

Secure and Bandwidth Efficient Industrial IoT Networks

Stephen Okwudili Ugwuanyi

A thesis submitted in fulfilment of the requirements for the degree of **Doctor of Philosophy**

Centre for Intelligent Dynamic Communications

Electrical and Electronic Engineering

University of Strathclyde, Glasgow

May 1, 2023

Copyright © 2023 by Stephen Ugwuanyi.

The copyright of this thesis belongs to the author under the terms of the United Kingdom Copyright Acts as qualified by University of Strathclyde Regulation 3.51.

Due acknowledgement must always be made of the use of any material contained in, or derived from, this thesis.

Declaration

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree. The copyright of this thesis belongs to the author under the terms of the United Kingdom Copyright Acts as qualified by University of Strathclyde Regulation 3.50. Due acknowledgement must always be made of the use of any material contained in, or derived from, this thesis.

The research is conducted using funds awarded by the Petroleum Technology Development Fund (PTDF), Abuja, Nigeria under the award number **PTDF/ED/PHD/USO/1092/17**.



Signed: Stephen Ugwuanyi

Date: 02/05/2023

Abstract

The Internet of Things (IoT) and industrial integration have recently become increasingly popular and investigated among researchers for industrial and consumer-based applications. Industrial Internet of Things (IIoT) presents an opportunity for industrial applications especially those in challenging environments to be provisioned remotely and more efficiently at a cheaper cost within the shortest time interval. As the journey to industrial digital transformation continues to increase, many wireless technologies have been used to deploy IoT solutions that have shown evidence of security, interoperability, latency, throughput, and bandwidth challenges. Based on recent events, these challenges are increasing when implementing IoT, especially in an industrial context with legacy communication and control infrastructure and result in data loss, overwhelming network resources, loss of access control, and total disruption of network performance. IoT-based cellular networks are more widely used as they have overcome some of these challenges through technology evolution from GSM to 5G. Most cellular network versions are not designed for constrained IoT devices and are very expensive for large-scale deployment.

In this thesis, the areas of contribution focus on security, protocols, bandwidth, and cost based on different test network scenarios. The performance of different licensed and unlicensed Low Power Wide Area Networks (LPWAN) test network scenarios is investigated. Focusing on Low Range Wide Area Networks (LoRaWAN) and Narrowband Internet of Things (NB-IoT) designed for massive machine-type constrained IoT applications, testbeds of LoRaWAN and NB-IoT were designed, implemented and their performances compared based on sensor networks QoS parameters such as power

utilisation, throughput, latency, and security. On average, NB-IoT outperformed LoRaWAN on data throughput, latency and security. NB-IoT consumed an excess of 2 mAh of power for joining the network and 1.7 mAh more for a 44 byte uplink message compared to LoRaWAN. With the maximum throughput of 264 bps at 837 ms measured latency, NB-IoT outperformed LoRaWAN and proved robust for machine-type communications. When sending between 29 - 48 bytes, the average throughput varied between 115 bps to 264 bps between the UE and the server. At 50 bytes retransmission of data payload, the successful transmission rate decreased and, in most cases, resulted in unsuccessful transmission.

The concept of Transport Layer Security (TLS) and Internet Protocol Security (IPSec) for securing IIoT infrastructure is presented based on the testbed at Strathclyde Power Network Demonstration Centre (PNDC), where novel bandwidth-efficient authentication and encryption mechanisms for utility network are contributed. In the case of IPSec test network scenario, the tests delivered an overhead of 25%. An increase of 15% against the 10% suggested in the literature. TLS with AES of 128-bit contributed 25% of additional overhead compared to IPsec for each analogue or digital command. From these findings, an analysis of the cost implications of introducing extra security layers is presented to guide the efficient use of scarce network resources like bandwidth. The cost of using IPSec to secure the industrial protocol connection between RTU and the router is higher than that of OpenVPN and is estimated at 45% with respect to bandwidth overhead. For each of the OpenVPN-based transmitted packets, 40 - 44 bytes of overhead were added via User Datagram Protocol (UDP), whereas IPSec added 60 - 68 bytes. The overhead of TLS keep-alive messages, IPsec, TCP connections, and IEC 104 consume more than 50% of the bandwidth (based on configuration and application). The security features evaluated added overhead of roughly 2-3 folds of the current data rate by the Distributed Network Operators (DNOs), for both levels of security (i.e. TLS and IPsec).

List of Publications

Publications included in the thesis:

1. Journal Papers

- **[JP1]** Stephen Ugwuanyi, Greig Paul, and James Irvine, “Survey of IoT for Developing Countries: Performance Analysis of LoRaWAN and Cellular NB-IoT Networks,” *Electronics* 2021, 10, 2224. <https://www.mdpi.com/2079-9292/10/18/2224>
- **[JP2]** Stephen Ugwuanyi and James Irvine, “Intelligent Internet of Things (IoT) Node Demonstrator for Device Monitoring and Control in the Oil and Gas Sector,” *Nigerian Journal of Oil and Gas Technology*, vol. 3 No. 2, pp. 222—222, March 2018. <https://rsustnjogat.org/admin/img/paper/VOL3%20N02-compressed-291-301.pdf>

2. Conference Papers

- **[CP1]** Stephen Ugwuanyi and James Irvine, ”Industrial and Consumer Internet of Things: Cyber Security Considerations, Threa Landscape, and Countermeasure Opportunities” *IEEE International Conference on Smart Applications, Communications and Networking (SmartNets)* - Glasgow, United Kingdom, 22 September → 24 September, 2021.
- **[CP2]** Stephen Ugwuanyi, Jidapa Hansawangkit, and James Irvine, ”NB-IoT Testbed for Industrial Internet of Things” *IEEE International Sympo-*

Chapter 0. List of Publications

sium on Networks, Computers and Communications (ISNCC), College de Maisonneuve, Montreal, Canada, 20 → 22 October, 2020.

- **[CP3]** Stephen Ugwuanyi and James Irvine, "Security Analysis of IoT Networks and Platforms" IEEE International Symposium on Networks, Computers and Communications (ISNCC), College de Maisonneuve, Montreal, Canada, 20 → 22 October, 2020.
- **[CP4]** Stephen Ugwuanyi and James Irvine, "Narrowband Internet of Things (NB-IoT) – Current Security Issues in an Emerging Industrial Sensor Networks." University of Strathclyde Doctoral School Multidisciplinary Symposium, 19 June, 2019.
- **[CP5]** Stephen Ugwuanyi, Agbo Okechukwu, Ohia Prince, Ndukwe Ogechukwu, and James Irvine, "Cybercrimes in Southern Nigeria and Survey of IoT Implications." 1st IEEE Multi-Conference Technical Series, 25 August, 2020.

Lists of Co-Authored Publications

In addition, related contributions to the following publications are also included:

1. Conference Papers

- **[C7]** Kinan Ghanem, Stephen Ugwuanyi, Rameez Asif, and James Irvine, "Challenges and Promises of 5G for Smart Grid Teleprotection Applications" IEEE International Symposium on Networks, Computers and Communications (ISNCC'21), Dubai-UAE, October 31 → November 2, 2021.
- **[C8]** Kinan Ghanem, Stephen Ugwuanyi, Jidapa Hansawangkit, Ross McPherson, Rameez Asif, and James Irvine, "Bandwidth Efficient Secure Authentication and Encryption Techniques on IEC-60870-5-104 for Remote Outstations" IEEE International Conference on Smart Applications, Communications and Networking (SmartNets) - Glasgow, United Kingdom, 22 September → 24 September, 2021.

Chapter 0. List of Publications

- **[C9]** Kinan Ghanem, Stephen Ugwuanyi, Rameez Asif, and James Irvine, "Bandwidth and Security Requirements for Smart Grid" IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe) - The Hague, Netherlands, 26 → 28 October, 2020.
- **[C10]** Kinan Ghanem, Stephen Ugwuanyi, idapa Hansawangkit, Ross McPherson, Rabia Khan and James Irvine, "Security vs Bandwidth: Performance Analysis Between IPsec and OpenVPN in Smart Grid" IEEE International Symposium on Networks, Computers and Communications (ISNCC'22), July 19 - 22, 2022, Shenzhen, CHINA.

Acknowledgements

I would like to acknowledge the contributions of many people without whom I would not have been able to complete this work. Firstly, my supervisor Dr James Irvine for his excellent guidance, mentorship, and provision of industrial engagement and collaboration opportunities at the critical stages of this research. These activities and his scholarly guidance, comments, and corrections undoubtedly contributed significantly to this innovative research on the security and bandwidth of emerging wireless networks for Industrial Internet of Things (IIoT). His supervision style gave me full control of the research and helped develop relevant research and problem-solving skills throughout the PhD journey.

To the mobile and cyber security research colleagues, particularly Dr Greig Paul and Dr Ross McPherson, for their technical support, comments and friendships, which made the research motivation very high, especially during the lockdown period due to COVID-19. My special gratitude is extended to Dr Kinan Ghanem and Dr Rameez Asif of Communication and Systems Integration research team at the University of Strathclyde Power Networks Demonstration Centre (PNDC) for their support, guidance and motivation.

My engagement as a Research and Development Engineer on several industrial IoT and security-based projects was instrumental to some of the technical chapters of this thesis. This allowed for real-world testing and industrial evaluations of the research objectives.

I would like to recognise my funder (PTDF) for the opportunity to undertake this PhD. My warm and sincere thanks go to my family and friends, whose constant contact

Chapter 0. Acknowledgements

and support kept me focused and resilient. Finally, I appreciate almighty God for the gift of life and good health, without which this research would not have been possible.

Dedication

This thesis is dedicated to my family and my late son and father. Late Master Mitchell Ugwuanyi and Chief Leonard Ugwuanyi passed onto greater glory during the second year of my PhD.

Contents

Declaration	ii
Abstract	iii
List of Publications	v
Acknowledgements	viii
Dedication	x
List of Figures	xvi
List of Tables	xx
Acronyms	xxiii
1 Introduction	1
1.1 Issues Industrial IoT Faces	4
1.2 Research Motivation	7
1.3 Research Questions	9
1.4 Methodology	10
1.5 Novelty and Contributions of the Research	12
1.6 Thesis Outline	14
2 Literature Review	16
2.1 IoT Historical Perspective	18

Contents

2.1.1	IoT Devices	21
2.2	Applications of IoT Technologies	25
2.2.1	Smart Grid	26
2.3	Industrial Internet of Things	27
2.3.1	Related Work	28
2.4	Industrial IoT Communication Protocols	31
2.4.1	Message Queue Telemetry Transport	31
2.4.2	Hypertext Transport Protocol	32
2.4.3	WebSocket Protocol	33
2.5	Architecture	34
2.6	Industrial IoT Security	35
2.6.1	Security Requirements of Industrial IoT	37
2.7	Security Layers in IoT Networks	41
2.7.1	Physical Layer	42
2.7.2	Perception Layer	43
2.7.3	Network Layer	44
2.7.4	Application Layer	46
2.8	Countermeasure Opportunities	47
2.8.1	Next-Generation Firewall and Gateway	48
2.8.2	Next-Generation Virtual Private Network	49
2.8.3	Defense-in-Depth Security Architecture	49
2.8.4	Encryption Techniques	49
2.8.5	Key Management	50
2.9	Cyber Security Considerations	52
2.10	Internet of Smart Grid (IoSG)	52
2.11	Introduction	52
2.12	A Review of Smart Grid Telecommunication Technologies	54
2.13	Wireless Technology in Smart Grid	55
2.13.1	Requirements of Wireless Technology in Smart Grid	58
2.14	Smart Grid Communication Protocols	60

Contents

2.14.1	Modbus	61
2.14.2	Distributed Network Protocol Version 3	62
2.14.3	IEC Standards Protocols	63
2.15	Bandwidth Consideration in Security	67
3	Methodology and Implementations	70
3.1	LoRaWAN	70
3.1.1	LoRaWAN Network Architecture	71
3.1.2	LoRAWAN Layers	72
3.1.3	LoRaWAN Physical Characteristics	73
3.1.4	Network Join Procedure	77
3.1.5	LoRaWAN Security	78
3.1.6	Network Performance	79
3.2	Cellular Internet of Things Technology	79
3.2.1	Long Term Evolution (LTE)	80
3.2.2	Key Characteristics of LTE Technologies	81
3.3	Narrowband Internet of Things (NB-IoT)	85
3.4	Fundamentals of NB-IoT	86
3.4.1	History and Standardisation	86
3.4.2	NB-IoT Architecture	87
3.4.3	Air Interface	88
3.4.4	Physical Layer Resources	90
3.4.5	Uplink and Downlink Operation	91
3.4.6	Downlink NB-IoT Channels	93
3.4.7	NB-IoT Uplink Transmission Channel	95
3.5	NB-IoT Operation	99
3.6	Security in Narrowband IoT	99
3.6.1	Benefits of NB-IoT Technology	101
3.7	NB-IoT Test Setup	103
3.7.1	Mobility Management Entity (MME)	103

Contents

3.7.2	Long Term Evolution Evolved Node B (LTEeNB)	104
3.7.3	NB-IoT Web Interface	105
3.8	Narrowband IoT 3GPP Standardisation	105
3.8.1	3GPP Standardisation Release 13	105
3.8.2	3GPP Standardisation Release 14	106
3.8.3	3GPP Release 15	111
3.8.4	3GPP Release 16	111
3.8.5	3GPP Release 17	112
3.9	Narrowband Fidelity (NB-Fi)	112
4	Narrowband IoT Testbed for Industrial Internet of Things	114
4.1	Introduction	114
4.2	NB-IoT Landscape	115
4.3	Technology for NB-IoT Testbed	116
4.3.1	NB-IoT Deployment Modes	118
4.4	Related Work	119
4.5	methodology	120
4.5.1	Industrial NB-IoT Devices	122
4.6	Results and Discussions for a Single IoT Module	124
4.6.1	Mobility Management Entity (MME)	125
4.6.2	Long Term Evolution Evolved Node B (LTEENB)	125
4.6.3	Latency	126
4.6.4	Power Consumption	127
4.6.5	NB-IoT Security	128
4.6.6	Conclusion	130
5	Performance Analysis of LoRaWAN and Cellular NB-IoT Networks	131
5.1	Introduction	132
5.2	Related Literature and Contribution	135
5.3	IoT Deployment Opportunities in Developing Countries	138
5.3.1	Leveraging Cellular Networks for IoT Deployments in Nigeria	140

Contents

5.3.2	Leveraging Unlicensed LPWANs for IoT Deployments	145
5.4	Low Power Cellular Technologies for IoT	147
5.4.1	EC-GSM-IoT	148
5.4.2	NB-IoT	149
5.4.3	5G and LPWAN Integration	155
5.4.4	5G and IoT Technology	156
5.5	LoRaWAN and NB-IoT Implementations	158
5.5.1	Design of LoRaWAN Testbed	158
5.5.2	Design of NB-IoT Network	159
5.6	Network Performance Analysis: NB-IoT vs LoRaWAN	161
5.6.1	Latency	162
5.6.2	Throughput	164
5.7	Conclusions	170
5.7.1	Potential Benefits and Drawbacks of Integrated LPWANs	171
6	Bandwidth and Security Analysis of TLS and IPSec-Based Internet of Smart Grid	173
6.1	Introduction	173
6.2	Security Requirements for Smart Grid	175
6.3	Communication Challenges in Power Utilities	177
6.3.1	Security Requirements for Secondary Substation	178
6.3.2	Availability of Radio Spectrum	180
6.4	The Bandwidth and Security Testing Setup	182
6.4.1	Cybersecurity Considerations for Secondary Substation	184
6.5	Bandwidth Analysis of TLS and IPSec Overhead in Secondary Substation	185
6.5.1	Internet Protocol Security for Secondary Substation Security . . .	185
6.5.2	Transport Layer Security for Secondary Substation Security . . .	187
6.5.3	Estimated Bandwidth for Secondary Substation	190
6.6	Summary	191

7	Bandwidth Efficient Security for Smart Grid	193
7.1	Introduction	194
7.2	Wireless Communication Technology for Smart Grid	196
7.3	Private vs Public LTE Networks for Power Utilities	198
7.4	Methodology	200
7.5	Security Techniques for Smart Grid	206
7.5.1	TLS Encryption	207
7.5.2	Secure Authentication	207
7.5.3	Virtual Private Network	209
7.6	Results and Analysis	211
7.6.1	Secure Authentication Overhead	212
7.7	OPEN VPN vs IPSec	213
7.7.1	Congestion	213
7.7.2	Connection Loss	214
7.7.3	Network Coverage	214
7.8	Data Rates	214
7.9	Spectral Efficiency	215
7.10	Encryption Scheme Challenges for Smart Grid	218
7.11	Emerging Security Strategies for OT Networks	220
7.12	Summary and Conclusion	221
8	Conclusions and Future Work	223
8.1	Conclusion	223
8.2	Summary of Contributions	226
8.3	Future Work	230
	Bibliography	233

List of Figures

1.1	An IoT Device by Pycom that supports many IoT protocols and ports for sensor network integration	11
1.2	University of Strathclyde, PNDC	11
1.3	Research Methodology	12
1.4	Thesis Outline	15
2.1	IoT Technology Enabler [1]	19
2.2	IoT Wireless Connectivity Landscape and Historical Development [2] . .	20
2.3	Internet of growth Forecast to 2020 [3]	21
2.4	IoT Applications	26
2.5	Key Technologies Driving Industrial IoT	29
2.6	MQTT Publish-Subscribe Architecture	32
2.7	IoT Protocols	33
2.8	Comparison of OSI Model, Generic and Industrial IoT Architectures . .	35
2.9	Certificate Authority Based Key Management System	51
2.10	Smart Grid Architecture [4]	57
2.11	DNP3 and IEC6180 with IEC2352 [5]	63
2.12	IEC 62351 Standard in RTU500 Series	65
2.13	ABB RTU 500 Series	67
3.1	LoRaWAN Architecture [6]	72
3.2	LoRaWAN Layers [7]	73
3.3	NB-IoT Architecture	89

List of Figures

3.4	NB-IoT Access Network	89
3.5	UE Features	90
3.6	NB-IoT UE Power Saving Modes [8]	93
3.7	NB-IoT DL Physical Channels/Signals and Time-multiplex over a sub-frame structure	94
3.8	OFDM	95
3.9	SC OFDMA	96
3.10	NB-IoT Constellation Diagram for 64 QAM	97
3.11	Three Formats of NB-IoT NPRACH Symbol Groups and their Respective Configuration Parameters	98
3.12	NB-IoT Deployment Modes	99
3.13	Benefits of NB-IoT	103
3.14	eNB Interface	104
3.15	UL and DL transmissions in Release 13 NB-IoT network	108
4.1	NB-IoT Practical Experimental Setup	121
4.2	NB-IoT Experimental Design	121
4.3	NB-IoT Network Attachment Procedure	122
4.4	NB-IoT Network Attach and Data Transfer Procedure	123
4.5	MME Interface showing UEs attached to the Network	125
4.6	UE Downlink and Uplink Data Rate	126
4.7	UE Data Transmission Modes	127
4.8	UE Data Retransmission	128
5.1	IoT Deployment Opportunities in Developing Countries.	137
5.2	Typical LTE Network Distribution in Urban Area in Nigeria	140
5.3	Secure LoRaWAN Architecture. (a) Typical LoRaWAN Architecture and (b) LoRaWAN Network Implemented on The Things Network. . .	147
5.4	Overview of UEs Duty Cycle and Power Utilisation due to G3PP Standardisation Effort.	151
5.5	NB-IoT Deployment Modes.	153

List of Figures

5.6	Global NB-IoT Deployment. Reproduced with permission from [Collins Burton Mwakwata], [Narrowband Internet of Things (NB-IoT): From Physical (PHY) and Media Access Control (MAC) Layers Perspectives, Sensors]; published by [MDPI], [8 June 2019] [9].	155
5.7	5G and LTE IoT Spectrum	158
5.8	LPWAN Network in Operation.	160
5.9	LPWAN Integrated Architecture.	161
5.10	Round Trip Time between the LTE eNB Server and client.	163
5.11	NB-IoT Throughput, Latency for Data UE-Server Payloads	163
5.12	NB-IoT Downlink and Uplink Bitrates for In-band Modes of Operation	165
5.13	Average Throughput between the LTE eNB server and MME Client	166
5.14	NB-IoT Data Throughput for Successful Interval Transmissions at a maximum of 7 packets/sec	166
5.15	NB-IoT CPU, Receive and Transmission Channels Power Consumption.	168
5.16	UE Security Capabilities.	169
6.1	Quality Illustration of Coverage and Capacity vs Frequency	180
6.2	High-level Bandwidth Requirement Testbed (https://pndc.co.uk)	182
6.3	Test Scenario	184
6.4	ESP Packets Before Entering and After Leaving VPN Tunnel	186
6.5	Protocols Estimated Bandwidth with IPSec	188
6.6	Actual Bandwidth without Security	189
6.7	TCP Retransmission	190
7.1	The Coverage Map of an MNO in Glasgow-Scotland for 2G, 3G, and 4G networks	201
7.2	The Coverage Map of an MNO in Nigeria for 2G, 3G, and 4G networks	202
7.3	IPsec VPN – WAN-Virtual Access RTU	204
7.4	IPsec VPN – WAN-ABB RTU	205
7.5	High Level VPN Test Setup at PNDC	211
7.6	OpenVPN and IPSec Overhead Comparison	213

List of Figures

7.7	LTE Spectral Efficiency in Large Number of Live Nokia Networks	216
-----	--	-----

List of Tables

2.1	General Classification of IoT Communication Protocols into Wide, Local and Home Area Networks	18
2.2	Characteristics Comparison of Licensed and Unlicensed LPWANs [10], [11], [12] [13].	25
3.1	Classification of Wireless Technologies Based on the Transmission Range	71
3.2	LTE TDD vs FDD	85
3.3	Available Resource Blocks in LTE Bandwidth	85
3.4	NB-IoT UE Category	91
3.5	NPUSCH Resource Unit Parameters	98
3.6	NB-IoT Frequency Bands [14]	106
3.7	Multi-carrier Overhead [15]	109
3.8	NB-IoT Release 14 Frequency Bands [16]	110
3.9	NB-IoT Release 15 Frequency Bands [17]	111
4.1	Test Parameters	124
4.2	Table of NB-IoT Devices	124
5.1	Overview of MNOs in Nigeria with NB-IoT and LTE-M bands deployment opportunities.	144
5.2	NB-IoT Features.	150
5.3	Mobile Network Evolution	157

List of Tables

5.4	NB-IoT Network Configurations. The coverage level corresponds to the NPRACH configurations	160
5.5	NB-IoT vs LoRaWAN Average Power Consumption, Latency, and Throughput.	169
6.1	Overview of IPSec Overhead with Message Sizes before Entering and after Leaving IPSec Tunnel	187
6.2	TLS and IPSec Protocol Bandwidth Percentage Estimation	189
6.3	Security and Data Rate Requirements for DNOs	190
6.4	Bandwidth per Protocols with TLS and no Security	191
7.1	Number of RTUs Connected via the Existing UHF Frequency	197
7.2	Public vs Private LTE Network Features	201
7.3	Configuration of IEC 104 Traffic Commands with Polling Frequencies that Created Congestion or Avoided Congestion	203
7.4	LTE FDD System Capacity and Downlink Peak Data Rates	215
7.5	Estimated Number of RTUs in an LTE Cell	217
7.6	RTUs per LTE FDD System Capacity and Throughput Computation	217
7.7	TLS and IPSec Estimated Security Overhead Security in IEC 104	219

Acronyms

ADSL Asymmetric Digital Subscriber Line. [53](#)

AMI Advanced Metering Infrastructure. [176](#)

DNO Distribution Energy Operators. [57](#), [174](#), [176](#), [177](#)

ESP Encapsulating Security Payload. [185](#)

ICT Information and Communication Technology. [175](#), [176](#)

IED Intelligent Electronic Devices. [53](#), [176](#)

IIC Industrial Internet Consortium. [35](#)

IoSG Internet of Smart Grid. [53](#)

IoT Internet of Things. [114](#)

IP Internet Protocol. [174](#)

IPSec Internet Protocol Security. [174](#)

M2M Machine-to-Machine. [34](#)

NB-IoT Narrowband Internet of Things. [114](#)

NIST National Institute of Standard and Technology. [67](#)

OfCom The Office of Communications. [180](#), [181](#)

Acronyms

PHEV Plug-in Hybrid Electric Vehicle. [176](#)

PLC Power Line Communication. [53](#)

PMU Phasor Measurement Unit. [176](#)

PNDC Power Networks Demonstration Centre. [53](#)

PRAT Private Radio Access Technology. [53](#)

PUF Physical Unclonable Function. [30](#)

RA Radio Access. [54](#)

RTU Remote Terminal Unit. [55](#), [174](#), [176](#), [179](#)

SCADA Supervisory Control and Data Acquisition. [60](#)

TLS Transport Layer Protocol. [174](#)

Chapter 1

Introduction

The Internet of Things (IoT) is a network of interconnected devices or things [18] that primarily collect, store, process and distribute information to achieve defined objectives efficiently. Today, IoT is one of the many emerging technology paradigms that play an essential role in advancing the benefits of the Information Technology (IT) and Operational Technology (OT) world. It creates a ubiquitous network that is distributed and composed of complex sub-systems where objects and humans interact [19]. It is a new technology-based research area that aims to provide efficient means of driving the connectivity of ubiquitous devices and networks designed to improve aspects of human life. The devices could be in the form of consumer sensors, industrial actuators, intermediate gateways and the like. One of the main requirements for IoT systems is that all heterogeneous IoT devices must communicate efficiently and securely. This means that IoT devices must have communications and computation capabilities embedded and become able to interconnect and communicate with other devices in networks through standard protocols and architecture, using internet system as their foundation [20], and Internet Protocols (IP)/non-IP [21]/non-internet protocols [22] for deployment. The rapid proliferation of IoT devices, protocols, and applications has sparked close collaborations between many fields to engage in multidisciplinary research efforts to identify potential benefits, prospects, and challenges. Whether consumer or industrial-oriented, IoT

This chapter introduces the reader to the general background of IoT, its historical perspective, the novelty of the research, research motivation, the key objectives for undertaking this study, and the methodology employed.

fundamental objectives encompass the concept of interconnecting various virtual/real-world objects to exchange data seamlessly and securely [23]. The data generated can be further processed to gain business and other application-related insights.

In recent years, the scope of research in IoT has evolved from simply obtaining sensor readings to using intelligence computing algorithms to solve the myriads of connectivity [24], security [25], [26], energy [27], latency [28], bandwidth [29], and data [30] challenges of anything connected to the internet. Examples of how to tackle these new research challenges such as security include the use of strong lightweight authentication, encryption and key distribution system in IoT devices [31], [32]. It will prevent attackers from exploiting the lack of strong security mechanisms when establishing a connected consumer and industrial environment. Others methods include building secure sensor networks as effective data sources and using energy-efficient protocols to optimise power consumption [33], [34] and occupancy compression algorithm to optimise bandwidth utilisation [35], creating interoperable communication protocols for the vast IoT protocols and devices [36], and implementing edge and cloud processing to improve data quality and security [37], [38].

Data security and management is also relevant in IoT data collection, analysis and distribution process since much of them collected by IoT devices can be considered sensitive either by application or ethical context. IoT network is an attractive environment for attackers, and it requires end-to-end security to protect the interfacing data sources as well as secure the execution of IoT applications. It is important to secure stream or stored IoT data by more than one method since it may be challenging to implement robust security in resource-constrained devices. When IoT networks deal with personal private identifiable information that ought to be protected by General Data Protection Regulation (GDPR) [39], privacy and data security become as important as providing a less complex and efficient IoT solutions. When threat actors steal or modify data, it could represent a huge loss to the IoT users. Secure IoT network can be achieved using security mechanisms such as encryption [40] and [41], [42], [43], [44]. Tamper-resistant [45] and software-based solutions may be relevant in the protection of such power and memory-constrained devices from the manipulation of its physical

characteristics [46]. These validate why many institutions and organisations must intensify efforts to secure their IoT Networks from any form of potential cyber-attacks. All of these challenges need to be addressed. Hence, larger organisations such as ARM and Intel are partnering to provide a standard IoT chip security that will allow secure IoT integration through data-driven IoT initiatives such as edge computing, Artificial Intelligence (AI), and autonomous systems [47]. IoT also requires standard and unified architecture to provide advanced interoperability for all IoT devices [48]. In the United States, the action of the California Government passing a conditional bill into law that will mandate manufacturers to equip IoT devices with a reasonable amount of protection in 2020 is one typical example [49]. These developments are meant to prevent the use of any default security features in IoT devices and improve security mechanisms to protect information handled by these devices. In the UK, security by design is the government-created code of practice for consumer IoT devices with the same objectives of avoiding the use of default passwords and giving the objects the capabilities to update, connect and communicate securely while ensuring software integrity and resilience, among others [50]. IoT devices are in most cases associated with the series of attacks witnessed by the vertical industries [51], [52], [53], [54], [46], hence the need to build new products and protocols that are secure by design and complemented by secure processes [55], [56], [57], [58], [59]. The interconnectedness of IoT networks could create more attack surfaces and increase the chance of IoT networks being exploited. Notable examples included the TRITON/TRISIS attack on Schneider Electric Industrial Control System in 2017 [60], the Mirai Botnet that was responsible for the increase in IoT-based DDoS attacks in 2018 [61] and hosts of other notable cyber-attacks within consumer IoT devices and networks. Against this backdrop, this research on IoT for consumer IoT and Critical National Infrastructure (CNI) development is crucial because it contributes to addressing IoT developments' security and bandwidth issues.

1.1 Issues Industrial IoT Faces

Several research issues constantly emerge in IoT networks because they are characterised by heterogeneous communication protocols and hardware infrastructure, and the lack of a standardised implementation framework to manage the network entities effectively. As expected with the increasing IoT deployment rate [62], [12], these challenges are increasing the security threats [63] and other network performance challenges that will be explained in this section. With the many new emerging research in the fields of IoT such as security and privacy [64], IoT device level security [65], [66], Blockchain [67], [68], [69], latency [70], power consumption [71], [72], [27], etc., to reach acceptance by consumers and industry, the following are the current IoT open research problems at the time of writing this thesis that needs to be addressed:

- Security - IoT-based solutions may suffer from different types of security challenges. Manual intervention and third party support are some of the challenges of IoT bugs detection and debugging challenges [73]. Security ensures smooth functionality of the IoT ecosystem and reduces operational damages by every means from attackers [74]. From the concerns on the data privacy of IoT users to the impact of cybersecurity attack on National Critical Infrastructure (CNI), cybersecurity and privacy issues has dominated IoT research space and can be categorised into attacks against IoT devices [54], communication networks [75], and IoT platforms [53]. To address the IoT security challenges, research gaps such as lightweight encryption and authentication mechanisms for Internet Protocol Security (IPSec) and Transport Layer Security (TLS) will need to be addressed.
- Connectivity - Connecting IoT devices have long remained one of the challenges facing IoT [76]. The procedure for authenticating, authorising and interconnecting IoT devices goes beyond the reliance on the centralised server/client method of traditional networks. The performance of IoT networks will depend on the quality of the access network available, coverage, data rate and power consumption, to mention a few. Different wireless technologies have been proposed for IoT applications in different scenarios based on the communication requirements [77], [78],

but will continue to require coverage enhancement to achieve ubiquitous coverage. LTE-M and NB-IoT [79], LoRaWAN [6], NB-IoT [70] and 5G [24] could drive Global Mobile Connectivity for Machine-to-Machine applications. In this thesis, LoRaWAN and NB-IoT were investigated as efficient Low Power Wide Area Networks (LPWANs).

- **Bandwidth** - The efficiency of IoT networks with the growing number of connected devices depends on resource-saving such as bandwidth to achieve reliable data transfer and edge/fog computing capabilities, without which inefficient networks are inevitable. Certain types of IoT services and applications may require more bandwidth than others and, as a result, will have varied impacts on the network traffic as the demand for more bandwidth is increasing [80]. Bandwidth issues pose Quality of Service (QoS) problems to the IoT networks and users. IoT devices operate by sharing the radio spectrum of a specific band, and it is expected to have QoS and latency challenges. Sentience efficiency is one emerging example used to tame the data-hungry IoT devices to minimise unwanted data acquisition and minimise energy and bandwidth consumption. Sentience efficiency as defined in [81] is a dynamic utilisation of hidden joint semantics of data and applications to reduce the work needed to execute IoT applications and minimise system dynamics and energy consumption profile.
- **Power Utilisation** - One major barrier to IoT development is implementing IoT solutions that have low power consumption techniques while it could be sensing, gathering, or sending out huge datasets. In NB-IoT, the excessive repetition of radio access procedure creates a significant imbalance energy consumption profile in IoT devices [71]. Power Saving Mode (PSM) and Extended Discontinuous Reception (eDRX) are two examples presented in chapter 4.
- **Standardisation** - Standardising IoT architecture, communication technologies, network protocols, and data-aggregation schemes are essential for advancing sensor network interoperability in IoT development and deployment. It will also enable a single platform that will provide users with a basis for understanding

IoT while striving to meet the technology needs of the present time [82]. The Institute of Electrical and Electronics Engineers (IEEE), International Telecommunication Union (ITU), Internet Engineering Task Force (IETF), International Organisation for Standardisation (ISO), and International Electrotechnical Commission (IEC) are among the bodies offering standards towards the development of IoT. It shows that multiple standards exist for a particular layer of the IoT due to the heterogeneity of IoT resources [83]. While some standards are open, others are closed and do not support open software, hardware and applications.

- Roaming - IoT concept is based on static nodes with different applications siloed with non-interoperable protocols. The roaming capabilities have been challenging for mobile IoT applications because there are no standardised procedures to interconnect different protocols in constrained environments. For single protocols like cellular networks, roaming agreements could easily be reached by Mobile Network Operators (MNOs). In others such as Wifi [84] and LoRaWAN [85], [86], they could be implemented in constrained environment but for each protocols at a time for optimal performance. There are problems of power consumption, base station handoff in the case of cellular networks and the difficulties of these constrained devices to navigate around frequency bands more efficiently while on low power. Applications with both mobile and fixed IoT devices will require technologies that support roaming similar to [87] where IoT applications have the advantages of being distributed, scalable, and flow controlled. Roaming in IoT allows seamless scaling with fewer configurations, human intervention, and global integration of existing IoT infrastructure.

In summary, as legacy industrial technologies are transforming into new, smart and intelligent ones, the research issues industrial IoT faces are not exhaustive lists. Industrial IoT is revolutionising industries like utilities by introducing an information communication technology ecosystem to the operation and management of the grid. However, the contribution of this thesis focuses on addressing the security and bandwidth issues described in subsection 1.1 above and the contributions presented

in chapter 5, 6, and 7 respectively. Utility networks as one of the industrial critical national infrastructures where IoT is increasingly used to improve the grid operation is a use case in this study. Acquiring real-time data of utility network resources holds the benefits of enabling remote monitoring of substations for fault detection and smooth operation of the system. The performance of Narrowband IoT and LoRaWAN networks was evaluated for industrial IoT in addressing the connectivity challenges presented in chapter 4 and 5. With NB-IoT wireless connectivity for industrial sensors and actuators, industrial IoT can translate existing isolated utility assets into a connected network.

The issues of industrial IoT security and the resulting bandwidth implication are presented in chapter 2.10, 6 and 7. These chapters address the bandwidth and security issues in smart grids by examining the security overhead required for smart grid applications alongside estimating the costs implications and defining the scale of future deployment and spectrum requirements needed to satisfy distributed networks operator's network requirements for grid monitoring and control.

1.2 Research Motivation

Through the World Wide Web (WWW) and Internet technologies came the Internet of Things (IoT), a hot technology utilised in industry to transform legacy industrial connectivity, communication and processes into a new era of smart industrial 4.0. Globally, the IoT ecosystem is faced with many rapidly growing problems that include security and bandwidth presented in chapter 2, 6 and 7. The security challenges for instance are targeted at the three major layers of IoT as discussed in subsection 2.7; the devices, network and application according to [56], [88], [89], and [90]. One may argue that an air-gap security approach is effective and can isolate sensitive network segments, but it does not allow IoT networks to be scaled easily in addition to its expensive deployment nature [63]. Also, authentication and encryption systems have specific advantages and tradeoffs that may make them unsuitable for certain applications. This paradigm shift comes with many challenges and opportunities for both the industry marketplace and

consumer applications. On the challenges, bandwidth can be overwhelmed [29], data can be compromised [91], network can be compromised [92], etc. On the other hand, applications can be remotely controlled [93], data aggregated and latency reduced [28], tasks can be automated [27], etc. From all indications, studies agree that most IoT networks, irrespective of their protocols and implementation strategy, are affected by one potential deployment challenge or the others, like security breaches. Security and bandwidth implementation-oriented problems facing IoT technologies needs thorough investigation of which this thesis has addressed.

Hence, this research is motivated by the need to evaluate new communication protocols and security schemes for secure and bandwidth-efficient communication networks for future consumer and industrial Internet of Things adoption that requires different protocols to coexist and interoperate. The vertical industries have witnessed an increasing number of cyber-attacks which could result from the growing convergence of operational technology (OP) and information technology (IT). New IoT products and applications are constantly introduced as methods of achieving this convergence. These new technologies and existing systems contribute to problems such as data breaches, plant shutdown, control system access denial, network outages, reconnaissance, etc., within the industrial systems. These incidences, such as Distributed Denial of Service (DDoS), have far-reaching implications on the overall performance of industrial IoT systems. These security problems slowing the industrial sectors from implementing these technologies need investigation, of which this thesis has made significant contributions in the areas of network protocols performance characteristics, security, and bandwidth. Therefore, the main motivations of this work are summarised below:

- To understand the general network requirements in the development efforts of IoT for consumer and industrial applications.
- To afford potential industrial and consumer IoT users the assurance of network performance and security using bandwidth-efficient techniques.
- To make industrial monitoring and control operations easy and accessible remotely such that CAPEX and OPEX costs are reduced.

- Give IoT users multiple options of implementing cost-effective IoT communication protocols and security techniques suitable for their organisations based on the budget and network architecture.
- To help design future IoT systems such that industries and users can judge between security, cost-effectiveness, and bandwidth efficiency in their network designs, deployment, and life cycle management.

1.3 Research Questions

Based on the motivations presented in section 1.2, the primary objective of this thesis is to design a secure and bandwidth-efficient IoT network centred on the argument that certain IoT technologies are not yet mature for the industrial domain. Also, the combination of certain security techniques presents significant advantages in terms of effectiveness in bandwidth utilisation and cost-saving while ensuring Confidentiality, Integrity, and Availability (CIA). By exploring emerging IoT protocols and security techniques, secure consumer and industrial IoT networks can be built with network breaches and failures eliminated to increase the users' confidence and identify cost-effective solutions based on the application scenario. Specifically, the objectives of this thesis are to answer the following research questions addressed in this thesis:

- Given the heterogeneous reference architecture of consumer and industrial IoT, it is feasible to apply consumer-oriented IoT security in the industrial IoT domain and mitigate performance impact?
- Is it possible to increase interoperability between industrial and consumer IoT domains and still maintain performance and security?
- What are the trade-offs between unlicensed LoRaWAN and licensed NB-IoT wireless technologies, and how can their performance impact IoT penetration in developing countries?
- To what extent does the performance of LoRaWAN and NB-IoT differ in terms

of security, data throughput, latency, and energy utilisation, and how can they be improved?

- How vulnerable are legacy IoT networks, and what security mechanisms could help retain security against potential attacks?
- What are the benefits of adding IEC 62351 security standard to industrial IoT networks, and can it increase security while reducing bandwidth?

1.4 Methodology

The research methodology adopted in this thesis is based on experimental and analytical research methods following the iterative process as shown in figure 1.3. The real-world problems to be addressed are first raised, and the premises provide the background for the research questions posed. Through the analysis of research problems, the limitations are identified and taken into account. The experimental research is adopted to design, build and investigate the security and network performance of IoT protocols such as LoRaWAN, NB-IoT and IEC 60870-5-104 protocols. An example of an IoT device used for the LoRaWAN and NB-IoT experiments is the Fipy 1.0 by Pycom, shown in figure 1.1. With this single embedded IoT device, different wireless technologies such as SigFox, LoRa, WiFi, Bluetooth Low Energy, LTE-M, and NB-IoT can be implemented independently. Implementing more than one protocol concurrently is still challenging due to memory and processing limitations but is subject to increasing energy consumed and technical complexities. When configured to support LoRa, the LTE features must be turned off for optimal performance. It also supports the encryption and authentication security schemes presented in chapter 6 and 7.

The analytical method is used to evaluate the network Quality of Service (QoS) and the effects of secure authentication, Internet Protocol Security (IPSec), Transport Layer Security (TLS), and IEC 62351 on the bandwidth and cost while varying the network resources and test scenarios. For these evaluations, an analysis of secure industrial IoT networks for remote outstation operations in smart grid is performed at the University of Strathclyde Power Network Demonstration Centre (PNDC) test facility shown in

Chapter 1. Introduction

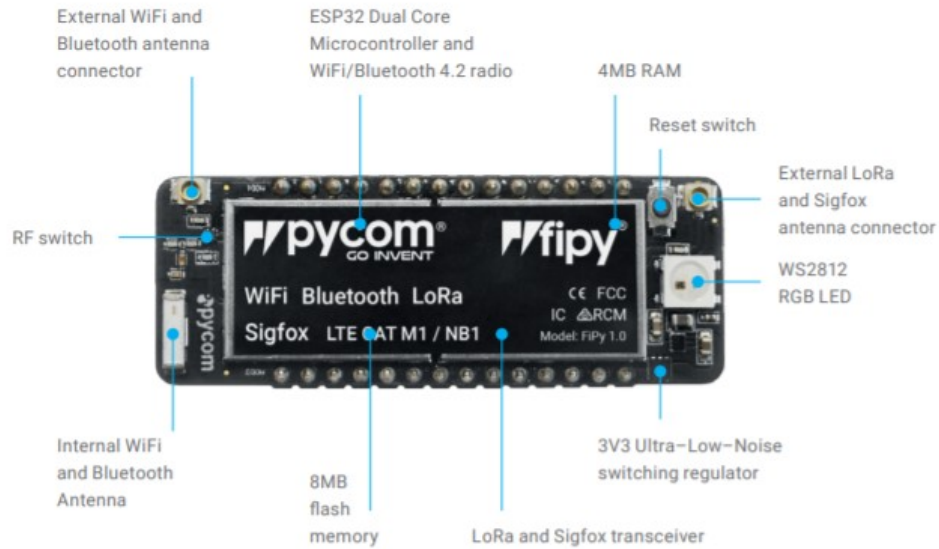


Figure 1.1: An IoT Device by Pycom that supports many IoT protocols and ports for sensor network integration

figure 1.2. This is one of the contributions to the security problems of interconnected industrial IoT devices, such as enabling fully integrated information and operational technology that is low-power, bandwidth-efficient, reliable and secure. Based on the research questions outlined in section 1.3, this study adopted the following step-wise research approaches:



Figure 1.2: University of Strathclyde, PNDC

In order to identify the key characteristics and application requirements of the IoT use cases, we first conceptualise and design secure network architecture for each exper-

iment. The key technologies, services and applications of industrial IoT use cases are identified through an extensive literature review process. The critical reviews formed the theoretical basis for answering all the research questions. The specifications of the protocols to be investigated are highlighted while obtaining a qualitative understanding of the design, deployment and accompanying implementation challenges. The systems are then implemented and evaluated based on the test performance requirements of the network scenarios. Key findings, conclusions and recommendations following the outcomes of each of the tests are highlighted to drive home the major contributions and possible new areas of research arising from the challenges encountered.

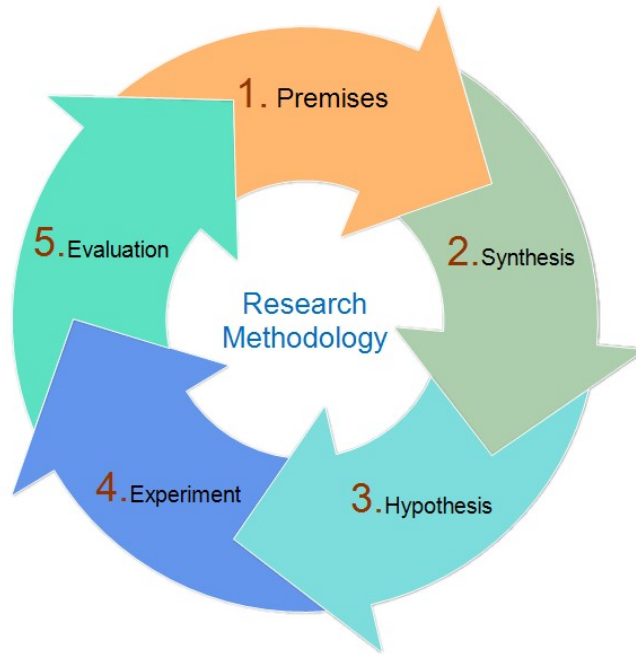


Figure 1.3: Research Methodology

1.5 Novelty and Contributions of the Research

Research in IoT is growing exponentially, but little work has focused on investigating the bandwidth, cost, and other network QoS performance implications of different security mechanisms or combining multiple security techniques in different industrial IoT protocols. Hence, the main contributions of this research are centred around multiple

technical issues and experiments for developing secure consumer and industrial IoT networks, determining the security overhead of each security scheme or the combination of security schemes tested and evaluating the network QoS performance, and the cost implications. Different transport and network layer security protocols were investigated in an industrial network to compute the resulting overhead, bandwidth, and costs. The summary of the contributions of this thesis are as follows:

- **Protocol** - An implementation of a robust and secure LoRaWAN and NB-IoT protocols for data acquisition system. IoT applications in constrained environments with limited memory, storage and processing capabilities are evaluated based on the network QoS parameters through design, implementation, test and validation. The testbed is presented in chapter 4 and its performance in chapter 5. Based on the performance of NB-IoT and LoRaWAN networks, both have the potential to drive non-critical industrial IoT. However, the results show that NB-IoT performed better than LoRaWAN in terms of data throughput, latency, and security but at higher deployment costs and power utilisation. Similarly, a smart grid test setup based on IEC 60870-5-104 at PNDC **See CP4** allowed bandwidth estimation following SCADA polling of RTU measurements.
- **Security** - A robust and secure IoT testbed is built and evaluated for Industrial IoT security model. The security model considered device capabilities, encryption and authentication techniques. An in-depth practical approach to setting up an NB-IoT test network is presented in chapter 5 alongside results of throughput, security, latency and power utilisation performance. The NB-IoT network leverages the coverage opportunities of licensed cellular networks. Also, for the utility network, TLS and IPSec were investigated alongside bandwidth and costs implications, **see C8**, **see C9** and **C10**.
- **Bandwidth** - For secure and bandwidth-efficient IoT networks, a TLS and IPSec-based Internet of Things is evaluated, see chapter 6. The security approach is based on the investigation of TLS and IPSec, an aspect of IEC 62351 security standard over Ethernet to provide adequate security for industrial IoT networks.

Based on test and security analysis, the use case examined the impacts of TLS and IPSec on the available bandwidth. The resulting overheads are presented with the pros and cons of each security scheme and when combined, **see C10**.

- **Cost** - Based on Internet of Smart Grid (IoSG) investigations, a model for industrial IoT security and bandwidth is developed to reduce costs and improve the security of power networks. The performance of TLS and IPSec over radio technology is presented with the addition of secure authentication. The bandwidth requirements of TLS, IPSec, and SA needed to secure a smart grid are computed, **see C8**. Different combinations of security schemes are recommended from the results but are dependent on hardware, network, communication, and budget requirements. As presented in chapter 7, it is found that secure authentication is cost-effective in constrained IoT assets compared to TLS and IPSec.

1.6 Thesis Outline

The thesis layout, as shown in figure 1.4 illustrates the relationship between chapters and how they are organised into sub-sections. Chapter 2 presents the literature review that introduces the concepts of the Internet of Things discussed in the technical chapters. The underlying principles of industrial and consumer IoT, communication protocols, security challenges, and bandwidth are explored. The first contribution is this thesis is presented in chapter 3. An NB-IoT testbed is designed, implemented, and tested alongside the LoRaWAN network to evaluate the performance of both networks. Through comparative analysis, deductions on power, security, latency, and throughput were made regarding real-world scenarios. Chapter 4 and 5 extends the evaluation of IoT networks to an industrial domain where the effects of different security schemes on bandwidth were examined at PNDC in collaboration with major utility network providers. Finally, chapter 8 concludes this thesis and outlined the contributions, and challenges of industrial IoT, and poses future research directions

Chapter 1. Introduction

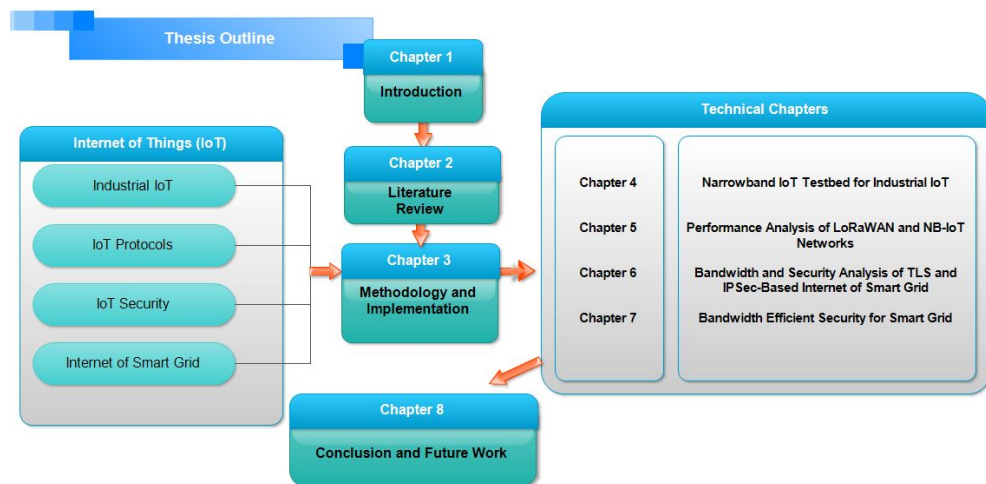


Figure 1.4: Thesis Outline

Chapter 2

Literature Review

The Internet of Things (IoT) overview is a widespread concept of connecting anything to the Internet irrespective of time and location. To this end, interoperable ubiquitous devices are integrated through different connectivity solutions through which technical, social, and economic objectives are achieved. This definition varies from one use case to another, and it depends on two important aspects of IoT: “*Things and Internet*”, including the hardware and software components. The following are current and relevant definitions of the IoT as referred to in this thesis:

- **IEEE, 2014** - “A network of items - each embedded with sensors - which are connected to the Internet”
- **IETF** - “IoT is the network of physical objects or *things* embedded with electronics, software, sensors, actuators, and connectivity to enable objects to exchange data with the manufacturer, operator, and/or other connected devices” [\[94\]](#)
- **NIST, Global City Teams, 2014** - “Connecting smart devices and systems in diverse sectors like transportation, energy, manufacturing and healthcare in fundamentally new ways. Smart Cities/Communities are increasingly adopting

In this section, an overview of the Internet of Things technology is provided by analysing the components of IoT domains. Specifically, the difference between consumer and industrial IoT is explained, their various types of applications and broader adoption perspectives of IoT are discussed. Various IoT state of the art is discussed in this chapter. The emergence of the paradigm, its fundamentals, protocols, architecture and security are covered and drawn from the relevant lists of publications in the preliminary pages.

CPS/IoT technologies to enhance efficiency and sustainability operation and improve the quality of life.” As considered by NIST, CPS and IoT are used interchangeably.

- **ITU-T Y.2060, 2012** “A global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving, interoperable information and communication technologies.”
- **In this context** - “IoT is considered as a network of memory, power and processing-constrained embedded devices with the capability of performing consumer or industrial related tasks through wired, unlicensed or cellular Low Power Wide Area Networks (LPWANs).”

The Internet of Things has gained significant attention in research institutions and industries, promising an intelligent and seamlessly connected world. The concept of “Internet of Things” (IoT) presumably began in 1999 when the MIT Executive Director of Auto-ID labs, Kevin Ashton, in a presentation for Procter and Gamble used the term to mean an extension of the capabilities of the Internet and Radio Frequency Identification (RFID) technologies that have the potential to improve the efficiency of machine-to-machine communication [95]. The IoT concept has since scaled towards achieving a fully connected IoT world through the creation of Internet Protocol (IP), where industry, academic institutions and government agencies collaborate to create an enabling environment for any operation that involves machines and human interactions. The essential requirement for creating IoT networks is that physical objects such as sensors and actuators must have unique IP addresses for relating sensing (interconnectivity) and actuating data, be able to communicate via wireless networks and its application performing notification and control functions [96]. The IoT ecosystem has been predicted to double in connected devices every five years. According to the 2021 Ericsson IoT growth forecast, short-range IoT is predicted to make the highest contribution with a CAGR of 12%, consisting of devices, communication technology, the Internet, data storage and processing components for any application. One would

ask, why monitor and control things remotely over the Internet?. Every IoT network connectivity is a hybrid of wired and wireless technologies. Still, specific applications such as teleprotection function, fault detection, and diagnostic operations in power networks are required to be performed faster, more efficiently, and with minimal costs over a secure internet connection. Table 2.1 is an overview of different technology protocols for IoT that could be integrated to drive the growth of IoT.

Table 2.1: General Classification of IoT Communication Protocols into Wide, Local and Home Area Networks

WAN	LAN	HAN
LoRa	DECT	ZigBee
Sigfox	M-bus	Bluetooth
2G/3G/4G/NB-IoT/LTE-M/5G/6G	Wavenis	NFC
Sigfox		Bluetooth Low Energy
WiFi		
GPRS		

The technology development disciplines enabling the Internet of Things, as shown in figure 2.1 are categorised into communication technologies, services, Internet and external peripherals. There are increasing contributions in IoT components, especially in cloud/edge computing, embedded systems, machine learning and artificial intelligence, etc., for applying IoT approaches in different contexts. For industrial IoT, this would add to the benefits of digital transformation by enabling interactions between large heterogeneous devices.

2.1 IoT Historical Perspective

Communication network concepts already existed and have been under development in line with the Internet development journey that started with the Advanced Research Project Agency Network (ARPANET) in 1969 [97]. ARPANET interconnected computing systems within academic research centres, government agencies and private organisations to share general-purpose resources. As an emerging technology paradigm, IoT is evidence of technology advancement that began in the 1980s with the introduc-

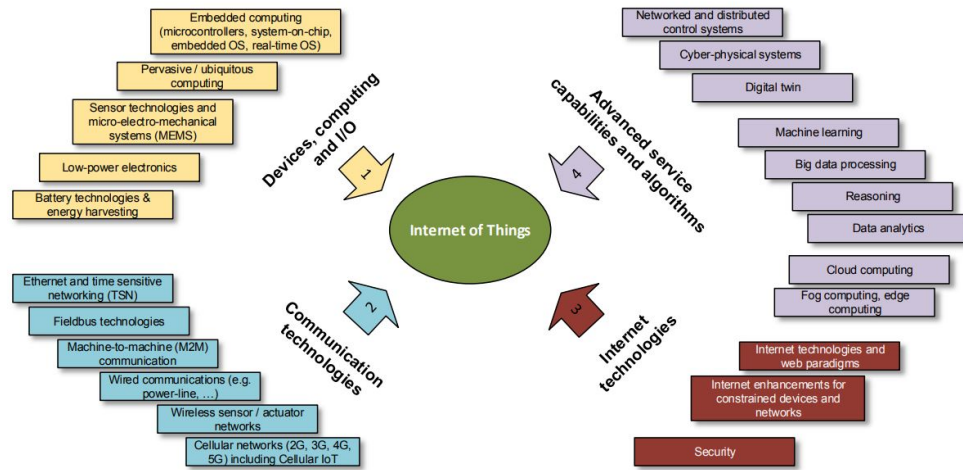


Figure 2.1: IoT Technology Enabler [1]

tion of Industrial Control Systems (ICS) and progressed in 1983 with the introduction of the first automated inventory systems [98]. The technology transformation journey has seen many inventions that make human-to-machine and machine-to-machine tasks simpler, shorter, and delivered with higher accuracy at minimal costs. The recent technology uptake took momentum in 1999. It can be seen from the widespread adoption of ubiquitous IP connectivity, the decreasing cost of semiconductor components due to miniaturisation advances in edge and cloud computing, virtualisation, and data analytics for the broader Internet needs.

In what could be classified as the first IoT applications in chronological order is the discovery of Radio-Frequency Identification (RFID) in the 1970s that enabled remote monitoring and control of non-line-of-sight objects in challenging locations [99]. With tags and bar codes technology, IoT objects are tracked for device location and identification, tolled for data visualisation, or monitored remotely like the door passive transponder. In the 1980s, the Coke Machine was one example of early IoT devices connected to the internet [100]. Embedded systems and sensor technologies were actively developed for different IoT applications in the 1990s with the first M2M protocol MQTT development. IoT and digital technologies have become mainstream in many applications from the 2000s and beyond but are considered mainly not secure and immature, reflecting the diversity of communication requirements. It has evolved to

Chapter 2. Literature Review

several areas of our daily lives due to its comfort and digitisation insights for industrial and generic applications with clear distinction [98]. See figure 2.2 for the remaining part of IoT historical development to 2020.

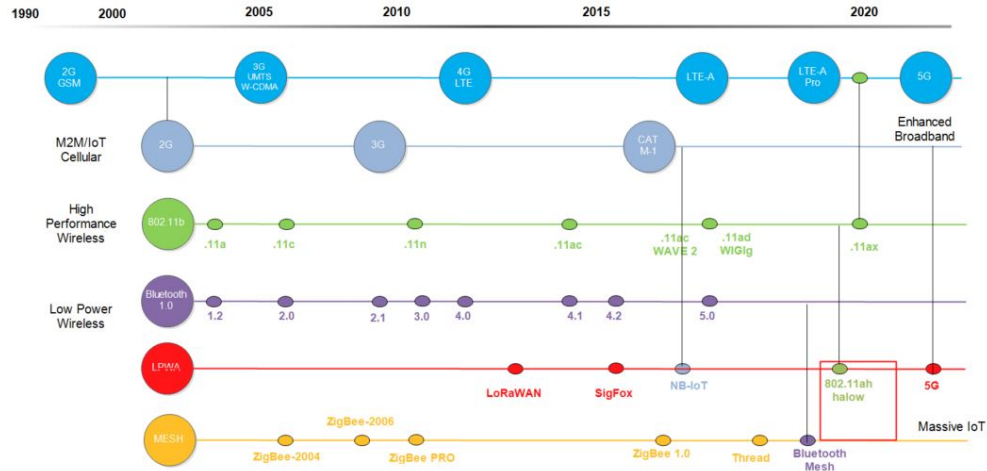


Figure 2.2: IoT Wireless Connectivity Landscape and Historical Development [2]

IoT development is also driven by different licensed and unlicensed wireless technology. Kimberly Tassin of Sequans Communications first identified the opportunities for IoT driven by licensed cellular technology. In Kinberly’s brief article, M2M LTE chipsets and modules were seen as the foundation for flexible, robust, secure, and low-cost global IoT solutions [101]. For LTE networks, the benefits of LTE-enabled IoT devices are the LTE’s IP-based architecture, economic of scale (cost/bit of data compared to 2G and 3G), security by design, high adoption of LTE for IoT, and an efficient (three-time and 20 times better than 3G and 2G respectively) data traffic management as the advantages [102]. The future potential benefits could include IoT devices being able to function autonomously. According to Cisco wireless connection analysis, LoRa and NB-IoT technologies for M2M are expected to contribute from 223 million devices in 2018 to 1.9 billion by 2023 [103]. The number of M2M applications across industries globally is expected to reach 14.7 Billion with 19% CAGR between 2018 and 2023. The historical growth of IoT is shown in figure 2.3.

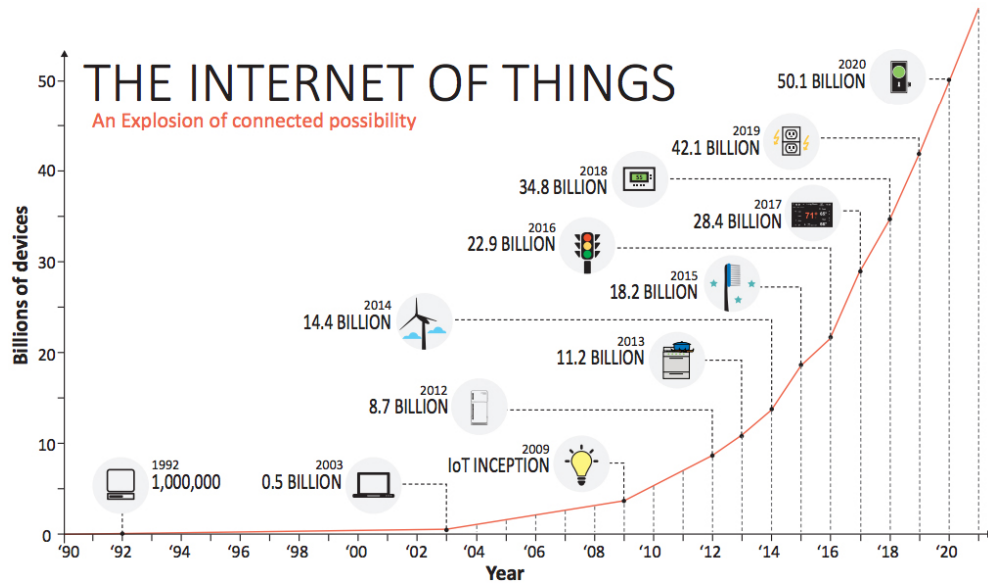


Figure 2.3: Internet of growth Forecast to 2020 [3]

2.1.1 IoT Devices

IoT devices, sometimes referred to as User Equipment (UE) in this thesis, are pieces of embedded hardware with limited connectivity, data storage, and processing capabilities, such as sensors ranging from consumer wearables to industrial actuators designed for specific applications that require transmitting data over the internet or other networks. IoT sensors can monitor and measure physical quantity such as temperature and humidity depending on the application, size, embedded operating systems and communication protocols [104]. Power utilisation, storage capacity, coverage, processing efficiency, size, cost, reliability, interoperability, and life cycle management are some of the challenges of IoT devices [105]. How the IoT networks are commonly set up impacts the roles of each IoT device often deployed in environments without human intervention. Where data is processed on the IoT edge, demand for more bandwidth/security and processing capabilities will increase [35, 80]. IoT devices are the perfect recipe for cybercrime as it presents an opportunity for cybercrimes to be committed, and the implications of their use have been understudied. As a new and emerging technology, stakeholders must pay more attention to security issues when driving market competitiveness. This has not been the norm, and as a result, IoT devices are manufactured with security

vulnerabilities, paving the way for cybercrimes to be committed as new devices are introduced [51]. Amy Webb of Future Today Institute highlighted that “ Technology can be like junk food. We will consume it, and even when we know it’s bad for us ” [106]. The security implications of the use of IoT devices are the compromise of data and privacy and the vulnerabilities due to:

- **Poor Implementation** - IoT manufacturers play a critical role in establishing the security features of IoT devices, and the focus should include both ease of use and the implementation process. Prioritising return on investment makes most IoT devices lack the proper authentication and other security features. Some IoT devices use default security credential, which is the same for similar or the same products. This makes it easy for an attacker to gain access to such a device. As IoT scales, lightweight authentication techniques like private and public keying infrastructure are needed to resolve these issues [107].
- **Unencrypted Messages** - Confidentiality is guaranteed when the messages exchanged between IoT devices are obscured from cyber attackers. The confidentiality of a network can be evaluated with plaintext, encoded, or encrypted data types exchanged between devices or devices and servers [51]. Due to the ease of use of many IoT devices, the communication between them appears unencrypted, making it possible for man-in-the-middle, side-channel, and other data-driven attacks to occur. When a message request is routed over the internet, it passes through various networked devices that different people and organisations maintain. When these devices transmit data as plain text (unencrypted), software on any of the other devices can read such data [89]. The threats also come from known operational inefficiencies like the inability to restrict access from a non-secure network or data mobility, which leaves sensitive information in the attacker’s domain. In [108], a wireless radio network was vulnerable to a DDoS attack due to unencrypted data at the radio link level. It is important to state that encrypted data does not mean absolute security. For instance, encrypted data tags available to an attacker can be used to obtain other information that

breaches privacy, such as the number of people in a building [109] or their location information.

