BRNO UNIVERSITY OF TECHNOLOGY

Faculty of Electrical Engineering
and Communication

MASTER'S THESIS

Brno, 2023

Dinh Thao Le

BRNO UNIVERSITY OF TECHNOLOGY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF TELECOMMUNICATIONS

ÚSTAV TELEKOMUNIKACÍ

IMPLEMENTATION OF THE LTE CAT-M COMMUNICATION TECHNOLOGY UTILIZING THE NS-3

IMPLEMENTACE TECHNOLOGIE LTE CAT-M V SIMULAČNÍM PROSTŘEDÍ NS-3

MASTER'S THESIS
DIPLOMOVÁ PRÁCE

AUTHOR
AUTOR PRÁCE

Dinh Thao Le

SUPERVISOR
VEDOUCÍ PRÁCE

Ing. Pavel Mašek, Ph.D.

BRNO 2023

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

Master's Thesis

Master's study program **Information Security**

Department of Telecommunications

Student:	Dinh Thao Le	***ID:***	243759
Year of study:	2	***Academic year:***	2022/23

TITLE OF THESIS:

Implementation of the LTE Cat-M Communication Technology Utilizing the NS-3

INSTRUCTION:

The diploma thesis aims to study the LTE Cat-M. As the technology is supposed to be used for the Industrial IoT scenarios, the theoretical part will compare the LPWA technologies, followed by a thorough description of the LTE Cat-M. The focus will be on 3GPP Rel.13 and Rel. 14 standards, with special attention to secured communication. The practical part will cover the implementation of the LTE Cat-M within the Network Simulator 3 (NS-3). Especially, the module LENA-NB/LENA 5G will be used and further modified. The target scenario is related to the remote metering use cases where the LTE Cat-M technology is utilized on the side of the end device for the secured data transmissions.

RECOMMENDED LITERATURE:

[1] Network Simulator 3: Documentation, A Discrete-Event Network Simulator [online], 2019. Available from: https://www.nsnam.org/doxygen/

[2] LIBERG, Olof, Mar̊ten SUNDBERG, Y.-P. Eric WANG, Johan BERGMAN a Joachim SACHS, [2018]. Cellular Internet of things: technologies, standards, and performance. San Diego, CA, United States: Academic Press, an imprint of Elsevier. ISBN 978-012-8124-581.

Date of project specification:	6.2.2023	***Deadline for submission:***	19.5.2023

Supervisor: Ing. Pavel Mašek, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
Chair of study program board

WARNING:

The author of the Master's Thesis claims that by creating this thesis he/she did not infringe the rights of third persons and the personal and/or property rights of third persons were not subjected to derogatory treatment. The author is fully aware of the legal consequences of an infringement of provisions as per Section 11 and following of Act No 121/2000 Coll. on copyright and rights related to copyright and on amendments to some other laws (the Copyright Act) in the wording of subsequent directives including the possible criminal consequences as resulting from provisions of Part 2, Chapter VI, Article 4 of Criminal Code 40/2009 Coll.

ABSTRACT

The master's thesis addresses the Long Term Evolution Machine Type Communication (LTE-M) technology and its implementation in Network Simulator 3 (NS-3). As a member of the Low-Power Wide-Area (LPWA) technology group, LTE-M aims at facilitating the connectivity requirements for massive Machine-Type Communication (mMTC). The main goal of the thesis in the theoretical part is to clarify the characteristics of LTE-M and other technologies in the LPWA group, thereby highlighting their advantages, disadvantages and suitable use cases. The practical part contains the attempt to identify the limit of the network regarding the maximum number of connected devices. Furthermore, the implementation of the power saving features of LTE-M to the NS-3 LENA module is also described, and the obtained simulation results are discussed.

KEYWORDS

LTE-M, Internet of Things, Low-Power Wide-Area Network, massive-MTC, NS-3, LENA, Power Saving Mode, extended Discontinuous Reception

ABSTRAKT

Diplomová práce se zabývá komunikační technologií Long Term Evolution Machine Type Communication (LTE-M) a její implementací v simulačním nástroji Network Simulator 3 (NS-3). Jako člen technologické skupiny Low-Power Wide-Area (LPWA) má LTE-M za cíl poskytovat konektivitu pro scénáře masivního nasazení koncových zařízení (mMTC). Hlavním cílem práce v teoretické části je objasnit charakteristiku LTE-M a dalších technologií ve skupině LPWA, a tím poukázat na jejich výhody, nevýhody a vhodné případy použití. Praktická část se snaží identifikovat limity sítě ve vztahu k maximálnímu počtu připojených zařízení. Dále je také popsána implementace funkcí úspory energie LTE-M do LENA modulu ve NS-3 a uvedeny výsledky simulace.

KLÍČOVÁ SLOVA

LTE-M, Internet věcí, Low-Power Wide-Area Network, massive-MTC, NS-3, LENA, Power Saving Mode, extended Discontinuous Reception

Typeset by the thesis package, version 4.07; http://latex.feec.vutbr.cz

ROZŠÍŘENÝ ABSTRAKT

V posledních letech roste význam Internetu věcí (IoT). Sítě v dnešní době neslouží pouze tradiční komunikaci mezi lidmi (H2H), ale také komunikaci mezi stroji (M2M). Jedním z nejrychleji rostoucích sektorů IoT je komunikace typu massive Machine-Type Communication (mMTC), která vyžaduje zřizování připojení pro obrovské množství jednoduchých, bateriově napájených zařízení distribuovaných v široké oblasti. Vzhledem k tomu, že požadavky mMTC jsou přísné, jsou k jejich splnění potřeba nová řešení, a proto byla definována skupina komunikačních technologií nazývaná Low-Power Wide-Area (LPWA). Technologie LPWA jsou schopny poskytovat široké pokrytí a umožňovat dlouhou životnost baterie pro zařízení IoT. Aplikace LPWA lze nalézt v různých oblastech, jako je chytré město, chytré zemědělství, chytré sítě a logistika. Tato práce se zaměřuje na technologii Long Term Evolution Machine Type Communication (LTE-M), která je členem skupiny LPWA. V rámci práce jsou rozebrány vlastnosti LTE-M. Její funkce pro úsporu energie jsou navíc implementovány v simulačním nástroji Network Simulatoru 3 (NS-3).

Diplomová práce je strukturována do šesti kapitol. První kapitola je věnována popisu konceptu IoT a M2M komunikace. Kromě toho je také uveden přehled nejvýznamnějších technologií LPWA a dalších bezdrátových technologií používaných v IoT s cílem poskytnout obecné informace o jejich vlastnostech a případech použití.

Druhá kapitola poskytuje přehled o vývoji celulárních sítí, od starších komunikačních systémů až po vznik technologie 5G. Kapitola zdůrazňuje několik důležitých milníků ve vývoji sítě směrem k M2M komunikaci a IoT, ke kterým došlo zejména od 3GPP Release 10. Druhá polovina kapitoly je věnována popisu komunikačních technologií pro mMTC, konkrétně čtyřem nejvýznamnějším technologiím LPWA: LTE-M, Narrowband IoT (NB-IoT), Sigfox a Long Range Wide Area Network (LoRaWAN).

Třetí kapitola práce je věnována analýze vlastností technologie LTE-M. V této kapitole je diskutována architektura, principy návrhu, fyzická vrstva a bezpečnostní aspekt LTE-M s cílem objasnit, jak byla technologie vyvinuta pro dosažení požadavků mMTC. Kromě toho je zdůrazněno několik rozdílů mezi LTE-M a NB-IoT, aby se identifikovaly jejich výhody a nevýhody.

Čtvrtá kapitola stručně představuje NS-3, která je simulační platforma použitá pro praktickou část práce. Kromě toho je krátce popsán také modul LTE/EPC Network SimulAtor (LENA) a jeho rozšíření, konkrétně LENA-NB a 5G-LENA.

Pátá a šestá kapitola představují praktický výstup práce. V páté kapitole jsou definovány simulační scénáře pomocí modulu LENA s cílem identifikovat limity sítě vzhledem k počtu připojených zařízení. Z výsledků simulací vyplývá, že maximální počet zařízení, která mohou být současně podporována základnovou stanicí (eNodeB), je 250. Ve šesté kapitole je popsána implementace funkcí Power Saving Mode (PSM) a extended Discontinuous Reception (eDRX) do modulu LENA v NS-3. Pomocí vylepšeného modulu LENA jsou definovány tři simulační sady pro vyhodnocení spotřeby energie koncových zařízení s povoleným PSM a eDRX. Z výsledků simulace je vidět, že při použití PSM, eDRX a málo častém přenosu dat lze u LTE-M zařízení s kapacitou baterie 5 Wh dosáhnout životnosti baterie více než 10 let.

LE, Dinh Thao. *Implementation of the LTE Cat-M Communication Technology Utilizing the NS-3*. Brno: Brno University of Technology, Faculty of Electrical Engineering and Communication, Department of Telecommunications, 2023, 106 p. Master's Thesis. Advised by Ing. Pavel Mašek, PhD.

Author's Declaration

Author:	Bc. Dinh Thao Le
Author's ID:	243759
Paper type:	Master's Thesis
Academic year:	2022/23
Topic:	Implementation of the LTE Cat-M Communication Technology Utilizing the NS-3

I declare that I have written this paper independently, under the guidance of the advisor and using exclusively the technical references and other sources of information cited in the paper and listed in the comprehensive bibliography at the end of the paper.

As the author, I furthermore declare that, with respect to the creation of this paper, I have not infringed any copyright or violated anyone's personal and/or ownership rights. In this context, I am fully aware of the consequences of breaking Regulation § 11 of the Copyright Act No. 121/2000 Coll. of the Czech Republic, as amended, and of any breach of rights related to intellectual property or introduced within amendments to relevant Acts such as the Intellectual Property Act or the Criminal Code, Act No. 40/2009 Coll. of the Czech Republic, Section 2, Head VI, Part 4.

Brno ....

author's signature*

[*] The author signs only in the printed version.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my supervisor Ing. Pavel Mašek, Ph.D. for his invaluable support and guidance throughout this Master's thesis. His expertise and insightful feedback have played a pivotal role in shaping the direction of this thesis.
I would like to express my heartfelt appreciation to my friend Roman Santa for his valuable ideas and ever positive attitude, as well as to Zuzana Gabřisová for her assistance in proofreading and providing continuous encouragement.
Last but not least, I would like to take this opportunity to express my deepest gratitude to my family for their unconditional love and unwavering belief in my abilities, which have been the driving force behind my journey.

Contents

List of Figures

List of Tables

Listings

Introduction

In recent years, the Internet of Things (IoT) has been growing in importance and it has become common that networks nowadays serve not only traditional Human-to-Human (H2H) communication, but also Machine-to-Machine (M2M) communication. One of the fastest growing sector of IoT is massive Machine-Type Communication (mMTC), which requires connection provisioning for a massive number of simple, battery-powered devices distributed in a wide area. Since the mMTC requirements are rigorous, novel solutions are needed to satisfy them, and therefore, a group of communication technologies called Low-Power Wide-Area (LPWA) technologies was defined. As the name partially suggested, the LPWA technologies are capable of providing wide coverage and enabling long battery life for IoT devices. Applications of LPWA can be found in various fields such as smart city, smart agriculture, smart meters and logistics. The focus of this master's thesis is a specific LPWA technology called Long Term Evolution Machine Type Communication (LTE-M). In the scope of the thesis, the characteristics of LTE-M is discussed and its power saving features are implemented in the Network Simulator 3 (NS-3).

The thesis is structured into six chapters. The first chapter is dedicated to describing the ideas behind IoT and M2M communication. In addition, an overview of the most prominent LPWA technologies and other wireless technologies used in IoT is also given in order to provide a general understanding about their characteristics and use cases.

The second chapter gives a historical overview about the evolution of cellular networks, from legacy communication systems to the emergence of 5G technology. The chapter highlights several important milestones in the development of the network towards M2M communication and IoT, which happened mainly since 3GPP Release 10. The second half of the chapter is dedicated to the description of the mMTC enablers, namely the four most prominent LPWA technologies: LTE-M, Narrowband IoT (NB-IoT), Sigfox and Long Range Wide Area Network (LoRaWAN).

The third chapter of thesis is dedicated to analyzing the characteristics of the LTE-M technology. In this chapter, the LTE-M architecture, design principles, physical layer, and security aspect is discussed with the aim to clarify how the technology was developed to achieve the requirements of mMTC. In addition, several differences between LTE-M and NB-IoT are highlighted to identify the their advantages and disadvantages.

The forth chapter gives a brief introduction of the NS-3, which is the simulation platform used for the practical part of the thesis. In addition, the LTE/EPC Network

SimulAtor (LENA) module and its extensions, namely LENA-NB and 5G-LENA, is also shortly described.

The practical output of the thesis is summarized in the fifth and sixth chapter. In chapter five, simulation scenarios are defined using the LENA module with the aim of identifying the limit of the network regarding the number of connected devices. In chapter six, the implementation of the Power Saving Mode (PSM) and extended Discontinuous Reception (eDRX) features for energy saving in LTE-M is described. Based on that, three simulation sets are defined to evaluate the energy consumption of end devices with PSM and eDRX enabled. The simulation results are presented in the form of tables and graphs.

1 The Internet of Things - IoT

1.1 Introduction to IoT

The Internet of Things (IoT) is a modern trend that is affecting all aspects of our lives, from business, healthcare to military applications and beyond. IoT refers to a system of interrelated, internet-connected objects that can gather and transfer data over a wireless or wired network without the need for human intervention. IoT embodies the vision of connecting virtually anything with everything. According to a report done by Ericsson in November 2021, there will be 30.2 billion IoT connections worldwide by 2027, from which 5.5 billion connections will be cellular IoT, and massive IoT will make up 51 % of those cellular IoT connections [1, 2].

The possibilities that IoT can offer are limitless. Any object that has the ability to gather and transfer data, such as an electricity meter, a motion sensor or an alarm system, can be considered a “thing” in IoT. Combined with emerging technologies such as 5G and cloud computing, IoT can greatly improve operational efficiency, minimize costs, improve decision-making, and enhance customer experience [1].

Fig. 1.1 shows an example of an IoT system. On the left side, there are physical assets such as machines or meters, and on the right side, there are applications interacting with the physical world. For example, suppose the physical assets are sensors that monitor vehicle flow on a city’s streets. In this case, the application could be a traffic control center that monitors traffic flows throughout the city. If the physical assets include traffic lights that can be activated by actuators, the application could use the observed traffic flow to manage the red-green periods of individual traffic lights. With this digital transformation enabled by an IoT system, a fixed-configuration traffic infrastructure is turned into a more intelligent one, where insights about the system’s states are gathered. Based on the obtained information, smart decisions can be made and executed within the infrastructure. Here, the IoT system is the service’s enabler. IoT devices are connected to the physical assets and interact with the physical environment through sensors and actuators. The IoT system connects the devices to the service’s specific application and allows the application to control the physical assets via actuators connected to IoT devices [1].

The IoT platform provides a wide range of functionalities, including connectivity, device identification and addressing, security functions, and device management. The aim of this thesis is focused on wireless communication technologies that enable IoT connectivity. In particular, the thesis will be dedicated to the Long-Term Evolution for Machines (LTE-M) technology, which stands out as a promising representative for the evolving Industrial IoT segment/Industry 4.0 [1].

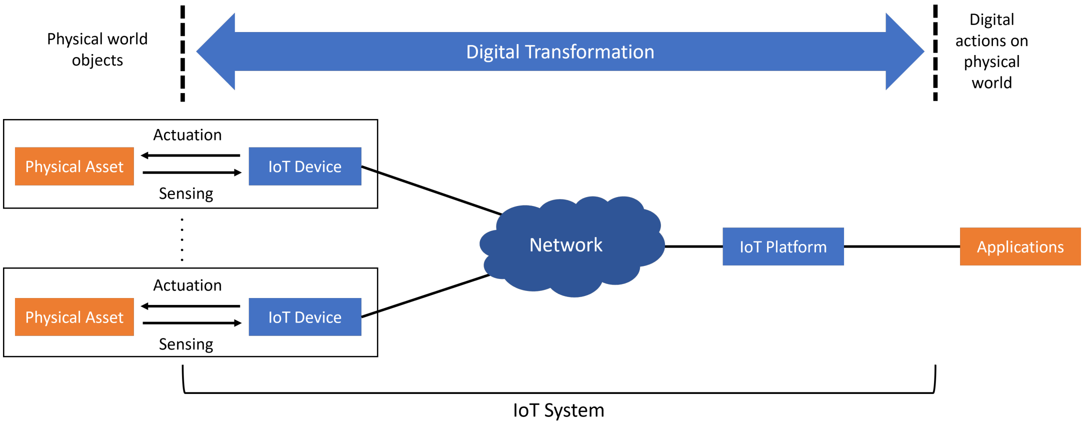

Fig. 1.1: IoT system connecting digital applications and the physical world [1]

1.2 Machine-to-Machine Communication

Machine-to-Machine (M2M) communication, also known as Machine-Type Communication (MTC), is an emerging type of communication that allows devices to communicate with each other without (or only with minimal) human intervention. It has grown significantly in popularity in recent years and is now a crucial component of wireless networks. M2M connections will account for half of all worldwide connected devices and connections by 2023, according to Cisco's Annual Internet Report (2018-2023) [3].

There are several distinguishing characteristics that differentiate M2M from conventional Human-to-Human (H2H) or Human-Type Communication (HTC) such as uplink-centric applications, a large number of connected devices, and long battery lifetime expectancy for end devices. Tab. 1.1 summarizes the key differences between M2M and H2H, thereby highlighting the characteristics of M2M communication [4].

It is also important to note that while the terms M2M and IoT may often be used interchangeably, they are not the same. IoT requires M2M, but M2M does not necessarily mean IoT. Some M2M communication solutions are custom-built to meet the communication requirements of a particular application, such as connectivity for electric appliances, remote-controlled lighting, baby monitors, etc. For many of those systems, the entire communication stack is designed for a single purpose. Even if it enables an environment with a broader range of connected devices and objects, it is still based on a particular M2M technology, utilizing proprietary networking protocols and without end-to-end Internet Protocol (IP) connectivity. In other words, those M2M systems are isolated, stand-alone networked equipment. This approach is different from the vision of IoT, which aims to create a common and interoperable connectivity framework that can be used to connect any device or

Tab. 1.1: Differences between M2M and H2H communications [4]

	M2M	**H2H**
Delay range	10 ms to several minutes	250 ms (voice) to a few seconds (data transferring, email)
Mobility	Most M2M devices are stationary	Humans are rarely considered fixed in practical mobile networks
Supported services	Mainly SMS or data reporting	SMS, voice, Web, data, multimedia, etc.
Uplink traffic	M2M traffic is mainly generated in uplink	Traditionally less traffic in the uplink. However, it is increasing rapidly with the rise of interactive applications such as live video streaming and social network
Downlink traffic	Usually less traffic except for some certain applications	Currently most traffic (Web browsing and multimedia)
Message size	Generally very short. In some cases could increase, for example, if video sequences are uploaded	Typically big messages, especially for multimedia and real-time transmission
Number of devices	Hundreds or thousands of devices per base station	At most hundreds of devices, typically tens of devices per base station
Battery life requirement	Up to several years, especially for deployment locations with difficult access	Order of days or weeks
Key metrics for user experience	Energy efficiency, latency	Latency, throughput, packet loss

smart object. IoT takes M2M to the next level, bringing together disparate systems into one large, connected ecosystem. The difference between isolated M2M systems and IoT system is depicted in Fig. 1.2 [1].

1.3 Overview of Wireless Technologies Used in IoT

When it comes to wireless connectivity, there are many technologies available for IoT. Each of them is designed to achieve a relatively specific set of goals, and while some technologies can be used for a wide range of applications, no technology is a one-size-fits-all. Therefore, the requirements and demands of a particular project

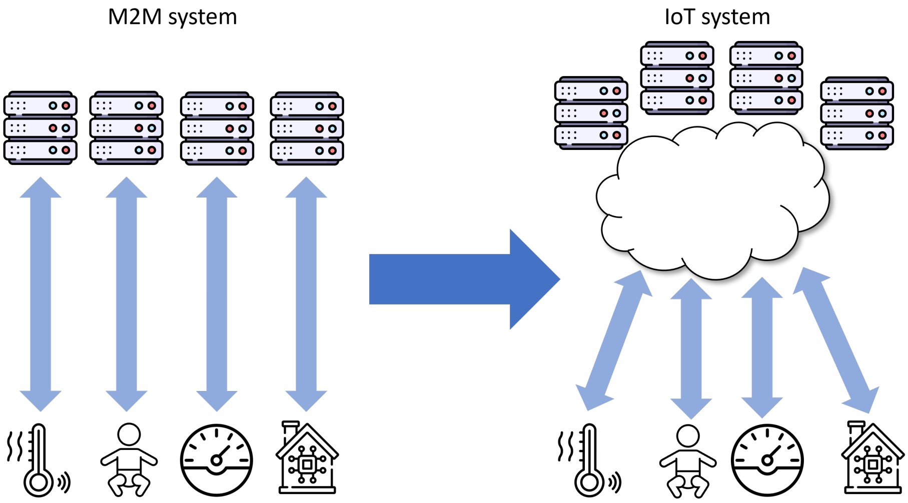

Fig. 1.2: Difference between M2M and IoT [1]

ultimately determine the communication technology (or technologies) that will be used for that project.

1.3.1 Low-Power Wide-Area Technologies

The tremendous rise of M2M communication over the last decade has prompted the development of new wireless communication technologies that are entirely focused on extending communication coverage for base transceiver stations (BTS) and battery life for terminal devices. Those technologies are generally referred to as Low-Power Wide-Area (LPWA) networking technologies [5].

LPWA networks (LPWAN) usually transmit data at slower rates. However, they cost less, consume less power, have better wireless coverage, and can transmit data to more devices in a condensed area than other wireless technologies. LPWA technologies are expected to cover a variety of applications, including logistics, smart cities, smart grids, and infrastructure monitoring [6].

LPWA technologies are characterized by the following features:

- **Low-power operations:** LPWA devices are expected to last for years on a single battery. This means that devices can be installed and left alone in buildings, outdoor areas, and other difficult-to-access locations over a long period of time, providing valuable data without the need for human attention [5, 6].
- **Coverages:** LPWANs are required to provide coverage of up to 5 km in metropolitan areas and over 10 km in country/desert areas. They are also expected to provide coverage for challenging indoor locations and coverage where signal must pass through obstacles such as walls and buildings. These

goals are achieved by the use of sub-GHz bands, which has good propagation characteristics, and message repetition, known as Coverage Enhancement technique. Furthermore, slow modulation techniques are employed to increase the energy for each bit and make it easier for receivers to demodulate the signal. However, these coverage-extending techniques come with a cost of reduction in data rates and increase in latency [5, 6].

- **Capacity:** One of the essential requirements for LPWANs is to support a massive number of connected devices with a low data rate. Many applications require support for up to 100,000 devices in a scalable manner [5, 6].

The four most prominent LPWA technologies nowadays are: (i) LTE-M, (ii) NarrowBand IoT (NB-IoT), (iii) Long Range Wide Area Network (LoRaWAN), and (iv) Sigfox.

LTE-M and NB-IoT are technology standards developed by the Third Generation Partnership Project (3GPP) organization to be cellular-based communication solutions for IoT applications. They are positioned by 3GPP to become a key part of the long-term 5G IoT strategy. LoRaWAN and Sigfox are non-3GPP, proprietary technologies that operate in license-free frequency bands. Besides, unlike LTE-M and NB-IoT, they are non-cellular wireless technologies. These four LPWA technologies will be described in more detail in the second chapter of the thesis.

LPWA technologies are crucial for the existence of IoT. Due to their unique characteristics, they have an important role when compared to other IoT communication technologies such as Bluetooth, Wi-Fi or ZigBee. The comparison of LPWA technologies with other wireless technologies used in IoT is shown in Tab. 1.2.

LPWANs typically have a star topology or use a cellular system in which terminal devices are connected to a server through a BTS. In addition, there is the possibility of using data transmission across multiple BTSs, which ensures constant connection even in the event that one of the BTSs has a failure, which otherwise may cause all the terminal devices connected to that BTS to be unreachable for a period of time [5].

The simplicity of the star topology helps reduce the complexity of the end devices and substantially lower their energy consumption. In this topology, the BTS, which has a stable energy supply from an electricity line, is located in the center and has to constantly listen on multiple channels to receive incoming messages. In contrast, the end devices, which are usually battery-powered, can remain in sleep mode for a long period of time to save energy and only have to wake up to transmit data when necessary [5].

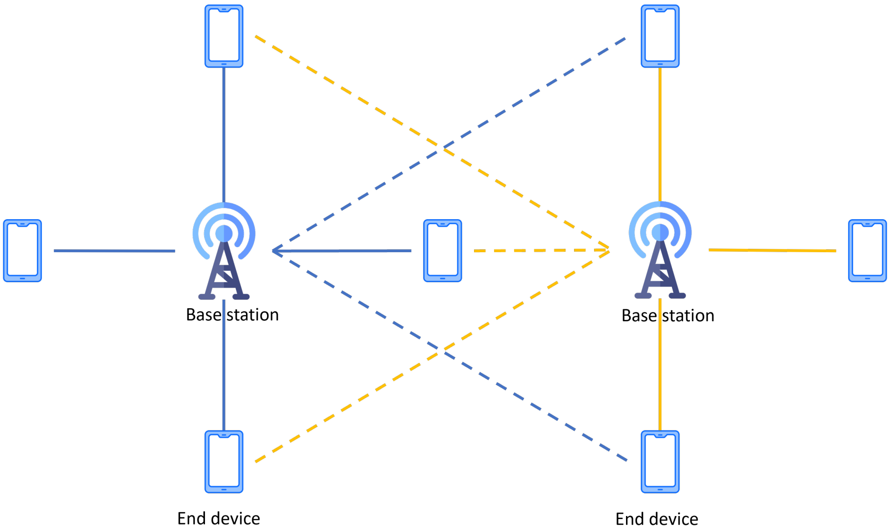

Fig. 1.3: Star topology in LPWA [7]

1.3.2 Wireless Technologies for Short-range and Medium-range Communication in IoT

While LPWA technologies are designed to support large-scale IoT networks sprawling over vast industrial and commercial sites, there are also other wireless technologies developed to tackle applications that only need to cover a relatively small area, but have other requirements such as higher data rates, more frequent communication between devices, lower latency, etc. Bluetooth, Wi-Fi, Z-Wave, and IEEE 802.15.4-based Technologies (Thread, ZigBee) are prominent representatives among such technologies.

