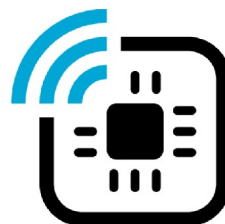Delft University of Technology
Master of Science Thesis in Embedded Systems

LPWAN Performance Enhancement for IoT in the Smart Grid

Anup Kiran Bhattacharjee

STEDIN.NET

Embedded Networked Systems

TU Delft
Delft University of Technology

LPWAN Performance Enhancement for IoT in the Smart Grid

Master of Science Thesis in Embedded Systems

Embedded and Networked Systems Section
Faculty of Electrical Engineering, Mathematics and Computer Science
Delft University of Technology
Mekelweg 4, 2628 CD Delft, The Netherlands

Anup Kiran Bhattacharjee
a.k.bhattacharjee@student.tudelft.nl
anup.kiran@outlook.com
TU Delft student Number: 4738845

19th September 2019

Author
 Anup Kiran Bhattacharjee (a.k.bhattacharjee@student.tudelft.nl)
Title
 LPWAN Performance Enhancement for IoT in the Smart Grid
MSc presentation
 27th September 2019

Graduation Committee
 Dr. Ir. Fernando Kuipers   Delft University of Technology
 Dr. Remco Litjens MSc   Delft University of Technology
 Ir. Shuang Zhang   Stedin

Abstract

With the proliferation of IoT devices across the globe, the adoption of IoT related technologies has been increasing rapidly. Newer technologies which fall in the category of Low Power Wide Area Network (LPWAN) have increased this adoption even further. A lot of research is being done in LPWAN licensed band as well as unlicensed band technologies to make them more efficient, such as in terms of power consumption and latency. In this thesis the author has focused on cellular IoT technologies (licensed spectrum LPWAN technologies), to improve the end-to-end behavior. The focus is to see and improve the effect of the device on the network behavior. We have done tests on different networks and went through the 3GPP Specification Release 14 to find possible areas of improvement. Keeping this in mind we have designed a solution to increase the number of pageable devices that can be maintained by the network to more than *2 times* of original capacity (when not using our solution). This solution can be used to optimize as per the use case, whether to provide lower latency or save energy consumption of the device. To verify that the solution can be used in real life, we have tested it with Stedin critical application device in their substation.

Preface

The basis for this thesis has stemmed from my interest in IoT and how it can actually be used in real life applications. IoT can help us make our lives easier, we already see examples such as smart car, smart street lighting, smart grids to name a few. With this thesis, I go into details of licensed band cellular IoT technologies namely NB-IoT and LTE-M, to see how I can improve their current adoption. This thesis has been done to fulfil the graduation requirements for Master of Science in Embedded Systems curriculum at TU Delft. I have engaged in researching and writing this thesis from December 2018 to September 2019. The thesis was done at the Telecom group in Stedin, Rotterdam. The research problem was formulated together with Shuang Zhang from Stedin and Fernando Kuipers from TU Delft.

I would like to thank my daily supervisor Shuang Zhang for taking out time from his schedule to guide me during my thesis. He has helped me by addressing my technical queries on NB-IoT and LTE-M while helping me to improve my research and planning skills. My gratitude also goes to Fernando Kuipers, my supervisor at TU Delft who helped me to devlop my researching skills by being critical of my work while helping me to shape the work (for writing and presentation). I would also like to thank Remco Litjens who agreed to be part of my thesis committee. My father Ramkrishna Bhattacharjee, my mother Champa Bhattacharjee, my brother Amit Bhattacharjee and my love Layla Brini have continued to provide me with their love and support throughout the thesis which helped me a great deal.

I hope you enjoy reading this work as much as I enjoyed doing it.

Anup Kiran Bhattacharjee

Delft, The Netherlands
19th September 2019

Contents

Chapter 1

Introduction

With the advent of Low Power Wide Area Network (LPWAN) technologies
(like LoRa, Sigfox, NB-IoT, LTE-M, EC-GSM), the adoption of IoT-related
use cases has significantly increased in the utility sector. When compared
with conventional IoT technologies (like, BLE and WiFi), LPWAN techno-
logies have the benefit of lower powered communication at the expense of a
reduced data rate for communicating to longer distances (also represented
in Figure 1.1).
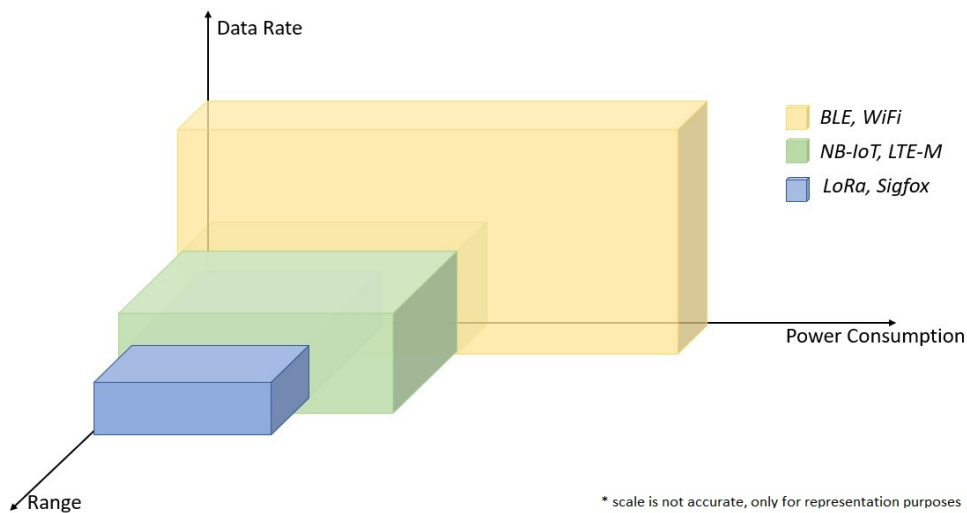
Figure 1.1:   Commonly used IoT technologies

Based on the spectrum of their operation, LPWAN technologies can be
broadly classified into two categories: licensed (mainly NB-IoT, LTE-M) or
unlicensed (mainly LoRa, Sigfox). In the Netherlands both licensed and un-
licensed spectrum based technologies are being widely used. Some examples
can be of TTN [17] and KPN LoRaWAN deployments; T-mobile, Vodafone
NB-IoT deployments; T-mobile, KPN and Vodafone LTE-M deployments.

In the present day these technology deployments are being tested out for various use cases. They are being tested to understand the pros, cons and the associated challenges with the deployment in real life scenarios. This is especially true when taking into consideration Distribution System Operators (DSOs) like Stedin in the Netherlands. Stedin is one of the first European DSO to have a cellular IoT (cIoT) trial (with NB-IoT) live in their distribution network. The reason for these trials is Stedin's wish to modernize its existing distribution grid with cellular IoT technologies, mainly for:

- Dealing with uncertainties introduced into the network by customers. Contrary to a decade or two ago, nowadays people have solar panels installed on their roofs. This means the consumer also generates electricity for the network. The amount of electricity generated by a household can vary as per the time of the day and year. Considering this, a substation that is connected to a neighbourhood may suddenly face a large influx of consumer electricity flowing into the network, it may damage the supply lines.

- Data Oriented Asset management, and decentralized monitoring and control. To understand this better lets take the following use case. Whenever there is a power outage due to fault in one of the substations, technicians have to go to fix the issue. The technicians have to go around majority of the substations to find out the cause of outage. To make this process cost and time efficient, devices are deployed in the substations. These devices notify the server whenever there is any issue at the substation. By providing cIoT technology on these devices instead of the current GPRS technology, device life is extended and deeper indoor penetration is possible (compared to GPRS).

- Majority of the distribution network in the cities is based around optical fibre network. But the optical fibre network is not available in many places, such as the rural areas. In the rural area substations, currently GPRS is being used. The cIoT technologies can be used for deep indoor coverage in the substations which have thick concrete walls while providing lower energy consumption.

But the initial cIoT trial for the proof of concept made by Stedin has been sub-optimal (cannot be used for critical applications). This is mainly because User Equipment (UE) and network were not behaving as expected, some of which are:

- Lower battery life than expected

- Unexpected deregistration from the network

- Network timers (discussed in Chapter 2) being used by the UE did not function properly

- Network and cellular module are currently black boxes for the user.

These issues have resulted in the need of studying the cIoT technologies from both user and network perspective. In cIoT technologies, user performance strongly depends on the network configuration, but the opposite is also equally valid. This calls for the need to have a study for observing how the network and user configurations affect each other in real life settings. Pertaining to this, a detailed study has been done using experiments and referring to 3GPP specifications (Rel. 14). From the observations made, the author suggests improvements, and proposes solution over the technology for further optimizing the performance of the user and network. After the introduction, firstly the required background for understanding the thesis in detail is provided in Chapter 2. Successively, Chapter 3 explains the initial literature survey done and hypothesis for the problem at hand, which has been derived from the initial background research done in Chapter 2. To further understand the cIoT (NB-IoT and LTE-M) technologies and make a concrete statement, initial measurements are conducted. The aim of these measurements is to shed light on the observations made from the User Equipment (UE) perspective, depending on various cellular modem and network settings/behaviour. These measurements are done on multiple networks using multiple cellular modems. The observations and inferences are shared in Chapter 4, which are kept in mind while coming up with the method. Using the observations made in Chapter 4 and referring to 3GPP specification Rel. 14, specific parameters that affect the behaviour of the E2E network as a whole have been selected.

In chapter 5, the solution design is presented. This chapter goes deep as to what are the reasons for different decisions made while designing the solution and their hypothesized effects. After explaining the theoretical side of the solution, chapter 6 shows the verification alongwith the comparison of the results of the solution to the baseline case. The implementation of solution for real life use case is also shown in 6. Lastly, the conclusion of the thesis is provided in chapter 7, alongwith the future work.

Chapter 2

Background

2.1 Introduction to cellular IoT Technology

As explained in previous section, Low Power Wide Area Network technology has brought about new possibilities in the domain of IoT. In this thesis the emphasis is on the licensed spectrum based LPWAN technologies such as NB-IoT and LTE-M. The licensed spectrum based LPWAN technologies are also known as cellular IoT technologies. The reason for this is simply because the telecom operators want to use the existing frequency bands to enable machine type communications (MTC). This is different from human type communications such as using mobile phones, as MTC constitutes of use cases such as data sent from sensor nodes (smart meters for example). The benefits of using cIoT technologies can be summarized into:

- Cellular IoT technologies **do not have the duty cycle restrictions** that are faced by unlicensed spectrum technologies. This leads to higher data rates and better Quality of Service for a higher cost of subscription.

- **Coverage enhancement** and **deep indoor penetration**. NB-IoT and LTE-M are able to provide coverage in places such as basements, where in general cellular connection/unlicensed spectrum LPWAN technologies can not reach [13].

- Compared to previous cellular technologies, the **energy consumption** of the devices that use cIoT technologies is considerably decreased. This is due to the introduction of extended Idle discontinuous Reception (eIDRX) and Power Saving Mode (PSM) [3]. They will be described further, but to understand it in brief, these two parameters are used to decrease the time the device is listening to the network for any downlink information.

2.2 Cellular IoT end-to-end architecture

The end-to-end architecture of cIoT in terms of device (User Equipment), eNB, Core Network and Application Server is depicted in figure 2.1.
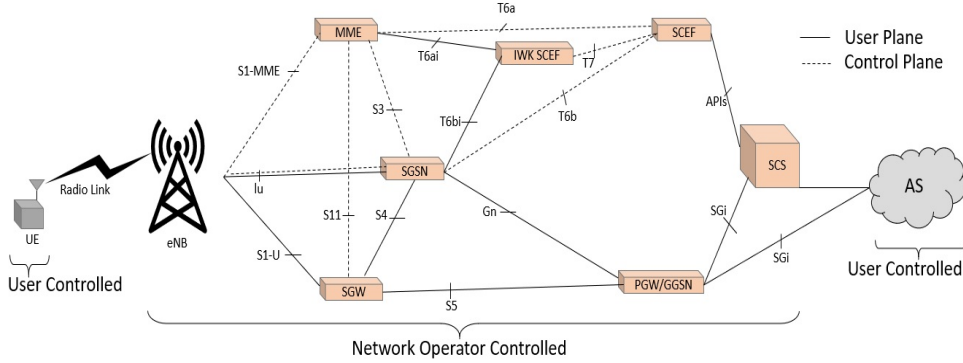
Figure 2.1: E2E Architecture for UE, Network and AS

The user equipment (UE) in general are sensor nodes which are sensing and actuating while having limited processing capabilities. The application server (AS) is used to accumulate all the data sent by the UEs which is forwarded to the AS by the network controlled elements. The AS then processes the received data and stores it. An example in the case of the utility sector can be sensor nodes placed in the substations to monitor the health of the substation. This information is processed on an AS running on a cloud and can be used for various use cases, such as to see if there is anything wrong within the substation or to predict when maintenance should be done. In the network controlled elements, the elements of focus are:

- **Mobility Management Entity (MME)** is the brains of the network. The MME is responsible for making major decisions such as deciding the downlink packet behaviour, timer configurations (like Tracking Area Update (TAU), Active time, paging retransmission time) to be used by UE and Network to synchronize (this is also termed as Radio Resource Management). MME also takes care of mobility management of the UE. This is done by talking to the various eNBs connected to the MME for helping the UE to move from one cell/sector to another (handover) without disruption of service.

- **Serving Gateway (SGW)** is used in the network for purposes such as overload control of MME, user plane data transfer from eNB towards the Packet Data Network Gateway (PGW), to receive and buffer data for UE coming outside of the network before sending it towards the UE (via eNB and MME).

- **Service Capability Exposure Function (SCEF)** [1] is a new element added from 3GPP specificaton Release 13, for providing a means to securely expose the services and capabilities provided by 3GPP network interfaces.

- **Serving GPRS Support Network (SGSN)** is used for dealing with data originated by the GPRS network.

- **Packet Data Network Gateway (PGW)** is used to interface between other outside networks and the core network elements.

2.3 Cellular IoT Optimizations

In order for the current cellular network to be suitable for machine type communications, there are optimizations on the User and Control planes (can also be seen in Figure 2.1). User and Control planes are logical planes which are used to send user application data and control data (messages except user data which are required to setup, maintain and release connection). In terms of protocol stack they are illustrated in Figure 2.2,
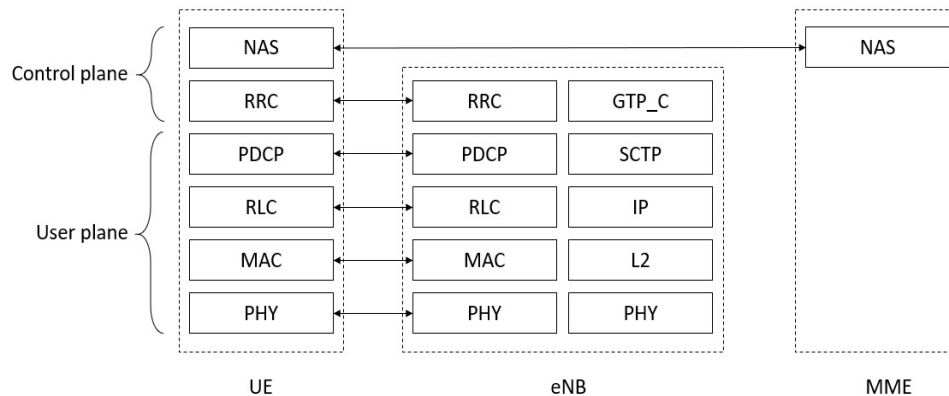
Figure 2.2: Protocol Stack

2.3.1 A bit about Radio Resource Control (RRC) and Non-Access Stratum (NAS) layers

In this thesis we are going to use the terms RRC and NAS often. Hence, this section is used to give a brief introduction to these two layers of the protocol stack. To learn more about these protocol layers, the reader can refer to [7] for RRC layer and [3] for NAS layer.

RRC is a part of the control layer, in the LTE protocol stack. It configures the user and control plane using signalling (between UE and eNB) according to the network status. RRC decides radio resource management strategies

to be implemented after receiving inputs from the NAS layer and the lower layers. Some of the functions for which RRC is responsible:

- Establishment of connections and release functions.

- Establishment, Reconguration and release of radio bearers.

- Outer loop power control.

NAS layer is used for communication of non-signalling related information between the UE and the network (MME). These can be for example:

- Information related to mobility management. For example, tracking area updates.

- Information related to session management. For example, release requests from network side (when the eNB want to do RRC Suspend procedure for example), packet data network (PDN) connection establishment and disconnection (for sending control/user plane data).

Now let's go further to understand what are the optimizations for user and control plane.

2.3.2 User Plane Optimization

In user plane optimization (defined further in [3]) the signalling procedures between the UE and network are optimized. When the UE enters RRC IDLE state, on the NAS level the state changes to IDLE instead of releasing the connection or considering that the exchange of NAS level messages have been terminated. This means the UE is still considered to be connected to the network and hence does not have to begin from RRC Setup procedure the next time it wants to send an uplink. This also leads to enabling bigger timer values for TAU and eIDRX cycles (defined in further subsection 2.4), which means the UE can sleep for longer periods of time to conserve energy.

2.3.3 Control Plane Optimization

In control plane optimization (defined further in [3]) data is sent by piggybacking the control level messages through MME. In this case no data bearers are setup, which leads to saving of energy consumed by the UE. This however makes sense only for data packets that are small in size and not sent frequently. For frequent large packets, it is better to send by establishing the data bearers in order to not strain the control plane.

2.3.4 Coverage Enhancement (CE) levels

For cellular IoT technologies, one of the major feature is the ability of the signal to reach deep indoor locations [13]. Places such as the basement, where regular cellular signals do not reach can be covered by the use of coverage enhancement techniques. When a device uses CE, then the network and the device repeats the same message several times. These repetitions result in the addition of 20 dB to the maximum allowable pathloss for the signal. But as one might expect, this comes at a cost of increased energy consumption due to the increased repetitions. For NB-IoT there are three CE levels (for LTE-M 2) defined. CE level 0 (CE mode A for LTE-M) to CE level 2 (CE mode B for LTE-M), where CE level 0 (CE mode A for LTE-M) corresponds to best possible channel conditions. And CE level 2 (CE mode B for LTE-M) corresponds to worse possible channel conditions. The thresholds to decide the the CE levels are left to the network operators.

2.4 Network Timers

The network timers are essential for synchronization between the UE and the network. There are various timers, but for the thesis our focus is on the following:

- T3412 also know as the Tracking Area Update (TAU) timer

- T3324 or Active time

- Inactive time

- Extended Idle Discontinuous Reception (e-I-DRX) cycle value

- Paging time Window

The TAU time is used by the UE to update the network regarding its location. This is also used as a keep alive message by the network for the UE. If the UE fails to send a TAU message to the network, then the network will consider that the UE is no longer in that specific tracking area and deregister the UE from the network. The Active time is the duration during which the UE will listen for paging requests from the network. Paging requests indicate that there is a downlink packet for the UE. On receiving a paging request from the network, the UE initiates the RRC setup procedure. When the Active time is combined with TAU, we get the Power Saving Mode (PSM) time duration. PSM corresponds to the time when the UE is unreachable by the network, PSM is used to decrease energy consumption on the UE. Inactive time describes the time period for which the UE is in RRC Connected mode after doing the RRC setup procedure. After the inactive time has passed, the eNB initiates the RRC suspend procedure due to which the

UE goes from RRC Connected state to RRC Idle state. The eIDRX cycle is used to limit the number of paging occasions that the UE listens to while in RRC Idle state, for saving the energy consumption of the UE. In one eIDRX cycle, energy can be further saved by defining Paging Time Window value, which is the time for which the UE does the discontinuous reception (DRX).

For clarity, Figure 2.3 shows the case when there is no Mobile Originated (communication initiated by UE) or Mobile Terminated (communication initiated by Network) data transfer. Here we can observe the time at which the different timers start and expire.

1. First the device does the RRC Setup procedure and the attach procedure to connect to the cellular network. The RRC state is changed to RRC_CONNECTED.

2. As there is no MO/MT communication, the network starts the inactive timer (defined by the network). During this period the UE keeps doing extended connected discontinuous reception (e-cDRX).

3. After the inactive timer has expired, the eNB starts the RRC Suspend procedure to change the RRC state of UE from RRC_CONNECTED to RRC_IDLE. This is done to utilise the resources that are allocated to the inactive user and allocate them to other users who are in RRC_CONNECTED state.

4. When the UE enters RRC_IDLE mode, the TAU and Active timers are resumed. For the duration of Active time, the UE keeps doing e-IDRX. After the Active timer has expired, the UE enters Power Saving Mode (PSM) and remains in PSM till the TAU timer expires.

