An Overlook on NB-IoT RRC Protocol

Michele Paffetti
University of Bologna
michele.paffetti@studio.unibo.it

General

With the Narrowband Internet of Things (NB-IoT) technology, 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.

NB-IoT support a reduced set of functionality w.r.t legacy LTE systems and is seen as a separate RAT from E-UTRAN. As reported by 3GPP documentation, the following features are not supported in NB-IoT and corresponding procedures and messages do not apply to the NB-IoT UE:

- Connected mode mobility (Handover and measurement reporting)
- Inter-RAT cell reselection or inter-RAT mobility in connected mode
- CSG (Closed Subscriber Group) and GBR (Guaranteed Bit Rate) (QoS)
- Relay Node (RN)
- support of HeNBs [1]
- Carrier Aggregation (CA)
- Dual connectivity (DC)
- ACB, EAB (Extended Access Barring), SSAC and ACDC;
- MBMS (Multimedia Broadcast Multicast Service)
- NAICS (Network Assisted Interference Cancellation and Suppression)
- Interference avoidance for in-device coexistence [1]
- Self-configuration and self-optimisation
- Measurement logging and reporting for network performance optimisation
- MDT (Minimization of Drive Test) [1]
- Public warning systems e.g. CMAS, ETWS and PWS
- Real time services (including emergency call)
- CS (Circuit Switching) services and CS fallback
- In-device coexistence
- RAN assisted WLAN interworking
- LWA and LWIP
- Sidelink (including direct communication and direct discovery)
- A UE specific DRX configured by upper layers in RRC_IDLE state
- SPS (Semi-Persistent Scheduling)

HANDOVER in NB-IoT?

- *HandoverPreparationInformation-NB* message exist (10.6.2 pag 663 TS 36.331 V14.2.1): This message is used to transfer the UE context from the eNB where the RRC connection has been suspended and transfer it to the eNB where the RRC Connection has been requested to be resumed.

- AS-Config and AS-Context (pag 665 TS 36.331 V14.2.1) exist.
- *MobilityControlInfo* → not defined for NB-IoT (not carried in RRCConnectionReconfig.-NB-r13-IE)
- T304 timer not exist: Used for reception of RRCConnectionReconfiguration message including the MobilityControl Info
- No Inter-RAT handover at all

In RRC_CONNECTED

- No handover
- No measurement reports

In RRC_IDLE

- Cell Reselection (intra frequency and Inter Frequency)
- Use SIB5-NB

RRC Introduction

Generally speaking, the major functions of the Radio Resource Control (RRC) protocol include connection establishment, maintenance, reconfiguration and release functions, broadcast of system information related to NAS (common and dedicated) and AS, radio bearer establishment, RRC connection mobility procedures, paging notification and security functions. The following figure show a general User Plane and Control Plane LTE protocol stack in order to highlight the RRC layer level.

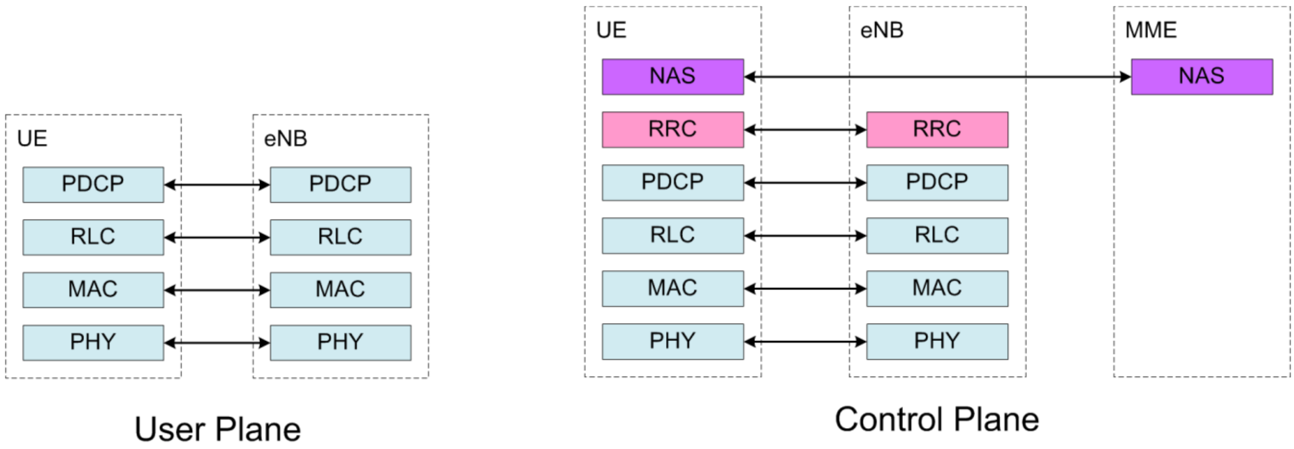

Figure 1 Control Plane and User Plane Protocol Stack

As will become more clear during this document, the RRC protocol for NB-IoT inherits directly from LTE RRC protocol some main functionalities but at the same time introduce strong simplification for others.

RRC States and State Transitions

With a system not supporting handover to a different technology (inter-RAT mobility) , the state model of the RRC becomes quite simple as shown in the following figure.

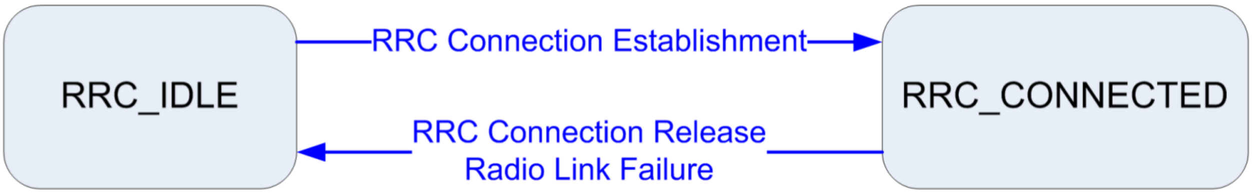

Figure 2 RRC State Model [2]

As in LTE, NB-IoT RRC states are only two: RRC_IDLE and RRC_ CONNECTED. However, there are no transitions to the associated UTRA and GSM states, because for NB-IoT handover between E-UTRA and UTRAN, GERAN and between E-UTRA and CDMA2000 1xRTT and CDMA2000 HRPD is not supported. There is also no handover to LTE, because LTE is regarded as a different RAT.

A UE is in RRC_CONNECTED when an RRC connection with E-UTRAN has been established, otherwise the UE is in RRC_IDLE state. The RRC states can further be characterised as follows:

- RRC_IDLE state
  - UE controlled mobility
  - UE monitors a Paging channel to detect incoming calls or system information change
  - UE performs neighbouring cell measurements and cell (re-)selection
  - UE acquires system information
  - UE performs logging of available measurements together with location and time for logged measurement configured UEs.
  - The UE shall have been allocated an ID which uniquely identifies the UE in a tracking area (TA)
  - No RRC context stored in the eNB (except for a UE that supports User Plane CIoT EPS optimizations)
- RRC_CONNECTED state
  - UE has an E-UTRAN-RRC connection;
  - UE has a stored context in E-UTRAN
  - E-UTRAN knows the cell which the UE belongs to
  - Transfer of unicast data to/from UE
  - At lower layers, the UE may be configured with a UE specific DRX
  - UE Monitors control channels associated with the shared data channel to determine if data is scheduled for it
  - the UE monitors the UE specific search space (USS) to obtain its UL grants and DL assignments [2].
  - Network controlled mobility (not for NB-IoT)

UE Procedure in RRC_IDLE mode [3]

5.2.3.2a Cell Selection Criterion for NB-IoT

The cell selection criterion S is fulfilled when:

Srxlev > 0 AND Squal > 0

where:

Srxlev = Qrxlevmeas – Qrxlevmin – Pcompensation - Qoffsettemp

Squal = Qqualmeas – Qqualmin - Qoffsettemp

where:

Srxlev	Cell selection RX level value (dB)
Squal	Cell selection quality value (dB)
$Qoffset_{temp}$	Offset temporarily applied to a cell as specified in [3] (dB)
$Q_{rxlevmeas}$	Measured cell RX level value (RSRP)
$Q_{qualmeas}$	Measured cell quality value (RSRQ)
$Q_{rxlevmin}$	Minimum required RX level in the cell (dBm) If UE is not authorized for enhanced coverage and $Qoffset_{authorization}$ is valid then $Q_{rxlevmin} = Q_{rxlevmin} + Qoffset_{authorization}$.
$Q_{qualmin}$	Minimum required quality level in the cell (dB)

Pcompensation	If the UE supports the *additionalPmax* in the *NS-PmaxList-NB*, if present, in SIB1-NB, SIB3-NB and SIB5-NB:
	$\max(P_{EMAX1} - P_{PowerClass}, 0) - (\min(P_{EMAX2}, P_{PowerClass}) - \min(P_{EMAX1}, P_{PowerClass}))$ (dB);
	else:
	if $P_{PowerClass}$ is 14 dBm:
	$\max(P_{EMAX1} - (P_{PowerClass} - Poffset), 0)$ (dB);
	else:
	$\max(P_{EMAX1} - P_{PowerClass}, 0)$ (dB)

P_{EMAX1}, P_{EMAX2}	Maximum TX power level an UE may use when transmitting on the uplink in the cell (dBm) defined as P_{EMAX} in TS 36.101 [33]. P_{EMAX1} and P_{EMAX2} are obtained from the *p-Max* and the *NS-PmaxList-NB* respectively in SIB1-NB, SIB3-NB and SIB5-NB as specified in TS 36.331 [3].
$P_{PowerClass}$	Maximum RF output power of the UE (dBm) according to the UE power class as defined in TS 36.101 [33]

5.2.7a Cell Selection when leaving RRC_CONNECTED state for NB-IoT

On transition from RRC_CONNECTED to RRC_IDLE, UE shall attempt to camp on a suitable cell according to redirectedCarrierInfo, if included in the RRCConnectionRelease-NB message. If the UE cannot find a suitable cell, the UE is allowed to camp on a suitable cell of any NB-IoT carrier. If the RRCConnectionRelease-NB message does not contain the redirectedCarrierInfo UE shall attempt to select a suitable cell on a NB-IoT carrier.

