# Narrowband Internet of Things
# Whitepaper

As part of Release 13, 3GPP has specified a new radio interface, the *Narrowband Internet of Things* (NB-IoT). NB-IoT is optimized for machine type traffic. It is kept as simple as possible in order to reduce device costs and to minimize battery consumption. In addition, it is also adapted to work in difficult radio conditions, which is a frequent operational area for certain machine type communication devices. Although NB-IoT is an independent radio interface, it is tightly connected with LTE, which also shows up in its integration in the current LTE specifications.

In this whitepaper we introduce the NB-IoT technology with an emphasis on the tight connection to LTE.

**Note:**

Visit our homepage for the most recent version of this application note (www.rohde-schwarz.com/appnote/1MA266).

NarrowBand_IoT — 1MA266_0e

J. Schlienz, D. Raddino

Whitepaper

ROHDE&SCHWARZ

# Contents

# 1 Introduction

One of the characteristics of Machine Type Communication (MTC) is the broad spectrum of capabilities. For example surveillance cameras have to deliver a huge amount of UL data while being almost stationary, whereas devices for fleet tracking have a small amount of data while performing a lot of handovers.

Yet another class of devices has neither of these capabilities. Examples are devices for meter reading like electricity, gas, or water consumption. They are often stationary, thus need not an optimized handover. Only a small amount of data is usually transferred, which is even not delay sensitive. However, the number of these MTC devices may become quite big, even up to several orders of magnitude compared to the traditional devices. Using existing LTE technology would lead to a network overload, because despite of their small amount of user data the amount of signaling is about the same. The first specification of NB-IoT focusses on this class of devices.

These devices are often installed at places without power supply. Consequently they run completely on battery and it may be very expensive to change the battery, because they may only be accessed by trained staff. Hence, in some cases the battery lifetime can even determine the lifetime of the whole device. An optimized power consumption is therefore essential for a proper operation. In addition, the coverage at these places is often quite bad. Therefore, the indoor coverage has to be significantly improved, up to 23 dB are regarded as necessary.

Due to their sheer amount of required devices, they have to be in the low cost range. As a goal, each module shall be in the price range of less than 5 US$.

In order to evaluate possible solutions, a study item was discussed in 3GPP in the GERAN TSG [1]. The main requirement in addition to the above ones was the coexistence with existing GSM, UMTS and LTE systems and the hardware used for those technologies.

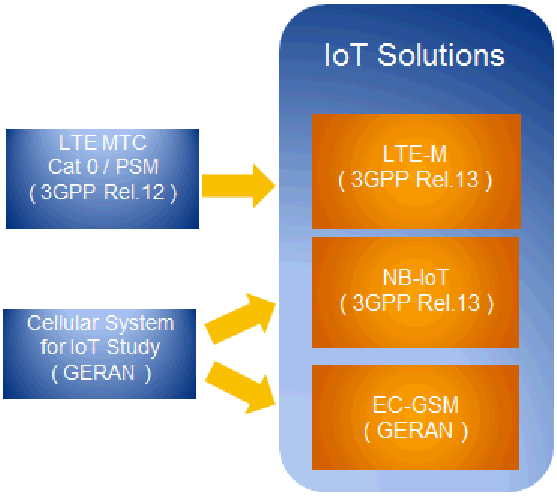


*Figure 1-1: The three different solutions for specifying an optimized internet of things standard*

Two solutions, the NB-IoT and the EC-GSM have been identified from this study, where the latter is building upon the GSM standard. In parallel, also a pure LTE solution, LTE-M, was brought into 3GPP. It continues the optimizations already done in Release 12 with the introduction of a new device category *cat-M1*.

In this whitepaper, the NB-IoT is presented. Although it is integrated in the LTE standard, it can be regarded as a new air interface. Therefore, it is not backward compatible with LTE. The coexistence is realized by specifying the time and frequency resources used from the existing standards, or in the neighborhood thereof.

The whitepaper is structured in the following way: We first give an overview of the more specific requirements and the network architecture and provide the details of the physical layer. After having described the access to the cell, we show how the data packets are transported over the air interface. Finally, an outlook to further developments of this technology is given.

# 2 Overview

## 2.1 Requirements

From the general MTC requirements mentioned in the previous chapter, the following standard specific requirements for NB-IoT were derived:

- Minimize the signaling overhead, especially over the radio interface
- Appropriate security to the complete system, including the core network
- Improve battery life
- Support delivery of IP and non-IP data [2, 3]
- Support of SMS as a deployment option [4]

In order to fulfill these requirements, many advanced and even basic features of LTE Release 8/9 are not supported [5]. The most striking example is the lack of handover for UEs in the connected state. Only cell reselection in the idle state is supported, which is even restricted to be within the NB-IoT technology. As there is no interaction with other radio technologies, also the associated features are not supported. Examples are the lack of LTE-WLAN interworking, interference avoidance for in-device coexistence, and measurements to monitor the channel quality.

Most LTE-Advanced features are also not supported. This concerns e.g. Carrier Aggregation, Dual Connectivity, or device-to-device services. In addition, there is no QoS concept, because NB-IoT is not used for delay sensitive data packets. Consequently, all services requiring a guaranteed bit rate, like real time IMS, are not offered in NB-IoT as well.

With these requirements, 3GPP uses a different approach than before. Instead of creating one air-interface for all types of applications, the air-interface for small non-delay sensitive data packets is split off and optimized separately. UEs which support to work on NB-IoT technology are tagged with the new UE category cat-NB1.

## 2.2 Network

### 2.2.1 Core Network

In order to send data to an application, two optimizations for the cellular internet of things (CIoT) in the evolved packet system (EPS) were defined, the *User Plane CIoT EPS optimisation* and the *Control Plane CIoT EPS optimisation*, see Figure 2-1. Both optimisations may be used but are not limited to NB-IoT devices.

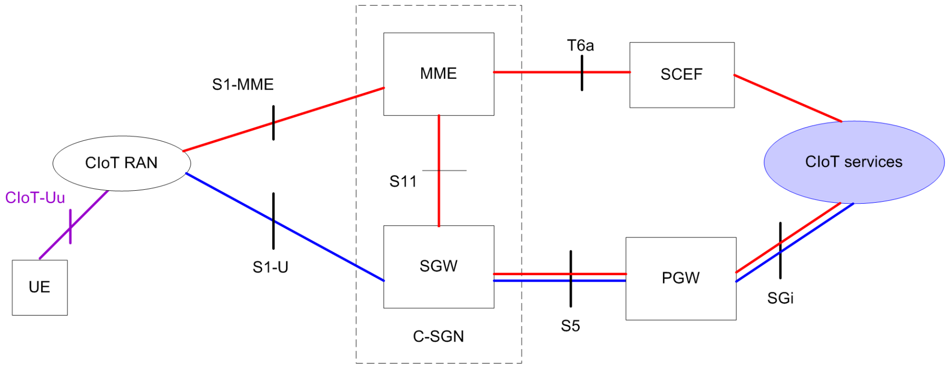


***Figure 2-1: Network for the NB-IoT data transmission and reception. In red, the Control Plane CIoT EPS optimisation is indicated, in blue the User Plane CIoT EPS optimisation.***

On the Control Plane CIoT EPS optimisation, UL data are transferred from the eNB (CIoT RAN) to the MME. From there, they may either be transferred via the *Serving Gateway* (SGW) to the *Packet Data Network Gateway* (PGW), or to the *Service Capability Exposure Function* (SCEF) which however is only possible for non-IP data packets. From these nodes they are finally forwarded to the application server (CIoT Services). DL data is transmitted over the same paths in the reverse direction. In this solution, there is no data radio bearer set up, data packets are sent on the signaling radio bearer instead. Consequently, this solution is most appropriate for the transmission of infrequent and small data packets.

The SCEF is a new node designed especially for machine type data. It is used for delivery of non-IP data over control plane and provides an abstract interface for the network services (authentication and authorization, discovery and access nework capabilities).

With the User Plane CIoT EPS optimisation, data is transferred in the same way as the conventional data traffic, i.e. over radio bearers via the SGW and the PGW to the application server. Thus it creates some overhead on building up the connection, however it facilitates a sequence of data packets to be sent. This path supports both, IP and non-IP data delivery.

### 2.2.2 Access Network

On the overal access network architecture there is no difference to LTE [6]:

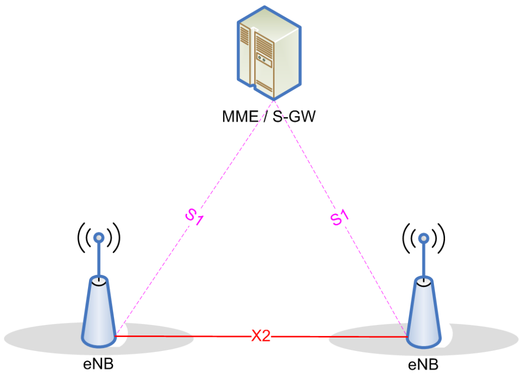


*Figure 2-2: Network architecture towards the air--interface*

The eNBs are connected to the MME and S-GW using the S1 interface, with the difference of carrying the NB-IoT messages and data packets. Even though there is no handover defined, there is still an X2 interface between two eNBs, which enables a fast resume after the UE goes to the idle state, see Chapter 4.5.1, "RRC Connection Establishment", on page 28 for details, even for the case that the resume process is to another eNB.

## 2.3 Frequency Bands

For the frequency bands, the same frequency numbers as in LTE are used, with a subset defined for NB-IoT. In Release 13, these are the following bands [7]:

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

It is worth mentioning that most frequencies are in the lower range of existing LTE bands. This reflects that for machine type communications there are a lot of devices expected in difficult radio conditions.

# 3 Physical Layer

## 3.1 Operation Modes

NB-IoT technology occupies a frequency band of 180 kHz bandwidth [8], which corresponds to one resource block in LTE transmission. With this selection, the following operation modes are possible:

- *Stand alone operation*. A possible scenario is the utilization of currently used GSM frequencies. With their bandwidth of 200 kHz there is still a guard interval of 10 kHz remaining on both sides of the spectrum
- *Guard band operation*, utilizing the unused resource blocks within an LTE carrier's guard-band
- *In-band operation* utilizing resource blocks within an LTE carrier

These modes are visualized in the following figure:

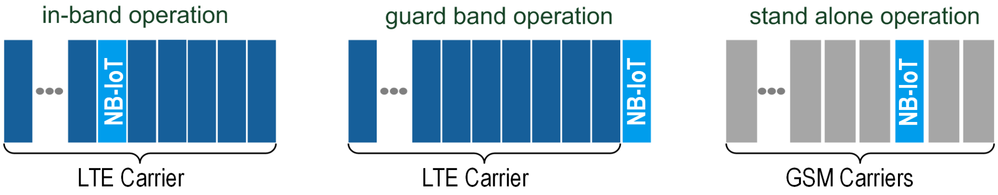


*Figure 3-1: Operation modes for NB-IoT*

For the stand alone operation, the GSM carriers in the right part of the figure are only shown as an example in order to indicate that this is a possible NB-IoT deployment. Of course, this operation mode also works without neighboring GSM carriers.

