Todo list

Embedded Massive Internet of Things Simulator using Software Defined Radios

Master Thesis Project Report

Mads Gotthardsen
Thomas Jørgensen

Aalborg University
Wireless Communication Systems
Frederiks Bajersvej 7
DK-9220 Aalborg

This report is compiled in LaTeX, originally developed by Leslie Lamport, based on Donald Knuth's TeX. The main text is written in *Computer Modern* pt 11, designed by Donald Knuth. Flowcharts and diagrams are made using Microsoft Visio, Inkscape and Tikz, a TeXpackage for generating graphics.

Connectivity
Department of Electronic Systems
Fredrik Bajers Vej 7
DK-9220 Aalborg Ø

AALBORG UNIVERSITY

STUDENT REPORT

Title:
Embedded Massive User Equipment Simulator using Software Defined Radios

Theme:
MSc Project (Wireless Communication Systems)

Project Period:
9-10. Semester

Project Group:
17gr950

Participant(s):
Mads Røgeskov Gotthardsen
Thomas Kær Juel Jørgensen

Supervisor(s):
Petar Popovski
Dong Min Kim

Industrial-supervisor:
Germán Corrales Madueño

Copies: 2

Page Numbers: Fucking mange!

Date of Completion:
April 4, 2018

Abstract:

□

Contents

List of Terms

3GPP 3rd Generation Partnership Project.

AL Aggregation Level.

AM Acknowledged Mode.

ARQ Automatic Repeat Request.

AS Access stratum.

BCCH Broadcast Control Channel.

BCH Broadcast Channel.

BS Base Station.

BSE Base Station (BS) emulator.

C-RNTI Cell-specific Radio Network Temporary Identifier.

CCCH Common Control Channel.

cDRX Connected Discontinuous Transmission.

CE Coverage Enhancement.

CFO Carrier Frequency Offset.

CIoT Cellular Internet of Things.

CRC Cyclic Redundancy Check.

DCCH Dedicated Control Channel.

DHCP Dynamic Host Configuration Protocol.

DL Downlink.

DL-SCH Downlink Shared Channel.

DTCH Dedicated Traffic Channel.

eDRX Extended Discontinuous Transmission.

EMM EPS Mobility Management.

eNB eNodeB.

EPS Evolved Packet System.

ESM EPS Session Management.

GPRS General Packet Radio Service.

GSM Global System for Mobile Communications.

HARQ Hybrid Automatic Repeat Request.

HSS Home Subscriber Server.

IoT Internet of Things.

IP Internet Protocol.

LoRa Long Range.

LPWA Low Power Wide-Area.

LSB least significant bit.

LTE Long Term Evolution.

MAC Medium Access Control.

MBSFN Multicast-Broadcast Single-Frequency Network.

MCL Maximum Coupling Loss.

MCS Modulation and Coding Scheme.

MIB-NB Master Information Block Narrow-band.

MME Mobility Management Entity.

NAS Non-Access stratum.

NB-IoT Narrow Band Internet of Things.

NB-PCID Narrow-band Physical Cell-specific Identity.

NB-SIB Narrow-band System Information Block.

NIDD non-IP Data Delivery.

NPBCH Narrow-band Physical Broadcast Channel.

NPDCCH Narrow-band Physical Downlink Control Channel.

NPDSCH Narrow-band Physical Downlink Shared Channel.

NPSS Narrow-band Primary Synchronization Signal.

NRAP Narrow-band Random Access Procedure.

NRS Narrow-band Reference Signal.

NSSS Narrow-band Secondary Synchronization Signal.

OFDM Orthogonal Frequency Division Multiplexing.

PCCH Paging Control Channel.

PCH Paging Channel.

PCRF Policy and Charging Resource Function.

PDCCH Physical Downlink Control Channel.

PDCP Packet Data Convergence Protocol.

PDN Packet Data Network.

PDU Packet Data Unit.

PGW Packet Data Network Gateway.

PHY physical layer.

PLMN Public Land Mobile Network.

PRB Physical Resource Block.

PSM Power Saving Mode.

QoS Quality of Service.

RACH Random Access Channel.

RAN Radio Access Network.

RAP Random Access Procedure.

RAR Random Access Response.

RE Resource Element.

RLC Radio Link Control.

RRC Radio Resource Control.

RRM Radio Resource Management.

RS Reference Signal.

S-TMSI S-Temporary Mobile Subscriber Identity.

SCEF Service Capability Exposure Function.

SDU Service Data Unit.

SFN Subframe Number.

SGW Serving Gateway.

SIB System Information Block.

SISO Single Input Single Output.

SNR Signal to Noise Ratio.

SRB Signaling Radio Bearer.

TB Transport Block.

TBCC Tail-Biting Convolution Coding.

TM Transparent Mode.

UE User Equipment.

UL Uplink.

UL-SCH Uplink Shared Channel.

UM Unacknowledged Mode.

USIM Universal Subscriber Identity Module.

Preface

Aalborg University, April 4, 2018

Mads Røgeskov Gotthardsen
mgotth13@student.aau.dk

Thomas Kær Juel Jørgensen
tkjj13@student.aau.dk

1 | Introduction

problem statement: As the IoT market is still in its infancy a main communication protocol should be chosen based on several performance metrics, which allows companies to compete on equal terms.

1.1 Motivation

1.2 Problem Analysis

1.3 Solution Analysis

The market of cellular technologies is changing and the need for a new type of technology has arisen. This is the need for Low Power Wide-Area (LPWA) networks, LPWA networks are classified by three main aspects: long battery lifetime, low cost and huge amount of users. With the development of LPWA networks especially in regards to the evolution of 5G as well as Internet of Things (IoT) technologies an increasing amount of focus has come to the massive part of communication. It was estimated that in 2016 0.4 billion devices were of the LPWA type, but this is predicted to reach 1.5 billion by 2021, equivalent to a yearly growth rate of 27 % [**?**]. This change sets some requirements that is not achievable with existing systems, however to accommodate this several technologies have been developed.

Generally the new technologies are classified into categories: (i) cellular networks based solution (ii) proprietary solutions as can be seen in Figure 1.1. All these technologies are competing to be the main standard of massive IoT communication.

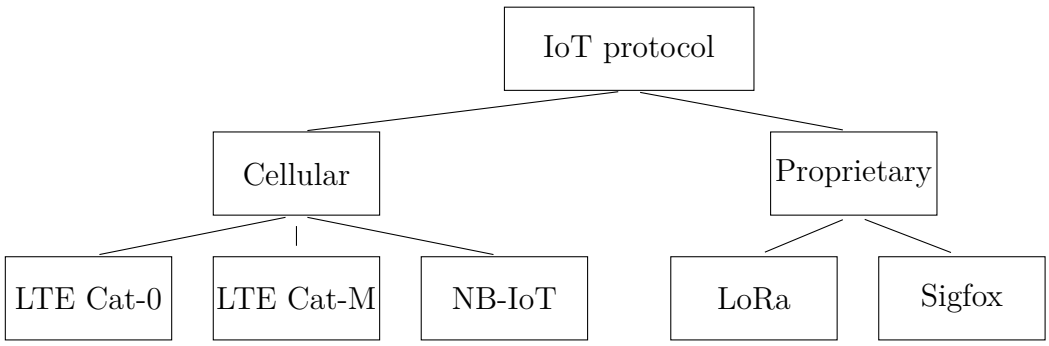

Figure 1.1: IoT protocol overview

Even though, the technologies in question have already been designed most is still in their infancy, because of this most metrics that can be found for the different protocols, are to our knowledge based on a theoretic approach and not on actual measurements.

Feature	**LoRa**	**Sigfox**	**LTE Cat-1**	**LTE-M**	**NB-IoT**
Modulation	SS Chirp	UNB/GSK/BPSK	OFDMA	OFDMA	OFDMA
Rx bandwidth	500-125 kHz	100 Hz	20 MHz	20-1.4 MHz	200 KHz
Data Rate	290 bps – 50 Kbps	100 bps / 8 bytes max	10 Mbps	200 kbps – 1 Mbps	20 Kbps
Max output power	20 dBm	20 dBm	23 – 46 dBm	23/30 dBm	20 dBm
Battery lifetime (2000 mAh)	105 months (∼9 years)	90 months (7.5 years)		18 months (1.5 years)	
Link budget	154 dB	151 dB	130 dB+	146 dB	150 dB
Security	Yes	No	Yes	Yes	

Table 1.1: Comparison of performance metrics between cellular solutions and proprietary solutions [**?**]

It can be seen from Table 1.1, that the different technologies have different advantages. The main differences between them are the bandwidth of the receiver as well as the battery lifetime.

As none of the protocols have been deployed at a large scale, it brings up different concerns especially because the massiveness in question is several magnitudes larger than anything seen before. Therefore to choose the main standard a lot of metrics are taken into consideration divided into three domains: reliability, energy consumption and massiveness i.e. the amount of supported users per km^2 or cell. One of the aims of IoT devices is a battery lifetime of around 10 years, to achieve this requirements for the energy consumption is of course a key metric. With the scope of billions of devices, several metrics in regards to the massiveness will also be extremely important. Because of the long lifetime coupled with the extreme number of devices the reliability also needs to be very high as it is not feasible to replace devices quickly.

