CORA Cork Open Research Archive
Cartlann Taighde Oscailte Chorcaí

Title	Enhancing the efficiency and security of NB-IoT: from battery depletion to energy optimization
Authors	Ionescu, Vlad
Publication date	2025
Original Citation	Ionescu, V. R. 2025. Enhancing the efficiency and security of NB-IoT: from battery depletion to energy optimization. PhD Thesis, University College Cork.
Type of publication	Doctoral thesis
Rights	© 2025, Vlad Radu Ionescu. - https://creativecommons.org/licenses/by-nc/4.0/
Download date	2026-11-07 11:29:32
Item downloaded from	https://hdl.handle.net/10468/18403



UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Ollscoil na hÉireann, Corcaigh

National University of Ireland, Cork



Enhancing the Efficiency and Security of NB-IoT: From Battery Depletion to Energy Optimization

THESIS PRESENTED BY

Vlad Radu Ionescu

FOR THE DEGREE OF

Doctor in Philosophy

University College Cork

School of Computer Science and Information Technology

Head of Department: Professor Dirk Pesch

Supervisor: Professor Utz Roedig, Professor Dirk Pesch

2025

Contents

List of Figures iii

List of Tables vii

Abstract viii

1 Introduction 1

1.1 Motivation . . . 1
1.2 Contributions . . . 6
1.3 Publications . . . 8
1.4 Thesis Structure . . . 9

2 Background and Related Work 10

2.1 Low Power Wide Area Network and Narrowband Internet of Things . . . 10
2.1.1 Introduction to LPWAN . . . 10
2.1.2 LPWAN Technologies . . . 12
2.1.3 Narrowband Internet of Things . . . 15
2.2 NB-IoT Communication . . . 17
2.2.1 Synchronisation and System Information Acquisition . . . 19
2.2.2 Narrowband Physical Random Access Channel . . . 25
2.2.3 Narrowband Physical Uplink Shared Channel . . . 27
2.3 Energy Optimization in IoT . . . 31
2.3.1 Energy Optimization Techniques . . . 31
2.3.2 Energy Optimisation in LPWAN Technologies . . . 32
2.4 NB-IoT Energy Consumption and EDT Mechanisms . . . 33
2.4.1 NB-IoT Energy Consumption . . . 33
2.4.2 C-IoT-Opt and EDT Mechanism . . . 35
2.4.3 Extended Coverage Level . . . 36
2.5 Clock Drift . . . 37
2.5.1 Introduction to Clock Drift . . . 37
2.5.2 Impact of Clock Drift on IoT Devices . . . 38

2.5.3 Mitigation Strategies for Clock Drift . . . 39
2.5.4 CFO and Time Drift in NB-IoT . . . 39
2.6 Interference . . . 41
2.6.1 Overview of Interference in Wireless Networks . . . 41
2.6.2 Interference in LPWAN Technologies . . . 42
2.6.3 Interference Management in NB-IoT . . . 43
2.7 Security Concerns in IoT . . . 44
2.7.1 Overview of IoT Security Concerns . . . 44
2.7.2 Security in Large-Scale IoT Deployments . . . 46
2.7.3 IoT Cyberattacks . . . 47
2.7.4 NB-IoT Security Concerns . . . 51
2.8 Battery Depletion Attacks . . . 56
2.8.1 Existing Research on Battery Depletion Attacks . . . 56
2.8.2 Interference-Based Battery Depletion Attacks . . . 57

3 Design and Methodology **59**
3.1 Attack Techniques . . . 60
3.1.1 Simple Jamming Technique . . . 61
3.1.2 Message Jamming Technique . . . 62
3.1.3 Message Injection Technique . . . 64
3.2 Energy Depletion Attacks . . . 65
3.2.1 Degradation of Quality of Signal Attack . . . 66
3.2.2 Random Access Procedure Attack . . . 67
3.2.3 Narrowband Master Information Block Attack . . . 69
3.2.4 Narrowband System Information Block 1 Attack . . . 70
3.2.5 Narrowband System Information Block 2 Attack . . . 70
3.3 Improved Early Data Transmission (EDT+) . . . 71
3.3.1 Overview . . . 71
3.3.2 Initial Connection and Message Transmission . . . 72
3.3.3 Time Slot Allocation . . . 73
3.3.4 Data Transmission . . . 74
3.3.5 Contingency Plan and Reconnection . . . 77
3.3.6 EDT vs EDT+ Comparison . . . 78
3.3.7 EDT+ Use Cases . . . 79

4 NB-IoT Testbed and Simulation Environment **81**
4.1 Simulation of NB-IoT Systems . . . 82
4.1.1 Matlab . . . 82
4.1.2 NS3 Lena NB-IoT module . . . 85

4.1.3 srsRAN . . . 86
4.2 Testbed for NB-IoT Devices . . . 87
4.2.1 Hardware . . . 88
4.2.2 Software . . . 90
4.3 Framework for Evaluating Jamming Vulnerabilities . . . 90
4.3.1 Evaluation Scenario . . . 91
4.3.2 Evaluation Metrics . . . 91
4.3.3 Jammer . . . 93

5 Evaluation Results **95**
5.1 Battery Depletion Results . . . 95
5.1.1 Baseline . . . 95
5.1.2 Jamming Attacks in Virtual Environment . . . 96
5.1.3 Jamming Attacks in Physical Environment . . . 99
5.1.4 Evaluation Discussions . . . 101
5.2 EDT+ Impact and Evaluation . . . 103
5.2.1 EDT+ Power Profiles . . . 103
5.2.2 Impact of inactivity timer in real-world scenario . . . 107
5.2.3 EDT+ Preliminary Study . . . 109
5.2.4 Static Time Window . . . 112
5.2.5 Environmental impact on clock accuracy using EDT+ . . . 115
5.2.6 Dynamic Time window . . . 116
5.2.7 Potential security vulnerabilities of EDT+ . . . 123
5.3 Battery Depletion Attacks Mitigation . . . 124
5.3.1 Mitigating Predictability with Dynamic Scheduling . . . 125
5.3.2 The Benefits of Dynamic Transmission Scheduling . . . 125

6 Conclusion **127**
6.1 Summary of Key Findings . . . 127
6.1.1 Key Results . . . 127
6.1.2 Implications of Results . . . 128
6.2 Limitations of the Study . . . 129
6.3 Recommendations . . . 131

Acronyms **133**

List of Figures

2.1 NB-IoT deployment modes, depicting the three different types: Standalone, In-band, and Guard-band. 17
2.2 Frame structure for NB-IoT uplink with 3.75 kHz subcarrier spacing. . . . 18
2.3 Narrowband Internet of Things (NB-IoT) time domain frame structure. . 19
2.4 Subframe allocation of Narrowband Primary Synchronization Signal (NPSS) and Narrowband Secondary Synchronization Signal (NSSS) with resource allocation in a Physical Resource Block (PRB), Subframe mapping of Code Sub-Block (CSB) for Narrowband Master Information Block (MIB-NB) and Narrowband System Information Block 1 (SIB1-NB). 21
2.5 An example of resource mapping for NRS is in an NPBCH, Narrowband Physical Downlink Control Channel (NPDCCH), Narrowband Physical Downlink Shared Channel (NPDSCH), or in any valid NB-IoT downlink subframe. 22
2.6 Examples of signals and messages exchanged within a typical NB-IoT Random Access Procedure (RAP). 25
2.7 Random Access Procedure (RAP) mapped to the required data for carrying out the procedure. The data is transmitted by the Evolved Node B (eNodeB) via the Narrowband System Information Block 2 (SIB2-NB). 26
2.8 NPUSCH Format 1. 29
2.9 C-IoT-Opt transmission 35
2.10 EDT transmission 35
2.11 ECL Map. 36

3.1 Real spectrum capture of a (a) Simple Jamming technique, (b)Message Jamming (MJ) attack and (c) Message Injection (MI) attack, using the SRSRan software and the HackRF One devices. 64
3.2 Transmission of NPBCH CSBs. 69
3.3 EDT+ transmission procedure. 72
3.4 Potential allocation of EDT+ within the Uplink Schedule. 75
3.5 Decision logic for EDT+. 77

3.6 EDT vs EDT+ (stationary NB-IoT): EDT repeats RA each report; EDT+ reuses prior config to skip RA and transmit. 78

4.1 NB-IoT waveform produced by the simulation environment in Matlab. Each subframe's assigned channels and signal are shown in the upper representation. The identical signals and channels are allocated in a time-frequency domain, as seen in the lower figure. 83
4.2 NB-IoT *emulation* testbed orchestration. Software roles (top) control SDR hardware (middle) to realise the RF link (bottom). Arrows show DL/UL paths and where message injection (MI) or message jamming (MJ) acts. 88
4.3 NB-IoT testbed utilising srsRAN software: The bottom left screen displays the eNodeB base station communicating with the UE in the bottom right. A malicious device in the centre executes a message injection attack on the SIB1-NB, while the central computer screen shows a standard connection scenario. 89

5.1 Battery lifetime of an NB-IoT node in the baseline scenario using communication parameters $t = 2h$, $b_{up} = 200byte$, and $b_{down} = 60byte$ under various Maximum Coupling Loss (MCL) conditions.Baseline scenario: no bandwidth limit, perfect battery, no jamming attack. 96
5.2 Energy Depletion Rate (EDR) for the receiving (downlink) and sending (uplink) channels for various attacks (iDQS, RAP, and iDQS + RAP). Communication parameters are set to $t = 2h$, $0 < b_{up} \leq 300$ bytes, and $0 < b_{down} \leq 300$ bytes. 99
5.3 EDR (blue) and Jammer Duty Cycle (JDC) (orange) relationship, for various attack types (iDQS, RAP, and iDQS + RAP). Communication parameters are set to $t = 2h$, $0 < b_{up} \leq 300$ bytes, and $0 < b_{down} \leq 300$ bytes. 100
5.4 NS3 Power Profile Normal NB-IoT Data Transmission. 104
5.5 NS3 Power Profile EDT+ Data Transmission. 104
5.6 (a) Power Profile EDT+ Fallback Normal Transmission. (b) Power Profile EDT+ Fallback EDT Transmission. 105
5.7 Power Profile for Normal Transmission with an inactivity timer of 10 sec. 108
5.8 End-to-end latency, assuming the device has a small CFO drift for "EDT+ with MIB" and a minimum drift for "EDT+", that allows reaching its designated window. The simulation assumes that SIB1 and SIB2 have already been received in non EDT+ transmissions. 110
5.9 Ideal battery lifetime and power consumption for High-Density scenario with minimum CFO drift. Inactivity timer present. 112

5.10 Average energy used per day, factoring in the size of the uplink payload and the number of transmissions occurring daily. 113
5.11 Success Rate Variation for 100 devices across Different Periodicity, for a time window size of 3 seconds, 49 bytes, perfect environmental conditions, no clock drift variation. 114
5.12 Success Rate Variation across Different Periodicity, for incremental time window, 49 bytes, and perfect environmental conditions, 1400 transmission/periodicity. 115
5.13 Success Rate Variation across Different Periodicity, for incremental time window, 49 bytes, with temperature variation, 1400 transmission/periodicity.116
5.14 Dynamic time window for one device, 1400 transmission, with a target success rate of 85% for a periodicity of 0.5 hours. 120
5.15 Dynamic time window for one device, 1400 transmission, with a target success rate of 85% for a periodicity of one hour. 120
5.16 Dynamic time window for one device, 1400 transmission, with a target success rate of 85% for a periodicity of 24 hours. 121
5.17 Dynamic window behaviour for 2 h, 6 h, and 12 h periodicities (target success 85%). Panels arranged with 2/6 h on the top row and 12 h centred beneath. 121
5.18 Dynamic time window for 100 devices, 1400 transmission, with a target success rate of 85% for a periodicity of one hour. 122
5.19 Dynamic time window for 100 devices, 1400 transmission, with a target success rate of 85% for a periodicity of 24 hours. 123

List of Tables

2.1 Low Power Wide Area Network (LPWAN) options by spectrum, physical-layer capabilities, network model and indicative applicability. 11
2.2 Stratification of IoT deployments (Cellular IoT (CIoT), enterprise Information Technology (IT), Industrial Internet of Things (IIoT)/Operational Technology (OT), Critical National Infrastructure (CNI)) by objectives, security controls, and suitable access technologies/edge enablers. 51
2.3 Key studies on interference-based battery depletion attacks in wireless IoT networks 58

3.1 Adversary device classes considered in our evaluation 61
3.2 Energy-depletion–oriented attacks and their effect on the UE. 65
3.3 Concise summary of EDT+ data-transmission settings. 74

5.1 EDR and JDC metrics for the different attack types evaluated (sDQS, iDQS, RAP, and iDQS + RAP). 97
5.2 Evaluation of MIB-NB, SIB1-NB, and SIB2-NB based on Active Receiving Time (T_R), Delay Time (T_D), and Active Jamming/Injecting Time (T_J) . 101
5.3 Percentage of energy used for transmission and deep sleep across different periodicities for each transmission mode in a **perfect environment, no repetition, one packet, no data loss, no inactivity timer.** 106
5.4 Evaluation Scenarios Summary highlighting Data Volume for Uplink Communications, Application Type, Device Density, and Reporting Interval. . 109
5.5 Average Time Window Sizes (ms) for Different Target Success Rates. . . . 123

Declaration

This is to certify that the work I am submitting is my own and has not been submitted for another degree, either at University College Cork or elsewhere. All external references and sources are clearly acknowledged and identified within the contents. I have read and understood the regulations of University College Cork concerning plagiarism and intellectual property.

Signed: _____ Date: _____

Vlad Radu Ionescu

Abstract

This thesis focuses on the attack surface and optimisation strategies of Narrowband Internet of Things (NB-IoT), one of the most commercially successful LPWAN technologies. The rapid adoption of NB-IoT in recent years can be attributed to its key features, such as energy efficiency, low cost and the ability to support massive deployments even in challenging environments. However, the same features that make NB-IoT attractive present significant challenges, particularly in the context of energy-efficient transmissions and battery depletion attacks within the heterogeneous nature of IoT deployments.

The research highlights the security risk of NB-IoT against battery depletion attacks, exploiting the protocol energy-saving mechanism. We created several types of attacks that can exhaust the end nodes' lifespan from decades to months. These cyberattacks are designed to remain undetected as they increase energy expenditure without entirely disrupting communication. To evaluate their effectiveness, we developed simulations in both virtual and physical environments and made them publicly available for future research.

Additionally, this thesis proposes EDT+, a new NB-IoT communication mode aimed at further reducing energy consumption while increasing the network's performance. EDT+ leverages the static nature of many IoT applications, minimising the overhead associated with each transmission. During simulation EDT+ achieved an efficiency of up to 45% during transmission compared to regular communication. Furthermore, by pre-scheduling communication in a pseudo-random time slot allocation, EDT+ can mitigate the effectiveness of battery depletion attacks.

Through comprehensive simulation in virtual and physical environments, this study overcomes research challenges associated with licensed telecommunication technologies. It provides an insight into the trade-offs between energy efficiency and security in NB-IoT networks. The proposed mitigation strategies and protocol optimisation enhance the network resilience and efficiency. Overall, this research contributes to the development of sustainable IoT systems with an emphasis on use cases where lifespan and security are paramount.

Chapter 1

Introduction

1.1 Motivation

Internet of Things (IoT) represents a technological paradigm that fundamentally alters how we interact with the world around us. Connecting a vast and diverse array of devices, this technological revolution enables intelligent applications in industry sectors, including, but not limited to, smart metering, advanced agriculture, city infrastructure management, healthcare, and many others. The IoT network promises to connect devices from vehicles to home appliances, from environmental sensors to smart grid systems, all equipped with specialised hardware and software to facilitate data acquisition and communication.

By interconnecting all of these elements through the Internet, IoT completes an ecosystem where the physical world meets the digital one. This, in turn, enables a suit of improvement from operational efficiency and data accuracy to economic advantages. Existing infrastructure is leveraged to provide remote monitoring and control, fostering new perspectives in industrial optimisation, improving life quality and promoting sustainability. Furthermore, IoT encourages innovations in traditional sectors, enabling them to become dynamic and resilient in today's ever-changing economics and society.

Low Power Wide Area Network (LPWAN) is segmented into licensed and unlicensed bands, each presenting unique pros and cons. Considering unlicensed technologies such as Long Range Wide Area Network (LoRaWAN) or SigFox, their low operation cost and affordable hardware, alongside network

customisation and configuration, make it ideal for deployments in the open access spectrum. However, the nature of the unlicensed spectrum leads to increased interference from different devices, therefore having a less reliable Quality of Service (QoS) than the licence LPWAN. On top of that, security and network management challenges, such as the elevated risk of unauthorised access and the self-management requirement within the network, make the device life span prediction hard to measure. Overall, technologies like LoRaWAN have proven themselves in the innovation and experimentation space, but their downfalls have become obstacles to large deployments and scalability. On the other hand, NB-IoT, LTE-M and other licence LPWAN protocols promise to solve this issue at the expense of licensing fees, regulatory compliance and limited flexibility.

Within the LPWAN evolution, Narrowband Internet of Things (NB-IoT) stands out as a key vector in telecommunication technologies as one of the essential advancements in the licence LPWAN [1]. These telecommunication protocols are explicitly developed for IoT applications with clear objectives such as low power consumption, extended network coverage and high connection density [2]. Due to these core design principles and the capability of being deployed on existing infrastructure, NB-IoT positions itself as a forerunner in the IoT connectivity race [3].

In 2016, the 3rd Generation Partnership Project (3GPP) released a white paper entitled "3GPP Low Power Wide Area Technologies" [4]. Two years later, ThingsLog released the first NB-IoT CE-certified devices. By the end of 2023, it was estimated that 54% of all LPWAN IoT connections (licence and unlicensed) were using the NB-IoT representing more than 700 million connected devices [5]. Behind this rapid adoption rate lies the protocol's unique advantages. For example, NB-IoT inherits legacy technologies from Long-Term Evolution (LTE) and was designed to work on existing infrastructure. It can refarm 200 kHz in the Global System for Mobile Communication (GSM) spectrum as a Stand-Alone deployment and 180 kHz in 4G and 5G when deployed in Guard-band or In-band. According to Wang et al., up to 52500 devices are supported in a single cell [6] and are capable of operating at the network edge with a 20 dB MCL beyond the legacy LTE [7]. These conditions make the technology ideal for deployments in both dense city areas as well as in environments with poor network coverage. NB-IoT supports a wide spread of commercial and industrial applications

by providing a reliable solution for remote monitoring and asset management, therefore contributing to the advancement of sustainable resource utilisation. 3GPP has set a ten-year minimum device life span target for NB-IoT, which is predicted to be overpassed in specific favourable scenarios by the industries. Furthermore, high deployment density, deep indoor coverage, and re-utilisation of the existing infrastructure have set this technology to become a catalyst for innovation in the transition to an interconnected society.

All of the above sets NB-IoT to be a perfect fit within the larger IoT ecosystem, supporting applications that require long-term deployment without frequent maintenance, highlighting its relevance in the push towards sustainable and energy-efficient IoT solutions.

In the realm of technology, innovation progresses at a staggering pace. Driven by ever-growing market demands, the race to introduce new features and achieve first releases is relentless. Companies strive to out-compete each other by promising services and products that meet the needs of consumers. This competition pushes beyond the existing boundaries, creating and reshaping industries at an unprecedented pace. However, the rapid advancement tends to postpone features like security or optimisation, leaving gaps for malicious entities to exploit the new technologies. Despite increased awareness of cyber threats and the risks that come with them, the market tends to be reactive rather than proactive. Tech companies too often develop with the mindset of "if a cyber attack happens" [8] instead of "when a cyber attack will happen" [9].

Wireless communication (the predominant type of communication in IoT applications) faces multiple security challenges: its inherent characteristics —such as susceptibility to interference and signal degradation— combined with exposure to remote cyber-attacks must be managed to ensure reliable data delivery. Interference from environmental factors and other entities, malicious or not, can degrade the Quality of Service (QoS), leading to data loss or resource expenditure. Ensuring signal integrity is essential for the information to be received accurately, and most communication protocols incorporate error-checking algorithms [10]. Additionally, the wireless medium is inherently more vulnerable to cyber-attacks. Man in the Middle Attack (MITM), Eavesdropping, Denial of Service (DoS) or Spoofing are just a handful of the wide range of attacks that can be performed without

physical access to the transmitter or receiver.

NB-IoT inherits its security framework from the mature LTE/EPS architecture [11].The NB-IoT protocol embeds key aspects of EPS-AKA such as mutual authentication between devices and the network, as well as data encryption and integrity protection to guarantee a secure information exchange. Mutual authentication ensures that both the User Equipment (UE) and the network verify each other's legitimacy before transmitting the payload, mitigating against unauthorised authentication access. Confidentiality is secured by data encryption and ensures that sensitive information can not be read by malicious entities even if they are intercepted. Integrity protects the data from being tampered with during transmission. Leveraging all this and operating on a licenced spectrum, NB-IoT provides a secure communication channel suitable for various applications with sensitive information [12].