Bluetooth

Bluetooth is a wireless technology standard that enables connected devices to exchange data over short distances. Originally created by Ericsson to connect wireless headsets, Bluetooth has expanded over the years and now offers significant flexibility in bandwidth, range and communications topologies to address different applications, including IoT. Bluetooth operates in the ISM 2.4 GHz band [8].

There are two different Bluetooth variants: Bluetooth Classic and Bluetooth Low Energy (LE). Bluetooth Classic is the original technology and is still very widely used in streaming applications, especially audio streaming. Bluetooth LE was introduced in 2010 in Bluetooth 4.0 specifications. It was designed to focus on low-bandwidth applications that require infrequent data transmission between devices. Bluetooth LE is recognized for its low power consumption and is widely used for IoT applications as it can fulfill many connectivity requirements. However, a big disadvantage of Bluetooth LE is that it can only support as many as seven devices per Master/Slave connection. Technically, a high number of devices can be connected to a Bluetooth LE mesh network, but for every seven additional devices, a new Bluetooth adapter is required [8, 9].

Use cases of Bluetooth technology for IoT include health and fitness devices, smart lighting systems, smart homes with interconnected devices and remote asset monitoring [8].

Wi-Fi

Wi-Fi is the trademark name used for any Wireless Local Area Network (WLAN) that adheres to the IEEE 802.11 standard. Wi-Fi operates on the ISM 2.4 GHz and 5 GHz bands. The most popular topology used in Wi-Fi is the star topology, in which nodes communicate with each other through a central hub [8, 9].

Being one of the most popular technologies in the world, Wi-Fi has the advantage of supporting a diverse range of applications. This means that it will play a role in most IoT environments, either alone or interworking with more specialized protocols, or with cellular networks. Moreover, Wi-Fi-enabled smart devices are usually less expensive and widely available. However, Wi-Fi also has several disadvantages when it comes to IoT applications. Transmitting at higher frequency bands, Wi-Fi offers high data rates, but in exchange, it consumes a lot of power and doesn't offer a lot of range. Furthermore, Wi-Fi can only support a very limited number of connected devices in comparison with other IoT communication technologies. Most Wi-Fi routers can only allow tens of devices to be connected at once, while other technologies such as LWPAN or ZigBee can handle thousands devices [9].

Wi-Fi is suitable for IoT applications that need to send a lot of data (e.g., video), that don't have strict power consumption requirements (e.g., devices that are plugged into an outlet), and that don't need very wide coverage. Moreover, Wi-Fi is most commonly used for devices that require a direct connection to the Internet. For example, a home security system with video surveillance would be an ideal use case for Wi-Fi in IoT [8, 9].

Z-Wave

Initially designed as a protocol for controlling lighting systems, Z-Wave has evolved into a wireless communications protocol used for residential and commercial building automation, allowing smart devices to connect and exchange control commands and data with each other. It is a proprietary technology designed by the Danish company Zensys and maintained by the Z-Wave Alliance [8, 9].

Z-Wave operates on the low-frequency 908/915 MHz band in the U.S. and 868 MHz band in Europe. This is to avoid interference with the 2.4 GHz ISM band where Wi-Fi and Bluetooth operate, and also to extend coverage [8].

A Z-Wave network is comprised of IoT devices and a primary controller, which is usually the only device connected to the Internet. The command from a smart home application can be routed by the Z-Wave controller across a network of up to 232 devices, including the controller itself. Z-Wave uses the source-routed mesh network technology, which allows signals from one Z-Wave device to hop through other devices to reach its destination. A maximum of 4 hops is supported by Z-Wave networks [8, 9].

IEEE 802.15.4-Based Technologies (Thread, ZigBee)

IEEE 802.15.4 is a technical standard that specifies the physical layer and media access control (MAC) layer for Low-Rate Wireless Personal Area Network (LR-WPAN). It focuses on facilitating low-cost, low-speed communication between wireless devices. IEEE 802.15.4 is the foundation for several technology standards. Among the technologies built on top of it are ZigBee and Thread, which are widely used for IoT applications, especially in the smart home domain [8, 10].

ZigBee can operate at either 915 MHz or 2.4 GHz and provide coverage from 10 m to 100 m. The most widely used topology in ZigBee is the mesh topology, where nodes are interconnected with other nodes so that there are multiple pathways between them. Connections between nodes are dynamically updated and optimized through a sophisticated, built-in mesh routing table. A ZigBee network can support up to 65000 connected devices, including a hub which coordinates the system. The supported data rates are 250 kb/s, 100 kb/s, 40 kb/s, and 20 kb/s [10].

Thread is an IPv6-based, low-power, open-source networking protocol specifically built for IoT devices. Similar to ZigBee, Thread operates on the ISM 2.4 GHz band and provides data rates of up to 250 kb/s. The most distinguishing characteristic of Thread is that it is an IP-based protocol, which means that a Thread network can seamlessly connect to the Internet without the need for an gateway in between. Furthermore, although it also utilizes the mesh topology, Thread does not require a hub to coordinate the system. Instead, it requires a border router to bridge the Thread network to the Internet, and any Thread device can connect to any Thread border router, regardless of manufacturer. A Thread network can support 250 connected devices in a range of 30 m [10].

These technologies are suitable for medium-range IoT applications with an even distribution of nodes in close proximity. Their use cases include home automation, wireless sensor network and medical data collection [8, 10].

Tab. 1.2: Comparison of different wireless technologies used in IoT [8, 10]

Attribute	**Bluetooth**	**Wi-Fi**	**Z-Wave**	**IEEE 802.15.4** (Zigbee, Thread)	**LTE-M**	**NB-IoT**	**Sigfox**	**LoRaWAN**
	Non-LPWA				LPWA			
Range	10 m - 1.5 km	15 m - 100 m	30 m - 50 m	30 m - 100 m	1 km - 10 km	1 km - 10 km	3 km - 50 km	2 km - 20 km
Throughput	125 kb/s – 2 Mb/s	54 Mb/s – 1.3 Gb/s	10 kb/s – 100 kb/s	20 kb/s – 250 kb/s	7 Mb/s UL[1], 4 Mb/s DL[1]	159 kb/s UL[2], 127 kb/s DL[2]	100 b/s (UL), 600 b/s (DL)	10 kb/s – 50 kb/s
Power Consump.	Low	High	Low	Low	Medium	Low	Low	Low
Topology	P2P, Star, Mesh, Broadcast	Star, Mesh	Mesh	Mesh	Star	Star	Star	Star
Primary Use Cases	Healthcare and fitness, smart lighting systems, indoor navigation applications	Most commonly for devices that need a direct connection to the Internet	Smart home applications	Wireless control and monitoring applications in the smart home space	Logistics, healthcare, automotive applications	Smart agriculture, smart city and smart meter applications	Smart city applications in the EU region	Smart city applications, supply chain and logistics

[1] LTE Cat-M2 [2] LTE Cat-NB2

2 From Legacy Systems to Machine-Type Communication in 5G

2.1 Legacy Communication Systems

Prior to the emergence of 4G and later the introduction of 5G, mobile networks were primarily intended to facilitate communication between humans, emphasizing services such as downlink (DL) data transmissions and voice calls. However, since 3GPP Release 10 in 2011, the approach began to shift towards accommodating networks that could support the growing needs of IoT. This section aims to provide a concise overview of the evolution of 3GPP mobile networks over time, illustrating the changes that have occurred as a result of this shift in focus [11].

2.1.1 2G Network

2G stands for the second-generation digital cellular network, which was developed as a replacement for the first-generation (1G) analog cellular network. 2G cellular networks were first commercially launched on the Global System for Mobile Communication (GSM) standard in Finland in 1991. GSM later became a global standard for mobile communication, achieving over 90 % market share and operating in over 193 countries and territories by the mid-2010s. Another notable 2G standard is the IS95 standard, which is based on Code Division Multiple Access (CDMA) and was deployed mainly in North America [12].

The GSM standard initially defined a digital, circuit-switched network optimized for full-duplex voice telephony. GSM uses Time Division Multiple Access (TDMA) to multiplex up to 8 calls per channel in the 900 MHz and 1800 MHz bands. In addition to voice transmission, GSM can also deliver circuit-switched data at speeds up to 14.4 kb/s [13].

However, towards the end of the 20$^{\text{th}}$ century, the limitations of circuit-switched data became apparent with the increasing prevalence of data applications. As a solution to this problem, 3GPP released an extension to the existing 2G networks, known as the General Packet Radio Service (GPRS). GPRS offered packet-based services and was capable of providing data rates ranging from units to tens of kilobits per second, enabling access to services such as Wireless Application Protocol, Multimedia Messaging Service, and Internet communication services including e-mail and World Wide Web access. In essence, GPRS expanded the capabilities of 2G networks to better accommodate the growing demand for data services [5, 13].

Additional enhancements to 2G networks were introduced with the deployment of Enhanced Data rates for GSM Evolution (EDGE) technology. EDGE was first deployed on GSM networks in 2003 initially by Cingular (now AT&T) in the United States. EDGE achieves higher data rates (up to 236.8 kb/s) by switching to a more sophisticated Eight-State Phase Shift Keying (8PSK) method of coding within existing GSM timeslots instead of the Gaussian Minimum-Shift Keying (GMSK) modulation scheme used in the original GSM and GPRS networks. The biggest advantage of EDGE is that the users don't have to install any additional hardware and software in order to make use of this technology, ex-GPRS users can utilize EDGE technology without paying any additional charge [5, 12].

2.1.2 3G Network

The third-generation mobile network (3G) is the upgrade over 2G, GPRS, and EDGE networks, offering faster data transfer, and better voice quality. 3G is based on a set of standards that comply with the International Mobile Telecommunications-2000 (IMT-2000) specifications defined by the International Telecommunication Union (ITU). To meet those specifications, a system must provide peak data rates of at least 144 kb/s [14].

3G has two main branded standards: the Universal Mobile Telecommunications System (UMTS) (mainly in GSM-predominated regions such as Europe) and the CDMA2000 (mainly in IS95-predominated regions). Both standards utilize the CDMA channel access method, where several transmitters can send information simultaneously over a single communication channel while unique codes are used to differentiate between data streams. Using CDMA, adjacent cells can operate on the same frequency band, which significantly improves the access network's efficiency. The fundamental architecture of 3G networks, however, is still rooted in that of 2G networks. Hence, the access network is still composed of BTSs (NodeB) and their Radio Network Controller (RNC). In the core network, the circuit-switched domain is used for voice services, and the packet-switched domain is used for packet-oriented applications [5].

Nevertheless, the increase in transmission speed of UTMS in the original Wideband Code Division Multiple Access (W-CDMA) radio interface, by a few hundreds kilobits per second in comparison with EDGE, was not very noticeable. The introduction of the High-Speed Packet Access (HSPA) specification marked truly significant improvements in 3G mobile networks. In addition to boosting the network's throughput, HSPA also reduced network latency, especially in the access section, by moving some of the radio control functions from the RNC to the NodeB. Later on, 3GPP introduced HSPA+ as a further upgrade to HSPA, featuring support for Multiple-Input Multiple-Output (MIMO) and 64-State Quadrature Amplitude

Modulation (64QAM). Theoretically, HSPA+ can provide data rates of up to 168 Mb/s in the DL and 22 Mb/s in the UL, making it a significant improvement over its predecessors [5].

2.1.3 4G Network

The fourth-generation mobile network (4G) represents further improvements in service quality, and it is also in this generation that the concept of M2M communication was officially taken into account in 3GPP releases. To be qualified as 4G, a system must provide capabilities defined by the ITU in the IMT-Advanced specifications, where, among other requirements, the peak data rate must be at least 100 Mb/s for high mobility communication (such as from trains and cars), and 1 Gb/s for low mobility communication (such as pedestrians and stationary users). Another important requirement in the IMT-Advanced specifications is scalable channel bandwidth from 5 MHz to 20 MHz. The 3GPP-developed 4G standard is called the Long-Term Evolution (LTE) standard and it is the most predominant 4G technology in the world [13].

Unlike its predecessors, LTE does not support circuit-switched telephony service. Instead, it relies entirely on IP-based communication with the option to fallback to circuit-switched system for voice service. The CDMA radio technology used in 3G systems is also abandoned and replaced by the Orthogonal Frequency-Division Multiple Access (OFDMA) method, making it possible to transfer very high bit rates despite extensive multi-path radio propagation. The peak bit rate is improved even more by smart antenna arrays for MIMO communications. Regarding network architecture, the evolved NodeB (eNodeB) is now the only type of entity in the radio access network, as the RNC controllers in 3G architecture were eliminated [5, 13].

The groundwork for the initial version of LTE was established in 3GPP Release 8, which introduced a significant number of advancements. However, it still did not satisfy the IMT-Advanced criteria, making it ineligible to be classified as a 4G network. It's noteworthy that this Release also marked the first exploration into enabling M2M communication within the 3GPP framework [5].

Release 9 brought about several improvements to LTE, among which was the introduction of femtocells, which are small cellular base stations that can be installed in homes or small offices. These femtocells, also known as Home eNodeBs, enhance indoor coverage and provide better signal quality for users. Release 9 also dedicated a part to M2M communication, providing a feasibility study on the security aspects of remote provisioning and subscription change for M2M equipment. This paved the way for further development of IoT applications within 3GPP networks [5].

Release 10 introduced LTE-Advanced, which was the first specification to meet

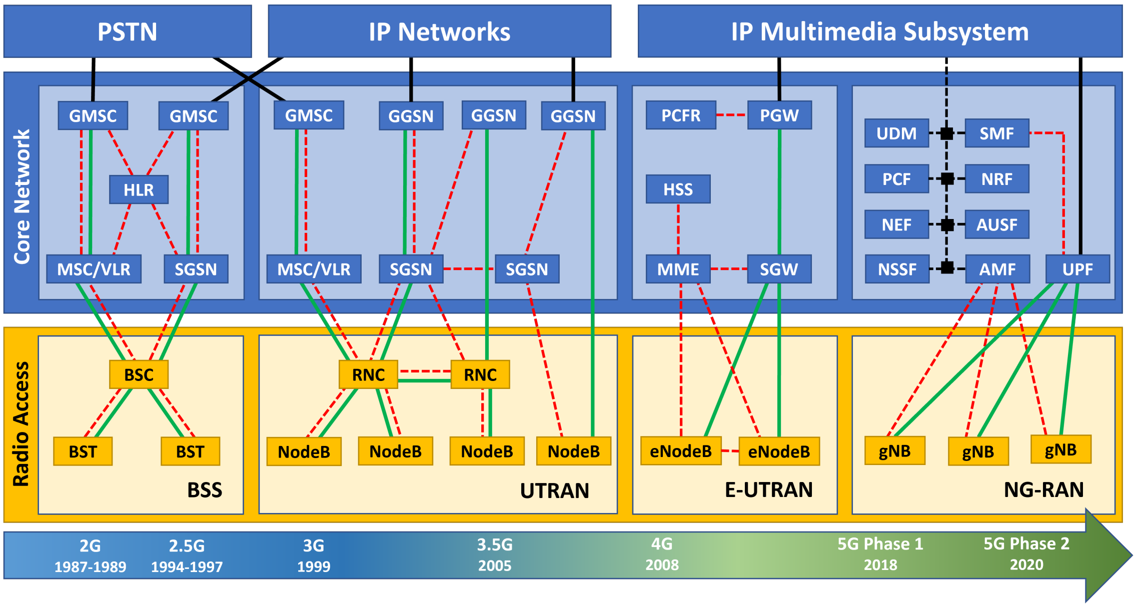

Fig. 2.1: 3GPP technologies evolution [5, 15]

the IMT-Advanced requirements, and therefore, was the first true 4G network. The maximum theoretical data rates of LTE-Advanced are up to 1 Gb/s for stationary users and up to 100 Mb/s for mobile users, which is achieved mainly through carrier aggregation. Additionally, this Release brought about other significant enhancements such as 8×8 MIMO antenna configuration in DL and 4×4 in UL, introduction of new communication bands, self-optimizing networks, and LTE relays. Attention was also given to M2M communication, which is referred to as MTC in 3GPP terminology. Two crucial issues concerning MTC were addressed, which were MTC Subscription, and Signaling Congestion and Overload Control [5, 11]:

- **MTC subscription:** In Release 10, MTC subscribers are seen as any regular subscriber in the mobile operator's network, and MTC devices are not classified as a distinct type of user equipment (UE). MTC subscribers may have subscriptions to multiple MTC features, and they can activate or deactivate these features as needed. The subscription to a specific MTC feature on a device is achieved by binding the International Mobile Subscriber Identity (IMSI) in the Universal Subscriber Identity Module (USIM) of the device to the MTC subscription with the individual MTC features in the Home Subscriber Server (HSS). The subscribed features are included in the subscriber's profile, which is downloaded to the Mobility Management Entity (MME) at the time when the MTC device attaches to the network or performs a registration (Tracking Area Update (TAU) or Routing Area Update (RAU)). The MME can perform a compatibility check and can disable MTC features that mismatch with other activated MTC features, as they might conflict with each other [5, 11].

- **Signaling Congestion and Overload Control:** Four techniques were introduced in Release 10 to handle network congestion and overload control. These techniques include assigning low access priority to certain connections, requiring the International Mobile Subscriber Identity (IMSI) at Public Land Mobile Network (PLMN) changes, setting longer minimum periodic PLMN search times, and implementing specific measures to manage invalid USIM states [5, 11].

Because all initially proposed MTC features and capabilities couldn't be tackled in Release 10, the remaining tasks were shifted into Release 11. The primary contributions in Release 11 involve finalizing the MTC architecture to improve cooperation with MTC devices in external networks, enabling online device triggering, and facilitating packet-switched-only service provision. Nonetheless, there is still no new UE type for MTC and the MTC-specific optimizations are also applicable to "normal" UE [5, 11].

2.2 Massive Machine-Type Communication Enablers

In the standardization of 5G, three requirement categories were defined. They are: Enhanced Mobile Broadband, Critical MTC (cMTC), and Massive MTC (mMTC). It is clear that M2M communication is becoming more and more important as two out of three requirement categories of 5G are focused on MTC, essentially addressing the IoT [1].

cMTC is designed to meet demanding IoT use cases that require high reliability, availability, and low latency. The cMTC category is also referred to as Ultra-Reliable and Low Latency Communication (URLLC) in the 3GPP standardization. Use cases of cMTC can be found in various fields, such as smart grid automation, remote driving, training and surgery [1].

On the other hand, mMTC is designed to facilitate communication for a large number of simple devices with a need for relatively small and infrequent data transfer. In mMTC, UEs are expected to be massively deployed, so the scalability to many connected devices is required, as well as the support to reach them with the network wherever they are located. The ubiquity of the deployment, in combination with a need to keep deployment and operation costs low, motivates the development of ultra-low-complex IoT devices that may need to rely on non-rechargeable, battery-powered operations for years. Examples of mMTC use cases exist in many fields, such as logistics, smart meters, smart buildings, smart agriculture, etc. In the scope of the thesis, only the mMTC communication technologies will be addressed [1].

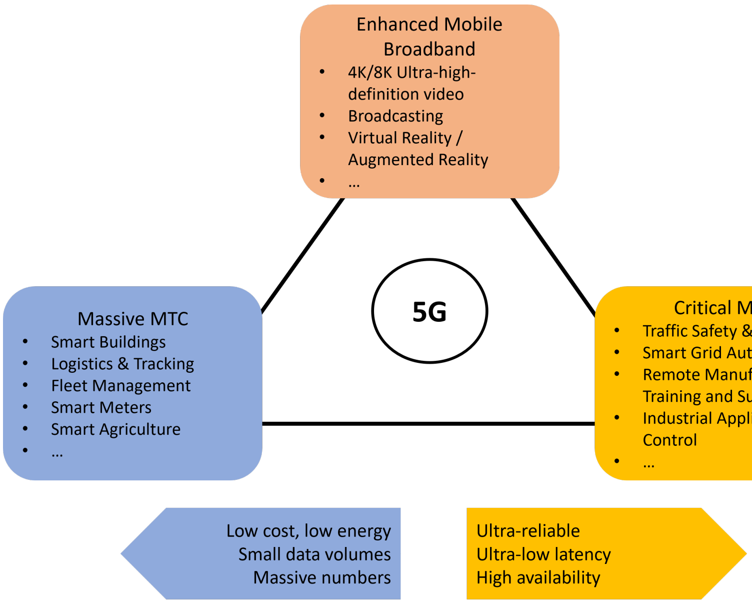

Fig. 2.2: 5G requirement categories [1]

LPWA technologies were developed to meet the demanding requirements of mMTC. LPWA networks are capable of providing extensive coverage and long battery life in low-cost and low-complexity devices. This family of technologies has become one of the leading enablers of mMTC and is now the fastest-growing sector of IoT. As introduced in chapter 1, LPWA technologies work in both licensed and unlicensed frequency bands. In licensed frequency bands, there are two technology standards defined by 3GPP, namely NB-IoT and LTE-M. In unlicensed bands, Sigfox and LoRaWAN are the most prominent technologies [5].

2.2.1 LTE-M

LTE-M is a LPWA radio technology standard developed by 3GPP to enable a wide range of cellular IoT applications. It is a standard for narrow-bandwidth cellular communications to connect resource-constrained devices. In general, LTE-M aims to facilitate transmission of small amounts of data over long periods of time, while providing high signal penetration and retaining low power consumption. The first specification for LTE-M was introduced in 3GPP Release 13 (LTE Advanced Pro) in June 2016. Over the following years, LTE-M has been constantly improved in 3GPP Releases and it is now integrated to be a part of the 5G network, specifically aimed to facilitate mMTC applications [6]. LTE-M technology is the main focus of the thesis and will be described in more detail in chapter 3.

2.2.2 NB-IoT

Similar to LTE-M, NB-IoT was first introduced in 3GPP Release 13. It is a new radio access technology dedicated to facilitating mMTC communication. In terms of functionality, NB-IoT has been designed specifically to achieve maximum simplicity, reduce the cost of UEs, and minimize battery consumption. NB-IoT uses the same licensed frequency bands as LTE [1, 6].

NB-IoT is aimed to be a network for simple battery-powered devices, where small amounts of data are transmitted with low transmission speed and relatively high latency. However, the network must provide wide, robust coverage and allow for low-energy operations. Specifically, an NB-IoT network must meet the following performance objectives [1, 16]:

- Support for ultra-low-complexity devices for IoT applications.
- Improved indoor coverage of 20 dB (compared to GPRS), corresponding to a Maximum Coupling Loss (MCL) of 164 dB.
- Support for a data rate of at least 160 b/s on the application layer.
- Support for a massive number of UEs with low throughput (at least 52547 devices within a cell-site sector).
- UEs' battery life of 10 years with a battery capacity of 5 Wh.
- Latency of 10 s or less for 99 % of the devices.

At the physical layer, NB-IoT only occupies a bandwidth of 180 kHz, which is substantially smaller than LTE bandwidths of 1.4 MHz – 20 MHz. The 180 kHz bandwidth of NB-IoT fits precisely into one LTE Physical Resource Block (PRB), and also into one 200 kHz GSM carrier. The maximum transmission power of NB-IoT UEs is 23 dBm. Unlike LTE-M, which has the ability to support both Time Division Duplex (TDD) and Frequency Division Duplex (FDD), NB-IoT only supports FDD half-duplex mode in order to reduce the UE's complexity. While half-duplex FDD has limitations in terms of ability to provide simultaneous bidirectional communication, it can be effectively used in applications where one direction of communication is more critical than the other, or where the amount of data being transmitted is relatively low. This makes it a suitable option for certain IoT applications, especially mMTC, where low power consumption and cost are more important factors [5, 16].

In the DL direction, Quadrature Phase-Shift Keying (QPSK) modulation is used in combination with OFDMA and a subcarrier spacing of 15 kHz. In the UL direction, QPSK or Binary Phase-Shift Keying (BPSK) is used in combination with Single-Carrier FDMA (SC-FDMA) [5, 16].

NB-IoT can be deployed in three operation modes: (i) in-band, (ii) guard-band, and (iii) stand-alone, see Fig. 2.3. In in-band operation mode, one or more LTE

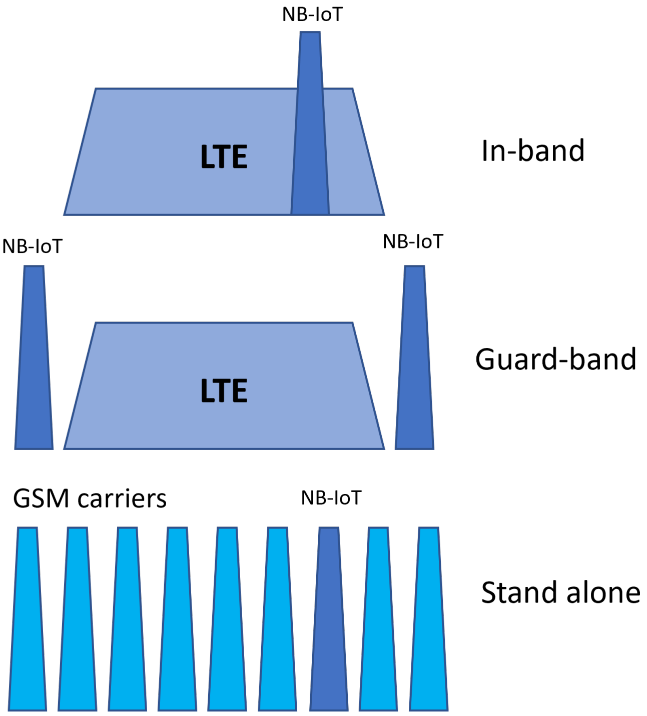

Fig. 2.3: NB-IoT operation modes [5]

PRBs are reserved for NB-IoT. Sharing of PRBs between NB-IoT and LTE allows for more efficient use of the spectrum. Furthermore, although they are two separate systems, they can be supported using the same eNodeB hardware. In guard-band operation, NB-IoT will be deployed within the guard band of an LTE carrier. In standalone operation, NB-IoT can be used as a replacement for one or more GSM carriers with a 10 kHz buffer on each side [5, 16].

In NB-IoT, two mechanisms for energy saving are used, which are Power Saving Mode (PSM) and Extended Discontinuous Reception (eDRX). PSM allows a device to turn off its radio part and go to sleep but still remain registered within the network so it doesn't have to reconnect itself to the network when it next wakes up. The device only wakes up and communicate with the network when required. In PSM sleep mode, the device consumes the least amount of energy. In addition, reconnecting to a network increases energy consumption, and PSM helps reduce that to the minimum. eDRX is a mode that improves power efficiency for cellular UEs by reducing conversation between the devices and the network. While in eDRX mode, a device can discontinuously listen for pending data indications from the network instead of having to establish a full connection. This way, the UE uses less power than if it has a full network connection [1, 6].