Signalling Radio Bearers (SRB)

"Signalling Radio Bearers" (SRBs) are defined as Radio Bearers (RB) that are used only for the transmission of RRC and NAS messages and they are partly re-used from LTE.

In particular, for NB-IoT, a new UE dedicated SRB (SRB1bis) is supported before AS security is activated and only one UE dedicated SRB is supported after AS security is activated

More specifically, the following SRBs for NB-IOT are defined:

- SRB0: for RRC messages transmitted over the CCCH logical channel
- SRB1 is for RRC messages (which may include a piggybacked NAS message) using DCCH logical channel
- SRB1bis is for RRC messages (which may include a piggybacked NAS message) as well as for NAS messages, prior to the activation of AS security, using DCCH logical channel. It is implicitly configured with SRB1 using the same configuration, however, until the AS security activation, no PDCP integrity protection and ciphering is applied to SRB1bis (bypass PDCP)
- SRB2 is not defined for NB-IOT

NOTE:

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. [2]

NOTE:

Piggybacking of NAS messages characterization:

- Downlink: only for bearer establishment/ modification/ release
- Uplink: only for transferring the initial NAS message during connection setup. Exploit *RRCConnectionSetupComplete* or *RRCConnectionResumeComplete* message for piggybacking.

For each SRB, the value provided by RRC to lower layers to derive the 5-bit BEARER parameter used as input for ciphering and for integrity protection is the value of the corresponding *srb-Identity* with the MSBs padded with zeroes.

Security Procedure (General)

AS security comprises of the integrity protection of RRC signalling (SRBs) as well as the ciphering of RRC signalling (SRBs) and user data (DRBs).

RRC handles the configuration of the security parameters which are part of the AS configuration:

- the integrity protection algorithm
- the ciphering algorithm
- keyChangeIndicator:

  Is used upon handover and indicates whether the UE should use the keys associated with the K_{ASME} key taken into use with the latest successful NAS SMC procedure.

- nextHopChainingCount:

  Is used upon handover, connection re-establishment and connection resume by the UE when deriving the new KeNB that is used to generate KRRCint, KRRCenc and KUPenc (see TS 33.401).

The integrity protection algorithm is common for signalling radio bearers SRB1 and SRB2, while the ciphering algorithm is common for all radio bearers (i.e. SRB1, SRB2 and DRBs). Neither integrity protection nor ciphering applies for SRB0. The integrity and ciphering algorithms can only be changed upon handover. Furthermore, integrity and ciphering are always activated together and never deactivated. However, there are two possibilities:

1. to switch to a 'NULL' ciphering algorithm (eea0)
2. to switch to a 'NULL' integrity protection algorithm (eia0) only for the UE in limited service mode (see TS33.401). (In case the 'NULL' integrity protection algorithm is used, 'NULL' ciphering algorithm is also used)

Lower layers discard RRC messages for which the integrity check has failed and indicate the integrity verification check failure to RRC.

Keys

The AS applies three different security keys derived upon Connection Establishment procedure:

1. for the integrity protection of RRC signalling (K_{RRCint})
2. for the ciphering of RRC signalling (K_{RRCenc})
3. for the ciphering of user data (K_{UPenc})

All three AS keys are derived from the K_{eNB} key that is based on its turn on the K_{ASME} key handled by upper layers. Furthermore, the four AS keys (KeNB, KRRCint, KRRCenc and KUPenc) change upon every handover, connection re-establishment and connection resume.

Counter

For each radio bearer an independent counter (COUNT, as specified in TS 36.323 [8]) is maintained for each direction. For each DRB, the COUNT is used as input for ciphering. For each SRB, the

COUNT is used as input for both ciphering and integrity protection. It is not allowed to use the same COUNT value more than once for a given security key. At connection resume the COUNT is reset. The eNB is responsible for avoiding reuse of the COUNT with the same RB identity and with the same KeNB, e.g. due to the transfer of large volumes of data, release and establishment of new RBs.

Transport of NAS messages

Please refer to 3GPP document TS 36.300 V14.1.0 c.7.3

CIoT Signalling Reduction Optimization

For a NB-IoT UE that only supports Control Plane CIoT EPS optimizations, as defined in TS 24.301, PDCP is bypassed. For a NB-IoT UE that supports both Control Plane CIoT EPS optimizations and User Plane CIoT EPS optimizations, as defined in TS 24.301 [20], PDCP is also bypassed (i.e. not used) until AS security is activated.

Please refer to 3GPP document TS 36.300 V14.1.0 c.7.3a

RRC Services and Functions

The RRC protocol offers/expect the following services to/from upper/lower layers:

- Offered to upper layers
  - Broadcast of common control information
  - Notification of UEs in RRC_IDLE
- Expected from lower layers
  - PDCP: integrity protection and ciphering
  - RLC: reliable and in-sequence transfer of information, without introducing duplicates and with support for segmentation and concatenation.

The RRC protocol covers the following main functionalities:

- Broadcast of System Information (SI):
  - Including NAS and AS common information
  - Information applicable for UEs in RRC_IDLE, e.g. cell (re-)selection parameters, neighbouring cell information and information (also) applicable for UEs in RRC_CONNECTED, e.g. common channel configuration information
- RRC Connection Control
  - Paging
  - Establishment/modification/suspension/resumption/release of RRC connection, including:
    - Assignment/modification of UE identity (C-RNTI)
    - Establishment/modification/release of SRB1 and SRB1bis
    - Access class barring
  - Initial security activation, i.e. initial configuration of AS integrity protection (SRBs) and AS ciphering (SRBs, DRBs);
  - Establishment/modification/release of RBs carrying user data (DRBs)
  - RRC connection mobility (including e.g. intra-frequency and inter-frequency handover)
  - Security handling and key management, i.e. key/algorithm change
  - Specification of RRC context information transferred between network nodes
  - Radio configuration control including e.g. assignment/modification of ARQ configuration, HARQ configuration, DRX configuration

- o Recovery from Radio Link Failure
- o Other functions including
    - transfer of dedicated NAS information and non-3GPP dedicated information
    - transfer of UE radio access capability information
    - support for E-UTRAN sharing (multiple PLMN identities)(for NB-IoT?)
- o Generic Protocol Error Handling

NOTE 1:

For a NB-IoT UE that supports User Plane CIoT EPS optimizations, as defined in TS 24.301, one DRB is supported by default and up to two DRBs are supported optionally

NOTE 2:

In NB-IoT, only key change (but no re-keying) at RRC Connection Resumption and RRC context information transfer are applicable.

NB-IoT RRC Procedures

For NB-IoT, only a subset of the LTE RRC procedural requirements applies. These, are shown in the following table and some of them are (partially) presented in the next sections. For further details, always refer official 3GPP documentation.

NB-IoT RRC Procedures
System Information
Connection Control
DL Information Transfer
UL Information Transfer
UE Capability Transfer
General Error Handling

System Information (SI)

For NB-IoT, a reduced set of system information block with similar functionality but different content is defined w.r.t. LTE. In particular, the UE applies the NB-IoT (NB) version of the MIB and the SIBs denoted as MasterInformationBlock-NB (MIB-NB) and SystemInformationBlockTypeX-NB (SIBx-NB). Furthermore, UEs exclusively use the NB-IoT SIBs and ignore those from LTE, even in the case of in-band operation [2].

The following table show the list of the System Information Blocks defined for NB-IoT and their content.

NB-IoT System Information Block	**Content**
MasterInformationBlock-NB	▪ Includes a limited number of most essential and most frequently transmitted physical layer parameters that are needed to acquire other system information from the cell ▪ Is mapped on the BCCH, carried on BCH transport channel and transmitted over the NPBCH physical channel ▪ Parameters: o *systemInfoValueTag* o *ab-Enabled* o *schedulingInfoSIB (see TS 36.213)*

	○ *…TS 36.331 (pag.524)*
SystemInformationBlockType1-NB	▪ Contains information relevant when evaluating if a UE is allowed to access a cell and defines the scheduling of other system information blocks ▪ Is mapped on the BCCH, carried on DL-SCH transport channel and transmitted over the NPDSCH physical channel ▪ In addition to broadcasting, E-UTRAN may provide SIB1-NB via dedicated signalling, i.e., within an *RRCConnectionReconfiguration* message ▪ Parameters: ○ *systemInfoValueTagSI* ○ *schedulingInfoList* ○ *… TS 36.331 (pag. 535)*
SystemInformationBlockType2-NB	▪ Contains common radio resource configuration information ▪ Is mapped on the BCCH and carried on DL-SCH transport channel ▪ *see TS 36.331 (pag. 539)*
SystemInformationBlockType3-NB	▪ Contains cell re-selection information for intra-frequency, inter-frequency ▪ Is mapped on the BCCH and carried on DL-SCH transport channel ▪ *see TS 36.331 (pag. 540)*
SystemInformationBlockType4-NB	▪ Contains neighbouring cell related information relevant for intra-frequency cell re-selection ▪ Is mapped on the BCCH and carried on DL-SCH transport channel ▪ *see TS 36.331 (pag. 541)*
SystemInformationBlockType5-NB	▪ Contains neighbouring cell related information relevant for inter-frequency cell re-selection ▪ Is mapped on the BCCH and carried on DL-SCH transport channel ▪ *see TS 36.331 (pag. 541)*
SystemInformationBlockType14-NB	▪ Contains information about Access Barring (AB) ▪ Is mapped on the BCCH and carried on DL-SCH transport channel ▪ *see TS 36.331 (pag. 542)*
SystemInformationBlockType16-NB	▪ contains information related to GPS time and Coordinated Universal Time (UTC) ▪ Is mapped on the BCCH and carried on DL-SCH transport channel ▪ *see TS 36.331 (pag. 543)*

(See chapter “*TS 36.331 V14.2.1 – NB-IoT enhancements*” for new SIBs)

It is always mandatory for a UE to have a valid version of MIB-NB, SIB1-NB and SIB2-NB through SIB5-NB (see later). The other SIBs have to be valid if their functionality is required for operation. For instance, if access barring (AB) field is indicated in MIB-NB, the UE needs to have a valid SIB14-NB [2].