5. On the expiration of TAU timer, the UE is obligated to send a Tracking Area Update (TAU) message to the network. To send the TAU message, the UE has to first change its RRC state from RRC_IDLE to RRC_CONNECTED. This is done by doing the RRC Resume procedure. It should be noted that after expiration of TAU timer both the Active and TAU timers are reset and paused till the device goes back to RRC_IDLE from current RRC_CONNECTED state.

6. On successful transmission of TAU message, the inactive timer is again started. The device keeps doing e-cDRX till the end of the inactive timer after which the procedures from point 3 are repeated.
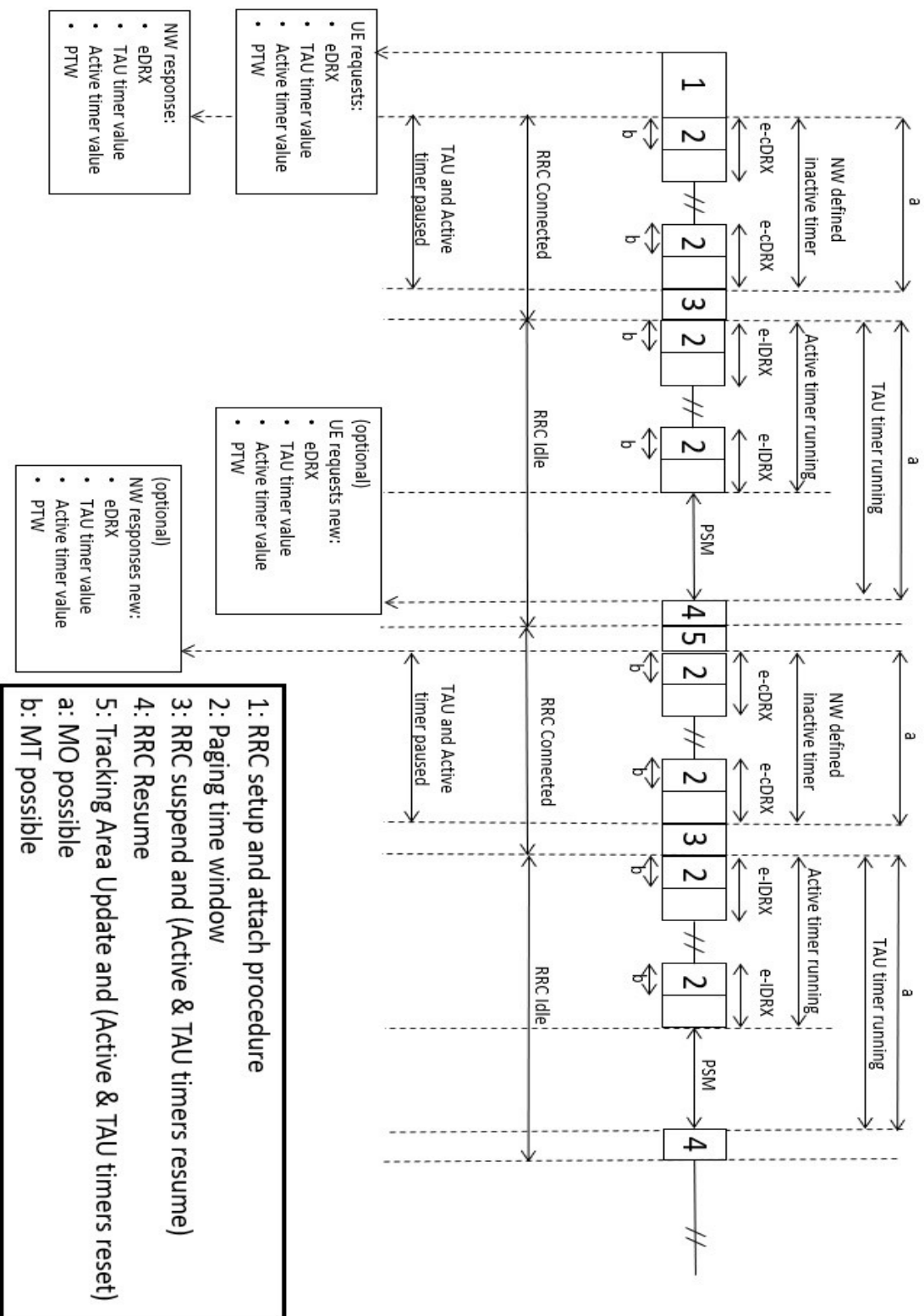
Figure 2.3: Network Timers firing and expiry

2.5   Paging Mechanism

To show the effect of the solution proposed, paging capacity is taken as a metric. To understand Paging Capacity which is defined as the number of devices pageable by the network, first paging has to be defined. Paging is the procedure used by the Network to inform the UE that there is downlink data available for the UE. The paging methodology can be briefly expressed in the following steps:

1. The SGW receives MT data from outside the network (for example an Application Server).

2. SGW does its own checks concerning the downlink (for example APN rate control for AS).

3. SGW buffers the packet and sends a downlink data notification to the serving MME.

4. The MME receives the indication and looks if the UE is available for receiving the data.

5. If the MME decides that the UE should be available (by looking into the Network timer values corresponding to the UE), it sends a paging request via the eNB.

6. The paging request is sent to the UE as a paging record, which is part of the paging occasion (in a paging occasion, there can be at most 16 paging records).

7. From MMEs perspective after sending the paging request, it waits for a specific time called paging retransmission time. After this time period if there is no response, the operation is considered as unsuccessful. Following this the MME uses a paging retransmission strategy.

8. After the UE receives the Paging request, it responds with a Paging Response by doing a RRC Resume procedure.

It should be noted that paging can also be used as a measure to show the massiveness of the network. The more number of devices pageable, the more devices can be accommodated in the network. This is due to the fact that the devices are kept in ECM_IDLE state due to the User plane optimization. We will talk about paging capacity in more detail in the later chapters.

2.6 Radio Link Quality Parameters

In the chapter 4, Radio Link Quality (RLQ) Parameters such as the following have been used to understand the device and network behaviour:

- Reference Signal Received Power (RSRP)

- Reference Signal Received Quality (RSRQ)

- Received Signal Strength Indicator (RSSI)

- Signal to Interference and Noise Ratio (SINR)

This section provides an adequate understanding of the mentioned parameters, such that the reader is aware of these parameters.

2.6.1 Reference Signal Received Power (RSRP)

As per [4], RSRP is defined as the linear average over the power contributions (in Watt) of the resource elements that carry cell-specific reference signals within the considered measurement frequency bandwidth. Since RSRP measures only the reference power we can say this is the strength of the wanted signal. But it does not give any information about signal quality.

2.6.2 Reference Signal Received Quality (RSRQ)

As per [4], RSRQ indicates the portion of pure Reference Signal power over the whole E-UTRA band received by the UE. However we do not get the absolute signal quality, as it will depend on the bandwidth of signal and the number of resource blocks used. RSRQ is calculated as follows:

$$RSRQ = \frac{N.RSRP}{E - UTRA\ carrier\ RSSI}$$

Here, N is the number of resource blocks over the measurement bandwidth.

2.6.3 Received Signal Strength Indicator (RSSI)

RSSI contains all sorts of power including power from co-channel serving and non-serving cells, adjacent channel interference, thermal noise, etc. Hence a higher RSSI value does not mean a better signal quality.

$$RSSI = Signal\ Power\ +\ Interference\ Power\ + Noise\ Power$$

RSSI can also be calculated as:

$$RSSI = \frac{N.RSRP}{RSRQ}$$

2.6.4 Signal to Interference and Noise Ratio (SINR)

SINR is considered to be a better representation of signal quality as it also considers the bandwidth of signal as well as the number of resource blocks used. SINR can be represented as:

$$SINR = RSRQ + 10 \log_{10} \left(\frac{RS\ EPRE}{PDSCH/PUSCH\ EPRE} (Number\ of\ Subcarriers) \right)$$

Here,

- Number of subcarriers=12 (as in LTE we have 12 sub carriers of 15KHz bandwidth).

- Energy Per Resource Element (EPRE) is defined as the energy allocated to one Resource Element.

- RS EPRE: Reference signal EPRE.

- PDSCH/PUSCH EPRE: EPRE across Physical Downlink. Shared Channel (PDSCH for downlink)/Physical Uplink Shared channel (PUSCH for Uplink).

Chapter 3

Related Work and Research Problem

In order to identify the problems to optimize the effect of user and network configuration, the author has first done a literature review. The emphasis was to go through the works published by the research community, to improve the current adoption of the cIoT technologies. The research community has come up with solutions such as,

- Implementing energy harvesting techniques [11] on the UE side to increase battery life. This solution does not consider the affect of user or network configurations on each other.

- Simulation of ML techniques [9] for the user to find the best channel. It takes the UE around 10^4 iterations to reach the case where the UE selects the best channel most of the time. The UE starts by randomly selecting channels which is suboptimal in real-life battery-operated node scenarios.

- Modelling of MO data for delay and energy consumption for NB-IoT [8]. But according to me the way the authors have used LTE procedures, RRC states and functioning of NB-IoT modem in their modelled is incorrect.

- In [15] the authors combine the unlicensed (LoRa) and licensed (NB-IoT) spectrum technology to improve the overall flexibility, reliability, and dependability of the device. They show how the two technologies can be combined to make up for each other's weaknesses. But they do not go into how the technologies themselves can be improved.

- Authors of [18],[12] propose techniques to improve performance from the UE perspective. [18] proposes a data transmission scheme to increase the total number of devices supportable by the network by 60%.

[12] proposes a technique that is better than the NB-IoT Access Reservation Protocol (ARP). Both the techniques involve changing the NB-IoT stack and do not show how sub-optimal configurations of user and network affect one another.

- There are other solutions which have focused on one part of the E2E (UE, CN and AS) network to improve upon it, like the work done in [16], which goes into detail about the schedulers on the eNB.

For most of the works done, the focus has been to improve a specific aspect, but it is the authors belief that the E2E network as a whole should also be considered. If there is only focus to have optimal configurations on one side (user for example) then it could lead to sub-optimal behaviour of the other side (network in that case). In order to move towards massiveness and sustainable IoT solutions, the effect of user application and network should be made optimal (in terms of energy consumption of device, latency for MO and MT, and capacity of network). The aim of this study is to,

1. Do extensive measurements to study the current network deployments of multiple telecom operators (T-mobile, KPN and Vodafone), along with the behaviour of various cellular modems (Quectel and Ublox modules used).

2. Make observations from the measurements and go through the 3GPP Release 14 to understand where improvements can be made.

3. Present a solution to introduce improvements from both user and network perspective.

4. Show the result of the improvements which can be seen from both user and network perspective.

5. Implement the solution for a real life use case.

Chapter 4

Initial Observations and Inferences

In this chapter we will perform the initial measurements, and present our results to understand device and network behaviour. The reason to conduct these measurements is to have a data driven approach during the thesis for studying the user and network side behaviours. From the observed behaviour, the need for a solution for co-ordination between the user and network is apparent. And at the same time, target parameters for optimizing the E2E communication are known. The network behaviour is understood by changing the device-side parameters and by inferring the flowcharts drawn for the 3GPP specification Rel 14 specification, (referred to [6], [7] and [3]).

This section can be divided into 4 parts, section 4.1 explains the setup used for performing the measurements. Section 4.2 explains the observations specific to NB-IoT measurements and section 4.3 explains observations specific to LTE-M measurements. Section 4.4 explains the observations for the common behaviour parts of NB-IoT and LTE-M.

4.1 Experimental Setup

The experimental setup consists of three parts: the device (with the cellular modem), the network and the application server (Node-RED is used). The experimental setup is shown in Figure 4.1.

Different cellular modems and networks have been used to study the behaviour of the device and networks for the NB-IoT and LTE-M technologies. Cellular modems used:

- Quectel BC95 and Quectel BG96 (Figure 4.2)

- Ublox R410 (Figure 4.2)

Networks used:
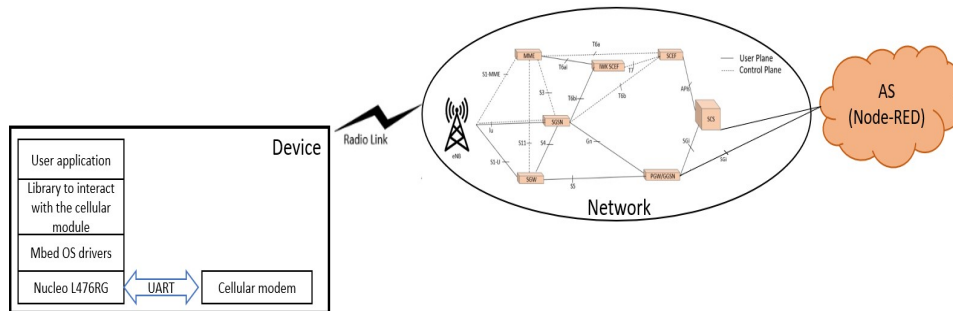
Figure 4.1:   Experimental Setup

Figure 4.2:   From left: Dragino (Quectel BG96)[10], Ublox [20], and Nucleo L476RG [14].

- NB-IoT: T-Mobile

- LTE-M: KPN, Vodafone and T-Mobile

For confidentiality purposes, the Mobile Network Operators (MNOs) have been depicted as MNO1, MNO2 and MNO3. Where MNO1 for example can be any one of the three network operators.

For Quectel BG96, ST Nucleo (shown in Figure 4.2) has been used to interact with the cellular module. As shown in Figure 4.2, the mbed OS has been used on top of Nucleo to interact with the cellular module using the AT Command parser library of mbed. The author has created his own libraries to communicate to the cellular module using the AT Command parser library of mbed OS.

4.2   NB-IoT Specific Observations

In this section, we will see the effect of RSRP due to different coverage enhancement levels and the delay of E2E communication when using UDP over NB-IoT for MNO1's network. The process of calculating delay is shown in Appendix A.

4.2.1 Behaviour due to different CE levels

The RSRP of a better CE level is observed to be better than that of a worse off CE level. In Figure 4.3, the measurements done at Stedin correspond to CE level 1 and the ones done at TU Delft correspond to CE level 0 are depicted as a histogram to show this difference. For a worse off CE level, the effect of interference and noise on RSRP is higher. Hence more fluctuation in RSRP. For measurements having a lower RSRP associated with CE1, this fluctuation leads to higher frequency of cell reselection. The same can be observed for Figure 4.4. This is seen for varied RSRQ cases, therefore the fact that the cell reselection occurred due to the RSRQ falling below -20 dB (one of the guidelines in 3GPP for cell reselection) can be ruled out. The cell reselection behaviour is further elaborated in section 4.4.1.
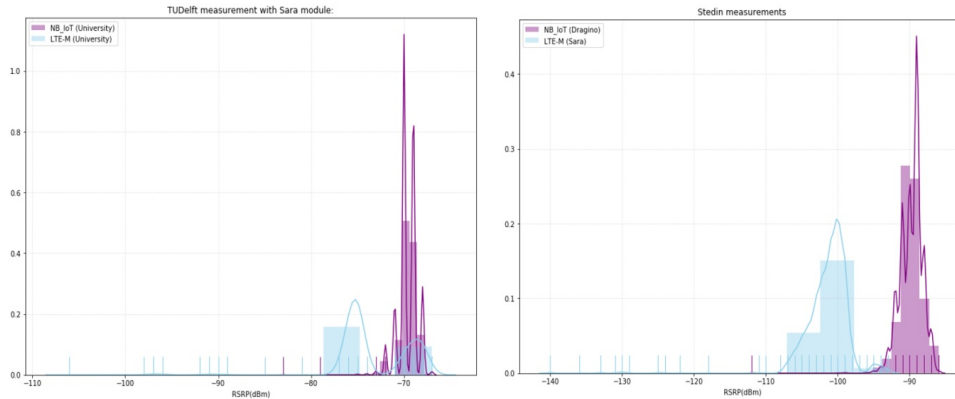
Figure 4.3: RSRP in CE0 (left) and CE1 (right).

4.2.2 E2E Delay for NB-IoT, using MNO1 network

For NB-IoT the average delay observed for E2E communication is *548 ms*. The delay behaviour is further shown in Figure 4.5. This delay can be expected to go much higher in the case of congestion in the network. The reason for the increase in delay would be due to the delay tolerance behaviour of NB-IoT.

4.3 LTE-M Specific Observations

In this section the focus is towards the E2E delay measurement over LTE-M for MNO2 and MNO1 networks. We could not measure this for MNO3 network, as we couldn't find an Access Point Name that provides the device with a public IP address. For the devices that are not provided public IP addresses, downlink communication is not possible from Application Server side hence E2E delay measurement is not possible.
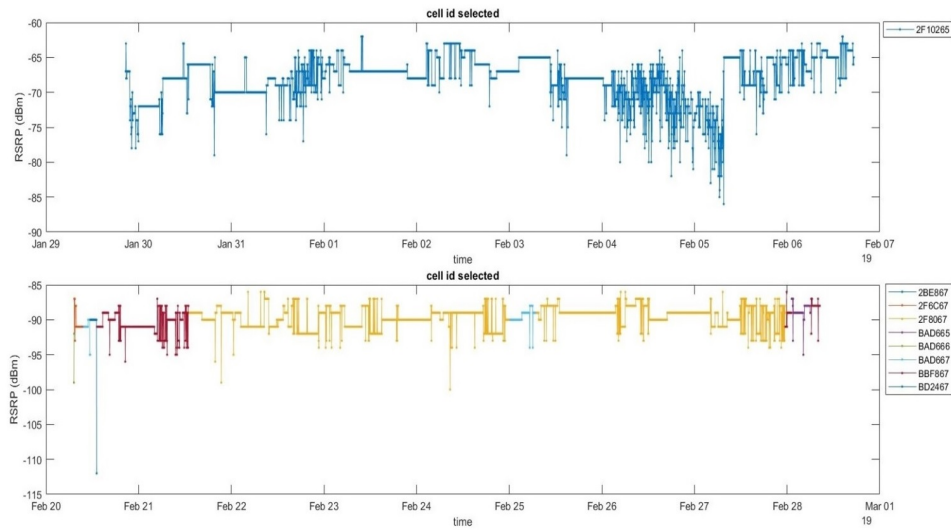
Figure 4.4: CE level effect on Cell Change.

The cellular modules used have the functionality to use only CE mode A for LTE-M, hence the RSRP comparison for CE mode A and B cannot be provided. But during the measurement, the two radio access technologies (RATs) have been measured with same devices while bein placed next to each other. It is hypothesized that the effect on cell reselection due to CE mode A and B will be similar as seen for NB-IoT in Figure 4.4. In the section 4.4, the observations for cell change are made such that they apply for LTE-M as well. This is because the cell selection mechanism for NB-IoT and LTE-M will remain the same for the same module. Now lets see the E2E delays observed for the MNO2 and MNO1 network. The process of calculating delay is shown in Appendix A. The delay behaviours of the current network deployments of MNO2 and MNO1 also show which network to choose for the use case with E2E optimized solution presented in chapter 5.

4.3.1 Delay over MNO2 and MNO1 network

The LTE-M delay for UDP E2E communication over MNO2 network is shown in Figure 4.6. The LTE-M delay for UDP E2E communication over MNO1 network is shown in Figure 4.7.

