University of Toulouse
Institut National des Sciences Appliquées de Toulouse
135 Avenue de Rangueil, 31400 Toulouse, France

DEPARTMENT OF
COMPUTER AND ELECTRICAL ENGINEERING

A REPORT

ON

"5G NB-IoT"

Protocols for Wireless Sensor Network

SUBMITTED BY

Michael EJIGU
Nhat Luan TRUONG
Andy XU
Thomas ZENNARO

FROM

5ISS B1

UNDER THE GUIDANCE OF

Prof. Daniela DRAGOMIRESCU

(Academic Year: 2020-2021)

December 16, 2020

Contents

Acronyms

3GPP Third-Generation Partnership Project. 3, 7–10

5G Fifth-generation Wireless. 9

APN Access Point Name. 9

BPSK Binary Phase Shift Keying. 3, 4

DL Downlink. 4

DMRS Demodulation Reference Signal. 5

DTLS Datagram Transport Layer Security. 9

eDRX Extended Discontinuous Reception. 7

FDMA Frequency-Division Multiple Access. 5

GSM Global System for Mobile Communications. 3

GSMA Global System for Mobile Communications Association. 7

IoT Internet of Things. 3, 5, 9, 10

LPWAN Low-Power Wide Area Networks. 3

LTE Long-Term Evolution. 3, 4

MAC Media Access Control. 5, 10

MIB Master Information Block. 5

mMTC Massive Machine Type Communication. 3

NB-IoT Narrowband Internet of Things. 1, 3–5, 7–10

NPBCH Narrowband Physical Broadcast Channel. 5

NPDCCH Narrowband Physical Downlink Control Channel. 5

NPDSCH Narrowband Physical Downlink Shared Channel. 5

NPRACH Narrowband Physical Random Access Channel. 5, 6

NPSS Narrowband Primary Synchronization Signal. 5

NPUSCH Narrowband Physical Uplink Shared Channel. 5

NRS Narrowband Reference Signal. 5

NSSS Narrowband Secondary Synchronization Signal. 5

OFDM Orthogonal Frequency Division Multiplexing. 3, 5

OFDMA Orthogonal Frequency Division Multiple Access. 4

PRB Physical Resource Block. 3

PSM Power Saving Mode. 7

QPSK Quadrature Phase Shift Keying. 3, 4

RF Radio Frenquency. 3

RSSI Received Sugnal Strength Indication. 5

RU Resource Units. 3

SC-FDMA Single-Carrier Frequency Division Multiple Access. 3–5

UDP User Datagram Protocol. 9

UE User Equipment. 3

UL Uplink. 4

VPN Virtual Private Network. 9

1 Introduction

Narrowband Internet of Things (NB-IoT) is a recent cellular radio access technology based on Long-Term Evolution (LTE) introduced by Third-Generation Partnership Project (3GPP) for Low-Power Wide Area Networks (LPWAN). The main aim of NB-IoT is to support Massive Machine Type Communication (mMTC) and enable low-power, low-cost, and low-data-rate communication.

2 Physical layer in NB-IoT

On the physical layer, NB-IoT adopts the same numerologies as legacy LTE along with Orthogonal Frequency Division Multiplexing (OFDM) and Single-Carrier Frequency Division Multiple Access (SC-FDMA) signal waveforms in downlink and uplink, respectively. However, the resource scheduling unit in NB-IoT is the subcarrier (or tone) instead of Physical Resource Block (PRB), to foster the network scalability by serving multiple User Equipment (UE) in a 180 kHz bandwidth. [1]

This section presents the main NB-IoT design changes from Release 13 until today that enabled the massive Internet of Things (IoT) connections with the corresponding solutions to respond to the adopted NB-IoT objectives:

- Mode of Operation: With the limited bandwidth requirement, NB-IoT can be deployed in three different modes: standalone, in-band, and guard-band. In in-band and guard-band modes, NB-IoT occupies one PRB of 180 KHz in LTE spectrum both in the downlink and uplink. It can also be allocated as standalone where it occupies the 200 KHz bandwidth by "refarming" the Global System for Mobile Communications (GSM) spectrum. [1]