SIBs other than SystemInformationBlockType1 (SIB1-NB) are carried in System Information (SI) messages and mapping of SIBs to SI messages is flexibly configurable by *schedulingInfoList* included in SIB1-NB. The only restrictions are that each SIB is contained only in a single SI message and at most once in that message. Only SIBs having the same scheduling requirement (periodicity) can be mapped to the same SI message. SI messages are transmitted over the DL-SCH transport channel and for NB-IoT, the maximum SIBs-NB and SI message size is 680 bits (see TS 36.213) [4].

System Information Scheduling for NB-IoT:

Both the MIB-NB and SIB1-NB use a fixed schedule. The MIB-NB contains all information required to acquire SIB1-NB and ,on its turn, SIB1-NB contains all information required to acquire other SI messages.

- MIB-NB (34 bits):
    - uses a fixed schedule with a periodicity of 640 ms (64 Radio frames) and repetitions made within the 640 ms.
    - The first transmission of the MIB-NB is scheduled in subframe #0 of radio frames for which the SFN mod 64 = 0 and repetitions are scheduled in subframe #0 of all other radio frames.
    - After physical layer baseband processing, the resulting MIB-NB is split into 8 independently decodable blocks of 80 ms duration. 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 the following blocks. This process is continued until the whole MIB-NB is transmitted.

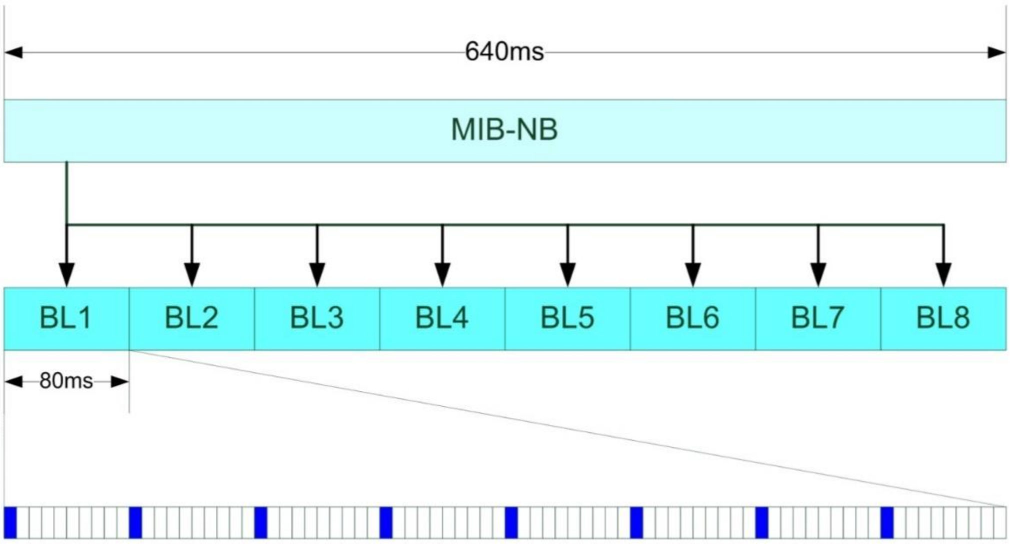

Figure 3 MIB-NB Mapping on the NB-IoT frame structure [2]

- SIB1-NB:
    - The SystemInformationBlockType1-NB (SIB1-NB) uses a fixed schedule with a periodicity of 2560 ms (256 Radio Frames).

    - SIB1-NB transmission occurs in subframe #4 of every other frame in 16 continuous frames. This means that in all radio frames transmitting SIB1-NB, the SF4 (subframe #4) is used for delivery SIB1-NB.
    - The starting frame for the first transmission of the SIB1-NB is derived from the cell PCID (Physical Channel Identity) and the number of repetitions within the 2560 ms period. Repetitions are made, equally spaced, within the 2560 ms period (see TS 36.213).
    - TBS (Transport Block Size) for SystemInformationBlockType1-NB and the repetitions made within the 2560 ms are indicated by *schedulingInfoSIB1*(see TS 36.213 Table 16.4.1.3-3) field in the MIB-NB. In particular, 4, 8 or 16 repetitions are possible, and 4 transport block sizes of 208, 328, 440 and 680 bits are defined, respectively [2].
    - SIB1-NB content may only be changed on each modification period, which has a length of 4096 radio frames, i.e. 40.96 seconds. [2]
- SI messages:
    - Are transmitted within periodically occurring time domain windows (referred to as SI-windows) using scheduling information provided in SIB1-NB.
    - Each SI message is associated with a SI-window and the SI-windows of different SI messages do not overlap. That is, within one SI-window only the corresponding SI message is transmitted.
    - The length of the SI-window is common for all SI messages and SIB1-NB configures the SI-window length and the transmission periodicity for all SI messages
    - Within the SI-window, the corresponding SI message can be transmitted a number of times over 2 or 8 consecutive NB-IoT downlink subframes depending on TBS
    - UE acquires the detailed time/frequency domain scheduling information and other information messages from *schedulingInfoList* field in SIB1-NB

System Information notification of changes/update

For NB-IoT, the UE is not required to detect SIB changes (SI update) when in RRC_CONNECTED state but only in RRC_IDLE, therefore, the network may release the NB-IoT UE to RRC_IDLE if it wants the NB-IoT UE to acquire changed SIB(s). [1] However, there are two particular case in which UE in RRC_CONNECTED state is required to acquire SI chages:

- when timer T311 is running (i.e. initiating the RRC connection reestablishment procedure)
- upon handover, where the UE is only required to acquire the MIB in the target PCell

In these cases, if a change occurs, the UE is informed either by paging or direct indication.

Change of System parameters only occur at specific radio frames (exception for SIB14-NB) and are indicated through a paging message. This requires to introduce the concept of modification period. System information may be transmitted a number of times with the same content within a modification period, as defined by its scheduling. The modification period boundaries are defined by H-SFN values for NB-IoT. In particular, boundaries are defined by SFN values for which (H-SFN * 1024 + SFN) mod m=0, where m is the number of radio frames comprising the modification period.

For instance, in NB-IoT, the possible boundaries of modification for SIB1-NB are defined by SFN values for which (H-SFN * 1024 + SFN) mod 4096 = 0.

NOTE:

For RRC_IDLE UEs configured to use a DRX cycle longer than the modification period, an eDRX acquisition period is defined for the purpose of enabling system information update/change notification being received by UE. In particular, for NB-IoT, the boundaries of the eDRX acquisition period are determined by H-SFN values for which H-SFN mod 1024 = 0.

When the network changes (some of the) system information, it first notifies the UEs about this change through a change/update notification and in the next modification period the network transmits the updated system information.

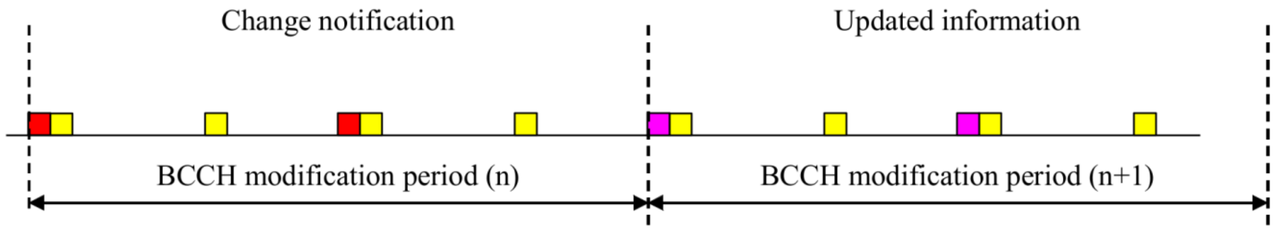

Figure 4 Change of System Information

Upon receiving a change notification:

- A UE not configured to use a DRX cycle that is longer than the modification period acquires the new system information immediately from the start of the next modification period.
- A UE in RRC_IDLE configured to use a DRX cycle that is longer than the modification period acquires the updated system information immediately from the start of the next eDRX acquisition period.

In any case, the UE applies the previously acquired system information until the UE acquires the new system information.

A Paging message including a *systemInfoModification* over the BCCH is used to inform UEs in RRC_IDLE and UEs in RRC_CONNECTED about a system information change starting from the next modification period boundary.

NOTE:
In case of a UE in RRC_IDLE that is configured to use a DRX cycle longer than the modification period, it has to receives in an eDRX acquisition period at least one Paging message including a *systemInfoModification-eDRX* and then acquiring the updated system information at the next eDRX acquisition period boundary.

An additional way to indicate changes in SIB1-NB or in SI messages is the concept of the value tag. MasterInformationBlock-NB (MIB-NB) in NB-IoT includes a value tag *systemInfoValueTag*, that indicates if a change has occurred in the SI messages. 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. [2]

Summarizing the SIB acquisition procedure:
The UE first obtains the PCID 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 H-SFN (the 2 LSBs) 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. [2]

System information Validity

UEs may use *systemInfoValueTag* to verify if the previously stored SI messages are still valid. In particular, NB-IoT UE considers stored system information to be invalid after 24 hours from the moment it was successfully confirmed as valid.

If a NB-IoT UE in RRC_CONNECTED state considers the stored system information invalid, the UE shall continue using it while in RRC_CONNECTED state in the serving cell.

For NB-IoT UEs, the change of specific SI message can additionally be indicated by a SI message specific value tag *systemInfoValueTagSI* included in the SIB1-NB.