- **Lack of Authentication** - Timely validation of software, hardware and activities logs ensures the authenticity and confidentiality of networks. Strong authentication pairs provide secure access to the IoT network and prevent attacks like Distributed Denial of Service (DDoS) and replay attacks. If network access control and updates are not correctly authenticated to know if the data is from a trusted source, then malicious programs could be installed in the guise of a genuine update. Usually, firmware updates equip IoT devices with an upgrade tool that will enable them to perform improved operational instructions without a corresponding upgrade in the hardware. The updated firmware will bring new performance in the various functions of the devices, such as security. IoT device security challenges could be tackled if authentications of firmware updates are periodically applied to ensure new security features are in place [89]. This could be common at the edge computing level and in training machine learning algorithms, where fake datasets or nodes are introduced early to deviate the system from learning valid model [109]. The combination of intrusion detection and authentication scheme, group authentication and key agreement, and electrocardiogram-based authentication with privacy preservation is the future research direction recommended for smart industrial devices [43].
- **Inadequate Storage and Processing** - IoT devices require high processing and storage capabilities to handle high volumes of security data. Fog/edge and cloud computing are concepts designed to overcome the limitation of storage and processing resources in IoT devices. IoT data could be text, audio, video, or images in either structured or unstructured format [105]. Adequate data storage and processing at the edge would also allow network-level processing to reduce latency and costs by reducing the volume of data sent to the cloud [110]. The data management for the traditional network is inadequate for IoT, but middleware or architecture-oriented data management approaches are used for integrat-

ing, indexing and managing IoT data [111]. This is most useful in latency and security-sensitive applications like the smart grid. Examples of some few available utility cloud platforms are Cisco IOx, PI System by OSIsoft [112], Predix Platform by General Electric Digital [113], Celebra by Flutura [114], Azure IoT by Microsoft [115], Watson IoT by IBM [116], etc.

- Insecure Protocol** - Communication technology is one of the essential parts of an IoT network that enhances security. LPWAN technologies are categorised in table 2.2 except Bluetooth, ZigBee, Z-Wave and other short-range near-field communication technologies. In this thesis, NB-IoT and LoRa are the two low-data wireless communication technologies considered for experimental evaluation. They are limited to not reliably supporting audio and video data transmission but find wide usage for connecting IoT devices securely transmitting a few bytes of data at intervals. This is mainly done when throughput is not as important as the range of transmission and power utilisation [117]. For short-distance communication below 100 meters and data rates below 250 kbps, Bluetooth and ZigBee should be used to establish a communication link between IoT devices. For the network types that require high data-carrying capacity, the protocols that should be employed must support low-latency bi-directional communication to provide reliable communication between network cores. However, radio interference exhibited in the industrial environment increases the delay and also reduces the rate of data transmission [118]. Also, one of the downsides of using LPWANs for IoT, especially in the unlicensed spectrum in addition to perceived interferences in all transmissions [98], is spectrum congestion [119]. 4G and 5G technologies, as discussed in section ??, are employed in IoT networks to deliver high reliability, security and throughput.

Table 2.2: Characteristics Comparison of Licensed and Unlicensed LPWANs [10], [11], [12] [13].

Network Items	SigFox [78]	LoRaWAN [11]	NB-Fi [120]	NB-IoT [121]	LTE-M [79]
Bandwidth	100 Hz	250 kHz & 125 kHz	50 Hz - 25.6 kHz	200 kHz	200 kHz
Modulation	BPSK	CSS	DBPSK	QPSK	QPSK
Standardization	SigFox/ETSI	LoRA Alliance	WAVIoT	3GPP	3GPP
Max. Data Rate	100 bps	50 kbps	25 kbps	200 kbps	200 kbps
Bidirectional	HD	HD	FD & HD	HD	HD
Architecture	SoS	SoS	SoS	SoS	SoS
Frequency	ISM-bands	ISM-bands	ISM-bands	LTE-bands	LTE-bands
Payload	UL-12B & DL-7B	243B	240B	1600B	256B
Security	AES-128	AES-128	AES-256	LTE Enc	LTE Enc
Interference	High	High	High	Low	low
Urban Range	10 km	5 km	10 km	1 km	1 km
Rural Range	40 km	20 km	40 km	4 km	4 km

Note: **B** - Bytes, **SoS** - Star-of-Stars, **UL** - Uplink, **DL** - Downlink, **Enc** - Encryption

2.2 Applications of IoT Technologies

As more devices from different fields of endeavour are getting connected to the internet daily, the scope of IoT applications continues to increase [122]. Various IoT-related services and applications have been greatly discussed in many articles where IoT is generally perceived as the driver of many business outcomes in different use cases by adopting different communication technologies, see figure 2.4. IoT has become a reality in various applications, from enabling home automation, smart banking, education and training services, and advancing manufacturing, transportation, and agriculture to smart cities. The implementations present different sets of challenges, some of which are presented in [123], [104], [124], [125], [62]. In industrial IoT, the challenges include semantics, computation, communication, identification, and sensing technologies [96]. In this thesis, smart grid is discussed in great depth to demonstrate the opportunities and challenges in a network environment critical to national development; see the technical chapters 5, 7, 6. The motivation is the concept of ensuring a reliable, secure and bandwidth-efficient utility IoT network as a way of solving monitoring and control

issues. Smart grid has real-life benefits where data security and privacy remain critical requirements as discussed below:

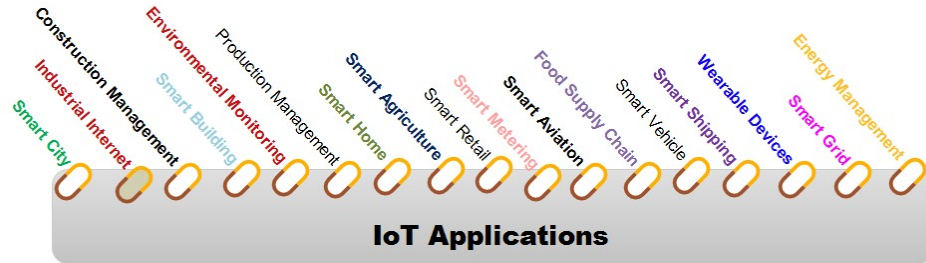


Figure 2.4: IoT Applications

2.2.1 Smart Grid

The Smart grid is the concept of modernising electric power systems, communication technologies, and information technologies to allow secure, efficient, and reliable power system operation. From a broader perspective, it is a communication network for gathering and analysing electricity generation, transmission lines, distribution substations, consumer infrastructure, and other grid components data to predict power demand and supply variations and ensure energy security. It introduces new functionalities such as increased power quality, self-healing, resistance to errors and attacks to the grid [126]. Smart metering, real-time grid monitoring, and Electric Vehicle (EV) charging are applications that could be deployed using wireless technologies to meet the communication requirements of challenging environments with limited infrastructures. When Advanced Metering Infrastructure (AMI) is interfaced with cellular technologies, grid measurements will be achieved in real-time. IoT provides various additional applications to the smart grid depending on the network types. IoT's sensing and processing capabilities can improve critical aspects such as self-healing, protection, disaster recovery, and reliability [127]. IoT can enhance the monitoring of different energy generation sources in electricity generation, but there are challenges to integrating IoT in the smart grid. A compromised smart grid-based IoT data could influence the grid's performance and could go as far as invading privacy. If, for instance, the consumer heating system

data is compromised, it could be used to determine when the consumer is at home or not, and targeted attacks could occur.

2.3 Industrial Internet of Things

The Industrial Internet of Things (IIoT) is an evolving technology that harnesses the wireless and computing power of industrial devices (OT and IT) to interact with the physical world through the Internet. IIoT is a network of machine-type IoT devices that finds applications in many fields [128] to facilitate IoT system efficiency, drive real-time automation, and reduce operational and maintenance costs [129]. Traditional IIoT is a network of industrial control systems termed Operational Technology (OT) with unique communication protocols. General Electric (GE) described it as “*an internet of things, machines, computers and people, enabling intelligent operations using advanced data analytics to transform business outcomes*” [130]. However, security concerns are always present for resource-constrained industrial IoT devices requiring additional resources to implement new cyber security features, including what industrial IoT device should be connected to the internet and for what purpose. The reasons have extended beyond a typical example of remotely turning ON or off electronic devices or for process automation [131]. Current requirements include making IoT devices smarter, interconnected, and sharing data seamlessly over secure internet platforms to improve efficiency and productivity levels [132]. Other benefits and future research areas include reconfigurability, remote access, scalability, interoperability, power utilisation, standardisation, and low latency communication.

The convergence of Information Technology (IT) and OT networks brings many control, monitoring, operational, and cost-saving benefits and exposes OT network boundaries to new cyber security threats. The convergences are occasioned by emerging technologies shown in figure 2.5. IT and OT networks have the same Confidentiality, Integrity, and Availability (CIA) priority in the network/information security model but ranked in different priority order, IT – (CIA) and OT - (AIC) [59]. This implies that certain compromises must be reached in some legacy OT use cases in prioritising safety

and availability against security. An IT system may trade availability with security by shutting down systems in the event of cyber-attacks. In contrast, OT may trade availability with security when not connected to the internet.

Industrial cybersecurity is the process of protecting Industrial Control Systems (ICS) from cyber-attacks. Industrial cyber threats could come from the inside or outside and relate to industrial safety to protect critical infrastructure. Privacy and security are among the leading concerns for applying IoT in industries. The security vulnerabilities recorded in generic IoT networks are increasingly seen in the industrial domains [131]. Notable examples include the Stuxnet discovered in 2010 by the VirusBlockAda that affected the Iranian uranium facility in 2014 [133], the Mirai botnet that affected millions of network routers and IP cameras in 2016 [61], the Distributed Denial of Service (DDoS) attack that took down the Finland heating system in 2016 [52], Brickerbot that leveraged the default password and user names on IoT devices in 2017 [134], and the 2021 Colonial Pipeline ransomware and data breach cyberattack that impacted computerised devices [53]. The security systems developed for consumer IoT networks cannot be directly deployed to industrial networks because of the differences in communication requirements. The communication requirements of Cyber-Physical Systems (CPS) and generic IoT are different and not defined [128], but they are expected to handle data processing with higher levels of CIA. Similarly, emerging IoT innovations enable the successful convergence of IT and OT networks with no formal boundary [55].

2.3.1 Related Work

Security is one of the existent gaps in industrial IoT systems. Industrial networks comprise legacy technologies such as Control and Data Acquisition (SCADA) systems, Human Machine Interface (HMI), Distributed Control Systems (DCS), ICS, and Intelligent Electronic Devices (IEDs) that have common security issues such as implementing lightweight authentication and encryption systems, updating security patches, enhancing interoperability, etc. They do not meet the cybersecurity requirements of the current IT threats permeating into OT environments by using new IoT devices for different purposes. IoT products are implemented based on market competitiveness

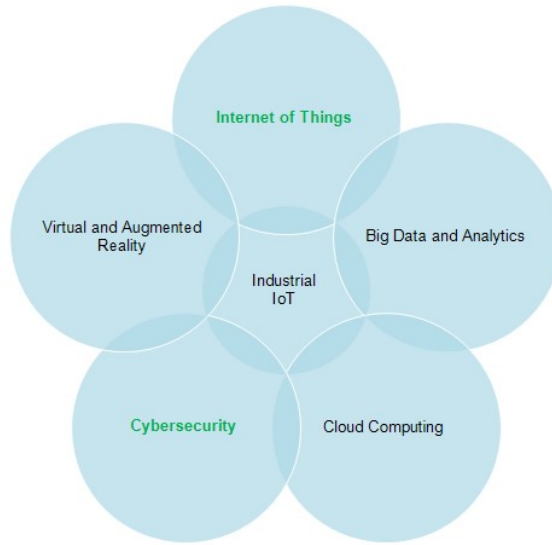


Figure 2.5: Key Technologies Driving Industrial IoT

to get hold of the market and increase return on investments rather than on building secured systems [55]. Software and hardware are often deployed from the research laboratories to real-life situations without proper testbed investigations. The testing, when carried out, is on a small scale [135], [136], [137] and cannot be extrapolated to the actual world scenario in capacity and performance.

The publications by the Industrial Internet Consortium (IIC) show a great deal of effort in ensuring that features such as “interoperability, security, connectivity, business models, and standards architecture are firmly rooted in reality” in the approved industrial IoT testbeds [138]. The report also indicates that most designs initially lack edge security implementation for Device-2-Device (D2D) and Device-2-Cloud (D2C) communications. According to the Internet Security Framework (IISF), most IoT security solutions claimed were not substantiated but are the same as the existing IT systems network and firewall security approaches. However, the current research effort is towards developing common security frameworks for cyber-security in IIoT systems that will smoothly realise industrial 4.0. IIoT refers to applications in manufacturing, healthcare, energy, smart city, transportation, while Industrial 4.0 refers to the manufacturing sector [130] – both terms are used interchangeably in this thesis.

There are many approaches to tackling industrial IoT security. One approach is

through modelling and validation of network designs. A Model-Based Design (MDB) has been proposed to handle cyber-attacks on CPS [139]. However, the methods have limitations on modelling and analysing capabilities for the physical and cyber domains, as observed in the Extended Data Flow Diagram (xDFD) approach and Attack Tree-Based Model [140]. For instance, the study of power networks could be modelled in MATLAB/Simulink to investigate fuzzy, interruption, man-in-the-middle, replay, overflow, and down-sampling security attacks (cyber security functions) scenarios and countermeasures opportunities before the method is implemented. Another approach uses nanoscale electronic technology primitives such as memristors, carbon nanotubes and graphene [141]. Integrating nanoscale technology into IoT design adds good authentication and secret key generation mechanisms with bits response rate error as the potential downside. Such errors can be resolved by error correction cryptographic systems such as the syndrome-based and code offset schemes, especially in **Physical Unclonable Function (PUF)** [142]. PUF security by design approach allows security to be introduced at the circuit level of IoT devices during the manufacturing process. More studies have been conducted on security key generation using PUF [65], in which some were found to be vulnerable to modelling attacks and are affected by other factors such as thermal noise, electrical properties, and ageing [66] [143], [144], [145].

Securing IoT nodes, in [146] used a traffic-aware detection and patching scheme to strengthen the wireless networks of IoT devices by resolving the critical sections of intermediate nodes using traffic information. The intermediate nodes here refer to gateways, computer systems, and access points that must be intelligent enough to detect the links where malware emanates from. However, the end nodes in industrial IoT are difficult to patch because of their limited processing capabilities, which stops them from recovering from attacks. Software-based security for IoT devices seems impracticable as problems of resource constraints, software update capabilities, and power consumption remain open research areas. However, Software Defined Networking (SDN) has been proposed to improve access security and defend industrial IoT from DDoS attacks [147]. Most known IIoT attacks are usually launched through servers, memory units, I/O bandwidth, sockets, Internet Control Message Protocol (ICMP), Domain Name System

(DNS), User Datagram Protocol (UDP), and Transmission Control Protocol (TCP).

The risks associated with IoT devices can be evaluated using a graphical approach. Gemini et al. used a three-phased model to pre-process network vulnerabilities, graphically analyse their dependencies, and visualise security parameters [148]. Cost modelling is the framework for improving the risk mitigation strategy for industrial IoT networks' overall security and operational efficiency. To introduce a secured IoT system with zero human intervention as against the user-dependent provisioning common in Amazon Web Service, Microsoft Azure, and OneNet, [149] implemented a Remote Authentication Dial-In User Service and one-time password authentication system to perform the provisioning process (discover and connect to IoT network) using a state machine. The method performs far better than the legacy ICS and can complete the provisioning process within 4 seconds.

2.4 Industrial IoT Communication Protocols

How IoT devices communicate data depends on networking technology. Many communication protocols exist for different IoT layers. Some are legacy communication protocols with security and bandwidth issues as described in section 2.14. Fulfilling IoT network performance characteristics such as reliability, security, and latency requirements becomes difficult to achieve [150]. For the application layer, protocols that are commonly used include but are not limited to Message Queuing Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP), HyperText Transfer Protocol (HTTP), Constrained Application Protocol (CoAP), Data Distribution Service (DDS), Extensible Messaging, and Presence Protocol (XMPP) [151]. The protocols used in this thesis are explained below. Refer to figure 2.7 [48] for an exhaustive list of IoT protocols for different network layers.

2.4.1 Message Queue Telemetry Transport

Message Queue Telemetry Transport (MQTT) is one of the lightweight messaging protocols for constrained IoT sensor networks and operate on publish-subscribe and

request-response patterns [152] as shown in the architecture in figure 2.6. It is specified by OASIS [153], developed by IBM and relies on TCP/IP protocol to incorporate Secure Service Layer (SSL) between clients and brokers. MQTT is more bandwidth efficient than HTTP and CoAP as a result of its data delivery models that make it suitable for use in constrained devices with limited resources. It is also used in applications platforms where data is efficiently handled. Mosquitto is a good example that has a standard server and client implementation tools for MQTT protocol [154]. MQTT broker facilitates the communication between two clients (mosquitto_pub and mosquitto_sub) that filters published data and distribute them to the clients that subscribed to the published topic. As shown in figure 2.6, the temperature reading of DHT 11 is published by the message source based on a specific topic and information and sent to the broker. The MQTT message subscribers for having subscribed to that particular topic can then receive the temperature value, and in this case, a single message sink is used. The messages are routed via reliable and secure (TCP/TLS) transport protocols.

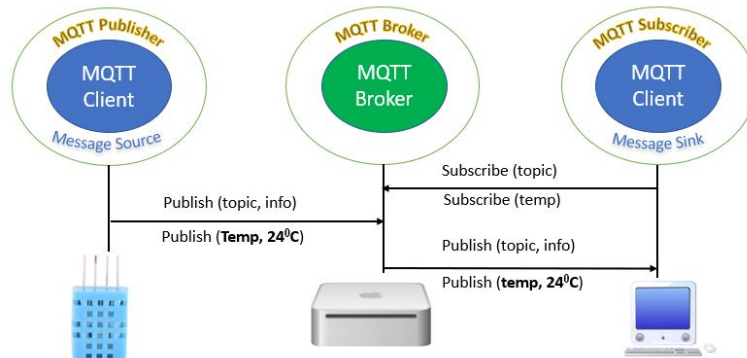


Figure 2.6: MQTT Publish-Subscribe Architecture

2.4.2 Hypertext Transport Protocol

Hypertext Transport Protocol (HTTP) is the standard stateless communication protocol for web-based IoT applications that relay IoT data over the internet [151]. Its operation is based on request/response protocol for a server-client communication model. In the form of data negotiation, the client sends a message request to the server, and the

server (host) in turn generates a response message. It has higher bandwidth demand due to the complex Extensible Markup Language (XML) header and is considered inefficient for constrained IoT applications. Over TCP transport, TLS security features provide a secure communication channel for IoT applications.

2.4.3 WebSocket Protocol

WebSocket protocol enables establishing (TCP connection) two-way communication between the IoT devices and the wireless systems. In the case of NB-IoT, as described in chapter 3.2 and chapter 4, WebSocket allows the UE (client) to access the LTE eNB (server) through a remote Application Peripheral Interface (API) as defined in the Request for Comments (RFC) 6455 [155] in JSON message format. Client messages communicated to the server represent an array of message object interactions in real-time via HTTP protocol. The first method in the WebSocket protocol stack establishes the HTTP connection and allows interactions between the server and client through the HTTP upgrade request. The connection is kept active with either the server and the client is able to send WebSocket frames until the client closes it at the end of the packet transfer. A new socket connection procedure is needed for subsequent transmissions.

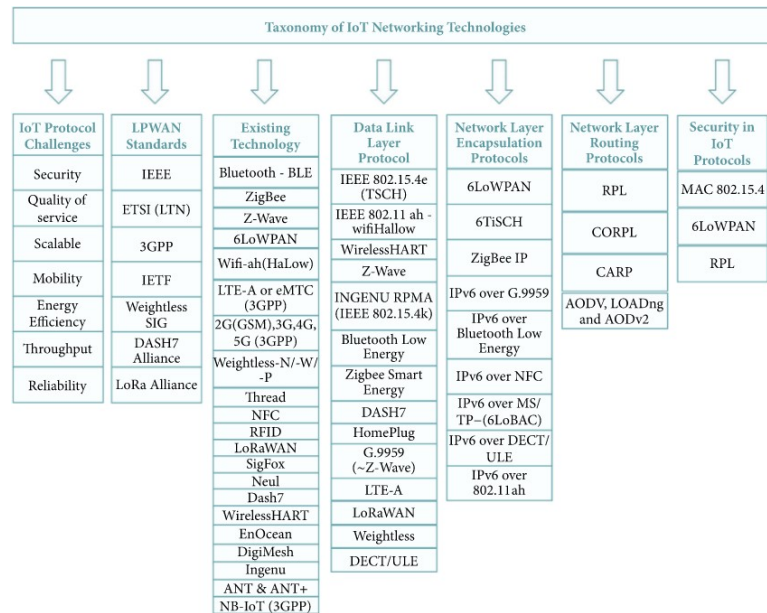


Figure 2.7: IoT Protocols

2.5 Architecture

In the literature, different tiers of IoT architecture have been proposed. While some reference frameworks do not consider the IoT management and security layer's capabilities, the tiers of IoT architecture mainly vary between two and five-tier. Standard organisations (ITU, IETF, ETSI, NIST) and industrial alliances such as OneM2M, Thread, and Open Connectivity Foundation (OCF) have continued to define IoT towards building a standard and interoperable IoT framework [156]. The development of IoT architecture is based on the TCP/IP protocol stack for digital communication. It is divided into five layers similar to the industrial IoT architecture explained in section 2.5 and shown in figure 2.8. However, researchers have different opinions on the layers of IoT architecture: three layers [41], four layers. See section 2.7 for the security details of some of the five IoT layers presented. An IoT project must consider whether the deployment environment is greenfield or brownfield [55].

The fundamental principle of industrial IoT architecture is the extension of [Machine-to-Machine \(M2M\)](#) design to the internet, making it more intelligent and open to the interconnectivity of other things. The core architecture of industrial IoT systems has specific security layers, each with specific security risks identified to originate from users, things to be connected, and the connection method [131]. In a comparative perspective, Mauro et al. believed that both object and user-driven security are important, but object-driven security is more difficult to achieve since user-driven security is of little benefit in object-driven security [157]. While Sadeghi et al. [64] think that Industrial IoT deployment will be dependent on security, others believe that data integrity and compatibility, Suresh et al. [131]; and policy concerns, Martonosi [158] are inclusive. The threats landscape of IoT devices falls within the remit of Open System Interconnection (OSI) reference architecture. However, a mix of the three- and four-layer IoT threat actors architecture can be adopted [159].

The architecture of industrial IoT shown in figure 2.8 has different levels of control processes and adopts a unified intelligent five-level architecture [123], [160] as applicable in most recent designs. It is the reference tool for connecting critical facilities (phys-

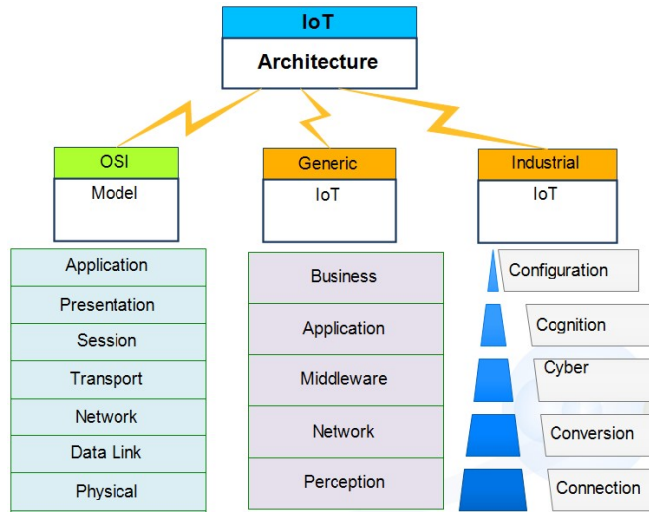


Figure 2.8: Comparison of OSI Model, Generic and Industrial IoT Architectures

ical devices) within the field network to the internet. The connection process creates inter-operational and security challenges due to the vertical and horizontal communication structures. Data transmission in industrial IoT consumes a reasonable amount of bandwidth, and the inadequacy of the required bandwidth causes packet retransmission, processing delay and noise. Edge computing is one way to save bandwidth and support short-latency applications. Interoperability and standardised are key architecture research problems [132] in IoT sectors like health [161], [152], [162], agriculture [105], [117], transportation [152] [163], and energy sectors [33], [164], [165], [166].

2.6 Industrial IoT Security

Security is one of the gaps that exist in industrial IoT systems. Most industrial IoT products are implemented based on market competitiveness [167], [55] to get hold of the market and increase return on investments rather than on building secured systems. Software and hardware are deployed from the research laboratory to real-life situations without proper testbed investigations. The testing, when carried out, is on a small scale [135], [136], [137] and cannot be extrapolated to the actual world scenario in capacity and performance. In [168], the **Industrial Internet Consortium (IIC)** is accelerating the global adoption of IIoT ecosystem by ensuring that features like “in-

teroperability, security, connectivity, business models, standards, architecture are firmly rooted in reality” in the approved industrial IoT testbeds. The IIC security committee report indicates that most designs initially lacked edge security implementation for Device-2-Device (D2D) and Device-2-Cloud (D2C) protection. In the Industrial Internet Security Framework (IISF) 2016 technical report, most of the security solutions claimed were not substantiated but are the same as the existing network and firewall security approach. However, the 25-member organisation is working to develop a common security framework for cyber-security in IIoT systems that will smoothly realise industrial 4.0.

Another good approach to tackling the security of industrial IoT is through modelling and validation of designs. In [139], Wan et al. proposed model-based designs (MDB) for handling cyber-attacks on CPS systems. The extended data flow diagram (xDFD) approach and attack tree-based model (ATBM) were said to have limitations on modelling and analysing the cyber domain. The innovative study on a car model used MATLAB/Simulink to investigate different security attacks (cybersecurity functions) and countermeasures on automation tools software (Amesim) before the system was built. The characterisation of the functional models made it possible to include cybersecurity functions and the future inclusion of a complex solution. The six attack models affected the electric vehicle export time: fuzzy, interruption, man-in-the-middle, replay, overflow, and down-sampling. Security cost metrics and a model that can capture both physical and cyber domain attacks are said to be a step toward improving this solution.

In [141], IIoT security is approached differently. The use of nanoscale electronic technology primitives such as memristors, carbon nanotubes and graphene improved IoT security. Merging nanoscale technology into IoT design introduces some security improvements, such as good authentication and secret key generation mechanisms, with cases of bits response rate error as the downside. However, such issues are known to be handled by error correction systems.

2.6.1 Security Requirements of Industrial IoT

The internet technology, which came to light in the late eighties and had significant improvement with the introduction of smart devices in mid-2007 is now projected to achieve a capacity of 50 billion nodes in 2020 [158]. The realisation of such a capacity will be made possible following the global deployment of IPv6 communication protocol. Industrial automation, remote process and monitoring control, telemetry, data management and protection are a few areas of IoT applications. “Industrial machinery, transportation monitoring, logistic tracking, asset tracking, healthcare, intelligent buildings, smart agriculture, and smart metering” are the use cases of IIoT [130]. IoT has generally improved beyond the level where only mobile devices and computers were linked to the internet [167]. Companies’ infrastructures and associated devices such as sensors, cars, cameras, drones, etc. are being added to the internet daily. This has brought a rapid increase in their number hitherto scaled to surpass 20 billion devices in 2020 [167], [169], [131], 30 billion, 10 billion [130] and 50 billion [170], [171], [56]. These varied assertions on the future capacity of industrial IoT can only indicate the need for good security taking into account the potential market value and complexity of the systems [64].

According to Pinto et al. [37], the cryptographic algorithms and security protocols such as microkernels, sandboxes, and virtualisations developed to tackle these security breaches were not able to stop these security attacks in industrial environments. As recommended by Pishva [108], adopting this new IoT technology is for companies to offset resource limitations. Security in the industrial domain is initially seen as safety (meaning, the protection of industrial workers and machines) [64], [37] when not associated with Information Technology. This means that developing a security solution for the industries now should be a convergence of OP and IT experts. Pishva [108] posited that the internet is now a dangerous platform for smart connected devices to obtain sensitive information. Security threats such as BadRabbit, WannaCry [172], Petya/Goldeneye spread worldwide in late 2017 [173], brought physical, financial and environmental damages to the affected companies. These threats, often grouped as cyber-attacks (external), malicious attacks (internal), and human errors and negligence

(internal) are always targeted at critical infrastructure such as offshore oil fields and power systems, to mention a few. Operational efficiency, safety, productivity, asset control, and reliability are generally compromised. The attacks usually focus on the industrial network router links and edge-generated data. Over time, their knowledge is used to gain business knowledge insight and behavioural patterns through deep machine learning techniques. Another phase of these security problems is the constrained nature of edge devices. Some do not have strong security features and are characterised by limited processing power.

The security requirements of industrial IoT are not limited to as categorised in the following literature [171], [130], [174] and [175]. The order of IoT security requirements is different from information technology (IT) systems. However, previous studies have adopted the IT requirements into the IoT security requirement. Pedro [176] implemented IoT security analysis and countermeasures adopting the confidentiality, integrity and availability (CIA) IT model. He argued that security requirements are objectively oriented, stating that other IoT requirements were not included. The following security requirements should be met to secure the industrial IoT system.

Confidentiality

The idea of confidentiality here is the restriction of access to data to only authorised devices and users. Confidentiality in [37] used a TrustZone strong spatial isolation mechanism to provide what is described as partial. TrustZone is a System-On-Chip (SoC) and CPU hardware-based system-wide security system for ARM microcontrollers. TrustZone architecture lacks channel security and resource access authentication leading to man-in-the-middle and channel attacks. Industrial IoT devices' data must be encrypted and accessible to only the desired recipient.

Integrity

This is to ensure that the machine configurations, software and data logs/updates are verifiable, remain unchanged, be in the correct format and are not compromised overtime at any point across the network. IoT integrity, as investigated in [37] could

only secure the system during the boot process. In the case of networked industrial equipment, [177] proposed a hybrid solution of TrustZone and security controllers (SC). The aim is to ensure that IoT nodes-to-node data is not tampered with by any malicious node injections.

Availability and Reliability

Making IoT part of a process control accommodates a very small amount of downtime. Access to any industrial IoT systems must be strictly limited to the authorised parties. The description of availability in [37] as high-level on the secured world part of the design was achieved by the asymmetric scheduling policy and interrupt sources adopted. Industrial IoT data must be available at all times irrespective of whether the system is compromised or not.

Mutual Authorisation and Authentication

Industrial IoT devices must have a reliable means of authorising and authenticating themselves in a network. [178] used network server key (NwKSKey) to authenticates two devices in a LoRa based IoT network. The devices in turns generates cryptographic keys based on security features received to validate each other. The method avoided malicious nodes from being added to the network. Also, entity authentication is necessary to maintain legitimate communication between entities and enforces non-repudiation.

Privacy

In [42], the privacy of user equipment (UE) participating in a group based communication managed by service network (SN) was achieved using UEs pseudonym. The existence of many SNs and devices mobility affected the performance of this scheme. A security system is needed to protect the backward and forward secrecy of new and existing devices participating in group communication. Key management according to [175] is a difficult research area without ideal solution and an important requirement for security mechanism in a networked devices communication.

Synchronisation

Time synchronisation plays important network management role for a two-way message exchange system. Harsh industrial environment and oscillator performance can drift the time speed estimation [179].

Latency and Jitter

Wireless communication is predicted by [132] to be the major medium of communication in the IoT network. The values are projected to reach 20 billion in 2023 with the introduction of 5G technology. IEEE 802.15.4 has been the protocol used to manage this compounding network. The delay associated with Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) makes it unsuitable for a protocol for IIoT. [132] identified the transport layer protocol as the layer where reliability and congestion control can be resolved to enhance security.

Interoperability

Interoperability is an essential feature in IoT development since it enhances the ease of integration of new IoT technologies with existing systems. IoT systems consists of very large heterogeneous new and existing systems, components, gateways, machines, applications and users. According to ETSI and 3GPP, interoperability in IoT context is the ability of two IoT systems or equipment from different manufacturer to interoperate, exchange data, use information or communicate using the same infrastructure or on another while roaming [180]. Interoperable heterogeneous IoT systems and components communicate and share information securely and seamlessly and categorised into technical, semantic, organisational, syntactical and platform. Standardisation will help achieve advanced interoperability between IoT devices and network protocols. The position of interoperability between IoT device and an industrial device by [132] is that it is not always feasible, and necessary especially when addressing issues of security and privacy.

Standardisation

Standardisation could scale the growth of IoT systems by bringing all the requirements of IoT applications to a reference basis. Among the strongest contributors to the standardisation of IoT is the ISO, IEEE, IEC, ITU-T, 3GPP, and ETSI [82]. software defined networks, cloud computing, wireless networks, and the transition to IPv6. The emergence of new industrial IoT systems without an internationally accepted standards is creating overlapping activities and affecting the deployment scenarios. Industrial standards are currently under study for proper integration. The devices, software, and networking systems must support the accepted security standards and cryptographic protocols. [83]

2.7 Security Layers in IoT Networks

The layers of industrial IoT system is the critical element of its security vulnerability. In [171], IoT security architecture is presented in a three-layered structure: application, network, and physical/Perception layer [181]. [56], and [175], divided the architecture into four layers. The processing layer so introduced supports the data storage and service management of the network and application layer with the main objective of intelligent and cloud computing. The security challenges such as malicious attacks and unauthorised access into the industrial facilities can be categorised based on the stages of industrial internet of things architecture and standardisation framework. A unified architecture is difficult to develop because approaches to IoT is different across various vertical industries. [171] identified hardware devices, software, communication network and the encryption scheme as the common sources of attacks. Also, a security survey analysed based on confidentiality, integrity and availability of industrial IoT network shows that different layers of the IoT models uses different security approaches and pose different security challenges. Industrial IoT attacks fall into element layer attack, network layer attack, service layer attack and application layer attack.

There are varieties of network attacks in recent times that has prompted the industries to consider security as a major concern. Most of the attacks take the forms of

denial of service attacks. A DDoS attack uses huge network generated traffic usually from edge devices to slow or eventually bring a network to a stop by exploiting the weakness in network communication protocols and within the devices. A major challenge is the computational capabilities of IoT devices when an improvement in their security features means more executable data files. The TrustZone technology introduced by ARM is an indication of how to improve security at the end devices [37]. To keep these devices operational for a long time considering the processing requirements, there is a need for an alternative security approach. The complex nature of the industrial IoT network will require securing the communication channels using strong encryption technology. Attention needs to be given to the nature of packets sent across the network, and the routers security. [37] focused on the end-to-end security of the end devices with a tradeoff on the real-time needs while recommending an alternative hardware-assistant security. The recommended security for industrial automation will be best realised using real-time cellular 4G/5G networks [132] which will be more expensive as a result of licensing of the frequency bands. Below is a list of three-layered attacks common in industrial IoT networks. The attack methods can be countered through appropriate security implementation. Man-in-the-middle threat, reply attack and eavesdropping are countered through the use of message authentication code mechanism, processing state machines and encryption respectively. Each layer of IoT architecture are vulnerable to various cyber attacks and are presented in detail in this section. In Service-Oriented Architecture, the security challenges can be attributed to the application, network, and physical layer. For IoT devices installed in public places, they have higher risks of being cloned, replaced or compromised through other physical attack mechanisms. The IoT security attack architecture presented is categorised into four:

2.7.1 Physical Layer

This is the most important part of the IoT network that must be protected from all forms of attacks. IoT devices are mostly made of various remotely interconnected nodes. In the physical layer attack, when the attacker exploits a vulnerable node to extract security information, the result is catastrophic and can lead to a total failure of

the network. All forms of physical security are associated with IoT users. An overload attack is another type of physical layer attack on an IoT device that decreases the strength of an IoT network. One of the ways to provide a solution to the attacks at this layer is by fixing strong physical layer security such as tamper proof, physical barriers, etc. Physical Unclonable Function (PUF) is a physical layer security that provides IoT devices with fingerprint identification [57].

2.7.2 Perception Layer

The perception layer comprises of various sensors that are responsible for the collection of data from the external world through wireless sensor networks such as ZigBee, Infra-red, RFID, Wi-Fi, etc. Perception layer attacks are focused on data manipulation and device destruction since little or no security exists on the sensors where interconnectivity, energy consumption and communication range is handled. The devices communicating either directly or indirectly needs a unique identity within the network. The identity can be provided by the device system-on-chip or by a secondary chip. Security attacks that could occur at this level are hardware focused as presented below. The security solution to mitigate this kind of attack is to provide a reliable means of authenticating each node and further implement node to node authentication. Achieving this may be limited in existing IoT devices but possible only in nodes powerful enough to support parallel processing.

- **Node Tampering** - Illegally making total or partial changes to a sensor node in order to have access to devices data, security and routing information. A successful node capture attack will result to malicious node replication using copy of legitimate network security parameters. Malicious code detection schemes can be deployed in a network of nodes in an attempt to control data flow and detect malicious nodes.
- **Social Engineering** - Users of IoT also constitute nodes. When their actions are compromised, private information will be given out and they can also perform tasks that would affect the overall system performance.

- **RF Interference on RFIDs** - Wireless networks are vulnerable and can be eavesdropped or jammed by malicious devices. In this situation, electrically generated noise is used to hinder the devices communication fidelity. It is a form of Denial of Service (DoS) attack over radio frequency signal that could be prevented using noise and frequency filtering/cancellation schemes [182].
- **Physical Damage** - Having physical access to the device is the greatest of the attack impacting the availability of service. The location where IoT devices is installed must be properly protected from direct adversary from damaging the device. Direct contact with the device will lead to other forms of attacks like reverse engineering. The encryption key of WSN has been successfully obtained through this approach [147].

2.7.3 Network Layer

This is the second most type of attack as it involves transmitting IoT data via the internet. The attacker is usually miles away from the target system relying on the knowledge of routing and security protocols for exploits that could make the network resources unavailable. The main security threat in the network layer consists of routing attacks such as malicious behaviour against right path topology and forwarding data, Distributed Denial of Service (DDoS), cyber-attacks across a heterogeneous network, asynchronous attacks, collusion attacks and the man-in-the-middle attacks [181]. Another type of attack is when a malicious node tries to drain network resources. Other attacks include node impersonation attack and it happens when a malicious node tries to gain access to a network in the guise of a genuine node. Spoofing attack; this type of attack occurs when an attacker tries to gain access to a device by pretending to be someone else. Replay Attacks; the attacker captures network data and replays it on the network to slow down the network operation. These types of attacks can be stopped by restricting traffic on each network node.

- **DoS Attacks** - Is a common malicious way of overrunning the available network resources by flooding the network with unprecedented traffic volume by attack

schemes such as TearDrop, UDP Flood, etc. DOS attack impact could result to service outage

- **Traffic Analysis Attacks** - Occurs when packets sent across a wireless network of any sort are scanned for confidential information using spoofing, address cloning, port scanning, addressing tracing, packet sniffing applications. Confidential data could be sniffed out by an attacker with a high knowledge of data traffic analysis.
- **Node Attacks** - Packets are intercepted along the traffic and lured into a metaphorical sinkhole thereby denying all the services through packet loss. The privacy of the node is also compromised when access to the network is eavesdropped and controlled. Through bombardment of the communication traffic with higher than the available resource, services will also be denied.
- **Routing Information Attack** - This attack manipulates the routing information table to creation routing loops that has the capabilities to reduces and/or increases the routing length. This will cause network congestion, packets loss and aid other related network attacks but can be mitigated using secure routing algorithms to protect IoT device identity and their communication paths.
- **Man in the Middle Attacks** - Malicious node located between two benign IoT devices could violate their CIA by compromising their communication link, eavesdrop to steal their identify, intercept and tamper with the data, and control the communication between the IoT devices. The use of secure communication and key agreement protocols prevents man in the middle attacks.
- **Sybil Attack** - Sybil node impersonates and behaves like a multitude of nodes in IoT network. This means that legitimate nodes could be fed with wrong traffic information from Sybil nodes and could result to DoS and network jamming. Authenticating and identifying every IoT devices in a network using lightweight and strong authentication protocols can mitigate against Sybil attacks.
- **Other Attacks** on this layer include session attack and Denial of Access (DOA)

attacks. These attacks can be stopped by using security tools to detect malicious codes, such security tool can be an antivirus. The security tools performs two major roles; to confirm that information is sent by an authenticated user/device and protected from threats and to send information to the network layer through wireless or wired technology [183]. The verification of the user and the information can be done in various ways, like the method of authentication which is implemented by using secret keys and passwords.

2.7.4 Application Layer

The application layer is responsible for handling user data, management processes, control, visualisation, and other services requested by users. An attack on the application layer targets the user confidential information by compromising web-based applications. Complex DDoS attacks like HTTP floods, and brute force are used to steal, destroy, share or modify user data. Inadequate passwords and key agreement could allow successful attacks that is likely to destroy privacy at the application layer. The software is the primary source of the attack in the industrial IoT system. Malicious software is used to steal confidential information, stop systems operation and even rewrite the operational instructions. The following challenges are common in the application layer.

- **Phishing Attacks** compromises the confidential data of IoT devices and users by analysing files (spoofing) containing confidential information of the devices and users. To overcome phishing attacks, the implementation of IoT devices and users must incorporate some level of intelligence through secure authentication access, smart identification and authorisation. This may be easier to achieve through users training than in constrained IoT devices.
- **Malicious Software Attack** includes the use of worms, trojan horses, spywares, and viruses to infect industrial IoT system. Through malicious activities, a successful attack could leads to access to private data, data tampering, data decryption and a possible DoS. Introducing NGFW-G and other intrusion detection systems will protect IoT network from malicious virus.

- **Side Channel Attack** extracts security details through physical parameters such as time stamp, power level, fault detection, and electromagnetic analysis techniques to retrieve the encryption key from IoT device [184]. The assumption of the knowledge of the plaintext and the hypertext help to retrieve the encryption key.

2.8 Countermeasure Opportunities

There are opportunities as well as challenges of interconnecting IoT devices of both Information Technology (IT) and Operational Technology (OT) settings also regarded in this thesis as consumer and industrial domains. Integrating IT and OT networks introduce security risks across each domain's interfaces. Existing OT legacy firewalls and gateways lack the security capabilities to protect the OT domain from IT-related threats actors given the trends of changing network architecture and the emergence of new security risks. IoT deployment can be inhibited by various deployment requirements classified into the node, link, path, and global problems [185]. The communication of dedicated physical devices in its simplest form is referred to as Device-2-Device (D2D) group communication. D2D security in Group-Based IoT Communication are originally designed to facilitate autonomous communication between IoT devices without cellular infrastructure other than the ISM band [186]. Limiting their use to Near Field Communications (NFC), Bluetooth and Wifi-Direct. Studies have shown that perception of D2D by the cellular network providers is changing with the coming of IoT. LTE resources are currently used by the cellular network providers to deliver and improve heterogeneous communications and services of IoT network. NB-IoT is recommended in the 3GPP release 12, 13, and 14 as the protocol of choice. KrishnaKanth and Sapna opined that IoT is more than machine to machine communication with challenges of security and privacy, robustness, big data and architecture as informed areas of study [107]. The growing number of IoT devices creates group security key and membership management problem that affect both the internal (group members) and external (non-group members) hence, constituting a problem of active internal

and external attacks. Given the real-time and reliability requirements of such systems, Time Division Multiple Access (TDMA) protocol such as IEEE802.15.4e based on Medium Access Control (MAC) layer will be key to solving such problems [187]. A security measure based on the time synchronisation of the group of connected sensors and their identity in the network. The effects of multiple protocols in the node and sensor mobility model can be analysed [28].

Deployment requirements can also be based on the hardware, networking and software perspective. Nodes have problems of energy depletion which at a certain level causes random behaviour. Such poor performance affects the functionality of other sensors within the system. The networking problems are mainly due to link type (symmetric or asymmetric), scheduling mechanism and energy utilisation. This is a big challenge in networks where different sensor data rate is occasionally sent to a lower data-carrying communication link. Link failure means that a greater part of the network will be cut off and data sets will be lost. This creates a network congestion problem within the MAC protocol layer. The software errors such as watchdog timers, buffer overflow, incorrect patch download often result in node reboot, wrong readings, and non-packet forwarding. The countermeasure opportunities for managing these risks include:

2.8.1 Next-Generation Firewall and Gateway

Next-Generation Firewalls and Gateways (NGFW-Gs) enables the protection of both legacy OT and emerging IT networks from advanced cybersecurity attacks based on premediated rules in implementing the security capabilities. NGFW-G are intermediate hardware, software, and data-driven security approach for logical and physical, IT and OT network segmentation with a higher level of intelligence. Its consideration in future hybrid networks should enforce access control, data encryption and management, system whitelisting, malware protection, patch update and management, and authorising communication from shielded IoT devices.

2.8.2 Next-Generation Virtual Private Network

Virtual Private Network (VPNs) provide encrypted connection tunnel for IoT devices that are in separate locations as a layer of security for data exchanged. A VPN connection can be encrypted using industrial-grade security protocols such as OpenVPN, Transport layer Security (TLS), WireGuard, Internet Protocol Security (IPSec), and strong cryptographic primitives. The disadvantage of applying VPN in OT network is the need for other software and support infrastructure that are not part of OT operating systems.

2.8.3 Defense-in-Depth Security Architecture

Implementing Defense-in-Depth (DiD) security approach with NGFW-G and Demilitarised Zone (DMZ) overcomes many security failures common in OT networks by providing multiple security layers. The many security layers introduce resilience for increased threats vectors detection. However, unified security models have the advantage of centralising the roles of network management and reducing the security hardware footprints across the network boundaries. DMZ will allow hybrid IT and OT networks to be decomposed into smaller network segments with each having NGFW-G. This offers more security visibility and effective in differentiating between cyber threats and system error as IT network security are limited in threat detection in OT networks.

2.8.4 Encryption Techniques

Various cryptographic algorithms have been proposed to solve the emerging cases of attacks on critical infrastructure. Cryptography security algorithms in the form of a private key (symmetric) and public-key (asymmetric) are the most commonly used security techniques [188]. Cryptography in this context is the methods of protecting user/device data from unauthorised access. This is realised using the original data generated by the device, encrypted to protect the data readability/decrypted to recover the original data and cipher text which is the recovered data [91]. The security levels of the encryption algorithm are dependent on the size of the cypher key used. From the review

of various crypto combinations, One-Time Password (OTP) and RSA, AES and RSA, AES and Fully Homomorphic Encryption (FHE), AES and Secure Hash Algorithm (SHA-2), OTP and Transposition Technique, Columnar cipher and vigenere cipher, and RSA and Triple DES have been implemented. Comparing the security requirement of AES, ARC4, Hash Message Authentication Code (HMAC), RNG, RSA, ECC security schemes at the code level in the SensorTile module (STEVAL-STLCX01V1) for industrial application, a stronger security system with increased speed of encryption and decryption and digitally signed keys were the observed advantages.

2.8.5 Key Management

Certificate Authority (CA) based Key Management System (KMS) function on the principles of cryptographic schemes in distributed automation networks [189]. KMS is responsible for registering and certifying Access Points (APs) and smart sensors and also manage their connection within trusted networks as shown in figure 2.9. The AP confirms the identity of smart sensors and issues them with a group key. The sensors termed smart should have the capabilities of aggregating datasets, manage power by switching between different power saving modes, and advertises routing information periodically. The roles of system initialisation, issuance of certification to initialised sensors, sensor's pseudonyms and private key generation, mutual authentication, secure group key distribution and key update resides at CA.

The problem of industrial IoT devices engaging in group communication is the management of key agreement protocol. Diffie-Hellman based security establishment protocols are useful in two-node active attack protection systems [42]. Studies requiring multiple nodes of active sensors message exchange invalidates the use of only Diffie-Hellman protocol as an attack protection protocol. The use of a pre-distribution key will also fail as more than two sensors will have the probability of choosing the same number of keys as the number of devices in the network grows resulting from an inextricable interconnectedness of the devices [169]. In end-to-end encryption, asymmetric cryptography is employed. The problem associate with the use of encryption in a multi-tenant network environment is multiple encryptions that lead to increased

data retransmission between the interconnected IoT devices, data traffic congestion and increased power consumption [29]. This makes this security method not suitable for constrained industrial IoT. Where the IoT devices can withstand the key computing requirements due to the availability of a constant power source or increased memory and computational resources, the key management system as illustrated in figure 2.9 allows secured communication between IoT device A and B with signed public and private keys.

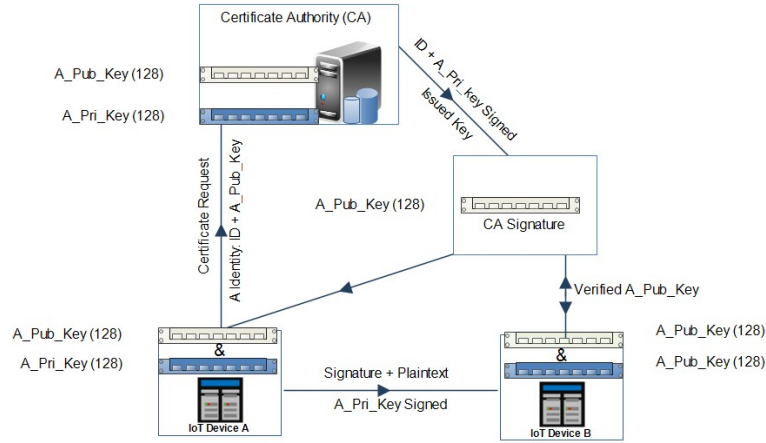


Figure 2.9: Certificate Authority Based Key Management System

For the security key size and cryptoperiod, the majority of IoT devices investigated in this thesis, see section table 4.2 of IoT devices used for the NB-IoT and RTUs in chapter 6 and 7 support 128 bits of all types of encryption and may not be able to secure IoT devices against brute-force attacks from higher computing power devices handling longer key sizes before their lifetime. Meeting the NIST security recommendation of between 1 to 3 years for using the same key of any key types (cryptoperiod) in LPWAN, makes it practically impossible to manually apply key updates in all the LoRaWAN and NB-IoT IoT devices deployed without remote update support feature. The security strength of 128 will, however, remain acceptable until 2031 [190]. The expected lifetime of most LPWAN IoT devices is 10 years [191].

2.9 Cyber Security Considerations

Many cyber security recommendations for network scenarios discussed in sections 6 and 7 are needed. Procedures such as categorising access authorisation and restriction for a specific group of IT devices to OT networks by incorporating active directory-based policy, whitelisting, and blacklisting. This can reduce the extra complexity of implementing deep packet inspection as one layer of security protection is inadequate in hybrid IT and OT networks. Next-generation firewall and gateway functionalities could be enriched with system-wide threat and vulnerability detection, anomaly detection, process and zone classification, asset discovery, and data collection. Unidirectional gateways and firewalls are most suitable for performing malware protection, intrusion prevention, and application intelligence and control in OT networks. A hybrid IT and OT network should never be administered from less-secured IoT devices and networks. All external and non-authenticated internal access should be classified as unsecured based on zero trust principles since they are the easiest path to compromising networks. OT and IT networks should incorporate security by design, lightweight encryption, and zero-trust architecture.

Industrial and generic IoT networks have existed in separate spheres with different network and security requirements, but modern OT systems are incorporating IT system's capabilities. This implies that in such network scenarios, certain IT devices are used in OT networks while still connected to the IT network. NGFW-G are required to provide fine-grained security and application policies across organisational boundaries. Implementing defence-in-depth strategies will also help to detect and respond to intrusions for both internal and external security risks.

2.10 Internet of Smart Grid (IoSG)

2.11 Introduction

The smart grid is an electric power system that integrates modern information and communication technology into the power network infrastructure to improve operational

performance—in a simpler term, improving the existing power systems by making them smarter. The demand for communication integration and cyber security compliance in the utility networks has increased as the power system distribution network becomes more flexible and smarter through the introduction of IoT enabling technology to the smart grid. Such an evolutionary change referred to in this thesis as the Internet of Smart Grid (**IoSG**) has brought an increase in the number of Intelligent Electronic Devices (**IEDs**) being used for digital connectivity, automation, control and remote monitoring of utility assets safely and cost-effectively. Device and network failures could easily be detected and mitigated through security and protection systems. For the smart grid to perform its protection and control, power measurements, asset monitoring, teleprotection, and voltage regulation functions, it relies on various communication technology to connect the distributed utility assets and control centres. Various communication technologies such as wired: Power Line Communication (**PLC**), fiber optics, Asymmetric Digital Subscriber Line (**ADSL**) and wireless: WiFi, mesh networks, microwave networks, UHF telemetry, cellular technologies (GSM, 3G, 4G/LTE, NB-IoT, 5G), and satellite communications have been proposed in power utilities to make it smarter [166]. The Distributed Network Operators (DNOs) mainly rely on combining more than three of these communication technologies for various grid applications and connectivity. Each technology of choice has advantages and disadvantages in cost, security, scalability, energy utilisation, complexity and reliability.

Smart grid communication technology will be the focus of this section as a use case and also the background into the technical chapters (6 and 7) of the studies conducted in collaboration with PNDC industrial partners (Cisco, SPEN, ABB) and the UK spectrum regulator (Ofcom) specifically to estimate the necessary long-term bandwidth and security needs of meeting the DNOs requirements to deploy both Ethernet and Private Radio Access Technology (**PRAT**) in power utility networks. Figure 6.2 is a high-level representation of the existing testbed at the University of Strathclyde Power Networks Demonstration Center (**PNDC**) used for these studies while figure 6.3 is the test scenario on which the experiment was conducted via Ethernet and figures 7.3 and 7.4 via radio technology. The reliability of such network operation is determined

by the type of Radio Access (RA), communication systems and the capabilities of IoT devices deployed. The overall aim is, therefore, to:

- Highlight the importance of dedicated spectrum for power utility and discuss the bandwidth implication of implementing IEC 62351 over Radio Access (RA) and Ethernet technology.
- Determine the frequency bandwidth for effective monitoring and controlling of secondary substation assets in rural and urban locations and the need for compliance with the cyber security standard IEC 62351.
- Ensure that the IoSG is secure using security protocols such as the Transport Layer Security (TLS), Internet Protocol (IP) Security (IPsec) and other certificate and authentication mechanisms.
- Discuss methods of improving the reliability of power utility systems and saving operational and maintenance costs.
- The study's findings and recommendations will guide the power utility companies when requesting bandwidth from regulators like Ofcom in the UK and when making inputs towards the development of smart grid data models.
- To bring to fore the need for dedicated spectrum for power utilities
- Analyse 5G communication requirements based on smart grid critical teleprotection category 1 application.

2.12 A Review of Smart Grid Telecommunication Technologies

Communications technologies are vital elements of a smart grid and can be categorised into wired and wireless technologies. Traditionally, power networks are designed based on SCADA systems to support only unidirectional power flow, i.e. from generation to consumers with efficiency and integration challenges [192], [193]. A modern smart

grid system now requires a data acquisition system that is able to provide bidirectional real-time communication between sensors/actuators and the data centre via Home Area Network (HAN), Neighborhood Area Network (NAN) or Wide Area Network (WAN). Communication between smart grid devices such as RTU for monitoring and control in a substation relies on the efficiency and reliability of both OT and IT infrastructure from generation point down to the consumers. In this section, the reader is introduced to the concept and components of a smart grid and the communication technology for connecting the infrastructure. A reliable, secure, and bandwidth-efficient transmission of real-time data collected from IoT devices can rely on wired technologies such as Digital Subscriber Line (DSL) [194] and others described in subsection ?? or wireless technologies such as ZigBee, cellular networks or WiMAX.

2.13 Wireless Technology in Smart Grid

Communication technology makes data exchange between the smart grid control centre and the field devices possible. As shown in figure 2.10, the capacity and reliability of the network in performing sensing and control function is increased by integrating modern communication technologies. It also allows power network engineers to manage these grid IoT devices remotely. The vendor diversity in smart grid IoT devices, the topology of the power networks, and the locations of the distributed field devices create several challenges in selecting suitable communications networks by the DNOs to enable such connectivity. Similarly, in secondary substations' automation, where many field devices are located in hard-to-reach areas, a reliable communication solution is needed to connect field assets to the control centre. DNOs have been in operation for several decades, providing people and businesses with a reliable power supply. Power outages and network failures cause significant damages and disruptions to the economy and our daily life. For that reason, there is an important requirement to make the current electricity network smarter in terms of reliability, efficiency, cost-effectiveness and security. This could be done utilising the smart grid, where a two-way flow of power and data is widely deployed in the distribution networks.

Deploying any wireless technology to enable such connectivity will need, among others, a proper spectrum allocation considering emerging applications because additional connected devices will require more bandwidth. However, a dedicated wireless network is considered more appropriate for on-demand changes or improvement in power system utility management. This will ensure secure communication and better service quality because of changes in the existing infrastructure due to capacity expansion, digitisation, network redesign, deployment and management of cyber-related functions. Narrowband Internet of Things discussed in 3.3, and chapter 4 offers reliable and secure communication for non-critical smart grid applications like smart metering. Due to its efficient power, high capacity, wide-coverage, and features that are difficult to achieve by the unlicensed LPWAN technologies, NB-IoT is regarded as a smart choice for the smart grid [166], perfectly satisfies the scalability, security and reliability requirements in AMI, Vehicle-to-Grid (V2G), Grid-to-Vehicle (G2V), and Demand Response Management (DRM).

Moreover, as smart grid infrastructure are transitioned into the IP world, the possibility of a cyber-attack that could target the power network will increase. Therefore, cyber security should be considered in any communication system for the power utility. This will also further increase the bandwidth and demand for more spectrum. In typical TCP/IP based Information Technology (IT) networks, overhead attributed to implementing these technologies are major concerns as a result of bandwidth limitations. In addition, implementing the power system security standards using these wireless technologies will scale the bandwidth required by a high margin. Spectrum is the core element of wireless solutions for the smart grid, and the power utility companies desire a secure and cost-effective wireless communication protocol that can be integrated into their legacy power system for efficient secondary substation monitoring and control.

The following limitations apply to wireless technology used in smart grid:

- Smart grid requires continuous availability of cellular communications with guaranteed services, which may not be possible due to network congestion from applications servicing many customers or natural disasters such as wind storms [195]. Shared network resource reduces network performance and will affect services

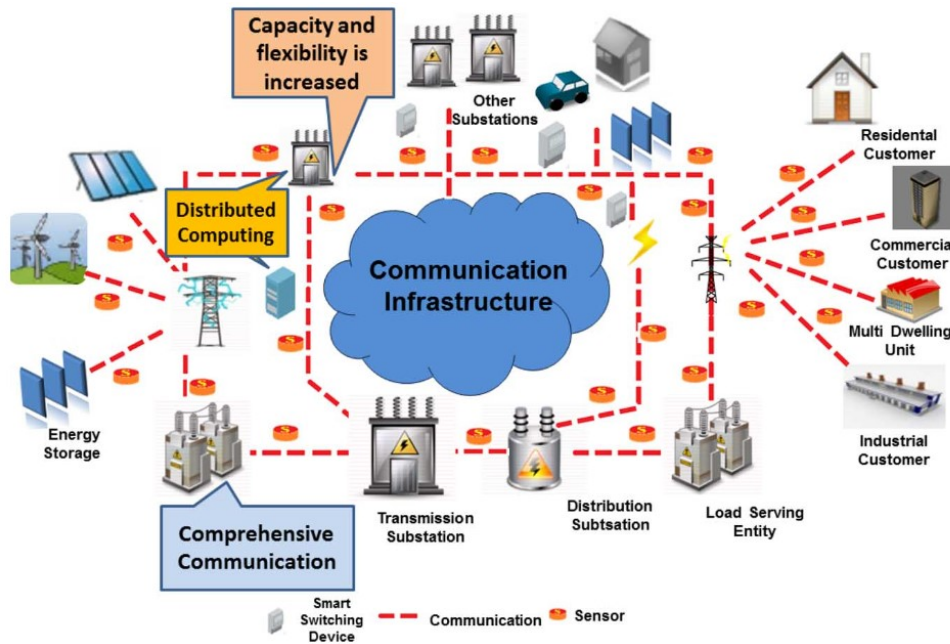


Figure 2.10: Smart Grid Architecture [4]

such as teleprotection. 5G beamforming and network slicing capabilities could prevent the DNOs from building private communication networks.

- Cellular communication channels for smart grid are narrowband and limited. In the UK, a limited bandwidth between 420 MHz (UHF 1) - 470 MHz (UHF 2) frequency bands is used by the DNOs. The UHF scanning telemetry uses an available spectrum band of 1 MHz, which comprises 80 channels of 12.5 kHz. Such limited bandwidth with its narrow channels will limit the number of connected outstations; also, it will not be sufficient to be used for the increasing demands for the smart grid (voice and secure data) traffic. Additional bandwidth is required to implement cyber security specifications. The license-free communication technologies such as ZigBee and LoRaWAN have processing, memory, latency, and interference implementation constraints and requires additional techniques to improve a specific part of the network performance [196].
- Difficult terrain affects the reach of wireless technologies. Systems integration, multi-drop communication channels, and noise are also considered.

- When a smart grid network is supported with wireless mesh where IoT nodes can join a network group where each node acts as an independent router, the network will experience high interference and loss in capacity and signal quality. The fact that data is routed via many access points managed by a third-party provider, data overhead will increase in addition to any security techniques that are applied to prevent packet sniffing as it travels around the network loop [4].
- In the case of PLC and DSL, they do not support bandwidth flexibility and are affected by the characteristics of the power line itself, such as distance between the devices and their number [196]. Their reliability may not meet the requirements for all critical applications such as teleprotection. They are expensive to maintain and not suitable for wide range deployment.

2.13.1 Requirements of Wireless Technology in Smart Grid

Understanding the communication network requirements for smart grid applications is not only essential for its performance but useful to the utility engineers for network design and maintenance operations. The wireless network requirements for smart grid include but are not limited to the grid's ability to accommodate long-term security needs, meet the demands for substation assets monitoring and control, and support remote access capabilities. The bandwidth measurement that translates to spectrum management will be achieved with accurate information on the number of devices connected to the secondary substations, the type of service rendered in each grid entity, network topology implemented, and the location of the devices, among others. The additional overhead in each service layer of the chosen protocol due to implementations of standards such as IEC 62351 (cyber security standard for smart grid networks) will affect the average network rate of data transmission. Other emerging services within the power network (such as charging points and battery storage systems) and services (such as data re-transmission and handling of black start scenarios) must also be accounted for in any bandwidth estimation process.

The Distribution Network Operators (DNOs) have employed the services of Mobile Network Operators (MNOs) over the years to meet their communication needs.

Requirements that involve economically providing different QoS to enhance the grid's reliability [197]. It is an expensive option, and the DNOs will have to accept the cost per byte of data per month as determined by the MNO's pricing on each carrier used for service delivery. The carrier, in most cases, does not support a complete security suite that will prevent incidences of security breaches that could lead to service outages. However, there are various recommendation strategies by the DNOs to upgrade the security and management suites for different Remote Terminal Units (RTUs), IEDs, Private Network Service (PNS) and including satellite communication systems. Generally, adding any security feature to the grid would increase the data overhead, but the additional cost of disruption and technical failure arising from such improvement on the power network cannot be overemphasised.

A communication system that is secure, resilient, reliable, and efficient is what is needed in an emerging smart grid network that is centrally automated and remotely controlled. This is due to the quick growth of intelligent IoT devices used in smart grid networks, increasing the demand for more spectrum. The analysis of bandwidth capacity of the dedicated wireless network shown in figure 6.2 is explained in subsection 6.5. However, deploying wireless communication systems within the power networks improves reliability when there is an accessible licensed radio spectrum to make the deployment possible. The unlicensed spectrum could be considered an option, but the data packet limitation, latency, and interferences make it unsuitable for real-time applications. Also, the unlicensed spectrum is not secure, and the quality of service it provides is far less than the non-critical grid application requirements. For teleprotection application requirements, this study will identify if the current recommended 1.4 MHz or the 2x3MHz spectrum for power utilities satisfy current and future smart grid requirements even when the IEC 62351 traffic overheads are considered. One of the consequences of the overhead is that the data transmission rate of the grid entities will depend on the magnitude of the allocated spectrum.

2.14 Smart Grid Communication Protocols

Power system communication protocols have evolved from the likes of legacy SCADA systems such as Modbus, DNP3 etc., industrial protocols to the current International Electrotechnical Commission (IEC) and communication standards, revolutionised by the emergence of the Internet of Things (IoT) and radio-based smart grid networks [198]. Safety, reliability, and security are the communication protocol's characteristics to ensure that the grid operates efficiently. Cellular technologies are a few of the communication standards that are high on demand today by the power utilities to establish reliable connections across their infrastructure and facilitate the transfer of data between the control centre and the secondary substations IEDs performing control, monitoring, metering or protection functions. The lack of coverage for these communication technologies in the hard to reach locations is influencing research in radio access technology. The practical implementation of these new protocols come with a wide range of technical challenges unique to power networks. Implementing security in bandwidth-limited protocols will require extra bandwidth that translates to an extra cost per data sent across the network. The commonly used smart grid protocols are described in detail in this section of the thesis, with the findings on IEC 62351-3 constituting a major part.