Nevertheless, novel attack approaches that aim not to access the data but instead are interested in exploiting the metadata, and the medium created by the protocol have proven difficult to counteract. Passive attacks such as localisation spoofing, radio fingerprinting, side-channel, and traffic analysis, as well as active attacks like DoS, battery depletion, and frequency hopping manipulation, are still present threats that must be addressed [13]. Although energy depletion and sleep deprivation attacks are established in low power wireless systems [14, 15, 16], and NB-IoT/LPWAN surveys cover standard vectors such as replay, jamming, synchronisation, and DoS [17, 18, 19], actual adversarial battery depletion work in NB-IoT is lacking: apart from detection-orientated studies [20, 21], only our prior work, to the best of our knowledge, constructs and evaluates concrete battery depletion attacks on NB-IoT devices [22]. Given battery longevity's critical role in this protocol, the need to understand, mitigate and prevent battery depletion attacks becomes clear. Specifically, in our work, we have shown that by using various types of attacks, such as jamming, replay, or MITM, we can perform battery drainage on User Equipment (UE). By understanding the connection procedures and the fact that most deployments are static, a bad actor can exploit some features, such as deep coverage enhancement or integrity protection, to keep the device awake and active, thus depleting its own battery. As a consequence, it undermines both the longevity of the deployments and also their reliability. UEs are expected to operate over ten years on a single

battery charge and might find them-self depleted in a matter of weeks. As a result, operational and maintenance costs are disrupted, which could render installing such devices financially impracticable compared to non IoT ones. Addressing these vulnerabilities is empirical for achieving a sustainable and robust smart ecosystem.

Energy efficiency plays a crucial role in the IoT domain, especially for devices deprived of constant power supply. Highly efficient chips paired with effective protocols have become a standard in IoT deployments. Technologies such as Bluetooth Low Energy (BLE), LoRaWAN, and NB-IoT have been designed with energy efficiency as a core feature. They can operate for a long period on battery power, reducing maintenance costs and expanding the deployment lifetime. Furthermore, this efficiency enables the utilisation of smart devices in remote and hard-to-reach locations without the need for frequent battery replacements or power supply interventions.

In the NB-IoT context, 3GPP has set a minimum lifespan target of ten years, which the industry has surpassed in favourable environments. Manufacturers such as U-blox [23] or Qualcomm [24] can achieve a lifespan of close to 20 years when the deployment is located in good signal area and has a transmission interval of 24 hours or greater. In contrast, a more aggressive interval (e.g. 1 hour) with poor coverage can yield a lifespan of just three years due to the high number of repetitions required for a successful transmission. Therefore, striking a balance between environmental conditions, device configuration, and the expected battery life is challenging but essential in ensuring robustness.

Additionally, NB-IoT inherits most of the properties from legacy LTE [25]. It is still designed with an emphasis on mobility, even though most of its deployed scenarios are static. Failing to take advantage of this factor causes additional resource expenditure in terms of energy, bandwidth, and device density. Improving the efficiency will prolong the operational life of the UE while sustaining its reliable performance. With the exponential growth of IoT devices, it will become essential to address these aspects in order to meet the demands and overcome the challenging IoT landscape.

Overall, these concerns form the core of my motivation in studying battery depletion attacks and energy efficiency as part of the NB-IoT ecosystem. By focusing on these aspects, my research seeks to fill a critical gap that will contribute towards a more resilient and efficient protocol. Gaining knowl-

edge into the mechanism of battery depletion attacks targeting NB-IoT UEs will allow future iterations to address these issues while improving the energy efficiency will support their sustainability. We believe that these research efforts will help NB-IoT to mature into a robust and viable technology for the future.

1.2 Contributions

Scientific contributions

1. *Formalisation and evaluation of NB-IoT battery-depletion attack models.* We define and analyse protocol-aware vectors—simple jamming, message jamming, and message injection—targeting broadcast/control and random-access occasions. The attacks are time-aligned to keep service up while forcing excess energy expenditure at the UE, with end-to-end evidence of feasibility and impact.

2. *New evaluation metrics for battery depletion.* We introduce Energy Depletion Rate (EDR) and Jammer Duty Cycle (JDC) to quantify, respectively, device-side energy impact and attacker effort. We demonstrate their use across coverage-enhancement levels, payload sizes, and uplink/downlink channels, enabling consistent comparison of attack strategies and severities.

3. *Quantitative characterisation of attack impacts.* We show that targeted interference degrades device lifetime by orders of magnitude under realistic MCL and payload regimes without full denial of service, highlighting repetitions and scheduling dynamics as principal levers exploited by adversaries.

4. *EDT+ design for static NB-IoT devices.* We propose a scheduled, parameter-carrying transmission mode that leverages stationarity to reduce control overhead. The design details adaptive windowing to tolerate oscillator drift while lowering energy and latency and giving the eNodeB direct control over load distribution.

5. *Analytical and simulation-backed window sizing under drift and temperature.* We develop a dynamic-window method that reaches target

success rates (e.g., 85–95%) across periodicities (0.5–24 h), quantifying the trade-offs between oscillator accuracy, window size, and cell capacity; results scale predictably with periodicity and temperature-driven drift.

6. *Security–efficiency interplay.* We hypothesise that EDT+ reduces timing predictability and thereby mitigates intelligent jamming while improving spectral and energy performance, linking an efficiency optimisation to measurable resilience under protocol-aware interference.

Engineering (artefacts and tooling) contributions

1. *MATLAB/LTE-Toolbox–based evaluation of NB-IoT under jamming.* We used off-the-shelf LTE Toolbox functions to generate NB-IoT downlink signals and measure BLER, quantifying receiver-side impact and battery-depletion effects of simple and protocol-aware jamming; results reported at ESORICS 2021 [22].

2. *srsRAN NB-IoT extensions and over-the-air testbed.* Implementation of SIB2-NB and configurations enabling experiments (with HackRF One and band-shifting to an unlicensed band) for message jamming/injection studies; code made publicly available [26] and evaluated in EWSN 2022 [27].

3. *ns-3 LENA NB-IoT scenarios for EDT+.* Simulation setups extending the LENA NB-IoT module (building on Pascal et al. [28]) to model and evaluate EDT+; used for the performance study reported at SenSys 2023 [29] and SenSys 2025 [30].

4. *Reproducible evaluation pipelines.* End-to-end scripts and scenarios used to compute and compare EDR/JDC across coverage-enhancement settings and traffic periodicities (cross-referenced in Chapters 5 and 5.2); where applicable we link to the public repository [26].

Context and impact Section 5.3 discusses how EDT+ mitigates protocol-aware interference. Additionally, in 2024, a grant was accepted to evaluate the implications of the EDT+ in the context of energy harvesting.

1.3 Publications

The subsequent publications are the results of the research conducted in this thesis:

P1 - Vlad Ionescu and Utz Roedig: "Battery Depletion Attacks on NB-IoT Devices Using Interference," in Computer Security, ESORICS 2021 International Workshops, Lecture Notes in Computer Science, vol. 13106, Cham: Springer International Publishing, 2022, held in Darmstadt, Germany. https://doi.org/10.1007/978-3-030-95484-0_17.

P2 - Vlad Ionescu and Utz Roedig: "NB-IoT Battery Depletion via Malicious Interference," in Proceedings of the 2022 International Conference on Embedded Wireless Systems and Networks, held in Linz, Austria. https://doi.org/10.1007/978-3-030-95484-0_17.

P3 - Vlad Ionescu, Ian Wassel, and Utz Roedig: "EDT+: Energy Consumption Optimization of NB-IoT," in Proceedings of the 11th International Workshop on Energy Harvesting & Energy-Neutral Sensing Systems, Istanbul, Turkey, November 2023. https://doi.org/10.1145/3628353.3628548.

P4 - Vlad Ionescu and Utz Roedig: "Reception Window Selection in EDT+ for Energy Efficient NB-IoT" Association for Computing Machinery, IRVINE CA, USA, 2025. https://doi.org/10.1145/3722572.3727927.

1.4 Thesis Structure

This thesis is structured into several chapters, each delving into different aspects of enhancing the security and efficiency of NB-IoT networks. It follows a clear and logical flow, starting with the introduction and ending with the final recommendations. The following represents a brief overview of each chapter:

Chapter 1: Introduction - Outlines the motivation behind the work, states the contributions at a high level, and summarises the overall structure of the thesis.

Chapter 2: Background and Related Work - Consolidates all related background. It first places NB-IoT within the broader LPWAN landscape, then details the NB-IoT communication procedures. It continues with energy consumption in LPWAN and the mechanisms relevant to Early Data Transmission (EDT), followed by clock drift, interference, IoT security, and a focused review of battery depletion attacks.

Chapter 3: Design and Methodology - Presents the design rationale and methodology for the attack models and EDT+. It formalises the adversary models and attack timing, and details the EDT+ communication design tailored to static NB-IoT devices, including scheduling and drift-tolerant operation.

Chapter 4: Implementation and Evaluation Setup - Describes the simulation environments and testbed used to study the system. It outlines the simulation environment, the physical testbed setup, and the evaluation metrics and scenarios used throughout the study.

Chapter 5: Results and Discussion - Analyses and discusses the results. It first reports the outcomes for battery depletion attacks, then evaluates EDT+ (latency, energy, and capacity) and discusses mitigation and security implications.

Chapter 6: Conclusions - Summarises the key findings and their implications. It also presents limitations of the study and recommendations.

Each chapter builds upon the information and insights presented in the preceding ones, culminating in a comprehensive examination of the challenges and solutions in securing and optimising NB-IoT devices.

Chapter 2

Background and Related Work

2.1 Low Power Wide Area Network and Narrowband Internet of Things

2.1.1 Introduction to LPWAN

Low Power Wide Area Networks (LPWANs) have become a pivotal technology in the IoT landscape. They offer long-range connectivity while minimising the power consumption and cost. LPWAN capabilities address the inherent limitations found in traditional cellular and short-range wireless networks, making LPWAN an ideal solution for various IoT applications [31]. Table 2.1 provides a compact, like-for-like snapshot of the principal LPWAN families, contrasting spectrum usage, physical layer/rates, network model, and typical applicability.

To achieve extended coverage and low energy consumption, LPWAN employs unique methodologies. It can operate on licensed and unlicensed frequency bands and strives to simplify the deployment process while reducing expenses. The prominent technologies for unlicensed spectrum are LoRa and Sigfox, while for the licensed, the forerunners are Narrowband Internet of Things (NB-IoT) and LTE-M.

LoRa, short for (Long Range), utilises a proprietary variant of chirp spread spectrum (CSS) modulation developed by Semtech to provide long-range connectivity with low power usage. Its deployment on the unlicensed

Tech.	Spectrum	PHY / Rate	Network model	Typical uses
LoRa	Unlicensed ISM	CSS; SF7–12; BW 125/250/500 kHz; ∼0.3–50 kbps; ADR optional	Public or private LoRaWAN (star via gateways)	Metering; asset tracking; smart city; agri-sensing
Sigfox	Unlicensed ISM	UNB (∼100 Hz BW); ∼100 bps; ∼12 B UL / 8 B DL; ∼140 UL msgs/day	Public operator (star); no private deployments	Simple telemetry; alarms; low-duty asset beacons
NB-IoT	Licensed (LTE/ GSM re-farmed), 180 kHz	Narrowband LTE (SC-FDMA/ OFDM); kbps-class; +20 dB MCL; repetitions up to 128	MNO-operated cellular core; deep-indoor coverage; very high device density (∼50k/cell)	Mass metering; smart city sensors; deep-indoor utilities
LTE-M	Licensed LTE, 1.4 MHz	Cat-M1 PHY; 100s kbps; lower latency; mobility/ VoLTE support	MNO-operated cellular (roaming, mobility, voice)	Wearables; telematics; mobile sensors; FW updates

Table 2.1: LPWAN options by spectrum, physical-layer capabilities, network model and indicative applicability.

bands made it one of the most popular choices for outdoor IoT applications, especially in Europe [32]. Sigfox, on the other hand, employs an Ultra Narrowband modulated signal, supporting long-range, highly efficient transmissions and caters for similar IoT demands as LoRa, namely long range, low power consumption, infrequent small payloads, and extended battery life[31]. For the licensed spectrum, NB-IoT developed by 3rd Generation Partnership Project (3GPP) empowers existing cellular infrastructure for wide-area coverage. Built on top of the legacy LTE and capable of existing within the GSM, 3G, 4G and 5G spectrum, it offers low infrastructure cost [33]. In 2023, Sinha et al. estimated that NB-IoT has become the predominant LPWAN technology due to its massive deployment in China [5]. Similar to NB-IoT, LTE-M, also developed by 3GPP, offers higher data rates and lower latency compared to NB-IoT, making it suitable for IoT devices that require these capabilities [34].

LPWANs features make them well suited for IoT applications. One key aspect is their ability to cover distances often spanning kilometres, which is essential for devices in remote locations [31]. This long-range capability is complemented by the power consumption of LPWAN devices, allowing them to operate for long periods on small batteries and reducing the need for frequent replacements. This efficiency is especially beneficial for scale projects where maintenance costs can be a concern [35].

Moreover, LPWANs are cost-effective with devices that are ideal for applications with budget limitations [31]. The low data rates typical of LPWAN networks are suitable for scenarios needing infrequent data transmissions such as monitoring or utility metering. However, there may be an increase in latency compared to traditional cellular networks, which could impact real-time applications. Nevertheless, most IoT use cases generally accept this latency [34].

The versatility of LPWANs enables applications in a wide range of scenarios. In cities LPWANs facilitate activities such as traffic flow monitoring, street lighting control and environmental conditions tracking, contributing to effective urban management [32]. In the metering field, LPWANs allow for remote monitoring of electricity, water and gas meters, which helps utilities streamline operations more efficiently [31]. Asset tracking is another use case where LPWAN technologies are utilised to track the whereabouts of vehicles, containers and other assets in time, improving logistics and supply chain management [31]. In agriculture, these networks play an important role in monitoring soil moisture levels, crop health status and livestock conditions, leading to increased farm productivity and better resource utilisation [35]. Industrial monitoring also sees benefits from LPWAN technologies by enabling oversight of machinery and sensors to prevent downtime and optimise efficiency [35]. Moreover, the healthcare industry leverages LPWAN for patient monitoring, wearable devices and telehealth services to enhance patient care quality while reducing healthcare expenses costs [35].

2.1.2 LPWAN Technologies

LoRa

LoRa is the predominant unlicensed LPWAN technology deployed up to this date. Technically, LoRa operates on a proprietary spread spectrum modulation technique developed by Semtech. This technique, derived from Chirp Spread Spectrum (CSS), includes integrated Forward Error Correction (FEC), which enhances robustness and efficiency over long distances [36]. LoRa transceivers have the ability to function over a range of frequencies spanning from 137 MHz to 1020 MHz. However, they are commonly used in the Industrial, Scientific and Medical (ISM) bands at 868 MHz and 433 MHz in Europe as well as at 915 MHz and 433 MHz in the USA [36]. LoRa

supports data rates ranging from 0.3 kbps to 50 kbps with the flexibility to adjust data rates based on Spreading Factor (SF) and bandwidth settings according to application needs [37]. The MAC layer protocol for LoRa, called LoRaWAN, operates within a star topology setup, where gateways play a role in relaying messages between end devices and a central network server for easier network management [38].

With its capabilities, LoRa applications span across various sectors effectively. In metering scenarios, LoRa proves efficient for monitoring electricity, water and gas meters due to its long-range coverage and minimal power consumption that facilitate infrequent data transmissions yet reliable, essential for these utilities [39]. Its extended reach and energy-efficient operation make it an excellent choice for tracking assets like containers, vehicles and equipment in logistics and supply chain management settings where real-time monitoring is vital [40]. In the field of agriculture, LoRa technology can be used to monitor factors such as temperature, humidity and soil moisture. This data is valuable for enhancing crop management practices and optimising the use of resources [38]. Moreover, LoRa technology is beneficial for city applications like controlling street lighting, managing waste and monitoring parking spaces by leveraging extended coverage and low power consumption [39]. Additionally, LoRa is well suited for IoT uses such as monitoring machinery and enabling remote control operations due to its reliability and ability to cover areas effectively [38]. In the context of sensing applications that involve collecting data from sensors spread across multiple locations, LoRa offers an efficient solution with its long-range capabilities and minimal power requirements [39].

Sigfox

Sigfox is another LPWAN technology known for its Ultra Narrowband (UNB) approach that enables efficient long-range communication in IoT settings. Sigfox utilises a proprietary UNB technology with a slow modulation rate to achieve extended communication ranges, making it particularly suitable for applications that need to transmit minimal data over significant distances, similar to LoRa[38]. Operating within unlicensed sub-GHz ISM bands, specifically 868 MHz in Europe, 915 MHz in North America and 433 MHz in Asia, Sigfox provides broad coverage while minimising interference. Sigfox offers data rates typically around 100 bps, which are sufficient for

many IoT applications that need occasional data transmission [38]. The network uses a star-shaped topology, where base stations link to a network server through an IP-based network, making the connection structure simple and accessible [38].

From an industrial IoT (IIoT) standpoint, Sigfox is well suited to non-critical telemetry (e.g., condition monitoring and asset tracking) where small, infrequent uplinks are acceptable. However, its tight duty-cycle and payload limits ($\approx$ 100 bps PHY, $\approx$ 12-byte uplink payload, $\approx$ 8-byte downlink, $\sim$ 140 uplink messages/day and typically $\leq$ 4 downlink/day) and the absence of deterministic QoS make it unsuitable for time-critical closed-loop control in IIoT; technologies with guaranteed latency are preferred for those use cases [38, 41, 42].

The design and functions of Sigfox make it suitable for applications, especially those that need low-cost connectivity across vast areas. Due to its reach and affordability, Sigfox is an option for tracking assets, particularly in areas with limited infrastructure [43]. It works well for monitoring conditions like air quality and water levels where intermittent data transmission is sufficient [38]. In building setups, Sigfox aids in managing energy usage, security systems and HVAC controls by leveraging its coverage and low power needs [38]. Similar to LoRa technology, Sigfox can oversee conditions such as temperature levels, humidity levels, and soil moisture content to provide information on enhancing farming methods. Moreover, Sigfox's capabilities can cater to city needs, like waste management, parking monitoring and street lighting control, by utilising its long-range [38]. The extended reach and energy efficiency of Sigfox makes it well-suited for metering applications, where devices need to send data sporadically across distances while conserving power.

Although LoRa and Sigfox each offer benefits for applications, there are distinct differences between the two technologies. LoRa supports higher data rates than Sigfox, making it more appropriate for applications that require updates or larger data transfers. When it comes to network scalability, both technologies promise to be highly scalable. However, LoRaWAN is anticipated to offer better scalability than Sigfox [38]. LoRa allows for both public and private network setups, offering flexibility based on the specific needs of the application, whereas Sigfox primarily functions as a public network provider. Both LoRa and Sigfox are generally seen as cost-effective

options compared to NB-IoT or LTE-M, which tend to be pricier due to their reliance on the licensed spectrum. The previously mentioned use cases highlight the advantages of both LoRa and Sigfox in driving IoT expansion. The decision between LoRa and Sigfox hinges on the application's demands in terms of data rate, cost considerations and network accessibility [38].

2.1.3 Narrowband Internet of Things

The introduction of NB-IoT by the 3rd Generation Partnership Project (3GPP) in Release 13 marked an advancement in tailored IoT telecommunication technology [6, 44, 45]. This innovative radio access technology is designed to offer coverage for machine-type communications (MTC) and caters to ultra-low-end IoT applications. According to Chen et al., the development of NB-IoT involved research into specific cellular networks for MTC services since 2005 with a primary focus on addressing network congestion and resource scarcity during simultaneous terminal access [45]. In Release 12, 3GPP introduced enhancements for GSM access networks concerning the design of low-cost MTC terminals. In 2017, both Chen et al. and Wang et al. reported that the standardisation and development of NB-IoT are ongoing processes with additional enhancements planned for future releases [6, 45].

Primary Characteristics of NB-IoT

NB-IoT is characterised by features that render it ideal for a diverse array of IoT applications. One standout quality is its energy efficiency. NB-IoT devices are crafted to have a long battery lifetime, with some scenarios lasting well over ten years. To achieve this, NB-IoT, devices can use power-saving features like Power Saving Mode (PSM), Extended Discontinuous Reception (eDRX), Early Data Transmission (EDT) and efficient modulation schemes [46, 44, 47, 45, 48]. They also provide extended coverage, surpassing existing cellular technologies with a 20 dB improvement in signal strength over GPRS, which is crucial for IoT applications situated in remote areas or places with poor signal penetration [44, 47, 45, 48].

When it comes to cost NB-IoT, devices are made to be budget-friendly, featuring simplified hardware and software components (compared to legacy LTE) that reduce manufacturing costs. Leveraging existing infrastructure

further cuts down deployment expenses [44, 47, 45, 49, 48]. Moreover NB-IoT can handle high connection densities of up to 50,000 devices per cell, making it ideal for large-scale projects with interconnected devices [46, 44, 45, 48].

In comparison to other released LPWAN technologies, NB-IoT stands out as a promising option. It represents the majority of licensed LPWAN while at the same time, in 2023, it surpassed the active LoRa devices [5]. Compared directly to LoRa, both technologies target low-power and long-range communication. However, while LoRa is typically deployed in an unlicensed spectrum, offering deployment flexibility, NB-IoT has advantages in terms of higher data rates and better security due to its standardised cellular technology [47, 45, 49, 48].

Compared with Sigfox in unlicensed ISM, NB-IoT generally offers broader effective coverage via licensed-spectrum operation, managed macro-cell deployments, and 3GPP coverage-enhancement (ECL0–ECL2 with repetitions). It also inherits LTE/5G-grade security—SIM-based AKA plus NAS/AS ciphering and integrity—yielding stronger guarantees than Sigfox's lighter, proprietary model [44, 47, 45, 50]. On the other hand, LTE-M has higher data rates and device mobility within the 3GPP framework. However, it lacks the NB-IoT energy efficiency and device density, which accommodates a large number of devices per cell, making the protocol suitable for IoT scalability [47, 45, 49, 48].