We can observe that for both the networks, the E2E delay can reach upto 3 seconds, sometime reaching upto 9 seconds (in case of MNO1 network). On average the delay for both the network operators is around *109 ms*. For the use case we choose MNO2. This is due to the MNO2 and MNO1 network's current deployment. As per the current deployment for MNO2
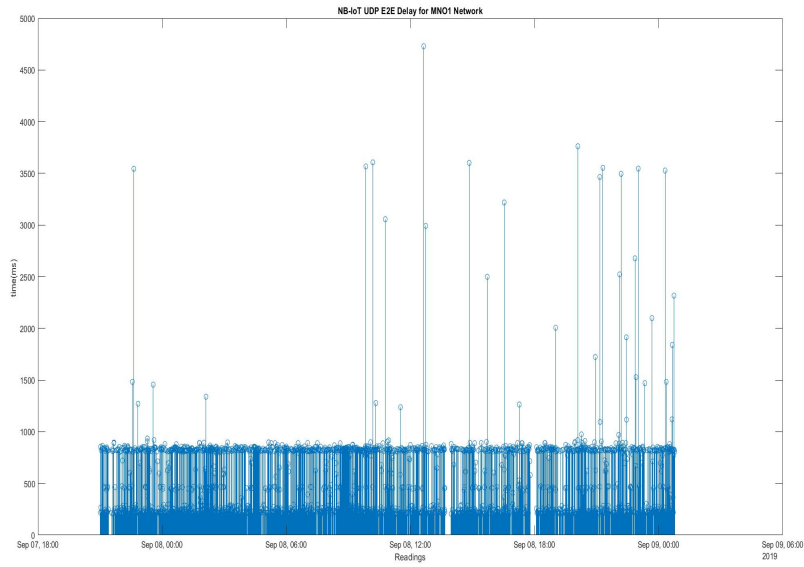
Figure 4.5: NB-IoT E2E UDP Delay for MNO1.
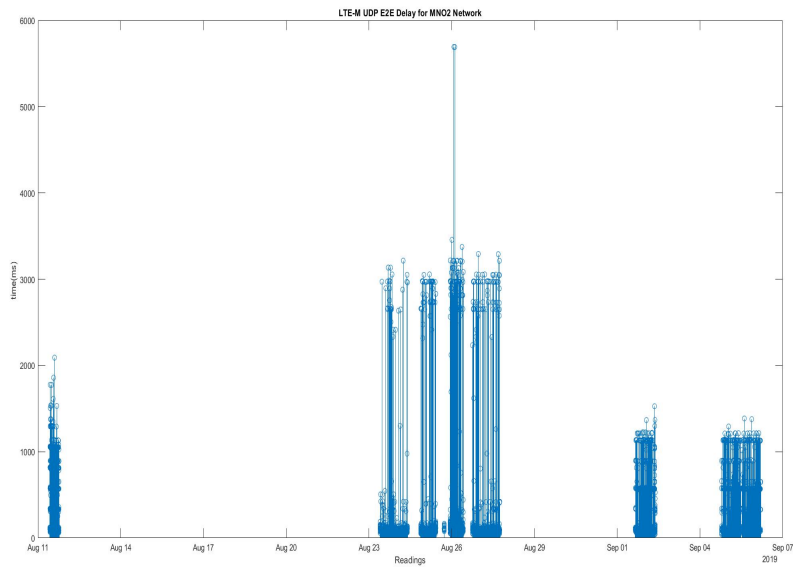
Figure 4.6: LTE-M E2E UDP Delay for MNO2.

the server can send downlink data without the device having to first send an uplink (in case of MNO1).
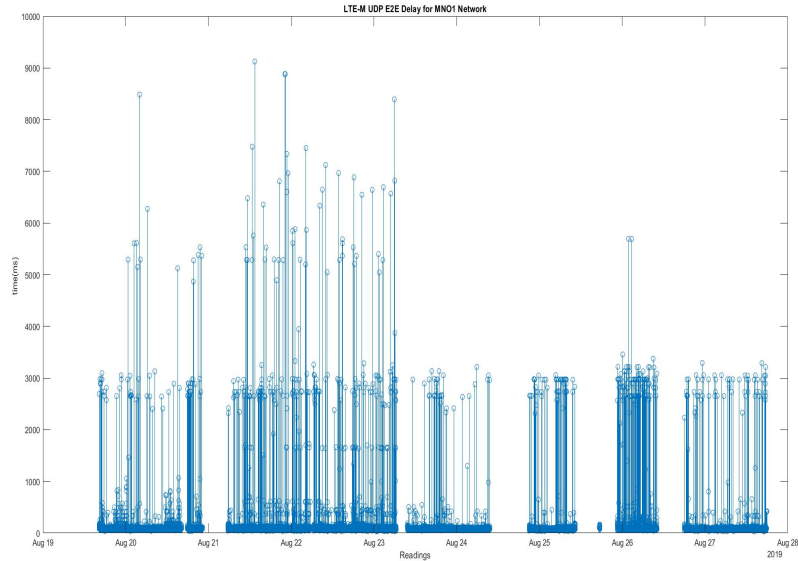
Figure 4.7:   LTE-M E2E UDP Delay for MNO1.

4.4   NB-IoT and LTE-M Common Observations

This section explains the observed behaviour from UE and network, that is common for both NB-IoT and LTE-M.

4.4.1   Cases observed for Cell Change by UE

In the previous section, we have seen the effect of CE level on the RSRP and hypothesized how it may affect the cell reselection behaviour. Now let's go deeper into how the UE is taking the decision to do a cell change. As cell reselection algorithm is implemented on the cellular module, its behaviour depends on the vendor implementation. For this, the data collected by the Sara SFF module is used. This is due to the fact that out of the three modules available, only the Ublox R410M module provides neighbouring cell RLQ data. From the measurements done, the following cases are observed:

- In most cases when the UE has just connected for the first time, it selects the one with the best RSRP and RSRQ.

- The UE selects a new cell if the RSRP of the new cell is better than that of the previous cell.

- It selects the cell with the better RSRP in most of the times even if the newer cell has a worse RSRQ. Even if the RSRQ decreases by a

21

factor of 14dB, the UE still does not change to any other cell, this is because the RSRP is still the same.

- In some cases for the same RSRP it selects the cell with the higher RSRQ.

These cases can be observed in Figure 4.8. The figure shows the selected cell and neighbouring cell RSRP, RSRQ which have been measured simultaneously.
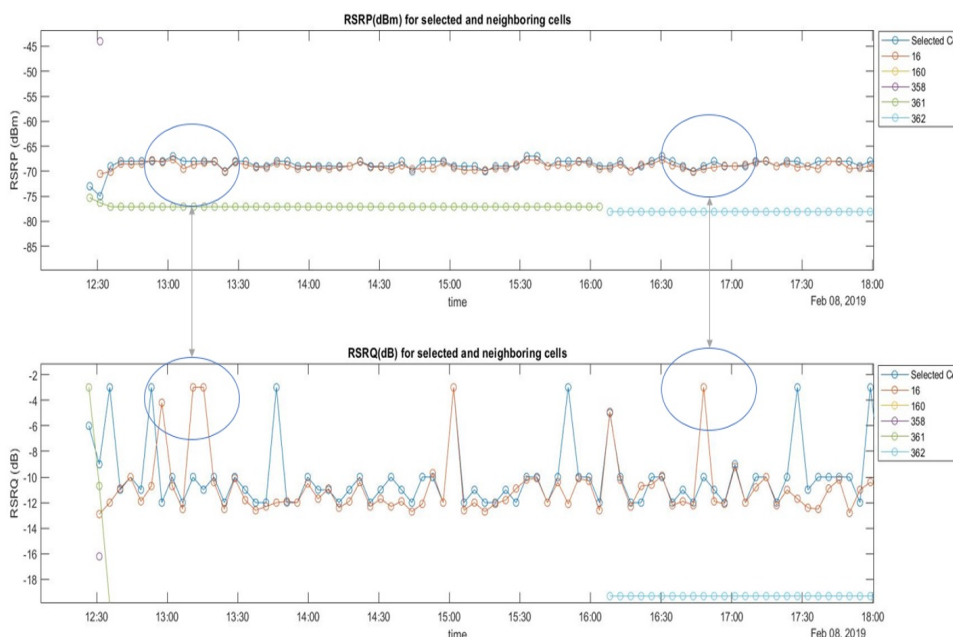
Figure 4.8: Cell Selection plot corresponding to RSRP and RSRQ.

The possible reason for not choosing RSRQ for cell reselection is its variability. For a given measurement, the observed RSRQ has a higher standard deviation compared to the RSRP. To prove this reasoning, the Figures 4.9 and 4.10 depict the variability of RSRP and RSRQ for NB-IoT and LTE-M.

From this observation it is evident that RSRQ is not a good metric to be used in combination with RSRP for cell reselection. This is because, if a UE relies on RSRQ alongwith RSRP, then due to the highly variable nature of the RSRQ, the UE will do more frequent cell reselections. On further observation of the data, it is noted that SINR shows a clear demarcation between a better CE level and a worse off CE level, as seen in Figure 4.11. And as we know from the previous observations that better CE levels occur during better radio conditions, hence here better SINR can be inferred for better cells (in terms of radio conditions). This means that the combination of RSRP and SINR will lead to a more optimal cell reselection when com-
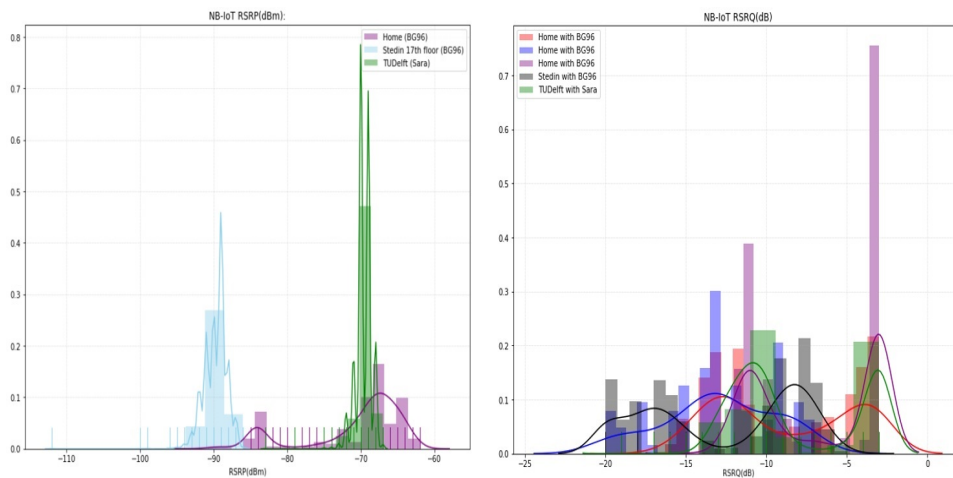
Figure 4.9: RSRP and RSRQ behaviour for NB-IoT.
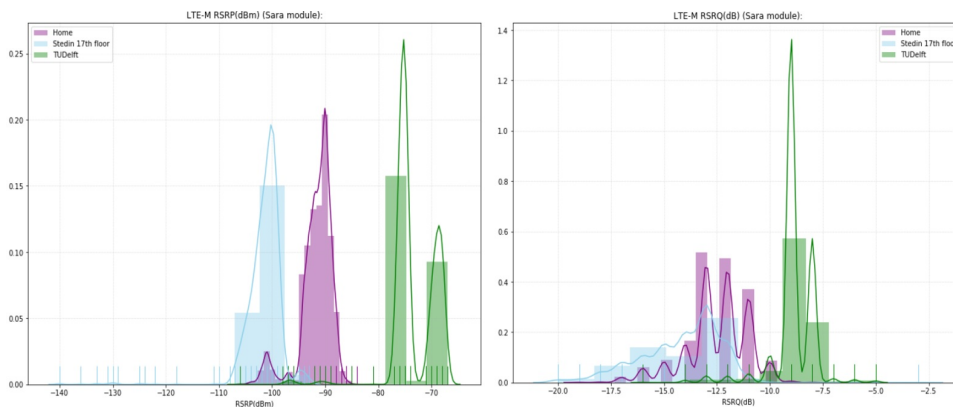
Figure 4.10: RSRP and RSRQ behaviour for LTE-M.

pared to selecting cells by just emphasizing on RSRP or the combination of RSRP and RSRQ.

4.4.2 Network Timer Behaviour

As seen in Chapter 2, network timers assist in co-ordination between the UE and the network. A better co-ordination (optimal timer settings for delay from AS perspective for MT communication, and power consumption for UE) results in an optimal UE and network performance. These measurements aim to show what are the pointers to be kept in mind while requesting timer values from the network. For now the timers that can directly be requested by the UE are observed (so inactive timer and paging retransmission timer behaviours have not been observed). The timers of interest are:
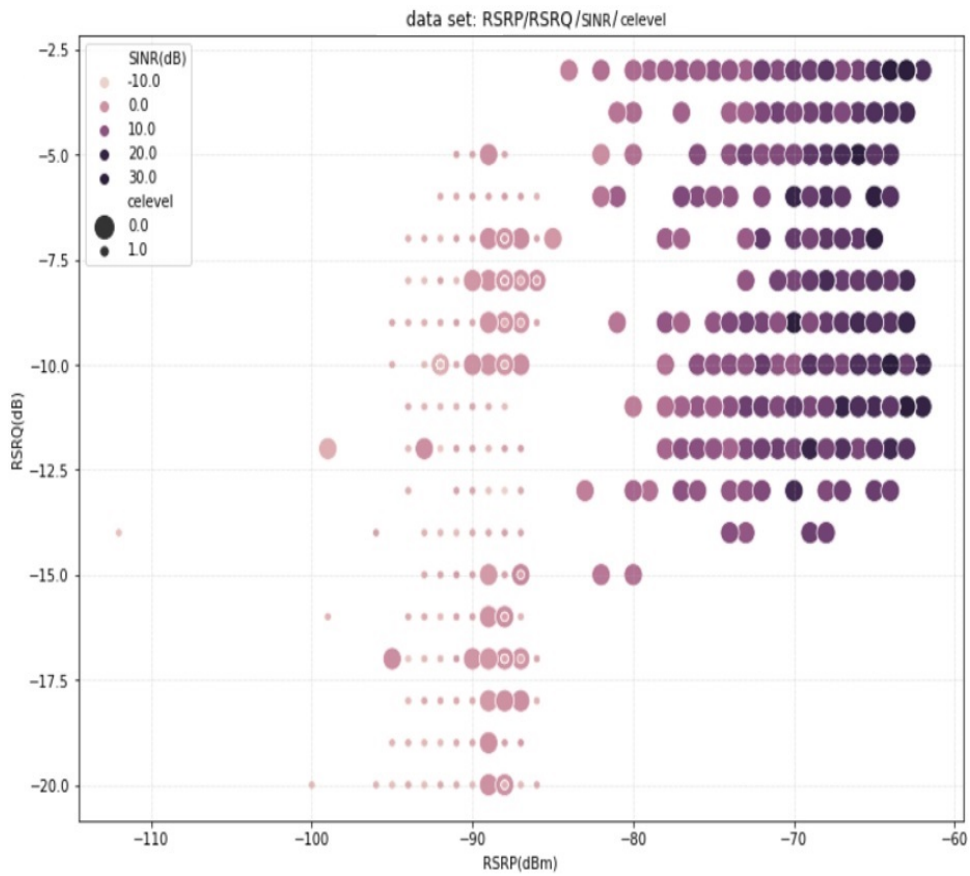
Figure 4.11: SINR and RSRQ behaviour for corresponding RSRP.

- Tracking Area Update: Used for keep-alive messages (also for control level information transfer).

- Active timer: Used together with TAU to define Power Saving Mode duration value.

- Extended Idle Discontinuous Reception (eIDRX) cycle value: For power saving by limiting Paging Occasions (POs) observed by the UE.

- Paging Time Window: Defines the time in an eIDRX cycle for which POs occur.

All the possible timer congurations that can be requested by the 3 available cellular modems have been tested. The observations from the 3 cellular modems are stated in the following subsections.

Observations related to UE behaviour

The observations from device side are as follows:

1. The user should not expect all the modules to have a sanity check. Sanity check of the module refers to the inbuilt functionality that checks if user requested timer combinations make sense or not. If the user request does not make sense, then the module requests a different combination of timer values, which is closest to the requested timer combination. This can be seen in the case of Ublox (R410) and Quectel (BC95, BG96) modules, where the Ublox module has a sanity check and the Quectel modules do not.

2. Not all timer values can be changed by all modems. BC95 gives the option of requesting PTW values, but this is not possible by the other two modems (Ublox and Quectel BG96).

3. Depending on the situation, the module is restricted to requesting certain timer values.

    (a) In case of BG96 when eIDRX cycle is disabled by the module, the network does not allow the module to request active time and TAU values.

    (b) In case of BC95 even if eIDRX cycle is disabled, different values for TAU and Active time can be obtained.

Observations related to network behaviour

For the current MNO1 network, mechanisms to check the validity of UE requested TAU, Active timer and eIDRX cycle are not implemented. When the UE requests for faulty timer value combinations, the network provides it. This should be seen as one of the important settings to be considered by the UE, as the user application cannot always depend on the network for sanity checks. The table in Figure 4.12 shows the invalid requested values alongwith the responses from the network. In the figure, the green highlighted cells represent valid combinations whereas red represents invalid combination of timer values.

But for PTW values, it can be observed that the network has implemented sanity checks. When the UE requests invalid timer congurations the network responds with valid values. The table in Figure 4.13, shows this clearly. In the figure, the green highlighted cells represent valid combinations whereas red represent invalid combination of timer values.

4.4.3 Network buffer behaviour

The network buffer behaviour has been checked for MT communication cases. This is done so that the user application will know how to send MT data from AS. In case of LTE-M (MNO1 and MNO2) there is no buffer implemented, for MNO3 MT is not available. Hence for LTE-M, if the UE

Requested TAU	Network TAU (seconds)	Requested Active timer value	Network Active timer value (seconds)	Requested eDRX value	Network eDRX value	Paging window length (0000 means 2.56 sec)
10 hours (010 00001)	36000	6 min (010 00001)	360	10485.76sec (1111)	1111	0000
10 hours (010 00001)	36000	6 min (010 00001)	360	5242.88sec (1110)	1110	0000
10 hours (010 00001)	36000	6 min (010 00001)	360	2621.44sec (1101)	1101	0000
10 hours (010 00001)	36000	6 min (010 00001)	360	1310.72sec (1100)	1100	0000
10 hours (010 00001)	36000	6 min (010 00001)	360	655.36sec (1011)	1011	0000
10 hours (010 00001)	36000	6 min (010 00001)	360	327.68sec (1010)	1010	0000
10 hours (010 00001)	36000	6 min (010 00001)	360	163.84sec (1001)	1001	0000
10 hours (010 00001)	36000	6 min (010 00001)	360	143.36 sec (1000)	0010	0000
10 hours (010 00001)	36000	6 min (010 00001)	360	122.88 sec (0111)	0010	0000
10 hours (010 00001)	36000	6 min (010 00001)	360	102.4 sec (0110)	0010	0000
10 hours (010 00001)	36000	6 min (010 00001)	360	81.92 sec (0101)	0101	0000
10 hours (010 00001)	36000	6 min (010 00001)	360	61.44sec (0100)	0010	0000
10 hours (010 00001)	36000	6 min (010 00001)	360	40.96 sec (0011)	0011	0000
10 hours (010 00001)	36000	6 min (010 00001)	360	20.48sec (0010)	0010	0000

Figure 4.12: Invalid timer configuration response from Network.

is not available then the packet is dropped. In case of NB-IoT for MNO1 network:

- The network buffer can contain a maximum of 10 (current MNO1 network buffer setting) downlink messages at a time.

- New messages are dropped if the buffer is full. This means that if there is no co-ordination between the AS and the network, then the UE has high chance of receiving stale messages (leads to wastage of UE energy and network resources).

- The network buffer sends each downlink message as a separate packet. This will lead to higher wastage of energy and resources especially when there are more number of stale messages present in the buffer.

Requested PTW (Sec)	NW PTW (Sec)	Requested eDRX (Sec)	NW eDRX (Sec)	Remarks
23.04 (1000)	0111	20.48 (0010)	0010	
	1000	40.96 (0011)	0011	
20.48 sec	1000	81.92 (0101)	0101	
	1000	163.84 (1001)	1001	
	1000	327.68 (1010)	1010	
	1000	655.36 (1011)	1011	
	1000	1310.72 (1100)	1100	
	1000	2621.44 (1101)	1101	
	1000	5242.88 (1110)	1110	
	1000	10485.76 (1111)	1111	
40.96 (1111)	0111	20.48 (0010)		
	1111	40.96 (0011)		
	1111	81.92 (0101)		
	1111	163.84 (1001)		
	1111	327.68 (1010)		
	1111	655.36 (1011)		
	1111	1310.72 (1100)		
	1111	2621.44 (1101)		
	1111	5242.88 (1110)		
	1111	10485.76 (1111)		

Figure 4.13: PTW timer configuration response from Network.

4.4.4 SIM Provisioning

Depending on what features have been enabled for a SIM Card by the network operator, UE behaviour will be affected. To understand this, we can look into two types of SIM cards provided by MNO1:

1. SIM Card with MT enabled

2. SIM Card with MT disabled

In the first case even if the UE does not send anything, the network is able to send MT data to the device as per device availability. The overview of this process is shown in Figure 4.14. This means that the MT data communication is possible for when the device is in both RRC_CONNECTED and IDLE states.
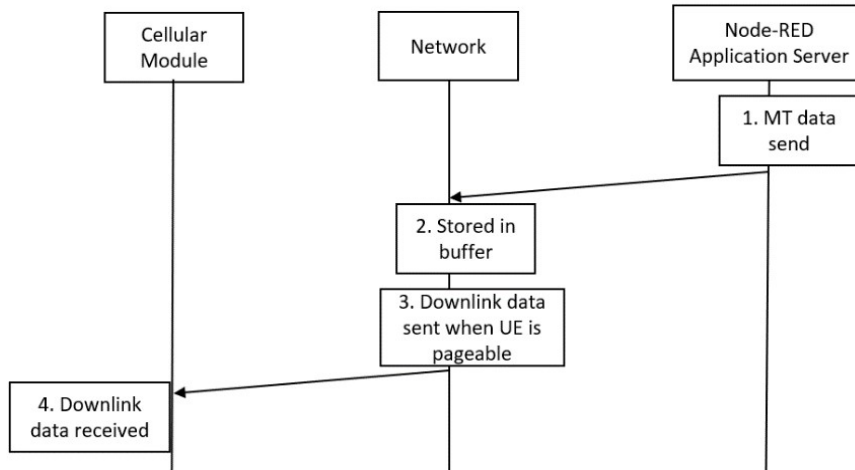
Figure 4.14:   MT data communication flow for MT enabled SIM Card.