- Multi-Tone Transmission Support: To reach the massive device deployment objective, NB-IoT introduces the allocation of Resource Units (RU) to multiple UE contrary to LTE where the whole resource block is allocated to a single UE in the uplink. In this regard, tones (frequency domain) with different duration are allocated to UE. For the uplink transmission, each tone may either occupy 3.75 kHz or 15 kHz of transmission bandwidth based on the SC-FDMA scheme; for downlink NB-IoT uses 15 kHz of transmission bandwidth with OFDM scheme as LTE. With 15 kHz spacing, NB-IoT can dedicate either single-tone (8 ms) or multi-tone (3 tones, 6 tones, and 12 tones) to different UE with the duration of 4 ms, 2 ms, and 1 ms, respectively. On the other hand, the 3.75 kHz spacing supports only single-tone allocation to different users with 48 subcariers of 32 ms duration. [1]

- Complexity and Cost Reduction Techniques: NB-IoT is required to have low complexity to reach the low-cost objective to facilitate massive connections. The features that were implemented to reach this objective include relaxed base-band processing, low memory storage, and reduced Radio Frenquency (RF) components. In this regard, the system bandwidth is set as narrow as 180 kHz with reduced frequency and time synchronization requirement. Also, NB-IoT uses the restricted Binary Phase Shift Keying (BPSK) and Quadrature Phase Shift Keying (QPSK) modulation schemes with only one antenna support both in uplink and downlink transmission. [1]

Parameters	NB-IoT
Access Medium	• UL: SC-FDMA • DL: OFDMA
Carrier Spacing	• UL: QPSK, $\frac{\pi}{4}$ QPSK, $\frac{\pi}{2}$ BPSK • DL: QPSK
Modulation	• UL: 15kHz, 3.75kHz • DL: 15kHz
Max Payload	• UL: 1000 bits • DL: 680 bits
Bandwidth	• Standalone Mode: 200kHz • In-band Mode: 180 kHz in LTE spectrum • Guard-band mode: 180 kHz in LTE spectrum

Table 1: Summary table of layer 1 (Physical layer) of NB-IoT [2].

3 Media Access Control in NB-IoT

The Media Access Control (MAC) layer controls how nodes access the media to communicate with the Base Station it is connected to.

3.1 Multiple Access scheme and Communication Channels

In NB-IoT, the acess protocol differs in uplink and downlink [3]. For downlink communications OFDM is used. It consists of closely spaced carrier frequencies that do not interfere with each other. We can therefore fir more slots in the same band size compared to simple FDMA. The theoretical peak speed of the downlink is 250 kb/s. In downlink the following communication channels are used:

- Narrowband Physical Downlink Shared Channel (NPDSCH) for downlink data packets transmissions.
- Narrowband Physical Downlink Control Channel (NPDCCH) to acquire System Information Block (SIBs) once every 2560 ms.
- Narrowband Reference Signal (NRS) to estimate link quality.
- Narrowband Primary Synchronization Signal (NPSS) for frequency and timing synchronization with the base station.
- Narrowband Secondary Synchronization Signal (NSSS) also for frequency and timing synchronization with the base station.
- Narrowband Physical Broadcast Channel (NPBCH) to acquire Master Information Block (MIB) once every 640 ms.

Synchronization is necessary because NB-IoT Nodes can sometimes be in sleep mode to save energy. Using the NPSS and NSSS channels, nodes run a synchronization algorithm to synchronize in time and frequency and detect the cell identity number.

If applications wish to use localization services, since NB-IoT nodes are connected to Mobile Network Base Stations, and their positions are known, they can use the Received Sugnal Strength Indication (RSSI) value between them and surrounding Base Stations to triangulate.

For Uplink communications (which is more used in IoT) SC-FDMA is used. SC-FDMA is basically OFDM with an extra step which is coding with a Discrete Fourier Transform (signals are coded with non overlapping Fourier transform coefficients). The theoretical peak of speed is 2267 kb/s. The following channels are used :

- Narrowband Physical Random Access Channel (NPRACH) 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) for uplink data packets transmissions.
- Demodulation Reference Signal (DMRS) for uplink channel estimation accuracy.

3.2 Collisions

To avoid collisions on the NPRACH channel, the Slotted Aloha protocol is used. This is a Collision Detection protocol.

In Aloha [4], nodes can transmit at any time, and then listen on the media to check if someone else is also transmitting end detect a collision. Slotted Aloha has the specificity of marking the possible slot beginning times. Therefore the probability of collision is reduced as it can only happen on specific times.

4 Power consumption

"NB-IoT dramatically improves network efficiency, increasing the capacity to support a massive number of new connections using only a portion of the available spectrum. This efficiency, in turn, minimises power consumption enabling battery life of more than ten years[5]" as is described by the GSMA. "NB-IoT is very flexible and can operate in 2G, 3G and 4G band. It eliminates the need for a gateway, which saves cost in the long run[5]".