In the in-band operation, the assignment of resources between LTE and NB-IoT is not fixed. However, not all frequencies, i.e. resource blocks within the LTE carrier, are allowed to be used for cell connection. They are restricted to the following values:

*Table 3-1: Allowed LTE PRB indices for cell connection in NB-IoT in-band operation*

| 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 |

As indicated in this table, there is no support for in-band operation of an LTE band with 1.4 MHz bandwidth. A conflict between resources used by the LTE system like the cell specific reference signals (CRS) or the downlink control channel at the start of each subframe must be taken into account when resources are allocated for NB-IoT. This is also reflected in Table 3-1 by not using the 6 inner resouce blocks, as these are allocated for the synchronization signals in LTE.

For the guard band operation, the UE only synchronizes to signals, for which the bands are completely in the guard band.

In order to cope with different radio conditions, there may be up to 3 coverage enhancement (CE) levels, CE level 0 to CE level 2. CE level 0 corresponds to normal coverage, and CE level 2 to the worst case, where the coverage may be assumed to be very poor. It is up to the network, how many CE levels are defined. A list of power thresholds for the received reference signals is broadcasted in the cell for each CE level. The main impact of the different CE levels is that the messages have to be repeated several times.

For Release 13, *FDD half duplex type-B* is chosen as the duplex mode. This means that UL and DL are separated in frequency and the UE either receives or transmits, however not simultaneously. In addition, between every switch from UL to DL or vice versa there is at least one guard subframe (SF) in between, where the UE has time to switch its transmitter and receiver chain.

## 3.2 Downlink

For the DL, three physical channels

- NPBCH, the narrowband physical broadcast channel
- NPDCCH, the narrowband physical downlink control channel
- NPDSCH, the narrowband physical downlink shared channel

and two physical signals

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

are defined. These are less channels than for LTE, the physical multicast channel PMCH is not included, because there is no MBMS service for NB-IoT.

The following figure illustrates the connection between the transport channels and the physical channels:

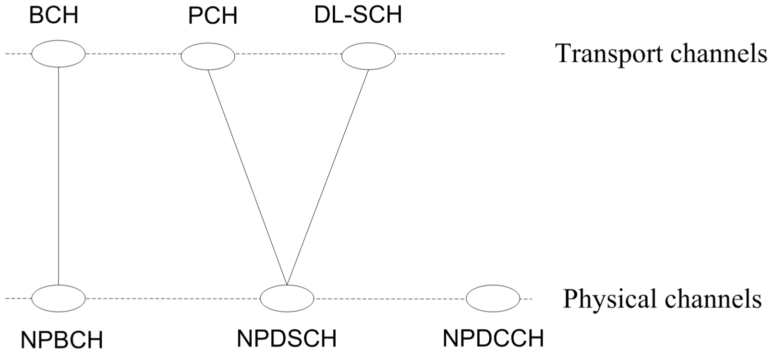


***Figure 3-2: Mapping of the transport channels to the physical channels***

MIB information is always transmitted over the NPBCH, the remaining signaling information and data over the NPDSCH. The NPDCCH controls the data transfer between UE and eNB.

The physical DL channels are always QPSK modulated. NB-IoT supports the operation with either one or two antenna ports, AP0 and AP1. For the latter case, *Space Frequency Block Coding* (SFBC) is applied. Once selected, the same transmission scheme applies to NPBCH, NPDCCH, and NPDSCH.

Like in LTE, each cell has an assigned physical cell ID (PCI), the *Narrowband physical cell ID* (NCellID). Totally 504 different values for NCellID are defined. Its value is provided by the secondary synchronization signal NSSS, see Chapter 3.2.3, "Synchronization Signals", on page 13.

## 3.2.1 Frame and Slot Structure

In the DL, OFDM is applied using a 15 kHz subcarrier spacing with normal cyclic prefix (CP). Each of the OFDM symbols consists of 12 subcarrier occupying this way the bandwitdh of 180 kHz. Seven OFDMA symbols are bundled into one slot, so that the slot has the following resource grid [9]:

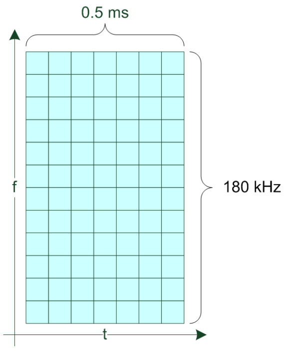


***Figure 3-3: Resource grid for one slot. There are 12 subcarriers for the 180 kHz bandwidth.***

This is the same resource grid as for LTE in normal CP length for one resource block, which is important for the in-band operation mode. A *resource element* is defined as one subcarrier in one OFDMA symbol and is indicated in Figure 3-3 by one square. Each of these resource elements carries a complex value with values according to the modulation scheme.

These slots are summed up into subframes and radio frames in the same way as for LTE:

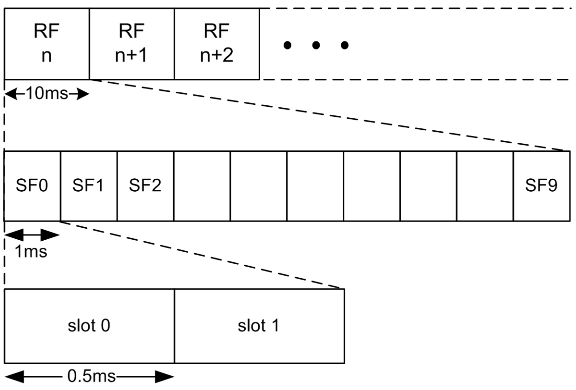


*Figure 3-4: Frame structure for NB-IoT for DL and UL with 15kHz subcarrier spacing*

There are 1024 cyclically repeated radio frames, each of 10ms duration. A radio frame is partitioned into 10 SFs, each one composed of two slots.

In addition to the system frames, also the concept of *hyper frames* is defined, which counts the number of system frame periods, i.e. it is incremented each time the system frame number wraps. It is a 10 bit counter, so that the hyper frame period spans 1024 system frame periods, corresponding to a time interval of almost 3 hours.

### 3.2.2 Narrowband Reference Signal

The narrowband reference signal (NRS) is transmitted in all SFs which may be used for broadcast or dedicated DL transmission, no matter if data is actually transmitted or not, see Chapter 3.2.5, "Dedicated Channels", on page 16 for more details.

Depending on the transmission scheme, NRS is either transmitted on one antenna port or on two. Its values are created like the CRS in LTE, with the NCellID taken for the PCI. The mapping sequence is shown in the following figure:

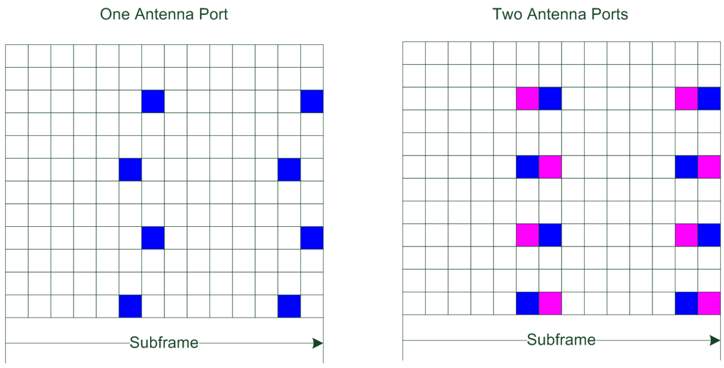


*Figure 3-5: Basic mapping of reference signals to the resource elements. In blue, NRS transmitted on antenna port 0, in magenta, NRS transmitted on antenna port 1.*

The NRS mapping shown in Figure 3-5 is additionally cyclically shifted by NCellID mod 6 in the frequency range. When NRSs are transmitted on two APs, then on every resource element used for NRS on AP0, the same resource element on AP1 is set to zero and vice versa.

For the in-band operation, the LTE CRS are also transmitted in the NB-IoT bands for the SFs which are not used for MBSFN. With the structure of the NRS there is no overlap between the LTE CRS and the NRS, however the CRS have to be taken into account for rate matching and resource element mapping. All DL transmissions must not use these resource elements and have to skip them.

An important point on the in-band operation concerns the NcellID. It may be the same as the PCI for the embedding LTE cell or not. This is indicated by the *opeartionMode* parameter in MIB-NB, see Chapter 3.2.4, "Narrowband Physical Broadcast Channel", on page 14, which distinguishes between in-band operation with same PCI as *true* or *false*. If this parameter is set to *true*, then NCellID and PCI are the same and the UE may assume that the number of antenna ports is the same as in the LTE cell. The channel may then be inferred from either reference signal set. Therefore, LTE CRS port 0 is associated with NRS port 0, and CRS port 1 is associated with NRS port 1. If *same-PCI* is set to *false*, the UE may not take any of these assumptions.

### 3.2.3 Synchronization Signals

For a first synchronization in frame and subframe and in order to determine the NCellID, the LTE concept of *Primary Synchronization Signal* (PSS) and *Secondary Synchronization Signal* (SSS) is reused. With these signals, also timing and frequency estimation may be refined in the UE receiver.

In order to distinguish these signals from their LTE counterparts, they are denoted as *NPSS* and *NSSS*, respectively. Their structure is depicted in the following figure:

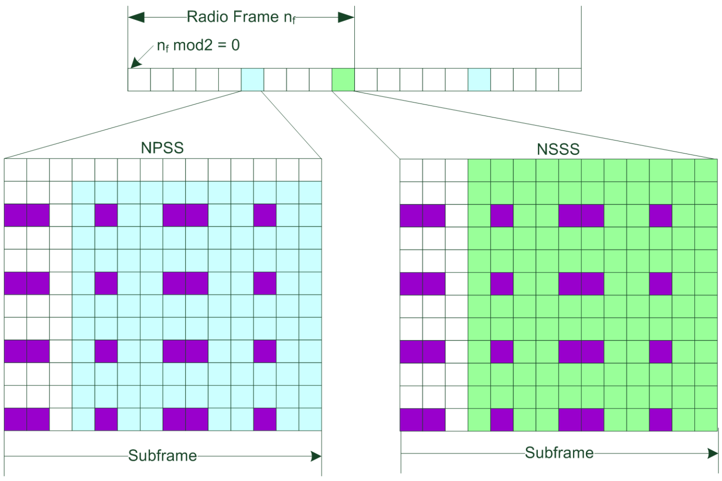


***Figure 3-6: Primary and secondary synchronization signals indicated in light blue and green, respectively. In violet, LTE CRS locations are shown. In this example we assume a 4 antenna port CRS transmission. NRS are not transmitted in the NPSS and NSSS subframes.***

The first 3 OFDM symbols are left out, because they may carry the PDCCH in LTE when NB-IoT is operated in the in-band mode. Note that during the time when the UE synchronizes to the NPSS and NSSS, it may not know the operation mode, consequently this guard time applies to all modes. In addition, both synchronization signals are punctured by the LTE's CRS. It is not specified, which of the antenna ports is used for the synchronization signals, this may even change between any two SFs.