Supervisory Control and Data Acquisition (SCADA) system protocol is specified in the IEC TC57 WG15 standardisation to deliver data communication over serial links and networks in RTUs, IEDs, and Programmable Logic Controller (PLCs) [199]. SCADA systems are vulnerable to both the internal and external attacks targeted at specific components of the grid network because SCADA systems cannot support the current power system cyber security needs [200] since they are lacking in the application and data link layer security to prevent attacks like side channel [193] and DoS on Phase Measurement Units (PMU). Interestingly, little research has been done on smart grid power network security focusing on SCADA systems over DNP3 [201]. As an unreliable communication media, integrating IoT resources into smart grid systems requires implementing new security mechanisms. The increasing integration of IoT devices such as smart meters that are not equipped with enough processing and storage

into industrial IoT has put stringent network QoS, security, scalability on modern SCADA systems. This shows a clear need for new security techniques to facilitate the integration of IoT into SCADA-based smart grid protocols described below, especially when they are unable to perform the security authentication and encryption functions.

2.14.1 Modbus

Modbus is an application layer protocol developed in 1978 [202] by Modicon [203] to deliver asynchronous serial communication between isolated industrial programmable controllers such as smart meters, RTU, and Distributed Control System (DCS) in a master-slave scenario [204]. It employs a request/reply mechanism over a message containing an Application Data Unit (PDU) and a Protocol Data Unit (PDU) between industrial devices and/or control centres. The communication over Modbus-TCP is usually of two types: Single frame or broadcast frame messages (device address, command, and data) embedded into a TCP frame. In the Modbus-Serial transmission mode, messages are routed between master and slave devices via serial lines. Modbus is not a secure industrial protocol and is vulnerable to man-in-the-middle, replay, and DoS [205] and the attack instances include interception, interruption, fabrication, and modification [202]. Through IoT gateway design that encapsulates packets between the IoT physical and network layers, Modbus data can be secure in legacy SCADA systems. It also extends the Modbus network's connectivity to different IoT platforms where data processing and analysis could be enhanced. The TCP/IP network introduces authentication capabilities between the masters and slave equipment. Sending data from a Modbus network to other networks has to be done with external security provisions because it is not designed with adequate security mechanisms fit for purpose against modern day security breaches [206]. Efforts to implement Modbus over TCP/IP began in 1999, and an examples of existing ModBus security mechanism is port scanning done to discover rogue Modbus devices [207] when migrating data to the edge and the cloud [203].

2.14.2 Distributed Network Protocol Version 3

The Distributed Network Protocol Version 3 (DNP3) was initially developed for Supervisory Control and Data Acquisition (SCADA) systems by General Electric [5]. Since the release of its technical specification in 1990, it has widely supported SCADA systems reliably, robustly, and efficiently [208]. DNP3 protocol was not designed to operate in an Internet environment [201] and has primarily been used for data communication across the industrial networks. Recent communication network design allows DNP3 over TCP/IP layer for end-to-end communication. DNP3 layers can be modified to introduce an additional security layer between DNP3 and TCP/IP protocol stack as shown in figure 2.11 since it lacks authentication and encryption. This process adopts protocol translation between legacy SCADA systems and smart grid and prevents any technical changes to the SCADA devices. The physical layer carries the measured data using media such as RS-232, radio technology, fibre, and copper. The data link layer packages the data into the required format by implementing redundancy checks and adding the link header. The transport layer determines data payload fragmentation and link capacity. The actual control or other functions to be performed between the master station and remote substation devices is done at the application layer. Securing DNP3 and IEC 61850 with IEC 62351 enhances the security of both SCADA protocols for power grid communication systems. It also offers a secure authentication security extension in IEEE 1815-20 DNP3 standard [209] that allows master and substation devices to be correctly identified during an authentication process, maintain the integrity of the data, and prevent any attack that would violate the confidentiality of the communication. In summary, DNP3 with secure authentication addresses spoofing, modification and replay attacks that would emanate from IoT integration into smart grid [210].

DNP3	IEC1850/IEC 62351	
Application Layer	Application Layer	
Encryption and Authentication	Encryption and Authentication	
TCP/IP Layer	TCP/IP Layer	TLS
	Authentication	
MAC Layer	MAC Layer	
Physical Layer	Physical Layer	

Figure 2.11: DNP3 and IEC6180 with IEC2352 [5]

2.14.3 IEC Standards Protocols

IEC 61850

The International Electrotechnical Commission (IEC) introduced the IEC 61850 standardisation to improve substation's automation process that is impracticable with legacy approaches like realising Ethernet-based communication for digital substations [211]. The versions of this standard applicable to the smart grid include the IEEE 1588 v2, IEC 61869 and IEC 62439-3 with different profiles, parts, editions and revisions [212]. Implementing the standards requires replacing physical wiring in the legacy power network with digital communication networks to facilitate protection and control. The features of IEC 61850 unique to these objectives include the ability to virtualise logical devices and nodes, define substation and device requirements using standard configurable language [213]. The installation cost of IEC 61850 is low since the additional cost for transducers and wirings will not be needed since a single merging unit can enable Generic Object-Oriented Substation Event (GOOSE), Generic Substation Event (GSE) and Sampled value (SMV) services to more than one device. These measurements and control signal protocols lack security recommendations that other IEC standards have provided.

IEC 62443

IEC-based industrial network security is of paramount importance in ensuring confidentiality, integrity protection, and authentication of control messages in critical utilities since it has suffered cyber-attacks. Following from the National Institute of Standards and Technology (NIST) best security practices, cyber security vulnerabilities in OT environment could originate from the operation, technical or human errors. The ISA/IEC 62443 security standard is developed to address existing and future security challenges for Industrial Automation Control Systems (IACS) like the implementation of concepts such as defense-in-depth. IEC 62443 have different parts that dictate what security model that is suitable and where it should be applied to reduce the impact of cyber attack across digital substations [58]. For instance, defence-in-depth where multiple security layers of protection are introduced is suitable for critical applications. The protection mechanisms can be categorised into many forms and achieved through network segmentation, trust zoning, demilitarised zone, [214].

IEC 62351

IEC 62351 is a new industrial security standard designed to provide integrity protection, authenticity, confidentiality, non-repudiation, and message level authentication to evolving power network protocols, including the ISO/IEC 61850, 60870, and DNP3 [5]. It provides adequate mutual authentication and encryption above the TCP/IP layer and over the transport security layer (TLS) protocol. It specifies the security requirements to address role-based access control, key management, and end-to-end encryption issues. The implementation of this standard alone does not guarantee security. The specifications of the standard comprise of ten different parts of the standard, each addressing different telecontrol equipment and systems application-layer authentication issues like spoofing, modification, replay and non-repudiation [215]. For instance, as shown in figure 2.12, the IEC 62351-3 standards provide a specification for security overhead for SCADA and TCP/IP protocols from the transport layer down to the physical layers of the OSI model in substation RTU. Other issues include the long connection duration, which is often permanent and require special means of updating

session keys, session re-negotiation and interoperability of different cipher suites and multiple applications supporting different bands. Additional overhead is introduced from issuing and distributing certificates, especially when short-lived key certificates are discouraged. IEC 62351-9 recommends using X.509 certificates for TLS based on public asymmetric keys.

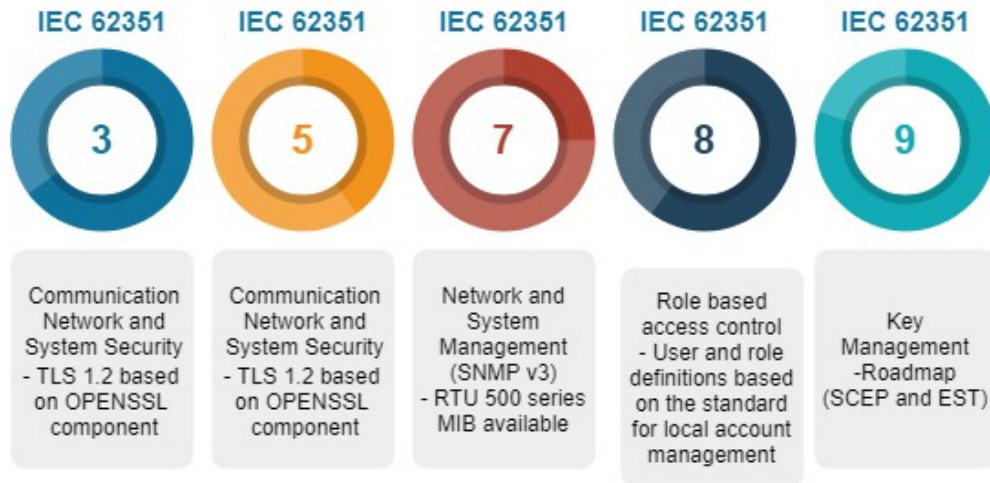


Figure 2.12: IEC 62351 Standard in RTU500 Series

The IEC 62351 standard is developed to provide efficient data authentication, intrusion detection, access control and prevent eavesdropping, playback and spoofing for IEC protocols at the application layer. It does not account for the security of the data link layer.

To estimate the cost of implementing IEC 62351 security standard in smart grid, the summation of the overheads in the conventional smart grid communication network between devices, substations and control centre is considered. Bandwidth is a limited resource for data transmission, and a dedicated/private wireless network will transform how the power utilities support the growing data traffic. The capacity of power utility networks is determined by the spectrum used and the limitations on frame length (255 octets) per transmission as it affects security bits to be added. The communication between field devices requires a small amount of bandwidth [216]. In the computation of bandwidth to support IEC 62351, the length (in bytes) of IEC protocol series Application Service Data Unit (ASDU), processor power computing the ASDU (ms),

challenge/response mechanism messages (bytes), critical ASDU request/response messages (bytes), frequency width, range and region covered are considered. The addition of more security mechanism increases the number of bytes which increase the bandwidth [193]. Other standards of IEC communication protocols and grid challenges being addressed by the research community are presented in [198]. The following recommendations apply when implementing IEC 62351:

- Interoperability between different security suites and the duration of TCP/IP connection to maintain security needs to be known. TLS algorithm is applied to maintain a TCP connection and X.509 certificates for data integrity and authenticity on the transport layer.
- A bi-directional certificate exchange of size ≤ 8192 octets, mandatory operation signature of 2048 bits of public key exchange such as RSA, and a minimum key length of 256 bits of elliptic curve operation signature.
- The authentication method in the application layer should be entity or message-by-message rather than authentication only at the beginning of a data stream as some connection-oriented protocols do.
- Access control to substations should only be possible through the control centre to prevent a third party from controlling the station's security credentials.
- Existing industrial IoT devices may not be able to cope with high processing power public-key encryption with very large key sizes. Low-security overhead is a solution to bandwidth limitation and reduces the link cost per octets transmitted.

The majority of IEC 62351 standard is supported in the ABB RTU 500 series shown in figure 2.12 used for the tests presented in chapter 6 and 7. The following cyber security standard requirements are fulfilled in the RTU; confidentiality to disclosure, availability to denial of service, authenticity to spoofing/forgery, authorisation to unauthorised access and auditability to hiding of attacks.

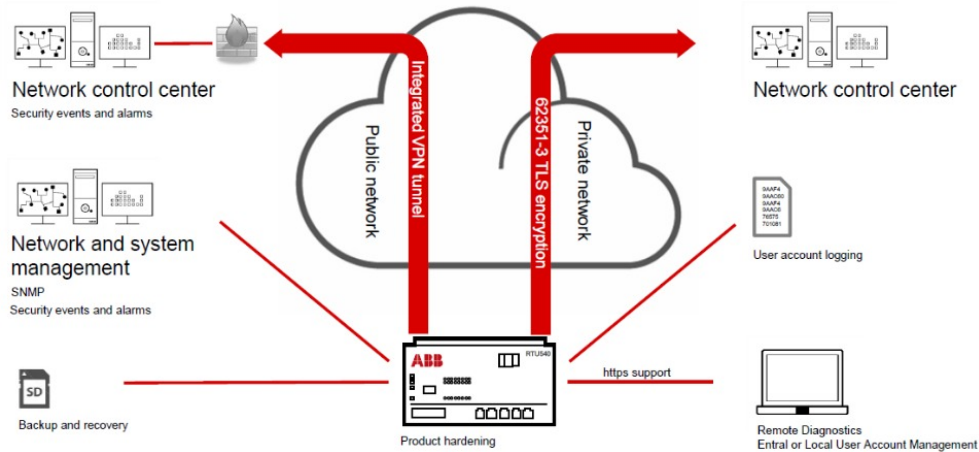


Figure 2.13: ABB RTU 500 Series

2.15 Bandwidth Consideration in Security

In IoT networks with devices limited in processing and storage capacity, the communication networks may also be limited in bandwidth to support bandwidth-intensive connections. Bandwidth is a prime design objective of utility networks; hence, any security techniques implemented must introduce a few octets of overhead and at the same time maintain an adequate level of security. According to [NIST](#) smart grid security design requirements [217] and the general smart grid key cybersecurity objectives for implementing IEC 62351 and other security standards, the following cybersecurity characteristics contribute to bandwidth utilisation:

Confidentiality

Protecting the contents of a message over a communication link from pseudo/unauthorised device is known as confidentiality. Confidentiality is achieved in power systems using cryptography algorithms involving public and private key infrastructure and other security schemes to ensure information protection against unauthorised access. Two types of cryptographic algorithms are in use. The asymmetric key cryptography (AKC), such as the Advanced Encryption System (AES) and Data Encryption Standard (DES), requires more resources for computation when compared to the symmetric key cryptography (SKC) like the Rivest-Shamir-Adleman (RSA). AKC is also known

as the public key infrastructure that utilises private and public keys to encrypt and decrypt information. On the other hand, symmetric-key cryptography maintains stable computational requirements even when the key size varies. The same key size is used for encrypting and decrypting. Ways of achieving this are implementing control systems (VPN/TLS), IEC 62351-3, IEC 60870-5-7, TLS for IEC 104, IEC 62351-5, secure authentication for IEC 104 and DNP3 and maintaining access (HTTPS) using temporary signed certificates.

Integrity

Message integrity is central to smart grid design, operation and administration. Communication network integrity mechanisms cannot be relied on to provide message integrity for security. Message sequence numbers designed to protect networks against replay attacks, frame counter and message checksum were not explicitly designed to counter cyber attacks [218]. Guarding against information modification or destruction during transmission guarantees non-repudiation and authenticity. This could be achieved through hash functions based on cryptographic algorithms to detect data integrity violations.

Availability

To increase the robustness of power networks, ensuring timely and reliable access to consumer's data by the utility companies is necessary to maintain high network availability. Availability is achieved by implementing IEC 62351-7, conducting system supervision through Simple Network Management Protocol Version 3 (SNMPv3), and handling security events to control system logs with trusted real-time timestamps based on Online Certificate Status Protocol (OCSP).

Authentication and Authorisation

The exchange of data across the power network ecosystem must be reliably authenticated. To ensure that the utility entities prove identities within the network, cryptographic keys are commonly used as means of authentication. Authentication and au-

thorisation are provided by implementing IEC 62351-8, Device Authentication (IEEE 802.1x), role-based access control, central account management based on Lightweight Directory Access Protocol (LDAP), and enforcing a strong password policy. On the other hand, non-repudiation ensures that the command and message are binded using digitally signed strong public-key certificates between the communicating entities.

Encryption

Encryption techniques such as AES-128 block cipher is an add-on to utility network security implementation for data link layer security since IEC 62351 only provides the application layer integrity protection mechanisms [193]. IEC 62351 standard was developed to cover authentication, encryption and key management security issues, given that the security of legacy systems lack application and data link layer security. Encryption is an essential security requirement for overcoming replay, modification and sniffing attacks to guarantee data integrity and confidentiality in legacy protocols and equipment susceptible to cyber threats.

Trust

Trust and revocation of key certificates are essential for securing power networks. Authenticated entities must only communicate with entities trusted by the certificate authority and the communicating entities. The expiration and revocation of key certificates roles reside with the key management system following ISO/IEC 11770 and NIST 800-57 key management design principles for power network operations [219]. There is additional overhead for issuing and distributing key certificates. TLS 1.2 is the most current public key infrastructure for the ISO/IEC 62351-3 implementations when compiling this thesis, while TLS 1.3 compatibility is in development. A good trust system ensures secure entity activity and the validation of an external logging concept known as auditability.

Chapter 3

Methodology and Implementations

Implementing this thesis methodology involving LoRaWAN, NB-IoT, and Smart Grid requires a systematic approach to designing, implementing, testing, and evaluating the research study results. The methodology typically includes steps such as problem identification, test network design and implementation, and experimentation for data collection and analysis. The overview of each method and implementation process is presented below:

3.1 LoRaWAN

Low Power Wide Area Network (LPWAN) technologies are of two types: The cellular LPWANs are provided by the Mobile Network Operators (MNOs) on licensed spectrum, and examples include NB-IoT and LTE-M discussed in section 3.4.1 and ?? respectively. The non-cellular-based LPWAN technologies are not licensed and leverage the unlicensed radio spectrum in the Industrial, Scientific and Medical (ISM) band. LORaWAN, Sigfox and NB-Fi are common examples. LPWANs are generally designed to meet the cost reduction deployment objectives of IoT devices that are on the increase. Requirements are that IoT applications operate optimally at high latency and low data rates for long periods with very low-cost radios and services. The recent

advancement in wireless technology for Internet of Things applications has enabled the development of various sensor networks for different user applications. Low Range (LoRa) and Wide Area Network (WAN), generally referred to as LoRaWAN, is one of the Low Power (LP) WANs encompassing classification requirements that are based on unlicensed spectrum, low cost, reduced power, and a wide range of data transmission [21]. Its operation is based on Chirp Spread Spectrum (CSS) modulation technique to connect multiple IoT devices through an open and standardised communication protocol for the Internet of Things and can be integrated with the licensed bands like the 4G/5G cellular networks [130]. The Internet of Things technology can be classified based on specific requirements of IoT applications. An example of such classification based on a range of transmission is shown in table 3.1.

Table 3.1: Classification of Wireless Technologies Based on the Transmission Range

Wireless Technologies	Range of Transmission (meters)	Range Classification
RPMA	0 - 13K	Medium
SigFox	10k - 50k	Long range
Weightless	2K - 13 K	Medium
RFID	0 - 10	very short range
Bluetooth and ZigBee	10 - 100	short range
Wi-Fi	100 - 1000	Medium range
Cellular 2G/3G/4G and LoRa	up to 100000	long range

3.1.1 LoRaWAN Network Architecture

LoRa is a physical layer radio modulation technology developed by Semtech in their LoRa Modem integrated circuit [7]. LoRa Alliance is a consortium of engineering professionals from different organisations developing LoRa communication protocol and system architecture, LoRaWAN - link layer protocol. The standard LoRaWAN architecture is a star-of-star topology shown in figure 3.1 with the front-end, gateways, and back-end as three distinct parts. The front end of the network is the proprietary LoRa RF connections between the end devices and the LoRa gateways. Sensor nodes (end device) data are transparent broadcast messages via LoRa gateways within range for uplink communications. The gateways act as repeaters by relaying the end device

message to a single network server where it is aggregated. This eliminates any handover requirements between the gateways within the network coverage. Mesh networks are used to support the LoRaWAN networks without network coverage, but the energy utilisation of IoT modules will be significantly impacted irrespective of the device class [220].

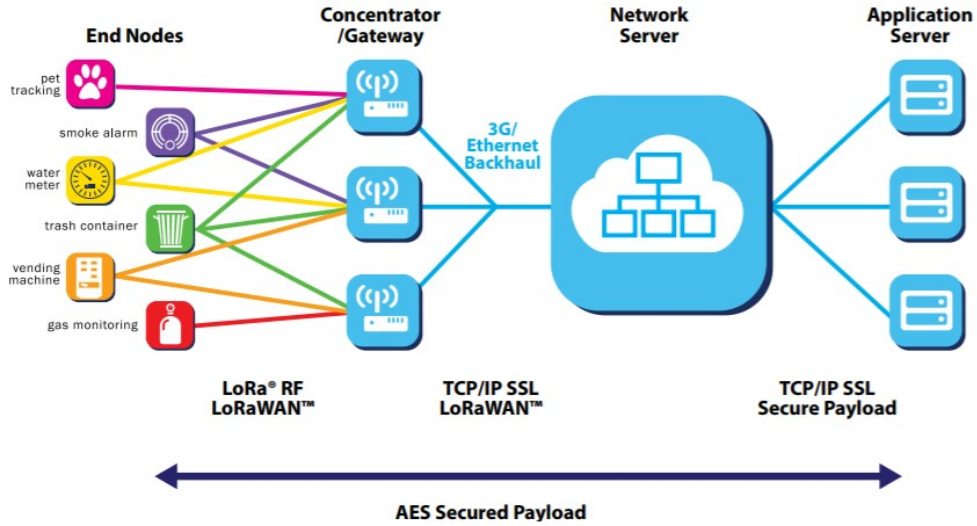


Figure 3.1: LoRaWAN Architecture [6]

The back-end is IP-based connection between the network/application servers and the gateways. The network server is the received data aggregation point, and the MAC layer encryption must be decrypted before an uplink data transfer to the application server of choice. The application key of each application server is then finally used to decrypt the real data payload. The reverse process occurs for a downlink data transfer requiring an uplink communication from the IoT devices.

3.1.2 LoRAWAN Layers

The physical layer of LoRa influences the quality of service, energy efficiency, security, and applications of the LoRaWAN network [6]. The key components of LoRaWAN layers are described in figure 3.2.

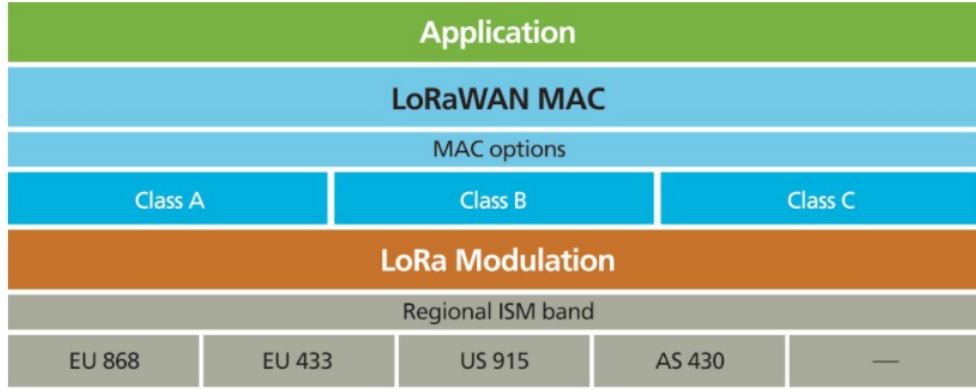


Figure 3.2: LoRaWAN Layers [7]

3.1.3 LoRaWAN Physical Characteristics

Modulation

LoRa modulation scheme is based on Chirp Spread Spectrum (CSS) whereby the chirp signal varies linearly with the frequency [21]. By applying different Spread Factors (SFs), a compromise may be achieved between power consumption or transmission distance for data rate according to equation 5.1 where R_C and R_S represents the symbol and chirp rate respectively. The advantages of this type of modulation scheme include constant envelope, scalable bandwidth, resistance to Doppler effect, interference and multipath fading, and improved range, network and geolocation capabilities [130]. It also reduces the complexity of the receiver design since the time and frequency offset is identical. Adaptive Data Rate (ADR) is another mechanism employed to reduce the RF power consumed and the data rates of the devices. To increase the transmission and reception distance, which decreases the data rate, SF varying between 7 to 12 is used based on the indicative physical data bit rates of 250 - 5470 bps. These are critical for determining the transmission range and energy efficiency of connections.

$$SF = \log_2 \left(\frac{R_C}{R_S} \right) \quad (3.1)$$

Transmission Scheme

Bidirectional asymmetric communication is allowed between the LoRaWAN IoT devices and the LoRa gateways, and the current implementations employ static configuration selection. The end nodes are set up to utilise different spreading factors, bandwidth, coding rate and transmission power configurations to achieve specific performance. Hence, optimising these parameters will render considerable benefits to the LoRa applications, hence the need for machine learning algorithms for optimum transmission parameter selection [221].

Device Classes

There are three Medium Access Control (MAC) operating classes of LoRaWAN IoT devices layers specified in the LoRaWAN standard to satisfy certain applications with trade-offs between latency and energy utilisation. Each class is distinguished by design in energy consumption profile which relates to the time (duty cycle) it takes their radio receivers to receive a LoRaWAN message. LoRaWAN devices are regulated to transmit 1% of the packet each time to manage the spectrum and reduce collisions. They are based on the same physical layer characteristics and includes Class A, B and C [222].

Class A is a generic feature in all LoRaWAN IoT modules that are battery-powered, energy efficient and are based on ALOHA operational principle. Its operation is based on higher uplink transmission predetermined by the downlink transmissions. No uplink transmission will potentially increase the latency of downlink transmissions because the uplink transmissions set the two possible transmission windows. In this case, the devices only receive downlink packets in two short-lived windows, RX1 and RX2, immediately after the uplink transmission, TX1. The duration of the downlink receive windows is recommended at 1-second intervals for maximum efficiency, depending on the spread factor. An acknowledged uplink transmission prevents packet retransmission in the downlink, thereby saving energy while the unacknowledged transmission, viewed as a compromised link causes packet retransmission with an increasing spread factor which reduces the noise floor.

Class B devices are designed to increase the receive windows of downlink trans-

missions with lower latency and energy consumption of the devices [223]. The synchronisation message from the gateways which increases the energy demand of IoT devices allows downlink re-transmissions to be rescheduled. In this case, a gateway can multicast a message to the IoT devices within the network.

Class C devices are application dependent. Typically, for non-battery powered IoT modules that can receive and transmit efficiently at any time. The low power characteristics of LoRaWAN are defeated in Class C IoT devices since they continuously listen for downlink messages. A suitable class C application is the traffic and packing systems where a power supply is fundamentally required.

Frequency

LoRa operates in the sub-GHz band, and frequencies are unique to a specific region and country. In the EU, an 868 Mhz LoRa end device is common and must support 863 - 870 Mhz ISM band according to ETSI regulatory EN300.220 standard [224]. In the United States and Canada, 902 - 928 MHz ISM band apply based on FCC regulations. Each LoRa IoT device must as a minimum requirement support a bandwidth of 125 kHz and <1% duty cycle. A standard LoRa platform consists of two major parts; the front-end and the back-end. The IoT devices and gateways constitute the front-end. The messages from the LoRa IoT devices below 50 kbps are sent directly to the gateways where they are aggregated. The LoRa Gateway receives messages from the sensor nodes via the frequency of operation and relays them through the Internet router to the backend of the LoRa platform. The LoRaWAN network platform implementation is based on star network topology separated into front-end and back-end as discussed in subsection 5.3.2, see figure 3.1.

Firmware Update

Updating IoT device firmware is an essential IoT security vulnerability prevention practice given the increasing exploits in IoT solutions deployed around the world. While the benefits of IoT continue to spread, it comes with challenges of ensuring security and privacy, especially in low power wide area networks. In LoRaWAN, firmware

can be updated Over-the-Air, but when other security features such as Blockchain are utilised alongside, the update procedure becomes more secure and active in fixing security vulnerabilities [67]. Applying IoT firmware update patches is one way of securing connected devices from vulnerabilities such as firmware modification, unauthorised firmware, and access authorisation [54]. For embedded systems, the firmware update requirements and process for IoT devices include the device first request for firmware update from an authorised entity, and the entity performs the firmware update after the driver has been authenticated and authorised with an update rollback mechanisms in the case of a failed update session. Remote firmware updates allow new security updates to reach end devices as quickly as against manual updates, which is expensive and inefficient for good incident response. Manual update is an expensive option and will be difficult to provision as the number of IoT continues to increase. Firmware Update Over-the-Air (FUOTA) in LoRaWAN network is difficult to achieve in large scale IoT deployment, especially in hard to reach locations due to poor data rate due to bandwidth constraint, low data rate due to battery power, and small duty cycle due to policy regulations. The LoRaWAN FUOTA architecture specifies the sequence of actions and the roles of end devices, network server, and application server to achieve secure firmware update [225]. The challenges in updating IoT devices include authentication, integrity check, error correction, and vision control by accepting data only from trusted sources with limited human intervention. Others include lack of standardisation in the network design process, manufacturing, implementation, and the fact that IoT devices are constrained in power, processing resources, coverage reach, and memory. Integrating other wireless technologies such as Wifi or Bluetooth for the purpose of firmware update could be a viable alternative but at the expense of increased security risks, higher battery utilisation and increased cost from installations of new LoRaWAN gateways and additional network resources given that Wifi and Bluetooth have a shorter transmission range.

3.1.4 Network Join Procedure

LoRaWAN network join procedure consists of a join request and accept messages between the IoT device and network server before any data transmission. Over-the-air-Activation (OTAA) and Activation by Personalisation (ABP) are the standard specifications when IoT end devices join a LoRaWAN network. For both methods, the IoT device first sends an unencrypted join request message containing the IoT Device Identifier (DevEUI) and address space, Application Identifier (AppEUI) and address space, and a 16 bits Device Nonce (DevNonce) to the network server [226].

In the **Over-the-air Activation (OTAA)**, the end device initiates a join request to the server with a 128-bit secret shared application Key (AppKey - AppEUI). The LoRa server acknowledges the join request message with a join accept message if the IoT device is granted access to the join the network; else, there is no acknowledgement for a failed join request. Both the server and device generate symmetric security keys that are then used to encrypt, authenticate and authorise device-to-server communication. OTAA is preferred for higher-level security because the security is root provisioned, the security details are generated during the connection establishment procedure as long as the OTAA end device has an interface to the key server.

The **Activation by Personalisation (ABP)**, as the name suggests, requires the manual programming of the unique network (NwkSKey) and application (AppSKey) session keys to be shared between the end device, network and application servers in a pre-selected network. They are not root provisioned and, as such, remain unchanged in an ABP provisioned IoT end device. The use of unique key generators and publicly available resources is extremely important to keep the network secure such that the knowledge used in compromising one IoT device does not apply to others. This will reduce the management cost of having to update manually large-scale IoT devices in any attack incidence. The manual programming of keys is the downside of this mode of deployment. To protect the keys hard-coded in the IoT devices, ABP should be avoided in a deployment scenario where downlink transmission is required since the network cannot update the session keys. If compromised, LoRa messages can be read and modified in the form of a man-in-the-middle attack. The general LoRaWAN join

procedure could be enhanced with other security mechanisms to prevent attacks like replay that could sniff join request messages. A Blockchain introduced between the join server and application server in the join procedure offers end-to-end encryption and authentication [68].

3.1.5 LoRaWAN Security

Security is an integral part of the LoRaWAN network primarily to ensure authenticated connections, integrity protection and confidentiality in the communication process. The IoT device activation modes, LoRaWAN key management/exchange and message authentication-encryption scheme are part of the security schemes embedded in the LoRaWAN architecture [227]. Three layers of security are expected in the LoRaWAN network: device, network, and application security. Device security ensures authenticity within the network. The network and application layer security ensures the authenticity of nodes and the confidentiality of data, respectively. The network and application layer security differs with respect to the mode of activation. The device address, application identifier, network session key and application session keys are stored in the IoT modules. It also includes other issues such as the implementation, user behaviour, protocol issues, types of security algorithms used, and the method of security protocol verification [228]. To build a truly secure LoRaWAN network, LoRa messages must be encrypted using a lightweight and authenticated key management method that would permit server tasks to be performed locally where possible. Others include message content being disguised using fixed payload, security key generators being random of significant length, security keys loaded on the end device in a trusted partition and other adequate security practices being enforced. In practice, LoRaWAN is affected by some challenges that indirectly violate security. When LoRaWAN IoT devices are heterogeneous, inefficient in energy management, complex in integration, and manufactured without proper standardisation, the entire network's privacy, integrity, and confidentiality could be compromised.

3.1.6 Network Performance

The performance of the LoRaWAN network using The Things Network (TTN) server is presented in chapter 5. TTN is an open LoRaWAN platform that runs server infrastructure as a service. End devices can join gateways added to the TTN network through the TTN API infrastructure for time on-air of 30s/day lower than 846s/day specified by the LoRa Alliance specifications. This reflects the potential challenges that will come from different LoRaWAN applications of different performance requirements sharing the same network resources. Private LoRaWAN platforms will be needed if some of these applications specific challenges such as latency, reliability, and transmission pattern are to be rectified. The network performance results were measured based on the security, battery utilisation, latency, and response time of the IoT device and join server for specific data throughput. The performance comes with tradeoffs between transmission and data rate range, and energy utilisation and time on air. To optimise the energy utilisation of the end devices, the transmission range, spreading factor and time on-air must be reduced. These parameters that reduce the coding gain can be achieved by increasing the capacity of the network (introducing more gateways), which affects the performance of the LoRaWAN network.

3.2 Cellular Internet of Things Technology

As an introductory part of this thesis's core chapters, this section introduces the concept of cellular IoT based on the Third Generation Partnership Project (3GPP). 3GPP-based cellular IoT networks are designed to interconnect machines and are estimated to reach 5 billion connections by 2025, a Compound Annual Growth Rate (CAGR) of 25% [229]. Global System for Mobile Communication (GSM), Long Term Evolution (LTE) for machines, and Fifth generation (5G) wireless networks will be discussed as they are the technologies on which NB-IoT and LTE-M evolved as an enabling protocol for industrial IoT deployment. NB-IoT and LTE-M are the two leading standardised mobile IoT technologies today and are an add-on to the 5G NR design. Their evolution has greatly emphasised Embedded/Integrated Subscriber Identity Module (eSIM

or nuSIM) for machine-to-machine communication. eSIM is a solution that promotes security, a unified global platform, interoperability of IoT modules, and efficient management of IoT systems.

3.2.1 Long Term Evolution (LTE)

Long Term Evolution (LTE) Long Term Evolution (LTE) is an air interface 3GPP standardised cellular network for Machine-Type Communications (MTC) with the deployment objectives of meeting the connectivity requirements of providing low latency communication, higher data rates, improved network capacity and coverage, low-cost operating IoT devices [230]. LTE enabled IoT devices can support more effective cell connectivity and applications that require in-depth coverage of cellular networks. LTE is the parent technology for NB-IoT and LTE-M radio access technologies. The first LTE specifications were concluded in 2008 by the 3GPP in Release 8 standard [231]. Subsequent LTE Releases 9 and 10 standards (LTE-Advanced) improved spectral efficiency, high peak data rate, and good user experience. LTE, LTE-A, and LTE-M were developed to improve the network's access and core part. Also, OFDMA access technology for TDMA and CDMA (Universal Mobile Telecommunications System (UMTS) and High-Speed Packet Network (HSPA) access technologies). The packet Switched EPC replaced Circuit Switched and Packet Switched for GSM and GPRS in the core network, respectively. This subsection provides a comprehensive background of LTE technology, its design specifications, and techniques suitable for IoT deployments. The following LTE terminologies will help the reader to have a good understanding of this section:

- 3GPP - Third Generation Partnership Project (3GPP) is a telecommunications standard development organisation for 3G cellular/mobile technologies and beyond.
- UMTS - Universal Mobile Telecommunications Systems (UMST), also known as the Evolved Packet System (EPS), handles packet routing for both the control and user plane via IP tunnels.

- RAN - Radio Access Network (RAN) refer to UTRAN and/or GERAN in Iu mode and/or E-UTRAN. It is the key component of a cellular network that connects UEs to the core network through radio links.
- E-UTRA - Evolved Universal Terrestrial Radio Access Network (E-UTRA) is an air interface packet-switched technology for cellular networks. Through a single evolution path, the data speed and spectral efficiency of the LTE network are increased with additional capabilities.
- EPC – Evolved Packet Core (EPC) defined the IP core network as an improvement to the circuit packet and switched networks which introduce higher throughput, reduced cost and latency and the ability to be integrated with legacy radio access technologies.
- eNB - LTE evolved nodeB (eNB) provides the E-UTRA user-plane and control-plane protocol termination towards the UEs. Connections between eNBs are via the X2 interface to the MME via the S1 interface.
- MME - LTE Mobile Management Entity (MME) is the core part of an LTE network with Serving Gateway (SGW), Packet Data Network Gateway (PGW), Policy and Charging Rule Function (PCRF), Home Subscriber Server (HSS) and Equipment Identity Register (EIR) in-built. It handles paging, authentication, bearer establishment procedure, and idle mode using uses Stratum Control Transmission Protocol (SCTP) to operate in the control plane.

3.2.2 Key Characteristics of LTE Technologies

The technologies enabling LTE evolution is discussed in this section, and some LTE characteristics are presented with the current research practices and standardisation efforts.

OFDM

Orthogonal Frequency Division Multiple (OFDM) is an LTE downlink modulation technique that allows a frequency band to be divided equally into sub-frequency channels for fast channel-independent scheduling of transmission in both the time and frequency domains [230]. In other words, it utilises a multicarrier transmission scheme, subdividing data symbols into different wideband subcarriers. The sub-frequencies are used to transmit parts of a radio signal simultaneously but with high inefficient transmitter power. OFDM is robust and easy to implement than other modulation techniques such as the Code Division Multiple Access (CDMA) [232], [233]. Orthogonal Frequency Division Multiple Access (OFDMA) is a variant of OFDM with uplink that operates differently in the LTE network. The improved capacity and robustness due to trunk multiplexing efficiency and frequency scheduling pattern in TDMA features of OFDMA allow for a dynamic allocation of subcarriers to the UEs. UEs are individually assigned resource blocks based on OFDMA for downlink and SC-FDMA for uplink. Different modulation techniques are supported in LTE systems, such as the Quadrature Phase Shift Keying (QPSK), Binary Phase Shift Keying (BQPSK), and Quadrature Amplitude Modulation (16, 64, and 256QAM). Each modulation technique is used based on the radio's operating condition. Adaptive LTE modulation techniques enable the eNodeB to select the most appropriate modulation technique depending on the SNR requirements and variable weather conditions. Modulation techniques such as QPSK withstand severe weather conditions.

SC-FDMA

Single-Carrier Frequency Division Multiple (SC-FDM) is adopted in the LTE network to handle problems of power consumption during uplink transmissions cycle and to be in-cell orthogonal [234]. To minimise variations in the transmitted power (Peak-to-Average Power Ratio (PAPR)), a precoded Discrete Fourier Transform (DFT) is added to an OFDM signal without impacting on the complexity of frequency scheduling and equalisation. It prevents the concept of spreading transmission over an entire bandwidth for UEs that are limited in power. Power and symbol resources are critical

for bandwidth and channel estimation in LTE networks. LTE uses OFDM for the connections from the eNB to the user/field device to carry the data traffic over many narrow band carriers of 180 kHz each (resource blocks), while it uses SC-FDMA for the connections from the user to the eNodeB. The user application determines the number of resource blocks required for each application. The more resource blocks dedicated, the higher the data rates that could be achieved. The available resources in terms of the number of resource blocks are shared between the network users. This feature offers more flexibility and better usability of LTE.

MIMO

Multiple-Input Multiple-Output (MIMO) technology makes using multiple antennae systems, which enhances radio signal coverage and physical layer capacity of UEs in the LTE system possible. Hence, using different MIMO algorithms, the maximum data rates and throughput are achieved due to reliable communication media, emphasising the design of the antenna air interface. MIMO naturally improves the performance of LTE networks by creating different physical paths for data transmission and enables a significant reduction of latency on the air interface [235]. Independent transmission of information on different antennas is used to achieve peak data rate in the spatial multiplexing algorithm. The data rate depends on the number of transmit antennas in the downlink configurable up to 4 and 8 antennas in the LTE and LTE-A, respectively. Beamforming and transmit diversity algorithms provide robustness in the transmission links by transmitting superfluous information on separate antennas while avoiding fading dips that limits latency.

Turbo Coding

Turbo coding is a convolutional legacy mobile communication channel performance technology. The implementation of Cyclic Redundancy Check (CRC) in LTE turbo encoder systems allows an efficient channel decoding of user data. Error-free transmissions are terminated early while transmissions with CRC check errors are decoded. This procedure saves power, improve performance and reduces the operational requirements

of turbo decoders.

Link Adaptation

Various modulation and coding techniques are used to manage the dynamics in the LTE communication channel. For instance, MIMO allows variation of antenna numbers in the transmit and receive channel. The transmission bandwidth can also be varied to guarantee network resource utilisation and Quality of Service (QoS). Similar to scheduling, it ensures that network resources are prioritised to achieve the best QoS.

Bandwidth

LTE systems have variable and flexible bandwidth for IoT applications. Table ?? show variants of LTE bandwidth with their respective PRBs that could be employed for NB-IoT and LTE-M networks. The LTE cell detection and synchronisation procedure is affected by the flexibility in bandwidth. Cellular network providers utilise a number of discrete slabs of frequency bands to deliver different services. LTE frequency bands use two LTE spectrum duplex modes to support deployment globally [236]. The Frequency Division Duplex (FDD) operate in the paired spectrum, and Time Division Duplex (TDD) operates in the unpaired spectrum. The FDD method divides the frequency bands into discrete frequencies for uplink and downlink transmissions, whereas the TDD method uses the same frequencies for both uplink and downlink transmissions at specified intervals. The main differences between LTE-TDD and LTE-FDD are shown in figure 3.2 [62]. When the required bandwidth is not available, Carrier Aggregation (CA) is a technique that allows contiguous carriers to be merged and offer the required data rate. If networks such as a power network application do not require data rate in Gbps, CA may not be needed. Usually, without CA, LTE networks can support maximum channel bandwidth of 20 MHz. The summary of the LTE bandwidths and the numbers of their resource blocks and sub-carriers are presented in table 3.3. The benefits of selecting the appropriate bandwidth for any application are avoiding an increase in latency due to signal overheads from increasing data traffic, a high number of connections, and overlapping control of data sessions. Above all, it helps determine

the operational costs of running a specific band and the compactible infrastructure.

Table 3.2: LTE TDD vs FDD

LTE Features	TDD	FDD
Paired Spectrum	Not Required	Required
Channel Exchange	Identical channel propagation in UL and DL	Different in both directions
UL and DL Capacity	Flexible, dynamically change UL and DL capacity ratio to match demand	Not flexible to make dynamic changes to match capacity
Hardware Cost	Duplexer cost is not needed to separate the transmitter and receiver	Diplexer is needed to segregate the transmitter and receiver, which could increase the cost.

Table 3.3: Available Resource Blocks in LTE Bandwidth

Bandwidth (MHz)	1.4	3	5	10	15	20
PRBs in LTE Bandwidth	6	15	25	50	75	100
Sub-carrier	72	180	300	600	900	120
Narrowbands (LTE-M)	1	2	4	8	12	16
NB-IoT PRBs below DC Subcarrier	-	2	2,7	4,9,14,19	A	B
NB-IoT PRBs above DC Subcarrier	-	12	17,22	30, 35, 40, 45	C	D
Note: A = 2, 7, 12, 17, 22, 27, 32						
B = 4, 9, 14, 19, 24, 29, 34, 39, 44						
C = 42, 47, 52, 57, 62, 67, 72						
D = 55, 60, 65, 70, 75, 80, 85, 90, 95						

3.3 Narrowband Internet of Things (NB-IoT)

The new cellular Radio Access (RA) interface introduced in the 3GPP Release 13 and 14 is known as the Narrowband Internet of Things (*NB-IoT*) with minor modifications of legacy LTE and GSM network resources [237]. It is also known as *LTE CAT-NB1*. NB-IoT shares the same basic radio principles with the regular LTE system, which helps integrate NB-IoT carriers with the LTE cells. Examples of the shared principles are the duration of the radio frames, the time slots, the communication between the core networks and the number of symbols. Elements of the technology

such as synchronisation signals and broadcast of the System Information Block (SIB) are done differently with the possibility of introducing a new radio interface in the Evolved-UMTS Terrestrial Radio Access Network (E-UTRAN).

This subsection provides the technological background of NB-IoT required to deliver the testbed, tests and the different areas of NB-IoT technology that informed the experimental design, implementation and analysis as presented in chapterand [4](#) and [5](#). NB-IoT adopts LTE and GSM protocol stacks as its building block, but the design improvements applied in the physical and medium access control layers are not exactly the same. With the implementation based on 3GPP Release 13 reference standard, relevant information about the current and future 3GPP Releases that supports NB-IoT applications are contained in section [3.8](#) for researchers and readers seeking current information about the technology up to standard Release 17.

3.4 Fundamentals of NB-IoT

3.4.1 History and Standardisation

As a cellular communication technology becoming mainstream for LPWAN, NB-IoT development, test, and evaluation is a hot topic among researchers. The increasing IoT market share for licensed LPWAN led to the development of NB-IoT as an alternative solution for unlicensed LPWAN such as LoRaWAN and SigFox. The NB-IoT project started back in 2016 with ambitious objectives to achieve higher network coverage and capacity, lower battery life and latency, massive connections, implementation through a software upgrade in GSM and LTE resources. This meant an enhancement of LTE and GSM structure that would allow backward compatibility to support EC-GSM-IoT (Clean Slate IoT (CL-IoT)) through spectrum refarming and directly in LTE carriers in different modes as discussed in subsection [4.3.1](#). In the 3GPP Release 13, the standardisation effort was completed with more ultra-low complexity and low data throughput in mid 2016 [[238](#)]. In the technical specifications, the uplink and downlink channels of NB-IoT is deployed in a bandwidth of 180 kHz as shown in figure [3.13](#). NB-IoT standardisation effort has gone through many standard releases to improve the

devices and network operational performances, the most recent being release 17, see section 3.8.5 for a detail of the additional features in each release. The adoption rate of NB-IoT has grown, amounting to 103 commercial NB-IoT launched in 62 countries by many MNOs as of February 2021 [239]. Similarly, the Cat-NB1 and Cat-NB2 chipsets modules supporting the technology has also grown to 36 [240] in the same year.

For IoT devices to be used in a challenging environment with low power consumption requirements to communicate reliably over NB-IoT network, an efficient design feature is required to reduce the complexity of NB-IoT devices in three major areas: RF design; baseband processing; and storage capacity. NB-IoT is designed to use close to unity envelope waveform in the uplink channel, which reduces the backoff power needed to achieve the best coverage while maintaining the power efficiency. Other variants of LTE, such as LTE-M and EC-GSM-IoT achieve coverage enhancement through repetitions at the expense of data rate and battery lifetime. The performance analysis of NB-IoT network is presented in section 4. NB-IoT network is mainly evaluated in cell capacity, battery life, latency, data rate, coverage capacity, and end device position accuracy depending on the deployment mode. However, the network implementation presented in chapter 5 is based on the in-band mode of operation. It is important to note that the performance for guard-band and standalone may not deviate heavily and is recommended for evaluation as future work. The advantages of the enhancements in the radio access design principles of NB-IoT are discussed below:

3.4.2 NB-IoT Architecture

The 3GPP specifies the GSM and LTE mobile communication systems standards from which NB-IoT technology evolved. The first NB-IoT standard architecture was released in June 2016. This development was made possible following the previous studies on Narrowband Machine-to-Machine (NB-M2M) communication by Huawei, Vodafone and Qualcomm in 2014. The investigations led to the development of Narrowband Cellular Internet of Things (NB-CIoT) in 2015. These, in addition to the Ericsson study on Narrowband Long Term Evolution (NB-LTE) that produced the NB-IoT 3GPP Work Item Release 13 in 2015 are the initial studies [241]. The architecture

of NB-IoT, as shown in figure 3.3 is an enhanced architecture of the existing Evolved Packet Core (EPC) network with Control Plane (CP) and User Plane (UP) functions added. The significant improvement is introducing the Service Capability Exposure Function (SCEF) in the EPC to manage IP and non-IP data packets in the UP and CP modes. NB-IoT's RA design provides connectivity for a higher number of Ultra-Low Machine-Type Communication (μ L-MTC) devices in a single radio cell. In the enhanced NB-IoT architecture illustrated in figure 3.3, its constituent parts are briefly explained:

- **Serving Gateway** - The Serving Gateway (SGW) handles UE local mobility between eNBs and inter-3GPP, load balancing by ensuring adequate packet forwarding and routing in the UL and DL, and an anchor point for any handover initiation and billing [234].
- **Packet Gateway** - The Packet Gateway (PGW) provide PDN connectivity to E-UTRAN and facilitate IP address allocation to UEs, packet filtering, etc.
- **Home Subscriber Server** - The Home Subscriber Server (HSS) is implemented in MME to store and update UE IMSI, TMSI, IMEISV, TAC, PLMN information. Security information such as K-asme is stored in the HSS to prevent unauthenticated devices from joining the network.
- **Mobility Management Entity (MME) and eNB** discussed in subsection 3.7.1 and 3.7.2 are used to provide control plane path between the two entities.
- The S1-U, S1-C, S11, T6a, T8, SGi, S5/S8, and X2 are some of the reference points between the entities for enabling different types of service functions.

3.4.3 Air Interface

The air interface enhances the physical layer specifications for User Equipment (UE) and NB-IoT Access Network introduced by the 3GPP in LTE technology to support the growing IoT market, starting from the Release 13 specifications. For key enhancements

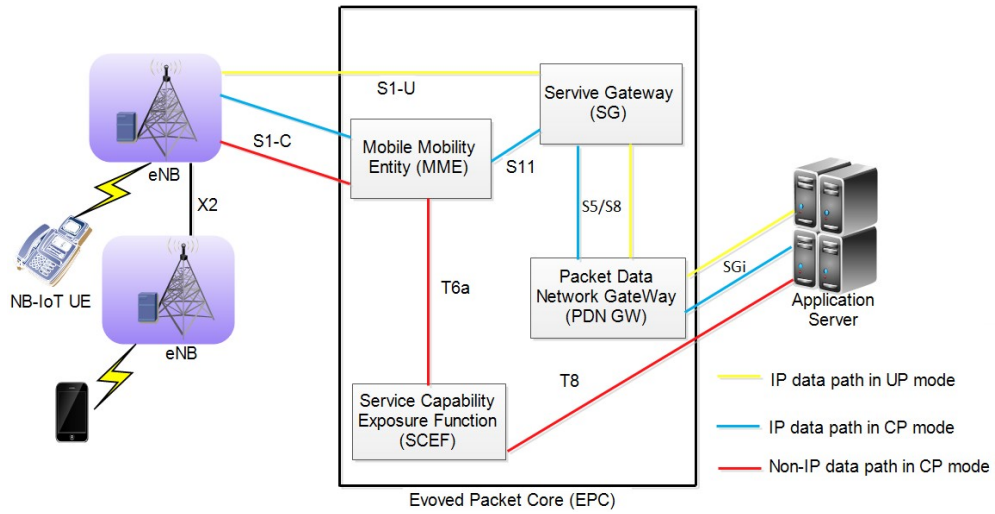


Figure 3.3: NB-IoT Architecture

of EC-GSM-IoT, LTE-M and NB-IoT specification, refer to [62]. A typical access network is shown in figure 3.4 with a network of eNBs and core networks (S-GW and MMEs) representing the access network. The core network communicates with the eNBs via the S1 interfaces, while the eNBs is networked via the X2 interfaces. Within the testing context, specific capabilities such as handover support occur between eNB cells and are only possible in experimental features for the intra-eNB. More than one eNBs, radio heads are needed to evaluate S1 and X2 handovers, which was not considered in this study.

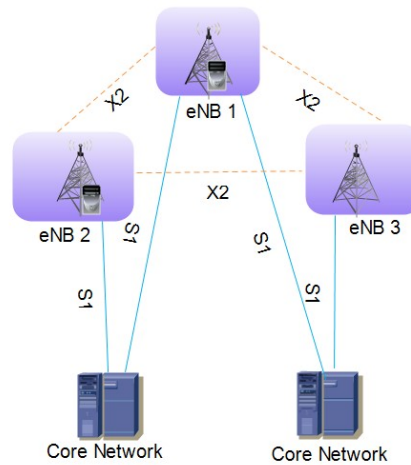



Figure 3.4: NB-IoT Access Network

In this scenario, the UE and handover monitor command will be used to initiate the process automatically by specifying the UE ID and Physical Cell Identity (PCI) with the DL EARFCN of the target cell as shown in figure 3.5. The specified cell neighbour properties must be valid and configured adequately for seamless cell interactions. Like ensuring that the eNBs are configured to support more than one LTE cell sharing the same S1 interface with the MME. When the eNB is started with more than one LTE cell, handover between cells is initiated by varying the downlink power levels between the cells, usually maintained at an excellent range to avoid interferences and retransmissions.



```

(mme) ue
      IMSI      IMEISV      M_TMSI REG      TAC #ERAB IP_ADDR
235047364000019 3543460998798300 0x1c0c0af9 N
(mme) enb
      PLMN      eNB_ID      IP:Port #UEctx      TACs
[REDACTED] 0x1a2d1      127.0.1.1:47302      0      0x2(NB-IoT)
(mme) █
  
```

Figure 3.5: UE Features

The UE category specifications for the air interface as applied to NB-IoT testing in chapter 4 is a *CAT-NB1*. General specifications of NB-IoT UE categories are summarised in table 3.4. When NB-IoT UE unique features are compared to LTE devices, it is usually based on complexity and cost as signalling consumes the limited resources in the NB-IoT network. The NB-IoT operational frequency of 180 kHz means that UE can only latch in either the primary or secondary carrier pair at a time. The multi-carrier operation was introduced to address this issue of signalling in both the uplink and downlink channels. BY specifying secondary carriers for data transmission function and scheduling messages only (see section 3.8.2), the primary carrier is used for signalling in the uplink and downlink.

3.4.4 Physical Layer Resources

The Physical Layer Resources (PLR) structure and signalling of NB-IoT in time and frequency domains in the uplink and downlink channels are described in this subsection.

Table 3.4: NB-IoT UE Category

Device category	NB1	NB2
3GPP Standard	Release 13	Release 14
Frequency	180 kHz	180 kHz
Bandwidth	3,5,10,15,20 MHz	3,5,10,15,20 MHz
Power class	20, 24 dBm	20, 23 dBm
Max. UL TBS	1000	2536
Max. DL TBS	680	2536
Device Antenna	1	1
Number of HARQ	1	1 or 2
Peak DL data rate	226.7 kbps	258.0 kbps
Soft Channels	2112	6400
Buffer size	4000	8000
Duplex mode	half duplex	half duplex

3.4.5 Uplink and Downlink Operation

Orthogonal Frequency Division Multiple Access (OFDMA) is employed in NB-IoT DL transmission following LTE numerology characteristics. The same numerology applicable in the UL is used in the DL but with Single Carrier Frequency Division Multiple Access (SC-FDMA) at 15 kHz or with 3.75 KHz subcarrier spacing. See subsections 3.2.2 and 3.2.2 for more information on OFDMA and SC-FDMA, respectively.

Numerology

NB-IoT numerology is from LTE, and as a result, one LTE PRB of 180 kHz is the channel bandwidth required for NB-IoT deployment in the guard-band (between two adjacent LTE carriers). The in-band modes are within an LTE carrier. For standalone, the un-used 200 kHz of GSM is refarmed. In practical terms, 180 kHz gives 15 kHz for 12 subcarriers for uplink and downlink transmissions. The LTE frame structure and the 48 subcarrier of 3.75 kHz [8] are examples of other numerologies introduced to enhance NB-IoT features, such as coexistence and coverage.

NB-IoT Network capacity

NB-IoT supports many UEs in one LTE carrier due to the spectral efficiency in the UL transmissions. For the relationship between the capacity of the NB-IoT network, the bandwidth required, and power consumed by the UEs, Shannon's channel capacity theorem is usually considered; see equation 3.2.

$$C = W \log(1 + \frac{S}{N}) = W \log(1 + \frac{S}{N_0 W}) \quad (3.2)$$

Where C, S, N, N_0 , and W represents channel capacity (bps), signal power, noise power, noise power spectral density, and noise bandwidth, respectively. The network capacity depends on the level of the received signal power.

Power Saving Category

Extended Discontinuous Reception (eDRX) and Power Saving Mode (PSM) are the two effective techniques applied to reduce the UE transmission power from 23dBm in power class 3 to 14 dBm in power class 6 [8]. Connected and idle operation modes are other techniques that contribute to UE efficient energy utilisation in the NB-IoT network.

In connected mode, the UE can receive downlink messages and send data over the radio channel. The lease timer determines when the UE enters into other modes of operation. In the idle mode, the UE is still attached to the network and able to receive SIB, which triggers it back into the connected mode based on the active timer configuration (can last up to 3 hours maximum). Because it still retains RA and data transmission information, it continues to monitor the paging channel for transmitted data. The frequency of these checks can be improved in the NB-IoT network to 175 minutes. In the PSM mode, while unreachable, the UE remains registered to the network with Tracking Area Update (TAU) performed periodically at the end of every PSM cycle (413 days maximum). The MIB and SIBs information must be retrieved for another transmission to occur as the UE has lost the connection with the network and gone into sleep mode, resulting in low power utilisation. A New RA procedure is

required to wake the UE and restart the transition process into the connected mode for uplink transmissions. The power-saving mode transition state diagram in figure 3.6 gives a better visualisation of how the UE state influences the various power-saving modes.

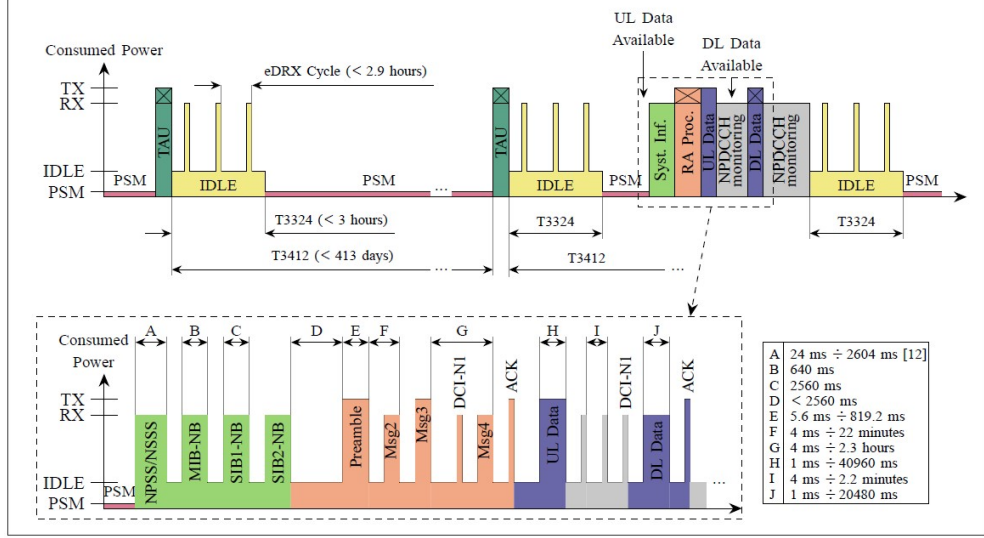


Figure 3.6: NB-IoT UE Power Saving Modes [8]

3.4.6 Downlink NB-IoT Channels

The set of channels and signals supported in NB-IoT is shown in figure 3.7. Whereas figure A is a representation of time-multiplex channels and signals mapped within a 20 ms time period, figure B represents the total DL physical signals and channels. As in the experiment described in chapter 4, when NB-IoT is implemented in an inband or guard-band mode of LTE network with Multicast-Broadcast Single-Frequency Network (MBSFN) configuration, subframes which are part of LTE network and are not carrying NPBCH, NPSS, and NSSS are not identified by the SIB1 due to cyclic prefix mismatch. NB-IoT transmission principle in the downlink is based on the OFDMA technique that eliminates guard bands and allows the sub-channels to be closely co-located orthogonal, thereby saving bandwidth. The sink function enables the sub-carriers peak and zero-crossing points to match without interference or cancellations.

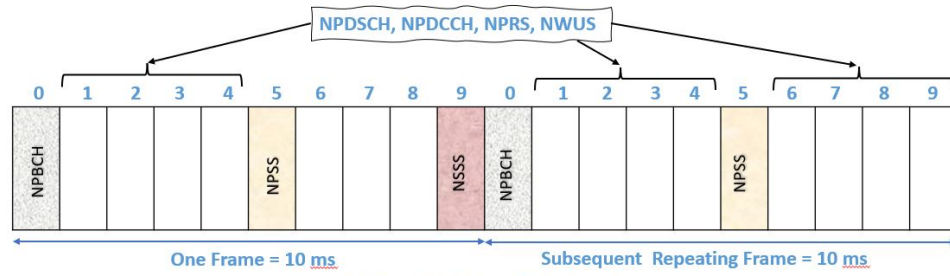


Figure (a) Time Multiplex of DL channels

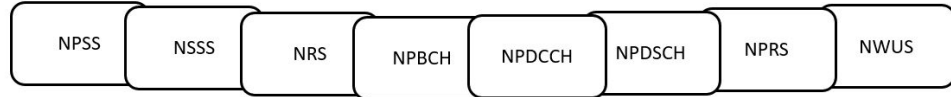


Figure (b) NB-IoT DL channels and Signals

Figure 3.7: NB-IoT DL Physical Channels/Signals and Time-multiplex over a subframe structure

Narrowband Referencing Signal

Narrowband Referencing Signal (NRS) helps the UE accurately demodulate DL channel signals and evaluate its measurements when in idle or connected mode. The general rules according to 3GPP and ETSI recommendations on where NRS is located within the subframe structure [232] include that for SIB1-NB, subframes 0 and 4 are used by the UE to transmit the NRS and in subframe 9 not containing NSSS. For SIB2-NB, NB-IoT NRS is transmitted in subframe 9 and in subframe 0 not containing NSSS. Subframes 1 and 3 are additional in the standalone and guard-band where NRS are present as well as in the valid DL subframes.

Narrowband Primary and Secondary Synchronisation Signal

NB-IoT synchronisation signals are essential for timely transmitting subframes and their repetitions at 80 ms intervals to properly detect UE cell information and identity over 504 Physical Cell Identities (PCIDs) and to connect to NB-IoT cell. Narrowband Primary Synchronisation Signal (NPSS), as shown in figure 3.7 is transmitted using subframe 5 of 10 ms periodicity and sequence pattern to avoid collision with LTE subframes. Its characteristics include 15 kHz subcarrier spacing, 180 kHz bandwidth and anchor carrier, which is the same as the Narrowband Secondary Synchronisation

Signal (NSSS). On the other hand, NSSS is transmitted using subframe 9 and 20 ms subframe periodicity and sequence pattern. Both NPSS and NSSS 1 ms subframes are made up of 14 OFDM symbols and 12 subcarriers.

Narrowband Wake Up Signal

Narrowband Wake Up Signal (NWUS) is a new feature added to higher NB-IoT releases to improve UE energy efficiency. As the energy consumption of UE is far lesser in the idle mode than in connected mode when the UE is scanning to determine whether it is paged. It is ideal for the UE to wake up from the idle mode to the connected mode only when there is paging occasions indicators but must be realised using a small amount of AWUS.

3.4.7 NB-IoT Uplink Transmission Channel

Most massive data transmission applications like sensor networks and management systems (use cases evaluated in this thesis) are uplink oriented, and the transmission is based on Single Carrier - Frequency Division Multiple Access (SC-FDMA) technique based on Frequency Division Multiplexing (FDM) in the LTE system. FDMA allows multiple UEs to share the same communication channel with each UEs allocated time-independent sub-channels, see figure 3.2.2.

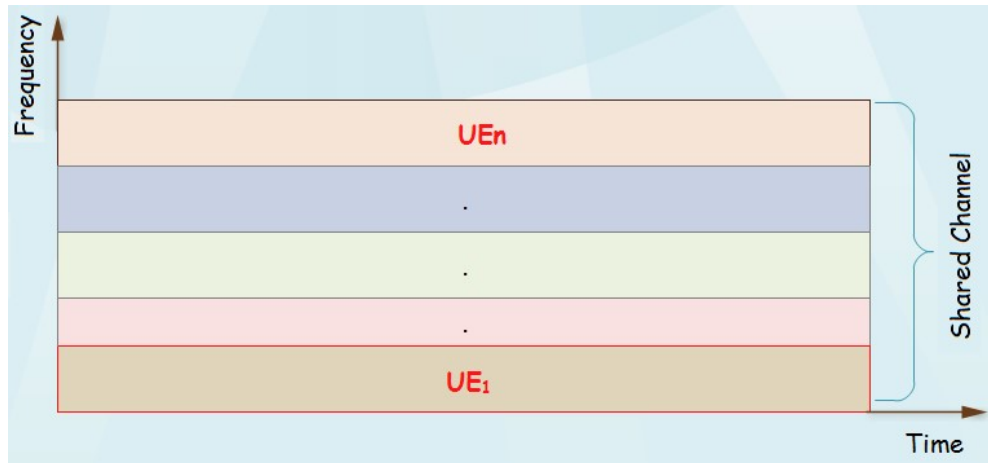


Figure 3.8: OFDM

On the other hand, SC-FDMA utilises time-dependent shared multiple sub-channels for efficient data transmission within a short period of time, see figure 3.9. The uplink modulation scheme is based on Quadrature Phase-Shift Keying (QPSK). QPSK allows the phase constant of the reference signal to be varied. The phase difference is a two bits digital value of the transmitted information in four possible outcomes (45 degree, 135, 225, 315). Figure 3.10 is an NB-IoT constellation diagram for 64QAM. When the constellation becomes denser, the signal strength and SNR required to decode the transmitted data will be higher. For the 64QAM in 6 bits/symbol, the resource block throughput will be equivalent to 1.08 MHz, the product of 168000 and 6 bits/symbol. For a forward error correction of 0.83, the actual throughput becomes 0.84 Mbps.