2.2.3 Sigfox

Sigfox is a proprietary technology of the French company Sigfox S.A. and is one of the first LPWA technologies available on the market (since 2009). Sigfox operates on the unlicensed ISM bands. The network typically has a star or star-of-stars topology consisting of UEs, gateways, and the cloud core [17].

Sigfox uses 192 kHz of the ISM bands (868 MHz in Europe, 915 MHz in North America, and 433 MHz in Asia) in order to exchange messages. Due to the low data rates used for IoT connections, the Sigfox network utilizes Ultra-Narrow Band (UNB) technology. The UL and DL have different characteristics [17]:

- **Uplink**: The UL bandwidth is only 100 Hz in the European area, although 600 Hz can be used in North America. The modulation scheme for UL is Differential Binary Phase-Shift Keying (DBPSK). UL frequency availability in Europe is limited to frequencies between 868.00 and 868.60 MHz, with a maximum power of 25 mW [6, 17].
- **Downlink**: For the DL, the channel bandwidth is 1.5 kHz and Gaussian Frequency Shift Keying (GFSK) modulation is used. This provides a data rate of 600 b/s. In Europe, the DL frequency band is limited to frequencies between 869.40 and 869.65 MHz, and the power output is limited to a maximum of 500 mW [6, 17].

The maximum length of a Sigfox packet is 24 B, where the payload data can take up a maximum of 12 B. As a result, each packet transmission takes approximately 2 seconds at a data rate of 100 b/s. The Sigfox BTSs monitor the full 192 kHz spectrum and look for UNB signals to demodulate. In the UL, the European Union has limited the maximum duty cycle of Sigfox UEs to a maximum mean transmission time of 1 % to ensure that spectrum usage is shared fairly among all users of this and other similar communications systems. This means that an UE can transmit only six 12-byte messages per hour or 140 messages per day. For the DL messages, the payload has a fixed size of 8 B. The duty cycle for the BTS is 10 %, which guarantees four DL messages per device per day. Furthermore, DL communication can only occur following an UL communication [6, 17].

In terms of random access, the transmission between the network and the UE is unsynchronized. The UE transmits a message on a random frequency and then sends 2 replicas of that same message on different frequencies and times. This is referred to by Sigfox as “time and frequency diversity”, see Fig. 2.4. In addition to that, Sigfox also utilizes the principle of “spatial diversity”, which means that an UE is not attached to a specific BTS, unlike cellular protocols. The emitted UL message is received by any BTS that is nearby and on average, the number of BTSs is 3. Spatial diversity in combination with the time and frequency diversity are the main factors behind the quality of service of the Sigfox network [17].

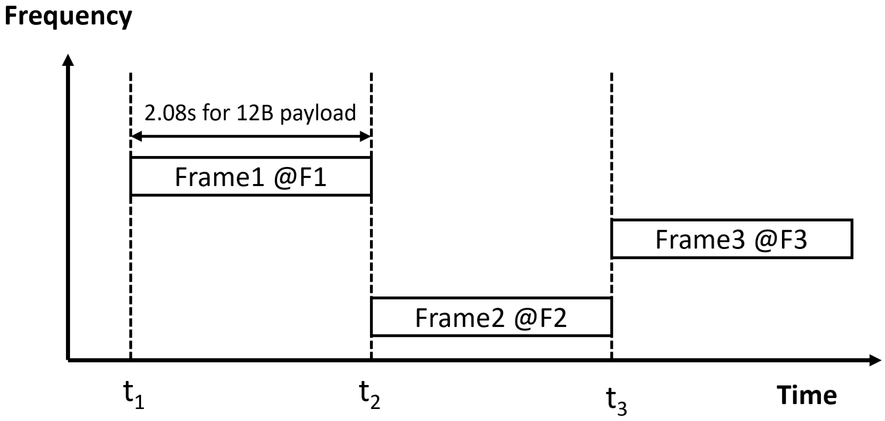

Fig. 2.4: Time and frequency diversity in Sigfox [17]

2.2.4 LoRaWAN

LoRaWAN is another representative of LPWA technologies operating in the ISM spectrum. In addition to the sub-Gigahertz 915 MHz, 868 MHz, and 433 MHz frequency bands, LoRaWAN can also operate on 2.4 GHz to achieve higher data rates, at the cost of range. The LoRaWAN protocol is developed and maintained by the LoRa Alliance [6, 18].

The fundamental building block of the LoRaWAN technology is the Long Range (LoRa) radio modulation technique, which is derived from Chirp Spread Spectrum (CSS) modulation. LoRa modulation is robust against disturbances and can be received across great distances. When compared to other competing wireless technologies, it can provide a significantly greater communication range with low bandwidth. This characteristic make LoRa an excellent choice for low-power sensors and actuators [6, 18].

LoRaWAN is a MAC layer protocol built on top of the LoRa modulation. While the LoRa physical layer is responsible for enabling the long-range communication link, LoRaWAN defines the system architecture and communication protocol for the network. In Europe, the bandwidth usage of LoRaWAN is limited to 125 kHz and 250 kHz, while in other regions, it can go up to 500 kHz. The modulation speed of LoRa is determined by spreading factors (SF), which can take six different values, ranging from SF7 to SF12. The choice of SF determines the trade-off between coverage area and bandwidth, and data rates can vary from 300 b/s to 50 kb/s, depending on the selected SF value [5, 18].

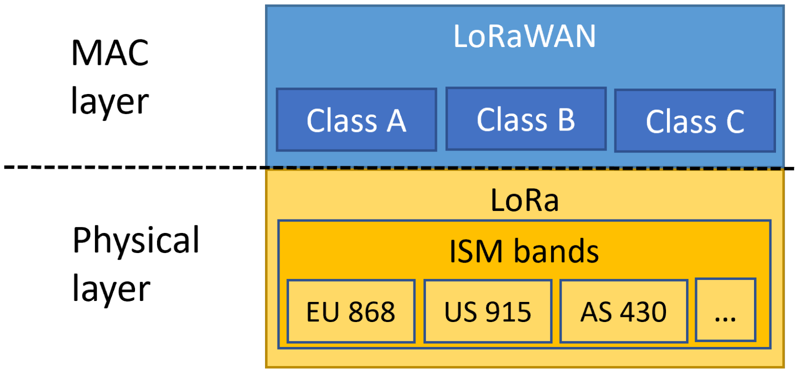

Fig. 2.5: Physical and MAC layers of LoRaWAN technology [18]

LoRaWAN defines three device types: Class A, Class B, and Class C. All LoRaWAN devices must implement Class A, while Class B and Class C are optional extensions. All device classes support bi-directional communication [6, 18].

- **Class A**: UEs allow bidirectional communication where each end-device's UL transmission is followed by two short windows for receiving DL messages. If the network server does not respond during these two receive windows, the next DL will be after the next UL transmission. Class A UEs spend most of the time in sleep mode and have the lowest energy consumption [6].
- **Class B** *(end-devices with scheduled receive slots)*: In addition to the uplink-initiated receive windows, Class B devices also have scheduled receive windows for receiving DL messages from the network server. Using time-synchronized beacons transmitted by the gateway, the devices periodically open receive windows. Therefore, Class B devices do not need to send an UL to receive a DL. As a result, the battery life is shorter in Class B than in Class A, because the UE spends more time in active mode [6].
- **Class C** *(end-devices with maximal receive slots)*: UEs continuously keep the DL receive windows open unless they are transmitting in UL. Class C devices have the lowest communication latency but are drastically more energy-intensive than devices of other classes. Class C devices are usually not battery-powered but have a stable energy source [6].

Like Sigfox, LoRaWAN networks are deployed in a star or star-of-stars topology. A typical LoRaWAN network consists of UEs, gateways, network servers, and application servers. Additionally, a join server can be incorporated to manage devices inter-network roaming. LoRaWAN networks use an ALOHA-based channel access method, so UEs do not need to peer with any specific gateway. Messages sent from the UEs travel through all gateways within range. If the network server receives multiple copies of the same message, it keeps a single copy and discards the others [6, 18].

Tab. 2.1: Comparison of current LPWA technologies [1, 5, 17, 18]

	Sigfox	**LoRaWAN**	**LTE Cat NB1**	**LTE Cat NB2**	**LTE Cat M1**	**LTE Cat M2**
Spectrum	ISM	ISM	Licensed	Licensed	Licensed	Licensed
Frequency	868/915 MHz	433/868/915 MHz	700-2100 MHz	700-2100 MHz	700-2600 MHz	700-2600 MHz
Technology	Proprietary	PHY Proprietary MAC Open	Open LTE	Open LTE	Open LTE	Open LTE
Bandwidth	100, 600 Hz	125, 250, 500 kHz	200 kHz	200 kHz	1.4 MHz	5 MHz
MCL	162 dB	157 dB	164 dB	164 dB	155.7 dB	155.7 dB
Max. EIRP	UL 14 dBm[1], DL 27 dBm	14 dBm	23 dBm	23 dBm	23 dBm	23 dBm
Max. playload	UL 12 B, DL 8 B	242 B	1600 B	1600 B	8188 B	8188 B
UL data rate	0.1-0.6 kb/s	0.3-50 kb/s	0.3-62.5 kb/s	0.3-159 kb/s	HD 375, 590 kb/s FD 1, 3 Mb/s	HD 2.625 Mb/s FD 7 Mb/s
DL data rate	0.6 kb/s	0.3-50 kb/s	0.5-27.2 kb/s	0.5-127 kb/s	HD 300, 800 kb/s FD 0.8, 1 Mb/s	HD 2.375 Mb/s FD 4 Mb/s
Power consumption	Tx: 14 mA Rx: 7 mA PSM < 1 µA	Tx: 44 mA Rx: 12 mA PSM < 1 µA	Tx: 240 mA Rx: 46 mA PSM < 3 µA	Tx: 240 mA Rx: 46 mA PSM < 3 µA	Tx: 360 mA Rx: 70 mA PSM < 8 µA	Tx: 360 mA Rx: 70 mA PSM < 8 µA
Battery life	10+ years	10+ years	10+ years	10+ years	10+ years	10+ years
Security	AES-128	AES-128	LTE Security	LTE Security	LTE Security	LTE Security

[1] The value is relevant for EU

3 Long Term Evolution Machine Type Communication – LTE-M

A very notable feature of LTE-M that makes it stand out from other LPWA technologies is that it is designed to support a wide range of IoT applications. Besides mMTC applications that require low device cost, low power consumption and wide coverage, LTE-M is also capable of supporting applications that require more mobility, lower latency and comparatively higher data rates, which otherwise could not be supported by other LPWA technologies. LTE-M also supports Voice over LTE (VoLTE) capability. Furthermore, unlike NB-IoT, which is targeted primarily at low-end IoT applications, LTE-M is designed so that its performance and functionality are suitable for both low-end and middle-end applications. These advantages, however, come with a cost. LTE-M requires more bandwidth, is generally more expensive and can not operate in guard-band mode for now [6].

LTE-M is well-suited for various IoT applications such as smart transportation, healthcare services, and industrial applications. It can also be used for applications that require deep and extensive coverage where there are less strict requirements for latency, voice capability, mobility, and data rates. Some examples of such applications include smart grid, smart city, and home automation. LTE-M is considered to have the most use cases among all LPWA technologies because of its wide performance capabilities and the use of LTE as its foundation [6].

3.1 LTE-M Architecture and 3GPP Standardization

LTE-M architecture is based on LTE. The radio access network is called Evolved UMTS Terrestrial Radio Access Network (eUTRAN) and is composed of UEs and the eNodeB. eUTRAN uses OFDMA in DL and SC-FDMA in UL. The eNodeB provides radio access, management functions and radio bearer to UEs. The core network is referred to as Evolved Packet Core (EPC). EPC's components provide mobility management, authentication, session management, setting up bearers and application of different Quality of Services (QoS). Together the eUTRAN and EPC define the Evolved Packet System (EPS) [1, 6].

EPC consists of several nodes which provide different functionalities. The Packet Data Network Gateway (P-GW) is responsible for communication to an external packet data network. The Serving Gateway (S-GW) acts as a router that routes user data packets between the P-GW and the eNB. A so-called EPS bearer, associated with QoS requirements, establishes the connection between the P-GW and the UE. Control signaling and data are separated using the Control Plane (C-Plane) and the

User Plane (U-Plane). The MME is connected to the eNodeB via the C-Plane. The MME is responsible for mobility management, location update, bearer management and handover support. In addition, the MME is also connected to the HSS, which is a central database containing user-related and subscription-related information for user authentication purposes [6].

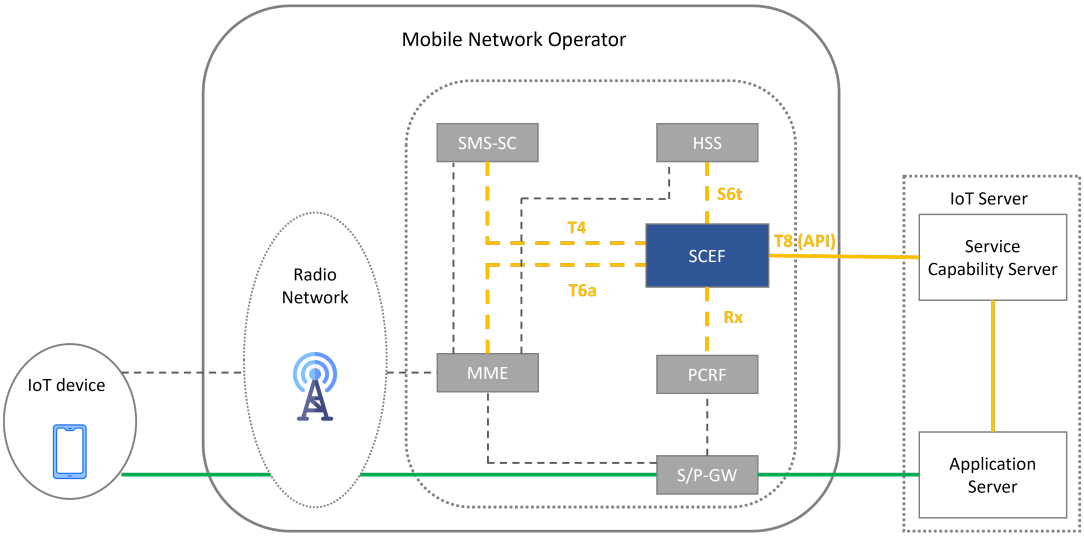

Fig. 3.1: LTE-M architecture [19]

Based on LTE, LTE-M was developed as a progressive set of 3GPP Releases 13–15. Although Release 12 was the first attempt of 3GPP to provide primitive support for IoT applications using the foundation of LTE, Release 13 is considered the first standardization for LTE-M with the completion of the work item *Further LTE Physical Layer Enhancements for MTC*. The advancements of Release 13 are mainly in coverage enhancement and additional power saving. It is also in Release 13 that LTE device category M1 (Cat-M1) was introduced. The LTE-M standard was then further developed in 3GPP Releases 14 and 15. Release 14 introduced various improvements, such as support for higher data rates, improved VoLTE, multicast support, improved positioning and the new device category M2 (Cat-M2). Release 15 introduced further improvements regarding reduced power consumption and latency, improved spectral efficiency and more [6, 20, 21].

3.2 LTE-M Radio Access Design Principles

3.2.1 Coverage Enhancement

The objective of coverage enhancement (CE) is to provide coverage for devices with challenging coverage conditions, such as stationary water/gas/electricity metering devices located in basements. CE is developed because LTE-M needs to support better coverage compared to LTE. The fact that many IoT applications have very relaxed requirements on latency and data rates is exploited to enhanced the coverage through repetition or retransmission techniques [6].

Maximum Coupling Loss (MCL) is a parameter used by 3GPP to evaluate coverage in wireless communication systems. MCL is defined as the maximum loss in the conducted power level that a system can tolerate and still be operational. The higher MCL value is, the more robust the link between the transmitter and the receiver. Without CE feature, previous LTE systems up to Release 12 had an MCL of around 144 dB, which is enough to satisfy most outdoor use cases. However, providing indoor coverage is more challenging due to high penetration loss caused by obstacles such as walls and floors. For instance, if a device is situated deep inside a building or underground, external wall penetration loss and in-building penetration loss can significantly attenuate the signal, making it harder to maintain a reliable communication link [6].

From Release 13, LTE-M supports two CE modes:

- **CE mode A:** This mode is mandatory and is the default operation mode for LTE-M devices and networks. It supports a maximum of 32 subframe repetitions of the data channels, and is optimized for moderate coverage enhancement while still maintains the high-performance features of LTE-M, such as higher data rates, voice call capability, and mobility support [6, 20].
- **CE mode B:** This mode supports up to 2048 subframe repetitions of the data channels. It is optimized to provide extremely deep coverage, which may be needed in more challenging indoor scenarios. This is achieved at the cost of throughput and latency since the number of repetitions is large. Limited or no mobility support is available. The number of repetitions in CE mode B is configurable (from 192 to 2048 repeats). Support for this mode is optional, if a device supports CE mode B, it also supports CE mode A [6, 20].

LTE-M devices only use CE mode when they are required to stay within coverage, i.e. when they are outside the normal coverage range. When in normal coverage, the devices will use normal LTE operation instead of CE mode. This allows them to take advantage of high performance in terms of data rates and latency [6, 20].

3.2.2 Power Saving and Extended Battery Life

LPWA technologies must be power-efficient to ensure long battery life for end devices. In most use cases, the battery of a device should be able to reach and exceed 10 years lifetime. In the case of LTE-M, power saving and extended battery life was addressed for the first time in Release 12 with the introduction of Power

Saving Mode (PSM). In Release 13, power saving was further improved by 3GPP with the introduction of extended Discontinuous Reception (eDRX). Although they are two separate features, PSM and eDRX complement each other and are usually deployed together. It is also noteworthy that these features are supported by both LTE-M and NB-IoT. The main idea behind PSM and eDRX is that they help reduce the energy consumption of a device by minimizing any unnecessary active time for its transmitter and receiver. However, power saving is achieved at the cost of reduced device reachability and increased DL latency. These features will be described in detail in chapter 6 of the thesis [6].

In addition to PSM and eDRX, other techniques are used to achieve power saving in LTE-M, including Connected Mobility Mode (CMM) and the use of control plane for data traffic [6, 20].

Two main mobility modes are supported by LTE: Idle Mobility Mode (IMM) and CMM. In IMM, the UE is responsible for reselecting a cell if it loses connection. This approach is used for smartphones in standard LTE network. In CMM mode, the network controls UE mobility. The network is in charge of deciding when the UE should connect to a new cell and triggers the handover process, which reduces complexity for the UE and hence reduces its power consumption. CMM is used for LTE-M devices and is supported only in CE mode A [6, 20].

In order to optimize power consumption for IoT applications that infrequently transmit small amounts of data, the control plane can be utilized to carry user data traffic. By using the control plane for user traffic, the amount of signaling required and the time needed to establish data bearers can be reduced, leading to a reduction in power consumption of UE [6].

3.2.3 Reduction of Device Complexity and Cost

Throughout the development of LTE-M, several efforts have been made by 3GPP to reduce the complexity of devices with the ultimate goal to bring down the LTE-M device cost substantially to make this technology more attractive for low-end IoT applications. The cost reduction methods utilized for LTE-M devices include reduced peak rates, single receive antenna, reduced bandwidth, half-duplex operation and reduced maximum transmit power [1].

In Release 12, LTE device Cat-0 was introduced. For devices in this category, the peak rate for user data was reduced to 1 Mbps in DL and UL (instead of at least 10 Mbps in DL and 5 Mbps in UL for Cat-1 and higher categories). Additionally, Cat-0 devices only have a single receiving antenna (instead of at least two) and can support half-duplex operation. Devices that only support half-duplex operation have a lower peak transmission rate compared to devices that support full-duplex operation – rather than reaching the peak performance of 1 Mb/s in UL and DL, transmission by these devices is only in the order of about 400 kb/s. In return, devices that only support half-duplex operation are less complex and less costly since they may be implemented with fewer and less expensive components [1].

Release 13 introduced the LTE Cat-M1 category. In addition to all the cost reduction features of Cat-0, Cat-M1 devices also support a reduced bandwidth of only 1.4 MHz and optionally a lower device power class (Power Class 5) with a maximum transmit power of 20 dBm (instead of 23 dBm as in conventional LTE). In Release 15, an even lower power class of 14 dBm (Power Class 6) was introduced. The main benefit which the lower power classes offer is that they facilitate integration of the power amplifier in a single-chip implementation. In addition, the device may be more compatible with simpler battery technologies that can only sustain a low battery discharge power [1, 20].

3.3 LTE-M Physical Layer

The physical layer of LTE-M will be discussed in this section with a focus on how the physical channels and signals are designed to achieve the goals that LTE-M targets, which include extended coverage, power saving, simple operation and low device cost, while still offering performance capable of facilitating both low-end and middle-end IoT applications.

3.3.1 Resource Grid and Frame Structure

As mentioned above, LTE-M is built on and extends the existing LTE technology with functionalities to support operation in IoT. Hence, the basic transmission models in UL and DL in LTE-M are the same as in LTE: SC-FDMA is used in UL and OFDMA in DL.

In LTE and LTE-M, DL and UL transmissions are organized into radio frames of 10 ms each. Each frame is divided into ten equally sized subframes (the length of each subframe is 1 ms). Each subframe is further divided into two equally sized time slots of 0.5 ms. On the higher level, 1024 frames compose one hyperframe of 10.24 s, and 1024 hyperframes make up one hyperframe cycle, which lasts 10485.76 s, see Fig. 3.2 [1].

The radio resource can be organized into a grid, where:

- One time unit equals one time slot. A time slot can contain 6 or 7 OFDM symbols, depends on the size of the Cyclic Prefix (CP), which is inserted at the beginning of each symbol to combat Intersymbol Interference (ISI). The normal CP length can support propagation conditions with a delay spread of

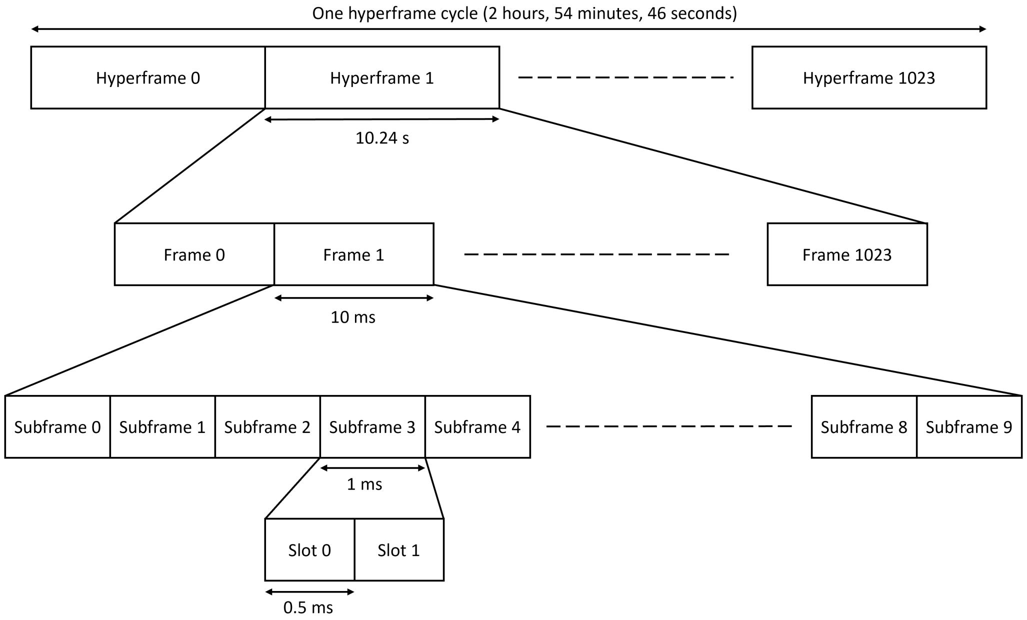

Fig. 3.2: Frame structure for LTE and LTE-M [1]

up to 4.7 µs, while the extended CP is designed to support delay spread of up to 16.7 µs [1].

- One frequency unit contains 12 subcarriers. Each subcarrier is 15 kHz, which makes a frequency unit span 180 kHz [1].

One time unit and one frequency unit make up a Physical Resource Block (PRB). In full-PRB transmission mode, the smallest time-frequency resource that can be scheduled to a device is one pair of PRB mapped over two slots, which corresponds to 12 subcarriers over 14 OFDM symbols (7 symbols per slot), see Fig. 3.3 [1].

The smallest unit in the LTE resource grid is the Resource Element (RE), which is composed of 1 OFDM symbol and 1 subcarrier [1].

3.3.2 Duplex Modes

Both TDD and FDD are supported by LTE-M. In FDD operation, two different carrier frequencies are used for UL and DL. If the device supports full-duplex FDD (FD-FDD) operation, it can perform transmission and reception at the same time. In contrast, if the device only supports half-duplex FDD (HD-FDD) operation, it has to alternate between reception and transmission [1, 20].

A device supporting only HD-FDD mode can work in two operating types:

- **Type A** is capable of fast switching between UL and DL transmission. For each direction of transmission, an oscillator is available for generating the carrier frequency [1].

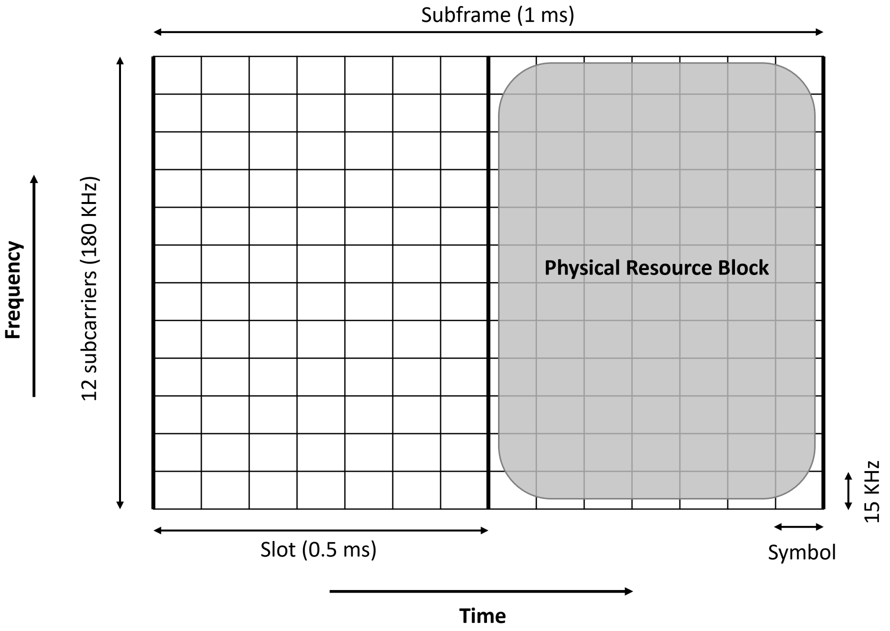

Fig. 3.3: Physical resource block pair in LTE and LTE-M [1]

- **Type B** is mainly used for LTE-M devices when only one oscillator is used for both UL and DL transmission (to reduce the devices' cost). When changing the direction of transmission from UL to DL or from DL to UL, a so-called guard subframe is inserted, which gives the device time to retune its carrier frequency [1].

