SAPIENZA
UNIVERSITÀ DI ROMA

FACOLTÀ DI INGEGNERIA DELL'INFORMAZIONE, INFORMATICA E STATISTICA

Corso di Laurea Magistrale in Ingegneria Elettronica

# NB-IoT system deployment for massive Machine to Machine communication: evaluation of coverage and capacity performances

Relatore
Prof. Maria-Gabriella Di Benedetto

Marco Pennacchioni
1497658

Correlatori
Ing. Camillo Carlini
Ing. Pietro Obino
TIM

Anno Accademico 2016/2017

# Ringraziamenti

Prima di tutto ringrazio la professoressa Maria-Gabriella di Benedetto per la disponibilità ed il sostegno offerti nello svolgimento di questo lavoro come relatrice, per la professionalità e la passione trasmessa come docente, e soprattutto come persona per i consigli e le parole di incoraggiamento che non sono mai mancate in tutti questi anni.

Ringrazio i miei correlatori Camillo e Pietro, per l'opportunità fornita di sviluppare questo lavoro in TIM e di affrontare una tematica così attuale ed affascinante per me; è soprattutto grazie al loro aiuto che questo lavoro è stato portato a termine con successo.

Ringrazio Renzo, Nicola, Raffaele e tutti i ragazzi del laboratorio *Pegasus*, che mi hanno fatto sentire a casa fin dal primo giorno.

Ringrazio i miei genitori Anna e Nicola, senza il loro affetto ed il loro sostegno tutto questo non sarebbe stato possibile. Ringrazio mia sorella Valeria, che è stata, è e sarà sempre il mio punto di riferimento.

Un grazie speciale va ad Elena, per essere stata sempre al mio fianco, per la forza data nei momenti di difficoltà e per aver condiviso con me ogni soddisfazione. Insieme nessun obiettivo è irraggiungibile.

Ringrazio infine i miei compagni di avventura Claudio e Marco, è stata una vera fortuna lavorare con due amici come voi.

# Abstract

Internet of Things offers a wide spectrum of opportunities for innovative applications designed to improve our life quality. In the energy sector, the developing of smart metering networks allows operators and companies to increase the production efficiency and to offer an enhanced service to customers. 3GPP introduced in Release 13 Narrowband Internet of Things (NB-IoT) as a new cellular technology for providing wide-area coverage for Internet of Things (IoT) and Machine Type Communication (MTC). Moreover, NB-IoT has be defined as the standard technology from which to start the development of MTC devices in 5G optic: first commercial devices are supposed to be released by the end of 2017.

This work propose a system deployment of a NB-IoT system for smart metering. The aim is the analysis of the performances of this technology in a Massive dense urban scenario in terms of coverage and capacity. Estimated number of UE that this system can serve and coverage enhancement considerations with respect to LTE technology are provided. In particular, we focus our attention on the effect of coverage enhancement on the system efficiency. The goal is to study how an operator can satisfy customer demands with this new functionality, while reusing the infrastructure of existing LTE technology.

# Abstract (ITA)

L'*Internet of Things* offre un'ampia gamma di opportunità per la creazione di applicazioni innovative, atte a migliorare la qualità della nostra vita. Nel settore energetico, lo sviluppo di reti di *smart metering* permette ad aziende ed operatori di incrementare la loro efficienza in produzione ed offrire agli utenti un servizio migliore. In Release 13 il 3GPP definisce il *Narrowband Internet of Things (NB-IoT)* come una nuova tecnologia cellulare sviluppata per fornire un servizio IoT per comunicazione *Machine to Machine* sulla preesistente rete LTE. Il NB-IoT è stato inoltre definito come tecnologia di base per lo sviluppo di sistemi MTC in ottica 5G: i primi dispositivi saranno lanciati sul mercato entro la fine del 2017.

Questo lavoro propone lo sviluppo di un sistema NB-IoT per lo smart metering in uno scenario massive dense urban, con lo scopo di analizzarne le prestazioni in termini di copertura e capacità. Vengono inoltre fornite una stima del numero di utenti che questo sistema riesce a servire, ed uno studio sull'ampliamento della copertura rispetto al caso LTE, con particolare attenzione a come questo influenzi l'efficienza del sistema. Lo scopo di questa analisi è quello di dimostrare come un operatore possa fornire questo nuovo servizio al cliente senza la necessità di installare nuove apparecchiature, riutilizzando totalmente le già presenti infrastrutture di rete LTE.

# Table of contents

# 1 Internet of Things: a technological revolution

The development of digital technologies is leading to a deep process of change in all aspects of everyday life, so that we can talk about a true technological revolution. Just think of smartphones, more and more powerful and cheaper, big data that allows managing huge masses of data from which new services and application rise, and cloud, offering services increasingly capable of processing and storing. Among these technologies, Internet of Things (IoT) is probably the one destined to generate major changes in the next 5-10 years. IoT refers to a networked interconnection between objects of everyday use, endowed with artificial intelligence: the purpose is to integrate every object to the ubiquity of the Internet via embedded systems in order to develop a highly distributed network of device communicating with other devices as well as human beings. Examples of IoT services include security, payment, tracking, smart grid and remote monitoring and maintenance. It has been estimated that by the end of 2020 there will be 50 billion connected devices worldwide. Internet of Things aims to blur the boundaries between the digital and physical worlds. The development of smart devices is driven by the growing number of mobile users and by the application of technologies based on the use of real-time information. IoT is going to open huge opportunities for a large number of innovative applications able to improve our life quality. In this context, leading enterprises are discovering great opportunities to use highly connected device to improve business performances and to give customers what they really want, not only new products or services, but also more meaningful outcomes.

## 1.1 Machine Type Communication (MTC)

Machine Type Communication (MTC) is required to support IoT. As said before, it has been estimated that by the end of 2020 there will be almost 50 billion connected device worldwide. This kind of projection encourages the industry to explore the wide range of opportunity that Machine Type Communication offers, enabling enhanced workflow efficiency, improved life quality and brand new business cases. On this way, it is no surprise that main telecommunication association and standardization companies such as 3GPP and ETSI are involved in developing standards in the context of MTC. The term Machine Type Communication refers to communications between devices such as computers, smart sensors, embedded systems or mobile devices without (or with only limited) human intervention: so that devices have to be able to generate, exchange and process data fully automatically. MTC is also known as M2M communication: the abbreviation denotes various concepts, namely Machine-to-Mobile, Mobile-to-Machine, or Machine-to-Machine. In our case is appropriate to consider this term in the latter meaning case. Machine Type Communication has a great potential in a wide range of applications and services: it allows a wide variety of machines to become nodes of a personal wireless network, and provides to develop monitoring and control applications. This will cause the decreasing of costs for human resources in automated workflow and will make the devices smarter and autonomous. By definition, MTC describes machines using network resources to communicate with remote application infrastructure for the purpose of monitoring and control, either of the surrounding environments, or of the machine itself. Therefore, MTC does not simply creates a passive data collection point but an intelligent inter-machine coordination ecosystem. In other words, we can say that MTC uses a device (sensor, meter…) to capture an event (temperature, inventory level…) which is relayed through a network to an application that finally translates the captured event into meaningful information. The communication among MTC devices can be handled through different technologies. Point-to-point and multi-hop wireless networks, such as sensor networks, can be considered as a means to provide Internet access for devices: here the definition of MTC for Internet of Things. Cellular systems such as LTE (Long Term Evolution) are considered as valid solutions to support the wide provision of MTC applications. Their ubiquitous presence saves the network installation cost and provides widespread coverage. Moreover, the communication links are more reliable because cellular systems are regulated and interference controlled. However, cellular systems are mainly designed to serve traffic between humans, characterized by huge exchange of data during active periods with a higher demand on downlink. Major MTC applications contrariwise have different traffic characteristic, as we can see below:

1. *Low Mobility*: MTC devices are almost stationary, or move infrequently only within a certain region;
2. *Time Controlled*: send or receive data only at certain pre-defined periods;
3. *Time Tolerant*: due to the infrequent transmission on the channel, data transfer can be delayed;
4. *Small Data Transmission*: MTC devices frequently send or receive only small amount of data;
5. *Monitoring*: MTC networks provide functionality to detect the events;
6. *Low Power Consumption*: MTC device are often installed without power supply, so that they need to run only on battery;
7. *Location Specific Trigger*: networks nodes or devices have to be able to trigger other MTC devices in a particular area, for instance to wake up the device.

The 3GPP (3rd Generation Partnership Project) is collaboration between groups of telecommunications associations, to make a globally applicable third-generation mobile phone system specification within the scope of the International Mobile Telecommunications-2000 project of the International Telecommunication Union. 3GPP specifications are based on evolved Global System for Mobile Communications specifications encompassing radio, core network and service architecture. In this vein, 3GPP has launched numerous activities to support MTC for future releases of LTE network, referred to as LTE-Advanced (LTE-A); it has already specified the general requirements for MTC applications and identified issues and challenges related to them. Network and device modifications have been considered in upcoming releases of LTE standardization to facilitate and better support the integration of MTC.

MTC offers a wide range of new services and applications that may have very different features and requirements. We can see below a list of the main applications of Machine Type Communication related to their imposed requirements.

- *Smart metering*: support of massive number of devices with high coverage and small data bursts; application in electric power, gas, and water metering.
- *Tracking:* high mobility and low power consumption; application in fleet management and assert tracking.
- *Payment:* high level of security; application in point of sale and vending machines.
- *Control systems and monitoring* high reliability and low-latency data transmission; application in industrial and home automation, and real-time control.
- *Security and public safety:* high reliability, high security and low latency; application in surveillance systems, home security and access control.

Although every particular application is different from each other, some basic stages are common to most MTC deployment:

1. Data collection;
2. Data transmission through the network;
3. Data evaluation;
4. Response to the available information.

In the following figure, we can see an example of the MTC basic architecture.

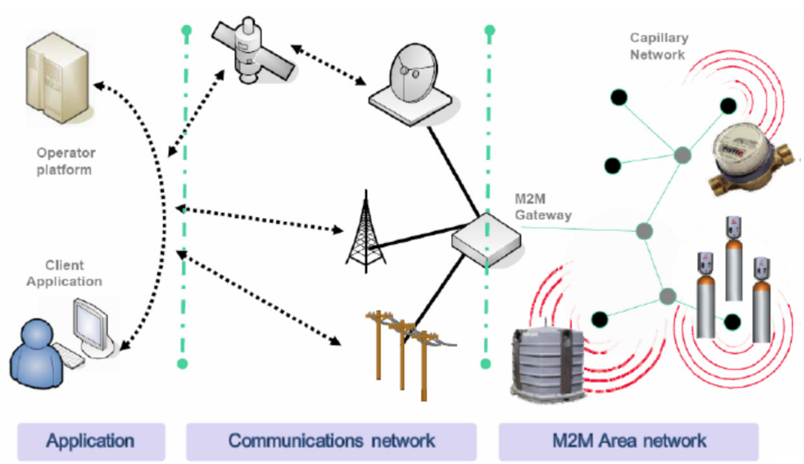


*Figure 1.1-1 – MTC basic architecture*

MTC devices reply to requests for data contained within them or transmit the data automatically. MTC devices may constitute an MTC area network that is linked to the M2M Gateway, which provides interconnection of devices and forwards data collected to communication network. The communication network links the UEs (through the Gateway) to the MTC end-user application or server: for this purpose, telephone lines, cellular network or communication satellites can be used. Finally, when data reach an application, they can be analyzed, reported and acted upon by a software agent or a process.

## 1.2 Smart metering and smart grid

In this work, we will focus our attention on smart metering and smart grid applications of MTC. As an example, electricity networks are currently hierarchically organized networks: energy is always generated in one specific location and then transmitted to a town or city, where it is further distributed to the consumers. Nowadays information on the consumer's usage flows back to the producer once a year wend the meter reading is sent back. Experts expect energy production and distribution to be more localized and require much more information exchange. In order for this to be possible extensive use of MTC using fixed and wireless networks is required. Smart metering is the first step in building a smart grid: through this technology, the meter can transmit real-time information on energy, which the consumers can access in their own home and which the energy company can use to manage the network. Costumers could be stimulated to change their behaviors by introducing differentiated pricing for peak use and informing them of when such peak occur. Moreover, smart meters can allow consumers delivering their locally generated energy, as in case of solar cells sending excess electricity back to the grid. Indeed new business models are emerging where energy companies install solar cells on people's homes and manages all those cells as a power station: in this way, the consumer gets a lower rate and the excess energy is sold on the grid. This requires constant communication to know where demand is and where production is available.

The diffusion of electric vehicles would also require the network to become smarter. This implies the development of parking spaces equipped with loading stations and able to support also a billing mechanism. Moreover, the use of electric cars could be a huge charge on the grid, which need to be well managed, in particular during peak times for the working hours. For example, in the morning, after people have driven to work, and in the evening, when they return home, there will be a spike in demand for energy to recharge cars. All this implies the need for proper management of the power grid, distributing the load cycles during the days and night based upon the requirements of the users, in order to save the countries from building several power stations just to service peak demands. The energy stored in vehicles could also be used to level out the spikes in demand placed on electricity networks, for example during the break in major sporting events.

As seen before, Machine Type Communication solutions for smart grids need to work in fixed locations, with no need for mobility. These solutions would be able to support millions of devices that generate infrequent and small amounts of data. These features implies that the network technology has to handle small bursts of data from a large number of devices. In addition, the metering devices may be developed in indoor environment; hence, they require enhanced coverage level for their connectivity. Finally, low-latency data transmissions are essential to develop a real-time control system. In a standard scenario, we can consider to have one meter per home or business and one to three more to allow for the charging of household cars and guest cars. In a dense urban scenario, like the case considered in this paper, we should assume up to 40 meters per building: it is precisely for this reason that we have to talk about *Massive MTC*. The European Union has mandated the use of smart meters by 2020, which means there will be a market for around 180 million meter at a rate of one per household. If we assume most OECD countries will follow, this market could became around of 400 million units, with the same rate of one meter per household. Finally, if the electric cars could really became the vehicle of the future, around one billion MTC devices could be necessary to support the coordination of these cars.

## 1.3 Business impact

It has already been described the plethora of opportunities for development of novel business cases offered by Machine Type Communication and the relative meaning impact that this technologies would have on the economic growth. Many industries will be transformed with respect to their business process, resulting from the changes driven by the spreading of MTC. In particular, in the energy sector, smart metering increases business efficiencies and decreases operational expense for energy companies. Transportation tracking solutions improve route optimization and mobile broadband plays a central role in the increasing of connectivity in the optic of Internet of Things. The healthcare industry is also looking for improvement of patient care through instant device communications, disease management and remote monitoring. In the following figure, we can see a representation of the main business improvement brought from MTC, according to Ericsson's projection for 2020 entailing the number of connected devices reaching 50 billion.

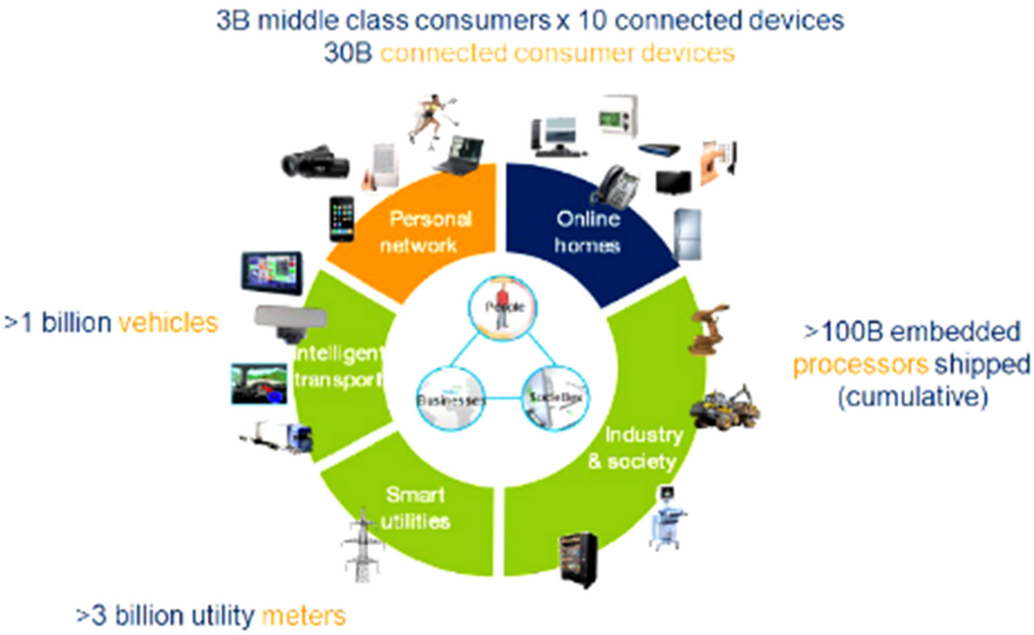


*Figure 1.3-1 – MTC future business improvements*

# 2 Narrowband Internet of Things

As seen before, the interest in applications of MTC as the integration of connectivity solutions with sensors or meters (gas, electric, water or parking) is developing very rapidly. In order to offer a wide-area coverage with machine type communication systems, the 3rd Generation Partnership Project (3GPP) has introduced in Release 13 two new features supporting narrowband MTC: these features are called eMTC (enhanced MTC) and Narrowband IoT (NB-IoT). In first case, eMTC introduces a new UE with reduced RF bandwidth of 1.4MHz in uplink and downlink and coverage enhancement to provide better indoor support. Narrowband Internet of Things (NB-IoT) is a technology defined to implement the Machine Type Communication (MTC) functionalities over the well-known LTE spectrum: this means to offer deployment flexibility allowing an operator to implement this technology using a small portion of its existing available spectrum. Although it is integrated in LTE standard, NB-IoT can be considered as a brand new air interface, and so is not backward compatible with LTE. During this work, we focus our attention on NB-IoT, in particular on the key aspects where this technology deviates from LTE.

## 2.1 LTE fundamentals

Long Term Evolution (LTE) is a 4G wireless broadband technology developed by 3GPP. This technology is named "Long Term Evolution" because it represents the next step (4G) in a progression from GSM (2G), to UMTS (3G) technologies based upon GSM. LTE target features are significantly increased peak data rates, reduced latency, scalable bandwidth capacity, and backwards compatibility with existing GSM and UMTS technology.

LTE architecture, named Evolved Packet System EPS, can be divided in two components:

1. the Evolved UMTS Terrestrial Radio Access Network (E-UTRAN), that is the radio access network;

2. the Evolved Packet Core EPC, that represents the evolution of the core network.

In general E-UTRAN is simply called LTE, while EPC can be also indicated as System Architecture Evolution SAE. *Figure 2.2-1* shows a model of EPS architecture, including logical IP interfaces at transport level. On the left, the eNodeB antennas represent the E-UTRAN, while all the other elements on the right represents the EPC.

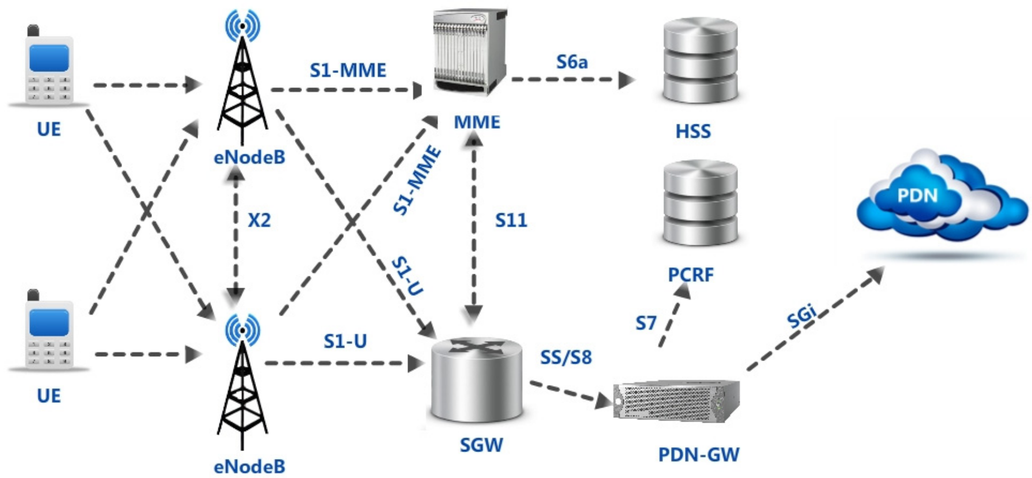


*Figure 2.2.5-1 – EPS architecture*

The E-UTRAN, on the left, is composed only by the Evolved NodeB eNB: it manage all the radio procedure to and from the user equipment, signaling and data transfer to the Core Network and other nodes. The advantages carried by the introduction of the eNB, is that it includes the Radio Network Controller functionality, leading to reduced delay values. Now we briefly describe the features of main elements included in the EPC:

- *Mobility Management Entity MME*: the control node responsible for traffic management at Non-Access Stratum (NAS) level, to and from UE; it handles the Mobility Management MM and the Connection Management CM. Through ESM protocol MME improve Session Management, allowing the establishment of the logic connection between UE and PDN.
- *Serving Gateway SGW*: allows the transfer of IP packets from and to the eNB. Its main function is to hold user plane data in case of mobility among different nodes.
- *Packet Data Network Gateway PGW*: represents the access point to external Packet Data Networks. It is responsible of the assignation of IP addresses to each UE.

- *Home Subscriber Server HSS*: gives information about on which PDN a determined UE can attach. It also contains information about possible roaming access restrictions and subscription data.
- *Policy and Charging Rules Function PCRF*: it handles the Policy and Charging Control, determining service management in terms of Quality of Service QoS. Then, it communicates the relative parameters to PGW that consequently configures the appropriate data radio bearers.

An X2 interface allow the connection between an eNB and nearby base stations and manages the handover procedure. S1 interface connects each eNB to the EPC. We can distinguish between two different S1 interfaces: S1-MME links the node to the MME, while S1-U links the node to the SGW. S11 interface connects MME and SGW, while S5 interface does the same for SGW and PGW.

### 2.1.1 Physical Layer

LTE PHY layer employs new technologies in mobile communication with respect to UMTS. This layer allows efficient transmission of both data and control information between UE and nodes. The LTE frame structure depends on the duplexing mode. We define:

1. *Frame structure Type 1* for Frequency Division Duplexing (FDD);
2. *Frame structure Type 2* for Time Division Duplexing (TDD).

In case of Frequency Division Duplexing (Type 1), for both uplink and downlink frames has a 10ms time duration. Each frame is split in 10 subframes of 1 ms, and each subframe is composed of two slots of 0.5 ms. This results in 20 slots in a single frame. The number of OFDM symbols included in a time slots depends on the cyclic prefix length: in case of Normal Cyclic Prefix, we have 7 OFDM symbols, while in case of Extended Cyclic Prefix we have only 6 symbols. The length of the CP is variable: it is about 5.2μs for the first symbol and about 4.7μs for the other six symbols, leading to an overall duration of (5.2+66.7) + (4.7*66.7) * 6 = 71.9 + 428.4μs = 0.5ms. In frequency domain, each slot corresponds to 180kHz divided in 12 15 kHz sub-carriers: as a consequence, the symbol duration is equal to 66.7 μs. Then a Physical Resource block (PRB) is composed by 12 subcarriers in frequency and 7 (or 6 in case of extended CP) OFDM symbols in time. A Resource Elements (RE) consists in a single subcarrier and a single OFDM symbol and includes information about the modulation order. *Table 2.2.1-1* shows the maximum number of PRB that can be assigned to each UE.

| *Bandwidth [MHz]* | 1.4 | 3 | 5 | 10 | 15 | 20 |
|---|---|---|---|---|---|---|
| *Number of PRB* | 6 | 15 | 25 | 50 | 75 | 100 |

*Table 2.1.1-1 - Maximum number of PRB that can be assigned to each UE*

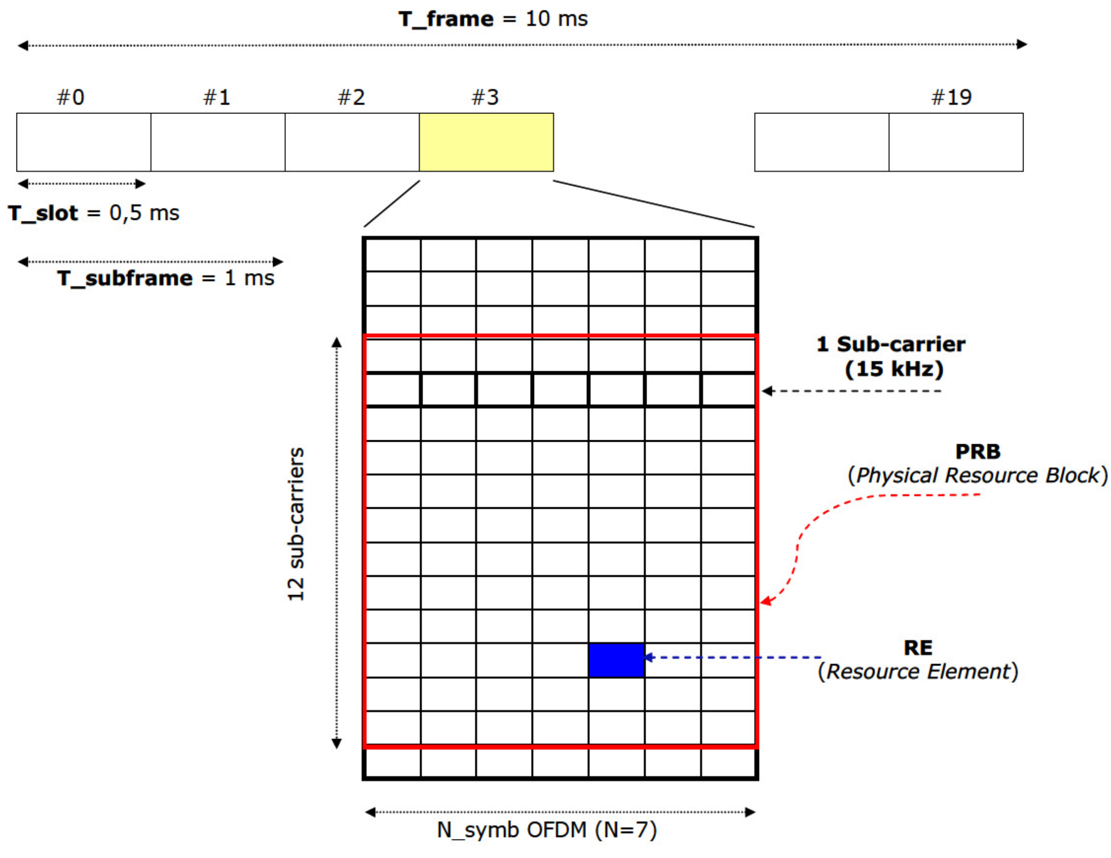


*Figure 2.1.1-1 – LTE frame structure in FDD (Introduzione all'LTE e alle funzionalità in tecnologia Huawei, Telecom Italia)*

In 3G communications code division access technique is implementedd. Each UE has a single fixed band portion and one or more codes to transmit or receive. Several multiple access techniques can be used: in particular, LTE uses Single Carrier Frequency Division Multiple Access SC-FDMA in uplink and Orthogonal Frequency Division Multiple Access OFDMA in downlink. OFDM is a multi-carrier technology that subdivides the bandwidth into a set of narrowband subcarriers that are mutually orthogonal. OFDMA allows high Peak-to-Average Power Ratio (PAPR), but requires expensive power amplifiers and consequently highly expensive devices. Instead of this technique, LTE in uplink uses SC-FDMA that guarantees a low PAPR and consequently reduced costs. In the following, we give a more detailed description of the multiple access techniques just mentioned.

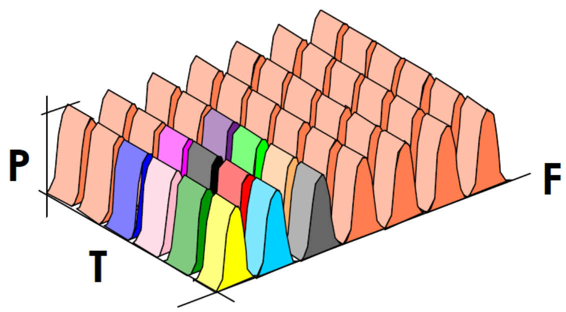


*Figure 2.1.1-2 – OFDMA access technique in LTE (Introduzione all'LTE e alle funzionalità in tecnologia Huawei, Telecom Italia)*

### 2.1.1.1 OFDMA

OFDMA consists in a transmission scheme characterized by Orthogonal Frequency Division Multiplexing (OFDM) using an elevated number of carriers to transmit information to and from the UE. OFDM carriers are spaced by a $\Delta f$ = 15kHz; data to transmit are divided in several streams, each one transmitted on a different carrier. This subcarrier spacing leads to a symbol time $T_u = 1/\Delta f = 66.7$ μs: this bound has to be respected in order to maintain orthogonality between the carriers. The overall system capacity depends linearly to the number of carriers used (these two variables are directly proportional).

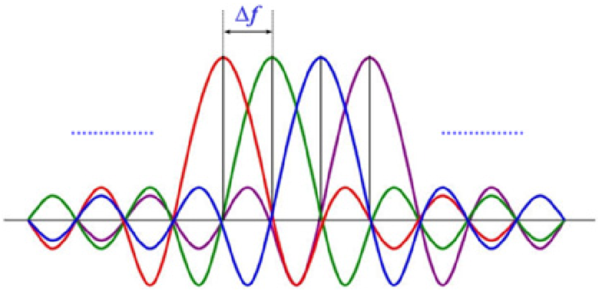


*Figure 2.1.1.1-1 – OFDM carriers*

A Cyclic Prefix Insertion is employed in order to avoid Inter-Symbol Interference (ISI): at the beginning of each symbol is inserted a prefix equal to its final part. This prefix in part overlap the previous symbol on the OFDM transmission: if the maximum delay spread between principal path and the signal replications is less than the duration of the prefix, othogonality is granted.

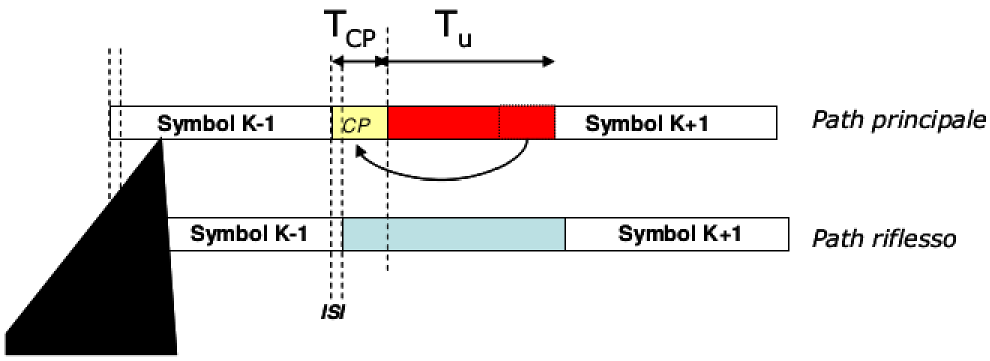


*Figure 2.1.1.1-2 – Cyclic prefix insertion (Introduzione all'LTE e alle funzionalità in tecnologia Huawei, Telecom Italia)*

In OFDM it is possible to apply a different modulation scheme for each subcarrier, according to the correspondent SINR level. The higher is the modulation index of the scheme applied, the higher will be the transmission speed. LTE allows the use of Binary Phase-Shift Keying BPSK, Quadrature Phase-Shift Keying QPSK, 16-Phase Quadrature Amplitude Modulation 16QAM and 64-State Quadrature Amplitude Modulation 64QAM. Higher modulation orders carries a greater number of bits per symbol leading to higher data rates, but lower robustnesss to noise.

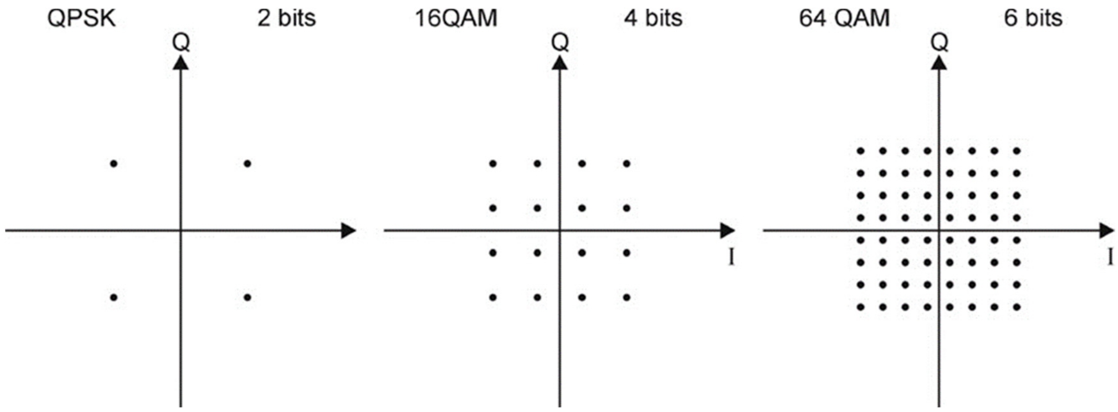


*Figure 2.1.1.1-3 – LTE modulation schemes*

### 2.1.1.2 SC-FDMA

While OFDMA technique result in a parallel data transmission, in SC-FDMA the transmission is serial: the symbols are no more associated to N subcarriers. In this way, this technique spreads the N modulation symbols over the N subcarriers, leading to an unique carrier in transmission. Then there is no more modulation for each single subcarrier and the PAPR is reduced.

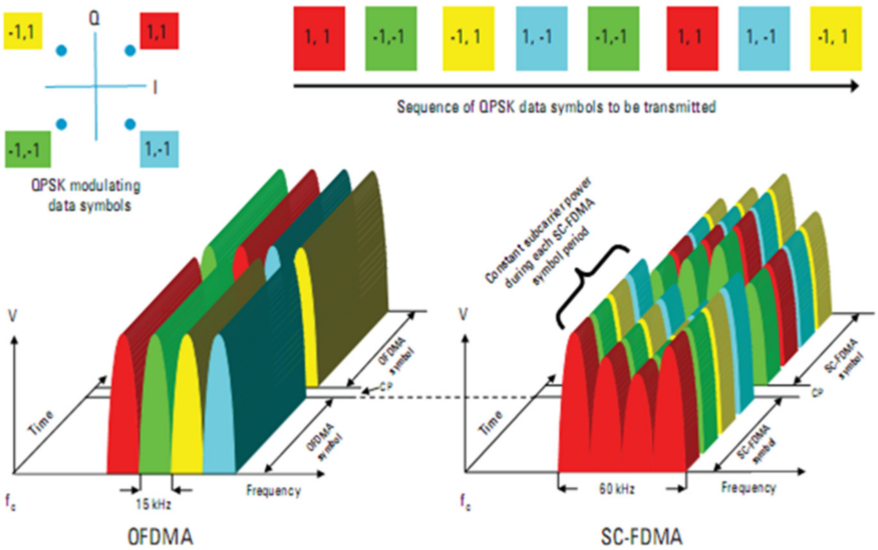


*Figure 2.1.1.2-1 – SC-FDMA*

### 2.1.2 Upper Layers

In this section, we give a brief description of the levels above the physical layer. In LTE, the radio interface protocol stack consists in:

- Medium Access Control MAC;
- Radio Link Control RLC;
- Packet Data Convergence Protocol PDCP;
- Radio Resource Control RRC.