This leads to the problem statement:

As the IoT market is still in its infancy a main communication protocol should be chosen based on metrics of the reliability, energy consumption and massiveness, which allows companies to compete on equal terms.

The focus of the project is to design an emulator combining both software and hardware, that can test how the standards perform in these domains. For this purpose emulation of multiple low performance IoT devices is needed. The system should also be able to simulate neighbouring cells to achieve realistic channel conditions. Implementation of a signal processing method that allow to change to different channel models would be optimal. The aim being a customizable emulator which provide performance metrics of the different protocol designs.

However as this is a huge endeavour, the focus will be on the core principles of this making a proof of concept emulator. When making an emulator it generally only works

for a single protocol so designing it for several protocols would be very time consuming and it is chosen that the benefit of supporting several protocols is not worth the extra time it takes to design the emulator. Another factor is the project will build upon existing software as just designing the BS emulator (BSE) or IoT device emulator could easily be an entire project in itself. Based on this different factors are taken in to account when choosing the protocol for the project which can be seen in Table 1.2.

	LTE Cat-0	**LTE Cat-M**	**NB-IoT**	**LoRa**	**Sigfox**
Licensed spectrum	Yes	Yes	Yes	No	No
BS emulator	Amarisoft	Amarisoft	Amarisoft * SRS	The Things Industries * LoRa Server	
User Equipment (UE) emulator		Amarisoft Asiatelco AT&T Digi Fibocom Gemalto H3C Huawei LinkLabs Longsung Meig Mobiletek Multitech Neoway NimbeLink pycom Quectel Sierra Wireless SimCom Skyworks Telit u-blox ZTEWelink	Amarisoft Cheerzing CMCC Digi H3C Lierda Longsung Meig Mobiletek Mokuai Neoway pycom Quectel Sierra Wireless SimCom Skyworks Telit u-blox ZTEWelink * SRS	The Things Industries Miromico Telit	Murata Telit * Telefonicaid
Modem complexity	High	Middle	Middle	Middle	Low

* Open source solutions

Table 1.2: Commercial solutions available for the different protocols. [**?????????**]

When looking at Table 1.2 it can be seen that for Long Term Evolution (LTE) Cat-0 no UE emulator was found for this protocol. This has to do with the development of LTE Cat-M and Narrow Band Internet of Things (NB-IoT) which shares most of the same properties but are more specialised to the IoT market. It can also be seen that for both LTE Cat-M and NB-IoT multiple UE emulators exist, this has to do with both protocols being cellular protocols developed by 3rd Generation Partnership Project (3GPP) this is very desired by the industry for various reasons. For Long Range (LoRa) there exists both

BS and UE emulators, it is also one of the most used proprietary protocols on the market. For the Sigfox protocol no BS emulators has been found. Based on these investigations it is chosen to use the NB-IoT, both because it has a lot of emulators already but mainly because it has an open source UE emulator. This is desired as to allow for modifications of the UE software.

To make the most realistic emulation the final solution needs to work in real time, this sets some limitations performance wise. One of the problems associated with real time computation is the computational capacity meaning the emulator will not be able to handle several thousands UEs simultaneously as the deployed system is required to. This is further explored in .

make ref to appropriate chapter

As all of these protocols are new the main focus will be on setting up a proof of concept model, this means that only a single cell will be emulated furthermore the emulator will only use a single channel model.

2 | NB-IoT Protocol

The structure of NB-IoT is still in the process of being defined, however some structure has been integrated in the LTE Rel-13 [**?**]. The primary difference between LTE and NB-IoT is the requirements set by the UE. For LTE it is the download capacity that is needed i.e. video streaming, internet surfing etc. however for the NB-IoT it is the uplink capacity that is needed, users are primarily smart meters and other measurement equipment [**?**]. These sort of devices has a low throughput and are fairly insensitive towards delay, however in terms of battery life time and coverage area the requirements are more severe as the equipment might be placed in hard to get to places e.g. cellars, sewers etc. A overview of the requirements set for NB-IoT is [**?**]:

- Ultra-low complexity UEs
  - The UE has a sample rate of 240 KHz
  - Only supports Tail-Biting Convolution Coding (TBCC)
  - Half-duplex
  - Uses Single Input Single Output (SISO) connection
- Improved coverage with a Maximum Coupling Loss (MCL) up to 164 dB
  - MCL surpassing General Packet Radio Service (GPRS) system with 20 dB
  - Improve coverage by introducing Coverage Enhancement (CE) levels
- Support massive number of UEs as high as 52547 devices per cell-site sector
- Improved power efficiency with a battery life time of 10 years with a battery capacity of 5 Wh
  - Using CE to minimize Power amplifier backoff increasing efficiency.
  - Using Connected Discontinuous Transmission (cDRX), Extended Discontinuous Transmission (eDRX) and Power Saving Mode (PSM)
- Deployment flexibility
  - The system should be able to be deployed both inside existing systems.
  - The system should be able to be deployed as a stand alone solution.

From this it can also be seen that there are no requirements to the latency of the communication between UE and the network. To describe how to fulfill the set requirements a top down method will be used. Starting with the network structure of NB-IoT.

2.1 Network Structure

The network structure NB-IoT is very similar to that of legacy LTE as can be seen in Figure 2.1. The system is divided into a control plane Cellular Internet of Things (CIoT) Evolved Packet System (EPS) optimization and a user plane CIoT EPS optimization.

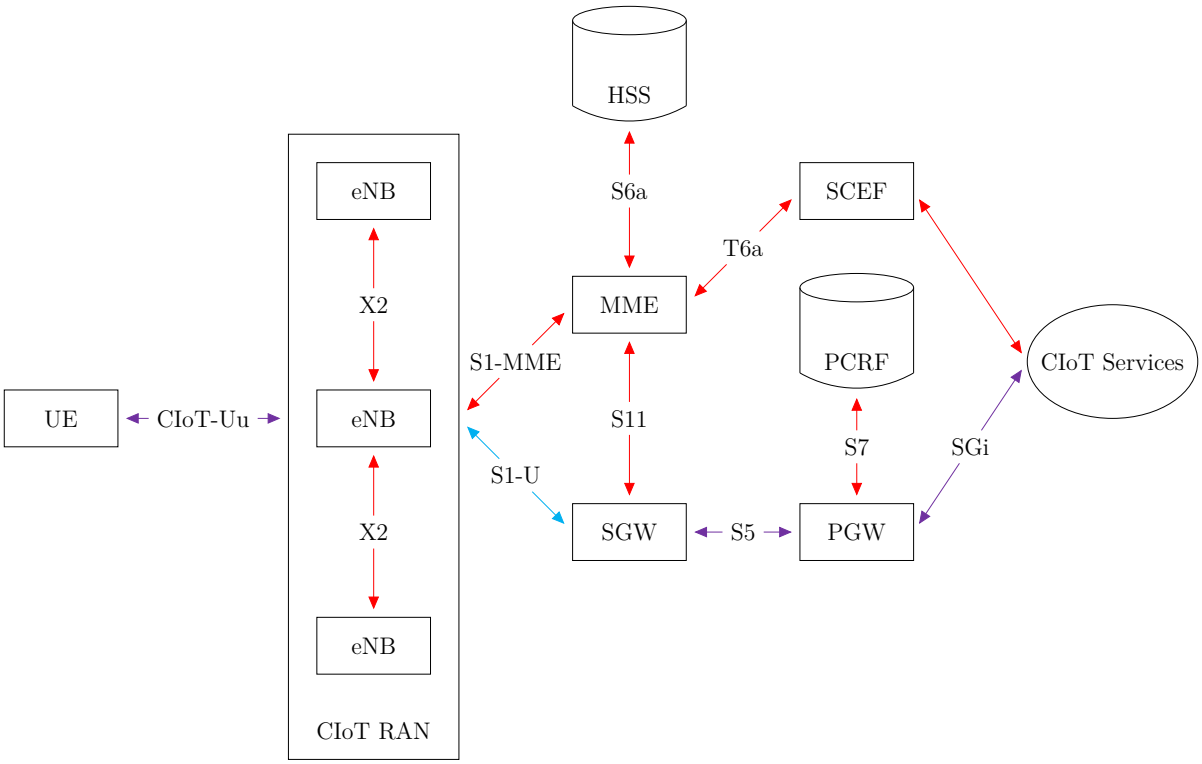

Figure 2.1: Overview over the network blocks and interfaces between blocks in NB-IoT. Blue lines are user plane CIoT EPS optimization, the red lines are control plane CIoT EPS optimization plane and the purple lines are both [**?**]

UE

The UE is the smart meters or other products as mentioned, they do not need to transmit a lot of data and it is not critical that it arrives within a certain time frame. They do however require a long battery life time. The problem comes in terms of placement, because many of these devices might be placed in basement like environment which means an increased path loss. The system needs to be able to operate with a MCL of 164 dB [**?**]. As in previous systems the Universal Subscriber Identity Module (USIM) is located on the UE for authentication purpose [**?**, ch. 3].