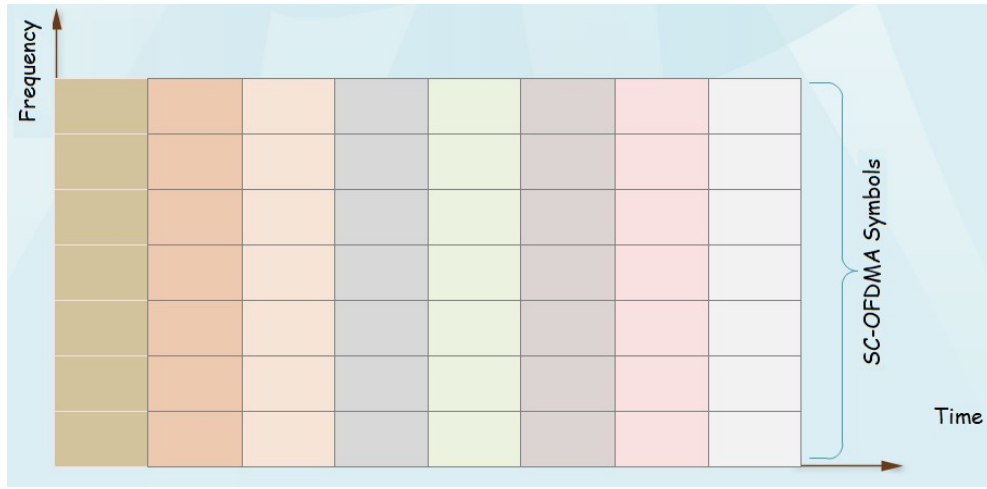


Figure 3.9: SC OFDMA

The subcarrier spacing of 15 kHz and 3.75 kHz supported in the uplink channel contributed to the increased number of UEs served by one eNB. During uplink transmission, subcarrier is dynamically allocated to the UEs by the core network. Within the same eNB, different EUs can have different subcarriers depending on their Signal to Interference Noise Ratio (SINR). Repetitive transmission is one of the methods of improving received signal strength and successful decoding of the transport block. The transmission of a single transport block can occur more than once but with an error correction mechanism that ensures that each transmitted block size with the same information is represented by different code bits. NB-IoT currently support only half-duplex

transmission. This means that the cost of duplexer is removed.

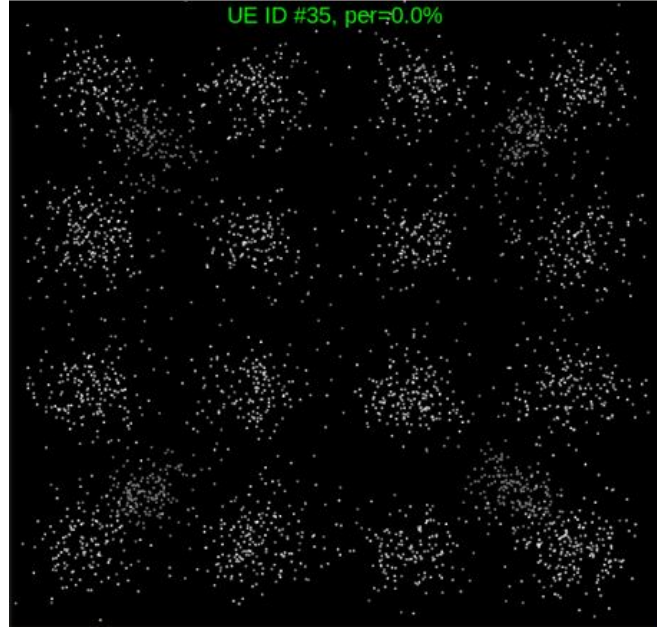


Figure 3.10: NB-IoT Constellation Diagram for 64 QAM

NPRACH

In NB-IoT, estimating the UE signal Time of Arrival (ToA) is one of the many vital steps when initiating a UE connection to an NB-IoT network. The received Narrowband Physical Random Access Channel (NPRACH) signal ToA is known as the round-trip propagation delay between the UE and the eNB. When more than one UE is involved in the transmission and reception of signals, without Timing Advance (TA), the orthogonality in the multiple UEs could be affected since SC-FDMA is used in the UL transmissions. For optimum performance, the LTE NPRACH preamble cannot be reused as NB-IoT NPRACH preamble because it has a smaller bandwidth and requires a Peak-to-Average Power Ratio (PAPR) close to 0 dB to improve efficiency and battery utilisation when based on a single-tone frequency hopping pattern. See figure 3.11 for the three NPRACH cell configuration formats used to support different classes of UEs in NB-IoT. Each of the NPRACH preamble units is made up of many symbols where each symbol consists of a CP and 5 symbols of single-tone frequency in the case of

format 0 and 1, while format 2 has only 3 symbols. The symbol group in a repetition unit and tone hopping range for formats 0, 1, and 2 are 4, 4, 6, and 12, 12 and 36, respectively. Aspects such as the cell radius could be improved using algorithms at the base stations. Refer to [242] for NPRACH performance and link budget improvement.

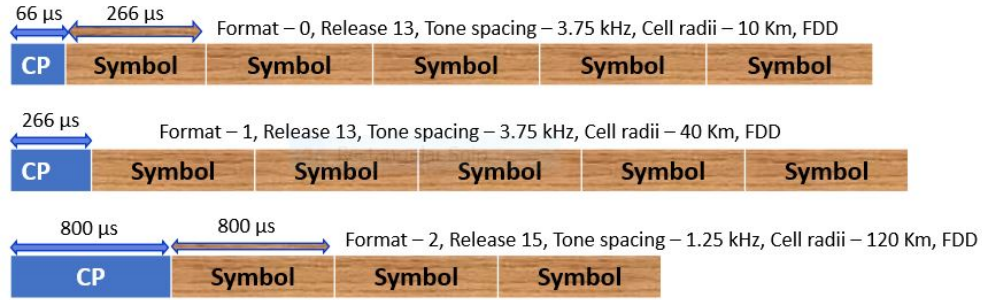


Figure 3.11: Three Formats of NB-IoT NPRACH Symbol Groups and their Respective Configuration Parameters

NPUSCH Resource Unit

Narrowband Physical Uplink Shared Control Channel (NPUSCH) is another important UL physical channel used in carrying HARQ, UL data or control information in NB-IoT transmissions between UEs and eNBs. NPUSCH, therefore, is a determining factor in the data-carrying capacity. NB-IoT has a maximum UE scheduled BW of 1 PRB, which would satisfy the data requirements for ultra low-end IoT applications in most use cases. Any increase in bandwidth for such power-constrained IoT devices would be of no significant benefit since 180 kHz PRB may never be fully occupied at low power. Table 3.5 shows the characteristics of different NPUSCH formats.

Table 3.5: NPUSCH Resource Unit Parameters

Features	Formats 1	Formats 2
Data	UL Transfer	HARQ Feedback
TBS (bits)	1000 (Cat-NB1)	2536 (Cat-NB2)
Modulation	SC-FDMA	SC-FDMA

3.5 NB-IoT Operation

NB-IoT has three modes of operation that utilises a maximum of 180 kHz frequency band for the uplink and downlink transmissions with subcarrier spacing options of 15 kHz or 3.75 kHz. 180 kHz of LTE resource is used to deploy NB-IoT in either guard-band or in-band modes. Similarly, 200 kHz of GSM resource is used to deploy NB-IoT in standalone mode as demonstrated in figure 3.12, creating a small guard-band of 10 kHz on each side of the band. The physical characteristics of uplink and downlink channels, as discussed in section 3.4.4 provide detailed explanations on how the 180 kHz is formed. An obvious advantage of this bandwidth range is that user equipment complexity is kept very low, but the support for real-time applications becomes unrealistic.

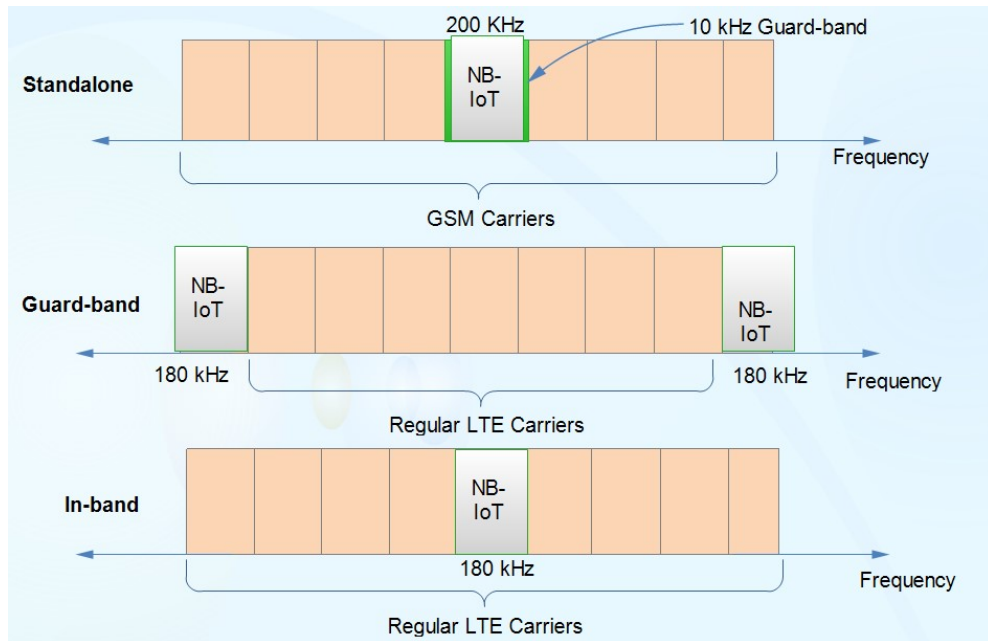


Figure 3.12: NB-IoT Deployment Modes

3.6 Security in Narrowband IoT

Security in NB-IoT relates to hardening of IoT products, securing communication links, complying with international standards, enforcing management policy, trusting third-party services and software, and implementing key management issues and embedded

security techniques. NB-IoT network comprises low-power IoT devices that require lighter security protocols and low processing units. The security of NB-IoT devices is critical at the perception level. The inefficiency of the devices means that attacks are imminent in the event of network traffic vulnerability. Following Min et al. [243] classification, NB-IoT security is classified in this thesis into three layers:

Perception Layer

This forms the edge part of the NB-IoT network. An attack on this part of the network can modify the program or steal the device information. This can occur in the form of reverse engineering, traffic analysis, node replication, message tampering, eavesdropping, etc. An attack can also occur through the wireless network connecting all the devices. [243] put the attacks into active and passive, with the active attack having far-reaching implications. Security measures such as encryption, authentication and integrity verification are commonly used. Stream cipher and block cipher are proposed for this layer by [158] to preserve the battery life and reduce processing delays at the terminals. The NB-IoT terminals were able to communicate directly with the NB-IoT enabled base station contrary to the multiple gateways that introduce routing problems in consumer-based IoT such as LoRa and Sigfox. The concern around this is the potential impact of pseudo-NB-IoT base stations in the system. Achieving safe bidirectional communication between base stations and NB-IoT terminals is still a major concern.

Transmission Layer

There is a significant difference in the complexity of this layer in both NB-IoT and other LPWAN. In NB-IoT, multi-networking and extra cost introduced by the gateways is eliminated. On the other hand, the single base station providing support for thousands of nodes means that node authentication and access control will give room for malicious code injection if not properly managed. Similarly, the total dependence on an open wireless network presents challenges such as network interferences, end-to-end authentication since the terminals are not user-assisted. Having an intrusion detection and protection system added to the base station will reduce these risks. [243] proposed

profile establishment of a certain group of nodes from previous, normal and abnormal operation scenarios.

Application Layer

The data generated by the heterogeneous network of NB-IoT devices are aggregated at the application layer. A great deal of these data originating from memory, power and processing constrained NB-IoT devices are not pre-processed at the node. This leads to the issues of identifying the devices and processing their big heterogeneous data logs, ensuring the authentication and integrity of the transmitted data, and managing how other devices are accessing the data.

3.6.1 Benefits of NB-IoT Technology

Narrowband IoT has a wide range of applications for consumer and industrial use cases. The broader benefits of using NB-IoT technology in monitoring and control applications as observed in this study are not limited to those shown in figure 3.13 and are explained in detail below:

- **High data rate:** The fraction of the channel capacity used for data transmission is known as the NB-IoT data rate and it is usually affected by the system's collision avoidance efficiency, channel utilisation, control overhead and latency [244]. NB-IoT has a reduced data rate by design to meet the low power consumption requirement of UEs. The effect of power consumption is low coverage area, but repetition technologies could enhance coverage. The UE capabilities mainly determine the maximum rate of transferring data over the NB-IoT communication channel. To determine the theoretical speed of data transfer using Shannon's Law, the bandwidth (180 kHz) and Signal to Noise Ratio (SNR) is determined by the power of the signal of up to 23dBm. The data rate for NB-IoT is usually up to 375 kbps and is subject to improvement with the emergence of new NB-IoT Releases. The effective theoretical downlink and uplink data rates are computed as the total number of information bits in the downlink and uplink

divided by the total transmission time, including overheads in the downlink and uplink, respectively.

- **Improved coverage:** For applications in the hard-to-reach locations such as oil rigs and platforms located miles away with localised gateways, coverage enhancement is achieved by using repetition transmission of up to 128 and 2048 for UL and DL, respectively but at a reduced data rate [9]. The extended indoor coverage of NB-IoT is within the range of 20 dB, and the maximum coupling loss of 20 dB is better than the LTE network. NB-IoT relies on 4G infrastructures to deliver broad coverage to indoor and dense locations with a reasonable response rate surpassing LoRa's reach of 20 km at low frequencies below 1 GHz. A software upgrade is one of the coverage enhancement options to achieve 100 km in exceptional use cases.
- **Latency insensitivity** - Latency is not a priority in the NB-IoT network, but the technology can accommodate a maximum delay of 10ms for error delivery in applications such as the alarm systems [245] and [246]. The delay in packet delivery is generally due to the transmission mode, the frequency of transmission, the timing, the process of cell acquisition, etc. Early Data Transmission (EDT) and Hybrid Automatic-Repeat-Request (HARQ) are new schemes developed to reduce repetition and guarantee successful transmissions.
- **Long battery life** - NB-IoT targets applications with a long battery life of up to 10 years at a maximum coupling loss (MCL) of 164 dB. The reduced power backoff also helps to improve battery efficiency. The UE goes into PSM in the inactivity period while attached to the base station and cannot be pinged by the eNodeB. The inactivity period of 413 days in Release 13 extends the battery life. In Extended Discontinuous Reception (eDRX) mode, the UE is inactive for a short period and synchronised to wake up by the sensor push data, an aspect controllable by the software implementation.
- **Possible firmware update** - Firmware Over-The-Air (FOTA) is still a challenging task to realise in the NB-IoT network. The downlink transmission rate

is low in recent designs and cannot support software updates. It goes further to affect the mobility of the devices as roaming will also be challenging to achieve.

- **Massive connectivity** - NB-IoT supports a massive number of UEs in one single carrier. With the help of the Resource Unit (RU) allocation, UEs are allocated to an RU where one UE occupies 3.75 kHz or 15 kHz UL bandwidth and 15 kHz for DL bandwidth.
- **Less complex and reduced cost** - The low-cost attribute of NB-IoT is attached to the UEs low storage capacity, the reduced frequency of operation, single antenna design and the modulation scheme limitations. The less complex UEs are the more packet delay, more channel interference and less estimation introduced in the transmission link.



Figure 3.13: Benefits of NB-IoT

3.7 NB-IoT Test Setup

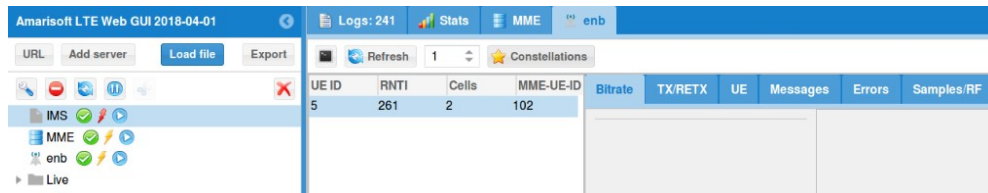
3.7.1 Mobility Management Entity (MME)

MME in NB-IoT test network is responsible for handling attach, detach, paging, authentication and authorisation of UEs as it accesses the network, manages the UE

communication mode, supervises handover procedure, and interact with the Serving Gateway (SGW), Packet Data Network Gateway (PGW) and Home Subscriber Server (HSS) interfaces [247]. It also supports relevant control plane functions in the LTE architecture regarding mobility management. Line of Sight (LoS) and LTE band interference affected the overall throughput of the transmission channel. To provide a software-defined configurable NB-IoT test network, the LTE core network interface (LTE MME) is attached to LTE eNB on the same processing machine using the S1 interface. A list of registered UEs registered and attached to the eNodeB is shown in 4.5. The pycom UE used for the implementation tolerated integrity checks and Advanced Encryption Standard (AES).

3.7.2 Long Term Evolution Evolved Node B (LTEeNB)

LTE eNB is a software-based base station that runs Stream Control and Transmission Protocol (STCP) on 5th generation or higher core processors configurable to support NB-IoT cells. The radio front end performs baseband signal conversion generated by the processor before interfaced with the LTE standard core network MME interface at S1 plane. With the 15 kHz and 3.75 kHz subcarrier spacing, single and multi-tone category NB1 and NB2 UEs are supported. The eNodeB is responsible for optimising the radio air interface by assigning the radio network temporary identifier to the UE to distinguish radio UEs and radio channels. The eNodeB also helps to reduce collisions in a multi-user transmission environment. As a precautional measure, UE antenna must be kept a few meters away from the base state (LMS7002M) antenna, and bands greater than band 7 are recommended if interference must be kept very low.



UE ID	RNTI	Cells	MME-UE-ID
5	261	2	102

Figure 3.14: eNB Interface

3.7.3 NB-IoT Web Interface

The NB-IoT's Graphical User Interface (GUI) is a Hypertext Transfer Markup Language (HTML5) used to monitor, analyse UE and Amarisoft data logs, physical layer statistics, and resource block allocation cell information and constellation information. The HTML5 is the LTE Web Interface that allowed the MME, eNB and UEs logs to be analysed in real-time through WebSocket. The real-time UE communication procedures were analysed using the WebSocket. Creating a web socket requires that the MME and eNB remote API be enabled and bound to a common address. The traffic between the LTE MME and eNodeB is monitored with Wireshark.

3.8 Narrowband IoT 3GPP Standardisation

The initial standardisation of NB-IoT for the Internet of Things was first actualised in the 3GPP standard Release 13. With the development of Low power Wide Area Network (LPWAN) IoT technology in 2014, NB-IoT was designed out of the LTE and GSM cellular systems to support 180kHz bandwidth for the uplink and downlink channel transmissions. The evolution of NB-IoT 3GPP standardisation Releases is discussed:

3.8.1 3GPP Standardisation Release 13

The network of non-human devices is referred to as Machine Type Communication (MTC) in the next generation of cellular networks. The 3GPP Release 13 standard spelt out the LTE and GSM support capabilities for MTC communications and the design targets of achieving long battery life, massive connectivity, greater coverage, deeper penetration and positioning enhancement [15]. NB-IoT development has evolved from the 3GPP Release 13 and 14 to improve standards such as positioning accuracy, data rates, coverage for MTC. Originally designed with the LTE modulation schemes, channel coding technique, and numerology features in communication type with low data rate, restricted mobility and latency requirements. Certain aspects of the standards like connected mobility mode were removed to reduce IoT module cost and complex-

ity [248]. The physical characteristics of NB-IoT technology is an enhanced version of parent LTE architecture. The frequency bands as used in the LTE network applies in NB-IoT with an exception in the standalone mode of operation as discussed in section 4.3.1. The general frequency bands in the 3GPP Release 13 documentation is presented in table 3.6. A license issued by government spectrum regulatory agencies in every country is required before transmitting in these bands (licensed spectrum) [249]. The allocations of the band vary from one country to another. In the UK, bands 1, 3, 7, 20, and 32 in the lower part of the LTE bands is used because of their indoor penetration capabilities.

Table 3.6: NB-IoT Frequency Bands [14]

NB-IoT Band	Uplink Band (MHz)	Downlink Band (MHz)
B1	1920-1980	2110-2170
B2	1850-1910	1930-1990
B3	1710-1785	1805-1880
B5	824-849	869-894
B8	880-915	925-960
B12	699-716	729-746
B13	777-787	746-756
B17	704-716	734-746
B18	815-830	860-875
B19	830-845	875-890
B20	832-862	791-821
B26	814-849	859-894
B28	703-748	758-803
B66	1710-1780	2110-2200

3.8.2 3GPP Standardisation Release 14

NB-IoT Release 14 standard offered the opportunity to support more IoT devices in one eNB by enhancing existing features and introducing new functionalities. To provide an enhanced user experience in NB-IoT applications and extend the applications to other use cases, 3GPP LTE Released 14 was introduced in 2017. The new features include coverage enhancement, positioning accuracy, improved data rates, multicast capability, lower power class features and non-anchor carrier support [15]. NB-IoT

is also considered for 5G technology as a result of these enhancements and others introduced in the LTE Release 15. The LTE Release 14 features are discussed in detail with respect to the following NB-IoT performance characteristics:

Increased UL and DL Data Rates

The data rate in the Release 14 is increased to improve features such as the latency, which is down prioritised in Release 13, where the UL and DL data rate is 62.5 kbps and 25.5 kbps respectively [15], [250]. An example of UL and DL transmissions obtained in the NB-IoT testbed described in chapter 4 is shown in figure 3.15. The data rates for these UL and DL transmissions are far below the values presented above. In Release 14, the Transport Block Size (TBS) and NPDCCH scheduling of (NPDSCH and NPUSH) are the factors that affect the data rate. The maximum TBS in Release 14 is 2536 bits [1], [15] in both the UL and DL. The single HARQ process in Release 14 increased the peak data rate for both the NPDSCH and NPUSH scheduling to 79 kbps and 106 kbps, respectively. Two HARQ processes peak data rate for NPDSCH and NPUSH is 127 kbps and 158.5 kbps respectively [15]. Figure 3.15 show the UL and DL data rates for sending a few bytes of sensor data over an NB-IoT Release 13 network. Full analysis of the test result is presented in subsection 5.6.2.

Device Firmware Multicast Update

Multicast is introduced in NB-IoT to efficiently deliver data transmission for software, tasks, and command updates to support large IoT UEs. Addressing data to a group of communicating devices is an important function in an IoT network. Multicast is a concept developed to improve transmission efficiency and resource utilisation when addressing a group of user equipment in a single transmission. Firmware update is an excellent example of multicast services, and the feature is reduced in NB-IoT Release 13. The introduction of Single Cell Point to Multipoint (SC-TMP) in the Release 14 enables group-based update messages to be delivered through the Multimedia Broadcast Multicast Service (MBMS) [15], [250]. The implementation of SC-TMP is in the NPDSCH based on Single Cell Multicast Control Channel (SC-MCCH) and Single Cell

```

21:44:55.557 [IP] UL      - len=44 IP/TCP 192.168.3.2:59619 > 192.168.3.1:8000
0000:  45 00 00 2c 00 01 00 00  ff 06 34 77 c0 a8 03 02  E.,.....4w...|
0010:  c0 a8 03 01 e8 e3 1f 40  00 00 19 6d 00 00 00 00  .....@...m....
...
21:44:55.558 [IP] DL      - len=40 IP/TCP 192.168.3.1:8000 > 192.168.3.2:59619
0000:  45 00 00 28 00 00 40 00  40 06 b3 7c c0 a8 03 01  E..(..@..|....
0010:  c0 a8 03 02 1f 40 e8 e3  00 00 00 00 00 00 19 6e  .....@.....n
...
21:44:55.558 [NAS] DL 0066 ESM: ESM data transport
0000:  27 6b 18 23 d6 05 52 00  eb 00 28 45 00 00 28 00  'k.#..R...(E..(
0010:  00 40 00 40 06 b3 7c c0  a8 03 01 c0 a8 03 02 1f  .@..@..|.....
0020:  40 e8 e3 00 00 00 00 00  00 19 6e 50 14 00 00 06  @.....nP....
0030:  eb 00 00                                     ...
Protocol discriminator = 0x7 (EPS Mobility Management)
Security header = 0x2 (Integrity protected and ciphered)
Auth code = 0x6b1823d6
Sequence number = 0x05
Protocol discriminator = 0x2 (EPS Session Management)
EPS bearer identity = 5
Procedure transaction identity = 0
Message type = 0xeb (ESM data transport)
User data container:
  Length = 40
  Data = 45 00 00 28 00 00 40 00 40 06 b3 7c c0 a8 03 01 c0 a8 03 02 1f 40
21:44:55.558 [S1AP] TO 127.0.1.1:39681 Downlink nas transport

```

Figure 3.15: UL and DL transmissions in Release 13 NB-IoT network

Multicast Traffic Channel (SCMTCH). Multicast with Fixed Guarantee (MFG) and Multicast with Priority (MP) as proposed in [251] are solutions for handling resources limitations in NB-IoT for multicast transmissions since NB-IoT is deployed on a single PRBs, it limits the number of resources available for MBMS to unity. Both strategies minimised the impact of multicast transmissions on unicast in the downlink channel when the number of UEs is high. However, MP is faster in infrequent multicast sessions with less impact on the unicast transmission.

Nonanchor Carrier Support

Multi-carrier enhancement is used to increase the capacity of the constrained services of NB-IoT in a carrier of 200 kHz bandwidth. To manage the system information and synchronisation signalling and increase capacity in the DL resources, one anchor carrier is dedicated for signalling and non-anchor carriers for data traffic. Signalling such as paging and random access directed to the non-anchor carrier by the eNB affects NB-IoT network capacity. The enhancement in Release 14 allows paging and random access on the non-anchor carrier without impacting on the capacity [15]. According to the

3GPP project on scenarios and requirements for next-generation access technologies, Release 14 is also designed for 5G environment to support 1 million devices per km² while the capacity for Release 13 is 60,680 devices per km² [1]. The Access Arrival Time (AAT) per second for both versions is within 6.8 and 112.2, respectively. To keep the device access arrival time and the rate of collision low, large amount of the radio access resource must be dedicated to NPRACH. The effect of this is that a large amount of UL resources is already occupied. The preamble request is probabilistic in nature and can be modelled. The deployment options for anchor and non-anchor multi-carrier overhead for Release 13 and 14 is shown in table 3.7.

Table 3.7: Multi-carrier Overhead [15]

Carrier	Standalone	Guard-band	In-band
Release 13 anchor	40	40	59
Release 14 anchor	44	44	62
Release 13 non-anchor	10	10	38
Release 14 non-anchor	10	10	38

Increased Positioning Accuracy

This part of the improvement presents an opportunity for increased use of NB-IoT across different sectors for device tracking. Positioning accuracy is a vital aspect of IoT and applicable to most use cases such as asset tracking, pipeline and environmental monitoring, wearable and smart agriculture. NB-IoT Release 13 can only associate UE to the serving cell, while Release 14 provides enhanced Serving Cell Identity (SCID) measurement and Observed Time Difference of Arrival (OTDOA) based on Narrowband Positioning Reference Signal supporting DL OTDOA [252]. The two Release 14 positioning improvement methods have been conducted for NB-IoT; Enhanced Cell Identity (eCID) and Observed OTDOA. The time advance (TA) eCID is a round-trip measurement between the eNodeB and the UE. The value is used to compare the position of UE to the serving cell. The OTDOA uses the measurement of Time of Arrival (ToA) on a set of DL Narrowband Positioning Reference Signals (NPRSs) from a set of time-synchronised eNodeBs serving the UE.

New Energy IoT Devices

Release 14 supports a power class of 14 dBm to enable the use of small cell batteries in future NB-IoT deployment. This improvement of the Release 13 helps to reduce the Power Amplifier (PA) drain current, which negatively affects the UL coverage and the maximum coupling loss (MCL) to 155 dB. UEs like Fipy is a Release 13 device that supports 20 and 23 dBm power classes. In Release 14, the maximum power class is now reduced to 14 dBm and must achieve smaller form factors and power consumption at a small cost. eDRX and PSM are other power-saving mode capabilities in NB-IoT.

Mobility Enhancement

NB-IoT mobility capabilities are limited to Radio Resource Control (RRC) 's ability to re-establish connection with an appropriate cell when a UE moves out of a cell coverage area through cell selection. The connection re-establishment is achieved through the user plane data support. The handover feature is totally not supported, and mobility needs create issues such as radio communication link failure when a UE moves from one serving cell to another. Release 13 support only stationary UEs, and in addition Release 14 supports UEs with low mobility [15].

NB-IoT Frequency Bands

The 3GPP Release 14 specifies the sets of frequency bands that support NB-IoT devices operating in HD-FDD duplex mode. The UL and DL operating frequency bands for the eNodeB and EUs are shown in figure 3.8. The support for these bands is different in different regions, see table 3.8.

Table 3.8: NB-IoT Release 14 Frequency Bands [16]

NB-IoT Band	Uplink Band (MHz)	Downlink Band (MHz)
B11	1427.9-1447.9	1475.9-1495.9
B25	1850-1915	1930-1995
B31	451.5-457.5	462.5-467.5
B70	1695-1710	1995-2020

3.8.3 3GPP Release 15

The 3GPP Release 15 optimises the Early Data Transmission (EDT) support during Radio Access (RA) connection procedure for NB-IoT and LTE. Data transmission in Release 13 and 14 is only possible after the RA procedure is completed. EDT mechanism enables transmission in the uplink channel within the RA connection procedure with a latency of 3 seconds and battery life of 3 years higher than in Release 13 [253]. The connection setup time and signalling overhead are reduced. This standard has the advantage to reduce latency and improve the battery life of IoT devices deployed in limited network areas. The procedure in EDT transmission is that the IoT module initially indicates the intention to transmit data during the RA procedure by using the special (N)PRACH preamble dedicated to EDT by the evolved base station in the SIB. The eNB transmits the maximum TBS for the data in EDT. The frequency bands added to the 3GPP Release 15 for NB-IoT applications is shown in table 3.9 [17].

Table 3.9: NB-IoT Release 15 Frequency Bands [17]

NB-IoT Band	Uplink Band (MHz)	Downlink Band (MHz)
B4	1710-1755	2110-2155
B14	788-798	758-768
B71	663-698	617-783
B72	451-456	461-466
B73	450-455	461-465
B74	1427-1470	1475-1518
B85	698-716	728-746

3.8.4 3GPP Release 16

NB-IoT in 3GPP Release 16 covers the enhancement of network operation and efficiency in the 3GPP standardisation Release 15 5G New Radio (5G-NR). The summary of enhancements in the existing features includes carrier aggregation, Multiple-Input Multiple-Output (MIMO), beamforming, dynamic spectrum forming, and UE power-saving mode [254]. NB-IoT new enhancements in the Release 16 standard are as follows:

- NR used as a fiber substitute for integrated network access and backhaul.

- Network management tool for self-organising ability, link and performance reporting.
- Able to coexist with NR through inter-RAT cell selection.
- Mobility and positioning enhancement
- Improved multi-carrier operation
- Scheduling enhancement to allow multiple downlink and uplink transport block
- Improved transmission efficiency and preconfigured resources.
- Improved UE enabling group wake up signal, early data transmission, and power saving.

3.8.5 3GPP Release 17

The scope of 3GPP Release 17 includes enhancements to existing features and new features that address different vertical industrial needs to support low latency, time-sensitive, NB-IoT applications and low capable NR devices. It will be most useful in the eMBB, uRLLC, and mMTC use cases with very high data traffic [255]. The support for non-terrestrial access in 5G NR enhancement enables NB-IoT, and eMTC deployment using satellites and High Altitude Platforms (HAPs) [256].

3.9 Narrowband Fidelity (NB-Fi)

Narrowband Fidelity (NB-Fi) is an open standard LPWAN bidirectional communication protocol developed by WAVIoT for IoT, M2M, and industrial IoT applications to effectively utilise the radio spectrum. NB-Fi has been approved by the Federal Agency for Technical Regulation and Metrology (Rosstandart) for national use in utility metering and other applications such as water, gas, and heat metering in Russia. It was developed under the project for the Russian communication standard for the Internet of Things [120]. NB-Fi protocol is designed to handle data exchange between the end

devices and the server and must to be end-to-end encrypted, guaranteeing confidentiality and integrity [11]. NB-Fi operates in the unlicensed frequency spectrum at devices power of between 25 to 100 mW, low SNR, high noise immunity, distance of up to 10 km, battery of 10 years. It supports adaptive data rates. This means efficient data transmission by the 4.3 million end devices supported in a single base station. NB-Fi uses encryption system to provide end-to-end security. Each NB-Fi end device generates 256-bit root key used by diversification function to further generate two other keys for the uplink and downlink transmissions. See Figure 2.2 for a comparison of NB-Fi with other LPWAN technologies.

Chapter 4

Narrowband IoT Testbed for Industrial Internet of Things

4.1 Introduction

The [Internet of Things \(IoT\)](#) is the general term for interconnecting physical and virtual objects interacting to achieve a common goal, such as in the monitoring of physical phenomena and control of mission-critical infrastructures. The recent paradigm shifts in industrial communication technology necessitate that industrial parameters such as temperature, pressure, vibrations and leaks should be remotely monitored using reliable wireless technologies. Wireless Technologies can provide a wide range of new service capabilities to improve industrial operations and meet other business needs. Examining the IoT wireless technologies proposed to enable such interconnections, factors such as the infrastructural interoperability, cost of deployment, security and mobility requirements are considered when determining the type of wireless technology to deploy. [Narrowband Internet of Things \(NB-IoT\)](#) as an enabler of such services with massive connectivity options, good power utilisation, long-distance transmission, and the higher data throughput in 4G and 5G applications has not been explored to a great degree . In this chapter, an in-depth practical approach to setting up an NB-IoT

Major part of this chapter is a conference paper presented at the 2020 IEEE International Symposium on Networks, Computers and Communications (ISNCC20), Montreal, Canada — 20-22 October

test network is fully presented alongside initial findings on its power utilisation, security, and latency performance results involving Cat-NB1 Pycom devices and Amarisoft LTE/NB-IoT base station. The findings provide the necessary security requirements, the test network power and latency performance and the global spectrum deployment options for a potential private licensed NB-IoT network. For interested readers, refer to chapter 5 for a detailed comparison of NB-IoT and LoRaWAN networks performance.

4.2 NB-IoT Landscape

The Internet of Things (IoT) is a prime technology for connecting huge numbers of electronic devices “things” remotely. Wi-Fi, Zig-bee, Bluetooth, Sigfox, LoRa, 4G/LTE and 5G are a few of the wireless technologies used for IoT [257]. Some of the reasons they are preferred over wired technology are as a result of the reduced installation/-maintenance cost and mobility requirements but are susceptible to vulnerabilities at the Radio Frequency (RF) interface. IoT technology came to light in the early-2000 and has significantly improved with the introduction of smart devices in mid-2007. It is projected to achieve a capacity of 50 billion nodes in 2020 [258] and over 100 billion devices in 2025 [256]. Furthermore, a simulation study by Ericsson claimed that NB-IoT could provide support for 200,000 nodes per cell [259]. The realization of such a capacity is made possible following the global deployment of IPv6 communication protocol [30] and other innovations.

Industrial automation, remote processing and monitoring control, telemetry, data management and protection are few areas where these innovations are already taking place in different magnitudes. “Industrial machinery, transportation monitoring, logistics/asset tracking, healthcare, intelligent buildings, smart agriculture and smart metering” are specific sectors where IoT is the catalyst for the development [260]. IoT has generally improved beyond the level where only mobile devices and computers were linked to the internet [25]. Internet connectivity now includes ‘things’ such as industrial sensors and actuators, home equipment, and personal handheld devices.

2020. Available at <https://ieeexplore.ieee.org/document/9297221>

4.3 Technology for NB-IoT Testbed

Narrowband Internet of Things (NB-IoT) is a Long-Term Evolution (LTE) based Radio Access (RA) technology for LPWAN IoT connectivity and services described in section 3.3. It is part of the new RA cellular technology in the Third Generation Partnership Project (3GPP) Release 13, 14, 15, 16 offerings and 17 Release due in 2021 [249]. NB-IoT is increasingly used to support machine-type legacy Global System for Mobile Communication (GSM), Long Term Evolution (LTE) and 5th Generation (5G) communication systems. The choice of NB-IoT for creating a network of sensors and other ultra-low IoT devices are based on the enhanced coverage, deployment flexibility options, deep penetration and reduced energy consumption (Power Save Mode (PSM) and Extended Discontinuous Reception (eDRx)) and the cellular IoT Evolved Packet System (EPS) optimisation. The flexibility in the deployment options come from the wide range of frequency bands LTE networks can be deployed. For instance, the minimum frequency of 180 kHz requirements for both uplink and downlink makes it possible to use one GSM carrier (200 kHz) or one Physical Resource Blocks (PRBs) existing within an LTE network for NB-IoT deployment [261]. The number of resource blocks reduces as channel bandwidth reduces. In the LTE downlink channel applicable to NB-IoT, bandwidths (MHz) of 1.4, 3, 5, 10, and 20 have 6, 15, 25, 50, 75, and 100 resources blocks per slot, respectively.

NB-IoT is the promising class of licensed LPWAN for licensed or unlicensed small data transfer protocols. LoRaWAN is an open and LoRa Alliance standardised LPWAN. LoRaWAN features in remote monitoring applications have been investigated within the same research group; Centre for Dynamic Intelligent Communication (CID-COM), University of Strathclyde. The study, which used a prototype fault passage indicator to monitor voltage faults along an 11kv power line, shows that LoRaWAN was suitable for remote applications of low data rate. NB-IoT was identified as a step further from LoRaWAN and Sigfox [93]. The 2019 Berlin LoRa Alliance event further and reveal how LPWA is enabling the internet of things across all sectors [262].

Comparing the coverage and other capabilities of licensed and unlicensed LPWAN

technologies, [263] and [264] demonstrated that NB-IoT has good penetrating power in all deployment modes with a maximum coupling loss performance of 164 dB. It also has better coverage, including indoor applications. In addition to other advantages, these have increased NB-IoT applications and services among Mobile Service Providers (MSP) and Network Professionals (NP) as a suitable protocol for the emerging IoT market. It is a clear indication that NB-IoT, which continues to evolve from GSM/LTE/5G networks, enabling good connectivity and services for a wide range of devices, is a technology of future IoT networks.

NB-IoT can be deployed by a software upgrade to an existing GSM and LTE network infrastructure, reallocating available frequency bands possibly from GSM, and the use of features in the new 5G design. The global deployment of NB-IoT, as shown in Figure 5.6 is facilitated by the mobile network provider within the regions around the world. A standalone NB-IoT network has been launched in Florida by Puloli using the 700 MHz A-Block spectrum to provide services to utilities and other parallel industries. Other identifiable use cases include the sea, agriculture, smart city, smart metering and tracking with major equipment manufacturers to improve network security [9] majorly. NB-IoT application in the streams of the oil and gas sector can track and reduce the number of wastages, but its global visibility is comparatively very small with other technologies.

There is an increasing interest in the Extremely High frequency (EHF) band with the advent of 5G. Facebook and Starry, according to Alasdair Gilchrist [265] launched broadband internet services on the 60 GHz frequency in the urban and rural areas using mesh network and point-to-point topology, respectively. Shorted frames allow very low latency at such a high frequency but at a distance less than 1 km on a clear line of sight, with poor penetration power and high fading due to rain and other environmental conditions. The health implications of using such high frequencies and power for IoT use cases is an area that needs much investigation.

4.3.1 NB-IoT Deployment Modes

Narrowband IoT has three modes of deployment options as presented in Figure 5.5. The standalone deployment, which is considered the most expensive, requires the installation of new network resources like in the case of GSM and skills to develop and deploy. On the other hand, NB-IoT deployment within an LTE network can be in either the in-band or guard-band mode, hence, having the same LTE design features such as security. The guard-band and in-band deployment options uses the 180 kHz single PRB of LTE core network and enables the support for Narrowband Uplink Shared Channel (NPUSCH) allocation. Narrowband Physical Downlink Shared Channel (NPDSCH) and the NPUSCH carries data packets for downlink (DL) and uplink (UL) respectively.

Standalone

Independently deployed as a dedicated carrier using spectrum greater than the required 180 kHz frequency bandwidth. GSM wireless access networks and satellite communication systems may be used to deploy NB-IoT in the standalone mode. This is achieved by refarming certain aspect of the frequency spectrum to include 200 kHz and 100 kHz guard-band for different operators and the same operator respectively deploying both GSM and LTE [266].

Guard-band

It is also possible to deploy NB-IoT within the existing LTE networks using the LTE guard-band. The LTE channel bandwidth is not fully occupied. The 5% unused resource blocks guard bands are used to deploy NB-IoT between LTE carriers.

In-band

Deployed in the PRB of an LTE carrier wave. Free LTE PRB is reused, making the deployment more advantageous for maintenance [267]. This is the operational mode on which this study was carried out. However, similar testing was also performed in standalone and guard-band modes.

4.4 Related Work

Narrowband IoT technology is new and the aspects regarding functional testing and deployment are few and not readily available. Unlicensed LPWAN technologies, such as the Sigfox and LoRa, were the preferred choices for communication infrastructure requiring good coverage, smaller data rate transmission and has been available longer than NB-IoT. Sigfox and LoRa are exempt from licensing and operate in the Industrial, Scientific and Medical (ISM) radio band of 868 MHz in Europe. However, studies exist with frameworks of enabling unlicensed NB-IoT (NB-IoT-U) in the Sub-1GHz [246] and [268]. Security was their greatest challenge until the emergence of NB-IoT in the 3GPP Release 13, initiated by Huawei and Vodafone in 2014 as a cellular Narrowband Machine to Machine (NB-M2M) technology. The 3GPP specifications provides important security and other attributes in the implementation of the NB-IoT network. The list is not limited to key type, key management, data freshness, authorisation, availability, data integrity, data authentication and confidentiality.

Literature focusing on NB-IoT deployment options are few and most of the studies are currently pilot testing. Vodafone, Huawei and Deutsche Telekom have test beds in various locations [256] globally. Three, a UK MNO is also running pilot LPWA network tests to help utilities improve their service performance, detect faults and determine their carbon footprint [269]. These studies have raised research questions in the aspects of power utilisation, battery life, price of the modules, the data-carrying capacity, coverage issues, radio frequency management, mobility management, scheduling, backward compatibility and a host of other variables [9].

However, work is in the area of extending NB-IoT coverage [270] and [263]; co-existence of NB-IoT in LTE environment [271] and [130]; NB-IoT design and specifications [272] and [261]; and applications [273], [249] and [261]. The effect of LTE and NB-IoT to exist in one cellular network resource as Junghoon and Hoyoung investigated [271], identified a significant interference and a consequence of a reduction in the network performance. The study found that the use of 15 kHz and 3.75 kHz subcarrier frequencies do not eliminate interference completely but seem to be more pronounced

in the 3.75 kHz as against the LTE 15 kHz standard.

4.5 methodology

NB-IoT test network setup, see figure 4.1, employed a functional Amarisoft wireless protocol stack based LimeSDR (LMS7002M) hardware using test network specification shown in table 4.1. See figure 4.2 as the radio front-end to generate the standard core LTE and NB-IoT base station physical signals on the same processor. It is a Multiple-Input Multiple-Output (MIMO) transceiver based on Field-Programmable Radio Frequency (FPRF) for hardcore Digital Signal Processing (DSP), low cost and wide frequency (100 kHz to 3.8 GHz) module that runs on Snappy Ubuntu Core. The Pycom IoT module (Fipy) attached to a Pycom Pysense board and Expansion Board 3.0 is the IoT Node. The Fipy is a new independent node scale IoT project-based board programmable in the Visual Studio Code and Atom. It has Cellular, WiFi, Sigfox, Lora, Bluetooth and LTE CAT M1/NB1 wireless technology implementation options.

To obtain the parameters needed to configure the Random Access Channel (RACH) procedure, the UE scans and detects synchronisation signals and reads System Information Block (SIB). The Narrowband Primary Synchronisation Signal (NPSS) for timing and modulation information and Narrowband Secondary Synchronisation Signal (NSSS) for cell information of the base station. The decoding of Memory Information Block (MIB) enable the UE to identify the System Frame Number (SFN), Hyper Frame Number (HFN), UL and DL information. With this information, the frequency hopping pattern is generated at the UE which is then used to identify the frequency carrier that Narrowband Physical Random Access Channel (NPRACH) lies and which is used to perform initial access to the NB-IoT network and request transmission resources. For the UE to know the selected carrier and the transmission time allocated to Narrowband Physical Random Access Control Channel (NPRACH), UE is configured for DL transmission, the Narrowband Physical Downlink Shared Channel (NPDSCH) and Narrowband Physical Uplink Shared Channel (NPUSCH) for UL transmission. The UE decodes the Memory Information Block (MIB) for scheduling information and Sys-



Figure 4.1: NB-IoT Practical Experimental Setup

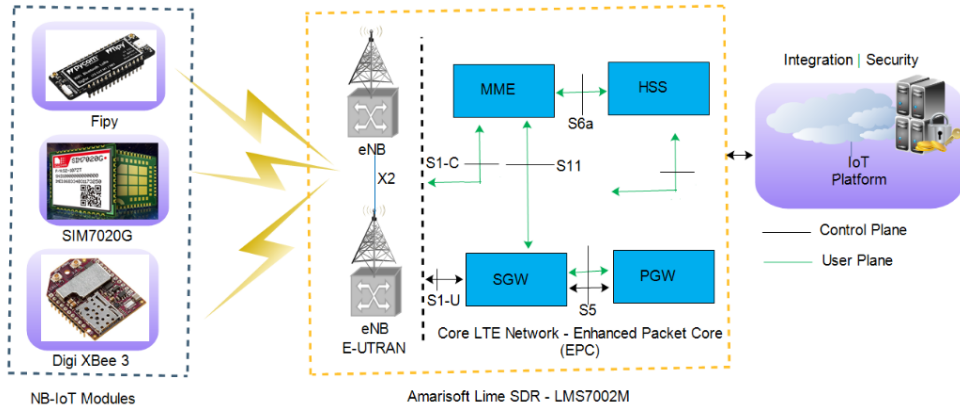


Figure 4.2: NB-IoT Experimental Design

tem Information Block 1 (SIB1) for system information types (mapping, periodicity, window length, etc.) respectively and broadcasted at intervals, see figure 4.3

While the NB-IoT EPC exchange control messages with the NAS of UEs and forward IoT data to the platform for processing, the eNB communicates the network

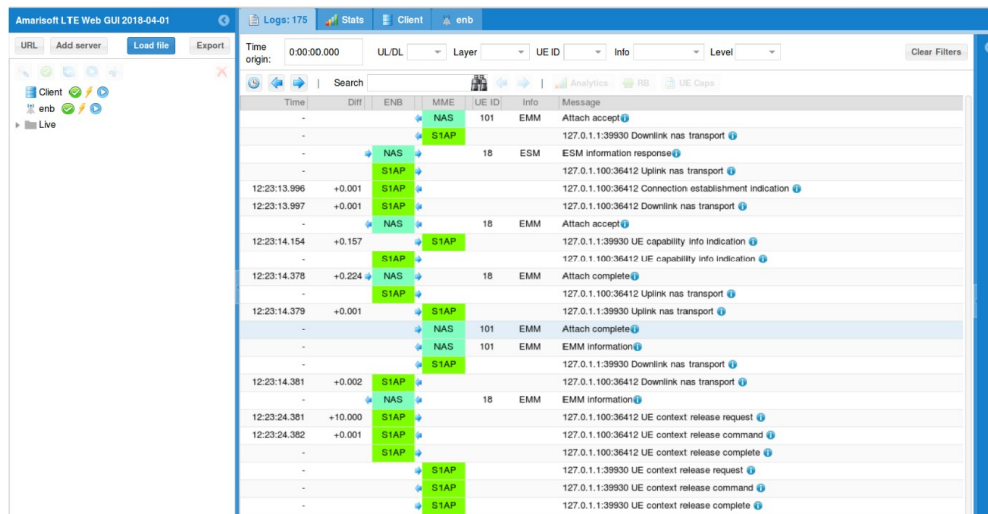


Figure 4.3: NB-IoT Network Attachment Procedure

access messages to the higher layer and handles cell management via the S1 interface. The IoT platform in figure 4.3 is the core network data visualisation interface for varied UEs, the eNB and core network (MME) data analytics and communication procedure. Implementing 3GPP NB-IoT Release 13, the network performance can be measured in terms of the extended indoor coverage, increasing the number of IoT devices supported in a cell-site, reducing the complexity of adding more devices to the network, improving the power utilisation and overall latency [245]. Cost, power utilisation and latency of NB-IoT is the focus of this chapter. The 3GPP Release 14 introduced enhanced location tracking, support for multicast downlink transmission, new power class(es) for UEs, multi-carrier operations and non-anchor carrier support [274]. The 3GPP release 15 optimises the support for EDT during the RA connection procedure. Release 16 covers the enhancement in the 3GPP standardisation Release 15 5G New Radio (5G-NR) to include the self-organising ability, the ability to coexist with NR, mobility, scheduling, transmission and equipment enhancement.

4.5.1 Industrial NB-IoT Devices

The SIMCom, Fibocom and Digi NB-IoT modules are other flexible cellular hardware IoT devices with good NB-IoT performance metrics such as data throughput and bat-

Algorithm 1. NB-IoT Network Attach and Data Transfer Procedure

```

1. Import Libraries
2. from network import LTE
3. import pycom
4. import time
5. import socket
6. import sys

7. lte = LTE()
8. def addBand(band,lte):
9.     if band in ['28']:
10.         lte.send_at_cmd('AT+CFUN=0')
11.         lte.send_at_cmd('AT^RESET')
12.         lte.send_at_cmd('AT!="clearscanconfig" ')
13.         if band == '28':
14.             lte.send_at_cmd('AT!="RRC::addScanFreq band=28 dl-earfcn=9435" ')
15.         else:
16.             flagband = True
17.         else:
18.             flagband = False
19.     return flagband
20.     band = input("28 ")
21.     flagband = addBand(band,lte)
22.     lte.send_at_cmd('AT+CGDCONT=1,"IP","internet" ')
23.     lte.send_at_cmd('AT+CFUN=1')
24.     lte.attach()
25.     while not lte.isattached():
26.         time.sleep(0.1)
27.     lte.connect()
28.     while not lte.isconnected():
29.         time.sleep(0.1)
30.         flag = False
31. s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
32. address = ' IP address'
33. port = 8000
34. try:
35.     s.connect((address,port))
36. except OSError:
37.     message=" "
38. s.sendall(message)
39. print(s.readall())
40. while amount_received < amount_expected:
41.     data = s.recv( )
42.     amount_received += len(data)
43.     print ("received %s" % data)
44. s.close()

```

Figure 4.4: NB-IoT Network Attach and Data Transfer Procedure

tery life. The bands, security supported, data rate and price of each device compared with Fipy is shown in Table 2 4.2 outweighing others in price, security capabilities and data rate. The Very High Frequency (VHF) bands are suitable for IoT implementation

Table 4.1: Test Parameters

Test Parameters	Values
Sample rater	30
Dec-inter	2
Rx-power	-15 dBm
Tx-power	-3 dBm
Bandwidth	180 kHz
Frequency Carrier	Band 28 (dl-carfcn=9435)

where commercial mobile network coverage is hard to reach. Access to such business spectrum is available on the [55.75625-60](#), [62.75625-64.8](#), [64.8875-66.2](#), [70.5-71.5](#) and [80.0-81.5 MHz](#) bands in the UK. Vodafone has already commercialised NB-IoT network using the 800 MHz band in the west part of the UK [269]. The bands in green are the current global deployable bands supported by the devices.

Table 4.2: Table of NB-IoT Devices

Devices	Bands	Support Features	Price Jan.2020
Pycom (Fipy)	1 , 2 , 3 , 4 , 5 , 8 , 12 , 13 , 18 , 19 , 20 and 28	300 kbps DL and 375 kbps UL in 1.4 MHz, 40 kbps DL and 55 kbps UL in 200 kHz, SSL/TLS 1.2, WPA, AES	\$ 46.89
Digi (Digi XBee3)	1 , 2 , 3 , 4 , 5 , 8 , 12 , 13 , 18 , 19 , 20 , 25, 26, 28 and 30	Multiple band, up to 27.2 kbps DL and 62.5 kbps UL	\$69.00
SIMCom (SIM7020G)	1 , 2 , 3 , 4 , 5 , 8 , 12 , 13 , 17 , 18 , 19 , 20 , 25, 26, 28 , 66, 70, and 71	Global bands, 3GPP Release 13, 14, 150 kbps UL, 100 kbps DL, TLS	\$69.00
Fibocom (M910-GL)	1 , 2 , 3 , 4 , 5 , 8 , 12 , 13 , 18 , 19 , 20 , 26 , 28 and 39 on TDD	32 kbps DL/70 kbps UL, eSIM, IPv6, TCP, UDP	\$109.00

4.6 Results and Discussions for a Single IoT Module

The NB-IoT test network performance presented below is analysed based on the following subheadings:

4.6.1 Mobility Management Entity (MME)

The MME has the Serving Gateway (SGW), Packet Data Network Gateway (PGW) and Home Subscriber Server (HSS) in-built. For the data rate of 151 Mbps for 20 MHz cell in LTE, eNodeB resources of 200kHz are shared among the IoT modules supporting all operation modes. Line of Sight (LoS) and LTE band interference affected the overall throughput of the transmission channel. To provide a software-defined configurable NB-IoT test network, the LTE core network interface (LTEMME) is attached to LTEENB on the same processing machine using the S1 interface. The list of registered UEs registered and attached to the eNodeB is shown in figure 4.5. The pycom UE tolerated integrity checks and Advanced Encryption Standard (AES).

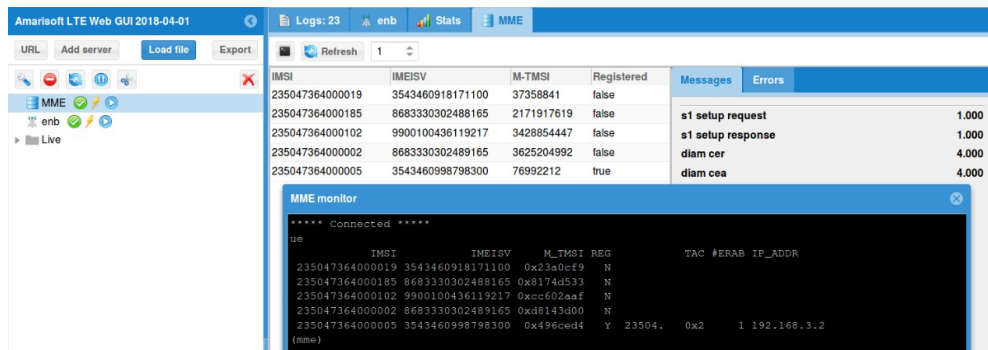


Figure 4.5: MME Interface showing UEs attached to the Network

4.6.2 Long Term Evolution Evolved Node B (LTEENB)

LTEENB is a software-based base station running Stream Control and Transmission Protocol (STCP) on 5th-generation or higher core processors configurable to support NB-IoT cells. The radio front end performs baseband signal conversion generated by the processor before being interfaced with the LTE standard core network (MME) interface at S1 plane. The 15 kHz and 3.75 kHz subcarrier spacing, single and multi-tone category NB1 and NB2 UEs were supported. The eNodeB is responsible for optimising the radio interface by assigning the radio network temporary identifier to the UE to distinguish radio UEs and radio channels. The eNodeB also helped to reduce the collision in a multi-user transmission environment. UEs antenna was kept a few meters away from

the LMS7002M antenna, and bands greater than band 7 is recommended if interference is to be kept very low.

4.6.3 Latency

Finding the transmission latency of NB-IoT UEs is an important way of ascertaining the network performance. Latency exists in IoT networks as a result of a large number of connected devices and channel conditions. More specifically, they include transmission mode, modulation scheme, error recovery pattern, propagation delay, low device complexity, queuing management, timing and frequency requirements. NB-IoT network can tolerate a latency value of 10 ms [9]. With a single UE being attached to the test network, latency here was based on carrying out a faster RRC release and the UE transmitting data as shown in 4.6 during the RACH procedure, which reduced latency and power consumption.

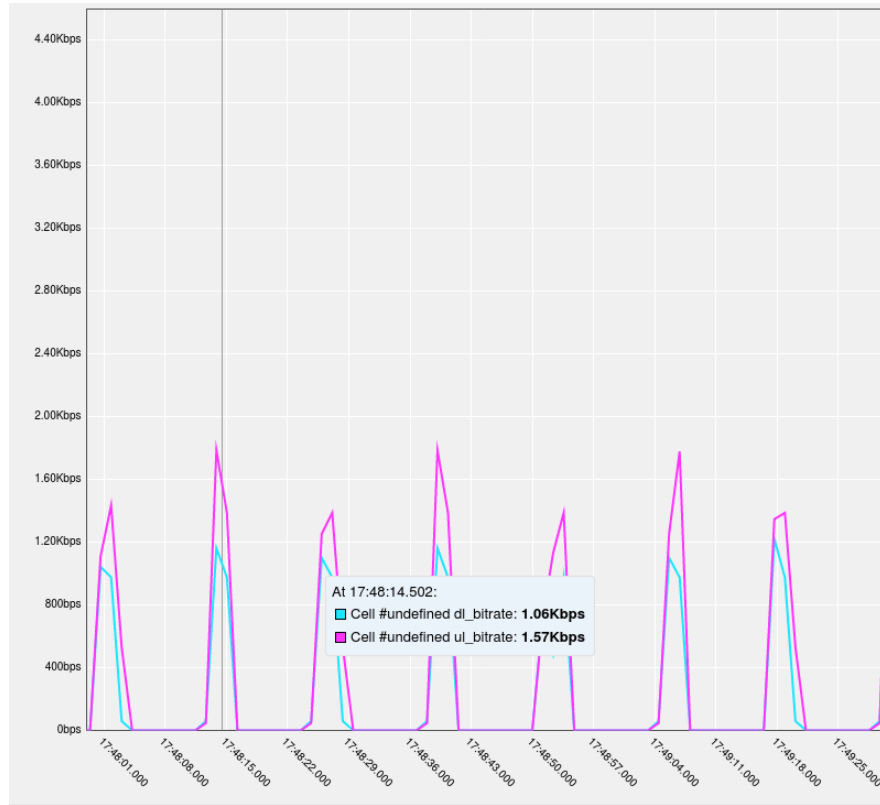


Figure 4.6: UE Downlink and Uplink Data Rate

4.6.4 Power Consumption

The functionality of UEs on the NB-IoT test network depends on the Lime microsystems SDR front-end and the entire system's performance. The energy efficiency of NB-IoT technology is aimed at providing long battery life of up to 10 years for a coupling loss of 164 dB. NB-IoT modules provide machine-to-machine communication either through a direct power source, battery or a combination. However, the 3GPP higher Releases incorporate Power Saving Mode (PSM) and Extended Discontinuous Reception (eDRx) options to improve IoT device battery life. The eDRx minimises power consumption in the downlink channel while PSM improves the energy utilisation in the uplink channel allowing longer transmission duration. The improvement in the new releases allows the UEs to transmit data even during the Radio Resource Control (RRC-idle) state as a way of reducing power consumed during the transmission and reception phases. The method of waking the UEs up from deep sleep mode, as shown in figure 4.7 also improves power consumption.

Ideal Mode

```

11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
-----DL-----
UE_ID CL RNTI C qcl rl mcs retx txok brate snr puc1 mcs rxko rxok brate
urbo phr pl ta
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [idle]
11 001 010b [
```

Figure 4.7: UE Data Transmission Modes

The average current measurements obtained when the IoT module scans the band and registers on the network in band 28 and sends a GET request message are 151 mA and 126 mA, respectively. A fraction of 3 mAh is extra energy needed to reconnect the module to the network, while 1.8 mAh is needed for an uplink message. These values however when compared to LoRaWAN, are observed to deviate largely from the 100 μ Ah average power consumed by the same module when joining a LoRa network and sending a few approximately 168 bytes of uplink data for spread factors of 7 and 12. The battery life reduces significantly as a result of the constant retransmission, especially

when the UE is a few meters away from the eNB as shown in figure 4.8. When the application requires data updates more frequently, the energy consumed increases. To improve the power consumption of the UEs, other efficient options for energising the modules independently should be explored.

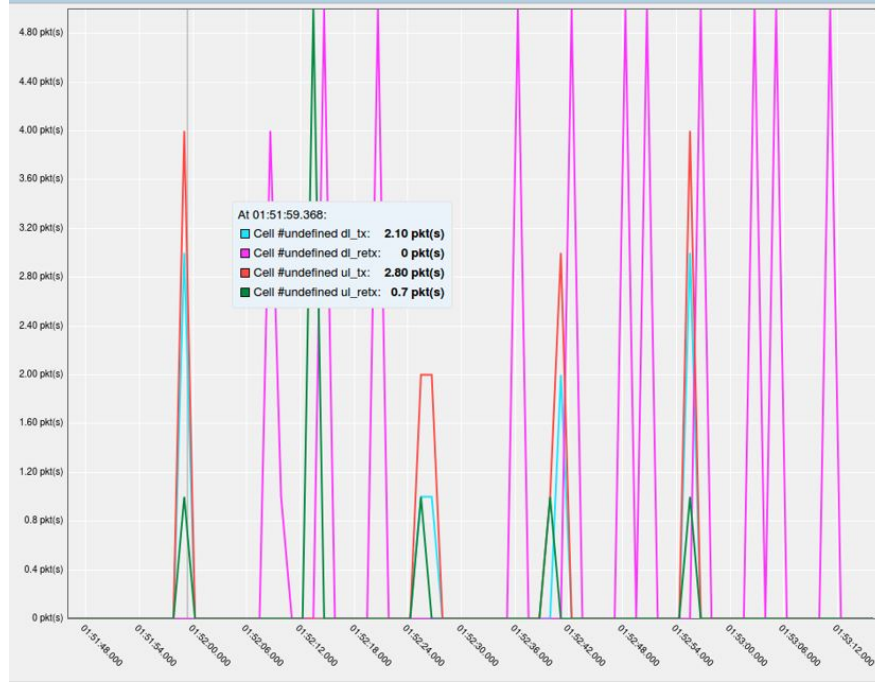


Figure 4.8: UE Data Retransmission

4.6.5 NB-IoT Security

Compared with the security requirements of other wireless technologies for IoT, NB-IoT security and privacy issues is challenging and considered in this thesis based on three IoT reference architecture; perception, network, and application layer, a simplified version as presented in figure 2.8. NB-IoT network is mainly characterised by low power consumption devices with low processing power and security requirements. In summary, security in NB-IoT then relates to hardening of IoT products, securing communication links, complying with international security standards (3GPP), enforcing management policy, trusting of third-party services and software, resolving key management issues and embedded security techniques. This indicate that the security of NB-IoT is hugely

located at the perception, network and application levels. The inefficiency of the devices for instance means that attacks are imminent in the event of a cyber incident. The 3GPP documentation on which this study is based specifies the security requirements between UEs and the NB-IoT network. In [248], NB-IoT security relied on SNOW 3G encryption to provide data confidentiality and ATR-128 to provide secure inter-mobile network data transfer. In this study, AES-128, 192, 256 is the Fipy supported security for encrypting the sensor payload before transmission. This guarantees NB-IoT security attributes such as privacy, confidentiality, data freshness, authorisation, and integrity as they are crucial in all critical IoT use cases. Hence, the need for further study on security especially when enabling NB-IoT on Unlicensed Spectrum (NB-IoT-U) [246]. Following security classifications in [243] and [88], NB-IoT security is classified here into perception, network, and application layers.

The application layer comprises of the service management and business services demanded by the IoT users through know protocols. CoAP, TCP, UDP, MQTT are good examples of efficient IoT protocols for relying services to the users. The security issues of application layer include privacy protection, and other problems of intellectual property protection. The end users of IoT applications in some use cases may require anonymity to protect user identity that advanced encryption techniques and digital signatures presented in chapter 6 and 7.7 can provide. As an intermediary function, the network layer allows data collected by the perception layer to be reliably transmitted to the application layer for processing and visualisation based on application requirements. Malicious insider and signal interference could result to network nodes being compromised through Dos, DDoS or by other network related attacks such as IP spoofing, bandwidth spoofing, etc. As presented in section 6.5.2 and 6.5.1, TLS and IPSec has been demonstrated as end-to-end security enabler for IoT deployment in constrained environment. In addition, the integrity and confidentiality of data in NB-IoT network can be secured by cryptographic based intrusion detection and prevention algorithms. This is the IoT data generation layer with the help of measurements by sensors and actuators located at the bottom of IoT architecture. The security of the data generating edge devices is a sensitive part of IoT networks as they are prone to

jamming, scrambling, spoofing, and other physical layer attacks [88]. The quality of data generated by the IoT depends on the edge computing. IoT devices deployed in attack prone areas need to be tamper proofed with each device to be authenticated, verified and the transmitted data encrypted.