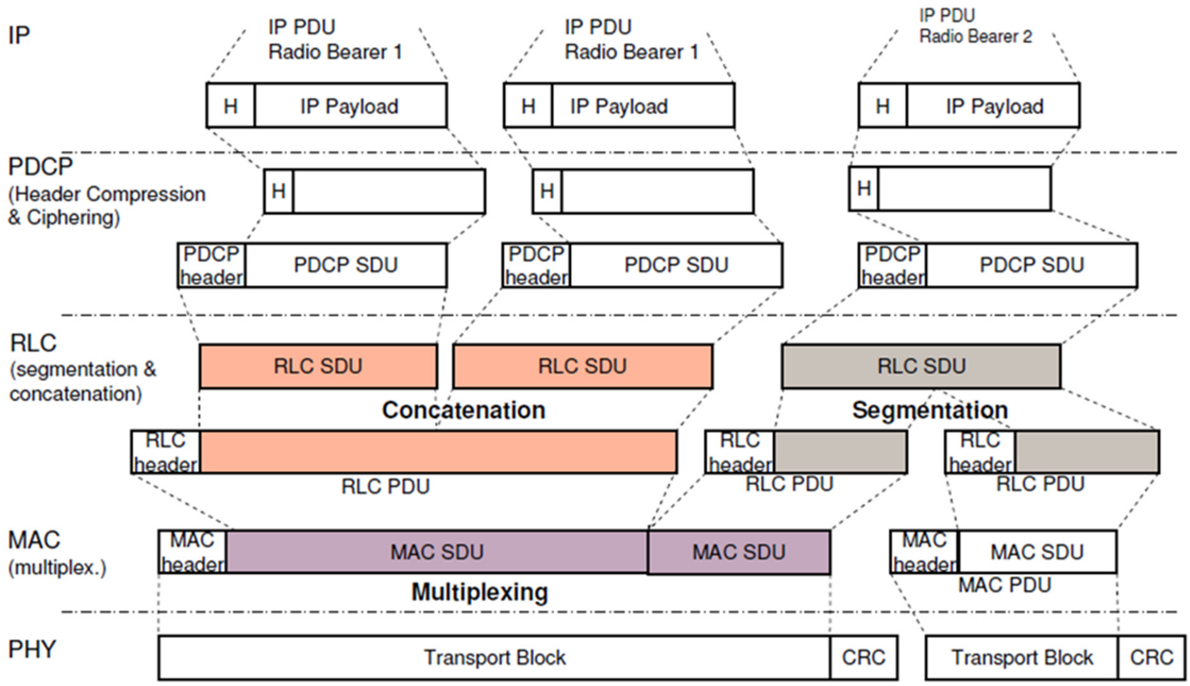


*Figure 2.1.2-1 – LTE Protocol Stack (3GPP)*

### 2.1.2.1 MAC Layer

In the following, we presents MAC layer's main functionality.

- Dynamic scheduling of radio resources: it determines the UEs that can be served during the i-th Transmission Time Interval (TTI) and on which RB they have to transmit.
- Generation of Transport Blocks by multiplexing of PDUs coming from upper layers.
- HARQ (Hybrid Automatic Repeat Request) management: MAC layer implements a Stop&Wait (S&W) retransmission protocol, in which the PDU transmission starts only after the transmitter receives an acknowledgement of the occurred transmission by the receiver. In LTE, in order to avoid deadlock situations in this process, an N-channel variant is introduced, leading to a maximum of N = 8 process operating in parallel.

In each TTI the UE report the perceived channel quality, in form of CQI, in order to evaluate the Modulation and Coding Scheme (MCS) to apply; the eNodeB respond assigning a priority level for each UE and then scheduling for each of them the radio resources. This process is valid for both downlink and uplink channels. Several scheduling algorithms can be implemented in LTE: in the following, we present the most common of them.

*Round Robin (RR) Scheduler*

RR scheduler allows the UE to access the resources in circular order, carrying an equal access opportunity for all of them. It offers a great fairness and a good bandwidth utilization, but provides a maximum throughput worse than the one offered by the other algorithms. It is used mostly in scenarios that do not require high speed.

*Proportional Fair (PF) Scheduler*

PF scheduler works by scheduling the user when the instantaneous channel quality is better with respect to its condition over time. It represents a tradeoff between the maximum average throughput and the user fairness. Moreover, PF scheduling improves multi-user diversity by scheduling high channel quality during different time slots.

*Best CQI Scheduler*

Best CQI scheduler assigns priority on the process to the users that have higher channel quality. Consequently, it offers better resources allocation to the users that are near the Base Station while those that are located at the cell edge have less probability of getting access to the shared resources.

#### 2.1.2.2 RLC Layer

Three operational setting are available for RLC layer:

1. *Acknowledged Mode (AM)*: RLC delivers PDU to higher layer without errors, implementing an ACK/NACK message transmission in order to communicate the "Status Report" for each PDU, depending on with there will be the necessity to retransmit them or not;
2. *Unacknowledged Mode (UM)*: since in this case there are no ACK/NACK messages and consequently also retransmissions, the PDU is always sent to the upper layer even if it is received with errors;
3. *Transparent Mode (TM)*: it works as a buffer for PDU transmission, so there are not overheads and it allows neither retransmission nor error recognition.

Although this error management mechanism handled by RLC, in general error-free delivery is handled by HARQ at MAC level. In case of HARQ failure, RLC layer has the task of guaranteeing the correct transmission.

**2.1.2.3 PDCP Layer**

PDCP layer provides the upper layer with Signaling Radio Bearer SRB (for Control Plane) and Data Radio Bearer DRB (User Plane). This layer manages the following aspects:

- PDU sequence numbering;
- integrity protection for signaling messages;
- compression of the protocol overhead through Robust Header Compression (ROHC) in order to improve transmission efficiency.

**2.1.2.4 RRC Layer**

RRC interface represents the overall air interface behavior: it controls the communication between UE and the node at IP level. It is mainly responsible for the radio resource management and lower layers configuration. In LTE, at RRC level an UE can be assumed in two different states, as described in the following.

1. *RRC_IDLE state*: the UE listens to the paging channel, reads system information (MIB and SIB), checks nearby cells and selects the cell it wants to camp on; all these procedures are optimized to ensure low power consumption in this state.
2. *RRC_CONNECTED state*: data transmission with the core network is allowed; the UE monitors the downlink channels to determine whether he should send and receive packets.

We can summarize the main functionalities of the RRC layer in the following way.

- *Broadcasting of System Information* - the UE reads system information in order to check the network status and obtain the parameters needed to access the core network. The main system information message, the *Master Information Block MIB,* reports the most significant system parameters such as frequency bandwidth and channels configurations. The remaining information are reported by in other messages named *System Information Blocks SIB*. In LTE they are generally grouped as:

  1. *SIB1* – cell access information and scheduling of the others SIB;
  2. *SIB2* – physical channels and signals radio configuration (PRACH, PDSCH, PUCCH, PUSCH, SRS);
  3. *SIB3* – information for inter-frequency and intra-frequency Cell Re-selection;

4. *SIB4* – specific information for intra-frequency Cell Re-selection among LTE frequencies;
5. *SIB5* – specific information for inter-frequency Cell Re-selection among LTE frequencies;
6. *SIB6 and SIB7* - specific information to control the Cell Re-selection for inter-RAT respectively towards UTRAN and GERAN;
7. *SIB8-13* – dedicated scope information (i.e. home eNB search).

- *Cell Selection and Re-Selection* - in LTE the node assigns to each UE that camp on the cell an access priority order. If the UE receives from a specific cell or frequency highest priority order it does not make further measures until the signal level of the serving cell is higher than a threshold value. If the measured priority order is lower, the UE needs to search a higher priority opportunity.
- *RRC Connection Establishment* – the node assigns radio resources to the UE so that it can switch to the RRC_CONNECTED mode.
- *Paging*: awakes the UE in IDLE mode, in order to notify the arrival of incoming calls or of an update of the System Information.
- *Measurement Control and Reporting*: parameters needed to allow the UE start one or more measures.

### 2.1.3 Frequency Allocation

In TS 36.104, 3GPP defines the LTE operation bands. In the following table, for each band is specified the duplex mode and the possibility to use the band in Carrier Aggregation mode.

| *Band* | *Duplex Mode* | *Uplink (MHz)* | *Downlink (MHz)* |
|---|---|---|---|
| 1 | FDD | 1920 – 1980 | 2110 – 2170 |
| 2 | FDD | 1850 – 1910 | 1930 – 1990 |
| 3 | FDD | 1710 – 1785 | 1805 – 1880 |
| 4 | FDD | 1710 – 1755 | 2100 – 2155 |
| 5 | FDD | 824 – 849 | 869 – 894 |
| 6 | FDD | 830 – 840 | 875 – 885 |
| 7 | FDD | 2500 – 2570 | 2620 – 2690 |
| 8 | FDD | 880 – 915 | 925 – 960 |
| 9 | FDD | 1749.9 – 1784.9 | 1844.9 – 1879.9 |
| 10 | FDD | 1710 – 1770 | 2100 – 2170 |

| | | | |
|---|---|---|---|
| 11 | FDD | 1427.9 – 1447.9 | 1475.9 – 1495.9 |
| 12 | FDD | 699 – 716 | 729 – 746 |
| 13 | FDD | 777 – 787 | 746 – 756 |
| 14 | FDD | 788 – 798 | 758 – 768 |
| 17 | FDD | 704 – 716 | 734 – 746 |
| 18 | FDD | 815 – 830 | 860 – 875 |
| 19 | FDD | 830 – 845 | 875 – 890 |
| 20 | FDD | 832 – 862 | 791 – 821 |
| 21 | FDD | 1477.9 – 1462.9 | 1495.9 – 1510.9 |
| 22 | FDD | 3410 – 3490 | 3510 – 3590 |
| 23 | FDD | 2000 – 2020 | 2180 – 2200 |
| 24 | FDD | 1626.5 – 1660.5 | 1525 – 1559 |
| 25 | FDD | 1850 – 1915 | 1930 – 1995 |
| 26 | FDD | 814 – 849 | 859 – 894 |
| 27 | FDD | 807 – 824 | 852 – 869 |
| 28 | FDD | 703 – 748 | 758 – 803 |
| 29 | FDD / CA | | 717 – 728 |
| 30 | FDD | 2305 – 2315 | 2350 – 2360 |
| 31 | FDD | 452.5 – 457.5 | 462.5 – 467.5 |
| 32 | FDD / CA | | 1452 – 1496 |
| 33 | TDD | 1900 – 1920 | 1900 – 1920 |
| 34 | TDD | 2010 – 2025 | 2010 – 2025 |
| 35 | TDD | 1850 – 1910 | |
| 36 | TDD | | 1930 – 1990 |
| 37 | TDD | 1910 – 1930 | 1910 – 1930 |
| 38 | TDD | 2570 – 2620 | 2570 – 2620 |
| 39 | TDD | 1880 – 1920 | 1880 – 1920 |
| 40 | TDD | 2300 – 2400 | 2300 – 2400 |
| 41 | TDD | 2496 – 2690 | 2496 – 2690 |
| 42 | TDD | 3400 – 3600 | 3400 – 3600 |
| 43 | TDD | 3600 – 3800 | 3600 – 3800 |
| 44 | TDD | 703 – 803 | 703 – 803 |
| 45 | TDD | 1447 – 1467 | 1447 – 1467 |
| 46 | TDD | 5150 – 5925 | 5150 – 5925 |
| 65 | FDD | 1920 – 2010 | 2110 – 2200 |
| 66 | FDD | 1710 – 1780 | 2110 – 2200 |
| 67 | FDD / CA | | 738 – 758 |

| | | | |
|---|---|---|---|
| 68 | FDD | 698 – 729 | 753 – 758 |
| 69 | FDD / CA | | 2570 – 2620 |
| 70 | FDD | 1695 – 1710 | 1995 – 2020 |

*Table 2.1.3-1 - LTE frequency bands from 3GPP TS 36.104*

## 2.2 NB-IoT: overview

One of the main features of Machine Type Communication is the large number of capabilities. For example, devices for fleet tracking have to evaluate a small amount of data while performing many handovers, whereas devices such as surveillance cameras have to deliver many data in Uplink while being almost stationary. Yet another class of devices has other different capabilities: devices for meter reading like water, electricity and gas consumption are often stationary (thus they have no need for handovers), and they sent only small amount of data, which is even not delay sensitive, due to the large time period they use in transmission. However, the number of this kind of devices may become quite big, even up to high order of magnitude if we consider a dense urban scenario. Due to this huge amount of required devices, they have to be in low cost range. Furthermore, these MTC devices are often placed and installed without power supply: they need to run completely on battery, and the battery lifetime have to be sufficiently extended in order to guarantee an adequate working time to the devices. In fact, change the battery may be very expansive and in some cases, the battery lifetime is often the lifetime of the whole device. So an optimized power consumption becomes essential for a proper operation. Yet, the coverage in the working place of these devices is quite poor, so that it has to be significantly improved, up to 23dB may be necessary. The first 3GPP specification of NB-IoT focuses on this class of devices. In this way, we can describe the following list of specific requirements for NB-IoT:

- minimization of the signaling over the radio interface;
- improvement of battery life by minimizing the power consumption;

- support of both IP and non-IP data transmission;
- improvement of the system security.

Many features of LTE and LTE-Advanced are not supported in NB-IoT in order to satisfy these requirements: we will widely describe the divergence between NB-IoT and LTE in section 2.3. Cat-NB1 is the category of UEs that support NB-IoT technology.

### 2.2.1 Network

In Cellular Internet of Things (CIoT) two optimization for EPS are defined, in order to send data to an application: the *User Plane CIoT optimization* and the *Control Plane CIoT optimization.*

1. *User Plane CIoT optimization* is built for infrequent transmissions of small data packets. In this case, the transmission of uplink data is due from the eNB (CIoT RAN) to the MME. Then data can be transferred via Serving Gateway (SGW) either to the Packet Data Network Gateway (PGW), or to the Service Capability Exposure Function (SCEF). Finally, data are forwarded to the application server (CIoT Services). The transmission of downlink data follows the same path but in opposite direction. The main feature of this solution is that, since no data radio bearer is set up, data are sent on the signaling radio bearer. Note that the SCEF can be used only for transmission of non-IP data over control plane.
2. In *Control Plane CIoT optimization* data transfer of both IP and non-IP data follows the conventional path, over data radio bearers through the SGW and PGW, to the CIoT application services.

*Figure 2.2.1–1* shows the general structure of both these optimizations

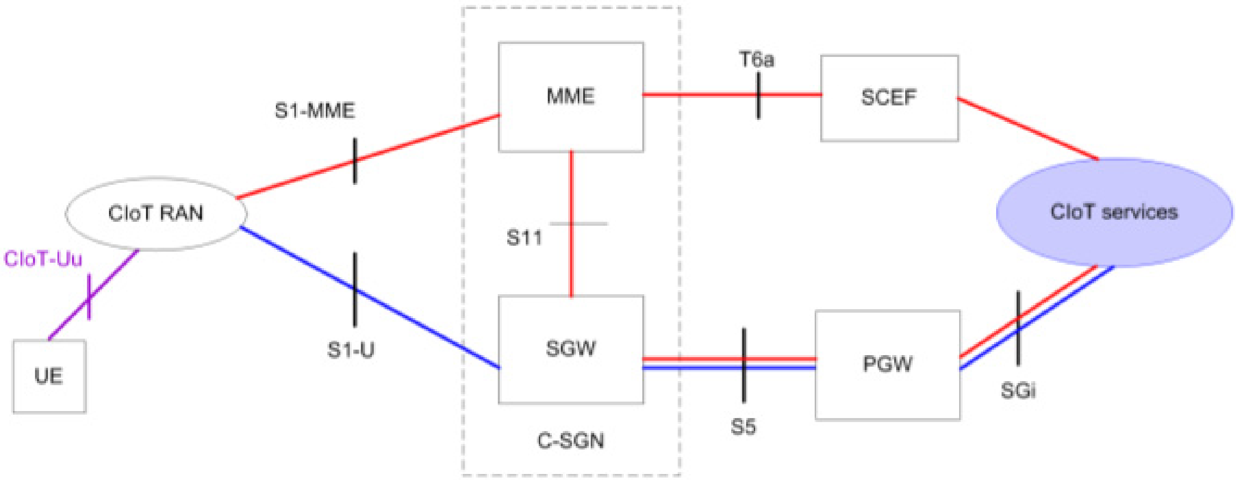


*Figure 2.2.1-1 – Control Plane (red) and User Plane CioT EPS optimization (Narrowband Internet of Things, Rohde & Schwarz)*

Access network in NB-IoT has the same structure as LTE: the eNBs are connecter to the MME and the SGW through S1 interface. X2 interface between two nodes allows an UE resuming fast after it gone to the idle state (there is no handover).

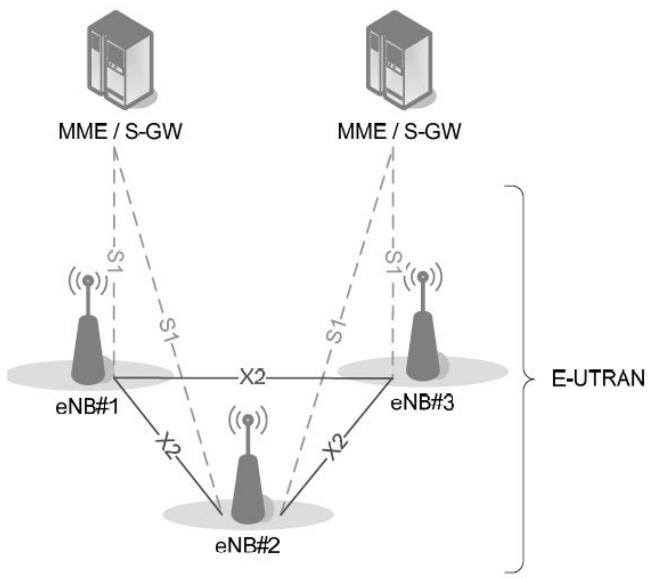


*Figure 2.2.1-2 – Access network architecture in NB-IoT*

In addition, the frequency bands in NB-IoT are defined in the same way as LTE. In our case study, we will consider the frequency band 20, in uplink in the range of 832 - 864 Mhz.

| 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 - 864 | 791 - 821 |
| 26 | 814 - 849 | 859 - 894 |
| 28 | 703 - 748 | 758 - 803 |
| 66 | 1710 - 1780 | 2110 - 2200 |

*Table 2.2.1-1 – NB-IoT frequency bands*

### 2.2.2 Physical Layer

NB-IoT work over a single LTE Physical Resource Block (PRB) with 180 kHz bandwidth. The 180 kHZ bandwidth allows the coexistence with LTE inside the standard 200 kHz GSM bandwidth since at both side of a PRB there is a guard band of 10 kHz. Three different operation mode are available:

1. *Stand-alone operation* using a dedicated carrier among the currently used GSM frequencies;

2. *In-band operation* using one resource block within an LTE carrier;

3. *Guard band operation* leveraging one of the unused resource blocks within an LTE carrier's guard band.

In *Figure 2.2.2–1* all the descripted operation modes are presented.

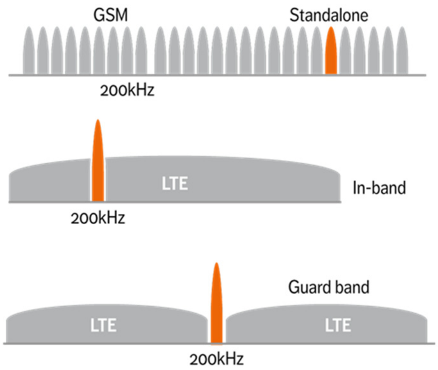


*Figure 2.2.2-1 – NB-IoT operation modes*

In case of in-band operation mode, only determined frequencies are allowed to be used for NB-IoT cell connection: the table below shows the indices of all the resource blocks available.

| LTE system bandwidth | 3 MHz | 5 MHz | 10 MHz | 15 MHz | 20 MHz |
|---|---|---|---|---|---|
| LTE PRB indices for NB-IoT synchronization | 2, 12 | 2, 7, 17, 22 | 4, 9, 14, 19, 30, 35, 40, 45 | 2, 7, 12, 17, 22, 27, 32, 42, 47, 52, 57, 62, 67, 72 | 4, 9, 14, 19, 24, 29, 34, 39, 44, 55, 60, 65, 70, 75, 80, 85, 90, 95 |

*Table 2.2.2-1 – Allowed LTE PRB indices for NB-IoT in in-band operation mode (Narrowband Internet of Things, Rohde and Schwarz)*

Note that there is no RB dedicated to NB-IoT in LTE with 1.4 Mhz bandwidth. Moreover, in order to avoid a conflict between NB-IoT and LTE, the inner 6 resource blocks of the LTE bandwidth are never used since these are dedicated to LTE synchronization signals.

One of the most important objective of NB-IoT is the expansion of coverage compared to the LTE case: the purpose is to increase the Maximum Coupling Loss (MCL) of 20 dB compared to the GSM. This coverage enhancement can be reached also thanks to the 180 kHz NB-IoT bandwidth: the node maintains the same transmission power as in LTE case (43 dBm) but concentrates it in a reduced frequency interval. This results in an higher Power Spectral Density (PSD) that allows the node to reach higher covered distance with respect to the GSM case. We must define three different Coverage Enhancement (CE) level: CE0, CE1 and CE2. CE0 represent the standard LTE coverage level, while in CE1 and CE2 cases some of the devices that would be out of coverage in LTE, are properly served by the network node. While in LTE a device results on coverage up to MCL = -144 dBm, in NB-IoT this lower bound has to be upgraded to MCL = -164 dBm. Among the possible implementation techniques of these extra-coverage levels, we choose to use in our case study the repetitions of data in uplink. For different CE levels, the UE will choose a different number of repetitions: in CE0, since we are in standard LTE conditions, the UE has not to repeat the data. In CE1 the UE would be out of LTE coverage, then it needs to repeat the packets 2, 4, 8 or 16 times; finally, in CE2, we have the worst channel conditions, so the UE must repeat the TB 16, 32 or 128 times. In NB-IoT, the user is able to estimate the coverage level in which is located according to the following operating principle:

1. UE send the DMRS (Demodulation Reference Signals) to the EnodeB;
2. EnodeB send back to the UE the DCI (Downlink Control Information) communicating to the user what is the condition of its channel in uplink;
3. According to the DCI, the UE estimate its CE Level and the relative number of repetitions.

With the increasing of the repetitions in transmitted packets and the consequent introduction of redundancy increases the possibility for the EnodeB to decode correctly the message send by the UE, but on the other hand decreases the capacity of the system.

In this work, we will try to figure out what is the right balance between capacity and repetitions, to ensure that the system works under optimal conditions.

#### 2.2.2.1 Downlink

In NB-IoT three downlink physical channels are defined. They are less than the LTE case, since Physical Multicast Channel is not defined for this technology:

- Narrowband Physical Broadcast Channel NPBCH;
- Narrowband Physical Downlink Control Channel NPDCCH;
- Narrowband Physical Downlink Shared Channel NPDSCH.

Transport channel are defined in the same way as in LTE. *Figure 2.2.2.1–1* illustrates the connection between the transport channels and the physical channels:

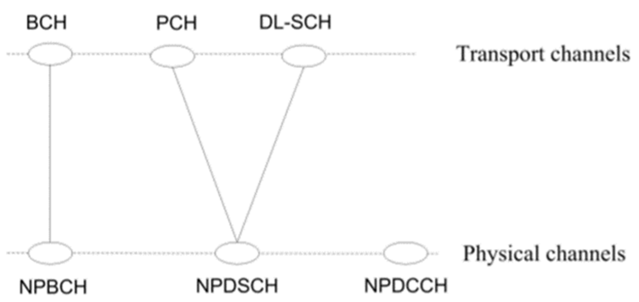


*Figure 2.2.2.1-1 – NB-IoT transport and physical channels (Narrowband Internet of Things, Rohde & Schwarz)*

Two downlink physical signals are defined:

- Narrowband Reference Signal NRS;
- Narrowband Primary and Secondary Synchronization Signals NPSS and NSSS.

The modulation applied on physical DL channels is always QPSK: the modulation order is much lower than LTE case, due to the reduced transmission performances requested by machine type communication. NB-IoT supports the operation with one or two antenna ports (AP0 and AP1). Each cell, like in LTE case, is qualified by a physical cell ID NcellID, defined in NSSS.

*Figure 2.2.2.1–2* describes the structure of a downlink time slot: OFDM is applied using a 15 kHz subcarrier spacing with normal cyclic prefix CP. As a result, the 180 kHz slot is divided into 7 OFDM symbols, each one composed of 12 subcarriers. A single subcarrier in one OFDM symbol is defined as a Resource Element (one square in figure).

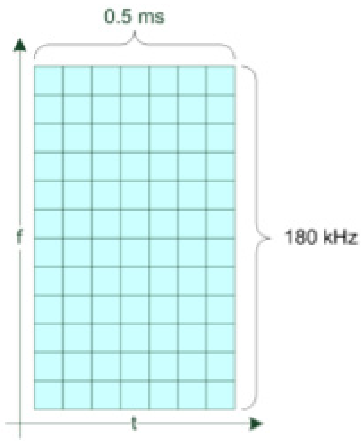


*Figure 2.2.2.1-2 – NB-IoT downlink subframe structure (Narrowband Internet of Things, Rohde & Schwarz)*

In time domain, the overall time slot occupies 0,5 ms. Two slots are summed up into a subframe of 1 ms, and 10 subframes into a radio frame of 10 ms, as in LTE.

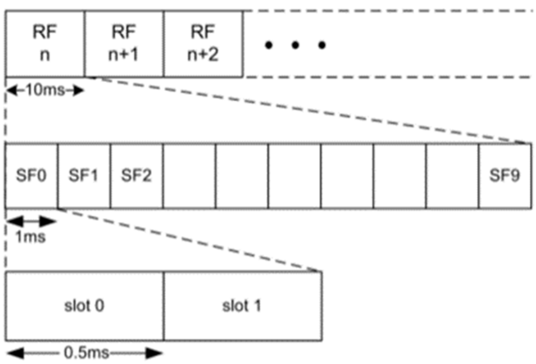


*Figure 2.2.2.1-3 – Frame structure for NB-IoT for DL and UL with 15 kHz subcarrier spacing (Narrowband Internet of Things, Rohde & Schwarz)*

Now we give a brief description of the physical structures of narrowband physical signals and channels.

*Narrowband Reference signal NRS*

NRS is transmitted in all subframes used for broadcast or dedicated data transmissions. Depending on the transmission mode, it can be either scheduled on one or two antenna ports: both cases are represented in *Figure 2.2.2.1–4* (AP0 in blue and AP1 in magenta):

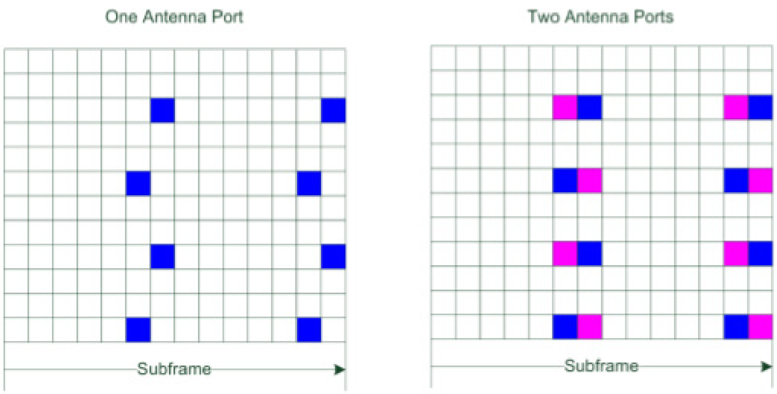


*Figure 2.2.2.1-4 – CRS mapping for one and two antenna ports respectively (Narrowband Internet of Things, Rohde & Schwarz)*

NRS are created as Cell-specific Reference Signals (CRS) in LTE: in case of in-band operation mode, in which also CRS are transmitted, NRS are built in order to avoid overlap between these two reference signals.

*Synchronization Signals*

As in LTE, Prymary and Secondary Synchronization Signals allow the UE to synchronize first on frame and subrfame, in order to determine NcellID, ad to develop a time and frequency estimation. *Figure 2.2.2.1–5* describes the structure of both these signals: NPSS is represented in blue, NSSS in green. Resource elements in violets represents the slots dedicated to LTE CRS.

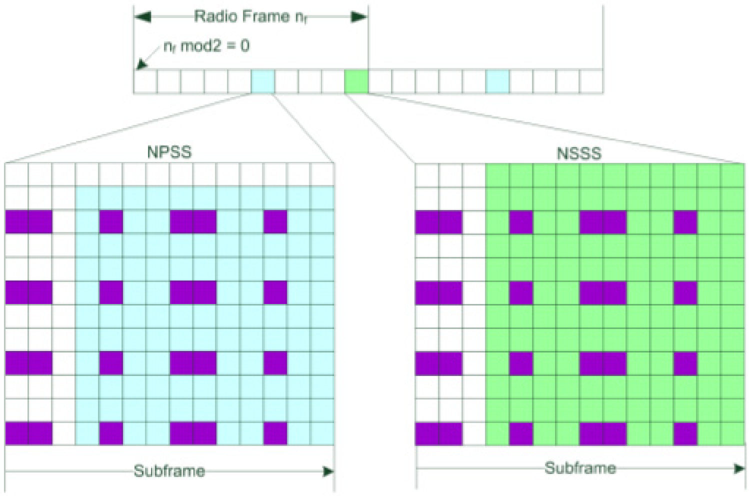


*Figure 2.2.2.1-5 – NPSS and NSSS mapping (Narrowband Internet of Things, Rohde & Schwarz)*

The first 3 OFDM symbols are left out because in in-band operation mode they are dedicated to PDCCH (while the UE synchronizes NPSS and NSSS it doesn't know the operation mode yet, so this choice is always done). NPSS is generated as a length-11 Zadoff-Chu sequence in frequency domain and is always transmitted in SF5 of each radio frame. NSSS is built as a length-131 Zadoff-Chu sequence in frequency domain and are transmitted in the last SF of each even number radio frame.

*Narrowband Physical Broadcast Channel NPBCH*

NPBCH is dedicated to the transmission of Narrowband Master Information Block MIB-NB: this signal has a 34 bit length and is transmitted every 640 ms. MIB-NB carries the following information:

- 4 bits for the most significant bits MSBs of the System Frame Number SFN;
- 2 bits for the two less significant bits LSBs of the hyper frame number;
- 4 bits for scheduling and size of SIB1-NB;
- 5 bits for the value tag of the system information;
- 1 bit indicating if access class bearing is applied;
- 7 bits for the operation mode;

- 11 spare bits reserved for future extensions.

In *Figure 2.2.2.1–6* NPBCH mapping to the subframes is shown: MIB-NB is split into 8 blocks. Each block is transmitted in the first subframe (SF0 in figure) and repeated in the first subframe of the next 7 radio frames: each block occupies a time interval of 80 ms, resulting in a complete MIB transmission of 640 ms.

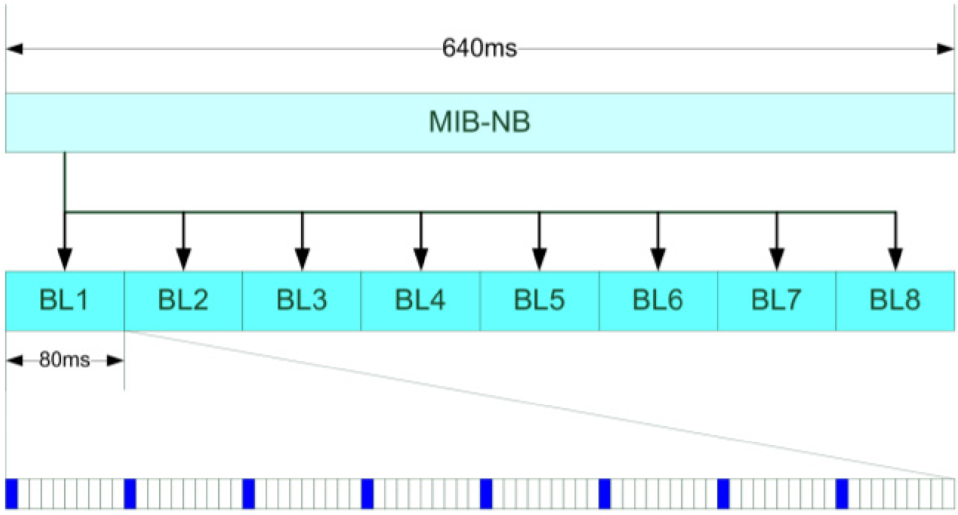


*Figure 2.2.2.1-6 – NPBCH mapping to subframes (Narrowband Internet of Things, Rohde & Schwarz)*

NPBCH is mapped in a single subframe around NRS and LTE CRS; again, first 3 OFDM symbols are left out to avoid conflicts with the LTE's control channel. *Figure 2.2.2.1-7* describes NPBCH mapping on a subframe, assuming four antenna port for LTE CRS and two for NRS.

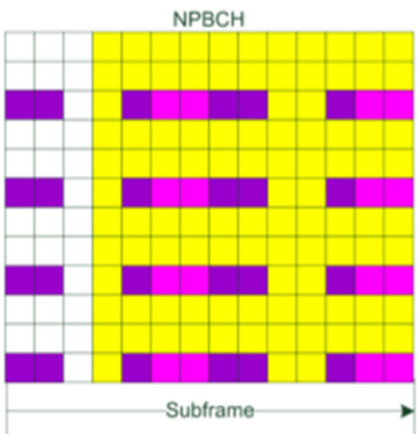


*Figure 2.2.2.1-7 – NPBCH mapping to a single subframe: NPBCCH resources are represented in yellow, NRS in magenta and LTE CRS in violet (Narrowband Internet of Things, Rohde & Schwarz)*

*Narrowband Physical Downlink Control Channel NPDCCH*

NPDCCH carries information about which UE is transmitting on NPDSCH, what frequency resource it is using in transmission and how often it transmits. In addition, NPDCCH carries uplink grants and other information like paging messages or system information update. *Figure 2.2.2.1-8* describes NPDCCH resource allocations in a single subframe, in case of one antenna port for LTE CRS and two for NRS.

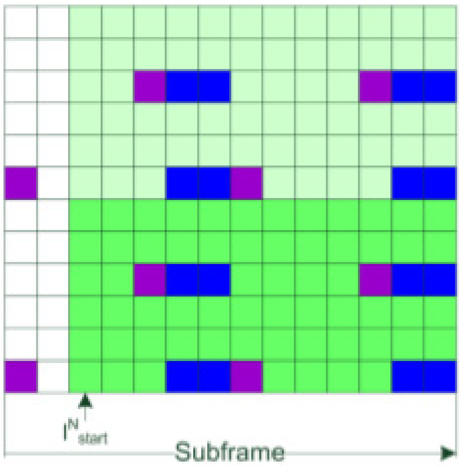


*Figure 2.2.2.1-8 – NPDCCH resources allocation in a subframe, in light and dark green; NRS in blue and LTE CRS in violet (Narrowband Internet of Things, Rohde & Schwarz)*

As shown in figure, each subframe contains two control channel elements NCCEs: NCCE0 and NCCE1. Their use depends on the format chosen:

1. *Format 0* uses a single NCCE (two of them can be transmitted within a subframe);
2. *Format 1* uses both NCCEs (single transmission in a subframe).