- If *systemInfoValueTag* included in the MIB-NB and *systemInfoValueTagSI* included in the SIB1-NB for a specific SI message are different from the one of the stored system information the UE shall consider this specific SI message to be invalid.
- If only *systemInfoValueTag* is included and is different from the stored one the NB-IoT UE should consider any stored system information except SIB14-NB to be invalid

In the following, some reference cases are presented:

- E-UTRAN may not update *systemInfoValueTag* upon change of some particular system information (e.g. Access Barring) and may not include the *systemInfoModification* within the Paging message
- The UE that is not configured to use a DRX cycle longer than the modification period verifies that stored system information remains valid by either checking *systemInfoValueTag* in the MIB-NB after the modification period boundary or attempting to find the *systemInfoModification* indication at least *modificationPeriodCoeff* times during the modification period in case no paging is received, in every modification period. If no paging message is received by the UE during a modification period, the UE may assume that no change of system information will occur at the next modification period boundary.
- If UE in RRC_CONNECTED, during a modification period, receives one paging message, it may deduce from the presence/ absence of *systemInfoModification* whether a change of system information will occur in the next modification period or not.
- When the RRC_IDLE UE is configured with a DRX cycle that is longer than the modification period, and at least one modification period boundary has passed since the UE last verified validity of stored system information, the UE verifies that stored system information remains valid by checking the *systemInfoValueTag* before establishing or resuming an RRC connection.

Access barring (AB) parameter change

An exception in system information modification is related to change of Access Barring (AB) parameters carried by SIB14-NB that can occur at any point in time. The reason behind this exception is that AB parameters may be required to change in a much shorter time scale [2]. Therefore, update of the AB parameters does not impact the *systemInfoValueTag* in the MIB-NB or the *systemInfoValueTagSI* in SIB1-NB.

A NB-IoT UE checks *ab-Enabled* indication in MIB-NB (Access Barring check) to know whether access barring is enabled. If access barring is enabled the UE shall not initiate the RRC connection establishment or resume for all access causes (except mobile terminating calls) until the UE has a valid version of SIB14-NB. Commercially available UEs have an access class from 0 to 9. In SIB14-NB there is an 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. [2]

System Information Acquisition

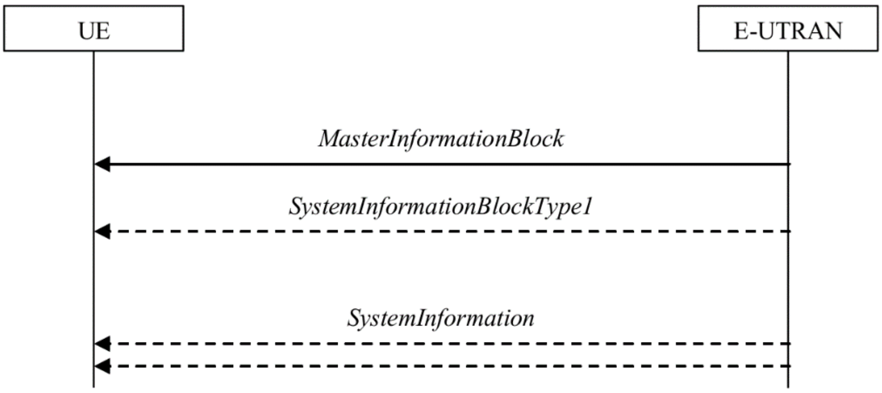

Figure 5 System Information Acquisition

The UE applies the system information acquisition procedure to acquire the AS and NAS system information that is broadcasted by the E-UTRAN. The system information acquisition procedure overwrites any stored system information and, for NB-IoT, this procedure applies only to UEs in RRC_IDLE state and only in some particular case for RRC_CONNECTED (previously mentioned).

For instance, The UE shall apply the system information acquisition procedure upon selecting or reselecting a cell, upon return from out of coverage, upon receiving a notification that the system information has changed or upon exceeding the maximum validity duration. In the following a list of possible event that trigger a system information acquisition procedure is presented:

- System information change notification
- if the UE is in RRC_IDLE and enters a cell for which the UE does not have stored a valid version of the system information required in RRC_IDLE
- A UE neither initiate the RRC connection establishment/resume procedure nor initiate transmission of the *RRCConnectionReestablishmentRequest* message until the UE has a valid version of the MIB-NB, SIB1-NB, SIB2-NB
- Following successful handover completion to a PCell for which the UE does not have stored a valid version of the system information required in RRC_CONNECTED
- If *ab-Enabled* included in MIB-NB is set to TRUE. In this case, UE not initiate the RRC connection establishment/resume procedure for all access causes (except mobile terminating calls) until the UE has acquired the SystemInformationBlockType14-NB

For further details, see 3GPP TS 36.331 (c. 5.2.2.4)

System Information required by NB-IoT UE:

A NB-IoT UE is always required to have a valid version of some System Information. In the following a list of the required SI by NB-IoT UE is presented in relation to the UE RRC state.

RRC_IDLE:

- MIB-NB
- SIB1-NB
- SIB2-NB through SIB5-NB

RRC_CONNECTED and T311 timer is running

- MIB-NB
- SIB1-NB
- SIB2-NB

As already mentioned, the UE will delete any SI after 24 hours from the moment it was confirmed to be valid and UE will consider any stored SI information (except SIB14-NB) to be invalid if the *systemInfoValueTag* included in the MIB-NB is different from the stored one and *systemInfoValueTagSI* is not broadcasted. Otherwise cosider the information validity as defined in the previous subsection.

For further details about System information procedure related to each specific NB-IoT SIB, please refer to the 3GPP TS 36.331 documentation as indicated in the table:

System Information procedure	**3GPP document**
Essential System Information Missing	TS 36.331 c. 5.2.2.5
Actions upon reception of MasterInformationBlock-NB	TS 36.331 c. 5.2.2.6
Actions upon reception of SystemInformationBlockType1-NB	TS 36.331 c. 5.2.2.7
Actions upon reception of SystemInformationBlockTypeX-NB	TS 36.331 c. 5.2.2.9 – 5.2.2.23
Acquisition of an SI message by a NB-IoT UE	TS 36.331 c. 5.2.3a

Connection Control

Introduction

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. 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 implemented in NB-IoT. If such a cell change would be required, the UE has first go to the RRC_IDLE state and re-select another cell therein. On the other hand, for the RRC_IDLE state, cell re-selection is defined for both, intra frequency and inter frequency cells (see 3GPP TS 36.304 V13.2.0) [2]

The Random Access procedure is entirely described in the MAC in 3GPP TS 36.321, therefore not mentioned in this document. On the contrary, this document focuses on the establishment of RRC connection between UE and E-UTRAN and all the related procedures.

RRC connection establishment involves the establishment of SRB1. As already mentioned in previous sections, in NB-IoT a new dedicated signalling radio bearer (SRB1bis) is supported. SRB1bis is established implicitly with SRB1, using the same configuration and the logical channel identity defined in TS 36.331 c. 9.1.2a but bypassing PDCP entity. In NB-IoT, SRB1bis is used until AS security is activated. In fact, E-UTRAN completes RRC connection establishment prior to completing the establishment of the S1 connection, i.e. prior to receiving the UE context information from the EPC. Consequently, AS security is not activated during the initial phase of the RRC connection. Furthermore, RRC messages to activate security (command and successful response) are sent over SRB1 being integrity protected only (ciphering is started after completion of the procedure). Upon receiving the UE context from the EPC, E-UTRAN activates security using the initial security activation procedure (see later). E-UTRAN should release the RRC connection if the initial security activation and/ or the radio bearer establishment fails. Once security is activated, new RRC messages shall be transmitted using only SRB1 and E-UTRAN initiates the establishment of possible DRBs, in this case applying both ciphering and integrity protection. In particular, NB-IoT UE only supports 0, 1 or 2 DRBs, depending on its capability.

NOTE:
A NB-IoT UE that only supports the Control Plane CIoT EPS optimisation (see TS 24.301) only establishes SRB1bis and does not need to support any DRBs and associated procedures.

The release or suspension of the RRC connection normally is initiated by E-UTRAN. The procedure may be used to re-direct the UE to an E-UTRA frequency. In particular, when the RRC connection is suspended the UE stores the UE AS context and the *resumeIdentity (*contained in the *RRCConnectionRelease-NB* message) and transit to RRC_IDLE state. The RRC message to suspend the RRC connection is integrity protected and ciphered and suspension procedure can only be performed when at least 1 DRB is successfully established.

The resumption of a suspended RRC connection is initiated by upper layers when the UE has a stored UE AS context, RRC connection resume is permitted by E-UTRAN and the UE needs to transit from RRC_IDLE state to RRC_CONNECTED state. When the RRC connection is resumed, RRC configures the UE according to the RRC connection resume procedure based on the stored UE AS context and any RRC configuration received from E-UTRAN. The RRC connection resume procedure re-activates security and re-establishes SRB(s) and DRB(s). The request to resume the RRC connection includes the *resumeIdentity*.

After this introduction, the next sections present more in details the relevant connection control procedures and their relevant parameters. In particular, the following table lists the Connection Control procedures that are applicable for NB-IoT. For further details, please refer to the 3GPP TS 36.331 documentation for each specific subsections as indicated.

Sub-clause	Procedures
5.3.2	Paging
5.3.3	RRC connection establishment
	RRC connection resume (see NOTE)
5.3.4	Initial security activation (see NOTE)
5.3.5	RRC connection reconfiguration (see NOTE)
5.3.7	RRC connection re-establishment (see NOTE)
5.3.8	RRC connection release
5.3.9	RRC connection release requested by upper layers
5.3.10	Radio resource configuration
5.3.11	Radio link failure related actions
5.3.12	UE actions upon leaving RRC_CONNECTED

Table 1 Connection Control procedures applicable to a NB-IoT UE

NOTE:
Not applicable for a UE that only supports the Control Plane CIoT EPS optimisation (see TS 24.301)

Paging

Figure 6 Paging

E-UTRAN initiates the paging procedure by transmitting the Paging message over the NPDSCH at the UE's paging occasion (PO) as specified in TS 36.304. The paging information is provided to upper layers, which in response may initiate RRC connection establishment, e.g. to receive an incoming call. E-UTRAN may address multiple UEs within a Paging message by including one *PagingRecord* for each UE in which a *ue-Identity* is specified.

