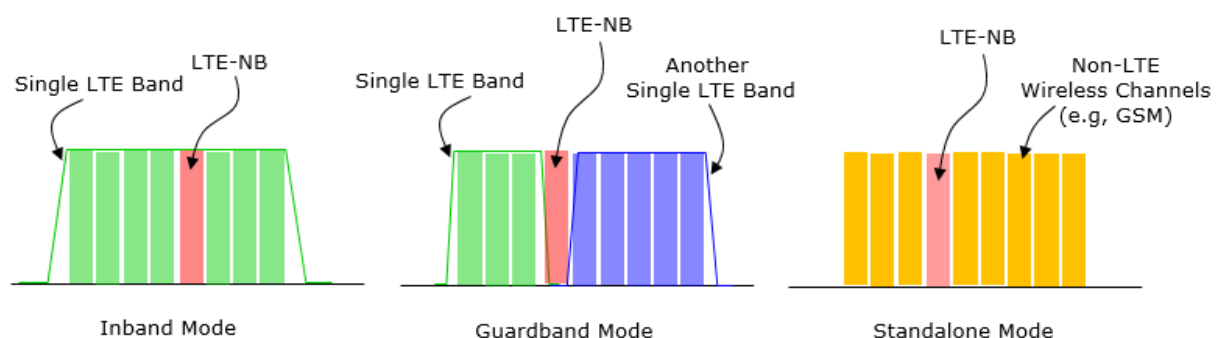


Figure 1: Examples of NB-IoT stand-alone deployment and LTE in-band and guard-band deployments in the downlink.

So, in In-band and guard-band modes, NB- IoT occupies PRB (Physical Resource Block) of 180 KHz in LTE spectrum in both downlink and uplink. Likewise, NB-IoT uses standalone mode which is a deployment using existing idle spectrum resources. These resources can be the operator's spectrum fragments with non-standard bandwidths or spared from other radio access technologies by refarming.

ii) Frequency Bands

Release 13 provides the following bands: NB-IoT uses the same numbers as LTE but only a subset is defined.

Band number	Uplink frequency range / MHz	Downlink frequency range / MHz
1	1920 – 1980	2110 - 2170
2	1850 - 1910	1930 – 1990
3	1710 – 1785	1805 – 1880
5	824 – 849	869 – 894
8	880 – 915	925 – 960
12	699 – 716	729 – 746
13	777 – 787	746 -756
17	704 – 716	734 – 746
18	815 – 830	860 – 875
19	830 – 845	875 – 890
20	832 – 862	791 – 821
26	814 – 849	859 – 894
28	703 – 748	758 – 803
66	1710 – 1780	2110 – 2200

Figure 2: NB-IoT frequency band

c) Drive system

To reach the massive device deployment objective, NB-IoT uses the allocation of Resource Units (RU) to multiple UE unlike LTE where the whole resource block is allocated to a single UE (User Equipment) in the uplink.

i) Downlink

The downlink (DL) of NB-IoT is based on OFDMA with the same 15 kHz subcarrier spacing as LTE. Slot, subframe, and frame durations are 0.5 ms, 1 ms, and 10 ms, respectively, identical to those in LTE.

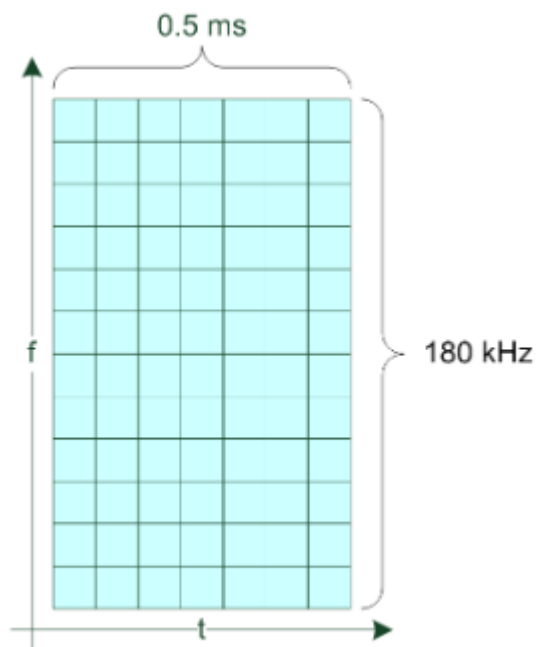


Figure 3: Downlink grid: 12 carriers with 15 kHz spacing yields a channel bandwidth of 180 kHz. One slot consists of seven OFDMA symbols

NB-IoT uses only 12 carriers, which leads to an occupied bandwidth of 180 kHz. One slot consists of seven OFDMA symbols.