Advantages and Limitations of NB-IoT

One of the key advantages of NB-IoT that makes it an attractive option for IoT application is its standardisation. NB-IoT guarantees interoperability between different vendors, reducing fragmentation in the IoT ecosystem [49]. It is supported by an extensive network of telecommunication providers, module vendors, and chip manufacturers who offer an array of solutions and devices. The technology's ability to scale makes it ideal for large implementations accommodating a high number of devices [7]. Additionally, NB-IoT inherits the cellular LTE security framework, including mutual authentication via AKA, encryption of user and control plane traffic, and integrity protection of signalling [50].

Nevertheless, NB-IoT does come with limitations. It is primarily intended for low data rate applications, which may not be suitable for tasks

with high-bandwidth applications such as CCTV [49, 48]. Furthermore, the availability of frequency bands for NB-IoT can also potentially impact signal penetration in specific environments.

In conclusion, NB-IoT has emerged as a leading technology for low power wide area connectivity. It offers significant benefits for large-scale IoT network deployments. Its key attributes, such as power consumption, extensive coverage, cost-effectiveness and high connection density, make it suitable for a wide range of applications. However, factors like data rates and complexity need to be taken into account when assessing its suitability for specific use cases. As technology progresses, further enhancements are anticipated to overcome these limitations and broaden its applicability across a range of scenarios.

2.2 NB-IoT Communication

With the advancement of telecommunications technology, there is an increasing demand for higher and faster bandwidth. These necessities can be satisfied by utilising higher frequencies in the radio spectrum, therefore accommodating the growing volume of data. NB-IoT was designed to work alongside GSM, LTE and 5G. Due to its low data rate needs, it can operate in three deployment modes, as shown in Figure 2.1.

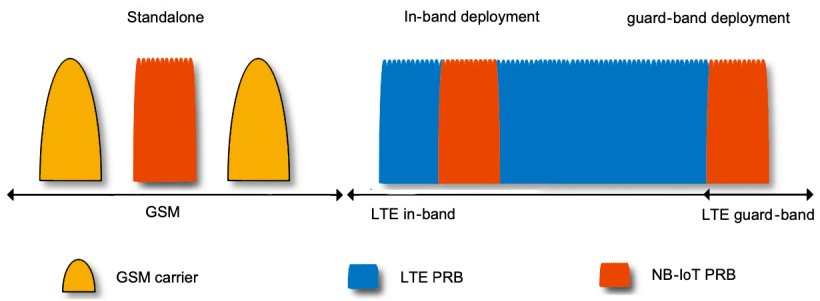


Figure 2.1: NB-IoT deployment modes, depicting the three different types: Standalone, In-band, and Guard-band.

- **Standalone**; inhabits a 200 kHz and is usually deployed in the GSM

spectrum [51]

- **In-Band**; occupies 180 kHz representing one PRB for both downlink and uplink
- **Guard-Band**; similar to In-Band deployment, it utilises 180 kHz, leveraging the guard band used by carriers in order to prevent overlaps and interference between them.

Furthermore, to meet the 5G's performance requirements of 1 million devices for every square kilometre, different time allocations with different tones (frequency domains) are assigned to each UE [7]. This, in turn, allows the network to assign multiple UE to one Resource Unit (RU), contrary to LTE, where every UE is assigned one RU [52]. A single tone can utilise a 3.75 kHz bandwidth for uplink when using Single-Carrier Frequency-Division Multiple Access scheme (SC-FDMA), illustrated in Figure 2.2 and

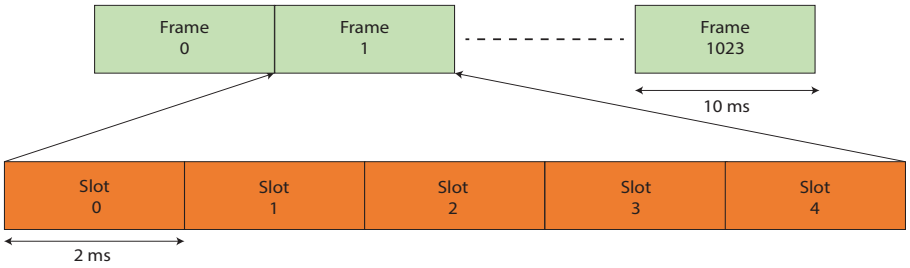


Figure 2.2: Frame structure for NB-IoT uplink with 3.75 kHz subcarrier spacing.

15 kHz when using Orthogonal Frequency-Division Multiplexing (OFDM) scheme (Figure 2.3) [53]. Moreover, while a 3.75 kHz spacing, with a duration of 32 ms, allows for only single-tone allocation to several UEs, on the 15 kHz spacing, both single-tone of 8 ms and multitone of 12, 6, or 3 tones with a duration of 1 ms, 2 ms and 4 ms can be employed for several UE [54].

Built on legacy LTE, NB-IoT uses a similar time frame structure with 1024 hyperframes. Each hyperframe is composed of 1024 System Frame Number (SFN), and each SFN contains ten subframes. The overall structure can be seen in Figure 2.3

In the frequency domain, each slot is mapped to 12 subcarriers with seven OFDM symbols. Additionally, if a 3.75 kHz uplink subcarrier spacing

is utilised, 48 subcarriers are assigned, with a duration of 2 ms.

NB-IoT communication is split into two parts: Downlink and Uplink. Each utilises several channels and signals to facilitate a reliable and secure connection between the UE and the base station.

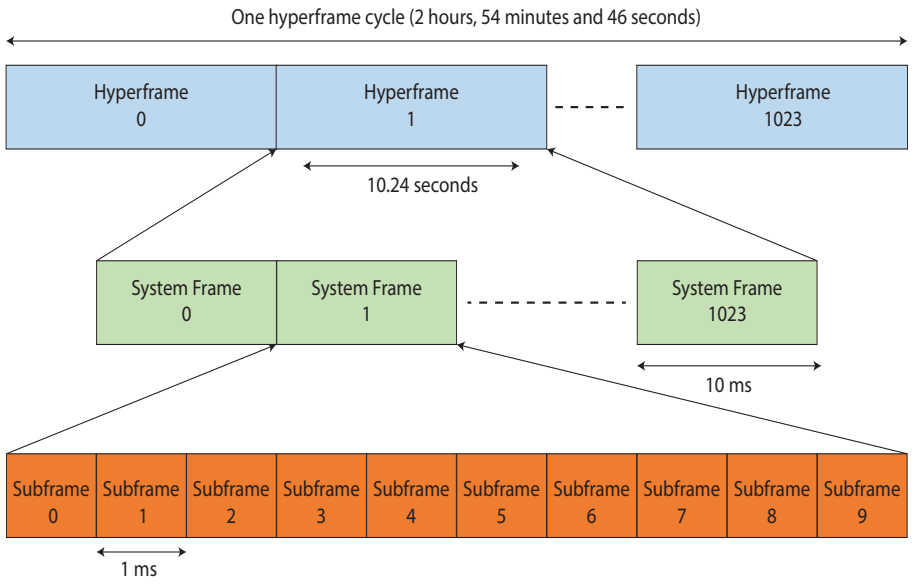


Figure 2.3: NB-IoT time domain frame structure.

2.2.1 Synchronisation and System Information Acquisition

The following is an enumeration of the most important downlink elements used in this research, with their allocation illustrated in Figure 2.4.

- Narrowband Primary Synchronization Signal (NPSS).
- Narrowband Secondary Synchronization Signal (NSSS).
- Narrowband Reference Signal (NRS).
- Narrowband Master Information Block (MIB-NB).
- Narrowband System Information Block 1 (SIB1-NB).
- Narrowband System Information Block 2 (SIB2-NB).

NPSS is the first signal a UE searches for after a prolong sleep time. It is used to achieve synchronisation in time and frequency. Due to the low-power oscillators used by the UE to track time during sleep mode, the frequency can be offset by as much as 20 ppm, adding up to 18 kHz in a 900 MHz band [55]. Thus, the NPSS needs to be noticeable even with an extensive frequency offset, and such has a static allocation, being transmitted always on Subframe five.

NSSS Following the time and frequency synchronisation, the next procedure is to acquire the NSSS in order to obtain cell identification and information about the frame structure. NB-IoT supports 504 unique Physical Cell Identities (PCIDs), each of them is determined by using the frequency-domain symbols from the 132 NSSS Resource Element (RE). There are four NSSS sequences transmitted within a periodicity of 80 ms, and it will always be mapped to every other subframe nine. After identifying this sequence and knowing that the duration of a frame is 10 ms, the UE is able to obtain the three Least Significant Bit (LSB) of the System Frame Number (SFN)

NRS is another critical signal allowing the device to perform demodulation, signal strength and quality measurements. It is carried within an NPBCH, NPDCCH, or NPDSCH subframe, but it can also be transmitted in other subframes. As some general rules:

- Regardless of the operation mode, NRS should be transmitted in subframes 0, 4 and 9 that do not contain an NSSS.
- It can be present in subframes 1 and 3 when deployed in guard-band or standalone
- Regardless of the operation mode, NRS should be transmitted in every valid downlink subframe.

The mapping of NRS within subcarriers and the symbol sequence is dictated by the number of logical antenna ports and the Physical Cell Identity (PCID). The sequence employed for randomising interference between cells is a pseudorandom Quadrature Phase Shift Keying (QPSK) sequence that repeats every 10 ms radio frame [55]. Figure 2.5 depicts the NRS mapping within a subframe.

MIB-NB is always utilised in subframe zero, and it bears the MIB-NB. Having a Transport Block Size (TBS) of 50 bits, it consists of eight CSBs

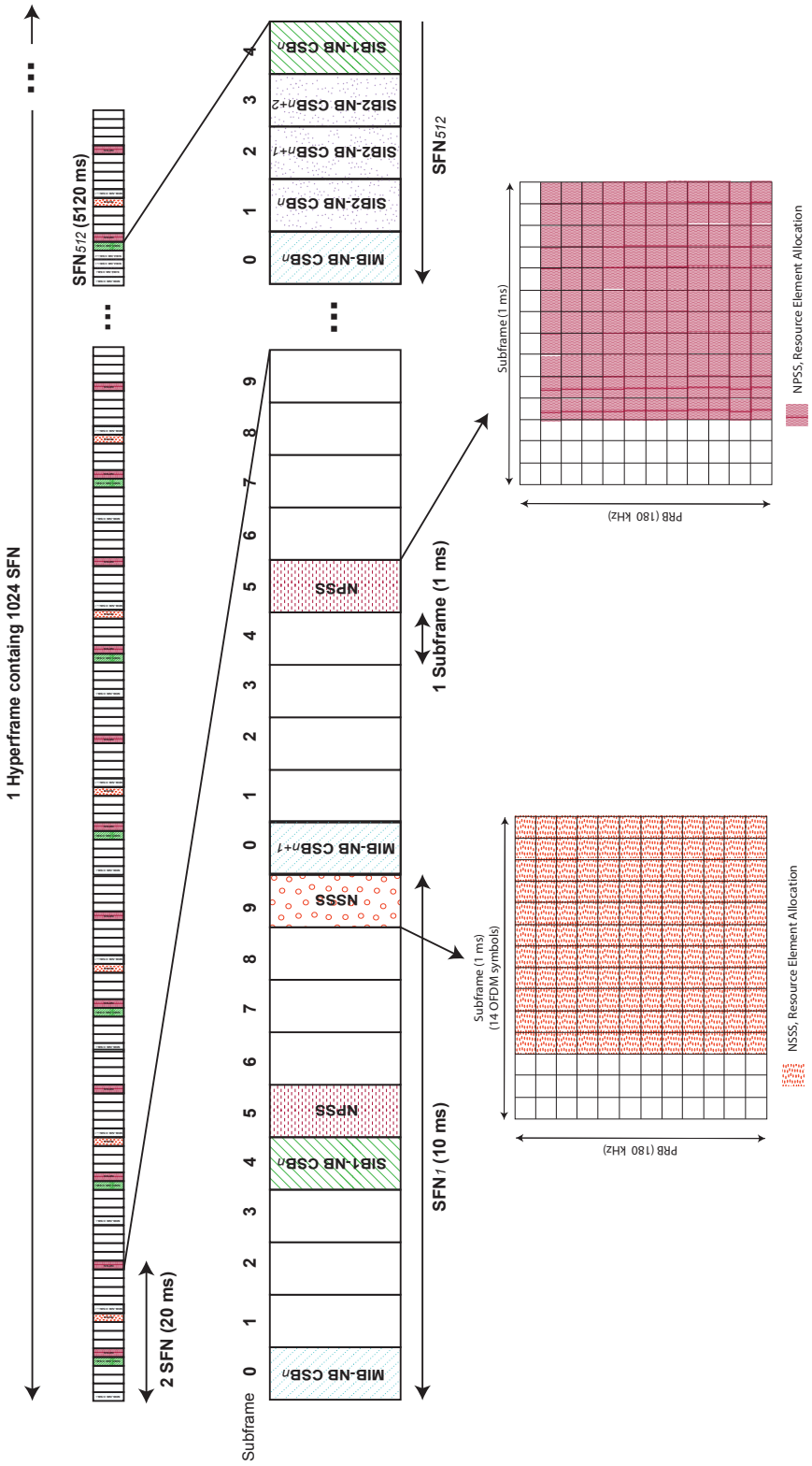


Figure 2.4: Subframe allocation of NPSS and NSSS with resource allocation in a PRB, Subframe mapping of CSB for MIB-NB and SIB1-NB.

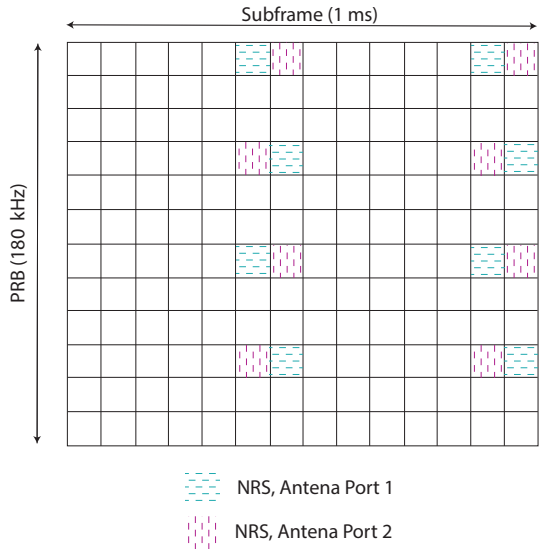


Figure 2.5: An example of resource mapping for NRS is in an NPBCH, NPDCCH, NPDSCH, or in any valid NB-IoT downlink subframe.

after encoding that is equally divided [56]. Each CSB is sent in subframe zero and repeated eight times, resulting in 64 subframes as depicted in Figure 2.4. The total duration for acquiring the MIB-NB is 640 ms. In order to coherently decode it, the UE has to acquire at least one of each repetition and utilise a Cyclic Redundancy Check (CRC) in order to validate the integrity of the MIB-NB.

The payload contained by the MIB-NB is significantly larger than the legacy LTE and includes information such as Access Baring, Scheduling Information for SIB1-NB, Operation Mode, four Most Significant Bit (MSB)s of the SFN, two LSBs of the Hyper-System Frame Number (H-SFN) and System Information value tag.

SIB1-NB After acquiring the MIB-NB, the UE turns its attention to SIB1-NB, another critical information block in the connection procedure. SIB1-NB employ a static repetition pattern with a periodicity of 256 frames (2560 ms) split equally into 16 frames. Depending on the configuration, the frames can be repeated evenly sixteen, eight, or four times. Usually, SIB1-NB is mapped to subframe four, every other SFN, as shown in Figure 2.4 [57]. However, due to the long acquisition time that might occur for devices with poor connection, 3GPP implemented in release 15, the ability to send SIB1-NB information in every subframe three preceding the SIB1-NB

subframe four [58]. This information is relayed to the UE by the MIB-NB.

Once the UE receives and decodes the SIB1-NB, it acquires the scheduling for other System Information (SI) messages, including the MSBs of the Hyper-System Frame Number (H-SFN).

SIB2-NB The final SI required for a UE before performing the RAP is the SIB2-NB. Unlike MIB-NB and SIB1-NB, the mapping of the SIB2-NB is dynamic and regularly broadcast by SIB1-NB. With the decoding of the SIB2-NB, the UE obtains all the configurations of the Radio Resource Control (RRC). These include the Narrowband Physical Random Access Channel (NPRACH) configurations and the ability to calculate its coverage class with the help of the NRS. The periodicity of the SIB2-NB is specified by the *si-WindowLenght* parameter, while the starting frame is defined by the *si-RepetionPattern*.

The Transport Block Size (TBS) of the SIB2-NB ranges from 56 to 680 bits. For a TBS of 56 or 120 bits, it utilises two consecutive subframes. For 280, 256, 328, 440, 552 or 680 bits, it will employ eight consecutive subframes that are not already predefined. Furthermore, when supporting extended coverage, the SIB2-NB can be repeated in every second, fourth, eighth or 16th frame.

Downlink Quality of Service

The NRS is found in each slot in the last two OFDM symbols. When considering the standard assignment of the NB-IoT, as depicted in Figure 2.4, the NRS can be transmitted in all subframes, with the exception of NPSS and NSSS which would conflict with the NRS alignment as shown in Figure 2.5.

In order to accurately evaluate the impact of introducing noise to the transmission, thus degrading QoS, it is necessary to explain several factors and their relationship for a comprehensive understanding.

Reference Signal Received Power (RSRP), is an important measurement for determining the quality of the received signal. It represents the average power of an NRS broadcast by the eNodeB and received by the NB-IoT device [59]. RSRP is measured in decibels-milliwatts (dBm) and is used for functions including cell selection, handover, and power regulation to ensure the NB-IoT network's reliability and performance.

Received Signal Strength Indicator (RSSI) is a measurement that calculates the average power received by a device in Watts. It particularly

looks at the power received from the configured OFDM symbol and within the measurement bandwidth over N resource blocks. The UE receives this input from several sources, such as co-channel and adjacent channel interference, thermal noise, and other factors. The estimated bandwidth is calculated by considering the downlink's operation with a 15 kHz spacing and the consistent use of 12 subcarriers as follows:

$$15kHz * 12 = 180kHz \tag{2.1}$$

This equates to exactly one PRB. Additionally, the RSSI changes depending on the assigned subcarriers and cell load [60].

Reference Signal Received Quality (RSRQ) is defined as the ratio RSSI and RSRP, with the requirement that both the denominator and the numerator have to be measured within the same set of resource blocks:

$$\text{RSRQ} = \frac{\text{RSSI}[W]}{\text{RSRP}[W]} \tag{2.2}$$

The **Signal-to-Interference and Noise Ratio (SINR)** is the ratio of the received signal level and the Interference amount (PI) from other sources, together with the Effective Noise Floor (PNeff):

$$\text{SINR} = \frac{\text{RSRP}[W]}{P_{I,15kHz} + P_{N,eff,15kHz}} = \frac{\text{RSSI}[W]}{P_{I,180kHz} + P_{N,eff,180kHz}} \tag{2.3}$$

In other research conducted by Matz et al. [60], they were able to validate the SINR and RSRQ correlation, with the activity factor x, proving the relation in [61] as the ratio inhabited by the Resource Element (RE) in a Resource Block (RB): x=RE/RB:

$$\text{SINR} = \frac{12}{\frac{1}{\text{RSRQ}} - \text{RE}} = \frac{12}{\frac{1}{\text{RSRQ}} - 12 * x} \tag{2.4}$$

Uplink

Once the UE has successfully decoded the SIB2-NB, it has the minimum requirements to initiate the Random Access Procedure (RAP). During the RAP, a suite of uplink and downlink messages are exchanged to ensure the authenticity and integrity of the data. Figure 2.6 depicts these exchanges.

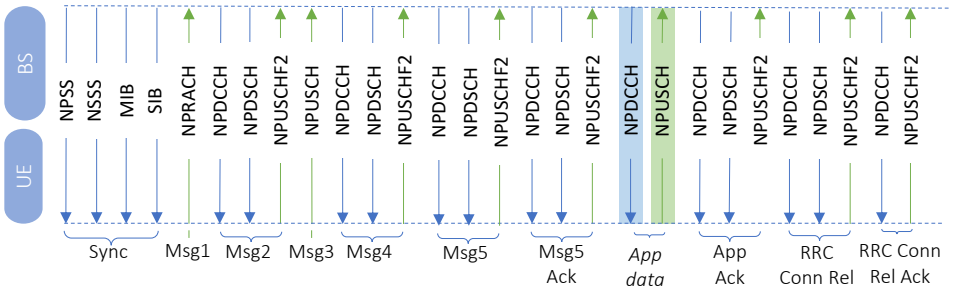


Figure 2.6: Examples of signals and messages exchanged within a typical NB-IoT Random Access Procedure (RAP).

The RAP is initiated by the UE sending MSG1 through the Narrowband Physical Random Access Channel (NPRACH), also known as the preamble. In response, the base station transmits two downlink messages through the NPDSCH followed by an uplink message from the UE, representing MSG2. These interactions repeat themselves until the acknowledgement of MSG5, after which the UE proceeds in sending its payload. The transmission ends with the acknowledgement of the Radio Resource Control (RRC) Connection Release.

It is worth mentioning that due to the low-cost oscillator used by the UE, 3GPP introduced uplink transmission gaps. These oscillators are not temperature-compensated and, therefore, are susceptible to frequency drift caused by self-heating. As a result, for every 256 ms of continuous Narrowband Physical Uplink Shared Channel (NPUSCH) or for every 64 repetitions of NPRACH preambles with format 0 or 1, as well as for every 16 repetitions of format 2, a 40 ms gap is used by the UE. During this gap, the UE reacquires the NPSS, NSSS and NRS, therefore achieving re-synchronisation.