Purpose of Paging procedure are:

- transmit paging information to a UE in RRC_IDLE
- inform UEs in RRC_IDLE about a system information change. (E-UTRAN may also indicate a change of system information in the Paging message)

Upon receiving a Paging message, a UE:

- if RRC_IDLE State and for each of the *PagingRecord* included (if any)
    - if one of the *ue-Identity* matches then forward the *ue-Identity* to upper layers
- if *systemInfoModification* or *systemInfoModification-eDRX* (for UE configured with a DRX cycle longer than the modification period) is included:
    - re-acquire the required system information using the system information acquisition procedure as specified previously
- if in RRC_IDLE, the *redistributionIndication* is included and the UE is redistribution capable
    - Perform E-UTRAN inter-frequency redistribution procedure as specified in TS 36.304 (5.2.4.10)

RRC Connection Establishment and Resuming

A RRC Connection Establishment procedure is depicted in the following figures. The message flow is like in LTE; however, the message content is different.

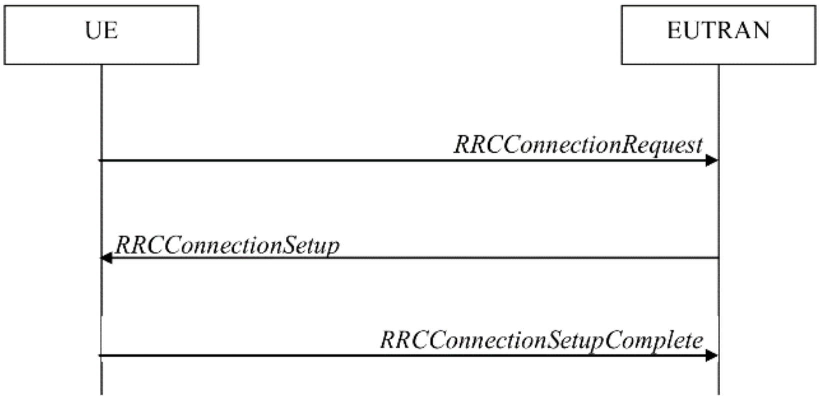

Figure 7 RRC Connection Establishment, successful

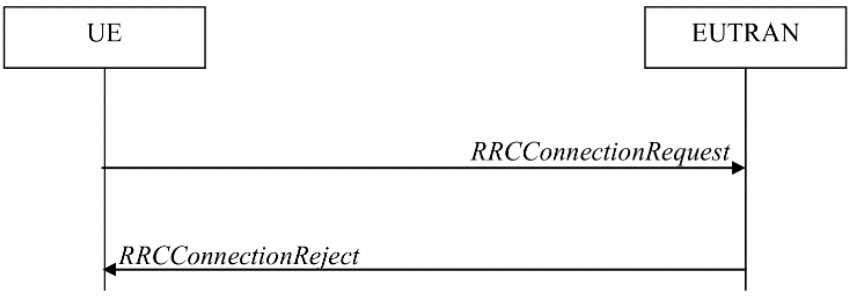

Figure 8 RRC Connection Establishment, network reject

The connection establishment procedure may be initiated for the following purposes, each of them characterize by possible responses from E-UTRAN.

- RRC first connection establishment
    - Successful

        - Network rejected
- RRC connection resume
    - Successful
    - Fallback to a RRC Connection Establishment
    - Network rejected or release

In NB-IoT, the connection establishment procedure involves SRB1 and SRB1bis establishment, while resuming an RRC connection involves restoring the AS configuration from a stored context including resuming possible SRB(s) and DRB(s). Furthermore, this procedure is also used to transfer the initial NAS dedicated information/message from the UE to E-UTRAN.

The UE initiates the procedure when upper layers request establishment or resume of an RRC connection while the UE is in RRC_IDLE. With the *RRCConnectionRequest* the UE indicates that it wants to connect to the network and for what purpose (*establishmentCause*). This *establishmentCause* is restricted to mobile originated signalling, 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 *(multiToneSupport)* and multi carrier support (*multiCarrierSupport)*. Although the UE capabilities are generally signalled in an own procedure (see later).

In particular, the NB-IoT UE shall:

- If the UE is establishing or resuming the RRC connection for mobile originating (exception) data and mobile originating signalling:
    - Perform access barring check and if access to the cell is barred, inform upper layers about the failure to establish/resume the RRC connection or failure to resume the RRC connection
- Apply the default physical channel, MAC and CCCH configuration (see TS 36.331 c. 9.2.4, 9.2.2, 9.1.1.2 respectively)
- Start timer T300
- Initiate transmission of the *RRCConnectionRequest* message (for RRC connection establishment) or *RCConnectionResumeRequest* message (for RRC connection resuming)

Upon response with the *RRCConnectionSetup* message the eNB provides configuration of the signalling radio bearer (SRB1 and SRB1bis), 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.

If the request for connection 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 (*waitTime or extendedWaitTime)*

A Connection Resume procedure is depicted in the following figures. The message flow is like in LTE; however, the message content is different.

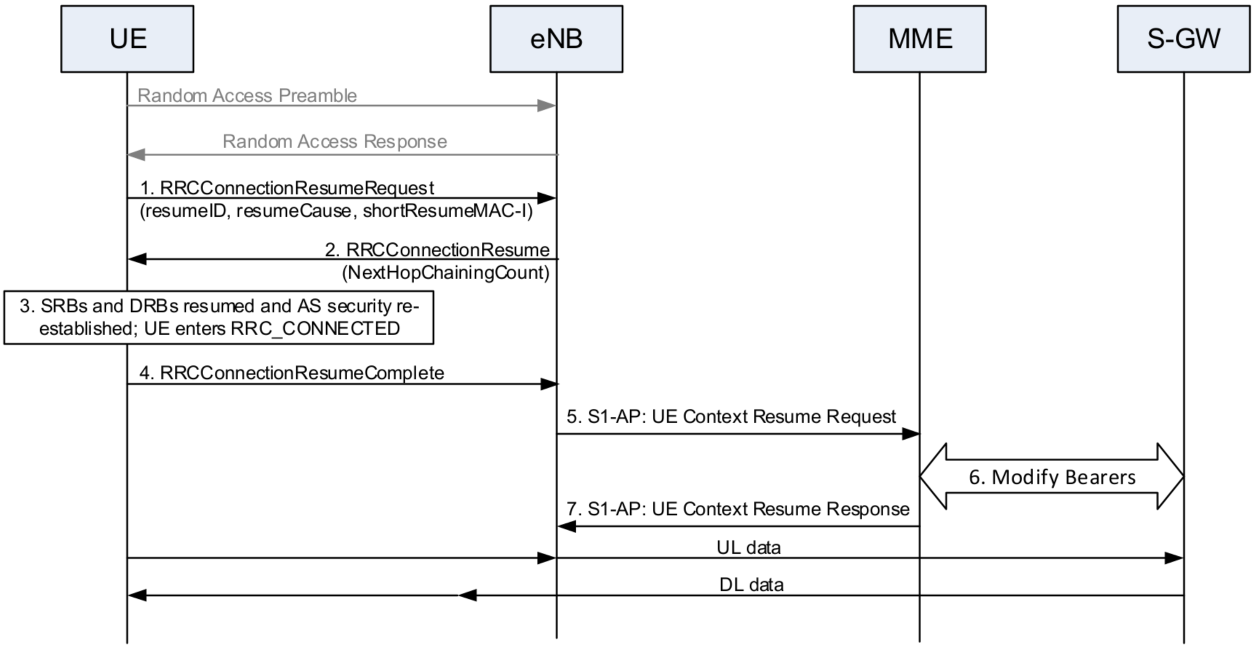

Figure 9 RRC Connection Resume, successful

In NB-IoT, 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 or reject 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 as shown in the following figures. [2]

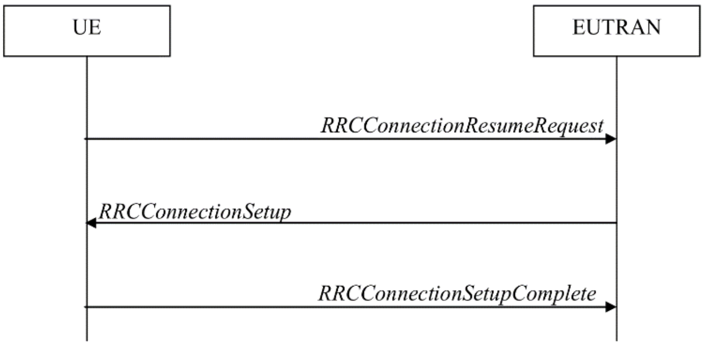

Figure 10 RRC Connection resume fallback to RRC Connection Establishment

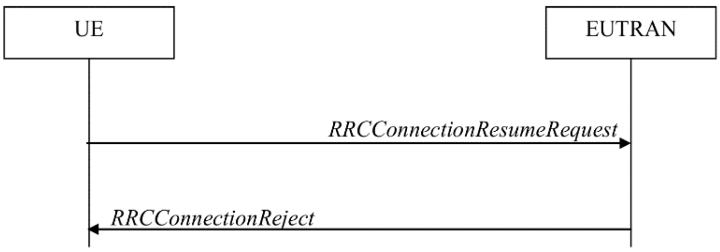

Figure 11 RRC Connection Resume, network reject

In the case the RRC Connection Resume fallback to an RRC Connection Establishment the UE releases the stored AS context and it is not possible anymore to resume this AS context for a later connection. On the other hand, if the resume procedure is rejected by the network, the eNB indicates whether the current UE context shall be released or kept further stored for a following resume request.