A length 11 Zadoff-Chu sequence in frequency domain is taken for the sequence generation of the NPSS. This sequence is fixed and therefore carries no information about the cell. It is transmitted in SF5 of each radio frame, so that its reception allows the UE to determine the frame boundary.

The NSSS sequence is generated from a length-131 frequency domain Zadoff-Chu sequence, binary scrambled and cyclically shifted depending on the radio frame number. NCellID is an additional input parameter so that it can be derived from the sequence. Like in LTE, 504 PCI values are defined. NSSS are transmitted in the last SF of each even numbered radio frame.

For the in-band operation, transmission of the NPSS and NSSS, as well as the NPBCH described in the next section, may only be done on PRBs as indicated in Table 3-1. The carrier selected for receiving this information is called *anchor carrier*.

Using this construction, the UE can not confuse the NB synhronization signals with those transmitted by the LTE system. Consequently, there is no danger of a false detection and UEs with either technology are automatically routed to the correct frequency range.

### 3.2.4 Narrowband Physical Broadcast Channel

NPBCH carries the Narrowband Master Information Block (MIB-NB). The MIB-NB contains 34 bits and is transmitted over a time period of 640ms, i.e. 64 radio frames. The following information is provided therein:

- 4 bits indicating the most significant bits (MSBs) of the System Frame Number (SFN), the remaining least significant bits (LSBs) are implicitely derived from the MIB-NB start
- 2 bits indicating the two LSBs of the hyper frame number
- 4 bits for the SIB1-NB scheduling and size
- 5 bits indicating the system information value tag
- 1 bit indicating whether access class barring is applied
- 7 bits indicating the operation mode with the mode specific values
- 11 spare bits for future extensions

Figure 3-7 shows its mapping to physical resources:

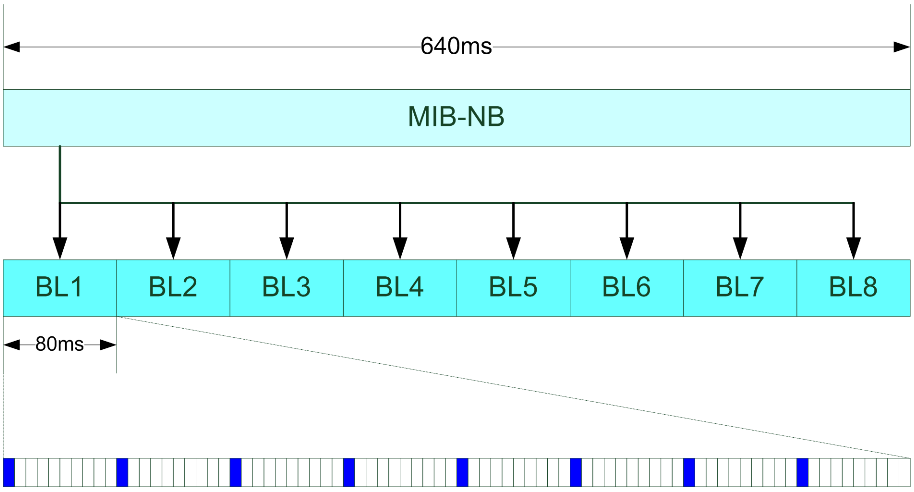


*Figure 3-7: NPBCH mapping to the subframes*

After physical layer baseband processing, the resulting MIB-NB is split into 8 blocks. The first block is transmitted on the first subframe (SF0) and repeated in SF0 of the next 7 consecutive radio frames, respectively. In SF0 of the following radio frame, the same procedure is done for BL2. This process is continued until the whole MIB-NB is transmitted. By using SF0 for all transmissions, it is avoided that NPBCH collides with a potential MBSFN transmission on LTE, if NB-IoT is deployed as in-band operation.

The SF structure of the NPBCH is shown in the following figure:

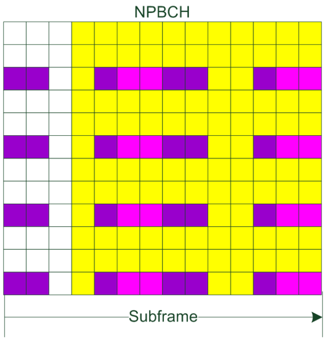


*Figure 3-8: Resource element occupation of the NPBCH indicated in yellow. In magenta, the NRS are shown, and in violet, the CRS.*

Symbols are mapped around the NRS and the LTE CRS, where it is always assumed that two antenna ports are defined for NRS and 4 antenna ports for CRS. This assumption is necessary, because the UE gets the actual antenna port information only from reading the MIB-NB. The reference signal location in the frequency range is given by the NCellID, provided by the NSSS. Although the NCellID may be different to the PCI in the in-band operation, its range is restricted so that it points to the same frequency locations, hence the CRS's cyclic shift in the frequency range is known to the UE. Again, the first 3 OFDM symbols are left out in order to avoid a possible conflict with the LTE's control channel.

## 3.2.5 Dedicated Channels

The principle of control and shared channel also applies for NB-IoT, defining the *Narrowband Physical Downlink Control Channel* (NPDCCH) and the *Narrowband Phsyical Downlink Shared Channel* (NPDSCH). Not all SFs may be used for transmission of the dedicated DL channels. In RRC signaling, a bitmap of either 10 or 40 bit indicating the valid SFs may be signaled, which is applied in a periodic way. For the case that a SF is not indicated as valid, dedicated DL channel transmission is postponed until the next valid SF.

### 3.2.5.1 Control Channel NPDCCH

The NPDCCH indicates for which UE there is data in the NPDSCH, where to find them and how often they are repeated. Also, the UL grants are provided therein, showing the resources the UE shall use for data transmission in the UL. Finally, additional information like paging or system information update is contained in the NPDCCH as well.

The NPDCCH subframe design is depicted in the following figure:

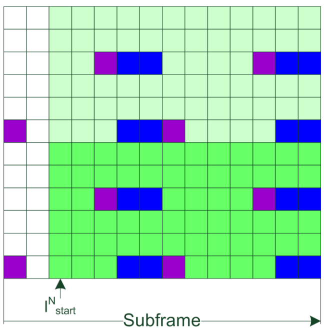


***Figure 3-9: Resource elements used by NPDCCH (light and dark green), LTE CRS (violet) and NRS (blue). This example shows the mapping for an in-band operation assuming a single antenna port in the LTE cell and two antenna ports in NB-IoT.***

Resource elements used for NPDCCH are indicated in green color. They have to be mapped around the NRS shown in blue, and for the in-band operation also around the CRS (violet). A parameter $l^N_{start}$, the control region size signaled by NB-SIB1, indicates the OFDM start symbol. This way conflict with the LTE control channel can be avoided for the in-band operation. For the guard-band and standalone operation modes, the control region size is by default *0*, which provides more resource elements for the NPDCCH.

On each SF, two narrowband control channel elements (NCCEs) are defined, NCCE0 and NCCE1. They are indicated in Figure 3-9 with dark green color (NCCE0), and light green (NCCE1). Two NPDCCH formats are defined to use them:

- NPDCCH format 0 taking one NCCE. Consequently, two of them can be transmitted within a SF.
- NPDCCH format 1 taking both NCCEs.

In order for the UE to find the control information with a reasonable amount of decoding complexity, NPDCCH is grouped into the following search spaces:

- Type-1 common search space, used for paging
- Type-2 common search space, used for random access
- UE specific search space

Each NPDCCH may be repeated several times with an upper limit configured by the RRC. In addition, Type-2 common search space and UE specific search space are provided by RRC, whereas the Type-1 common search space is given by the paging opportunity SFs, see Chapter 4.7, "Paging", on page 32.

Different *radio network temporary identifier* (RNTI) are assigned to each UE, one for random access (RA-RNTI), one for paging (P-RNTI), and a UE specific identifier (C-RNTI) provided in the random access procedure. These identifiers are implicitely indicated in the NPDCCH's CRC. So, the UE has to look in its search space for that RNTI, and, if found, decodes the NPDCCH.

Three DCI formats are defined in Release 13, DCI format N0, N1 and N2 [10]:

| DCI Format | SIze / bit | Content |
|---|---|---|
| N0 | 23 | UL grant |
| N1 | 23 | NPDSCH scheduling<br>RACH procedure initiated by NPDCCH order |
| N2 | 15 | Paging and direct indication |

When the UE receives the NPDCCH, it can distinguish the different formats in the following way: DCI format N2 is implicitely indicated in the way that the CRC is scrambled with the P-RNTI. If the CRC is scrambled with the C-RNTI, then the first bit in the message indicates whether DCI format N0 or N1 is contained. For the case that the CRC is scrambled with the RA-RNTI, the content is a restricted DCI format N1 including only those fields required for the RACH response.

Included in the DCI formats N0 and N1 is the the scheduling delay, i.e. the time between the NPDCCH end and the NPDSCH start or the NPUSCH start. This delay is at least 5 SFs for the NPDSCH and 8 for the NPUSCH. For DL transmission via DCI format N2, the scheduling delay is fixed to 10 SFs.

#### 3.2.5.2 Traffic Channel NPDSCH

An NPDSCH SF has the same structure as for the NPDCCH shown in Figure 3-9. It starts at a configurable OFDM symbol $l^{N}_{start}$ and is mapped around the NRS and, for in-band operation, the LTE CRS. $l^{N}_{start}$ is provided by RRC signaling for the in-band operation, and is *0* otherwise.

A maximum transport block size (TBS) of 680 bit is supported. The mapping of a transport block spans $N_{SF}$ SFs. The transport block is repeated providing $N_{Rep}$ identical copies, using an SF interleaving for an optimized reception at the UE. Both values, $N_{SF}$ and $N_{Rep}$ are indicated in the DCI. The resulting SF sequence is mapped to $N_{SF} \cdot N_{Rep}$ consecutive SFs defined for NPDSCH.

For the DL there is no automatic acknowledgement to a transmission, the eNB indicates this in the DCI. If this is done, the UE transmits the acknowledgement using

NPUSCH format 2, see Chapter 3.3.2, "Physical Uplink Shared Channel", on page 19. The associated timing and subcarrier is indicated in this DCI as well.