What determines power consumption is the current usage of the device. It spikes when sending and receiving data but also uses power when the device is on, like every electronic device. NB-IoT can be said to be low-power consumption thanks to its specifications and using Extended Discontinuous Reception (eDRX) and Power Saving Mode (PSM)[5] (see Figure 1).

These modes put the device on stand-by, sleep mode which greatly reduce the current consumption. Indeed, a device can go to sleep when it does not transmit messages. As multiple devices cannot transmit at the same time, the network dynamically schedules the sleep time to every devices on the same cell[6]. Moreover, one device also does not need to listen at all times, which permits an instant reaction, since NB-IoT is mostly used for sensor networks, that is data transfer. So the active time of a device can be freely configured in order to reduce the power consumption to the minimum possible [6].

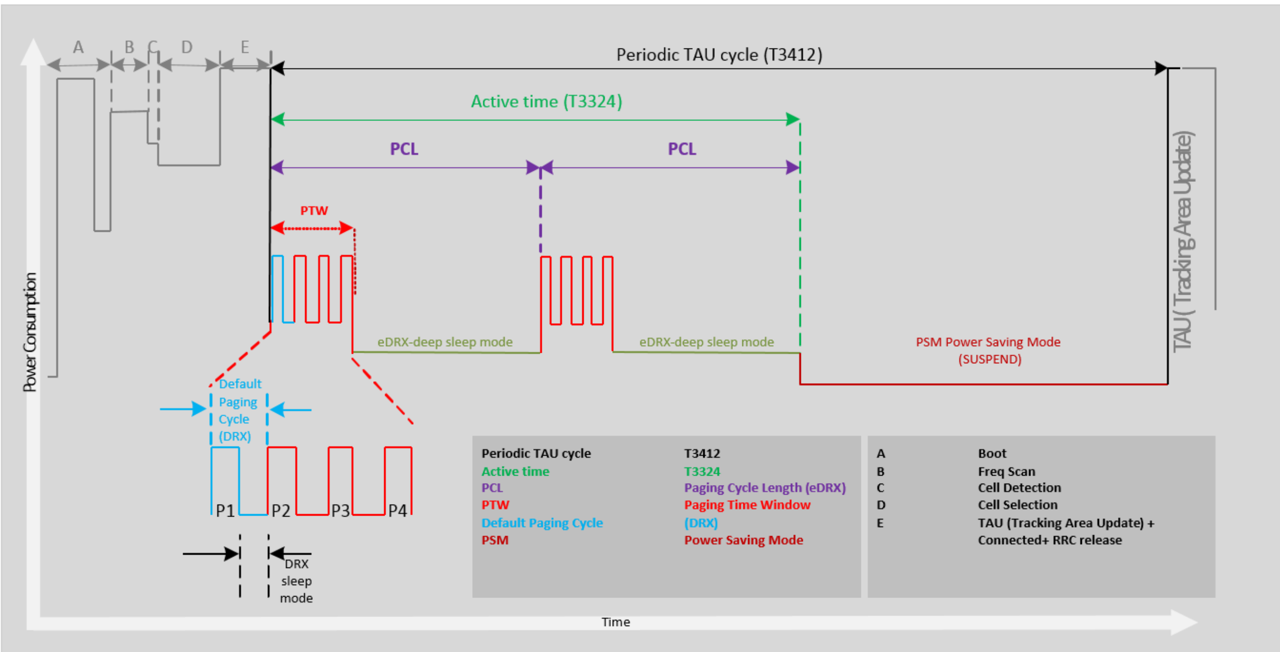

Figure 1: NB-IoT power consumption over time graph [6]

In term of numerical values, a device consumes 750 mW when transmitting at 23 dB. Continuous reception requires 220 mW, while the discontinuous reception and PSM sleep states consume respectively 22 mW and 25 µW[7]. Even though the power spikes can be higher compared to other 3GPP technologies, NB-IoT compensates the losses with its extended sleep mode. However, it is also noticeable that the transfer rate is thus impacted as the duty-cycle is set to reduce power consumption.