2.2.2 Narrowband Physical Random Access Channel

Narrowband Physical Random Access Channel (NPRACH) is responsible for managing the initial access of NB-IoT devices to the network. When a device needs to communicate with the network, it must first perform a random access procedure to establish a connection. NPRACH provides the means for the device to send a random access preamble to the base station (eNodeB). This process is crucial for synchronising the device with the network and allocating the necessary resources for subsequent data transmission [62].

The NPRACH operates within the uplink frequency band and utilises a narrowband of 180 kHz, which aligns with the overall narrowband requirement of NB-IoT. The channel structure of NPRACH is specifically designed to be robust against typical NB-IoT challenges, such as very low SNR due to high coupling loss, large propagation delays and timing uncertainty from wide-area cells, and frequency-selective fading[63, 64, 65, 66, 4].

The Random Access Procedure (RAP), as shown in Figure 2.7, begins with the device transmitting a preamble. This preamble is a sequence of symbols that allows the base station to detect the presence of the device and estimate the timing offset. The NPRACH preamble consists of multiple subcarriers spread over time and frequency, following a frequency hopping pattern to enhance robustness and reduce interference [45].

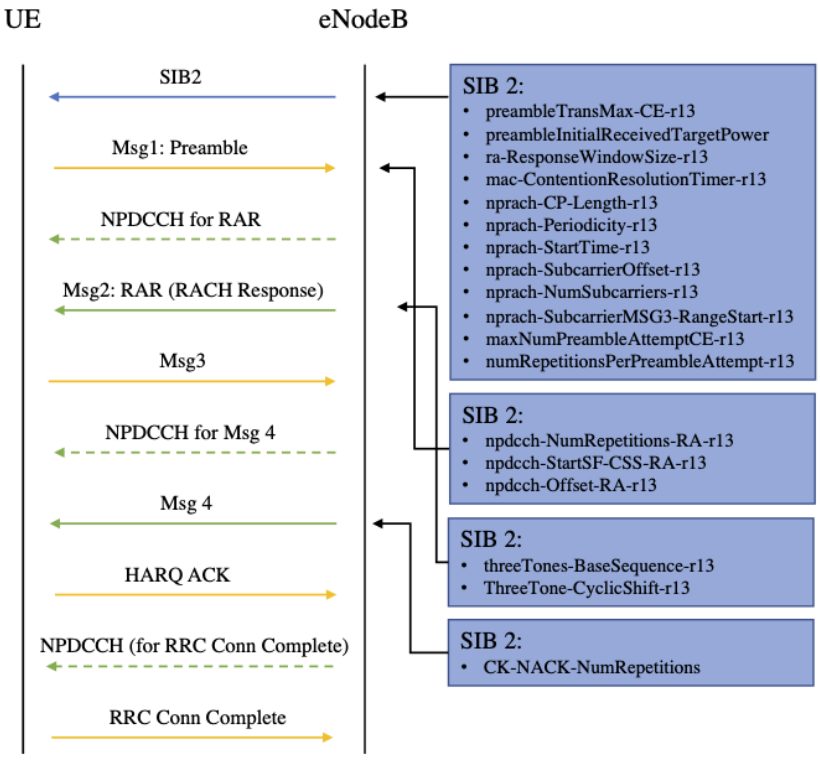


Figure 2.7: Random Access Procedure (RAP) mapped to the required data for carrying out the procedure. The data is transmitted by the eNodeB via the SIB2-NB.

Upon receiving the preamble, the base station performs detection and timing estimation. If the preamble is successfully detected, the base station responds with a Random Access Response (RAR) message. This message includes timing adjustment information, an initial uplink grant for data transmission, and a temporary identifier for the device [44].

Several challenges arise in the operation of NPRACH, particularly in environments with poor signal conditions or high interference. The use of frequency hopping in the preamble transmission helps mitigate these issues by spreading the signal over multiple subcarriers and time slots, thereby increasing the likelihood of successful detection.

Accurate timing alignment is critical for the success of the random access procedure. The NPRACH preamble design, which includes repeated transmission of symbols over different subcarriers, aids in achieving precise timing synchronisation. This design ensures that even if some symbols are lost due to interference, enough information remains for the base station to perform accurate timing estimation [63].

Interference management is another crucial aspect of NPRACH. The frequency hopping mechanism, combined with narrowband operation, reduces the impact of interference from other devices and systems. Additionally, the repeated transmission of preamble symbols allows the base station to perform diversity combining techniques, further enhancing detection reliability [67].

NPRACH is a vital component of the NB-IoT architecture, enabling devices to initiate communication with the network effectively. Its robust design, featuring frequency hopping and repeated symbol transmission, addresses the unique challenges of NB-IoT environments. Understanding the operation and significance of NPRACH is essential for optimising NB-IoT deployments and ensuring reliable connectivity for a multitude of devices.

2.2.3 Narrowband Physical Uplink Shared Channel

NPUSCH stands for Narrowband Physical Uplink Shared Channel, a communication channel used in cellular networks to transmit data from a device to a base station (BS). NPUSCH is used explicitly in NB-IoT technology, designed for low-power, low-bandwidth Internet of Things (IoT) devices [68, 69].

In simpler terms, NPUSCH is a way for IoT devices to send small

amounts of data to a cellular network using low power. NPUSCH has two transmission formats, Format 1 and Format 2, which are used for different data types [69]. Format 1 is used for uplink data transfer when the IoT device sends data to the network [69]. It uses a type of error correction called turbo coding, which helps ensure the data is transmitted accurately [70]. Turbo coding here means the LTE parallel-concatenated convolutional code (two 8-state constituent encoders with an internal quadratic interleaver) with a coding rate of 1/3 [71]. In NPUSCH Format 1 the UL-SCH is encoded with this turbo code and then rate-matched to the configured code rate, with iterative decoding improving error performance (i.e., lower BLER at a given SNR) [70]. The maximum amount of data that can be sent in one transmission is called the Transport Block Size (TBS), and the maximum TBS for NPUSCH Format 1 depends on the type of device being used[70] [69].

Format 2 is used for signalling Hybrid Automatic Repeat Request (HARQ) feedback and uplink scheduling requests [69]. It uses a different type of error correction called repetition coding, which is more straightforward than turbo coding but still helps ensure accurate transmission [70, 69].

Both Format 1 and Format 2 use a type of waveform called Single Carrier Frequency Division Multiple Access (SC-FDMA), which involves a process called Discrete Fourier Transform (DFT) precoding and a guard period [68]. SC-FDMA is a type of modulation that helps ensure reliable transmission in cellular networks [72]. Unlike OFDMA used on the downlink, SC-FDMA applies a DFT precoder that lowers the peak-to-average power ratio at the UE while still assigning orthogonal subcarriers, so intra-cell interference is avoided by orthogonality and scheduling, not by inserting guard bands between users [68, 72]. In NB-IoT uplink the only “extra spacing” you see is time-domain: a cyclic prefix for multipath and, when retuning between narrowbands/channels, short guard periods (empty SC-FDMA symbols); these are not frequency-domain guard bands [68].

NPUSCH supports both multitone and single-tone device scheduling bandwidth options, as explained in 2.2 [69]. In single-tone, the UE uses one subcarrier ($RU_N sc = 1$) with 15 kHz or 3.75 kHz spacing; the spec allows BPSK/QPSK here, and in practice single-tone commonly uses $\pi/2$-BPSK or $\pi/4$-QPSK to keep peak-to-average power ratio (PAPR) low and extend coverage [68, 69]. In multi-tone, the UE uses 3, 6, or 12 contiguous 15 kHz

subcarriers ($RU_N sc \in 3, 6, 12$) with QPSK, trading higher instantaneous rate for a higher PAPR compared with single-tone [69]. NB-IoT devices can send data using either multiple frequencies or just one frequency. Using a single frequency can have advantages in reducing the PAPR, which can help save power [72].

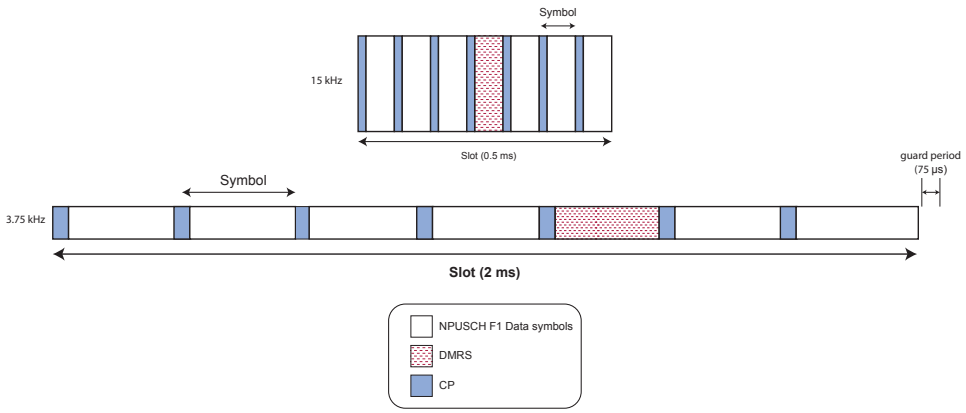


Figure 2.8: NPUSCH Format 1.

The slot formats applicable to NPUSCH Format 1 are illustrated in Fig 2.8. The definition of CP and OFDM symbol durations for 15 kHz subcarrier spacing are identical to those in LTE. For broadcasts that use a single tone and have a subcarrier spacing of 3.75 kHz, NB-IoT offers a new layout, illustrated in Figure 4.7. The slot duration in this scenario is two milliseconds, which includes seven SC-FDMA symbols and a guard period (GP) at the end. The duration of each SC-FDMA symbol is 275 milliseconds, including a cyclic prefix (CP) of 8.33 milliseconds.

Simply put, each slot is a small unit of time in which data can be transmitted. In NPUSCH Format 1, the way the slot is structured is the same as in LTE technology, but for single-tone transmissions with a lower frequency, there are some differences in how the slot is set up. The guard period is a small buffer at the end of the slot that helps prevent interference from other signals.

For 15 kHz subcarrier spacing, the middle OFDM symbol in each slot is used as a Demodulation Reference Signal (DMRS), which allows the BS to estimate the uplink propagation conditions. For 3.75 kHz subcarrier spacing, the placement of the DMRS is shifted to the fifth OFDM symbol in the slot. DMRS is a way for the BS to measure the quality of the signal transmitted

by the IoT device. In NPUSCH Format 1, the DMRS is located in the middle of the slot.

Uplink Quality of Service

In NB-IoT, the quality of uplink signals has a significant impact on overall network performance and dependability. Uplink quality, which refers to how data is transmitted from UE to the base station, has a direct impact on data communication efficiency, network capacity, and end-user experience.

The Maximum Coupling Loss (MCL) parameter, expressed in decibels (dB), is the result of the difference between Power Level at the Antenna Connector (PTX) and Receiver Sensitivity (PRXmin):

$$MCL\,[\text{dB}] = \text{PTX}\,[\text{dBm}] - \text{PRXmin}\,[\text{dBm}] \tag{2.5}$$

MCL plays a crucial role in the proper functioning of the NB-IoT protocol. It is a key metric used by both the UE as well as the eNodeB in estimating the radio coverage, setting the number of repetitions and the PTX. Moreover, in the situation where the uplink transmission requires a maximum of two repetitions, the UE has the ability to adjust its PTX after measuring the coupling loss and other cell-specific variables. Otherwise, in case the communication demands more than two repetitions, the UE will use the maximum PTX acquired during the Random Access Procedure (RAP) [55].

The receiver sensitivity, PRXmin, is the minimal input energy level at the receiver antenna required to meet a QoS threshold. In NB-IoT, the Modulation and Coding Scheme (MCS) can be dynamically adjusted by the eNodeB based on link quality indicators reported by the UE, such as the RSRP, RSRQ, and the Signal-to-Noise Power Ratio (SNR), which together characterise the current radio conditions. The MCS is defined by the number of usable bits that may be transferred per RE, thus relating MCS directly to the quality of the radio link and the error probability. Essentially, the MCS is changed periodically to maintain the connection within a Block Error Rate (BLER)) threshold, typically 10% for the NPDSCH and NPUSCH channels [55]. Furthermore, NB-IoT can broaden its reach by increasing the number of symbol repetitions (NRep). The BLER is affected by both the MCS and the NRep used for a specific SNR. To accomplish the stated BLER, the minimal SNR (Minimum Signal-to-Noise Power Ratio (SNRmin)) must

take into consideration thermal noise, as:

$$P_N = 10 * log(kTB/1mW) \tag{2.6}$$

where k = Boltzmann constant, T = temperature, B = bandwidth. [60] and [55] describe the PNeff as the combination of the receiver front-end's Noise Figure (NF) and the Thermal Noise (PN). Based on the above definitions, the PRXmin can be calculated as:

$$\text{PRXmin} = P_N + NF + \text{SNRmin} = \text{PNeff} + \text{SNRmin}. \tag{2.7}$$

2.3 Energy Optimization in IoT

Energy efficiency is essential in IoT deployments. By optimising the energy consumption, a UE can prolong its lifespan as well as reduce the operation cost and minimise environmental impact. More specifically, devices that are meant to operate uninterrupted for long periods of time demand high energy efficiency. There are general approaches for energy optimisation [73, 74], including the adoption of low-power communication protocols, the use of energy-efficient hardware, and the exploitation of advanced algorithms for resource usage [75, 76].

2.3.1 Energy Optimization Techniques

Several techniques can be employed to optimise energy consumption in IoT systems:

- **Sensing Patterns Optimisation** Reducing sensing energy consumption techniques include adaptive sensing, where the sensing rate can be adapted to the environment conditions or the application requirements [73, 77]. Event-driven sensing rather than constant monitoring can help to reduce energy consumption.
- **Network Complexity Reduction** Among the techniques to reduce the network energy consumption is the simplification of network protocols; for example, reducing the complexity of communication protocols

can contribute to minimising the overhead during the data transmission [77, 78]. Examples of this simplification include adopting a reduced control message size and reducing the number of bits in the overhead.

- **Transceiver Use Optimization** Techniques to reduce the energy consumption of transceivers include optimising the transmission power, using sleep modes and efficient modulation schemes. These techniques are widely employed in Low-Power Wide Area Network (LPWAN) technologies [74, 76].

2.3.2 Energy Optimisation in LPWAN Technologies

LPWAN technologies, such as LoRaWAN, Sigfox and NB-IoT, are designed to operate over great distances with very little power consumption. Optimal strategies include controlling the duty cycle of transmissions and using adaptive data rates in combination with efficient coding schemes.[77, 78]. As an example, for LPWAN, the implementation of IoT in precision agriculture has demonstrated the feasibility of optimising the sleep/active schedule. The sensors need to meet the requirements of long-distance coverage for network-wide applications, and as a result, they can potentially extend the operational lifetime of the network. For instance, Singh et al. have managed to extend the lifespan of the network from four to six years with a specific LoRaWAN deployment probing pulse interval modulation (PIM) sleep/active schedules [77]. Furthermore, empirical evaluation of energy consumption from different LPWAN technologies has shown that these optimal strategies demonstrate the importance of choosing the right technology depending on the application [74]. Overall, most strategies drawn from the literature are effective and have been demonstrated in many real-world applications, though we note that good strategies exist whose effectiveness remains to be demonstrated.

Overall, energy efficiency for IoT requires a series of approaches that are adapted to the application and the technology being used. Developing better communication protocols, hardware designs, and algorithms is essential to achieve more efficient use of energy in IoT deployments.

2.4 NB-IoT Energy Consumption and EDT Mechanisms

2.4.1 NB-IoT Energy Consumption

NB-IoT design primarily focuses on supporting Machine-Type Communications (MTC), which involves data exchange between devices without human intervention. While NB-IoT boasts of features like extended coverage, enabling connectivity even in challenging environments such as underground or deep inside buildings, it grapples with issues related to energy consumption and device density [75].

When it comes to numerous applications of the NB-IoT, it is anticipated that devices would function for extended periods of time, frequently exceeding ten years, on a single charge of their batteries. Despite research conducted on energy harvesting techniques for NB-IoT [79], the application of these methods is primarily limited to outdoor environments [80]. As a consequence, energy efficiency is an essential factor to take into consideration, particularly for solutions involving net-zero energy use and energy harvesting. NB-IoT devices, despite being designed to consume a small amount of power, face energy-related challenges [81]. These challenges are driven by a variety of circumstances, including that which follows:

- **Control and Signaling Overheads**: Most communication protocols, such as LTE, NB-IoT and LoRaWAN, implement signalling and control data overhead to establish and maintain the network connection.

  Each communication protocol contains control and signalling data that have to be transmitted in order to establish and maintain a connection. When considering the case of NB-IoT, it is possible that these overheads, which are necessary for the device to function properly, might sometimes be rather substantial in comparison to the transmitted payload. These overheads have the potential to result in increased energy consumption, which in turn causes the device's effective operational life to be reduced [82].

- **Signal Transmission Repetition**: To improve reception in demanding environments and ensure data integrity, NB-IoT utilises Coverage

Enhancement (CE) levels. This approach involves multiple transmissions of the same data to boost the likelihood of successful reception. However, each transmission (uplink or downlink) depletes the UEs energy levels. This can be problematic in areas with poor coverage or in highly dense environments (e.g. stadiums, concerts or tourist venues). For these edge cases, the high number of retransmissions becomes common and can strain the device's power-saving mechanisms [83].

- **Parameter Configuration**: The energy consumption profile of an UE is influenced by the operational parameters of the NB-IoT network. Most of these parameters are configurable and, depending on the environment and load of the network, are changed multiple times a day. The UE is notified of these configurations through paging intervals, which is another parameter that determines the frequency the UE has to check for downlink messages. Longer intervals can significantly reduce the UEs energy consumption but might increase the latency of the communication. Michelinakis et al. [75] have demonstrated that slight tweaks and changes in the default settings lead to a significant reduction in energy use.

Device Density

NB-IoT's capability to cater for a vast number of UEs within a limited geographical area positions it as a frontrunner for dense IoT applications, such as smart cities where thousands of sensors and devices must communicate frequently. However, this density, while being an advantage, also poses challenges. For instance, when many devices attempt to connect to the network simultaneously, it can lead to network congestion. This is particularly evident during Random Access Procedures (RAPs), where devices try to establish a connection with the network. Collisions during these procedures, either due to simultaneous attempts or because of sub-optimal channel conditions, can necessitate multiple RAP retries. Each retry consumes energy and bandwidth, leading to increased energy consumption for the device and potential degradation in the overall service quality of the network [84].

2.4.2 C-IoT-Opt and EDT Mechanism

High device density areas, such as urban regions with large populations, can be challenging when addressing spectral efficiency, energy usage, or address latency. For this reason, 3GPP introduced features like Cellular Internet of Things Optimization (C-IoT-Opt) and Early Data Transmission (EDT) with the scope of improving the NB-IoT network performance [28, 85, 86].

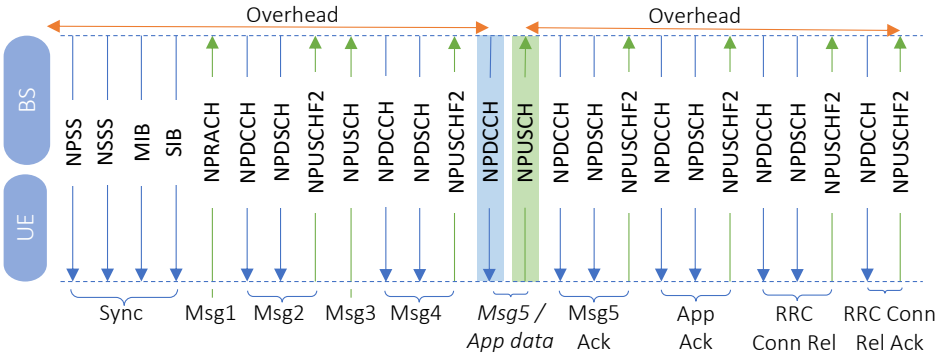


Figure 2.9: C-IoT-Opt transmission

C-IoT-Opt: Enables small amounts of payload to be transmitted at the RRC level, between the UE and the eNodeB. Figure 2.9 shows the ability of the network to piggyback data in both downlink and uplink transmission through Msg4 and Msg5. This is possible by utilising the "dedicatedInfoNAS" Information Element (IE) [28].

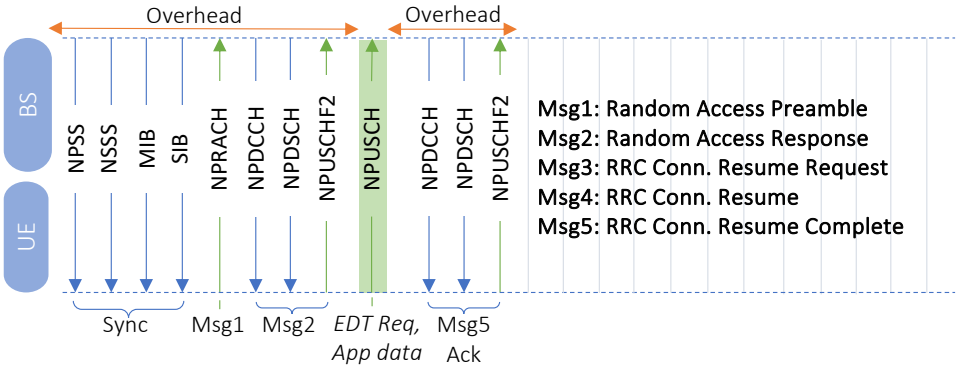


Figure 2.10: EDT transmission

EDT: The diagram in Figure 2.10 illustrates the process by which a UE

can transmit data using EDT. This feature was introduced in Release 15 by 3GPP, and it allows an idling UE to wake up and send data via the RRC Connection Resume Request (Msg3). Upon successfully receiving the data, the eNodeB ends the transmission by sending an RRCEarlyDataComplete alongside any downlink payload. EDT significantly reduces the transmission overhead when compared to normal procedures. Additionally, it improves spectral efficiency as well as energy usage. Pascal et al. [28] has observed a reduction of 2.9 times in latency and 3.7 times in spectral occupancy during an EDT transmission. As a result, EDT transmission is always favourable, bringing advantages for both the network operator and the application.