The second case relates to the situation when the network by itself does not send any MT data. When the device sends MO data, the network can send stored MT data, which means that MT data communication is only possible when device is in RRC_CONNECTED state. The process is shown in Figure 4.15.

This observation gives the idea to use SIM provisioning to improve the coordination between the user application and the Network as stated in chapter 5.

4.4.5 Observations from 3GPP Rel. 14 specification

To understand the Core Network procedures for predicting the potential areas of improvement, the procedures related to IP and non-IP data delivery
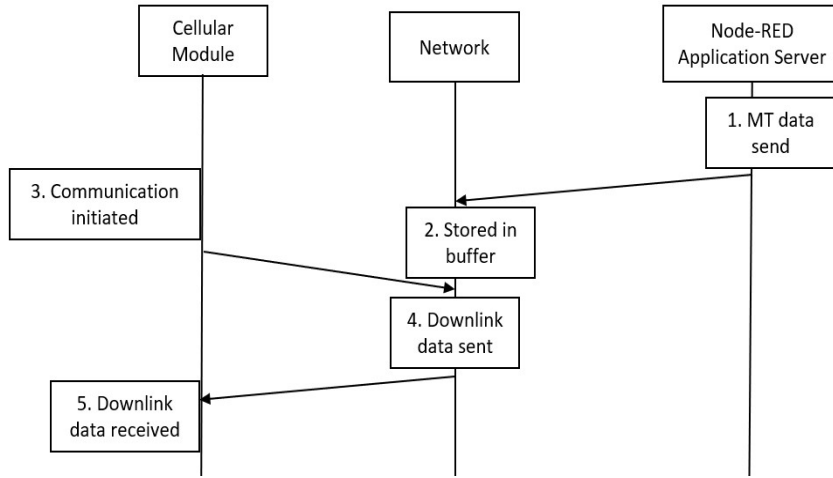
Figure 4.15: MT data communication flow for MT disabled SIM Card.

are studied. After studying these procedures, the flowcharts are drawn for better understanding and targeting of the potential areas for improvement. These flowcharts can be seen in Appendix B. When looking into procedures for data delivery for IP/non-IP, there are mainly 3 paths that the packets can follow. These 3 paths are marked in the Figure 4.16 with three coloured dotted lines. For the scope of this thesis, path 3 is not considered, as most of the network operators implement with path 1 or 2 for MTC data transfer.
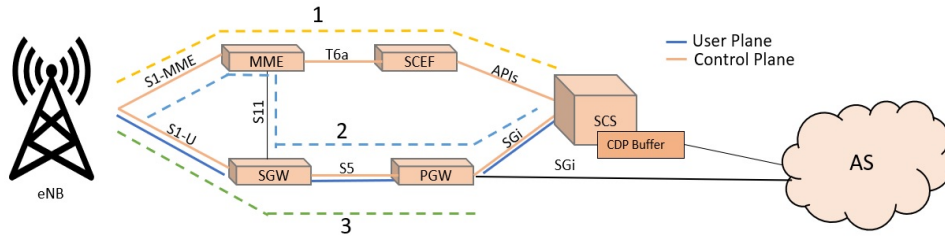
Figure 4.16: IP/non-IP data delivery paths in Core Network.

From the flowchart and reading the related procedures from 3GPP specification, the authors aim is to find parameters or behaviours in the CN. These parameters will make the most impact on E2E communication, using the proposed solution in Chapter 5. The selected parameters are:

1. NAS Inactivity timer value decision: affects the network capacity and UE power consumption.

2. Paging Capacity due to the timer congurations: affects the network resources for paging.

29

Currently as per 3GPP Rel. 14, when the MME is overloaded, the SGW drops the downlink data and does not notify the AS that sent it. Implementing the downlink data delay on AS can result in decreased load on the network and improve reliability of communication.

Chapter 5

Intelligent Layer

In order to optimize the E2E deployment, an intelligent layer is proposed. The parameters to be optimized are found by studying the 3GPP specifications and observing from the measurements done (as explained in Chapter 4). The parts chosen to further optimize E2E communication are:

- NAS Inactivity timer value decision: affects the network capacity and UE power consumption.

- Paging Capacity due to the timer configurations: affects the network resources for paging.

NAS inactivity timer can only be controlled by the network, but affects the UE as well. It translates to the time period from when an UE completes any data transfer after RRC Suspend/RRC Setup procedure, to the time it enters RRC_IDLE state. As the name suggests, inactivity timer is used to determine the inactivity period of an UE by the network (more specifically by the eNB). From the network perspective, inactivity timer is used for diverting the resources being used for one UE to cater to other UEs. From UE perspective, a higher inactivity timer value consumes more energy of UE. This is because, UE listens for paging occasions more often in the RRC_CONNECTED state then compared to RRC_IDLE state. The inactive time can be seen in the Figure 2.3 of timer diagram. The optimization of the NAS inactivity timer will help the UE to save energy and the network to save resources. Hence one of the roles of the Intelligent Layer is to show the effects (shown in chapter 6) of inactivity timer on paging capacity of network and UE energy consumption.

Paging capacity refers to the network capacity to cater to devices with paging. The timer configurations of the UEs can indirectly affect the amount of Paging Records consumed, which means sub-optimal timer configurations on the UE side will lead to higher chances of lowered maximum number of devices maintainable by the network which can be paged (i.e., more devices in ECM_IDLE state instead of being deregisterd by the network). As the

maximum number of pageable devices maintainable for the network will also contribute to massiveness (as the UEs are in ECM_IDLE mode and not deregistered from the network due to User plane cIoT optimization), optimizing the timer configurations of the UEs hence contributes to massiveness.

5.1 Intelligent Layer Architecture

The intelligent layer can be divided into three parts, as can be seen in Figure 5.1:

- UE implementation

- eNB and CN implementation

- AS implementation
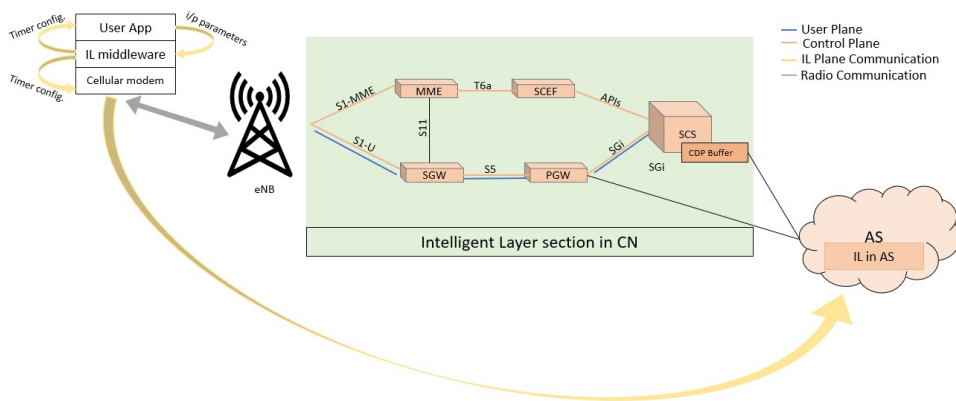
Figure 5.1: Intelligent Layer Architecture.

These three parts can exchange information with each other or take decisions separately to optimize the E2E behaviour.

5.2 Optimizing the network timers by Intelligent Layer

The current role of the IL is to optimize the network timers that are going to be requested by the user application. This is due to the fact that in many cases the user might not be aware of the potential effect of these timers on the device and network. This could lead to unnecessary consumption of energy from the user application and at the same time could lead to higher consumption of paging resources from the network. The intelligent layer asks the user application for its application requirements. The IL gets input

32

parameters from the user application for the application requirements, such as:

- MO behaviour periodic: Is user application on device going to send any periodic MO data?

- MO behaviour aperiodic: How critical is the aperiodic MO data to be sent from the device?

- Latency class of user application (MT): How tolerant to latency is the user application?

- MT expectation for user application: Does the user application on device expect any MT data for its usual functionality?

Depending on these four parameters, the IL decides the optimal network timers and requests to the network. It should be noted that the difference in the logic of optimizing timers for NB-IoT and LTE-M is only for PTW (due to the different ranges and step sizes of the PTW timer values as per 3GPP [2]). There are two ways in which this can be done which are discussed further.

5.2.1 IL on device

Implementation of the IL on UE. In this case the IL acts like a middleware (as shown in Figure 5.2) in the UE and talks to the network instead of the user application talking directly. This is the case when there is an option to change the firmware on the device.
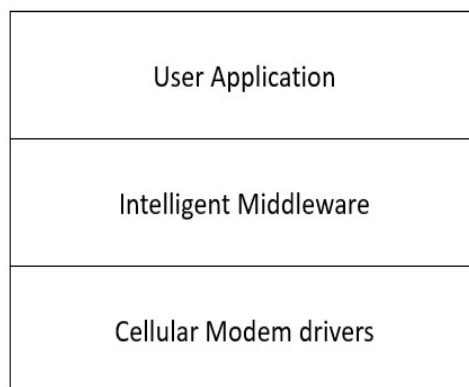
Figure 5.2: Intelligent Layer UE middleware.

5.2.2   IL on AS and CN

The second case is by using the IL on the AS and CN. In this case we do not have an option of changing firmware from the device side. The AS uses the IL to negotiate the timer configurations with the network. Following steps are followed:

1. On the AS side the IL input parameter values for a given device are provided to the AS.

2. The AS uses the intelligent layer to decide the corresponding timer values.

3. The IL on the AS then notifies the network for the device specific timer values.

4. The intelligent layer on the network (CN) stores these timer configuration as per device International Mobile Subscriber Identity (IMSI). IMSI is the unique identifier for a SIM card, hence used for SIM provisioning.

5. Hence the IL introduces a SIM provisioning (like what we have observed in section 4.4.4) like method to store IMSI specific timer configurations.

6. When the device connects to the network, it requests for its own timer configurations to the network as per the user application running on the device.

7. The network checks if the device can be allotted its own requested timer values (for devices having IL implemented in them) or the timer configurations specified by the AS side intelligent layer will be used.

8. The network then allocates the timer configurations to the device.

9. In this way, even though there is no intelligent layer on the device, the application server and CN are used to make the device more intelligent by providing it optimized timer configuration.

In both the cases the logic to decide the timer configurations by the intelligent layer remains the same. In brief the process is as depicted in Figure 5.3. Now we will go further into the mechanisms to see how the timers are individually configured.

5.2.3   TAU timer decision making

As seen in chapter 2, the TAU timer is used to do location updates in form of keep alive messages from the device (control layer info also sent,
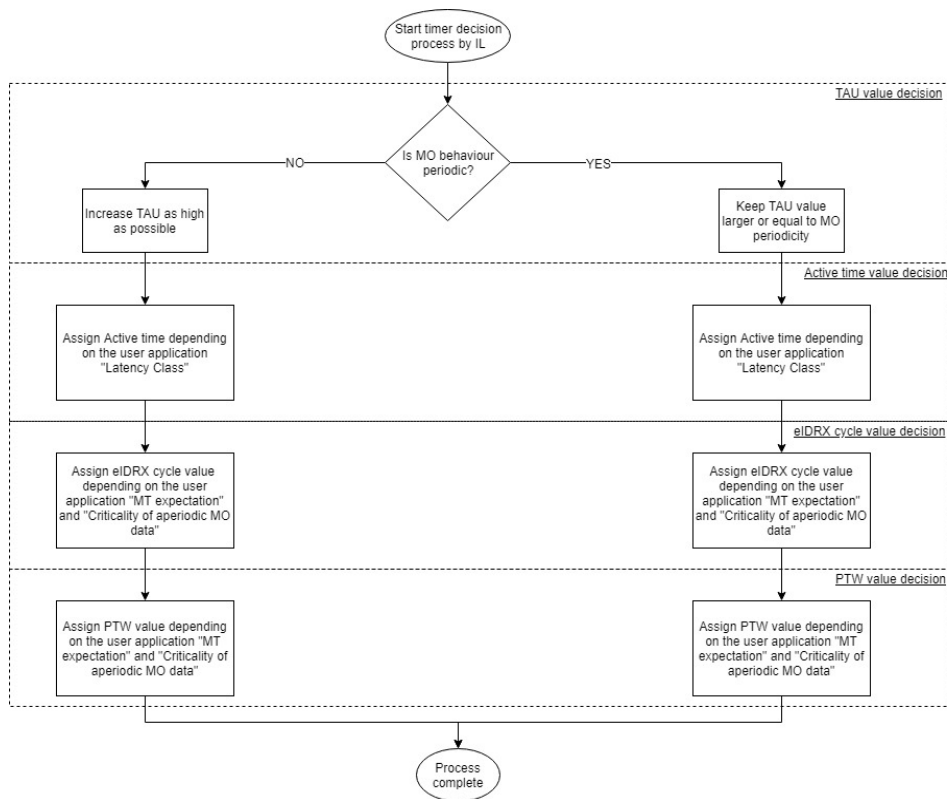
Figure 5.3: Intelligent Layer timer configuration decision.

see [3] for more info). Whenever a device has to do TAU it should first do the RRC Resume procedure to go into RRC_CONNECTED state, and then do its location update. If the device does not do the TAU procedure on time, then the network will consider the device to be not present in the network. This will result in the device being mistakenly kicked out. The way TAU procedure should be done also changes with respect to the mobility of the device. Since in this thesis we are considering the utility sector, the assumption is that the devices are not mobile, hence long TAU periods can be acceptable. It should be noted that the TAU timer gets paused on RRC_CONNECTED state and resumes counting in RRC_IDLE state. If a device sends MO data, location update also takes place simultaneously resulting in the TAU timer getting reset. Considering all these information, the IL always prefers the TAU timer to be greater than or equal to the MO data periodicity. This is done to avoid unnecessary wastage of energy consumption due to doing the RRC setup procedure twice, which would happen if TAU procedure was done before the MO periodic data is sent (and the inactive timer has passed). If the device does not send any periodic MO data, then the TAU is assigned as large value as possible. The process is depicted in Figure 5.4.
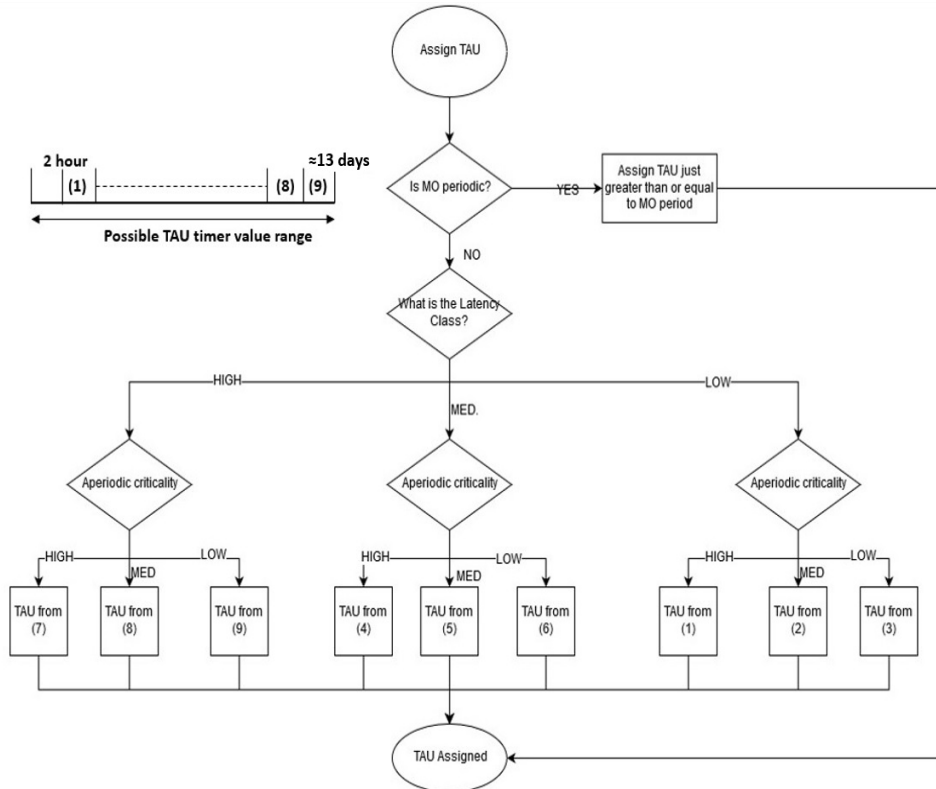
Figure 5.4: Intelligent Layer TAU timer configuration decision.

Here the IL first checks if the user application data is periodic or not, then the latency class is checked. If latency class is high it means that high latency is tolerable, in this case the TAU timer is given as large as possible. On the other hand, for low latency tolerable class the TAU timer is given as small possible to ensure lower latency in MT data communication. The TAU is further divided corresponding to the aperiodic data criticality, if the aperiodic data is highly critical then IL lowers the assigned TAU values to ensure lower latency for MT data (as it could be a response to the highly critical data). It should be noted that the IL never gives TAU timer value lower than 2 hours, as the device is not considered to be mobile. The TAU timer is allotted randomly from the chosen range of possible TAU timer values. This is done to create more diversity among the choice made for timers by the IL for the device. If the choice of TAU timer made by the IL is not randomized then the network will have more devices to be paged for a certain time period compared to the other time period. This can also be observed in section 6.2.3.

5.2.4   Active timer decision making

Active time decides the time period for which the device is available to listen for paging requests from the network. The IL tries to make the Active time to be as small as possible so that Power Saving Mode duration can be as large as possible. This is done to save device energy consumption and saving paging records of network. The deciding factor for choosing the Active time is the latency tolerance class of the device. For lower latency tolerable device a higher value of Active time is provided and vice versa. The decision making process is shown in Figure 5.5. First the IL checks the periodicity of the device and then correspondingly assigns Active time value based on the latency tolerance class of the device.