Reusing the same OFDM numerology as LTE ensures the coexistence performance with LTE in the downlink. For example, when NB-IoT is deployed inside an LTE carrier, the orthogonality between the NB-IoT PRB and all the other LTE PRBs is preserved in the downlink.

ii) Uplink

In the uplink (UL), two different possibilities are defined. It can use either a single carrier or multiple carriers.

- **Single-tone:** 15 kHz or 3.75 kHz carrier spacing (single-tone is mandatory)
- **Multitone:** SC-FDMA with 15 kHz carrier spacing (optional)

Here, the carrier spacing in the multitone process is the same as in the downlink and in LTE.

With a carrier spacing of 15 kHz, 12 carriers are available: 3.75 kHz spacing yields 48 carriers.

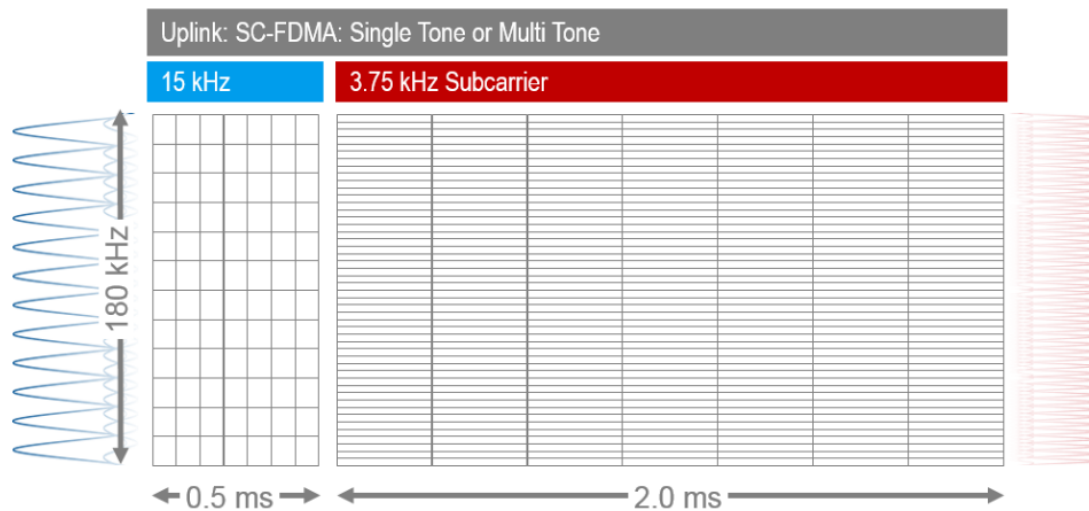


Figure 4: Resource element grid in the uplink

The numerology is identical to LTE and thus achieves the best coexistence performance with LTE in the uplink. The 15 kHz single-tone numerology uses 2 ms slot duration. Like the downlink, an uplink NB-IoT carrier uses a total system bandwidth of 180 kHz.

d) Modulation

The NB-IoT protocol uses the the **BPSK** and **QPSK** modulation schemes with only one antenna support both in uplink and downlink transmission.

- In Uplink, the modulation used is **QPSK**, $\frac{\pi}{4}$ **QPSK**, and $\frac{\pi}{2}$ **BPSK**. Indeed, for single-tone, the modulation is $\pi/2$ -BPSK or $\pi/4$ -QPSK; for multitone it is always QPSK.
- Moreover, the quadrature phase-shift keying (**QPSK**) is the only modulation format that can be used for NB-IoT downlink transmissions.

e) Datarate & Scope

NB-IoT supports ultra-low complexity devices with very narrow bandwidth, **200 kHz**. Due to its narrow bandwidth, the data rate peaks at around **20 until 250 Kbits/s**.