The use of certain wireless technology for IoT connectivity is pervasive. In early 2020, the number of commercial NB-IoT networks globally has increased from 45 in 2018 [248] to 92 [275] with no visibility in many countries. LTE and 5G networks provide suitable platforms for mobile NB-IoT development and require minimal technical changes such as a software upgrade. By inheriting the design features of 4G and 5G, NB-IoT is considered more secure than other LPWAN technologies and suitable for pervasive applications. As the demand for connectivity continues to increase using NB-IoT ecosystem, the technology could be expanded to include other IoT technologies such as LTE-M to support all kinds of IoT devices with greater data payload. Other research needs include delivering backward compatibility and interoperability issues while ensuring adequate security. Also, finding robust algorithms to manage mobility and software updates in the network while maintaining very low UE complexity.

4.6.6 Conclusion

This section has presented the methodological approach for testing of a typical industrial NB-IoT network, outlining the current trends in NB-IoT development, and demonstrating that NB-IoT is a more appropriate technology for massive industrial IoT applications. The section also provides testing insight into IoT UE power utilisation, cost, latency, and equipment standard security requirements for NB-IoT deployment in the face of a cyber-connected world. However, the frequency of operation and license is a critical parameter as one must have the legal right to transmit on any LTE frequency in a country and be sure to ensure reduced interference through the deployment of evaluated NB-IoT devices.

Chapter 5

Performance Analysis of LoRaWAN and Cellular NB-IoT Networks

Recently, Internet of Things (IoT) deployments have shown the potential of aiding the realisation of Sustainable Development Goals (SDGs). Concerns regarding how IoT can drive specific SDGs goals 6, 11 and 9 in developing countries have been raised with respect to the challenges of deploying licensed and unlicensed Low Power Wide Area Network (LPWAN) IoT technologies and the opportunities for IoT consumers and service providers. With IoT infrastructure and protocols being ubiquitous and each being proposed for different SDG goals, we review and compare various performance characteristics of LoRaWAN and NB-IoT networks. From the performance analysis of our networks, NB-IoT, one of the standardised promising cellular IoT solutions for developing countries, is more expensive and less energy-efficient than LoRaWAN. Utilising the same User Equipment (UE), NB-IoT consumed an excess of 2 mAh of power for joining the network and 1.7 mAh more for a 44 byte uplink message compared to LoRaWAN. However, NB-IoT has the advantage of delivering higher network connection

Majority of this chapter is a journal article, Survey of IoT for Developing Countries: Performance Analysis of LoRaWAN and Cellular NB-IoT Networks, Electronics 2021, 10, 2224. <https://doi.org/10.3390/electronics10182224>

capacity reliably and securely in IoT use cases, leveraging existing cellular infrastructure. With the maximum throughput of 264 bps at 837 ms measured latency, NB-IoT outperformed LoRaWAN and proved robust for machine-type communications. These findings will help IoT consumers and service providers to understand the performance differences and deployment challenges of NB-IoT and LoRaWAN and establish new research directions to tackle the IoT issues in developing countries. With Nigeria as a case study, for consumers and organisations at a crossroads in their long-term deployment decisions, the proposed LPWAN integrated architecture is an example of deployment opportunities for consumer and industrial IoT applications in Developing countries.

5.1 Introduction

The Internet of Things (IoT) plays a crucial role in achieving connected living through increased business activities, remote operations, and social interactions. IoT technologies are more pronounced in urban areas through applications like Smart City, Smart Manufacturing, Wearables, Smart Homes, Self-Driving Cars, etc. These applications are driven by factors such as established business use cases, availability of communication network resources and coverage, power and regulatory frameworks. These factors affect the rate of IoT penetration in rural localities, especially in developing countries where power and communication network coverage issues limit deployment opportunities and the realisation of the United Nation's Sustainable Development Goals (SDGs) [276]. We believe that regions with limited terrestrial infrastructure will be best serviced by Low Earth Orbiting (LEO) Satellites and LPWAN-based IoT applications for services such as asset tracking and environmental monitoring, as these have the lowest demand for infrastructure. These approaches, however, may have drawbacks if two-way communication is not supported for communications between LEO satellites and ground-based IoT infrastructure.

As the Internet of Everything (IoE) continues to evolve, so too do the protocols and challenges associated with its applications and deployment. The traditional wired and short-range wireless technologies cannot meet the scale of demand for remote data

visualisation of wireless sensor networks. Adopting LPWANs allows such scalability and ease of deployment, but with new scalability challenges including security, power consumption, and latency. These were identified as few of the LPWAN deployment and applicability index towards best practice in LPWANs [72]. An adaptive battery-aware algorithm has been proposed to effectively manage power consumption and charging process in medical IoT devices that remotely collect patients data continuously [161]. The latency of data transmission in IoT networks are multi-faced at different part of the network. The data payload size for typical IoT networks are within few bytes, LoRaWAN has a payload size of 51 bytes [277]. To transmit higher data payload, technologies such as NB-IoT reduces the number of transmissions, latency and energy consumption that would have come from multiple transmissions in LoRaWAN. An analytical framework has been proposed to examine the effects of scheduling of data, control information, and coverage classes on latency and battery lifetime in distributed IoT networks [70]. The proposed models minimised the communication delay with high performance tradeoffs in channel scheduling. LPWANs are vulnerable, but LoRaWAN and NB-IoT offer sufficient security for certain applications if implemented with strong security policies and enforcement [191]. In [278], we identified the current security challenges of different Low Power Wide Area Network (LPWAN) IoT networks and platforms as they apply to different IoT use cases. The integrity, confidentiality, authenticity, privacy, and trust of IoT systems are still open research issues. Similarly, in [279], we presented an early insight into the Narrowband Internet of Things (NB-IoT) testbed design and implementation procedure.

In this chapter, we evaluate the performance of licensed and unlicensed Low Power Wide Area (LPWA) IoT network options to demonstrate the use of cellular LPWANs to meet SDG goals. NB-IoT and LoRaWAN are sustainable solutions for interconnecting billion IoT devices and the technologies (GSM and LTE) on which NB-IoT depends are available in developing countries. Both technologies are among the most popular in the research community for industrial and consumer applications. These capabilities will help towards the provision of services such as safe drinking water through pollution monitoring systems - (SDG goal 6), extending business opportunities to rural areas

through sustainable city creation – (SDG goal 11), and extending affordable internet connectivity to hard-to-reach locations to fast track business opportunities by bridging the digital divide gap - (SDG goal 9). A few of the most significant challenges of IoT adoption is selecting the most efficient, secure, and cost-effective technology that will stand the test of time in this fast-changing technology regime. Following the network practical simplicity, long-term cost efficiency, feasibility, and information security performance index [72], the performance of each IoT technology can be ranked based on the network QoS. However, the multiplicity of different IoT options makes developing IoT networks a challenging task, with issues including a shared hardware infrastructure at the gateway level, and global harmonisation of spectrum bands suitable for IoT applications. As demonstrated in this chapter, a unified proof of concept IoT platform reduces the number of physical infrastructure types across the IoT ecosystem as the technology evolves.

Despite the promises of IoT, research involving testbeds performance of cellular IoT networks is limited. Research in cellular IoT network performance such as NB-IoT often relies on simulations and theoretical approaches. Based on network performance analysis, we evaluated NB-IoT and LoRaWAN testbeds for applications of IoT in developing countries, hard-to-reach locations and rural localities. Using the same IoT devices (UE) as sensor nodes in the NB-IoT network and as sensor nodes and gateways in the LoRaWAN network allows establishing networks performance baseline towards building a multi-tenant IoT infrastructure. Specifically, the main contributions of this chapter are as follows:

- A critical review of the requirements, opportunities and challenges of IoT for developing countries.
- A critical review of unlicensed and cellular LPWAN technologies focused on security, energy utilisation, standardisation, interoperability, policy regulations and QoS requirements.
- Evaluation of the performance of NB-IoT testbed and proposal of a hybrid NB-IoT and LoRAWAN proof of concept to scale IoT deployment in developing countries.

- Investigation and evaluation of the performance of LPWANs. We compared the performance of both LoRaWAN and NB-IoT in terms of transmission latency, throughput and battery utilisation and analysed the benefit of NB-IoT for IoT applications against unlicensed LPWAN for developing countries.
- Through the evidence of the findings, offer recommendations on the potential benefits and drawbacks of integrating LPWANs to scale IoT deployments.

The remaining part of this chapter is organised into the following sections: Section 5.2 presents the review of current literature on LPWANs and the main research goals. Section 5.3 discusses both the licensed and unlicensed LPWAN IoT deployment opportunities in developing countries. Using Nigeria as a case study, a more comprehensive analysis of the technical challenges, policy regulations, spectrum, and security issues of unlicensed and cellular IoT technologies were also presented. Section 5.4 explains the underlying principles of low power cellular technologies for IoT, including NB-IoT, EC-GSM-IoT, LTE-M, and 5G. The design framework and implementation of NB-IoT and LoRaWAN testbeds are given in section 5.5 to evaluate the real-world performance of IoT networks. Through comparative analysis, results on power utilisation, security, latency, and throughput were presented in section 5.6. The limitation and future research directions are presented in section ?? before section 5.7 concludes the chapter with key points on how LPWANs can help the realisation of the SDGs in developing countries, potential benefits and drawbacks of the study.

5.2 Related Literature and Contribution

Adopting IoT technology in developed and developing countries has various opportunities and challenges. Most global climate change events in 2020 and early 2021 revolve around how human activities and waste impact climate and water bodies and have created an increasing research interest in the field of IoT. Internet of Things [280] solutions have been used to monitor, collect and analyse different environmental measurements such as water quality data from small remote locations. In the Fiji Islands [281], IoT and Remote Sensing (RS) techniques were used to monitor the potential hydrogen,

oxidation and reduction potential, temperature and conductivity levels of four different water sources. A Wireless Sensor Network (WSN) as reviewed in [34] considered the use of LoRa and Sigfox technologies over Internet/3G/LTE to deliver an energy-efficient wireless sensor system for water quality monitoring. Other LoRaWAN studies for water quality monitoring were carried out due to its long-range of data transmission in difficult terrain and low power consumption rate as proposed by Jorge et al [130]. For instance, the Lake Dardanelle in the United States [282], Facilities of South Africa Council for Scientific and Industrial Research (CSIR) [283], and Dong Lake in National Dong Hwa University China [284], all used LoRaWAN technology as a test field for various characteristics of water quality monitoring.

A GSM-based IoT solution has equally been used to monitor the PH and turbidity level of water tanks in India [285]. The water quality of fish ponds and aquarium systems has been monitored using IoT solutions. FishTalk enabled remote feeding of fish and intelligent water quality control [286]. The study augmented the network with more IoT services such as smart agriculture, where farm owners will receive feedback on the health status of their farms remotely. An early mathematical study on energy-abundant vehicle-based relays for using NB-IoT to support crowded IoT deployment proved to increase link reliability and energy utilisation of the IoT devices [287]. All these studies are based on 4G Mobile Network Operators (MNO) networks, which are not readily available in rural areas. GSM and cellular network standards older than LTE are mostly deployed in more rural areas, where these remote monitoring activities will be required. These aspects of IoT applications in developing countries require both licensed and unlicensed LPWANs. The contribution in this chapter will leverage a mix of LPWANs to bridge the IoT network connectivity gap surrounding IoT application opportunities in developing countries as shown in figure 5.1. An integrated IoT solution that would offer improved quality of Service (QoS) of NB-IoT and LoRaWAN, cheaper to deploy with redundancy, and specifically promote the reuse of IoT radio access infrastructure. The power consumption, latency, throughput, and latency performance of NB-IoT and LoRaWAN networks are compared with measurements of environmental temperature and humidity that could be replaced with other applica-

tions of IoT in developing countries. These aspects of QoS requirements considered both the uplink (path between the IoT device and the server) and downlink (server to device) transmissions.

The main research goal of this section was to implement, test and evaluate licensed and unlicensed LPWANs technology and, based on the findings, present IoT LPWAN deployment opportunities and challenges for expanding IoT connectivity in developing countries. As most existing studies, especially in cellular networks such as NB-IoT are simulation and survey [220], [77], [70], [9], this chapter presents the results on the latency, data throughput, power consumption, and security of LPWANs. We analyse and compare the results with the LoRaWAN and NB-IoT testbeds using the same UE to fill the literature gap for unlicensed and licensed test network performance. Few experiments that investigate NB-IoT and LoRaWAN performance exist but are limited to power consumption and costs [288], power consumption [289], [71], and [290] using different UEs.

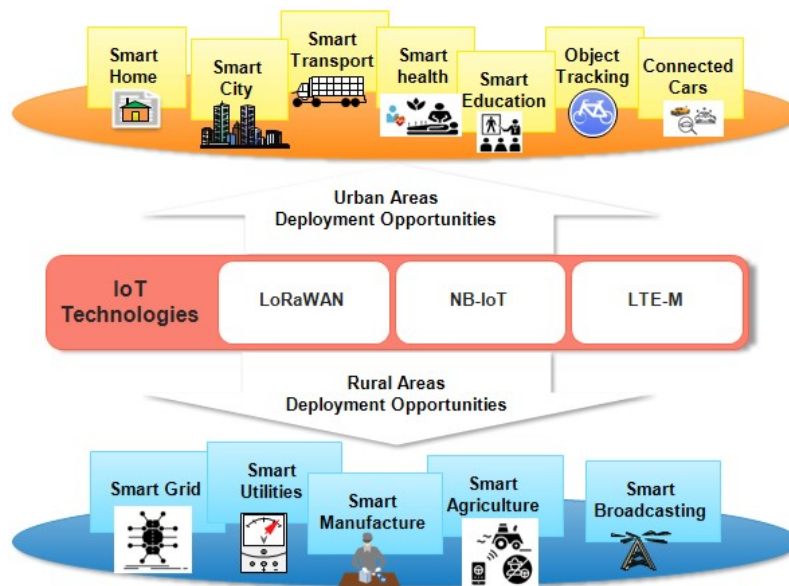


Figure 5.1: IoT Deployment Opportunities in Developing Countries.

5.3 IoT Deployment Opportunities in Developing Countries

There are Business to Consumer (B2C) and Business to Business (B2B) potential opportunities of using LPWAN IoT technologies in developing countries, as shown in figure 5.1. For example, the digital transformation of the farming sector in developing countries will ensure food security for the increasing population and may increase the Gross Domestic Product (GDP), and Return on Investment (ROI) [121, 291] and support aspects of investment decision making through intelligent computing and big data analytics [292]. Other opportunities include improved security monitoring, increased productivity, quality control, transportation and supply chain optimisation. A well-established GSM and LTE cellular infrastructure could enable IoT to be more widely deployed in developing countries. LTE, 5G and other 3GPP standardised Machine-to-Machine (M2M) IoT solutions can be relied on to deliver more bandwidth and device connection density per cell at lower latency. LoRa is also standardised, although perhaps to a lesser extent towards co-existing with 4G and 5G ecosystems for IoT applications [293]. Different aspects of LPWAN technologies can meet the requirements of massive, broadband and critical IoT applications. Generally, massive IoT applications are delay-tolerant infrequent IoT devices of small data volumes used in challenging network connectivity and energy supply environment. Examples include smart metering and asset management, where network roaming, extended coverage and long battery life capabilities are required to reach all assets seamlessly. EC-GSM-IoT, NB-IoT, and LTE-M are the 3GPP standardized protocols that meet the requirements of low-complexity IoT devices through GSM and LTE enhancements. This is the IoT application segment where the unlicensed LPWANs are also applicable.

The Broadband IoT supports high throughput IoT devices that deliver large data volumes at low latency based on mobile broadband MTC. The Broadband IoT segment relies purely on LTE device capabilities to perform better than massive IoT. LTE-based IoT devices often support multiple antennae, carrier aggregation, scheduling mechanism, and spectral efficiency, and as a result can operate in extended coverage

and power-saving mode. Examples include drones and wearables that require real-time operation and control. 5G NR broadband IoT will offer additional capabilities that can improve bandwidth and throughput mechanisms such as ultra-short duration transmission and retransmission, seamless base station handover, transmission diversity, and improved link budget and adaptation [62]. Frequencies greater than 6GHz have extremely low latency, limited coverage and are suitable for local area services with high capacity and ultra-high reliability demand. The disadvantage of high frequency is the cost due to additional radio resources needed to increase signal coverage – with higher frequencies being used, a denser distribution of cells is required in order to provide coverage, compared with lower frequencies. The mid bands ranging from 1GHz to 6GHz are suitable for wide-area IoT services with extremely low latency and ultra-high reliability. Frequency bands as low as sub-1GHz are also suitable for wide-area IoT applications but the devices must have limited capacity requirements due to the relatively lower quantities of spectrum available in these bands.

Critical IoT on the other hand will be suitable for addressing extreme IoT connectivity requirements of many applications of ultra-low latency, ultra-reliable, and very highly available IoT services. Examples of these use cases include traffic control systems, smart grid automation, and automobile control that requires low latency (5-20 ms) [294] and high reliability (99.9999%) [295]. The automation segment covers industrial digital transformation supplemented by cellular networks. Industrial and consumer IoT or rural and urban IoT networks are a mix of the various IoT segments depending on the service and use-case requirements.

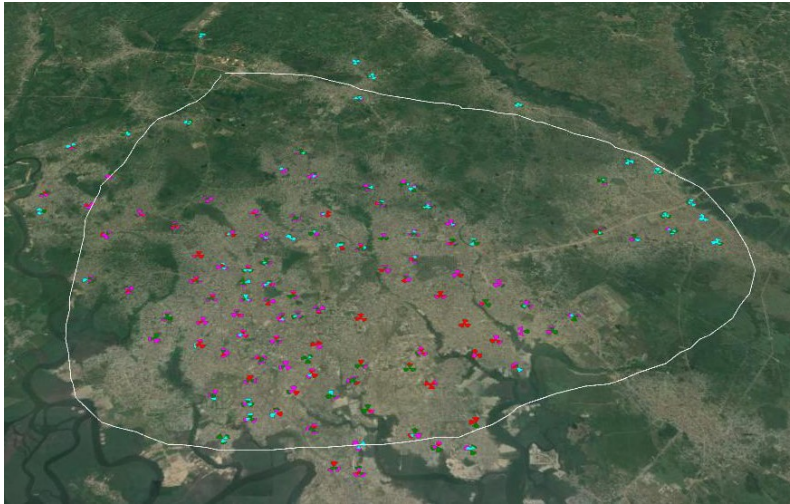


Figure 5.2: Typical LTE Network Distribution in Urban Area in Nigeria

5.3.1 Leveraging Cellular Networks for IoT Deployments in Nigeria

The Mobile Network Operators (MNOs) in Nigeria as presented in table 5.1 fall within the ITU Region 1 deployment bands [296]. All the deployment bands can support either NB-IoT or LTE-M based IoT network, except band 42 and other Time Division Duplex (TDD) band-based frame structure. Following the national approach of allocating the spectrum to the MNOs, NB-IoT and LTE-M are set to thrive once roaming agreement and infrastructure sharing exists between the MNOs. This presents a massive deployment opportunity for LTE-based IoT technologies in the in-band and guard-band modes in Nigeria (see figure 5.2), as also identified for India NB-IoT deployment towards smart city applications in the rural villages, suburban hub, and urban capital of the city tower density [297]. NB-IoT deployment leverages LTE infrastructure which is mainly clustered within an urban locality. The dots as shown in figure 5.2 represent different sectors of co-located two 1800 MHz and 900 MHz sites. Red - current number of users exceeded planned users per cell, Purple - maximum number of users reached, Green - number of users within range, Blue - number of users on the cell is low. Spectrum will be repurposed to support more efficient new services.

In the Nigerian Communications Commission's (NCC) frequency assignment tables, bands 3 and 8 are predominantly used for GSM while band 1 is used for GSM, 3G,

and LTE [298]. Band 3 is the largest spectrum used for LTE deployment globally due to its large coverage and the ability of its services to be refarmed into Band 1 with a robust option of carrier aggregation configuration for different bandwidths. The 900 MHz on the other hand is generally used for 2G, GSM and data communications supporting broadband deployment and could have huge potential for IoT deployment. Depending on the deployment mode to be adopted by the MNOs to support NB-IoT and LTE-M technologies, the possible impact on their networks would be the upgrade of baseband units, antenna systems, and eNB software and the introduction of new RF modules. The main technical challenge of NB-IoT penetration in developing countries such as Nigeria as presented by Oluwaseun et al is the sole reliance on broadband connectivity which stood at 50% in 2019 [121]. However, we envisage that power supply, MNOs business scenarios, security, policy standardisation, privacy, interoperability, and the cost of acquiring IoT devices are potential challenges that could be turned into opportunities. Other network infrastructures to be mentioned as the common factors affecting IoT development globally include the provision of base stations for the extension of coverage to rural areas without an exponential rise in Capital Expenditure (CapEx) and Operational Expenditure (OpEx). Where practicable, the use of band 20 and band 8 for LTE-M and NB-IoT is recommended if indoor and outdoor penetration is desirable at the same time, but at a trade-off compared with Band 3 in that each operator has less spectrum. With band 20 and band 3 making available 30 MHz and 75 MHz respectively, carrier aggregation will be needed to support non-NB-IoT users. IoT services will have lower performance/throughput on B20, but better range, meaning more users served with poorer connections.

Policy and Regulatory IoT Issues

To accelerate IoT development and investment in developing countries, a good policy and regulatory framework are needed in the areas of security and privacy, standards, and government regulation [276]. This is seen, for example, in the code of practice for consumer IoT security in the UK [299], the Unmanned Aircraft Systems (UAS) regulations and guidelines by United State Federal Aviation Administration [300], and

security requirements for consumer IoT devices by ETSI [301]. Other policy and regulatory themes to be addressed include fair access to sufficient spectrum, managing communication taxes, ensuring end-to-end security, numbering and addressing, etc [302]. Radio spectrum is critical to IoT deployment and the regulation of Radio Frequency (RF) according to the International Telecommunication Union (ITU) can be done independently at national, regional, and global levels. In Africa, the African Telecommunication Union (ATU) comprises mobile and fixed telecom companies that formulate policies and strategies that promote technology integration across the continent. The regional approach sees regulatory bodies such as the West Africa Telecommunications Regulatory Assembly (WATRA), the East Africa Communication Organisation, and the Communication Regulators' Association of Southern African (CRASA) managing regulations. Nigeria is a member of ITU Region 1 (ITU-R1) with the Spectrum Administration Department of National Communications Commission (NCC) responsible for managing, planning, and licencing the RF spectrum as specified in the NCC Spectrum Administration Charter (SAC) [303]. The Federal Ministry of Communications (FMC) is the regulatory body governing the communication policy. Poor management of RF spectrum is the result of lack of adequate regulatory frameworks for an expensive and scarce natural resource described as a technology service of all economic interest [296]. RF harmonisation allows direct reuse of other countries' spectrum allocation tables on different services without issues within the same ITU region, since RF crosses national boundaries. However, different countries usually have different operators with varying allocations of spectrum based on their auction's strategy.

Spectrum and IoT Issues

The advent of IoT technologies has pushed for more wireless devices to operate in a different spectrum. Whereas NB-IoT and LTE-M operate in the licensed spectrum with minimal interferences, it uses Hybrid Automatic Repeat Request (HARQ) to guarantee data delivery, Narrowband Fidelity (NB-FI), SIGFOX and LoRaWAN operate in the unlicensed ISM spectrum with duty cycle limitations. For these reasons, NB-IoT and LTE-M are most suitable for applications with higher QoS of non-time-critical require-

ments. Transmissions within the ISM bands are not reliable and require acknowledgment of uplink and downlink packets, due to the inherent potential for interference and collisions with other users of the spectrum. The higher QoS in NB-IoT and LTE-M networks are at the expense of a higher cost of acquiring licensed spectrum. The sub-GHz spectrum auction was over \$500 million/MHz in 2017 [220] and in 2021, an increase is seen in Ofcom's auctioning prices of the 700 MHz and 3.6-3.8 GHz for 5G in the UK [304]. 6 lots of 2x5 MHz (700 MHz band), 4 lots of 10 MHz (700 MHz band), and 24 lots of 5 MHz (3.6 GHz band) amounted to reserved prices of £100 million/slot, £1 million/slot, and £20 million/slot respectively.

Spectrum sharing is an essential part of IoT development. Spectrum bands between 1 to 6 GHz that are suitable for IoT development in a cost-effective manner have been allocated for other uses. Finding an unused block of frequencies within a specific area is one easy way of solving spectrum issues or building a contiguous spectrum to meet a particular service requirement if applicable (suitable for the national auction approach). Due to the unavailability of free spectrum, gray space sharing as described in [305] is most applicable in situations where there is not a dynamic technology, a particular frequency is used over a wide geographical area. In spectrum sharing, there is technical inter-dependencies and information exchange between the primary and secondary spectrum equipment and users are intertwined. A more interactive policies is best for this type of sharing where devices reuse spectrum if gains in spectral efficiency is to be achieved. A secondary user is only possible through established policy regulation and governance frameworks. White Space Spectrum (WSS) is generally regarded as the regions of unused spectrum within or around existing bands, and are potential opportunities for IoT deployment in rural areas and developing economies [306].

Table 5.1: Overview of MNOs in Nigeria with NB-IoT and LTE-M bands deployment opportunities.

Operators	Bands	Channel Bandwidth
9 Mobile	B1 (2100 MHz)	
	B3 (1800 MHz)	10
Airtel	B1 (2100 MHz)	
	B3 (1800 MHz)	5
MNT	B1 (2100 MHz)	
	(1800 MHz)	15
	B20 (800 MHz)	10
	B42 (3500 MHz)	10, 20
VDT	B40 (2300 MHz)	10, 20
ntel	B3 (1800 MHz)	15
	B8 (900 MHz)	5
Glo	B1 (2100 MHz)	
	28 (700 MHz)	10

Security and IoT Issues

Based on the security requirements of other wireless technologies for IoT, security and privacy issues is challenging and considered in this chapter on three IoT reference architecture; perception; network; and application layer.

Application Layer - The application layer comprises the service management and business services demanded by the IoT users through known protocols. Constrained Application Protocol (CoAP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Message Queue Telemetry Transport (MQTT) are good examples of efficient IoT protocols for relaying services to the users. In our test networks, we used TCP protocol due to the high reliability of data transmission. The security issues of the application layer include privacy protection and other problems of intellectual property protection. The end users of IoT applications in some use cases may require anonymity to protect user identity. In this scenario, advanced encryption techniques and digital signatures can intelligently provide the necessary security [169].

Network Layer - As an intermediary function, the network layer allows data collected by the perception layer to be reliably transmitted to the application layer for processing and visualisation based on application requirements. Different internet

based access network technologies applicable to IoT have been presented in table 2.2 for device-to-device communication. However, it is also a channel through which security risks are introduced to the network. Malicious network signal interference could compromise network nodes through Denial of Service (Dos), Distributed Denial of Service (DDoS), or other network-related attacks such as IP and bandwidth spoofing. Transport Layer Security (TLS) and Internet Protocol Security (IPSec) has been demonstrated as end-to-end security enabler for IoT deployment in constrained environments. In addition, cryptographic-based intrusion detection and prevention algorithms can secure the integrity and confidentiality of data in the NB-IoT network [307].

Perception Layer - This is the IoT data generation layer with the help of measurements by sensors and actuators located at the bottom of IoT architecture. The IoT devices can support edge processing and mostly wireless sensing enabled for remote access and tracking capabilities through gateways. The security of the data-generating edge devices is a sensitive part of IoT networks as they are prone to jamming, scrambling, spoofing, and other physical layer attacks [88]. The quality of data generated by the IoT depends on edge computing. IoT devices deployed in attack-prone areas need to be tamper-proof, with each device to be authenticated, verified and the transmitted data encrypted.

5.3.2 Leveraging Unlicensed LPWANs for IoT Deployments

The advancement in wireless technology recently for Internet of Things applications has enabled the development of a wide range of sensor networks for environmental data collection. Low Range (LoRa) Wide Area Network (WAN) generally referred to as LoRaWAN is one of the Low Power (LP) WANs encompassing classification requirements that are based on unlicensed spectrum, low cost, reduced power, and a wide range of data transmission [21]. LoRaWAN connects multiple IoT devices through an open and standardised communication protocol for the Internet of Things and can be integrated with licensed bands like the 4G/5G cellular networks [130]. Based on the Chirp Spread Spectrum (CSS) modulation technique at the physical layer, LoRaWAN offers low channel interferences and high coverage against reduced data rate as shown

in equation 5.1 where SF, R_b, and BW represent the spread factor, symbol rate and bandwidth respectively.

$$R_b = SF \times \frac{1}{\frac{2^{SF}}{BW}} \text{ bits/s} \quad (5.1)$$

For a fixed BW of 125 kHz, the symbol rates possible for the maximum (12) and minimum (7) values of SF is 366 bits/s and 6835 bits/s respectively before encoding.

LoRaWAN Network Architecture

The standard LoRaWAN network architecture is a star-of-stars topology with the front-end, gateways, and back-end as three distinct layers. The front-end of the network is the proprietary LoRa Radio Frequency (RF) connections between the end devices and the LoRa gateways, see figure 5.3. The Fipy LoRa gateway incorporates the Semtech SX1272 chip which supports up to 22 km with 100 nodes capacity. It collects the temperature and humidity data from the Pysense Node and forwards it through the TTN to the application server where it is stored and processed. Our model is configured to operate in the 868 MHz frequency band and on the TTN V2 cluster due for deprecation and shut down in December 2021. For uplink communication, UE data is broadcast via LoRa gateways within range. The gateways act as repeaters by relaying the end device messages to a single network server where they are aggregated and de-duplicated. This eliminates any handover requirements between gateways when they are within the network coverage. The back-end is an IP-based connection between the network/application servers and the gateways. The network server is the received data aggregation point and the MAC layer encryption must be decrypted before an uplink data transfer to the application server. Application Servers can be run by the network operator, or by the end-user of the application. The application key of each application server is then finally used to decrypt the real data payload. The reverse process occurs for a downlink data transfer. It is important to note that in most classes of operation, as discussed below, downlink messages can only be sent in response to an uplink message since most LoRa devices will not listen at all times for downlink

messages. The TTN network allows different applications and database integration. In JSON format, node data are stored through a REST API for data access. An access key is needed for an HTTP request to the database. The application server is an HTTP web server for accessing the database. Refer to subsection 3.1.3 for information on LoRaWAN Physical Characteristics such as modulation scheme and devices classes.



Figure 5.3: Secure LoRaWAN Architecture. (a) Typical LoRaWAN Architecture and (b) LoRaWAN Network Implemented on The Things Network.

5.4 Low Power Cellular Technologies for IoT

Wireless technologies play different and important roles in the development of IoT. The comparison of key technologies enabling IoT deployments is presented in table 2.2. The goal is to develop IoT technologies that maximise ROI in communication infrastructure and still maintain reliable connection and secure data transmission. While wired technology is a unique component of IoT networks in special use cases mostly for on-premises applications and for backhaul connection to 5G or 4G infrastructure, wireless technologies are increasingly used for cost reduction, mobility, deployment flexibility and power consumption reasons. For deployment flexibility, a smart manufacturing environment for instance can be re-configured within a day without having to re-do the infrastructure, while on the other hand, re-laying of fibre might take days or weeks to complete the same task.

For seamless convergence of wired and wireless networks, it is necessary to advance throughput, latency, and capacity of wireless technologies to meet the requirements of

critical IoT applications in 5G/IoT era [22]. The communication requirements, QoS, and use cases for WiFi (802.11) standards and wireless IoT technologies are different [308]. Factors such as hardware design, area of application, and technology of implementation impact the technology of choice. In the use cases of IoT that require the transmission of a small amount of latency insensitive data over a long distance at lower costs, such as water quality and environmental monitoring, licensed should be considered if QoS is needed. Unlicensed should be considered (in addition to the licensed) options if QoS/reliability is not needed. Other wireless technologies like Zig-Bee, Wifi, and Z-wave are alternatively used to support short-range applications but are categorised as power-hungry technologies [309].

3GPP initially standardised the licensed technologies such as NB-IoT and LTE-M in the standard Release 13 and some improvements introduced in the subsequent 3GPP Releases to provide a more efficient, secure and trusted IoT environment [62]. Currently, NB-IoT can achieve coverage enhancement of between 18 km to 25 km in the urban and rural locations [280], operates through GSM and LTE infrastructures for a channel of 200 kHz [241] and 180 kHz [310] respectively, supports low power consumption. LoRaWAN and Sigfox are examples of unlicensed LPWAN technologies with LoRaWAN as a popular option in this category operating in the sub-GHz ISM band. However, deploying LoRa and NB-IoT together is a potential opportunity to scale coverage and capacity of IoT networks [280] but the backhaul of each network should be provisioned separately since their QoS/reliability requirements are different.

5.4.1 EC-GSM-IoT

Extended Coverage Global System for Mobile Communication (EC-GSM-IoT) is one of the early solutions proposed for cellular machine-to-machine IoT applications from GSM and General Packet Radio Service (GPRS) that got standardised by 3GPP. The software enhancement of the design features of GSM was to support mobile IoT development because of its global wide coverage and the business needs between the early 90's and 2015. The number of frequency bands pairs for global GSM deployment - 900 MHz with 1800 MHz and 850 MHz with 1900 MHz make the manufacture of

global GSM device easier since an IoT device worst case complexity is to have dual band capabilities and low module price (multiple bands support) and are some of the characteristics that make GSM suitable for IoT. GSM standards were defined for voice and data based on voice and packet-switched technologies respectively [62]. General Packet Radio Service (GPRS), Enhanced Data Rates for GSM Evolution (EDGE), and Enhanced General Packet Radio Service Phase 2B (EGPRS2B) are variants of GSM enhancement to support higher data rates of up to 2 Mbit/s. An EC-GSM-IoT based IoT is designed to co-exist with higher versions of cellular networks and benefits from their high capacity, extended coverage, roaming support, deep indoor penetration, low energy consumption depending on the number of RF bands supported, security and privacy features [311]. This is a good option for IoT deployment in developing countries where cellular networks are predominately used for voice like in Nigeria where the GSM mobile share by technology stands at 99.8% in 2021 [312] and in places where GSM coverage exceeds 4G.

It is important to state that the management of spectrum has been a major challenge with some being refarmed and others shared between mobile network operators in order to provision global IoT services. With the coming of 5G, the small spectrum allocated for GSM may be further refarmed to support new technologies.

5.4.2 NB-IoT

NB-IoT has been discussed extensively in chapter 4. In the southern part of Nigeria, where the untapped natural gas and crude oil deposits stand at a record high, water and air pollution resulting from oil and gas exploration activities in and around these localities has been endemic as a result of illegal exploration activities such as pipeline vandalism and oil theft [121]. Crude oil spills and other chemical wastes constitute the major water pollution threatening the health of those who live and work in those regions. With NB-IoT and other LTE-based sensor networks, it is possible to monitor such parameters remotely. An integrated wireless LPWAN presents varieties of interoperable protocols for water and environmental data gathering and sending it over to a central data centre for analytics. Through the survey of wireless technologies available

in the region, the authors are not aware of any LoRa and NB-IoT based environmental monitoring system in and around the oil polluted regions in Nigeria for either private or public use. The availability of wide LTE and GSM network coverage is what this study is leveraging to demonstrate the advantages of using unlicensed spectrum to complement licensed technologies for scaling IoT deployment in developing counties.

Table 5.2: NB-IoT Features.

Benefits of NB-IoT
Improved indoor coverage
New radio technology from 3GPP Release 13 and above
Supports massive low data devices
Low latency sensitivity
Ultra-low device cost
Low device power utilisation
High assurance of quality of service
Inherited LTE security

NB-IoT Standardisations

The initial standardisation of NB-IoT was established in the 3GPP standard Release 13 to utilise 180 kHz bandwidth of LTE and 200 kHz bandwidth of GSM carriers for the uplink and downlink channel transmissions as shown in figure 5.5. Refer to section 3.8 for a detailed presentation on NB-IoT standardisation. The 3GPP Release 13 standard outlines the LTE and GSM support capabilities for machine-type communications and the design targets of achieving long battery life, massive connectivity, greater coverage, deeper penetration, and positioning enhancement. It was originally designed with the LTE modulation schemes, channel coding techniques, and numerology features in communication type with low data rate, restricted mobility, and latency requirements. To reduce IoT module cost and complexity, the LTE connected mode mobility is removed in NB-IoT [248].

To provide an enhanced user experience in NB-IoT applications and extend the applications to other use cases, 3GPP LTE Released 14 was introduced. This allowed service offerings such as coverage enhancement, positioning accuracy, improved data rates, multicast capability, lower power class features, non-anchor carrier support, and

the opportunity to support more IoT devices in one eNB [15]. Release 15 optimises Early Data Transmission (EDT) support during Radio Access (RA) connection procedure. It is used to enable transmission in the uplink channel within the RA connection procedure thereby reducing the connection setup time and signalling overhead as shown in figure 5.4. The process in EDT transmission is that the IoT module initially indicates the intention to transmit data during the RA procedure by making use of the special (N) Narrowband Physical Random Access Channel (PRACH) preamble dedicated to EDT by the evolved base station in the System Information Blocks (SIB). Data transmission in Release 13 and 14 is only possible after the RA procedure is completed. This standard has the advantage of reducing latency and improving the battery life of IoT devices deployed in limited network reception areas. The eNB transmits the maximum Transport Block Size (TBS) for the data in EDT mode. Release 16 covers the enhancement in the 3GPP standardisation Release 15 5G New Radio (5G-NR) [62]. The NB-IoT enhancement in the standard includes self-organising ability, able to co-exist with NR, mobility enhancement, improved multi-carrier operation, scheduling enhancement, improved transmission efficiency, and improved user equipment power consumption. The support for non-terrestrial access in 5G NR enhancement will enable the support for NB-IoT and eMTC deployment using satellites and High-Altitude Platforms (HAPs). The deployments standard is based on MNOs and UE capabilities but 3GPP Release 14 and higher is recommended. With new IoT network roaming agreements in place, IoT devices will work out of the box in developing countries when they become available.

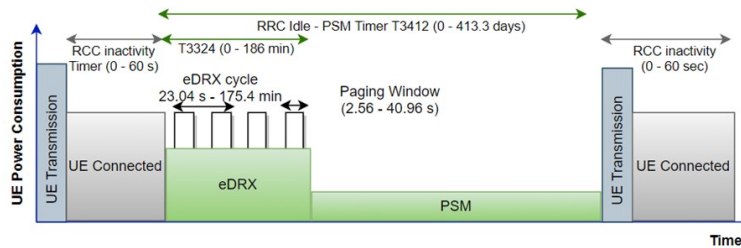


Figure 5.4: Overview of UEs Duty Cycle and Power Utilisation due to G3PP Standardisation Effort.

NB-IoT Deployment Modes

NB-IoT has three modes of deployment options as presented in Figure 5.5. The standalone deployment, which is considered the most expensive, requires the installation of new radio like in the case of GSM and skills to develop and deploy. On the other hand, NB-IoT can be deployed in either the in-band or guard-band mode. The guard-band and in-band deployment options use the 180 kHz single PRB of the LTE core network. The standalone mode is independently deployed as a dedicated carrier using spectrum greater than the required 180 kHz frequency bandwidth (400 kHz minimum). GSM wireless access networks and satellite communication systems may be used to deploy NB-IoT in standalone mode. This is achieved by refarming certain aspect of the frequency spectrum to include 200 kHz and 100 kHz guard-band for different operators and the same operator respectively deploying both GSM and LTE [291]. Guard-band mode is deployed within the existing guard-band of LTE networks since 5% of the LTE channel bandwidth is not fully occupied. NB-IoT design technology according to 3GPP Release 15 will be migrated to 5G radio access to provision LPWAN services since both have been designed to support the same frequency bands and can coexist orthogonally [313], but has a limitation of unwanted NR emission which degrade NB-IoT carrier power level. The In-band deployment mode exists in the PRB of an LTE carrier. This is the operational mode on which the NB-IoT study was conducted. The initial features and specification of the NB-IoT is outlined in table 5.5, leading to MNOs running trials and testbeds in different countries as shown in Figure 5.6.

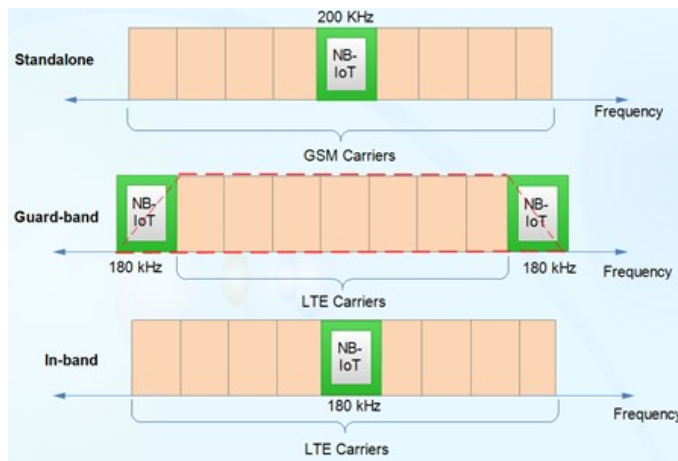


Figure 5.5: NB-IoT Deployment Modes.

NB-IoT Positioning Accuracy

Positioning accuracy is an enhancement of the NB-IoT network that could increase the application of NB-IoT across different sectors. Positioning accuracy is a vital aspect of IoT and applicable to most use cases such as asset tracking, environmental monitoring, wearable, and smart agriculture. The NB-IoT Release 13 on which the test was based can only associate the UE to the serving cell. Release 14 and other higher release standards provide enhanced Serving Cell Identity (SCID) measurement and Observed Time Difference of Arrival (OTDOA) which are more reliable options of obtaining UE position more accurately. The Time Advance (TA) eCID is a round-trip measurement (initial Round Trip Time (iRTT)) between the eNodeB and the UE, measured as $48.5 \mu\text{s}$ for sending 44 bytes of data through a 5744-window size. The value is used to compare the UE position to the serving cell. The OTDOA uses the measurement of Time of Arrival (ToA) on a set of DL Narrowband Positioning Reference Signals (NPRSs) from a set of time-synchronised eNodeBs serving the UE. In LoRaWAN, the Time of Difference Arrival (TDoA) and Received Signal Strength Indicator (RSSI) are two methods of determining IoT module position. It is important to state that the methods discussed above do not require the use of Global Positioning System (GPS) or Assisted (AGPS) which would make IoT devices more complex, expensive and power hungry [314].

NB-IoT Mobility Enhancement

NB-IoT device mobility is limited by the Radio Resource Control (RRC) being able to re-establish connection with an appropriate cell when a UE moves out of a cell coverage area through cell selection. The connection re-establishment is achieved through the user plane data support. The handover feature is not supported in Release 13, and mobility creates issues such as radio communication link failure when a UE moves from one serving cell to another. Release 13 support only stationary UEs, while Release 14 supports low mobility UEs [15]. Mobility on the other hand, is an inherent feature of LoRaWAN and the impact of mobility on LoRa communications is the reduction of packet delivery ratio. Mobility analysis does not apply under this scenario since the UE and LoRa gateway are within a single location (see figure 5.3). However, in [315], it is observed that message size and mobility degrade LoRa signal propagation and even higher in urban areas where high rise buildings would make light of sight more difficult to achieve. Applying NB-IoT for remote monitoring applications presents coverage, low cost, high connection, and other benefits. We identified the following as possible challenges of deploying NB-IoT:

- The availability of IoT networks such NB-IoT will depend on the mobile network providers offering and government regulatory frameworks.
- Most cellular IoT devices available are based on 3GPP Release 13. A significant gap exists in the implementation of new technology features and the technology process.
- To a certain degree, the security and privacy of NB-IoT solutions can rely on the robust security features of LTE. NB-IoT data within the LTE environment is encrypted except for connections between the application and cloud server where other security mechanisms, such as TLS can be considered.
- For scalability reasons, NB-IoT modules need to support IPv6 addressing scheme.

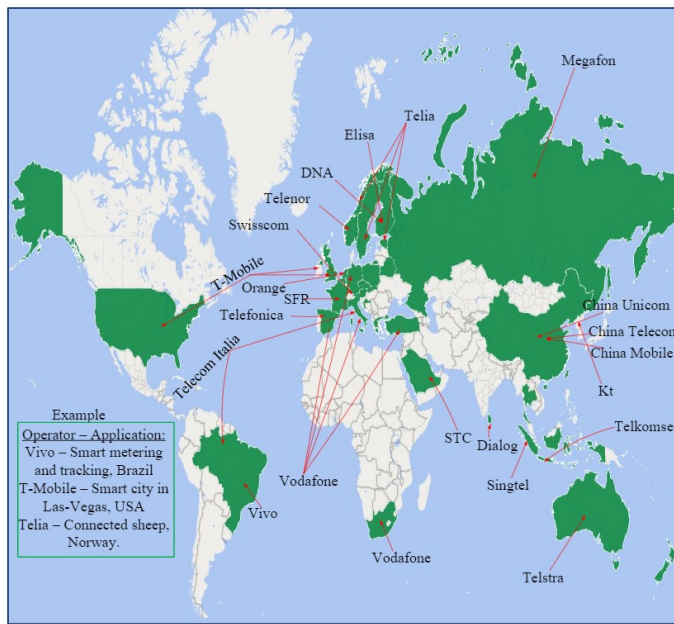


Figure 5.6: Global NB-IoT Deployment. Reproduced with permission from [Collins Burton Mwakwata], [Narrowband Internet of Things (NB-IoT): From Physical (PHY) and Media Access Control (MAC) Layers Perspectives, Sensors]; published by [MDPI], [8 June 2019] [9].

5.4.3 5G and LPWAN Integration

The Fifth Generation Cellular Network (5G) is the most recent cellular IoT standardisation effort. The 5G development agenda was not to replace cellular LTE IoT technology as it has dominated the IoT market but to meet the growing demand for network capacity and coverage. 5G is projected to reach 3.5 billion subscriptions in 2026 exclusive of IoT according to the 2020 Report by Ericsson [316]. In the same report, the 2026 IoT connection outlook based on NB-IoT and LTE-M was estimated to account for 45% of mobile IoT deployment. Hence, they were left out in the first 5G New Radio (NR) Release since MTC is already offered in LTE [317]. In 3GPP Release 15, LTE could offer reliability as high as 99.99%. However, to meet the LPWAN needs in 5G standards, 3GPP added features that allow cellular LPWAN to be seamlessly integrated into 5G with provisions for potential coexistence enhancement to be considered. The NR frequency band, numerology, beamforming, and duplex mode features are research areas of interest when integrating MTC into NR. Network slicing, network sharing,

and machine learning are other research areas of interest to determine secure means of leveraging the public network infrastructure to deploy 5G private networks [62].

5G is most suitable for low latency applications. The Ultra-Reliable and Low Latency (uRLL) teleprotection and remote access services in utility networks are examples of the benefits of using 5G to complement other LTE technologies. In the 3GPP Release 16 and above, 5G NR is being evaluated to support IoT deployment in the unlicensed spectrum and the possibility of achieving Integrated Access Backhaul (IAB) and unified non-terrestrial networks based on satellites to scale network coverage to hard-to-reach locations. The International Telecommunication Union (ITU) has since 2018 established a focus group to drive a vision beyond 5G by formulating the requirements of network 2030 and beyond [318]. The 3GPP standardisation process is expected to begin in 2023 and the possible release of the first 6G standard before 2030. There are many speculative studies already on 6G and development efforts by companies such as Samsung [319], Huawei [320], LG [321], establishing 6G research centres. The 6G road-map as proposed in [322] identified Ubiquitous Mobile Broadband (uMBB), Ultra-Reliable Low broadband (ULBC), and Massive Ultra-Reliable Low Latency Communication (mULC) as the major enhancements in 5G to be provisioned in 6G. The technologies that will enable 6G include aspects of new spectrum: dynamic spectrum management, millimeter wave, terahertz communication, visible light communication, optical wireless communication; new networking: Softwarisation and virtualisation, Radio Access Network (RAN) slicing, open RAN, quantum security; new air interface; new architecture; new modulation; and New Paradigms such as Artificial Intelligence (AI), Reconfigurable Intelligent Surfaces (RIS), Blockchain, digital twin and intelligent edge computing.

5.4.4 5G and IoT Technology

The introduction of Fifth Generation (5G) mobile technology in the early-2020s is driving industrial use cases with support for Enhanced Mobile Broadband (eMBB), Massive Machine-Type and Critical Machine-Type Communication (cMTC & mMTC) applications. Other industrial IoT concepts include Vehicle-to-Anything (V2A), Vehicle-

to-Everything (V2X), Vehicle-to-Vehicle (V2V), Device-to-Device (D2D), Machine-to-Machine (M2M). The previous versions of mobile communication, from 1G to 4G as shown in table 5.3 are unable to meet the stringent requirements of mMTC as it is focused on meeting the consumer oriented services such as voice, data and multimedia corresponding largely to cellular IoT. As discussed in section 4 and 3.1, NB-IoT and LoRaWAN are mMTC technologies that support latency insensitive applications. LTE-M and NB-IoT are cellular mMTC IoT technologies to be migrated into 5G environment, detailed explanation is found in 3GPP Release 15, see subsection 3.8.3. 5G technology is developed to support mMTC and provide better user experience in a consumer oriented services. In [323], ultra low latency, high data rate, ultra reliability and high availability are some of the features addressed in 5G use cases. The studies on 5G began in 2015 with 3GPP outlining the requirements and model designs. The study was scheduled to become livestream in 2020 with the 3GPP Release 14, 15, and 16 where New Radio (NR) air interface specifications and enhancements are discussed.

Table 5.3: Mobile Network Evolution

Network Version	Technology	Year	Speed
1G	Voice: NMT, AMPS, TACS	1980s	<2.4 kbps
2G	SMS: GSM, D-AMPS, IS-95, IEEE 802.11a	1990s	<64 kbps
2.5G	GPRS, IS-136, IEEE 802.11b	1990s	<64 kbps
3G	Web: WCDMA, HSPA, UMTS, Edge, IEEE 802.11g	2000s	2-100 Mbps
3.5G	HSDPA, HSUPA, IEEE 802.16d	2004s	<100- Mbps
4G	Mobile Internet: LTE, LTE-A, IEEE 802.16m, WiMAX	2010s	<2 Gbps
5G	Industrial IoT: NR, BDMA, SDN, Mm-Wave	2020s	20 Gbps
6G	Intelligent Connectivity: Blockchain, Terahertz	2020s	Tbps

5G NR is a configurable OFDM radio interface technology covering the sub-GHz frequency bands up to 100 GHz Millimeter Wave (mmW) as shown in figure 5.7. The compatibility of LTE network and NR technology becomes an important requirement to leverage the vast coverage of LTE networks and user devices. NR could be deployed within LTE carriers just like the current practices of NB-IoT and LTE-M. For 5G applications, Ultra-Reliable Low-Latency Communications (URLLC) is a major requirement and can be achieved by optimising retransmission down to a single event. Link adaptation and antenna diversity are two possible ways of varying data frame structure with

respect to meeting the correct symbol and slot characteristics [324].

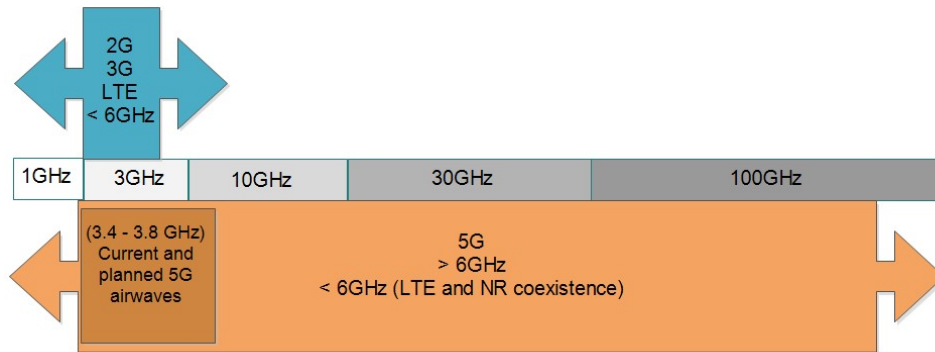


Figure 5.7: 5G and LTE IoT Spectrum

Cellular technology from 1G to 5G has design physical layer, network layer and other research problems. Some of the security issues include 1G - illegal interceptions, cloning and masquerading; 2G - message spamming and false injection; and 3G - IP-based attacks [325].

5.5 LoRaWAN and NB-IoT Implementations

The contribution of this paper is two-fold. The LoRaWAN and NB-IoT Testbed is implemented to demonstrate their capabilities and to measure and analyse the performance of QoS parameters under testing.

5.5.1 Design of LoRaWAN Testbed

The LoRaWAN network implementation is based on star network topology separated into front-end and back-end as shown in figure 5.3. The Things Network (TTN) is an open LoRaWAN platform that runs server infrastructure as a service. The Pysense node joined the Fipy gateway in Over the Air Activation (OTAA) mode added to TTN through the TTN Application Programming Interface (API) with limited time on-air of 10 messages in the downlink and 30 s duration per device per day. A Hypertext Transfer Protocol (HTTP) web application interface and database is integrated with the LoRaWAN application server to display TTN data. LoRaWAN private infras-

structure may deliver close to 846s/day time on-air as specified in the LoRa Alliance specifications. This reflects the potential challenges of applying LoRaWAN protocol to different applications of different performance requirements sharing the same network resources. Private LoRaWAN network platforms will be needed if the requirements of latency, reliability, and transmission patterns of different IoT applications in developing countries are to be satisfied, though as an alternative to licensed spectrum IoT solutions like NB-IoT and LTE-M.

5.5.2 Design of NB-IoT Network

In our recent publication, we have demonstrated the design and implementation procedure of NB-IoT testbed [279]. The NB-IoT testbed specification includes a LimeSDR (LMS7002M) that generates the standard LTE core MME and eNB physical signals from the same CPU that runs Ubuntu Intel Core i7-8550U at 4GHz, Ubuntu 16.04 x64 OS, 32G RAM, and x86_64-bit kernel. A Multiple-Input Multiple-Output (MIMO) transceiver based on Field-Programmable Radio Frequency (FPRF) for integrated circuit Digital Signal Processing (DSP). The eNB has a 30.72 MHz reference clock, 780.500 MHz DL frequency, 725.500 MHz UL frequency on band 28 (DL EARFCN = 9435), filter order 4, filter bandwidth of 5MHz, real pole 1st order filter of 2.5 MHz, and transmit and receive sample rate of 1.92 MSps. The NB-IoT node device is the Fipy and Pysense expansion board programmable in the Visual Studio Code and Atom and supports NB-IoT, LTE-M, SigFox, LoRa, Wifi, and Bluetooth IoT wireless technologies. Figure 5.8 shows our testbed in operation with illustrations on the functionalities and table 5.4 the parameters configurations. With this, sensors could then be strategically positioned in various regions to monitor water quality and air pollution levels and the data collected transmitted to IoT cloud platform for analysis.

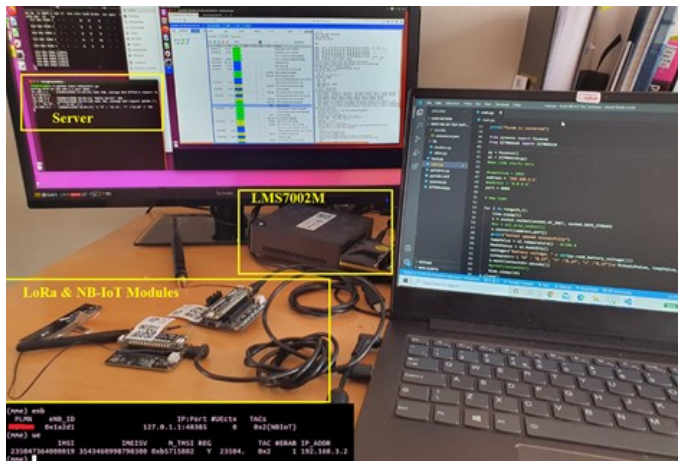


Figure 5.8: LPWAN Network in Operation.

Table 5.4: NB-IoT Network Configurations. The coverage level corresponds to the NPRACH configurations

NB-IoT Features	Values
NPRACH Detection Threshold	40dB
NPDSCH Repetition & TBS	1 & 3
UL Subcarrier Spacing	1
Subcarrier	15 KHz
NPDCCH	8
NPUSCH Subcarrier	12
frequency carrier	Band 28
Bandwidth	180 KHz
Receive Power	-15 dBm
Transmit Power	-3 dBm
Sample Rate	30

A similar study that routed LoRaWAN traffic through EPC demonstrates that licensed and unlicensed LPWAN technologies can be integrated and served by a single network core [130]. Such integration is very relevant given the emerging theoretical studies on deploying NB-IoT on the Sub-1 GHz unlicensed band that complies with the Federal Communication Commission (FCC) and European Telecommunication Standards Institute (ETSI) regulatory requirements [326, 327]. The MulteFire Alliance (MFA) specification presents an opportunity to utilise LTE in unlicensed, shared, and large bandwidth in the global unlicensed 5G spectrum bands to lower the cost of deploy-

ing private LTE networks. However, in this scenario, our contribution lies in demonstrating the real-world performance of a licensed NB-IoT technology for IoT application using the same end device that has been evaluated in the LoRaWAN Things Network platform. An integrated gateway and network core as shown in figure 5.9 then become a novel deployment alternative in an environment where cellular network occupies more than 99% coverage like the telecommunications services market share by technologies as deployed in Nigeria [298].

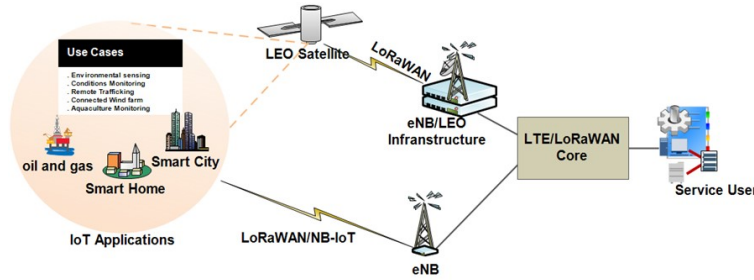


Figure 5.9: LPWAN Integrated Architecture.

A multi-standard approach can be adopted where, for instance, a cellular IoT device can support more than one cellular network standard. Multi-Radio Access Network (Multi-RAN) technology will allow multiple LPWAN technologies to be integrated and separated based on use case requirements. Hybrids of Wi-Fi and LoRaWAN [328], and LoRaWAN and NB-IoT [289] are a few of the multi-RAN technologies proposed for global IoT connectivity. These will however come with increased processing, memory and energy consumption requirements. The increased device complexity means an increase in the cost of building applications and support infrastructure.

5.6 Network Performance Analysis: NB-IoT vs LoRaWAN

Like other IoT networks, NB-IoT network performance is evaluated based on the data latency, throughput, battery utilisation, and security. In summary, we present the general NB-IoT testbed performance in the in-band mode of operation that uses the LTE PRBs as specified in the 3GPP Release 13 164 dB MCL. However, the general performance mostly differs irrespective of any standard assumptions, depending on the

mode of operation, the IoT device specifications, and the eNB and MME implementations. The many performance results as presented in the 3GPP TR 45.820 [329], and in [70, 330] are theoretical in the light of limited practical NB-IoT test network performance results. In [10], field testing was performed using different test equipment and was based on simply evaluating the performance of RF coverage and MNO's signal quality. The results of our NB-IoT and LoRa test networks is presented based on battery life, throughput, security and latency QoS parameters. While quantifying the power consumption of the testbed, two approaches have been used, RTT of a PING request and transmission of certain data sizes. With the testbed configured with high a NPDCCH repetition rate of 8 and a low coding rate in the case of NB-IoT to increase the detection rate, the power consumption analysis is considered robust. An average delay that is inclusive of the RRC transmission is obtained for TCP transmissions between UE and Server located within the same location. The equivalent average power peaks are shown in figure 5.15.

5.6.1 Latency

As expected, NB-IoT experiences high delay than the LTE network due to the transmission pattern of the Downlink Control Information and data being sent via the downlink control and shared channels, respectively. The coverage capacity of NB-IoT network depends on several factors such as the RF link budget, antenna gain, transmission power, and the target is to achieve a high data rate at 164 dB MCL through an adequate performance of LTE or GSM physical channels. For instance, this would mean, a 90% Narrowband Primary Synchronisation Signal (NPSS) and Narrowband Secondary Synchronisation Signal (NSSS) detection rates with high synchronisation accuracy to meet the latency requirement of 10s, and also, the NPRACH timing advance of 3 μ s. The latency target of NB-IoT network performance during RRC connection procedure and data rate transmission is to deliver 10 s. The stateful nature of LTE uplink and downlink transmissions increases the data overhead. The TCP Retransmission Timeout (RTO) of 244 ms occurred following a 44 bytes transmission segment. The latency in the uplink and downlink channels as presented is the sum of the time spent in the

synchronisation, resources reservation, data transmission and reception processes. As observed, the message size does not directly impact the delay although it does increase the energy consumed as the UE has to wait for message acknowledgement in successful transmission. In the LoRaWAN platform, we considered latency as the duration between when the data is sent by the Fipy and received by the web server. For sending 16 bytes of data in a custom format to the web server per day, for every experiments, between 2 to 3.5 seconds latency was measured between when the data was send and received by the web application. In the LoRaWAN network, with a packet length of 20 bytes in class A mode, a high latency of 2s is needed for packet retransmission. However, the success rate of every transmission is above 50%.

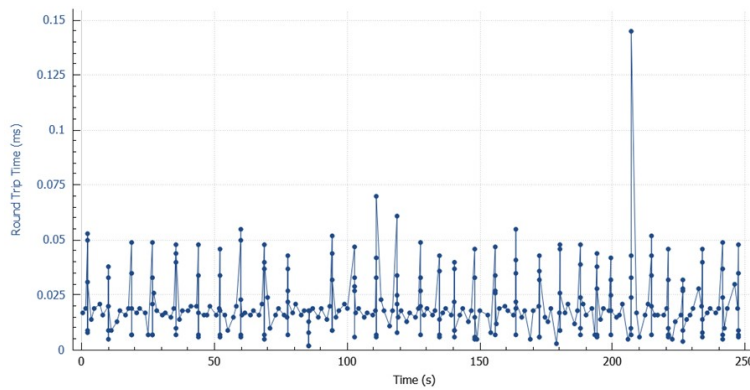


Figure 5.10: Round Trip Time between the LTE eNB Server and client.

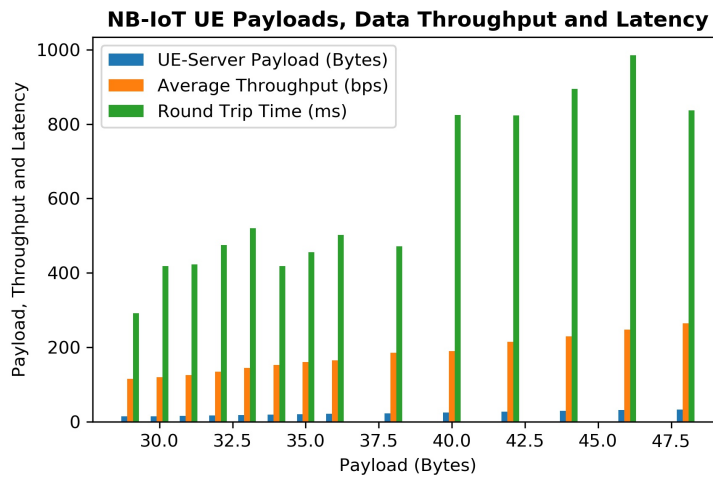


Figure 5.11: NB-IoT Throughput, Latency for Data UE-Server Payloads

5.6.2 Throughput

Data transfer technologies, as specified in the 3GPP documentation such as the Multiple Input Multiple-Output and Carrier Aggregation provides higher data transfer rate and high-speed packet access networks in LTE. The test results for bidirectional data transfer, uplink and downlink data throughput in LMS7002M for sending 44 bytes of TCP message. For the in-band mode of operation, maximum of 1.57 kbps and 1.59 kbps were obtained for the uplink and downlink channels respectively. It is important to note that the performance of the network could be improved if a different UE is used and the number of packet losses is reduced. The actual data throughput for NB-IoT is usually a fraction of the percentage data lower due to overheads. The category of UE, network cell bandwidth configuration, and mode of transmission play an important role in achieving good NB-IoT network performance. In a case where a single UE is attached to an NB-IoT network, it makes use of the whole available bandwidth for transmission. The highest signal level is required for high data rate transmission and aspects such as fading, link loss, the line of sight, noise and interference from other base stations could degrade the signal level. For sending between 29 - 48 bytes, the average throughput varied between 115 bps to 264 bps between the UE (192.168.3.2) and the server (192.168.3.1). In LoRaWAN, the size of the data sent to and received from the TTN is 16 bytes with LoRaWAN overhead of 14 bytes. The size of the LoRa payload is one of the features that determine the transmission time. For the 20 bytes LoRaWAN packet size, with a separation distance of 3 meters between the Pysense node and the Fipy gateway to avoid saturating the receiver amplifier, an estimated time on-air of 31.024 ms is obtained for SF of 7, BW of 125 kHz, data rate of 5 and indicative bit rate of 5470 bits/s. As a single channel gateway, when the distance is increased, the transmission time increases resulting in reduced throughput and an increase in bit error rate. NTdl & Ntul is the number of transmissions in the downlink and uplink channels, while BRdl & Brul is the Bitrate in the downlink and uplink channels, respectively. In the event of retransmissions, the latency increases, as shown in the Ntul spikes between 40 - 48 bytes of data payload in figure 5.11.