There is multi-carrier support for all operation modes, see Chapter 5.2.2, "Multi Carrier Configuration", on page 35, which means that another carrier may be used when the UE is in the connected state. In the idle state, the UE camps on the NB-IoT carrier from which it received the synchronization signals and broadcast information, i.e. the anchor carrier. It waits there for paging or starts access for mobile originated data or signaling, both by transmitting a preamble in the associated UL carrier provided in SIB2-NB.

**SIB1-NB Transmission**

SIB1-NB is transmitted over the NPDSCH. Its has a period of 256 radio frames and is repeated 4, 8 or 16 times. The transport block size and the number of repetitions is indicated in the MIB-NB. 4, 8 or 16 repetitions are possible, and 4 transport block sizes of 208, 328, 440 and 680 bits are defined, respectively. The radio frame on which the SIB1-NB starts is determined by the number of repetitions and the NCellID. SF4 is used for SIB1-NB in all radio frames transmitting SIB1-NB. As the other transmission parameters are also fixed, there is no associated indication in the control channel.

SIB1-NB content may only be changed on each modification period, which has a length of 4096 radio frames, i.e. 40.96 seconds. This corresponds to 4 SFN periods, which is why the 2 LSBs of the hyper frame number are indicated in MIB-NB. If such a modification occurs, it is indicated in the NPDCCH using DCI format N2.

Although sent over the NPDSCH, SIB1-NB resources are mapped like the MIB-NB shown in Figure 3-8, i.e. leaving out the first 3 OFDM symbols. This is necessary, because the UE knows the start of the resource mapping from SIB1-NB, so it needs to decode this SIB first.

## 3.3 Uplink

For the uplink (UL), the two physical channels

- NPUSCH, the narrowband physical uplink shared channel
- NPRACH, the narrowband physical random access channel

and the

- DMRS, Demodulation Reference Signal

are defined. The connection between the physical channels and the associated transport channels is depicted in the following figure:

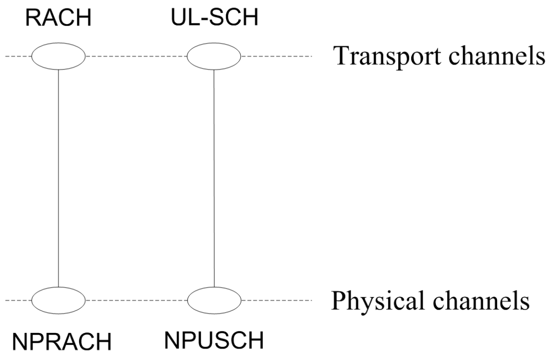


*Figure 3-10: Mapping between the transport channels and the physical channels in UL*

Except for RACH transmission, all data are sent over the NPUSCH. This includes also the UL control information (UCI), which is transmitted using a different format. Consequently there is no equivalent to the PUCCH in LTE.

### 3.3.1 Slot Structure

In the UL, *Single Carrier Frequency Division Multiple Access* (SC-FDMA) is applied, either with a 3.75 kHz or 15 kHz subcarrier spacing. eNB decides which one to use.

The resource grid for the UL is the same as for the DL, when the 15kHz subcarrier spacing is applied, see Figure 3-3. For the 3.75kHz subcarrier spacing, the resource grid for a slot has a modified structure:

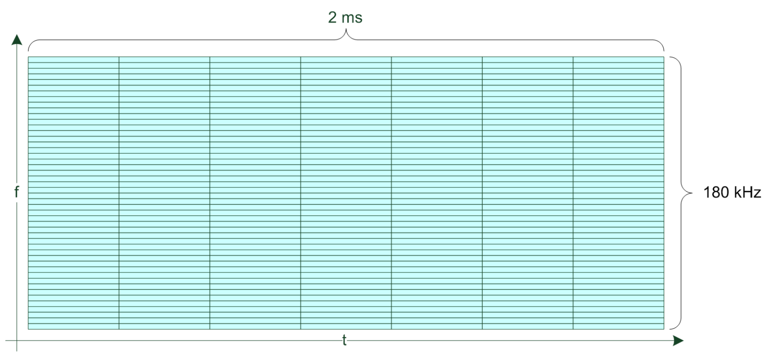


*Figure 3-11: Resource grid for 3.75 kHz subcarrier spacing. There are 48 subcarrier for the 180 kHz bandwidth*

Again there are 7 OFDM symbols within a slot. According to the OFDM principles, the symbol duration for 3.75 kHz subcarrier spacing has four times the duration compared to 15 kHz, which results in a slot length of 2 ms.

### 3.3.2 Physical Uplink Shared Channel

On the physical UL shared channel NPUSCH, two formats are defined. NPUSCH format 1 is for UL transport channel data over the UL-SCH, with transport blocks not bigger than 1000 bits. NPUSCH format 2 carries UL control information (UCI), which in Release 13 is restricted to an acknowledgement of a DL transmission.

The smallest unit to map a transport block is the *resource unit* (RU). Its definition depends on the PUSCH format and subcarrier spacing.

For NPUSCH format 1 and 3.75 kHz subcarrier spacing, an RU consists of 1 subcarrier in the frequency range, and 16 slots in the time range, i.e. an RU has a length of 32 ms. On the 15 kHz subcarrier spacing there are 4 options:

| Number of subcarriers | Number of slots | RU Duration |
|---|---|---|
| 1 | 16 | 8 ms |
| 3 | 8 | 4 ms |
| 6 | 4 | 2 ms |
| 12 | 2 | 1 ms |

For NPUSCH format 2, the RU is always composed of one subcarrier with a length of 4 slots. Consequently, for the 3.75 kHz subcarrier spacing the RU has an 8 ms duration and for the 15 kHz subcarrier spacing 2 ms.

For NPUSCH format 2, the modulation scheme is always BPSK. The allowed modulations for NPUSCH format 1 depend on the selected RU:

- For RUs with one subcarrier, BPSK and QPSK may be used
- For all other RUs, QPSK is applied

A grant for UL-SCH transmission is indicated in the NPDCCH via DCI format N0. The start time of the NPUSCH, the number of repetitions, the number of RUs used for one transport block, and the number of subcarriers including their position in the frequency range are indicated in this DCI. Also the MCS index is contained, providing the modulation scheme for the one subcarrier RUs and in addition, together with the number of RUs, the transport block size.

Finally, the time signal is created by applying an inverse fourier transrformation and prepending a cyclic prefix (CP). For the 15kHz subcarrier spacing, this CP is the same as for LTE using normal CP, while for 3.75kHz it is 256 samples, corresponding to 8.3 µs. For the latter case, a period of 2304 samples (75µs) at the end of each slot remains empty, which is used as a guard interval. For the in-band operation, this guard interval may be used to transmit Sounding Reference Signals in the LTE system.

Contrary to the DL transmission, where it is configurable whether a transmission shall be acknowledged, there is always an acknowledgement in the associated DL.

### 3.3.3 Reference Signals

In UL, *demodulation reference signal* (DMRS) is defined. It is multiplexed with the data so that it is only transmitted in RUs containing data transmission. There is no MIMO transmission defined for the UL, consequently all transmissions use a single antenna port.

Depending on the NPUSCH format, DMRS is transmitted in either one or three SC-FDMA symbols per slot. For NPUSCH format 1 these are the symbols indicated in red in Figure 3-12.

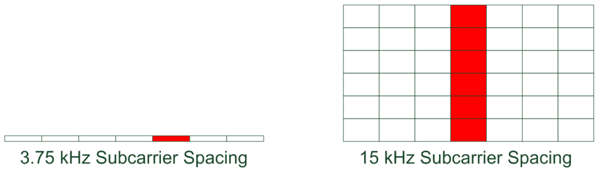


*Figure 3-12: Resource elements used for demodulation reference signal in NPUSCH format 1. This figure shows the example of an RU occupation with 6 subcarrier for the 15 kHz subcarrier spacing.*

As one can see from this figure, the SC-FDM symbols for DMRS transmission depend on the subcarrier spacing. This is also true for NPUSCH format 2 shown in Figure 3-13:


*Figure 3-13: Resource elements used for demodulation reference signals in NPUSCH format 2. In this format, the RU generally occupies only one subcarrier.*

DMRS symbols are constructed from a base sequence multiplied by a phase factor. They have the same modulation as the associated data. For NPUSCH format 2 DMRS symbols are spread with the same orthogonal sequence as defined for the LTE PUCCH formats 1, 1a and 1b.

### 3.3.4 Random Access Channel

In the Random Access Channel, NPRACH, a preamble is transmitted. The associated random access procedure, described in Chapter 4.4, "Random Access Procedure", on page 27, may be used to signal to the cell that the UE is camping on it and wants to get access.

The preamble is based on symbol groups on a single subcarrier. Each symbol group has a cyclic prefix (CP) followed by 5 symbols. The following structure shows this sequence:

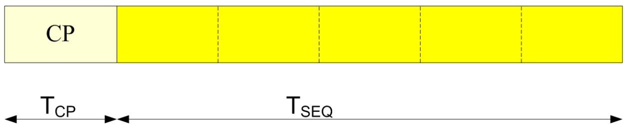


*Figure 3-14: Preamble symbol group*

Two preamble formats are defined, format 0 and format 1, which differ in their CP length. The five symbols have a duration of $T_{SEQ}$ = 1.333 ms, prepended with a CP of $T_{CP}$ = 67 µs for format 0 and 267 µs for format 1, giving a total length of 1.4 ms and 1.6 ms, respectively. The preamble format to be used is broadcasted in the system information.

The preamble is composed of 4 symbol groups transmitted without gaps. Frequency hopping is applied on symbol group granularity, i.e. each symbol group is transmitted on a different subcarrier. By construction, this hopping is restricted to a contiguous set of 12 subcarrier. Depending on the coverage level, the cell may indicate that the UE shall repeat the preamble 1, 2, 4, 8, 16, 32, 64, or 128 times, using the same transmission power on each repetition.

NPRACH resources are provided for each CE group separately. They consist in the assignment of time and frequency resources and occur periodically, where NPRACH periodicities between 40 ms and 2.56 s may be configured. Their start time within a period is provided in system information. The number of repetitions and the preamble format determine their end.

In the frequency range, subcarrier spacing of 3.75 kHz is applied. NPRACH resources occupy a contiguous set of either 12, 24, 36 or 48 subcarriers and are located on a discrete set of subcarrier ranges. Depending on the cell configuration, the resources may be further partitioned into resources used by UEs supporting multi-tone transmission for msg3 and UEs that do not support it.

Figure 3-15 shows an example of a preamble repeated at least 4 times. Here, each blue rectangle describes one preamble symbol group as depicted in Figure 3-14, hence a preamble repetition consists of four rectangles.