A parameter $l_{start}^{N}$ indicates the start OFDM symbol, in order to avoid collision with LTE control channel. NPDCCH also carries Radio Network Temporary Identifier RNTI assigned to each UE, one for random access (RA-RNTI), one for paging (P-RNTI) and a cell-specific identifier C-RNTI. Information carried by downlink control channel are grouped in Downlink Control Indicators (DCIs). Three DCI formats are defined in NB-IoT:

1. *DCI Format N0* – 23 bits, contains UL grants;
2. *DCI Format N1* – 23 bits, contains NPDSCH scheduling and information for RACH procedure;
3. *DCI Format N2* – 15 bits, contains paging and direct indications.

**Narrowband Physical Downlink Shared Channel NPDSCH**

NPDSCH is the channel dedicated to the transmission of downlink data. Its subframe structure is the same described for downlink control channel. The maximum transport size supported is of 680 bits. A transport block can be repeated $N_{Rep}$ times and its mapping spans over $N_{SF}$ subframes, starting from the OFDM symbol indicated by $I_{start}^{N}$: both $N_{Rep}$ and $N_{SF}$ are indicated in downlink DCI. This results in a frequency occupation of $N_{Rep} \cdot N_{SF}$ subframes for NPDSCH. All operation modes supports multi-carrier transmission. NPDSCH is also dedicated to the transmission of SIB1-NB: it is transmitted every 256 radio frames and can be repeated 4, 8 or 16 times. The radio frame on which NPDSCH transmission starts depend on the number of repetitions an on the NCellID.

### 2.2.2.2 Uplink

In uplink NB-IoT defines two physical channels and one physical signal, as follows:

- Narrowband Physical Uplink Shared Channel NPUSCH;
- Narrowband Physical Random Access Channel;
- Demodulation Reference Signal DMRS.

Note that in uplink, all data except for RACH transmission are sent over the NPUSCH (both data and control information). The connection between transport ad physical channels in uplink is depicted in *Figure 2.2.2.2-1*.

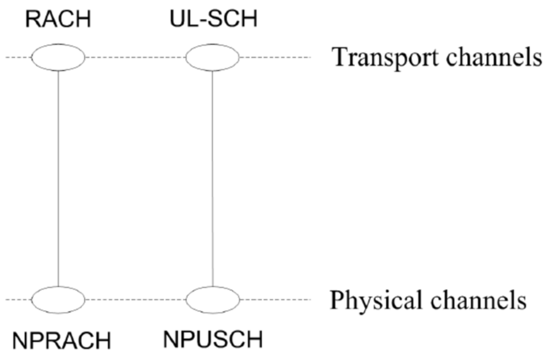


*Figure 2.2.2.2-1 – Physical and transport channels mapping (Narrowband Internet of Things, Rohde & Schwarz)*

Single Carrier Frequency Division Multiple Access SC-FDMA is applied. Two kinds of subcarrier spacing can be set: 3,75 kHz and 15 kHz. In case of 15 kHz subcarrier spacing, the uplink resource grid is the same described for downlink. For 3,75 kHz subcarrier spacing, a 180 kHz slot is composed of 48 subcarriers and 7 OFDM symbols, that in this case has four times the duration measured in the previous case. This leads to an overall slot duration of 2 ms.

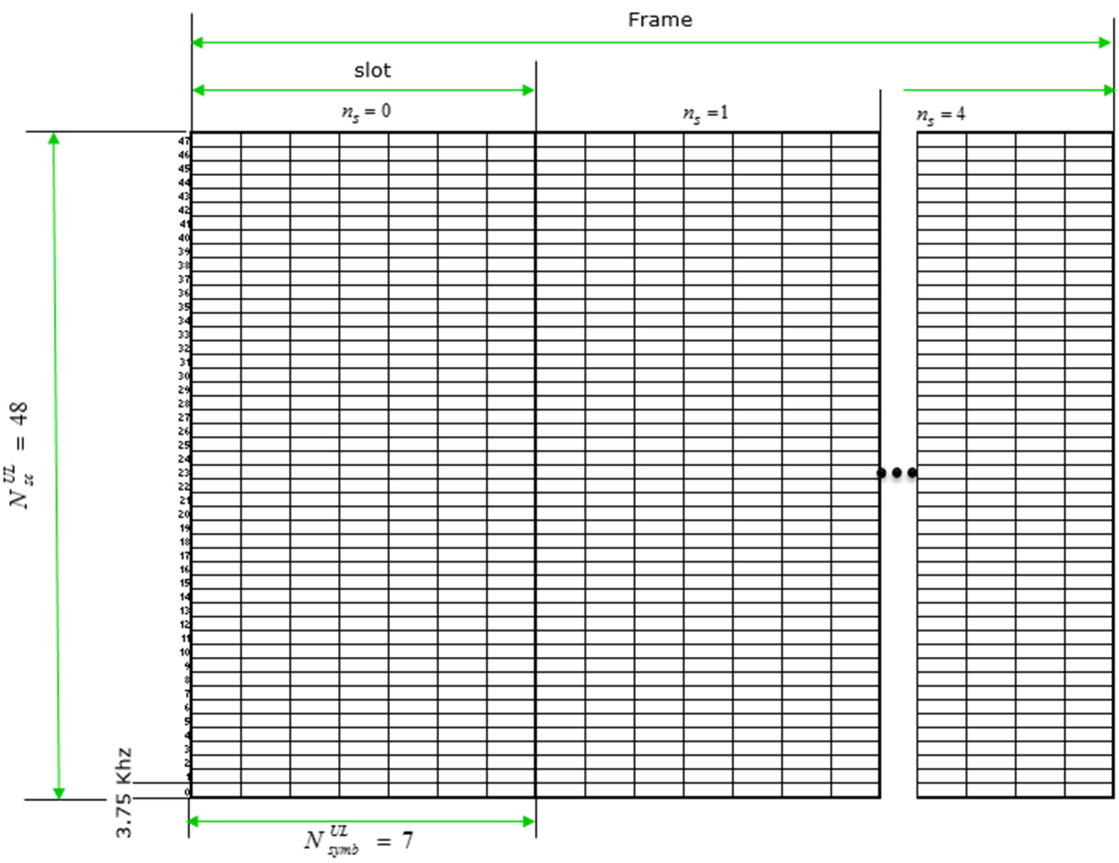


*Figure 2.2.2.2-2 – Uplink resource grid in case of 3,75 kHz subcarrier spacing*

**Narrowband Physical Uplink Shared Channel NPUSCH**

In NB-IoT, two formats are defined for uplink shared channel:

1. *NPUSCH Format 1*, for uplink transport channel data, with maximum TB size of 1000 bits;
2. *NPUSCH Format 2*, for Uplink Control Information UCI transmission.

A transport block can be divided in resource units: their definitions depends on the format and on subcarrier spacing.

For NPUSCH Format 1 and 3,75 kHZ spacing, a RU is composed of 1 subcarrier in frequency range and 16 slots in time range. If 15 kHz spacing for Format 1 several options have to be considered:

1. 1 subcarrier and 16 slots, resulting on a duration of 8 ms;
2. 3 subcarriers and 8 slots, resulting on a duration of 4 ms;
3. 6 subcarriers and 4 slots, resulting on a duration of 2 ms;
4. 12 subcarriers and 2 slots, resulting on a duration of 1 ms.

For RU with one subcarriers may be used both BPSK and QPSK modulation, while for all others RU QPSK is applied.

For NPUSCH Format 2, a RU always consists of 1 subcarrier and 4 time slots: consequently, in case of 3,75 spacing this leads on a duration of 8 ms, while in case of 15 kHz spacing the duration is equal to 2 ms. The modulation is always BPSK.

NPUSCH carries also DCI for uplink channel: DCI Format N0 contains UL grants, along with NPUSCH start time, number of repetitions, number of RUs used for a single transport block and parameters for frequency mapping. DCI contains also the MCS index and the transport block size. Contrary to DL case, there is always an acknowledgement in DL associated to an UL transmission.

**Demodulation Reference Signal DMRS**

In uplink, demodulation reference signals are sent multiplexed with data, so that they are only allocated in RUs dedicated to data transmission. In NB-IoT uplink is defined only for a single antenna port, so that there is no MIMO transmission. The number of SC-FDMA symbols reserved for DMRS transmission depends on NPUSCH format and subcarrier spacing. *Figure 2.2.2.2-3* shows DMRS allocation in case of NPUSCH Format 1, for 3,75 kHz and 15 kHz spacing respectively.

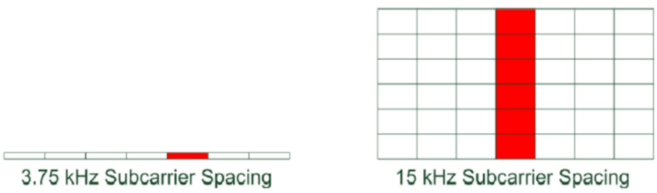


*Figure 2.2.2.2-3 – DMRS Format 1 resource allocation (Narrowband Internet of Things, Rohde & Schwarz)*

*Figure 2.2.2.2-4* shows DMRS allocation in case of NPUSCH Format 2, for 3,75 kHz and 15 kHz spacing respectively.


*Figure 2.2.2.2-4 – DMRS Format 2 resource allocation (Narrowband Internet of Things, Rohde & Schwarz)*

### 2.2.3 NPRACH and Random Access Procedure

Since Random Access procedure is trivial for the performance evaluation of a NB-IoT system, we reserve for this procedure and for the Random Access Channel a dedicated analysis. In the following, we first describes the physical structure of NPRACH, then we describe how the Random Access Procedure works, focusing our attention on the contention resolution. Finally, we give an estimation of the impact of the RACH collisions on the overall transmission.

#### 2.2.3.1 Narrowband Physical Random Access Channel

Narrowband Physical Random Access Channel NPRACH is a newly designed physical channel, different from the Physical Random Access Channel PRACH used in LTE since it uses a 1.08 MHz bandwidth, more than the bandwidth dedicated for NB-IoT Uplink channels. In NPRACH, a preamble is transmitted: it can be used by an UE to signal to the cell that it wants to access the network. We will describe the associated Random Access Procedure in the next paragraph. One preamble consist of 4 symbol groups, and each symbol group is composed by a cyclic prefix CP and 5 symbols. The following figure show an example of preamble symbol group.


*Figure 2.2.3.1-1 – Preamble symbol group (Narrowband Internet of Things, Rohde & Schwarz)*

Two preamble format are defined:

- *Format 0*: for cell radius up to 10 km, characterized by CP length $T_{CP} = 66.7\mu s$;
- *Format 1*: for cell radius up to 40 km, characterized by CP length $T_{CP} = 266.7\mu s$.

Each symbol is modulated on a 3.75 kHz tone with a symbol duration $T_{SEQ} = 1.333ms$, leading to a total length of $1.4ms$ for *Format 0* and $1.6ms$ for *Format 1*. One UE can read the preamble format to be used in the system information. The 4 symbol groups of the preamble are transmitted without gasps using frequency hopping on a maximum contiguous set of 12 subcarrier: each symbol group is transmitted on a different subcarrier. NPRACH resources are assigned in time and frequency separately for each CE group. NPRACH periodicity may be configured between 40 ms and 2.56 s. The start time of the NPRACH within a period is specified in system information, while repetitions and format determines the NPRACH end. In frequency range for NPRACH it's applied a subcarrier spacing of 3.75 kHZ: the random access channel resources occupy a contiguous set of 12, 24, 36 or 48 subcarriers.

According to NB-IoT features, to serve UEs in different coverage classes with different ranges of pathloss, the network can configure up to three different NPRACH configurations in a cell, associated to a different number of preamble repetition. So an UE can repeat a NPRACH preamble 1, 2, 4, 8, 16, 32, 64 or 128 times, using the same transmission power on each repetition. To estimate its coverage level an UE measures its downlink received signal power and consequently transmit the preamble according to the measured configuration. Here we show an example of preamble repeated at least 4 times: the blue rectangles represent the symbol groups, hence a preamble repetition consists of four rectangles.

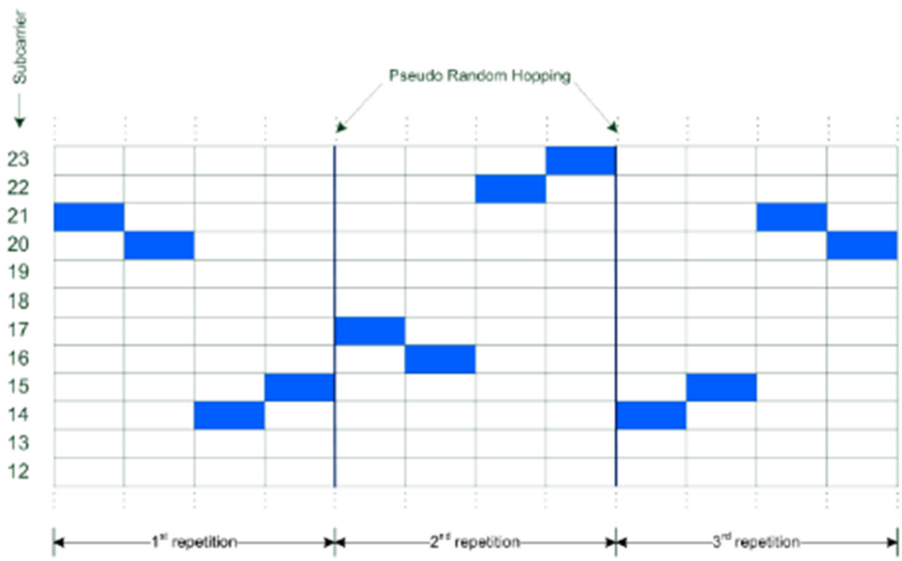


*Figure 2.2.3.1-2 – Preamble sequence in a frequency range between subcarrier 12 and 23 (Narrowband Internet of Things, Rohde & Schwarz)*

Among the 12 available subcarriers the UE choose one subcarrier for the transmission of the first symbol group. Then, the next 3 symbol groups of the first preamble repetition are scheduled by an algorithm which depends only on the location of the first one. Finally, a pseudo-random hopping algorithm selects the subcarrier for the transmission of the first group of the next repetition. The inputs of this algorithm are the NCellID and the repetition number. As for the first repetition, the subcarrier selection of the 3 remaining symbol groups depends only on this choice. Thanks to the frequency hopping algorithm, different choice of the first subcarrier leads to schemes that never overlap. The preamble is built over a Zadoff-Chu sequence that depends on the subcarrier location.

#### 2.2.3.2 Random Access Procedure

In NB-IoT, an UE start a Random Access Procedure to achieve initial access when it needs to establish a radio link. One main objective of random access is to obtain uplink synchronization, which is trivial for maintaining uplink orthogonality. The Random Access Procedure is always contention based and has the same message flow implemented in LTE, with different parameters:

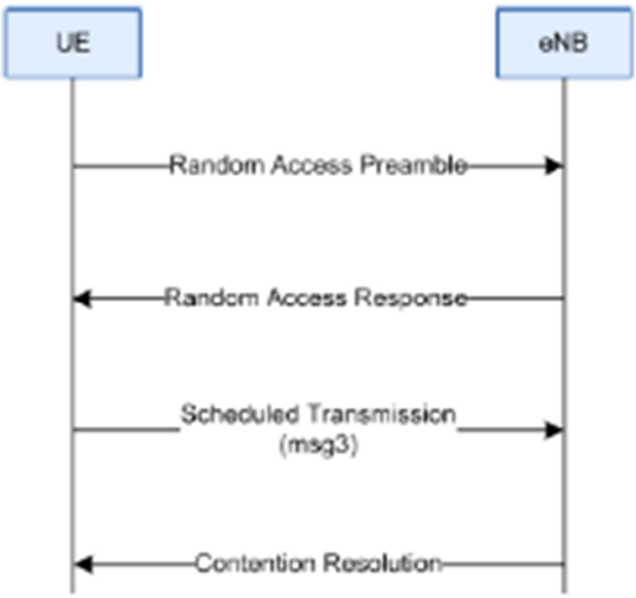


*Figure 2.2.3.2 – RACH procedure: message flow (Narrowband Internet of Things, Rohde & Schwarz)*

Each of the message represented in figure is repeated according to the coverage level measured by the UE. The RACH procedure always starts with the transmission of a *Random Access Preamble*, as described before. Upon transmission of the preamble, the UE depending on the transmission time evaluates its RA-RNTI (Random Access - Radio Network Temporary Identifier) and then reads the DCI Format N1, sent in the PDCCH from the EnB. Scrambling the DCI with the RNTI the UE finds the *Random Access Response (RAR)*: this message is contained in a Response Window, which starts 3 SFs after the last preamble SF. In case of RAR is not received, the UE knows that the preamble transmission was not successful and transmits another one: this process is valid up to a maximum number of repetitions, depending on the CE level. If the UE reaches this maximum number of preamble transmission without obtaining the RAR, it proceeds to the next CE level if it is configured, or eventually reports a failure connection message to the RRC. Other relevant parameters contained in the RA Response are a time advance command and the UL grant for synchronization and transmission of *Message3 (msg3)*. This message is sent after the reception of the Random Access Response in order to start the contention resolution process. Once the contention is resolved, a *Contention Resolution* message is transmitted to the UE and the RACH procedure is successful completed. This last part of the procedure is done like in LTE, as we will see in the next section.

#### 2.2.3.3 Contention resolution

In this section, we show an example of the contention resolution process as implemented in LTE since the same processing flow is valid in NB-IoT. Suppose we have three UE, UE-A, UE-B and UE-C, which are powered on and initiates the Random Access Procedure at exactly the same time. Then suppose two of them (UE-A and UE-B) happen to pick the same preamble. This result in a RACH collision, that we suppose is in favor of UE-A. UE-C picks a different preamble so it has no problem in succeeding the procedure. The sequence diagram below describes in detail how the contention resolution process can solve this collision.

1. The devices synchronize with the downlink channel by decoding the Primary Synchronization Signal (PSS) and the Secondary Synchronization Signal (SSS): they achieve synchronization when both the signals are decoded.
2. The three UE download the Master Information Block (MIB) from the broadcast channel and the System Information Block (SIB) from the Uplink Shared Channel: SIB2 download contains parameter for initial access transmission.
3. The UE-A randomly selects a Preamble 1 from the set of sequences available in the cell. The preamble selection consist in a shift in the Zadoff-Chu code for the cell. UE-A transmits the chosen preamble on a RA channel: depending on the timing of the Preamble 1 transmission is specified an RA-RNTI 1 (Random Access-Radio Network Temporary Identifier) for the UE.
4. UE-B happens to select Preamble 1 (the same as UE-A) and transmits it at the same time: UE-B also assumes a RA-RNTI 1.
5. UE-C randomly chooses between the available preambles and it picks the Preamble 3. UE-C transmits it at the same time as UE-A and UE-B but, since Preamble 3 and Preamble 1 are orthogonal to each other, the node receives both of them.
6. Preambles processing:
    a. Processing of Preamble 1: the EnodeB detects the preamble transmission and estimates the uplink transmission timing of the UE, reading the RA-RNTI 1 from the timeslot number in which receives the Preamble 1. Therefore, the EnodeB assigns a C-RNTI 1 to the UE in subsequent messages;
    b. Processing of Preamble 3: the EnodeB detects the preamble transmission and estimates the uplink transmission timing of the UE, reading the RA-RNTI 3 from the timeslot number in which receives the Preamble 3. Therefore, the EnodeB assigns a C-RNTI 3 to the UE in subsequent messages.
7. The EnodeB assign resources via the PDCCH.

8. The EnodeB transmits the RA Response on the DL Shared Channel, including timing and uplink resource allocation for Preambles 1 and 3.
9. Processing of the RA Response:
   a. UE-A saves the C-RNTI 1 for Preamble 1, synchronizes and then can transmits data bursts to the EnodeB;
   b. UE-B wrongly believes that the RA Response is referred to it, since the RA-RNTI 1 and Preamble 1 match. UE-B has no way of understanding the mistake. He is continuing with the procedure even if he had been rejected. This situation will be solved in the Contention Resolution phase.
   c. UE-C saves the C-RNTI 1 for Preamble 1, synchronizes and then can transmits data bursts to the EnodeB normally. The Rest of Random Access Procedure is not shown in this flow.
10. Contention Resolution:
    a. UE-A picks a Random Number A as UE identity and send it to the EnodeB included in the RRC connection request. Then, starts the T300 timer and awaits the RRC Connection Setup message;
    b. UE-B picks a Random Number B as UE identity and send it to the EnodeB included in the RRC connection request. UE-B transmits on the same assignment and collides with the message sent by UE-A; its message will not be received correctly by the node since it is transmitting with a time advance not reserved for the UE (let's suppose it has been transmitted for a while after the UE-A). UE-B’s message is lost. However, UE-B starts the T300 timer and awaits the RRC Connection Setup message;
    c. The EnodeB accepts the transmission from the UE and signals a downlink assignment sending the RRC Connection Setup message addressed with the C-RNTI 1;
    d. UE-A and UE-B both receive the RRC Connection Setup message since it, is addressed with C-RNTI 1; this message also contains the Random Number A as the initial identity;

e. UE-A, recognizing its own identity, concludes that the RA was successful and send the RRC Connection Setup Completed message;
f. UE-B reads an identity different from Random Number B and recognizes it has lost out to another UE in the contention resolution.

11. UE-B reties the Random Access Procedure.

### 2.2.4 Power control

In uplink, the power transmitted by an UE depends on the number of repetition. In case of maximally two repetitions, the power on slot $i$ can be computed as:

$$P_{NPUSCH,c}(i) = min\begin{cases} P_{CMAX,c}(i) \\ 10log_{10}\left(M_{NPUSCH,c}(i)\right) + P_{0_{NPUSCH},c}(j) + \alpha_c(j) \cdot PL_c \end{cases}$$

where

$P_{CMAX,c}(i)$ : cell specific maximum transmit power on slot i (transmitted power may never exceed this threshold);

$M_{NPUSCH,c}(i)$ : depends on the subcarrier spacing and the bandwidth of the selected RU;

$P_{0_{NPUSCH},c}(j)$ : a combination of parameter signaled by the RRC, depends on whether the TB is for data on NPUSCH ($j$ = 1) or on RACH ($j$ = 2);

$PL_c$ : path loss, estimated by the UE;

$\alpha_c(j)$ : represents a way for the path loss $PL_c$, it is provided by RRC for NPUSCH Format 1, otherwise is fixed to 1.

In case of more than two repetitions, the transmitted power is given by $P_{CMAX,c}(i)$.

In downlink, transmitted power corresponds to NRS transmission power: its power is given by the node to the UE in order to estimate the path loss. For NPBCH, NPDCCH and NPDSCH it depends on the transmission scheme: in case on single antenna port, transmitted power is the same as for NRS, reduced by 3 dB.

### 2.2.5 Cell Access

Cell access procedure in NB-IoT follows the same flow as LTE case: an UE that wants to access the network first search a cell working at a certain frequency reads the network status in the SIB and then starts a random access procedure in order to obtain the connection. In addition, the protocol stacks are the same as for LTE, with optimized features for NB-IoT.

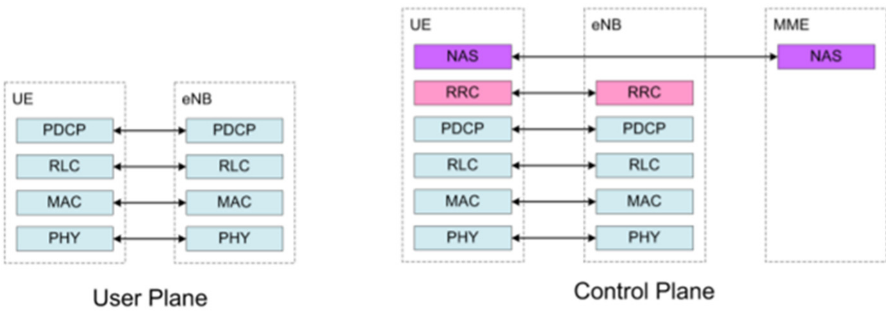


*Figure 2.2.5-1 – User Plane and Control Plane protocol stacks (Narrowband Internet of Things, Rohde & Schwarz)*

The System Information Blocks defined for NB-IoT are a subset of the ones defined for LTE. We describe the overall set of SIB along with the correspondent carried information.

- *MIB-NB*: principal information message, required to receive other SIB;
- *SIBType1-NB*: cell access and selection, scheduling of the others SIB;

- *SIBType2-NB*: radio resource configuration;
- *SIBType3-NB*: inter- frequency and intra-frequency cell re-selection;
- *SIBType4-NB*: information on neighboring cells, used for intra-frequency cell re-selection;
- *SIBType5-NB*: information on neighboring cells, used for inter-frequency cell re-selection;
- *SIBType14-NB*: access barring parameters;
- *SIBType16-NB*: GPS time and Coordinated Universal Time (UTC) information.

Note that the UE is not expected to read System Information during the RRC_CONNECTED state: SIB and MIB acquisition is done always in RRC_IDLE state. As seen before, MIB-NB and SIB1-NB are broadcasted on NPBCH, while the remaining SIB information, as for LTE case, are grouped into SI messages and transmitted in separate SI windows. Within a single SI window, several SI messages are sent over 2 or 8 consecutive subframes in downlink, and repeated several times, depending on the coverage level.

#### 2.2.5.1 Cell Selection and Mobility

When an UE tries first to access the network, it has to select the cell it wants to be served. In order to find a cell, the UE measures the quality and the power level of the NRS and then compares this value with specific thresholds provided by the SIB-NB. If both these values are under the thresholds, the UE must be considered in coverage of the cell and is able to camp on it. In case of this condition is not satisfied, the UE starts a cell re-selection procedure, comparing the NRS parameter with thresholds associated to other cells. Cell re-selection in RRC_IDLE state is defined both for inter-frequency cells, referring to two 180 kHz carriers within the same LTE carrier (in in-band operation mode), and intra-frequency cells, in case of different LTE carriers. Even if the MTC devices considered in our case study have fixed position, in general we have to consider how NB-IoT behaves with the mobility of the UE. Since this technology is designed to support transmission of infrequent and short messages, the handover procedure during RRC_CONNECTED state is not required. Then, if the UE needs to change the cell it is camping on, it has first to go to the RRC_IDLE state and re-search another cell therein. Contrary to LTE case, there is no frequency priority in cell re-selection. Moreover, when an UE leaves the RRC_CONNECTED state and pass to the RRC_IDLE state, it reads in the *RRCConnectionRelease* message the frequency on which it has to search a suitable cell. Then, if this search doesn’t lead to a successful connection, it may try to find a suitable cell on another frequency.

#### 2.2.5.2 Connection Control

Since handover is not required for NB-IoT, the RRC state model is very simple: there are only two states, RRC_IDLE and RRC_CONNECTED.

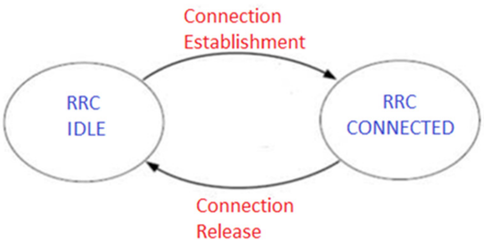


*Figure 2.2.5.2-1 – RRC states model*

*RRC Connection Establishment* has the same message flows as for LTE:

1. the UE send to the node an *RRCConnectionRequest* message to communicate that it wants to connect to the network, indicating its capabilities to support multi-tone transmission and multi-carrier support;

2. the eNB responds with an *RRCConnectionSetup* message, providing configuration of signaling radio bearer (SRB1), one or two data radio bearers (DRB) and the protocols;

3. the UE concludes the procedure sending the *RRCConnectionSetupComplete* indicating the selected PLMN and MME.

*Figure 2.2.5.2-2* shows a representation of the described connection establishment procedure:

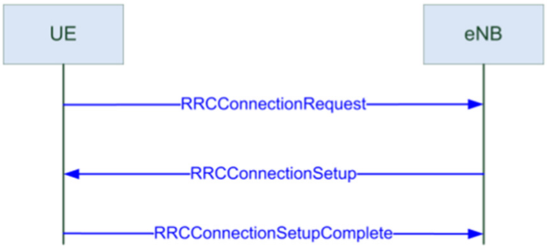


*Figure 2.2.5.2-2 – RRC Connection Establishment procedure (Narrowband Internet of Things, Rohde & Schwarz)*

When the transmission ends and the UE has to leave the connection, the node starts *RRC Connection Release* once this procedure ends, the UE enters the RRC_IDLE state.


*Figure 2.2.5.2-3 – RRC Connection Release procedure (Narrowband Internet of Things, Rohde & Schwarz)*

The RRC connection can also be suspended upon RRC release and UE context be stored; consequently, the RRC connection can be resumed using the stored UE context. This allows the UE to obtain again the connection optimizing the message flows since he knows yet parameters characterizing his previous connection. This saves considerable signaling overhead for the transmission of small and infrequent data packets. Upon reception of *RRCConnectionResumeRequest* the node determine if the connection can be resumed or not. In the first case, it send to the UE the *RRCConnecctionResume* message and allows the reconnection.

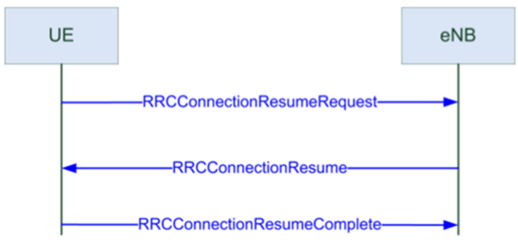


*Figure 2.2.5.2-4 – RRC Connection Resume procedure (Narrowband Internet of Things, Rohde & Schwarz)*

In case of the request is rejected, the UE has to switch to the standard connection procedure, as shown in the figure below:

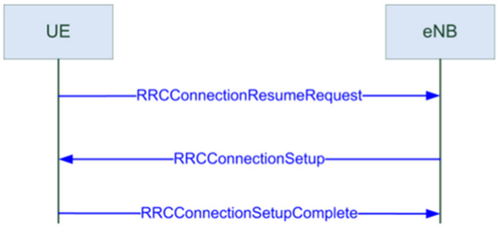


*Figure 2.2.5.2-5 – RRC Connection Resume request rejected (Narrowband Internet of Things, Rohde & Schwarz)*

### 2.2.6 Data transfer

Since we are analyzing a smart metering system, we will focus our attention first on Uplink data transmission. Because of the coverage enhancement reached by NB-IoT with respect to the LTE case, a transport block in uplink can be repeated several times by the UE. The DCI format N0 indicates UL grants for transmission over NPUSCH, along with the Sounding Reference Signals: depending o the reception of these signals the UE can establish its coverage level and consequently the number of repetition. The arrangement of the repetitions, as well as the repetition number, depends on the number of subcarriers for a resource unit and the subcarrier spacing. In case of 15 kHz subcarrier spacing a RU is composed by 3 subcarriers over 8 slots: as a consequence a transport block is transmitted on two Rus. *Figure 2.2.6-1* represents the transmission of a transport block, named Test Word (TW), repeated 8 times. $T_i$ denotes the i-th slot of the first RU and $W_j$ the j-th slot of the second RU. First of all the two slots are transmitted and repeated three more times (resulting on 4 repetitions); then, this procedure is applied every pair of slots, until we have 4 repetitions of the transport block TW. Finally, the transmission sequence is repeated once again, leading to the 8 repetitions requested.

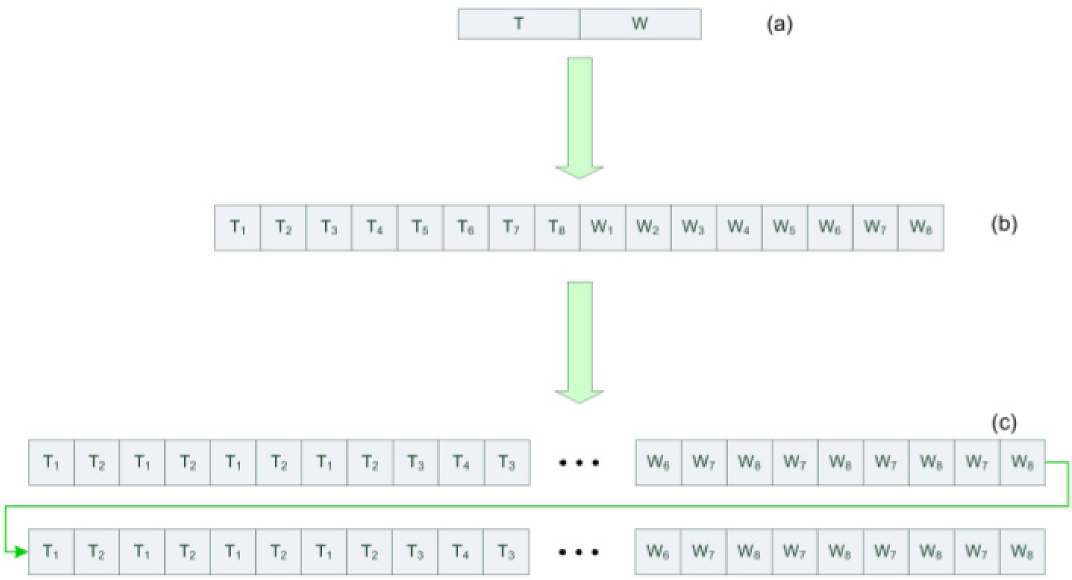


*Figure 2.2.6-1 – NPUSCH transmission in case of 8 repetitions (Narrowband Internet of Things, Rohde & Schwarz)*

In general, in case of 15 kHz spacing the repetition schemes is based on pairs of slots, while in case of 3.75 kHz spacing is based on single slots. The total number of the first repetition corresponds to half the total number of repetitions with an upper bound of 4 if the RU has more than one subcarrier, 1 if the RU has only a single subcarrier. The overall sequence is mapped to a contiguous set of slots. If the transmission reach the maximum time duration of 256 ms, a gap of 40 s is applied before the transmission continues. This gap is requested to allow the UE to stop UL transmission and receive the DL channel, in order to avoid the loss of synchronization to the eNB.

Downlink transmission follows the same principle descried for the uplink, with data packets that in this case are not grouped into RU. Information about where and how data are transmitted over NPDSCH are contained in DCI format N1.

### 2.2.7 Real measures and signaling

In this paragraph, we report the results of some tests made on a NB-IoT prototype connected to a commercial cellular network, to better understand and verify the behavior of signaling protocols, cell connection and access procedures. The prototype was cable-connected to the network: consequently, its radio conditions are optimal. Moreover, it transmits with a transmission frequency much higher with respect to a real metering case: since these tests aims to study the NB-IoT signaling protocols this is not a relevant parameter. Note that this device, unlike what is defined above, only provides control plane optimization (user plane optimization is not implemented). In this analysis, we will focus in particular on the random access procedure and attach to the cell. The following measures were detected and analyzed by means of an analytical tool gently granted by TIM. All graphs and signals are reported in time order.