5.2.5   eIDRX cycle and PTW duration decision making

The way intelligent layer optimizes the eIDRx and PTW duration values for NB-IoT and LTE-M is different. This is due to the different ranges of NB-IoT and LTE-M for PTW. IL assigns combination of eIDRX cycle value and PTW duration such that the devices get Paging Occasions assigned to them as per the user application input parameters. For example, devices with high latency tolerance are given longer eIDRX cycle value and smaller PTW duration. This results in the decrease of number of paging opportunities that the device gets. For devices having low latency tolerance, the IL provides smaller eIDRX cycle value and longer PTW duration. This is due to the fact that with smaller eIDRX cycles and longer PTWs, the UE will have access to more paging opportunities. The decision making process for eIDRX and PTW is shown in Figure 5.6 for NB-IoT and Figure 5.7 for LTE-M.
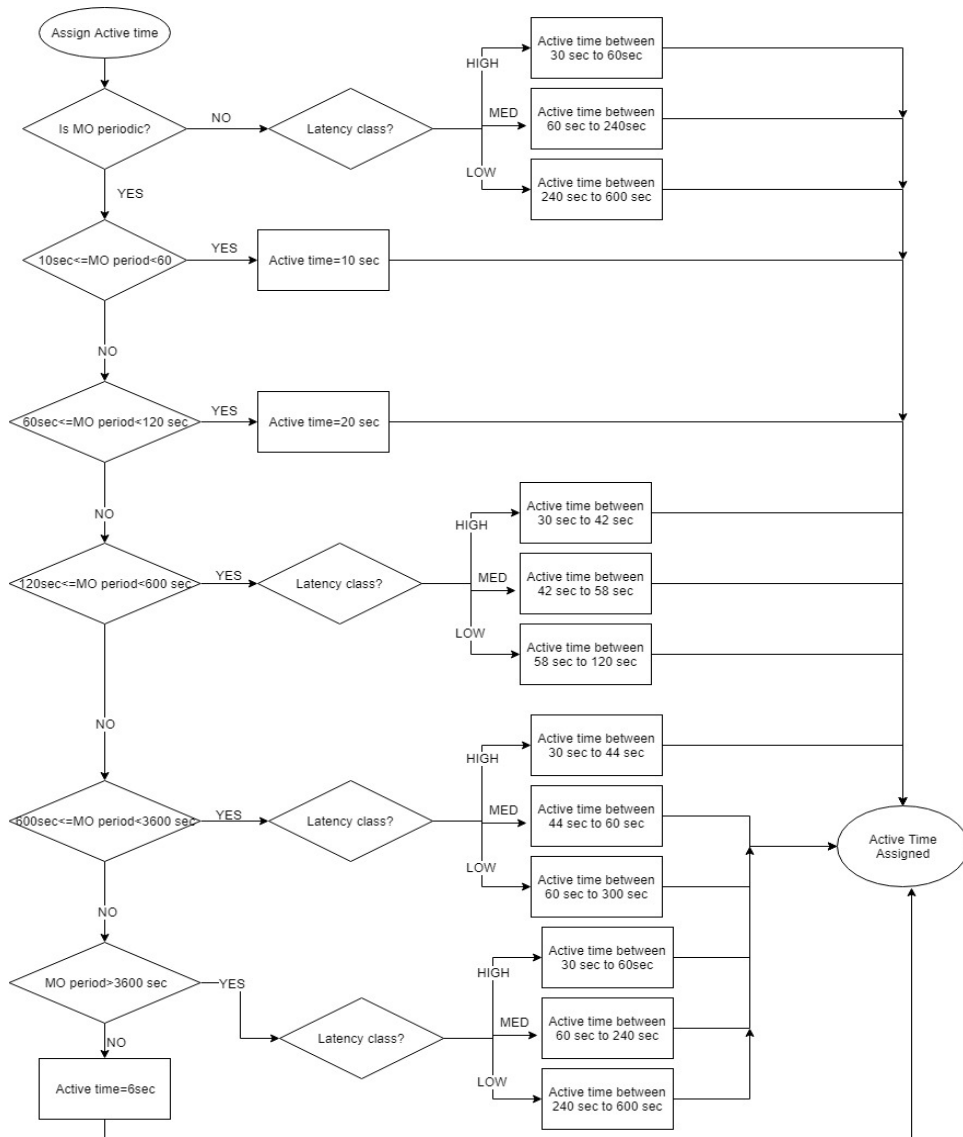
Figure 5.5: Intelligent Layer Active timer configuration decision.
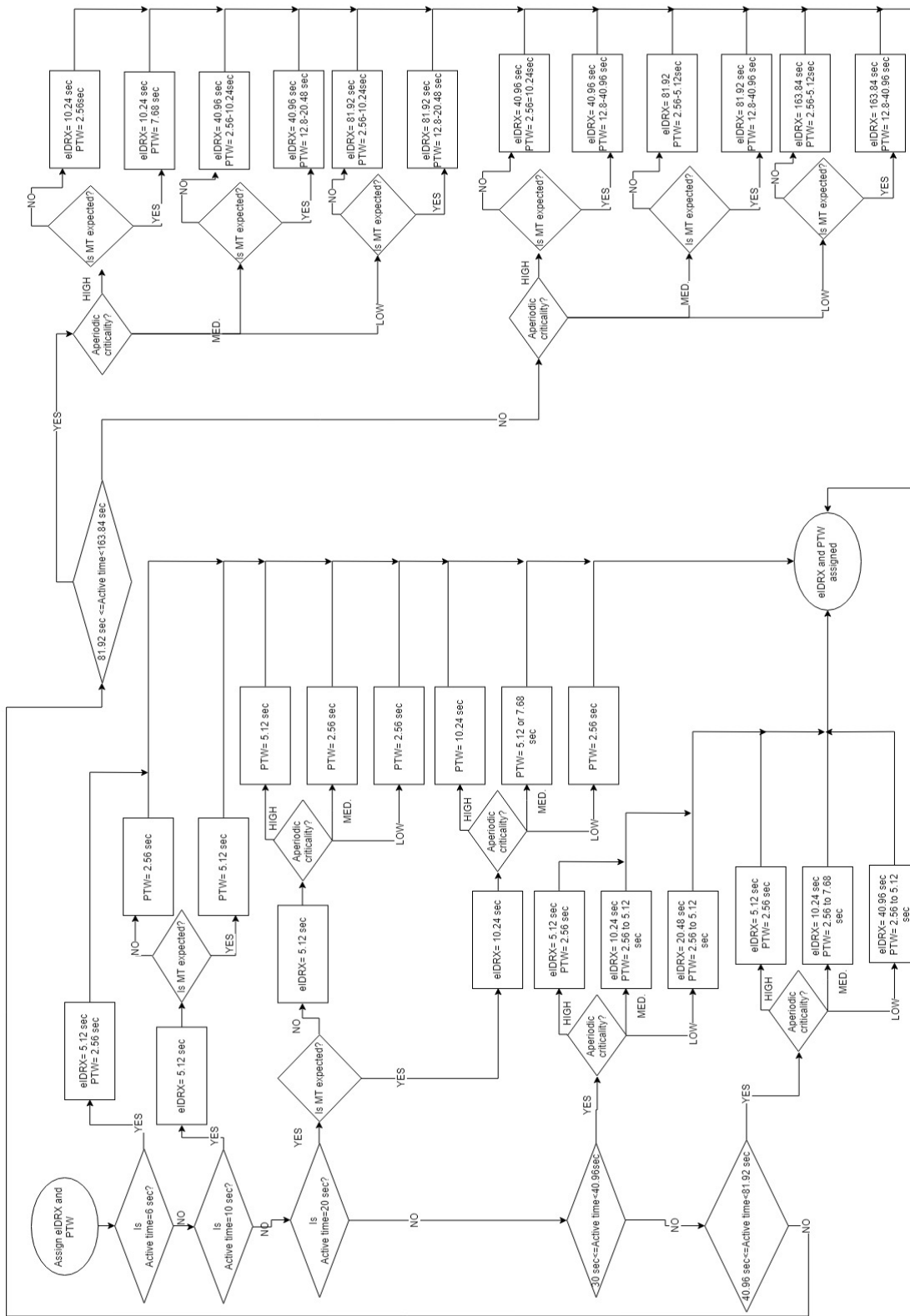
Figure 5.6: Intelligent Layer eIDRX cycle and PTW configuration decision for NB-IoT.

Figure 5.7: Intelligent Layer eIDRX cycle and PTW configuration decision for LTE-M.

Chapter 6

Verification, Results and Implementation

In the previous chapters, we have done measurements on different networks, made observations that should be kept in mind for enhancing the E2E performance and proposed an intelligent layer solution that can be implemented to improve E2E performance. In this chapter we verify if the proposed solution will work, and what are the gains and trade-offs to implement such an intelligent layer. The main obstacle in verification is the availability of devices for checking the implementation. This is due to the fact, that the intelligent layer takes decisions which will impact and improve the network behaviour as a whole. To overcome this dilemma of less number of nodes, the author has made a model in MATLAB to see the effect of intelligent layer. The model is discussed further in this chapter. After this brief introduction, the chapter delves into the verification part of the study where the author talks about the method used to verify the intelligent layer. In the verification, the metrics for which the author has modelled are also described further. Consecutively the author then talks about the comparison of the results generated, to show the effect of the intelligent layer. Finally, the author presents a real life use case for which the intelligent layer has been implemented.

6.1 Verification Method

For verifying the intelligent layer and predicting the gains, a MATLAB model has been created. The purpose of this model is to show the effect of timer configurations present on the devices using NB-IoT and LTE-M separately. The effect is in terms of total network paging records being used per second, the energy consumption of device and the latency of communication (MT data communication). The model considers a cell where there is a single eNB catering to the devices that want to communicate using the

telecom network. All the devices present in the cell are considered to use the same Radio Access Technology (either NB-IoT or LTE-M). As the interest is to show the effect of timers on the network capacity, energy consumption and latency of downlink communication, the model considers that the packets sent from eNB reach the UE on its first try. The simulation is running discretely on time domain with unit time period as 1 second. The devices keep joining the network till the number of devices joined surpasses the indicated threshold. For example, if the model intends to check for 50,000 devices then the devices keep on joining till the threshold reaches or surpasses 50,000 devices. After the threshold is reached, no more devices will join. To calculate the number of paging records consumed per second by the devices in the network, the way the downlink messages are sent is described next.

In the model, the network does not always have a downlink packet for the devices. The model defines a probability of downlink packet being present in the network for the device. This probability is further defined into two parts,

- Probability of having downlink packet in inactive time period, i.e., when the device is in RRC_CONNECTED state.

- Probability of having downlink packet in active time, i.e., when the device is in RRC_IDLE state.

Whenever the device is available to receive the downlink packets and a packet is available, one paging record is consumed. This signifies that the device was successfully sent the paging request. The model calculates the total network paging records being consumed per second by summing up the paging records being consumed by each device individually for that second. It should be noted that, as the time unit of model is in seconds, a device can consume maximum one paging record per second, which is almost the same as one cDRX cycle value (in the model 1 cDRX cycle is 128 Radio Frames or 1.28 seconds). Here, we use the information that is mentioned in [5] page 39. When DRX is used, the UE needs only to monitor one Paging Occasion (PO) per DRX cycle. This means UE can have maximum paging requests of 1 per DRX cycle. Now we look further into the metrics for which we later evaluate the intelligent layer.

6.1.1 Paging Capacity Modelling

To model the paging capacity, first the theoretical maximum and minimum values that the network can offer should be known. For calculating the paging capacity we have referred to [5] and [7].

Calculating the Maximum Paging Capacity

From the specifications, we understand that the maximum number of Sub-Frames (SFs) per Radio Frames (RFs) to do paging for both NB-IoT and LTE-M is 4. We can have 1 Paging Occasion per Sub-Frame. In 1 Paging Occasion we can have maximum 16 paging records. Each paging record can contain maximum 1 paging request for a specific device/UE. This means,

$$Paging\ Capacity\ of\ Network\ per\ second = \frac{4*16}{0.01} PR/sec = 6400\ PR/sec$$

It should be noted that this is in the case when there is always UEs available for paging and have to be paged by the network. This means that there is maximum 6400 devices can be paged by the network per second, but the timer configurations of the devices and behaviour of occurrence of downlink packets for the devices will further affect the way these 6400 paging records per second are being used.

Energy Consumption of Device

For cIoT devices, the majority of the energy saving comes form the usage of extended idle discontinuous reception and power saving mode. In power saving mode the energy consumed is much less, as the device does not listen for any paging occasions as compared to listening for paging occasions in extended idle discontinuous reception mode. Hence, to save energy the device has to:

- Increase duration of power saving mode.

- Increase duration of extended idle discontinuous reception and at the same time decrease the value of paging time window. Paging time Window can be defined as the ON period time in e-I-DRX, when the device listens for paging. In the time period except for PTW, the device does not listen for paging occasions. Please refer to Figure 2.3 to observe the relation of these timers.

Latency in communication

The timer configurations will also affect the MT data communication latency, as the network can only send for a paging request when the device is actually listening to its designated paging occasion. The maximum latency due to the timers can be accredited to the power saving mode duration. The minimum latency is the cDRX value, which is the DRX value in inactive time period. But here it should also be noted that the number of e-I-DRX cycles in the Active time period will also tell how many chances the device gets to receive the paging request. If the number of e-I-DRX cycles is less, then user has more chances of experiencing a larger delay for receiving the

MT data. Along with the e-I-DRX cycle value the duration of PTW also matters. The larger the duration of PTW, the more paging occasions the device can listen to.

6.2   Results and comparison

The model explained in the previous section is implemented in MATLAB to show the effects of the intelligent layer for the metrics explained. The aim of the comparison is to show:

- Effect of different network inactive time values on the number of total network paging records consumed per second.

- Difference between effect of timer configurations of intelligent layer and generic UE timer configurations.

- Difference between effect of timer configurations of intelligent layer and default network timer configurations.

- Difference between intelligent layer and generic user timer configurations on energy consumption of device and latency of communication.

The first case is done to show the effect of changing network inactive time, which can only be controlled by the network, for showing the effect of optimizing the network inactive time value. The second case is to show the benefits of optimizing the timer configuration that is requested by the user application. To do this we compare between the effect on total network paging records consumed, when the user application uses the intelligent layer timer configurations and when it uses the original user application timer configurations. We divide the comparisons as per the metric to be considered.

6.2.1   Effect of Inactive time on network total paging records consumed per second

Effect of changing inactive time on network paging records consumed. The Figures 6.1 and 6.6 show the plot for total number of network paging records consumed with varying inactive time duration. The inactive time values taken into consideration are 20.48 seconds, 10.24 seconds and 5.12 seconds. The result is shown using the generic user application timer configurations and total number of devices being 10,000, 50,000 and 100,000. Majority of the devices are joining in the initial moments, hence we observe the high peak, but after the devices have joined and enter RRC_IDLE state according to the inactive time, the total network paging records consumed decreases to a stable region of values. This decrease is due to the fact that all the devices are observing paging occasions as per their own timer configurations.

The effect of inactive timer on network paging records consumed is seen to increase as the number of devices in the network increases. Both for the cases of NB-IoT and LTE-M, in case of 10,000 devices when inactive time is changed from 20.48 sec to 5.12 sec, around **750 extra devices are pageable per second** . For 100,000 devices when inactive time is changed from 20.48 sec all devices cannot be accommodated by the network as the maximum goes above 6400 paging records per second. But when the inactive time changes to 5.12 sec, around **750 extra devices are pageable per second**.
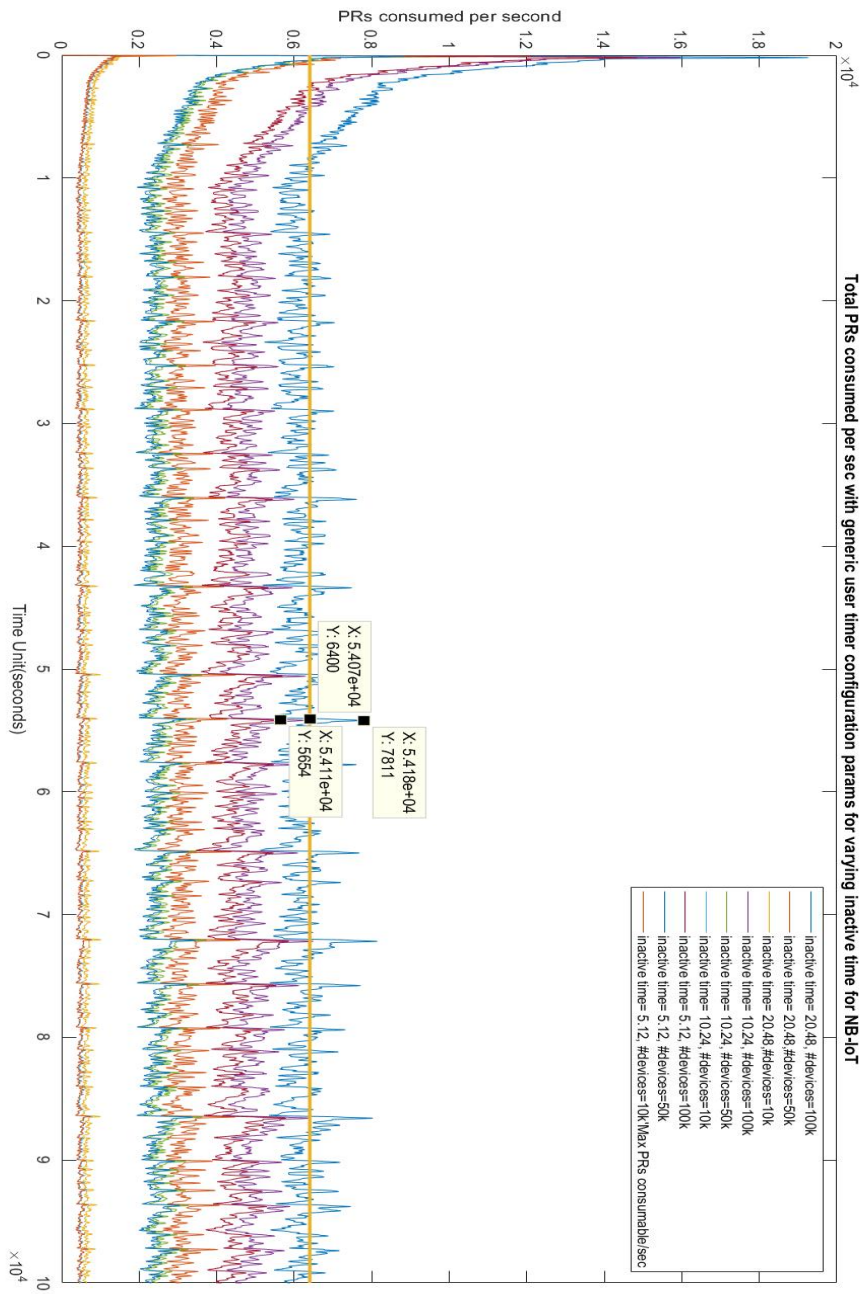
Figure 6.1: Effect of changing inactive time on total network paging record consumed for NB-IoT.
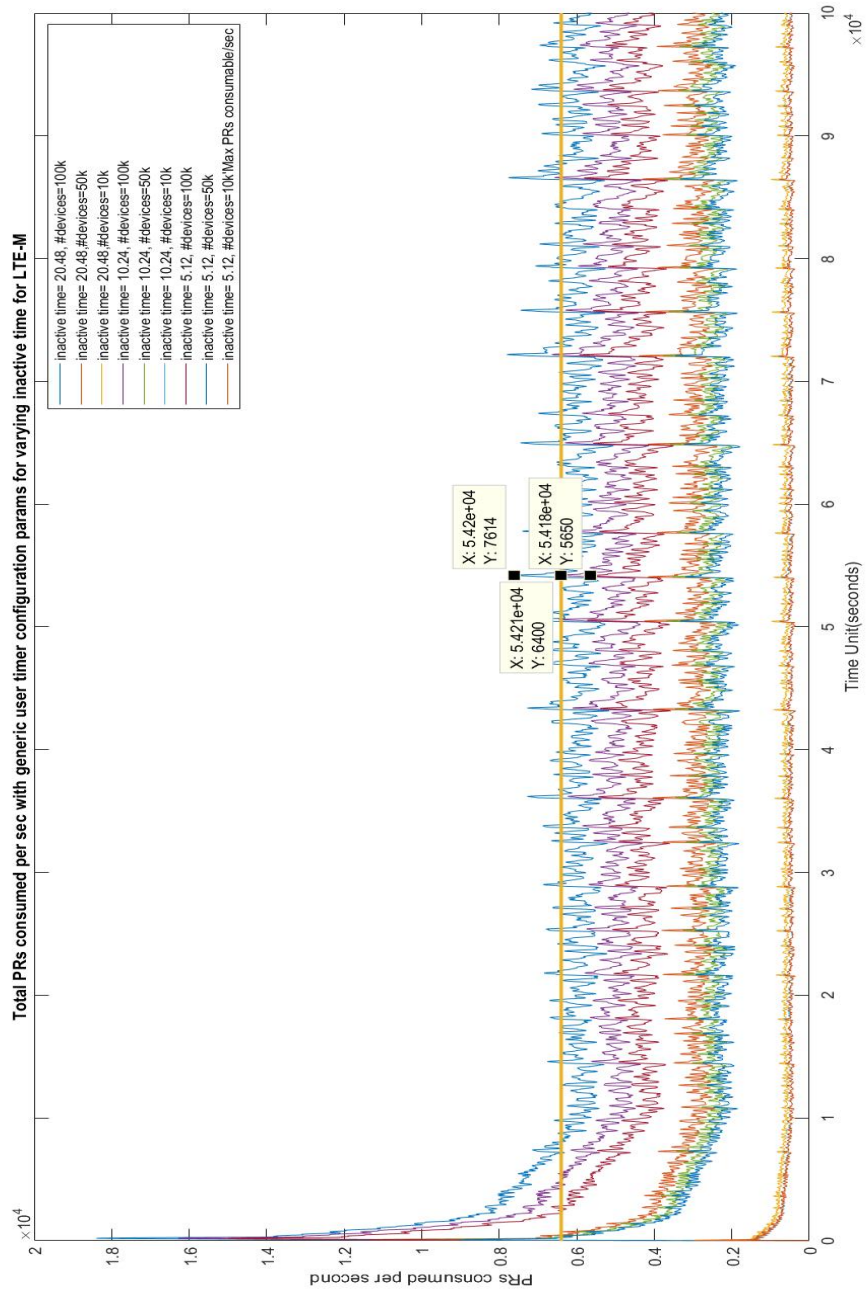
Figure 6.2: Effect of changing inactive time on total network paging record consumed for LTE–M.

47

6.2.2 Difference between IL timer configurations and generic user application timer configurations

Here it should be noted that the user application is always requesting for valid timer configurations (i.e., TAU duration > Active time duration > e-I-DRX cycle value > PTW duration). The user application requests for random timer values while supplying the intelligent layer the four input parameters: MO periodicity, MO aperiodic data criticality, latency tolerance class and MT data expected or not for the application.