Furthermore, the scope is:

- 1 km in urban area
- 10 km in rural area

f) Summary table of Physical layer

Parameters	NB-IoT
Bandwidth	<ul style="list-style-type: none"> ○ Standalone Mode: 200kHz ○ In-band Mode: 180 kHz in LTE spectrum ○ Guard-band mode: 180 kHz in LTE spectrum
Modulation	<ul style="list-style-type: none"> ○ Uplink: $QPSK, \frac{\pi}{4} QPSK, \frac{\pi}{2} BPSK$ ○ Downlink: QPSK
Data rate	○ 20 until 250 Kbits/s
Max Payload	<ul style="list-style-type: none"> ○ Uplink: 1000 bits ○ Downlink: 680 bits
Access Medium	<ul style="list-style-type: none"> ○ Uplink: SC-FDMA ○ Downlink: OFDMA
Coverage	<ul style="list-style-type: none"> ○ 1km in urban area ○ 10 km in rural area
Roaming	○ No contrary to LTE-M
Latency	○ < 10 seconds
Handover	○ End-devices join a single base station
Channel Coding	○ Turbo Codes

Channel Access and Mac Layer in NB-IoT

The Medium Access Control layer is the interface between the physical and the network layer. Access Control is a mechanism that controls the access of stations to the transmission link.

a) Physical Channels and Signals

In NB-IoT, the access protocols are different between uplink and downlink.

i) Access protocols on Downlink

For downlink communications, OFDMA is used. It is a form of multicarrier modulation and consists of several closely spaced modulated carriers that do not interfere with each other. So, it's possible to use more slots in the same band size compared to simple FDMA.

Indeed, according to Release 13, the theoretical peak speed of the downlink is around 250 kb/s. NB-IoT provides the following physical signals and channels in the downlink:

- Narrowband Primary Synchronization Signal (**NPSS**), this signal is used by the UE to perform time and frequency synchronization.
- Narrowband Secondary Synchronization Signal (**NSSS**), it is the second essential signal transmitted by the eNB. It only carries the cell identity (cell ID) information to the base station.
- Narrowband Reference Signal (**NRS**), it is dedicated to channel estimation in the frequency domain. The NRS is used to estimate link quality.
- Narrowband Physical Broadcast Channel (**NPBCH**) that is the first essential channel for the NB-IoT UE modules as it is the first to be decoded. Moreover, this channel carries the narrowband master information block (MIB-NB) once every 640ms.
- Narrowband Physical Downlink Shared Channel (**NPDSCH**), it is dedicated to data transmissions. It is used to transmit system information blocks and the data for users.
- Narrowband Physical Downlink Control Channel (**NPDCCH**). As in LTE, a control channel is needed to prepare the phase of data transmission. In NB-IoT, the NPDCCH is dedicated to the transmission of control information from the network towards the UEs.

ii) Access protocols on Uplink

For Uplink communications, the access protocol is SC-FDMA. SC-FDMA is a digital radio coding technology used in particular in 4th generation LTE mobile phone networks; it uses

both frequency division multiple access and time division multiple access techniques (frequency and time division multiplexing).

Indeed, according to Release 13, the theoretical peak speed of the uplink is around 2267kb/s. NB-IoT includes the following channels in the uplink:

- Narrowband Physical Random-Access Channel (**NPRACH**), this signal is used to perform initial access to the network, to request transmission resources and to reconnect to the base station after a link failure.
- Narrowband Physical Uplink Shared Channel (**NPUSCH**), it is dedicated to data packet transmissions.
- Demodulation Reference Signal (**DMRS**), for the accuracy of the uplink channel estimation.

b) Collisions

To avoid collisions on the NPRACH channel, NB-IoT use the **Slotted ALOHA protocol**. ALOHA is a medium access control (MAC) protocol for transmission of data via a shared network channel. Using this protocol, several data streams originating from multiple nodes are transferred through a multi-point transmission channel.