CIoT Radio Access Network (RAN)

The CIoT RAN is the base stations, the most typically used is the eNodeB (eNB) base station. All radio communication terminates at this node. Any UE that wish to use an external service, interfaces with the eNB [**?**]. The eNB interfaces with both the Mobility Management Entity (MME) and the Serving Gateway (SGW). On the control plane

(connection to the MME) the eNB is in charge of Radio Resource Management (RRM), i.e. allocating radio resources in the user plane to the individual UE based on Quality of Service (QoS) measures.

MME
The MME takes care of mobility issues, it also keep track of where in the network different UEs are connected [**?**]. Another very important function of the MME is to handle authentication of UEs and setting up security for the data bearers. The MME might be connected to multiple UEs, however a UE may only be connected to a single MME [**?**, ch. 3]. In NB-IoT handovers are omitted and the only way to change cell is by releasing the existing connection [**?**]. The MME also handles paging procedures [**?**].

Home Subscriber Server (HSS)
The HSS stores the identity of the users, which the MME uses for authentication purposes. It records the location of the UE in level of visited network control nodes such as MME, it also keep track of which networks the user is allowed to roam to [**?**, ch. 3].

Service Capability Exposure Function (SCEF)
The SCEF is a multi functional unit, task it handles include: device trigger delivery, sponsored data, UE reachability, 3GPP network issues, QoS for a UE session etc. Many of these functionalities are meant for normal LTE use. Uses meant for NB-IoT include UE reachability which enables the application layer to be informed when a UE reconnects to the network i.e. after an eDRX or after PSM. Another functionality it handles is non-IP Data Delivery (NIDD), which enables UEs with small data volumes to send it data with less overhead and thereby have a longer battery life time [**?**].

SGW
The SGW is primarily a routing unit. It interfaces with the eNB, the MME and the Packet Data Network Gateway (PGW). When the UE transmit data it is send to the eNB and then routed via the SGW to the PGW before reaching the providers. The SGW typically serve a particular geographic area with several eNBs, likewise could the MME also serve a particular geographic area. In LTE this was the last node in the network that could change during a connected state meaning that all SGWs needs to be connected to all PGWs [**?**, ch. 3]. This is however not equally important in NB-IoT as no handovers are expected [**?**]. During connected state the SGW works as a relay, however in idle mode the resources are released in the eNB and the data path terminates at the SGW it then stores the data from the PGW and request the MME to initiate paging of the UE [**?**, ch. 3].

PGW
The PGW is the edge of the EPS. It function as the point of attachment for the UEs Internet Protocol (IP) traffic. The IP-address of the UE is allocated during the connection procedure when the UE request a Packet Data Network (PDN) connection and during any subsequent PDN connection request. It is the PGW that performs the Dynamic Host

Configuration Protocol (DHCP) functionality [**?**, ch. 3]. The PGW handle interfaces to external CIoT services on a higher level.

Policy and Charging Resource Function (PCRF)
The PCRF is a server that makes decision on how to handle services provided for the UE in terms of QoS. It informs the PGW and if applicable the SGW about appropriate bearer policy can be set up. A default bearer is set up during connection request and either the UE or the service domain can request additional bearers which is handled by the PCRF [**?**, ch. 3].

CIoT services
The CIoT services are typically storage functionalities, but could be control algorithms or other services needed for specific products.

2.2 Protocol Layers

The following is focused on the communication protocol in the CIoT-Uu interface, it consist of six layers respectively:

- Non-Access stratum (NAS) layer
- Radio Resource Control (RRC) layer
- Packet Data Convergence Protocol (PDCP) layer
- Radio Link Control (RLC) layer
- Medium Access Control (MAC) layer
- physical layer (PHY) layer

The purpose and functionalities of these layers are explained in the following.

2.2.1 NAS

The NAS layer is the top layer in the control plane. It signals directly between the UE and the MME [**?**, ch. 3]. There are two protocols in the NAS layer, the EPS Mobility Management (EMM) and the EPS Session Management (ESM). The EMM handles re-activation from idle mode. The UE initiated case is called service request, the network initiated case is called paging. The EMM protocol is used for handling attachment and detachment from the system when the UE is in idle mode, in connected mode lower layer protocols handles this instead [**?**, ch. 3]. It has been suggested that a new protocol should be implemented allowing the UE to transmit a small amount of data directly in the NAS layer, the details of this protocol has not yet been established [**?**].

2.2.2 RRC

The RRC layer of the protocol is strictly control plane layer. It handles a great deal of control functions in the system including transition between UE states and bearer request. The functionalities provided by the RRC is [**?**, ch. 6.6]:

- Broadcast of system information
- Paging
- Establishment, maintenance and release of an RRC connection between UE and the eNB
- Security functions including key management
- Establishment, maintenance and release of point to point radio bearers
- UE measurement reporting and control of the reporting
- UE cell selection and reselections and control of cell selection and reselection
- Context transfer between eNBs
- UE capability transfer
- Generic protocol error handling
- Support of self-configuration and self-optimization

One of the biggest changes from LTE to NB-IoT is the focus on reducing power consumption therefore a new state has been introduced compared to the LTE system this can be seen in Figure 2.2.

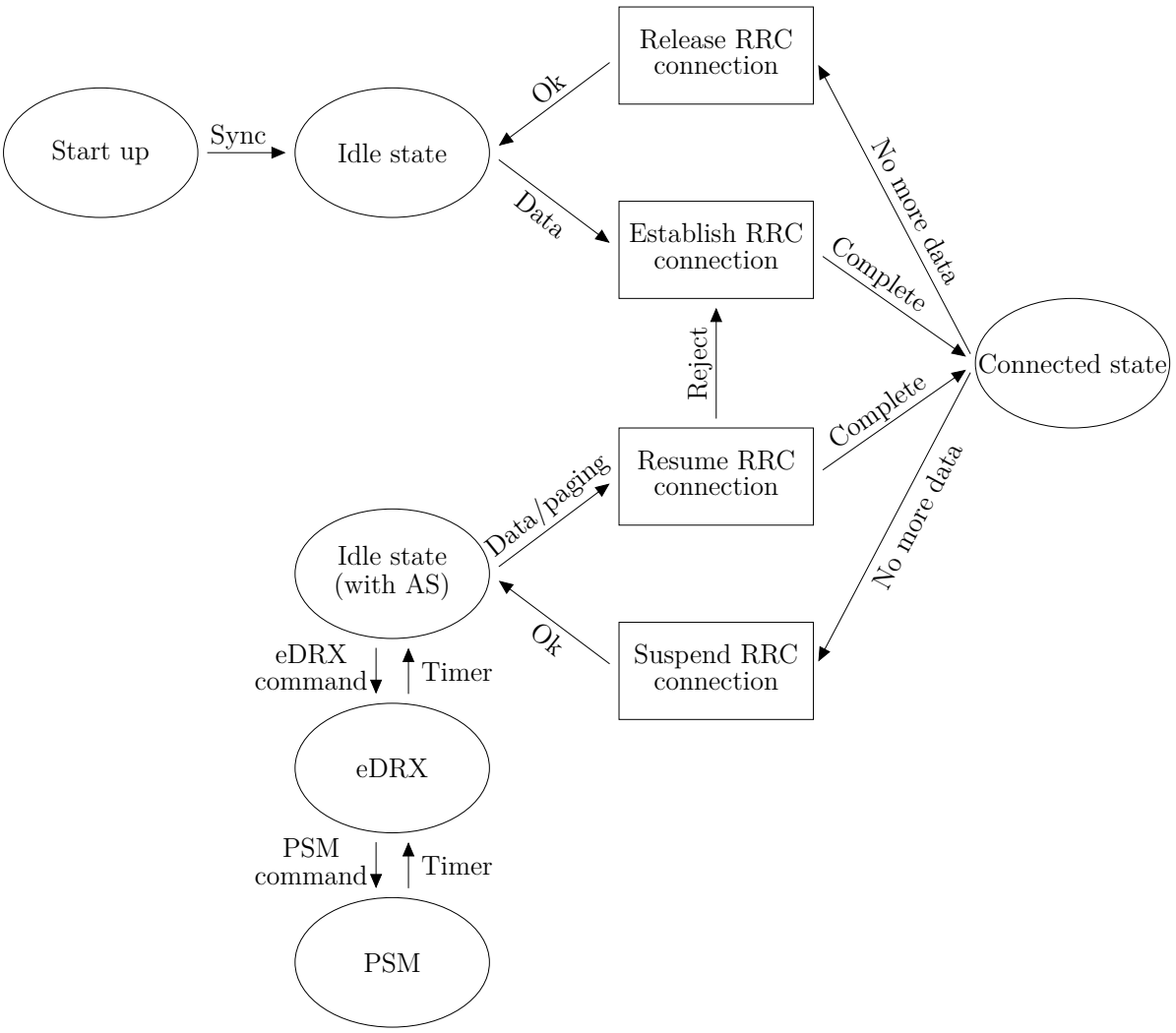

Figure 2.2: State diagram with transition options for a UE.