Just as observed before for both NB-IoT (Figure 6.3) and LTE-M (Figure 6.4), the majority of the devices are joining in the initial moments of the simulation, we observe the high peak. But after the devices have joined and enter RRC_IDLE state according to the inactive time, the total network paging records consumed decreases to a stable region of values. In the stable region we can see that the number of extra devices pageable for **NB-IoT** is around **2.1 times** (when considering 6400 as maximum PRs/sec), and for **LTE-M** is around **2.38 times** (when considering 6400 as maximum PRs/sec) for devices using intelligent layer compared to using the generic user application timer configurations. The extra increase in number of extra devices for LTE-M is due to the different range of values for PTW when compared with NB-IoT. For NB-IoT the range is from 2.56 seconds to 40.96 seconds, and for LTE-M the range is from 1.28 seconds to 20.48 seconds, referred to [2].

6.2.3 Difference between IL timer configurations and network default timer configurations

When the UE joins the network, it is provided with default network timer configurations. If the user application does not request any timer configurations, but just enables eDRX and PSM then the default network timer configurations are used.

The Figures 6.5 and 6.6 shows the effect on the network paging records being consumed when the user application uses the timer configurations provided by the intelligent layer and when it uses the default network timer configurations. From the figures we observe that if the devices use the network default timer values, then there are certain periods of time when the number of paging records consumed is very high and then some periods where no paging records are consumed. This is due to the fact that all the devices have same timer configurations, leading to an identical pattern of paging record consumption will be generated. This is prevented by the use of the intelligent layer where the way the timers configurations are assigned have some randomness associated. Hence such a pattern of paging record consumption is not created, leading to a much more uniform consumption of paging records over time for both LTE-M and NB-IoT.
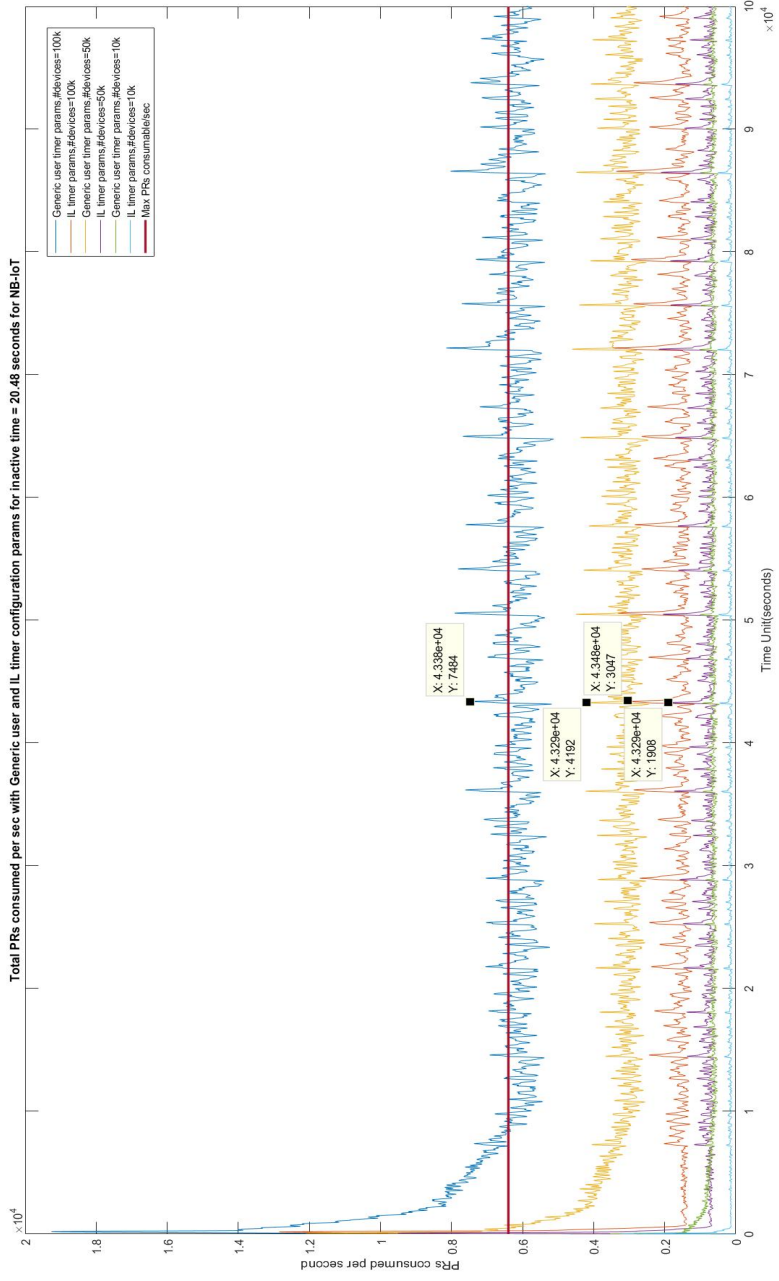
Figure 6.3: Effect of using generic user application and IL timer configurations on total network paging record consumed for NB-IoT.
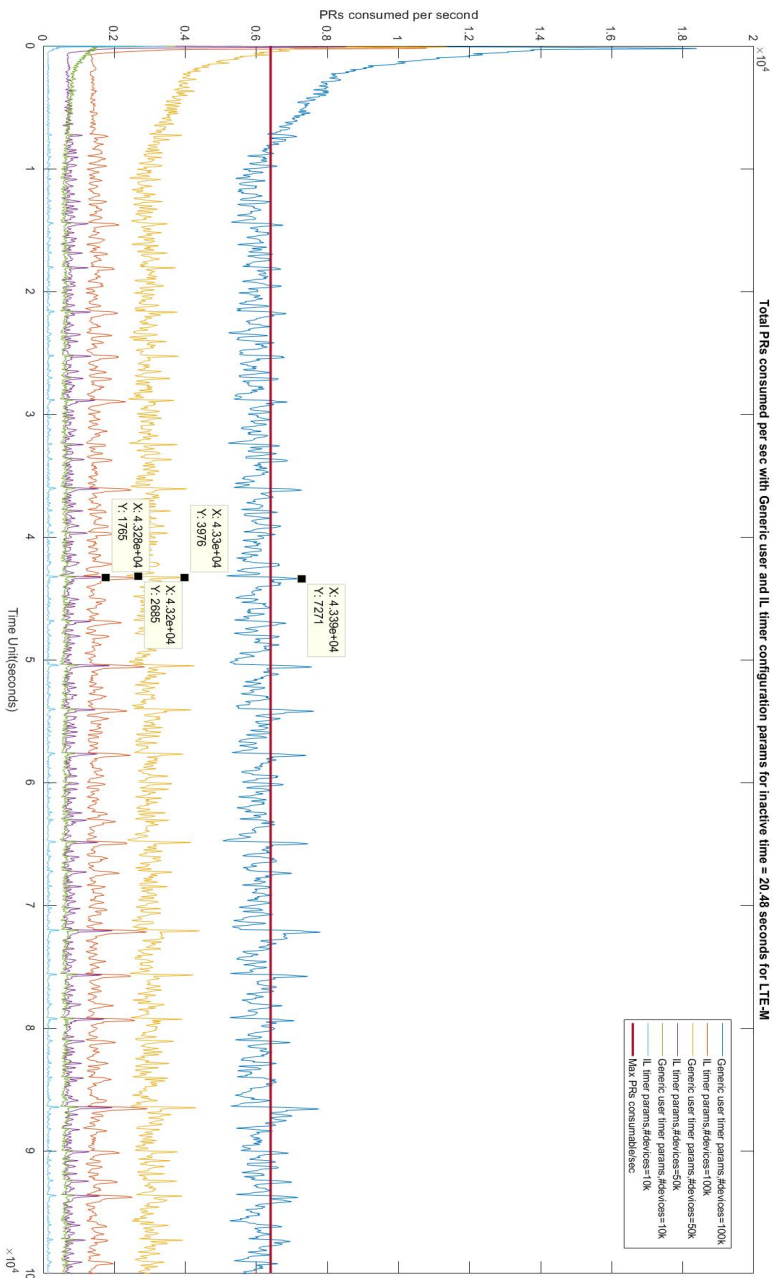
Figure 6.4: Effect of using generic user application and IL timer configurations on total network paging record consumed for LTE-M.
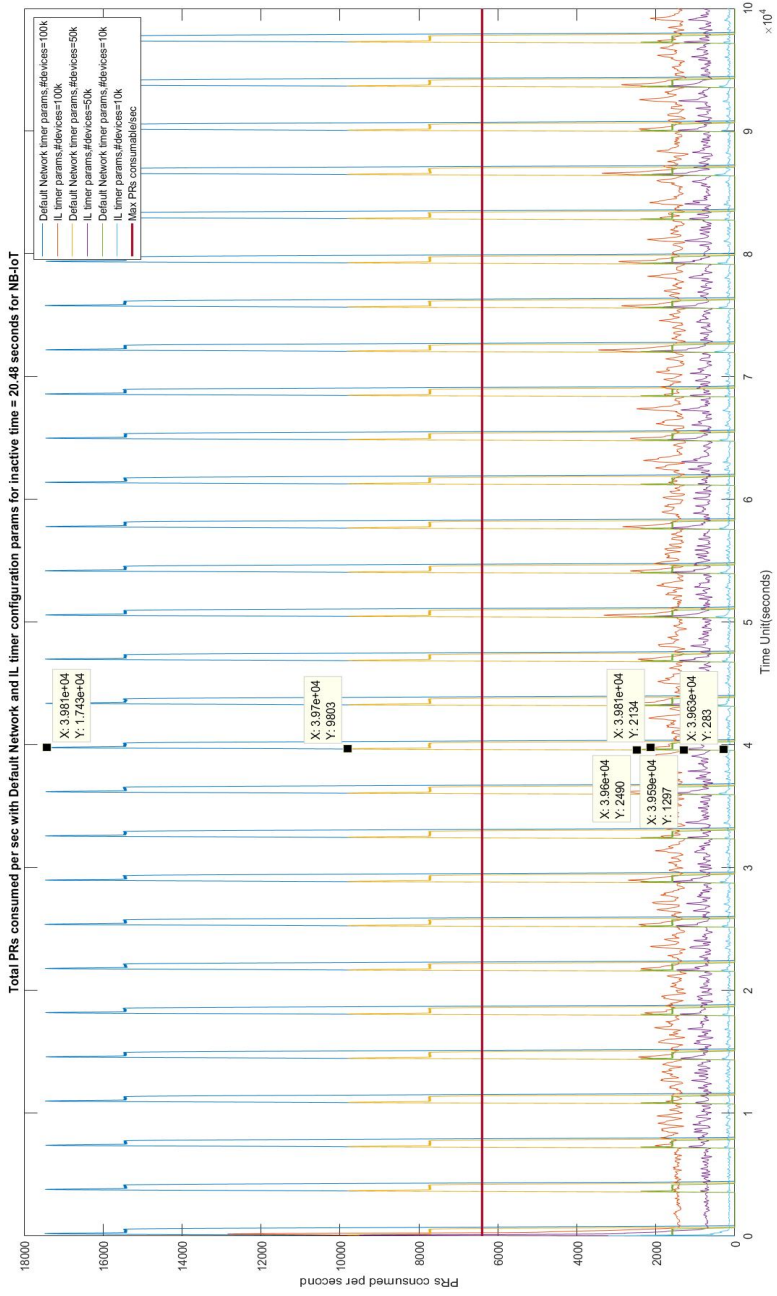
Figure 6.5: Effect of using network default and IL timer configurations on total network paging record consumed for NB-IoT.
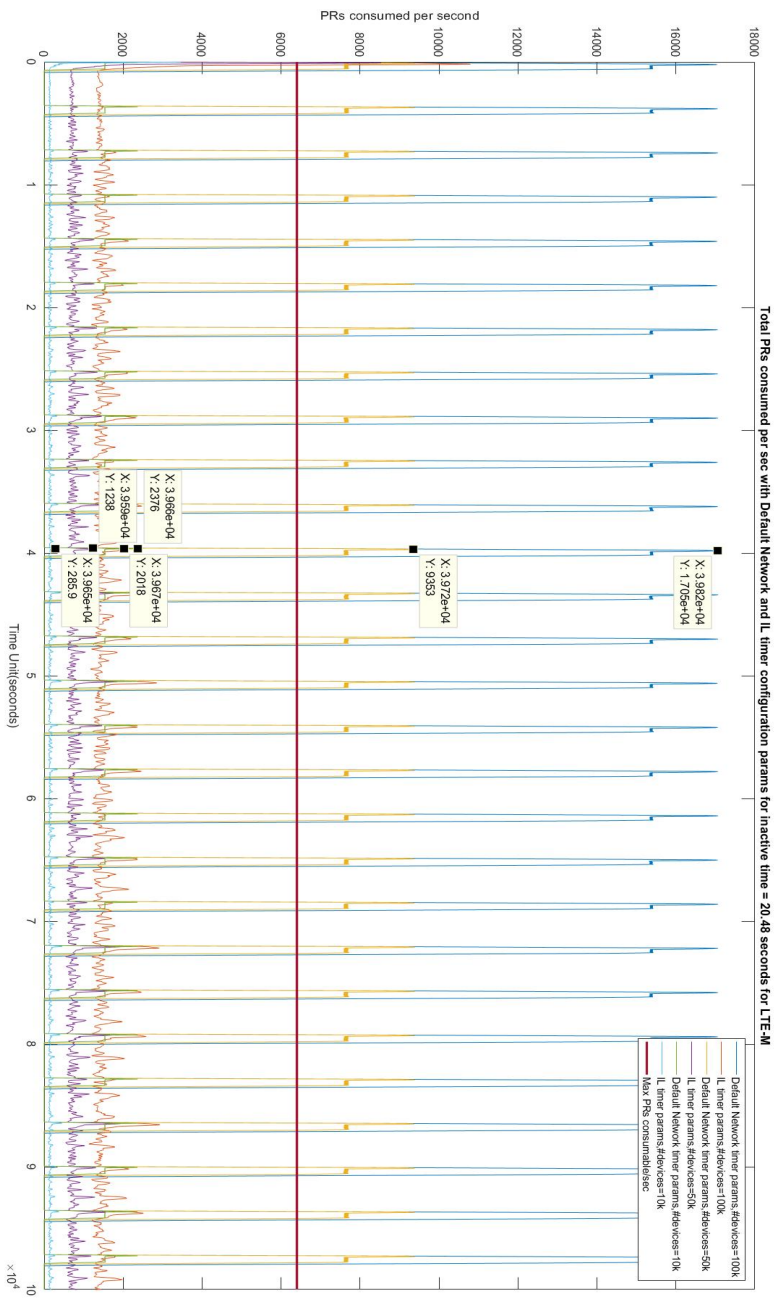
Figure 6.6: Effect of using network default and IL timer configurations on total network paging record consumed for LTE-M.

52

6.2.4 Effect of Intelligent Layer on Energy Consumption of Device and Latency of Communication

For observing the effect of generic timers versus the intelligent layer timers on energy consumption of the device, we use the datasheet provided for Quectel BG96 [19]. The effect of timers affects the RRC_IDLE mode, hence we are interested in the effect of energy consumption due to changing TAU, Active time, e-I-DRX cycle value and PTW duration. The energy consumption of the module as per the datasheet is shown in Table 6.1.

NB-IoT	
State	Current Consumption
PTW	15 mA
eIDRX Off Duration	1.1 mA
PSM	10 μA
LTE-M	
State	Current Consumption
PTW	15 mA
eIDRX Off Duration	1.2 mA
PSM	10 μA

Table 6.1: Energy consumption of BG96 module

To calculate the energy consumption of the cellular module, the voltage consumption is taken as 3.3 Volts. The formula to calculate energy consumption in 1 TAU cycle, if the device does not do any MO data transmission and does not receive any MT data is,

$$EnergyConsumption = (P_{PTW}T_{PTW} + P_{eIDRXOff} + T_{eIDRXOff})N_{eIDRX} + P_{PSM}T_{PSM} \tag{6.1}$$

where,

P_{PTW}	Power consumption in PTW
T_{PTW}	Time duration of PTW
$P_{eIDRXOff}$	Power consumption in eIDRX off duration
$T_{eIDRXOff}$	Off state time duration of eIDRX
N_{eIDRX}	number of eIDRX cycles
P_{PSM}	Power consumption in PSM
T_{PSM}	Time duration of PSM

With the implementation of the intelligent layer, the effect for user applications that sends and receives high priority aperiodic data, expect downlink data and has indicated low tolerance to latency is:

- On average the number of eIDRX cycles in an active time is increased by 1.87 times. The eIDRX cycle duration on average is increased by 1.57 times. This means the device is now available to receive downlink data more often when compared to generic user timer configurations.

- In order to try and save energy, the paging time window length on average is decreased to 0.73 times of original paging time duration.

- The power saving mode duration is increased by 1.69 times, to further facilitate the power saving of the device.

The effect on timers when the user application sends and receives low priority aperiodic data, expects downlink data and has indicated high tolerance to latency is:

- On average the number of eIDRX cycles in an active time period is decreased to 0.28 times of original number of eIDRX cycles. The eIDRX cycle duration on average is increased by 1.65 times. On average the paging time window is decreased to 0.44 times the original value. This means that there will be lesser power consumption due to the lesser time the device is available for receiving paging occasions.

- In order to further save energy, the power saving mode duration is increased to 1.86 times of its original duration.

From the two cases above, we observe that if the user application has high priority data to communicate, then more energy will be expended to listen for paging. In deployments, it is expected that most of the communication is device originated. Hence most of the times the response from server is sent after the device sends uplink data, which means the device should be in RRC_IDLE or in listening to paging occasions as per its active time. This implies that the increase in PSM to save energy should not have a severe impact on delay downlink data communication. As the device is listening for paging more often the energy consumed by device also increases. This is trade-off for decreasing the latency of downlink data communication. In the second case low latency is tolerable by the user application. Hence the intelligent layer tries to maximize energy saving to increase the battery life at the expense of increased delay for downlink data. To see the effect on energy consumption an example can be taken. In this example the user timer settings when not using an intelligent layer is:

- Paging time window: 10.24 seconds

- eIDRX cycle value: 20.48 seconds

- Active time: 300 seconds/ 5 minutes

- TAU period: 4 hours

This is the example of a device which sends uplink after every 4 hours and after every uplink is available for 5 minutes to receive paging from network. By using the energy consumption information given in 6.1, we calculate the energy consumption for a TAU period. In case of using the timer settings provided by the user application the energy consumption is **8.08 Joules**. When using the intelligent layer there can be many timer configuration possible, here we will take the case of the two cases explained earlier:

- When the user application states the conditions as in the first case (low latency tolerance, aperiodic data communication is high priority and downlink is expected), the energy consumption is **12.893 Joules**. This means that the now the device will expend more energy in order to give a better performance in terms of latency of downlink data communication for the high priority data.

- If the user application states the conditions as in the second case (high latency tolerance, aperiodic data communication is low priority and downlink is expected), the energy consumption is **2.14 Joules**. This means the intelligent layer prioritised the saving of energy consumption while incurring higher latency for downlink data.

6.3 Implementation in Real Life Use Case Scenario

To show that the intelligent layer is implementable in real life use cases, the intelligent layer logic for the UE side implementation has been created. This section will discuss the implementation and the use case of the device. The device is created using the Nucleo L476 RG as the base. On top of the Nucleo, Dragino BG96 is used for using NB-IoT and LTE-M. The Nucleo is running mbed OS, which will use the cellular drivers and the intelligent layer logic we have created. The setup along with the device architecture can be seen in Figure 6.7.