In the following some relevant RRC message and actions for RRC connection establishment and resuming procedure are reported with a list of the main parameters carried. For further details, please refer to the 3GPP document TS 36.331 in the corresponding chapters as indicated.

(5.3.3.3) Action related to transmission of RRCConnectionRequest message

Parameters:

- *ue-Identity*
- *establishmentCause*
- *multiToneSupport*
- *multiCarrierSupport*

(5.3.3.3a) Actions related to transmission of RRCConnectionResumeRequest message

Parameters:

- *resumeID = resumeIdentity*
- *resumeCause*
- *shortResumeMAC-I*

(5.3.3.4) Reception of the RRCConnectionSetup by the UE message

Transmission of the RRCConnectionSetupComplete message

Parameters:

- *s-TMSI*
- *registeredMME → plmnIdentity*
- *mmegi*
- *mmec*
- *attachWithoutPDN-Connectivity* (if CIoT EPS optimization supported)
- *up-CIoT-EPS-Optimisation*
- *dedicatedInfoNAS*
- *ue-CE-NeedULGaps*

(5.3.3.4a) Reception of the RRCConnectionResume by the UE

Parameter:

- *drb-ContinueROHC*
- *radioResourceConfigDedicated*
- *measConfig* (not the case of Nb-IoT)
- *nextHopChainingCount*

Transmission of the RRCConnectionResumeComplete message

Parameter:

- *selectedPLMN-Identity*
- *dedicatedInfoNAS*

(5.3.3.5) Cell re-selection while T300, T302, T303, T305, T306, or T308 is running

(5.3.3.6) T300 expiry

(5.3.3.8) Reception of the RRCConnectionReject by the UE

Parameters:

- *extendedWaitTime*

- *deprioritisationReq*
- *rrc-SuspendIndication*

(5.3.3.9) Abortion of RRC connection establishment

(5.3.3.14) Access barring check for Nb-IoT

Initial Security Activation

After having set up the RRC connection, the first step is to establish AS level security. This is done via the Initial Security Activation procedure as shown in the following figure.

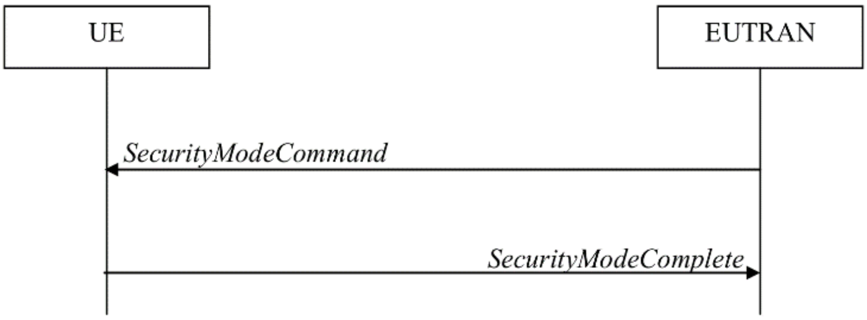

Figure 12 Security Activation, successful

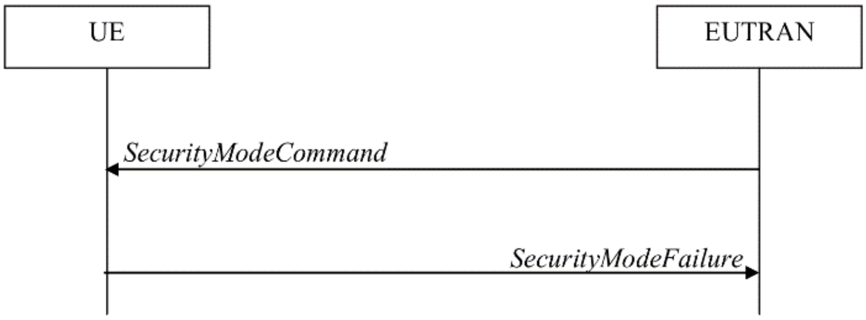

Figure 13 Security Activation, failure

E-UTRAN initiates the security mode command procedure to a UE in RRC_CONNECTED providing a *SecurityModeCommand* message (integrity protected but not ciphered) which include 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. Moreover, E-UTRAN applies the procedure when only SRB1 and SRB1bis are established. [2]

In the following some relevant RRC messages and actions for Security Activation procedure are reported with a list of the main parameters carried. For further details, please refer to the 3GPP document TS 36.331 in the corresponding chapters as indicated.

5.3.4.3 Reception of the SecurityModeCommand by the UE

Parameters:

- *integrityProtAlgorithm*
- *cipheringAlgorithm*

RRC Connection Reconfiguration

After the security is activated, RBs are set up or reconfigured using the RRC Connection Reconfiguration procedure as shown in the following figures:

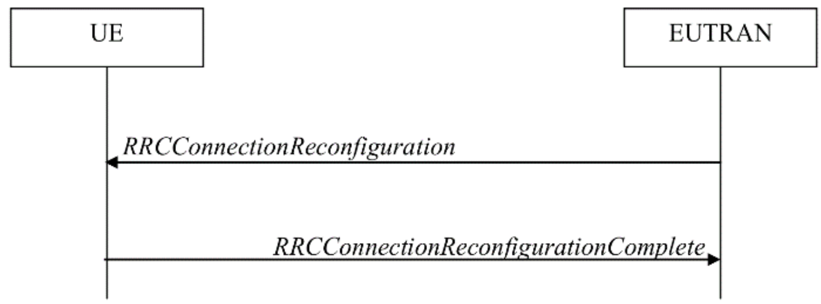

Figure 14 RRC Connection Reconfiguration, successful

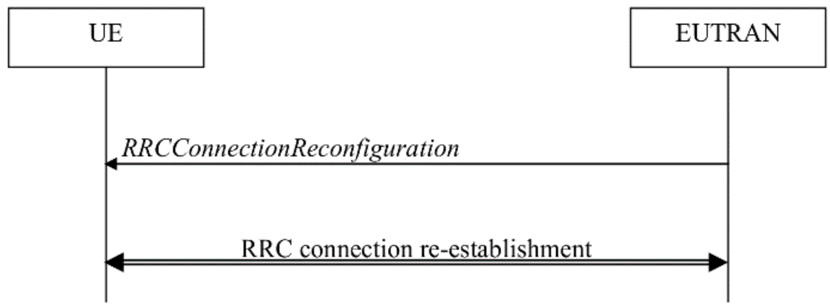

Figure 15 RRc Connection Reconfiguration, failure

E-UTRAN may initiate the RRC connection reconfiguration procedure to a UE in RRC_CONNECTED. As already mentioned, the purpose of this procedure is to modify an RRC connection, e.g. to establish/ modify/ release RBs, to perform or to add/ modify/ release SCells. In the reconfiguration message, the eNB provides the UE with the radio bearer, including the configuration of the RLC and the logical channels while PDCP is only configured for DRBs. As part of the procedure, NAS dedicated information may be transferred from E-UTRAN to the UE.

NOTE: (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. Once the non-anchor carrier is configured, the UE solely listens to this one when it is in the RRC_CONNECTED state while return on its anchor carrier when it is released to the RRC_IDLE state. In UL the same principle applies. [2]

In the following some relevant RRC messages and actions for RRC reconfiguration procedure are reported with a list of the main parameters carried. For further details, please refer to the 3GPP document TS 36.331 in the corresponding chapters as indicated.

5.3.5.3/4 Reception of an RRCConnectionReconfiguration by the UE

Parameters:

- *radioResourceConfigDedicated*
- *sCellToReleaseList*
- *systemInformationBlockType1Dedicated*
- *dedicatedInfoNASList*
- *otherConfig…*

5.3.5.5 Reconfiguration failure

5.3.5.8 Radio Configuration involving full configuration option

RRC Connection Re-establishment

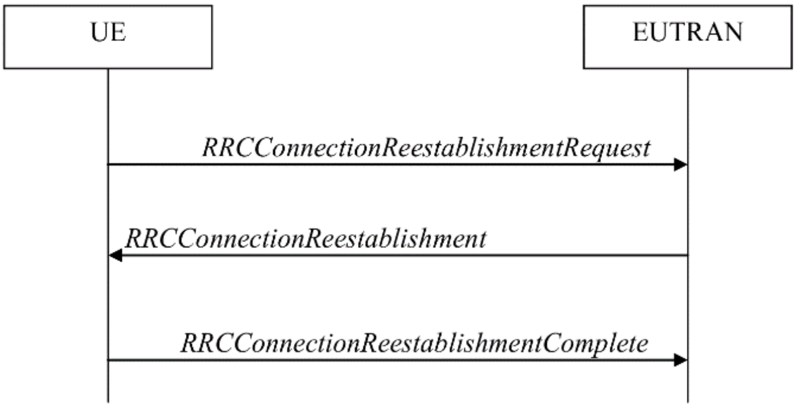

Figure 16 RRC Connection Re-establishment, successful

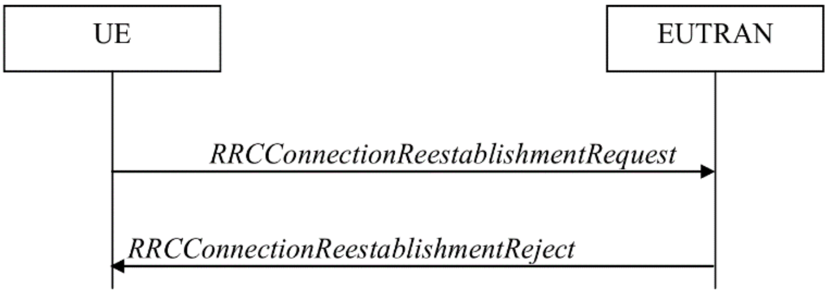

Figure 17RRC Connection Re-establishment, reject

The purpose of this procedure is to re-establish the RRC connection, which involves the resumption of SRB1 operation, the re-activation of security (without changing algorithm) and the configuration of only the PCell. A UE in RRC_CONNECTED, for which security has been activated, may initiate the procedure in order to continue the RRC connection. The connection re-establishment succeeds only if the concerned cell is prepared i.e. has a valid UE context. In case E-UTRAN accepts the re-establishment, SRB1 operation resumes while the operation of other radio bearers remains suspended. If AS security has not been activated, the UE does not initiate the procedure but instead moves to RRC_IDLE directly. The UE shall only initiate the procedure when AS security has been activated and when one of the possible following condition is met:

- detecting radio link failure
- integrity check failure indication from lower layers
- RRC connection reconfiguration failure
- …complete list in TS 36.331 c.5.3.7.2

In the following some relevant RRC messages and actions for RRC connection re-establishment procedure are reported with a list of the main parameters carried. For further details, please refer to the 3GPP document TS 36.331 in the corresponding chapters as indicated.