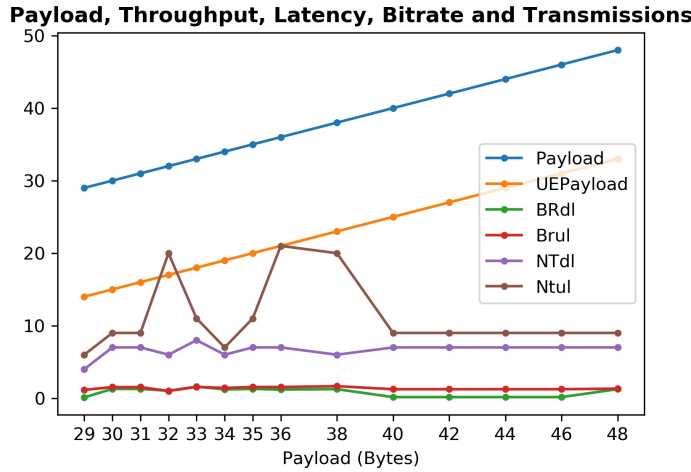


Figure 5.12: NB-IoT Downlink and Uplink Bitrates for In-band Modes of Operation

As shown in figure 5.6.2, for every transmission window as shown in figure 5.14, maximum data throughput of 264 bits/s is achieved by the UE which is far below the average throughput established between the LTE eNB server and the client server. During periodic ping requests of 48 bytes between the UE and the network, an average of 655.84 ms Round Trip Time (RTT) is recorded due to the high repetition rate in the subframes. A high repetition rate is expected in NB-IoT networks where signal propagation is inefficient. Note that the Server to UE transmissions was a constant value of 15 Bytes that with a constant DL and UL Bitrate of 396 and 436 within 3 and 5 number of transmissions respectively. Maximum and minimum throughput of 308 and 45 bytes respectively for the round trip time in figure 5.10. Retransmissions (rtx 1, 2 and 2) occurred in a few of the transmissions windows and courses spikes in the number of packets that increased the maximum packet to 9 packets/sec. At 50 bytes (rtx3) of data payload, the successful transmission rate decreased and, in most cases, resulted in unsuccessful transmission.

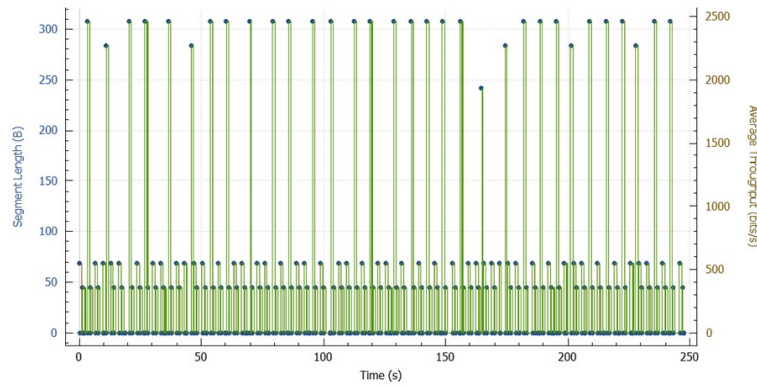


Figure 5.13: Average Throughput between the LTE eNB server and MME Client

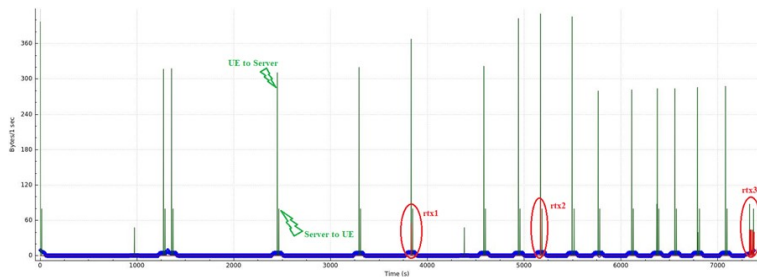


Figure 5.14: NB-IoT Data Throughput for Successful Interval Transmissions at a maximum of 7 packets/sec .

Battery Life

The energy consumption of IoT devices are use case dependent and influenced mainly by several protocol-specific factors like hardware synchronisation, OFDM modulation scheme, network coverage levels, high message repetitions, software and application capabilities [71]. The energy consumption target of NB-IoT devices according to 3GPP Release 13 standard is 10 years when operated between 20dBm and 23dBm. This requirement includes devices that are battery-powered, non-rechargeable and used in the most difficult terrain. The power consumption analysis is one way of computing the battery life of IoT modules. The comparison of power consumption analysis of Fipy module in NB-IoT and LoRa networks is based on USB power meter. It is important to note that the timing resolution of the power meter is a critical requirement and may affect the following results presented in table 5.5. As Fipy is a Release 13 standard,

its radio components remain turned off once registered to the NB-IoT network except when there is scheduled data transmission. At this point, the UE is in an idle state, and the channel is monitored for any handover procedure using paging signals. The eDRX included in the higher 3GPP standardisation is to allow UEs to stay in a sleep state for up to T413 (413.3 days) to save more energy. For every packets transmissions, bursts of power consumption is observed in the CPU and NB-IoT power transmission measurements in figure 5.15.

Since the Fipy was not battery powered and to keep the tests to a reasonable period, the evaluation of battery life was limited to the RCC connection procedure and data transmission. With an average of 3 mAh needed to reconnect the NB-IoT module to the network, an uplink message consumed an average of 1.8 mAh for 44 bytes of data at 3.3v regulated output voltage. For instance, this deviates by a high margin from the 100µAh measured for uplink messages in LoRaWAN. As concluded in [62] based on ideal conditions, the 10 years lifetime in NB-IoT can be met if 24-hour data transmission intervals are implemented and lowering the time scale to 2 hours becomes unrealistic at 146 dB MCL. The mode of operation does not impact the uplink transmission, a major determinant of power consumption reduction. In release 14, where a power class of 14 dBm enables the use of smaller cell batteries in new NB-IoT deployment, more efficient power consumption is expected. This improvement over Release 13 helps to reduce the Power Amplifier (PA) drain current which negatively affects the UL coverage and the maximum coupling loss (MCL) to 155 dB. An example is the Fipy NB-IoT module, a Release 13 device that supports 20 and 23 dBm power classes. As shown in figure 5.15, without transmissions, -20.4dB and -2.72dB full scale is the maximum power, -35.5dB and -17.7dB Root Mean Square (RMS) full-scale value, 8.40% and 2.72% CPU power for the transmit and receive channels respectively. During transmissions, an average of -5.68dB and -2.99dB full scale is the maximum power, -31.4dB and -17.1dB RMS full-scale value, 6.32% and 1.85% CPU power for the transmit and receive channels respectively. This shows that NB-IoT consumed more power than LoRaWAN due to its complicated communication procedure irrespective of the PSM and eDRX power saving modes. A greater part of the energy is drawn during the synchronisation, joining,

and connected state of the UE.

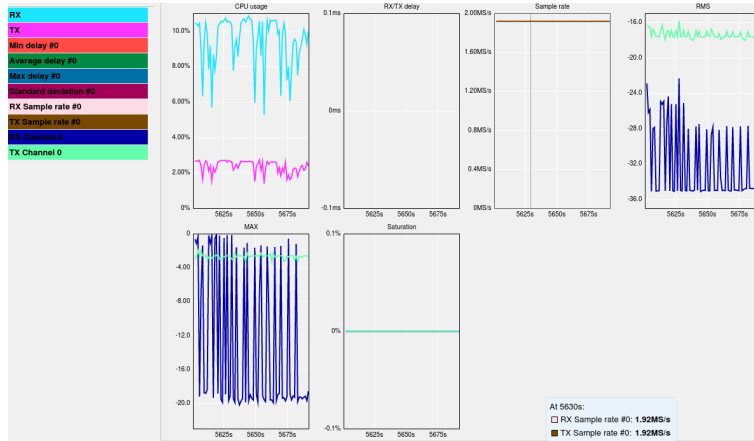


Figure 5.15: NB-IoT CPU, Receive and Transmission Channels Power Consumption.

In the LoRaWAN test, the IoT module (Fipy is used as the LoRa gateway and LoRa Node) and the test parameters include coding rate of 4/5, 125 kHz bandwidth, class A and Spread Factor (SF) of 7. The SF influences the power consumption level since it determines the time it takes radio links to transfer data. LoRa network gateways are diverse, a receiving gateway can become a serving gateway. This reduces end devices power consumption since devices closer to the edge can become gateways. The asynchronous nature of the LoRaWAN network allows UE to sleep as often as desirable based on the class of configuration. To achieve an instant downlink communication, the IoT device must be configured as a Class C, and scheduled transmission modes in Class B and A is recommended for efficient power consumption. In both networks, allowing more frequent data transmission would reduce the battery lifespan. The total energy required to perform a single test procedure in LoRaWAN was measured as 1mAh. Similarly, the uplink transmission for LoRa consumed approximately 100 μ Ah which far lower than 1.8mAh consumed in NB-IoT network. This shows that LoRa is more power efficient than NB-IoT and should be considered as a primary deployment option for extremely low data applications. To achieve reduction in energy consumption in LoRaWAN such as water quality monitoring, transmission should be scheduled based on use case.

Table 5.5: NB-IoT vs LoRaWAN Average Power Consumption, Latency, and Throughput.

Features	NB-IoT	LoRaWAN
Joining Network	3mAh	1 mAh
Uplink Message (44 bytes)	1.8 mAh	100 μ Ah
UE Class	Cat NB1	A
Data rate (20 bytes)	0.6 bps - 4 bps	
Frequency	28 Mhz	EU868 MHz

Security

NB-IoT security capabilities are based on the radio access, network core and user data encryption of LTE system. As detailed in our previous study on the security of IoT networks [278], LTE-based technologies use encryption, authentication, and integrity protection mechanisms to provide data access and non-access stratum signaling confidentiality, integrity and availability between UE and core network, and UE and Radio Network (RN) respectively. In the network shown below in figure 5.5, the MME uses NAS signaling security commands to secure UE and MME messages as shown in figure 5.16. UE contains the universal subscriber identity module (USIM) where the security keys and UE identifier are stored. Communication between UE and access network (AN)/serving network (SN) requires authentication and secure access to services over radio interfaces with ciphering and user data integrity support between UEs and MME.

```

Replayed UE security capabilities:
0xf0 (EEA0=1, 128-EEA1=1, 128-EEA2=1, 128-EEA3=1, EEA4=0, EEA5=0, EEA6=0, EEA7=0)
0xf0 (EIA0=1, 128-EIA1=1, 128-EIA2=1, 128-EIA3=1, EIA4=0, EIA5=0, EIA6=0, EIA7=0)
0x00 (UEA0=0, UEA1=0, UEA2=0, UEA3=0, UEA4=0, UEA5=0, UEA6=0, UEA7=0)
0x00 (Spare=0, UIA1=0, UIA2=0, UIA3=0, UIA4=0, UIA5=0, UIA6=0, UIA7=0)
IMEISV request = 1
Hash MME:
Length = 8
Data = 38 24 7d 1c e6 35 71 f1

```

Figure 5.16: UE Security Capabilities.

Security is also an important part of LoRaWAN network primarily in ensuring an authenticated connection, integrity protection and confidentiality in the communication process. Three layers of security are common in LoRaWAN network: device; network; and application security. Device security ensures that only authenticated IoT

device connection is accepted by the network. For NB-IoT, Network and application layer security ensures the authenticity of nodes and confidentiality of data respectively. To build a truly secure LoRaWAN network, in this scenario, LoRa messages must be encrypted using either AES-128, DES-128 or SHA-256 since they are the best hash/encryption algorithm support in IoT modules such as Fipy in addition to WPA, TLS/SSL security support for applications. Due to the limitations of Release 13 UEs in carrying out successful transmissions at 50 bytes as shown in figure 5.14, we will present the evaluation of these security mechanisms using higher standard UEs in future work. Security techniques contribute substantial data overhead that will be better processed using IoT devices with higher processing power. Most importantly, securing IoT networks could be as simple as implementing security measures such as performing server tasks locally where possible to reduce the security vulnerabilities of the public internet/servers; ensuring message content length-padded to avoid disclosure of side information through the length of a short message; security key generators being random of significant length; security keys loaded on the end device in a trusted partition and other good security practices of LPWANs [300].

5.7 Conclusions

In this section, we have presented the sustainable opportunities that licensed and unlicensed LPWAN could offer for IoT development in developing countries and equally compared LoRaWAN and NB-IoT from power consumption, security, latency, and throughput perspectives. With Nigeria as a case study, we discussed the practical challenges and opportunities of deploying LoRaWAN and NB-IoT technologies. The real-world performance/power measurements as presented show that NB-IoT and LoRaWAN can potentially drive the actualisation of SDG goals in developing countries, such as providing effective asset tracking and environmental monitoring solutions. However, the increased energy efficiency of LoRaWAN suggests that when the QoS requirements of a licensed solution are not required, LoRaWAN could offer savings in a like-for-like deployment though at a reduced QoS. However, the test results proved

that, on average, NB-IoT outperformed LoRaWAN on data throughput, latency and security. On the other hand, the roles that the current GSM and LTE MNOs will play to facilitate licensed IoT penetration in developing countries here considered hard-to-reach locations were also presented. The important features of NB-IoT 3GPP standard Release 14, 15, and 16 were discussed; while the performance of Release 13 was demonstrated in our testbed, we have shown the specific performance of the testbed on power consumption, data throughput, latency and security of the network as four network features for facilitating NB-IoT for other use-cases. New experimentation capabilities, as introduced in our testbed allowed LoRaWAN integration and present evidence of spectrum needs, power utilisation, latency, data rate, and security to guide deployment decisions. These are essential in determining the reliability of LPWANs service requirements like NB-IoT guarantees data delivery but at higher energy costs while the duty cycle regulations and ISM signal interference affect the reliability of LoRaWAN at the benefit of less energy and cheaper to deploy.

5.7.1 Potential Benefits and Drawbacks of Integrated LPWANs

- **Wider Range of Applications** - When multiple LPWANs such as LoRaWAN and NB-IoT are supported and integrated on a single IoT device, the effective coverage area will be that of LoRaWAN and NB-IoT. Though switching between multiple technologies causes an increase in energy consumption, cost of the IoT modules and computational overhead increase, it has the potential to rapidly increase the IoT footprint in developing countries as the networks can be extended using a single gateway. The IoT devices can dynamically switch between the LPWANs available. Optimisation of circuit and components design could improve cost, energy and data overhead challenges.
- **Improved Reliability** - An integrated LoRaWAN and NB-IoT network guarantees message delivery. This means a more robust and intelligent network that can periodically switch technology types based on message sizes and QoS requirements. NB-IoT for more frequent transmissions while LoRaWAN network for less sensitive and periodic data transmissions.

- **Improved Latency** - The availability of more than one LPWAN option for message delivery increases the opportunity to spread IoT data over multiple technologies based on the criticality of the application, payload size, and power source. Depending on the application, variable message sizes can be efficiently and reliably sent. For instance, indoor transmissions can be performed using NB-IoT [331].
- **Reduced Cost** - The cost of deploying NB-IoT is generally higher than LoRaWAN. NB-IoT operates in the licensed spectrum, and the costs of acquiring spectrum and base stations limit the deployment of private cellular networks. However, when studies on NB-IoT in the unlicensed band become successful [327], [326], it will be less expensive and power-efficient to design IoT modules to support multi-radio access technologies.

Chapter 6

Bandwidth and Security Analysis of TLS and IPSec-Based Internet of Smart Grid

6.1 Introduction

The use of legacy IoT devices and protocols in the modern smart grid networks makes the power system very vulnerable to different forms of internal and external cyber threats. The implementation of new power network security standards such as the IEC 62351 and IEC 62443 is a reliable way of providing the power networks with common security functions such as data encryption and integrity, and information confidentiality. Secure communication networks is a fundamental part of generation, transmission and distribution smart grid architecture. With the evolution of smart grids and applications, power distribution networks need scalable, flexible, distributed and secure end-to-end communication networks to protect the grid from all potential vulnerabilities. This chapter highlights the necessary security mechanisms and the resulting bandwidth needed to effectively monitor and communicate with all of the secondary substations of any Distribution Network Operators (DNOs) via Ethernet. In order to determine the security and bandwidth requirements, the existing and emerging

applications in each utilities industrial IoT devices were discussed. In this regard, we employed two-level of security - Internet Protocol (IP) Security (IPsec) and Transport Layer Security (TLS) to give flexibility and resilience in such a study. In this section, the bandwidth and security requirements of secondary substations of the future are investigated, considering the security overhead caused by applying different security techniques. The study involved testing of different cybersecurity scenarios and several setups on a fully secured Internet Protocol (IP) based Remote Terminal Units (RTU) running IEC 62870-05-104 protocol. Aiming to understand the bandwidth implications of applying (TLS), IPsec or the combination of the different security techniques, we carried out a security and bandwidth analysis by applying different configurations on a test network setup that resulted in an average of 2-3 folds of increase in bandwidth if both IPsec and TLS are used to secure the connected smart grid IoT devices over Ethernet. The results presented in this section are part of the University of Strathclyde Power Network Demonstration Centre's (PNDC) core research project, a setup of a functional smart grid experimental testbed. Different configurations and setups were investigated aimed at understanding the effects of adding security techniques to the existing system from which recommendations were made to the DNOs for medium and long-term needs.

This chapter is divided into four sections: section 6.2 explains the key security and spectrum requirements for the Internet of smart grid; section 6.3 presents the current spectrum and security challenges facing the power utilities from adopting IoT technology. It also discusses the current DNOs smart grid practices and key published work in smart grid security; Section 6.4 discusses the security and bandwidth test setup procedures; Section 6.5 analysed the findings; and Section 6.6 concludes the paper with a summary, and necessary recommendations for DNOs and highlights the future work presented in section 7 that would focus on radio technology involving other manufacturer's RTUs for remote access investigations.

Majority of this chapter is a conference paper presented at the IEEE PES Innovative Smart Grid Technologies Conference (ISGT-Europe), The Hague, The Netherlands — 25-28 October 2020

6.2 Security Requirements for Smart Grid

The next-generation power networks are smart grid systems with intelligent communication infrastructure with the security objectives of ensuring availability, integrity and confidentiality [332]. Being intelligent, the scope of security requirements of such systems increases as a result of growing dependency on Information and Communication Technology (ICT). Implementing security in the smart grid should meet key bandwidth requirements in order to achieve robust and cost-effective solutions. Other cyber security objectives include high flexibility, reliability, and sustainability [333]. The smart grid requires reliable communications technology for data exchange between control centres and the associated inter-connected IoT devices throughout the power networks and in the area of efficient remote management. The heterogeneous nature of the smart grid system (numerous IoT devices of varying age from a number of different vendors over a wide range) creates several challenges for the communication network. It makes a single unified functional protocol impracticable to enable seamless connectivity and unified security solutions. Secondary substation automation, where many devices are in the hard-to-reach areas, will need reliable communication technologies to connect field IoT assets to the control centres. Wireless technologies such as the LTE and 5G are suitable solutions for such use cases, but deploying any wireless technology is expensive. It will require the acquisition of an appropriate spectrum based on the data overhead [334].

While some wireless technologies such as LoRaWAN, an unlicensed spectrum discussed in section 3.1 can be relied on for general IoT services, they cannot guarantee security and good quality of service in smart grid critical applications. On the other hand, for mission-critical applications, one would suggest commercial cellular network operators since they utilise licensed spectrum technology and are readily available at low costs. While cellular industrial IoT solutions such as NB-IoT and LTE-M may be applicable where low latency is not a critical requirement, the utility networks have far more stringent connectivity and security requirements than most commercial M2M wireless networks. Specifications of LTE and 5G technologies meet the technical ob-

jectives of smart grid applications such as Advanced Metering Infrastructure (AMI), Plug-in Hybrid Electric Vehicles (PHEV), and Phasor Measurement Units (PMU). The topology of the power networks and the locations of the distrusted industrial IoT devices make it harder for DNOs to rely on one technology for deployment. Therefore, this suggests the need for dedicated wireless networks to be provided by the utility networks themselves, requiring dedicated spectrum allocations. Wireless spectrum for utility network provisions will take into account that future applications will involve greater numbers of devices and that each of these devices will require more bandwidth to give increased quality of measurement, and the possibility of cyber-attacks that could target the power network will increase. Cybersecurity is therefore essential for any communication technology for power utilities. Moreover, as the power utilities are interconnected with ICT infrastructure, the possibility of cyber-attacks that could target the power network will increase. This will also increase the security requirement and, in turn, the spectrum allocation needed.

Various wireless and wired communication technologies such as Power Line Communication (PLC), Fiber Optic Communications, Asymmetric Digital Subscriber Line (ADSL), Narrowband Internet of Things (NB-IoT), WiFi, Microwave Networks, Ultra High Frequency (UHF) Telemetry, Mobile Technologies (GSM, 3G, 4G/LTE, 5G) and Satellite Communications have been employed in power utilities [335]. Most DNOs globally rely on a combination of more than three of these communication technologies for various grid applications and connectivity. For instance, the UK national coverage maps of DNOs suffer from the lack of coverage, especially in the hard to reach parts of Scotland [336]. While the data rates needed for each RTU from DNOs differs from one DNO to another, all the existing data rates are without any security plan and recovery methods in place, i.e implementing IEC 62351 and IEC 62443. While a great deal of literature exists on smart grid security, ensuring privacy in smart grid metering network [165], security challenges of retrofitting IEDs in smart grid [337], research implementing IEC 62351-7 [211], the effect of adding security (multiple) on the bandwidth requirements has not been investigated.

6.3 Communication Challenges in Power Utilities

Communication technology is central to the performance of smart grid functions such as teleprotection, control, monitoring and management. There are several challenges facing the deployment of any communication technology in power networks today. Some of the main challenges include the reliability, security, availability and cost-effectiveness of the communication links between the control centre and secondary substation on-field IoT devices. Wireless technologies can be deployed rapidly and may not require complicated construction and civil engineering work, making them easier to use in different smart grid applications. Currently, power utilities globally use many different communication technologies to connect on-field devices to control centres. Communication technology will be chosen based on the application and the availability of the wireless signals, coverage intensity and strength. Ultra High Frequency (UHF) telemetry is widely deployed by the power utilities worldwide as an option to support Supervisory Control and Data Acquisition (SCADA) and other power system communication protocols to control and monitor reclosers and switches. Recently, some DNOs in the UK have deployed Broadband Global Area Network (BGAN) satellite technology to remotely control and monitor their distributed assets in hard-to-reach areas [338]. Other wireless Low Power Wide Area Network (LPWAN) technologies such as LoRaWAN and Sigfox can be used for asset monitoring and fault detection [93].

Legacy utility communication protocols suffer from many limitations. Some are vulnerable to cyber-attacks. Others have some drawbacks preventing them from supporting massive integration with the new utility applications (i.e., electric vehicle charging stations, distributed storage, distributed generation, and demand response-related needs for IoT devices). Another important point is the overhead issues that come from integrating these legacy power communication protocols with the IP network, which is the underlying network protocol for establishing a connection between the IoT devices and the central control centre. The status of most wireless technology used in connecting the secondary substation suffers from limitations such as the narrowband channels, lack of coverage and integration with legacy assets. The lack of coverage is

because secondary substations are in hard-to-reach areas. Extending the network coverage will increase the cost due to extra network resources required to manage the diverse communication technologies operated by the power utilities to enable the connectivity of the secondary substation with the control centres. Systems integration, multi-hop communication channels, and any electrical/environmental noise could affect deploying security measures in the secondary substation.

With the evolution of the smart grid and the growth of the new end-user applications and number of endpoints, many existing wireless technologies (such as UHF telemetry) will not offer the needed connection capacity. Also, the EU National Information Systems (NIS) directive [339] and the security requirements of other grid applications such as Low Voltages (LV) monitoring, solid-state transformer control and active network management will drive bandwidth requirements and increase the demand. This agrees with [193] that the addition of more security mechanism increases the number of data bytes, which increase the bandwidth. The question of how much bandwidth the power utilities need to cope with the current and emerging intelligent grid requirements is not easy to answer. To estimate the required bandwidth, different scenario testing was carried out at PNDC to help understand the bandwidth required for the secondary substation taking into consideration security overhead, as will be illustrated in the remaining part of this chapter.

6.3.1 Security Requirements for Secondary Substation

Wireless technology plays a vital role in the remote monitoring of smart grid assets in hard to reach areas. Power utilities need a real-time and reliable two-way communications network that extends beyond the distribution substations to the customer premises [340]. To meet these objectives, the wireless communication networks used in power utilities must have enough capacity to support the increasing data requirements of the grid due to increasing energy sources while being highly reliable and providing low latency communications. Moreover, the technology should provide high security to prevent cyber-attacks. Other requirements include supporting legacy equipment and having a high degree of power back-up to maintain the operation during any power

failure since the communications network will be required to bring the power network back online. When deciding which communication technologies are appropriate for secondary substations, the basic requirements of smart grid communication infrastructures such as bandwidth and security must be met. Additionally, network performance metrics such as availability, accessibility, quality of service, maintainability, resilience and affordability are also considered for the following reasons:

- **Availability** - The service/network is always required to be available and guarantee 24 hours (uninterruptible service) for control applications.
- **Accessibility** - The RTU uses the communication networks to send the required messages to the control centre. This means having enough bandwidth capacity for the RTU to transmit data via wireless technology.
- **Quality of Service** - Any appropriate communication technology should be able to manage and exchange high-quality data with less packet loss, latency and jitter.
- **Maintainability** - The communication technology should be able to be repaired in a suitable time frame irrespective of technical challenges.
- **Resilience** - The technology should be able to deal with any connection failure and recover rapidly.
- **Affordability** - This should be considered for large-scale field deployments and how cost-effective their integration with existing systems (e.g. enterprise network) is, along with the lifetime cost of operating the communications solution.
- **Power backup** - The substation batteries should have enough capacity to meet the standing demand for 72 hours. This will guarantee adequate backup power for the site to remain in operation for at least 72 hours after a power supply loss. Confirming that auxiliary systems and command and control structure remain unaffected after grid failure (i.e. black start procedure after a blackout) [341] - [342]. For secondary substation applications, at least 24 hours of backup power is needed to maintain the operation during any unexpected loss of power scenario.

6.3.2 Availability of Radio Spectrum

Radio spectrum is a scarce resource when reference is made to the spectrum bands suitable for cellular services. The scarcity comes from the underlying constraints of cellular devices to deliver various services without interference. Spectrum allocation is an important requirement for any wireless technology and must be planned if the coverage and capacity obligations that come with the licenses are to be met. Meeting the coverage and capacity requirements is crucial for the smart grid of the future. With enough spectrum in a proper band, rural coverage and urban capacity can be satisfied, keeping in mind that the demand for spectrum will continue to grow as power applications inter-connectivity increases. A single spectrum band will not be suitable to address the divergent future market needs for coverage and capacity as evident in figure 6.1 contained in Euro-5G project [343]. Low band (700 MHz), mid band (3.4 - 3.8 GHz) and high band (24.25 - 27.5 GHz) are considered for 5G deployment across Europe. In the UK, the Office of Communications [OfCom](#) is developing a strategy for managing some spectrum frequency bands over the next decade, and part of the process is to understand the bandwidth requirements for smart grid applications.

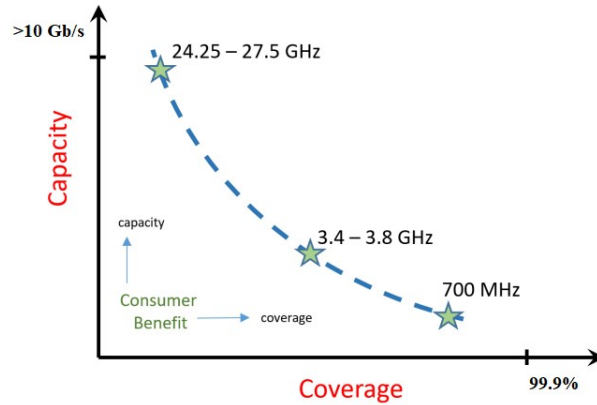


Figure 6.1: Quality Illustration of Coverage and Capacity vs Frequency

DNOs require a spectrum below 2 GHz that offers better rural coverage with good capacity and better signal penetration for their remote sites. However, the available bandwidth below 2 GHz is restricted to few narrow frequency bands that are considered a very busy spectrum and its link bandwidths are constrained below 10 Mbps according

to Ofcom's frequency band review [344]. Higher frequency bands of more than 2 GHz suffer from several challenges and drawbacks for power utility applications. While the utilities have many infrastructures, access to sites suitable for mounting transmission equipment is more limited. Much control equipment is underground or in basements in cities. The limited coverage and weak signal penetration of higher frequencies would make deployment costs at high frequencies uneconomic. The main limitations for the use of high-frequency band signals can be summarised as follow:

- **Coverage** - Massive cells will be required to improve the limited coverage of tens of meters and get as much throughput as possible. Maximising distance while maintaining low costs and attenuation problems are better achieved using lower bands.
- **Weak signal penetration** – High-band spectrum signals can carry lots of data for a limited short distance due to attenuation since they are easily absorbed by the atmospheric moisture, gases and physical objects such as buildings.
- **Cost of deployments** – Limited transmission range and reception. The cost of deployment will be high due to the increase in new communications infrastructure.

In the UK, there are several bands available below 2GHz, which could be considered as potential options for the DNOs for any future development of a private wireless technology (Private LTE) for the smart grid. The availability of 87, 88 and 31 MHz bands are possible options for a dedicated spectrum for the smart grid. The advantage of such bands is that the transmitted signals can better penetrate through the surrounding environment and offer excellent coverage. However, the bandwidth will be strictly limited and may not exceed 5 MHz bandwidth in each band. For instance, the bands 410-415 and 420-425 MHz consists of 2 x 4 MHz with 10 MHz duplex spacing, which is currently fragmented across these two 5 MHz blocks [345]. The use of this spectrum in the future may be possible if OfCom decides to release them. However, in the face of considerable demands from other sectors of the economy, any frequency allocation decisions must be based on validated results of tests evidence as presented in the remaining part of this chapter.

6.4 The Bandwidth and Security Testing Setup

In order to determine the bandwidth requirements for secondary substations, the data transmissions between the communicating entities were considered. This is the SCADA polling of the RTU measurements and the protocol used to link the RTU with the SCADA control centre. The RTU collects the measurement data from the on-field IoT devices. The bandwidth set-up and its calculations considered the use of IEC 60870-5-104 (IEC104) protocol applied to the test set-up at this stage. It is assumed that future deployment of RTU connectivity will comply with the IEC 62351, which is the security standard for substation communication, including the ISO/IEC 61850, DNP3 or IEC 60870-5-104 [5].

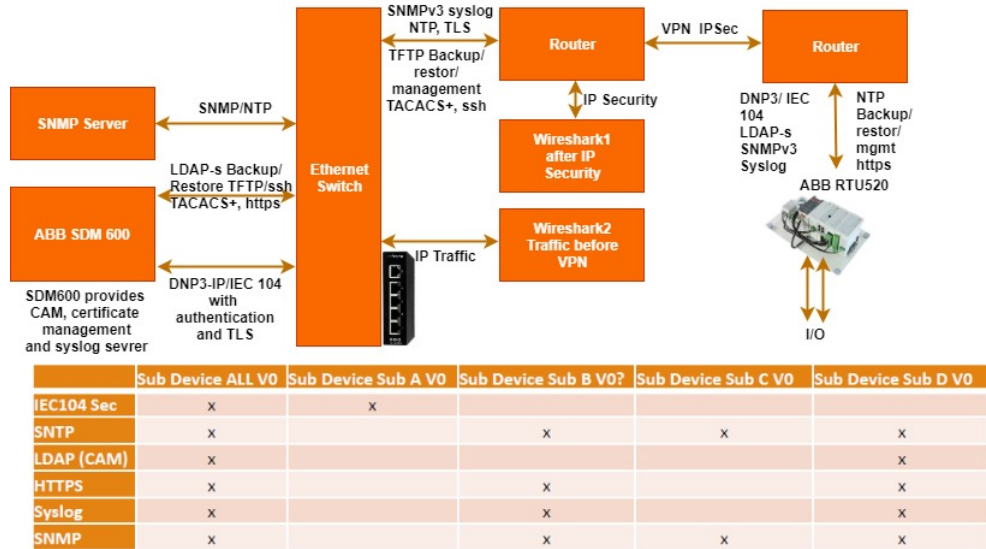


Figure 6.2: High-level Bandwidth Requirement Testbed (<https://pndc.co.uk>)

A complete setup of a fully-secured IP network is installed at the PNDC to understand the bandwidth and security requirements (see Figure 6.2). The RTU is part of the ABB RTU500 series, IP-based and designed to meet the DNO's needs in transmission and distribution automation. The RTU supports many different security approaches for authentication and encryption. The cyber security approaches complied with the NIS directives and IEC 62351 standards of creating secure connections between RTUs, increasing system robustness and ensuring efficient user data management. An example

application for secondary substation automation was designed. This monitored several analogues and digital measurements transmitted from the RTU to the control centre (Slave RTU to Master RTU in this setup). It was assumed that the RTU needs to send 18 measurements of analogues every 10 minutes. This configuration and protocol were based on the experience of one DNO at PNDC considering:

- The capabilities of PNDC's communication network as a suitable test and demonstration environment. They range from the DNP3/IEC104 protocols through batching/class reporting mechanism down to the cybersecurity considerations at the centre.
- The size of the data measured, set points or values.
- The frequency of the transmitted analogue/digital measurements in time

Various scenarios were considered in the testing as shown in figure 6.3 based on the table in figure 6.2. Different tests were performed to check the background traffic, considering activations and deactivations of the security for the IEC104. The tests were delivered over two days of different configurations for IEC104, namely: 4 analogues each 10 seconds (this test checks the connection reliability and the IPSec) and 18 analogues each 10 minutes (fully secure package for IEC 104 along with remote access and syslog with and without VPN were performed). The IEC 104 keep alive each 30 seconds is used in this test. Keep alive probes that generate extra network traffic is useful in this application as faulty and inactive devices and communication links due to network inactivity are detected.

The Virtual Private Network (VPN) aspect of the testing was set-up using Cisco modules via an IP tunnel between two routers to represent the connection through a wide area network (WAN). Another level of security came from activating different security approaches from the ABB RTU, namely, TLS V1.2 (i.e. LDAP, HTTPS) and syslog. The tests ran over 48 hours, and the data were captured via Wireshark before and after entering the VPN tunnel. The analysis of the research findings is described in subsection 6.5 and 6.5.3.

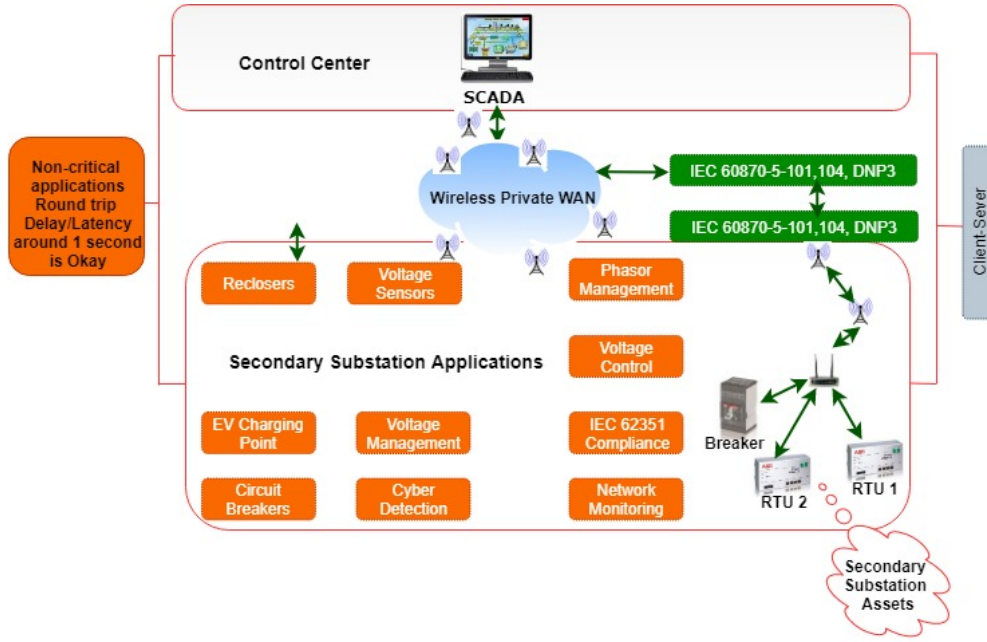


Figure 6.3: Test Scenario

6.4.1 Cybersecurity Considerations for Secondary Substation

The bandwidth estimation analysis considered the overhead of security requirements applicable to modern power utilities. Legacy power networks have been deployed without adequate cybersecurity to mitigate cyber-attacks. Based on NIS directive [339] and compliance with the IEC 62351 standard, connections via DNP3 and IEC 60870-05-104 must be secured. In this study, two levels of security were applied to the connection and the transmitted data. The first level is device-to-device between RTU and the control unit, and the second level of security is from the IPSec through a VPN between the routers. There is no unified approach to cybersecurity in the secondary substation as security is shared. The power utilities use several security techniques/protocols for authentication, management, encryption and certificate update. For instance, the Internet Protocol Security (IPSec) authentication and encapsulation standard is widely used to establish secure VPN communications. Such protocols are considered in the bandwidth calculations as a level of security when using a WAN. Moreover, TLS, Hypertext Transfer Protocol Secure (HTTPS), File Transfer Secure Protocol (FTSP) and

Simple Network Management Protocol (SNMP) can also be applied to secure the connection through the smart grid. TLS and IPSec were applied based on the power network application requirements, as some applications may not require some of these protocols. Also, both cybersecurity solutions prominently stood out in the current cybersecurity discussions between the MNOs, DNOs, regulators, manufacturers, and policymakers.


6.5 Bandwidth Analysis of TLS and IPSec Overhead in Secondary Substation

This section highlights the different testing scenarios' findings to determine the bandwidth requirements due to IPSec and TLS security overheads over RTU communication channels in a secondary substation. The percentage of the security overheads based on the two security approaches applied to enable secured communication links between slave and master RTUs in secondary substations was determined. The comparative analysis of the results is also presented to allow DNOs and other IoT organisations of interest to make cost-effective and strategic security decisions that meet new and emerging cybersecurity challenges.

6.5.1 Internet Protocol Security for Secondary Substation Security

Internet Protocol Security (IPSec) is a network layer authentication and encapsulation standard used in establishing secure VPN connections by wrapping each TCP packet payload in a new and secure frame. The Encapsulated Security Payload (ESP) data format guarantees the authentication, integrity and confidentiality of packets payload encapsulated by IPSec headers and trailers as shown in figure 6.4. In this study, IPSec is considered as a level of security between two RTUs via Wide Area Network (WAN), see figure 6.2.

The strategy employed in computing the security overhead involves capturing the payloads of the packets before entering and after leaving the VPN tunnel. The process also consists of filtering the Wireshark captured packets of master and slave RTUs



Protocol	Length	Protocol	Length	Info
TCP	60	ESP	118	ESP
TCP	60	ESP	118	ESP
104apci	1404	ESP	118	ESP
104apci	1156	ESP	118	ESP
TCP	60	ESP	150	ESP
TCP	60	ESP	1478	ESP
TCP	60	ESP	1222	ESP
TCP	60	ESP	118	ESP
104apci	1192	ESP	118	ESP
TLsv1.2	85	ESP	118	ESP
TCP	60	ESP	118	ESP
TLsv1.2	139	ESP	1254	ESP
TCP	60	ESP	150	ESP
104apci	89	ESP	118	ESP
TCP	60	ESP	214	ESP
104apci	99	ESP	118	ESP
104apci	189	ESP	166	ESP
104apci	239	ESP	118	ESP
TCP	60	ESP	166	ESP
TCP	99	ESP	262	ESP
TCP	60	ESP	310	ESP
104asdu	188	ESP	118	ESP
104apci	99	ESP	166	ESP
TCP	60	ESP	118	ESP
TCP	60	ESP	118	ESP

Figure 6.4: ESP Packets Before Entering and After Leaving VPN Tunnel

with respect to their IP addresses and matching the captured packets before entering and after leaving the VPN tunnel as illustrated in figure 6.4. Further sorting of the packets based on their length also made the comparison and matching process more straightforward. The test data shows considerable variations in the message size in both the encapsulated message and message without security. The percentage overheads introduced by the IPSec tunnel is presented in table 6.1. Without IPSec, the lower and upper limits of 60 bytes and 1404 bytes of message sizes were obtained, as shown in subsection 6.5.2. Over the IPSec tunnel, an increase spanning 118 bytes and 1478 bytes of upper and lower limits were obtained. The analysis of the percentage of IPSec overhead as presented in figure 6.5 shows small message sizes being recorded more frequently compared to the larger message sizes of above 200 bytes for different test scenarios.

The deep inspection and comparison of packets with and without IPSec for different scenarios allowed small size packets of TCP handshake, IEC 104 keep-alive, and APCI origins to be examined. They contribute 25% of the overheads in the packets below 200 bytes. This is similar to the findings when TLS was activated for remote access and role-based access control authentication (i.e. https and LDAP). The packet size of TLS v1.2 was larger than the captured data before TLS was activated for remote access,

Table 6.1: Overview of IPSec Overhead with Message Sizes before Entering and after Leaving IPSec Tunnel

Payloads without IPSec (Byte)	Payloads with IPSec (Byte)	IPSec Overhead (%)
60	118	49.153
70	134	44.776
90	150	40.000
188	246	23.577
199	262	24.046
210	272	22.794
244	310	21.790
296	358	17.318
341	406	16.010
358	422	15.166
410	470	12.766
453	518	12.548
838	902	7.095
1404	1478	5.100

for which the IPsec overhead did not exceed 15% (for TLS captured packets with more than 360 Bytes). The actual message size significantly influenced the security overhead as a percentage of the packets caused by applying the IPSec. The overhead attributed to IPSec decreased with message sizes. Smaller message sizes resulted in a higher overhead in terms of the proportion of the required bandwidth. In summary, between 22% to 28% of additional bandwidth will be required if IPSec security is considered for securing communication channels between RTUs in a secondary substation of the future as shown in figure 6.5. It shows the estimated bandwidth requirement for the secondary substation RTU based on un-batched reporting (which results in the worst-case bandwidth requirements).

6.5.2 Transport Layer Security for Secondary Substation Security

Transport Layer Security (TLS) is applicable in IoT security for the following reasons: To ensure that only authorised users and devices have access to the network (authentication), to keep data packets secret from all users (encryption), and to guarantee the originality of data (Integrity). Hence, applying TLS enables device authentication, data encryption and integrity checks. In the TLS security level setup, a TLS certificate

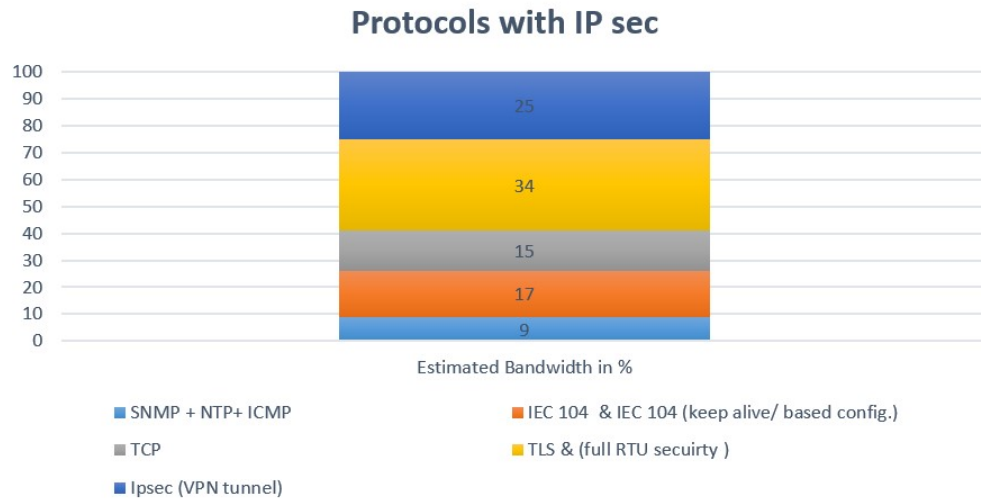


Figure 6.5: Protocols Estimated Bandwidth with IPsec

of the IP-enabled RTU is activated and managed remotely. When TLS is applied, the captured packets get larger, especially during remote access testing. It is important to note that https packets with relatively larger sizes are generated during remote access operations and transmitted only during that operation window. Maximum https packets of 1203 bytes of application data were achieved on a TLS traffic without IPsec. This should be considered the minimum packet size when establishing the bandwidth needed to activate remote access over TLS. The TLS application for remote access may be needed several times a month or even less, depending on the use case and the IEC 62351 specification. TLS session resumption which is expected to be more frequent than session renegotiation over remote access is allowed not more than 24 hours, but the real configuration parameters should be determined based on application related risks. This means that the greater impact of security on the bandwidth requirement is mainly dependent on IPsec packets rather than the TLS packets.

Table 6.2 shows the impact of each protocol on the bandwidth based on TLS and IPsec for polling 18 analogue values. It demonstrates that TLS authentication and encryption and the IPsec will require doubling the bandwidth used by the DNOs. This will be relevant in making the critical decisions of what section in the network should have two levels of security. Not all applications will require two levels of security,

Table 6.2: TLS and IPSec Protocol Bandwidth Percentage Estimation

Protocols	Bandwidth (%)
SNMP+NTP+ICMP	07 - 11
IEC 104 ASDU and Keep-alive	15 -19
TCP	13 - 17
HTTP over TLS	29 -39
IPSec (VPN tunnel)	12 - 38

and overheads can be reduced if both are not used together. However, approaches to identifying the level of security suitable for each NDO's across their organisation infrastructure varies. In many test scenarios, the approach that relied on VPNs connection for a location to location security combined with TLS for the IoT devices makes security deployment less complicated and more efficient.

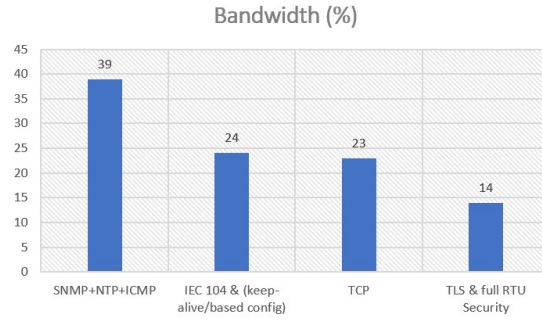


Figure 6.6: Actual Bandwidth without Security

The actual bandwidth estimated for TLS security without IP security based on specific protocols is shown in figure 6.6. Applying TLS security without IPSec contributed up to 40% of the increase witnessed in the bandwidth overhead. This however, depends on the DNO's application, test network setup, and configurations. The results are specific to tests configurations of one vendor's equipment that helped in ascertaining the impact of the unique RTU and the configurations on the required bandwidth overhead. For future optimisation, this study may require further testing by extending the test setup to include more vendors and a greater number of RTUs which may have a slight variations in the presented results.

6.5.3 Estimated Bandwidth for Secondary Substation

The summary of the data estimated for different DNOs for remote monitoring of secondary substation as presented in table 6.3 suggest that it is influenced by the communication technology, the protocols (i.e. IEC 104/DNP3), the number of connected industrial IoT devices and their configuration, and other operational circumstances. A data rate of 0.33 kbps is the lowest achieved throughput without security by DNO1, while 22.3 kbps is the highest throughput with both TLS and IPsec obtained by DNO5. An increase in data rate requires a corresponding increase in the bandwidth if the agreed service level agreement is to be met. The implication is an increase in the cost depending on the extra data in kbps. Additional security introduced increased the data rate in both the TLS and IPsec if an efficient bandwidth is used. This shows a slight increase in the estimated data rate without security. TLS and IPsec were computed to add 34% and 25% of bandwidth into the existing data rates from the test result.

Table 6.3: Security and Data Rate Requirements for DNOs

Data Rate (kbps)	DNO1	DNO2	DNO3	DNO4	DNO5
No Security	0.33	3	4	6	9.6
TLS	0.59	5.4	7.2	10.8	17.2
TLS and IPsec	0.77	7	9.3	14	22.3

Retransmissions due to lost packets, packets being out of order or fragmented also contribute to the additional bandwidth required. As shown in figure 6.7, an Ethernet-based connection TCP packet is seen being fragmented into 1404, 520, and 586 bytes for retransmissions. These types of retransmissions are necessary to keep the client RTU to server RTU connection active. Still, it can double the packet as a result of overhead associated with each retransmitted packet. The performance of wireless network connections can be affected by operating conditions such as the weather, modulation techniques, data throughput, etc.

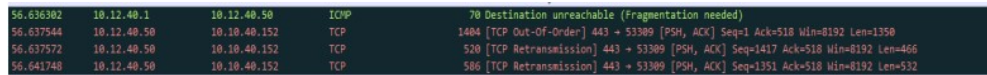


Figure 6.7: TCP Retransmission

Whereas the estimated data for polling 18 analogue values in 10 sec is 1 kbps under optimal laboratory performance, the test results shows higher values with the addition of TLS and IPsec. Based on the summary of results presented in table 6.4, IPsec and TLS requires bandwidth of 25% and 34% respectively.

Table 6.4: Bandwidth per Protocols with TLS and no Security

Protocol with TLS	Bracket Bandwidth (%)	Av. Bandwidth (%)
SNMP+NTP+ICMP	11-17	14
IEC 104 ASDU and (keep-alive)	20-30	25
TCP	19-27	23
TLS	33-43	38
Protocols Without security	Bracket Bandwidth (%)	Av. Bandwidth (%)
SNMP+NTP+ICMP	17-25	21
IEC 104 ASDU and (keep-alive)	32-42	37
TCP	37-47	42

6.6 Summary

The impact of IPsec and TLS security overheads on the bandwidth for an Ethernet-based smart grid network is presented. The results show that IPsec carries an average overhead of 25%, but this value is highly dependent on the payload and RTU configuration. Remote access communications tend to be bursty and bandwidth-intensive. A good application response time is required for it to be effective. The overhead of TLS keep-alive messages, IPsec, TCP connections, and IEC 104 consume more than 50% of the bandwidth (based on configuration and application). The security features evaluated added overhead of roughly 2-3 folds of the current data rate by the DNOs, for both levels of security (i.e. TLS and IPsec). The background traffic for security also added significant overhead to the bandwidth but was not considered in the analysis.

The increasing use of IEDs and IT-based utility assets increases the importance of having adequate cybersecurity measures in power networks. By default, DNOs should consider smart grid security to include asset vulnerability, data management, data encryption, access control and data authentication, privacy concerns and threat profiling. Different data rates apply to DNOs based on their preferred configurations, applica-

tions, communications technology types, and the type of vendor's RTU, along with the number of set points and frequency of the measurements. These were the main parameters affecting the required data rate translating to bandwidth overhead and cost.

Chapter 7

Bandwidth Efficient Security for Smart Grid

Utility networks require wireless technologies to monitor and remotely operate smart grid IoT assets. For this to be achieved in a low-cost, reliable and secure way, the Distributed Network Operators (DNOs) would require sufficient licensed spectrum with good coverage and capacity in the rural and urban areas for long-term service provisioning strategy. To determine the required bandwidth of industrial IoT devices interconnected over LTE radio access technology, two RTUs were employed to evaluate LTE analysis of operational technology under Secure Authentication (SA), IPSec, and TLS encryption techniques needed to secure future smart grid at the PNDC Lab. Based on the DNO's protocols and configuration, the DNOs application requirements, such as the analogue and digital measurements in the secondary substation to be transmitted to the control centre, were obtained by comparing overheads from each security technique. Recommendations and discussions covering the main challenges and prospects for the appropriate security approach for secondary substations are also presented .

Major part of this chapter is a conference paper presented at the 2021 IEEE International Conference on Smart Applications, Communications and Networking (SmartNets): Communication technologies for Smart grids and Energy management, Glasgow, Scotland — 22-24 September 2021. Available at <https://smartnets.ieee.tn/>

7.1 Introduction

As power networks transition into intelligent grids to provide control and effective oversight of remote smart grid infrastructure, the security and communication landscape has continued to evolve. Many field IoT devices require reliable network connections with high-quality measurements. Similarly, future secondary substations automation systems will need reliable communication solutions to connect the distributed and ubiquitous IoT field devices to the management centre securely and reliably [346]. They are also expected to meet the security of Networks and Information Systems (NIS) directives [347]. This implies that critical national infrastructure, such as utility networks, must employ adequate security techniques and other cybersecurity specifications that may lead to more bandwidth demand. However, installing and securing each connection in smart grids is crucial, and these communication systems present several challenges. Wireless networks reduce many of these challenges and are an efficient option for power utilities to deploy. Wireless technologies provide the control centre with reliable connections for field IoT devices and guarantee secure remote access operations. But, as the number of devices and their measurement requirements increases, so does the bandwidth required to operate them. It has financial and practical limitations for utility networks, as wireless systems require a limited spectrum. As part of a Critical National Infrastructure (CNI), smart grid infrastructure has security and bandwidth requirements far more stringent than the MNOs can support in their public networks and may need a dedicated spectrum to reliably and securely deliver these types of services. For instance, private or sliced mobile networks would require dedicated spectrum allocations to ensure stable operation and smooth recovery from any potential black start scenario. Spectrum regulators and major DNOs are also involved in this research to identify the appropriate spectrum for their future wireless communication requirements.

The largest single providers of wireless networks are mobile network operators. They lease licensed spectrum in various bands and own thousands of masts providing comprehensive geographical coverage. However, current generations of mobile networks

provide between 99.50% (2 days downtime per year) and 99.92% (7 hours downtime per year). Compared to the energy regulators that require 99.999% uptime (six minutes downtime per year). These more stringent requirements mean that most commercial wireless networks cannot support critical infrastructure without independent reliable power sources. 5G network, as discussed in section 5.4.3 offer a solution to this problem through a higher frequency spectrum that allows for increased data rate. However, this may not be practical and cost-effective for utility networks with assets in rural areas, where a high-frequency spectrum would struggle to permeate, and huge costs would be needed for the extra network resources to provide comprehensive coverage. Then, this leaves the highly sought-after low-frequency spectrum range as the most efficient option based on coverage and penetration capabilities. This necessitates the need for effective bandwidth utilisation since the impact would increase the demand for the limited spectrum [29].

Another novel approach to measuring bandwidth for power networks is to consider the network operating over new wireless technologies if the long-term requirements of the smart grid are met. Wireless technology is the most efficient, reliable and cost-effective telecommunication option for the smart grid, especially when connectivity and remote access to distributed assets in the remote areas are essential. Securing the right bandwidth will be critical to support future applications such as charging, energy storage facilities, and the integration of renewable energy sources. In terms of security requirements for the secondary substation, the two-level of security (IPSec and TLS) considered in section 6 will also apply in this scenario where IPSec and TLS are used over a mobile network link (LTE network) rather than through Ethernet. The technical details of OpenVPN, IPSec Tunnelling, cyber security considerations, and challenges regarding the test setup are presented. The main contributions of this chapter include determining the bandwidth due to cybersecurity overhead needed for smart grid applications of the future and detailing the impacts of different vendor's RTUs on the bandwidth overhead through a radio access network. Also, this chapter compared and identified the wireless technologies/security techniques with minimum bandwidth requirements to support the functionalities of modern RTUs.

This section of the thesis is based on the contributions and test analysis from several ongoing technical projects and research activities of applying several security approaches (IPSec, TLS, VPN, and SA) in smart grid of the future at PNDC. This study is based on the IEC 60870-5-104 protocol for Supervisory Control and Data Acquisition (SCADA) systems to remotely monitor and safely operate distribution assets in substations of the future. The findings will help the DNOs, and other interested readers understand the cost of adding security to the smart grid and ascertain the appropriate bandwidth needed to introduce any security feature. The findings will also be beneficial to spectrum regulators for spectrum planning and licensing for the growing utility networks. The rest of this section is organised as follows: Section II gives an overview and summary of related work. Section III presents a high-level overview of the security techniques used in the test. Sections IV and V then introduce the encryption test setup and the test results analysis, respectively. Next, Section VI presents a summary of the leading encryption challenges for smart grids. Finally, Section VII concludes this section.

7.2 Wireless Communication Technology for Smart Grid

To regularly maintain and monitor substations, a telemetry solution is one that DNOs uses to connect their RTUs to the control centre. Frequencies between the 420 - 470 MHz UHF 1 and UHF 2 bands demand in the UK by the DNOs, and other band users for business-critical applications are growing because of their increasing data collection requirements. They also have good propagation characteristics such as coverage and in-building penetration [348]. Limited bandwidth of the range is dedicated to the power companies that operate over fixed multi-point communication links for remote sites data acquisition, monitoring, and control. The UHF scanning telemetry uses an available spectrum band of 1 MHz, comprising 80 channels of 12.5 kHz. Such limited bandwidth with its narrow channels will limit the number of connected outstations; it will not be sufficient for the increasing demands for the smart grid voice, data applications, new EV charging points, and LV distributed assets. The current spectrum for UHF

scanning (with a 12.5 kHz channel) cannot serve more than one fully secured RTU per channel (i.e., the need for fully secure IP RTU is considered to be 7 kbps). Moreover, the existing 12.5 kHz is not appropriate to carry voice and secured data together. As shown in table 7.1, scanning telemetry computations are based on Differential Phase Shift Keying (DPSK). In another modulation technique like 256 QAM, higher data rates could be achieved under excellent weather conditions. Such a high modulation technique with high theoretical spectrum efficiency should not be used in the planning and requirements stage because it does not reflect and consider the worst-case scenario. Lab demonstrations show that with a channel of 200 kHz, a data rate of 1.1 Mbps could be achieved for a modulation technique of 256 QAM. Telemetry could bring limited measurement to the control centre. However, adding security overhead and the need for voice communication and increasing demands to connect new assets make it impossible for UHF/VHF Telemetry to meet the increasing demand requirements of the smart grid.

Table 7.1: Number of RTUs Connected via the Existing UHF Frequency

Bandwidth (kHz)	Modulation Technique	Data Rate (kbps)	RTUs/Channel	RTU/Bandwidth
12.5	DPSK	9.6	1	80
25	DPSK	19.2	3	120
100	DPSK	69.3	9	95
200	DPSK	137.5	18	94

The most frequent bandwidth channels for VHF/UHF scanning telemetry in use are 6.25 kHz, 12 kHz and 25 kHz, where the maximum data rates will not exceed 22 kbps. Further enhancements of the UHF radio modems, which use 50 kHz and 200 kHz channels as presented in chapter 4 (NB-IoT and LTE-M), may offer higher data rates suitable for power networks applications. Reliable monitoring of distributed power assets is crucial to safeguard power suppliers and rapidly restore any unexpected power interruption. This will not be achievable without real collaboration between the involved parties, mainly; DNOs, Ofcom, Department of Business Energy and Industrial Strategy (BIES), vendors and the technology providers. The Joint Radio Company (JRC) seeks an additional 2 x 3 MHz of spectrum on behalf of the fuel and power

industries to maintain the UK and EU's energy sector operational challenges by 2020. Whether 2 x 3 MHz of spectrum is sufficient to meet the requirements of the DNOs will be clarified based on the results presented in this chapter from tests conducted at the PNDC. This chapter presents the data rates that can be obtained based on bandwidth availability, considering the real/actual data rates an RTU can receive on an LTE mobile network. LTE is considered a potential, successful and widely used technology for many sectors, including utilities and other industrial applications. However, public LTE networks are unsuitable for supporting the utilities' critical requirements due to inadequate latency in establishing communication links in the event of power outages and rural coverage are not determined by the DNOs but the business needs of the MNOs.

7.3 Private vs Public LTE Networks for Power Utilities

LTE is one of the most reliable wireless technologies deployed widely across different industries to meet their growing data rate requirements. When operated privately or publicly, it has the capabilities to provide power utility with the benefits of simple IP network design and flat architecture, low latency and high bandwidth, international standard and industry support, enterprise-wide coverage, and a secure ecosystem. Others include scalable and flexible bandwidth, cost-efficient and affordable, policy control and life cycle management, and a wide range of power IoT use cases. The communication networks for utilities are categorised based on their high reliability/availability and low latency. DNOs require reliable and affordable private networks to run their operational communications networks and maintain communications reliability during extended power outages or when public communications networks are unavailable. Digitalisation requires more devices to be connected, and the current UHF telemetry suffers from many limitations such as narrowband channels and scalability. DNOs are looking for an option to deploy private 4G/5G networks and integrate them into a 4G/5G public network. Such a private network may take a variety of forms, but it should integrate and interwork with commercial 4G/5G infrastructure operated by MNOs. The distin-

guishing features of private and public LTE infrastructure are presented in figure 7.2.

Several reasons that utilities might want to deploy private networks include:

- The private network can be designed to operate in the absence of primary power, which could help recover any power outage quickly. Extended backup power and diverse and redundant routing of backhaul communications networks are crucial for any DNOs.
- To implement new security techniques and standards as recommended by the regulators and comply with the industrial and international standards with fewer technical challenges.
- Extend the coverage into more rural areas housing power infrastructure not served by the MNOs, where MNOs have no business interest. Rural coverage requires low band spectrum allocation such as the 400 MHz bands to ensure that coverage could reach the hard-to-reach areas where the distributed power assets are located.
- Performance assurance via high availability and reliable networks and guarantee QoS for critical power applications.
- Ensure that power utility technicians and engineers can communicate when repairing lines or restoring service after an outage has occurred.
- To help in enabling and optimising critical business processes. As it is targeting specific services and applications, the power utility can go through this option to assure optimised, dedicated and secured network [349]
- **Integration** - The majority of the existing power assets are over 30 years old. Despite this, they are still within their useful life cycle. The DNOs may find it expensive to replace all the legacy assets before reaching the end of their useful life. DNOs may continue to invest in the operation of the existing infrastructure and install new interfaces and more innovative kits. This could create a significant challenge for the connectivity and integration between the current power infrastructure and radio technologies in supporting different vendors and various legacy

protocols. DNOs must consider the interoperability of their radio communication interfaces across multiple applications and different use cases.

- **Distributed resources and Multiple Communication Protocols** - Utility networks currently rely on more than two different communication technologies in their network operation, and this does not include any LV automation or active network management systems. Future considerations of power networks may double the number of communication systems, especially meeting the connectivity in the hard-to-reach areas. They may end up with several incompatible networks that add further complications to the operations of the grid. If the DNOs could simplify this and deploy a single communication technology that satisfied all the requirements, this would significantly impact the whole business and the stability and reliability of the smart grid.
- **Coverage** - For power utilities, the lack of coverage in the hard to reach areas and the signal penetration are among the main concerns for the DNOs, where most of their assets are located in rural areas and are looking for higher data rates. The availability of the mobile signal is the main issue for any mobile service in the smart grid, where the coverage is still sub-optimal from what the power utilities are looking for to be made available. To date, no mobile operator considers the rural coverage a priority to be met in any deployment plan. The national coverage maps from all the MNOs suffer from a lack of coverage in the rural areas, as shown in figure 7.1 [350] and figure 7.2 [351]. Given the coverage reach, it will be more expensive for the MNOs in Nigeria to extend services to the rural areas compared to the UK.