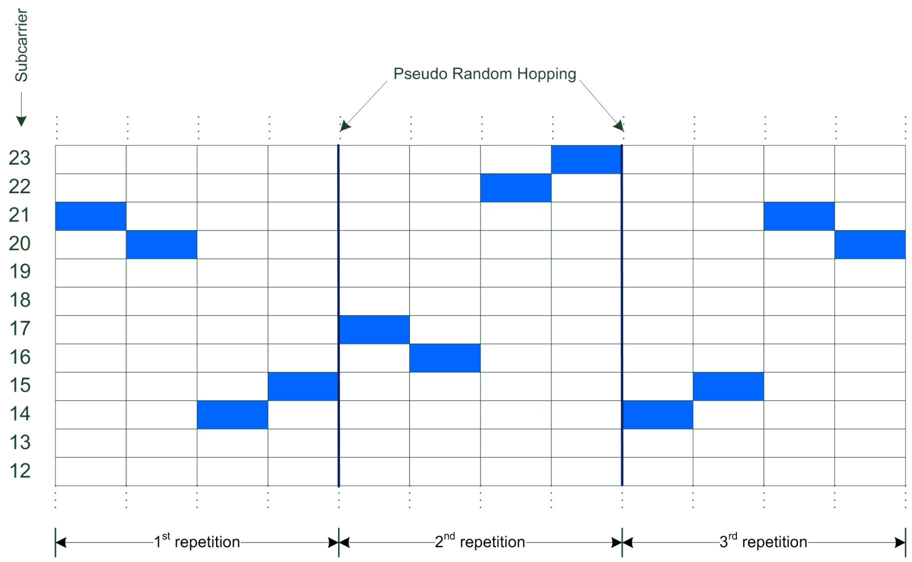


*Figure 3-15: Preamble sequence in a frequency range between subcarrier 12 and 23*

Among the 12 possibilities, the UE selects the subcarrier for the transmission of the first preamble symbol group, if not provided by the eNB for the case of an ordered preamble transmission. The next 3 symbol groups are determined by an algorithm which depends only on the location of the first one. For the subcarrier selection of the first symbol group of the next repetition, a pseudo-random hopping is applied, where NCellID and the repetition number are used as input. The subcarrier selection of the following symbol groups again depend only on this result.

This frequency hopping algorithm is designed in a way that different selections of the first subcarrier lead to hopping schemes which never overlap. Hence there are as many different congestion free preambles as there are subcarrier allocated to the

NPRACH. No further partitioning is done for NB-IoT, i.e. there is no concept like the preamble indices applied in LTE.

The preamble sequence is built upon a Zadoff-Chu sequence, which depends on the subcarrier location. Modulation and upconversion to the carrier frequency is done in the same way as for LTE.

## 3.4 Power Control

### 3.4.1 Uplink

In the UL, the transmitted power depends on a combination of cell specific parameters, the selected RU and UE measured parameters [11]. For the case that there are maximally 2 repetitions, the power on slot *i* is given by

$$P_{\mathrm{NPUSCH,c}}(i) = \min \begin{Bmatrix} P_{\mathrm{CMAX},c}(i), \\ 10\log_{10}(M_{\mathrm{NPUSCH,c}}(i)) + P_{\mathrm{O\_NPUSCH,c}}(j) + \alpha_c(j) \cdot PL_c \end{Bmatrix}$$

If there are more than two repetitions, the transmission power is generally given by $P_{CMAX,c}(i)$.

$P_{CMAX,c}(i)$ is the cell specific maximum transmit power on slot *i*. With the above construction, the transmitted power may never exceed this threshold. $M_{NPUSCH,c}$ depends on the bandwidth of the selected RU and the subcarrier spacing, $P_{O\_NPUSCH,c}$ a combination of different parameters signaled by the RRC, which depends on whether the transport block is for UL-SCH data *(j=1)* or for the RACH message *(j=2)*. $PL_c$ is the path loss estimated by the UE. This factor is weighted by $\alpha_c$ *(j)*, which for NPUSCH format 1 is provided by RRC, otherwise the fixed value of *1* is applied. In other words, this factor indicates how strong the path loss shall be compensated.

### 3.4.2 Downlink

DL transmission power refers to the NRS transmission power. Its value is indicated to the UE in order to estimate the path loss. It is constant for all resource elements carrying the NRS and all SFs.

For the NPBCH, NPDCCH and NPDSCH the transmit power depends on the transmission scheme. If only one antenna port is applied, the power is the same as for the NRS, otherwise it is reduced by 3dB.

A special case occurs if the in-band operation mode is used and the *samePCI* value is set to *true*. Then the eNB may additionally signal the ratio of the NRS power to the CRS power, enabling the UE to use the CRS for channel estimation as well.

# 4 Cell Access

When a UE accesses a cell, it follows the same principle as for LTE: It first searches a cell on an appropriate frequency, reads the associated SIB information, and starts the random access procedure to establish an RRC connection. With this connection it registers with the core network via the NAS layer, if not already done. After the UE has returned to the RRC_IDLE state, it may either use again the random access procedure if it has mobile originated data to send, or waits until it gets paged.

## 4.1 Protocol Stack and Signaling Bearer

The general principle for the protocol layers is to start with the LTE protocols, reduce them to a minimum and enhance them as needed for NB-IoT. This way, the proven structures and procedures are re-used while overhead from unused LTE features is prevented. Consequently, the NB-IoT technology can be regarded as a new air interface also from the protocol stack point of view, while being built on a well established fundament.

One example thereof is the bearer structure. Signaling radio bearer are partly re-used from LTE. There is the SRB0 for RRC messages transmitted over the CCCH logical channel, and the SRB1 for RRC messages and NAS messages using the DCCH logical channel. However, there is no SRB2 defined.

In addition, a new signaling radio bearer, the *SRB1bis* is defined. It is implicitely configured with SRB1 using the same configuration, however without the PDCP. This channel takes the role of the SRB1 until security is activated, then SRB1bis is not used anymore. This also implies that for the Control Plane CIoT EPS optimisation, only SRB1bis is used at all, because there is no security activation in this mode.

The protocol stacks are the same as for LTE with functionalities optimized for NB-IoT:

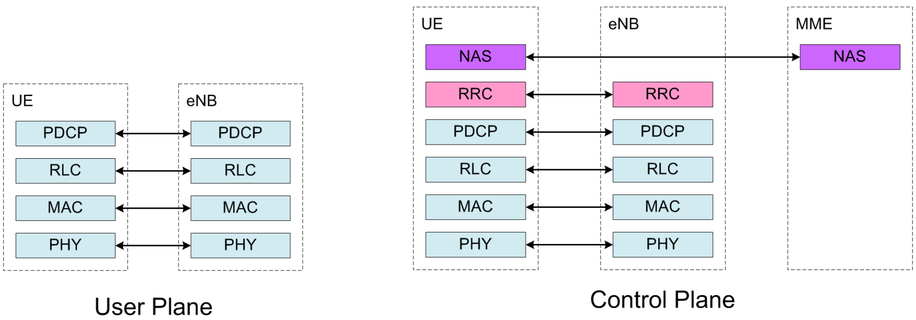


*Figure 4-1: Protocol stacks for NB-IoT*

## 4.2 System Information

Like in LTE, system information is used to broadcast information which is valid for all UEs within a cell. As broadcasting system information takes resources and causes battery consumption for each UE, it is kept to a minimum, as well in its size as in its occurence.

Consequently, a set of System Information Blocks (SIBs) is defined, which is a subset of the SIBs defined for LTE. These are shown in the following table:

| System Information Block | Content |
|---|---|
| MIB-NB | Essential information required to receive further system information |
| SIBType1-NB | Cell access and selection, other SIB scheduling |
| SIBType2-NB | Radio resource configuration information |
| SIBType3-NB | Cell re-selection information for intra-frequency, inter-frequency |
| SIBType4-NB | Neighboring cell related information relevant for intra-frequency cell re-selection |
| SIBType5-NB | Neighboring cell related information relevant for inter-frequency cell re-selection |
| SIBType14-NB | Access Barring parameters |
| SIBType16-NB | Information related to GPS time and Coordinated Universal Time (UTC) |

SIBs are indicated with the suffix *NB*. Each of these SIBs is defined with a reduced and modified set of information elements, however, the type of content is the same as in LTE, e.g. SIB16-NB describes the time information. UEs exclusively use these SIBs and ignore those from LTE, even in the case of in-band operation.

It is always mandatory for a UE to have a valid version of MIB-NB, SIB1-NB and SIB2-NB through SIB5-NB. The other ones have to be valid if their functionality is required for operation. For instance, if access barring (AB) is indicated in MIB-NB, the UE needs to have a valid SIB14-NB.

System information acquisition and change procedure is only applied in the RRC_IDLE state. The UE is not expected to read SIB information while being in the RRC_CONNECTED state. If a change occurs, the UE is informed either by paging or direct indication. The eNB may also release the UE to the RRC_IDLE state for the purpose of acquiring modified system information.

### 4.2.1 Scheduling

The MIB-NB and SIB1-NB are transmitted as indicated in Chapter 3.2, "Downlink", on page 10. Scheduling of the remaining SIB information is done in an analogous way to LTE: SIB-NB messages are grouped into SI messages, which are then transmitted in separate SI-windows. The SI windows of different SI messages do not overlap. Their length is indicated in SIB1-NB and is the same for all SI messages. The maximum size of each SIB and SI message is 680 bit.

Within an SI window, the SI messages are sent over 2 or 8 consecutive valid DL SFs, depending on their transport block size, and may be repeated several times. Scheduling information is indicated in SIB1-NB, consequently there is no indication in the NPDCCH necessary and there is no SI-RNTI needed.

### 4.2.2 Change Notification

As already mentioned in "SIB1-NB Transmission" on page 18 system information may only change at the time boundaries of a modification period and is indicated with a paging message. An exception is the change in the access barring (AB) indicated via SIB14-NB, this information may be changed at any given point in time. The reason behind this exception is that AB parameters may be required to change in a much shorter time scale. Of course, SIB16-NB is not indicated by a paging notification, as it changes its content regularly.

An additional way to indicate changes in SIB1-NB or in SI messages is the concept of the value tag. The associated field *systemInfoValueTag* is contained in MIB-NB. This concept is used for UEs returning from an out-of-coverage location back to coverage and for returning from a longer DRX cycle. In these cases the UE could not receive the paging message, so it checks the value tag. If there were SIB changes, the value tag is modified. However, the UE must read the system information anyway if it was out-of-coverage for more than 24 hours.

### 4.2.3 Summarizing SIB Acquisition

The UE first obtains the NCellID from the NSSS. By reading the *schedulingInfoSIB1* in MIB-NB it knows SIB1-NB size and number of repetitions, and can infer its starting position. In SIB1, the location of the other SIB-NB messages are indicated. Finally, with help of the 2 LSBs of the hyperframe number obtained from MIB-NB, the UE knows when to check SIB updates, if a SIB change is indicated either by a modified value tag or by paging.