For large-scale scenarios, C-IoT-Opt and EDT have a crucial part in optimising the NB-IoT network. C-IoT-Opt optimises the transmission of small data at the RRC level while, EDT reduces the latency and improves the spectral efficiency.

2.4.3 Extended Coverage Level

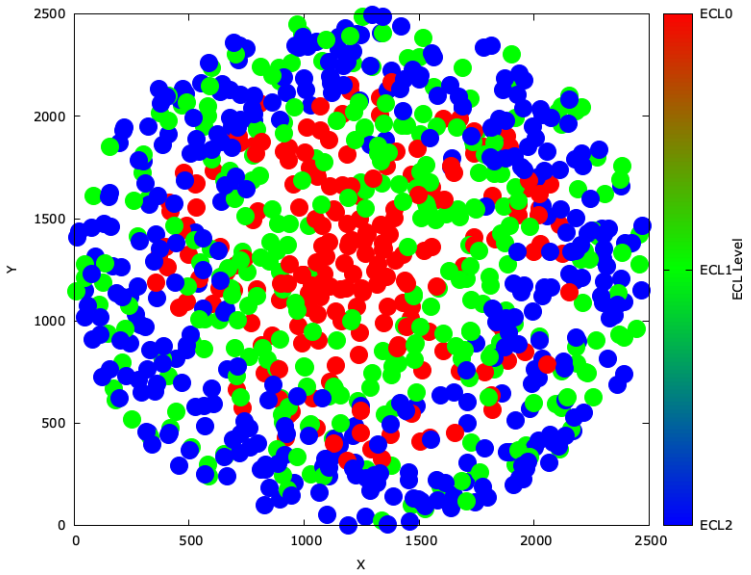


Figure 2.11: ECL Map.

In real-world scenarios, the signal distribution is not uniform, particularly in deep indoor environments, rural areas, and at the edge of the network, where signal quality can degrade significantly. NB-IoT adapts its resource allocation by classifying devices into three Enhanced Coverage Lev-

els (ECL0–ECL2) [87], each associated with different transmission power, repetition counts, and modulation robustness. This classification ensures that devices in challenging locations receive the additional link budget and transmission repetitions needed for reliable communication. The UE experiences dynamic selection of the Extended Coverage Level (ECL) depending on the measured signal quality, an adjustment performed during the RRC connection procedure via the NPRACH. As the ECL number increases, more robust signal processing capabilities are required, typically leading to higher power consumption but also enhanced penetration and range. NB-IoT uses repetition techniques, such as transmitting the same data packet more than once, to boost the likelihood of successful transmission and reception in weak signal environments and reach these increased coverage levels [60]. The level of repetition and thus the time-on-air increases from ECL0 to ECL2 [75]. Higher ECLs affect battery life even though they can significantly improve coverage since they need more energy to transmit signals repeatedly.

EDT+ (see Section 3.3) is not directly impacted by the ECL as it does not address the repetition procedure. When evaluating an equal distribution of ECL0, ECL1, and ECL2 as seen in figure 2.11, with repetition numbers ranging from 8 to 64, we did not see any significant changes in our result. The overall energy and resource allocation per device increase equally to the increase seen by normal transmission and EDT transmission. This is explained by the fact that NB-IoT already uses a highly sophisticated and dynamic repetition procedure. The primary modification required is in the scheduling of subsequent transmissions; specifically, the repetition count must be predetermined for the upcoming transmission rather than being communicated during the NPRACH.

2.5 Clock Drift

2.5.1 Introduction to Clock Drift

Clock drift occurs when the time shown by a clock drifts away from the actual time, causing discrepancies between devices' notion of time. In the IoT, where large numbers of devices collaboratively operate in a distributed setting, this phenomenon has a major negative impact on the performance

and reliability of applications that require synchronisation of time on multiple devices. In the framework developed by Skiadopoulos et al. [88], clocks in IoT devices can drift away from synchronisation with each other by orders of seconds over short timeframes – too much drift to be effectively addressed by traditional synchronisation protocols.

Factors such as manufacturing deviations in clock parts, thermal variations and hardware ageing contribute to clock drift. According to Schmid et al., [89], the frequency of the crystal oscillator may depend on the environmental parameters and/or it may be subject to manufacturing imprecision, causing drift. Moreover, Sundararaman et al.[90] explain that variations in the frequency of quartz crystals in distributed systems result in clock values that gradually diverge, leading to inconsistent notions of time. Clock drift can cause increased response latency, packet loss and overall degradation of system performance.

2.5.2 Impact of Clock Drift on IoT Devices

Clock drifts can have devastating impacts on IoT communication protocols, especially those connected to synchronisation mechanisms. Bankov et al. [91] claim that Target Wake Time (TWT) mechanism recovery on Wi-Fi networks may break on clock drift when a device misses its scheduled transmission time, which increases its active time and power consumption. According to Elson et al., [92], clock drift can skew the time-stamped data, making it difficult to determine the time difference between two events on two devices.

There are many case studies that describe the implications of clock drifts for IoT systems. One such case described by Mani et al. [93] reports several challenges faced by IoT devices raised by clock drift, which can lead to erroneous data. Similarly, Gachhadar and Ruttik [94] describe clock errors in Narrowband IoT (NB-IoT) that can cause Carrier Frequency Offset (CFO) and sampling errors, impacting the performance of radio links. Overall, these studies highlight the importance of clock accuracy in IoT systems, including for protocols that incorporate mitigation strategies.

2.5.3 Mitigation Strategies for Clock Drift

Clock drift can be addressed in several ways. A simple example suggested by Schmid et al. [89] is to leverage manufacturing differences caused by cost-efficient oscillators for algorithmic correction, thereby enhancing timekeeping accuracy without the need for expensive hardware. Another approach is outlined by Sundararaman et al. [90], emphasising the need for clock synchronisation protocols that are tailored to the specific requirements of IoT environments, such as energy efficiency and robustness.

Synchronisation schemes can be used to ameliorate the effects of clock drift, such as the Reference Broadcast Synchronization (RBS) method used by Elson et al. [92]. This method allows nodes in a broadcast domain to set their clocks to the reference pulses received, even when jitter is present. Traditionally, NTP (Network Time Protocol) is employed for synchronisation procedures. However, newer approaches such as [90] have been proposed that are specific to sensor networks, helping them to maintain synchronisation across multiple devices while being more efficient at the same time.

2.5.4 CFO and Time Drift in NB-IoT

The rapid proliferation of smart devices necessitates robust and efficient communication protocols. NB-IoT is one such protocol designed for LPWAN applications. Nevertheless, the inherent difficulties linked to the frequency references in these UEs, especially when considering temperature fluctuations, might result in problems such as Clock Frequency Offset (CFO) [95], and time drift [96], [97].

CFO and time drift are critical aspects to consider in wireless communication systems, especially in NB-IoT networks and other embedded sensor networks. These factors can significantly impact communication systems' synchronisation, accuracy, and overall performance.

CFO: CFO arises due to the mismatch between the transmitter and receiver oscillators' frequencies. In wireless systems, even a slight discrepancy in these frequencies can lead to a shift in the received signal's phase and frequency, causing Inter-Carrier Interference (ICI) and degrading the system's performance. In NB-IoT, CFO can be particularly challenging due to the technology's focus on low power and cost-effectiveness, which might lead to using less precise oscillators.

Time Drift in Embedded Sensor Networks: Time synchronisation is a crucial service in embedded sensor networks, enabling data correlation between nodes and efficient communication scheduling. However, one of the significant challenges in achieving precise synchronisation is the effect of environmental temperature changes on the clock frequency. It's a well-known fact that a quartz crystal's resonant frequency, commonly used in these systems, changes with temperature variations. This phenomenon can lead to time drift, where the clock gradually becomes out of sync. Solutions such as the Temperature Compensated Time Synchronization (TCTS) have been proposed to address this issue. TCTS leverages onboard temperature sensors to automatically calibrate the local oscillator [96].

Crystal Oscillators and Temperature Dependency: In *PSM/deep-sleep*, NB-IoT UEs keep time with a low-frequency sleep/RTC Uncompensated Crystal Oscillator (XO) (32.768 kHz), typically uncompensated and specified in the tens of ppm (e.g., 20–50 ppm; ±40 ppm is common) [23, 98, 99]. Together with temperature variation, this clock drives the observed *timing* drift [97, 100]. The accuracy of the sleep/RTC oscillator is not specified by 3GPP; its type and ppm rating are an implementation choice by the module/device manufacturer (XO, TCXO, or MEMS), and therefore vary across products [23, 98, 99]. However, the frequency offset of such XOs can present inefficiencies in the network acquisition procedures. This effect can be easily observed in scenarios with poor network coverage. In extreme cases, a significant portion of an NB-IoT device's power is expended during cell selection and connection procedures. The frequency offset of an AT-cut XO is temperature-dependent, and as the temperature varies, the frequency offset can drift significantly [97].

Compensation Mechanisms: To address the frequency offset challenge, several compensation mechanisms have been proposed. One approach is to use a Temperature Compensated XO (TCXO). This oscillator is used in precision applications due to its relatively high cost and power consumption. On-chip compensation methods, such as using a switched-capacitor array or a digital-to-analogue converter (DAC), have also been explored [97]. An alternative method involves utilising a high-resolution fractional-N PLL (FPLL) in the frequency synthesiser of the NB-IoT UE. By leveraging the existing FPLL, the device can offset its reference with minimal overhead [97]. Furthermore, a Temperature-Compensated Fractional-N PLL (TC-

PLL) can yield even better results in addressing the temperature-dependent frequency offset of low-cost AT-cut XOs. The TCPLL uses a control logic that translates the temperature offset into a corresponding FPLL compensation offset. This functions as a frequency demodulator, counteracting the modulation effect of a varying reference frequency. The TCPLL prototype demonstrates remarkable accuracy across the industrial temperature range, enabling energy-efficient, low-latency network acquisition and data transfer even in conditions of poor network coverage. [97].

Network Acquisition and Frequency Offset: After waking up from deep sleep, an NB-IoT device needs to synchronise in time and frequency with the eNodeB. The device's initial frequency offset significantly affects the duration of this network acquisition. At the edge of the network, an accurate reference can expedite acquisition, while a high initial frequency offset can prolong it. After the device compensates for its frequency offset, any remaining offset can be detected and further adjusted at the base station eNodeB. A smaller residual frequency offset ensures more energy-efficient communication, especially under low network coverage [97].

In conclusion, clock drift raises substantial challenges in IoT systems, impacting communication and synchronisation. When designing IoT applications, it is important to understand what causes clock drift, what its effects are, and what measures can be taken to minimise these shortcomings.

2.6 Interference

2.6.1 Overview of Interference in Wireless Networks

Interference is one of the main obstacles faced in the operation of wireless systems, degrading the coverage and capacity of communication systems. Today, as wireless systems continue to proliferate worldwide, the interference problem becomes critical for the designers and service providers of these systems as it reduces the throughput of both new and existing systems [101]. One of the main causes of interference is that multiple wireless networks coexist in the same geographical area, leading to a complex interference environment where the signal coming from the transmitter (desired) is superposed with a signal coming from another transmitter (interfering) at the receiver [102].

Interference can be classified into different categories, such as narrowband interference, wideband interference, multipath interference and adjacent channel interference. Narrowband interference refers to signals that occupy a smaller frequency space, which disrupts communication done with a specific channel of a network but doesn't completely result in a Denial of Service (DoS) for an entire band. Haider et al. [102] explain that narrowband signals are usually of high amplitude and corrupt frames by forcing retransmissions. In contrast, wideband interference disrupts communication across the entire frequency band. An example of wideband interference is a wideband jammer that can completely block a band, like the 2.4 GHz ISM band. Multipath interference is when signals traverse a variety of paths to reach the receiver to produce Inter Symbol Interference (ISI) due to the time delays between the first and the reflected signal. It can cause channel degradation, resulting in data corruption and forcing retransmissions. Adjacent channel interference is caused by having overlapping frequency spaces due to poor channel reuse design. Therefore, performance across adjacent channels is reduced [102].

In wireless networks, interference has a direct proportionality with the Quality of Service (QoS), such as reduced throughput, high latency and degraded user experience. For example, in wireless local area networks (WLANs), such as Bluetooth and Wi-Fi, interference can prevent a radio from being able to transmit, which consequently causes delays and retransmissions, thereby further decreasing the throughput of the network [102]. In wireless sensor networks, the interference range (the region where a receiving node can mask a node sending a signal) has a direct effect on the throughput, thus leading to potential outages [102]. This impact highlights the importance of the interference effect in managing its acceptable level. Therefore avoiding disastrous outcomes for the network and its behaviour as well as the device's functionality.

2.6.2 Interference in LPWAN Technologies

LPWAN technologies, such as LoRa and SigFox, applicable over unlicensed bands, are particularly prone to interference from a variety of sources. However, most interference issues arise from their duty cycle access. As the number of connected devices grows, so does the probability that these will interfere with each other. Measurements made by Lauridsen et al. [103] in

the European 868 MHz ISM band show that the probability of finding an interfering signal above -105 dBm is at 22-33 per cent in urban areas, which reduces the coverage and the capacity of LoRa and SigFox networks.

Interference measurements from Northern Denmark showed that LP-WANs were significantly affected in shopping districts and business parks. While the probability of interference was less than 3 per cent in some cases, urban environments, in general, pose more of a challenge. Lauridsen et al. conclude that careful installation and deployment are necessary to avoid and minimise interference [104].

2.6.3 Interference Management in NB-IoT

Narrowband IoT is a latency-tolerant cellular technology that supports massive machine-type communication where thousands of devices send and receive small packets of information. The majority of data packets in the NB-IoT network introduce narrowband interference (NBI) to other traditional broadband systems such as LTE. [105] The key to the successful coexistence of the telecommunications protocols lies in managing NBI. The interference can be managed using either conventional techniques or the recently emerging theory of sparse recovery. The conventional techniques often have data loss or require a priori knowledge of the characteristics of NBI, while the sparse recovery techniques exploit the sparsity of NBI to estimate it more precisely [25]. In 2019, Liu et al. [25] introduced a sparse machine learning-based framework that tackles the problem of estimating NBI accurately while mitigating the interference to the LTE system caused by NB-IoT.

Sparse cross-entropy minimisation (SCEM) and regularisation of the loss function are techniques that help make the recovery more accurate and faster when NBI is present [25]. SCEM exploits the spatial correlation of NBI, and it can be generalised to multiple-input multiple-output systems to help mitigate interference in the NB-IoT deployment.

In summary, interference will continue to be a significant issue for wireless networks, particularly for emerging technologies such as LPWAN, including licensed ones. Understanding what interference is, how it occurs and how to mitigate it are key steps in helping network operators provide better communication services in the most densely packed frequency bands.

2.7 Security Concerns in IoT

2.7.1 Overview of IoT Security Concerns

IoT introduces a range of security issues due to its scale, diverse nature and interconnectedness. Ensuring the security of setups, particularly on a broad scale, is vital for maintaining these connected systems' dependability, privacy and functionality. This section outlines the security challenges encountered in IoT and explains why safeguarding ample deployments is crucial.

Resource Constraints

IoT devices often come with restricted processing capabilities, memory capacity and battery life. This makes it challenging to implement computationally intensive security measures. For example, advanced encryption algorithms might consume power or processing resources, which is a significant concern for devices running on batteries. Sisinni et al. (2018) point out that resource constraints present an obstacle in establishing security protocols in IoT devices [106].

Physical Access

IoT devices are commonly placed in environments where attackers can physically access them, increasing the risk of attacks such as tempering. This susceptibility underscores the need for physical security measures; however, implementing and managing measures across widespread deployments can be challenging [106].

Network Security

When it comes to IoT devices, they often use wireless networks for communication, making them vulnerable to various attacks such as eavesdropping, spoofing and denial of service. Securing these communications is complex due to the diverse communication protocols in use and the limited resources of the devices [107].

Software Vulnerabilities

IoT devices commonly operate on embedded operating systems that may have areas and vulnerabilities that attackers can exploit. Zhang et al. report that these vulnerabilities can arise from a lack of updates, inadequate testing during development, and outdated software [108].

Data Privacy

When considering the holistic picture of the IoT ecosystem, vast amounts of data are gathered and transmitted, including personal information, which is crucial to safeguard from unauthorised access. Protecting data privacy requires securing data at rest and in transit, enforcing access controls, and using anonymisation techniques where necessary [109].

Authentication and Authorization

One of the challenges is ensuring that only authorised entities can access and interact with IoT devices and their data. This involves verifying identities and granting privileges. This task is made more complex when dealing with a large number of devices and use cases [108].

Identity Management

Each IoT device must be uniquely identified, and these IDs have to be managed securely during the lifecycle of devices in order to build trust and control. Good identity management systems must be scalable and adaptive to the dynamic nature of IoT environments [106].

Data Integrity

The transmitted and stored data must remain accurate and uncompromised to have confidence in the system. Mechanisms to check and ensure data integrity are needed to prevent malicious alterations that can lead to bad decisions or system failures.[109]

Interoperability

The diversity of protocols and standards of device use can pose a challenge in implementing security measures across the ecosystem. Achieving inter-

operability while upholding security standards requires collaboration and standardisation among stakeholders [106].

In summary, IoT security poses unique challenges due to its diverse nature and environmental constraints. The lack of standardisation, limited processing capabilities, energy restrictions, cost limitations, fast development, and adoption rates contribute to a complex security landscape that requires multifaceted approaches. As IoT continues to expand, addressing these security concerns will be vital in ensuring the reliability, privacy, and overall trustworthiness of IoT systems.

2.7.2 Security in Large-Scale IoT Deployments

Security becomes a more pressing concern in large-scale IoT deployments as it is paramount to ensure privacy and reliability. First, large-scale IoT deployments increase the attack surface. The more connected devices, the larger the attack surface and the more possible targets attackers have. Since each device might be integrated into many different systems, the potential attack targets provide numerous entry points for attackers [107]. Moreover, the complexity of managing so many devices and their dependencies increases the exposure, making many IoT devices vulnerable to compromise, especially in large networks [107].

Second, connected devices in large-scale IoT deployments are often prone to interdependence. Many IoT devices rely on each other to function. Compromising one device sometimes means compromising other devices. For example, one self-driving car may depend on another car on the road or a nearby streetlight to function properly. If one car is compromised, so is the other and the whole system, potentially [107]. Hence, robust security measures need to be in place so that the failure of a single device does not cause widespread system failures.

Third, large-scale IoT deployments are particularly sensitive to data. In any large-scale IoT deployment, financial and personal data might be exchanged. Some of these deployments, such as medical services, can be life-threatening and have extreme consequences. Security breaches in these deployments can result in leaked personal data and revenue loss, potentially leading to legal issues [109]. Since many deployments handle discreet data, it is crucial to prevent data leaking and ensure its integrity [107]. For instance, ensuring a connected health-monitoring system is secure is vital so patients

can trust the information being collected and analysed by their doctor.

Fourth, large-scale IoT deployments can be critical to vital infrastructure such as power grids and transportation networks. Securing these deployments is essential because they are vital to daily business operations. For example, if a smart grid is not secure, it could interrupt the power supply for thousands of users or even entire cities. This large-scale downtime could cause disruption and loss of money if the service is unavailable. The potential for widespread downtime clearly highlights the urgency of robust security strategies. This is particularly important for physical entities such as power grids, transportation and emergency systems due to the high risks associated with their operation[107].

Addressing these challenges requires a multifaceted approach involving robust security mechanisms, continuous monitoring, and cooperation of all individuals and institutions involved in large-scale IoT ecosystems.

2.7.3 IoT Cyberattacks

In this section, we will review several types of cyberattacks that are specifically directed towards IoT vulnerabilities. Given the extensive IoT ecosystem, which consists of numerous devices, networks, protocols, and software, it is worth mentioning that not all IoT devices are susceptible to the following cyberattacks.

Attacks Against Confidentiality and Integrity

Cloning of Things is an attack in which an untrusted manufacturer duplicates a device's physical characteristics, firmware or security configuration to introduce a backdoor, compromising the device. The malicious substitution involves the replacement of a legitimate device with a lower-quality variant at the time of installation, compromising the integrity and functionality provided by the device. Firmware replacement occurs when an attacker swaps the entire embedded image (e.g., via OTA or during maintenance through service interfaces); this is equally applicable in IIoT, where periodic servicing and long device lifetimes increase the attack surface [110, 111]. In contrast, firmware modification does not replace the image; it selectively alters code or state (e.g., small patches, code injection, or key/config changes) to achieve the attacker's goal [111]. The extraction of security parameters

happens when an attacker leverages physical access to a device in order to extract sensitive information (e.g., a cryptographic key, IMEI, SIM card credentials) to compromise its confidentiality [110].

Eavesdropping and man-in-the-middle attacks are threats to confidentiality in passive and active ways. Eavesdropping is the passive attack of a communication channel in order to extract confidential data silently [110, 112] In this case, a bad actor obtains information by just listening to the data exchange between legitimate parties. In contrast, a man-in-the-middle attack consists of a malicious agent intercepting, forwarding, and potentially manipulating the communication between two parties, therefore compromising the confidentiality and the integrity of the dataset between a source and a destination [110].