In TDD mode, the same carrier frequency is used for both DL and UL transmission. The division of so-called "normal subframes" within a frame into UL and DL subframes depends on the UL-DL configuration of the cell in which the device is operating, see Tab. 3.1. The switching from DL to UL and vice versa happens during a guard period within a so-called "special subframe", indicated by the letter "S" in the table. The symbols before the guard period are intended for DL transmission, and the symbols after the guard period are for UL transmission [1].

LTE-M devices can be implemented with one or any combination of the duplex mode mentioned above. This allows the capability of the devices to be set according to the requirements of a particular application and the price range [1].

3.3.3 LTE-M Narrowband and Wideband Operation

LTE supports system bandwidths of 1.4, 3, 5, 10, 15 and 20 MHz including guard bands. Without the guard bands, the greatest system bandwidth (20 MHz) allows for the scheduling of up to 100 PRBs, or 18 MHz. In the case of LTE-M technology, reduced bandwidth is sufficient for receiving and transmitting data. The simplest

Tab. 3.1: UL-DL configuration for TDD operation in LTE and LTE-M [1]

UL-DL configuration	**Subframe number**									
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	DL	S	UL	UL	UL	DL	S	UL	UL	UL
1	DL	S	UL	UL	DL	DL	S	UL	UL	UL
2	DL	S	UL	DL	DL	DL	S	UL	DL	DL
3	DL	S	UL	UL	UL	DL	DL	DL	DL	DL
4	DL	S	UL	UL	DL	DL	DL	DL	DL	DL
5	DL	S	UL	DL	DL	DL	DL	DL	DL	DL
6	DL	S	UL	UL	UL	DL	S	UL	UL	UL

LTE-M devices support a maximum channel bandwidth of 6 PRBs. Oftentimes, the transmissions to or from LTE-M devices have to take place inside one of many nonoverlapping narrowbands with the size of 6 PRBs, as shown in Fig. 3.4 for the 15-MHz system bandwidth case [1].

For all system bandwidths, with the exception of the smallest one (1.4 MHz), the bandwidth cannot be evenly divided into narrowbands of 6 PRBs. Therefore, some PRBs will not be part of any narrowband. If the total number of PRBs of a system bandwidth is odd, the PRB at the center of the bandwidth will not be included in any narrowband, and if there are any remaining PRBs not included in any narrowband, they will be distributed evenly at the bandwidth's edges. The PRBs which do not belong to any narrowband cannot be used for LTE-M-related transmissions on the following channels: Physical Downlink Shared Channel (PDSCH), Physical Uplink Shared Channel (PUSCH) and MTC Physical Downlink Control Channel (MPDCCH). However, those PRBs can be utilized for LTE-M-related transmissions on other physical channels/signals and for any other LTE transmissions in the cell [1].

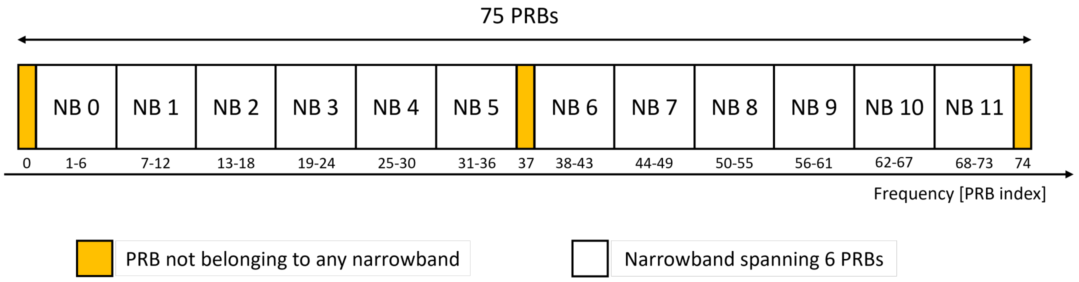

Fig. 3.4: LTE-M narrowbands in 15 MHz bandwidth [1]

The support for larger data channel bandwidths than 6 PRBs was introduced in

Release 14, which motivates the definition of widebands. Each wideband consists of up to 4 adjacent nonoverlapping narrowbands. For smaller bandwidths (1.4, 3, 5 MHz) the wideband contains the whole system bandwidth. For larger system bandwidths (10, 15 and 20 MHz), the number of widebands in each bandwidth is 2, 3 and 4 respectively [1].

3.3.4 Device Categories

As mentioned above, LTE-M defines two low-cost device categories: Cat-M1 and Cat-M2. Introduced in Release 13, Cat-M1 is suitable for MTC applications with low data rate requirements. This would apply to many utility metering applications. Cat-M1 devices can have peak data rates of 1 Mb/s in both DL and UL. With the introduction of Release 14, these devices can support a larger UL transport block size (TBS) of up to 2984 bits instead of the previous 1000 bits. While optional, this larger TBS can be used by Cat-M1 devices in any duplex mode. In FD-FDD mode, the theoretical peak data rate of a Cat-M1 device can reach up to 3 Mb/s with this larger TBS, as opposed to the previous 1 Mb/s [1, 5].

Introduced in Release 14, Cat-M2 is a direct upgrade to Cat-M1, designed to handle higher data rates while still maintaining a long battery lifetime and low device cost. The most significant upgrade of Cat-M2 devices over Cat-M1 is that they support a maximum bandwidth of 5 MHz instead of 1.4 MHz. The larger bandwidth allows data transmission of Cat-M2 to have a maximum channel bandwidth of 24 PRBs (a wideband) in both UL and DL instead of just 6 PRBs (a narrowband), as supported by Cat-M1. Cat-M2 devices can offer peak data rates of 7 Mb/s in UL and 4 Mb/s in DL. In terms of speed, LTE Cat-M2 is currently the fastest device category standardized in any LPWA technology. It's considerably faster than Cat-M1, which is already much faster than NB-IoT and other competing technologies like Sigfox. Even with the introduction of LTE Cat-NB2 (the evolution of NB-IoT), no LPWA device category can compete with Cat-M2 when it comes to data upload and download speeds [20].

Another notable feature is that Cat-M2 is fully backward-compatible with Cat-M1, which means that Cat-M2 devices can operate as Cat-M1 devices in an LTE-M network that has not been upgraded to support Cat-M2 yet. A Cat-M2 device only activates the advanced features when it is configured to do so by a BTS. The physical layer parameters of Cat-M1 and Cat-M2 devices are shown in Tab. 3.2 [1].

Tab. 3.2: Cat-M1 and Cat-M2 physical layer parameters. [1]

Device category	**Cat-M1**	**Cat-M1 with extra-large UL TBS**	**Cat-M2**
Introduced in	Release 13	Release 14	Release 14
Maximum channel bandwidth [MHz]	1.4 (6 PRBS)	1.4 (6 PRBS)	5 (25 PRBS)
Maximum UL transport block size [bits]	1000	2984	6968
Maximum DL transport block size [bits]	1000	1000	4008
Total number of soft channel bits for decoding [bits]	25344	25344	73152
Total layer 2 buffer sizes [bits]	20000	40000	100000
Duplex modes	HD-FDD, FD-FDD, TDD		
HD-FDD operation type	Type B		

3.4 Data Transmission in Downlink

This section will be dedicated to describing the DL physical channels and signals of LTE-M. In the physical layer, Primary Synchronization Signal (PSS), Secondary Synchronization Signal (SSS) and Physical Broadcast Channel (PBCH) are periodically transmitted in the center of the the carrier. MTC Physical Downlink Control Channel (MPDCCH) and Physical Downlink Shared Channel (PDSCH) are transmitted in a narrowband. Downlink Reference Signals (RS) are transmitted in each PRB [1].

The set of DL channels and signals of LTE-M, including physical channels, transport channels and logical channels, is shown in Fig. 3.5. The physical layer provides data transport mechanism to higher layers using transport channels through the MAC layer. The Downlink Control Information (DCI) shown in the figure is not a transport channel, which is indicated by the dashed line. The MAC layer in turn provides data transport mechanism through the use of logical channels [1].

3.4.1 Downlink Subframes

In the System Information (SI), it is possible to broadcast a subframe bit-map with the purpose of indicating which subframes are valid for transmission in LTE-M. The bitmap can take on a size in the range from 10 to 40 bits, which corresponds to the

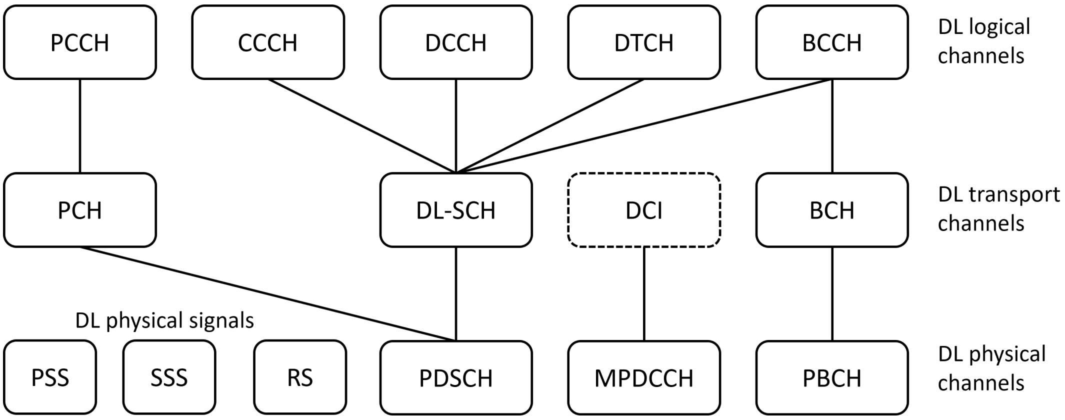

Fig. 3.5: DL channels and signals in LTE-M [1]

number of subframes within 1 to 4 frames (each frame contains 10 subframes). Based on the network's implementation, auxiliary subframes used in DL such as Positioning Reference Signal (PRS) can be marked as invalid for LTE-M transmission [1].

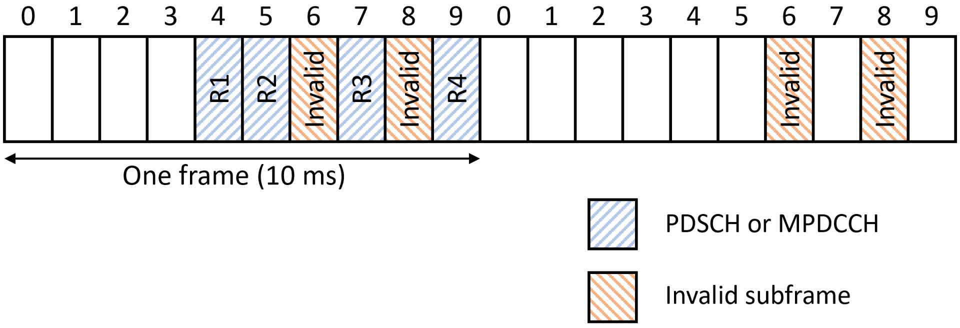

Fig. 3.6: LTE-M subframe bitmap [1]

An example of a 10-bit subframe bitmap is shown in Fig. 3.6, where subframes #6 and #8 are marked as invalid. Normally, if all subframes are valid for LTE-M transmission, the repetitions denoted R1, R2, R3, R4 would be mapped to subframe #4, #5, #6 and #7. However, as shown in the figure, since subframes #6 and #8 were marked as invalid, repetitions of the DL transmission are tied to valid subframes #4, #5, #7, and #9 instead [1].

The DL subframe of LTE-M only utilizes a portion of the REs in an LTE subframe. The DL subframe structure in LTE contains an LTE control region and an LTE data region. The control region consists of one or more OFDM symbols at the beginning of a subframe, and the data region is made up of the remaining OFDM symbols in the subframe. In LTE, data transmissions on PDSCH are mapped to the data region, while a number of control channels, such as the Physical Downlink Control Channel (PDCCH) and Physical Hybrid

Automatic Repeat Request Indicator Channel (PHICH), are mapped to the control region. These control channels are wideband and can cover almost the entire LTE system bandwidth. Since LTE-M is implemented with a much smaller bandwidth, the wideband LTE control channels mentioned above are not used. Instead, a new control channel called MPDCCH is used for LTE-M devices. MPDCCH is narrowband and is mapped to the LTE data region rather than the control region of a subframe to avoid collisions between it and the original LTE control channels. This means that both the control channel (MPDCCH) and the data channel (PDSCH) of LTE-M are mapped to the data region of an LTE subframe [1].

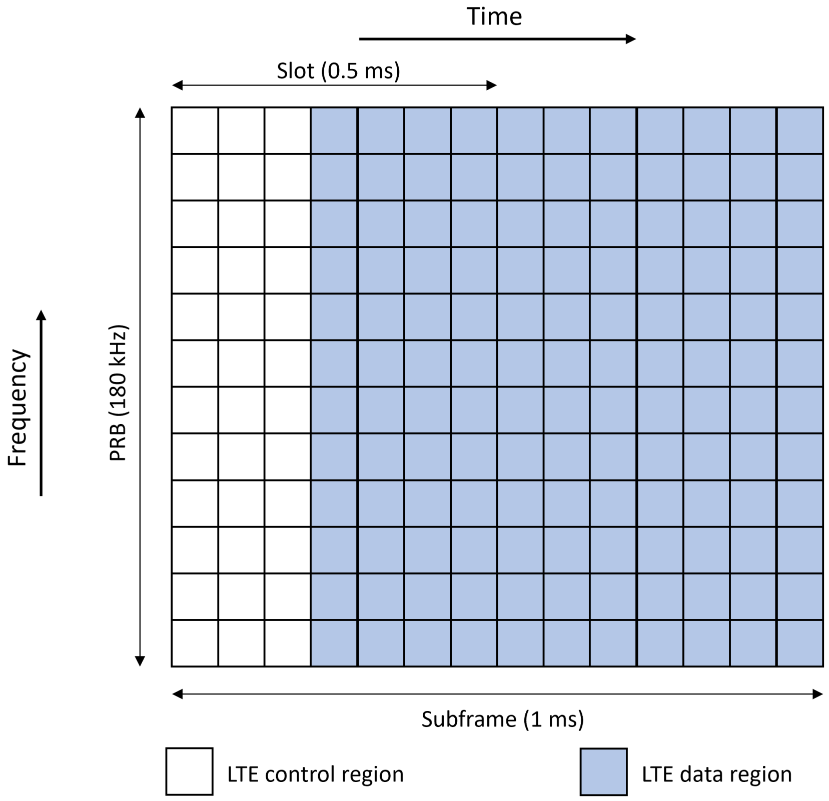

Fig. 3.7: DL subframe structure in LTE [1]

The starting symbol for LTE-M transmissions in a subframe is explicitly configured for each individual cell and is broadcasted in the SI. The possible LTE-M starting symbols are the second, third and fourth symbol in an LTE subframe, with the exception of the 1.4 MHz bandwidth, where the possible LTE-M starting symbols are the third, fourth and fifth symbol. In case of TDD, in subframes #1 and #6, the starting symbol of LTE-M is no later than the third symbol due to the position of PSS/SSS [1].

3.4.2 PSS and SSS

The same synchronization technique used by LTE is also used by LTE-M. UEs use PSS and SSS to obtain information about carrier frequency, duplex mode, frame timing, CP length and Physical Cell Identity (PCID) of a cell. The same PCID can be used in two or more cells given that they are far apart enough to prevent ambiguity due to overhearing, which means the number of PCIDs does not limit the total number of cells in a network [1].

Since PSS and SSS are periodically transmitted, an UE can combine the signals received over multiple frames to acquire sufficient information about the cell without the need for additional repetitions on the transmit side (at the cost of increased acquisition delay) [1].

PSS is transmitted every 5 ms in a cell, which allows UEs to acquire the "half-frame" timing of that cell. Like PSS, SSS is also transmitted every 5 ms, but the 2 SSS within every 10 ms are different from each other, which enables the UEs to acquire the frame timing of the cell [1].

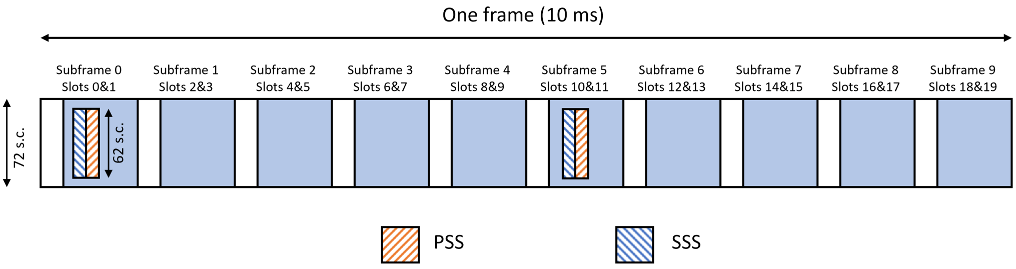

Fig. 3.8: Location of PSS and SSS in FDD mode [1]

In FDD, PSS is mapped to the last OFDM symbol in slots #0 and #10, while SSS is mapped to the symbol right before PSS. In TDD, PSS is mapped to the third symbol of subframes #1 and #6, and SSS is mapped to the symbol three symbols before PSS. This means that UEs can detect the duplex mode of a cell from these synchronization signals. Furthermore, the exact PSS/SSS symbol positions vary slightly depending on the CP length, which means that base on the detection of synchronization signals, UEs can also detect whether normal or extended CP length is used [1].

On the frequency axis, PSS and SSS are mapped to the center 62 subcarriers around a carrier's Direct Current subcarrier (the subcarrier used by the mobile device to locate the center of the OFDM frequency band). This means that the signals fit within the smallest system bandwidth (1.4 MHz – 72 subcarriers) [1].

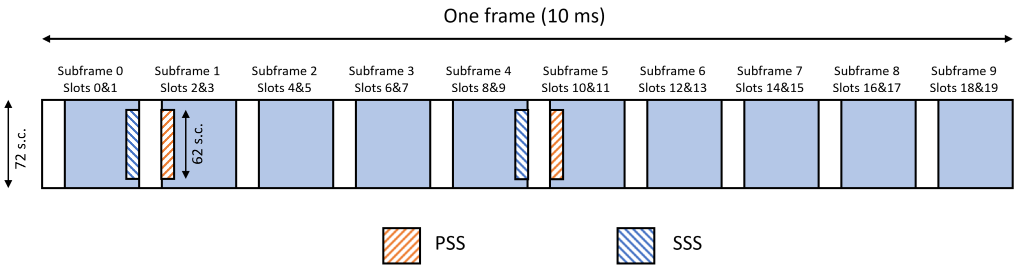

Fig. 3.9: Location of PSS and SSS in TDD mode [1]

3.4.3 Downlink Reference Signals

Unlike physical channels which have higher layer channels mapped to them, reference signals (RS) are special signals that exists only at the physical layer and is not for delivering any specific information. The main purpose of RS is to provide a reference point for the DL power. When an UE needs to know the DL power (the power of the signal from an eNB), it measures the power of this RS and take it as DL cell power. Another crucial role of RS is to help the receiver demodulate the received signal. Since the RS is made up of data known to both transmitter and receiver, the receiver can figure out how the communication channel distorts the data by comparing the decoded received RS and the predefined RS. The result of this comparison is then used to equalize the received user data. The process for the receiver to perform this comparison and figure out the characteristics of a communication channel is called "Channel Estimation" [1, 22].

The Cell-specific Reference Signal (CRS) is a fundamental signal in LTE that serves to provide a stable, dense, and always present DL RS for the UEs. As the name suggests, CSR is common to all users in a certain cell. Besides the functions mentioned above, CRS is used for demodulation of PBCH or PDSCH. CRS is present in every subframe in the cell and is transmitted from one, two, or four logical antenna ports numbered 0-3, with each logical antenna port corresponding to a physical antenna in most cases. CRS is designed to be very dense in time and frequency in order to perform well also in the most demanding cases of data channel demodulation. A CRS port occupies one in every six subcarriers in frequency, and a total two or four OFDM symbols within a subframe, see Fig. 3.10 [1, 22].

Other RSs in the DL include Demodulation Reference Signal (DMRS) and Positioning Reference Signal (PRS). DMRS is used for demodulation of PDSCH or MPDCCH and is device-specific. PRS is a broadcast signal used for the Observed Time Difference of Arrival (OTDOA) positioning method. Using OTDOA, a receiving device's position can be determined based on differences in time of arrival between PRS signals from different, time-synchronized eNodeB [1, 22].

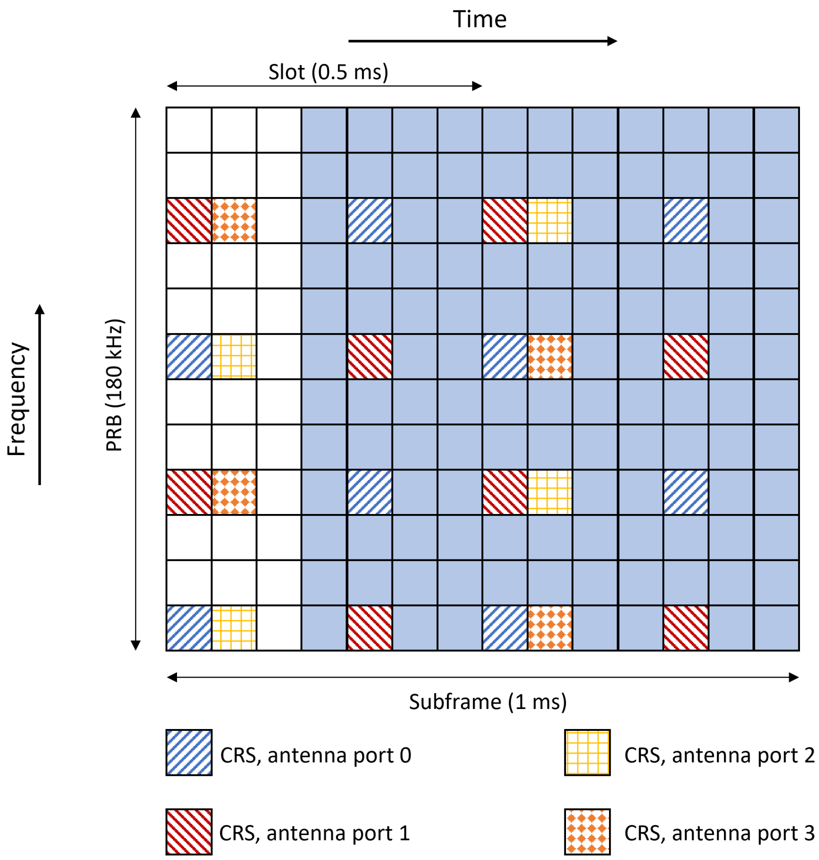

Fig. 3.10: CRS in LTE and LTE-M [1]

3.4.4 MPDCCH

The MTC Physical Donwlink Control Channel (MPDCCH) is one of the most critical features of the LTE-M design. It allows LTE-M to exist inside a standard LTE signal, sharing its radio resources efficiently without requiring any changes to the LTE specifications. As mentioned in 3.4.1, MPDCCH is mapped to the data region of an LTE subframe, so a legacy LTE system is not affected by the presence of LTE-M in the signal [1].

The MPDCCH channel is used to carry DCI, from which UEs can obtain the following types of information [1]:

- UL power control command
- UL grant information
- DL scheduling information
- Paging information and information about changes to the cell's configuration

In the radio physical layer, the address of an UE is a 16-bit number known as the Radio Network Temporary Identifier (RNTI). Every device connected to an eNodeB is assigned an RNTI when the radio channed is established. DCI messages to a device are then scrambled with the RNTI of that destination device, making it very unlikely that one device will accidentally decode a message sent to another device. At any given moment, an idle LTE-M device is monitoring a single MPDCCH in a single narrowband, decoding specific sections of the signal that may contain messages addressed to it, using its own RNTI for descrambling [1].

3.4.5 PDSCH

The Physical Downlink Shared Channel (PDSCH) channel is the main data bearing channel in LTE which is allocated to UEs on a dynamic and opportunistic basis. The PDSCH is also used to transmit broadcast information not transmitted on the PBCH, which includes System Information Blocks (SIB), paging messages and random-access-related messages. The higher layers' data packets are segmented into one or more transport blocks, and PDSCH transmits one transport block at a time [1, 22].

Tab. 3.3: PDSCH modulation and coding schemes and TBS in LTE-M [1]

			TBS in CE mode A						**TBS in CE mode B**	
MSC	**Modulation**	**TBS**	**# PRB pairs**						**# PRB pairs**	
index	**scheme**	**index**	**1**	**2**	**3**	**4**	**5**	**6**	**4**	**6**
0	QPSK	0	16	32	56	88	120	152	88	152
1	QPSK	1	24	56	88	144	176	208	144	208
2	QPSK	2	32	72	144	176	208	256	176	256
3	QPSK	3	40	104	176	208	256	328	208	328
4	QPSK	4	56	120	208	256	328	408	256	408
5	QPSK	5	72	144	224	328	424	504	328	504
6	QPSK	6	328	176	256	392	504	600	392	600
7	QPSK	7	104	224	328	472	584	712	472	712
8	QPSK	8	120	256	392	536	680	808	536	808
9	QPSK	9	136	296	456	616	776	936	616	936
10	16QAM	9	136	296	456	616	776	936	-	-
11	16QAM	10	144	328	504	680	872	1032	-	-
12	16QAM	11	176	376	584	776	1000	1192	-	-
13	16QAM	12	208	440	680	904	1128	1352	-	-
14	16QAM	13	224	488	744	1000	1256	1544	-	-
15	16QAM	14	256	552	840	1128	1416	1736	-	-

Tab. 3.3 shows the modulation and coding schemes (MCS) and TBS for PDSCH in CE mode A and B in Release 13. Since the low-cost Cat-M1 device is restricted to a maximum TBS of 1000 bits, the TBS values greater than 1000 bits do not apply to Cat-M1, only to higher device categories configured with CE mode A. In addition, as

can be seen in the table, CE mode A supports both QPSK and 16QAM modulation scheme, while CE mode B only uses QPSK [1].