## 4.3 Cell Selection and Mobility

NB-IoT is designed for infrequent and short messages between the UE and the network. It is assumed that the UE can exchange these messages while being served from one cell, therefore, a handover procedure during RRC_CONNECTED is not needed. If such a cell change would be required, the UE has first go to the RRC_IDLE state and re-select another cell therein.

For the RRC_IDLE state, cell re-selection is defined for both, intra frequency and inter frequency cells [12]. Inter frequency refers here to the 180 kHz carrier, which means that even if two carriers are used in the in-band operation embedded into the same LTE carrier, this is still referred to as an inter frequency re-selection.

In order to find a cell, the UE first measures the received power and quality of the NRS. These values are then compared to cell specific thresholds provided by the SIB-NB. The S-criteria states that if both values are above these thresholds, the UE considers itself to be in coverage of that cell. If the UE is in coverage of one cell, it camps on it.

Depending on the received NRS power, the UE may have to start a cell re-selection. The UE compares this power to a re-selection threshold, which may be different for the intra-frequency and the inter-frequency case. All required parameters are received from the actual serving cell, there is no need to read SIB-NBs from other cells.

Among all cells fulfilling the S-criteria, the UE ranks the cells with respect to the power excess over another threshold. A hysteresis is added in this process in order to prevent too frequent cell reselection, and also a cell specific offset may be applied for the intra frequency case. Contrary to LTE, there are no priorities for the different frequencies. The UE finally selects the highest ranked cell which is suitable, i.e. from which it may receive normal service.

When the UE leaves RRC_CONNECTED, it does not necessarily select the same carrier to find a cell to camp on. The *RRCConnectionRelease* messsage may indicate the frequency on which the UE first tries to find a suitable cell. Only if the UE does not find a suitable cell on this frequency, it may also try to find one on different frequencies.

## 4.4 Random Access Procedure

The RACH procedure has the same message flow as for LTE, however, with different parameters [13]:

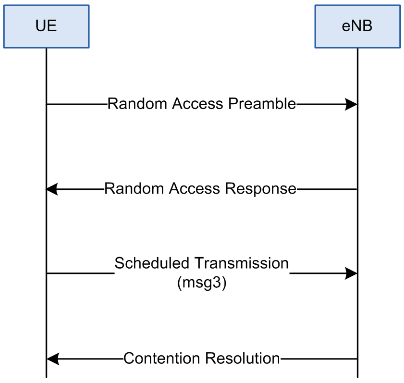


***Figure 4-2: Message flow for the RACH procedure. Each of these messages is repeated according to the UEs coverage enhancement level.***

For NB-IoT the RACH procedure is always contention based and starts with the transmission of a preamble as outlined in Chapter 3.3.4, "Random Access Channel", on page 21. After the associated response from the eNB, a scheduled message, msg3, is transmitted in order to start the contention resolution process. The associated contention resolution message is finally transmitted to the UE in order to indicate the succesful completion of the RACH procedure.

Upon transmission of the preamble, the UE first calculates its RA-RNTI from the transmission time. It looks then in the PDCCH for the DCI format N1 scrambled with the RA-

RNTI, in which the *Random Access Response* message is indicated. The UE expects this message within the *Response Window*, which starts 3 SFs after the last preamble SF and has a CE dependent length given in SIB2-NB.

If the preamble transmission was not successful, i.e. the associated *Random Access Response* (RAR) message was not received, the UE transmits another one. This is done up to a maximum number, which again is depending on the CE level. For the case that this maximum number is reached without success, the UE proceeds to the next CE level, if this level is configured. If the total number of access attempts is reached, an associated failure is reported to the RRC.

With the RAR, the UE gets in addition to a temporary C-RNTI the timing advance command. Consequently, the following msg3 is already time aligned, which is necessary for transmission over the NPUSCH. Further, the RAR provides the UL grant for msg3, containing all relevant data for msg3 transmission.

The remaining procedure is done like in LTE, i.e. the UE sends an identification and upon reception of the Contention Resolution indicating this identification the random access procedure is successfully finalized.

## 4.5 Connection Control

With a system not supporting handover to a different technology , the state model of the RRC becomes quite simple (Figure 4-3).

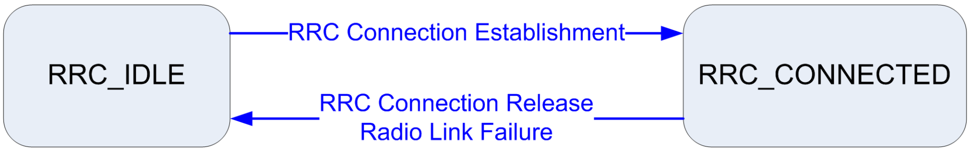


***Figure 4-3: Model of the RRC states and their transitions***

As in LTE, there are only two states, RRC_IDLE and RRC_CONNECTED. However, there are no transitions to the associated UTRA and GSM states, because handovers to these technologies are not supported. There is also no handover to LTE, because LTE is regarded as a different RAT.

### 4.5.1 RRC Connection Establishment

The RRC Connection Establishment has the same message flow as for the LTE system:

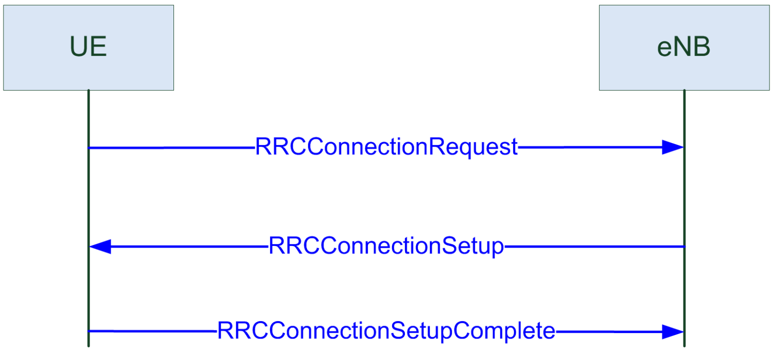


***Figure 4-4: RRC Connection Establishment. The message flow is like in LTE, however the content is different***

With the *RRCConnectionRequest* the UE indicates that it wants to connect to the network and for what purpose. This *Establishment Cause* is restricted to mobile originated signaling, mobile originated data, mobile terminated access and exceptional reports. There is no establishment cause for delay tolerant traffic, because in NB-IoT all traffic is assumed to be delay tolerant. In addition to the establishment cause, the UE also indicates its capability to support multi-tone traffic and multi carrier support. Although the capabilities are generally signaled in an own procedure, see Chapter 4.6, "UE Capability Transfer", on page 31, these capabilities have to be signaled already here so that the eNB can apply them for following UL grants in this procedure.

Upon response with the *RRCConnectionSetup* message the eNB provides configuration of the signaling radio bearer (SRB1), up to 2 data radio bearer (DRB) and the protocols. Finally, in the *RRCConnectionSetupComplete* message the UE includes its selected PLMN and MME, and can piggyback the first NAS message.

After the connection is set up for User Plane CIoT EPS optimisation, security and RRC connection reconfiguration procedures are done in the same way as for LTE with functionalities restricted to NB-IoT. Also the RRC connection re-establishment procedure is defined for this case. For Control Plane CIoT EPS optimisation, these procedures are not applied.

When the eNB releases the connection, see Chapter 4.5.2, "RRC Connection Release", on page 31, it may also suspend the UE. In this case, the UE transits to the RRC_IDLE state and stores the current AS context. It may resume later the RRC_CONNECTED state with that context. Radio bearer are automatically set up, and security is activated with updated keys. In addition, parts of the AS context may be changed. Obviously, this saves considerable signaling overhead for the transmission of infrequent small data packets.

The RRC Connection Resume is depicted in the following figure:

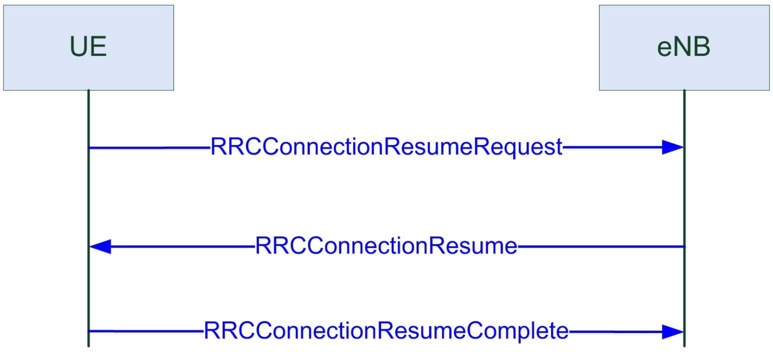


*Figure 4-5: RRC Connection Resume request accepted by the eNB*

The resume request may only be applied, when the UE is configured for User Plane CIoT EPS optimisation and is configured with at least one DRB. Upon reception of the *RRCConnectionResumeRequest*, the eNB decides whether it accepts this request or whether a conventional RRC Connection Setup shall be started. If the eNB does not accept the resume request, it switches back to the connection request:

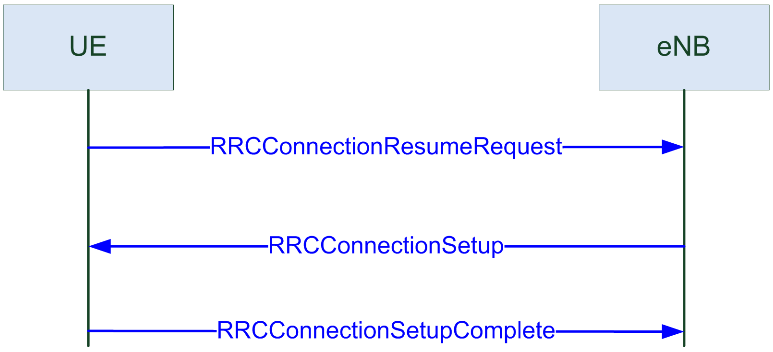


*Figure 4-6: RRC Connection Resume request not accepted by the eNB*

In this case, the UE releases the stored AS context and it is not possible anymore to resume this AS context for a later connection.

When the eNB indicates in the MIB-NB that access is subject to access class barring and broadcasts SIB14-NB, the UE has first to do an access barring check when it wants the connection for mobile originated signaling or data, before it tries to establish or resume an RRC connection. Commercially available UEs have an access class from 0 to 9. In SIB14-NB there is a associated bitmap containing one bit for each access class. If the bit associated to the access class is set, then access to that cell is barred. The UE has then to wait for an update of SIB14-NB to check again the actual barring status. Note that this access barring check may be skipped for some exceptional data, depending on the SIB14-NB settings.