The main characterizes about this protocol are:

- Slotted Aloha divides the time of shared channel into discrete intervals called as time slots.
- Any station can transmit its data in any time slot
- The only condition is that station must start its transmission from the beginning of the time slot
- If the beginning of the slot is missed, then station has to wait until the beginning of the next time slot
- A collision may occur if two or more stations try to transmit data at the beginning of the same time slot

Power consumption

a) The mechanism behind the power management of an NB-IoT device

The NB-IoT standard principal power consumption real advantage comes from two technologies: PSM and eDRX, which are two modes that allows the device to drastically reduce the amount of power used at certain points of time.

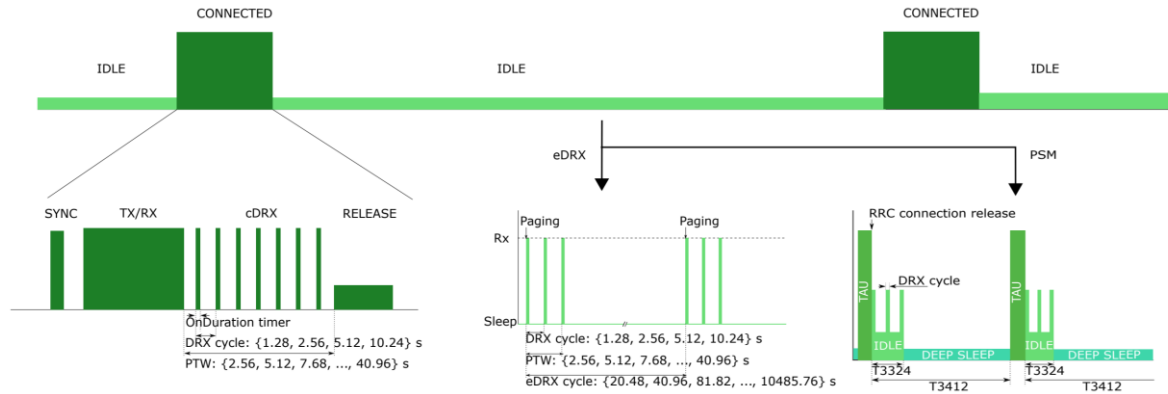


Figure 5 : Different state and mechanism of an NB-IoT device [2]

The eDRX mechanism consist in different listening/sleep cycles, it is called Paging Time Windows (PTW) and is followed by a long sleep period. This required very low power because when asleep the radio of the device is off. It can still be contacted by the network within a limited time interval, which is why it still uses a bit of power.

The PSM mechanism, on the other hand, is the most effective power saving technique, when in this mode the device can be in three states. In deep sleep, it completely switches off its radio and therefore is not reachable by the network anymore. The only thing that is still going on when in this mode, is a Connection Resume Operation that notify the network to remain registered. It also periodically performs a Tracking Area Update (TAU), which is to transmit its location to the network. It also alternates with classical DRX cycles during which it is activately listening.

Those different states are managed by timers that are unique to every mode, except for DRX mode timer that can be applying to the two others.

Mode	Timer	Description	Min Value	Max Value
DRX	OnDurationTimer	Time spent in active listening	1 ms	200 ms
	DRXcycle	Time interval between the beginning of two active listenings	2 ms	2.56 s
eDRX	PTW	Duration of Paging Occasions monitoring, composed of multiple DRX cycles	2.56 s	40.96 s
	eDRXcycle	Time interval between the beginning of two PTWs	20.48 s	10485.76 s
PSM	T3324	Active Timer: duration of DRX/eDRX within Idle state (listening for paging)	2 s	410 hours
	T3412	TAU timer: interval between two TAUs	2 s	410 hours
	Inactivity timer	Time spent in Connected state, after the end of the last TX/RX	0 s	65.536 s

Figure 6: Timers used in the different mode of NB-IoT [2]

We notice that a device can stay up to 17 days in PSM mode which is huge to power consumption since it reduces the need by more than 90%.[2]

Two other parameters that are aimed at making the communication more reliable can also play an important part in the power consumption of the device.

First, the Extended Coverage Level (ECL) has 3 levels depending on the received power that will determine the number of times a message can be repeated. This feature helps provide a better robustness but can increase the cost in power depending on the number of times a message is repeated, in ECL: 2, it can be sent 2048 times.