With this new structure comes a greater focus on RRC resume connection, which is very advantageous with regards to power consumption as it allows the UE to suspend its connection and save its Access stratum (AS) go into eDRX, when it then wakes up again it can make a resume request where it uses its previous AS to transmit its data reducing the overhead considerably. This can also be seen from Table 2.1 where a comparison between the different procedures is shown.

Direction	Legacy Service Request Procedure	RRC Connection Resume	Control Plane Data Transfer
UL	Preamble		
DL	Random Access Response (RAR)		
UL	RRC Connection Request	RRC Connection Resume Request	RRC Connection Request
DL	RRC Connection Setup	RRC Connection Resume	RRC Connection Setup
UL	RRC Connection Request Complete	RRC Connection Resume Complete	RRC Connection Complete
DL	Security Mode Command	-	-
UL	Security Mode Complete	-	-
DL	RRC Connection Reconfiguration	-	-
UL	RRC Connection Reconfiguration Complete	-	-
Total number of messages	**9**	**5**	**5**

Table 2.1: Signaling comparison between different methods [**?**]

Signaling Radio Bearer (SRB)
The RRC sets up three different SRBs. The SRBs is used to carry RRC and NAS messages. SRB0 is used for Common Control Channel (CCCH) during RRC connection setup or during link failure, messages carried here include RRC connection request, RRC connection setup, RRC connection reject, RRC connection reestablishment request, RRC connection reestablishment and RRC connection reestablishment reject. SRB1 is used when a RRC connection is established, it is used to transfer both RRC messages using Dedicated Control Channel (DCCH) and NAS messages until security is established. Once security is established the NAS messages is carried on SRB2 which has a lower priority. [**?**, ch. 6.6]

System Information Block (SIB)s
Before the UE attempts to access the system it needs a lot of information about the system, that is carried in the SIBs. For NB-IoT there are eight different SIBs messages. A list of the information carried in the different SIBs can be seen in Table 2.2. The RRC

takes care of updating these messages and paging UEs if changes occur.

Name	Information	Update rate
Master Information Block Narrow-band (MIB-NB)	Essential information required to receive further system information	640 ms
Narrow-band System Information Block (NB-SIB)1	Cell access and selection, other SIB scheduling	40.96 s
NB-SIB2	Radio resource configuration information	NA
NB-SIB3	Cell re-selection information for intra-frequency, inter-frequency	NA
NB-SIB4	Neighboring cell related information relevant for intra-frequency cell re-selection	NA
NB-SIB5	Neighboring cell related information relevant for inter-frequency cell re-selection	NA
NB-SIB14	Access Barring parameters	Fast
NB-SIB16	Information related to GPS time and Coordinated Universal Time (UTC)	Fast

Table 2.2: List of different SIB messages and the information carried within [**??**].

Paging
Paging serves two main functions, the first is to notify a UE in RRC idle state to set up a RRC connection to handle incoming data, the second is to inform UEs both in RRC idle and RRC connected state the system information has changed. [**?**, ch. 7]

Establishment, Maintenance and Release of RRC Connection
When an RRC connection setup is requested, the eNB has the option to reject it with a wait timer if the network is overloaded and can set the access barrer parameters appropriately in the NB-SIB14. In the RRC connection request message the UE can trasmit its S-Temporary Mobile Subscriber Identity (S-TMSI) if it possess a valid version else it will transmit a 40 bits random value. Five different establishment causes has been defined: emergency, high-priority access, mobility-terminated access, mobile-originated signaling and mobile-originated data. In NB-SIB1 there exists at most six different Public Land Mobile Network (PLMN) identities, the UE selects one and reports it in the RRC con-

nection setup complete message along with any MME the UE might already be registered to. The eNB then finds the MME and starts the S1 connection setup. When a connection setup is successful the UE moves to the RRC connected state. [**?**, ch. 6.6]

2.2.3 PDCP

The PDCP layer is just below the RRC it handles both control functions as well as user data. The key function of the PDCP include [**?**, ch. 6.5]:

- Header compression and decompression of IP packets. This is an important function especially for small data packets as the overhead could become quite significant.
- Ciphering and deciphering of both user plane and most of control plane data.
- Integrity protection and verification to ensure control data comes from the correct source.

The PDCP gets PDCP Service Data Unit (SDU)s from the RRC and NAS layer.

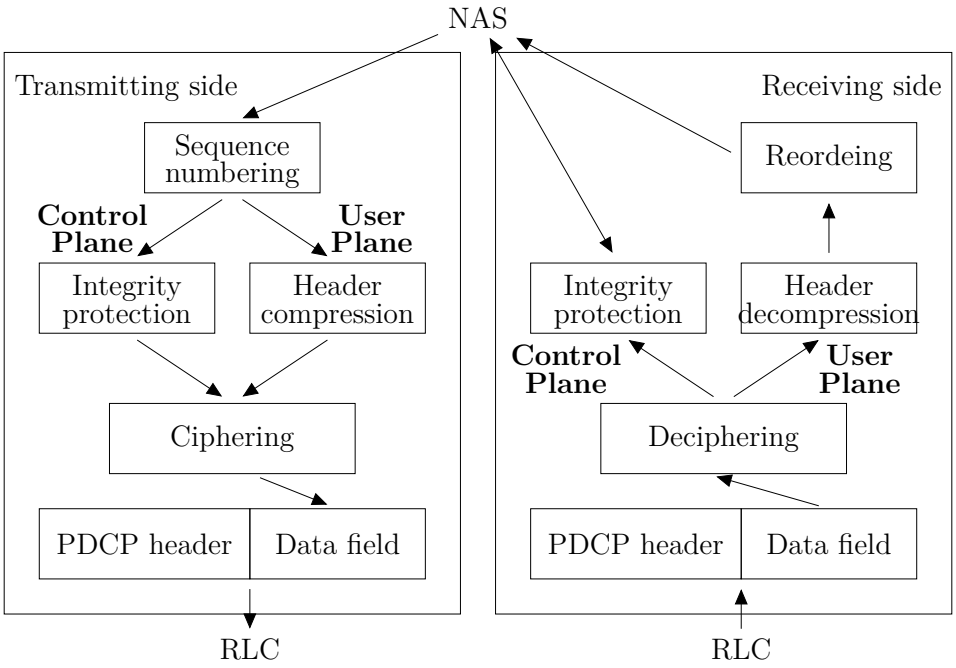

Figure 2.3: PDCP layer operation with associated PDCP SDU [**?**, fig. 6.12]

As can be seen in Figure 2.3 before forwarding the data to the RLC layer, it is first numbered and then either integrity protection or header compression is applied, depending on whether or not it is control plane data or user plane data. It is then ciphered and forwarded. When the PDCP receive data from the RLC layer, it is first deciphered and again depending on whether it is control pane data or user plane data it is integrity

protected or header decompression and reordered and then forwarded to the NAS. [**?**, ch. 6.5]

2.2.4 RLC

The RLC layer has three basic functionalities [**?**, ch. 6.4]

- To transfer Packet Data Unit (PDU)s from higher layers i.e. RRC, NAS or PDCP
- Depending on the RLC mode used, error correction with Automatic Repeat Request (ARQ), concatenation/segmentation, in-sequence delivery and duplicate detection may occur
- Protocol error handling to detect and recover from protocol error states caused by for example signaling errors

The modes mentioned before include Transparent Mode (TM), Unacknowledged Mode (UM) and Acknowledged Mode (AM) [**?**, ch. 6.4].

TM operation
In TM the RLC receives and deliver the PDUs without adding any header to it. Therefore it does not track received PDUs between receiving and transmitting entities. This mode is only suitable for communication that does not require physical layer retransmission or the data is not sensitive to delivery order and is therefore not very suitable to NB-IoT.

UM operation
The UM adds some control functions to the data stream. It enables segmentation of the data and keeps track of sequence numbering. This mode also makes in-sequence delivery of out-of-sequence data, which can occur because of lower layer Hybrid Automatic Repeat Request (HARQ) operation. The data is segmented and a header is added which includes a sequence number to facilitate reordering and duplicate detection on the receiving side.

AM operation
The AM adds all the functionalities of the UM but also provide retransmission, the header will in this case contain the last correctly received packet on the receiving side additionally to the sequence number.