Moreover, IoT components such as edge nodes (sensors, actuators or gateways) are targeted in order to launch more attacks against third parties. Invading their confidentiality and integrity is based on the victim/target scenario [113]. The critical factor of this type of attack is that it disrupts the integrity of commands and information collected from sensors, which can be crucial and disruptive for several applications [113]. A data integrity attack aims to disrupt the process or system output by changing the state from a benign to a compromised or more aggressive state. For example, false data injection (FDI) attacks manipulate data by injecting it into sensors in various ways. This interferes with autonomous control in smart devices by providing false information, therefore fooling a system and misleading processes [111].

Attacks Against Availability and Network Operation

Attacks against the network availability are meant to disrupt the operation of services. This type of attack usually blocks communication between legitimate parties and often represents a gateway to finding other exploits. The following is an enumeration of several types of cyber attacks that can disrupt availability and network operations.

DoS attacks try to disrupt the operation of devices or systems by overcrowding the network with requests or false data [113]. Routing attacks attempt to exploit routing information to create potential loops, attract or repel traffic, or modify source routes, therefore bypassing the attached system and compromising the operation of the network, potentially leading to

data loss or service denial [110]. Packet fragmentation attacks, opportune for Routing Protocol in Low-Power and Lossy Networks (RPL), abuse the fragmented packets to impact its routing process [110]. Rank attacks manipulate the rank of an already-connected node to its own advantage [110]. In contrast, masquerading attacks refer to the acts of the attacker impersonating a trusted device, which would disrupt the network operations or gain access to sensitive information [112]. Device capture attacks involve gaining physical control of devices to access or modify sensitive data without authorisation, violating both availability and integrity [111]. Sybil attacks create fake identities to manipulate the network's topology or disrupt communication, violating network operation [111]. Sinkhole attacks divert network traffic to a malicious node to potentially leak or destroy sensitive data or disrupt the network [111, 110].

General Vulnerabilities and Challenges

There are several general vulnerabilities and challenges of IoT systems. The heterogeneous nature, large scale, and resource limitation of IoT increase security risks and pose a significant threat. These factors make privacy enforcement particularly challenging, as it often depends on traditional methods that have proven ineffective [114].

Sicari et al. and Neshenko et al. [111, 114] emphasise the importance of good practices when it comes to IoT coding, setup or utilisation. Simple solutions, such as port management or logging, can minimise the effect of an attack or even prevent it. Below, we enumerate some of the most common vulnerabilities found in the IoT ecosystem:

- Lack of access control allows the attacker to harvest weak credentials management.
- Lack of patch management allows for exploitation based on out-of-date firmware, emphasising the importance of timely security updates.
- Weak programming practices such as the use of backdoors or plain-text passwords underscore the importance of secure coding practices.
- Inadequate audit mechanisms allow the attacker to conceal actions, as no logging mechanisms are present.

- Lack of appropriate authentication allows the unauthorised access or manipulation of communications
- Inappropriate port control provides entry points for the attacker to access your devices

Massive IoT, 5G/6G and the security underlay

In 3GPP, NB-IoT and Long Term Evolution for Machines (LTE-M) form the massive Machine-Type Communications (mMTC) family. They run on the 5G System (5GS) (and legacy Evolved Packet System (EPS)) to connect very large device populations at low cost and low energy per UE [115, 116, 117]. Looking ahead, 6G research targets more scale, tighter Artificial Intelligence (AI) and edge integration, and non-terrestrial extensions. This increases the need for strong at-scale device identity, runtime integrity verification, and zero-touch lifecycle management [118, 119, 120, 121].

Security enablers in the network.

- *Network Slicing (NS) (5G).* Slices provide logical isolation and per-slice policy, binding NB-IoT/LTE-M traffic to dedicated control/user-plane functions and security (AAA, keys, telemetry) per tenant/use case [116, 122, 123].
- *Non-Public Network (NPN) (private 5G).* Enterprises/utilities deploy local 5GS with on-prem User Plane Function (UPF) and dedicated Access Point Names (APNs)/policies for IoT fleets, improving containment, compliance and local breakout [115, 124].
- *Edge (Multi-access Edge Computing (MEC)).* Hosting security functions (protocol brokers, anomaly detection, key custodians) at the access/Radio Access Network (RAN) edge reduces latency and limits data exposure [125].

Information Technology (IT)/ Operational Technology (OT) convergence and deployment strata. In large IoT deployments, enterprise IT (business applications, cloud services) and industrial OT (control and safety systems) coexist but must be treated as separate security domains. A practical baseline is to (i) segment by criticality into zones with controlled conduits, (ii) terminate field traffic at a broker/ gateway

Deployment stratum	**Typical objectives**	**Security controls**	**Access technologies & 6G/edge enablers**
Consumer IoT (CIoT)	Cost, ease of use, broad coverage	Cloud-managed, best-effort; app-layer crypto; basic Network Access Control (NAC)	LoRa, Sigfox, Wireless Local Area Network (WLAN); NB-IoT for metering; public Mobile Network Operator (MNO) cores
Enterprise IoT (IT)	Facilities/asset telemetry; fleet mgmt.	Identity/NAC, micro-segmentation, SIEM/SOAR; policy via Software-Defined Networking (SDN)	WLAN/Ethernet; NB-IoT/LTE-M via MNO; campus SDN; edge gateways
IIoT / OT	Safety, determinism, uptime; IEC 62443 compliance	Zones/conduits, strict change control, real-time monitoring/SOC	Private LTE/5G; TSN Ethernet; MEC; QoS scheduling; local processing
CNI	National-service resilience; assured QoS/Service-Level Agreement (SLA); survivability	Strong isolation, dual-homing, HW roots of trust, rigorous SOC/audit	Private 4G/5G with NS; hardened 5G Core (5GC) (UPF on-prem); MEC; URLLC for protection

Table 2.2: Stratification of IoT deployments (CIoT, enterprise IT, IIoT/OT, CNI) by objectives, security controls, and suitable access technologies/edge enablers.

layer placed at the IT/OT boundary, and (iii) align controls with sector frameworks (NIST SP 800-82 for Industrial Control Systems; IEC 62443 for industrial automation) [126, 127]. Table 2.2 summarises how these strata map to objectives, security controls, and suitable access/edge enablers. In practice, NB-IoT is used for monitoring/telemetry in OT/CNI, while time-critical closed-loop control prefers deterministic links such as Time-Sensitive Networking (TSN) Ethernet or Ultra-Reliable Low-Latency Communications (URLLC) in private 5G.

2.7.4 NB-IoT Security Concerns

The NB-IoT security trajectory suffers from distinctive and unique challenges due to its goals such as low cost, low power consumption, limited resources and designed for long battery life. This results in NB-IoT devices offering a wide attack surface, making them vulnerable to several cyberattacks. This section presents a literature review on the nature of security threats faced by NB-IoT.

Security challenges for NB-IoT

NB-IoT devices have limited processing power and memory due to their small size and rigorous requirements. As a result, they can't accommodate complex security protocols like those based on strong encryption algorithms or sophisticated cryptographic protocols. According to Jha et al. and Lin et al., [128, 129], the limited resources in terms of processing power and energy expenditure hinder the utilisation of powerful encryption methods. A further emphasis on energy efficiency in NB-IoT devices drove Tengshe et al. to speculate that the benefit of extending battery life ultimately prioritises weaker security protocols, thereby making systems more vulnerable. [130].

Furthermore, the narrowband nature of NB-IoT (single 180 kHz carrier with low data rates and high latency) limits message size and frequency, making heavyweight security protocols, such as full TLS/DTLS with certificate exchanges and revocation checks, IPsec/IKEv2 key negotiations, or frequent asymmetric rekeying, impractical without adaptation. Lin et al. and Coman et al. highlight that this limitation affects the ability to effectively encrypt and authenticate data [129, 131]. Even though NB-IoT inherits the security aspect of LTE, Kumar et al. argue that the lack of NB-IoT security standardisation might lead to exploitable vulnerabilities. [17]. Additionally, the 3GPP goal of high device density and massive deployments exposes the protocol to widespread attacks, according to Coman et al. and Tengshe et al. [131, 130].

NB-IoT is regarded as a highly secured network compared to other LPWAN protocols. However, devices are often deployed in remote or unattended locations, exposing UEs to a variety of physical and physical-proximate threats. Examples include device tampering or theft, invasive probing and side-channel attacks (such as power analysis), unauthorized hardware modification or replacement, and local interference methods like jamming or spoofed signalling that require attacker proximity [129]. Taken together with the other challenges, the security landscape for NB-IoT is both challenging and complex.

NB-IoT Cyberattack Examples

A malicious entity can compromise a UE to retrieve sensitive user information, either by infecting the device with malware or by data leakage.

Tengshe et al. [130] note that inadequate and poor security measurement poses a significant threat in some NB-IoT implementations. Furthermore, similar to other LPWAN networks, NB-IoT is vulnerable to DoS attacks. Tengshe et al. and Kumar et al. stated that the NB-IoT network can be flooded with malicious requests. Such an attack could undermine access to essential services that depend on NB-IoT connectivity [130, 17].

A particularly high-risk attack vector for NB-IoT is Man in the Middle Attack (MITM). In this case, the attacker intercepts data between UEs and the eNodeB, stealing or modifying critical information while staying undetected. Kumar et al. illustrate how an NB-IoT device can be attacked by using a MITM method [17]. In such attacks, the malicious entity positions itself between the targeted UE and the eNodeB and replaces messages along the way, removing security checks while inserting its own code or placing messages in an incorrect order to impersonate receivers and disrupt IoT services. This attack shows that, even with a private key provided by the SIM card and proper device configuration referring to the SIM-allows list, incoming requests could be falsified. Coman et al. and Mlongeni et al. detailed how such advanced attacks necessitate a better association between the end device and the network [131, 132].

MITM walk-through. Consider a smart water-meter UE that reports once per hour over NB-IoT. An adversary deploys a rogue eNodeB on the same Public Land Mobile Network (PLMN), slightly higher power, favourable E-UTRA Absolute Radio Frequency Channel Number (EARFCN), so the UE prefers it. The attacker then *relays* signalling to the legitimate network (RF or backhaul relay) so that normal Authentication and Key Agreement (AKA) runs with the real core and security keys are established as per 3GPP EPS security [50]. From that point on, Non-Access Stratum (NAS) and RRC are integrity-protected (and typically ciphered), so the in-path device cannot read or modify protected messages, but it can still *forward, delay or drop* them while pretending to be the serving eNodeB [131, 129, 17]. In practice, the sequence is:

1. *Cell selection:* the UE camps on the rogue eNodeB (same PLMN, suitable EARFCN/priority).

2. *Pre-auth relay:* initial RRC and NAS requests (unprotected before security activation) are relayed so AKA with the real Mobility Man-

agement Entity (MME) completes [50].

3. *Post-auth forwarding:* once Access Stratum (AS)/NAS security is active, the attacker operates as a *forward-only* in-path node: cannot decrypt or alter protected payloads, but can pass, delay or drop frames selectively [131, 17].

What a MITM enables (even after authentication):

- *Traffic analysis (metadata only).* Observe timings, message sizes, attach/TAU periodicity and paging activity to infer device behaviour and reporting schedules without decrypting content [131, 129].
- *Selective DoS / energy drain.* Drop or delay specific RRC/NAS messages (e.g., RRC reconfiguration completions, service requests), forcing retransmissions and re-attachments, raising UE energy use [131, 17].
- *Uplink starvation.* As the apparent serving eNodeB, starve the UE of uplink grants/scheduling so reports time out or back-off, degrading availability (content still protected) [131].
- *Targeted downlink loss.* Withhold forwarded paging or downlink transfers so the UE never receives application commands/ACKs—impacting QoS without breaking confidentiality [129].
- *Timed disruption of initial access.* During future re-attachments, exploit the short pre-security window (e.g., inject or replay early control messages) to force delays or RAT reselections before protection is re-enabled [50, 17].

What a MITM cannot do (without key compromise). It cannot decrypt NAS/RRC or user-plane payloads, cannot forge integrity-protected messages, and cannot impersonate the subscriber, because session keys are derived from AKA secrets held in the Universal Subscriber Identity Module (USIM)/core [50].

Existing security measures in NB-IoT

Existing NB-IoT security measures focus mainly on confidentiality and integrity. Following this, we will provide an account of these based on the relevant literature and current standards.

Authentication and Key Management: All NB-IoT communications require the device to be authenticated by the network through the Generalised Bootstrapping Architecture (Generalised Bootstrapping Architecture (GBA)) mechanism. The GBA mechanism is based on the Authentication and Key Agreement (AKA) protocol, which allows the device and the network to generate a session key in a secure way. The session key depends on a unique identity stored in the SIM card and a secret key used for authentication or key agreement. To further ensure that the device can only be registered under the SIM card, a logical binding is used, which stores the relationship between the device's serial number (IMEI), the SIM card's IMSI, and its Mobile Station International Subscriber Directory Number (MSISDN). This helps the network avoid unauthorised and illegal use of the device by other entities. [129]. However, it is noted in the research conducted by Lin et al. that these registered relationships can be easily intercepted [129].

Secure Communication: NB-IoT employs standardized cryptographic algorithms, including SNOW 3G stream cipher (SNOW3G) (128-bit stream cipher), Advanced Encryption Standard (AES) (128-bit block cipher), and ZUC stream cipher (ZUC) (128-bit stream cipher), for protection of Radio Resource Control (RRC) and Non-Access Stratum (NAS) signaling. These provide confidentiality, integrity, and replay protection between the device, eNodeB, and MME. For higher-assurance application scenarios such as smart-grid gateways, NB-IoT link-layer security can be augmented with tamper-resistant secure elements to establish a hardware root of trust[133]. These modules support strong mutual authentication, key protection, and end-to-end encryption and are typically backed by a Public Key Infrastructure (PKI)/Certification Authority (CA) infrastructure. Such layered deployments increase operational complexity, as noted by Lin et al. [129].

Inheritance from LTE (secure by design) NB-IoT (Rel-13/14) and LTE-M (Cat-M1/M2) directly reuse the LTE/EPS security architecture [50]: mutual authentication and key derivation via EPS-AKA; derivation of session keys (e.g., $K_{\text{ASME}} \rightarrow K_{\text{NASenc}}/K_{\text{NASint}}, K_{\text{RRCenc}}/K_{\text{RRCint}}, K_{\text{UPenc}}$); integrity and ciphering of NAS/RRC with the aforementioned 128-bit SNOW3G/ AES/ ZUC; replay protection; and operator-managed USIM credentials. For C-IoT-Opt, control-plane data over NAS remains protected by the same NAS security, while user-plane optimisation still relies on the EPS key hi-

erarchy. This inheritance underpins the "secure-by-design" characterisation of cellular IoT in the literature [31, 129].

Other security measures: NB-IoT also utilises other security measures, which enhance data integrity. Data integrity protection mechanisms, such as integrity protection keys and integrity check codes (ICC), ensure the reliability of data from the source to the destination without tampering, making sure that the data is not corrupted or tampered with along the transmission channel [134].

2.8 Battery Depletion Attacks

Battery depletion attacks, also known as Energy Depletion Attack (EDA) or Vampire attacks, are exploits used by malicious entities to force a battery power device (mainly IoT devices) to exhaust its energy resources. The damage resulting from such attacks can be severe, ranging from end nodes shutting down and becoming inoperative to increasing maintenance costs and causing operational delays. The consequences of battery-draining attacks are particularly serious in IoT applications, as the small physical size of transceiver modules often limits the reserve power of individual nodes. Notably, perpetrating such attacks usually does not require a high level of technical skill and does not necessitate expensive tools [135]. The attack vectors for battery depletion can be multiple, including flooding with unnecessary control traffic to prevent low-power sleep modes, manipulating communication protocols to increase energy consumption, and attacking the target's hardware and/or software. For instance, Bhattasali et al. [136] describe attacks that force the nodes to stay active as a central part of a wider sleep deprivation attack. Employing such a technique, adversaries can forcefully exhaust the battery of a victim network within several hours.

2.8.1 Existing Research on Battery Depletion Attacks

Battery depletion attacks are well-documented across IoT technologies. Research has shown that these attacks can drastically reduce the useful lifetime of IoT devices, with some studies, such as Cao and Nguyen, focusing on protocols like ZigBee and Bluetooth Low Energy in their work [137, 15]. An early study by Khouzani in 2011 analysed the dynamics of malware in mobile sensor networks, demonstrating that an attacker can cause optimal harm by

thoughtfully managing the infected nodes in relation to their energy consumption [138]. Existing research on battery depletion attacks concludes that such attacks can be achieved in various ways, including through the manipulation of duty-cycling and interference-based methods. Studies often rely on simulation and mathematical modelling to derive conclusions on attack vectors, and their effects [138, 15]. One such model would be to utilise Pontryagin's maximum principle that can be used in optimising strategies for attacking mobile sensor networks [138]

2.8.2 Interference-Based Battery Depletion Attacks

Interference-based battery depletion attacks are executed by injecting noise or jamming signals into the communication channels of wireless devices. Faced with such interference on their channels, devices often require increased energy consumption to maintain normal communication. A comparative overview of attack vectors and measured battery effects is provided in Table 2.3.

These attacks can degrade network performance and drain batteries extremely fast, leading to device failure [137, 15]. Interference-based attacks can be executed through the broadcast of excessive control messages, manipulation of MAC protocol parameters, and use of jamming devices to disrupt normal communication. Tools for executing such attacks range from simple scripts to more sophisticated hardware setups that can be used to generate interference. Some examples of tools for executing these attacks can be found in the research of Cao et al. and Nguyen et al. [137, 15]. Countering battery depletion, especially from interference, requires robust anomaly detection, resilient protocols, and energy-efficient routing. For instance, Bhattasali et al. [136] proposed a hierarchical framework that can be used to detect sleep deprivation attacks, but such techniques can also be extended to detect interference-based attacks. Furthermore, Gabriela et al. utilised the UEs available data as an indirect interference measurement [21]. Additionally, techniques such as frequency hopping and spread spectrum can also mitigate the impact of jamming and interference [137, 15].

In summary, battery depletion attacks have a significant impact on IoT devices by restricting their functionality and reducing their lifespan. Ongoing research continues to identify effective approaches that can be used for the detection of these attacks, as well as strategies to mitigate their results.

Study	Attack vector / method	Key findings / impact on battery
Cao *et al.* (2016)[137]	Ghost attack on ZigBee networks – crafted frames that trigger MAC-layer security checks and excessive processing/retransmissions.	Severe energy depletion: legitimate nodes perform superfluous computations and retries; device lifetime drops from years to days under sustained attack.
Nguyen *et al.* (2019)[15]	Survey of jamming and protocol-abuse EDAs – physical-layer noise injection/hidden-channel signalling; MAC-layer overload (excess control, duty-cycle manipulation).	Defines Energy Depletion Attacks and shows intentional interference can rapidly drain node energy; cross-layer taxonomy highlights significant battery drain even without full DoS.
Bhattasali *et al.* (2012)[136]	Sleep deprivation (denial-of-sleep) in WSNs – adversary keeps nodes awake via frequent requests/dummy traffic.	Identifies denial-of-sleep as a high-impact battery-drain vector that maximises power draw and minimises node lifetime; introduces a hierarchical detection framework.
Morillo *et al.* (2023)[21]	Targeted NB-IoT interference – selective jamming of downlink/control signalling causing repeated retries without total outage.	Experimental NB-IoT results: retries induced by targeted interference markedly accelerate battery drain; estimated lifetime can drop from ∼17 years to months; UE-side metrics used as indirect interference indicators.
Ruotsalainen *et al.* (2022)[139]	LoRaWAN physical-layer attacks including jamming/DoS that raise device current draw and retransmissions.	Shows that PHY-level interference drastically increases consumption and reduces lifetime of constrained LoRaWAN nodes (DoS → battery depletion).
Šabić *et al.* (2025)[140]	Practical reactive jamming on LoRa using COTS SDR; short bursts timed to frames.	Reactive jamming disrupts frames with minimal jammer airtime, inducing repeated transmissions and higher energy use in end devices.
Dosa *et al.* (2025)[141]	Reactive jamming on LoRaWAN (theory + experiments) including repeated-symbol jamming.	Shows small jamming windows can severely cut frame success rates, driving retries/on-air time and thus battery drain in LPWAN nodes.
Shakhov *et al.* (2018)[142]	WSN depletion-of-battery model including jamming/interference as a drain vector.	Formalises depletion attacks; highlights that jamming/interference (intentional or "accidental") escalates energy use and shortens node lifetime.
Osanaiye *et al.* (2018)[143]	Jamming in WSNs as DoS with resource (battery) exhaustion effects.	Notes that malicious signals directed at sensor channels deplete node resources (energy) even without permanent denial, via repeated access/retransmissions.

Table 2.3: Key studies on interference-based battery depletion attacks in wireless IoT networks

Chapter 3

Design and Methodology

Emerging sensing applications increasingly employ LPWAN for their communication requirement [47]. Technologies such as LoRaWAN and NB-IoT offer unique advantages to this domain, ranging from low power consumption to deep indoor coverage and high connection density [47, 144]. The novel approach of these telecommunication protocols towards the IoT field unlocks deployments of smart devices in new environments where traditional connectivity methods were previously impossible [47]. This advancement facilitates the integration of IoT solutions in remote or challenging areas, enhancing data collection and automation for the greater scope of resource management and optimisation, but also long-term financial gains [145, 146].