Initially, once the cell the UE wants to camp on is located, it reads the relative channel conditions through system information: the node sends to the user MIB and SIB2. In the MIB message we can read the cell ID we are referring to, the index of the SF we are working on, the system frequency and the operation mode.

| | | | | |
|---|---|---|---|---|
| 451... | 2017 Jun 14 13:35:17.604 | 0xB0C1 | LTE RRC MIB Message Log Packet | |
| 456... | 2017 Jun 14 13:35:17.768 | 0xB0C0 | LTE RRC OTA Packet | BCCH_DL_SCH_NB |
| 502... | 2017 Jun 14 13:35:19.716 | 0xB0C0 | LTE RRC OTA Packet | BCCH_DL_SCH_NB |

*Figure 2.2.7-1 – System information transmission*

**2017 Jun 14 13:35:17.604 [9A] 0xB0C1 LTE RRC MIB Message Log Packet**

```
Version = 16
Physical cell ID          = 84
FREQ                      = 6290
SFN                       = 302
SFN MSB4                  = 4
HSFN LSB2                 = 0
Sib1 Sch Info             = 2
Sys Info Value Tag        = 2
Access Barring Enabled    = 0
Op Mode Type              = INBAND_SAME_PCI
InbandSamePci
   Eutra CRS Sequence Info = 22
```

*Figure 2.2.7-2 – Master Information Block (MIB)*

```
2017 Jun 14  13:35:19.716  [D2]  0xB0C0  LTE RRC OTA Packet  --  BCCH_DL_SCH_NB
Pkt Version = 15
RRC Release Number.Major.minor = 13.2.1
Radio Bearer ID = 0, Physical Cell ID = 84
Freq = 6290
SysFrameNum = 513, SubFrameNum = 2
PDU Number = BCCH_DL_SCH_NB Message,    Msg Length = 26
SIB Mask in SI =  0x04

Interpreted PDU:

value BCCH-DL-SCH-Message-NB ::=
{
  message c1 : systemInformation-r13 :
      {
        criticalExtensions systemInformation-r13 :
          {
            sib-TypeAndInfo-r13
            {
              sib2-r13 :
                {
                  radioResourceConfigCommon-r13
                  {
                    rach-ConfigCommon-r13
                    {
                      preambleTransMax-CE-r13 n10,
                      powerRampingParameters-r13
                      {
                        powerRampingStep dB2,
                        preambleInitialReceivedTargetPower dBm-104
                      },
                      rach-InfoList-r13
                      {
                        {
                          ra-ResponseWindowSize-r13 pp5,
                          mac-ContentionResolutionTimer-r13 pp8
                        }
                      }
                    },
                    bcch-Config-r13
                    {
                      modificationPeriodCoeff-r13 n32
                    },
                    pcch-Config-r13
                    {
                      defaultPagingCycle-r13 rf256,
                      nB-r13 one64thT,
                      npdcch-NumRepetitionPaging-r13 r8
                    },
                    nprach-Config-r13
                    {
                      nprach-CP-Length-r13 us66dot7,
                      nprach-ParametersList-r13
                      {
                        {
                          nprach-Periodicity-r13 ms640,
                          nprach-StartTime-r13 ms8,
                          nprach-SubcarrierOffset-r13 n36,
                          nprach-NumSubcarriers-r13 n12,
                          nprach-SubcarrierMSG3-RangeStart-r13 one,
                          maxNumPreambleAttemptCE-r13 n4,
                          numRepetitionsPerPreambleAttempt-r13 n2,
                          npdcch-NumRepetitions-RA-r13 r8,
                          npdcch-StartSF-CSS-RA-r13 v2,
                          npdcch-Offset-RA-r13 zero
                        }
                      }
                    }
```

*Figure 2.2.7-3 – SIB2*

Then, once the RRC Connection Setup is completed, the UE starts the attach procedure (refers to *Figure 2.2.7-4*, from r.583): it first reads the *Sum Sys Info* message that reports a summary of the physical channel conditions. In particular, we can read in this message the measured RSRP level and parameters corresponding to MIB information such as cell ID, operation mode and system frequency.

| # | Time | Type | Description | Subtitle |
|---|---|---|---|---|
| 543... | 2017 Jun 14 13:35:20.446 | 0xB0C0 | LTE RRC OTA Packet | DL_CCCH_NB / RRCConnectionSetup |
| 545... | 2017 Jun 14 13:35:20.448 | 0xB0C0 | LTE RRC OTA Packet | UL_DCCH_NB / RRCConnectionSetupCon |
| 546... | 2017 Jun 14 13:35:20.451 | 0xB24B | LTE NB1 ML1 Sum Sys Info | |
| 555... | 2017 Jun 14 13:35:20.687 | 0xB246 | LTE NB1 ML1 GM PDSCH STAT Ind | |
| 556... | 2017 Jun 14 13:35:20.687 | 0xB0C0 | LTE RRC OTA Packet | DL_DCCH_NB / DLInformationTransfer |
| 556... | 2017 Jun 14 13:35:20.688 | 0xB0EA | LTE NAS EMM Security Protected Incoming Msg | |
| 557... | 2017 Jun 14 13:35:20.688 | 0xB0EC | LTE NAS EMM Plain OTA Incoming Message | Authentication request Msg |
| 560... | 2017 Jun 14 13:35:20.753 | 0xB0ED | LTE NAS EMM Plain OTA Outgoing Message | Authentication response Msg |
| 560... | 2017 Jun 14 13:35:20.753 | 0xB0EB | LTE NAS EMM Security Protected Outgoing Msg | |
| 560... | 2017 Jun 14 13:35:20.753 | 0xB0C0 | LTE RRC OTA Packet | UL_DCCH_NB / ULInformationTransfer |
| 561... | 2017 Jun 14 13:35:20.786 | 0xB244 | LTE NB1 ML1 GM DCI Info | |
| 565... | 2017 Jun 14 13:35:20.887 | 0xB245 | LTE NB1 ML1 GM TX Report | |
| 568... | 2017 Jun 14 13:35:20.984 | 0xB240 | LTE NB1 Random Access Request (MSG1) Report | |
| 569... | 2017 Jun 14 13:35:21.015 | 0xB241 | LTE NB1 Random Access Response (MSG2) Report | |
| 570... | 2017 Jun 14 13:35:21.015 | 0xB242 | LTE NB1 UE Identification Message (MSG3) Report | |
| 571... | 2017 Jun 14 13:35:21.040 | 0xB243 | LTE NB1 Contention Resolution Message (MSG4) Re... | |
| 578... | 2017 Jun 14 13:35:21.166 | 0xB0C0 | LTE RRC OTA Packet | DL_DCCH_NB / DLInformationTransfer |
| 578... | 2017 Jun 14 13:35:21.166 | 0xB0EA | LTE NAS EMM Security Protected Incoming Msg | |
| 578... | 2017 Jun 14 13:35:21.166 | 0xB0EC | LTE NAS EMM Plain OTA Incoming Message | Security mode command Msg |
| 579... | 2017 Jun 14 13:35:21.168 | 0xB0ED | LTE NAS EMM Plain OTA Outgoing Message | Security mode complete Msg |
| 579... | 2017 Jun 14 13:35:21.168 | 0xB0EB | LTE NAS EMM Security Protected Outgoing Msg | |
| 579... | 2017 Jun 14 13:35:21.168 | 0xB0C0 | LTE RRC OTA Packet | UL_DCCH_NB / ULInformationTransfer |
| 583... | 2017 Jun 14 13:35:21.247 | 0xB24B | LTE NB1 ML1 Sum Sys Info | |
| 585... | 2017 Jun 14 13:35:21.287 | 0xB246 | LTE NB1 ML1 GM PDSCH STAT Ind | |
| 588... | 2017 Jun 14 13:35:21.387 | 0xB244 | LTE NB1 ML1 GM DCI Info | |
| 591... | 2017 Jun 14 13:35:21.486 | 0xB245 | LTE NB1 ML1 GM TX Report | |
| 595... | 2017 Jun 14 13:35:21.624 | 0xB240 | LTE NB1 Random Access Request (MSG1) Report | |
| 596... | 2017 Jun 14 13:35:21.655 | 0xB241 | LTE NB1 Random Access Response (MSG2) Report | |
| 597... | 2017 Jun 14 13:35:21.655 | 0xB242 | LTE NB1 UE Identification Message (MSG3) Report | |
| 598... | 2017 Jun 14 13:35:21.680 | 0xB243 | LTE NB1 Contention Resolution Message (MSG4) Re... | |
| 603... | 2017 Jun 14 13:35:21.758 | 0xB0C0 | LTE RRC OTA Packet | DL_DCCH_NB / DLInformationTransfer |
| 603... | 2017 Jun 14 13:35:21.758 | 0xB0EA | LTE NAS EMM Security Protected Incoming Msg | |
| 603... | 2017 Jun 14 13:35:21.759 | 0xB0E2 | LTE NAS ESM Plain OTA Incoming Message | ESM information request Msg |
| 603... | 2017 Jun 14 13:35:21.759 | 0xB0E3 | LTE NAS ESM Plain OTA Outgoing Message | ESM information response Msg |
| 603... | 2017 Jun 14 13:35:21.759 | 0xB0E1 | LTE NAS ESM Security Protected Outgoing Msg | |
| 604... | 2017 Jun 14 13:35:21.760 | 0xB0C0 | LTE RRC OTA Packet | UL_DCCH_NB / ULInformationTransfer |
| 610... | 2017 Jun 14 13:35:21.887 | 0xB246 | LTE NB1 ML1 GM PDSCH STAT Ind | |
| 614... | 2017 Jun 14 13:35:21.986 | 0xB244 | LTE NB1 ML1 GM DCI Info | |
| 616... | 2017 Jun 14 13:35:22.000 | 0xB0C0 | LTE RRC OTA Packet | DL_DCCH_NB / DLInformationTransfer |
| 616... | 2017 Jun 14 13:35:22.000 | 0xB0EA | LTE NAS EMM Security Protected Incoming Msg | |
| 616... | 2017 Jun 14 13:35:22.001 | 0xB0EC | LTE NAS EMM Plain OTA Incoming Message | Attach accept Msg |

*Figure 2.2.7-4 – Attach procedure, from RRC Connection Setup Complete to Attach accept Message*

```
2017 Jun 14  13:35:21.247  [DE]  0xB24B  LTE NB1 ML1 Sum Sys Info
Version                       = 1
OP Mode                       = SAME_PCI
Meas BW                       = mbw6 RBs
Cell Id                       = 84
Frequency                     = 6290
Inst Meas RSRP                = -57 dBm
Srxlev                        = -57 dB
```

*Figure 2.2.7-5 – Sum Sys Info*

Then, the node sends to the UE the DCI message, indicating values of RNTI, UL grants and MCS. A transmission report message follows, showing all the parameters that characterize the uplink transmission, like NPUSCH Format, number of repetitions, RACH collisions occurred and ACK/NACK messages. Note that, since the device is in optimal channel conditions (is cable-connected to the network), the power level it has to send to the node is very low (-9/-13 dBm).

```
2017 Jun 14  13:35:21.387  [BD]  0xB244  LTE NB1 ML1 GM DCI Info
Version                       = 2
Num Records                   = 4
Records
```

| # | NPDCCH Timing SFN | NPDCCH Timing Sub FN | RNTI Type | UL Grant Present | DL Grant Present | PDCCH Order Present | NDI | SC Index | Redundancy Version | Resource Assignment | Scheduling Delay | MCS | Repetition Number | DCI Repetition Number | HARQ Resource |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 645 | 6 | C_RNTI | TRUE | FALSE | FALSE | 0 | 0 | 0 | 0 | 0 | 9 | 0 | 0 | |
| 1 | 649 | 6 | C_RNTI | TRUE | FALSE | FALSE | 1 | 0 | 0 | 0 | 0 | 9 | 0 | 0 | |
| 2 | 652 | 1 | C_RNTI | FALSE | TRUE | FALSE | 0 | | | 0 | 0 | 10 | 0 | 0 | 0 |
| 3 | 657 | 6 | C_RNTI | FALSE | TRUE | FALSE | 1 | | | 1 | 0 | 10 | 0 | 0 | 0 |

*Figure 2.2.7-6 – DCI info*

```
2017 Jun 14  13:35:21.486  [48]  0xB245  LTE NB1 ML1 GM TX Report
Version                 = 1
Subcarrier Space        = 15 kHz
Num Records             = 5
Records
```

| # | NPUSCH Timing SFN | NPUSCH Timing Sub FN | NPUSCH Format | Is MSG3 | ITBS | Repetition Number | Num RU | RV Index | Num Tone | Start Tone | TX Power (dBm) | NPUSCH format 1 TX Type | ACK NACK | RFLM | PRACH Collision Valid | PRACH collision 7680ms | Scrambling Mask |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 644 | 4 | FORMAT 1 | TRUE | 6 | 1 | 1 | 0 | 1 | 0 | -13 | NEW TRANSMISSION | | 0 | 0 | 0 | 983859284 |
| 1 | 646 | 5 | FORMAT 1 | FALSE | 9 | 1 | 1 | 0 | 1 | 0 | -9 | NEW TRANSMISSION | | 0 | 0 | 0 | 1013727316 |
| 2 | 650 | 5 | FORMAT 1 | FALSE | 9 | 1 | 1 | 0 | 1 | 0 | -9 | NEW TRANSMISSION | | 0 | 0 | 0 | 1013727316 |
| 3 | 653 | 5 | FORMAT 2 | FALSE | | 2 | | | 1 | 0 | 16 | | ACK | 0 | 0 | 0 | 1013727316 |
| 4 | 659 | 5 | FORMAT 2 | FALSE | | 2 | | | 1 | 0 | 16 | | ACK | 0 | 0 | 0 | 1013727316 |

*Figure 2.2.7-7 – Tx Report*

In this moment Random Access Procedure starts. The UE first send a Random Access Request message, indicating EARFCN (800 MHz in UL), CP Length, CE Level (CE0 due to the channel condition) and number of repetitions. After receiving a Random Access Response, the UE send to the node a MSG3 reporting the physical resource allocation state. The procedure ends with a Contention Resolution message: since we tested a single user scenario, there are no collisions over RACH.

```
2017 Jun 14  13:35:21.624  [15]  0xB240  LTE NB1 Random Access Request (MSG1) Report
Version                              = 1
UL EARFCN                            = 24290
UL Frequency Offset                  = 2
CP Length                            = RACH_CP_SHORT
Coverage level                       = 0
Subcarrier Index                     = 6
Subcarrier Offset                    = 36
Prach Tx Power                       = -22
Num Rep                              = 2
RA Rnti                              = 177
PRACH Actual Tx Power                = -22
Timings
   ----------------------------------
   |                    |SFN |Sub FN|
   ----------------------------------
   |           Scheduled| 704|     3|
   |            PRACH Tx| 704|     8|
   |  PRACH Window Start| 706|     4|
   |    PRACH Window End| 714|     4|

Hop Offset                           = { 6, 10 }
```

*Figure 2.2.7-8 – Random Access Request*

```
2017 Jun 14  13:35:21.655  [77]  0xB241  LTE NB1 Random Access Response (MSG2) Report
Version                       = 1
RACH Procedure Mode           = CONNECTED_MODE_RACH_PROCEDURE
RNTI Type                     = TEMP_RNTI
RNTI Value                    = 60619
TA Included                   = NOT_INCLUDED
Timing Advance                = 0
RAR Timing
   SFN                        = 707
   Sub FN                     = 1
```

*Figure 2.2.7-9 – Random Access Response*

```
2017 Jun 14  13:35:21.655  [77]  0xB242  LTE NB1 UE Identification Message (MSG3) Report
Version                       = 1
Subcarrier Spacing            = 15 kHz
I SC                          = 0
Num Subcarrier                = 1
Subcarrier Index              = 0
I Delay                       = 12
I Rep                         = 1
I MCS                         = 2
Timings
   -------------------------
   |          |SFN |Sub FN|
   -------------------------
   | Scheduled| 707|     4|
   |   MSG3 Tx| 708|     4|
```

*Figure 2.2.7-10 – MSG3*

```
2017 Jun 14  13:35:21.680  [AD]  0xB243  LTE NB1 Contention Resolution Message (MSG4) Report
Version                       = 1
Contention Result             = 1
Timings
   ----------------------
   |        |SFN |Sub FN|
   ----------------------
   | MSG4 Rx|   0|    15|
   |     ACK|   0|    15|
```

*Figure 2.2.7-11 – Contention Resolution*

If Random Access Procedure is correctly completed, the node first send to the UE an Attach accept message then, once all needed message and protocols are done, the final Attach complete message.

| | | | | |
|---|---|---|---|---|
| 616... | 2017 Jun 14 13:35:22.001 | 0xB0EC | LTE NAS EMM Plain OTA Incoming Message | Attach accept Msg |
| 616... | 2017 Jun 14 13:35:22.001 | 0xB0E2 | LTE NAS ESM Plain OTA Incoming Message | Activate default EPS bearer context request |
| 618... | 2017 Jun 14 13:35:22.005 | 0xB0F6 | LTE NAS EMM Forbidden TAI List | |
| 619... | 2017 Jun 14 13:35:22.005 | 0xB0E6 | LTE NAS ESM Procedure State | |
| 619... | 2017 Jun 14 13:35:22.005 | 0xB0EE | LTE NAS EMM State | |
| 619... | 2017 Jun 14 13:35:22.005 | 0xB0E4 | LTE NAS ESM Bearer Context State | |
| 619... | 2017 Jun 14 13:35:22.005 | 0xB0E5 | LTE NAS ESM Bearer Context Info | |
| 630... | 2017 Jun 14 13:35:22.014 | 0xB0E4 | LTE NAS ESM Bearer Context State | |
| 631... | 2017 Jun 14 13:35:22.014 | 0xB0EE | LTE NAS EMM State | |
| 631... | 2017 Jun 14 13:35:22.014 | 0xB0EB | LTE NAS EMM Security Protected Outgoing Msg | |
| 631... | 2017 Jun 14 13:35:22.014 | 0xB0ED | LTE NAS EMM Plain OTA Outgoing Message | Attach complete Msg |
| 632... | 2017 Jun 14 13:35:22.014 | 0xB0EB | LTE NAS EMM Security Protected Outgoing Msg | |

*Figure 2.2.7-12 – Attach procedure completed*

Before data transmission the node activate the Control Plane Optimization, that represent the main protocol innovation since this message is not implemented in LTE case. Then, the UE can finally transmit data over NPUSCH, as we can see in *Figure 2.2.7-14*.

```
2017 Jun 14  13:36:14.276  [98]  0xB0ED  LTE NAS EMM Plain OTA Outgoing Message  --  Control Plane service request Msg
pkt_version = 1 (0x1)
rel_number = 9 (0x9)
rel_version_major = 5 (0x5)
rel_version_minor = 0 (0x0)
security_header_or_skip_ind = 0 (0x0)
prot_disc = 7 (0x7) (EPS mobility management messages)
msg_type = 77 (0x4d) (Control Plane service request)
lte_emm_msg
  emm_ctrl_serv_req
    tsc = 0 (0x0) (cached sec context)
    nas_key_set_id = 0 (0x0)
    active_flag = 0 (0x0)
    ctrl_plane_service_type = 0 (0x0) (mobile originating req)
    esm_msg_container_incl = 1 (0x1)
    esm_msg_container
      eps_bearer_id_or_skip_id = 5 (0x5)
      prot_disc = 2 (0x2) (EPS session management messages)
      trans_id = 0 (0x0)
      msg_type = 235 (0xeb) (ESM data transport)
      lte_esm_msg
        esm_data_transport
          user_data_container
            user_data_container_len = 40 (0x28)
            user_data[0] = 70 (0x46)
            user_data[1] = 0 (0x0)
            user_data[2] = 0 (0x0)
            user_data[3] = 40 (0x28)
            user_data[4] = 0 (0x0)
            user_data[5] = 0 (0x0)
            user_data[6] = 0 (0x0)
            user_data[7] = 0 (0x0)
            user_data[8] = 1 (0x1)
            user_data[9] = 2 (0x2)
            user_data[10] = 158 (0x9e)
            user_data[11] = 119 (0x77)
            user_data[12] = 100 (0x64)
            user_data[13] = 64 (0x40)
            user_data[14] = 66 (0x42)
            user_data[15] = 2 (0x2)
            user_data[16] = 224 (0xe0)
            user_data[17] = 0 (0x0)
            user_data[18] = 0 (0x0)
            user_data[19] = 22 (0x16)
            user_data[20] = 148 (0x94)
            user_data[21] = 4 (0x4)
            user_data[22] = 0 (0x0)
            user_data[23] = 0 (0x0)
            user_data[24] = 34 (0x22)
            user_data[25] = 0 (0x0)
            user_data[26] = 234 (0xea)
            user_data[27] = 3 (0x3)
            user_data[28] = 0 (0x0)
            user_data[29] = 0 (0x0)
            user_data[30] = 0 (0x0)
            user_data[31] = 1 (0x1)
            user_data[32] = 4 (0x4)
            user_data[33] = 0 (0x0)
            user_data[34] = 0 (0x0)
            user_data[35] = 0 (0x0)
            user_data[36] = 239 (0xef)
            user_data[37] = 255 (0xff)
            user_data[38] = 255 (0xff)
            user_data[39] = 250 (0xfa)
          release_assistance_ind_incl = 0 (0x0)
    nas_msg_container_incl = 0 (0x0)
    eps_bearer_context_incl = 1 (0x1)
    eps_bearer_context_status
```

*Figure 2.2.7-13 – Control Plane Service request message*

```
2017 Jun 14  13:36:14.928  [BD]  0xB0E3  LTE NAS ESM Plain OTA Outgoing Message  --  ESM Data Transport Msg
pkt_version = 1 (0x1)
rel_number = 9 (0x9)
rel_version_major = 5 (0x5)
rel_version_minor = 0 (0x0)
eps_bearer_id_or_skip_id = 5 (0x5)
prot_disc = 2 (0x2) (EPS session management messages)
trans_id = 0 (0x0)
msg_type = 235 (0xeb) (ESM data transport)
lte_esm_msg
  esm_data_transport
    user_data_container
      user_data_container_len = 1022 (0x3fe)
      user_data[0] = 69 (0x45)
      user_data[1] = 0 (0x0)
      user_data[2] = 3 (0x3)
      user_data[3] = 254 (0xfe)
      user_data[4] = 0 (0x0)
      user_data[5] = 1 (0x1)
      user_data[6] = 0 (0x0)
      user_data[7] = 0 (0x0)
      user_data[8] = 1 (0x1)
      user_data[9] = 17 (0x11)
      user_data[10] = 31 (0x1f)
      user_data[11] = 178 (0xb2)
      user_data[12] = 100 (0x64)
      user_data[13] = 64 (0x40)
      user_data[14] = 66 (0x42)
      user_data[15] = 2 (0x2)
      user_data[16] = 239 (0xef)
      user_data[17] = 255 (0xff)
      user_data[18] = 255 (0xff)
      user_data[19] = 250 (0xfa)
      user_data[20] = 192 (0xc0)
      user_data[21] = 4 (0x4)
      user_data[22] = 14 (0xe)
      user_data[23] = 118 (0x76)
      user_data[24] = 3 (0x3)
      user_data[25] = 234 (0xea)
      user_data[26] = 169 (0xa9)
      user_data[27] = 178 (0xb2)
      user_data[28] = 60 (0x3c)
      user_data[29] = 63 (0x3f)
      user_data[30] = 120 (0x78)
      user_data[31] = 109 (0x6d)
      user_data[32] = 108 (0x6c)
      user_data[33] = 32 (0x20)
      user_data[34] = 118 (0x76)
      user_data[35] = 101 (0x65)
      user_data[36] = 114 (0x72)
      user_data[37] = 115 (0x73)
      user_data[38] = 105 (0x69)
      user_data[39] = 111 (0x6f)
      user_data[40] = 110 (0x6e)
      user_data[41] = 61 (0x3d)
      user_data[42] = 34 (0x22)
      user_data[43] = 49 (0x31)
      user_data[44] = 46 (0x2e)
      user_data[45] = 48 (0x30)
      user_data[46] = 34 (0x22)
      user_data[47] = 32 (0x20)
      user_data[48] = 101 (0x65)
      user_data[49] = 110 (0x6e)
      user_data[50] = 99 (0x63)
      user_data[51] = 111 (0x6f)
      user_data[52] = 100 (0x64)
      user_data[53] = 105 (0x69)
      user_data[54] = 110 (0x6e)
```

*Figure 2.2.7-14 – ESM Data Transport Message*

In addition, we also show results from different tests made on the same prototype, but in worse radio condition: we can see how, when the device measures lower RSRP values, CE1 and CE2 are activated. The thresholds for activating these levels and the corresponding number of repetitions are manufacturer-specified information.

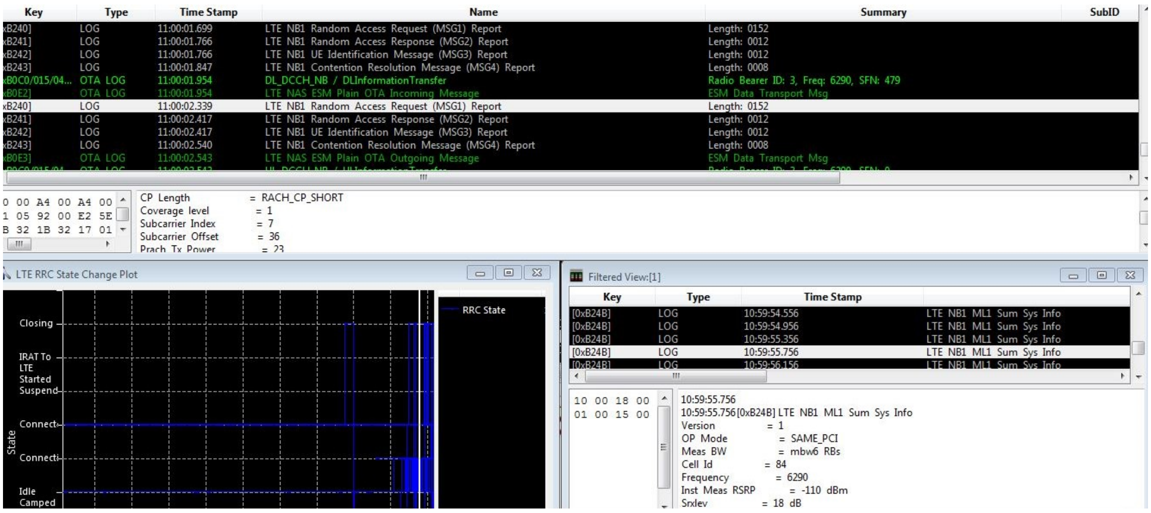


*Figure 2.2.7-15 – CE1 activation, RSRP = -110 dBm*

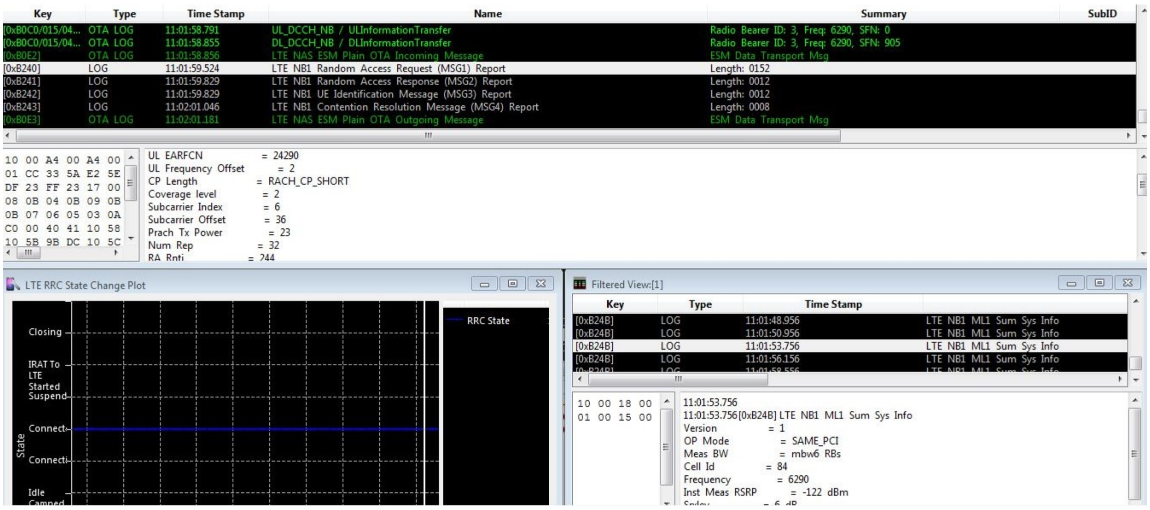


*Figure 2.2.7-16 – CE2 activation, RSRP = -122 dBm*

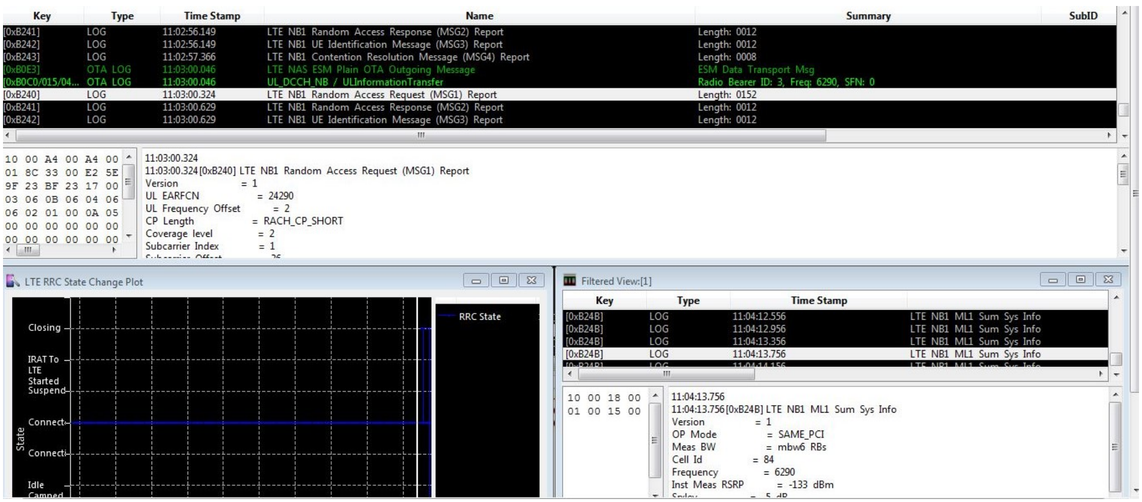


*Figure 2.2.7-17 – CE2 lower bound, RSRP = -133 dBm*

*Figure 2.2.7-18* shows the front and back of the NB-IoT prototype used in our tests.

*Figure 2.2.7-18 – NB-IoT prototype used in tests, front and back*

## 2.3 NB-IoT: difference from LTE standards

In this section, starting from the NB-IoT overview just described, we provide a brief description of all the differences between this technology and LTE standards (some of which have already been mentioned above).

Since MTC devices are stationary, in NB-IoT there is no handover for the UE in RRC_CONNECTED state. There is no interaction with other radio technologies and consequently associated features are not implemented: this result in the lack of LTE-WLAN interworking, interference avoidance for in-device coexistence, and channel quality monitoring. Most LTE-Advanced functionalities are not implemented, such as Carrier Aggregation, Dual Connectivity, and device-to-device services. Since data transmission is delay tolerant, there is no QoS concept and other services built to guarantee a determined bit-rate. Network architecture is the same as the LTE, with the exception of the lack of Data Radio Bearer in EPC Control Plane: the data transmission runs over the signaling radio bearers. Frequency bands are numbered in the same way as LTE frequencies: NB-IoT bands represents a subset of them.

### 2.3.1 Physical Layer

As seen previously, NB-IoT frequency band corresponds to a single 180 kHz LTE Physical Resource Block. In case of in band operation mode the resource blocks utilization is not fixed but only a subset of them is available for NB-IoT transmission (see *Table 2.2.2-1*). FDD half-duplex type-B is set as duplex mode: uplink and downlink channels are always separated in frequency (the UE either transmits or receives) from one guard SF, so that the user equipment has time to switch its transmitter and receiver chain. Two additional coverage enhancement levels CE1 and CE2 are added in order to reach higher Maximum Coupling Loss level (154 dBm and 164 dBm respectively). Consequently, an UE that in LTE is considered out of coverage, within these limits, in NB-IoT succeed to transmit without loss of information, thanks to the implementation of a determined number of repetitions that the UE must assume in the transmission. The repetitions number depends on the estimated coverage level.

#### 2.3.1.1 Downlink

Downlink physical and transport channels defined in NB-IoT are less with respect to the LTE case: there is not a channel equivalent to the Physical Multicast Channel PMCH, as there is no Broadcast Channel BCH, Paging Channel PCH or Shared Channel SCH. The NB-IoT Physical Resource Block in downlink corresponds to an LTE Resource Block with Normal Cyclic Prefix. QPSK modulation is applied. In the following, we describe how the resource allocation for each physical downlink signal or channel is defined in NB-IoT with respect to the LTE case.

Narrowband Reference Signals NRS are transmitted in each SF (for both data and control information), on the two lasts RE of the subcarriers 1, 4, 7 and 10; LTE maintains the same subcarriers offset but transmits the reference signals on the symbols 1 and 5.

For the transmission of the narrowband synchronization signals is not allowed the use of the first 3 OFDM symbols, since they are dedicated to PDCCH LTE in in-band operation mode. NPSS is transmitted on SF 6 and 12 of each 20 ms chain: it occupies an area of 11 subcarriers * 11 OFDM symbols (from 4 to 14), with overlap of LTE CRS. In LTE PSS is transmitted on slots 0 and 10 of a 10 ms chain, 31 subcarriers above and 31 subcarriers under the system carrier frequency, on the 7$^{th}$ OFDM symbol. NSSS is transmitted on SF 10 of each 20 ms chain and occupies and area of 12 subcarriers * 11 OFDM symbols (from 4 to 14), with overlap of LTE CRS. In LTE SSS is transmitted exactly with the same scheme described for PSS, but on the 6$^{th}$ OFDM symbol. The following figure compares the transmission schemes described above.