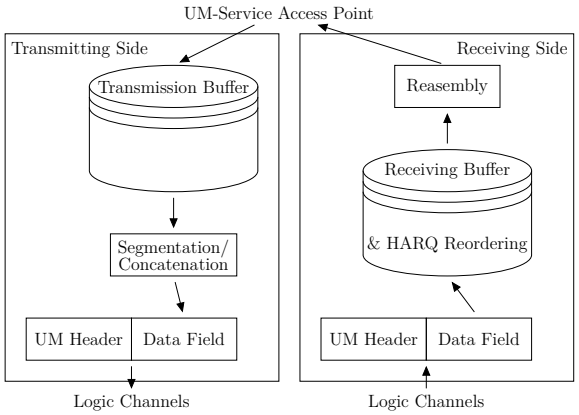

Figure 2.4: RLC UM operation [**?**, ch. 6.4]

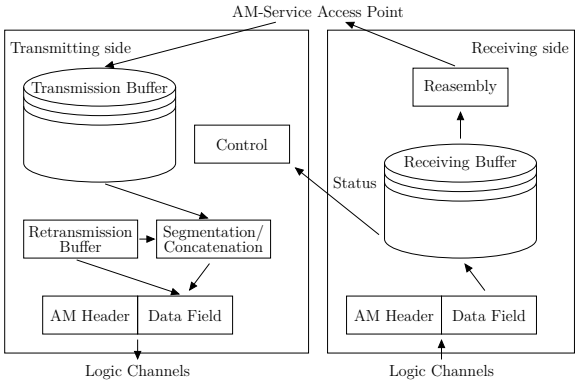

Figure 2.5: RLC AM operation [**?**, ch. 6.4]

In LTE several logic channels are defined in the RLC layer three for uplink and five for downlink [**?**, ch. 6.3].

Common logical channels:

- The CCCH is used to transport control information before a RRC connection exist.
- The DCCH is used to transport control information after a RRC connection is established.
- The Dedicated Traffic Channel (DTCH) is used to carry user data.

Downlink specific logical channels:

- The Broadcast Control Channel (BCCH) is used to carry the system information and other system access related information.
- The Paging Control Channel (PCCH) is used to carry paging information to reach UEs that are not in connected mode.

2.2.5 MAC

The MAC layer takes care of several things first of it maps the logical channels to the transport channels. Five transport channels are defined: the Random Access Channel (RACH), the Uplink Shared Channel (UL-SCH), the Downlink Shared Channel (DL-SCH) the Broadcast Channel (BCH) and the Paging Channel (PCH). All logical channels are mapped to these depending on the direction of the information as can be seen in Figure 2.6 and Figure 2.7. The RACH handles the random access procedure this is solely a MAC layer functionality there are therefore no logic channel mapped to it. The MAC

layer further handles multiplexing/demultiplexing of RLC PDUs into Transport Block (TB) for the physical layer including padding if a PDU is not completely filled with data. It also handles traffic volume measurement and reporting and provides this information for the RRC layer. Another function the MAC layer handles is the error correction through HARQ along with scheduling of the physical layer. The final thing the MAC layer handles is the transport format selection, this includes Aggregation Level (AL), Modulation and Coding Scheme (MCS) and power ramping.

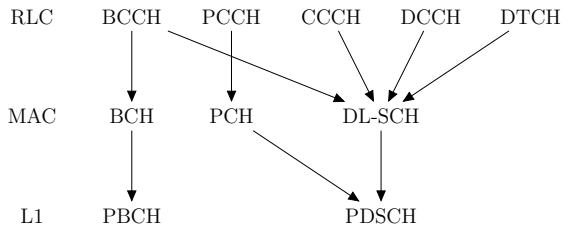

Figure 2.6: MAC layer Downlink (DL) mapping structure

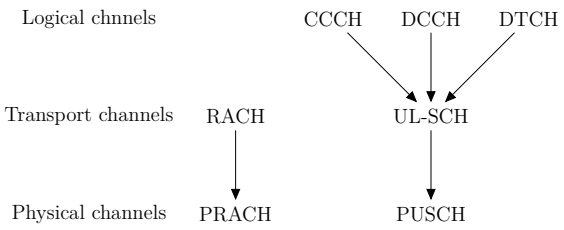

Figure 2.7: MAC layer Uplink (UL) mapping structure

A MAC PDU consist of the MAC header along with the MAC control elements and the MAC SDUs and potentially some padding as can be seen in Figure 2.8

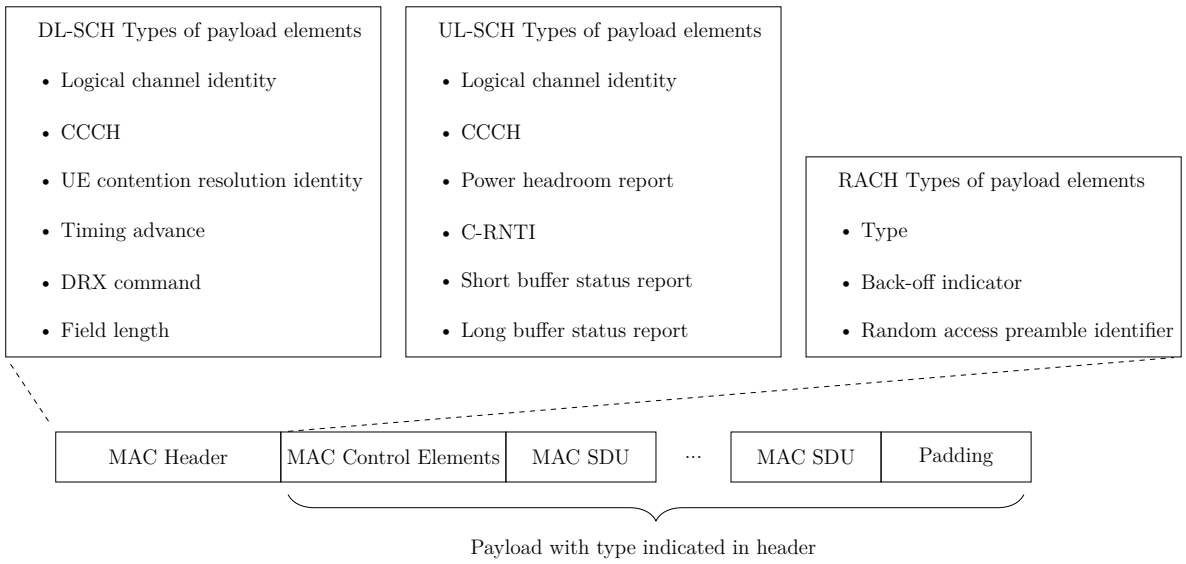

Figure 2.8: MAC PDU structure

The header is different depending upon which transport channel is used as can be seen in Figure 2.8. It include key parameter for control of both the physical layer as well as the logical channel identity. It is also the MAC layer that handles contention resolution with HARQ, for this purpose the header includes CCCH and Cell-specific Radio Network Temporary Identifier (C-RNTI) for the UE. When a UE tries to connect to the network the MAC layer also calculates timing advance.

2.2.6 PHY

To accommodate the new requirements set by the IoT development as described in the beginning of chapter 2, the physical layer design also needs to be revised. The idea is to allow for three different deployments methods: in-band, guard-band and standalone [**?**]. This is to take advantage of the existing LTE and Global System for Mobile Communications (GSM) networks. The idea behind the three deployments can be seen in Figure 2.9, the in-band mode takes up one of the Physical Resource Block (PRB) from the LTE cell, where the guard-band mode places it just outside the LTE carriers. This is possible because none of the LTE cells utilize the entire allocated spectrum to reduce the spectral disturbance. The proposed design also allows for the standalone case to utilize a GSM band taking advantage of the lower frequency compared to legacy LTE to increase the coverage area. To work inside and alongside these system provides some restrictions that needs to be respected. Therefore is the physical structure of the system the same for all deployment methods, however the use and spectrum allocation differs slightly. The most commonly discussed deployment scenario is the in-band operation as this set the most restriction for the NB-IoT system. [**??**].

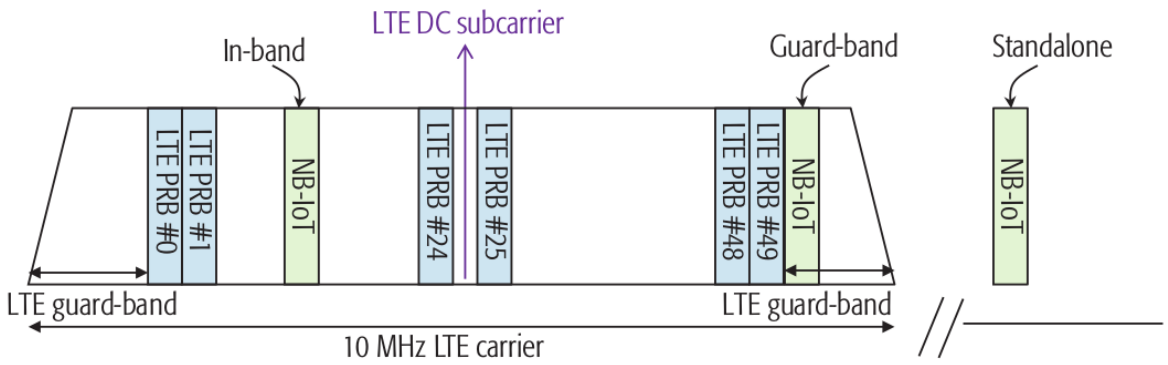

Figure 2.9: Deployment of the NB-IoT as in-band, guard-band or standalone [**?**].