7.4 Methodology

Different communication nodes have been chosen to enable the right connectivity on the SCADA software needed to control the field IoT devices to investigate the bandwidth requirements for remote outstations. The process control system is set up to poll the

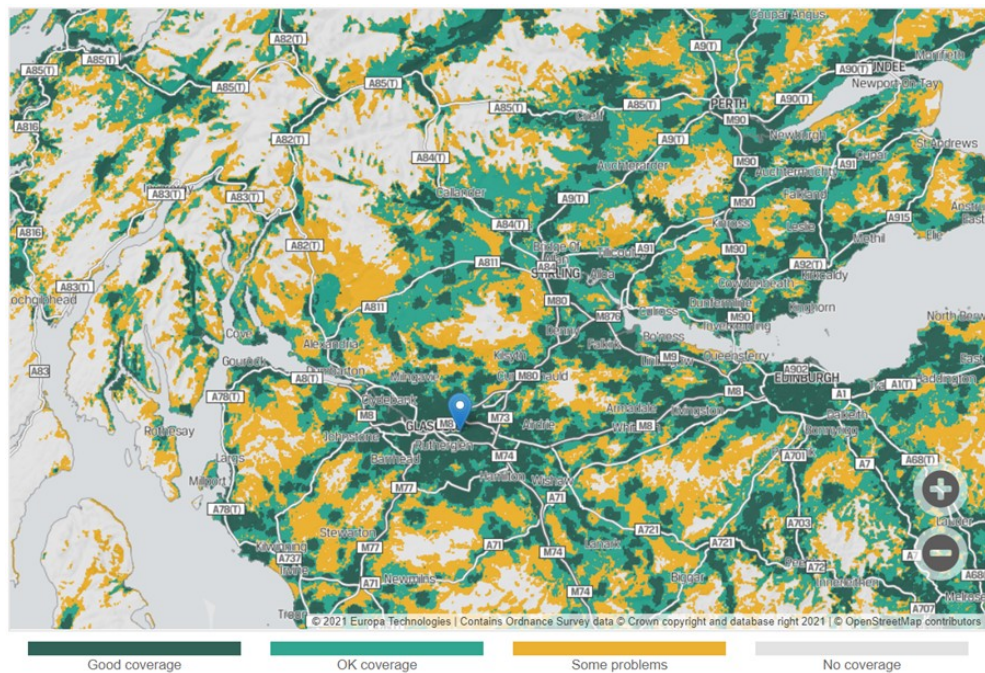


Figure 7.1: The Coverage Map of an MNO in Glasgow-Scotland for 2G, 3G, and 4G networks

Table 7.2: Public vs Private LTE Network Features

Public Networks	Private Networks
Controlled, managed and owned by the MNOs	Controlled, managed and owned by the DNOs
Spectrum licensed to mobile operator	Unlicensed/shared/leased spectrum
Shared network	Enterprise personalised network
Coverage subject to people locations	Dedicated enterprise coverage
Data/voice services are dominant	Adapted services
Low start-up cost	Higher start-up costs

RTU through an industrial SCADA protocol to enable the connectivity between the RTU and control centre, as shown in figure 7.5. The DNOs application requirements in the secondary substation for polling analogue and digital measurements between the substation and the control centre is established based on RTUs configurations. The test network includes industrial grade M2M routers and RTUs of different manufacturers (virtual access and ABB). Communication protocol Test Harness from Triangle MicroWorks Inc for generating the IEC 60870-5-104 traffics is used to link the RTU with the SCADA control centre. Others include off-the-shelf SIM cards with OpenVPN and



Figure 7.2: The Coverage Map of an MNO in Nigeria for 2G, 3G, and 4G networks

multi-network functionality, an intermediate server to facilitate the secure connection between the router and RTUs. The test security approaches followed NCSC directives and IEC 62351/62443 and ISO 27001 smart grid security standard specifications. The test scenarios considered IPsec for remote access (configurations, maintenance or firmware update) and secondly to encrypt the measured data by applying TLS. These tests meet DNOs security test specifications to compare OpenVPN and IPsec and use only secure transport without OpenVPN or IPsec mechanisms for maintaining a secure smart grid.

The functionalities of the test devices and tools are described as follow:

- Virtual Access Router (GW2027) is an M2M LTE enabled industrial router that supports different M2M applications.
- IEC 62351 compliant Gateways integrates security, connectivity (M2M wireless router with multi SIMs), RTU, HMI and SCADA protocols to enhance the busi-

ness case for extending coverage.

- Communication protocol Test Harness by Triangular MicroWorks to generate the IEC 104 standard traffic.
- Two off-the-shelf multi-network SIM cards enabled the connectivity through a public radio network.
- SCADA concentrator encrypts the IEC 104 traffic and transfers the train traffic into a fully secured one. It is used to comply with the IEC 62351 standard for any transmitted IEC 60870-5-104 protocol (protection through TLS encryption).

Based on two configuration patterns of the IEC 104 protocol as shown in table 7.3, the identification of the data flow between the communicating components such as during the SCADA polling of the RTU measurements is essential. The frequency of polling helped to establish the effects of congestion. In congested polling, the IEC 104 is configured to be polled in a series of 15 seconds for a specific time slot to create congestion. In 300 seconds, up to 5 commands arrived within the same time frame. More traffic was injected in order of 15 seconds to reflect congestion of specific peak time polling. The results are quite different from the IEC 104 generated traffics without congestion.

Table 7.3: Configuration of IEC 104 Traffic Commands with Polling Frequencies that Created Congestion or Avoided Congestion

IEC 104 Commands	Congested Polling (s)	Uncongested Polling (s)
General integration	60	15
Double point command	90	13
Floating measurement	180	31
Counter integration	120	31
Single point of measurement	30	23
Clock synchronisation	15	17

The tests configuration scenarios were chosen based on the discussion with several power networks operators as a trail to reflect the actual status of their existing network configurations. With the right RTU and router configurations, an end-to-end

secure connection was established via a mobile radio network. Different SCADA generator configurations were investigated over many days to determine the reliability of the link and the implications of the security configuration to the bandwidth requirements. The main digital commands of interest include general integration, counter integration, single point, and double point. The analogue commands were normalised, scaled, floating-point measured, Clock synchronisation and 32-Bit string. The same configurations have been repeated for each security approach, aiming to understand the overhead caused by each security approach. As mentioned in section 7.4, the tests were conducted based on two scenarios as shown in figures 7.3 and figure 7.4 respective:

Scenario 1 - Plain IEC 104 data sent via a VPN server based on IPsec protocol configuration. Applicable in remote access for configuration and software updates. Virtual Access RTU and wireless routers were used for the test setup.

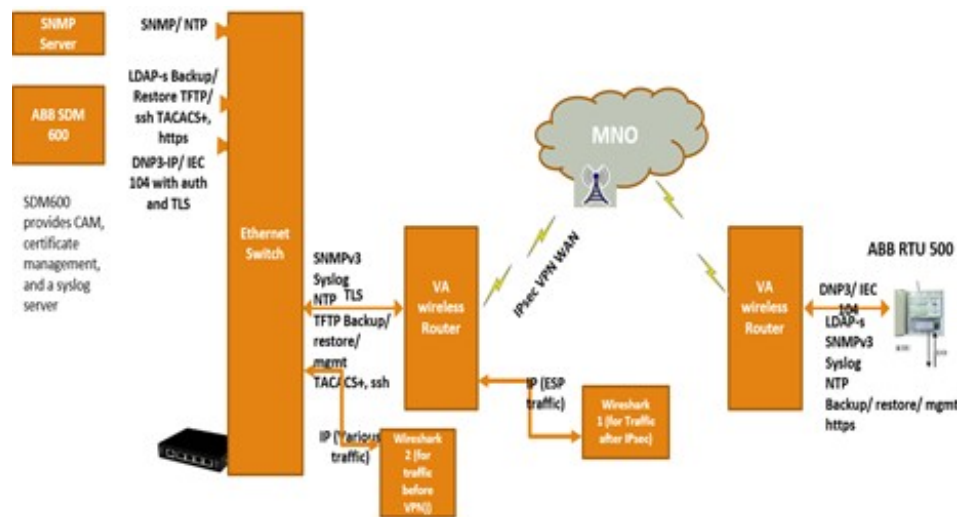


Figure 7.3: IPsec VPN – WAN-Virtual Access RTU

Scenario 2 - IEC 104 encrypted data is sent via TLS.

The functions of the security techniques/protocols (application specific) as shown in figure 7.3 and 7.4 helped in the authentication, management, encryption and certificate updates functions as presented below:

- The Internet Protocol Security (IPsec) authentication and encapsulation standard are widely used to establish secure VPN communications. This protocol is

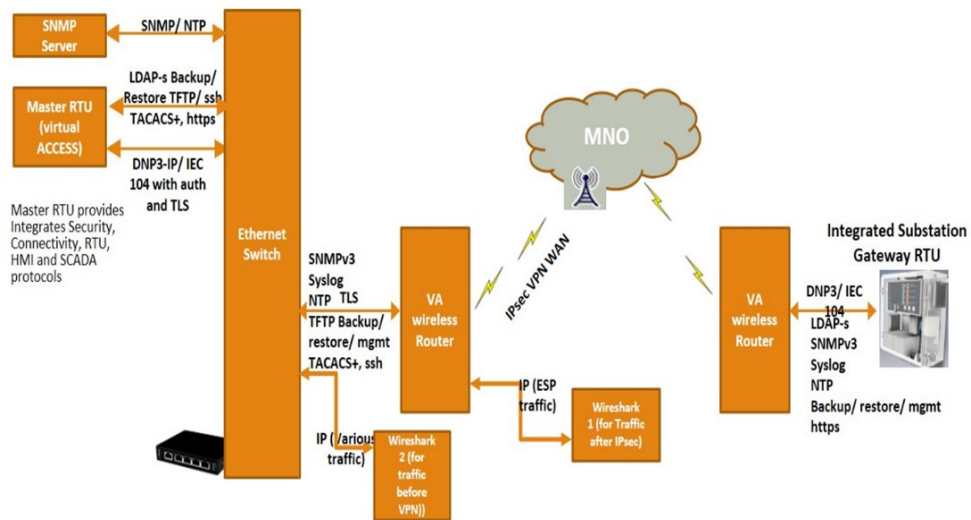


Figure 7.4: IPsec VPN – WAN-ABB RTU

considered in the bandwidth calculations as a level of security when using Wide Area Network (WAN).

- Simple Network Management Protocol (SNMP) is used to monitor network devices' health and provide data security and authentication.
- File Transfer Protocol Secure (FTSP) is used securely to transfer files between clients and a server in the network.
- Syslog is used by the field devices to send event messages to a logging server.
- Lightweight Directory Access Protocol (LDAP) is used to allow access to an application directory via its ability to store credentials in a network security system and retrieve it with the right password and decrypted key.
- Terminal Access Controller Access - Control System (TACACS) is an authentication protocol that enables a remote access server to forward the login password to the authentication server to give access permission.
- Hypertext Transfer Protocol Secure (HTTPS) is used for securing the connection between the server and the web, ensuring the protection and the privacy of the data.

- Transport Layer Security (TLS) is a security protocol that can provide end-to-end communications security when transferring data through a network.
- Simple Mail Transfer Protocol Secure (SMTPS) provides authentication and data confidentiality for email messages.

7.5 Security Techniques for Smart Grid

According to previous studies, legacy secondary substations technologies are deployed without adequate security. To prevent cyber attacks on power networks, they require an upgrade to make the technologies more resilient, secure, and efficient while improving capacity and reliability with increased automation [352]. This implies that in remote outstations, to secure the distributed assets and ensure that field measurements are transmitted securely, the network must be implemented with new security standards (i.e. IEC62351 [215], IEC62443/ISO27001 [353] and following the ENA Security Procurement guidance [164]) for power networks. This will protect secondary substations of the future that will include more functionalities to perform additional monitoring, reporting and control capabilities from cyber attacks. Different security techniques are used in power utilities for authentication, encryption and certificate updates purposes [278]. TLS, Hypertext Transfer Protocol Secure (HTTPS), File Transfer Secure Protocol (FTSP) and Simple Network Management Protocol (SNMP), etc., are commonly applied to secure connections in smart grid. For example, IPsec authentication and encapsulation standards are widely used to establish secure VPN connections between RTUs [29]. Cryptographic methods such as VPNs and protocol security extensions are other concepts of implementing security in distribution networks [209]. While TLS aims to secure the application level data between the IoT devices and the control centre, IPsec provides protection through a VPN tunnel between routers. IPsec provides robust authentication, integrity verification and sufficient encryption to the communication channels. The protocol security extension such as Distributed Network Protocol 3 Secure Authentication (DNP3-SA) aims to authenticate the end devices and ensure the message integrity between the master and the filed device [209], [33].

7.5.1 TLS Encryption

Transport Layer Security (TLS) is used to provide privacy and data integrity over private and reliable connections that are transparent to higher layer protocols and independent of application protocols [354]. TLS is used in the industry for end-to-end encryption in several existing applications through the layers of Handshake and Record protocols. TLS handshake authenticates the end connected devices and ensures successful exchanging of the cipher suites, symmetric session keys and parameters between the client and the server prior to any communication between the end devices. Once the entire TLS Handshake is successfully completed and the peers validated, the applications on the peers can begin communicating with each other. On the other hand, the TLS record protocol encrypts and authenticates application packets. However, TLS technical challenges identified in this study include enforcing a unique certificate for each field outstations and gateways (Virtual Access and ABB) with unique public and private keys and ensuring the TLS sessions certificate update. IEC 62351 standard recommends updating the Session Key at least once in 24 hours. Following the NIST recommendations, a public key certificate signed by a trusted certification authority containing secure Cipher Suites that offer at least 128-bit encryption keys is needed [352], [33]. TLS is supported by different utility protocols such as IEC 60870-5-104 employed in this study in the power networks. TLS encryption for both DNP3 and IEC 60870-5-104 communication, when enabled in the RTU, secure the exchange of data between the control centre and the RTUs.

7.5.2 Secure Authentication

Secure Authentication (SA) is another approach presented to improve the security of power networks. It is derived from IEC 62351 and applies to a range of protocols such as IEC 60870-5-101, IEC 60870-5-104, and IEC 61850 to improve data transmission and authentication security in smart substations. When activating the SA in SCADA systems, each critical message requires authentication before any execution as messages can be authenticated based on challenge-response procedure to prevent spoofing, modification and replay attacks [210]. This security mechanism efficiently

reduces bandwidth through flexible security options that leave specific devices unsecured, including in non-connection oriented networks. It places the role of security function on IoT devices. DNP3 SA v5 (i.e., IEEE 1815-2012) enables the DNP3 master RTU to include the Hash-based Message Authentication Code (HMAC) in its original transmitted DNP3 message. Including the necessary authentication data in the original message can reduce the bandwidth needed as fewer messages are transmitted [40]. The test setup, which uses the SCADA gateway from Virtual Access, supports SA as defined in the IEC 60870-5-7 standard. Adding authentication - based on IEC 62351 security standard to an existing SCADA protocol ensures that any critical commands are safe and may avoid any possibility of a man-in-the-middle attack that may affect the connection. The main advantages are the ability to support low bandwidth and serial networks for legacy protocols such as IEC 60870-5-101 and create low overhead for remote outstations that may not be capable of processing any public/private certificates or encryption.

Many existing Operational Technology (OT) protocols and devices may not have security features such as authentication due to several limitations and restrictions such as memory and processing power. The limited available channel to add any security to the existing technology makes it more difficult for the power utility to deploy security. Recently, many energy networks have started to include security in their network protocols, especially those designed by the IEC group. For legacy protocols and applications where TLS and IPsec discussed in section 7.5.1 and 6.5.1 respectively may not be able to provide end-to-end encryption and identity management, SA then becomes the only security option. This could open the door to the importance of lightweight encryption approaches which can be used in such constrained environments. In computationally constrained environments, new lightweight encryption standards are required to execute asymmetric cryptography. This is evident by the NIST drive for more encryption-focused research on developing and evaluating new, efficient, cost-effective, lightweight algorithms [307]. This research development activities involve extensive analysis and performance benchmarking of new cryptographic algorithms. New lightweight encryption and heavy protection standard will be added to NIST's portfolio based on the

findings. The utilities will use this to provide end-to-end encryption and identity management as a projected option to be used in a limited environment in terms of bandwidth and resources. Moreover, lightweight encryption algorithms are a way out of the OT security protocol issues in terms of the absence of authentication and confidentiality in certain applications.

7.5.3 Virtual Private Network

Routing IoT data via untrusted public or third-party networks requires end-to-end security. Virtual Private Network (VPN) is employed to encrypt and authenticate remote access connections between IoT devices when end-to-end security is desirable to perform configurations and maintenance tasks. The second layer of protection provided by the VPN tunnel goes as far as protecting databases, legacy and security limited IoT devices. For example, code injection, spoofing, and unauthenticated attacks are prevented, and a change of the device's IP due to network handover does not affect VPN connections. In addition to WireGuard, an emerging VPN security protocol that provides faster and resilient communication links with more robust cryptographic primitives, TLS and IPSec are the two most common VPN connection protocols with little difference in the vulnerability risk between using IPSec and TLS VPN [355]. However, IPSec-based VPN is an open standard built into many systems that allow many IoT client and servers security solutions to be developed and integrated. This reduces the maintenance and configuration cost of applying proprietary VPN solutions. But when accessing a third-party VPN network that restricts IPSec, the IPSec VPN protection is lost, thereby rendering the network vulnerable due to IPSec connection setup challenges. When network access involves Network Address Translation (NAT) or Next-Generation Firewalls (NGFW) and gateways, TLS VPN can reliably secure data transfer between different on-premises networks. Additional costs will be required to access the third-party VPN services of a single vendor to avoid interoperability issues. Remote access in networks with little or no on-premises services VPNs are better done following Zero Trust Architecture (ZTA) or hybrid VPN and zero trust architecture. ZTA uses permissible policies to removes network inherent trust and implements strong

authentication, authorisation, and user/device identity for remote network access. The use of single sign-on and strong authentication, encryption, and device configuration are of great importance as ZTA has higher attack surfaces.

The client and server implementations are central to how robust and resilient VPN solutions are. To benefit from vendor diversity, IPSec is more suitable in addition to the following VPN best security practices as recommended by NCSC:

- Authentication should be certificate-based (X.509) with private security keys stored in the hardware through Trusted Execution Environment (TEE) or Trusted Platform Module (TPM) implementations.
- System built-in VPN client should be used with the understanding that its functionality limitations are not risks to the VPN services. The risk of software integration and upgradation must be considered when using a third-party VPN.
- VPN client or client NGFW should be used to force route all traffic through the VPN tunnel for cyber monitoring. Where compatibility issues exist, other authentication mechanisms is recommended to prevent circumventing VPN security policies.
- For a higher user experience and to maintain robust and resilient VPN connections, an automatic VPN with forced configuration is most suitable. Triggered and the manual option is a matter of usability and network performance-oriented.
- Per-application VPN configuration common in Bring Your Own Device (BYOD) should be avoided. A full device VPN implementation prevents unforced application sensitive data from being routed outside the VPN tunnel. Similarly, split tunnelling should be avoided regardless of its bandwidth cost, saving from high-bandwidth and latency-sensitive applications access to networks without passing through a VPN tunnel.
- For high-bandwidth applications that VPN may impact, managed tunnels should be used when accessing third party services. Such a tunnel managed connection

must use the platform's built-in captive portal helper and mutual TLS authentication to replicate VPN security standards.

- The TLS [356] and IPSec [357] cryptographic profiles recommendations by NCSC should be followed.

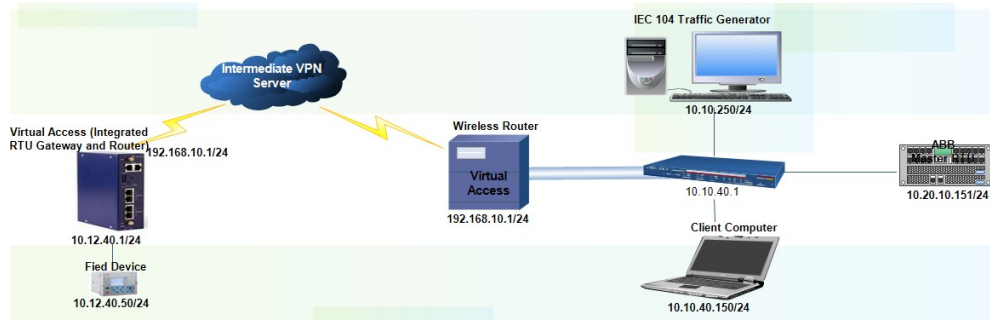


Figure 7.5: High Level VPN Test Setup at PNDC

As shown in 7.5, IPSec tunnel could be established between secondary substation RTUs via an intermediate third-party VPN server. The results presented in section 7.7 demonstrate the capabilities of establishing VPN connection in M2M networks. Both OpenVPN and IPSec tunnels can be established in power networks with external VPN security services. External access to the networks is blocked for security reasons. As recommended in this study, a dedicated DNO's private LTE network could be deployed to serve as the intermediate VPN security. LTE core deployed locally would allow direct VPN connections between RTUs in a substation. In this case, direct pseudo connectivity is created in a unified network through dedicated M2M SIM cards. However, aspects of this are expected to generate additional overheads and be considered a future research direction.

7.6 Results and Analysis

The following test results are based on the analysis of the RTU data captured using Wireshark network and security analyser features based on the test setups with various security techniques over the same configurations in IEC 60870-5-104 (IEC 104) protocol.

Each test scenario is analysed to identify the unique packet size, which was scaled and used to estimate the monthly data usage needed by an RTU. The network configurations determined the percentage of monthly security and data overhead. The estimated monthly data without any security is 49.3 Mbyte, whereas the overhead caused by the authentication while using IEC-104 is about 55 Mbyte a month. The estimated security overhead for reply/challenge authentication is less than 10% of bandwidth, and the maximum data rates did not exceed 7% of the existing data rate needed in bps.

7.6.1 Secure Authentication Overhead

In the secure authentication mode, MAC is used to authenticate the critical commands using session keys. Because MAC authentication requires a challenge and response mechanism for each command, it doubled the required bandwidth for configurations having a high number of polls in order of seconds. Based on the same configurations with a limited number of command polls each in minutes, the data overhead for the tests was computed, analysed and scaled over a month. For the fact that secure authentication supports legacy protocols and devices that may not be capable of processing existing encryption techniques such as TLS or IPsec described in section [7.5.1](#) and [6.5.1](#) respectively, a feature that makes it suitable to work in low bandwidth conditions when the number of transmissions is limited. In smart grid applications where the frequency of the critical commands is limited, authentication is an efficient security technique used to ensure reliable communication between the control centre and authenticated field devices. This option should be applied where there are restrictions in using available bandwidth for specific applications. Authentication proves that a legitimate device sent a message, as it allows the sending device to confirm other device IDs via multiple means before transmission.

7.7 OPEN VPN vs IPsec

The comparative analysis of bandwidth implications due to OpenVPN and IPsec security is evaluated to determine the overhead introduced by both VPN protocols for sending unencrypted IEC 104 traffic through secondary substation RTU of different vendors. Also, the percentage of overhead introduced by applying TLS encryption creates more reliable communication links between the substation equipment. The IPsec wraps each packet in a new and secure frame by adding an average of between 60 - 80 bytes to each frame. On the other hand, OpenVPN added an average of between 40 - 44 bytes to each frame. Based on the results of packet size as presented in the analysis in figure 7.6, IPsec introduced an average of 23% bandwidth higher than OpenVPN.

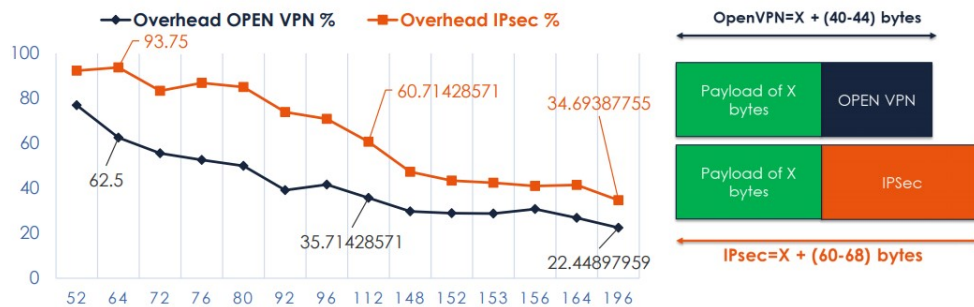


Figure 7.6: OpenVPN and IPsec Overhead Comparison

7.7.1 Congestion

The effect of increased congestion was a higher packet loss rate, which resulted in a high packet retransmission rate and a drop in network performance. This to the power network is the inability to meet the network operational requirements during black-start scenarios and very high demand at peak times. The worst-case congestion tests scenarios indicated a packets drop rate of around 1.3%. The percentage packets loss of this value is not suitable for real-time applications since it increases packets latency and delay variations (jitter). No packet loss was recorded in the tests scenarios without congested configuration, and few retransmissions were observed in few congested cases.

7.7.2 Connection Loss

Connection loss to third-party cloud servers could also affect the network performance. Connection losses are expected in networks where there is an increased number of multiple hops for each packet. The end-to-end delay was introduced when multiple hops is needed before packets can reach the third-party network and can potentially affect critical applications. Network issues and service outages due to the inability of the eSIM platform to maintain stable connections with the router and RTU at all times affected the network's reliability.

7.7.3 Network Coverage

The received signal strength and performance of radio frequency signals depend on the network coverage. The test network performance under weak signal strength shows a higher rate of packet losses resulting in degradation of the end applications. These findings raise questions about the network performance in hard to reach areas and the cost implications of extending radio network connectivity. Using off-the-shelf SIMs could promote global network coverage through multi-network roaming support.

7.8 Data Rates

The flexible bandwidth supported in LTE contributes to the network capacity, which can be attributed to the number of Resource Blocks (RBs). The number of RBs reduces as the number of bandwidth reduces, see table 3.3. The peak data rates show the theoretical throughput that defines the typical subscriber/field device operation and the average sector throughput. This throughput estimates how much bandwidth can be delivered within a sector under real-world conditions. The aggregate throughput estimates the number of concurrent devices and field assets served by the network site or sector. The average sector throughput values help operators understand their deployment costs and operating costs better, allowing for better dimensioning exercise and network profitability. The theoretical peak data rates for different bandwidths are, however, challenging to achieve by MNOs. The effective data rates of an LTE

network is affected by the network traffic load, Signal-to-Noise Ratio (SNR), signal fading and attenuation, the environmental and atmospheric conditions. While the channel bandwidth, together with the type of modulation technique, duplex mode, UE SNR, antenna configuration, and spectral efficiency, determines the actual data rate, as evidenced by the engagement of the stakeholders at the PNDC. Live network data rates are far below the theoretical peak data rate presented in table 7.4. The effects of spectral efficiency on the bandwidth and the number of RTU served per LTE cell is elaborated in section 7.9. In the uplink channel, the transmit and modulation constraints of the UE offers limited bandwidth benefits.

Table 7.4: LTE FDD System Capacity and Downlink Peak Data Rates

[358]

BW (MHz)	SISO (Mbps)	MIMO 2x2 (Mbps)	16 QAM (Mbps)	64 QAM (Mbps)
1.4	4.4	8.8	3	4.4
3	11.1	22.1	7.5	11.1
5	18.3	36.7	12.6	18.3
10	36.7	75	25.5	36.7
15	55.1	110	37.9	55.1
20	75	150	51	75

7.9 Spectral Efficiency

Spectral efficiency is a crucial factor to be considered during the planning of any wireless communication network. It is the data rate in bps/Hz obtained by dividing the measured data rate in bps by the used channel bandwidth measured in hertz. The value of spectral efficiency changes based on the LTE network parameters such as the network load, the operational circumstances, Signal-to-Interference Ratio (SIR), the modulation techniques and the distance of the UE to the base station. In power network applications, to accurately estimate the actual capacity for a private LTE network for the smart grid, field results from MNOs and field trials were considered to understand the actual bandwidth requirements for secondary substation automation. Field data of spectral efficiency of greater than 80 live Nokia networks from carried traffic per cell with 15 MHz bandwidth during busy hours show that load affects the spectrum

efficiency, where some base stations recorded spectrum efficiency of 0.53 as shown in figure 7.7. The data presented were obtained from base stations that operate on 16 QAM, 20% of them generate 50% of the traffic data, and busy hour indicates 7% of the daily traffic. The spectral efficiency at 0.54 could reflect the black start scenario where the power network is expected to be loaded and may be considered a worst-case scenario for planning and selecting bandwidth requirements.

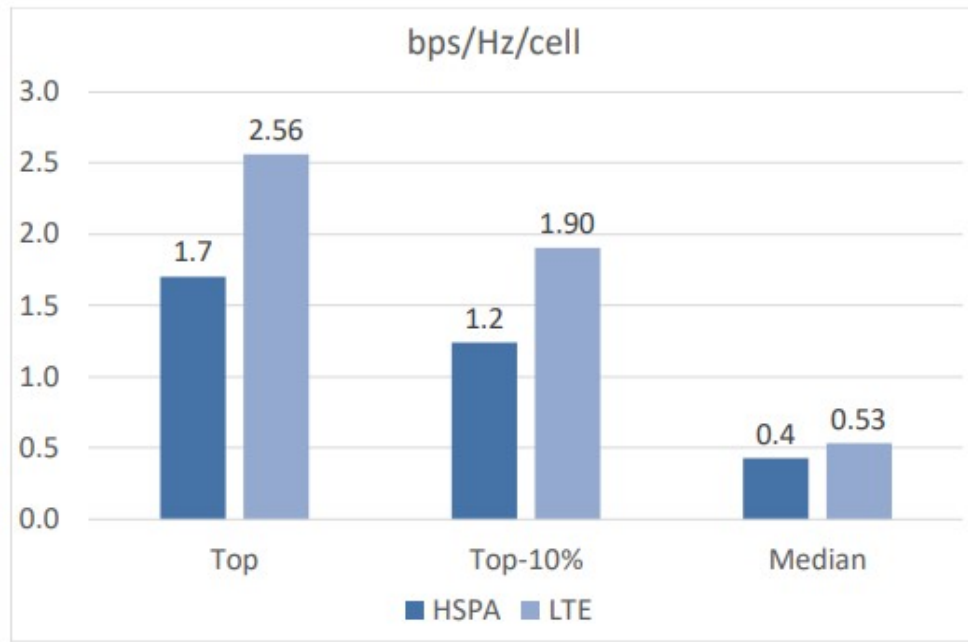


Figure 7.7: LTE Spectral Efficiency in Large Number of Live Nokia Networks [359]

For a private LTE for power utility, dedicated bandwidth of up to 5 MHz should be considered. Different spectrum efficiency values are used (0.54 reflects loaded networks and 1.9 which could represent unloaded networks). The data rate for a fully secured RTU for secondary substation automation is estimated at 7 kbps. For the estimated number of RTUs in an LTE cell, as shown in table 7.5, the data rate varies based on the spectral efficiency that influences the number of RTU. Start-up bandwidth is needed, and it is crucial to be identified carefully, as it is important data for any DNOs to be considered as a worst-case scenario. When losing power under any circumstances, the RTUs connections should be restored within a short period so the DNOs may operate

them quickly to configure the network properly. This could add extra traffic to the network and increase its load, affecting the required time needed to activate the RTU, along with the number of exchange messages between the centre and the RTU. Table 7.6 summarise the effects of a start-up scenario on the number of RTUs that can be served based on different bandwidth and different network loads. The data rates in a loaded network may not exceed 1.6 Mbps per cell, which means that the maximum number of serving RTUs may not exceed 219 RTUs(considering that each fully secured RTU requires 7.2 kbps). This number could be lower in severe weather conditions, therefore concluding the need for a bandwidth requirement in excess of 3MHz.

Table 7.5: Estimated Number of RTUs in an LTE Cell

BW (MHz)	Loaded	Unloaded	Loaded (RTUs)	Unloaded (RTUs)
1.4	0.74 Mbps	2.7 Mbps	106	380
3	1.59 Mbps	5.7 Mbps	227	814
5	2.65 Mbps	9.5 Mbps	378	1357

For satisfactory operation of a private LTE for power utility, this study recommends a dedicated spectrum of 5 MHz for the smart grid. This bandwidth could be used to securely connect the remote assets to the control centre and be able to cope with many future applications in the LV monitoring (i.e. connecting charging stations). The calculated number of RTUs per cell shown in figure 7.6 provides an overview of the capability of LTE based on the available spectrum.

Table 7.6: RTUs per LTE FDD System Capacity and Throughput Computation

BW (MHz)	DR Loaded	DR (Mbps)	Loaded (RTUs)	Unloaded (RTUs)
1.4	0.756	2.66	103	364
3	1.6	5.7	219	780
5	2.65	9.5	350	1300

Based on the spectral efficiency and data throughput analysis, the average data rate for each RTU and the spectrum efficiency value will determine the number of RTUs that can be served inside the cell. However, the network load and distance from the LTE cell will affect the throughput, which in turn affects the number of RTUs served. The scenario is more likely to occur in urban density areas where capacity is a major

challenge. The same capacity could satisfy the DNOs requirements in rural areas as bandwidth requirements tend to be lower. For a black start scenario consideration, adequate network planning before any field deployment is required to avoid latency issues during such time critical event. Also, Cell edge user throughput and spectral efficiency (bit per second per Hz) is limited due to low signal level and the high degree of interference from neighbouring cells. Test results and shared data from the mobile operators show that the spectral efficiency may not exceed 10% for many rural areas (macro-cells environment) [360].

Average Spectral Efficiency vs Peak Spectral Efficiency vary and is dependent on the environment and the operational conditions. Indoor environment and lab results are far away from the typical cell average and cell edge experience. Many factors such as Signal to Interface Noise Ratio (SINR), frequency allocation, cell size, cell power transmission, modulation technique and antenna arrangements and configurations also affected the spectral efficiency, which in turn, affected the number of RTUs served by each eNB.

7.10 Encryption Scheme Challenges for Smart Grid

The smart grid comprises many electrical IoT devices in the distribution, transmission, operation, etc., and is interconnected by subnetworks such as Home Area Networks, MNO, etc. The majority of the subnetworks are vulnerable to cyber attacks, which can breach the supply of critical energy networks in which authentication could be used to provide reliable data security with reduced overhead. Encryption mechanisms in smart grid networks vary and depend on many factors such as the network architecture, communication technology, device capabilities, the end application, etc. Secure authentication is very useful in limited resources and legacy devices, but it does not provide the authenticity, confidentiality and integrity of the packet data exchanged. IPsec and TLS provide security by encrypting the exchanged messages. TLS encrypt, authenticate, and check data integrity in applications and protocols, including VoIP and web-based applications. While TLS encrypts the data between the control centre

and end device, IPSec in tunnel mode encrypts the data between routers connecting different networks and is most useful in unidirectional communication.

In terms of bandwidth utilisation analysis between TLS and IPSec, TLS is more bandwidth efficient than IPSec, as shown in table 6.5. The monthly cost of IPSec encryption is higher than what is needed for TLS, but in the black start scenario, TLS contributed an additional 40% of the overhead needed to restore the service. Following DNOs engagement, complete reliance on private networks is one of the future requirements that would allow the avoidance of third-party services that require IPSec for internetwork security. IPSec ensures that a secure tunnel is established between the different network interfaces when using third-party service providers. For the future smart grid, where substations interfaces are essential gateways for RTU and LV applications, reliable network connection with adequate bandwidth will continue to be a bottleneck.

Table 7.7: TLS and IPSec Estimated Security Overhead Security in IEC 104

IEC 60870-5-104	No Authentication	TLS	IPsec
Monthly data usage - MByte	54.6	57.2	67.8
Monthly security overhead MByte	5.3	7.9	18.5
Monthly security overhead (%)	9	16	37.5
Data rate overhead - bps (%)	6.8	10.3	23.4

For network connectivity provided by a third party, RTUs and gateways can be fitted with appropriate roaming sim cards (multi-network sim cards). When a network issue is detected in one mobile network operator's service, the devices can automatically join another provider, thereby increasing redundancy. The architecture of existing public mobile networks prohibits direct device to device connections, implying that all connections have to go through an intermediary link. If this service were to fail, so would the device connection. The lack of control and influence of the third-party network could create high network interruption during a blackout. Private mobile networks employing control and user plane separation with a local user plane function can enable direct device to device connectivity.

Inadequate network coverage and traffic congestion increased the number of dropped

packets, resulting in network performance degradation. The reliability in terms of packet loss and retransmission rate is highly affected by the quality of the communication medium (coverage and signal quality). The Encryption techniques as investigated secured RTU transmissions with high reliability in all test scenarios. For connection issues, field devices supporting multi-sim cards means that different MNO's networks can be selected depending on the reliability of the network connection. On the other hand, using multi-network sims from a third-party provider could terminate connections and cause the tunnel to fail when there is a problem with the third-party server. The reliability of smart grid connections are affected by the following:

- Power failure will result in loss of radio signal, TLS or IPsec connections that provide data security and secure command exchanging path for the field device. Redundancy is the key to solving power outage problems.
- The involvement of third-party service providers will reduce the network's reliability and increase network congestion, configuration errors, and packet loss.
- Synchronisation issues between the master clock and field devices could drop the network reliability. Any network delay can lead the authentication process to fail.
- The required bandwidth increases with the size of the encryption key. For lightweight encryption, NIST recommends that AES of 128-bit is sufficient for current cyber security challenges. Future smart grid networks will require key sizes of 256-bit or more that will consume more bandwidth. The requirement for higher key length is the high-end processing capabilities that may not be possible in all gateway and field devices.

7.11 Emerging Security Strategies for OT Networks

As industrial OT networks continue to undergo digital transformation (IT/OT convergence), they become more vulnerable to cyber attacks as their data become more available. The following strategies can address the IoT cyber security challenges in OT environments in addition to the IPsec, and TLS discussed above:

- **Implementation of Zero Trust Architecture:** All access to the network must be risk accessed based on the access privilege and must start with zero trusts. IoT devices and users in power networks are qualified to determine what resources they can access and the impact when compromised.
- **Network Segmentation:** By classifying every network resource as not secure based on zero trust architecture, network segmentation is another security layer introduced to reduce the impact of a breach.
- **OT Protocol Security:** Security tools with specific requirements such as SCADA or ICS for OT networks should be identified and deployed.
- **Business Analytics:** There are many ways of analysing business processes to detect, report and mitigate malicious operations before they can disrupt business operations. Business analytics strategy should incorporate the above points to maintain proactive defense mechanisms for OT networks.

7.12 Summary and Conclusion

This section discusses and compares the security overhead of secure authentication with TLS and IPsec encryption for smart grid remote outstations to identify the lightweight security scheme in remotely connecting distributed smart grid assets to the control centre. In this type of network with high-reliability objectives, secure authentication is a cost-effective scheme in constrained assets that cannot support encryption protocols such as TLS or IPsec. TLS with AES of 128-bit contributed 25% of additional overhead compared to IPsec for each analogue or digital command from the findings. The cost and security overhead from using secure authentication, IPsec and TLS for securing smart grid assets varies. For instance, to estimate the cost of using IPsec to encrypt the connection between entities within the smart grid, the size of the original packet before transmission is a key factor to consider. The cost of using IPsec to secure the IEC60870-5-104 connection between RTU and the router is higher than that of OpenVPN and estimated at 45% with respect to bandwidth overhead. For each of the

OpenVPN-based transmitted packets, 40 - 44 bytes of overhead were added via User Datagram Protocol (UDP), whereas IPSec added 60 - 68 bytes. One level of security may be sufficient for remote outstations, as less than 100 Mbyte a month can easily fit with the security requirement for each sim card needed to connect an RTU to the control centre securely. In summary:

- Using TCP come with high retransmission rates irrespective of configuration types, but when the master RTU exchanges data based on command and response protocol (polling), the retransmission rate is reduced.
- The common problems of degradation of mobile network performance during peak periods was evident. Packets could be lost or dropped due to poor coverage or network congestion due to disaster incidents, black start scenarios or service demand over-weighing the available resources. Good mobile network coverage and configurations reduced TCP retransmission due to packet loss.
- The security overhead due to IPSec is higher than that of UDP-based OpenVPN. Both resulted in frequent smaller messages sizes that influence the bandwidth overhead.
- Using third-party VPN network services increases network latency that will degrade the performance of the critical industrial IoT applications.
- The optimal data usage of wireless communication technology for remote outstations is best obtained by choosing the correct test configurations in addition to the appropriate security technique needed to secure the connection.
- Multi-networks sim card which can pick the best available mobile operator's signal increases the reliability of the connection, i.e. reducing packets loss and retransmission rate.
- Encryption key of length 256-bit and above will consume more bandwidth and will require high processing IoT end devices that is not currently fulfilled.

Chapter 8

Conclusions and Future Work

To conclude this thesis, it will be necessary to present the reflections on the obtained results and the research questions posed in section 1.1 of chapter 1. As evidenced in chapter 2 through the review of recent studies, IoT is still new with many research challenges in the areas of security, communication protocol design, bandwidth/power utilisation, etc. New protocols developed for IoT have suffered interoperability, security, and performance issues through which its deployment in industrial domains have not scaled as expected. Key IoT protocols for industrial applications are considered in this thesis backed up by demonstrating their unique security and other network performance characteristics for use in industrial utilities and sensor networks.

8.1 Conclusion

Industrial Internet of Things (IIoT) is an evolving paradigm that is widely investigated because of its growing benefits towards digital transformation. Generally, in the industries, it has the potential to aid autonomous services, remote monitoring, and asset tracking of IoT infrastructure. The Internet of Things (IoT) requirements are constantly changing due to advances in sensor technologies, demand for massive connectivity, and secured communication systems to foster real adoption of IoT in the industry. The number of IoT devices added to the industrial networks continues to increase, and this requires that IoT devices, networks and software are constantly im-

proved upon to ensure IoT systems' integrity and resilience. The last decades have shown the magnitude of challenges facing industries wishing to adopt IoT as a solution towards their digital transition. IoT is associated with cases of cyber-attacks, and their increasing interconnectedness creates more attack surfaces and aids reconnaissance of industrial networks for different exploits. Industrial IoT implemented without security by design leaves open opportunities for a compromise that could lead to unauthorised access to the network resources, and loss of IoT data and privacy preservation. As demonstrated in this thesis, IoT protocols are only one part of the problem as the vast majority of IoT networks depend on many devices, software, and third party service providers. However, there are many regulations and standards, which seek to address these problems.

Recent studies have proposed Low Power Wide Area Networks (LPWAN) as relevant technologies for specific industrial IoT solutions. While the communication standards for NB-IoT, LTE-M, and Long Range Wide Area Network (LoRaWAN) have not been explored to a great extent for different industrial deployment domains, there are still many open research and development challenges to be addressed. The list as discussed in see subsection 1.1 is not exhaustive. However, studies on industrial IoT networks with quality of services (QoS) metrics, bandwidth requirements and cost analysis for utilities and sensor networks are not yet available in the literature. Based on unlicensed and cellular wireless networks devoted to the design, implementation, and experimentation of wireless IoT technologies, the performance evaluation of LoRaWAN, NB-IoT and LTE networks presented in chapter 5 are some key elements of this thesis for which the conclusion is presented.

Narrowband Internet of Things (NB-IoT) is an example of an IoT M2M protocol introduced by 3GPP to meet the increasing demand for low-cost, reliable connection and secured IoT solutions in many industries. NB-IoT is considered because outside other requirements of IoT networks such as the hardware, by design, it delivers a secure network that can support very large IoT devices. This is a significant benefit as security is a prime consideration for industrial IoT. While NB-IoT can support specific IoT applications with good network performance and security, it is expensive when scaling

IoT, especially in hard-to-reach locations. Against this backdrop, studies as presented in this thesis on industrial IoT for industrial systems integration are essential because more communication devices are making industrial processes easier, more autonomous, and cost-effective. It meets one of the objectives of this research which is to explore NB-IoT for industrial IoT deployment, emphasising cost, security, and connectivity.

In this research, a design and implementation approach using current cutting-edge hardware allowed real-world scenarios to be evaluated. The evaluation of the effectiveness of the proposed solutions employed different network testbeds, industrial IoT devices, network standards, and wireless communication protocols, see chapter 4. The idea extends existing literature where key technologies, services, and applications of industrial IoT use cases have been identified. The design, testing and validation process are aligned with the University of Strathclyde 5G Centre and Power Network Demonstration Centre (PNDC) projects that provides real-world results in emerging IoT networks for utility networks.

Smart grid is one practical example of industrial IoT presented in this thesis that requires the integration of next-generation communication systems such as LTE and 5G with power networks IoT infrastructure. Such convergence makes it mandatory to improve critical requirements of the grid to prevent system failure, service disruption, and system breakdown due to any malfunction. To address the bandwidth and security requirements of wireless technologies for smart grid as presented in chapter 1 and identified by the utilities, this thesis also presented innovative approaches based on different test network setups and scenarios established to determine secondary substation security standard overhead contributions and the cost implications. The findings suggest that two-level of security based on TLS and IPSec are inadequate in the long term but contribute an average of 2-3 times of the existing bandwidth without future network management requirements. With at least 5 MHz of spectrum allocated for secondary substation automation function in a private LTE network satisfying the current DNO's requirements. The experimental evaluation of the network motivated by the project objectives outlined below highlighted the issues that may possibly undermine the deployment of IoT for smart grid:

- The need to improve utility services such as rapid detection and isolation of faults, reduction of power outage count, increased security and utilisation of resources through remote access monitoring. Security means data overhead, which raises the question of the need for additional bandwidth and cost.
- Increase Return on Investment (ROI) by implementing Active Network Management (ANM) system enabled by cloud integration.
- The need to integrate and scale industrial networks towards future developments and long-term vision to cope with the increasing grid complexity due to increasing energy sources, charging stations and battery storage systems.
- Investigate the impact of high traffic volume in congested network and black start scenarios. The number of analogues and digital measurements transmitted from the IoT devices in the field to the control centre is determined. That is, an RTU client connected to the server RTU with the required security bandwidth information.

8.2 Summary of Contributions

The proliferation of IoT in many fields has diversified the recent research challenges that need to be addressed. A few, as identified in chapters 1, 2, 3, and 4 include heterogeneous, inter-connectivity, bandwidth, standardisation, roaming, ubiquitous and security issues identified in IoT networks similar to what is discussed in **JP2**. Others include implementing concepts such as Artificial Intelligence, Machine Learning, Software Defined technologies in IoT solutions. In this thesis, the areas of contribution shown below focuses on the security, protocols, bandwidth, and cost. Based on the findings drawn from the reviews, designs, implementations, tests, and analysis as presented in this thesis (see list of publications in the preliminary pages), a number of key contributions have been made to the field of IoT to address the key research questions posed in chapter 1:

- security and costs - is seen as one of the biggest challenges that the IoT is facing

today. To address some of the security issues, Chapter 2, 6, 7, and **CP1** in the list of publications has explored the cyber security considerations and countermeasure opportunities in industrial and consumer IoT environment. Although the review focused on the current security models for IT and OT convergence, it also considered requirements for achieving trust, confidentiality, integrity, and authenticity. The security of IoT networks and platforms as presented in another conference paper **CP3** and largely discussed in chapter 2 revealed how the security of LoRa and NB-IoT platforms could be enhanced by integrating new security and networking techniques. This is in addition to the use of standardised protocols efficient enough to protect the IoT networks from different forms of attacks. A secured industrial IoT presented in chapter 6 and 7 has the potential to increase operational safety, reduce operational overhead and allow for more rapid detection of incidents ahead of potential failure. It will also enhance infrastructural performance through condition based monitoring giving a more targeted approach to equipment safety and performance.

One of the aims of which is to explore through experiments the current IoT security research trends and challenges pertaining to industrial IoT networks and devices alongside evidencing the need for standard communication protocols and countermeasure opportunities to prevent IoT threats and attacks. Firstly, a detailed review of security challenges and possible countermeasure opportunities relating to implementation methods in IoT networks and devices in industrial frameworks (smart grid) was identified in chapter 7. The methods of identifying risks and the impact of each security mechanisms while transmitting, receiving, processing data is also presented. This research outcomes can help strengthen the security of industrial IoT networks by integrating appropriate security techniques in IoT devices.

While investigating the bandwidth implications of secure authentication discussed in chapter 7 and contained in **C9** and **C8**, TLS and IPSec over Ethernet and LTE networks in remote monitoring of substations, the differences in the security bandwidth overhead needed for each security techniques was investigated. Where

the bandwidth overhead of IPSec was compared with OpenVPN over a smart grid network, the cost of IPSec will require an average of 23% of more bandwidth to OpenVPN. The observed results where bandwidth is insufficient, represented by a congested network, include packets drop rate of 1.3% that make it unsuitable for real-time applications due to end-to-end delay.

- NB-IoT – The scope of demands for research on Industrial IoT has increased due to advances in sensor technologies and the associated incidences of security breaches. LTE and 5G cellular networks are the essential wireless technologies predicted to bring about the Fourth Industrial Revolution (Industrial 4.0) through machine-to-machine and human-to-machine interconnections. NB-IoT is an evolving licensed LPWAN protocol that is widely investigated because of its unique benefits in M2M communication and the massive business opportunities it brings through low-cost connectivity that could aid autonomous services such as assets telecontrol and monitoring. Recent studies have only highlighted the importance of narrowband-based LPWAN as a relevant technology for IoT deployment and are mostly simulation-based. Research addressing security overhead, bandwidth utilisation, and connectivity remains a topical research area and are in high demand by cellular service providers, consumers, and chipset manufacturers. Work is in the area of extending NB-IoT coverage, co-existence of NB-IoT in LTE environment, NB-IoT design and specifications, and applications as presented in **CP3** and **CP4**.

To investigate NB-IoT's performance in the inband operational deployment mode, a design and implementation approach presented in chapter 4 is used to integrate an Amarisoft software-based Lime SDR LMS7002M, which provide LTE/NB-IoT cellular base station for wireless communication standard and Pycom Fipy module served as the sensor nodes. The findings as presented in **JP1** and chapter 5 provide insight and understanding into what standard network requirements are for NB-IoT deployment and its performance implications for varying data traffic, which would be used to deliver new applications. The practical implication of

this study is that a better understanding of NB-IoT network requirements for IoT deployment would enable more deployment, increasing the demand for connectivity and giving increased business output. The findings of this study are very important to the IoT device manufacturers, service providers and service users and would serve as a key decision indicator for NB-IoT technology.

Also, haven investigated the performance of NB-IoT testbed and compared with LoRaWAN on power consumption, data throughput, latency, and security of the networks to guide deployment decisions.

- Bandwidth - A fair share of and access to spectrum is required to build a resilient communication infrastructure and meet the increasing demand for low carbon technologies driven by IoT. The wireless communication testbed implemented at PNDC was used to estimate the bandwidth required by the DNOs to deploy a private communication solution. By investigating the overhead added when implementing IPSec, TLS, and secure authentication over standard communication media, the requirements for smart grid applications were evidenced alongside the bandwidth required under a number of different scenarios that will satisfy the future power networks, see papers **C8**, **C9** and **C10**.

In summary, the findings show that the bandwidth required to support future smart grid applications will be higher for both the utility sector's short and long term needs. In the case of IPSec, the tests delivered an overhead of 25%. An increase of 15% against the 10% suggested in the literature. The findings will also inform strategic discussions on the utilities sector's spectrum policies and communication network specifications. The results could contribute to the technical evidence which could see Ofcom allocate spectrum to support utility networks due to emerging applications and the need to support legacy communication protocols within the power networks in few years. These findings will also be relevant to other industries such as manufacturing when selecting technologies towards embracing digital manufacturing through Digital Twin, Augmented Reality, and Virtual Reality. Aspects such as standards and 3GPP influencing

standards to support the utility sector could be driven by bodies such as Ofgem. Similarly, communication technologies' security and bandwidth specifications for future power networks could be improved, and risks reduced.

8.3 Future Work

To improve the bandwidth aspects of this study, conducting the same research with different vendor RTUs over a specific radio technology such as LTE-M, 5G, satellite or private/public LTE will determine the impact of the same security protocols over different technology. By doing this, the long-term spectrum requirements implications of DNOs in adopting a particular for emerging applications such as charging stations and battery storage could be highlighted. With the promises of 5G technology for utility applications described in [361] and the benefits of other new technologies, repeating these security testing scenarios using different vendors RTUs is essential, see chapter 7.

As an improvement to this study, packet losses due to signal propagation challenges should be considered when planning IoT networks, especially in challenging environments. Link quality is essential in this type of wireless network to determine the type of service deployed in a particular environment and the packet losses. Refer to [290] for propagation losses comparison of NB-IoT and LoRaWAN due to transmissions in underwater, underground, and metallic surfaces. NB-IoT is also faced with roaming problems when the service is to be deployed on a global scale. This means that deploying NB-IoT in more than one country will require the ability to establish international commercial roaming agreements with local carriers, produce NB-IoT carrier-specific modules, and create robust SIM and network management systems to provide cross-border IoT services. Based on the Deutsche Telekom and Vodafone NB-IoT roaming trial, it is still challenging to take an NB-IoT module with Deutsche Telekom SIM and use it in another country's NB-IoT carrier like T-Mobile in the United States [362].

Since NB-IoT and LoRaWAN will be deployed in challenging environments, continuous improvement will also be required in data security, self-configuration/organising/healing, cloud and edge computing capabilities, resource mapping and air interface. NB-IoT

services are primarily provided by the Mobile Network Operators (MNOs) using their available infrastructure with a decision on the business implication and technical alterations to be made at the base station. However, it is also possible to provide clean slate NB-IoT services but at a higher cost. The air interface is one of the optimisation challenges in the in-band deployment of NB-IoT in an LTE network. It makes use of the core LTE design features like channel coding, uplink and downlink frequency division access, data rate matching, interleaving, etc. For efficient coexistence of NB-IoT inside an LTE carrier, orthogonality to LTE signal must be protected when mapping NB-IoT to LTE resources. The UE needs to be designed to automatically detect the deployment mode and subsequently identify LTE resource blocks. Similarly, to achieve scalability in LPWANs, new LPWAN modules should incorporate adequate memory, processing power, and bandwidth.

For readers who have an interest in further exploring some of the possible directions for future research work in the field of IoT, LPWAN, and its wide range of applications, a number of research areas that require further investigation have been identified and are not limited to the following:

- **Ubiquitous NB-IoT Network** - In this thesis, a section has specifically focused on the design, implementation and evaluation of NB-IoT network performance. The NB-IoT testbed performance and evaluation are presented in chapters 4 and 5, respectively. Network QoS parameters such as latency, power utilisation, throughput and security were evaluated but with a limited number of UE and eNB. As NB-IoT is a perfect platform for massive industrial IoT deployment, it will be worthwhile to investigate the testbed performance under an increased number of test equipment. The results presented in chapter 5 based on the testbed discussed in chapter 4 is a small scale test of an inband mode of deployment and less likely to be regarded as encompassing as it has been found that guardband mode outperforms inband mode based on Bit Error Rate (BER) performance analysis [363]. NB-IoT network test performance of guard-band and standalone modes are not available at the time of writing this thesis. Given this improvement, there would be additional benefits if future work explores UEs handover, extended

coverage features, suitability of NB-IoT for other domains, Random Access (RA) load control strategy, implementation of self optimisation, etc. This could also show more insights into resource allocation and traffic efficiency in congested network scenarios.

- **Cellular (LTE-M) Network** - LTE-M outperform NB-IoT in some network QoS parameters [79] and should be studied for use cases that may require higher throughput and other benefits. LTE-M is only presented as a review in this thesis but could be tested using the same testbed but by applying some network and device configurations tweaks, using LTE-M enables UEs. Although, the thesis focused on realising the performance of LoRaWAN and NB-IoT using one eNB and two UEs, the same approach could be applied to cellular LTE-M and other unlicensed LPWAN. LoRaWAN and NB-IoT were selected since they have gained research and industrial interest with their wide coverage, low power consumption, good security, and low cost. By introducing additional UEs and eNBs to the testbeds, a better understanding of a larger IoT network performance can be achieved but can explored further in future work. Although the NB-IoT experiment was performed based on 3GPP Release 13, new features have been introduced to the standard Release 17 as discussed in subsection 3.8.5. The UE used can only support standard Release 13, a gap between NB-IoT standardisation and manufacturing. Similarly, LoRaWAN network was performed in TTN version 2, latency and other QoS presented could be enhanced when performed in TTN version 3.
- **Edge and Cloud Intelligence through Containerisation** - The IoT network management techniques presented in [364] could be evaluated to provide seamless interoperability between IoT devices in two network domains and understand how the intelligence can be leveraged to monitor and control distributed IoT assets. Edge and cloud computing reduce the amount of data transmitted and improve industrial IoT networks' overall bandwidth and latency. This will require the implementation of new cybersecurity frameworks to identify threats,

protect network resources, detect attack vectors, respond to cyber incidents and recover from cyber attacks following NIST directives, ENA and ISO standards recommendations such as IEC 62443 and ISO17002. The security approaches for the industrial automation and control systems, process control systems and information exchange in energy networks are related, and studies on their interoperability are essential for scaling and integrating industrial IoT networks.

Bibliography

- [1] O. Liberg, M. Sundberg, E. Wang, J. Bergman, and J. Sachs, *Cellular Internet of Things: Technologies, Standards, and Performance*. Academic Press, 2017.
- [2] EETimes, “Redpine do-it-all iot chip heads for home.” <https://www.eetimes.com/redpine-do-it-all-iot-chip-heads-for-home/>, 05 2019. (Accessed on 04/05/2023).
- [3] SmartBear, “Iot and it’s impact on testing.” <https://smartbear.com/blog/internet-of-things-101/>, 08 2019. (Accessed on 04/05/2023).
- [4] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, “Smart grid technologies: Communication technologies and standards,” *IEEE transactions on Industrial informatics*, vol. 7, no. 4, pp. 529–539, 2011.
- [5] W. Wang and Z. Lu, “Cyber security in the smart grid: Survey and challenges,” *Computer networks*, vol. 57, no. 5, pp. 1344–1371, 2013.
- [6] L. Alliance, “A technical overview of lora and lorawan.” https://www.mouser.com/pd.docs/LoRaWAN101_final.pdf, 2016. (Accessed on 01/24/2021).
- [7] SEMTECH, “What is lora?.” <https://www.semtech.com/lora/what-is-lora>. (Accessed on 01/24/2021).
- [8] L. Feltrin, G. Tsoukaneri, M. Condoluci, C. Buratti, T. Mahmoodi, M. Dohler, and R. Verdone, “Narrowband iot: A survey on downlink and uplink perspectives,” *IEEE Wireless Communications*, vol. 26, no. 1, pp. 78–86, 2019.

Bibliography

- [9] C. B. Mwakwata, H. Malik, M. M. Alam, Y. L. Moullec, S. Parand, and S. Mumtaz, “Narrowband internet of things (nb-iot): From physical (phy) and media access control (mac) layers perspectives,” *Sensors*, vol. 19, no. 11, p. 2613, 2019.
- [10] A. Sikora *et al.*, “Performance measurements of narrowband-iot network in emulated and field testbeds,” in *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, vol. 2, pp. 780–785, IEEE, 2019.
- [11] WAVIoT, “Nb-fi - the iot standard.” <https://waviot.com/news/nb-fi-is-an-approved-national-iot-standard-detail/>, 02 2019. (Accessed on 01/29/2021).
- [12] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, “A comparative study of lpwan technologies for large-scale iot deployment,” *ICT express*, vol. 5, no. 1, pp. 1–7, 2019.
- [13] M. Chochul and P. Ševčík, “A survey of low power wide area network technologies,” in *2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, pp. 69–73, IEEE, 2020.
- [14] E. TS, “Lte; evolved universal terrestrial radio access (e-utra); user equipment (ue) radio transmission and reception,” vol. 136, no. 101, p. 34, 2017.
- [15] A. Hoglund, X. Lin, O. Liberg, A. Behravan, E. A. Yavuz, M. Van Der Zee, Y. Sui, T. Tirronen, A. Ratilainen, and D. Eriksson, “Overview of 3gpp release 14 enhanced nb-iot,” *IEEE Network*, vol. 31, no. 6, pp. 16–22, 2017.
- [16] ETSI, “Lte; evolved universal terrestrial radio access (e-utra); user equipment (ue) radio transmission and reception,” vol. 136, no. 101, p. 38, 2017.
- [17] ETSI, “Lte; evolved universal terrestrial radio access (e-utra); user equipment (ue) radio transmission and reception,” vol. 136, no. 101, p. 41, 2018.
- [18] I. T. Union, “Overview of the internet of things,” *Recommendation ITU-T Y*, vol. 2060, 2012.

Bibliography

- [19] M. Roberto, B. Abyi, and R. Domenico, “Define iot - ieeeee internet of things.” <https://iot.ieee.org/definition.html>, 05 2015. (Accessed on 09/27/2021).
- [20] B. Sosinsky, *Cloud computing bible*, vol. 762. John Wiley & Sons, 2010.
- [21] A. Lavric and V. Popa, “Internet of things and loraTM low-power wide-area networks: a survey,” in *2017 International Symposium on Signals, Circuits and Systems (ISSCS)*, pp. 1–5, IEEE, 2017.
- [22] A. Kanno, H. Tode, A. Nakao, D. C. Kilper, H. Kimura, H. Murata, and F. Nawabi, “Wired and wireless network convergence in 5g/iot era,” in *2019 24th OptoElectronics and Communications Conference (OECC) and 2019 International Conference on Photonics in Switching and Computing (PSC)*, pp. 1–1, IEEE, 2019.
- [23] S. Ugwuanyi and J. Irvine, “Industrial and consumer internet of things: cyber security considerations, threat landscape, and countermeasure opportunities,” in *2021 International Conference on Smart Applications, Communications and Networking (SmartNets): Security and Privacy for Smart IoT and CPS*, 2021.
- [24] M. Pätzold, “5g unlocks its power for global mobile connectivity [mobile radio],” *IEEE Vehicular Technology Magazine*, vol. 15, no. 2, pp. 5–11, 2020.
- [25] S. Naik and V. Maral, “Cyber security — iot,” in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*, pp. 764–767, 2017.
- [26] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, “A survey on security and privacy issues in edge computing-assisted internet of things,” *IEEE Internet of Things Journal*, 2020.
- [27] C. S. Abella, S. Bonina, A. Cucuccio, S. D’Angelo, G. Giustolisi, A. D. Grasso, A. Imbruglia, G. S. Mauro, G. A. Nastasi, G. Palumbo, *et al.*, “Autonomous energy-efficient wireless sensor network platform for home/office automation,” *IEEE Sensors Journal*, vol. 19, no. 9, pp. 3501–3512, 2019.

Bibliography

- [28] S. Bhandari, S. K. Sharma, and X. Wang, “Latency minimization in wireless iot using prioritized channel access and data aggregation,” in *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pp. 1–6, IEEE, 2017.
- [29] K. Ghanem, R. Asif, S. Ugwuanyi, and J. Irvine, “Bandwidth and security requirements for smart grid,” in *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, pp. 36–40, IEEE, 2020.
- [30] G. Mulligan, “Ipv6 for iot and gateway,” *Internet of Things and Data Analytics Handbook*, pp. 187–196, 2017.
- [31] Y. Sun, F. P.-W. Lo, and B. Lo, “Light-weight internet-of-things device authentication, encryption and key distribution using end-to-end neural cryptosystems,” *IEEE Internet of Things Journal*, 2021.
- [32] S. Li, S. Zhao, G. Min, L. Qi, and G. Liu, “Lightweight privacy-preserving scheme using homomorphic encryption in industrial internet of things,” *IEEE Internet of Things Journal*, 2021.
- [33] D. Tan and D. Novosel, “Energy challenge, power electronics & systems (peas) technology and grid modernization,” *CPSS Transactions on Power Electronics and Applications*, vol. 2, no. 1, pp. 3–11, 2017.
- [34] S. O. Olatinwo and T.-H. Joubert, “Energy efficient solutions in wireless sensor systems for water quality monitoring: A review,” *IEEE Sensors Journal*, vol. 19, no. 5, pp. 1596–1625, 2018.
- [35] T. Xu and I. Darwazeh, “Non-orthogonal narrowband internet of things: A design for saving bandwidth and doubling the number of connected devices,” *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2120–2129, 2018.
- [36] F. Lelli, “Interoperability of the time of industry 4.0 and the internet of things,” *Future Internet*, vol. 11, no. 2, p. 36, 2019.

Bibliography

- [37] S. Pinto, T. Gomes, J. Pereira, J. Cabral, and A. Tavares, “Ioteed: an enhanced, trusted execution environment for industrial iot edge devices,” *IEEE Internet Computing*, vol. 21, no. 1, pp. 40–47, 2017.
- [38] C.-H. Hong and B. Varghese, “Resource management in fog/edge computing: a survey on architectures, infrastructure, and algorithms,” *ACM Computing Surveys (CSUR)*, vol. 52, no. 5, pp. 1–37, 2019.
- [39] C. Badii, P. Bellini, A. Difino, and P. Nesi, “Smart city iot platform respecting gdpr privacy and security aspects,” *IEEE Access*, vol. 8, pp. 23601–23623, 2020.
- [40] F. Cleveland, “Iec tc57 security standards for the power system’s information infrastructure—beyond simple encryption,” in *Transmission and Distribution Conference and Exhibition*, vol. 2006, pp. 1079–1087, 2005.
- [41] M. Mehta and K. Patel, “A review for iot authentication—current research trends and open challenges,” *Materials Today: Proceedings*, 2020.
- [42] M. Wang and Z. Yan, “Privacy-preserving authentication and key agreement protocols for d2d group communications,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3637–3647, 2017.
- [43] M. A. Ferrag, L. Maglaras, A. Derhab, and H. Janicke, “Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues,” *Telecommunication Systems*, vol. 73, no. 2, pp. 317–348, 2020.
- [44] S. Lakshminarayanan, “Authentication and authorization for smart grid application interfaces,” in *2011 IEEE/PES Power Systems Conference and Exposition*, pp. 1–5, IEEE, 2011.
- [45] A. Koivu, L. Koivunen, S. Hosseinzadeh, S. Laurén, S. Hyrynsalmi, S. Rauti, and V. Leppänen, “Software security considerations for iot,” in *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCoM) and IEEE Smart Data (SmartData)*, pp. 392–397, IEEE, 2016.