As an example, if we consider a residential water provider upgrading its water meters to IoT-enabled ones, it might seem like a financial burden in the short term. In the medium to long term, it enables the company to predict water consumption at a granular level, therefore allowing for better water pump management, early detection of broken pipes and leakages, and eliminating the need for transportation and human resources solely for meter reading [147]. Additionally, it can facilitate the analysis of water pressure, temperature, and quality, along with other specific use cases where data collection is vital [148]. The data must be transmitted robustly and securely to facilitate all of this. Furthermore, due to the environment where the water meters are deployed (typically underground or deep indoors), the telecommunication technology must operate at the edge of the network with poor signal conditions for an extended period of time [144].

NB-IoT addresses these issues with features such as extended coverage

capabilities and a minimum lifespan of ten years [149]. To achieve this, the communication link between the User Equipment (UE) and the base station has to be dynamically adjusted to the environment. For example, transmission power and the number of repetitions are modified to compensate for link quality fluctuations [150, 151]. These steep requirements and the solutions developed for achieving them allow for an angle of attack where an adversary can interfere with the communication link performing Denial of Service (DoS), Energy Depletion Attack (EDA), Man in the Middle Attack (MITM), replay attacks, and other types of attacks that target the wireless connection [152, 153].

This research focuses on battery depletion attacks, also known as EDA. The goal of a malicious entity is to maximise the victim's energy usage while remaining undetectable [22]. To achieve this, the bad actor needs to (i) understand and adapt to the changes of the NB-IoT protocol, (ii) ensure that communication is still possible, and (iii) ensure that the energy used to disrupt the service is less than the energy exhausted by the User Equipment (UE). Depending on an attack's impact, it can render the smart device commercially infeasible. Simultaneously, these attacks are difficult to detect as they do not interrupt data communication from the User Equipment (UE) and the base station; the attacker is not continuously jamming but meticulously times its activity [27].

3.1 Attack Techniques

IoT security is a multi-faced domain encompassing a wide variety of threats, ranging from data and network security to privacy and regulatory compliance. Device manufacturers, network providers, and other entities involved in the deployment and maintenance of the system must be conscious of these threats and address them. The security of the system is only as strong as its weakest link; therefore, misconfigurations, the inability to update software and social engineering attacks represent the majority of the attacks. Combining all of this with the complexity of a technology such as NB-IoT creates conditions conducive to malicious interference. Moreover, NB-IoT is deployed on existing critical telecommunication infrastructure, making the security aspect particularly concerning.

This research focuses on Energy Depletion Attack (EDA) through inter-

ference. The main goal of the attacker is to maximise the energy expenditure of a targeted device while remaining undetected. This can be achieved with the help of jamming devices or fake base stations.

Three different devices are considered for our tests: *simple jammer*, *Message Jamming (MJ)* or Intelligent Jammer, and *Message Injection (MI)*, as presented in Table 3.1 and detailed in the following sub-chapters.

Device (as used here)	**Signal type / bandwidth**	**Timing / procedure**	**Intended effect**
Simple jammer	Noise-like interference (wideband to cover hopping or narrowband over NB-IoT carrier); constant or partial-band; no protocol structure	Unscheduled /unsynchronized; continuous or duty-cycled transmission; "all-in-one" wideband jamming to defeat frequency hopping [154, 155]	Raise noise floor to increase BLER, repetitions and UE TX power while keeping service up; easily detectable; high attacker energy cost for battery devices [22, 27]
Message Jamming (MJ) (intelligent jammer)	Short noise bursts aligned to targeted NB-IoT channels/messages (NPUSCH, NPRACH, NPDCCH); narrowband on active resources	Reactive/pulsed; synchronized by decoding unencrypted NPSS /NSSS /NRS /MIB-NB /SIB1-NB /SIB2-NB; repeated for each configured repetition	Keep UE out of sleep and inflate resource allocation (repetitions/monitoring/TX power) while remaining stealthier and more energy-efficient than constant jamming [22, 27]
Message Injection (MI)	Structurally valid overshadowing message (capture effect) replacing the first CSB/SIB subframe and its repetitions	Protocol-aware, time-synchronized injection just before the legitimate transmission; minimal airtime/power	Force CRC failure and UE reacquisition of the whole sequence (resource exhaustion); appears legitimate and is hard to detect [156, 157, 158]

Table 3.1: Adversary device classes considered in our evaluation

3.1.1 Simple Jamming Technique

One of the easiest ways to disrupt a wireless network connectivity flow is to output an interference signal on the same frequency as the entities involved in the data transfer. To achieve this, a malicious entity can employ

a device capable of emitting interference signals, thus performing a DoS attack. When it comes to the licence spectrum, this attack type is not as efficient as it can easily be detected. It can be counteracted by either physically removing the adversary device or by changing the frequency. For our use case, the device goal is to force the UE and the eNodeB to exhaust more resources than needed while remaining undetectable as long as it can [22]. To accomplish this, the simple jammer emits adjustable-power additive white Gaussian noise (AWGN) to raise the noise floor so the UE perceives degraded SNR.

Furthermore, an "all-in-one frequency jammer" is needed to overcome the frequency hopping [154, 155]. With these capabilities, malicious devices will be able to mislead the UE into thinking that its environment is more challenging than it actually is while still enabling communication at a higher cost. Because NB-IoT transmissions are intermittent, a simple jammer must emit jamming signals continuously, which effectively requires a constant power supply. In other words, if the jamming device has a limited power supply (i.e. battery), it will exhaust it by constantly transmitting before creating any relevant damage to the UE. Figure 3.1 (a) captures a simple jamming technique at a high transmission power [27].

3.1.2 Message Jamming Technique

Contrary to simple jamming, a Message Jamming (MJ) utilises complex, protocol-aware devices such as NB-IoT message jammers that burst on specific system messages (e.g., SIB1-NB) [27], synchronisation-aware reactive jammers targeting NPSS/NSSS [159], control-channel jammers aligned to NPDCCH subframes [160], uplink-slot jammers timed to NPRACH / NPUSCH occasions [161], and overshadowing/message-injection platforms that forge valid frames [156, 157, 158]. The device has a good understanding of the protocol and its behaviour. It can acquire and decode unencrypted messages such as slot occupancy, transmission times, synchronisation signals, and other overhead data. This information will enable the jammer to analyse and target specific messages by transmitting noise interference in a burst-like pattern. By corrupting a small subset of symbols within each scheduled occasion, MJ forces HARQ/coverage-repetition retransmissions and prevents entry into eDRX/PSM during the window, increasing both TX retries and RX monitoring time [69, 22]. The MJ attack goal is to

prevent the UE from switching into a sleep state while consuming as little power as possible. Initially, the MJ device will try to acquire as much information about the network as possible [14]. Data such as NRS, NPSS, NSSS, MIB-NB, SIB1-NB, SIB2-NB are all unencrypted and can easily be acquired as described in Section 2.2. Upon decoding the SIB2-NB, the jamming device learns the uplink frequency and is ready to perform an eavesdropping attack. The sole purpose of this initial attack is to understand the targeted device's communication patterns (i.e., every 4 hours). This enables the jammer to target specific communication messages and signals at the right time in a way that both the UE and the eNodeB are forced to increase their resource allocation. Once periodicity is learned, the jammer fires narrowly timed bursts only when the UE is scheduled, maximizing UE energy expenditure while minimizing its own airtime [22, 27]. By still enabling the communication to go through and changing the attacked message and its timing, it makes it very hard for the jammer to be detected. No legitimate party employs any mechanism that will raise suspicion and most likely mislabel it as a natural interference or poor coverage. Figure 3.1 (b) illustrates an MJ instance targeting a SIB1-NB transmission; the same timing-aligned procedure can target other downlink broadcasts (MIB-NB, SIB2-NB) and control occasions (NPDCCH) [68, 69]. In the spectrum, MJ appears as short noise bursts confined to the NB-IoT narrowband. Choosing SIB1-NB rather than MIB-NB/ SIB2-NB mainly alters the burst timing, duration, and repetition count; the narrowband spectral footprint is otherwise essentially unchanged (given the same jammer bandwidth/pulse shaping). The duration of the burst-like interference can be as little as 1 ms but needs to be repeated for every message repetition. While such burst-like jamming can be recognised in spectrograms, reliable automatic detection requires continuous, high-resolution monitoring of the NB-IoT narrowband and protocol-aware classification of short-duration anomalies, an energy-intensive task for battery-powered monitors. Alternatively, an event-triggered detector that arms around known broadcast/control occasions can reduce the monitoring duty cycle [21]. Nevertheless, removing the MJ remains difficult: its low duty cycle and small footprint complicate localisation (e.g., Time Difference of Arrival (TDOA)/Angle of Arrival (AoA)), and field intervention can be cost-prohibitive.

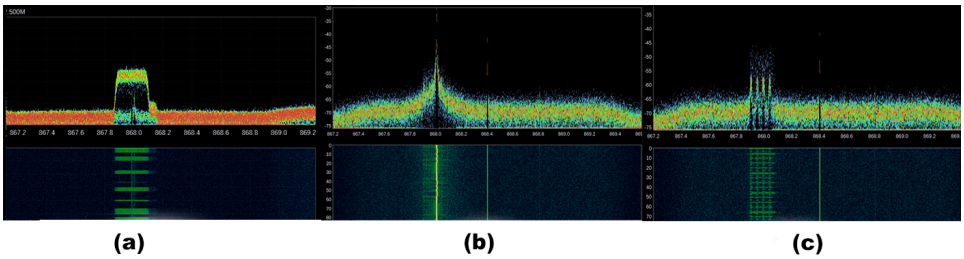


Figure 3.1: Real spectrum capture of a (a) Simple Jamming technique, (b)Message Jamming (MJ) attack and (c) Message Injection (MI) attack, using the SRSRan software and the HackRF One devices.

3.1.3 Message Injection Technique

Message Injection (MI) is similar to MJ when it comes to the knowledge needed and the synchronisation of the attack. Unlike MJ, the MI attack exploits the capture effect, also known as a Physical Signal Overshadowing Attack proven by Yang et al. on the LTE network [156], sending a *structurally valid* downlink block such as an MIB-NB on Narrowband Physical Broadcast Channel (NPBCH) or a SIB1-NB/SIB2-NB transport block on NPDSCH with a correct CRC and the appropriate RNTI (e.g., SI-RNTI), that arrives slightly earlier or at marginally higher power than the legitimate one [68, 69, 156, 157, 158]. than the legitimate one. Similar works, such as those by Kim et al. [157], and Hussain et al. [158], have demonstrated vulnerabilities in LTE. While these studies explore different types of attacks, this research specifically focuses on the aspect of resource exhaustion.

Contrary to MJ, where it targets all the parts of a message, an MI attack can replace only the first CSB or System Information Block (SIB) subframe and their repetitions. Due to the valid structure of the fake message (i.e., a PHY-conformant MIB-NB on NPBCH, or SIB1-NB/SIB2-NB on NPDSCH, with valid CRC/RNTI) [68, 69], the UE will not process further repetitions. Upon receiving all the packets needed for decoding the targeted message, the UE will perform an integrity check by calculating the CRC. This CRC failure is intentional and is the success condition for the attacker, because it forces the UE to reacquire the entire sequence. In other words, the forged block is only used to win capture, the UE then discards it on integrity check but expends extra energy in repeated NPDCCH blind decodes, NPDSCH receptions, and reacquisition, which can be the objective of the attack. When

Attack	**Technique (what/where)**	**UE impact (why it drains energy)**
DQS	Add low-power noise on measurement references (DL NRS; UL NPUSCH/NPRACH refs) to bias RSRP/RSRQ/SINR.	eNB/UE pick worse MCS and more repetitions or single-tone UL → longer Tx/Rx time, higher PTX.
RAP	Jam RAR on NPDSCH; or spoof cell/SIB2-NB to raise repetition and PTX limits.	Repeated RA attempts/backoff or inflated per-attempt energy; added access delay.
MIB-NB	Selective MJ or MI on NPBCH subframe 0 (hit CSB repetitions).	MIB decode fails → re-acquisition loop; prolonged idle listening/decoding.
SIB1-NB	Narrowband MJ/MI on mapped SF4 per configured repetitions.	Missed SIB1 → periodic wake-ups and retries until next period.
SIB2-NB	Narrowband MJ or MI (fake) on mapped subframes across the SI-window.	Extra monitoring across window → more repetitions/PTX.

Table 3.2: Energy-depletion–oriented attacks and their effect on the UE.

compared to MJ, MI utilises less transmission power as it only needs to replace one CSB or subframe and their repetitions. Additionally, as illustrated in Figure 3.1 (c), the injected message is indistinguishable from a valid one, thus making it even harder to detect. A full explanation of the attacks for each targeted message is presented in the following sections 3.2.3, 3.2.4 and 3.2.5.

3.2 Energy Depletion Attacks

In the realm of IoT cybersecurity, energy depletion attacks represent a significant concern due to their potential to incapacitate devices by draining their power resources. These attacks exploit the limited energy reserves of IoT devices, often leveraging techniques that force devices to perform unnecessary operations, leading to premature battery exhaustion. For resource-constrained NB-IoT sensors and meters that operate unattended, where battery charging or access is rare, these attacks can cause prolonged service outages and gaps in reported data. Understanding the mechanisms and implications of energy depletion attacks is crucial for developing robust countermeasures to protect the growing ecosystem of IoT applications.

3.2.1 Degradation of Quality of Signal Attack

Estimating the channel quality, also known as QoS indicators (RSRP/ RSRQ/ SINR), is an important aspect that enables the telecommunication networks to remain robust and efficient. In NB-IoT, 3GPP provides a framework that helps both the UE and eNodeB better understand the environment in which they operate, by specifying what is measured, how it is reported, and how it is used for link adaptation [59]. For a thorough assessment of QoS, both uplink and downlink channels have to be considered. For the downlink channel, the measurement is done with the help of the NRS, from which the UE derives RSRP/RSRQ and SINR and reports them via RRC [59]. For the uplink channel, the Single-Carrier Frequency-Division Multiple Access scheme (SC-FDMA) is employed within a 3.75 kHz or a 15 kHz configuration, and the eNodeB estimates uplink SINR and path loss from NPUSCH demodulation reference symbols and NPRACH preambles, using these measurements to set MCS, repetition numbers, and single versus multi-tone allocation [68, 69]

The goal of this work is to evaluate the ability of a malicious entity to perform a Degradation of Quality of Signal (DQS) attack by adding noise interference to the NB-IoT channel.

By fully understating the implications the MCL has over the NB-IoT protocols' ability to alter the transmission power as well as the number of repetitions, a bad actor can potentially degrade the quality of the signal. Adding any type of noise to all the subframes that carry the NRS on both uplink and downlink channels, the malicious entity can deceive the eNodeB and the UE into a higher coverage level, thus depleting the UEs battery and increasing the number of resources needed for completing the data transfer. Specifically, an NPDSCH broadcast at PTX = 35dBm, having an NF of 7dB with a temperature of T = 290 Kelvin and a bandwidth of 180kHz would result in a PNeff of:

$$\text{PNeff} = 10 * log(k * 290 * 180) + 7dB = -104.4dB \tag{3.1}$$

Additionally, using a SNRmin at -14dB (medium coverage level), we can calculate the MCL as:

$$\text{MCL} = \text{PTX} - \text{PRXmin} \approx 154dB \tag{3.2}$$

This calculation can provide the adversary with the ability to perform an efficient attack by using an intelligent jammer such as the MJ or devices similar to the one used by Roger et al. [162] that can target certain control channels. Furthermore, this type of intrusion will result in the allocation of additional resources in the form of subcarriers, therefore decreasing the maximum bandwidth.

This form of attack does not attempt to disrupt transmission immediately; therefore, the jamming device can use Additive White Gaussian Noise (AWGN), which has statistical properties similar to thermal noise generated by natural electronic processes, [163] making it even more difficult to detect than full jamming. Furthermore, the increase in MCL could be organically caused by changing environmental conditions, minimising suspicion even more.

In summary, to conduct a successful Degradation of Quality of Signal (DQS) attack, the malicious device must estimate the MCL class of the UE and add noise to the communication channels that are being used. This, in turn, will force the eNodeB and the UE to dedicate additional resources, such as increasing repetitions and energy usage.

3.2.2 Random Access Procedure Attack

The Random Access Procedure (RAP) in NB-IoT is a fundamental mechanism that allows UE to communicate with the network. This operation is required for initial access, reestablishing a connection following a loss, or switching from idle to connected state. In NB-IoT, the RAP is optimised to address the particular difficulties of LPWAN networks, such as extended coverage, device density, and power efficiency.

For NB-IoT, the RAP is carried out by the Narrowband Physical Random Access Channel (NPRACH). Even though the protocol inherits most mechanisms from the legacy LTE, the NPRACH has been entirely redesigned [63]. The LTE Physical Random Access Control Channel (PRACH) inhabits a bandwidth of up to 1.05 MHz, which is larger than the whole NB-IoT carrier. NPRACH is using a Single-Tone configuration with a 3.75 kHz subcarrier spacing and has the ability for frequency hopping. It accommodates varying cell sizes by offering two cyclic prefix lengths, using bandwidths ranging from 45 kHz to 180 kHz depending on the number of subcarriers [164]. Furthermore, transmissions can be repeated up to 128 times for in-

creased coverage.

Before initialising the RAP, the UE needs to acquire all the SIBs up to SIB2-NB minimum. Figure 2.7 illustrates a complete RAP procedure, including the information needed for successfully transmitting all the messages.

As previously discussed, NB-IoT introduces a feature called Extended Coverage Level (ECL), which permits the same uplink message to be repeated up to 128 times [165]. Even though this feature enables devices to communicate in areas unreachable beforehand, it makes the RAP vulnerable to EDA for devices that do not need it. By utilising a MJ (see Section 3.1), a bad actor can listen for the first preamble, also known as Random Access Preamble Transmission (Msg1), and then decide which Random Access Response (RAR) transmitted using the NPDSCH to jam. Additionally, a capable MJ, in terms of transmission power, can also deploy a Man in the Middle Attack (MITM) Attack. Acting as a fake base station, the adversary can broadcast synchronisation signals and system information blocks (e.g., SIB2-NB) with higher signal strength than the legitimate cell, thereby forcing the UE to camp on the rogue cell. Once connected, the attacker can transmit modified parameters—such as artificially high repetition values and elevated transmission power settings—causing the UE to consume more energy for each uplink attempt. This exploitation is possible because NB-IoT system information and shared channels are unencrypted, allowing unauthorised modification without triggering integrity checks. For optimisation reasons, 3GPP introduced a new element in release 16 [58] called Preconfigured Uplink Resources (PUR). This pre-configuration allows the UE to bypass Msg1 and Random Access Response (Msg2) in the distinct circumstance where the latency is equal to or greater than 64ms with a 12-tone allocation. It is noteworthy that if both the eNodeB and the UE support this feature, energy consumption will be reduced, and the efficiency of the aforementioned attack will be diminished, though not entirely prevented [166].

In summary, a malicious actor can carry out a RAP attack by intercepting the downlink channel and jamming the RAR. They can monitor the number of repetitions to ensure it stays below the limit set in SIB2-NB, allowing the connection to complete and not raising suspicion. Additionally, an MITM attack can be used to change the maximum transmission count

up to 128. The fake base station can also alter the cell ID, disrupting the PUR settings of the UE [166].

3.2.3 Narrowband Master Information Block Attack

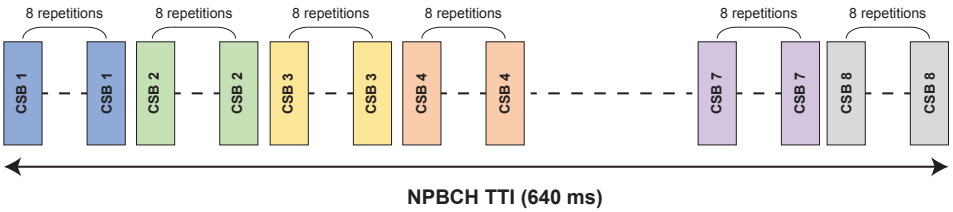


Figure 3.2: Transmission of NPBCH CSBs.

Using the NPBCH, the eNodeB always broadcasts the Narrowband Master Information Block (MIB-NB) in subframe zero in every frame. Its TBS equals 50 bits, which are split into eight CSB after the modulation. As depicted in Figure 3.2, each CSB is repeated eight times, resulting in a Transmission Time Interval (TTI) of 640 ms. The MIB-NB is unencrypted, and its previously mentioned configuration is static, as defined by 3GPP [59]. After receiving all the CSBs and their repetitions, the MIB-NB is demodulated and decoded. From a security point of view, we have identified two types of vulnerabilities that would force the UE to reacquire the MIB-NB and consequently use more resources.

Firstly, by using a MJ, that is able to jam any CSB and its repetitions. To achieve this, the jamming device needs to transmit a signal comparable to Figure 3.1(b) for every subframe that contains the targeted CSB. In simpler terms, it needs to be capable of jamming at least eight subframes zero, with a nine-millisecond split. Due to the fact that the CSBs are not indexed, it is not possible to determine the repetition that they belong to by just observing one of them. To overcome this, the MJ needs to keep track of the CSBs sequence and observe when any adjacent CSB differ, therefore knowing that a new repetition cycle has begun. After waiting for the newly found cycle to finish (80 ms), it can start jamming in the pattern described above. This observing strategy has to be employed only at the beginning of the jamming cycle or in the case the MJ loses the CSB tracking. This technique will result in the UE failing to receive a CSB, therefore being

unable to decode the data.

Secondly, by using a MI device, the attacker can disrupt the acquisition of the MIB-NB, similar to the jamming attack. Unlike the MJ, the MI can target only one repetition by replacing it with a fake CSB. Because the UE is not able to tell which repetition is valid or not, it will trigger a CRC fail, forcing the UE to restart the MIB-NB acquisition.