To allow in-band operation the physical layer of NB-IoT needs to follow the overall structure of LTE, to describe this it is split into the DL and UL part. First the DL part will be investigated as this accounts for most of the critical factors of the communication i.e. synchronization and system information.

Downlink

As the primary users of legacy LTE does not know of the NB-IoT system the primary concern is the interference it causes. Some structural guidelines is therefore needed when designing the NB-IoT system, first it needs to blend in with the Orthogonal Frequency Division Multiplexing (OFDM) symbols of the LTE system meaning that timing alignment and subcarrier spacing is already determined [**?**, ch. 7.2].

Channel Raster

As NB-IoT functions as an individual system it needs it own overhead. To ensure the functionality of both systems the PRBs used for NB-IoT is therefore placed outside the six center PRB's, as these are used for LTE synchronization. This implies that only the LTE cells with a bandwidth larger than 1.4 MHz can host NB-IoT [**?**]. Furthermore to keep the receiver complexity and the battery consumption at a minimum the UE searches for the NB-IoT cell on a raster of 100 kHz [**?**, ch. 7.2]. The center of the bandwidth host a DC-subcarrier, and the PRB's is placed around this. This means that the center of a PRB will be offset from the raster for instance PRB #25 in Figure 2.9 has a center of 97.5 kHz which is 2.5 kHz off from the raster. Because of this an additional requirement is made that only those PRB's where the offset is less than 7.5 kHz can be used to host a NB-IoT cell [**?**]. The PRB's that fulfil this criteria can be seen in Table 2.3.

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

Table 2.3: available-PRBs [**?**]

Frame Structure

To fit into a LTE PRB the frame structure needs to be very similar to legacy LTE, the structure is divided into: hyperframe, frame, subframe and slots. Where two slots make a subframe, ten subframes make a frame and 1024 frames make a hyperframe. A complete cycle takes 1024 hyperframes which corresponds to 2 hours 54 minutes and 46 seconds. Figure 2.10 [**?**, ch. 7.2].

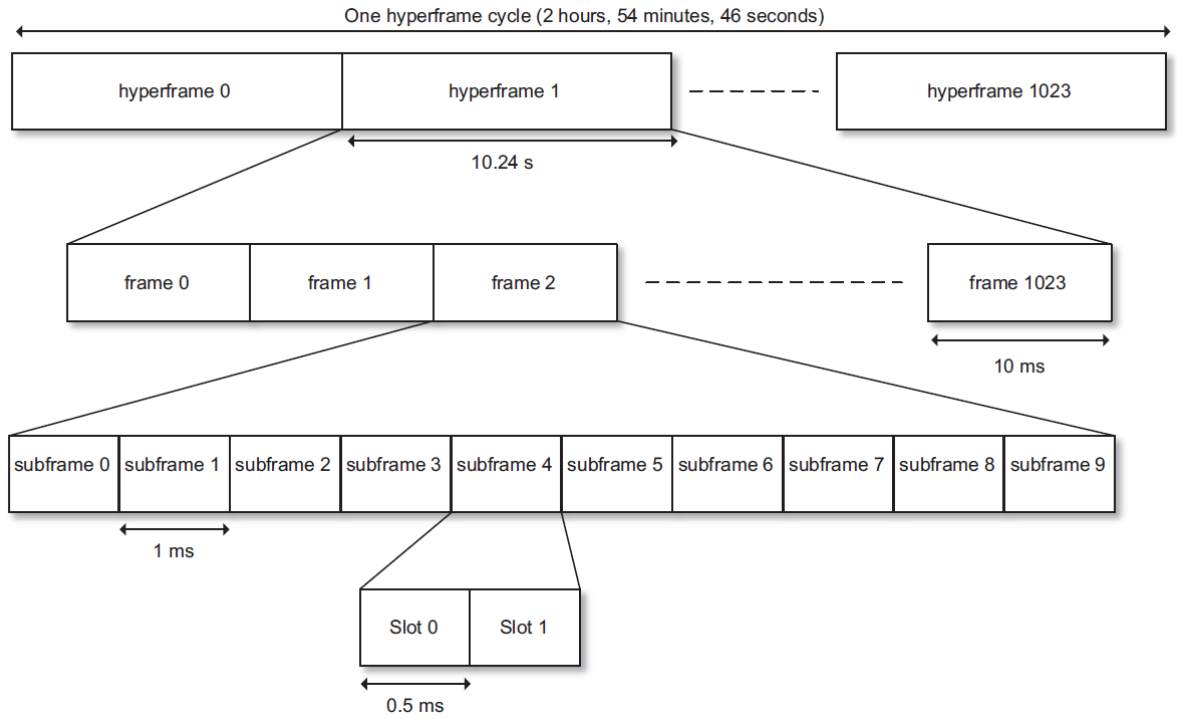

Figure 2.10: NB-IoT downlink structure [?, Fig. 7.7]

As the NB-IoT system is placed outside the PRBs used for LTE synchronization most of the subframes are available to use, the only exception is if a Multicast-Broadcast Single-Frequency Network (MBSFN) is present, this can occupy either of subframes (1,2,3,6,7,8) [?]. Therefore the Narrow-band Primary Synchronization Signal (NPSS) and Narrow-band Secondary Synchronization Signal (NSSS) is placed in subframe 5 and 9 respectively as seen in Figure 2.11. By having the NSSS being present only in even frame numbers, the least significant bit (LSB) of the frame numbers can be deduced directly, this increases the efficiency of the system by freeing subframe 9 in odd frames and omitting that bit from the NB-IoT overhead. The Narrow-band Physical Broadcast Channel (NPBCH) is located in the subframe 0 and contains the MIB-NB which was explained in subsection 2.2.2 [?].

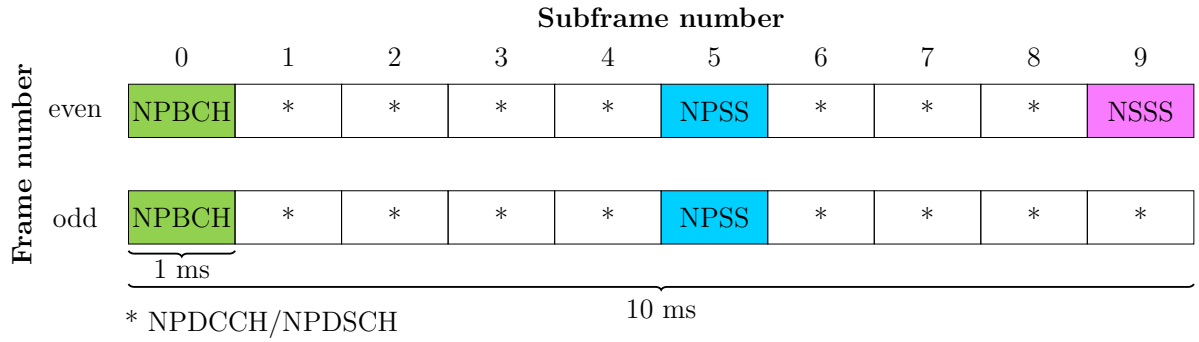

Figure 2.11: NB-IoT frame structure [?]

By zooming in on a subframe, it is possible to see how the different OFDM symbols is utilized. During a subframe 14 OFDM symbols are transmitted each having 12 subcarriers. As can be seen from Figure 2.12 almost half of the Resource Element (RE) in a subframe might be reserved for different signals and LTE control information [**?**]. An LTE cell can allocate up to three symbols for Physical Downlink Control Channel (PDCCH), an might use up to four carriers needing four Reference Signal (RS)s [**?**]. The NB-IoT structure allows for up to two carriers and needs therefore two RS namely Narrow-band Reference Signal (NRS)1 and NRS2 [**?**]. The placement of all these signals can be seen in Figure 2.12.