Second, the Release Assistance Indicator (RAI) has 3 flag values and is used to give information about his future state to the base station. It allows the device to go in sleep mode right after sending a message in which it will be stated by the flag.

Under good condition the use of those specific flags can drastically improve the battery life as we can see in the next figure.

Module	Op.	Default timers			RAI-400		
		1h	4h	24h	1h	4h	24h
Quectel-BC95	Op1	0.8	3.2	9.9	6.1	25.5	45.4
	Op2	2.4	8.5	13.0	6.4	30.1	47.6
SARA-N211	Op1	0.5	1.9	6.0	6.0	18.5	44.1
	Op2	1.6	5.9	5.7	5.9	17.7	43.3

Figure 7: Expected battery lifetime depending of transmissions interval and timers [2]

In this experiment there is a good signal condition, and the transmission is a single 20-byte UDP packet. Also, it is grouped by transmissions interval, the results however show that depending on the use or not of RAI-400 the lifetime of the battery can increase up to 7 times for the same module and operator.

b) Measurement of an NB-IoT power consumption

Now that we've explained the different mechanism involved in the power consumption of a NB-IoT device, we will explore how much it actually consumes in different scenarios.

As we have seen before the device is not always in the same mode and each mode need a different amount of power to work. There is also a huge different between uplink and downlink, sending data consume more than receiving it, but to receive data the module must be listening which also involve more energy. Nevertheless, we can pick the four most common state a device will be in and measure the power consumption for each.

In the following figure, the device A is already commercialized whereas the device B is only a prototype not totally functional which is probably why it needs more power.

	Device A	Device B
Transmit [†]	716 mW	840 mW
Receive	213 mW	240 mW
Sleep [‡]	21 mW	23 mW
Standby [§]	0.013 mW	0.035 mW

Figure 8: Measured power consumption on two NB-IoT devices [3]

The transmit measure were made with a 23dBm signal, the sleep correspond to eDRX mode and standby to PSM mode. As we can see the two modes, we previously talked about are very helpful in saving power up to a point where it barely consumes any.

Now to go further we will figure how much energy a bit uses to transmit. Based on the data from figure 8 and using the device A, the device B is not yet commercialized, we can estimate the Joule per bit.

We know that $1W = 1J.s^{-1}$ so here we have $0.716W = 0.716J.s^{-1}$ also based on the first part we know that the data rate can go from 20 to 250kbit/s. We will start by the lowest possible data rate which is 20 000 bit/s, we then have:

$$\frac{0.716}{20000} = 0.036mJ.bit^{-1}$$

So, we get that the energy consumption of a NB-IoT device is **36μJ/bit**.

According to the data in figure 8 and depending on the quality of the transmission we can make estimation around the battery lifetime, as shown in the figure below.

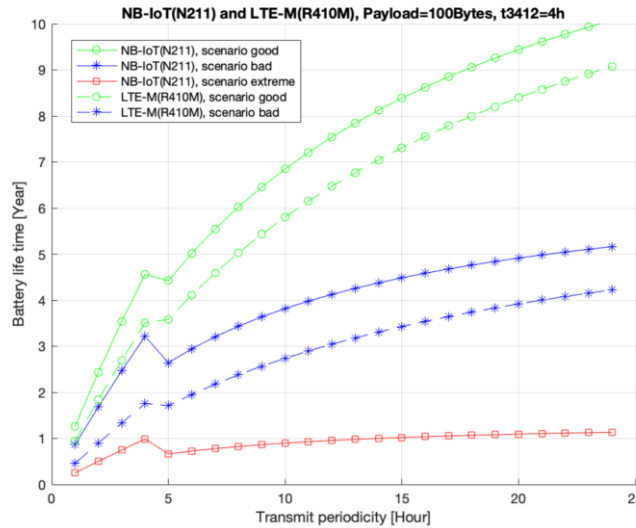


Figure 9: Battery life time as a function of the transmit periodicity [4]

This figure shows that a NB-IoT device has a really good lifespan but that it can be drastically lowered by the environment, from 10 years to 1 year depending only on the condition.