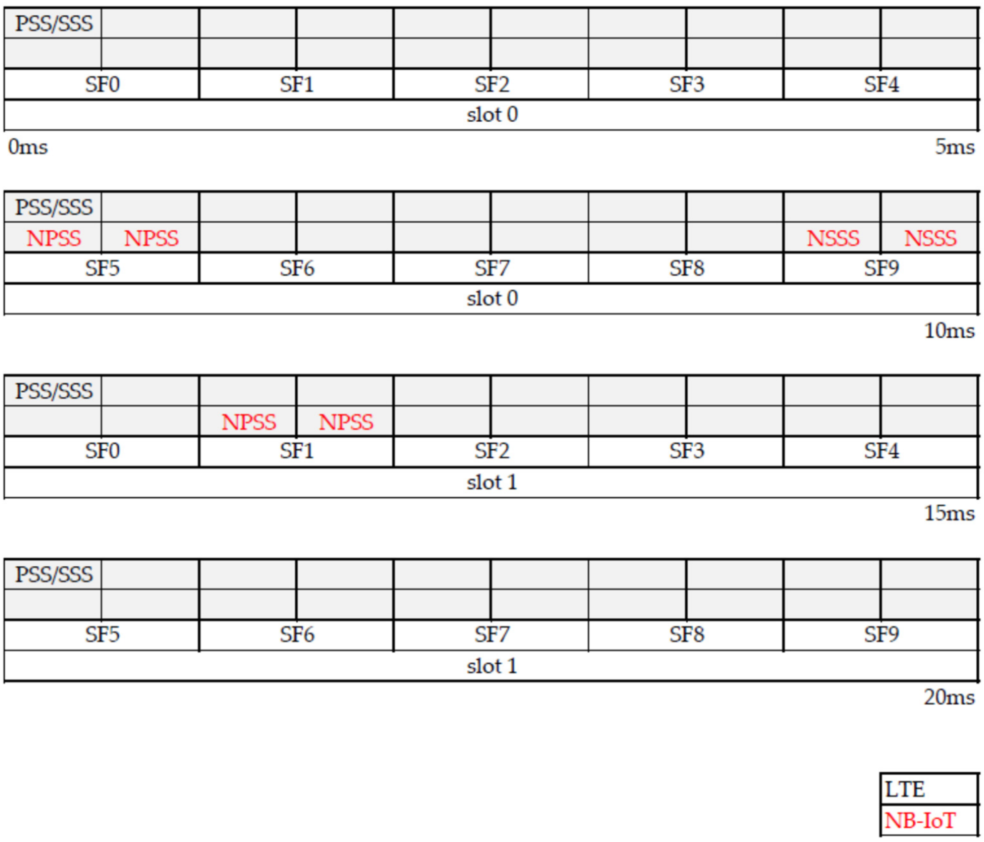


*Figure 2.3.1.1-1 – Synchronization signals allocation in LTE and NB-IoT*

NPBCH is dedicated to the transmission of Master Information Block in NB-IoT. MIB-NB contains a 34 bit message and is transmitted over a 640 ms period (64 radio frame), divided in 8 blocks of 80 ms (8 radio frames). The first block occupies an area of 12 subcarriers * 11 OFDM symbols (from 4 to 14) and is transmitted on SF0 of each RF composing the block, and so on for all the blocks. In LTE, MIB is transmitted on SF0 of 4 10 ms consecutive chains, 36 subcarriers above and 36 subcarriers under the system carrier frequency, on 4 OFDM symbols (the first 4 of the second time slot of SF0).

NPDCCH structure is described in *Section 2.2.2.1* is mapping starts from an OFDM symbol indicated by the parameter $I_{start}^{N}$ in a region of 12 subcarriers (6 for NCCE0 and 6 for NCCE1) * *N* OFDM symbols. Each NPDCCH can be repeated a number of times defined in RRC system information. In LTE PDCCH is placed on the firsts 1, 2 or 3 OFDM symbols of each SF: the number of symbols used is indicated in PCFICH. NPDSCH has the same structure described for NPDCCH. In LTE PDSCH is scheduled in SF4 with a period of 80 ms.

#### 2.3.1.2 Uplink

In NB-IoT there is not a channel equivalent to the LTE Uplink Control Channel PUCCH: except for RACH transmission, all signals are transmitted in UL over the Narrowband Physical Uplink Shared Cannel NPUSCH (including Uplink Control Information UCI). Uplink transport channels and physical signals are equal to the LTE ones. While in LTE the uplink subframe structure corresponds to the one defined in downlink, in NB-IoT this is completely different. Each subcarrier occupies a 3,75 kHz bandwidth instead of the 15 kHz in DL: this leads to 4-time duration for the transmission of the 7 OFDM symbols composing the slot (2 ms), with respect to the 0,5 ms duration of a DL slot. The transmission scheme is SC-FDMA as in LTE case. BPSK or QPSK modulation is applied. As already done for downlink channel, now we describe how the resource allocation for each physical uplink signal or channel is defined in NB-IoT with respect to the LTE case.

NPUSCH can be implemented in two different formats: NPUSCH Format 1 resource unit in scheduled on 1 subcarrier in frequency and 16 slots in time (leading to a duration of 32 ms), while NPUSCH Format 2 resource unit is scheduled only on 1 subcarrier in frequency and 4 time slots (resulting in this case in an 8 ms duration). Once the signal over NPUSCH is carried in time domain through an Inverse Fourier Transform IFT, a cyclic prefix is apposed with a length of $128\, samples = 8{,}3\, \mu s$. DMRS are sent over NPUSCH only in case of data transmission: in case of Format 1 they are allocated on the 5th OFDM symbol of a slot, in case of Format 2 on the first 3 OFDM symbols. In LTE DMRS are mapped at the center of the slot, with 1 OFDM symbol in Format 1 and 3 in Format 2.

RACH resources occupy a contiguous set of 12, 24, 36 or 48 subcarriers. Resource allocation for random access channel in NB-IoT is described in detail in *Section 2.2.3.1*. Since there is no PUCCH in NB-IoT, the overall available bandwidth is dedicated to data region and RACH, while in LTE it is split in control region (1 PRB at each bound) and data region (the remaining bandwidth).

### 2.3.2 Cell Access: Selection and Mobility

Cell access in NB-IoT follows the same principles expressed for LTE: the UE search an available cell on a determined frequency, reads the relative system information and starts a random access procedure in order to establish and RRC connection. In NB-IoT compared to the LTE case there is no SRB2, but there is and additional SRB1bis that is equal to SRB1 but without PDCD: it assume SRB1 functionalities the security is activated (when SRB1 occurs, SRB1bis stops working). The protocol stack is an optimized version of the LTE one. NB-IoT implements only a subset of the LTE system information: MIB, SIB1, SIB2, SIB3, SIB4, SIB5, SIB14 and SIB16 (the last two are optional).

In NB-IoT no support for handover procedure: if an UE needs to camp on a different cell with respect to the one it is attached in a determined time instant, it has first to switch to the RRC_IDLE state and then start a cell re-selection process in order to find a different cell. Unlike the LTE case, there is no priority order for different frequencies in cell re-selection procedure. The connection procedure is equal to the LTE case, with the difference that when sending the RRC connection request message the UE must not specify the establishment cause, since the transmission is delay tolerant. There is no Paging and other relevant functionalities for RRC_IDLE state. As described in *Section 2.2.5.2* in NB-IoT there is the possibility to implement an optimized connection resume when an UE loose the connection and needs to re-connect to the cell avoiding to re-operate the overall connection procedure: this is allowed by the storage of an AS Context message.

# 3 Scenario

The aim of this analysis is the evaluation of the performance of a Massive Narrowband-IoT system. The use case represented in the simulation is a smart metering system, developed over a Machine Type Communication network implemented from an Internet of Things point of view. The system is massive because we place our case study in a dense urban scenario: we want to simulate an urban area, supposing to have a device every four people. Checking the population density of the main European cities results in an average value of $15000/km^2$ for a massive dense urban scenario. This leads to an UE density of $3750/km^2$ for a single smart metering use case. We place in this scenario 5 site, each one characterized by three sectors.

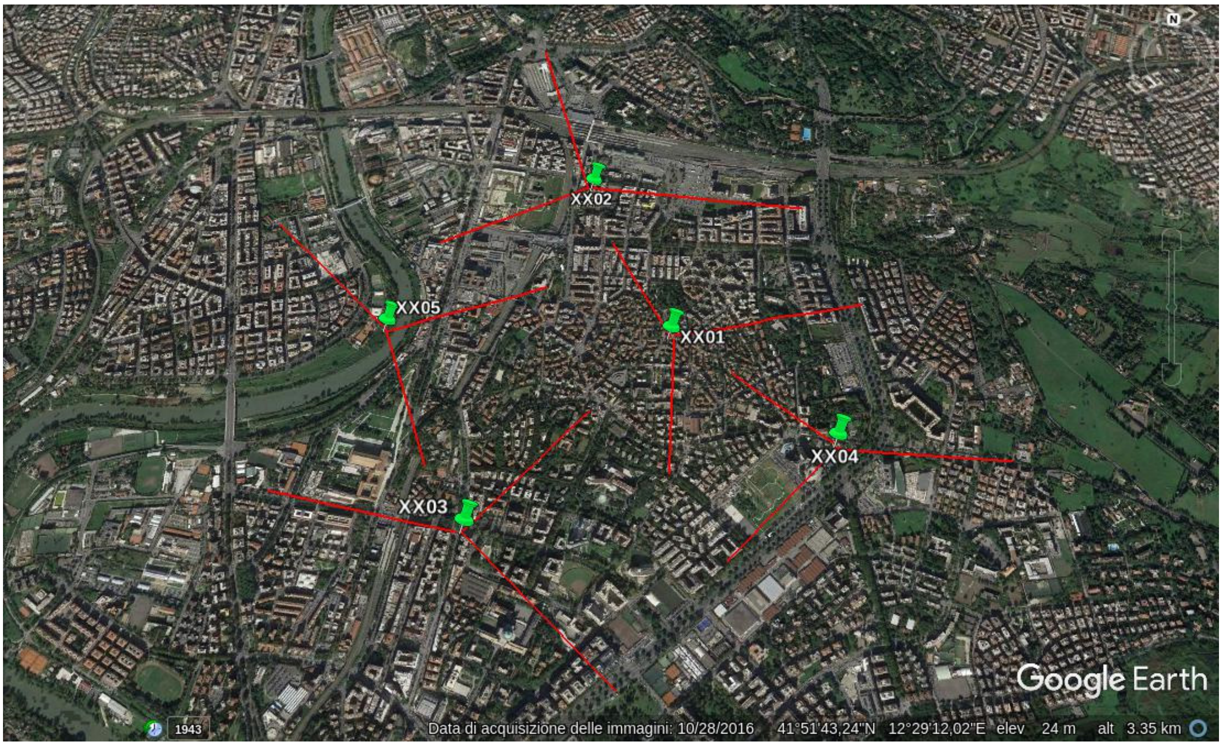


*Figure 3-1 – Simulation scenario: site location and cell-site orientation*

As seen previously, following features characterize a general smart metering system:

1. *No Mobility*: devices are stationary, so that we have not to consider mobility or in the same way handover and cell reselection;

2. *Uplink Transmission*: devices transmit exclusively on uplink channel, while downlink is used by the UEs only to receive DCI and in particular channel information from EnodeB;
3. *Small Amount of Data*: the devices must only send system information, so that they have to send at most packet of 200 bytes;
4. *Time Controlled*: UEs send data only at certain pre-defined periods;
5. *Infrequent transmission*: generally the inter arrival time of each UE can be equal to 24h, 2h, 1h or 30min;
6. *Time Tolerant*: due to the infrequent transmission on the channel, data transfer is not delay;
7. *Monitoring*: MTC networks provide functionality to detect the events;
8. *Low Power Consumption*: MTC device are often installed without power supply, so that they need to run only on battery.

According to this, we want to simulate a set of devices transmitting with a determined inter packet interval, leading to a fixed transmission frequency. In particular, in our study we consider three different classes of smart metering devices, each characterized by a different transmission frequency and consequently by a different periodic inter-arrival time. The use cases represented in our scenario are:

1. Class A – Energy metering (e.g. Gas metering):
   this class of user equipment is placed in a deep indoor scenario, so they are affected by an additional pathloss with respect to the outdoor propagation, caused by the attenuation due to metal screen or underground areas; after the installation, their position is fixed.
2. Class B – Air quality metering:
   this class of meters aims monitoring the air quality in an households or in public spaces; they are assumed to be stationary and placed in outdoor areas.
3. Class C – Outdoor smart parking:

these devices are sensors placed on columns or poles in order to monitor the behavior of an outdoor parking area; their position is fixed and they are assumed to be not affected by any additional pathloss.

As described in *3GPP Specification 45.820 - Cellular system support for ultra-low complexity and low throughput Internet of Things (CIoT)*, we assume for these class of user equipment the following set of periodic inter-arrival time:

1. Class A: 1 day;
2. Class B: 2 hours;
3. Class C: 1 hour.

According to these values of transmission frequency, we can assume to study a time interval of 24 hours. Always from *3GPP 45.820*, the UEs should have the following payload size distribution: Pareto distribution with shape parameter $\alpha = 2.5$ and minimum application payload size $20bytes$ with a cutoff of $200bytes$ (payloads higher than $200bytes$ are assumed equal to the cutoff).

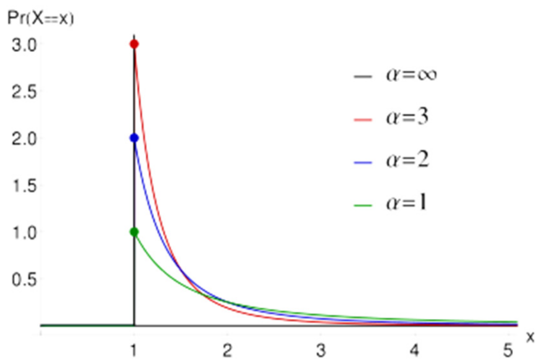


*Figure 3-2 – Pareto distribution*

The antennas employed in our scenario transmit a fixed power of 23 dBm and works over the LTE frequency band of 800MHz. Finally, we assume in Uplink a 3,75 kHz subcarrier spacing: this results on a set of 48 subcarriers available for the UL transmission.

## 3.1 Propagation model

The aim of the simulation is to implement a time-variant channel, in order to represent correctly the main features of a dense urban scenario, as explained previously. At this scope we choose to model the channel propagation following the *Recommendation ITU-R P.1411-8 ("Propagation data and prediction methods for the planning of short-range outdoor radiocommunication systems and radio local area networks in the frequency range 300 MHz to 100 GHz", 07/2015)*. As expressed in the title, this recommendation describes propagation model for short-range outdoor communication in the frequency range 300 MHz to 100 GHz; the communication range is considered "short" if the distance between the user and the core network is under 1 km. The predominant effect on propagation over this kind of paths is due to buildings and trees, since most short-path radio links are found in an urban or suburban scenario. The effect of variations in ground elevation in these cases is not significant. The considered ITU recommendation defines categories for short propagation paths, and provides methods for estimating path loss, cross correlation, delay spread and angular spread.

### 3.1.1 Physical operating environments and cell types

Radiowave propagation is affected by environments such as building structures and eights, the position of the antennas and the usage of mobile terminal (that can be considered as vehicular or pedestrian). Note that environments in this recommendation are categorized only from radio prospective. In the following, we identify the most typical environments described in *ITU-R P.1411.8*, with the relatives characterizing elements:

1. Urban very high-rise:
   - Busiest urban deep canyon, characterized by streets lined with high-density buildings with several tens of floors which results in an urban deep canyon;
   - Rows of tall buildings provide the possibility of very long path delays;

– High dense buildings and skyscrapers interleave with each other which yields to the rich scattering propagation paths in NLoS;
– Heavy traffic vehicles and high flow rate visitors in the area act as reflectors adding Doppler shift to the reflected waves;
– Trees beside the streets provide dynamic shadowing;

2. Urban high-rise:
   – Busiest urban deep canyon, characterized by streets lined with high-density buildings with several tens of floors which results in an urban deep canyon;
   – High dense buildings and skyscrapers interleave with each other which yields to the rich scattering propagation paths in NLoS;
   – Rows of tall buildings provide the possibility of very long path delays;
   – Heavy traffic vehicles and high flow rate visitors in the area act as reflectors adding Doppler shift to the reflected waves;
   – Trees beside the streets provide dynamic shadowing;
3. Urban low-rise/Suburban:
   – Typified by wide streets;
   – Building heights are generally less than three stories making diffraction over roof-top likely;
   – Reflections and shadowing from moving vehicles can sometimes occur;
   – Primary effects are long delays and small Doppler shifts;
4. Residential:
   – Single and double storey dwellings;
   – Roads are generally two lanes wide with cars parked along sides;
   – Heavy to light foliage possible;
   – Motor traffic usually light;
5. Rural:
   – Small houses surrounded by large gardens;
   – Influence of terrain height (topography);
   – Heavy to light foliage possible;

– Motor traffic sometimes high.

*Recommendation ITU-R P.1411-8* defines, for each of the five different environments, two possible kinds of mobile: users are divided into pedestrian and vehicular, and each of these kind of UEs has different velocity, yielding different Doppler shifts. In our case study, we can ignore this distinction, since we are dealing only with stationary users.

The propagation mechanism that we have to consider is affected also by the height of the base station antenna relative to the surrounding buildings. We list in the following table the typical cell types relevant for outdoor short-path propagation.

| Cell type | Cell radius | Typical position of base station antenna |
|---|---|---|
| Micro-cell | 0,05 to 1 km | Outdoor; mounted above average roof-top level, heights of some surrounding buildings may be above base station antenna height |
| Dense urban micro-cell | 0,05 to 0,5 km | Outdoor; mounted below average roof-top level |
| Pico-cell | Up to 50 m | Indoor or outdoor (mounted below roof-top level) |

*Table 3.1.1-1 - ITU-R P.1411-8, definition of cell types*

### 3.1.2 Path categories

The recommendation considers three level of locations of the antennas, all included in the urban scenario represented in *Figure 1*:

1. Over the rooftop (designated as L1);
2. Below rooftop but above head level (designated as L2);
3. Below head level (designated as L3).

Consequently, since antennas and UEs can be considered in Line of Sight (LoS) or non-Line of Sight (NLoS) propagation, we have to consider six different kinds of links depending on the location of the devices.

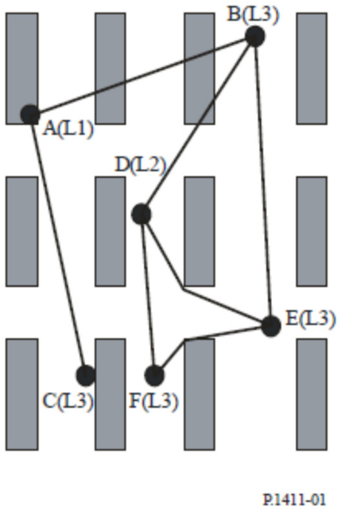


*Figure 3.1.2-1 – ITU-R P.1411-8, Typical propagation situation in urban areas*

In figure, the points are *stations*, which can represent equivalently antennas or devices. When one station (A) is placed above rooftop level and another (B or C) is located at the head level, we have to consider a micro-cell: this is the kind of scenario that we will consider in our simulation, where A is the antenna and B or C are generic UEs. The difference between B and C is that user C is Los, while B is NLoS. The other points in figure represent the case in which one station (D) is mounted below rooftop level but above-head level and another one (E or F) is located at head level, in LoS or NLoS case. In addition, mobile-to-mobile links are depicted in figure by the couples B-E (LoS) and E-F (NLoS), assuming both stations in each link to be at the head level. In particular, for our simulation case it is important to consider the NLoS case represented by the link A to B described before: *Figure 2* shows in detail the radiowave propagation relative to this case and the correspondent parameters. In our case study STN1 (A) represent the eNodeB and STN2 (B) the UE.

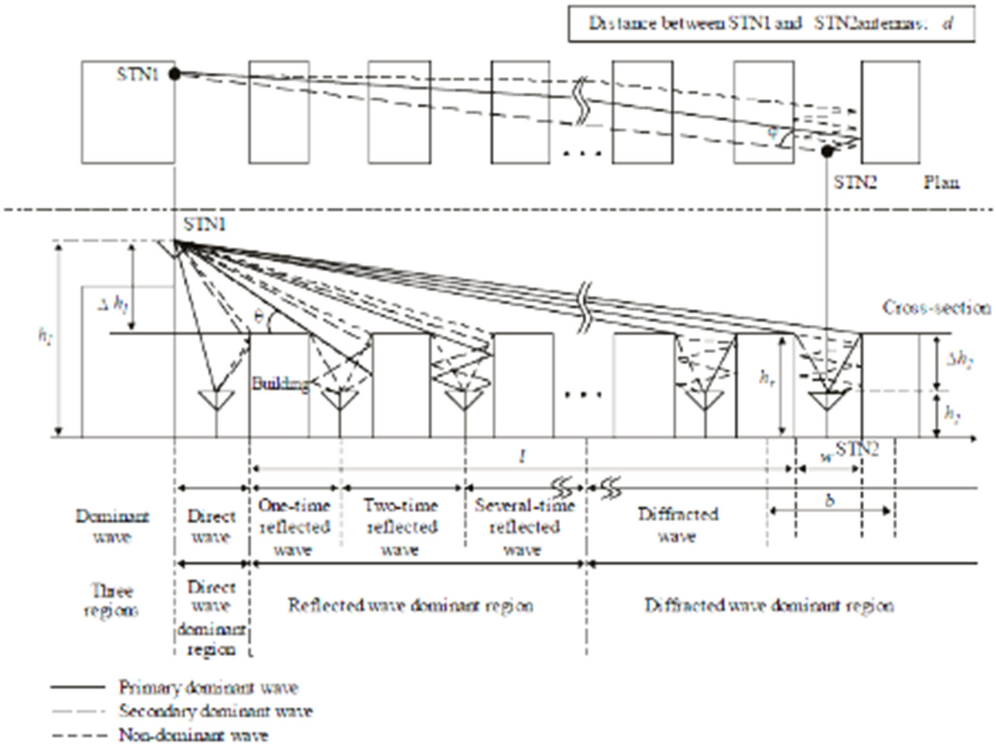


*Figure 3.1.2-2 – ITU-R P.1411-8, Definition of parameters for the NLoS1 case*

The main parameters characterizing this kind of propagation are:

- $h_r$: average height of buildings (m);
- $w$: street width (m);
- $b$: average buildings separation (m);
- $\varphi$: street orientation with respect to the direct path (degrees);
- $h_1$: Station 1 antenna height (m);
- $h_2$: Station 2 antenna height (m);
- $d$: distance from Station 1 to Station 2 (m);
- $l$: length of the path covered by buildings (m).

### 3.1.3 Urban area

The considered path loss model, as seen before, is designed for Non-Line-Sight short-range outdoor communication over rooftop in the frequency range 300 MHz to 100 GHz. Since we want to simulate an urban scenario deployed over an average cell-site sector of

≈ 0.9 km$^2$, at the frequency of 800 MHz, we can assume this propagation model coherent with the uplink channel that we are going to consider. In detail, the model describe the propagation loss as the sum of free-space loss$L_{bf}$, the diffraction loss from rooftop to street $L_{rts}$ and the reduction due to multiple screen diffraction past rows of buildings $L_{msd}$. The formula is:

$$L_{NLOS} = \begin{cases} L_{bf} + L_{rts} + L_{msd} & for L_{rts} + L_{msd} > 0 \\ L_{bf} & for L_{rts} + L_{msd} \leq 0 \end{cases}$$

The free-space loss is given by:

$$L_{bf} = 32.4 + 20 log\left(\frac{d}{1000}\right) + 20 log(f)$$

where:

$f$: Frequency [MHz]

$d$: Distance (where $d > 1$) [m]

The term $L_{rts}$ takes into account the width of the streets and its orientation, according to the formulas:

$$L_{rts} = -8.2 - 10\, log(w) + 10\, log(f) + 20\, log(\Delta h_2) + L_{ori}$$

$$L_{ori} = \begin{cases} -10 + 0.354\varphi & for 0^\circ < \varphi < 35^\circ \\ 2.5 + 0.075(\varphi - 35) & for 35^\circ \leq \varphi \leq 55^\circ \\ 4.0 - 0.114(\varphi - 55) & for 55^\circ < \varphi \leq 90^\circ \end{cases}$$

$$\Delta h_2 = h_r - h_2$$

where:

$h_r$: is the height of the rooftop [m]

$h_2$: is the height of the mobile [m]

$\varphi$: is the street orientation with respect to the direct path [degrees]

The multiple screen diffraction loss depends on the BS antenna height relative to the building height and on the incidence angle. The former is selected as the higher antenna in the communication link. Regarding the latter, the "settled field distance" is used for select the proper model; its value is given by:

$$d_s = \frac{\lambda d^2}{\Delta h_1^2}$$

with:

$$\Delta h_1 = h_1 - h_2$$

For the evaluation of $L_{msd}$, the distance $d_s$ is compared to the distance $l$ over which the buildings extend.

$$L_{msd} = \begin{cases} -\tanh\left(\frac{\log(d) - \log(d_{bp})}{\chi}\right) \cdot (L1_{msd}(d) - L_{mid}) + L_{mid} & for\, l > d_s \, and\, dh_{bp} > 0 \\ \tanh\left(\frac{\log(d) - \log(d_{bp})}{\chi}\right) \cdot (L2_{msd}(d) - L_{mid}) + L_{mid} & for\, l \leq d_s \, and\, dh_{bp} > 0 \\ L2_{msd}(d) & for\, dh_{bp} = 0 \\ L1_{msd}(d) - \tanh\left(\frac{\log(d) - \log(d_{bp})}{\zeta}\right) \cdot (L_{upp} - L_{mid}) - L_{upp} + L_{mid} & for\, l > d_s \, and\, dh_{bp} < 0 \\ L2_{msd}(d) + \tanh\left(\frac{\log(d) - \log(d_{bp})}{\zeta}\right) \cdot (L_{mid} - L_{low}) + L_{mid} - L_{low} & for\, l \leq d_s \, and\, dh_{bp} < 0 \end{cases}$$

where:

$$dh_{bp} = L_{upp} - L_{low}$$

$$\zeta = (L_{upp} - L_{low})\upsilon$$

$$L_{mid} = \frac{L_{upp} + L_{low}}{2}$$

$$L_{upp} = L1_{mid}(d_{bp})$$

$$L_{low} = L2(d_{bp})$$

$$d_{bp} = |\Delta h_1| \sqrt{\frac{1}{\lambda}}$$

$$\upsilon = 0.0417$$

$$\chi = 0.1$$

Therefore, in case of $l > d_s$ (where $l$ is the distance over which the building extend):

$$L1_{msd} = L_{bsh} + k_a + k_d log\left(\frac{d}{1000}\right) + k_f log(f) - 9log(b)$$

$$L_{bsh} = \begin{cases} -18log(1 + \Delta h_1) & for h_1 > h_r \\ 0 & for h_1 \leq h_r \end{cases}$$

$$k_a = \begin{cases} 71.4 & for h_b > h_r \wedge f > 2000MHz \\ 73 - 0.8\Delta h_1 & for\ h_1 \leq h_r, f > 2000MHz \text{ and } d \geq 500m \\ 73 - 1.6\Delta h_1 \frac{d}{1000} & for\ h_1 \leq h_r, f > 2000MHz \text{ and } d < 500m \\ 54 & for h_1 > h_r \wedge f \leq 2000MHz \\ 54 - 0.8\Delta h_1 & for h_1 \leq h_r \wedge f > 2000MHz \\ 54 - 1.6\Delta h_1 & for h_1 \leq h_r \wedge f \leq 2000MHz \end{cases}$$

$$k_d = \begin{cases} -18 & for h_1 > h_r \\ 18 - 15\frac{\Delta h_1}{h_r} & for h_1 \leq h_r \end{cases}$$

$$k_f = \begin{cases} -8 & for f > 2000MHz \\ -4 + 0.7\left(\frac{f}{925} - 1\right) & for medium city \wedge suburban centres \wedge f \leq 2000MHz \\ -4 + 1.5\left(\frac{f}{925} - 1\right) & for metropolitan centres \wedge f \leq 2000MHz \end{cases}$$

Alternatively, in case of $l < d_s$, the formula became:

$$L2_{msd} = -10log(Q_M^2)$$

Where

$$Q_M = \begin{cases} 2.35\left(\frac{\Delta h_1}{d}\sqrt{\frac{d}{\lambda}}\right)^{0.9} & for h_1 > h_r \\ \frac{b}{d} & for h_1 \approx h_r \\ \frac{b}{2\pi d}\sqrt{\frac{\lambda}{\rho}}\left(\frac{1}{\theta} - \frac{1}{2\pi + \theta}\right) & for h_1 < h_r \end{cases}$$

where:

$$\theta = arctan\left(\frac{\Delta h_1}{b}\right)$$

$$\rho = \sqrt{\Delta h_1^2 + b^2}$$

Additional losses are introduced by the presence of vegetation. Two major mechanism can be identified:

- Propagation through trees;
- Propagation over trees.

The first mechanism predominates when the antennas are below tree-tops while the latter is more significant for geometries where one antenna stands much higher the others. Then, we are more interested in the second case, which is also the simplest: in fact, this propagation mode con be modeled by using an ideal knife-edge diffraction model as reported in ITU-R P.526.

## 3.2 Sounding chain

Depending on the channel model just described if we know the power that each UE transmits to the node during the sounding, we can estimate the power that the node actually receives after propagation. Once it has received the sounding signal from the j-th UE, the node compute the correspondent value on SINR depending on its noise figure and the measured interference in the transmission. Finally, from the SINR value the node evaluates and assigns to the UE all the features needed for the uplink transmission. In *Figure 3.2-1* shows a block diagram of the *Sounding Chain* for a generic UE.

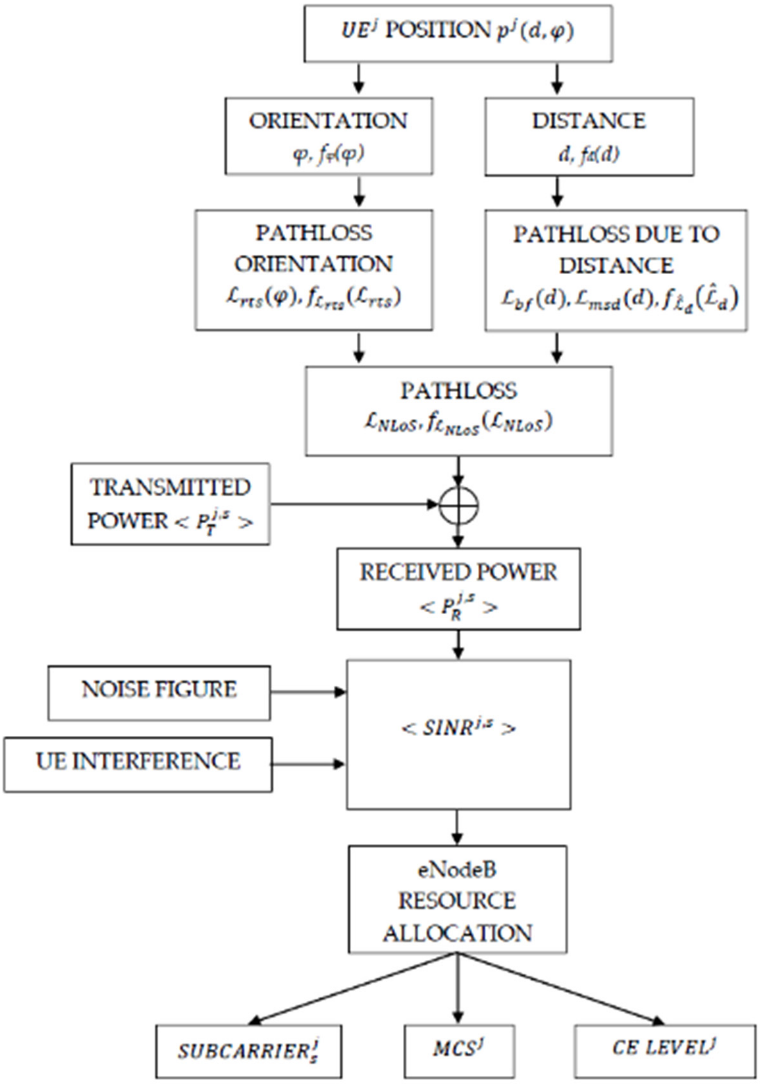


*Figure 3.2-1 – $UE^j$ sounding chain*

First, the transmitted power is determined as well as the transmission and reception gains. While in the case of a single simulation, as described above, the position of users is deterministic, in a general traffic model we have to consider it as a random variable. Therefore, the whole model becomes a function of two random variables: it can be described as a random variable itself. Since the variables are independent, it is possible to analyze each contribution to the total path loss separately. First, we provide a brief theory recall.

Given a random variable $x$, with density function $f_X(x)$, let $y=g(x)$ be its correspondence. Now, we want to determine the probability distribution of $f_Y(y)$. If $g$ is a monotonically increasing (or decreasing) and differentiable function we have:

$$f_y(y)dy = f_x(x)dx$$

and for differentiability hypothesis we can write:

$$dy = g'(x)dx$$

so that we finally have:

$$f_y(y)g'(x)dx = f_x(x)dx$$

$$f_y(y) = \frac{f_x(x)}{g'(x)}$$

According to the theory, we can divide the terms depending on distance $d$, $L_{bf}$ and $L_{msd}$, from that depending on the orientation $\varphi$, $L_{rts}$. We can assume for both $d$ and $\varphi$ an uniform probability density function.

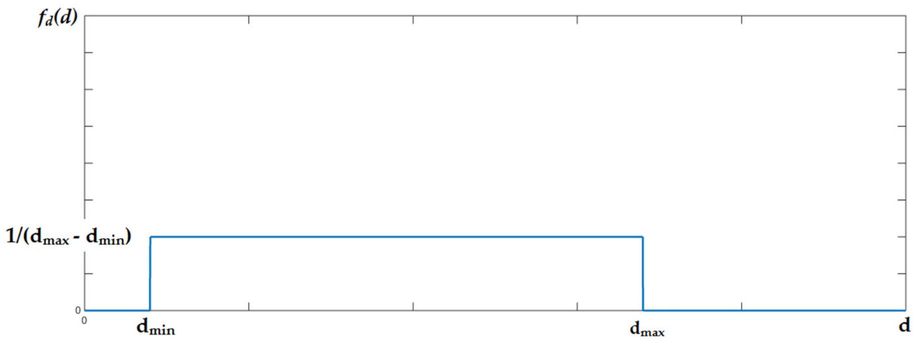


*Figure 3.2-2 – Probability density function of the distance d*

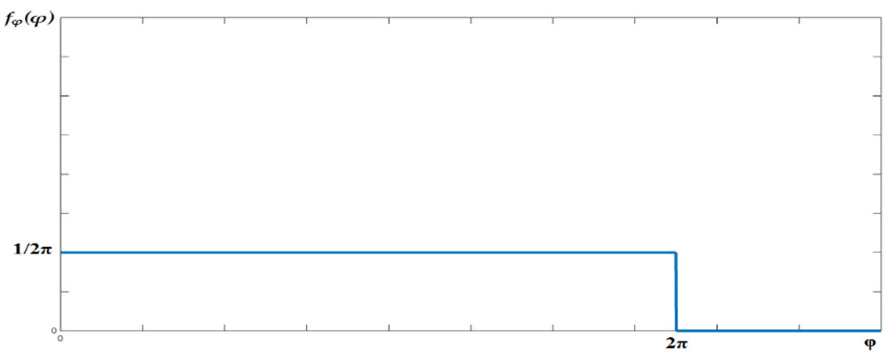


*Figure 3.2-3 – Probability density function of φ*

First, we study this last:

$$L_{rts} = -8.2 - 10\log(w) + 10\log(f) + 20\log(\Delta h_2) + L_{ori}$$

$$L_{ori} = \begin{cases} -10 + 0.354\varphi & for 0^{\circ} < \varphi < 35^{\circ} \\ 2.5 + 0.075(\varphi - 35) & for 35^{\circ} \leq \varphi \leq 55^{\circ} \\ 4.0 - 0.114(\varphi - 55) & for 55^{\circ} < \varphi \leq 90^{\circ} \end{cases}$$

$$\Delta h_2 = h_r - h_2$$

From these formulas we can see that the only term depending on $\varphi$ is $L_{ori}$. Since it is a piecewise function, we need to analyze each sub-term. First we linearize $L_{rts}$:

$$L_{rts} = 10^{\frac{-8.2}{10}} \frac{f}{w} \Delta h_2^2 10^{\frac{L_{ori}}{10}} = T 10^{\frac{L_{ori}}{10}}$$

where:

$$T = 10^{\frac{-8.2}{10}} \frac{f}{w} \Delta h_2^2$$

To evaluate the overall probability density function $f_{L_{rts}}(L_{rts})$ we have to verify that the integral of the pdf over the considered range $\varphi = [-60^{\circ}; +60^{\circ}]$ is one. Then the sum of the pdf integrals corresponding to each sub-term has to be one. In this way every pdf has to be normalized.