3.4.6 PBCH

The Physical Broadcast Channel (PBCH) carries the Master Information Block (MIB), which contains the basic physical system information and cell-specific information needed by the UEs in the cell search. After the UE correctly acquires the MIB, it can then read the DL control and data channels and perform necessary operations to access the network [1, 22].

The PBCH is always confined to the first fours OFDM symbols in the first slot of the first subframe of every radio frame. The eNodeB maps the MIB on the PBCH across four radio frames (40 ms), with portions transmitted in the first subframe of every frame. On the frequency axis, PBCH occupies 72 subcarriers centered around the Direct Current subcarrier [1, 22].

3.5 Data Transmission in Uplink

The set of UL channels of LTE-M is shown in Fig. 3.11. The physical layers provides data transport services to higher layer using transport channels through the MAC layer. The MAC layer then provides data transport mechanism through logical channels. Similar to DCI in DL, the Uplink Control Information (UCI) is not a transport channel, which is indicated by the dashed line. UL Reference Signals are not shown in the figure but they are sent together with Physical Uplink Shared Channel (PUSCH) or Physical Uplink Shared Channel (PUCCH), or they can be sent separately [1].

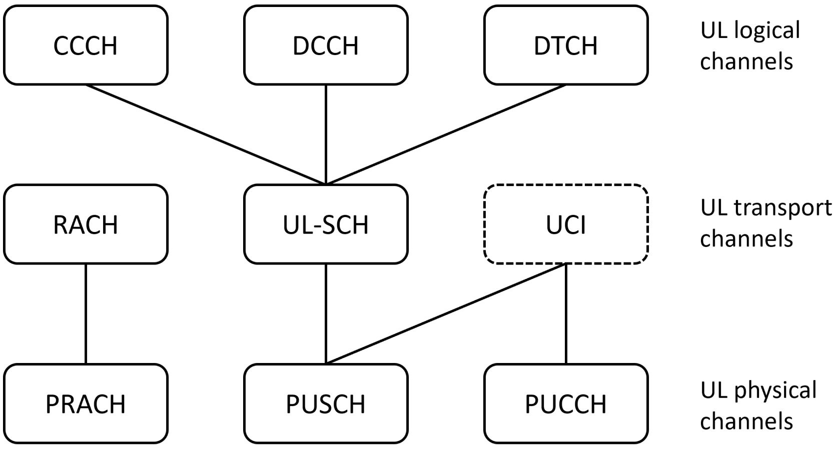

Fig. 3.11: UL channels in LTE-M [1]

3.5.1 Uplink Subframe

Similar to DL, a cell-specific subframe bitmap is broadcasted in the SI to indicate which subframes are valid for LTE-M transmission. The bitmap length for FDD UL is 10 bits, which corresponds to the UL subframes inside 1 frame. The bitmap length for TDD is 10 or 40 bits, corresponding to subframes within 1 or 4 frames. Typically, all UL subframes are set to be valid [1].

When an LTE-M device needs to retune from one UL narrowband to another between two subframes, it creates a guard period for narrowband retuning. This guard period is achieved by not sending two SC-FMDA symbols. If the two subframes both carry PUSCH or PUCCH, the last symbol in the first subframe and the first symbol in the second subframe is truncated. If one of the two subframes carries PUCCH and the other carries PUSCH, two symbols of the subframe carrying PUSCH will be truncated. This is because PUSCH has a more robust channel coding and retransmission scheme than PUCCH. This retuning mechanism is also applied in the DL. In Release 14, the guard period can be configured to be smaller than 2 symbols if the device is capable of performing faster frequency retuning [1].

A shortened format may be used for PUCCH/PUSCH to make room for the transmission of Sounding Reference Signal (SRS) in the last SC-FDMA symbol in an UL subframe, see Fig.3.14 [1].

3.5.2 PRACH

The Physical Random Access Channel (PRACH) is the UL channel used by UEs to initialize the connection to the serving eNodeB. Furthermore, the time of arrival of the received PRACH signal can be used to determine the round-trip propagation delay between the eNodeB and the device [1, 22].

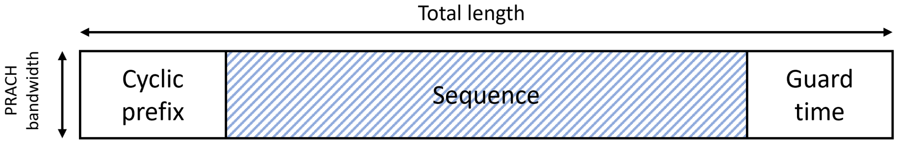

Fig. 3.12: LTE PRACH preamble structure [1]

Tab. 3.4 shows the PRACH formats of LTE, which are reused in LTE-M. Up to 64 PRACH preamble sequences can be defined and a device can use one of these sequences to make a connection attempt in any PRACH opportunity. PRACH configuration is cell-specific in terms of mapping the signal on the subframe structure, a configuration can be dense or sparse in time. An example is shown in Fig. 3.13, where for PRACH format 0, PRACH configuration 2 uses one in every

20 subframes, while PRACH configuration 14 uses every subframe. In LTE-M, with the use of CE, a PRACH preamble structure can be repeated up to 128 times. The repetitions are mapped onto the subframes that are included in the PRACH configuration of the cell [1, 22].

Tab. 3.4: PRACH formats in LTE-M [1]

PRACH format	CP length [ms]	Sequence length [ms]	Total length [ms]	Cell range from guard time	FDD PRACH configurations	TDD PRACH configurations
0	0.10	0.8	1	15 km	0-15	0-19
1	0.68	0.8	2	78 km	16-31	20-29
2	0.20	1.6	2	30 km	32-47	30-39
3	0.68	1.6	3	108 km	68-63	40-47

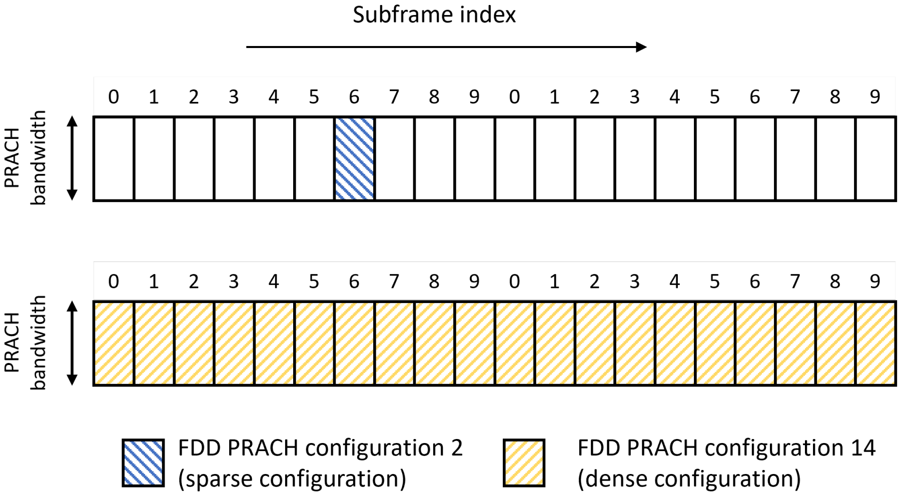

Fig. 3.13: Example PRACH configurations in LTE-M [1]

3.5.3 Uplink Reference Signals

In the UL, reference signals are transmitted from UEs to allow the serving eNodeB to estimate the UL propagation channel in order to demodulate UL physical channel, perform UL quality measurement and so on [1, 22].

The UL Demodulation Reference Signal (DMRS) is used to demodulate PUCCH and PUSCH. DMRS is transmitted in each slot in the transmitted UL subframe. The bandwidth of DMRS is equal to the bandwidth of the associated PUSCH or PUCCH transmission. For PUCCH, the channel bandwidth is always 1 PRB, but for PUSCH, the bandwidth can vary from 1 to 6 PRBs [1].

The Sounding Reference Signal (SRS) is used by the eNodeB to get a more accurate calculation of a particular UE's UL channel in the whole system bandwidth.

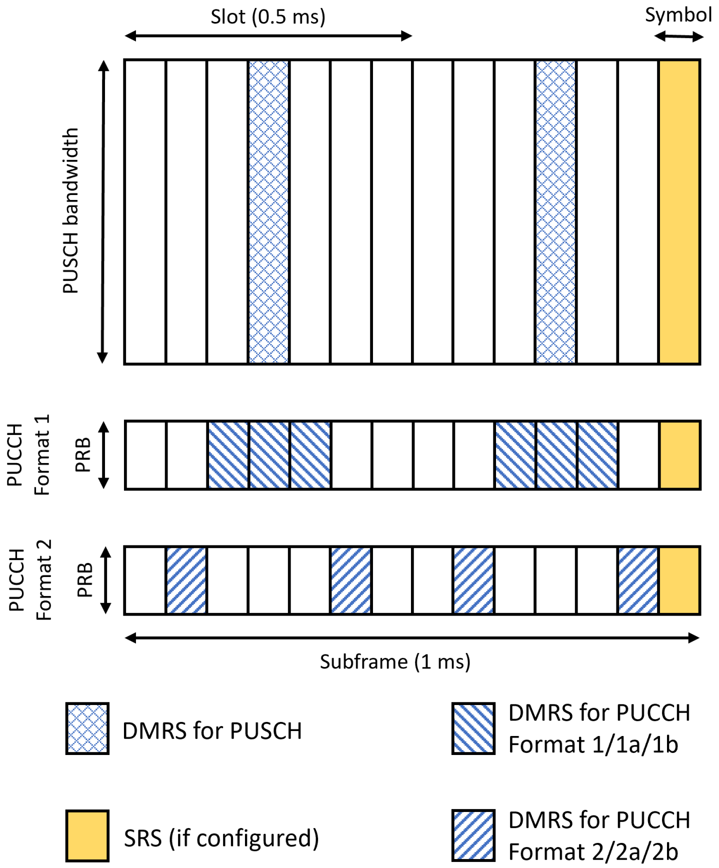

Fig. 3.14: UL reference signals in LTE-M [1]

If SRS is enabled, the last SC-FDMA symbol of some UL subframes in a cell will be reserved for SRS transmission. In this case, UEs will use shortened format for PUCCH and PUSCH in the related subframes to make room for SRS. SRS can be transmitted periodically or aperiodically. Periodic SRS transmission can be configured in RRC configuration, while aperiodic SRS transmission can be triggered when needed by setting the SRS request bit in DCI. Both periodic and aperiodic SRS transmission are supported by CE mode A. CE mode B does not support SRS transmission, but the device will still use shortened format for PUCCH and PUSCH according to the configuration of the cell to avoid collision with SRS transmission from other devices [1, 22].

3.5.4 PUCCH

The Physical Uplink Control Channel (PUCCH) is used to carry three types of control signaling information [1]:

- UL scheduling request (SR)
- ACK/NACK signals for DL transmission

- DL channel state information (CSI)

PUCCH is mapped to a configurable PUCCH region that consists of two PRB locations that are equal distances from the center frequency of the LTE system bandwidth and are commonly chosen to be at the system bandwidth's edges. PUCCH is mapped to the SC-FDMA symbols that are not used by DMRS [1, 22].

Tab. 3.5: PUCCH formats in LTE-M [1]

PUCCH format	**Description**	**Modulation scheme**	**Comment**
1	Scheduling request	On-off keying (OOK)	Supported in CE mode A and B
1a	1-bit HARQ feedback	BPSK	Supported in CE mode A and B
1b	2-bit HARQ feedback for TDD	QPSK	Only supported in CE mode A
2	10-bit CSI report	QPSK	Only supported in CE mode A
2a	10-bit CSI report + 1-bit HARQ feedback	QPSK + BPSK	Only supported in CE mode A
2b	10-bit CSI report + 2-bit HARQ feedback in TDD	QPSK + QPSK	Only supported in CE mode A

The number of PUCCH repetitions used in CE is configured specifically for each device. With CE mode A, the number of PUCCH repetitions can be 1, 2, 4 and 8 repetitions, and different repetition numbers can be configured for different PUCCH format. For CE mode B, a higher number of repetitions can be configured, namely up to 4, 8, 16, 32 in Release 13 and 4, 8, 16, 32, 64, 128 in Release 14 [1, 22].

If a device in connected mode has a periodic PUCCH resource for SR, it can use the allocated resource to request an UL grant when needed, if not, it has to rely on the random access procedure using PRACH to request UL grant [1, 22].

A PUCCH resource for HARQ feedback (ACK or NACK) is allocated when a DL data (PDSCH) transmission is scheduled, and since Release 14 the HARQ feedback for up to 4 DL TB can be bundled into a single ACK or NACK using the HARQ-ACK bundling feature [1, 22].

3.5.5 PUSCH

The Physical Uplink Shared Channel (PUSCH) is mainly used to carry unicast data from the UE to the eNodeB. When the UE receives an UL scheduling grant, the PUSCH carries UL user data and signalling transport blocks arriving from the MAC layer to the physical layer. The transport blocks are sent by the UE one at a time, where CRC is attached to them to help the eNodeB to detect errors. PUSCH can also be used for UCI transmission when required [1, 22].

The MCS and TBS for PUSCH defined in Release 13 is shown in Tab. 3.6. In CE mode A, PUSCH is modulated with QPSK or 16QAM and mapped to 1 to 6 PRB pairs anywhere within a narrowband. In CE mode B, PUSCH is modulated with QPSK and mapped to 1 or 2 PRB pairs within a narrowband [1, 22].

Tab. 3.6: PUSCH modulation and coding schemes and TBS in LTE-M [1]

			TBS in CE mode A						**TBS in CE mode B**	
MSC	**Modulation**	**TBS**	**# PRB pairs**						**# PRB pairs**	
index	**scheme**	**index**	**1**	**2**	**3**	**4**	**5**	**6**	**1**	**2**
0	QPSK	0	16	32	56	88	120	152	56	152
1	QPSK	1	24	56	88	144	176	208	88	208
2	QPSK	2	32	72	144	176	208	256	144	256
3	QPSK	3	40	104	176	208	256	328	176	328
4	QPSK	4	56	120	208	256	328	408	208	408
5	QPSK	5	72	144	224	328	424	504	224	504
6	QPSK	6	328	176	256	392	504	600	256	600
7	QPSK	7	104	224	328	472	584	712	328	712
8	QPSK	8	120	256	392	536	680	808	392	808
9	QPSK	9	136	296	456	616	776	936	456	936
10	QPSK	10	136	296	456	616	776	936	504	1032
11	16QAM	10	144	328	504	680	872	1032	-	-
12	16QAM	11	176	376	584	776	1000	1192	-	-
13	16QAM	12	208	440	680	904	1128	1352	-	-
14	16QAM	13	224	488	744	1000	1256	1544	-	-
15	16QAM	14	256	552	840	1128	1416	1736	-	-

3.6 Security in LTE-M

The security measures of LTE-M are similar to those of the LTE system, from which they originate. The following section will provide an overview of LTE-M security features, including UE's credentials, identity protection, and mutual authentication process between the UE and the network [6, 23].

3.6.1 Credentials and Their Provisioning

In the LTE and LTE-M systems, the International Mobile Subscriber Identity (IMSI) is used as a unique and reliable identifier for the end devices. The IMSI is stored on the Subscriber Identity Modules (SIM) card or Universal SIM (USIM) and is provisioned securely along with an associated subscriber authentication key K_i during the certification procedures to ensure its reliability. The IMSI is used in the authentication process, where the UE asserts its identity, and the network verifies that the device's credentials match that identity. The IMSI is assumed to be unique and permanently associated with a specific subject and is used as a reliable identifier for subscriber devices. By using the IMSI as a unique identifier, LTE and LTE-M systems can establish secure and reliable communication between devices and the network [6, 23].

3.6.2 Identity Protection

Certain protocols need to incorporate measures to safeguard privacy by minimizing the use of fixed identifiers like IMSI that may pose a risk of interception and correlation with the device's activities over time. For example, if the IMSI was broadcasted in the clear over the air, anyone listening would have the UE's unique identifier and then be able to track its locations and movements. Therefore, the use of IMSI over the air should be limited to a minimum, and an alternative mechanism that offers better privacy protection must be implemented [6, 23].

During the first exchange, the UE is forced to send it's IMSI since that is the only way it can authenticate to the network. However, once the device has been authenticated and the radio link has been encrypted, a temporary identifier, called the Temporary Mobile Subscriber Identity (TMSI), is assigned to the UE by the serving MME. The TMSI is assigned to the UE once encryption is setup, so only the network and the device are aware of the mapping between IMSI and TMSI. The TMSI is utilized for all future communication between the UE and the network, hiding the IMSI. The TMSI can be updated or changed at regular intervals to ensure that the IMSI–TMSI mapping cannot be derived by a process of elimination. The TMSI is 4 B long, and only has significance for the serving MME [6, 23].

3.6.3 Authentication

The mutual authentication process between an UE and the LTE-M network is conducted using the Authentication and Key Agreement (AKA) procedure, which is inherited from the LTE system. The AKA authentication procedure is described below and is illustrated in Fig. 3.15.

Authentication Data Request and Response

When an UE tries to access the network for the initial attachment, it sends an Attach Request message containing the IMSI, UE network capability (i.e., the supported security algorithms) and $\mathrm{KSI}_{ASME} = 7$ (Key Set Identifier) to the MME via the eNodeB. The value $\mathrm{KSI}_{ASME} = 7$ signifies that the UE does not have an access security management key (K_{ASME}) yet [6, 23].

When the MME receives an Attach Request, it identifies the UE using the IMSI number attached in the request, and issues a message called Authentication Data Request to the HSS [6, 23].

The HSS, after receiving the request from the MME, is responsible for: (i) checking whether the subscriber corresponding to the ISMI value is a genuine subscriber belonging to the network, (ii) generate an Authentication Vector (AV) to challenge the UE for authentication [6, 23].

The HSS then sends a response called Authentication Data Response to the MME, which contains a number of AVs. An AV includes a random byte array denoted by RAND, the expected response from the UE denoted by XRES, the authentication response denoted by AUTN_{HSS}, and a shared key K_{ASME}. The derivation of all keys in Crypto Functions blocks in this step is based on AKA procedure utilizing MILENAGE (or TUAK) algorithm. The K_{ASME} is kept at the MME and not transmitted to the eNodeB [6, 23].

Authentication Vector Generation

The most crucial component in the authentication procedure is the LTE key K_i, which is 128-bit long and is stored on the USIM of the UE. On the network's side, the same key K_i is also stored in the authentication center (AuC) [6, 23].

On receiving the Authentication Data Request, the HSS checks for the existence of a database record corresponding to the subscriber and retrieves the K_i from the AuC, it also generates a sequence number SQN. The HSS then generates a 16-byte random value and stores it in RAND. The K_i, SQN and RAND values are fed into the MILENAGE algorithm which generates the AUTN_{HSS} token, Cipher Key (CK), Integrity Key (IK) and an expected response XRES. Another set of algorithms called Key Derivation Function (KDF) uses the generated CK, IK from the MILENAGE algorithm to compute the key K_{ASME} [6, 23].

Authentication Request and Response

The MME removes the XRES from the Authentication Data Response received from the HSS, packages the $\{\mathrm{AUTN}_{HSS}$, RAND, $\mathrm{KSI}_{ASME}\}$ into an AV, and then sends an Authentication Request to the UE [6, 23].

The UE computes an AUTN_{UE} token using its K_i and the parameters provided in the Authentication Request. The UE then compares it to the value AUTN_{HSS} that has been provided to authenticate the network. If $\mathrm{AUTN}_{UE} = \mathrm{AUTN}_{HSS}$, the network is authenticated. Once the UE has successfully validated the network it is communicating with, it generates a RES, which is sent as an Authentication Response to the MME [6, 23].

To generate the response RES, the UE needs: K_i, RAND and SQN. The key K_i is stored in the device's USIM, and the RAND is provided by the HSS in the Authentication Request. The SQN, however, is not transmitted directly, but is concealed in $AUTN_{HSS}$. To derive back the SQN, the UE passes the RAND and K_i to the input of the f5 function, which is a part of the MILENAGE algorithm, and then XORs the output with $AUTN_{HSS}$, which produces the required SQN value. With K_i, RAND and SQN, the RES is generated and is sent to the MME for validation [6, 23].

The MME checks if the received response RES from the UE matches the expected response XRES from the HSS and sends a successful (or unsuccessful) authentication message to the UE. If RES and XRES match, the UE is authenticated and attached to the network [6, 23].

K_{ASME} Key Generation

The key K_{ASME} is derived from CK, IK, SQN, and serving network ID (SN ID) through the use of the secure hash algorithm (HMAC SHA-256). For the HSS, CK and IK are derived from the LTE key K_i, which it receives from AuC. The SQN is generated by the HSS itself [6, 23].

For the UE, the CK and IK are derived from the K_i, which is stored on the USIM, and SQN is received from the Authentication Request message. After all the required inputs are derived, they are passed through the Key Derivation Function to generate the K_{ASME}, which is the same on both the HSS and the UE sides [6, 23].

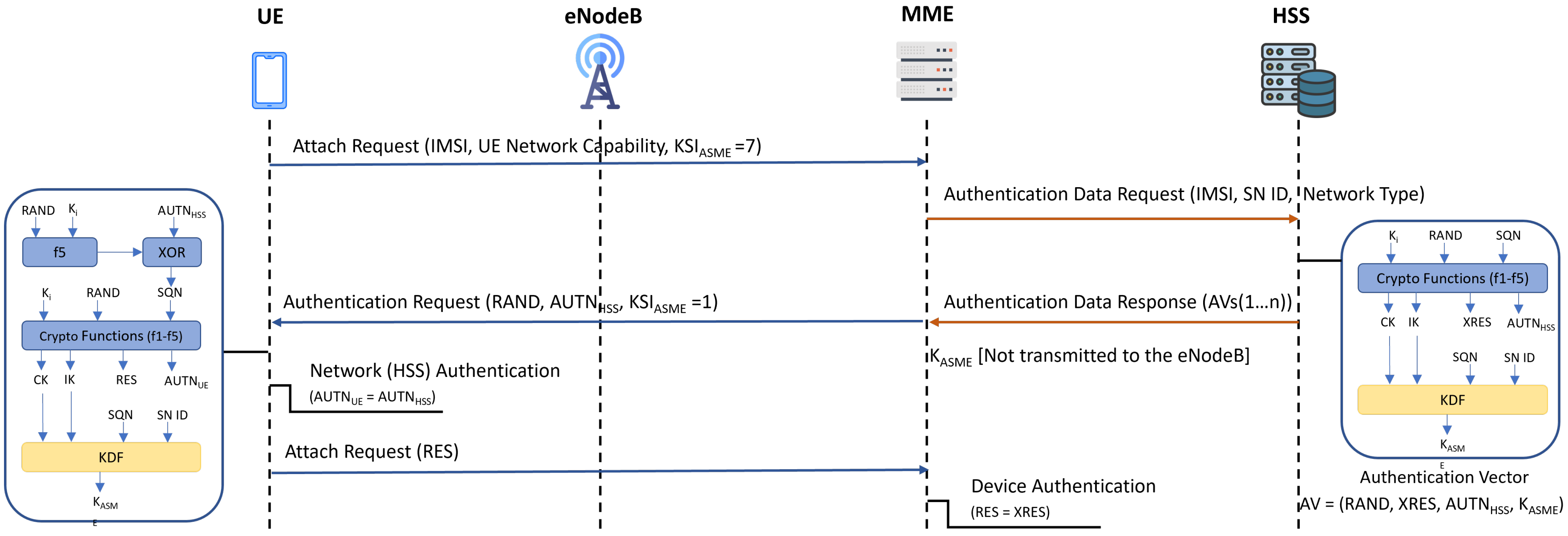
UE
eNodeB
MME
HSS
Attach Request (IMSI, UE Network Capability, KSI$_{ASME}$ =7)
Authentication Data Request (IMSI, SN ID, Network Type)
Authentication Request (RAND, AUTN$_{HSS}$, KSI$_{ASME}$ =1)
Authentication Data Response (AVs(1…n))
K$_{ASME}$ [Not transmitted to the eNodeB]
Network (HSS) Authentication
(AUTN$_{UE}$ = AUTN$_{HSS}$)
Attach Request (RES)
Device Authentication
(RES = XRES)
RAND
K$_i$
AUTN$_{HSS}$
f5
XOR
SQN
Crypto Functions (f1-f5)
CK
IK
RES
AUTN$_{UE}$
SN ID
KDF
K$_{ASME}$
XRES
Authentication Vector
AV = (RAND, XRES, AUTN$_{HSS}$, K$_{ASME}$)

Fig. 3.15: Authentication procedure in LTE-M [6]

4 Network Simulator 3 and The LTE Modules

In this chapter, the Network Simulator 3 (NS-3) and the LTE/EPC Network SimulAtor (LENA) module are briefly described. In addition, the extensions of the LENA module, namely LENA NarrowBand (LENA-NB) and 5G-LENA, are also introduced and their characteristics analyzed.

4.1 Network Simulator 3

NS-3 is an open-source, discrete-event simulation platform for communication networks. It mainly targets research and educational use and is well-known for its good reputation among researchers. It is licensed under the GNU GPLv2 (General Public License version 2) and is publicly available for development and research.

NS-3 is written in C++ and Python, and is designed to be extensible and configurable, allowing users to simulate a wide range of networking technologies and protocols, including wireless networks, cellular networks, and the IP suite. Additionally, NS-3 has a built-in visualization tool called NetAnim that can provide graphical representation of the network topology, making it easier to understand the simulation results [24].

In NS-3, there are five basic components that make up a simulation [24]:

- **Node**: The abstraction of computing devices, which can be used to represent hosts, servers, routers, UEs, eNodeB, etc.
- **Application**: The abstraction of applications that run on NS-3 `Nodes` to drive simulations. These applications are usually used to generate and receive data between the `Nodes` in a simulation.
- **Channel**: The abstraction of communication sub-network, including the media and the used communication technology, such as Wi-Fi channel, Point-to-Point channel, etc.
- **Net Device**: The abstraction of both the hardware network devices and their software drivers. In NS-3, a `NetDevice` is installed on a `Node` to allow that `Node` to communicate with other `Nodes` via `Channels`.
- **Topology Helper**: Topology helpers combine common, repetitive tasks of creating a network topology such as installing `NetDevices to Nodes`, connecting `NetDevices` to `Channels`, assigning IP addresses to interfaces, and so on, into a single, general task for the user's convenience.