Security

Narrowband-IoT is a cellular technology and therefore is operated in a licensed spectrum. It is based on the LTE standard and thanks to that that advantage of the tested and approved security mechanism of LTE.

The use of OFDMA with 64QAM for downlink communication and SC-FDMA with 64QAM for uplink implies a great robustness against disturbances but also make RF Jamming as well as Fake base stations possible to do. However, if it's easy to set-up a rogue base station it's very hard to integrate in a network due to mutual authentication.

Due to the fact that NB-IoT devices use LTE standard, it must be equipped with a SIM card that is secure and tamper-resistant. Since SIM manufacturers are regularly certified by the CSMA and works with high-security data center, the security is greatly enhanced.

Therefore the three main advantages of the NB-IoT Initial Attach procedure are [5] :

- Explicit mutual authentication (based on pre-shared key in SIM and HSS)
- Secure key generation
- SIM is a secure element

Regarding the data transmission there are two possibilities.

First the Data Over NAS (DoNAS) allows the user data, that are transported via the MME (Mobility Management Entity), to be encapsulated in NAS (Non-Access Stratum). It can be used to transport IP or non-IP traffic. The key security advantage of this is that it ensures the same level of protection that is reserved for network signalling.

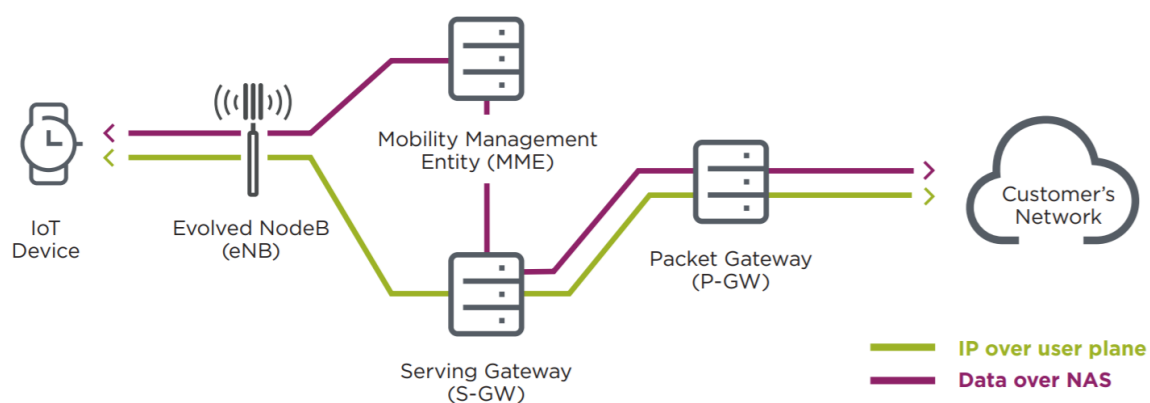


Figure 10: Path for DoNAS data in contrast with traditional IP over user plane path [6]

Then there is the Non-IP Data Delivery (NIDD) that is used when the amount of data is so small it would be a waste to add large IP headers. There is two ways to make this work :

- « Transport data using a point-to-point (PtP) SG interface tunnel to the application server. This means that the device can only communicate with the pre-defined application server, making the communications link more secure by restricting the destination, as discussed in the Managed Connectivity section » [6]
- « Transport data using the service capability exposure function (SCEF). The SCEF provides a means to securely expose service and network capabilities through network application programming interfaces (APIs). In this way, access to the IoT devices is restricted to application servers that have been authenticated and authorised to access the IoT devices. » [6]