The first sub-term is defined for $0^{\circ} < \varphi < 35^{\circ}$ and the corresponding probability density function is:

$$f_{\varphi}(\varphi) = \frac{1}{\varphi_{max1} - \varphi_{min1}} = \frac{1}{35}$$

And

$$L_{ori} = -10 + 0.354\varphi$$

Then

$$L_{rts} = T 10^{-1} 10^{0.0354\varphi} = T' 10^{0.0354\varphi}$$

From here, we get:

$$\varphi = \frac{log\left(\frac{L_{rts}}{T'}\right)}{0.0354} = \frac{log(L_{rts}) - log(T')}{0.0354}$$

So, from the theory we need to evaluate $g'(\varphi) = \frac{d\varphi}{dL_{rts}} \stackrel{\text{def}}{=} g'(L_{rts})$:

$$g'(L_{rts}) = \frac{1}{0.0354}\frac{log(e)}{L_{rts}}$$

And then:

$$f_{L_{rts}}(L_{rts}) = \beta_1 \frac{1}{35}\frac{0.0354}{log(e)} L_{rts} = \beta_1 \gamma_1 L_{rts}$$

Where:

$$\gamma_1 = \frac{1}{35}\frac{0.0354}{log(e)}$$

$\beta_1$ is a normalization term that we have to introduce since the original pdf is uniform: in this way, we force the integral of $f_{L_{rts}}(L_{rts})$ to be equal to the corresponding sub-range:

$$\int_{L_{rtsmin1}}^{L_{rtsmax1}} f_{L_{rts}}(L_{rts})\, dL_{rts} = \frac{35}{120}$$

$$L_{rtsmin1} = L_{rts}|_{\varphi=0°} = 10^{\frac{-8.2}{10}} \frac{f}{w} \Delta h_2^2 10^{\frac{-10+0.354\varphi}{10}}\Big|_{\varphi=0°} = 10^{-1.82} \frac{f}{w} \Delta h_2^2$$

$$L_{rtsmax1} = L_{rts}|_{\varphi=35°} = 10^{\frac{-8.2}{10}} \frac{f}{w} \Delta h_2^2 10^{\frac{-10+0.354\varphi}{10}}\Big|_{\varphi=35°} = 10^{-0.581} \frac{f}{w} \Delta h_2^2$$

Then:

$$\int_{L_{rtsmin1}}^{L_{rtsmax1}} \beta_1 \gamma_1 L_{rts}\, dL_{rts} = \frac{1}{2}\beta_1\gamma_1 \left[{L_{rts}}^2\right]_{L_{rtsmin1}}^{L_{rtsmax1}}$$

$$= \beta_1 \frac{1}{70}\frac{0.0354}{log(e)}\left[\left(\frac{10^{-0.581} f \Delta h_2^2}{w}\right)^2 - \left(\frac{10^{-1.82} f \Delta h_2^2}{w}\right)^2\right] = \beta_1 \frac{1}{70}\frac{0.0354}{log(e)}\frac{f^2 \Delta h_2^4}{w^2} 0.0386$$

$$= \beta_1 \frac{4.494}{10^5}\frac{f^2 \Delta h_2^4}{w^2} \triangleq \frac{35}{120}$$

$$\Rightarrow \beta_1 = \frac{35}{120}\frac{10^5}{4.494}\frac{w^2}{f^2 \Delta h_2^4} \cong 6.5 \cdot 10^3 \frac{w^2}{f^2 \Delta h_2^4}$$

$$\Rightarrow f_{L_{rts}}(L_{rts}) = 6.5 \cdot 10^3 \frac{w^2}{f^2 \Delta h_2^4} \frac{1}{35} \frac{0.0354}{log(e)} L_{rts} \cong 15.14 \frac{w^2}{f^2 \Delta h_2^4} L_{rts}$$

The second sub-term is defined for $35^{\circ} < \varphi < 55^{\circ}$ and the corresponding probability density function is:

$$f_{\varphi}(\varphi) = \frac{1}{\varphi_{max2} - \varphi_{min2}} = \frac{1}{20}$$

And

$$L_{ori} = 2.5 + 0.075(\varphi - 35) = 0.075\varphi - 0.0125$$

Then

$$L_{rts} = T10^{-0.00125}10^{0.0075\varphi} = T''10^{0.0075\varphi}$$

From here, we get:

$$\varphi = \frac{log\left(\frac{L_{rts}}{T''}\right)}{0.0075} = \frac{log(L_{rts}) - log(T'')}{0.0075}$$

So, again:

$$g'(L_{rts}) = \frac{1}{0.0075} \frac{log(e)}{L_{rts}}$$

And then:

$$f_{L_{rts}}(L_{rts}) = \beta_2 \frac{1}{20} \frac{0.0075}{log(e)} L_{rts} = \beta_2 \gamma_2 L_{rts}$$

Where:

$$\gamma_2 = \frac{1}{20} \frac{0.0075}{log(e)}$$

$\beta_2$ is the normalization term.

$$\int_{L_{rtsmin2}}^{L_{rtsmax2}} f_{L_{rts}}(L_{rts})\, dL_{rts} = \frac{20}{120} = \frac{1}{6}$$

$$L_{rtsmin2} = L_{rts}|_{\varphi=35^\circ} = 10^{\frac{-8.2}{10}} \frac{f}{w} \Delta h_2^2 10^{\frac{0.075\varphi - 0.0125}{10}}\Big|_{\varphi=35^\circ} = 10^{-0.559} \frac{f}{w} \Delta h_2^2$$

$$L_{rtsmax2} = L_{rts}|_{\varphi=55^\circ} = 10^{\frac{-8.2}{10}} \frac{f}{w} \Delta h_2^2 10^{\frac{0.075\varphi - 0.0125}{10}} \bigg|_{\varphi=55^\circ} = 10^{-0.409} \frac{f}{w} \Delta h_2^2$$

Then:

$$\int_{L_{rtsmin2}}^{L_{rtsmax2}} \beta_2 \gamma_2 L_{rts} \, dL_{rts} = \frac{1}{2} \beta_2 \gamma_2 \left[ {L_{rts}}^2 \right]_{L_{rtsmin2}}^{L_{rtsmax2}} = \beta_2 \frac{1}{40} \frac{0.0075}{log(e)} \frac{f^2 \Delta h_2^4}{w^2} 0.704 = \beta_2 \frac{3.04}{10^4} \frac{f^2 \Delta h_2^4}{w^2} \triangleq \frac{1}{6}$$

$$\Rightarrow \beta_2 = \frac{1}{6} \frac{10^4}{3.04} \frac{w^2}{f^2 \Delta h_2^4} \cong 548.25 \frac{w^2}{f^2 \Delta h_2^4}$$

$$\Rightarrow f_{L_{rts}}(L_{rts}) = 548.25 \frac{w^2}{f^2 \Delta h_2^4} \frac{1}{20} \frac{0.0075}{log(e)} L_{rts} \cong 0.47 \frac{w^2}{f^2 \Delta h_2^4} L_{rts}$$

The last sub-term is defined for $55^\circ < \varphi < 60^\circ$ and the corresponding probability density function is:

$$f_\varphi(\varphi) = \frac{1}{\varphi_{max3} - \varphi_{min3}} = \frac{1}{5}$$

And

$$L_{ori} = 4.0 - 0.114(\varphi - 55) = 10.27 - 0.114\varphi$$

Then

$$L_{rts} = T 10^{1.027} 10^{-0.0114\varphi} = T''' 10^{-0.0114\varphi}$$

From here, we get:

$$\varphi = \frac{-log\left(\frac{L_{rts}}{T'''}\right)}{0.0114} = \frac{log(T''') - log(L_{rts})}{0.0114}$$

In this case, since the function is decreasing, we have to consider in $g'(x)$ the modulus of $\frac{dy}{dx}$:

$$g'(L_{rts}) = \frac{1}{0.0114} \frac{log(e)}{L_{rts}}$$

And then:

$$f_{L_{rts}}(L_{rts}) = \beta_3 \frac{1}{5} \frac{0.0114}{log(e)} L_{rts} = \beta_3 \gamma_3 L_{rts}$$

Where:

$$\gamma_3 = \frac{1}{5}\frac{0.0114}{log(e)}$$

$\beta_3$ is the normalization term.

$$\int_{L_{rtsmin3}}^{L_{rtsmax3}} f_{L_{rts}}(L_{rts})\, dL_{rts} = \frac{5}{120}$$

$$L_{rtsmin3} = L_{rts}|_{\varphi=60°} = 10^{\frac{-8.2}{10}}\frac{f}{w}\Delta h_2^2 10^{\frac{10.27-0.114\varphi}{10}}\Big|_{\varphi=60°} = 10^{-0.48}\frac{f}{w}\Delta h_2^2$$

$$L_{rtsmax3} = L_{rts}|_{\varphi=55°} = 10^{\frac{-8.2}{10}}\frac{f}{w}\Delta h_2^2 10^{\frac{10.27-0.114\varphi}{10}}\Big|_{\varphi=55°} = 10^{-0.42}\frac{f}{w}\Delta h_2^2$$

Then:

$$\int_{L_{rtsmin3}}^{L_{rtsmax3}} \beta_3\gamma_3 L_{rts}\, dL_{rts} = \frac{1}{2}\beta_3\gamma_3\left[L_{rts}{}^2\right]_{L_{rtsmin3}}^{L_{rtsmax3}} = \beta_3\frac{1}{10}\frac{0.0114}{log(e)}\frac{f^2\Delta h_2^4}{w^2}(0.035) = \beta_3\frac{9.18}{10^5}\frac{f^2\Delta h_2^4}{w^2} \triangleq \frac{5}{120}$$

$$\Rightarrow \beta_3 = \frac{5}{120}\frac{10^5}{9.18}\frac{w^2}{f^2\Delta h_2^4} \cong 453.89\frac{w^2}{f^2\Delta h_2^4}$$

$$\Rightarrow f_{L_{rts}}(L_{rts}) = 453.89\frac{w^2}{f^2\Delta h_2^4}\frac{1}{5}\frac{0.0114}{log(e)}L_{rts} \cong 2.38\frac{w^2}{f^2\Delta h_2^4}L_{rts}$$

Finally, since we are working only on a range of 60°, the sum of the three pdf integrals will be equal to $\frac{1}{2}$:

$$\int_{L_{rtsmin1}}^{L_{rtsmax1}} 15.14\frac{w^2}{f^2\Delta h_2^4}L_{rts}\, dL_{rts} + \int_{L_{rtsmin2}}^{L_{rtsmax2}} 0.47\frac{w^2}{f^2\Delta h_2^4}L_{rts}\, dL_{rts} + \int_{L_{rtsmin3}}^{L_{rtsmax3}} 2.38\frac{w^2}{f^2\Delta h_2^4}L_{rts}\, dL_{rts} \triangleq \frac{1}{2}$$

Now, we take in account the pathloss terms depending on the distance $d$, which are:

$$L_{bf} = 32.4 + 20log\left(\frac{d}{1000}\right) + 20log(f)$$

$$L_{msd} = \begin{cases} -\tanh\left(\frac{\log(d) - \log(d_{bp})}{\chi}\right)(L1_{msd}(d) - L_{mid}) + L_{mid} & \text{for } l > d_s \text{ and } dh_{bp} > 0 \\ L2_{msd}(d) & \text{for } dh_{bp} = 0 \\ L1_{msd}(d) - \tanh\left(\frac{\log(d) - \log(d_{bp})}{\zeta}\right) \cdot (L_{upp} - L_{mid}) - L_{upp} + L_{mid} & \text{for } l > d_s \text{ and } dh_{bp} < 0 \end{cases}$$

In particular, for our study case we can consider the sub-terms of $L_{msd}$ in which is $l > d_s$, since we can consider the building extension infinite. First, we linearize both functions:

$$\mathcal{L}_{bf} = \left(\frac{4\pi}{c} df\right)^2 = Kd^2$$

where:

$$K = \left(\frac{4\pi}{c} f\right)^2$$

And:

$$\mathcal{L}_{msd} = \begin{cases} 10^{\frac{-\tanh\left(\frac{\log(d) - \log(d_{bp})}{\chi}\right)(L1_{msd}(d) - L_{mid})}{10}} 10^{\frac{L_{mid}}{10}} & \text{for } dh_{bp} > 0 \\ 10^{\frac{L2_{msd}(d)}{10}} & \text{for } dh_{bp} = 0 \\ 10^{\frac{L1_{msd}(d)}{10}} \, 10^{\frac{-\tanh\left(\frac{\log(d) - \log(d_{bp})}{\zeta}\right)(L_{upp} - L_{mid})}{10}} 10^{\frac{-L_{upp}}{10}} \, 10^{\frac{L_{mid}}{10}} & \text{for } dh_{bp} < 0 \end{cases}$$

The whole pathloss term depending on $d$ is:

$$\mathcal{L}_d(d) = \mathcal{L}_{msd}\mathcal{L}_{bf}$$

In order to show a numerical example of the behavior of the function $\mathcal{L}_d(d)$, we plot it used the following parameters:

- Frequency: $f = 800MHz$;
- Average building level: $b = 30m$;
- Distance between rooftops and antennas: $\Delta h_1 = 2m$.

With these assumptions, the formula becomes:

$$L_d(d) = 32.4 + 20\log(d) + 20\log(800) - \tanh\left(\frac{\log(d) - 0.51}{0.1}\right)(19.9 + 18\log(d) + 3.7) - 3.7$$

We show its logarithmic and its linear behavior, evaluated for $dh_{bp} > 0$. Note that in case of $dh_{bp} < 0$ the trend of the function is the same.

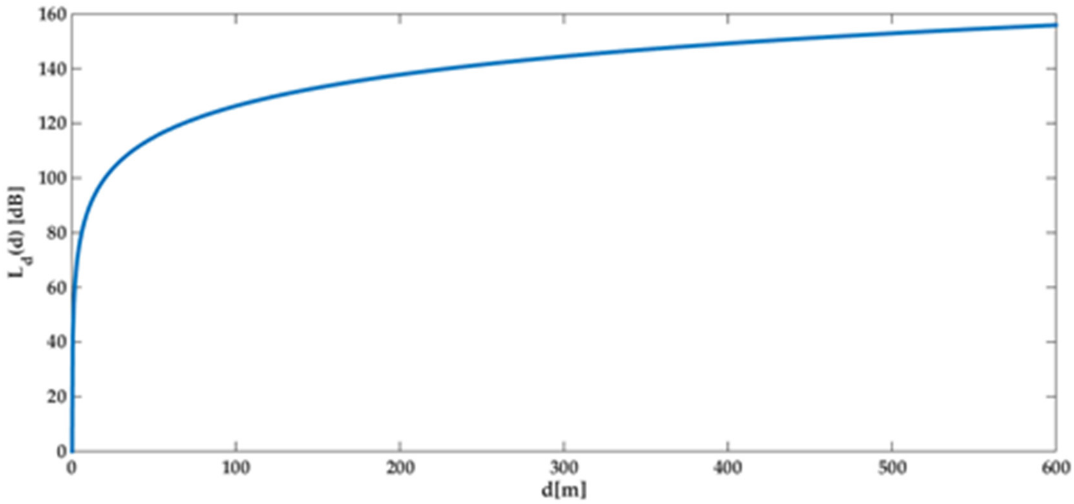


*Figure 3.2-4 – Qualitative behavior in log scale for* $dh_{bp} > 0$

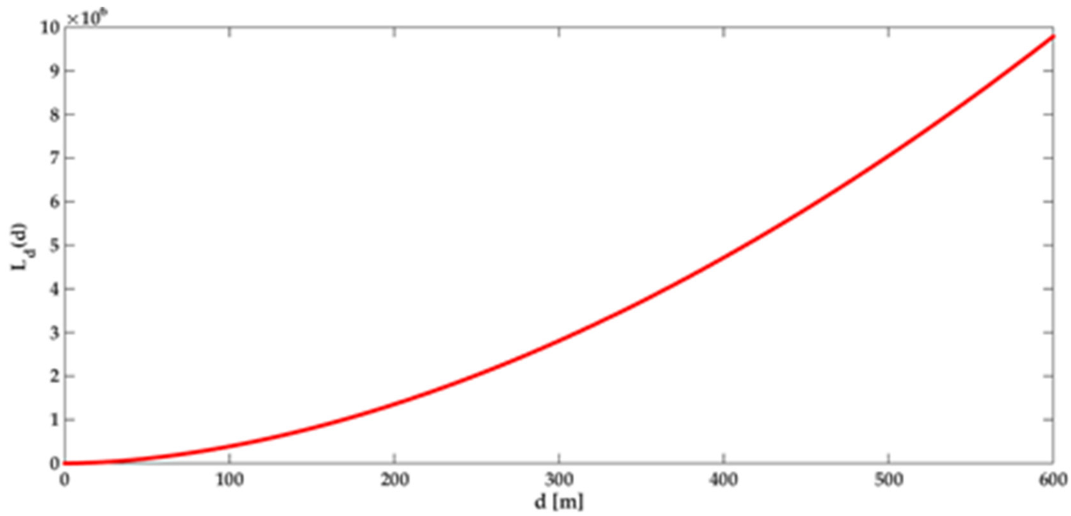


*Figure 3.2-5 – Qualitative behavior in linear scale for* $dh_{bp} > 0$

As we can see in the figures, both in logarithmic and linear behavior, the dominant term is the one referring to the free-space loss. It is impossible to make the calculus to get the pdf of this function in closed form, due to the high complexity in evaluating the inverse function of the pathloss. For this reason, we have to approximate it with an even function like the one we propose (in linear scale):

$$\hat{L}_d(d) = Ad^4 + Bd^2$$

where $A$ and $B$ are constants that have to represent all the constant terms in $L_d(d)$. Once the constants are determined, it is possible to develop the same calculus made for the pathloss term depending on the orientation and to obtain a qualitative probability density function $f_{\hat{L}_d}(\hat{L}_d)$. We can follow the same theory described for $L_{rts}$, supposing once again to have for $d$ an uniform pdf:

$$f_d(d) = \frac{1}{d_{max} - d_{min}}$$

$$g(\hat{L}_d) = \frac{1}{\sqrt{2}} \left[ \frac{B\sqrt{4A\hat{L}_d + B^2} - 2A\hat{L}_d - B^2}{2\hat{L}_d{}^2\sqrt{4A\hat{L}_d + B^2}\sqrt{\frac{\sqrt{4A\hat{L}_d + B^2} - B}{\hat{L}_d}}} \right]$$

$$f_{\hat{L}_d}(\hat{L}_d) = \frac{\sqrt{2}}{d_{max} - d_{min}} \frac{2\hat{L}_d{}^2\sqrt{4A\hat{L}_d + B^2}\sqrt{\frac{\sqrt{4A\hat{L}_d + B^2} - B}{\hat{L}_d}}}{B\sqrt{4A\hat{L}_d + B^2} - 2A\hat{L}_d - B^2}$$

Now, we should define the pdf relative to the overall path loss function $L_A(d, \varphi)$, including the terms depending on $d$ and on $\varphi$. The overall path loss function in linear scale is:

$$L_{NLOS}(d, \varphi) = L_d(d)L_{rts}(\varphi)$$

Since this is the product of two independent random process, to evaluate the overall probability density function $f_{L_{NLOS}}(L_{NLOS})$ we need to apply the following procedure, as expressed in theory.

If $X$ and $Y$ are two random variables, let $Z$ be their product $Z=XY$. Then, we may find the product distribution as follows:

$$f_Z(z) = \int_{-\infty}^{\infty} \frac{1}{|u|} f_X(u) f_Y\left(\frac{z}{u}\right) du$$

To demonstrate it, we need to suppose that the distribution of $X$ is continuous in the origin

$$P(Z \le z) = P(XY \le z) = P\left(Y \le \frac{z}{X}\middle| X > 0\right) P(X > 0) + P\left(Y \ge \frac{z}{X}\middle| X > 0\right) P(X > 0)$$

$$= \int_0^{\infty} P\left(Y \le \frac{z}{u}\right) f_X(u)du + \int_{-\infty}^{0} P\left(Y \ge \frac{z}{u}\right) f_X(u)du$$

Then, to get the pdf, we need to derivate

$$f_Z(z) = \int_0^{\infty} \frac{1}{u} f_Y\left(\frac{z}{u}\right) f_X(u)du + \int_{-\infty}^{0} \frac{-1}{u} f_Y\left(\frac{z}{u}\right) f_X(u)du = \int_{-\infty}^{\infty} \frac{1}{|u|} f_X(u) f_Y\left(\frac{z}{u}\right) du$$

In our case study this formula becomes:

$$f_{L_{NLOS}}(L_{NLOS}) = \int_{-\infty}^{\infty} \frac{1}{|u|} f_{L_d}(u) f_{L_{rts}}\left(\frac{L_{NLOS}}{u}\right) du$$

Once the propagation loss is determined, we can evaluate the power received by a node, determined as follows:

$$P_{R_{dB}} = P_{T_{dB}} - A_{dB}$$

where $P_{R_{dB}}$ is the received power by the node, $P_{T_{dB}}$is the sounding power transmitted by each UE and $A_{dB}$ is attenuation due to the overall pathloss. From the received power, each node along with its noise figure and the inter-UE interference, evaluates the Signal-To-Interference-Plus-Noise-Ratio:

$$SINR(x) = \frac{P_R(x)}{I + N}$$

From the SINR the node can evaluate the quality of the uplink channel and assign all the features, for each UE, which will characterize the transmission, as shown in the block diagram presented previously. In particular, the node will communicate to the UE the index of the subcarrier to use for the uplink transmission, the MCS (Modulation and Coding Scheme) index and its coverage level. Depending on this last parameter, the UE must define a number of repetitions to apply in the uplink transmission.

## 3.3 Analytical model

Our aim is to evaluate the performance of a NB-IoT system: we are interested in assessing the ability of the system to serve all users in the considered area. In a given period, each transmitting UE must be able to access the cell and disposing of the IP traffic, according to the predetermined traffic model. In particular, we are interested in evaluating how the implementation of coverage enhancement levels and consequently of repetitions, affects the system capacity and the performances of the overall transmission. In order to estimate the quality of this uplink transmission, we choose to evaluate the efficiency of the system, operating a measure of a parameter like the system Goodput. In detail, we define the *Efficiency* $\eta$ as the ratio between the number of packets received correctly by the nodes within the considered period ($C_R$), and the number of packets that the overall set of UE has transmitted to the nodes ($C_T$). In our results, we will see the throughput at RLC level: the real throughput will be lower, because of the introduction of overheads necessary for passing from the lowest layers to the RLC. It is still possible to quantify these overheads in order to evaluate the real throughput. Note that we are not interested in the real time throughput, as defined in theory. Since we are considering a delay tolerant transmission, we do not want to assess the speed with which traffic is being disposed of, but only the amount of packets that can be transmitted and so the numbers of UEs that the system is able to serve during the simulation time. We also consider the five EnodeB connected to the same remote host: we will estimate the UDP traffic at the remote host, summing the transmissions coming to each node.

We can describe the analytical formula of the *Efficiency* $\eta$ that we want to measure in our simulation. Since we must consider only an Uplink transmission, in order to determine $\eta$ we have first to evaluate the amount of packets $C_T$ that the overall set of UE transmits to the remote host during the considered time interval. $C_T$ depends on all variables that characterize uplink transmission in NB-IoT. We assume the distribution of the devices in the area we are considering as uniform. Once all users have first accessed the cell, having zero mobility, their position will be deterministic. The payload size is constant. As shown in propagation model, the probability density function of the MCS index used for the transmission cannot be evaluated since is not possible to calculate the pdf of the propagation loss in closed form. In addition, the transmission frequency for each user is a deterministic variable: the whole timing in uplink depends on when j-th UE access first the cell and send the first data to the EnodeB. For this reason, we can say that the randomness in a NB-IoT scenario is contained only in the time instant in which j-th UE starts transmitting: we call this random variable $t_0^j$, the transmission start time relative to the j-th UE. We can consider for $t_0^j$ a uniform probability density function: using this assumption we are considering the worst case in which all the users has the same probability to transmit in every time instant. We define the variable $P_{i,j}^T$ as the i-th packet sent by the j-th UE to the core network: it depends on the transmission start time $t_0^j$. Since $P_{i,j}^T$ depends on a random variable, $C_T$ also depends on a random variable and so we have to consider it a stochastic process. The resulting formula of $C_T$ will be the sum of that $P_{i,j}^T$ over all the set of UEs, in the whole simulation time (we consider a sum since we assume to have discrete time domain):

$$C_T = S \sum_{j=1}^{N} \sum_{i=1}^{P_{maxj}{}^T\left(t_0^j, f_t^j\right)} P_{i,j}^T\left(t_0^j\right)$$

Where:

$S$ = Packet size;

$N = N_n N_s N_{ue}$: Number of considered UEs;

$N_n$: Number of nodes;

$N_s$ = 3: Number of cell-site sector;

$N_{ue}$: Number of UE per cell-site sector;

$j$: UE index;

$i$: Packet index;

$f_t$: Transmission frequency, determined for each UE as described previously;

$P_{maxj}{}^{T}(t_0^j, f_t^j)$: Max number of packets that $UE_j$ sends during simulation time.

Note that $P_{maxj}{}^{T}(t_0^j, f_t^j)$ depends on the transmission start time and the transmission frequency relative to the j-th UE: for different values of $t_0^j$ and/or $f_t^j$, $UE_j$ has to send a different number of packet in the same time interval.

We can consider the same assumptions for $C_R$, the number of packets received correctly by the nodes within the considered period. In this case, we call $P_{i,j}^R$ the i-th packet sent by the j-th UE, received, and correctly decoded by the core network. Consequently, $P_{maxj}{}^{R}(t_0^j, f_t^j)$ represents the max number of packets received by the node from the j-th UE. The reception of those packets depends on the propagation loss and on the inter-user interference, which determines the quality of the uplink channel for each UE. $P_{i,j}^R$ is again a stochastic process since it depends on the random variable $t_0^j$: $C_R$ is also a stochastic process. The correspondent formula for $C_R$ is:

$$C_R = S \sum_{j=1}^{N} \sum_{i=1}^{P_{maxj}{}^{R}(t_0^j, f_t^j)} P_{i,j}^R(t_0^j)$$

Finally we have a formula for the *Efficiency* $\eta$, that consequently has to be considered a stochastic process:

$$\eta = \frac{C_R}{C_T} = \frac{S \sum_{j=1}^{N} \sum_{i=1}^{P_{maxj}{}^{R}(t_0^j, f_t^j)} P_{i,j}^R(t_0^j)}{S \sum_{j=1}^{N} \sum_{i=1}^{P_{maxj}{}^{T}(t_0^j, f_t^j)} P_{i,j}^T(t_0^j)}$$

Since the pdf of parameters characterizing the transmission as the propagation loss cannot be calculated in closed form, we cannot obtain a determined behavior for the distribution of the efficiency $\eta$. From the results of each simulation we evaluate a particular realization of the whole random process $\eta$. Repeating the simulation n times, changing the initial conditions of the system, we will get a set of results from which it is possible to extract the efficiency distribution and its average value. The block diagram in Figure 3.3-1 summarize the overall behavior of the NPUSCH chain of the whole system.

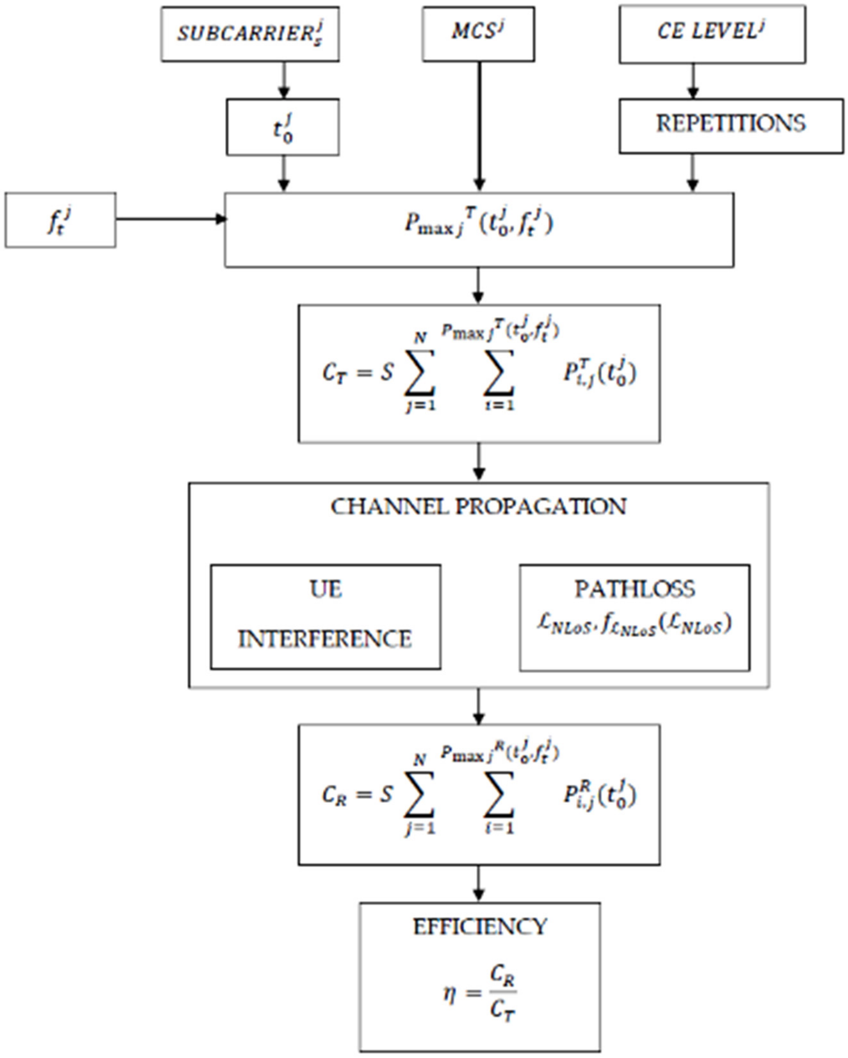


*Figure 3.2-1 – NPUSCH chain*

In addition to this scenario, we need to model the effect of the Random Access Procedure that a user does when it want to connect to the network. This procedure is defined as *Contention Based*: when two or several UE try to access the network picking the same preamble in the same time interval, the node has to schedule the connection in order to give UE a contention resolution message. This procedure will affect the uplink transmission, delaying transmission for those devices that cannot access the network at the first connection attempt.

# 4 Network simulator-3

## 4.1 Architecture

Ns-3 is a discrete-event network simulator for Internet systems, developed primarily for research and educational use. The goal of the ns-3 project is to develop an open simulation environment for networking research. In order to reach the goal the simulator has to be aligned with the needs of modern networking research, encouraging community contribution, review, and validation of the software. Ns-3 is built as a C++ library: it implements different network simulation models as C++ object, wrapped in python. Users can deploy the simulation scenario of interest writing an application in C++ or python.

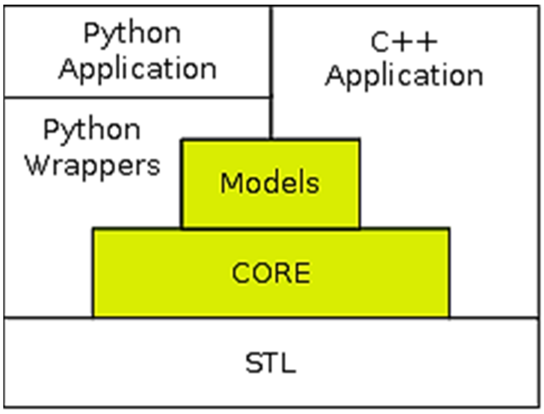


*Figure 4.1-1 – Ns-3 key technologies (nsnam.org)*

Even if ns-3 is designed as a set of libraries, in order to interpret simulations, we can use different animators or data analysis tools. Simulation models in ns-3 are sufficiently realistic to allow the use of ns-3 as a real-time network emulator: ns-3 also supports a real-time scheduler that facilitates a number of "simulation-in-the-loop" use cases that allows the user to interact with real systems. Since it is a discrete-event network simulator, the simulation run as a sequence of events executed in the same order the user call them. Once the current event in ended, the next one can start. Each event is able to call other new events, building the simulation continuous time flow. Ns-3 source code is included in the directory *src*, organized as in the figure below.

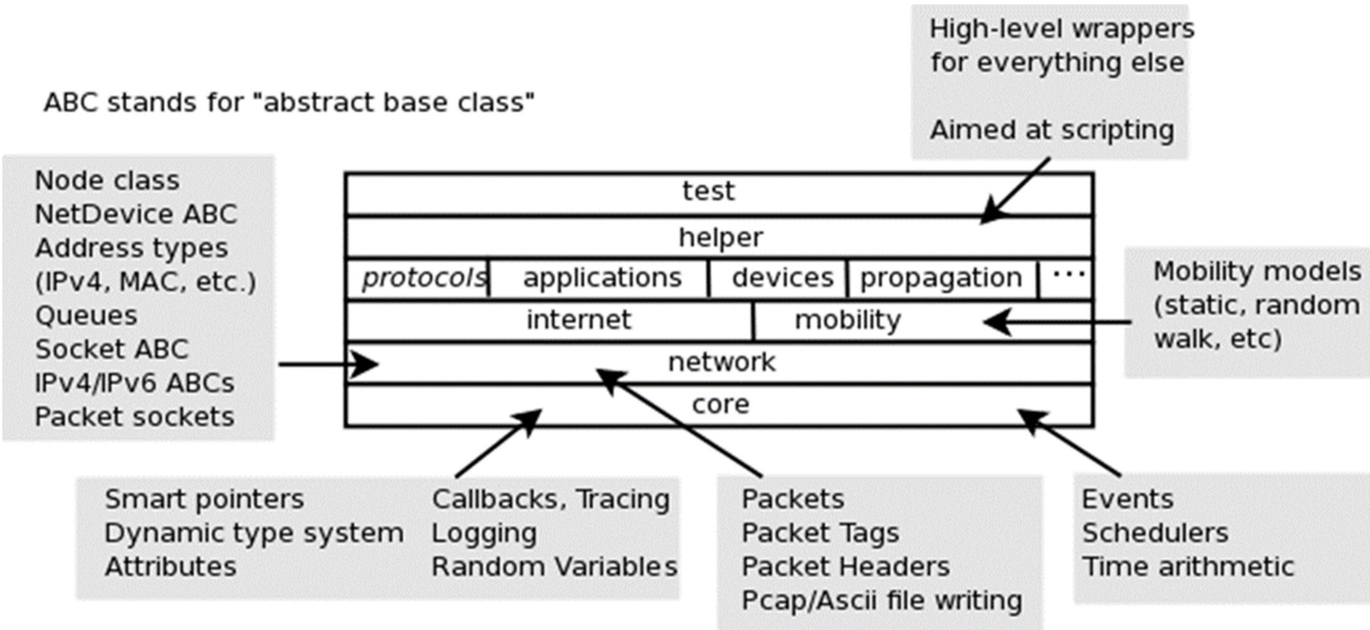


*Figure 4.1-2 – Ns-3 source code organization (nsnam.org)*

We can summarize the simulator behavior in the following concepts.