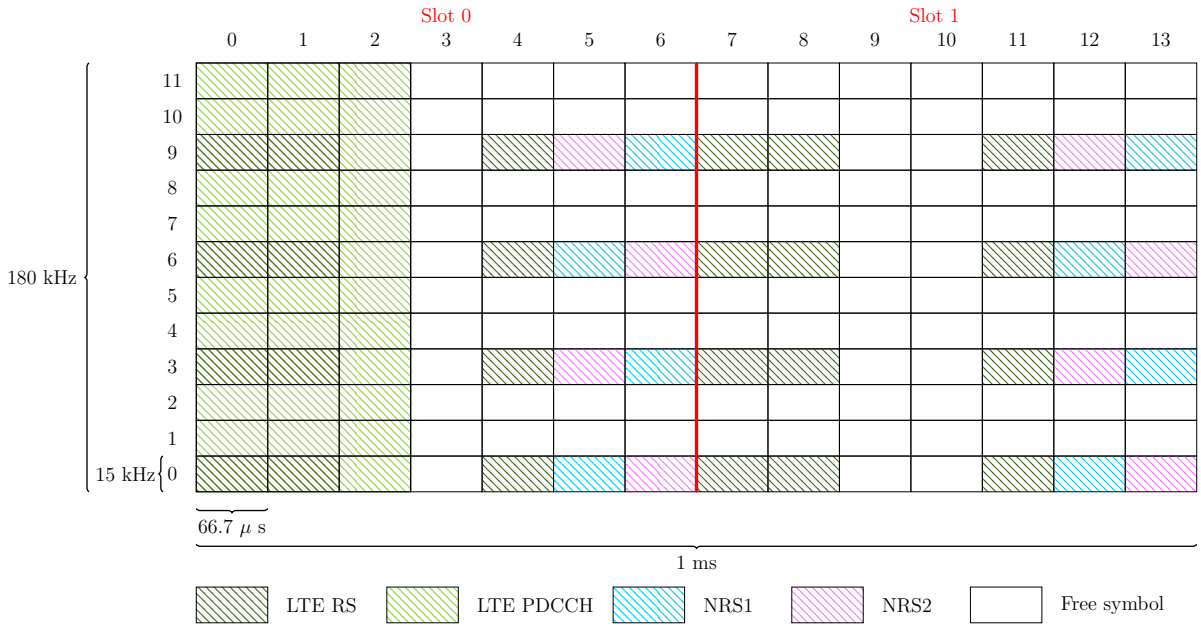

Figure 2.12: subframe structure [**??**]

It should be noted that the described allocation is a worst case scenario for the DL. If the system is deployed either in guard-band or as stand-alone only the NRS is actually used, but before the UE is synchronized it does not know what is in use and needs to guard for this worst case scenario. When the UE receive the MIB-NB and NB-SIB1 will it get information in regards to the number of carriers and the size of LTE PDCCH [**?**].

Uplink

As mentioned in chapter 1 most of the data in the system is UL data. Therefore has the UL spectrum been tuned to accommodate the massive amount of users. The timing alignment of the UL follows the DL meaning when synchronized to the DL band, the UE is also synchronized to the UL except for the delay introduced by the travelling time of the signal. This delay is found at the beginning of the Random Access Procedure (RAP), which will be further explained in subsection 2.3.2.

Frame Structure
Compared to legacy LTE the UL frame can take different formats. It is 180 kHz wide as the DL frame, however the sub carrier width can be both 3.75 kHz and 15 kHz.

2.2.7 Channels

All subframes that are not used for the above mentioned or used for MBSFN can be used for either Narrow-band Physical Downlink Control Channel (NPDCCH) or Narrow-band Physical Downlink Shared Channel (NPDSCH). The NPDCCH is meant for indicate for which UE there is data, where to find it and how often it is repeated. It also provides UL grant and position for UL data. Finally paging or system information update is also indicated on this channel [**?**]. It should be noted that which subframes contain NPDCCH is signaled during RRC in the connection phase typically a 10 or 40 bits bitmap [**?**].

2.3 Network Access

2.3.1 Cell Search and Synchronization Procedure

Synchronization
The synchronization procedure is very similar to that of a LTE as can be seen in Figure 2.13.

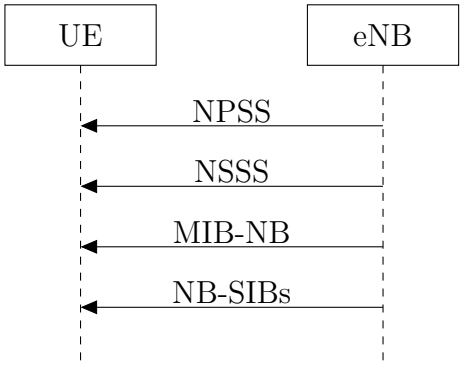

Figure 2.13: sync-NB

First the NPSS is located this provides the initial Carrier Frequency Offset (CFO) as well as timing alignment. Then the NSSS is decoded this provides the Narrow-band Physical Cell-specific Identity (NB-PCID) and timing within a 80 ms block [**?**]. For low complexity UEs a single 10 ms segment might not suffice at a low Signal to Noise Ratio (SNR), the structure of the NPSS is therefore made so the signals can accumulate coherently over multiple 10 ms segments [**?**]. The next step is to decode the MIB-NB, it consists of 34 bits and 16 Cyclic Redundancy Check (CRC) bits, they are transmitted in eight self-decodeable blocks which is repeated eight times resulting in a total transmission time of 640 ms as can be seen on Figure 2.14.

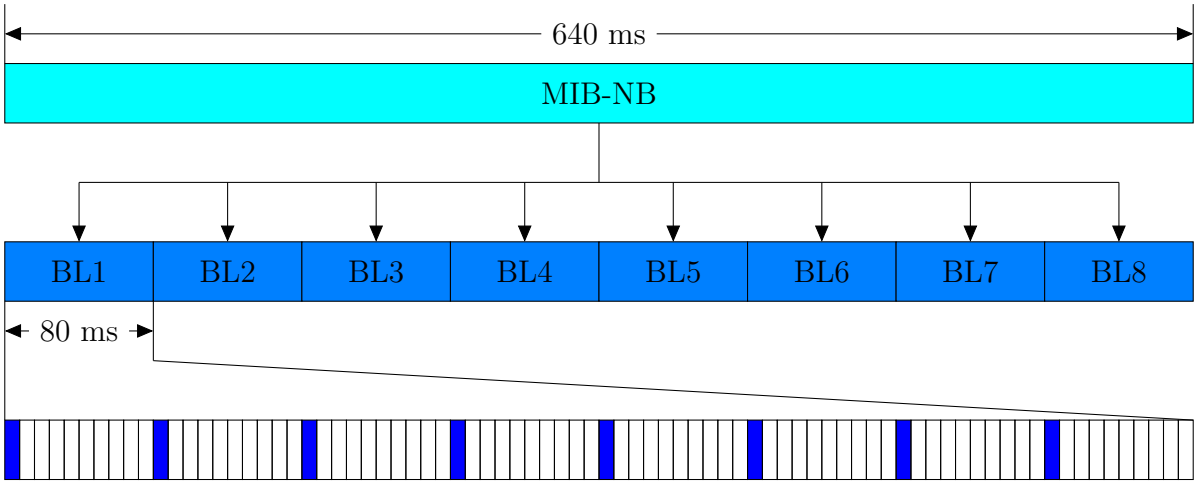

Figure 2.14: MIB-NB

The information carried in the MIB-NB are:

2 bit hyper frame number

4 bit Subframe Number (SFN)

4 bit NB-SIB1 scheduling

5 bit value tag

1 bit access barrer

7 bit operation mode and values

11 bit reserved for future use

From the MIB-NB the schedule for NB-SIB1 is found, this is always transmitted in subframe 4 however only the frames indicated by MIB-NB carry NB-SIB1. The next step is to decode all the NB-SIBs.

When the UE have read all NB-SIBs it has fully synchronized with the eNB. The complete synchronization process can be seen in Figure 2.13. It is mandatory for the UE to have a valid version of MIB-NB as well as NB-SIB1-5, NB-SIB14 and 16 is only read when required. Furthermore once connected to the system the UE is not expected to update its version of the NB-SIBs unless instructed to [**?**]. Now the UE is ready to start the Narrow-band Random Access Procedure (NRAP) which is described later.

2.3.2 Random Access Procedure

2.3.3 Connection Control

RRC connection resume PSM eDRX NAS data transfer

2.4 Data Transfer

2.4.1 Control Plane Optimization

2.4.2 Multi Carrier Configuration

2.4.3 Repetition Schemes

3 | System Setup

3.1 Overview

First, there should be a conceptual diagram of the setup; this should go into a description of how the emulator is actually put together. There should be a mention of how an external device can be put into the system to be tested also due to the cellular nature of NB-IoT. The physical connection needs to be explained, how to connect everything and where to put attenuators combiners and so forth. There could also be a section of practical limitation due to digitalization. Should end with differentiation of main and auxiliary components.

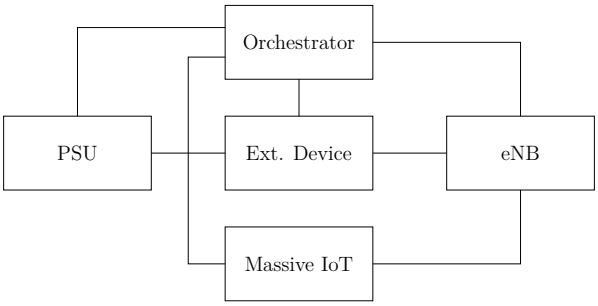

Figure 3.1: Testbed overview

eNB
Here should be mentioned that the BSE is not primary concern, therefore use of exsiting BSE. It should also be mentioned that it should be changeable so commercial BS can also be tested. It should end with use we use Amarisoft LTE 100 as primary and support it with UXM. Amarisoft Here should be a list of relevant features it have, and how to use them. It should also be mentioned, how we can access it from a main PC to set these features. It should be described how the core network interacts with the eNB. It should also be described where to put USIM data to allow network attach. UXM Here should be a list of relevant features it have, and how to use them. It should also be mentioned, how we can access it from a main PC to set these features. It should be described how the core network interacts with the eNB. It should also be described where to put USIM data to allow network attach.