The application running on top of the mbed OS uses the intelligent layer to request timer configurations as per its needs. To do this, the user application provides input information such as periodicity of uplink, criticality of aepriodic data, latency tolerance of the user application and if downlink is expected or not by the user application to the intelligent layer. As per the inputs received from the user application, the intelligent layer interacts with the cellular drivers to communicate with the cellular modem via AT commands over UART. The cellular modem then requests the cellular network for the optimal timer configurations that it received from the intelligent layer. After the network has assigned the timer configurations to the

device, the user application then continues running its own logic. It should be noted that the intelligent layer is designed such that it can be used with any cellular modem. This is due to the intelligent layer not directly sending AT commands to the cellular modems, but using the cellular modem drivers to send the commands. For example, if the intelligent layer wants to initialize the device and join a network, it will use a function *initializeDevice()*. But the definition of *initializeDevice()* will be using functions from cellular modem driver files as per the cellular modem being used. For this use case we used the cellular driver that we made for BG96. But drivers for other cellular modems can also be used to interact with the intelligent layer. One of the biggest benefits of intelligent layer is its ability to request the optimized timer configurations without application being aware of the network timers and what is the effect of changing these timers. When using the intelligent layer, the user only needs to know the application requirements making development simpler and more efficient.
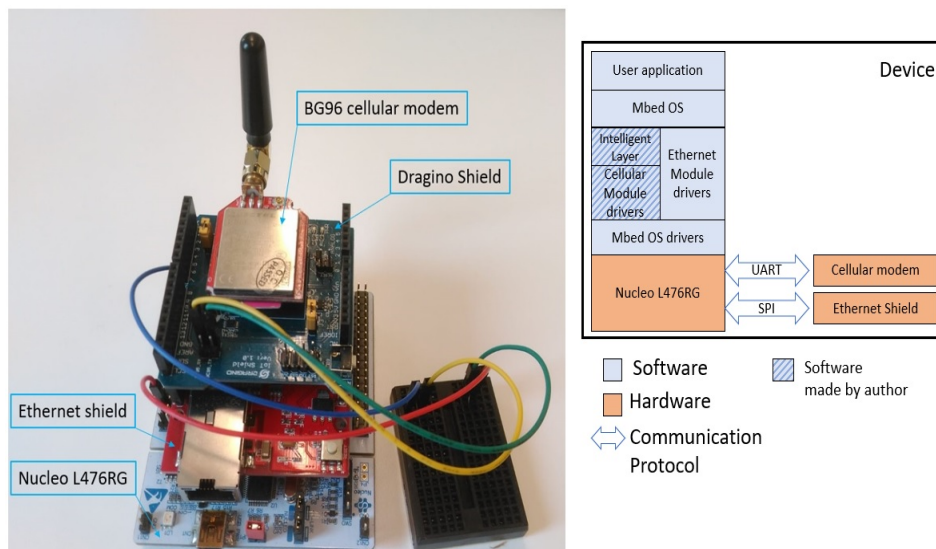
Figure 6.7: Device Hardware and Software Setup.

For the use case the device needs to interact with the critical application device (uses Ethernet for communication) in the substation, hence an Ethernet shield is also needed. Using the above device, the following use case is tackled:

Instead of having the critical application device connect to the network with Ethernet cable to the optical fibre network or use GPRS, our device is used to give it cellular IoT connectivity. For this use case LTE-M is used as we get a public IP address that helps to communicate with the server. The overall communication flow is shown in Figure 6.8. The job of our device is to activate the critical application device and help it send data to the

56

server using the cIoT network. The application running on top of the mbed OS talks to the critical application in the substation via the Ethernet shield and to the server using the cellular modem on the Dragino. As shown in the Figure 6.7, the application on top of the running on top of the mbed OS talks to the cellular drivers of Dragino module using the intelligent layer. We have tested the device and noticed that it is able to successfully deliver the data from server to critical application device and vice versa (logs in Appendix C). Our device can also be used for critical infrastructure in substations which don't have the optical fibre connectivity. In this case we can use the cIoT connection instead of GPRS (as all the critical infrastructure devices have Ethernet ports to connect to the Ethernet shield on our device).
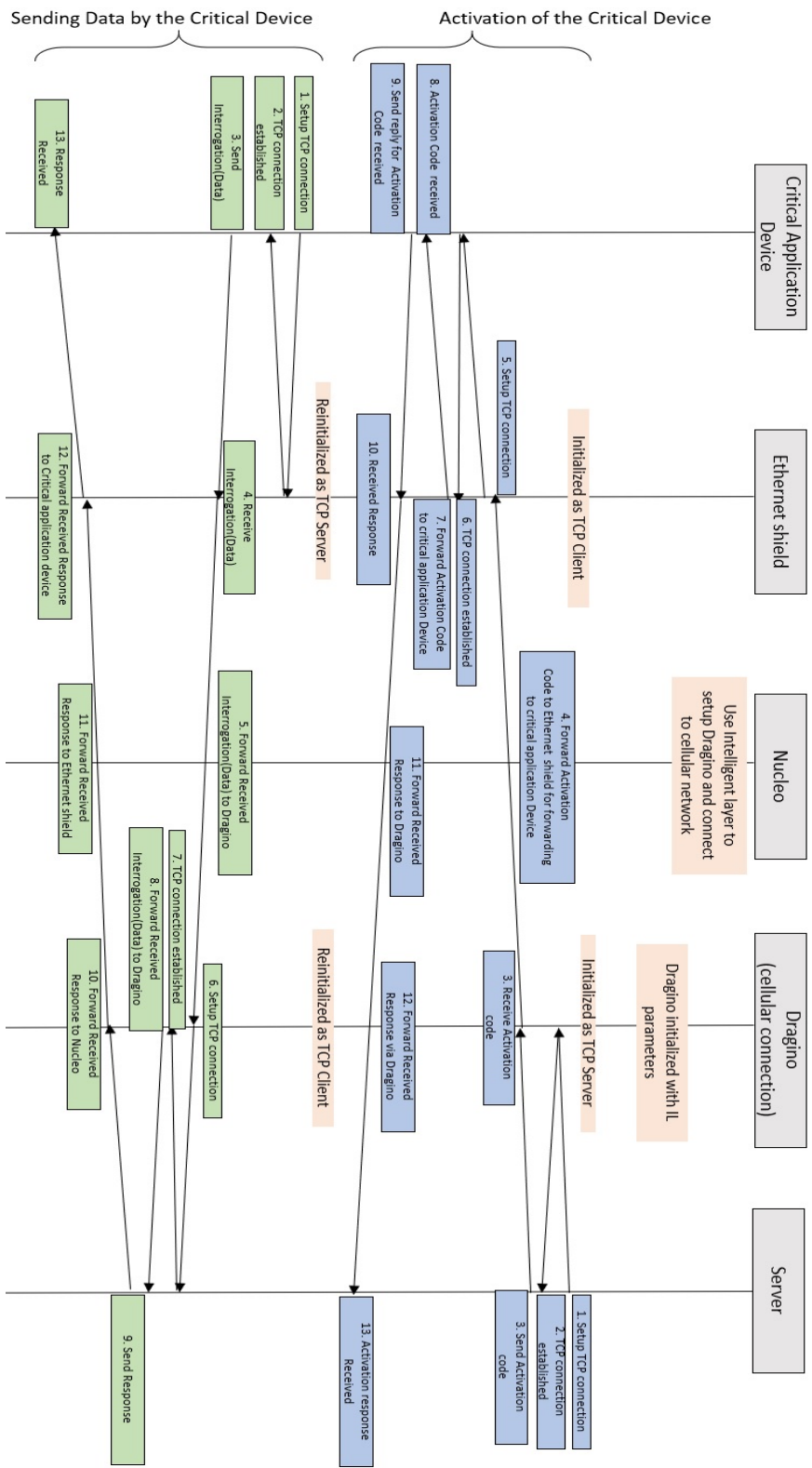
Figure 6.8: Waterfall Diagram for User Application working.

Chapter 7

Conclusions and Future Work

7.1 Conclusions

The work done in this thesis shows the effect of optimizing the way device behaves, will improve the network behaviour. The intelligent layer used in the device shows the result to be more than **2 times** improvement in the number of pageable devices that can be maintained in the network. This will ultimately contribute to the massiveness of the network. With this thesis, the current network deployments have been studied for multiple networks to show network and device level behaviours. These behaviours when kept in mind alongwith the 3GPP IP and non-IP data flows, help in identifying the key areas of improvement using the intelligent layer. To show the validity of intelligent layer in real life implementation, we have implemented the intelligent layer for real life critical applications in substations of Stedin.

Hence the thesis demonstrates a plausible solution to improve the E2E communication to improve massiveness of the network by changing parameters of the device.

7.2 Future Work

The thesis suggests the following points that can be done in the future to further improve the E2E performance:

- Giving more preference to SINR for re selecting cells from UE side.

- The intelligent layer can be used for implementing the prioritised downlink data transmission on AS while knowing the availability of device, to improve the reliability of communication and decrease the load on the network.

Bibliography

[1] 3GPP. Etsi ts 123 682 v14.8.0 (2018-06). `https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=862`, 2019. [Online; accessed 10-September-2019].

[2] 3GPP. Etsi ts 124 008 v14.8.0 (2019-01). `https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1015`, 2019. [Online; accessed 10-September-2019].

[3] 3GPP. Etsi ts 124 301 v14.10.0 (2019-01). `https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1072`, 2019. [Online; accessed 10-September-2019].

[4] 3GPP. Etsi ts 136 214 v14.4.0 (2018-01). `https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2428`, 2019. [Online; accessed 10-September-2019].

[5] 3GPP. Etsi ts 136 304 v14.7.0 (2018-10). `https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2432`, 2019. [Online; accessed 10-September-2019].

[6] 3GPP. Etsi ts 136 321 v14.11.0 (2019-07). `https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2437`, 2019. [Online; accessed 10-September-2019].

[7] 3GPP. Etsi ts 136 331 v14.10.0 (2019-05). `https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2440`, 2019. [Online; accessed 10-September-2019].

[8] Hilal Bello, Xin Jian, Yixiao Wei, and Min Chen. Energy-delay evaluation and optimization for nb-iot psm with periodic uplink reporting. *IEEE Access*, 7:3074–3081, 2019.

[9] Marwa Chafii, Faouzi Bader, and Jacques Palicot. Enhancing coverage in narrow band-iot using machine learning. In *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6. IEEE, 2018.

[10] Dragino. Dragino webpage. `https://wiki.dragino.com/index.php?title=NB-IoT_Shield`, 2018. [Online; accessed 14-December-2018].

[11] ANAND Haridas, Vijay S Rao, R VENKATESHA Prasad, and CHAYAN Sarkar. Opportunities and challenges in using energy-harvesting for nb-iot. *ACM SIGBED Review*, 15(5):7–13, 2018.

[12] Taehoon Kim, Dong Min Kim, Nuno Pratas, Petar Popovski, and Dan Keun Sung. An enhanced access reservation protocol with a partial preamble transmission mechanism in nb-iot systems. *IEEE Communications Letters*, 21(10):2270–2273, 2017.

[13] Mads Lauridsen, Huan Nguyen, Benny Vejlgaard, István Z Kovács, Preben Mogensen, and Mads Sorensen. Coverage comparison of gprs, nb-iot, lora,

and sigfox in a 7800 km² area. In *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, pages 1–5. IEEE, 2017.

[14] ST Microelectronics. Nucleo l476rg webpage. `https://www.st.com/en/evaluation-tools/nucleo-l476rg.html`, 2018. [Online; accessed 14-December-2018].

[15] Konstantin Mikhaylov, Martin Stusek, Pavel Masek, Vitaly Petrov, Juha Petajajarvi, Sergey Andreev, Jiri Pokorny, Jiri Hosek, Ari Pouttu, and Yevgeni Koucheryavy. Multi-rat lpwan in smart cities: Trial of lorawan and nb-iot integration. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2018.

[16] V. Nair, R. Litjens, and H. Zhang. Assessment of the suitability of nb-iot technology for orm in smart grids. In *2018 European Conference on Networks and Communications (EuCNC)*, pages 418–423, June 2018.

[17] The Things Network. The things network webpage. `https://www.thethingsnetwork.org/`, 2019. [Online; accessed 02-September-2019].

[18] Sung-Min Oh and JaeSheung Shin. An efficient small data transmission scheme in the 3gpp nb-iot system. *IEEE Communications Letters*, 21(3):660–663, 2017.

[19] Qualcom. Bg96 webpage. `https://www.quectel.com/product/bg96.htm`, 2018. [Online; accessed 14-December-2018].

[20] Sodaq. Sodaq sara sff ublox r410m webpage. `https://shop.sodaq.com/sodaq-sara-sff-r410m.html`, 2018. [Online; accessed 14-December-2018].

Appendix A

Delay Methodology

The flowchart in Figure A.1 shows the delay calculation method.

Figure A.1: Delay Calculation Methodology

Appendix B

Flowcharts for IP and non-IP data delivery

Figure B.1: MT data communication flow for IP and non-IP using S11-U Control Plane (part 1)

65

Downlink Buffering Requested to the S-GW in the Downlink Data Notification Ack msg, containing Downlink Buffering Duration time and optionally Downlink Buffering Suggested Packet Count

NO

Is the UE registered to MME considered to be reachable(estimate)?

Reachability of UE will depend on:
1. Timer configuration
2. Mobility of UE
3. what else?

Paging Priority:
-> Only included if Downlink Data Notification had an ARP priority level associated with priority services
-> One paging priority level can be used for multiple ARP priority level values
-> During a congestion situation the ENB may prioritise the paging of UEs according to the Paging Priority indications
-> If MME sent Paging Request without Paging Indication, and now receives a Downlink Data notification with ARP priority ,then MME will send another Paging Request with the new PAging Priority

YES

Send Paging Message to each eNB belonging to the same TAC
NAS ID for paging, TAI(s), UE identity-based DRX index, Paging DRX length, list of CSG IDs for paging, Paging Priority indication, Enhanced Coverage Restricted, CE mode B Restricted

Paging Strategies may be configured in MME
(Page 181, 23.401 v14.10.0)

If the information on Recommended Cells and eNBs is available to MME, it uses it to determine the eNBs for paging.
The MME may transparently convey the information on recommended cells to the eNB.
The MME may include in the S1AP Paging msg(s) the paging attempt count information.

eNB pages the UE

If there is C-IoT control Plane optimisation then there is no Data radio bearer establishment by the MME and the MME can immediately send Downlink Data it receives using a NAS PDU to the eNodeB
MME uses a timer to expect the response from UE, if no response is obtained then MME may repeat using an applicable paging strategy

on receiving paging msg, sends Control Plane Service Request NAS message over RRC Connection request and S1-AP initial message.

eNB retreives the EPS negotiated QoS profile for the UE.
eNB may apply prioritisation between requests from different UEs

Figure B.2: MT data communication flow for IP and non-IP using S11-U Control Plane (part 2)

66

Figure B.3: MT data communication flow for IP and non-IP using S11-U Control Plane (part 3)

The MME encrypts and integrity protects Downlink data and sends it to the eNodeB using a NAS PDU carried by a Downlink S1-AP message

For IP PDN type PDN connections configured to support Header Compression, the MME shall apply header compression before encapsulating data into the NAS message

for the NAS PDU retransmission strategy, with CE, the MME should take into account the transmission delay of the NAS PDU and the CE mode B Restricted parameter stored in MME's MM context and if applicable, the CE mode, i.e. set the NAS timers long enough according to the worst transmission delay.

The UE receives NAS PDU with data via a Downlink RRC msg.
This is taken as implicit ack of the Service Request msg.
If header compression was aplied, to the PDN, the UE shall perform header decompression to rebuild the IP header.

more uplinks and downlinks can take place while the RRC connection is up

NAS inactivity timer expired?

YES

NO

eNB initiates the S1 release procedure.

The UE and MME shall store the ROHC configuration and context for the uplink/downlink data transmission when entering the ECM_CONNECTED state next time

Figure B.4: MT data communication flow for IP and non-IP using S11-U Control Plane (part 4)

The eNB sends a NAS Delivery indication to MME if requested.

was the delivery a failure?

NO

YES

if data was received over T6a interface, MME responds to SCEF

If eNB doesnt support S1-AP NAS delivery, MME indicates a cause code 'Success Unack Delivery' or 'Success Ack Delivery' for the the SCEF to know if reliable delivery was possible or not.

eNB sends an unsuccessful delivery with S1-AP NAS Non Delivery Indication

wait for sometime until the UE has potentially changed cell and re-established contact.

Resend the Downlink S1-AP msg to the eNB

Report unsuccessful delivery to SCEF in case of T6a procedure
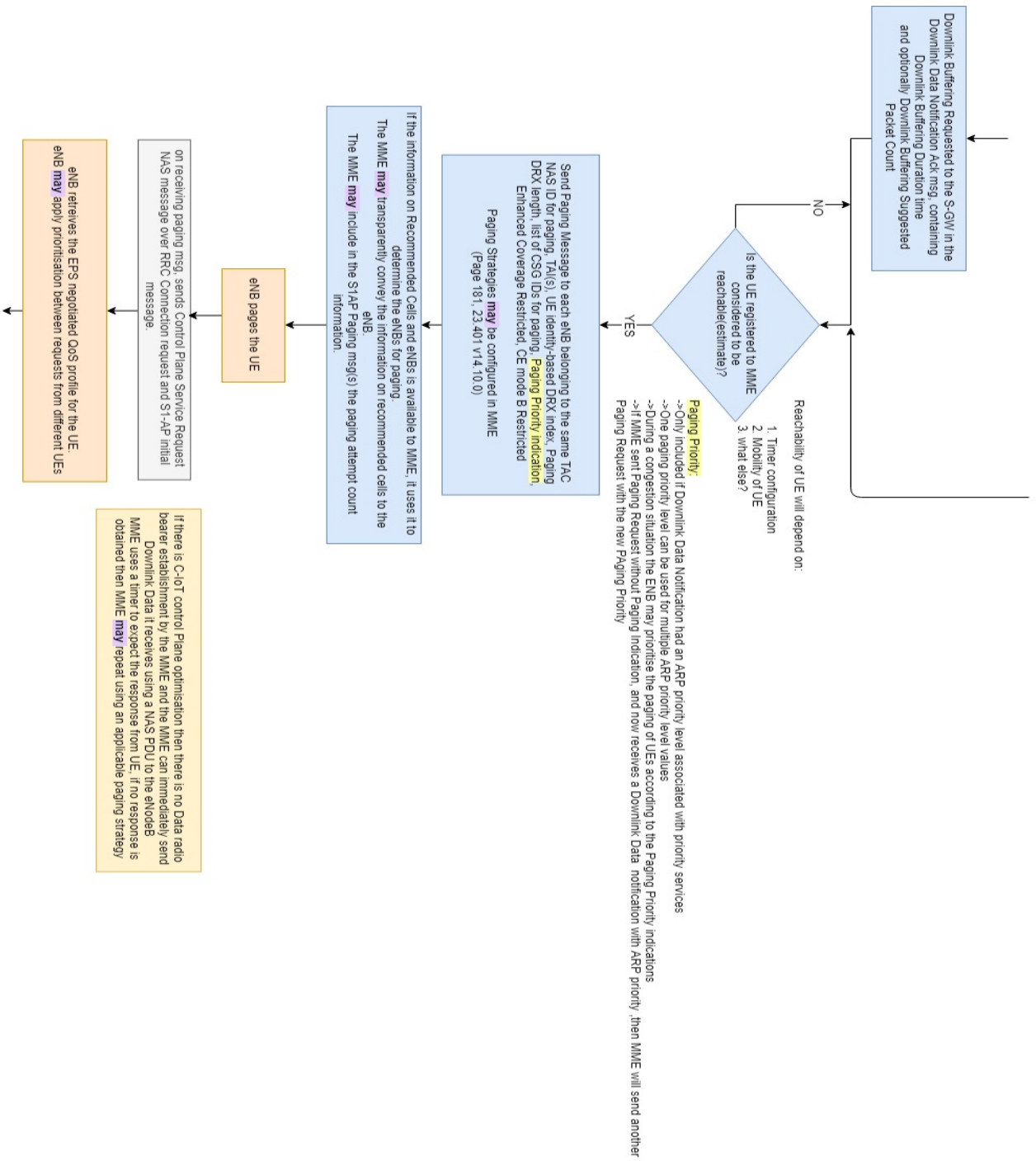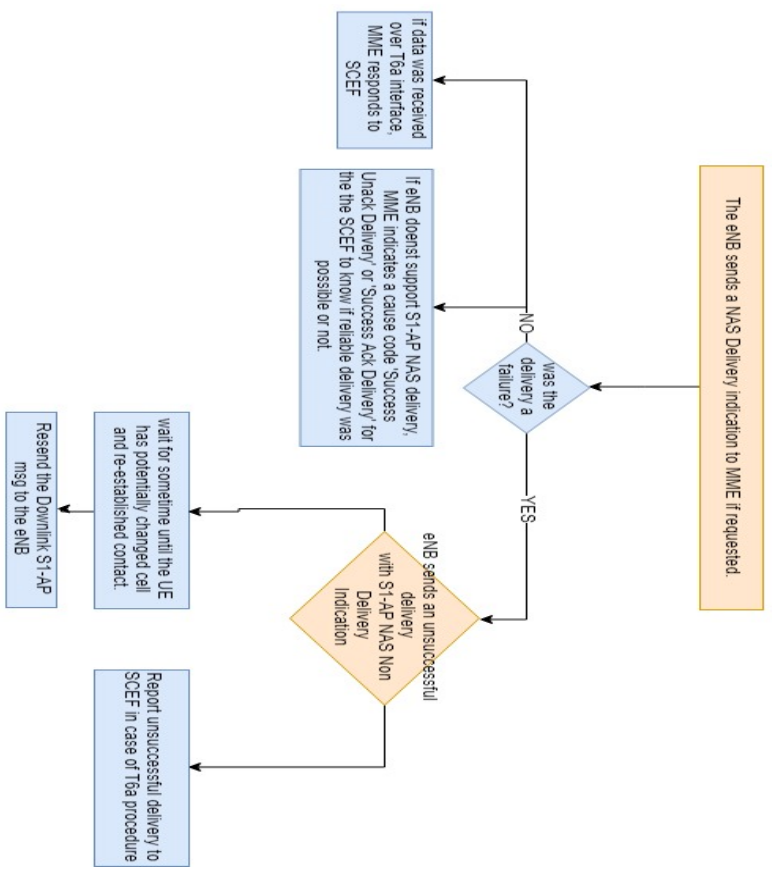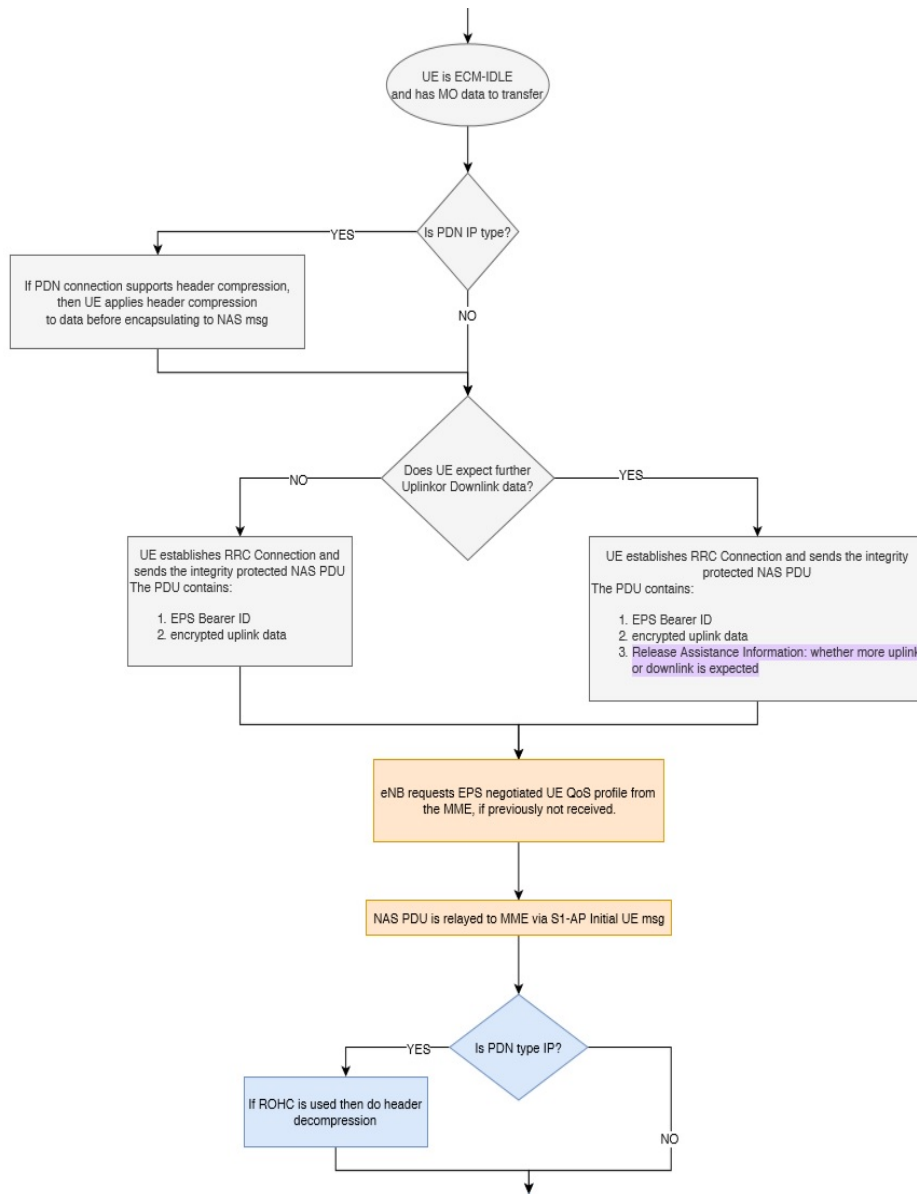
68