4.2 LENA Module

NS-3 includes a mature LTE module called LENA. This module was developed by the University Center Tecnològic de Telecomunicacions de Catalunya (CCTC) and is distributed under an open-source license. The LENA module is divided into two main parts [25]:

- **LTE Model**: This model contains the LTE Radio Protocol stack (Radio Resource Control (RRC), Packet Data Convergence Protocol (PDCP), Radio Link Control (RLC), Medium Access Control (MAC), LTE Physical Layer (PHY)). These entities are located within the UE and the eNodeB nodes.
- **EPC Model**: This models contains core network interfaces, protocols and entities. These entities and protocols are housed within the S-GW, P-GW and MME nodes, and partially within the eNodeB node.

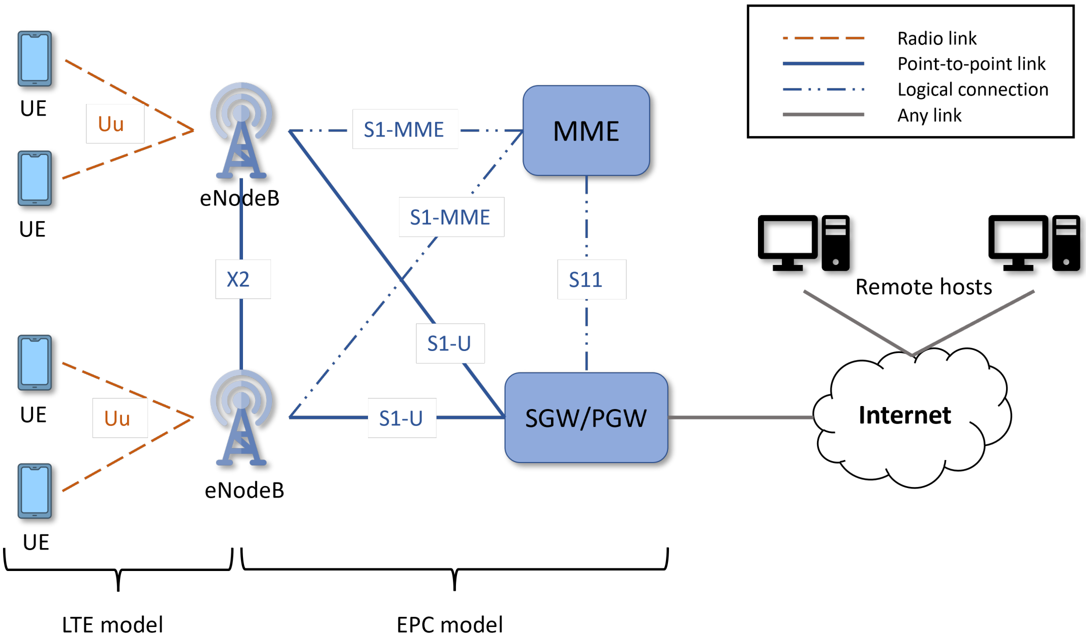

Fig. 4.1: Overview of the LENA module [25]

LENA implements every stack member as an individual C++ class and uses so-called Service Access Points (SAPs) to connect them. These SAPs are divided into two groups, provider SAPs and user SAPs. Provider SAPs implement the interactions performed by a higher layer to a lower one, while user SAPs implement the interactions in the opposite direction, see Fig. 4.2.

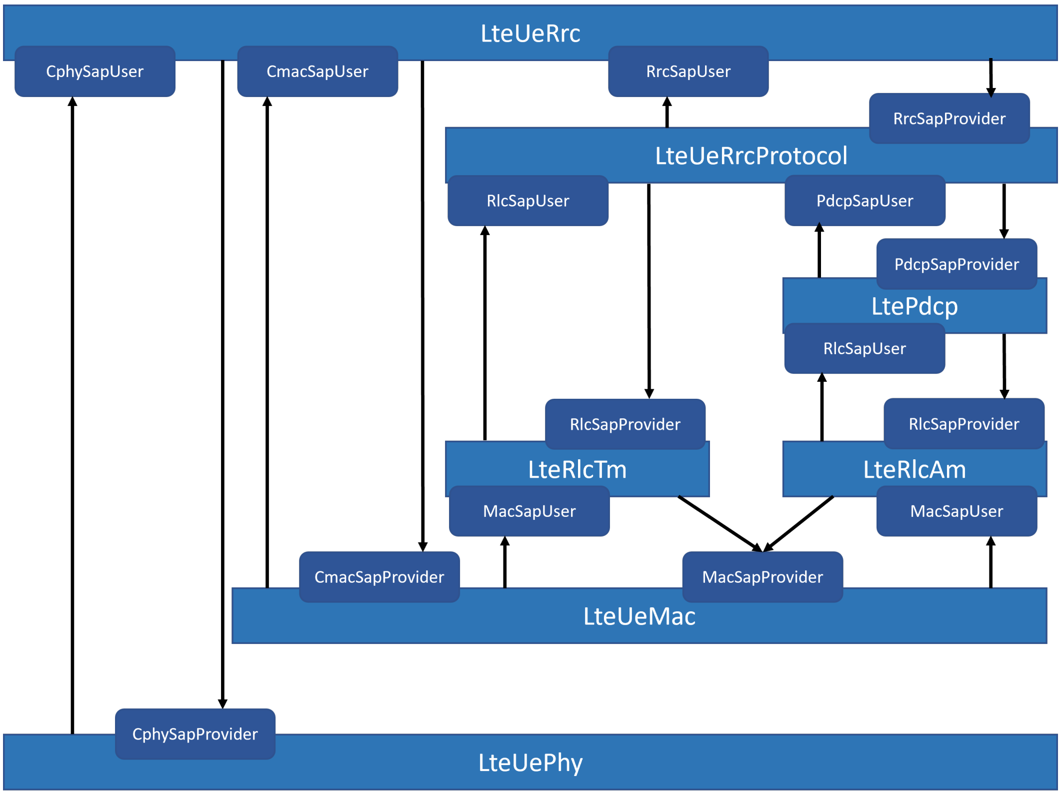

Fig. 4.2: LENA protocol stack [25]

4.3 LENA-NB Module

The LENA-NB module is an extension to the LENA module, developed by the Communication Networks Institute of the Technical University Dortmund. The module is available for public use under the GNU GPLv2 license. The main contribution of LENA-NB is the detailed implementation of the NB-IoT communication technology within the NS-3 simulation framework. It introduced many NB-IoT enhancements to the foundation of LTE inherited from the LENA module [26].

The implementation of NB-IoT was done thoroughly in LENA-NB. For system information exchange, the module's authors implemented the new Master Information Block Narrowband (MIB-NB) and System Information Block Narrowband (SIB-NB) by modifying and extending the *LteEnbRrc* and *LteEnbPhy* layers in the LENA module. The random access procedure of NB-IoT is implemented by modifying the *LteUeRrc*, *LteUeMac* and *LteUePhy* layers. Here, the new Narrowband Physical Random Access Channel (NPRACH) is included to facilitate the random access procedure. The LENA-NB module also includes the connection resume procedure, which is a key component of NB-IoT. Other enhancements include power-saving features and the implementation of an NB-IoT compliant resource scheduler [26].

Besides the core features, two improvements to NB-IoT were also implemented in LENA-NB. The first improvement is Cellular IoT Optimization (C-IoT). This feature enables the transmission of user data over the NB-IoT control plane, which aims to optimize communication efficiency for small UL user messages. The second implemented improvement is the Early Data Transmission (EDT) feature. This feature was introduced in Release 15 and was aimed to provide significant overall performance improvement. EDT is designed to optimize energy and spectral efficiency for short and single data transmission by implementing a new mechanism to the random access procedure, allowing the UE to send data quickly and then return directly to PSM mode [26, 27].

During the creation of the thesis, the LENA-NB module was closely studied and it functionalities were tested with several simulation scenarios. The module functioned properly and the obtained results are in line with the results presented in the published papers of the module's authors. However, it was realized that for the implementation of NB-IoT, the LENA module was fundamentally changed with a large number of modifications and extensions across multiple files, classes and their members. In addition, a close inspection at the code base revealed many unfinished tasks, which could suggest that the module development is still in progress. Therefore, the LENA-NB module is not suitable to be modified and adapted for the implementation of the LTE-M technology in NS-3. Furthermore, the documentation provided by the module's author is very limited, making the task even less viable.

The Power Saving Mode (PSM) and extended Discontinuous Reception (eDRX) features are two important techniques for energy saving and battery life extension for the UEs. They are crucial for mMTC since end devices are often battery-powered and are deployed in hard-to-reach locations. PSM and eDRX are common for NB-IoT and LTE-M, since they are both 3GPP technology standards. Therefore, the way these features are implemented in the LENA-NB module can be used as an inspiration for their implementation for LTE-M in the LENA module. With PSM and eDRX implemented in the LENA module and proper configuration of the simulation environment regarding system bandwidth, transmit power and channel, the behavior of LTE-M can be approximated. Hence, the LENA module enhanced with PSM and eDRX features can serve as a step towards the implementation of the LTE-M technology in NS-3 and can be used for certain purposes, such as energy consumption evaluation of UEs with different communication scenarios and PSM/eDRX settings. The implementation of PSM and eDRX features will be described and the obtained simulation results will be discussed in detail in chapter 6 of the thesis.

4.4 5G-LENA Module

5G-LENA is a new module developed by the CCTC institute to allow simulation of the 5G New Radio (NR) access technology in NS-3. The module was first introduced in 2019 and is distributed under the GNU GPLv2 license [28, 29].

5G-LENA was built as a hard fork of the millimeter-wave (mmWave) module, which was developed by the New York University and the University of Padova. The mmWave module modified the physical layer and the MAC layer of the existing LENA module in order to support mmWave channel, propagation, beamforming and antenna model. Based on the mmWave module, 5G-LENA was developed to be a 3GPP-compliant NR module capable of providing NS-3 simulation capabilities in the bands above and below 6 GHz, aligned with 3GPP NR Release 15. As such, the module incorporates fundamental PHY-MAC NR features, such as a flexible frame structure by means of multiple numerologies support, bandwidth parts (BWPs), Frequency Division Multiplexing (FDM) of numerologies, among others. However, the module still relies on higher layers and core network (RLC, PDCP, RRC, NAS, EPC) of the LENA module, and therefore it only provides a non-standalone 5G implementation [28, 29].

Although the 5G-LENA module significantly extends the LENA module with 5G NR capabilities, it does not implement any additional features to support MTC in general, and the LTE-M technology in specific. The main focus of the module is to allow end-to-end simulation of the NR network. Therefore, the LENA module is still a more suitable platform to be used for the implementation of LTE-M.

5 Performance Evaluation in mMTC Scenarios

In this chapter, several simulation scenarios are created to observe the behavior and evaluate the performance of the LTE system when a large number of UEs is connected to the network. First, the initial simulation scenario with basic elements of the LENA module is created to verify the network's functionality. Then, two extended simulation scenarios are defined. In these scenarios, the number of connected UEs is gradually increased while the information about network performance is gathered and analyzed with the aim to identify the maximum number of UEs that an eNodeB can simultaneously support.

5.1 Initial Testing Scenario

In this scenario, 5 UEs and 1 eNodeB are used. The topology of the scenario is shown in Fig. 5.1. In the figure, it can be seen that the eNodeB is connected to the S-GW, which is then connected to the P-GW and the MME (Node 2). The P-GW is also connected to a remote host, which acts as a server to send and receive data to and from the UEs.

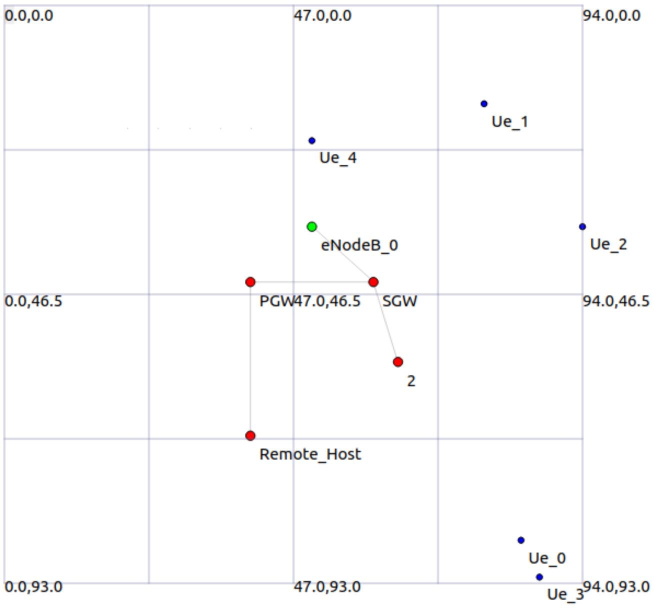

Fig. 5.1: Initial simulation scenario with 5 UEs

The output data from the simulation are gathered using the `FlowMonitor` module, which serves as a system to measure the performance of network protocols

Tab. 5.1: Simulation parameters for the initial testing scenario

Description	**Value**
Number of UEs	5
Number of eNodeB	1
Number of remote host	1
Simulation time	20 s
UE distribution area	0.01 km^2
Bandwidth	5 MHz
Inter packet interval	100 ms
SRS peridiocity	40 ms
Tx power UE	23 dBm
Application	Bulk (TCP)

in NS-3. `FlowMonitor`'s output can be recorded in a XML file and specific parameters of interest can be accessed and printed to the console for better clarity. `FlowMonitor` will be further used to record the results of all simulation scenarios in the thesis.

Fig. 5.2 illustrates the average throughput and Packet Delivery Rate (PDR) of the data streams sent from the UEs to the remote host and back. From the graph, it can be seen that data throughput is reasonable for the 5 MHz system bandwidth, fluctuating around 3000 kb/s for UL data streams. Furthermore, PDR is constantly high, keeping around 100 % for all streams.

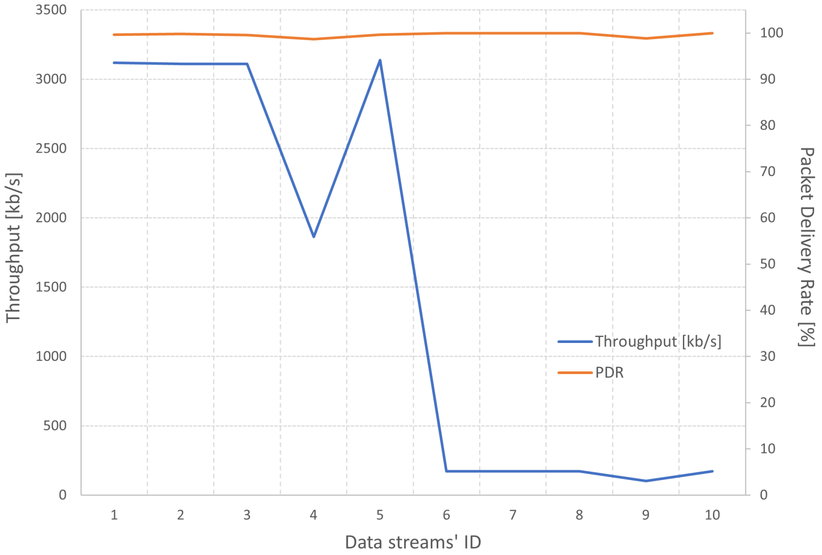

Fig. 5.2: Throughput and Packet Delivery Rate for the initial testing scenario

5.2 Network Performance Evaluation in Extended Scenarios

In the extended simulation scenarios, the number of connected devices is gradually increased. These scenarios are created to evaluate the performance and verify the limitation of the LTE network when it comes to a large number of connected devices, leading to the need for LTE-M technology.

In these simulation scenarios, the UEs are expected to tolerate longer latency and not require high data throughput (under 300 kb/s), but are connected to the eNodeB in much larger numbers. The UEs are distributed randomly in the simulation area. In addition, with the number of UEs increased, the area of the simulation is expanded to 1 km^2, see Fig. 5.3.

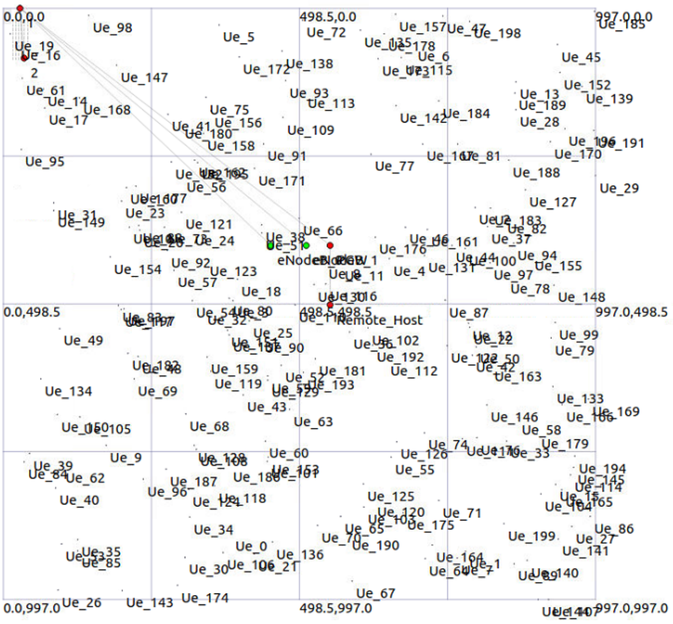

Fig. 5.3: Extended simulation scenario

5.2.1 Extended Scenario Using Bulk Application

In this simulation scenario, the UL data is generated using the `BulkSendApplication` class, which utilizes TCP protocol and generates data at the best effort to fill the communication channel. Definition of the application is shown in Listing 5.1.

Listing 5.1: Definition of the Bulk application

```
uint16_t port = 9; // Echo port number on the remote host
BulkSendHelper source("ns3::TcpSocketFactory", InetSocketAddress(remoteHostAddr, port));
source.SetAttribute("MaxBytes", UintegerValue(0)); // Set the amount of data to send to unlimited

ApplicationContainer sourceApps;
for (uint16_t i = 0; i < numberOfNodes; i++){
    sourceApps.Add(source.Install(ueNodes.Get(i)));
}
```

The simulation results obtained for different numbers of UEs are summarized in Tab. 5.2. From the results, we can see that with the growing number of UEs, the mean throughput decreased as expected. The data are transmitted with relatively high PDR from 5 UEs to 75 UEs but after that, PDR is under 90 % and keeps declining as the number of UEs grows. The rise in mean delay also corresponded to the increasing number of UEs, reaching as high as 1875.54 ms at 250 UEs. The simulation with more devices (275 UEs) led to an execution error, suggesting the network has reached its limit.

Tab. 5.2: Network performance in relation with the number of UEs using Bulk application

Number of UEs	**Mean throughput [kb/s]**	**Packet delivery rate [%]**	**Mean delay [ms]**
5	2868.54	99.44	18.58
10	1457.98	99.34	32.21
20	725.95	98.83	65.23
40	372.12	97.82	165.30
60	92.71	93.30	554.89
75	71.55	93.18	703.76
100	55.34	89.79	836.64
125	46.79	87.93	1005.18
150	37.29	86.75	1288.17
175	34.46	84.98	1497.48
200	30.23	83.58	1641.43
225	29.60	80.11	1804.29
250	26.31	76.42	1875.54
275	0	0	-

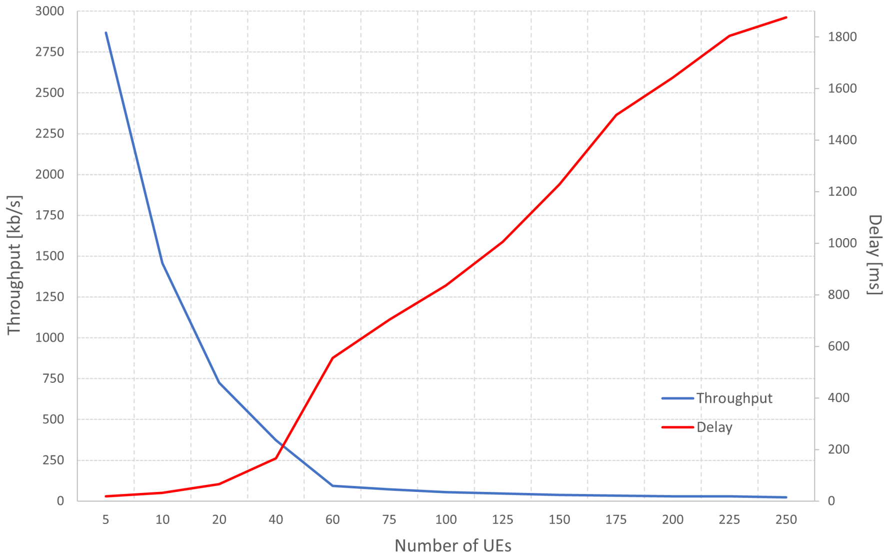

Fig. 5.4: Throughput and latency in relation with the number of UEs using Bulk application

The graph describing mean throughput and delay of the simulation scenario is shown in Fig. 5.4. The graph shows a steep decline of the throughput in the range from 5 UEs to 75 UEs. After that, the throughput started decreasing gradually until it reached 26.31 kb/s at 250 UEs. Mean delay steadily increased as the number of UEs grows.

5.2.2 Extended Scenario Using On-off Application

The `OnOffApplication` allows for better control over the simulation scenario. The application utilizes UDP protocol and allows the data rate, packet size, on time and off time to be configured by the user. After the application starts, on time and off time alternate. During the on time, the application generates constant-bit-rate traffic, while in the off time, no traffic is generated. These features enable a more realistic situation and produces more meaningful results. In the simulation scenario, four On-off applications were defined and installed on the UEs randomly. These applications have different start/end time and on/off interval in order to schedule the UEs' transmission. The definition of an On-off application is shown in Listing 5.2. Since the UEs in this simulation scenario don't require high throughput, the *Datarate* attribute of the application is set to 300 kb/s.

Listing 5.2: Definition of the On-off application

```
//Define application 4
uint16_t portApp4 = 55556;
OnOffHelper onoff4("ns3::UdpSocketFactory",Address(
    InetSocketAddress(remoteHostAddr, portApp4)));
onoff4.SetAttribute("DataRate",DataRateValue(DataRate("300kbps")))
    ; //Set datarate to 300 kb/s
onoff4.SetAttribute("MaxBytes", UintegerValue(uint32_t(10e6)));
onoff4.SetAttribute("PacketSize", UintegerValue(512));

//Set the application to only send 1 s every 2 s
onoff4.SetAttribute("OnTime", StringValue("ns3::
    ConstantRandomVariable[Constant=1]"));
onoff4.SetAttribute("OffTime", StringValue("ns3::
    ConstantRandomVariable[Constant=2]"));
.....
//Define the sink application on the remote host
PacketSinkHelper sink4("ns3::UdpSocketFactory", InetSocketAddress(
    remoteHostAddr, portApp4));
ApplicationContainer sinkApps4 = sink4.Install (remoteHost);
.....
```

Tab. 5.3: Network performance in relation with the number of UEs using On-off application

Number of UEs	**Mean throughput [kb/s]**	**Packet delivery rate [%]**	**Mean delay [ms]**
5	115.01	100	22.42
10	115.01	100	22.48
20	113.97	100	23.27
40	113.45	100	24.12
60	112.64	100	24.07
75	112.17	100	23.73
100	111.18	100	34.51
125	111.06	99.77	76.79
150	110.46	96.96	155.91
175	100.56	89.34	233.03
200	91.66	82.08	287.13
225	83.23	75.15	344.94
250	75.63	69.52	405.71
275	69.79	63.88	462.01

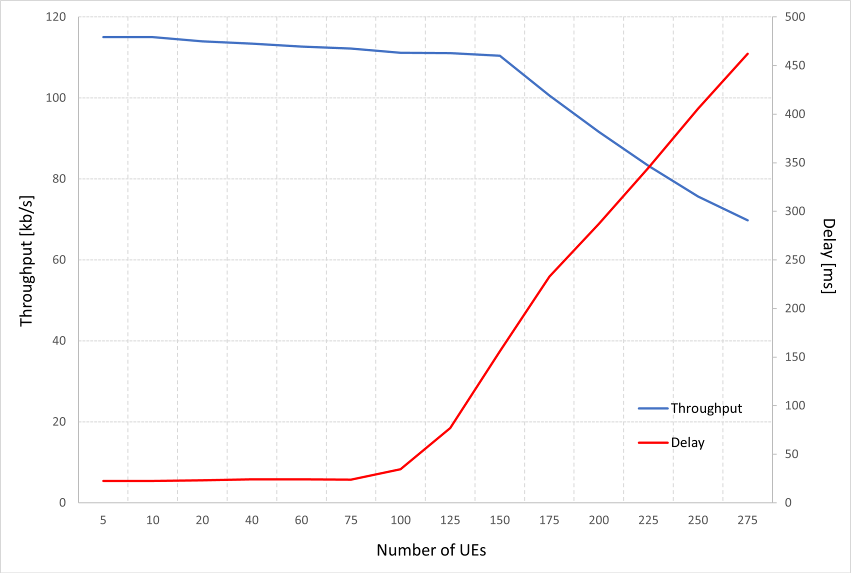

Fig. 5.5: Throughput and latency in relation with the number of UEs using On-off application

The simulation results obtained for different number of UEs are shown in Tab. 5.3 and illustrated in Fig. 5.5. It can be seen from the graph that as the number of UEs grows, the decline in mean throughput and the increase in mean delay are not as steep as when the Bulk application is used. Mean throughput constantly remained above 110 kb/s from 5 UEs to 150 UEs and started declining more quickly from 175 UEs. Mean delay followed the same pattern as it remained relatively low for the number of devices from 5 to 125, and started to increase more drastically from 150 UEs. PDR keeped at 100 % for small number of devices and only started decreasing from 125 devices. However, PDR plummeted rather rapidly and at 275 UEs, it is only 63.88 %, indicating poor communication quality.

From the results obtained from both simulation scenarios using Bulk and On-off applications, it can be concluded that an eNodeB can support a maximum number of approximately 250 end devices communicating simultaneously. While this number is reasonable for H2H communication scenarios, it is far from sufficient for mMTC, where thousands of devices need to be supported. Therefore, enhancements for cellular IoT technologies, namely LTE-M and NB-IoT, are required.

6 Energy Evaluation of LTE-M with PSM and eDRX Features

Power Saving Mode (PSM) and extended Discontinuous Reception (eDRX) are two fundamental features of LTE-M. Since LTE-M devices are usually battery-powered and located in hard-to-reach locations, energy-efficient communication is essential to keep the device functional for a long period of time without the need for battery replacement. PSM and eDRX mechanisms take advantage of the relaxed communication requirements of IoT applications and adjust the pattern of device communication with the network by modifying and extending the RRC state transition timers. With PSM, eDRX and infrequent communication between the device and the network, the battery of an LTE-M device is expected to last more than 10 years.