Massive IoT
Here should be a description of the software from SRS. How the core structure of the code is and how it is expanded to accommodate multiple UEs. There should be a description of how to change key parameters in the code and how to use the system from a main PC (or if the main PC should host the MassM2M).

PSU
Short description of the feature of the PSU and the limitation (can not measure and

change settings simultaneously). There should also be a description of how the PSU responds to SCIPI commands.

External device
An explanation of why it is nice to include (possibility to test commercial devices). Some examples of commercial devices.

Orchestrator
What are the function of the orchestrator? Mention the use of TAP. A list of all connections and communication protocols.

4 | Performance Evaluation

Here should be an introduction of what we will test (the emulator and/or the protocol).

4.1 Evaluation Points

Here should be a list of all requirement that is tested and criteria for passed not passed. Requirements:

- Emulator
    1. Amount of users
        - Support TBD active users and TBD users total
    2. Configurable
        - Changeable parameters: Channel type, path loss, number of devices, data profile
    3. Power control
        - Should support a output power up to 23 dB with a range of TBD dB
- Protocol
    4. Ultra-low Complexity Devices
        - The UE has a sample rate of 240 KHz
        - Only supports TBCC
        - Half-duplex
        - Uses SISO connection
    5. Improved Coverage
        - Support a MCL of 164 dB
        - Improve coverage by introducing CE levels
    6. Support Massive Number of Devices
        - Support 52547 devices per cell-site sector based on a TBD data profile
    7. Improved Power Efficiency
        - Achieve a battery life time of 10 years with a battery capacity of 5 Wh
        - Using CE to minimize Power amplifier backoff increasing efficiency
        - Utilize cDRX, eDRX and PSM to increase efficiency
    8. Deployment flexibility
        - The system should be able to be deployed inside legacy LTE.

– The system should be able to be deployed as a stand alone solution.

Based on both the focus explained in chapter 1 as well as some issues with the emulator explained TBD. The only points that is actually tested are:

- Emulator
  1. Configurable
- Protocol
  2. Improved Power Efficiency

4.2 General Test Setup

Here should be a description of the general setup (including figure) used in all test and a list of baseline values for all parameters. Including physical setup, BSE, UEE.

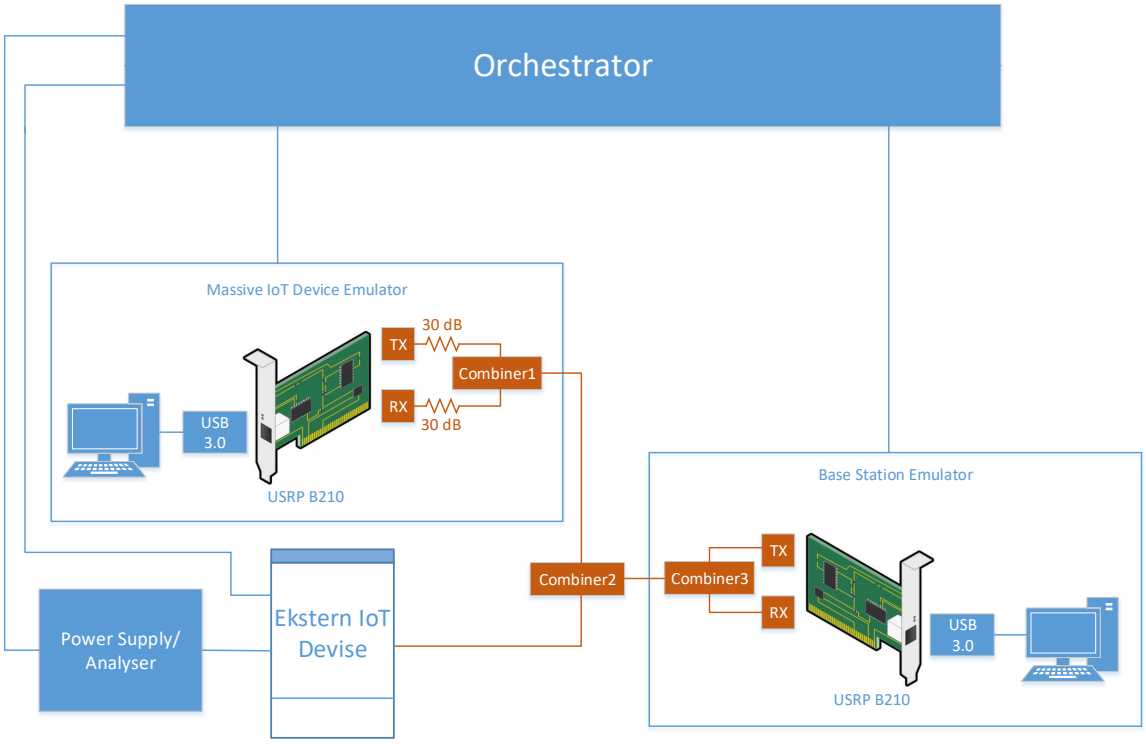

Figure 4.1: General test setup

Massive IoT Emulator	
Parameter	**Value**
Number of devices	0
Rx gain	40 dB
Tx gain	40 dB
R14	False
Dl_EARFCN	6310
UE_category	Nb1
Power Supply/Analyser	
Enable	Off
Volt	3.6 V
Ampere	1 A
Ekstern IoT device	
Enable	Off
Dl_EARFCN	6310
Base Station Emulator	
Cell type	NB-IoT
Number of cells	1
Operation mode	Standalone
Dl_EARFCN	6310
Cell ID	0
Tx gain	89 dB
R14	False
nprach_detect_threshold	19 dB

Table 4.1: My caption

4.3 Evaluation

4.3.1 Amount of Devices

4.3.2 Configurable

4.3.3 Power Control

4.3.4 Ultra-low Complexity Devices

4.3.5 Improved Coverage

4.3.6 Support Massive Number of Devices

4.3.7 Improved Power Efficiency

Test Overview

Test Setup

Test Procedure

4.3.8 Deployment Flexibility

4.4 Results

Here should be a list of all results produced from the test. A short note should be attached to the results if the requirement is passed and if not why not.

Requirement	**Performance**
Amount of Devices	
Configurability	
Power Control	
Low Complexity Devices	
Improved Coverage	
Support Massive Amount of Devices	
Improved Power Efficiency	
Deployment Flexibility	

Table 4.2: My caption

5 | Conclusion

6 | Discussion

Appendix

A | Battery Consumption Model

(Should be limited to only 1 device in the network)

$$L(t_i) = \frac{C_{bat} \cdot SF_{bat}}{P_m(t_i) + P_{device}} \tag{7.1}$$

Where:

$L(t_i)$	is the expected lifetime of the battery	[h]
t_i	is the transmission time interval	[h]
C_{bat}	is the capacity of the battery	[Wh]
SF_{bat}	is the safety factor of the battery	[1]
$P_m(t_i)$	is the power consumption of the modem	[W]
P_{device}	is the power consumption of the IoT device	[W]

Battery capacity
This is set from the requirements to 5 Wh

Battery safety factor
set to 0.5 in paper we probably can not use

Device power consumption
Modem off on the used devices. It is a little irrelevant as none of the devices are final and low power. Should still be measured to draw some conclusion anyway, might be negligible.

Modem power consumption

$$P_m(t_i) = \frac{E_{conn} + E_{tx} + E_{disconn} + E_{idle}}{t_i} \tag{7.2}$$

Where:

E_{conn}	is the energy used to connect to the network	[J]
E_{tx}	is the energy used during transmission	[J]
$E_{disconn}$	is the energy used to disconnect from the network	[J]
E_{idle}	is the energy used during the idle period	[J]

Energy used to Connect to the Network

$$E_{conn} = E_{modem,on} + E_{sync} + E_{attach} \tag{7.3}$$

$E_{modem,on}$
parameters: modem
The energy to turn the modem on.

E_{sync}
parameters: modem, frequency, operation mode, coverage level
The energy to synchronize to the network.

E_{attach}
parameters: modem, frequency, path loss, operation mode, coverage level
The energy to attach to the network. Should be split so that attachment from different idle states is supported (with and without AS).

Transmission Power

$$E_{tx} = P_{tx} \cdot t_{tx} \tag{7.4}$$

P_{tx}
parameters: modem, frequency, path loss
Transmission power

t_{tx}
parameters: operation mode, coverage level, amount of data
Transmission time

Disconnection Energy Overhead of detach procedure

Idle Mode Power

$$E_{idle} = P_{eDRX} \cdot t_{eDRX} + P_{PSM} \cdot t_{PSM} \tag{7.5}$$

$P_{eDRX,PSM}$
parameters: modem, paging interval
Power consumed in idle modes

$t_{eDRX,PSM}$
parameters: timer settings
Time spent in eDRX and PSM mode respectively.