- *Event*: is something scheduled to happen at a given time. It represents in general the occurrence of something changing the status of a system component. Each event is represented by a time of execution and some parameters, like the component it is going to modify and the variable used. A discrete-event simulator orders events and executes them sequentially.
- *Node*: is an object that aggregates other objects. In Interne, a computing device that connects to a network is called *host*. Because *ns-3* is a *network* simulator, not specifically an *Internet* simulator, we use a more generic term proper of the Graph Theory — the *node*.
- *NetDevice*: is the logical representation of a communication interface in layer 2 (L2). It is installed in a Node in order to allow them to communicate with other Nodes in the simulation via Channels. As in a real case, a Node may be connected to several Channels via multiple NetDevices.
- *Channel*: is the logical connections between two NetDevices. Channels represent the effect of the signal transmission over a medium: they represent the

propagation loss due to the medium and the interference from other sources. A channel can be wired or wireless.

- *Protocol*: is the representation of a specific high-level protocol, such as IPv5, IPv6 or ICMP. Since protocols are implemented following the standards, there is no difference between ns-3 protocol behavior and the corresponding real one.
- *Application*: is responsible of the generation of data traffic, according to specific statistical distributions, and of data reception. Applications in general represent traffic generators or a data sinks.
- *Attributes*: represent the way to change an object properties.

Ns-3 is organized in modules, each one carrying a single functionality. In the next sections, we provide a brief description of the modules in which we are mainly interested.

### 4.1.1 Internet Module

Internet Module in ns-3 implements a several functionalities belonging to the TCP/IP stack, such as:

- IP (v4 and v6);
- ICMP (v4 and v6);
- UDP;
- TCP.

Some routing protocols are included in this module like Static Routing.  Some notable missing functionalities are:

- Media Independent handover (MIH);
- DHCPv4 and DHCPv6;
- Mobile IP / NEMO / PMIP.

We use this module, in combination with the Application Module, to configure the IP addresses of the core network and of the devices.

### 4.1.2 Application Module

Application Module in ns-3 provides the applications available for each node placed in the simulation scenario. To create an API, it is necessary to define a socket, that can be both TCP and UDP, and that can be selected by modifying the *PacketSink* module. Finally, there are client classes that allow us to set the parameters for the data flow.

### 4.1.3 LTE Module

This is the main module we use in our simulation. According to the LTE structure showed previously, the LTE module is composed of the following two main components.

1. The *LTE model*, that includes the overall LTE Radio Protocol stack (RRC, PDCP, RLC, MAC and PHY layers). These entities reside within the UE and eNB nodes.
2. The *EPC model*, which includes core network interfaces, protocols and entities. Entities and protocols reside within the PGW, SGW, MME, and in part in the eNB nodes.

*Figure 4.1.1-1* presents an overview of the LTE Module general architecture.

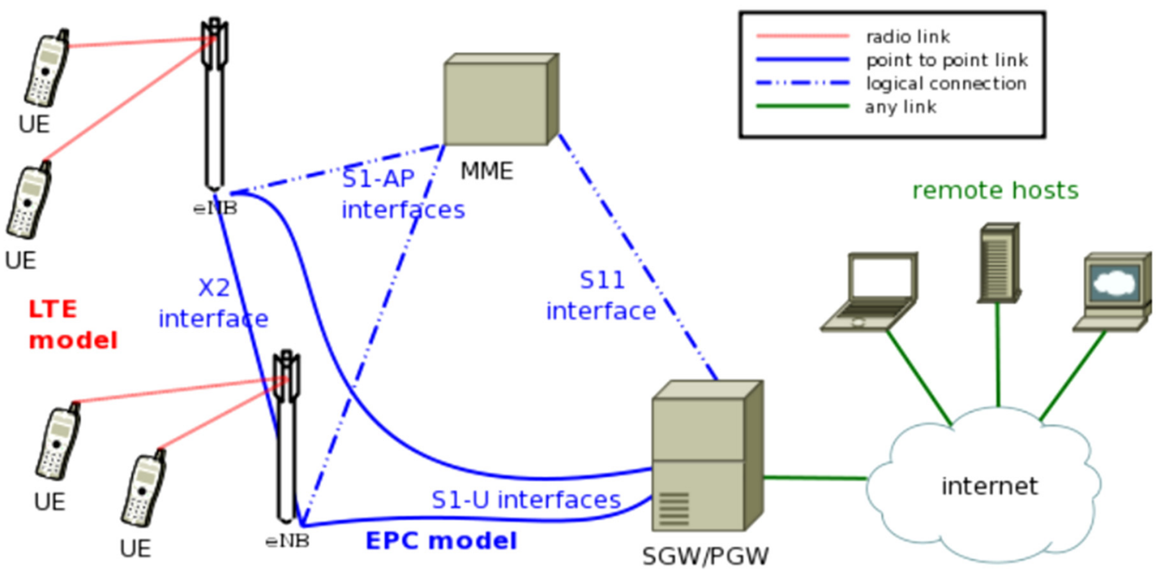


*Figure 4.1.1-1 – LTE module general structure (nsnam.org)*

The LTE model supports the evaluation of the main aspects of an LTE system, such as:

- Radio resource management;
- QoS-aware packet scheduling;
- Inter-cell interference coordination;
- Dynamic spectrum access

The simulator is able to scale up to tens of eNBs and hundreds of UEs, with the possibility to configure different cells in order to use different bandwidths and different carrier frequencies. The granularity of the model at radio level is at least that of the Resource Block (RB), since this is the fundamental unit used for the resource allocation. This granularity level allows the simulator to model accurately both packet scheduling and inter-cell interference. To represent fairly the resource scheduling of a real LTE system, LTE model supports the MAC scheduler API published by the FemtoForum (FFAPI).

The EPC model implements in simulation the end-to-end IP connectivity over the LTE model. It supports the interconnection of several UEs to the internet, via a radio access network of multiple eNBs connected to a single SGW/PGW node (both entities functionalities are included in the same node). The only Packet Data Network (PDN) type supported in simulation is IPv4. The EPC model is built to simulate the end-to-end performance of a realistic use case, so it allows the use of any regular ns-3 application working on TCP or UDP. It’s also possible for a single UE to use different applications with different QoS profiles; so multiple EPS bearers are supported for each UE. EPC model supports the X2-based handover between two eNBs.

As seen before, SGW and PGW functionalities in the simulator are included in a single node. This simplification leads to the removal of S5 and S8 interface between LTE and EPC model. This is the only assumption done to simplify the model: all the other layers and interfaces are included as specified by standard 3GPP. *Figure 4.1.1-2* shows a representation of hoe the end-to-end LTE-EPC data plane protocol stack is implemented in the simulator.

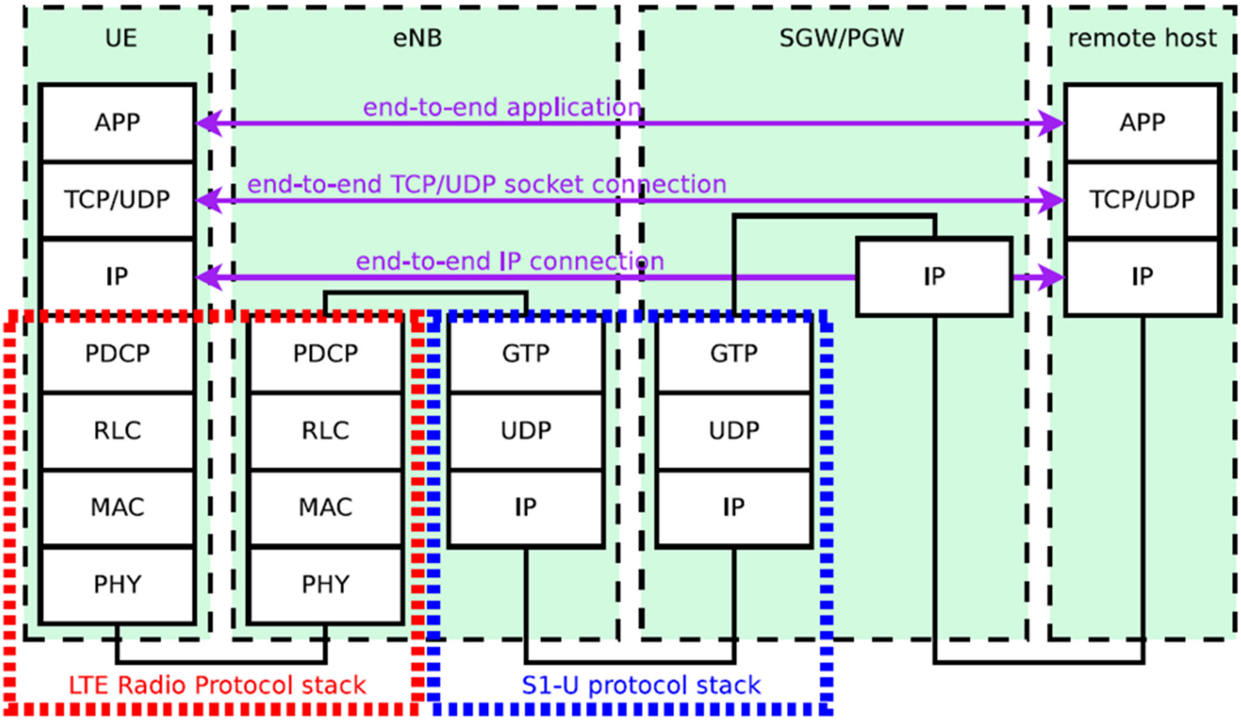


*Figure 4.1.1-2 – LTE-EPC data plane protocol stack (nsnsm.org)*

Channel propagation in LTE module is modelled using the *SpectrumChannel* interface provided by the *Spectrum model*. The simulator gives the possibility to set the propagation model through the *Building module*, which is built properly over LTE module to represent the pathloss due to reflection, diffraction and attenuation caused by the propagation in an urban area. The LTE module also includes a trace-based fading model derived from the one developed during the GSoC 2010. Antennas can be modelled In LTE PHY model via the ns-3 *AntennaModel* class: for instance, it is possible to set a Cosine, Parabolic or Isotropic antenna model (Isotropic is used by default).

The physical layer model is very fair to the one described in standards. It includes the inter cell interference calculation and the simulation of uplink traffic, including both packet transmission and CQI generation. As seen in LTE standards description, the subframe is divided into control and data part. *Figure 4.1.1-3* shows this division focusing on the physical channel implemented both in downlink and in uplink.

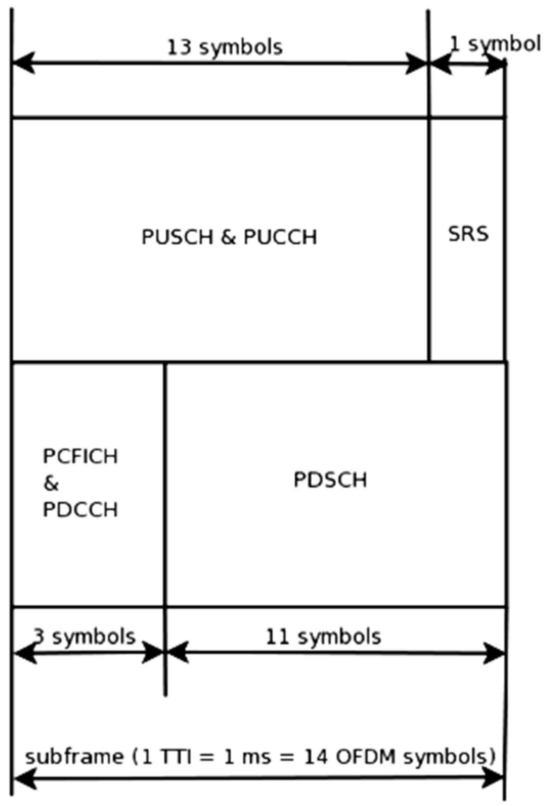


*Figure 4.1.1-3 – LTE subframe division (nsnam.org)*

The simulator includes an error model for the data plane as the one defined in the standard link-to-system mapping (LSM) techniques. This represents properly an OFDMA radio transmission technology. In particular, the specific LSM method adopted is the one based on the usage of a mutual information metric known as Mutual Information Effective SINR Mapping (MIESM). LSM allows the usage of the Code Block Error Rate curves as the parameter to analyze the performance of a single link. Ns-3 uses Vienna LTE Simulator for the extraction of the link layer and the MIESM.

Medium Access Control (MAC) model in LTE module describes how resource allocation is handled in LTE, including the effects of the Adaptive Modulation and Coding (AMC). The simulator provides two AMC models. The former is the result of a model proposed by ns-3 authors themselves, and is described as follows: let $i$ be a generic user and $\gamma_i$ be its SINR. The spectral efficiency $\eta_i$ evaluation is described by the formulas:

$$\eta_i = log_2\left(1 + \frac{\gamma_i}{\Gamma}\right)$$

$$\Gamma = \frac{-ln(5 \cdot BER)}{1.5}$$

$$BER = 0.00005$$

The spectral efficiency depends directly on the value measured for the channel quality indicator (CQI), and is mapped to the corresponding MCS scheme.

The latter model, according to the physical error model described in standards, base the MCS selection to the actual PHY layer performance, evaluated via CQI report.

Among the different schedulers provided by ns-3 in the MAC scheduler interface, we choose the PF Scheduler (Proportional Fair) in our simulation. We now show a brief description of the scheduler behavior. We define as$i, j$ the index referring to generic users. $t$ is the subframe index and $k$ the resource block index. $M_{i,k}(t)$ represents the MCS usable by user$i$ on resource block $k$ according to what reported by the AMC model, and $S(M, B)$ represents the TB size in bits for the case where a number $B$ of resource blocks is used. The achievable rate $R_i(k, t)$ in bit/s for user$i$ on resource block group$k$ at subframe $t$ is defined by the formula

$$R_i(k, t) = \frac{S\big(M_{i,k}(t), 1\big)}{\tau}$$

where

$\tau$ : TTI duration.

The index $\hat{\imath}_k(t)$ to which RBG $k$ is assigned at time $t$ is described by the formula

$$\hat{\imath}_k(t) = \underset{j=1,\dots,N}{argmax} \left( \frac{R_j(k, t)}{T_j(t)} \right)$$

where

$T_j(t)$ : past throughput performance perceived by the user $j$.

Then an user can be allocated to different RBGs, adjacent or not, depending on the condition of the channel and the past throughput performance $T_j(t)$, determined at the end of the subframe $t$ as:

$$T_j(t) = \left(1 - \frac{1}{\alpha}\right) T_j(t-1) + \frac{1}{\alpha} \hat{T}_j(t)$$

where

$\alpha$ : time constant of the exponential moving average;

$\hat{T}_j(t)$ : current throughput achieved by the user $i$ in the subframe $t$.

#### 4.1.4 Propagation and Spectrum Module

The Propagation Module implements complex propagation and error models on the transmission of wireless signals. Several channel model are included in ns-3, such as Friis, Okamura-Hata and an attenuation model due to the presence of buildings in the channel. Depending on the propagation conditions and Tx/Rx parameters that the user can set in simulation, such as antenna gains and channel models, transmission power associated to each signal is attenuated and delayed.

The Spectrum model describes each transmitted packet as a signal with its relative power spectral density representation. This allows taking into account mutual interference between signals, even considering out-of-band spectral components.

The goal of both models is to provide a measure of the received packet signal power along with the noise (both thermal and interference noise). It is up to the receiver to convert the power into a Bit Error Rate (BER) and to evaluate, by using a simple statistical approach, if a certain packet has been received correctly or not.

#### 4.1.5 Mobility Module

This module allows to set the position and the mobility of the nodes placed in simulation by setting the coordinates of the positions and direction and speed that the considered node has to assume in this movement. It is possible to choose how to position a determined device among the following position allocators:

- ListPositionAllocator;
- GridPositionAllocator;
- RandomRectanglePositionAllocator;
- RandomBoxPositionAllocator;
- RandomDiscPositionAllocator;
- UniformDiscPositionAllocator.

Depending on the allocator chosen, the position can be defined either randomly or assigning precisely the coordinates. There is also the possibility to set many different kinds of mobility for the nodes:

- ConstantPosition;
- ConstantVelocity;
- ConstantAcceleration;
- GaussMarkov;
- Hierarchical;
- RandomDirection2D;
- RandomWalk2D;
- RandomWaypoint;
- SteadyStateRandomWaypoint;
- Waypoint.

#### 4.1.6 Flow Monitor Module

This module offers a flexible performance calculator that allows the user to read the simulation results in an easier way. Flow Monitor works only at IP level and provide several output such as the transmitted and received bytes and packets, the lost packets, the duration of the transmission and the throughput. All these parameters are evaluated both for downlink and uplink transmissions.

## 4.2 Assumptions and changes

In this paragraph, we give a description of the implementation choices done when simulating, due to the necessity to overcome some limitations of the simulator in order to implement properly the main features of a NB-IoT system. In fact, the simulator features are continuously renewing and enhancing but it does not provide yet any NB-IoT functionalities. For this reason, since this technology is built upon LTE functionalities, we have applied some substantive changes to the LTE model in ns-3 with the aim of forcing it to work according to the characteristics of a NB-IoT system.

In this simulator, the tri-sector antenna is not available as a single entity: we implement each tri-sectorial node placing in the scenario three antennas in the same point, setting their orientations according to the scenario described in *Section 3*. The model chosen for the antennas is the CosineAntennaModel, characterized by a 3 dB beamwidth = 60°, a shift angle of 120° and gain that can be 15 or 20 dB. Orientations and gains value for each antenna are set in order to maximize the coverage in the area of interest: we will develop a detailed coverage analysis in the next section. Each antenna has a 23 m height with respect to the ground level and works at frequency of 800 MHz. We can select the system frequency setting for each antenna the value of EUTRA Absolute radio-frequency channel number (Earfcn), according to the table below. In our case study, we have to work on the mid uplink frequency of frequency band 20.

| E-UTRA Operating Band | Downlink | | | Uplink | | |
|---|---|---|---|---|---|---|
| | Low | Mid | High | Low | Mid | High |
| 20 | 6200 | 6300 | 6400 | 24200 | 24300 | 24400 |

*Table 2.3-1 – Frequency band and Earfcn (3GPP)*

The transmission is deployed only on uplink channel. Since we work on the LTE module, is not possible by definition use in transmission one Physical Resource Block. In particular, LTE module in ns-3 allows the use of 6, 15, 25, 50, 75 or 100 PRB: each of these values corresponds to a different bandwidth in transmission, e.g. 50 PRB correspond to a 10 MHz bandwidth (this is the value set by default). We can allow the use of different numbers of PRB by modifying the libraries lte-enb-net-device.cc (r. 226) and lte-ffr-algorithm.cc (r.94). We show an example of the UL bandwidth definition in the source code below.

```
void
LteEnbNetDevice::SetUlBandwidth (uint8_t bw)
{ NS_LOG_FUNCTION (this << uint16_t (bw));
  switch (bw)
      {
      case 6:
      case 15:
      case 25:
      case 50:
      case 75:
      case 100:
      m_ulBandwidth = bw;
      break;
      default:
      NS_FATAL_ERROR ("invalid bandwidth value " << (uint16_t) bw);
      break;
```

```
    }
}
```

The minimum number of PRB we can physically use in transmission is 7: with less than these resource blocks, an UE fails to complete the random access procedure and cannot connect to the network. In our simulation, we choose to use 12 PRBs in transmission in order to maintain frequency proportionality with the 12 subcarriers used in NB-IoT uplink channel. This implementation choice is allowed since we are simulating a NB-IoT in in-band operation mode without implementing at the same time an LTE system: no frequency resources that are in general dedicated to LTE are used and consequently we can use them for NB-IoT transmission. This leads to a distribution of the packets that we have to transmit on a greater bandwidth: we must compensate this effect introducing in the packetsize a normalization factor = 12 (in order to increment the transmitted data flow of this factor). We can set 12 PRB in the simulator adding a "`case 12`" in the switch reported previously. All these features are chosen according to the datasheets of the antenna used in a commercial cellular network. According to what is described in *Section 3.1 – Propagation model*, we implement a time-variant channel representing a high dense urban scenario. Ns-3 provides the implementation of the model defined by *Recommendation ITU-R P.1411-8*: we have to define the frequency band and the rooftop level, while the dense urban scenario is set by default. Ns-3 simulator provides the following transmission modes:

- Transmission Mode 0 - SISO;
- Transmission Mode 1 - MIMO;
- Transmission Mode 2 - MIMO Open Loop.

In our case study, we simulate a SISO UL transmission setting the transmission mode TM0.

We report below the definition of a three-node antenna as implemented in the code:

```
lteHelper->SetEnbAntennaModelType ("ns3::CosineAntennaModel");

      lteHelper->SetEnbAntennaModelAttribute ("Orientation", DoubleValue (10));

      lteHelper->SetEnbAntennaModelAttribute ("Beamwidth",  DoubleValue (60));

      lteHelper->SetEnbAntennaModelAttribute ("MaxGain", DoubleValue (20.0));

      lteHelper->SetEnbDeviceAttribute ("UlEarfcn", UintegerValue (24300));

      lteHelper->SetEnbDeviceAttribute ("UlBandwidth", UintegerValue (12));

      lteHelper→SetAttribute ("PathlossModel", StringValue ("ns3::ItuR1411NlosOverRooftopPropagationLossModel"));

      lteHelper->SetPathlossModelAttribute ("Frequency", DoubleValue (800e6));

      lteHelper->SetPathlossModelAttribute ("RooftopLevel", DoubleValue (15.0));

      enbDevs.Add ( lteHelper->InstallEnbDevice (enbNodes1.Get (0)));


      lteHelper->SetEnbAntennaModelType ("ns3::CosineAntennaModel");

      lteHelper->SetEnbAntennaModelAttribute ("Orientation", DoubleValue (120));

      lteHelper->SetEnbAntennaModelAttribute ("Beamwidth",  DoubleValue (60));

      lteHelper->SetEnbAntennaModelAttribute ("MaxGain", DoubleValue (15.0));

      lteHelper->SetEnbDeviceAttribute ("UlEarfcn", UintegerValue (24300));

      lteHelper->SetEnbDeviceAttribute ("UlBandwidth", UintegerValue (12));

      lteHelper->SetAttribute ("PathlossModel", StringValue ("ns3::ItuR1411NlosOverRooftopPropagationLossModel"));

      lteHelper->SetPathlossModelAttribute ("Frequency", DoubleValue (800e6));


      lteHelper->SetPathlossModelAttribute ("RooftopLevel", DoubleValue (15.0));

      enbDevs.Add ( lteHelper->InstallEnbDevice (enbNodes1.Get (1)));


      lteHelper->SetEnbAntennaModelType ("ns3::CosineAntennaModel");

      lteHelper->SetEnbAntennaModelAttribute ("Orientation", DoubleValue (280));

      lteHelper->SetEnbAntennaModelAttribute ("Beamwidth",  DoubleValue (60));
```

```
lteHelper->SetEnbAntennaModelAttribute ("MaxGain", DoubleValue (20.0));

lteHelper->SetEnbDeviceAttribute ("UlEarfcn", UintegerValue (24300));

lteHelper->SetEnbDeviceAttribute ("UlBandwidth", UintegerValue (12));

lteHelper->SetAttribute ("PathlossModel", StringValue ("ns3::ItuR1411NlosOverRooftopPropagationLossModel"));

lteHelper->SetPathlossModelAttribute ("Frequency", DoubleValue (800e6));

lteHelper->SetPathlossModelAttribute ("RooftopLevel", DoubleValue (15.0));

enbDevs.Add ( lteHelper->InstallEnbDevice (enbNodes1.Get (2)));
```

The communication system is massive since we are simulating a high dense urban environment: we place in our simulation 500 UE per site, leading to a total number of 2500 UE in the considered scenario. Each cell has an average radius of $550m$, corresponding to an average area of $\cong 0{,}9\ km^2$: this results in an UE density of $555{,}56\ UE/km^2$. It is not possible in the simulator to implement a higher number of UE, since the SRS periodicity value represents for it an upper bound. In LTE real networks, eNBs use Sounding Reference Signals sent by the UE to figure out the channel quality of the uplink path. These signals are transmitted with a periodicity that can be 2, 5, 10, 20, 40, 80, 160, 320 ms in accordance with Table 8.2-1 of 3GPP TS 36.213 (described here in *Table 2.3-1*).

| **SRS Configuration Index $I_{SRS}$** | **SRS Periodicity $T_{SRS}$ (ms)** | **SRS Subframe Offset $T_{offset}$** |
|---|---|---|
| 0 – 1 | 2 | $I_{SRS}$ |
| 2 – 6 | 5 | $I_{SRS}$ – 2 |
| 7 – 16 | 10 | $I_{SRS}$ – 7 |
| 17 – 36 | 20 | $I_{SRS}$ – 17 |
| 37 – 76 | 40 | $I_{SRS}$ – 37 |
| 77 – 156 | 80 | $I_{SRS}$ – 77 |
| 157 – 316 | 160 | $I_{SRS}$ – 157 |
| 317 – 636 | 320 | $I_{SRS}$ – 317 |
| 637 – 1023 | reserved | reserved |

*Table 2.3-2 – SRS periodicity, 3GPP TS 36.213, Table 8.2-1*

In ns-3, the number of devices that we can simulate must be lower of the SRS periodicity value chosen: for instance, with a SRS periodicity fixed at 80ms, the maximum number of allowed UE is 69. This is because during the Random-Access Procedure for the attachment, many RNTIs to be assigned to UEs are generated and then never used due to collisions. This bound can be neglected adding in the libraries *lte-phy.cc* (rows 150-174), *lte-enb-rrc.cc* (rows 2352-2369) and *lte-phy.h* (rows 149-155) higher periodicity values, estimating them following this criterion:

$$SRSperiodicity = 10 \cdot 2^n$$

$$LOWvalue = 10 \cdot 2^n - 3$$

$$HIGHvalue = 10 \cdot 2^{n+1} - 4$$

$$SrsSubframeoffset = 10 \cdot 2^n - 3$$

$$SrsCiLOW = 10 \cdot 2^n - 3$$

$$SrsCiHIGH = 10 \cdot 2^{n+1} - 4$$

An example of this modification is:

```
uint16_t
LtePhy::GetSrsPeriodicity (uint16_t srcCi) const
{
  // from 3GPP TS 36.213 table 8.2-1 UE Specific SRS Periodicity
  uint16_t SrsPeriodicity[10]={0, 2, 5, 10, 20, 40, 80, 160, 320, 640};
  uint16_t SrsCiLow[10] = {0, 0, 2, 7, 17, 37, 77, 157, 317, 637};
  uint16_t SrsCiHigh[10] = {0, 1, 6, 16, 36, 76, 156, 316, 636, 1276};
  uint8_t i;
  for (i = 10; i > 0; i --)
    {
      if ((srcCi>=SrsCiLow[i])&&(srcCi<=SrsCiHigh[i]))
        {
          break;
        }
    }
  return SrsPeriodicity[i];
}
```

With these assumptions, we can implement SRS values up to 640 ms, 1280 ms or higher, but in this cases the SRS are transmitted with a too long time period and they lose its impact on channel quality evaluation. Since this process is trivial for the coverage level estimation in NB-IoT, we must maintain SRS periodicity of 320 ms and place in our simulation a number of devices lower than this value. According to the features described in *Section 3*, we create three different node containers corresponding to three class of devices transmitting with different inter-packet intervals. The simulation time should be at least of 24. This would lead to a very too heavy simulation. In order to obtain a simulation time fair with our necessities, we assume a simulation time of 24 seconds: as a consequence we maintain the proportionality between this period and the inter-packet interval of each UE class, we have to scale these values, that became:

- Class A: 24 s;
- Class B: 2 s;
- Class C: 1 s.

With the settings just described, the resulting effective simulation time is equal to $\cong 10$ hours. All the UE are placed in the simulation scenario using a position allocator implemented in ns-3 called `RandomBoxPositionAllocator`: it allows the implementation of a random distribution of the UE in the selected area. We have only to specify the x-axis, y-axis and z-axis bounds of the box in which we want to place the devices. This allocator does not allow 0 value for z-axis: we assume for all UE a height of 1 m. Note that repeating the same simulation two or more times, maintaining the same bounds and the same number of UE, the allocation remains the same. Since NB-IoT devices are stationary, we install on every UE a `ConstantPositionMobilityModel`. In ns-3, the modulation order assignation depends on the correspondent measured values of spectral efficiency, Channel Quality Indicator CQI and Transport Block size. The relations between these parameters are implemented according to 3GPP TS 36.213 v.08 *Table 7.1.7.1-1* and *Table 7.2.3-1*. These tables are described in ns-3 in the library *lte-amc.cc*: in order to impose the maximum modulation order to QPSK, we have modified this file limiting the tables to MCS = 9 and CQI index = 6.

| MCS Index $I_{MCS}$ | Modulation Order $Q_m$ | TBS Index $I_{TBS}$ |
|---|---|---|
| 0 | 2 | 0 |
| 1 | 2 | 1 |
| 2 | 2 | 2 |
| 3 | 2 | 3 |
| 4 | 2 | 4 |
| 5 | 2 | 5 |
| 6 | 2 | 6 |
| 7 | 2 | 7 |
| 8 | 2 | 8 |
| 9 | 2 | 9 |
| 10 | 4 | 9 |
| 11 | 4 | 10 |
| 12 | 4 | 11 |
| 13 | 4 | 12 |
| 14 | 4 | 13 |
| 15 | 4 | 14 |
| 16 | 4 | 15 |
| 17 | 6 | 15 |
| 18 | 6 | 16 |
| 19 | 6 | 17 |
| 20 | 6 | 18 |
| 21 | 6 | 19 |
| 22 | 6 | 20 |
| 23 | 6 | 21 |
| 24 | 6 | 22 |
| 25 | 6 | 23 |
| 26 | 6 | 24 |
| 27 | 6 | 25 |
| 28 | 6 | 26 |
| 29 | 2 | reserved |
| 30 | 4 | |
| 31 | 6 | |

*Table 2.3-3 – MCS and TB size, 3GPP TS 36.213, Table 7.1.7.1-1*

| CQI index | modulation | code rate x 1024 | efficiency |
|---|---|---|---|
| 0 | out of range | | |
| 1 | QPSK | 78 | 0.1523 |
| 2 | QPSK | 120 | 0.2344 |
| 3 | QPSK | 193 | 0.3770 |
| 4 | QPSK | 308 | 0.6016 |
| 5 | QPSK | 449 | 0.8770 |
| 6 | QPSK | 602 | 1.1758 |
| 7 | 16QAM | 378 | 1.4766 |
| 8 | 16QAM | 490 | 1.9141 |
| 9 | 16QAM | 616 | 2.4063 |
| 10 | 64QAM | 466 | 2.7305 |
| 11 | 64QAM | 567 | 3.3223 |
| 12 | 64QAM | 666 | 3.9023 |
| 13 | 64QAM | 772 | 4.5234 |
| 14 | 64QAM | 873 | 5.1152 |
| 15 | 64QAM | 948 | 5.5547 |

*Table 2.3-4 – MCS, CQI and spectral efficiency, 3GPP TS 36.213, Table 7.2.3-1*

Each node has a transmission power of 43 dBm and each UE of 23 dBm (as in LTE standard), as we can see from an extract of the simulation code.

```
Config::SetDefault ("ns3::LteUePhy::TxPower", DoubleValue (23.0));
Config::SetDefault ("ns3::LteEnbPhy::TxPower", DoubleValue (43.0));
```

The only parameters that remain to be defined for the simulation scenario are the packetsize and the number of UE that compose each of the three defined class. We will see in *Section 5* how the results expected by the simulations depends on the choice of these values. To visualize and analyze the results of our simulations, we implement in the code the use of the flow monitor module and the compilation of statistics over PHY, MAC and RLC levels, and of statistics related to measured SINR levels.

## 4.3 NPRACH collision impact

Random Access Procedure in NB-IoT is always contention based: a contention starts when we have a collision on NPRACH. An NPRACH collision occurs when two (or more) UE initiates the Random Access Procedure at exactly the same time and both of them happen to pick the same preamble of the set provided by the node. Random Access Procedure in ns-3 is non-contention based: in case of a collision between two UE, the node discards both of them not allowing the connection to the network. In this way, the amount of traffic estimated by the simulations lacks in the data sent by all the users that in a real network met a collision and won the contention resolution. In order to assess how this percentage of transmissions influences the traffic of a NB-IoT system, in this section we evaluate the probability that a collision occurs on the Random Access Channel.

We represent with the variable $\tau$ the value of the NPRACH periodicity and with $T$ the time interval that we are considering. We define as a RACH occasion a complete Random Access Procedure cycle. The number of RACH occasions that occur in the time $T$ is computed as:

$$N_{RACH} = \frac{T}{\tau}$$

Since each node provides a set of preambles for the devices placed in the correspondent coverage area, we have to evaluate the probability to hit a collision for each cell site sector. $N_{ue}$ is the number of User Equipment included in a cell-site sector. As seen in the scenario description, if we want to evaluate the behavior of several smart metering use cases we can consider three different set of UE (A, B and C), corresponding to different values of inter packet interval, and consequently three different transmission frequency values. In this way, we assume to have:

4. ${N_{ue}}_A = 0{,}4N_{ue}$ users transmitting with the inter-packet interval $t_A$;
5. ${N_{ue}}_B = 0{,}4N_{ue}$ users transmitting with the inter-packet interval $t_B$;
6. ${N_{ue}}_C = 0{,}2N_{ue}$ users transmitting with the inter-packet interval $t_C$.

If we assume that every UE completes the first data transmission within a time equivalent to its inter-packet interval, the number of transmissions that an UE sends during the time $T$ is, for the sets A, B and C:

$$k_A = \frac{T}{t_A}$$

$$k_B = \frac{T}{t_B}$$

$$k_C = \frac{T}{t_C}$$

The transmission start time relative to the j-th UE $t_0^j$ is a uniform random variable: the time instant in which j-th UE starts transmitting is not scheduled at the beginning of the process. However, once the process has stabilized, the transmission becomes deterministic; so we can neglect in this analysis the randomness of transmission and numerically evaluate the number of transmission in the considered time interval as follows:

$$k_{tx} = N_{ue_A} k_A + N_{ue_B} k_B + N_{ue_C} k_C$$

Consequently, the probability to have an NPRACH transmission during a RACH occasion in $T$ corresponds to the ratio between the overall number of transmissions $k_{tx}$ and the number of RACH occasions that occur in $T$:

$$Pr(1tx) = \frac{k_{tx}}{N_{RACH}}$$

Since the attempts by two different UE to access the network are independent events, the probability to have two NPRACH transmission during the same RACH occasion in $T$ can be evaluated as follows:

$$Pr(2tx) = \frac{k_{tx}}{N_{RACH}} \frac{(k_{tx} - 1)}{N_{RACH}}$$

Then, we have a collision if the two transmitting UEs pick the same preamble from the set provided by the node. The probability relative to this event is:

$$Pr(samepreamble) = \frac{1}{P}\frac{1}{P} = \frac{1}{P^2}$$

where

$P$ : number of preambles provided by the node for each NPRACH period.

$Pr(2tx)$ and $Pr(samepreamble)$ are independent events again: the probability to have a collision during a RACH occasion corresponds to the product of these two probability.