In term of battery life expectancy, we approach what 3GPP describes with 10 year of work time for NB-IoT devices if used as intended[7]. Using a 27.7 Wh battery, the result of comparing the transmit interval of 100 bytes at 300 bps every hour or every day is in the following in Figure 2.

t_i	Technology	I-eDRX	PSM	Power cycle
1 h	3GPP [4]	88 d (0.2 y)	256 d (0.7 y)	108 d (0.3 y)
	Device A	17 d (0.0 y)	230 d (0.6 y)	103 d (0.3 y)
24 h	3GPP [4]	126 d (0.3 y)	4998 d (13.7 y)	2583 d (7.1 y)
	Device A	18 d (0.1 y)	4677 d (12.8 y)	2462 d (6.7 y)

Figure 2: Estimated lifetime for a transmit interval t_i=[1h, 24h] [7]

5 Security

5.1 5G in terms of security

5G is based on the 3GPP standard that supports IoT devices. [8] [9] [10]
As the field of connected objects is dominant in our society, 5G faces many security challenges:

- Be careful about the authentication process and access control
- Ensure data integrity when trading across the network, which means avoiding information leakage and ensuring reliability
- Ensure the confidentiality of data exchanged between IoT devices, which requires end-to-end data encryption

5.2 Security regarding the NB-IoT

NB-IoT will use the security mechanisms used in mobile infrastructure. It thus makes it possible to have features such as:

- authentication: for instance, ensure that the sensor that sends information to the Cloud has access rights;
- encryption of exchanged information: only the entity receiving the data has the encryption key to interpret the data;
- data integrity: no alteration of the data exchanged between a device and the cloud.

These features are directly related to the 5G, whose objective is to ensure these same safety conditions.
The protocol used by the NB-IoT is UDP. This protocol allows the exchange of data in unconnected mode. It facilitates the implementation of the Datagram Transport Layer Security (DTLS) protocol in order to secure the exchanged data.

5.3 Improvement of security regarding the NB-IoT

The user can configure his Access Point Name (APN) to effectively manage his network of IoT devices. Indeed, we can have an intermediate server to collect information from the NB-IoT network.

- *Advantage*: This avoids going through the Internet, thus avoiding potential security vulnerabilities. A Virtual Private Network (VPN) channel can also be set up between the NB-IoT network and the data platform.
- *Drawback*: The cost of implementation can be significant.

6 Conclusion

We tried to described the Narrowband Internet of Things (NB-IoT) in this report in four major parts: the physical specifications, the MAC layer, the device power consumption and the protocol's security options.

NB-IoT applications can cross many service categories, these include: Smart city infrastructures such as street lamps or dustbins, Facility management services, Connected personal appliances measuring health parameters, Tracking of persons, animals or objects... Telecommunication giants such as Huawei, Ericsson, Qualcomm, and Vodafone have collectively put together this standard in conjunction with 3GPP. Huawei, Ericsson, and Qualcomm are interested in NB-IoT because it has a number of benefits, such as: power efficiency, potential cost savings, reliability, wider deployment, global reach... It's no wonder that with the dawn on 5G and the strong growth of semiconductor industry, cellular IoT has an even brighter future.

References

[1] C. Mwakwata, H. Malik, M. Alam, Y. Le Moullec, S. Parand, and S. Mumtaz, "Narrowband internet of things (nb-iot): From physical (phy) and media access control (mac) layers perspectives," *Sensors*, vol. 19, 06 2019.

[2] E. Rastogi, N. Saxena, A. Roy, and D. R. Shin, "Narrowband internet of things: A comprehensive study," *Computer Networks*, vol. 173, p. 107209, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128619313593

[3] M. Mwakwata, "Narrowband internet of things (nb-iot): From physical (phy) and media access control (mac) layers perspectives," June 2019. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6603562/

[4] K. Laya, "Goodbye, aloha." [Online]. Available: https://core.ac.uk/download/pdf/81571287.pdf

[5] T. Group, "Narrowband iot (nb-iot)." [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/resources/innovation-technology/nb-iot

[6] Thales Group, "The low power modes of the cellular iot." [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/resources/developers/cellular-iot-low-power-mode

[7] M. Lauridsen, R. Krigslund, M. Rohr, and G. Madueno, "An empirical nb-iot power consumption model for battery lifetime estimation," in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, 2018, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/8417653

[8] L. Liu and M. Han, *Privacy and Security Issues in the 5G-Enabled Internet of Things*, 05 2019, pp. 241–268.

[9] C. Corde, "Pourquoi le nb-iot peut être une alternative sérieuse?" [Online]. Available: https://blog.rtone.fr/nb-iot

[10] R. Ligero and O. Patau, "The security of nb-iot devices," Sep 2019. [Online]. Available: https://accent-systems.com/blog/security-of-nb-iot-devices/