In this chapter, the PSM and eDRX features of LTE-M are implemented into the LENA module in NS-3. In addition, a separate energy module is also created for energy consumption evaluation of LTE-M devices with PSM and eDRX. After that, three simulation sets with different combinations of PSM timers, eDRX timers and UL data intervals are defined to evaluate the impact of different parameters on UE energy usage as well as battery lifetime expectation.

6.1 Implementation of PSM and eDRX

6.1.1 PSM and eDRX Mechanisms and Timers

Although PSM and eDRX can be deployed separately, it is common that they are deployed together as they are complimentary and can help achieve the balance between end-device reachability and power saving. The combined implementation of PSM and eDRX is shown in Fig. 6.1.

With eDRX enabled, LTE-M devices use paging occasions to listen to DL transmissions instead of having to continuously monitor the control channel for paging. The time period between two paging occasions is referred to as the eDRX cycle and can be configured to a maximum length of 175 minutes. During the configured eDRX cycle, the UE turns off its reception in order to save power. The time the UE spends in eDRX mode is determined by the T3324 Active Timer, which is also known as the eDRX timer. This timer starts when the device moves from connected to idle mode and determines the duration during which the device remains reachable by the network before entering PSM. The maximum value of the T3324 timer is 186 minutes.

After the eDRX timer T3324 expires, the UE moves to PSM, which is an ultra-low-power mode. In PSM, the UE practically shuts down all of its hardware except for the clock, which remains active to keep track of time. This way, the UE can use the lowest amount of energy. The time the UE spends in PSM is determined by the T3412 Extended Timer, which is also known as the periodic Tracking Area Update (TAU) timer. The maximum value of the T3412 timer is 413.3 days. Choosing a proper T3412 timer is very important since when the UE is in PSM, it remains unreachable for the network until there is UL data available to be transmitted, or until the T3412 timer expires and triggers a TAU occasion.

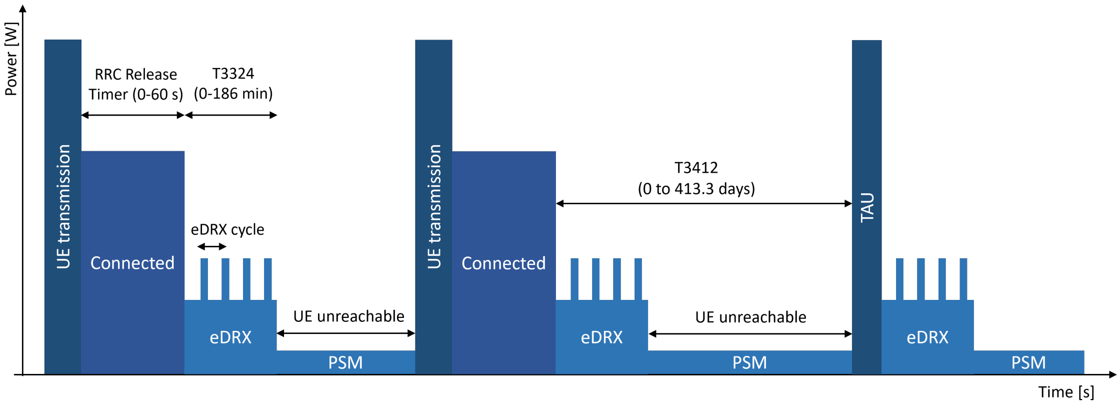

Fig. 6.1: PSM and eDRX mechanisms in LTE-M [30]

6.1.2 Implementation of PSM and eDRX

The implementation of PSM and eDRX here is inspired by the LENA-NB module and the NB-IoT Energy Evaluation module developed by the IDLab research group from the University of Antwerp and the University of Ghent. After a close inspection, it is revealed that the Energy Evaluation module is also based on the LENA module and only minor NB-IoT modifications were made since the focus of the module is to enable power saving features. Therefore, modifications could be made to this module to implement PSM and eDRX for LTE-M [26, 31].

As the first modification, the LTE-M MIB and SIB control messages were implemented to the *lte-control-messages.h* file of the LENA module according to Release 13 specifications. Secondly, new energy states are defined in order to implement power saving features. In the LENA module, the RRC states are defined in the *lte-ue-rrc.cc* file for the UE and *lte-enb-rrc.cc* file for the eNodeB. For the implementation of PSM and eDRX, it is necessary to add news states to these files. In addition, the PSM timer T3412, eDRX timer T3324, RRC release timer and the eDRX cycle must also be implemented.

The timers are added as private member variables to the classes `LteUeRrc` and `LteEnbRrc`. Also, they are made accessible using the *AddAttribute* mechanism of NS-3. Listing 6.1 shows the definition of the timers in the `LteEnbRrc` class in *lte-enb-rrc.cc*, the similar approach is used to define the timers in the `LteUeRrc` class. The `LteHelper` class is then modified to include these timers when the `LteNetDevice` is installed to the eNodeB and the UE, allowing them to be configured by the user during simulation setup.

Listing 6.1: Definition of timers in the `LteEnbRrc` class

```
TypeId LteEnbRrc::GetTypeId (void)
{
  NS_LOG_FUNCTION ("LteEnbRrc::GetTypeId");
  static TypeId tid = TypeId ("ns3::LteEnbRrc")
    .....
    .AddAttribute ("T3324",
                "Timer for the T3324 ",
                IntegerValue ( (0)),
                MakeIntegerAccessor (&LteEnbRrc::m_t3324_d),
                MakeIntegerChecker<int32_t> ())
    .AddAttribute ("T3412",
                  "Timer for the T3412 ",
                  IntegerValue ( (10000)),
                  MakeIntegerAccessor (&LteEnbRrc::m_t3412_d),
                  MakeIntegerChecker<int64_t> ())
    .AddAttribute ("TeDRXC",
              "Timer for the TeDRXC ",
              IntegerValue ( (0)),
              MakeIntegerAccessor (&LteEnbRrc::m_edrx_cycle_d),
              MakeIntegerChecker<int32_t> ())
    .AddAttribute ("RrcReleaseInterval",
              "Rrc Release Interval in ms",
              UintegerValue(10000),
              MakeUintegerAccessor (&LteEnbRrc::
   m_rrcreleaseinterval_d),
              MakeUintegerChecker<uint16_t> (0, 60000) )
    .....
}
```

The definition of new energy states for the UE is shown in Listing 6.2. Because the amount of energy consumed when the UE listens for paging is greater than the amount of energy consumed when the UE remains idle during an eDRX cycle, these two states are defined as different energy states, namely *EDRX_PAGING* and *EDRX_IDLE*. In the Energy Evaluation module, there was no energy state defined for the TAU transmission after the T3412 timer expires. This does not reflect the correct behavior of the UE and the calculation of energy consumption in this case would be inaccurate. Therefore, a new state called *CONNECTED_TAU* was added for the TAU occasions. This state serves as a trigger for the energy calculation method for the TAU message in the energy module, and ensures the correct transition flow of the UE after it exists the PSM mode. After the *CONNECTED_TAU* state, the UE enters eDRX mode to receive paging from the network.

After the new states are added, the timers and the transition between the states are handled mainly by the *SwitchToState* and the *DoSetFrameSubframe* methods. In addition, while the UE is in a state, the time it spent in that state is recorded for energy consumption calculation by the energy module. The example for the *PSM_SLEEP* state is shown in Listing 6.3.

Listing 6.2: RRC states for UE in *lte-ue-rrc.cc*

```
static const std::string g_ueRrcStateName[LteUeRrc::NUM_STATES] =
{
  "IDLE_START", "IDLE_CELL_SEARCH", "IDLE_WAIT_MIB_SIB1",
  "IDLE_WAIT_MIB", "IDLE_WAIT_SIB1", "IDLE_CAMPED_NORMALLY",
  "IDLE_WAIT_SIB2", "IDLE_PAGING", "IDLE_RANDOM_ACCESS",
  "IDLE_CONNECTING", "CONNECTED_NORMALLY", "CONNECTED_HANDOVER",
  "CONNECTED_PHY_PROBLEM", "CONNECTED_REESTABLISHING",
  "EDRX_IDLE", //eDRX Idle
  "EDRX_PAGING", //eDRX Paging occasion
  "PSM_SLEEP", //PSM mode
  "CONNECTED_TAU" //Tracking Area Update occasion
};
```

Listing 6.3: Modification of methods to handle transition between states in *lte-ue-rrc.cc*

```
void LteUeRrc::SwitchToState (State newState){
  .....
  State oldState = m_state;
  //Callback for energy consumption calculation
  Callback<void, double> trigger;
  .....
  switch (oldState)
  {
      .....
      case PSM_SLEEP:
          trigger = MakeCallback(&EnergyModuleLtem::
   Only_psm_decrease, &LEM);
          //Calculate time in PSM mode
          idleTime= ((Simulator::Now()-m_lastUpdateTime).
   GetNanoSeconds());
          m_lastUpdateTime=Simulator::Now();
          trigger(idleTime);
          // Reset timers
          m_t3324 = m_t3324_d;
          m_t3412 = m_t3412_d;
          m_edrx_cycle = m_edrx_cycle_d;
          break;
      .....
  }
  .....
}

void LteUeRrc::DoSetFrameSubframe(uint32_t frame, uint32_t
   subframe){
    .....
    else if(PSM_SLEEP == m_state)
    {
        --m_t3412;
        if ( 0 >= (m_t3412 - m_t3324) )
        {
            SwitchToState(CONNECTED_TAU);
        }
    }
}
```

Similar to the UE side, new states are added to the *lte-enb-rrc.cc* file to implement PSM and eDRX on the eNodeB side. Here, two new states are defined, namely *CONNECTION_EDRX* and *CONNECTION_PSM*, see Listing 6.4. The transition between the states is handled using the *SwitchToState* method, which was modified to enable the two newly added states, see Listing 6.5.

Listing 6.4: RRC states for eNodeB in *lte-enb-rrc.cc*

```
static const std::string g_ueManagerStateName[UeManager::
    NUM_STATES] =
{
  "INITIAL_RANDOM_ACCESS", "CONNECTION_SETUP",
  "CONNECTION_REJECTED", "CONNECTED_NORMALLY",
  "CONNECTION_RECONFIGURATION", "CONNECTION_REESTABLISHMENT",
  "HANDOVER_PREPARATION", "HANDOVER_JOINING",
  "HANDOVER_PATH_SWITCH", "HANDOVER_LEAVING",
  "CONNECTION_EDRX", //eDRX mode
  "CONNECTION_PSM" //PSM mode
};
```

Listing 6.5: Modification of *SwitchToState* method to handle transition between states in *lte-enb-rrc.cc*

```
void UeManager::SwitchToState (State newState){
  .....
  switch (newState)
    {
    .....
    case CONNECTION_EDRX:
        if (false == m_datareceived) //No DL data received in eDRX
        {
            //Schedule transition to PSM when T3324 expires
            id = Simulator::Schedule ( (m_t3324), &UeManager::
    SwitchToState, this, CONNECTION_PSM);
            .....
        }
        break;

    case CONNECTION_PSM:
        //Schedule transition to eDRX after T3412 expires
        id = Simulator::Schedule ( m_t3412 - m_t3324, &UeManager::
    SwitchToState, this, CONNECTION_EDRX);
        .....
        break;
    .....
    }
}
```

6.2 Implementation of Energy Module

For the purpose of evaluating energy consumption of LTE-M devices with PSM and eDRX features, a separate energy module called `EnergyModuleLtem` was created and integrated into the LENA module. The energy module is implemented in the *energy-module-ltem.h* and *energy-module-ltem.cc* files, which are located in the *model* folder in the LENA source code. The energy consumption for each energy state is shown in Tab. 6.1. For the battery, the `LiIonEnergySource` model of NS-3 is utilized. The battery model is located in the *li-ion-energy-souce.h* and *li-ion-energy-source.cc* files in the *energy* module of NS-3. The capacity of the battery is set to 18000 J (5 Wh), which is a common battery capacity for LTE-M devices.

Tab. 6.1: Energy consumption for different states

State	Voltage [V]	Current [A]	Power [W]
PSM	3.6	$7 \cdot 10^{-6}$	$25.2 \cdot 10^{-6}$
Connected	3.6	$10 \cdot 10^{-3}$	$36 \cdot 10^{-3}$
eDRX	3.6	$8.5 \cdot 10^{-3}$	$30.6 \cdot 10^{-3}$
Idle	3.6	$24 \cdot 10^{-6}$	$86.4 \cdot 10^{-6}$
Tx	3.6	$360 \cdot 10^{-3}$	$1296 \cdot 10^{-3}$
Rx	3.6	$70 \cdot 10^{-3}$	$252 \cdot 10^{-3}$

As mentioned above, the energy module is linked to the RRC layer of the UE in the *lte-ue-rrc.cc* file. Each time the UE switches between states, a callback for the corresponding method in the energy module is triggered. The energy module keeps track of the time the UE spends in each state and thereby every time the state changes, it determines the time spent in the old state and calculates the energy usage. The remaining energy in the battery is then reduced accordingly.

An example of the method in the `EnergyModuleLtem` class for calculating energy consumption in PSM is shown in Listing 6.6.

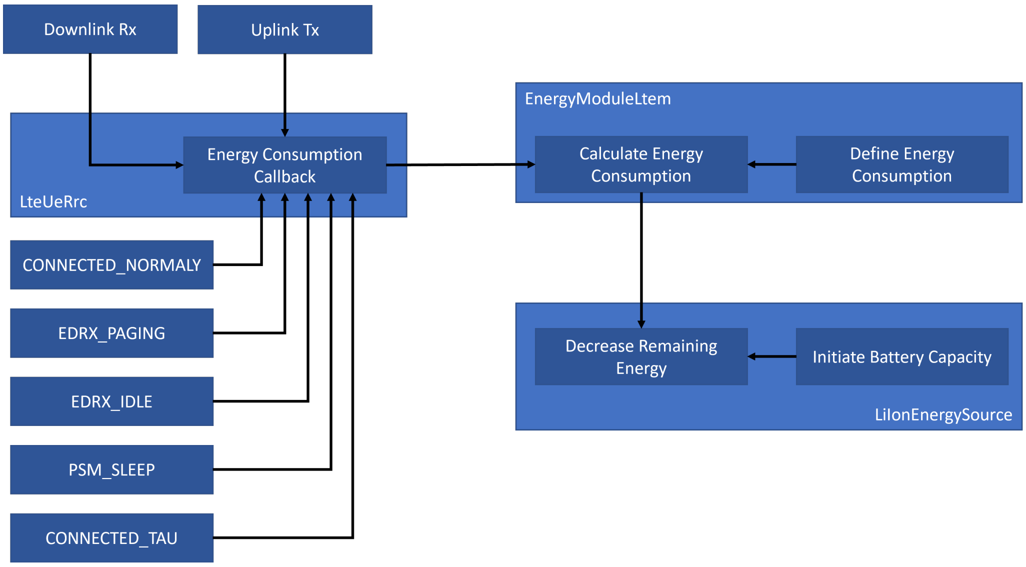
Downlink Rx
Uplink Tx
Energy Consumption Callback
LteUeRrc
CONNECTED_NORMALY
EDRX_PAGING
EDRX_IDLE
PSM_SLEEP
CONNECTED_TAU
EnergyModuleLtem
Calculate Energy Consumption
Define Energy Consumption
Decrease Remaining Energy
Initiate Battery Capacity
LiIonEnergySource

Fig. 6.2: Implementation of the LTE-M Energy Module

Listing 6.6: Energy consumption calculation in PSM mode

```
void EnergyModuleLtem::Only_psm_decrease(double timeInMode)
{
    m_total += timeInMode;
    std::cout<<"Only_psm_decrease: 1 "<<timeInMode<<std::endl;
    Callback<void, double> only_psm;
    only_psm = MakeCallback(&LiIonEnergySource::
   DecreaseRemainingEnergy, &LIES);
    double energyDecreasedPsm = m_voltage * m_psm_current *
   timeInMode / (pow(10,9));
    only_psm(energyDecreasedPsm);
}
```

6.3 Simulation Setup

The LTE-M settings used in the simulation are shown in Listing 6.7. The bandwidth in both UL and DL is set to 6 PRBs, which corresponds to the system bandwidth of 1.4 MHz used by LTE Cat-M1. In addition, the licensed frequency Band 8 is chosen for the simulation. This frequency band (942.5 MHz in DL and 897.5 MHz in UL) is widely used for LTE-M since it balances between good propagation characteristics and data rates. The transmit power of the eNodeB is set to 46 dBm and the transmit power of the UE is set to 23 dBm, which corresponds to Power Class 3.

Listing 6.7: Configuration of LTE-M parameters in simulation scenario

```
//Set the bandwidth to 6 PRBs = 1.4 MHz
lteHelper->SetEnbDeviceAttribute("DlBandwidth", UintegerValue(6));
lteHelper->SetEnbDeviceAttribute("UlBandwidth", UintegerValue(6));

//Set the EARFCN to Band 8 (DL 942.5 MHz, UL 897.5 MHz)
Config::SetDefault("ns3::LteEnbNetDevice::DlEarfcn", UintegerValue(3625));
Config::SetDefault("ns3::LteEnbNetDevice::UlEarfcn", UintegerValue(21625));
Config::SetDefault("ns3::LteUeNetDevice::DlEarfcn", UintegerValue(3625));

//Set the transmission power of the eNB and the UE
Config::SetDefault("ns3::LteUePhy::TxPower", DoubleValue(23.0));
Config::SetDefault("ns3::LteEnbPhy::TxPower", DoubleValue(46.0));
```

The `UdpClient` application is used to generate data. This application allows the packet size, maximum number of packets to be sent and time interval between them to be configured. The inter-packet interval is used in the simulation scenario to determine the communication pattern between the UE and the network. On the remote host, a `PacketSink` application is installed to receive the data from the UE. The definition of the applications is shown in Listing 6.8.

Listing 6.8: Definition of the applications used in the simulation

```
uint16_t ulPort = 2000;
ApplicationContainer clientApps;
ApplicationContainer serverApps;

for (uint16_t u = 0; u < ueNodes.GetN(); ++u){
   ++ulPort;
   PacketSinkHelper ulPacketSinkHelper("ns3::UdpSocketFactory", InetSocketAddress (Ipv4Address::GetAny(), ulPort));
   serverApps.Add(ulPacketSinkHelper.Install(remoteHost));

   UdpClientHelper ulClient (remoteHostAddr, ulPort);
   ulClient.SetAttribute("Interval", TimeValue (MilliSeconds(interPacketIntervalul)));
   ulClient.SetAttribute("MaxPackets", UintegerValue(maxPacket));
   ulClient.SetAttribute("PacketSize", UintegerValue(packetsize));
   clientApps.Add(ulClient.Install(ueNodes.Get(u)));

}
   serverApps.Start (Seconds (1));
   clientApps.Start (Seconds (2));
```

6.4 Simulation Results

For the purpose of evaluating energy consumption of LTE-M device with PSM and eDRX features, three simulation sets are defined:

- Energy consumption for different PSM timers and UL data intervals
- Energy consumption for different PSM timers and eDRX timers
- Energy consumption for different eDRX timers and UL data intervals

Each simulation set will be described and the obtained simulations results regarding energy usage and battery lifetime expectancy will be discussed in the following subsections.

6.4.1 Energy Consumption for Different PSM Timers and UL Data Intervals

In this simulation set, the RRC release timer, eDRX timer T3324 and eDRX cycle remain constant, while the PSM timer T3412 and the intervals between UL transmission change. The simulation time is set to 24 hours. The parameters used for this simulation set are summarized in Tab. 6.2.

Tab. 6.2: Main parameters of simulation set 1

Description	**Value**
Simulation time	86400 s (24 h)
RRC release timer	20 s
eDRX timer T3324	60 s
eDRX cycle	25 s
PSM timer T3412	variable
UL data interval	variable
Packet size	100 B
Tx power UE	23 dBm

The results of the simulation set are shown in Tab. 6.3 and illustrated in Fig. 6.3. The values in the table are the amount of energy the UE consumed in the entire simulation time of 24 hours when configured with different combinations of PSM timer and UL data interval. The unit of measurement is joules per day (J/day).

From the figure, it can be seen that when the PSM timer T3412 is larger than the UL data interval, the amount of energy consumed is the same for different PSM timers. This is due to the fact that the UE wakes up from PSM and initiates UL transmission before the T3412 timer expires, and after each transmission, the timers are reset. Therefore, in this case, the amount of energy consumed by the UE decreases solely in accordance with the increase of the UL data interval.

Tab. 6.3: UE energy consumption per day for different PSM timers T3412 and UL data intervals

UL data	**PSM timer T3412 [h]**			
interval [h]	**1**	**3**	**6**	**12**
1	20.2507	20.2507	20.2507	20.2507
2	11.5461	11.2500	11.2500	11.2500
6	5.7430	5.3482	5.2495	5.2495
12	4.2922	3.8974	3.7987	3.7494
24	3.5668	3.1721	3.0734	3.0240
	Energy consumed [J/day]			

However, in the opposite case,when the PSM timer T3412 is shorter than the UL data interval, the amount of energy consumed increases according to the difference between the T3412 timer and the UL data interval. The shorter the T3412 timer is in comparison with the UL data interval, the more energy is consumed. This is

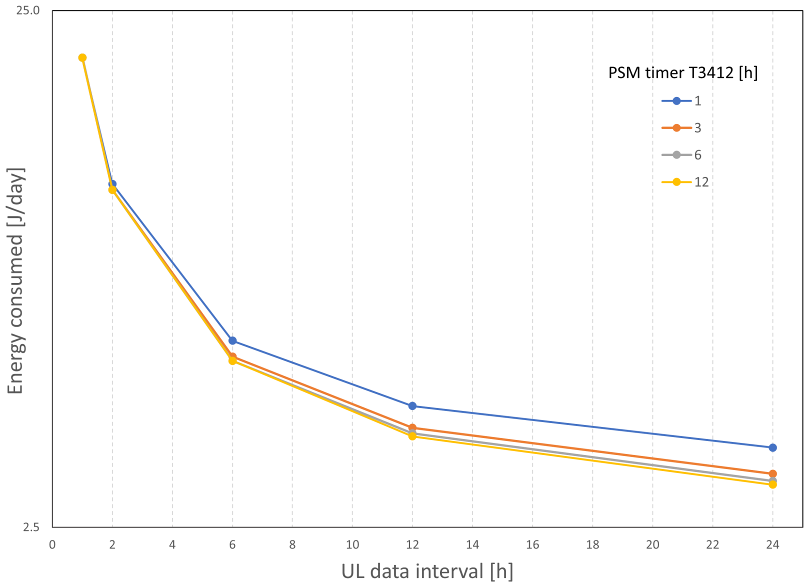

Fig. 6.3: Energy consumption per day for different T3412 timers and UL data intervals

because in the period between the scheduled UL data transmissions, the UE has to wake up to send TAU update messages when the T3412 timer expires. Therefore, in order to maximize energy saving and extend battery lifetime, the PSM timer T312 should be set as close to the typical expected period between UL data transmissions as possible. Nonetheless, we should also take into consideration the fact that when the UE is in PSM mode, it can not be contacted by the network, and DL data has to wait until the T3412 timer expires or when the UE has UL data to send to the network. For this reason, in use cases where it is expected that the UE will have to receive DL data from the network relatively frequently, the T3412 timer shouldn't be too long to ensure device reachability.

The results from Tab.6.3 were translated to battery lifetime by extrapolating the amount of energy the UE consumes in 1 day to the number of days that the battery would last. In the simulation scenario, the capacity of the battery is 18000 J (5 Wh). The resulting battery lifetime in years is shown in Fig. 6.4. It can be seen from the graph that for the most relaxed use case, where the T3412 timer is 12 hours and the UL data interval is 24 hours, the battery could last up to 16.31 years. In contrast, for the use case where the UE sends data once every hour, the battery lifetime expectancy is 2.44 years.

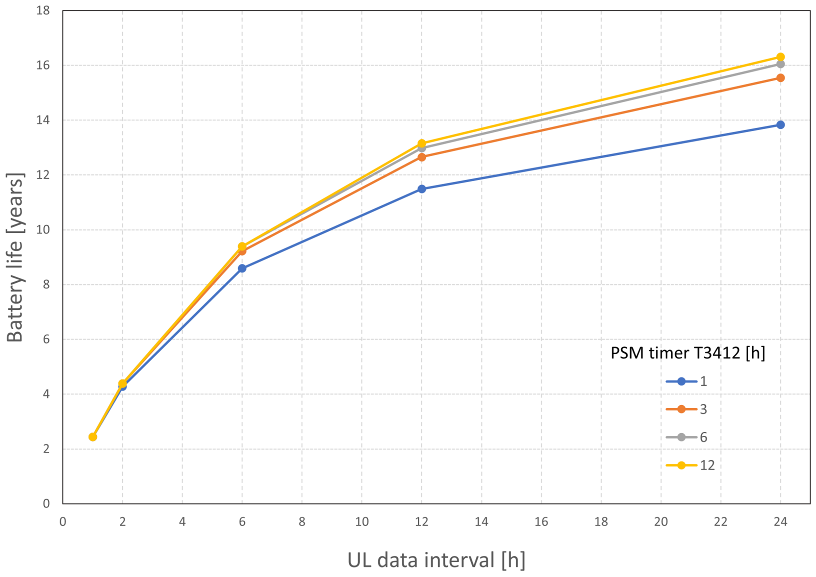

Fig. 6.4: Battery lifetime expectancy for different T3412 timers and UL data intervals

6.4.2 Energy Consumption for Different PSM Timers and eDRX Timers

In this simulation set, the RRC release timer, eDRX cycle and UL data interval remain constant, while the PSM timer T3412 and the eDRX timer T3324 change. The parameters used for this simulation set are shown in Tab. 6.4. The aim of this simulation set is to evaluate the impact of eDRX timer T3324 on energy consumption, therefore, the UL data interval is set to 24 hours, which means the UE only sends data once at the beginning of the simulation time. After the UL transmission, the UE only has to wake up to send TAU messages when the PSM timer T3412 expires. It then stays in eDRX mode to receive potential paging from the network for the period defined by the eDRX timer T3324. After the T3324 timer expires, the UE enters PSM sleep mode again.

The simulation results are shown in Tab. 6.5 and illustrated in Fig. 6.5. From the obtained results, it can be seen that the eDRX timer T3324 has significant impact on energy consumption. Although increasing this timer allows the network more opportunities to transmit DL data, it also greatly increases the amount of energy consumed each time the UE wakes up.