Bibliography

- [46] Y. Pan, J. White, D. Schmidt, A. Elhabashy, L. Sturm, J. Camelio, and C. Williams, “Taxonomies for reasoning about cyber-physical attacks in iot-based manufacturing systems,” 2017.
- [47] L. Wigle, “Intel and arm share iot vision to securely connect ‘any device to any cloud’.” <https://newsroom.intel.com/editorials/intel-arm-share-iot-vision-securely-connect-any-device-any-cloud/#gs.bto8p1>, 10 2018. (Accessed on 09/27/2021).
- [48] A. Triantafyllou, P. Sarigiannidis, and T. D. Lagkas, “Network protocols, schemes, and mechanisms for internet of things (iot): Features, open challenges, and trends,” *Wireless communications and mobile computing*, vol. 2018, 2018.
- [49] C. L. C. Bureau, “Sb-327 information privacy: connected devices.” https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327, 09 2018. (Accessed on 06/08/2021).
- [50] DCMS, “Secure by design.” <https://www.gov.uk/government/collections/secure-by-design>, 02 2019. (Accessed on 06/08/2021).
- [51] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, “Systematically evaluating security and privacy for consumer iot devices,” in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, pp. 1–6, 2017.
- [52] L. Mathews, “Hackers use ddos attack to cut heat to apartments.” <https://www.forbes.com/sites/leemathews/2016/11/07/ddos-attack-leaves-finnish-apartments-without-heat/#4e13f6f71a09>, 11 2016. (Accessed on 06/07/2021).
- [53] M. PEÑALOZA, “Ransomware attack shuts down colonial pipeline.” <https://www.npr.org/2021/05/08/995040240/cybersecurity-attack-shuts-down-a-top-u-s-gasoline-pipeline?t=1621954536124>, 05 2021. (Accessed on 06/07/2021).

Bibliography

- [54] M. Bettayeb, Q. Nasir, and M. A. Talib, “Firmware update attacks and security for iot devices: Survey,” in *Proceedings of the ArabWIC 6th Annual International Conference Research Track*, pp. 1–6, 2019.
- [55] A. Gilchrist, *IoT security issues*. Walter de Gruyter GmbH & Co KG, 2017.
- [56] M. M. Ahemd, M. A. Shah, and A. Wahid, “Iot security: A layered approach for attacks & defenses,” in *2017 International Conference on Communication Technologies (ComTech)*, pp. 104–110, IEEE, 2017.
- [57] R. Román-Castro, J. López, and S. Gritzalis, “Evolution and trends in iot security,” *Computer*, vol. 51, no. 7, pp. 16–25, 2018.
- [58] D. Dolezilek, D. Gammel, and W. Fernandes, “Cybersecurity based on iec 62351 and iec 62443 for iec 61850 systems,” in *15th International Conference on Developments in Power System Protection (DPSP 2020)*, pp. 1–6, 2020.
- [59] A. Mittal, A. Slaughter, and P. Zonneveld, “Protecting the connected barrels: Cybersecurity for upstream oil and gas,” *Deloitte Insights, London, UK, Tech. Rep*, 2017.
- [60] K. J. Higgins, “Industrial safety systems in the bullseye.” <https://www.darkreading.com/operations/industrial-safety-systems-in-the-bullseye/d/d-id/1330912>, 01 2018. (Accessed on 06/08/2021).
- [61] C. D. McDermott, F. Majdani, and A. V. Petrovski, “Botnet detection in the internet of things using deep learning approaches,” in *2018 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–8, IEEE, 2018.
- [62] 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.

Bibliography

- [63] S. Cheruvu, A. Kumar, N. Smith, and D. M. Wheeler, *Demystifying internet of things security: successful iot device/edge and platform security deployment*. Springer Nature, 2020.
- [64] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, “Security and privacy challenges in industrial internet of things,” in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–6, IEEE, 2015.
- [65] Y. Ikezaki, Y. Nozaki, and M. Yoshikawa, “Iot device oriented security module using puf,” in *2016 IEEE International Meeting for Future of Electron Devices, Kansai (IMFEDK)*, pp. 1–2, IEEE, 2016.
- [66] T. Idriss, H. Idriss, and M. Bayoumi, “A puf-based paradigm for iot security,” in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pp. 700–705, IEEE, 2016.
- [67] A. Anastasiou, P. Christodoulou, K. Christodoulou, V. Vassiliou, and Z. Zinonos, “Iot device firmware update over lora: The blockchain solution,” in *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 404–411, IEEE, 2020.
- [68] S. M. Danish, M. Lestas, H. K. Qureshi, K. Zhang, W. Asif, and M. Rajarajan, “Securing the lorawan join procedure using blockchains,” *Cluster Computing*, vol. 23, no. 3, pp. 2123–2138, 2020.
- [69] H. Lu, K. Huang, M. Azimi, and L. Guo, “Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks,” *IEEE Access*, vol. 7, pp. 41426–41444, 2019.
- [70] A. Azari, Č. Stefanović, P. Popovski, and C. Cavdar, “On the latency-energy performance of nb-iot systems in providing wide-area iot connectivity,” *IEEE Transactions on Green Communications and Networking*, vol. 4, no. 1, pp. 57–68, 2019.

Bibliography

- [71] D. Yang, X. Zhang, X. Huang, L. Shen, J. Huang, X. Chang, and G. Xing, "Understanding power consumption of nb-iot in the wild: tool and large-scale measurement," in *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, pp. 1–13, 2020.
- [72] H. Zhu, K. F. Tsang, Y. Liu, Y. Wei, H. Wang, C. K. Wu, and W. H. Wan, "Index of low-power wide area networks: A ranking solution toward best practice," *IEEE Communications Magazine*, vol. 59, no. 4, pp. 139–144, 2021.
- [73] A. Makhshari and A. Mesbah, "Iot bugs and development challenges," in *2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE)*, pp. 460–472, IEEE, 2021.
- [74] O. I. Abiodun, E. O. Abiodun, M. Alawida, R. S. Alkhawaldeh, and H. Arshad, "A review on the security of the internet of things: Challenges and solutions," *Wireless Personal Communications*, pp. 1–35, 2021.
- [75] L. Mathews, "Hackers use ddos attack to cut heat to apartments," *URL: <http://www.forbes.com/sites/leemathews/2016/11/07/ddos-attackleaves-finnish-apartments-without-heat/>* (cited on pp. 1, 3, 14, 35), 2016.
- [76] A. Banafa, "Three major challenges facing iot," *IEEE Internet of things*, 2017.
- [77] M. Lauridsen, H. Nguyen, B. Vejlgaard, I. Z. Kovács, P. Mogensen, and M. Sorensen, "Coverage comparison of gprs, nb-iot, lora, and sigfox in a 7800 km² area," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, pp. 1–5, IEEE, 2017.
- [78] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovács, P. Mogensen, and M. Sorensen, "Coverage and capacity analysis of sigfox, lora, gprs, and nb-iot," in *2017 IEEE 85th vehicular technology conference (VTC Spring)*, pp. 1–5, IEEE, 2017.

Bibliography

- [79] M. Lauridsen, I. Z. Kovács, P. Mogensen, M. Sorensen, and S. Holst, “Coverage and capacity analysis of lte-m and nb-iot in a rural area,” in *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, pp. 1–5, IEEE, 2016.
- [80] Y. Al Mtawa, A. Haque, and B. Bitar, “Does internet of things disrupt residential bandwidth consumption?,” in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, pp. 1–5, IEEE, 2018.
- [81] Y. Xu, S. Helal, C. Lee, and A. Khaled, “Energy savings in very large cloud-iot systems,” 2019.
- [82] N. G. Miloslavskaya, A. Nikiforov, K. Plaksiy, and A. I. Tolstoy, “Standardization issues for the internet of things,” in *WorldCIST (2)*, pp. 328–338, 2019.
- [83] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim, and S. R. Chaudhry, “Iot architecture challenges and issues: Lack of standardization,” in *2016 Future technologies conference (FTC)*, pp. 731–738, IEEE, 2016.
- [84] F. Ertam, I. F. Kilincer, O. Yaman, and A. Sengur, “A new iot application for dynamic wifi based wireless sensor network,” in *2020 International Conference on Electrical Engineering (ICEE)*, pp. 1–4, IEEE, 2020.
- [85] M. Hammache, R. Kacimi, and A.-L. Beylot, “Unifying lorawan networks by enabling the roaming capability,” in *2021 IEEE 46th Conference on Local Computer Networks (LCN)*, pp. 371–374, IEEE, 2021.
- [86] F. Flammini, A. Gaglione, D. Tokody, and D. Dohrilovic, “Lora wan roaming for intelligent shipment tracking,” in *2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT)*, pp. 01–02, IEEE, 2020.
- [87] S. Ezekiel, D. M. Divakaran, and M. Gurusamy, “Dynamic attack mitigation using sdn,” in *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 1–6, IEEE, 2017.
- [88] R. K. Jha, H. Kour, M. Kumar, S. Jain, *et al.*, “Layer based security in narrow band internet of things (nb-iot),” *Computer Networks*, vol. 185, p. 107592, 2021.

Bibliography

- [89] G. Nebbione and M. C. Calzarossa, “Security of iot application layer protocols: Challenges and findings,” *Future Internet*, vol. 12, no. 3, p. 55, 2020.
- [90] B. Yang and M. Yang, “Data-driven network layer security detection model and simulation for the internet of things based on an artificial immune system,” *Neural Computing and Applications*, vol. 33, no. 2, pp. 655–666, 2021.
- [91] P. Semwal and M. K. Sharma, “Comparative study of different cryptographic algorithms for data security in cloud computing,” in *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)*, pp. 1–7, IEEE, 2017.
- [92] B. Mostefa and G. Abdelkader, “A survey of wireless sensor network security in the context of internet of things,” in *2017 4th International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, pp. 1–8, IEEE, 2017.
- [93] R. McPherson, C. Hay, and J. Irvine, “Using lorawan technology to enhance remote power network monitoring,” in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, pp. 1–5, IEEE, 2019.
- [94] IETF, “The internet of things at the ietf.” <https://www.ietf.org/topics/iot/>. (Accessed on 07/15/2021).
- [95] K. Foote, “A brief history of the internet of things.” <https://www.dataversity.net/brief-history-internet-things/>, 08 2016. (Accessed on 10/15/2021).
- [96] A. Rayes and S. Salam, “Internet of things from hype to reality,” *Springer*, 2017.
- [97] B. Bolt and I. Newman, “A history of the arpanet: The first decade.” <https://www.scribd.com/document/202131512/A-History-of-the-ARPANET-The-First-Decade-Report-Arlington-VA-Bolt-Beranek-New> 04 1981. (Accessed on 06/03/2021).
- [98] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, “Internet of things in the 5g era: Enablers, architecture, and busi-

Bibliography

- ness models,” *IEEE journal on selected areas in communications*, vol. 34, no. 3, pp. 510–527, 2016.
- [99] C. M. Roberts, “Radio frequency identification (rfid),” *Computers & security*, vol. 25, no. 1, pp. 18–26, 2006.
- [100] C. Machine, “The” only” coke machine on the internet,” 2014.
- [101] K. Tassin, “Lte and the internet of things.” <https://www.3gpp.org/news-events/3gpp-news/1607-iot>, 2016. (Accessed on 02/24/2021).
- [102] N. Sharma, M. Shamkuwar, and I. Singh, “The history, present and future with iot,” in *Internet of Things and Big Data Analytics for Smart Generation*, pp. 27–51, Springer, 2019.
- [103] Cisco, “Cisco annual internet report (2018–2023) white paper.” <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf>, 03 2020. (Accessed on 11/02/2021).
- [104] S. Bhattarai and Y. Wang, “End-to-end trust and security for internet of things applications,” *Computer*, vol. 51, no. 4, pp. 20–27, 2018.
- [105] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow, and M. N. Hindia, “An overview of internet of things (iot) and data analytics in agriculture: Benefits and challenges,” *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3758–3773, 2018.
- [106] A. Faulkner, “Evolution of fraud in the iot era.” <https://www.techradar.com/sg/news/evolution-of-fraud-in-the-iot-era>, 08 2018. (Accessed on 06/09/2021).
- [107] K. Gupta and S. Shukla, “Internet of things: Security challenges for next generation networks,” in *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*, pp. 315–318, IEEE, 2016.

Bibliography

- [108] D. Pishva, “Internet of things: Security and privacy issues and possible solution,” in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, pp. 797–808, IEEE, 2017.
- [109] A. Mosenia and N. K. Jha, “A comprehensive study of security of internet-of-things,” *IEEE Transactions on emerging topics in computing*, vol. 5, no. 4, pp. 586–602, 2016.
- [110] G. Premsankar, M. Di Francesco, and T. Taleb, “Edge computing for the internet of things: A case study,” *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1275–1284, 2018.
- [111] B. Diène, J. J. Rodrigues, O. Diallo, E. H. M. Ndoeye, and V. V. Korotaev, “Data management techniques for internet of things,” *Mechanical Systems and Signal Processing*, vol. 138, p. 106564, 2020.
- [112] OSIsoft, “Operational intelligence.” <https://www.osisoft.com/>. (Accessed on 07/13/2021).
- [113] G. Digital, “Overview predix platform.” <https://www.ge.com/digital/documentation/predix-platforms/predix-insights-overview.html>. (Accessed on 07/13/2021).
- [114] Flutura, “Industrial ai and iiot.” <https://www.flutura.com/>. (Accessed on 07/13/2021).
- [115] M. Azure, “Azure iot – internet of things platform.” <https://azure.microsoft.com/en-gb/overview/iot/>. (Accessed on 07/13/2021).
- [116] IBM, “Watson iot platform.” <https://www.ibm.com/cloud/watson-iot-platform>. (Accessed on 07/13/2021).
- [117] X. Feng, F. Yan, and X. Liu, “Study of wireless communication technologies on internet of things for precision agriculture,” *Wireless Personal Communications*, vol. 108, no. 3, pp. 1785–1802, 2019.

Bibliography

- [118] P. Stenumgaard, J. Chilo, J. Ferrer-Coll, and P. Angskog, “Challenges and conditions for wireless machine-to-machine communications in industrial environments,” *IEEE Communications Magazine*, vol. 51, no. 6, pp. 187–192, 2013.
- [119] ETSI, “Low throughput networks (ltn): Use cases, functional architecture, and protocols,” *ETSI GS LTN 001*, 2014.
- [120] A. S. Petrenko, S. A. Petrenko, K. A. Makoveichuk, and P. V. Chetyrbok, “The iiot/iot device control model based on narrow-band iot (nb-iot),” in *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pp. 950–953, IEEE, 2018.
- [121] O. Ologun, S. Wu, Y. Gao, and X. Zhou, “Narrowband-iot as an effective developmental strategy for internet of things in sub-saharan africa: Nigerian case study,” in *International Conference on Wireless and Satellite Systems*, pp. 56–69, Springer, 2019.
- [122] P. Goyal, A. K. Sahoo, T. K. Sharma, and P. K. Singh, “Internet of things: Applications, security and privacy: A survey,” *Materials Today: Proceedings*, vol. 34, pp. 752–759, 2021.
- [123] J.-Q. Li, F. R. Yu, G. Deng, C. Luo, Z. Ming, and Q. Yan, “Industrial internet: A survey on the enabling technologies, applications, and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1504–1526, 2017.
- [124] B. Omoniwa, R. Hussain, M. A. Javed, S. H. Bouk, and S. A. Malik, “Fog/edge computing-based iot (feciot): Architecture, applications, and research issues,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4118–4149, 2018.
- [125] Q. F. Hassan, *The Internet of Flying Things*, pp. 529–562. 2018.
- [126] S. S. Reka and T. Dragicevic, “Future effectual role of energy delivery: A comprehensive review of internet of things and smart grid,” *Renewable and Sustainable Energy Reviews*, vol. 91, pp. 90–108, 2018.

Bibliography

- [127] A. Ghasempour, “Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges,” *Inventions*, vol. 4, no. 1, p. 22, 2019.
- [128] Y. Uygun and E. B. Reynolds, “Advanced manufacturing innovation ecosystems: The case of massachusetts,” in *Industrial Internet of Things*, pp. 691–715, Springer, 2017.
- [129] S. Ugwuanyi and J. Irvine, “Intelligent internet of things (iot) node demonstrator for device monitoring and control in the oil and gas sector,” *arXiv preprint arXiv:1902.10255*, 2019.
- [130] J. Navarro-Ortiz, S. Sendra, P. Ameigeiras, and J. M. Lopez-Soler, “Integration of lorawan and 4g/5g for the industrial internet of things,” *IEEE Communications Magazine*, vol. 56, no. 2, pp. 60–67, 2018.
- [131] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. Aswathy, “A state of the art review on the internet of things (iot) history, technology and fields of deployment,” in *2014 International conference on science engineering and management research (ICSEMR)*, pp. 1–8, IEEE, 2014.
- [132] T. Lennvall, M. Gidlund, and J. Åkerberg, “Challenges when bringing iot into industrial automation,” in *2017 IEEE AFRICON*, pp. 905–910, IEEE, 2017.
- [133] A. Nourian and S. Madnick, “A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet,” *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 1, pp. 2–13, 2015.
- [134] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “Ddos in the iot: Mirai and other botnets,” *Computer*, vol. 50, no. 7, pp. 80–84, 2017.
- [135] M. Hemmatpour, M. Ghazivakili, B. Montrucchio, and M. Rebaudengo, “Diig: a distributed industrial iot gateway,” in *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, vol. 1, pp. 755–759, IEEE, 2017.
- [136] S. Raza, *Lightweight security solutions for the internet of things*. PhD thesis, Mälardalen University, Västerås, Sweden, 2013.

Bibliography

- [137] A. P. Castellani, “Design, implementation and experimentation of a protocol stack for the internet of things,” 2012.
- [138] I. I. Consortium *et al.*, “Why we build testbeds: First results,” 2017.
- [139] J. Wan, A. Canedo, and M. A. Al Faruque, “Security-aware functional modeling of cyber-physical systems,” in *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, pp. 1–4, IEEE, 2015.
- [140] A. Presekal, A. Ştefanov, V. S. Rajkumar, and P. Palensky, “Attack graph model for cyber-physical power systems using hybrid deep learning,” *IEEE Transactions on Smart Grid*, 2023.
- [141] G. S. Rose, “Security meets nanoelectronics for internet of things applications,” in *Proceedings of the 26th edition on Great Lakes Symposium on VLSI*, pp. 181–183, ACM, 2016.
- [142] K. Sun, Y. Shen, Y. Lao, Z. Zhang, X. You, and C. Zhang, “A new error correction scheme for physical unclonable function,” in *2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, pp. 374–377, IEEE, 2018.
- [143] B. Karpinsky, Y. Lee, Y. Choi, Y. Kim, M. Noh, and S. Lee, “8.7 physically unclonable function for secure key generation with a key error rate of $2e-38$ in 45nm smart-card chips,” in *2016 IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 158–160, IEEE, 2016.
- [144] W. Liu, Z. Lu, H. Liu, R. Min, Z. Zeng, and Z. Liu, “A novel security key generation method for sram puf based on fourier analysis,” *IEEE Access*, vol. 6, pp. 49576–49587, 2018.
- [145] H. Kang, Y. Hori, T. Katashita, M. Hagiwara, and K. Iwamura, “Cryptographic key generation from puf data using efficient fuzzy extractors,” in *16th International Conference on Advanced Communication Technology*, pp. 23–26, IEEE, 2014.

Bibliography

- [146] Devices and Systems, “Traffic-aware patching for iot device cyber security.” <https://innovate.ieee.org/innovation-spotlight/traffic-aware-patching-intermediate-nodes-cyber-security-iot-devices/>, 12 2017. (Accessed on 06/07/2021).
- [147] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, “A multi-level ddos mitigation framework for the industrial internet of things,” *IEEE Communications Magazine*, vol. 56, no. 2, pp. 30–36, 2018.
- [148] G. George and S. M. Thampi, “A graph-based security framework for securing industrial iot networks from vulnerability exploitations,” *IEEE Access*, vol. 6, pp. 43586–43601, 2018.
- [149] D. Wang, S. Lee, Y. Zhu, and Y. Li, “A zero human-intervention provisioning for industrial iot devices,” in *2017 IEEE International Conference on Industrial Technology (ICIT)*, pp. 1271–1276, IEEE, 2017.
- [150] S. Jaloudi, “Communication protocols of an industrial internet of things environment: A comparative study,” *Future Internet*, vol. 11, no. 3, p. 66, 2019.
- [151] E. Al-Masri, K. R. Kalyanam, J. Batts, J. Kim, S. Singh, T. Vo, and C. Yan, “Investigating messaging protocols for the internet of things (iot),” *IEEE Access*, vol. 8, pp. 94880–94911, 2020.
- [152] V. S. Naresh, S. Reddi, and V. D. Allavarpu, “Lightweight secure communication system based on message queuing transport telemetry protocol for e-healthcare environments,” *International Journal of Communication Systems*, vol. 34, no. 11, p. e4842, 2021.
- [153] O. Standard, “Mqtt version 3.1. 1 plus errata 01,” 12 2015.
- [154] R. A. Light, “Mosquitto: server and client implementation of the mqtt protocol,” *Journal of Open Source Software*, vol. 2, no. 13, p. 265, 2017.
- [155] IETF, “Rfc 6455 - the websocket protocol.” <https://tools.ietf.org/html/rfc6455>, December 2011. (Accessed on 09/24/2020).

Bibliography

- [156] N. Pawar, T. Bourgeau, and H. Chaouchi, “Study of iot architecture and application invariant functionalities,” in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 667–671, IEEE, 2021.
- [157] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of things security and forensics: Challenges and opportunities,” 2018.
- [158] M. Martonosi, “Keynotes: Internet of things: History and hype, technology and policy,” in *2016 49th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, pp. 1–2, IEEE, 2016.
- [159] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, “Challenges and opportunities in securing the industrial internet of things,” *IEEE Transactions on Industrial Informatics*, 2020.
- [160] W. Jin, Z. Liu, Z. Shi, C. Jin, and J. Lee, “Cps-enabled worry-free industrial applications,” in *2017 Prognostics and System Health Management Conference (PHM-Harbin)*, pp. 1–7, IEEE, 2017.
- [161] H. Magsi, A. H. Sodhro, N. Zahid, S. Pirbhulal, L. Wang, and M. S. Al-Rakhami, “A novel adaptive battery-aware algorithm for data transmission in iot-based healthcare applications,” *Electronics*, vol. 10, no. 4, p. 367, 2021.
- [162] F. Nasri and A. Mtibaa, “Smart mobile healthcare system based on wbsn and 5g,” *IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 8, no. 10, 2017.
- [163] L. Chunli, “Intelligent transportation based on the internet of things,” in *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, pp. 360–362, IEEE, 2012.
- [164] ENA, “Energy delivery systems cyber security procurement guidance.” <https://www.energynetworks.org/industry-hub/resource-library/energy-delivery-systems-cyber-security-procurement-guidance.pdf>, 2018. (Accessed on 06/23/2021).

Bibliography

- [165] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, “Smart grid metering networks: A survey on security, privacy and open research issues,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2886–2927, 2019.
- [166] Y. Li, X. Cheng, Y. Cao, D. Wang, and L. Yang, “Smart choice for the smart grid: Narrowband internet of things (nb-iot),” *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1505–1515, 2018.
- [167] M. D. Cavelty, “Cyber-security,” *The routledge handbook of new security studies*, pp. 154–162, 2010.
- [168] I. I. Consortium, “Why we build testbeds: First results.” <https://www.iiconsortium.org/test-beds.htm>, 2017. Last accessed 17 April 2020.
- [169] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, “Security and privacy in device-to-device (d2d) communication: A review,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1054–1079, 2017.
- [170] L. Chen, “Security management for the internet of things,” 2017.
- [171] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, “Internet of things: Security vulnerabilities and challenges,” in *2015 IEEE Symposium on Computers and Communication (ISCC)*, pp. 180–187, IEEE, 2015.
- [172] S.-C. Hsiao and D.-Y. Kao, “The static analysis of wannacry ransomware,” in *2018 20th International Conference on Advanced Communication Technology (ICACT)*, pp. 153–158, IEEE, 2018.
- [173] A. Batcheller, S. C. Fowler, R. Cunningham, D. Doyle, T. Jaeger, and U. Lindqvist, “Building on the success of building security in,” *IEEE Security & Privacy*, vol. 15, no. 4, pp. 85–87, 2017.
- [174] Y. Chahid, M. Benabdellah, and A. Azizi, “Internet of things security,” in *2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*, pp. 1–6, IEEE, 2017.

Bibliography

- [175] H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: a review,” in *2012 international conference on computer science and electronics engineering*, vol. 3, pp. 648–651, IEEE, 2012.
- [176] D. Pietro, “Security and trust challenges in the area of iot,” 2012.
- [177] C. Lesjak, D. Hein, and J. Winter, “Hardware-security technologies for industrial iot: Trustzone and security controller,” in *IECON 2015-41st Annual Conference of the IEEE Industrial Electronics Society*, pp. 002589–002595, IEEE, 2015.
- [178] J. Kim and J. Song, “A secure device-to-device link establishment scheme for lorawan,” *IEEE Sensors Journal*, vol. 18, no. 5, pp. 2153–2160, 2018.
- [179] H. Wang, L. Shao, M. Li, B. Wang, and P. Wang, “Estimation of clock skew for time synchronization based on two-way message exchange mechanism in industrial wireless sensor networks,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4755–4765, 2018.
- [180] v. d. V. Hans and W. Anthony, “Achieving technical interoperability - the etsi approach.” [https://www.etsi.org/images/files/ETSIWhitePapers/IOP,04 2008](https://www.etsi.org/images/files/ETSIWhitePapers/IOP,04%2008.pdf). (Accessed on 10/16/2021).
- [181] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.
- [182] N. Phungamngern, P. Uthansakul, and M. Uthansakul, “Digital and rf interference cancellation for single-channel full-duplex transceiver using a single antenna,” in *2013 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*, pp. 1–5, IEEE, 2013.

Bibliography

- [183] A. S. Elmaghraby and M. M. Losavio, “Cyber security challenges in smart cities: Safety, security and privacy,” *Journal of advanced research*, vol. 5, no. 4, pp. 491–497, 2014.
- [184] S. Bhunia and M. Tehranipoor, *Hardware security: a hands-on learning approach*. Morgan Kaufmann, 2018.
- [185] G. Ferrari, *Sensor Networks: where theory meets practice*. Springer Science & Business Media, 2010.
- [186] M. Wang and Z. Yan, “A survey on security in d2d communications,” *Mobile Networks and Applications*, vol. 22, no. 2, pp. 195–208, 2017.
- [187] W. Yang, Y. Wan, and Q. Wang, “Enhanced secure time synchronisation protocol for ieee802. 15.4 e-based industrial internet of things,” *IET Information Security*, vol. 11, no. 6, pp. 369–376, 2017.
- [188] M. Shankar and P. Akshaya, “Hybrid cryptographic technique using rsa algorithm and scheduling concepts,” *International Journal of Network Security & Its Applications*, vol. 6, no. 6, p. 39, 2014.
- [189] Z. Sun, Q. Guo, and F. Sun, “Key management for feeder automation systems with centralized mode,” in *2009 International Conference on Information Management, Innovation Management and Industrial Engineering*, vol. 4, pp. 456–459, IEEE, 2009.
- [190] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, “Nist special publication 800-57,” *NIST Special publication*, vol. 800, no. 57, pp. 1–142, 2007.
- [191] F. L. Coman, K. M. Malarski, M. N. Petersen, and S. Ruepp, “Security issues in internet of things: Vulnerability analysis of lorawan, sigfox and nb-iot,” in *2019 Global IoT Summit (GIoTS)*, pp. 1–6, IEEE, 2019.
- [192] D. Baimel, S. Tapuchi, and N. Baimel, “Smart grid communication technologies-overview, research challenges and opportunities,” in *2016 International Sym-*

Bibliography

- posium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM)*, pp. 116–120, IEEE, 2016.
- [193] D. S. Pidikiti, R. Kalluri, R. S. Kumar, and B. Bindhumadhava, “Scada communication protocols: vulnerabilities, attacks and possible mitigations,” *CSI transactions on ICT*, vol. 1, no. 2, pp. 135–141, 2013.
- [194] M. Garau, G. Celli, E. Ghiani, F. Pilo, and S. Corti, “Evaluation of smart grid communication technologies with a co-simulation platform,” *IEEE Wireless Communications*, vol. 24, no. 2, pp. 42–49, 2017.
- [195] Guardian, “Storm barra leaves thousands without power in ireland.” <https://www.theguardian.com/uk-news/2021/dec/07/storm-barra-thousands-without-power-ireland-met-office-uk>, 12 2021. (Accessed on 12/09/2021).
- [196] D. M. Lavery, D. J. Morrow, R. Best, and P. A. Crossley, “Telecommunications for smart grid: Backhaul solutions for the distribution network,” in *IEEE PES General Meeting*, pp. 1–6, IEEE, 2010.
- [197] R. Ma, H.-H. Chen, Y.-R. Huang, and W. Meng, “Smart grid communication: Its challenges and opportunities,” *IEEE transactions on Smart Grid*, vol. 4, no. 1, pp. 36–46, 2013.
- [198] L. Tightiz and H. Yang, “A comprehensive review on iot protocols’ features in smart grid communication,” *Energies*, vol. 13, no. 11, p. 2762, 2020.
- [199] F. Cleveland, “Iec tc57 wg15: Iec 62351 security standards for the power system information infrastructure,” *White Paper*, 2012.
- [200] F. Ye, Y. Qian, and R. Q. Hu, “Security challenges in the smart grid communication infrastructure,” 2017.
- [201] R. Amoah, S. Camtepe, and E. Foo, “Securing dnp3 broadcast communications in scada systems,” *IEEE Transactions on Industrial Informatics*, vol. 12, no. 4, pp. 1474–1485, 2016.

Bibliography

- [202] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi, “Attack taxonomies for the modbus protocols,” *International Journal of Critical Infrastructure Protection*, vol. 1, pp. 37–44, 2008.
- [203] G. Corotinschi and V. G. Găitan, “Enabling iot connectivity for modbus networks by using iot edge gateways,” in *2018 International Conference on Development and Application Systems (DAS)*, pp. 175–179, IEEE, 2018.
- [204] F. Shu, H. Lu, and Y. Ding, “Novel modbus adaptation method for iot gateway,” in *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, pp. 632–637, IEEE, 2019.
- [205] I. N. Fovino, A. Carcano, M. Masera, and A. Trombetta, “Design and implementation of a secure modbus protocol,” in *International conference on critical infrastructure protection*, pp. 83–96, Springer, 2009.
- [206] M. K. Ferst, H. F. de Figueiredo, G. Denardin, and J. Lopes, “Implementation of secure communication with modbus and transport layer security protocols,” in *2018 13th IEEE International Conference on Industry Applications (INDUSCON)*, pp. 155–162, IEEE, 2018.
- [207] C. Fachkha, “Cyber threat investigation of scada modbus activities,” in *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–7, IEEE, 2019.
- [208] M. Cebe and K. Akkaya, “A bandwidth-efficient secure authentication module for smart grid dnp3 protocol,” in *2020 Resilience Week (RWS)*, pp. 160–166, IEEE, 2020.
- [209] C. Rosborough, C. Gordon, and B. Waldron, “All about eve: Comparing dnp3 secure authentication with standard security technologies for scada communications,” 2019.

Bibliography

- [210] G. Gilchrist, “Secure authentication for dnp3,” in *2008 IEEE Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century*, pp. 1–3, IEEE, 2008.
- [211] A. Albarakati, C. Robillard, M. Karanfil, M. Kassouf, R. Hadjadj, M. Debbabi, and A. Youssef, “Security monitoring of iec 61850 substations using iec 62351-7 network and system management,” in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (Smart-GridComm)*, pp. 1–7, IEEE, 2019.
- [212] A. Riccardo and H. Vardhan, “Iec 61850 digital substation design tutorial for novices,” in *2019 72nd Conference for Protective Relay Engineers (CPRE)*, pp. 1–7, IEEE, 2019.
- [213] R. E. Mackiewicz, “Overview of iec 61850 and benefits,” in *2006 IEEE Power Engineering Society General Meeting*, pp. 8–pp, IEEE, 2006.
- [214] A. L. Franceschett, P. R. A. d. Souza, F. L. Pereira de Barros, and V. R. de Carvalho, “A holistic approach - how to achieve the state-of-art in cybersecurity for a secondary distribution automation energy system applying the iec 62443 standard,” in *2019 IEEE PES Innovative Smart Grid Technologies Conference - Latin America (ISGT Latin America)*, pp. 1–5, 2019.
- [215] T. IEC, “62351-1 (2007) power systems management and associated information exchange—data and communications security part i: Communication network and system security—introduction to security issues.”
- [216] R. Mattioli and K. Moulinos, “Communication network interdependencies in smart grids,” *EUA FNAI Security, Ed., ed. EU: ENISA*, 2015.
- [217] A. Lee, “Guidelines for smart grid cyber security,” 2010.
- [218] IEC, “Iec-62351-5 — power systems management and associated information exchange - data and communications security - part 5: Security for iec 60870-5 and derivatives,” 2009. (Accessed on 12/14/2021).

Bibliography

- [219] BSI, “Iec 62351-9 - power systems management and associated information exchange - data and communications security - part 9: Cyber security key management for power system equipment,” 2017. (Accessed on 12/14/2021).
- [220] R. S. Sinha, Y. Wei, and S.-H. Hwang, “A survey on lpwa technology: Lora and nb-iot,” *Ict Express*, vol. 3, no. 1, pp. 14–21, 2017.
- [221] R. Kufakunesu, G. P. Hancke, and A. M. Abu-Mahfouz, “A survey on adaptive data rate optimization in lorawan: Recent solutions and major challenges,” *Sensors*, vol. 20, no. 18, p. 5044, 2020.
- [222] F. W. L. Alliance, “Lorawan® remote multicast setup specification v1.0.0.” <https://lora-alliance.org/resource-hub/lorawanr-remote-multicast-setup-specification-v100>, September 2018. (Accessed on 10/13/2020).
- [223] D. Ron, C.-J. Lee, K. Lee, H.-H. Choi, and J.-R. Lee, “Performance analysis and optimization of downlink transmission in lorawan class b mode,” *IEEE Internet of Things Journal*, 2020.
- [224] L. Alliance, “Lorawan regional parameters v1.1.” <https://lora-alliance.org/wp-content/uploads/2020/11/lorawan-regional-parameters-v1.1ra.pdf>, 2017. (Accessed on 11/24/2021).
- [225] L. Alliance, “Fuota process summary technical recommendation tr002 v1.0.0 - lora alliance®.” https://lora-alliance.org/resource_hub/fuota-process-summary-technical-recommendation-tr002-v1-0-0/, 30 2019. (Accessed on 09/17/2021).
- [226] S. Tomasin, S. Zulian, and L. Vangelista, “Security analysis of lorawan join procedure for internet of things networks,” in *2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, pp. 1–6, IEEE, 2017.

Bibliography

- [227] H. Noura, T. Hatoun, O. Salman, J.-P. Yaacoub, and A. Chehab, “Lorawan security survey: Issues, threats and possible mitigation techniques,” *Internet of Things*, p. 100303, 2020.
- [228] M. Eldefrawy, I. Butun, N. Pereira, and M. Gidlund, “Formal security analysis of lorawan,” *Computer Networks*, vol. 148, pp. 328–339, 2019.
- [229] Ericsson, “Ericsson mobility report november 2019.” <https://d110erj175o600.cloudfront.net/wp-content/uploads/2019/11/report.pdf>, 09 2019. (Accessed on 09/17/2021).
- [230] M. Rinne and O. Tirkkonen, “Lte, the radio technology path towards 4g,” *Computer Communications*, vol. 33, no. 16, pp. 1894–1906, 2010.
- [231] D. H. Zarrinkoub, *Understanding LTE with MATLAB®: From Mathematical Modeling to Simulation and Prototyping*, vol. 9781118443415. Chichester, UK: John Wiley & Sons, Ltd, 2014.
- [232] 3GPP, “Evolved universal terrestrial radio access (e-utra); physical channels and modulation (3gpp ts 36.211 version 15.2.0 release 15).” https://www.etsi.org/deliver/etsi_ts/136200_136299/136211/15.02.00_60/ts_136211v150200p.pdf, 10 2018. (Accessed on 11/26/2021).
- [233] 3GPP, “Third generation partnership project, technical specification 36.211, v15.5.0. evolved universal terrestrial radio access (e-utra); physical channels and modulation.” https://www.arib.or.jp/english/html/overview/doc/STD-T104v4_10/5_Appendix/Rel13/36/36211-d20.pdf, 06 2016. (Accessed on 05/20/2021).
- [234] S. Ahmadi, *LTE-Advanced: a practical systems approach to understanding 3GPP LTE releases 10 and 11 radio access technologies*. Academic Press, 2013.
- [235] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, “Massive mimo for next generation wireless systems,” *IEEE communications magazine*, vol. 52, no. 2, pp. 186–195, 2014.

Bibliography

- [236] 3GPP, “Lte.” <https://www.3gpp.org/technologies/keywords-acronyms/98-lte>. (Accessed on 08/05/2021).
- [237] J. Schlien and D. Raddino, “Narrowband internet of things whitepaper,” *White Paper, Rohde&Schwarz*, pp. 1–42, 2016.
- [238] 3GPP, “Standardization of nb-iot completed.” <https://www.3gpp.org/news-events/1785-nbiotcomplete>, 06 2016. (Accessed on 11/16/2021).
- [239] GSMA, “Mobile iot lpwa - lte-m and nb-iot commercial launches.” <https://www.gsma.com/iot/mobile-iot-commercial-launches/>, 02 2021. (Accessed on 02/14/2021).
- [240] GSA, “Nb-iot & lte-m december 2020: Member report.” <https://gsacom.com/paper/nb-iot-lte-m-december-2020/>, 12 2020. (Accessed on 11/16/2021).
- [241] A. D. Zayas and P. Merino, “The 3gpp nb-iot system architecture for the internet of things,” in *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 277–282, IEEE, 2017.
- [242] X. Lin, A. Adhikary, and Y.-P. E. Wang, “Random access preamble design and detection for 3gpp narrowband iot systems,” *IEEE Wireless Communications Letters*, vol. 5, no. 6, pp. 640–643, 2016.
- [243] M. Chen, Y. Miao, Y. Hao, and K. Hwang, “Narrow band internet of things,” *IEEE access*, vol. 5, pp. 20557–20577, 2017.
- [244] H. Malik, H. Pervaiz, M. M. Alam, Y. Le Moullec, A. Kuusik, and M. A. Imran, “Radio resource management scheme in nb-iot systems,” *IEEE Access*, vol. 6, pp. 15051–15064, 2018.
- [245] N. Mangalvedhe, R. Ratasuk, and A. Ghosh, “Nb-iot deployment study for low power wide area cellular iot,” in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–6, 2016.

Bibliography

- [246] R. Sun, S. Talarico, W. Chang, H. Niu, and H. Yang, “Enabling nb-iot on unlicensed spectrum,” in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1–7, 2019.
- [247] X. An, F. Pianese, I. Widjaja, and U. G. Acer, “dmme: Virtualizing lte mobility management,” in *2011 IEEE 36th Conference on Local Computer Networks*, pp. 528–536, IEEE, 2011.
- [248] K. K. Nair, A. M. Abu-Mahfouz, and S. Lefophane, “Analysis of the narrow band internet of things (nb-iot) technology,” in *2019 Conference on Information Communications Technology and Society (ICTAS)*, pp. 1–6, IEEE, 2019.
- [249] 3GPP, “3gpp release 16.” <https://www.3gpp.org/release-16>, 2020. Last accessed 01 April 2020.
- [250] C. Hoymann, D. Astely, M. Stattin, G. Wikstrom, J.-F. Cheng, A. Hoglund, M. Frenne, R. Blasco, J. Huschke, and F. Gunnarsson, “Lte release 14 outlook,” *IEEE Communications Magazine*, vol. 54, no. 6, pp. 44–49, 2016.
- [251] G. Tsoukaneri, M. Condoluci, T. Mahmoodi, M. Dohler, and M. K. Marina, “Group communications in narrowband-iot: Architecture, procedures, and evaluation,” *IEEE Internet of things Journal*, vol. 5, no. 3, pp. 1539–1549, 2018.
- [252] K. Radnosrati, G. Hendeby, C. Fritsche, F. Gunnarsson, and F. Gustafsson, “Performance of otdoa positioning in narrowband iot systems,” in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–7, IEEE, 2017.
- [253] A. Hoglund, D. P. Van, T. Tirronen, O. Liberg, Y. Sui, and E. A. Yavuz, “3gpp release 15 early data transmission,” *IEEE Communications Standards Magazine*, vol. 2, no. 2, pp. 90–96, 2018.
- [254] 3GPP, “Release 16.” <https://www.3gpp.org/release-16>, Jun 2019. (Accessed on 05/12/2021).

Bibliography

- [255] Ericsson, “3gpp releases 16 & 17 overview – 5g nr evolution.” <https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-nr-evolution>, 03 2020. (Accessed on 12/20/2021).
- [256] S. Sibiya and O. O. Olugbara, “Reliable internet of things network architecture based on high altitude platforms,” in *2019 Conference on Information Communications Technology and Society (ICTAS)*, pp. 1–4, 2019.
- [257] D. C. Sicker, “Policy and regulatory issues,” *IEEE Internet of Things Magazine*, vol. 2, no. 3, pp. 2–3, 2019.
- [258] M. Martonosi, “Keynotes: Internet of things: History and hype, technology and policy,” in *2016 49th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, pp. 1–2, 2016.
- [259] T. Winchcomb, S. Massey, and P. Beastall, “Review of the latest development in the internet of things,” *Cambridge Consultants, Ofcom contract number 1636 (MC370)*, 2017.
- [260] J. Navarro-Ortiz, S. Sendra, P. Ameigeiras, and J. M. Lopez-Soler, “Integration of lorawan and 4g/5g for the industrial internet of things,” *IEEE Communications Magazine*, vol. 56, no. 2, pp. 60–67, 2018.
- [261] Y. Wang, X. Lin, A. Adhikary, A. Grovlen, Y. Sui, Y. Blankenship, J. Bergman, and H. S. Razaghi, “A primer on 3gpp narrowband internet of things,” *IEEE Communications Magazine*, vol. 55, no. 3, pp. 117–123, 2017.
- [262] L. Alliance, “Lora alliance™ bringing lorawan® live! to berlin; biggest lorawan event of the year will showcase value of lorawan deployments and certification.” <https://www.globenewswire.com/news-release/2019/05/02/1815427/0/en/LoRa-Alliance-Bringing-LoRaWAN-Live-to-Berlin-Biggest-LoRaWAN-Event-of-the-Year-will-Showcase-Value-of-LoRaWAN-Deployments-and-Certification.html>, 5 2019. (Accessed on 03/31/2020).

Bibliography

- [263] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovacs, P. Mogensen, and M. Sorensen, “Coverage and capacity analysis of sigfox, lora, gprs, and nb-iot,” in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, pp. 1–5, 2017.
- [264] M. Lauridsen, H. Nguyen, B. Vejlgaard, I. Z. Kovacs, P. Mogensen, and M. Sorensen, “Coverage comparison of gprs, nb-iot, lora, and sigfox in a 7800 km² area,” in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, pp. 1–5, 2017.
- [265] A. Gilchrist, *Industry 4.0: the industrial internet of things*. Springer, 2016.
- [266] J. L. R. Sarmiento, *Interference Management in NB-IoT for Heterogeneous Wireless Network*. PhD thesis, Tallinn University of Technology, 2019.
- [267] E. Shin and G. Jo, “Structure of nb-iot nodeb system,” in *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 1269–1271, 2017.
- [268] R. Sun, W. Chang, S. Talarico, H. Niu, and H. Yang, “Design and performance of unlicensed nb-iot,” in *2019 16th International Symposium on Wireless Communication Systems (ISWCS)*, pp. 469–473, 2019.
- [269] Ofcom, “Connected nations 2019 - uk report.” https://www.ofcom.org.uk/_data/assets/pdf_file/0023/186413/Connected-Nations-2019-UK-final.pdf, 2020. Last accessed 02 April 2020.
- [270] S. Ha, H. Seo, Y. Moon, D. Lee, and J. Jeong, “A novel solution for nb-iot cell coverage expansion,” in *2018 Global Internet of Things Summit (GloTS)*, pp. 1–5, 2018.
- [271] J. Oh and H. Song, “Study on the effect of lte on the coexistence of nb-iot,” in *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 610–612, 2018.

Bibliography

- [272] Y. Miao, W. Li, D. Tian, M. S. Hossain, and M. F. Alhamid, “Narrowband internet of things: Simulation and modeling,” *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2304–2314, 2018.
- [273] V. Nair, R. Litjens, and H. Zhang, “Assessment of the suitability of nb-iot technology for orm in smart grids,” in *2018 European Conference on Networks and Communications (EuCNC)*, pp. 418–423, 2018.
- [274] R. Ratasuk, N. Mangalvedhe, Y. Zhang, M. Robert, and J. Koskinen, “Overview of narrowband iot in lte rel-13,” in *2016 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 1–7, 2016.
- [275] GSMA, “Mobile iot network launches.” <https://www.gsma.com/iot/mobile-iot-commercial-launches/>, 2020. Last accessed 31 January 2020.
- [276] A. López-Vargas, M. Fuentes, and M. Vivar, “Challenges and opportunities of the internet of things for global development to achieve the united nations sustainable development goals,” *IEEE Access*, vol. 8, pp. 37202–37213, 2020.
- [277] M. Ballerini, T. Polonelli, D. Brunelli, M. Magno, and L. Benini, “Experimental evaluation on nb-iot and lorawan for industrial and iot applications,” in *2019 IEEE 17th International Conference on Industrial Informatics (INDIN)*, vol. 1, pp. 1729–1732, IEEE, 2019.
- [278] S. Ugwuanyi and J. Irvine, “Security analysis of iot networks and platforms,” in *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–6, IEEE, 2020.
- [279] S. Ugwuanyi, J. Hansawangkit, and J. Irvine, “Nb-iot testbed for industrial internet of things,” in *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–6, IEEE, 2020.
- [280] X. Zhang, M. Zhang, F. Meng, Y. Qiao, S. Xu, and S. Hour, “A low-power wide-area network information monitoring system by combining nb-iot and lora,” *IEEE Internet of things Journal*, vol. 6, no. 1, pp. 590–598, 2018.

Bibliography

- [281] A. Prasad, K. A. Mamun, F. Islam, and H. Haqva, "Smart water quality monitoring system," in *2015 2nd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE)*, pp. 1–6, IEEE, 2015.
- [282] N. Wu and M. Khan, "Lora-based internet-of-things: A water quality monitoring system," in *2019 SoutheastCon*, pp. 1–4, IEEE, 2019.
- [283] O. Khutsoane, B. Isong, N. Gasela, and M. Abu-Mahfouz, "Watergrid-sense: A lora-based sensor node for industrial iot applications," *IEEE Sensors Journal*, vol. 20, no. 5, pp. 2722–2729, 2019.
- [284] Y.-T. Liu, B.-Y. Lin, X.-F. Yue, Z.-X. Cai, Z.-X. Yang, W.-H. Liu, S.-Y. Huang, J.-L. Lu, J.-W. Peng, and J.-Y. Chen, "A solar powered long range real-time water quality monitoring system by lorawan," in *2018 27th Wireless and Optical Communication Conference (WOCC)*, pp. 1–2, IEEE, 2018.
- [285] I. S. Laktionov, O. V. Vovna, M. M. Kabanets, I. A. Getman, and O. V. Zolotarova, "Computer-integrated device for acidity measurement monitoring in greenhouse conditions with compensation of destabilizing factors.," *Instrumentation, Mesures, Métrologies*, vol. 19, no. 4, 2020.
- [286] Y.-B. Lin and H.-C. Tseng, "Fishtalk: An iot-based mini aquarium system," *IEEE Access*, vol. 7, pp. 35457–35469, 2019.
- [287] V. Petrov, A. Samuylov, V. Begishev, D. Moltchanov, S. Andreev, K. Samouylov, and Y. Koucheryavy, "Vehicle-based relay assistance for opportunistic crowdsensing over narrowband iot (nb-iot)," *IEEE Internet of Things journal*, vol. 5, no. 5, pp. 3710–3723, 2017.
- [288] M. Ballerini, T. Polonelli, D. Brunelli, M. Magno, and L. Benini, "Nb-iot versus lorawan: An experimental evaluation for industrial applications," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 12, pp. 7802–7811, 2020.
- [289] K. Mikhaylov, M. Stusek, P. Masek, V. Petrov, J. Petajajarvi, S. Andreev, J. Pokorny, J. Hosek, A. Pouttu, and Y. Koucheryavy, "Multi-rat lpwan in smart

Bibliography

- cities: Trial of lorawan and nb-iot integration,” in *2018 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2018.
- [290] A. Lombardo, S. Parrino, G. Peruzzi, and A. Pozzebon, “Lorawan vs nb-iot: Transmission performance analysis within critical environments,” *IEEE Internet of Things Journal*, 2021.
- [291] C. Houston, S. Gooberman-Hill, R. Mathie, A. Kennedy, Y. Li, and P. Baiz, “Case study for the return on investment of internet of things using agent-based modelling and data science,” *Systems*, vol. 5, no. 1, p. 4, 2017.
- [292] C. Sun, “Research on investment decision-making model from the perspective of “internet of things+ big data”,,” *Future Generation Computer Systems*, vol. 107, pp. 286–292, 2020.
- [293] D. Moore, “Lorawan will co-exist with the 5g ecosystem as a de facto unlicensed lpwan standard.” <https://www.fiercewireless.com/sponsored/lorawan-will-co-exist-5g-ecosystem-as-a-de-facto-unlicensed-lpwan-standard>, Oct 2019. (Accessed on 05/12/2021).
- [294] Z. Ali, H. Yasir, H. Marie, and K. Christian, “Cellular iot evolution for industry digitalization.” <https://www.ericsson.com/en/reports-and-papers/white-papers/cellular-iot-evolution-for-industry-digitalization>, 01 2019. (Accessed on 06/14/2021).
- [295] L. Wan, Z. Guo, Y. Wu, W. Bi, J. Yuan, M. Elkashlan, and L. Hanzo, “4g5g spectrum sharing: Efficient 5g deployment to serve enhanced mobile broadband and internet of things applications,” *IEEE Vehicular Technology Magazine*, vol. 13, no. 4, pp. 28–39, 2018.
- [296] H. Mazar, *Radio spectrum Management: Policies, regulations and techniques*. John Wiley & Sons, 2016.
- [297] A. Ahuja, U. Upadhyay, H. Manocha, and B. Singh, “Analysis of nb-iot deployment, obstacles and opportunities for indian telecommunication operators,” in

Bibliography

- 2019 International Conference on Power Electronics, Control and Automation (ICPECA)*, pp. 1–6, IEEE, 2019.
- [298] NCC, “Frequency assignment tables.” <https://www.ncc.gov.ng/technical-regulation/spectrum/frequency-assignments>, Dec 2020. (Accessed on 05/12/2021).
- [299] DCMS, “Code of practice for consumer iot security.” <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security>, Oct 2020. (Accessed on 05/12/2021).
- [300] FAA, “Unmanned aircraft systems (uas).” <https://www.faa.gov/uas/>, Jan 2021. (Accessed on 05/12/2021).
- [301] S. Fischer, K. Neubauer, and R. Hackenberg, “A study about the different categories of iot in scientific publications,” *CLOUD COMPUTING 2020*, p. 24, 2020.
- [302] GSMA, “Iot knowledgebase for policy and regulation.” <https://www.gsma.com/iot/knowledgebase/>. (Accessed on 05/12/2021).
- [303] NCC, “Spectrum administration department service charter.” <https://www.ncc.gov.ng/servicom-dept-charters/137-spectrum-administration-department-service-charter>. (Accessed on 05/12/2021).
- [304] Ofcom, “Award of 700 mhz and 3.6-3.8 ghz spectrum by auction.” <https://www.ofcom.org.uk/spectrum/spectrum-management/spectrum-awards/awards-in-progress/700-mhz-and-3.6-3.8-ghz-auction>, May 2021. (Accessed on 05/12/2021).
- [305] J. M. Peha, “Spectrum sharing in the gray space,” *Telecommunications Policy*, vol. 37, no. 2-3, pp. 167–177, 2013.

Bibliography

- [306] R. Hislop, “Ideas for solving rural south african internet connection - ee publishers.” <https://www.ee.co.za/article/ideas-for-solving-rural-south-african-internet-connection.html>, Sept 2018. (Accessed on 05/12/2021).
- [307] M. S. Turan, “Lightweight crypto, heavyweight protection.” <https://www.nist.gov/blogs/taking-measure/lightweight-crypto-heavyweight-protection>, 01 2021. (Accessed on 06/23/2021).
- [308] I. . Nendica, “Ieee 802 nendica report: Flexible factory iot: Use cases and communication requirements for wired and wireless bridged networks,” pp. 1–48, April 2020.
- [309] A. K. Sultania, F. Mahfoudhi, and J. Famaey, “Real-time demand response using nb-iot,” *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11863–11872, 2020.
- [310] L. Feltrin, G. Tsoukaneri, M. Condoluci, C. Buratti, T. Mahmoodi, M. Dohler, and R. Verdone, “Narrowband iot: A survey on downlink and uplink perspectives,” *IEEE Wireless Communications*, vol. 26, no. 1, pp. 78–86, 2019.
- [311] GSMA, “Extended coverage - gsm - internet of things (ec-gsm-iot).” <https://www.gsma.com/iot/extended-coverage-gsm-internet-of-things-ec-gsm-iot/>. (Accessed on 05/12/2021).
- [312] NCC, “Industry statistics - percentage market share by technology.” <https://ncc.gov.ng/statistics-reports/industry-overview>. (Accessed on 05/12/2021).
- [313] ETSI, “Ts 138 104 - v15.3.0 - 5g; nr; base station (bs) radio transmission and reception (3gpp ts 38.104 version 15.3.0 release 15).” https://www.etsi.org/deliver/etsi_ts/138100_138199/138104/15.03.00_60/ts_138104v150300p.pdf, Oct 2018. (Accessed on 05/12/2021).

Bibliography

- [314] W. Choi, Y.-S. Chang, Y. Jung, and J. Song, “Low-power lora signal-based outdoor positioning using fingerprint algorithm,” *ISPRS International Journal of Geo-Information*, vol. 7, no. 11, p. 440, 2018.
- [315] Ó. Alvear, J. Herrera-Tapia, C. T. Calafate, E. Hernández-Orallo, J.-C. Cano, and P. Manzoni, “Assessing the impact of mobility on lora communications,” in *Interoperability, Safety and Security in IoT*, pp. 75–81, Springer, 2017.
- [316] Ericsson, “Ericsson mobility report - november 2020 - ericsson.” <https://www.ericsson.com/en/mobility-report/reports/november-2020>, Nov 2020. (Accessed on 05/12/2021).
- [317] 3GPP, “Interim conclusions on iot for rel-16.” <https://portal.3gpp.org/ngppapp/TdocList.aspx?meetingId=18659>, Mar 2018. (Accessed on 05/12/2021).
- [318] ITU-T, “Focus group on technologies for network 2030.” <https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx>. (Accessed on 05/12/2021).
- [319] Samsung, “Next generation communications.” <https://research.samsung.com/next-generation-communications>. (Accessed on 12/23/2021).
- [320] D. Li, “Huawei started research on 6g network.” <https://www.huaweicentral.com/huawei-started-research-on-6g-network/>, 08 2019. (Accessed on 12/23/2021).
- [321] C. Mu-Hyun, “Lg sets up 6g research centre at kaist.” <https://www.zdnet.com/article/lg-sets-up-6g-research-centre-at-kaist/>, 01 2019. (Accessed on 12/23/2021).
- [322] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, “The road towards 6g: A comprehensive survey,” *arXiv preprint arXiv:2102.01420*, 2021.
- [323] O. Liberg, *Cellular Internet of things : technologies, standards, and performance / [internet resource]*. 2018.

Bibliography

- [324] P. M. Afif Osseiran, Jose F. Monserrat, “5g mobile and wireless communications technology.” <https://b-ok.org/book/2928839/d6147d>, 2016. Last accessed 17 April 2020.
- [325] L. Chettri and R. Bera, “A comprehensive survey on internet of things (iot) toward 5g wireless systems,” *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16–32, 2020.
- [326] R. Sun, W. Chang, S. Talarico, H. Niu, and H. Yang, “Design and performance of unlicensed nb-iot,” in *2019 16th International Symposium on Wireless Communication Systems (ISWCS)*, pp. 469–473, IEEE, 2019.
- [327] R. Sun, S. Talarico, W. Chang, H. Niu, and H. Yang, “Enabling nb-iot on unlicensed spectrum,” in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1–7, IEEE, 2019.
- [328] W. B. Alliance, “Wi-fi & lorawan trials - wireless broadband alliance.” <https://wballiance.com/wi-fi-lorawan-trials-an-overview-of-use-cases-across-regions-combining-two-pow> (Accessed on 05/12/2021).
- [329] 3GPP, “Cellular system support for ultra-low complexity and low throughput internet of things (ciot).” <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2719>, Aug 2016. (Accessed on 05/12/2021).
- [330] R. Ratasuk, N. Mangalvedhe, J. Kaikkonen, and M. Robert, “Data channel design and performance for lte narrowband iot,” in *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, pp. 1–5, IEEE, 2016.
- [331] M. Dangana, S. Ansari, Q. H. Abbasi, S. Hussain, and M. A. Imran, “Suitability of nb-iot for indoor industrial environment: A survey and insights,” *Sensors*, vol. 21, no. 16, p. 5284, 2021.

Bibliography

- [332] J. G. Wright and S. D. Wolthusen, “Limitations of iec62351-3’s public key management,” in *2016 IEEE 24th International Conference on Network Protocols (ICNP)*, pp. 1–6, IEEE, 2016.
- [333] F. G. Bîrleanu, P. Anghelescu, N. Bizon, and E. Pricop, “Cyber security objectives and requirements for smart grid,” in *Smart Grids and Their Communication Systems*, pp. 607–634, Springer, 2019.
- [334] K. McLaughlin, I. Friedberg, B. Kang, P. Maynard, S. Sezer, and G. McWilliams, “Secure communications in smart grid: Networking and protocols,” in *Smart Grid Security*, pp. 113–148, Elsevier, 2015.
- [335] G. Research, “Trends in utility smart grid communications management.” <https://www.ericsson.com/assets/local/news/latin-america/2016/docs/3/trends-in-utility-smart-grid-communications-management.pdf>, 2013.
- [336] Ofcom, “Broadband and mobile coverage checker.” <https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/advice/ofcom-checker>, 2020.
- [337] X. Ding, J. Wu, Y. Zheng, M. Liu, W. Zhou, and D. Nan, “Research on retrofitting scheme of merging unit and intelligent terminal in 500kv smart substation,” in *2019 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia)*, pp. 2079–2083, IEEE, 2019.
- [338] K. Ghanem, F. Coffele, and J. Irvine, “The reliability and optimal data usage of bgan satellite communications for remote outstations,” in *2018 International Conference on Smart Communications and Networking (SmartNets)*, pp. 1–5, IEEE, 2018.
- [339] N. Directive, “Directive (eu) 2016/1148 of the european parliament and of the council of 6 july 2016 concerning measures for a high common level of security of network and information systems across the union,” *OJ L*, vol. 194, no. 19.7, p. 2016, 2016.

Bibliography

- [340] R. Mattioli and K. Moulinos, “Communication network interdependencies in smart grids - annexes.” <https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/communication-network-interdependencies-in-smart-grids-annexes>, 2015.
- [341] ENA, “Engineering recommendation g91 issue 1 2012 substation back start resilience.” <https://www.spenergynetworks.co.uk/userfiles/file/App8-2012-ENA-EngRecommendG91BlackStartRes.pdf>, 2012.
- [342] ENA and DBEIS, “Energy delivery systems – cyber security procurement guidance.” <https://www.energynetworks.org/electricity/engineering/cyber-security-procurement-language-guidance.html>, 2016.
- [343] T. Tjelta, S. Temple, and R. W. Mohr, “Euro-5g-supporting the european 5g initiative,” *EURO-5G Consortium Parties: Heidelberg, Germany*, 2015.
- [344] Ofcom, “Statement: Review of spectrum used by fixed wireless services.” <https://www.ofcom.org.uk/data/assets/pdf/0017/115631/statement-fixed-wireless-spectrum-strategy.pdf>, 2018.
- [345] DotEcon and A. M. Group, “Report for ofcom on allocation options for selected bands.” <http://www.dotecon.com/assets/images/selectedbands.pdf>, 02 2005. (Accessed on 07/24/2021).
- [346] K. Ghanem, I. Abdulhadi, A. Kazerooni, and C. McGookin, “Communication requirements for future secondary substations to enable dso functions,” in *CIREN Workshop 2020*, 2020.
- [347] NCSC, “Ncsc cyber assessment framework (caf) guidance.” <https://www.ncsc.gov.uk/collection/caf>, 09 2019. (Accessed on 06/22/2021).
- [348] Ofcom, “Strategic review of uhf spectrum at 420-470 mhz uhf bands 1 and 2.” https://www.ofcom.org.uk/__data/assets/pdf_file/0020/47414/420-470-mhz.pdf, 12 2014. (Accessed on 07/29/2021).

Bibliography

- [349] Frost and Sullivan, “Private lte for the smart grid.” https://www-file.huawei.com/-/media/CORPORATE/PDF/white%20paper/wp_hw_smart_grid_cam.pdf?la=en, 2017. (Accessed on 07/29/2021).
- [350] Ofcom, “View mobile availability - ofcom checker.” <https://checker.ofcom.org.uk/en-gb/mobile-coverage>. (Accessed on 07/30/2021).
- [351] nPerf, “3g / 4g / 5g coverage map, nigeria.” <https://www.nperf.com/en/map/NG/-/169661.MTN-Mobile/signal/?ll=2.818686797111579&lg=9.04540926218033&zoom=6>. (Accessed on 08/05/2021).
- [352] H. Michael, N. Damir, and C. Mariesa, “[pdf] electric power grid modernization trends, challenges, and opportunities.” <https://www.cmu.edu/epp/irle/readings/henderson-novosel-crow-electric-power-grid-modernization.pdf>, 11 2017. (Accessed on 06/23/2021).
- [353] P. Carlos, H. Maarten, T. Fook, and S. Han, “Implementing an isa/iec-62443 and iso/iec-27001 ot cyber security management system at dutch dso enexis.” <https://www.cired-repository.org/handle/20.500.12455/404?show=full>, 06 2019. (Accessed on 06/23/2021).
- [354] N. R. Indukuri, “Layer 2 security for smart grid networks,” in *2012 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 99–104, IEEE, 2012.
- [355] NCSC, “Virtual private networks (vpns).” <https://www.ncsc.gov.uk/collection/mobile-device-guidance/virtual-private-networks>, 01 2020. (Accessed on 03/15/2021).
- [356] NCSC, “Using tls to protect data.” <https://www.ncsc.gov.uk/guidance/tls-external-facing-services>, 12 2017. (Accessed on 03/15/2021).
- [357] NCSC, “Using ipsec to protect data.” <https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data>, 09 2016. (Accessed on 03/15/2021).

Bibliography

- [358] ETSI, “Ts 136 213 - v12.3.0 - lte; evolved universal terrestrial radio access (e-utra); physical layer procedures (3gpp ts 36.213 version 12.3.0 release 12).” https://www.etsi.org/deliver/etsi_ts/136200_136299/136213/12.03.00_60/ts_136213v120300p.pdf, 10 2014. (Accessed on 08/06/2021).
- [359] R. de Janeiro, “Ieee summit - nokia.” <https://tinyurl.com/yyt3xh9h>, 11 2018. (Accessed on 08/06/2021).
- [360] R. Wireless, “Microsoft word - final report v1.4 - appendices v1.4.docx.” https://www.ofcom.org.uk/__data/assets/pdf_file/0038/74999/4gcapacitygainsfinalreporta1.pdf, 01 2011. (Accessed on 08/06/2021).
- [361] K. Ghanem, U. Stephen, A. Rameez, and J. Irvine, “Challenges and promises of 5g for smart grid teleprotection applications,” in *2021 International Symposium on Networks, Computers and Communications (ISNCC): Trust, Security and Privacy*, IEEE, 2021.
- [362] H. Lecht, “The state of roaming: Narrowband iot & lte cat m1 — 1ot - global cellular connectivity for iot.” <https://1ot.mobi/resources/blog/the-state-of-roaming-narrowband-iot-lte-cat-m1>, 08 2018. (Accessed on 08/19/2021).
- [363] H. Kim, S. C. Cho, Y. Lee, and J. Shin, “Performance analysis of nb-iot system according to operation mode,” in *2019 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 876–878, IEEE, 2019.
- [364] S. Ugwuanyi, R. Asif, and J. Irvine, “Network virtualization: proof of concept for remote management of multi-tenant infrastructure,” in *2020 IEEE 6th International Conference on Dependability in Sensor, Cloud and Big Data Systems and Application (DependSys)*, pp. 98–105, IEEE, 2020.