Finally, multiplying for the number of RACH occasions $N_{RACH}$ we obtain the number of collision $N_C$ that occurs during the time interval T:

$$Pr(collision) = Pr(2tx)Pr(samepreamble) = \frac{k_{tx}}{N_{RACH}} \frac{(k_{tx} - 1)}{N_{RACH}} \frac{1}{P^2} = \frac{k_{tx}(k_{tx} - 1)}{{N_{RACH}}^2} \frac{1}{P^2}$$

$$N_C = N_{RACH} Pr(collision) = \frac{k_{tx}(k_{tx} - 1)}{N_{RACH}} \frac{1}{P^2}$$

We can apply this analysis to the values set in the simulation. In this case, we have $500$ UE for each node, leading to $167$ UE for each cell-site sector. Since the simulation time is

$$T = 24s$$

we have to divide all the time values considered in the 24h simulation time case for $24 \cdot 60 \cdot 60 : 24 = 3600$. The parameters became:

$$\tau = 0{,}00071s = 0{,}71ms$$

$$N_{ue} = 167$$

$$N_{ue_A} = 0.4N_{ue} = 67$$

$$N_{ue_B} = 0.4N_{ue} = 67$$

$$N_{ue_C} = 0.2N_{ue} = 33$$

$$t_A = 24s$$

$$t_B = 2s$$

$$t_C = 1s$$

This leads to a probability to have a collision during a RACH occasion

$$Pr(collision) \cong 3{,}3 \cdot 10^{-6}$$

and then to an estimated number of collision

$$N_C \cong 0{,}11$$

over the number of RACH occasions that occurs in $24s$, that is in this case $N_{RACH} = 35294$. The number of additional transmissions is a minimal percentage with respect to their total number, so we can assume to ignore it in calculating the overall throughput.

# 5 Simulations and results

In this section we study in detail the simulations done and the results obtained. We first give a brief description of the preliminary simulations needed to obtain and extrapolate some significant parameters and assumptions, arriving finally to the analysis of the overall NB-IoT system simulation.

## 5.1 Coverage analysis

We design the simulation scenario setting the positions of the antennas, the orientation of the beams and their relative gains in order to maximize the coverage on the area of interest. The simulator provides a tool that allow us to analyze the SINR levels measured in the scenario, the Radio Environment Map REM Helper. We include this tool in our code setting the system frequency (Earfcn) and the number of points we want to use in the representation. We choose an UL Earfcn = 2400 (800 MHz, as described previously in the antennas definition) and 1000 points in representation: a higher number of points would lead to an higher quality but also on a too heavy simulation. The output is a set of files each containing a list of the positions of eNBs, UE and the level of SINR for each point of the map. We used them to visualize, through the Linux visualizer *gnuplot*, a map of the SINR level measured in the overall area. This analysis leads to the coverage map represented in *Figure 5.1-1*. In the representation, one can distinguish a circular area around each tri-sectorial node: it corresponds to the settled field distance $d_s$, as described in the propagation model. Over this distance, the propagation model equation changes its behavior. As espressed previously, the UE are placed using a random box position allocator: we suppose to fix the z-axis coordinate of every UE at 1 m, so that the placing area became a 2-dimension rectangular scenario. The bounds of this area are:

- $x_{min} = -1200\ m$ , $x_{max} = 800\ m$ ;
- $y_{min} = -900\ m$ , $y_{max} = 800\ m$ ;

· $z = 1\ m.$

We represent below an example of UE allocation in the code: in particular, here is descripted the allocation of the Class A users, but the same method is applied to the others classes.

```
MobilityHelper mobilityUEOne;
mobilityUEOne.SetMobilityModel ("ns3::ConstantPositionMobilityModel");
mobilityUEOne.SetPositionAllocator ("ns3::RandomBoxPositionAllocator",
      "X", StringValue("ns3::UniformRandomVariable[Min=-1200.0|Max=800.0]"),
      "Y", StringValue("ns3::UniformRandomVariable[Min=-900.0|Max=800.0]"),
      "Z", StringValue("ns3::UniformRandomVariable[Min=1.0|Max=1.0]"));
```

*Figure 5.1-2* shows the result of the allocation of the overall set of 2500 UE in the described area, along with the SINR level measured by each user due to its position. To link each UE to the core network we use thens-3 function *AttachToClosestEnb* that allow the user to attach to the nearest node with respect to its position.

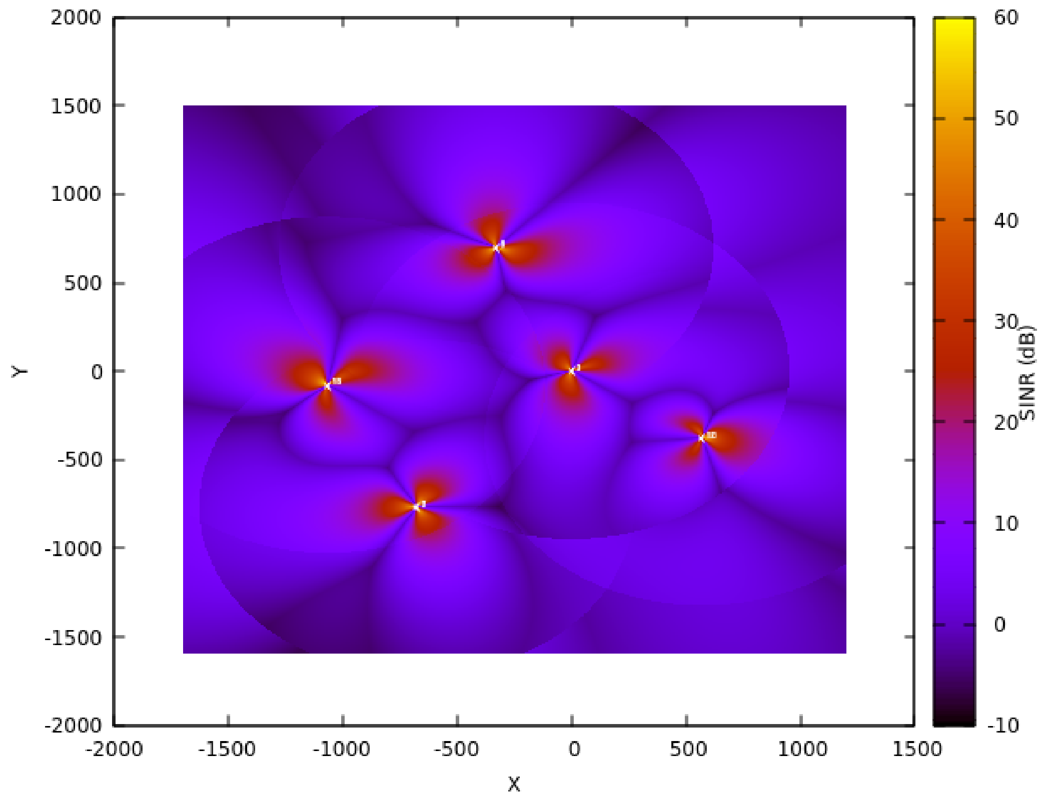


*Figure 5.1-1 – SINR level map at 800 MHz*

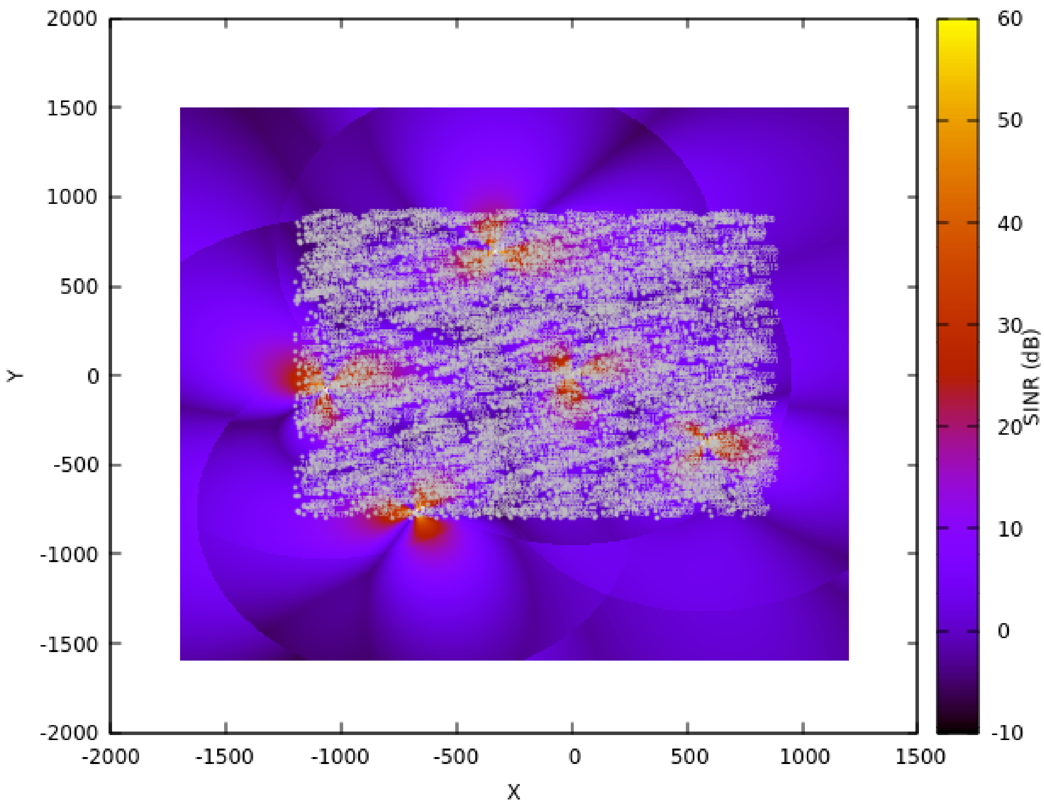


*Figure 5.1-1 – SINR level map and UE allocation*

In this coverage scenario, an average percentage of UE equal to 75% is served by the core network and succeeds in correctly transmitting uplink data. The remaining devices cannot access the network since their bad channel conditions: those UE are in the upper left corner where there is no serving node, or in the same situation at the upper right, or in the shadow areas caused by the interference between different lobes at the cell bounds.

### 5.1.1 Single user coverage

In order to evaluate a possible coverage extension, according to NB-IoT features defined by 3GPP, we studied the coverage measured for a single UE in the five tri-sectorial node scenario descripted previously. In detail, we analyzed the SINR level measured for an UE attached to the node at the bottom left (under the 300° orientation lobe) in order to find the distance at which it lose its connection to the network. In this scenario we measured a maximum y-axis coordinate in which the UE is in coverage $y = -1733\,m$, that, considering the y coordinate of the serving node that is $y_{node} = -771\ m$, corresponds to a distance of $962\ m$. At this distance the linear SINR level measured by the UE is $SINR_{min} =$ 2,89857: under this SINR level an user equipment lose the connection and is no more attached to the core network.

### 5.1.2 Coverage enhancement

The results obtained through the single user analysis show how in in our simulation scenario, in which cells has an average radius of 550 m, all the UE results in LTE standard coverage level, that corresponds to CE0 in NB-IoT. The simulation aim consist in evaluating the impact of the coverage enhancement on the capacity and the efficiency of the communication system. To make this effect emerge from simulations, we chose to evaluate, as described above, several smart metering use cases at the same time. In particular, as Class A we consider devices designed for gas metering. These UE are placed in a deep indoor scenario: they suffer an additional pathloss as they are installed in most cases in underground floors, basements or behind metal screen. So we assume to have for this kind of device an additional attenuation of 6 dB: the equivalent SINR level at which the UE loose its connection will be higher than the former case.

$$SINR_{min} = 2{,}8986$$

$$SINR_{min}[dB] = 4{,}6218\ dB$$

$$SINR_{min}'[dB] = 4{,}6218 + 6 = 10{,}6218\ dB$$

$$SINR_{min}' = 11{,}5393$$

Consequently, the correspondent distance along with the equivalent CE0 extension will be shorter. Checking in the same scenario described in the previous case the SINR level measure for an UE positioned closer to the node, until the sought level $SINR_{min}'$ is reached, we obtain a maximum equivalent coverage distance $d' = 639\ m$, corresponding to $SINR_{min}' = 11.5525$.

## 5.2 Complete simulations and results

We consider $d' = 639\ m$ equal to the CE0 extension for Class A devices: NB-IoT provides coverage across the cell by imposing for users beyond this limit a certain number of repetitions to be made in uplink transmission. In order to ensure that the ns-3 LTE Module works as defined in NB-IoT, it would be necessary to implement in our simulations repetitions based on an estimate of the RSRP or alternatively of the SINR. Unfortunately, this is not a viable implementation option because the simulator does not allow the management of RSRP and SINR parameters in our code main: they compares only in libraries and header files. Accordingly, since NB-IoT devices are stationary and operate very short-lived transmissions, we can assume that the channel condition of an UE and consequently the measured SINR level does not change during a single transmission: this allow us to implement repetitions based on the measured distance between the UE and the node from which it is served. E.g. if we want to implement a number of 4 repetitions, first we check with a *C++ if construct* if the distance between the UE and the node is greater than 640m, so if the condition is verified we multiply the packetsize to be sent in uplink for a factor 4. In this way, differently from 3GPP definition, we choose to implement only the first coverage enhancement level CE1, with users making a fixed number of repetitions. As seen for the packetsize and the number of UE appertaining to each class, the repetitions number is trivial for the system efficiency evaluation, so we will discuss it during the description of the different simulation cases. We give a detailed example of this code implementation in the following. Note that this setting is done only for Class A devices since they only are in a deep indoor scenario and are affected from the 6 dB additional pathloss. In the example described below, the variable *pacchetto* represents the packetsize, in bytes.

```
Ptr<MobilityModel> modelNodeOne=ueNodesOne.Get(u)> GetObject<MobilityModel>();
      double distance1 = modelNodeOne->GetDistanceFrom(modelENB1);
      double distance2 = modelNodeOne->GetDistanceFrom(modelENB2);
```

```
double distance3 = modelNodeOne->GetDistanceFrom(modelENB3);
double distance4 = modelNodeOne->GetDistanceFrom(modelENB4);
double distance5 = modelNodeOne->GetDistanceFrom(modelENB5);
double distance6 = modelNodeOne->GetDistanceFrom(modelENB6);
double distance7 = modelNodeOne->GetDistanceFrom(modelENB7);
double distance8 = modelNodeOne->GetDistanceFrom(modelENB8);
double distance9 = modelNodeOne->GetDistanceFrom(modelENB9);
double distance10 = modelNodeOne->GetDistanceFrom(modelENB10);
double distance11 = modelNodeOne->GetDistanceFrom(modelENB11);
double distance12 = modelNodeOne->GetDistanceFrom(modelENB12);
double distance13 = modelNodeOne->GetDistanceFrom(modelENB13);
double distance14 = modelNodeOne->GetDistanceFrom(modelENB14);
double distance15 = modelNodeOne->GetDistanceFrom(modelENB15);
double distancearray[] = {distance1, distance2, distance3, distance4,
      distance5, distance6, distance7, distance8, distance9, distance10,
      distance11, distance12, distance13, distance14, distance15};
double distance = distancearray[0];
for ( int i = 1; i < 15; i++ )
      {
      if ( distancearray[i] < distance )
      distance = distancearray[i];
      }

if (distance > 640)
{
ulClientOne.SetAttribute ("PacketSize", UintegerValue(pacchetto*4));;
}
else
{
ulClientOne.SetAttribute("PacketSize",UintegerValue(pacchetto));;
}
```

Summarizing, we finally have the following simulation scenario. We consider a rectangular area of 2000 m * 1700 m, in which we place 2500 stationary UE uniformly distributed. The area is covered by 5 tri-sectorial node transmitting with an average 15 dB gain at an altitude of 23 m. The considered simulation time is equal to 24 s. The UE are divided in three Classes, each one characterized by a different transmission frequency and consequently by different inter-packet intervals (24s, 2s and 1s respectively for Class A, B and C). Each UE is attached to the nearest node and transmits data in uplink to the core network. Class A devices are assumed to be in a deep indoor scenario, so they are affected by an additional pathloss with respect to the other devices: if they are at a distance greater than 640 m from the serving node, they repeat data in UL a determined number of times. The aim is to analyze the efficiency of this communication system, changing its initial condition (packetsize, number of repetitions and device class) in order to understand how coverage enhancement influence this value. We now presents the results obtained for each simulation cases. Note that while trying different parameters settings we find out an upper bound of 8000 bytes transmitted in uplink by an UE. In the determination of settings for the various simulations, we should always keep the single transmissions under this limit: its saturation would lead to unrealistic results.

### 5.2.1 Small amount of transmitted data, high number of repetitions

In this first simulation case, we set the following initial conditions ($N_{rep}$ is the number of repetitions that an UE in CE1 has to implement in uplink):

- $Packetsize = 12 * 20 = 240\ bytes$ ;
- $N_{rep} = 32$ .

As explained previously, we must multiply each data flow for a factor 12 since we are using 12 times the frequency resource that are dedicated to NB-IoT (12 PRB instead of 1 PRB): this assumption is valid for all cases. First, we assume to have a medium number of Class A devices, resulting in a low number of UE repeating packets in UL. The UE are so divided in this way:

- 30% - Class A, inter-packet interval = 24 s;
- 40% - Class B inter-packet interval = 2 s;
- 30% - Class C inter-packet interval = 1 s.

Once the simulation is run with these settings, we are going to analyze the measured statistics at RLC level. These stats allow us to visualize, at each time instant (with a definition of 1 ms) the IMSI assigned to the transmitting UE, the Cell-ID of the serving node, the number of bytes sent in UL by the UE and the number of bytes received by the node. From Sinr stats we can also analyze the relative SINR level measured for each UE at each time instant (again with a 1 ms definition). In particular, we must apply the following post-processing on the obtained results, in uplink RLC stats:

- if an UE sends less than 240 bytes, the correspondent received bytes value has to be forced to 0, since the transmission of an incomplete packet gives no contribute to the system efficiency;
- if an UE repeats its data in UL and the correspondent received bytes value is greater than 240 bytes (the node has received correctly almost one packet), this value has to be forced equal to the one of the transmitted bytes, because the repetitions increase the system efficiency.

After this data processing, we sum all the bytes correctly received from the network and all bytes transmitted by the devices. The ratio between the two values obtained provides the measurement of system efficiency, which results in this case:

$$\eta_{30\%} = \frac{C_R}{C_T} = 0{,}98681$$

In order to better assess the effect of repetition on the efficiency, we repeat the same simulation with this new device class assignation:

- 80% - Class A, inter-packet interval = 24 s;

- 10% - Class B inter-packet interval = 2 s;
- 10% - Class C inter-packet interval = 1 s.

In this case, after the overall data processing we obtain the following system efficiency value:

$$\eta_{80\%} = \frac{C_R}{C_T} = 0{,}99123$$

Obtained results shows as

With 30% of Class A devices, a good percentage of the ones appertaining at Class B and C result in poor radio conditions. These devices suffer a deterioration in transmission efficiency, differently from Class A case in which poor channel condition are compensated by repetitions, through which the devices can still successfully send uplink data. For this reason, the efficiency is not so close to the excellent 100% value, as it would be required for a high fidelity system. Increasing the percentage of users in Class A corresponds to passing in this class a percentage of those in Class B and C: this way those B and C users who were previously lost in transmission now benefiting from the repetition effect succeed in completing it correctly their broadcasts. For this reason, the efficiency measured in this second case is higher than the previous one.

### 5.2.2 Medium amount of transmitted data and number of repetitions

In this first simulation case, we want analyze an average situation, in which the devices transmits more data with respect to the previous case. We balance the effect of this increase on total data flow by decreasing the number of repetitions that Class A devices in CE1 must perform. Therefore, we set the following initial conditions:

- $Packetsize = 12 * 40 = 480\ bytes$ ;
- $N_{rep} = 16$ .

The starting class device assignation is the same expressed in the previous case:

- 30% - Class A, inter-packet interval = 24 s;
- 40% - Class B inter-packet interval = 2 s;
- 30% - Class C inter-packet interval = 1 s.

We apply in this case the same evaluation and post-processing criteria considered for the previous simulations. The measured system efficiency results:

$$\eta_{30\%} = \frac{C_R}{C_T} = 0{,}98667$$

Also with these initial conditions, we repeat the simulation increasing the coverage enhancement effects. We consider:

- 80% - Class A, inter-packet interval = 24 s;
- 10% - Class B inter-packet interval = 2 s;
- 10% - Class C inter-packet interval = 1 s.

This leads to a measured system efficiency equal to:

$$\eta_{80\%} = \frac{C_R}{C_T} = 0{,}99084$$

By increasing the size of the packets to 40 bytes and decreasing the number of repetitions at 16 we measure an intermediate situation. The channel results unloaded again, since each UE still transmits a low amount of data. Even in this case while passing a greater number of devices in Class A, the efficiency increases. The measured behavior is very similar to those obtained with a packetsize of 20 bytes. This trend is valid until the channel is unloaded.

### 5.2.3 High amount of transmitted data and low number of repetitions

In order to show how the system behave when it sees a congestion of the channel, we finally analyze the extreme case in which every UE transmits a high amount of uplink data. Also in this scenario, we have to balance the effect of this increase on total data flow by decreasing the number of repetitions that Class A devices in CE1 must perform. The set initial conditions are:

- $Packetsize = 12 * 160 = 1920\ bytes$ ;
- $N_{rep} = 4$ .

The first simulation runs on a low number of Class A devices, as seen before:

- 30% - Class A, inter-packet interval = 24 s;
- 40% - Class B inter-packet interval = 2 s;
- 30% - Class C inter-packet interval = 1 s.

This leads to the following measured system efficiency:

$$\eta_{30\%} = \frac{C_R}{C_T} = 0{,}98413$$

Once again, increasing the number of Class A devices we increase the number of occurred repetitions along with their effect on transmission:

- 80% - Class A, inter-packet interval = 24 s;
- 10% - Class B inter-packet interval = 2 s;
- 10% - Class C inter-packet interval = 1 s.

The system efficiency measured with these settings results:

$$\eta_{80\%} = \frac{C_R}{C_T} = 0{,}96251$$

The obtained results shows how the trend revealed by previous cases is no longer valid. When we pass from 30% to 80% the percentage of Class A user equipment, those Class B and C devices who previously suffered a loss in the broadcast due to their poor channel conditions now benefit from repetitions and then succeed in successfully completing the packet transmission. However, unlike the previous case, that 20% devices remaining in Class B and C suffer the conditions of the channel, which results now overloaded. Now, 80% of the devices are sending a number of bytes near to the maximum transmittable number, and a consistent percentage of these UE is also repeating the packets: this makes the overall uplink transmission close to its physical limit. This effect causes a major deterioration in the system transmission efficiency. Consequently, the beneficial effect of Class A repetitions is overwhelmed by channel congestion worsening: this leads to a total system efficiency decreasing.

In a smart metering system, considering a single use case we can assume to have a device every four people. Checking the population density of the main European cities results in an average value of $15000/km^2$ for a massive dense urban scenario. This leads to an UE density of $3750/km^2$ for a single smart metering use case. Since we placed in our scenario three different use cases, this density becomes $\cong 11250/km^2$. The actual UE density we placed in the simulation scenario, due to physical limits of the simulator, is equal to $555{,}56\, UE/km^2$: Considering that only 75% of them transmit, we will have an average number of transmitting UE $\cong 416\, UE/km^2$: the number of simulated UE differs from the estimated number of NB-IoT devices of a factor = 27. Developed simulations shows that the average duration of an uplink transmission is $\cong 0{,}96\ s$: this time interval is valid for a single transmission even if we consider an overall observation time of 24 h, instead of the 24 s simulation time. The simulated scenario represents a peak situation in the UL transmission: having a longer time range available, we can imagine repeating this transmission pattern several times, shifted at uniformly spaced intervals. This equates to the same transmission scheme developed by a larger number of users. E.g. we can consider 125 Class C devices (30%-40%-30% class division, considering only the third class) transmitting 20 bytes in uplink every 1 s. Scaling the observation time up to 24 h, the considered inter-packet interval becomes equal to 1 h: this means that for uplink data transmission we have 3600 times longer time available. If we try to repeat the same traffic at 30 s intervals, we can consider up to 116 transmissions. This result largely satisfies the factor 27 required to move to real time scale and UE density values. These considerations are valid for all other traffic models considered in simulation, and leads to the same conclusions. For this reason, we can state that the NB-IoT system implemented can simultaneously serve multiple smart metering cases in a typical high dense urban scenario.

# 6 Conclusions and future works

The rapid spread of Internet of Things along with the plethora of offered development opportunities brought an increasing interest on this technology and its possible applications. In particular, business efficiencies enhancement and operational expense decrease brought by smart metering has pushed the main telecommunications and energy companies to evaluate a sudden implementation of this technology. 3GPP defines NB-IoT as the standard from which to start the development of MTC devices in 5G optic: first commercial devices are supposed to be released by the end of 2017.
In our work, we analyzed the 3GPP standardization of NB-IoT for machine-type communications, focusing our attention to physical layer and radio protocols, starting from LTE standards definition. We studied the difference between this technology and LTE, providing a detailed description of how the implementation choices made for NB-IoT fit the nature of the application for which this technology is developed. In addition, we focused on the analysis of Random Access procedure and its influences on the performance of the system, providing an estimate of the collisions impact on transmission. We made measurements on a NB-IoT prototype connected to a real cellular network, in order to better understand and verify the behavior of signaling protocols, cell connection and access procedures.

The main work was the implementation of the NB-IoT functionality on ns-3 LTE Module: we needed to modify the processes implemented in the simulator to fit the Narrowband 3GPP specification by creating new features and circumventing obvious limits due to the nature of the used module. Then, we deployed massive communication system placed in a high dense urban scenario, analyzing its performances in terms of capacity and system efficiency. We studied several deployment scenarios in order to assess the effect of coverage enhancement on the transmission.

Measured data show how the technical features of NB-IoT technology allow a mobile operator to serve customers with this new functionality without the need for installing new network equipment, and reusing the pre-existing portion of spectrum dedicated to LTE, while maintaining the fairness with this technology. Moreover, the measured efficiency values show how this system ensures high performance, suitable for a high fidelity system like the one we are considering.

Results we obtained show that NB-IoT coverage enhancement brings an improvement in system performance, until the channel is not congested: repetitions applied to uplink traffic, introducing redundancy, allow reaching successful broadcasts to those devices that in LTE would be out of coverage. Conversely, increasing the traffic developed by each user in order to overload the channel, the trend is reversed: the effect of enhancement brought by coverage enhancement is overshadowed by the worsening due to channel congestion, resulting in a consequent degradation of the system efficiency.

In a general smart metering system, considering a single use case we can assume to have a device every four people. Checking the population density of the main European cities results in an average value of $15000/km^2$ for a massive dense urban scenario. This leads to an UE density of $3750/km^2$ for a single smart metering use case. Obtained results show how NB-IoT performance allow the operators to serve the customers with one or several metering use cases, without exceeding the measured capacity of the system.

Future work will include the implementation of a dedicated NB-IoT module in the simulator, to overcome the limits represented by LTE's typical features. A key aspect would be the implementation of the physical structure of this technology, as well as the extension of coverage levels based on measured RSRP values.

## List of the abbreviations

| | |
|---|---|
| 2G | Second Generation |
| 3G | Third Generation |
| 3GPP | Third Generation Partnership Project |
| 4G | Fourth Generation |
| 5G | Fifth Generation |
| ACK | Acknowledge |
| AM | Acknowledged Mode |
| AMC | Adaptive Modulation and Coding |
| AP | Antenna Port |
| API | Application Programming Interface |
| BER | Bit Error Rate |
| BPSK | Binary Phase-Shift Keying |
| BS | Base Station |
| C-RNTI | Cell-specific RNTI |
| CDMA | Code Division Multiple Access |
| CE | Coverage Enhancement |
| CIoT | Cellular Internet of Things |
| CM | Connection Management |
| CP | Cyclic Prefix |
| CQI | Channel Quality Indicator |
| CRS | Cell-specific Reference Signal |
| DCI | Downlink Control Information |
| DHCP | Dynamic Host Configuration Protocol |
| DL | DownLink |
| DL-SCH | DownLink Shared Channel |
| DMRS | Demodulation Reference Signal |
| DRB | Data Radio Bearer |
| EARFCN | EUTRA Absolute Radio-Frequency Channel Number |
| EDGE | Enhanced Data rates for GSM Evolution |
| eNB | eNodeB |
| EPC | Evolved Packet Core |
| EPS | Evolved Packet System |
| ESM | EPS Session Management |
| E-UTRA | Evolved Universal Terrestrial Access |
| E-UTRAN | Evolved Universal Terrestrial Access Network |
| FDD | Frequency Division Duplexing |

| | |
|---|---|
| GSM | Global System for Mobile Communications |
| GERAN | GSM EDGE Radio Access Network |
| HARQ | Hybrid Automatic ReQuest |
| HSS | Home Subscriber Server |
| ICMP | Internet Control Message Protocol |
| IoT | Internet of Things |
| IP | Internet Protocol |
| ISI | Inter-Symbol Interference |
| ITU | International Telecommunication Union |
| LoS | Line of Sight |
| LSB | Less Significant Bit |
| LSM | Link-to-System Mapping |
| LTE | Long Term Evolution |
| LTE-A | LTE-Advanced |
| M2M | Machine to Machine |
| MAC | Medium Access Control |
| MCL | Maximum Coupling Loss |
| MCS | Modulation and Coding Scheme |
| MIB | Master Information Block |
| MIESM | Mutual Information Effective SINR Mapping |
| MIH | Media Independent handover |
| MIMO | Multiple Input Multiple Output |
| MM | Mobility Management |
| MSB | Most Significant Bit |
| MTC | Machine Type Communication |
| NAS | Non-Access Stratum |
| NACK | Non-Acknowledge |
| NB-IoT | Narrowband Internet of Things |
| NCCE | Narrowband Control Channel Element |
| NEMO | Network Mobility |
| NLoS | Non-Line of Sight |
| 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 |
| NPUSCH | Narrowband Physical Uplink Shared Channel |
| NRS | Narrowband Reference Signal |
| NSSS | Narrowband Secondary Synchronization Signal |
| OFDM | Orthogonal Frequency Division Multiplexing |

| | |
|---|---|
| OFDMA | Orthogonal Frequency Division Multiple Access |
| P-RNTI | Paging RNTI |
| PAPR | Peak-to-Average Power Ratio |
| PCRF | Policy and Charging Rules Function |
| PDCCH | Physical Downlink Control Channel |
| PDCP | Packet Data Convergence Protocol |
| PDF | Probability Density Function |
| PDN | Packet Data Network |
| PDSCH | Physical Downlink Shared Channel |
| PDU | Protocol Data Unit |
| PF | Proportional Fair |
| PGW | Packet GateWay |
| PHY | Physical Layer |
| PLMN | Public Land Mobile Network |
| PMIP | Proxy Mobile IP |
| PRACH | Physical Random Access Channel |
| PRB | Physical Resource Block |
| PS | Packet Switch |
| PSD | Power Spectral Density |
| PUCCH | Physical Uplink Control Channel |
| PUSCH | Physical Uplink Shared Channel |
| QAM | Quadrature Amplitude Modulation |
| QoS | Quality of Service |
| QPSK | Quadrature Phase-Shift Keying |
| RA-RNTI | Random Access RNTI |
| RAT | Radio Access Technology |
| RBG | Resource Block Group |
| RE | Resource Element |
| REM | Radio Environment Map |
| RLC | Radio Link Control |
| RNTI | Radio Network Temporary Identifier |
| ROHC | Robust Header Compression |
| RR | Round Robin |
| RRC | Radio Resource Control |
| RSRP | Reference Signal Received Power |
| RU | Resource Unit |
| S&W | Stop & Wait |
| SAE | System Architecture Evolution |
| SC-FDMA | Single Carrier Frequency Division Multiple Access |
| SCEF | Service Capability Exposure Function |

| | |
|---|---|
| SF | Subframe |
| SFN | System Frame Number |
| SGW | Serving Gateway |
| SI | System Information |
| SIB | System Information Block |
| SINR | Signal-to-Noise Ratio |
| SISO | Single Input Single Output |
| SRB | Signaling Radio Bearer |
| SRS | Sounding Reference Signal |
| TBS | Transport Block Size |
| TCP | Transmission Control Protocol |
| TDD | Time Division Duplexing |
| TM | Transmission Mode |
| TR | Technical Report |
| TS | Technical Specification |
| TTI | Transmission Time Interval |
| TW | Test Word |
| UCI | Uplink Control Information |
| UDP | User Datagram Protocol |
| UE | User Equipment |
| UL | UpLink |
| UM | Unacknowledged Mode |
| UMTS | Universal Mobile Telecommunications System |

# References


- 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception", 3rd Generation Partnership Project (3GPP), TS 36.101, v. 14.4.0
- 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception", 3rd Generation Partnership Project (3GPP), TS 36.104, v.13.0.0
- 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation", 3rd Generation Partnership Project (3GPP), TS 36.211, v. 13.2.0
- 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures", 3rd Generation Partnership Project (3GPP), TS 36.213, v. 13.0.0
- 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio access capabilities", 3rd Generation Partnership Project (3GPP), TS 36.306, v.14.1.0
- 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification", 3rd Generation Partnership Project (3GPP), TS 36.331, v. 13.0.0
- 3GPP, "Study on provision of low-cost Machine-Type Communications (MTC) User Equipments (UEs) based on LTE", 3rd Generation Partnership Project (3GPP), TR 36.888, v. 12.0.0
- 3GPP, "Study on scenarios and requirements for next generation access technologies", 3rd Generation Partnership Project (3GPP), TR 38.913, v. 14.0.0
- 3GPP, "Cellular system support for ultra-low complexity and low throughput Internet of Things (CIoT) (Release 13)", 3rd Generation Partnership Project (3GPP), TR 45.820, v. 13.1.0
- F. Chiti, D. Di Giacomo, R. Fantacci, L. Pierucci, and C. Carlini, "Optimized Narrow-Band M2M Systems for Massive Cellular IoT Communications," Global Communications Conference (GLOBECOM), 2016 IEEE, 2016

- Y.-P. E. Wang, X. Lin, A. Adhikary, A. Gr¨ovlen, Y. Sui, Y. Blankenship, J. Bergman, and H. S. Razaghi, “A Primer on 3GPP Narrowband Internet of Things (NB-IoT),” IEEE Communications Magazine, Vol. 55, Issue 3, March 2017, 2017
- Rapeepat Ratasuk, Benny Vejlgaard, Nitin Mangalvedhe, and Amitava Ghosh, “NB-IoT System for M2M Communication”, Workshop on Device to Device communications for 5G NETWORKS, 2016
- ITU-R P.526-13, “Propagation by Diffraction”, November 2013
- ITU-R P.1411-8, "Propagation data and prediction methods for the planning of short-range outdoor radiocommunication systems and radio local area networks in the frequency range 300 MHz to 100 GHz", July 2015
- Castellani A., Angilè F., “Introduzione all’LTE (Long Term Evolution) e alle funzionalità in tecnologia Huawei”, Technical Note, TIM, July 2009
- J. Schlienz, D. Raddino, “Narrowband Internet of Things,” Rhode and Schwarz White Paper, 2016
- “ns-3” [Online]. Available: http://www.nsnam.org