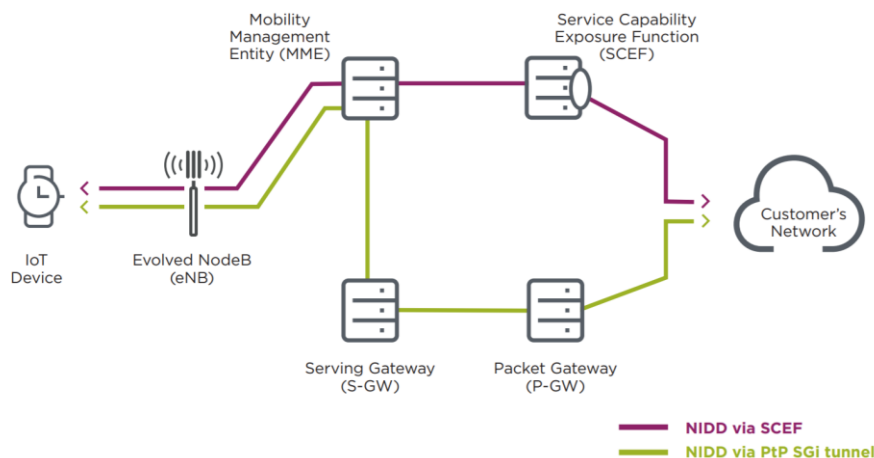


Figure 11: The two paths of NIDD [6]

To summarize, NB-IoT device benefit from using the same features of LTE mobile network for [7]:

- User identity confidentiality
- Entity authentication
- Data integrity
- Mobile device identification

We have seen that, using the LTE network, NB-IoT device have a very high level of security. However, it does not mean there is no vulnerabilities. The device can use UMTS (3G) network if no LTE access is available, this increases the attack surface. Those networks were not as secured as LTE is now. The fact that NB-IoT network heavily rely on IP technology also can be an issue since it's a widely known technology for security expert but also for cybercriminal. [5]

Conclusion

The IoT is rapidly gaining prominence due to its nearly limitless potential in terms of applications for individuals and industries.

In this work, we addressed the Release 13 of the NB-IoT 3GPP LPWA technology. More specifically, we addressed its physical layer, its MAC layer, the device power consumption, and the protocol's security option.

From the beginning, the specification of NB-IoT included considerations for its coexistence with both LTE and GSM. Parts of the physical layers of LTE were reused in NB-IoT.

Due to the reduction of the NB-IoT bandwidth to 180 kHz, low data rate devices can have extended coverage, complexity reduction, and low power consumption. For scenarios with coverage problems of cellular network operators, NB-IoT is seen as the future of IoT devices using mobile network infrastructure.

References

- [1] « The Low Power Modes of the Cellular IoT » by Thales Group available here <https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/resources/developers/cellular-iot-low-power-mode>
- [2] « Dissecting Energy Consumption of NB-IoT Devices Empirically » by Foivos Michelinakis, Anas Saeed Al-selwi, Martina Capuzzo, Andrea Zanella, Kashif Mahmood, Ahmed Elmokashf available here <https://arxiv.org/pdf/2004.07127.pdf>
- [3] « An Empirical NB-IoT Power Consumption Model for Battery Lifetime Estimation » by Lauridsen, Mads; Krigslund, Rasmus; Rohr, Marek; Madueno, Germán available here <https://vbn.aau.dk/ws/portalfiles/portal/279633819/vtcSpring2018.pdf>
- [4] « A Modelling and Experimental Framework for Battery Lifetime Estimation in NB-IoT and LTE-M » by Andre Sørensen available here <https://arxiv.org/pdf/2106.13286.pdf>
- [5] Comparison and Analysis of Security Aspects of LoRaWAN and NB-IoT by Philipp Hofmann, Yvonne Schmitz, Bernd Quink, Mona Parsa, Jens Olejak available here <https://iot.telekom.com/resource/blob/data/489050/f9fb87f65ada3528c8c08a1cb0364a1d/security-aspects-lorawan-nb-iot.pdf>
- [6] Security Features of LTE-M and NB-IoT Networks by GSMA available here <https://www.gsma.com/iot/wp-content/uploads/2019/09/Security-Features-of-LTE-M-and-NB-IoT-Networks.pdf>
- [7] Narrowband IoT (NB-IoT) by THALES available here <https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/resources/innovation-technology/nb-iot>
- [8] “Cellular networks for massive IoT,” Ericsson White Paper, Jan. 2016. [Online]. Available: https://www.ericsson.com/res/docs/whitepapers/wp_iot.pdf
- [9] 3GPP TR 45.820. Cellular System Support for Ultra Low Complexity and Low Throughput Internet of Things. Technical Report; 2015
- [10] K. Laya, “Goodbye, aloha.” [Online]. Available: <https://core.ac.uk/download/pdf/81571287.pdf>