The effect of different PSM–eDRX timer combinations on energy consumption is demonstrated in graph 6.5. For the shorter PSM timers, the impact of different eDRX timers is magnified greatly. For instance, for the PSM timer of 1 hour, the UE

Tab. 6.4: Main parameters of simulation set 2

Description	**Value**
Simulation time	86400 s (24 h)
RRC release timer	20 s
eDRX timer T3324	variable
eDRX cycle	25 s
PSM timer T3412	variable
UL data interval	86400 s
Packet size	100 B
Tx power UE	23 dBm

Tab. 6.5: UE energy consumption per day for different PSM timers T3412 and eDRX timers T3324

eDRX timer	**PSM timer T3412 [h]**				
T3324 [min]	**1**	**3**	**6**	**12**	**24**
0.5	3.3758	3.1084	3.0415	3.0081	2.9913
2	3.9487	3.2993	3.1370	3.0558	3.0152
4	4.8593	3.6029	3.2887	3.1317	3.0531
6	5.7700	3.9065	3.4405	3.2076	3.0911
15	9.6476	5.1990	4.0868	3.5307	3.2527
	Energy consumed [J/day]				

consumes 9.6476 J per day with the eDRX timer of 15 minutes, but only consumes 3.3758 J per day with the eDRX timer of 0.5 minutes. This is due to the fact that for shorter PSM timers, the UE has to wake up more frequently to send TAU messages and every time it wakes up, it has to spend time in eDRX mode. Therefore, the energy consumption for larger eDRX timers is greatly increased in this case.

On the other hand, the impact of different eDRX timers T3324 on energy consumption is not very significant for larger PSM timers T3412. This is because in this case, the UE wakes up less frequently, and therefore, the difference between energy consumption for longer and shorter eDRX timers is reduced. However, we should also take into consideration that the maximum possible value of eDRX timer T3324 can be up to 186 minutes. For this T3324 timer, energy consumption would be high, even if the UE doesn't wake up frequently.

The obtained results from Tab. 6.5 is converted to battery lifetime expectancy in Fig. 6.6. For the most relaxed use case, where the T3324 timer is 0.5 minutes

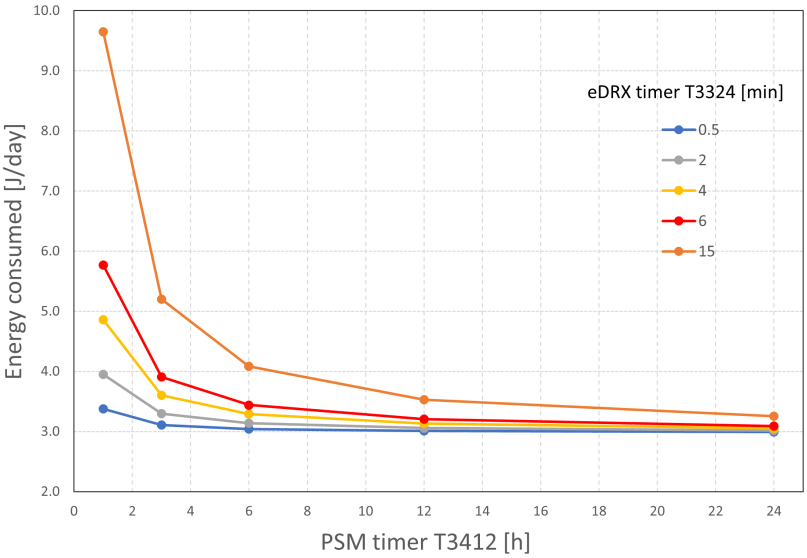

Fig. 6.5: Energy consumption per day for different T3412 timers and T3324 timers

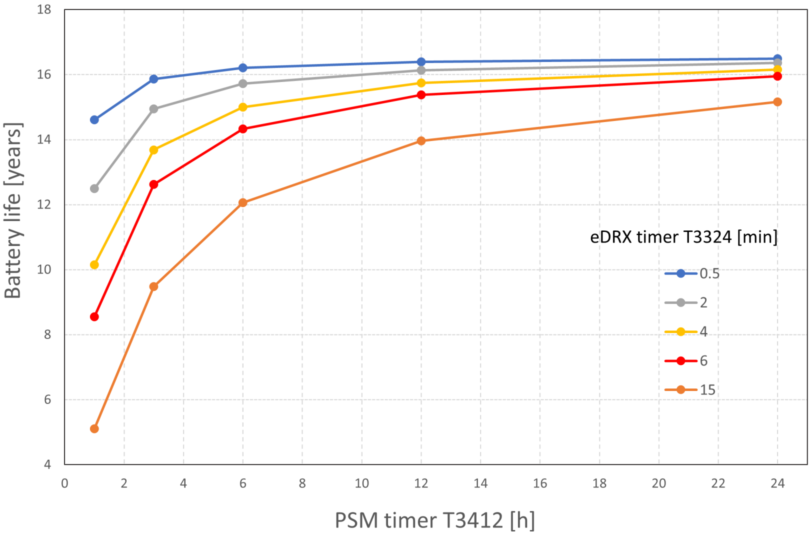

Fig. 6.6: Battery lifetime expectancy for different T3412 timers and T3324 timers

and T3412 timer is 24 hours, the battery of 18000 J can be expected to last up to 16.48 years. In contrast, for the most demanding use case, where the T3324 timer is 15 minutes and T3412 timer is 1 hour, the battery lifetime expectancy is 5.11 years.

6.4.3 Energy Consumption for Different eDRX Timers and UL Data Intervals

The aim of this simulation set is to further evaluate the impact of eDRX timer T3324 on energy consumption by combining different T3324 timers with UL data intervals. For this purpose, in the simulation set, the RRC release timer, PSM timer T3412 and eDRX cycle remain constant, while the eDRX timer T3324 and the intervals between UL transmission change. The simulation parameters are summarized in Tab 6.6.

Tab. 6.6: Main parameters of simulation set 3

Description	**Value**
Simulation time	86400 s (24 h)
RRC release timer	20 s
eDRX timer T3324	variable
eDRX cycle	25 s
PSM timer T3412	10800 s (3 h)
UL data interval	variable
Packet size	100 B
Tx power UE	23 dBm

The obtained simulation results are shown in Tab. 6.7 and illustrated in Fig. 6.7. The battery lifetime expectancy derived from the results is shown in Fig. 6.8. From the results, we can see that the frequency of UL data transmission and the eDRX timer T3324 have immense effect on UE energy consumption. Frequent data transmission, in combination with long eDRX period can drain the UE's battery very quickly. For instance, for the UL data interval of 1 hour and the eDRX timer of 15 minutes, the UE consumes up to 26.3316 J per day, leading to a battery life of only 1.87 years. Furthermore, it can be seen that data transmission frequency is the deciding factor when it comes to UE energy consumption. To be more precise, graph 6.8 shows that with the UL data interval of 1 hour, the battery can only last approximately 2 years for all eDRX timers, even for the shortest eDRX timer of 0.5 minutes. However, with UL data interval of 24 hours, the battery lifetime is expected to be more than 12 years for all eDRX timers, except for the longest eDRX timer of 15 minutes, where the battery lifetime closely approaches 10 years.

Tab. 6.7: UE energy consumption per day for different eDRX timers T3324 and UL data intervals

eDRX timer	**UL data interval [h]**				
T3324 [min]	**1**	**2**	**6**	**12**	**24**
0.5	20.0598	11.1545	5.2846	3.8338	3.1084
2	20.6326	11.4410	5.4755	4.0247	3.2993
4	21.5433	11.8963	5.7791	4.3283	3.6029
6	22.4539	12.3516	6.0826	4.6318	3.9065
15	26.3316	14.2904	7.3752	5.9244	5.1990
	Energy consumed [J/day]				

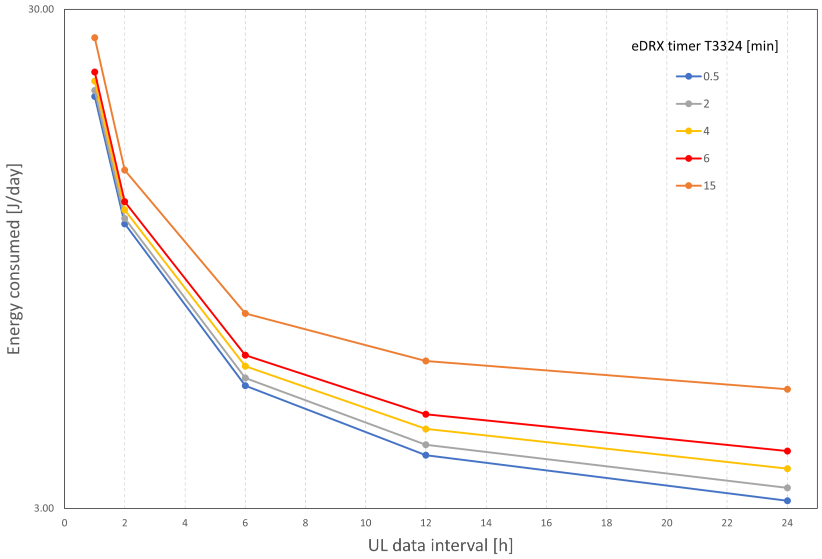

Fig. 6.7: Energy consumption per day for different T3324 timers and different UL data intervals

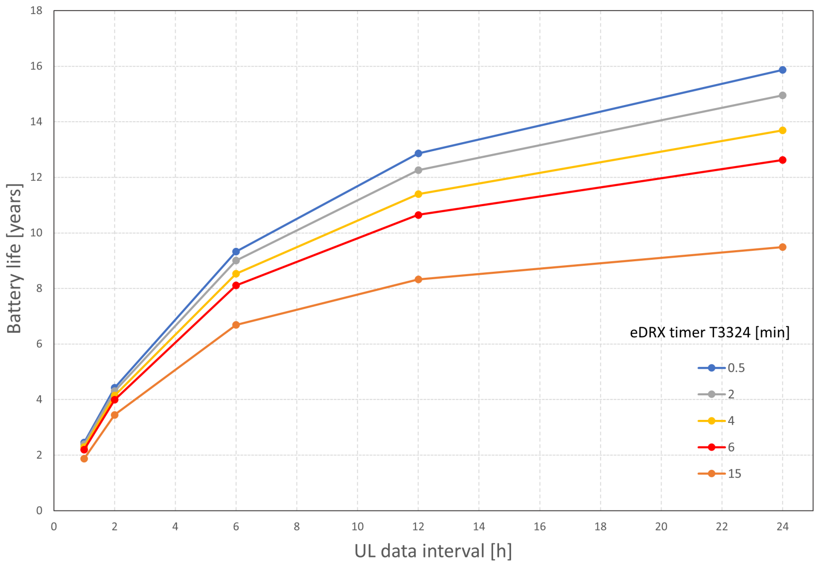

Fig. 6.8: Battery lifetime expectancy for different T3324 timers and different UL data intervals

Conclusion

The rapid growth of the Internet of Things (IoT) market in recent years has led to the evolution of wireless technologies in order to meet the new communication requirements that it has introduced. The 5G standardization specified two requirement categories, namely massive Machine-Type Communication (mMTC) and critical Machine-Type Communication (cMTC), for different IoT use cases and purposes. While cMTC focuses on enabling fast and reliable connection to a small number of sophisticated IoT devices, mMTC focuses on providing connection to a massive number of simple, battery-powered devices. With their distinctive characteristics, i.e. wide coverage, low energy consumption and the ability to support a large number of devices, the Low-Power Wide-Area (LPWA) technology group has emerged to be one of the most prominent enablers for mMTC in both the licensed and license-free frequency bands. The master's thesis focuses on the Long Term Evolution Machine Type Communication (LTE-M) technology, which is a member of the LPWA group, operating in the licensed frequency bands.

The first chapter of the thesis clarified the concept of IoT and Machine-to-Machine (M2M) communication, highlighting the differences between traditional Human-to-Human (H2H) communication and M2M. In addition, the characteristics of LPWA technologies were discussed and compared to those of other wireless technologies used in IoT. At the end of the chapter, the technical parameters and use cases of the technologies were summarized in Tab. 1.2.

The second chapter briefly described the evolution of cellular networks towards the emergence of MTC. With the keys characteristics of legacy systems and the important milestones in their development towards MTC summarized in the first half, the second half of the chapter introduced the four LPWA technologies, namely LTE-M, Narrowband IoT (NB-IoT), Sigfox and Long Range Wide Area Network (LoRaWAN), as mMTC enablers in the 5G era. In addition, a detailed comparison of the LPWA technologies was given at the end of the chapter in Tab. 2.1.

The characteristics of the LTE-M technology was analyzed in detail in the third chapter. First, the designing objectives, architecture and standardization of the technology were summarized. Then, the mechanisms used by LTE-M in order to achieves its objectives such as coverage enhancement, power saving, reduction of operation complexity and device's cost were discussed in depth. The sections 3.3, 3.4, 3.5 were dedicated to describing the physical layer of LTE-M. In these sections, the resource grid, duplex mode, device categories, physical channels and signals used in LTE-M were analyzed. Furthermore, the security features of LTE-M was shortly described in section 3.6.

Chapter four gave a brief introduction of the Network Simulator 3 (NS-3), the LENA module and its extensions, namely LENA-NB and 5G-LENA. The characteristics of the different LENA-based modules and their usability for the implementation of the LTE-M technology in NS-3 were discussed in this chapter and in the end, the LENA module was chosen to be the platform for the implementation of LTE-M features.

Chapter five and six represent the practical part of the thesis. In chapter five, simulation scenarios with growing number of UEs were run in order to identify the limit of the network when it comes to the number of connected devices. The achieved number was 250 devices communicating simultaneously. Chapter sixth was dedicated to the implementation of LTE-M power saving features, namely Power Saving Mode (PSM) and extended Discontinuous Reception (eDRX) into the LENA module. Using the LENA module enhanced with PSM and eDRX, three simulation sets with different configurations of PSM timer, eDRX timer and communication pattern were defined to evaluate the impact these features have on energy saving and battery life of the UE. From the simulation results in Tab. 6.3, 6.5 and 6.7, it can be seen that PSM and eDRX are the most effective in use cases where data transmission is infrequent. In cases with more frequent data transmission, they have little impact on energy saving. Furthermore, it can be concluded from the obtained results that with the combination of PSM, eDRX and a relaxed communication pattern, the battery lifetime of more than 10 years can be achieved for an LTE-M device with a battery capacity of 5 Wh.

Bibliography

[1] O. Liberg, M. Sundberg, E. Wang, J. Bergman, J. Sachs, and G. Wikström, *Cellular Internet of Things: From Massive Deployments To Critical 5G Applications.* Academic Press, 2019.

[2] Ericsson, "Ericsson Mobility Report", Tech. Rep., Nov. 2021. [Online]. Available: `https://www.ericsson.com/4ad7e9/assets/local/reports-papers/mobility-report/documents/2021/ericsson-mobility-report-november-2021.pdf`.

[3] Cisco, "Cisco Annual Internet Report (2018–2023) White Paper", *Cisco: San Jose, CA, USA*, 2020.

[4] Q. Song, L. Nuaymi, and X. Lagrange, "Survey of Radio Resource Management Issues and Proposals for Energy-efficient Cellular Networks That Will Cover Billions of Machines", *EURASIP journal on wireless communications and networking*, vol. 2016, no. 1, pp. 1–20, 2016.

[5] M. Stůsek, "Research on Reliable Low-Power Wide-Area Communications Utilizing Multi-RAT LPWAN Technologies for IoT Applications", Ph.D. dissertation, Brno University of Technology. Faculty of Electrical Engineering and Communication, 2021.

[6] B. S. Chaudhari and M. Zennaro, *LPWAN Technologies for IoT and M2M Applications.* Academic Press, 2020.

[7] R. Drápela, "Implementace a Vyhodnocení Komunikační Technologie LTE Cat-M1 v Simulačním Prostředí Network Simulator 3", M.S. thesis, Brno University of Technology. Faculty of Electrical Engineering and Communication, 2019.

[8] M. Afaneh, "Wireless Connectivity Options for IoT Applications–Technology Comparison", Apr. 2020. [Online]. Available: `https://www.bluetooth.com/blog/wireless-connectivity-options-for-iot-applications-technology-comparison/`.

[9] S. J. Danbatta and A. Varol, "Comparison of Zigbee, Z-Wave, Wi-Fi, and Bluetooth Wireless Technologies Used in Home Automation", in *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, 2019, pp. 1–5. DOI: `10.1109/ISDFS.2019.8757472`.

[10] R. Sandre, "Thread and Zigbee for Home and Building Automation", *Texas Instrum., Dallas, TX, USA*, 2018.

[11] A. Kunz, L. Kim, H. Kim, and S. Husain, "Machine Type Communications in 3GPP: From Release 10 to Release 12", *2012 IEEE Globecom Workshops (GC Wkshps)*, pp. 1747–1752, Dec. 2012. DOI: 10.1109/GLOCOMW.2012.6477852.

[12] M. Sauter, *From GSM to LTE-advanced: An Introduction to Mobile Networks and Mobile Broadband.* John Wiley & Sons, 2014.

[13] A. Kukushkin, *Introduction to Mobile Network Engineering: GSM, 3G-WCDMA, LTE and The Road to 5G.* John Wiley & Sons, 2018.

[14] ITU-R working group, "Spectrum Requirements for International Mobile Telecommunications-2000 (IMT-2000)", *Report ITU*,

[15] M. Condoluci and T. Mahmoodi, "Softwarization and Virtualization in 5G Mobile Networks: Benefits, Trends and Challenges", *Computer Networks*, vol. 146, pp. 65–84, 2018.

[16] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT System for M2M Communication", pp. 1–5, 2016. DOI: 10.1109/WCNC.2016.7564708.

[17] Sigfox, "Sigfox Connected Objects: Radio Specifications v1.6", Tech. Rep., Mar. 2022.

[18] E. Li, "An Introduction of Long Range and LoRaWAN Technology", 2020. [Online]. Available: https://www.seeedstudio.com/blog/2020/08/03/lorapedia-an-introduction-of-lora-and-lorawan-technology/.

[19] R. Belyaev, "SCEF for IoT", Aug. 2019. [Online]. Available: https://www.linkedin.com/pulse/scef-iot-ruslan-belyaev.

[20] GSMA, "LTE-M Deployment Guide to Basic Feature Set Requirements", Tech. Rep., Jun. 2019.

[21] R. Ratasuk, N. Mangalvedhe, D. Bhatoolaul, and A. Ghosh, "LTE-M Evolution Towards 5G Massive MTC", in *2017 IEEE Globecom Workshops (GC Wkshps)*, IEEE, 2017, pp. 1–6.

[22] M. Elsaadany, A. Ali, and W. Hamouda, "Cellular LTE-A Technologies for The Future Internet-of-Things: Physical Layer Features and Challenges", *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2544–2572, 2017.

[23] GSMA, *Security Features of LTE-M and NB-IoT Networks*, 2019.

[24] Network Simulator 3, "NS-3 Tutorial", [Online]. Available: https://www.nsnam.org/docs/tutorial/html/index.html#ns-3-tutorial.

[25] CTTC, "The LENA NS-3 LTE Module Documentation Release v8", Jan. 2014. [Online]. Available: https://dokumen.tips/documents/lena-lte-module-doc.html.

[26] P. Jörke, T. Gebauer, and C. Wietfeld, "From LENA to LENA-NB: Implementation and Performance Evaluation of NB-IoT and Early Data Transmission in NS-3", in *Proceedings of the 2022 Workshop on ns-3*, 2022, pp. 73–80.

[27] P. Jörke, T. Gebauer, S. Böcker, and C. Wietfeld, "Scaling Dense NB-IoT Networks to the Max: Performance Benefits of Early Data Transmission", in *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, 2022, pp. 1–7. DOI: `10.1109/VTC2022-Spring54318.2022.9860611`.

[28] N. Patriciello, S. Lagen, B. Bojovic, and L. Giupponi, "An E2E Simulator for 5G NR Networks", *Simulation Modelling Practice and Theory*, vol. 96, p. 101 933, 2019.

[29] K. Koutlia, B. Bojovic, Z. Ali, and S. Lagén, "Calibration of The 5G-LENA System Level Simulator in 3GPP Reference Scenarios", *Simulation Modelling Practice and Theory*, p. 102 580, 2022.

[30] Velos, "What are PSM & eDRX features in LTE-M and NB-IoT?", 2022. [Online]. Available: `https://blog.velosiot.com/what-are-psm-edrx-features-in-lte-m-and-nb-iot`.

[31] A. K. Sultania, C. Delgado, and J. Famaey, "Implementation of NB-IoT power saving schemes in NS-3", in *Proceedings of the 2019 Workshop on Next-Generation Wireless with ns-3*, 2019, pp. 5–8.

Symbols and abbreviations

3GPP	Third Generation Partnership Project
8PSK	Eight-State Phase Shift Keying
AKA	Authentication and Key Agreement
ALOHA	Abramson’s Logic of Hiring Access
BTS	Base Transceiver Station
BWP	Bandwidth Parts
CDMA	Code Division Multiple Access
CE	Coverage Enhancement
C-IoT	Cellular Internet of Things Optimization
cMTC	Critical Machine-Type Communication
CP	Cyclic Prefix
C-Plane	Control Plane
CRS	Cell-specific Reference Signal
CSI	Channel State Information
CSS	Chirp Spread Spectrum
DBPSK	Differential Binary Phase-Shift Keying
DCI	Downlink Control Information
DMRS	Demodulation Reference Signal
ED	End Device
EDGE	Enhanced Data rates for GSM Evolution
eDRX	Extended Discontinuous Reception
EDT	Early Data Transmission
EIRP	Equivalent Isotropic Radiated Power
eNodeB	Evolved Node B

EPC	Evolved Packet Core
EPS	Evolved Packet System
EU	European Union
eUTRAN	Evolved UMTS Terrestrial Radio Access Network
FDD	Frequency Division Duplex
GMSK	Gaussian Minimum-Shift Keying
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
H2H	Human-to-Human
HSDPA	High-Speed Downlink Packet Access
HSPA	High-Speed Packet Access
HSS	Home Subscriber Server
HSUPA	High-Speed Uplink Packet Access
HTC	Human-Type Communication
IMSI	International Mobile Subscriber Identity
IoT	Internet of Thing
IP	Internet Protocol
ISI	Intersymbol Interference
ITU	International Telecommunication Union
KSI	Key Set Identifier
LENA	LTE/EPC Network SimulAtor
LENA-NB	LTE/EPC Network SimulAtor NarrowBand
LoRaWAN	Long Range Wide Area Network
LPWA	Low-Power Wide-Area
LR-WPAN	Low-Rate Wireless Personal Area Networks

LTE	Long-Term Evolution
LTE-M	Long Term Evolution Machine Type Communication
M2M	Machine-to-Machine
MAC	Media Access Control
MCL	Maximum Coupling Loss
MIB	Master Information Block
MIB-NB	Master Information Block Narrowband
MIMO	Multiple-Input Multiple-Output
MME	Mobility Management Entity
mMTC	Massive Machine-Type Communication
mmWave	Millimeter-Wave
MPDCCH	MTC Physical Downlink Control Channel
MTC	Machine-Type Communication
NB-IoT	NarrowBand IoT
NPRACH	Narrowband Physical Random Access Channel
NR	New Radio
OFDMA	Orthogonal Frequency-Division Multiple Access
PBCH	Physical Broadcast Channel
PCID	Physical Cell Identity
PDCCH	Physical Downlink Control Channel
PDR	Packet Delivery Rate
P-GW	Packet Data Network Gatewa
PLMN	Public Land Mobile Network
PRACH	Physical Random Access Channel
PRB	Physical Resource Block

PRS	Positioning Reference Signal
PSM	Power Saving Mode
PSS	Primary Synchronization Signal
PUCCH	Physical Uplink Shared Channe
PUSCH	Physical Uplink Shared Channel
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase-Shift Keying
RAU	Routing Area Update
RE	Resource Element
RNC	Radio Network Controller
RS	Reference Signal
SC-FDMA	Single-Carrier Frequency-Division Multiple Access
SI	System Information
SIB	System Information Block
SIB-NB	System Information Block Narrowband
SSS	Secondary Synchronization Signal
TAU	Tracking Area Update
TBS	Transport Block Size
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
TMSI	Temporary Mobile Subscriber Identity
UCI	Uplink Control Information
UE	User Equipment
UMTS	Universal Mobile Telecommunications System

UNB	Ultra-Narrow Band
U-Plane	User Plane
URLLC	Ultra-Reliable and Low Latency Communication
USIM	Universal Subscriber Identity Module
VoLTE	Voice over LTE
W-CDMA	Wideband Code Division Multiple Access
WLAN	Wireless Local Area Network

A Content of Electronic Appendix

The content of the electronic appendix is summarized in the structure below. The electronic appendix contains the used simulation scenarios, the simulation outputs and the derived graphs from the outputs. The directory */Energy_consumption_evaluation/ns-3.32_psm_edrx* is the NS-3 project containing the implementation of the LENA module with PSM and eDRX features. Inside the project, the simulation scripts and simulation outputs can also be found.

```
/ ........................................ root directory of electronic appendix
├── Performance_evaluation Data and code from performance evaluation of mMTC
│   ├── Simulation_Bulk ................................. Using Bulk application
│   │   ├── Data_Bulk.xlsx
│   │   ├── Graph_Bulk.pdf
│   │   └── Scenario_Bulk.cc
│   └── Simulation_Onoff ..............................Using On-off application
│       ├── Data_Onoff.xlsx
│       ├── Graph_Onoff.pdf
│       └── Scenario_Onoff.cc
└── Energy_consumption_evaluation......Data and code from energy consumption
    evaluation
    ├── ns-3.32_psm_edrx.......NS-3 project for implementation of PSM and eDRX
    │   ├── scratch.................Directory containing simulation scenario scripts
    │   ├── output ........................ Directory containing simulation outputs
    │   ├── change_summary.txt .......................... Modified files summary
    │   └── src
    │       └── lte ........... Modified LENA module with PSM and eDRX features
    ├── Set1_T3412_ULInterval
    │   ├── Data_set1.xlsx
    │   ├── Set1_EnergyConsumption.pdf
    │   └── Set1_BatteryLife.pdf
    ├── Set2_T3412_T3324
    │   ├── Data_set2.xlsx
    │   ├── Set2_EnergyConsumption.pdf
    │   └── Set2_BatteryLife.pdf
    └── Set3_T3324_ULInterval
        ├── Data_set3.xlsx
        ├── Set3_EnergyConsumption.pdf
        └── Set3_BatteryLife.pdf
```