Figure B.5: MO data communication flow for IP and non-IP using S11-U Control Plane (part 1)

Figure B.6: MO data communication flow for IP and non-IP using S11-U Control Plane (part 2)
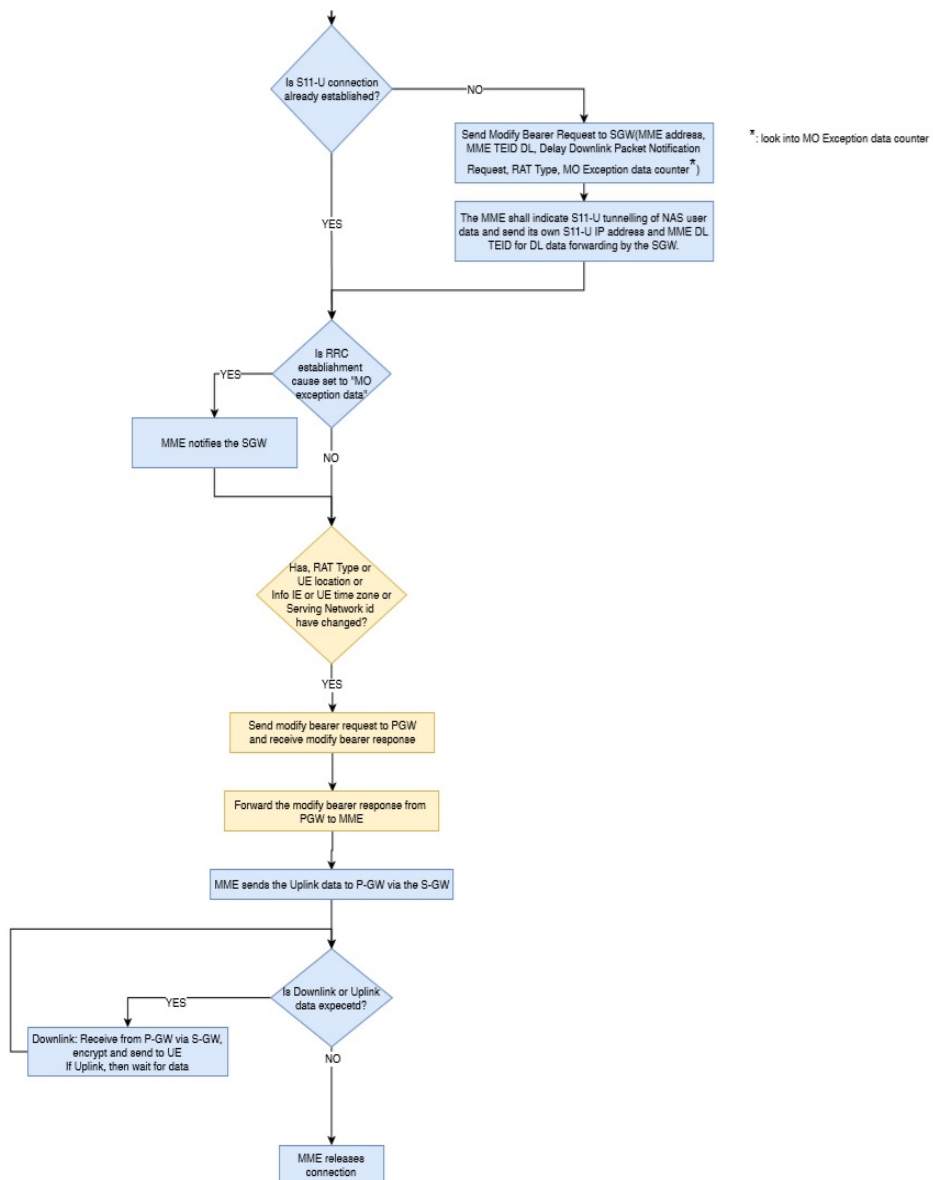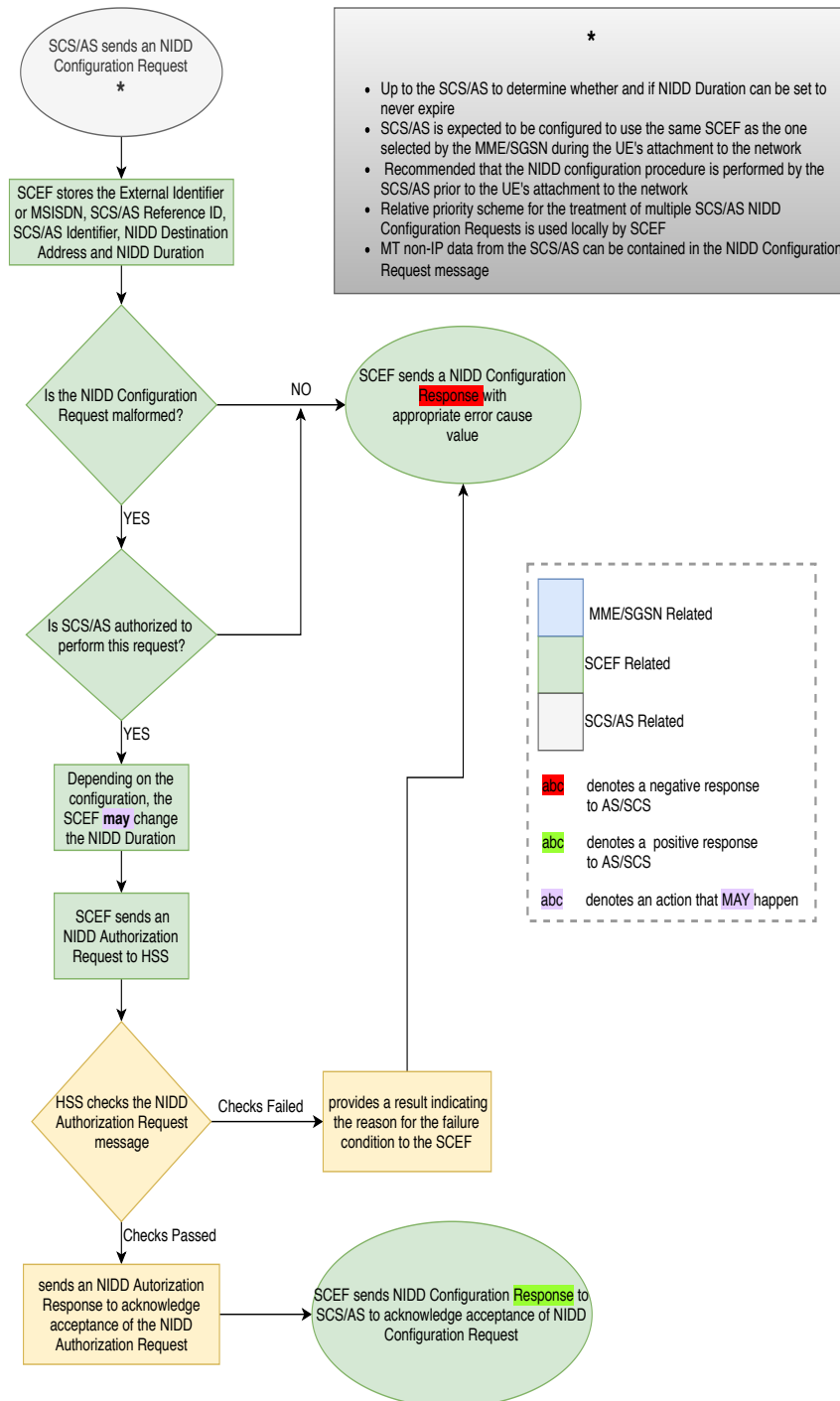
NIDD Configuration Procedure

SCS/AS sends an NIDD
Configuration Request
*

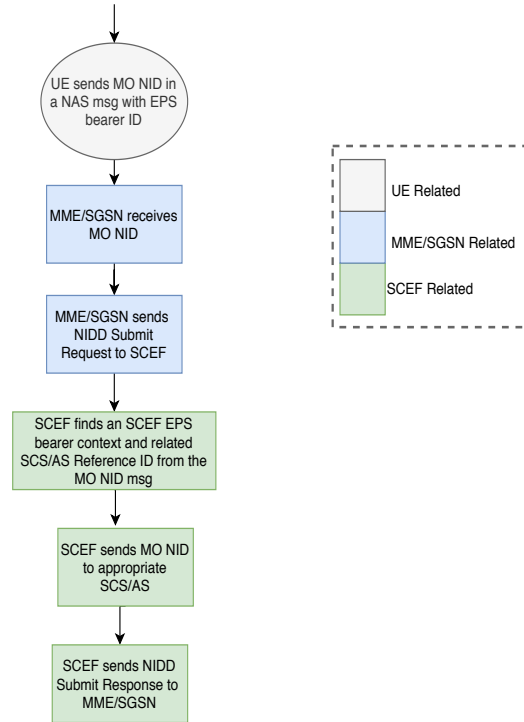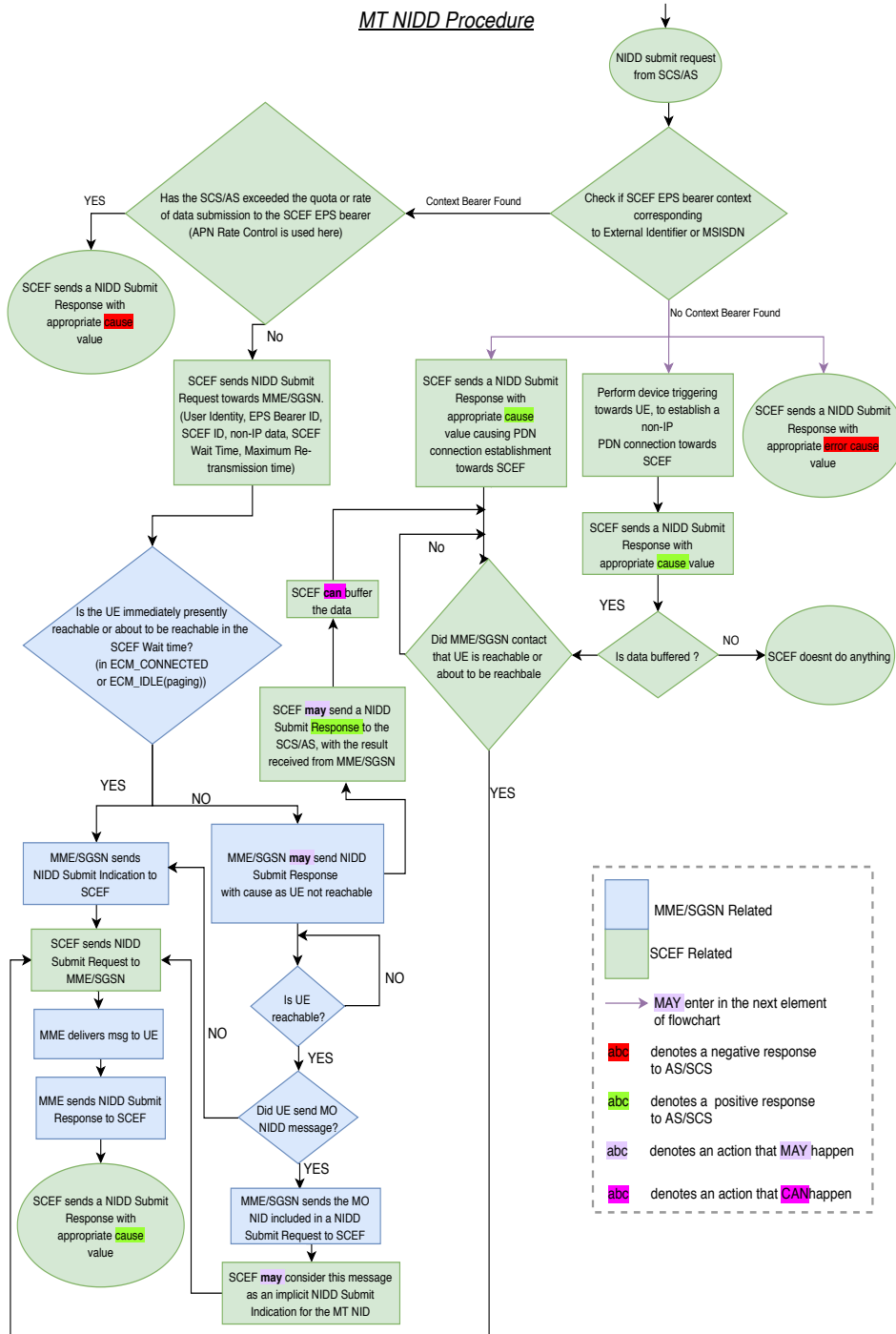SCEF stores the External Identifier
or MSISDN, SCS/AS Reference ID,
SCS/AS Identifier, NIDD Destination
Address and NIDD Duration

*

- Up to the SCS/AS to determine whether and if NIDD Duration can be set to never expire
- SCS/AS is expected to be configured to use the same SCEF as the one selected by the MME/SGSN during the UE's attachment to the network
- Recommended that the NIDD configuration procedure is performed by the SCS/AS prior to the UE's attachment to the network
- Relative priority scheme for the treatment of multiple SCS/AS NIDD Configuration Requests is used locally by SCEF
- MT non-IP data from the SCS/AS can be contained in the NIDD Configuration Request message

Is the NIDD Configuration
Request malformed?

NO

SCEF sends a NIDD Configuration
Response with
appropriate error cause
value

YES

Is SCS/AS authorized to
perform this request?

YES

Depending on the
configuration, the
SCEF **may** change
the NIDD Duration

SCEF sends an
NIDD Authorization
Request to HSS

HSS checks the NIDD
Authorization Request
message

Checks Failed

provides a result indicating
the reason for the failure
condition to the SCEF

Checks Passed

sends an NIDD Autorization
Response to acknowledge
acceptance of the NIDD
Authorization Request

SCEF sends NIDD Configuration Response to
SCS/AS to acknowledge acceptance of NIDD
Configuration Request

MME/SGSN Related

SCEF Related

SCS/AS Related

abc   denotes a negative response
       to AS/SCS

abc   denotes a positive response
       to AS/SCS

abc   denotes an action that MAY happen

Figure B.7:   NIDD Configuration.

Figure B.8: MO data communication flow for IP non-IP data delivery via SCEF.

Figure B.9:   MT data communication flow for non-IP using SCEF.

Appendix C

Logs from the Use Case

The following is the log from the device using IL:

```
Sending AT to check connection with Dragino....

Success!!....

Initializing....

Connecting to Operator....

Connected!!

Operator:20408, Access Technology: LTE-M

IMEI:
8664250314

AT+CPSMS=1,,,"00000110","00101010"

AT+CEDRXS=1,4,"0011"

Starting Ethernet Server ...

Initialized, MAC= 00:08:DC:12:34:56


Connected to ethernet shieldCheck Ethernet Link
- Ethernet PHY Link-Done
Etherent Connection Established !
```

```
IP=10.55.129.250

MASK=255.255.255.0

GW=10.55.129.1

Server open

recvd str: 11,4,31831,"62.72.193.89"

 data received from Client!!!!

 536886296

buffer: h
 Trying to connect to TCP server on RTU
 Connected to RTU
 Data from FrontEnd sent to RTU

server data received: h536896790

data recevd:h

 536896790
```

The following is the log directly taken from the communication of the cellular module to the device using the IL:

```
AT+COPS=1,2,"20408",8

OK
AT+CGPADDR

+CGPADDR: 1,62.133.82.107
+CGPADDR: 17,0.0.0.0
+CGPADDR: 2,0.0.0.0

OK
AT+COPS?

+COPS: 1,2,"20408",8

OK
AT+GSN
```

```
866425031413778

OK
AT+CPSMS=1,,,"00000110","00101010"

OK
AT+CEDRXS=1,4,"0011"

OK
AT+QPSMS?

+QPSMS: 1,,,"3600","600"

OK
AT+CEDRXS?

+CEDRXS: 4,"0011"
+CEDRXS: 5,"1111"

OK
AT+QICLOSE=4

OK
AT+QIOPEN=1,4,"TCP LISTENER","62.72.193.89",0,2404,0

OK

+QIOPEN: 4,0

+QIURC: "incoming",11,4,"62.72.193.89",31831

+QIURC: "recv",11
at+qird=11

+QIRD: 6
h

OK
AT+QISTATE

+QISTATE: 4,"TCP LISTENER","62.133.82.107",0,2404,3,1,4,0,"uart1"
+QISTATE: 11,"TCP INCOMING","62.72.193.89",31831,2404,2,1,4,0,"uart1"

OK
```

```
AT+QISEND=11,6

> 536896
SEND OK
```