5.3.7.3 Actions following cell selection while T311 is running

5.3.7.4 Actions related to transmission of RRCConnectionReestablishmentRequest message

Parameters:

- *reestablishmentCellId*
- *ue-Identity → c-RNTI, physCellId, shortMAC-I*
- *reestablishmentCause*

5.3.7.5 Reception of the RRCConnectionReestablishment by the UE

Parameters:

- *radioResourceConfigDedicated*
- *nextHopChainingCount*

5.3.7.6 T311 expiry

5.3.7.7 T301 expiry or selected cell no longer suitable

5.3.7.8 Reception of RRCConnectionReestablishmentReject by the UE

RRC Connection Release

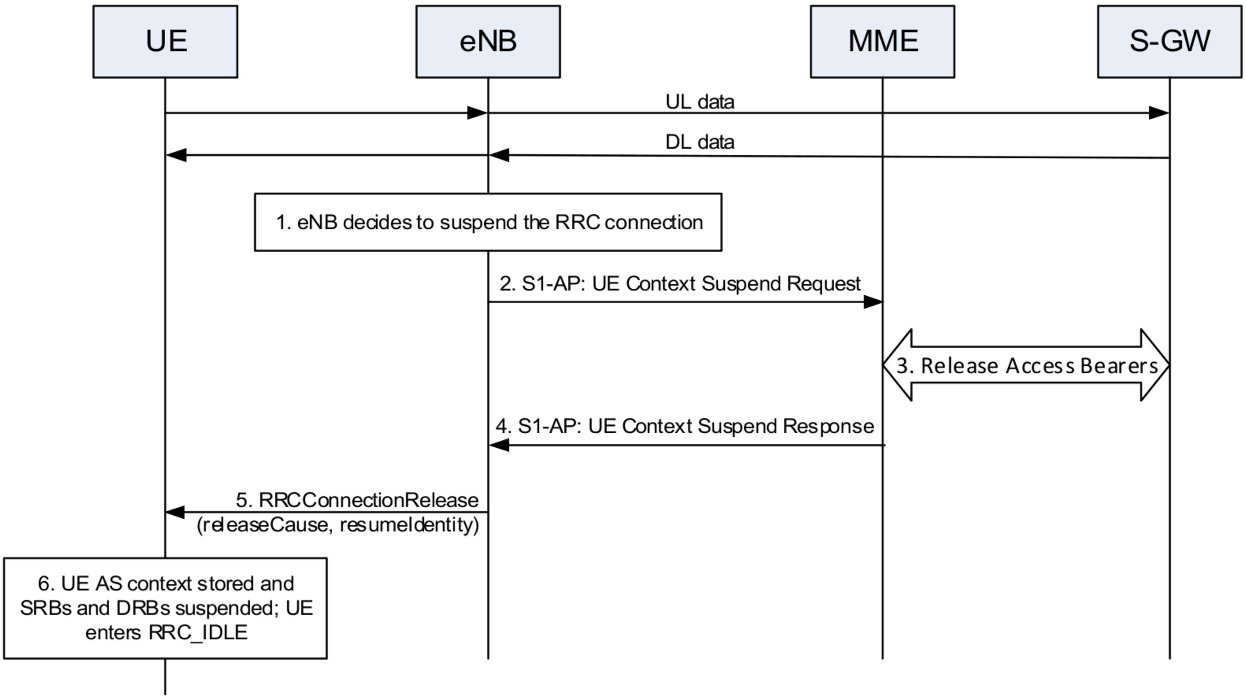

Figure 18 RRC Connection Release

The purpose of this procedure is to release the RRC connection (which includes the release of the established radio bearers as well as all radio resources) or to suspend the RRC connection (which includes the suspension of the established radio bearers). E-UTRAN initiates the RRC connection release procedure to a UE in RRC_CONNECTED and after this procedure has been finalized, the UE enters the RRC_IDLE state. 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.In the following some relevant RRC messages and actions for RRC Connection Release procedure are reported with a list of the main parameters carried. For further details, please refer to the 3GPP document TS 36.331 in the corresponding subsections as indicated.

5.3.8.3 Reception of the RRCConnectionRelease by the UE

Parameters:

- *idleModeMobilityControlInfo*
- *releaseCause*
- *extendedWaitTime*

RRC Connection Release requested by upper layers

The purpose of this procedure is to release the RRC connection. Access to the current PCell may be barred as a result of this procedure. Upper layers invoke the procedure, e.g. upon determining that the network has failed an authentication check (see TS 24.301). Furthermore, the UE shall not initiate the procedure for power saving purposes.

Radio Resource configuration

The UE receive a *radioResourceConfigDedicated* (i.e. carried by *RRCConnectionReconfiguration*) message that may include one of the following parameters. Depending on the parameter type, UE may perform different procedures as indicated in the following.

- *srb-ToAddModList (SRB addition)*
  - perform the SRB addition or reconfiguration as specified in 5.3.10.1
- *drb-ToReleaseList (DRB release)*
  - perform DRB release as specified in 5.3.10.2
- *drb-ToAddModList (DRB addition)*
  - perform DRB addition or reconfiguration as specified in 5.3.10.3
- *mac-MainConfig (MAC reconfiguration)*
  - perform MAC main reconfiguration as specified in 5.3.10.4
- *sps-Config* (not for NB-IoT)
  - perform SPS reconfiguration according to 5.3.10.5
- *physicalConfigDedicated (physical channel configuration)*
  - reconfigure the physical channel configuration as specified in 5.3.10.6.
- *rlf-TimersAndConstants (Radio link failure)*
  - reconfigure the values of timers and constants as specified in 5.3.10.7
- …

For further detail, please refer to the 3GPP document TS 36.331 in the corresponding subsections.

Radio link failure related actions

In the following some relevant actions in case of Radio Link Failure are reported. For further details, please refer to the 3GPP document TS 36.331 in the corresponding subsections as indicated.

5.3.11.1 Detection of physical layer problems in RRC_CONNECTED

Two possible situation can occur:

- UE receive N310 consecutive "out-of-sync" indications for the PCell from lower layers while neither T300, T301 nor T311 is running
  - UE must start timer T310
- UE receive N313 consecutive "out-of-sync" indications for the PSCell from lower layers (not in NB-IoT)

5.3.11.2 Recovery of physical layer problems

5.3.11.3 Detection of radio link failure

UE actions upon leaving RRC_CONNECTED

Please refer to 5.3.12 subsection of 3GPP Document TS 36.331

Data Transfer

For NB-IoT UE that support 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*. Contained in all these messages is a byte array containing 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. [2]

DL Information Transfer

The purpose of this procedure is to transfer NAS or (tunnelled) non-3GPP dedicated information from E-UTRAN to a UE in RRC_CONNECTED. E-UTRAN initiates the DL information transfer procedure whenever there is a need to transfer NAS or non-3GPP dedicated information by sending the *DLInformationTransfer* message (see Figure below).

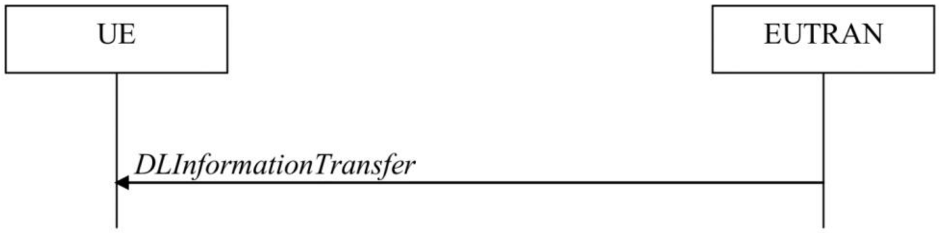

Figure 19 Downlink Information Transfer

In the following some relevant actions for DL Information Transfer procedure are reported with a list of the main parameters carried. For further details, please refer to the 3GPP document TS 36.331 in the corresponding subsections as indicated.

5.6.1.3 Reception of the DLInformationTransfer by the UE

- If the *dedicatedInfoType* is set to *dedicatedInfoNAS*
    - the UE has to forward the *dedicatedInfoNAS* to the NAS upper layers
- ….

UL Information Transfer

The purpose of this procedure is to transfer NAS or (tunnelled) non-3GPP dedicated information from the UE to EUTRAN. A UE in RRC_CONNECTED initiates the UL information transfer procedure whenever there is a need to transfer NAS or non-3GPP dedicated information, except at RRC connection establishment or resume in which case the NAS information is piggybacked to the *RRCConnectionSetupComplete* or *RRCConnectionResumeComplete* message correspondingly. The UE initiates the UL information transfer procedure by sending the *ULInformationTransfer* message.