If the request for connection or resume request is rejected, e.g. because there are no free resources anymore, the eNB replies with an *RRCConnectionReject* instead. Then, the UE has to wait for an amount of time provided by the reject message. This way, the eNB can prevent an excessive jam when by any reason too many UEs start network connection simultaneously. If the reject is for a resume procedure, the eNB indicates whether the current UE context shall be released or kept further stored for a following resume request.

### 4.5.2 RRC Connection Release

The RRC connection release is initiated by the eNB and is depicted in Figure 4-7.


***Figure 4-7: RRC connection release, always triggered by the eNB***

For User Plane CIoT EPS optimisation the eNB may indicate here the suspension of the connection with the *rrcSuspend* flag. In this case, the UE stores the AS context and may request an RRC connection resume as described above, otherwise the AS context is deleted and the UE may only get another RRC connection using the complete RRC connection setup.

After this procedure has been finalized, the UE enters the RRC_IDLE state.

## 4.6 UE Capability Transfer

When the UE connects to the network, the eNB does neither know on which release the UE is built upon, nor which of the optional features defined therein it supports. In order to get this information the *UE Capability Transfer* procudure is defined, which is shown in Figure 4-8:

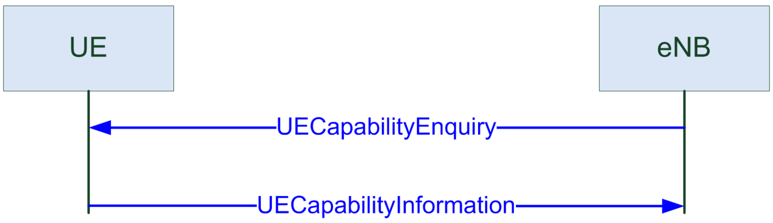


***Figure 4-8: UE capability transfer***

UE capability transfer is always initiated by the eNB, because the UE cannot know whether the eNB has this information already from the network or from a previous session.

The capabilities include the release the UE is built upon, the UE category, the list of supported bands and the capability to set up multiple bearer. In addition, the UE may indicate whether it supports multi carrier operation, and multi tone transmission in UL. Also the maximal number of RoHC context sessions and the supported profiles may be contained.

This message is usually considerably smaller than the corresponding LTE message, because all LTE features which are not supported in NB-IoT, like further access technologies or carrier aggregation, are left out.

## 4.7 Paging

Paging is used to trigger an RRC connection and to indicate a change in system information for UE in RRC_IDLE mode.

A paging message is sent over the NPDSCH and may contain a list of UEs to be paged and the information, whether paging is for connection setup or whether system information has changed. Each UE which finds its ID in this list forwards to its upper layer that it is paged, and may receive in turn the command to initialize an RRC connection. If system information has changed, the UE starts to read SIB1-NB and may obtain from there the information, which SIBs have to be read again.

The UE in the RRC_IDLE state only monitors some of the SFs with respect to paging, the *paging occasions* (PO) within a subset of radio frames, the *paging frames* (PF). If coverage enhancement repetitions are applied, the PO refers to the first transmission within the repetitions. The PFs and POs are determined from the DRX cycle provided in SIB2-NB, and the IMSI provided by the USIM card. DRX is the discontinous reception of DL control channel used to save battery lifetime. Cycles of 128, 256, 512 and 1024 radio frames are supported, corresponding to a time interval between 1.28s and 10.24s.

Due to the fact that the algorithm to determine the PFs and POs also depends on the IMSI, different UEs have different paging occasions, which are uniformly distributed in time. It is sufficient for the UE to monitor one paging occasion within a DRX cycle, if there are several paging occasions therein, the paging is repeated in every one of them.

The concept of extended DRX (eDRX) may be applied for NB-IoT as well. This is done using the hyper frames outlined in Chapter 3.2.1, "Frame and Slot Structure", on page 11. If eDRX is supported, then the time interval in which the UE does not monitor the paging messages may be considerably extended, up to almost 3 hours. Correspondingly, the UE must know on which HFN and on which time interval within this HFN, the *paging time window* (PTW), it has to monitor the paging. The PTW is defined by a start and stop SFN. Within a PTW, the determination of the PFs and POs is done in the same way as for the non-extended DRX.

# 5 Data Transfer

As described in Chapter 2.2.1, "Core Network", on page 5 , there are two ways for the data transfer, the Control Plane CIoT EPS optimisation and the User Plane CIoT EPS optimisation. The MME indicates support for each of those optimizations. For mobile originated data, the UE may select among the supported options. For mobile terminated data the MME choses the optimization and may take the UE preference into account, which is signaled to the network in the attach procedure.

## 5.1 Control Plane CIoT EPS Optimisation

For the Control Plane CIoT EPS optimisation, data exchange between the UE and the eNB is done on RRC level. In the DL, data packets may be piggybacked in the *RRCConnectionSetup* message or in the UL in the *RRCConnectionSetupComplete* message. If this is not sufficient, data transfer may be continued using the two messages *DLInformationTransfer* and *ULInformationTransfer*:

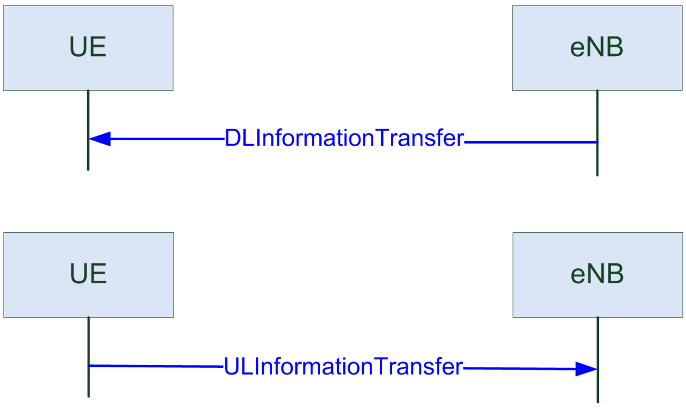


*Figure 5-1: NAS dedicated information transfer between the UE and the eNB*

Contained in all these messages is a byte array containg NAS information, which in this case corresponds to the NB-IoT data packets. Consequently it is transparent to the eNB, and the UE's RRC forwards the content of the received DLInformationTransfer directly to its upper layer. Between the eNB and the MME, the dedicatedInfoNAS is exchanged via the S1-MME interface.

For this data transfer method, security on AS level is not applied. As there is also no RRC connection reconfiguration, it may immediately start after or during the RRC connection setup or resume procedure, respectively. Of course, the RRC connection has to be terminated afterwards with the RRC connection release.

## 5.2 User Plane CIoT EPS optimisation

In the *User Plane CIoT EPS optimisation* data is transferred over the conventional user plane through the network, i.e. the eNB forwards the data to the S-GW or receives it from this node. In order to keep the UE complexity low, only one or two DRB may be configured simultaneously.

Two cases have to be distinguished: When the previous RRC connection was released with a possible resume operation indicated, see Chapter 4.5.2, "RRC Connection Release", on page 31, the connection may be requested as a resume procedure as shown in Figure 4-5. If this resume procedure is successful, security is established with updated keys and the radio bearer are set up like in the previous connection. If there was no previous release with a resume indication, or if the resume request was not accepted by the eNB, security and radio bearer have to be established as shown in the next section.

### 5.2.1 Establishment and Configuration of the Data Connection

After having set up the RRC connection as shown in Figure 4-4 or Figure 4-6, the first step is to establish AS level security. This is done via the *Initial security activation* procedure:


***Figure 5-2: Establishment of AS level security***

In the *SecurityModeCommand* message, the eNB provides the UE with the ciphering algorithm to be applied on the SRB1 and the DRB(s), and the integrity protection algorithm to protect the SRB1. All algorithms defined for LTE are also included in NB-IoT. With this message, the SRB1bis automatically changes to the SRB1, which is used for the following control messages.

After the security is activated, DRBs are set up using the *RRC connection reconfiguration* procedure:


***Figure 5-3: RRC connection reconfiguration procedure***

In the reconfiguration message, the eNB provides the UE with the radio bearer, including the configuration of the RLC and the logical channels. The latter includes a priority used to balance the data transmission according to the actual requirements. PDCP is only configured for DRBs, because the SRB only uses the default values.

In the included MAC configuration, the configuration for buffer status report (BSR), scheduling request (SR), time alignment and DRX are provided. Finally, the physical configuration provides the necessary parameters for mapping the data to the slots and frequencies.

### 5.2.2 Multi Carrier Configuration

The RRCConnectionReconfiguration may contain the settings for an additional carrier in UL and DL, the *non-anchor carrier*.

When a non-anchor carrier is provided in DL, the UE shall receive all data on this frequency. This excludes the synchronization, broadcast information and paging, which are only received on the anchor carrier. A bitmap may be provided indicating the allowed DL SFs. The non-anchor carrier may contain considerable more SFs for data, since it does not require synchronization and broadcast information.

Once the non-anchor carrier is configured, the UE solely listens to this one while it is in the RRC_CONNECTED state. Consequently the UE requires only one receiver chain.

In UL the same principle applies. If an additional UL carrier is configured, the UE only takes this one for data transmission, there is no simultaneous transmission in this carrier and the anchor carrier.

For both, DL and UL, the UE returns to its anchor carrier when it is released to the RRC_IDLE state.

Figure 5-4 shows a scheduling example:

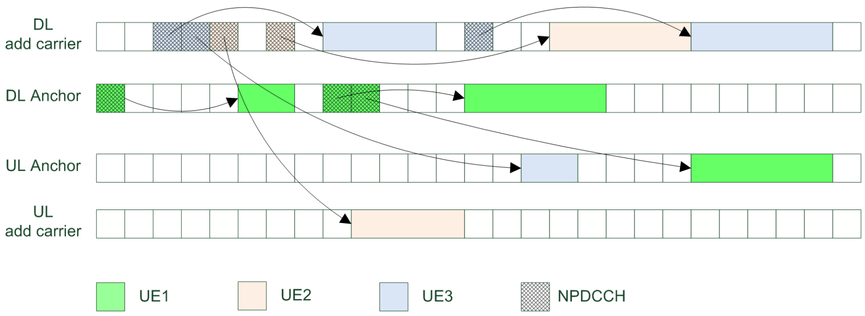


***Figure 5-4: Scheduling example for 3 UEs. Every square denotes one subframe.***

UE1 is configured with the anchor carrier, UE2 with other carrier in DL and UL, and UE3 with a different carrier only on DL. For simplicity, this diagram neither considers the NPDCCH period explained in the next section nor the SFs which are not allowed for DL data. It shall only be interpreted in a schematic way.

Even in the in-band operation, the assigned DL carrier is not restricted to the values shown in Table 3-1. This restriction is only for those carrier transmitting the NPSS, NSSS and NPBCH, i.e. which may be used as anchor carrier. For a provided DL frequency, all carriers are allowed.