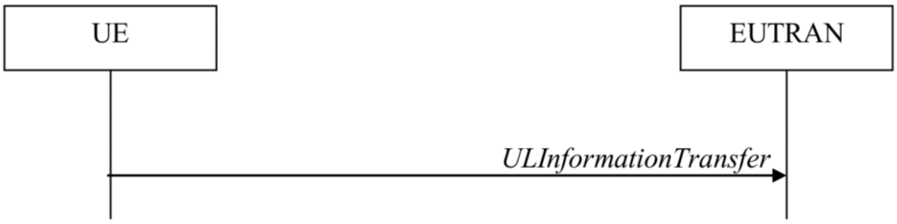

Figure 20 Uplink information transfer

In the following some relevant actions for UL Information Transfer procedure are reported with a list of the main parameters carried. For further details, please refer to the 3GPP document TS 36.331 in the corresponding subsections as indicated.

5.6.2.3 Actions related to transmission of ULInformationTransfer message

Parameters:

- *dedicatedInfoNAS*
- *dedicatedInfoType*

5.6.2.4 Failure to deliver ULInformationTransfer message

5.6.2.4 Failure to deliver ULInformationTransfer message

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 procedure is defined, which is shown in the following figure.

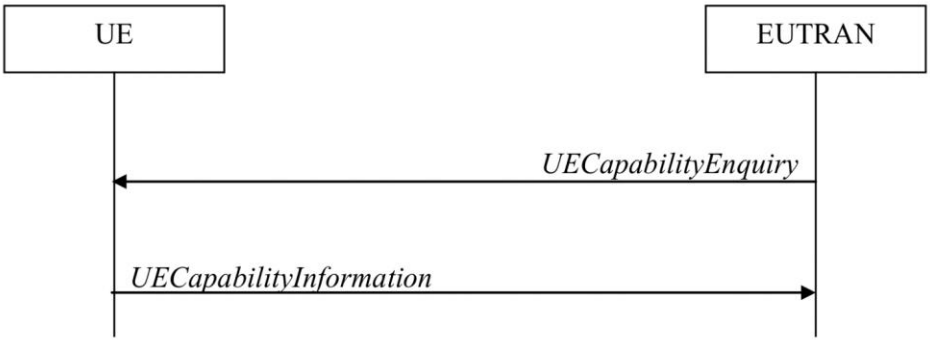

Figure 21 UE Capability Transfer

The purpose of this procedure is to transfer UE radio access capability information from the UE to E-UTRAN. If the UE has changed its E-UTRAN radio access capabilities, the UE shall request higher layers to initiate the necessary NAS procedures (see TS 23.401) that would result in the update of UE radio access capabilities using a new RRC connection. E-UTRAN always initiates this procedure to a UE in RRC_CONNECTED when (additional) radio access capability information is needed from UE by sending a *UECapabilityEnquiry* message. The *UECapabilityInformation* 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. [2]

In the following some relevant actions for UE Capability Transfer procedure are reported with a list of the main parameters carried. For further details, please refer to the 3GPP document TS 36.331 in the corresponding subsections as indicated.

5.6.3.3 Reception of the UECapabilityEnquiry by the UE

Transmission of UECapabilityInformation message

Parameters:

- *ue-Capability-Container*
- *ue-RadioPagingInfo*

Generic Error Handling

Please refer to 3GPP TS 36.331 V14.1.0 c.5.7

NB-IoT RRC messages

Please refer to 3GPP TS 36.331 V14.1.0 c.6.7

NB-IoT Timers

TIMER	START	STOP	AT EXPIRY
T300	Transmission of RRCConnectionRequest or RRCConnectionResume Request	Reception of RRCConnectionSetup, RRCConnectionReject or RRCConnectionResume message, cell re-selection and upon abortion of connection establishment by upper layers	Perform the actions as specified in 5.3.3.6
T301	Transmission of RRCConnectionReestabil shmentRequest	Reception of RRCConnectionReestablishment or RCConnectionReestablishmentReject message as well as when the selected cell becomes unsuitable	Go to RRC_IDLE
T310	Upon detecting physical layer problems for the PCell i.e. upon receiving N310 consecutive out-ofsync indications from lower layers	Upon receiving N311 consecutive in-sync indications from lower layers for the PCell, upon triggering the handover procedure and upon initiating the connection re-establishment procedure	If security is not activated: go to RRC_IDLE else: initiate the connection re-establishment procedure
T311	Upon initiating the RRC connection reestablishment procedure	Selection of a suitable E-UTRA cell or a cell using another RAT.	Enter RRC_IDLE

NB-IoT Constants

CONSTANT	USAGE
N310	Maximum number of consecutive "out-of-sync" indications for the PCell received from lower layers
N311	Maximum number of consecutive "in-sync" indications for the PCell received from lower layers
N313	Maximum number of consecutive "out-of-sync" indications for the PSCell received from lower layers
N314	Maximum number of consecutive "in-sync" indications for the PSCell received from lower layers

TS 36.331 V14.2.1 – NB-IoT enhancements [5]

In the following the main enhancements introduced for NB-IoT RRC layer in the late TS 36.331 V14.2.1 version are presented. For further details, please refers the 3GPP spec. and the corresponding CR (Change Requests) approved for the new V14.2.1 version of Rel.14.

Extension of timer T311 (CR 2703)

Timer T311 is not long enough for a UE in extended coverage to perform RRC connection re-etablishment due to the time required to acquire MIB-NB, SIB1-NB and SIB2-NB in the new cell. Extend the value range of T311 up to 2 minutes in IE RLF-TimersAndConstants-NB and IE UE-TimersAndConstants-NB

Clarification on prioritization of multiple Pmax values (CR 2624)

Adding procedure text for SIB3-NB and SIB5-NB regarding to how UE determines one p-max value from the list of p-max values in SIB3-NB and SIB5-NB, respectively. The procedure text is similar to the SIB1 procedure text.

See TS 36.331 V14.2.1- 5.2.2.10 and 5.2.2.12

Introduction of NB-IoT Enhancements other than Multicast (CR 2625)

1)Multicast: Place holders for SIB15 and SIB20

- Introduction of IE SystemInformationBlockType15-NB containing the MBMS Service Area Identities (SAI) of the current and/ or neighbouring carrier frequencies. SIB15 is broadcasted by the PCell.
- Introduction of IE SystemInformationBlockType20-NB contains the information required to acquire the control information associated with transmission of MBMS using SC-PTM.

2) Multi-PRB enhancements: Paging and PRACH

3) Mobility enhancements (dedicated frequency offset at redirection)

4) Positioning (no impact identified)

5) Higher data rate

6) Low power class UEs

7) Other

- Release assistance indication
- SA2: IRAT mobility
- SA2: UE-SCEF reliable communication
- SA2: Authorisation of coverage

CHANGES:

Abbreviations→RAI (Release Assistance Indication)

5.2.2.3 System Information required by NB-IoT UE:

A NB-IoT UE is always required to have a valid version of some System Information. In the following a list of the required SI by NB-IoT UE is presented in relation to the UE RRC state.

RRC_IDLE:

- MIB-NB
- SIB1-NB
- SIB2-NB through SIB5-NB

- SIB22-NB (depending on support of multi-carrier paging/NPRACH)

RRC_CONNECTED and T311 timer is running

- MIB-NB
- SIB1-NB
- SIB2-NB
- SIB22-NB (depending on support of multi-carrier paging/NPRACH)

NOTE:

The IE SystemInformationBlockType22-NB contains radio resource configuration for paging and random access procedure on non-anchor carriers.

5.2.2.4 System information acquisition by the UE

5.2.2.5 Essential system information missing

5.2.2.9 Actions upon reception of SystemInformationBlockType22-NB

Upon receiving SystemInformationBlockType22-NB, the UE shall apply the configuration included in:

- dl-CarrierConfigList
    - List of DL non anchor carriers that can be used for paging and/or random access
- ul-CarrierConfigList
    - List of UL non anchor carriers that can be used for random access
- pcch-MultiCarrierConfig
    - Provide the configuration for paging on non-anchor carriers.
- nprach-MultiCarrierConfig
    - Provide the configuration for random access non-anchor carriers

5.3.3.4 Reception of the RRCConnectionSetup by the UE

See the corresponding CR for further specifications

Extension of QRxLevMin value range (CR 2622)

In guard-band or in-band mode of operation with 164dB MCL, some UEs cannot find a cell to camp even though within NW coverage, due to the too high minimal value of Qrxlevmin (i.e. -140dBm). Extend the minimal value of Qrxlevmin from -140 dBm to -156 dBm in SIB1-NB (for cell selection) and SIB3-NB/SIB5-NB (for cell reselection).

CHANGES:

SystemInformationBlockType1/3/5-NB

See corresponding CR for further details

Indication of S1-U data transfer (CR 2528)

To align RRC with NAS specification where a UE that supports S1-U data transfer may not support User Plane CIOT EPS optimisation. Explain in the field description of up-CIoT-EPS-Optimisation for the RRCConnectionSetupComplete-NB message that indicates UE's support of the S1-U data transfer or, S1-U data transfer and User plane CIoT EPS Optimisation.

CHANGES:

RRCConnectionSetupComplete→ *up-CIoT-EPS-Optimisation* field

Introduction of SC-PTM for feMTC and NB-IoT enhancements (CR 2578)

CHANGES:

Feature not supported in NB-IoT and corresponding procedures and messages do not apply to the UE in NB-IoT:

- …
- MBMS→ except for MBMS via SC-PTM in Idle mode
- ..

5.2.2.4 System information acquisition by the UE → SystemInformationBlockType20-NB in NB-IoT

5.8a SC-PTM (Single Carrier Point-to-Multi-Point) (introduction of NB-IoT functionalities)

6.2.2 Message definitions

6.7.2 SCPTMConfiguration

See the corresponding CR for further details

References

[1] 3GPP, “TS 36.300 V14.1.0”.

[2] R. &. Schwarz, “Narrowband Internet of Things - Whitepaper,” 2016.

[3] 3GPP, “TS 36.304 V14.2.0”.

[4] 3GPP, “TS 36.331 V14.1.0”.

[5] 3GPP, “TS 36.331 V14.2.1”.