This structure allows to roll out an NB-IoT broadband network, although each UE only has one transmitter / receiver chain with a narrow bandwidth available. The overhead of synchronization, broadcast in DL, and the NPRACH resources in the UL may be restricted to one or a view pairs of carrier, while the other ones may be completely used for data transmission. As the reception and transmission is never done simultaneously and always restricted to one band, respectively, it is sufficient that the UE only has one transmitter / receiver chain with a bandwidth of 180 kHz.

### 5.2.3 Receiving the Control Channel

In the RRC connected state, the UE only monitors the UE specific search space (USS) to obtain its UL grants and DL assignments. The reconfiguration message contains the maximum number of repetitions, which ranges from 1 up to 2048 in powers of 2. However, the actual number of repetitions may be smaller, as indicated in the following table:

| Max nr. of repetitions $R_{max}$ | Actual nr. of repetitions |
|---|---|
| 1 | 1 |
| 2 | 1, 2 |
| 4 | 1, 2, 4 |
| >= 8 | $R_{max}/8$, $R_{max}/4$, $R_{max}/2$, $R_{max}$ |

For the case that the actual number of repetitions is smaller than its maximum number, the remaining SFs may be used to send a different NPDCCH to another UE. For example, if the maximum number of repetitions is 4, then all SFs may contain the DCI for one UE, or two SFs may be used for each of two UEs, or each SF for a different UE, respectively. Of course, the UE has to monitor all these candidates.

The reconfiguration message also contains a parameter to describe the *NPDCCH period*. With respect to the start of this period, the USS starts either at the beginning or at an offset of 1/8, 1/4 or 3/8 of the period length.

### 5.2.4 Transmitting the UL Data Channel

The DCI format N0 indicates an UL grant for transmission on the NPUSCH, including all relevant parameters. One transport block can be repeated several times. The arrangement of the repetitions depends on the number of subcarriers for one RU, the subcarrier spacing and the number of repetitions. This shall be first illuminated with an example shown in Figure 5-5:

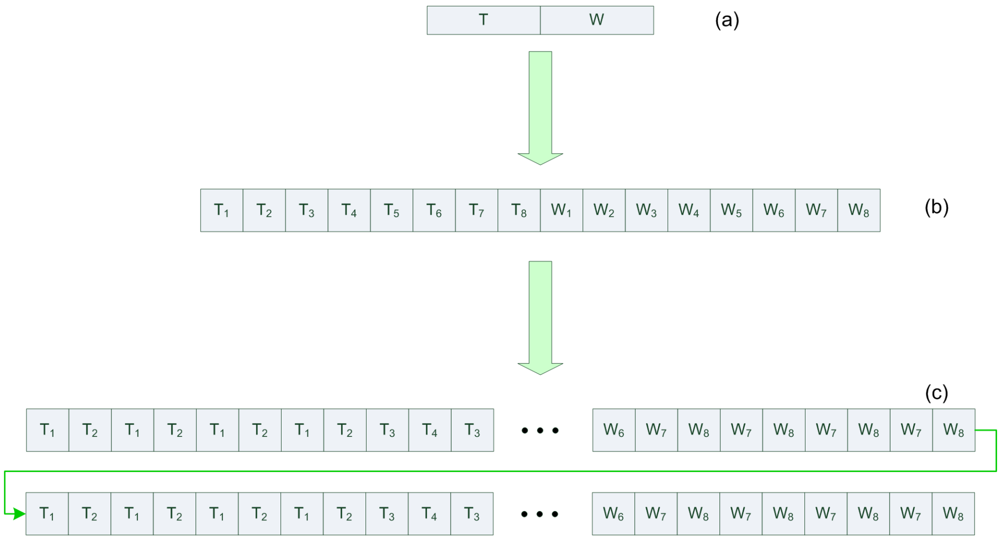


*Figure 5-5: Example of an arrangement for NPUSCH transmission with repetitions. For the case of no repetitions, the slot sequence shown in (b) would be transmitted.*

For the case of a 15 kHz subcarrier spacing, a transport block, named *test word* (TW), is transmitted on two RUs (a), where each RU has the format of 3 subcarrier over 8 slots (b). A total number of 8 repetitions is applied. In Figure 5-5 $T_n$ denotes the n-th slot of the first RU, $W_m$ the m-th slot of the second RU.

In a first step, the two slots $T_1$ and $T_2$ are transmitted. This pair is repeated three more times, so that there are 4 transmissions of these slots. Then the same procedure is done with the next two slots. This is continued until the slots $W_7$ and $W_8$ are pairwise transmitted four times. Finally, as there are now 4 repetitions of the TW, the transmission sequence is repeated once again, reaching this way the 8 repetitions.

In the general case, the first repetition of two slots is always done for a subcarrier spacing of 15 kHz. On the 3.75 kHz subcarrier spacing it is done for every slot separately. The total number of first repetitions is half the number of total repetitions with an upper limit of four, if the RU has more than one subcarrier, or one if the RU has only one subcarrier. On the above example this would mean that if there would be 32 repetitions, the sequence generation would be like in Figure 5-5 (c), however the total sequence would be repeated 7 additional times.

Usually, the sequence is mapped to a contiguous set of slots. An exception occurs on a larger number of repetitions. To be more precisely, after a transmission of 256 ms, a gap of 40 ms is created before the NPUSCH transmission is continued. This gap is necessary, because when the UE transmits on the NPUSCH, it cannot simultaneously receive the DL channel and may so lose the synchronization to the eNB. During this gap, synchronization is fine-tuned again.

### 5.2.5 Receiving the DL Data Channel

The DCI format N1 indicates a DL assignment describing where and how the data symbols are transmitted on the NPDSCH. The principle is essentially the same as for the UL, see the example shown in Figure 5-5, however the data packets are not grouped first into RUs. If there are no repetitions, the data packets are consecutively mapped into slots and sent in NPDSCH SFs.

For the case that there are repetitions, the mapping is similar like in multi-tone UL. Data for two slots are first mapped into one SF, which is now repeated with the total number of repetitions, again with an upper limit of four. Then the mapping is continued the same way until all SFs are transmitted. Finally this whole structure is repeated until the desired number of repetitions is reached.

There is an exception, when the DL data contains SIB-NB information. In this case, the slots are transmitted consecutively like in the example in Figure 5-5 (b), and then this whole block is repeated the appropriate number of times.

Transmission gaps may be configured by the RRC for NPDSCH transmissions with a large number of repetitions. The *RRCConnectionReconfiguration* message may provide the information how big the number of repetitions shall be in order to trigger such gaps, the periodicity and the length of their occurences. When the gap occurs, the NPDSCH transmission is postponed to the next available SF after the gap. These gaps do not apply for NPDSCHs carrying MIB-NB or SIB-NB information.

# 6 Summary and Outlook

With the NB-IoT technology specified in Release 13, 3GPP has created a new cellular air interface which is fully adapted to the requirements of typical machine type communications. It is optimized to small and infrequent data packets and abstains from cellular features not required for that purpose. This way, the UE can be kept in a cost efficient way and needs only a small amount of battery power.

Data transmission is kept to a small frequency band of 180 kHz. However, due to the multi-band construction a broad spectrum of frequencies may be used. The signaling part may be reduced to one or only a few NB-IoT carrier, whereas the remaining ones may be fully utilized for data transfer. This way, a considerable amount of bandwidth is used for data transfer, although the single UEs have only a comparatively narrowband transmitter and receiver.

With Release 14, the development of NB-IoT will continue [14]. According to the current plans, NB-IoT will be extended to include positioning methods, multicast services required e.g. for software update or for messages concerning a whole group, mobility and service continuity, as well as further technical details to enhance the field of applications for the NB-IoT technology. We will provide the associated technology description, so please check our website for a new version of this document.

# 7 References

[1] 3GPP TR 45.820 V13.1.0, November 2015; Cellular system support for ultra-low complexity and low throughput Internet of Things (CIoT)

[2] 3GPP TS 23.272 V13.3.0, March 2016; Circuit Switched (CS) fallback in Evolved Packet System (EPS)

[3] 3GPP TS 23.401 V13.6.1, March 2016; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network

[4] 3GPP TS 23.682 V13.5.0, March 2016; Architecture enhancements to facilitate communications with packet data networks and applications

[5] 3GPP TS 36.331 V13.2.0, June 2016; Radio Resource Control (RRC); Protocol specification

[6] 3GPP TS 36.300 V13.4.0, June 2016; Overall description

[7] 3GPP TS 36.101 V13.4.0, June 2016; User Equipment (UE) radio transmission and reception

[8] 3GPP TS 36.201 V13.2.0, June 2016; LTE physical layer; General description

[9] 3GPP TS 36.211 V13.2.0, June 2016; Physical channels and modulation

[10] 3GPP TS 36.212 V13.2.0, June 2016; Multiplexing and channel coding

[11] 3GPP TS 36.213 V13.2.0, June 2016; Physical layer procedures

[12] 3GPP TS 36.304 V13.2.0, June 2016; User Equipment (UE) procedures in idle mode

[13] 3GPP TS 36.321 V13.2.0, June 2016; Medium Access Control (MAC) protocol specification

[14] 3GPP RP-161324 3GPP Work Item Description *Enhancements of NB-IoT*

# 8 Additional Information

Please send your comments and suggestions regarding this white paper to

**TM-Applications@rohde-schwarz.com**

# 9 Rohde & Schwarz

Rohde & Schwarz is an independent group of companies specializing in electronics. It is a leading supplier of solutions in the fields of test and measurement, broadcasting, radiomonitoring and radiolocation, as well as secure communications. Established more than 80 years ago, Rohde & Schwarz has a global presence and a dedicated service network in over 70 countries. Company headquarters are in Munich, Germany.

**Sustainable product design**

- Environmental compatibility and eco-footprint
- Energy efficiency and low emissions
- Longevity and optimized total cost of ownership

| Certified Quality Management<br>ISO 9001 | Certified Environmental Management<br>ISO 14001 |
|---|---|

**Regional contact**


- Europe, Africa, Middle East
  Phone +49 89 4129 12345
  customersupport@rohde-schwarz.com
- North America
  Phone 1-888-TEST-RSA (1-888-837-8772)
  customer.support@rsa.rohde-schwarz.com
- Latin America
  Phone +1-410-910-7988
  customersupport.la@rohde-schwarz.com
- Asia/Pacific
  Phone +65 65 13 04 88
  customersupport.asia@rohde-schwarz.com
- China
  Phone +86-800-810-8228 / +86-400-650-5896
  customersupport.china@rohde-schwarz.com


**Headquarters**


Rohde & Schwarz GmbH & Co. KG

Mühldorfstraße 15 | D - 81671 München

+ 49 89 4129 - 0 | Fax + 49 89 4129 – 13777

www.rohde-schwarz.com