3.2.4 Narrowband System Information Block 1 Attack

Similar to the MIB-NB, the Narrowband System Information Block 1 (SIB1-NB) has mostly a static configuration as described in Section 2.2.1, but in some specific scenarios might differ and utilise an extra subframe [58]. For this reason, we assume that the attacker has successfully obtained and decoded the MIB-NB, therefore gaining all the knowledge necessary for targeting the SIB1-NB. Within the information obtained from the MIB-NB, the value of the *schedulingInfoSIB1* parameters dictated the number of repetitions of each SIB1-NB CSB. This parameter can be configured with a value of four, eight or sixteen times. The TTI of the SIB1-NB is always 256 frames or 2560 ms and carries eight CSB that are equally spread out and repeated, as previously mentioned.

In our testbed, the SIB1-NB repetition is set up with four repetitions, implying that the subsequent SIB1-NB is transmitted in an interval of 64 frames. Within these 64 frames, eight subframes carry the payload in every alternate subframe four. Consequently, to target the SIB1-NB using MJ or MI, it is necessary to interfere with subframe four for one millisecond every 64 milliseconds, repeating this process four times.

3.2.5 Narrowband System Information Block 2 Attack

Unlike the initial two messages, the Narrowband System Information Block 2 (SIB2-NB) has a dynamic configuration and can be altered by the eNodeB. Some of the changes can include the TBS and frequency. All of this information is relayed to the UE via the SIB1-NB (see Section 2.2.1). For this reason, we assume that the bad actor is capable of receiving and decoding the SIB1-NB. In the setup used for our experiment, we configured the SIB2-NB to have a periodicity of 512 SFN, a TBS of 440 bits, with a *si-RepetitionPattern every4thRF* and a *si-WindowLenght* of 960ms. This

configuration results in 24 repetitions.

In this situation, the MJ device must disrupt a single SIB2-NB subframe (see Figure 2.4) for a length of 1 millisecond. This disruption should be repeated every fourth frame during the entire *si-WindowLength* in order to ensure that all subframes carrying the SIB2-NB payload within the window are affected. Subsequently, the jammer can remain inactive until the frame count hits the designated periodicity threshold (512 frames or 5.12 seconds in our specific scenario). The MI functions in a comparable manner to MJ, but with one key distinction: instead of jamming a subframe, MI broadcasts a fake subframe, repeating it 24 times (every fourth frame within a 960ms time-frame).

3.3 Improved Early Data Transmission (EDT+)

In the realm of the IoT, stationary devices hold a distinctive position due to their consistent connectivity to the same cell and relatively stable signal strength. This stability ensures that the parameters of these devices remain primarily unaltered, thus providing a reliable platform for optimising communication and energy efficiency [167]. In this work, we propose a new communication mode called Improved Early Data Transmission (EDT+) that is able to leverage the static nature of smart metering and most static NB-IoT applications. EDT+ reuses parameters from previous communications, thereby significantly reducing the communication overhead observed in Normal, C-IoT-Opt, EDT mode (see Fig. 2.9 and Fig. 2.10), as shown in Fig. 3.3. Its primary goal is to enable immediate data transmission upon wake-up, fully exploiting the stationary nature of the UE [29].

3.3.1 Overview

Upon initial connection, the UE will request an EDT+ allocation from the eNodeB. If the request is granted, it will save all the necessary information for the future connection to be EDT+. After each EDT+ transmission, the UE will receive the necessary parameters for the next one, including the deep sleep duration.

If the UE has the EDT+ parameters saved, when waking up, it will acquire the NPSS and NSSS. Depending on its clock accuracy, the UE can

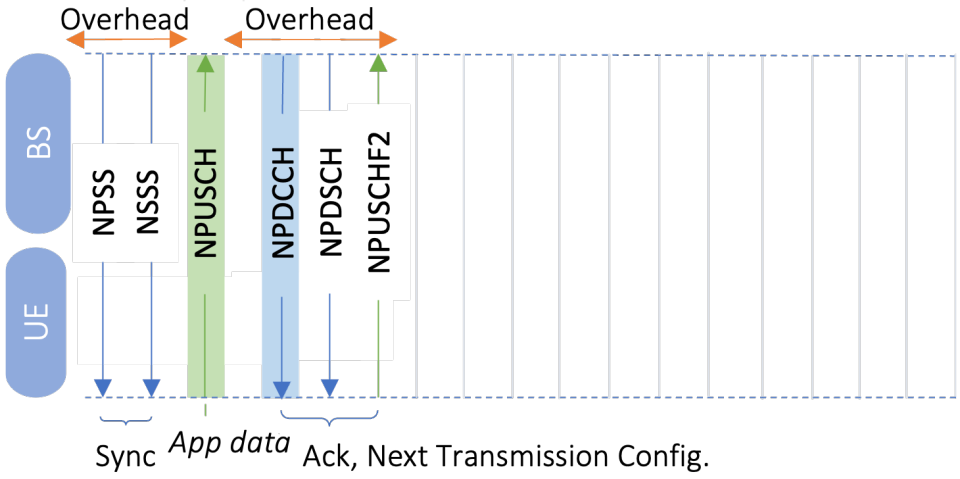


Figure 3.3: EDT+ transmission procedure.

choose to send the payload directly. Otherwise, if there is any uncertainty regarding synchronisation or if the UE does not receive any Acknowledgement (ACK) from the eNodeB, it will obtain the MIB-NB and the SIB1-NB. Decoding the SIB1-NB provides all the necessary information to assess its clock accuracy discrepancy as it contains the SFN and H-SFN.

Data transmission proceeds if synchronisation within the current time slot is secured. Alternatively, the device returns to the default connection method. Following each transmission, the system gets the configuration for the subsequent transmission and synchronises its clock to counteract any potential deviation prior to the next transmission proactively.

3.3.2 Initial Connection and Message Transmission

Similar to the normal NB-IoT connection, the initial EDT+ transmission procedure starts with the UE sending a Random Access Preamble (Msg1) to the eNodeB, followed by the Random Access Response (RAR) also known as Msg2 on the downlink channel. Further on, the EDT+ expands the RRC Connection Resume Request (Msg3), including additional information regarding the static nature of the device. Specifically, the UE appends a boolean flag "EDT+" to Msg3, allowing the eNodeB to identify static devices as early as possible.

Additional to the "EDT+" boolean, the UE should send the "transmis-

sionPeriodicity" and the "payloadSize". Because EDT+ is a fully scheduled transmission procedure, these two parameters are vital in determining the scheduling scheme. The "transmissionPeriodicity" represents the average periodicity an UE wants to achieve, and the "payloadSize" represents the maximum payload the UE will send using the EDT+ handling mode.

3.3.3 Time Slot Allocation

As soon as the eNodeB receives a Connection Request with the true "EDT+" flag, it follows by processing it as a normal request. Additionally, it evaluates the "transmissionPeriodicity" and the "payloadSize" and computes the next feasible time interval, taking into consideration the predicted network load at that time.

During a typical transmission, the UE obtains all its dedicated radio configurations after receiving the RRCConnectionSetup message. Some of these configurations include values for the sub-layers: PHY, MAC, RLC or PDCP [97]. Similar to normal transmission in EDT+, the UE will receive all of these parameters alongside the allocated TBS, time slot, wake-up time and the number of repetitions.

We set up the EDT+ TBS to be identical to the EDT TBS, meaning that a TBS will allow a payload size of 328, 408, 504, 584, 680, 808, 936, or 1000 bits. It is preferred for the TBS to have the smallest feasible size for the first EDT+ transmissions, as it would facilitate an increased number of repetitions without putting a strain on the available bandwidth.

To calculate the number of repetitions the UE has to transmit, the eNodeB has to take into consideration the MCL level, the clock accuracy and the TBS. Unlike a typical connection, the number of repetitions can also increase the chances of the UE hitting its allocated time slot. For example, if we consider the scenario where the oscillator is slower, denoting an early wake-up, an increased number of repetitions might still allow for the transmission to go through. We envision the EDT+ protocol to be self-optimising, meaning that the more EDT+ transmission a static UE has, the better it can predict its clock drift between transmissions, therefore increasing its chances of hitting the allocated time-slot. The eNodeB will monitor this behaviour and adjust the number of repetitions, time-slot allocation and wake-up periods for each transmission with the goal of optimising the network resources.

3.3.4 Data Transmission

Aspect	Setting	Purpose / notes
Uplink subcarriers	$\geq$1 @ 3.75 kHz; up to 6 @ 15 kHz (six-tone)	Keeps $\geq$50% uplink bandwidth for normal NB-IoT; per NPUSCH.
Transmission window	Dynamic (eNodeB); TX $\leq$ 410 ms; spacing $\geq$ 40 ms	Avoids overheating; Device can listens for ACK between bursts.
Half-duplex / ACK	TX$\rightarrow$RX gap $\geq$ 3 ms; monitor next NPDCCH	Enables RX switch and timely ACK detection.
Payload field	Repetition index included	Allows per-device resource adjustment by eNodeB.
eNodeB adaptations	Listen-slot duration; UL repetitions; Time-of-Arrival Offset (TAO)/Timing Offset Propagation (TOP); window shift	Optimises timing/repetitions; handles drift.
Drift / CFO	Correct via TAO; stable offset $\Rightarrow$ TOP	Temperature drift mitigation; may widen/shift listen window.
Security	Inherits NB-IoT security; payloads encrypted	Credentials already provisioned at eNodeB.

Table 3.3: Concise summary of EDT+ data-transmission settings.

To enable successful transmission of a package in EDT+, the eNodeB needs to assign a minimum of one 3.75 kHz subcarrier for the EDT+ connection. Additionally, it should allocate a maximum of 6 subcarriers for a 15 kHz spacing and a six-tone transmission. This allocation ensures that at least half of the bandwidth is available for normal NB-IoT connections while still adhering to the NPUSCH configurations. The settings can be customised based on the number of EDT+ requests.

Moreover, the assigned time interval for transmission should be dynamic on the eNodeB side and should account for potential time discrepancies on the UE side. It should be noted that a UE should not transmit for more than 410 ms at once in order to prevent time drift caused by overheating. Similar to the NPUSCH and NPRACH, there should be a 40-millisecond interval between broadcasts. During this time, the device should go back to listening mode and wait for the acknowledgement. Considering the half-duplex characteristic of the UE, it is necessary to have a minimum 3-ms gap to enable the device to transition from transmission mode to reception mode.

This allows the UE to prepare for monitoring the subsequent NPDCCH search space candidate for the ACK, as seen in Fig. 3.4

When sending the payload, the device should additionally incorporate the repetition index. This information is important as it enables the eNodeB to make necessary adjustments to the resources allocated for that particular device. Possible adjustments might include:

- Adjust the duration of the listening time slot.
- Adjust the number of uplink repetitions
- Increase/decrease the TAO

We have to mention that the EDT+ transmissions will have all the security characteristics of the NB-IoT protocol, and all payloads will be encrypted. This is possible since the eNodeB should already possess the cryptographic credentials from the initial transmission.

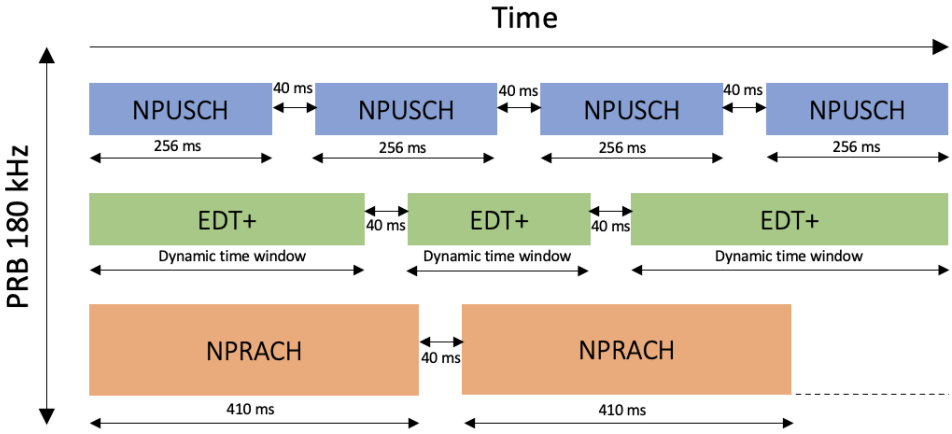


Figure 3.4: Potential allocation of EDT+ within the Uplink Schedule.

Adjust the duration of the listening time slot

The eNodeB adapts the listening period for each device based on criteria like oscillator accuracy, payload size, and available resources, as illustrated in Figure 3.4. For example, if the resource utilisation of the EDT+ is 20%, the eNodeB may increase the allocated time for a device in anticipation of substantial or unknown clock drift. This is possible by using past data as

a basis. This modification enables the process of identifying the repetition and its corresponding index, which in turn assists in determining the full TAO. Therefore, the UE adjusts its clock drift based on the received TAO, optimising it for future communications. The dynamic adjustments made by the eNodeB, which corrects even minor deviations by modifying the time slot, ensure an efficient transmission environment [29].

Adjust the number of uplink repetitions

During uplink transmission, the UE has to provide the repetition index to assist the eNodeB in evaluating and compensating for clock drift, as explained previously. In addition to adjusting the time period for listening, the eNodeB may direct the device to change the repetition number (in future transmissions) in order to improve resource utilisation, often prioritising a decrease in repetitions.

In a scenario where there are enough transmission resources and the listening time can be maximised, and if a message can be decoded with a repetition index of less than 10, a device that is currently set to 16 repetitions should reduce the count to 10 in order to conserve battery life. On the other hand, in regions where there is poor coverage and issues regarding synchronisation, the base station might be unable to decode the message even when it is using the entire allocated listening span. In this case, it should send a failure acknowledgement. This acknowledgement should include the TAO and a raise directive in the repetition numbers. This will encourage adaptive responses to different conditions and improve the efficiency and reliability of the system.

Increase/decrease the Time-of-Arrival Offset (TAO) and Timing Offset Propagation (TOP)

According to research studying CFO [95] and time drift [96], [97], there are inherent difficulties linked to the frequency references of NB-IoT end devices. CFO adjustments and time drift can be particularly difficult with temperature variations.

The TAO is the setting that enables UE to maintain synchronisation with the eNodeB. It is crucial for the protocol as it informs the device about the required offset for adjusting the oscillator for future transmission. If we

assume an ideal UE with no clock drift, this parameter will be calibrated once, resulting in a nearly flawless communication. The UE becomes active, sends the payload, and the eNodeB promptly receives it. However, as there are no existing devices of this kind, the TAO will need to be computed and delivered each time for minor changes. If the device exhibits a consistent deviation, the Timing Offset Propagation (TOP) can be determined by the UE through repeated receptions of the TAO. Alternatively, eNodeB can modify the length and offset of its listening time window to provide greater flexibility.

3.3.5 Contingency Plan and Reconnection

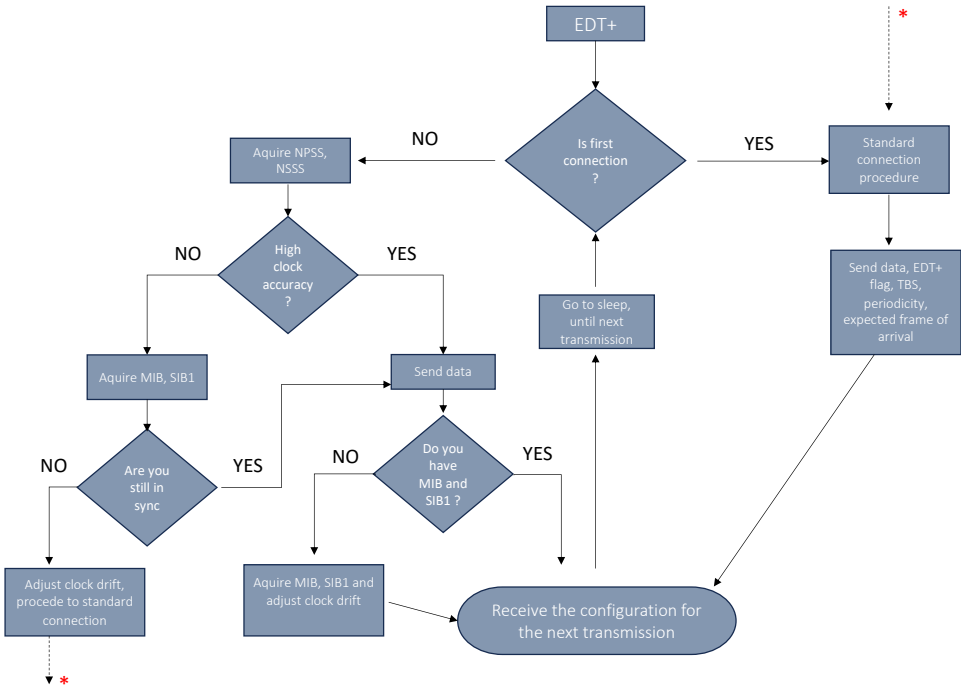


Figure 3.5: Decision logic for EDT+.

The EDT+ protocol incorporates a fail-safe mechanism to handle situations when the device successfully transmits the initial packet but fails to receive the acknowledgement within the designated time frame. In the absence of any communication within a certain time frame, the UE will commence a normal procedure for establishing a connection. This guarantees that the UE is not left in a state of uncertainty or indecision. In order

to optimise its active time while monitoring the NPDSCH, it is important for the device to acquire the MIB-NB and the SIB1-NB. These will enable the UE to calculate the SFN and the H-SFN. By possessing this information, the UE will have a good understanding of its synchronisation. Upon receiving the EDT+ request for the second time, the eNodeB removes the device's prior entry from its list of devices. This guarantees that the eNodeB maintains accurate and current records without any unnecessary or duplicate entries. [29]. Figure 3.5 depicts the full logic of the EDT+ protocol, including the contingency plan.

3.3.6 EDT vs EDT+ Comparison

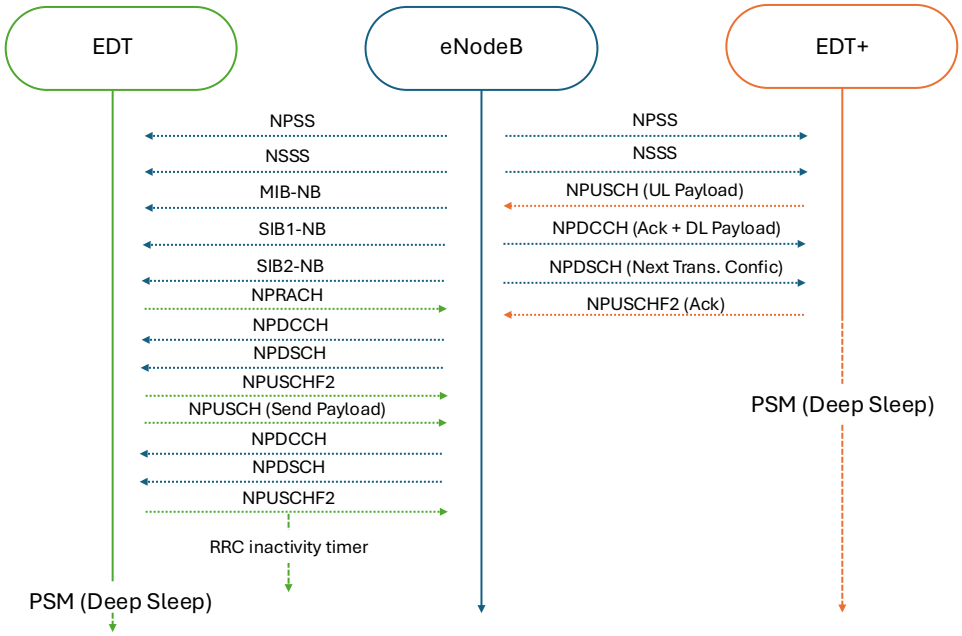


Figure 3.6: EDT vs EDT+ (stationary NB-IoT): EDT repeats RA each report; EDT+ reuses prior config to skip RA and transmit.

If we compare EDT to EDT+ (Figure 3.6) we can say that EDT treats each report as a fresh access: the device wakes, re-establishes context, competes for the channel, and then sends its data; EDT+ shifts coordination upfront and turns later reports into scheduled one-step bursts: the device wakes, does a quick timing check, and transmits in a pre-arranged window reserved by the network for that stationary device. Conceptually, EDT is per-report, reactive and contention-based, while EDT+ is predictive and

reservation-based, reusing cached context (schedule, configuration, timing guidance) and updating it after each exchange. Both preserve the standard security posture and logic; the key difference is where the effort sits: every time for EDT versus once and reusing prior configuration and refreshing it after each exchange for EDT+, with EDT+ falling back to the standard or EDT path whenever the pre-arranged window are not met.

3.3.7 EDT+ Use Cases

In Improved Early Data Transmission (EDT+), the oscillator accuracy plays a crucial role in determining the window size for successful data transmission. The window size refers to the time frame within which the device must initiate its data transmission to ensure successful reception by the BS. Oscillator accuracy affects the device's ability to maintain synchronisation with the BS over time. Devices with higher oscillator accuracy (See Section 2.5.4) can maintain synchronisation for longer periods (p), thereby reducing the need for frequent re-synchronisation and leading to smaller window sizes for data transmission.

This mechanism determines how many devices a single BS can serve. With high-accuracy UE oscillators, listening windows align closely, allowing smaller per-UE windows and thus more devices. With lower accuracy, windows must be enlarged to absorb drift, consuming time resources per device and reducing the number of UEs the BS can support.

Therefore, in EDT+, the *device-support capacity* of a BS (number of UEs it can serve), N, is inversely related to the per-UE *listening window size*, W; both N and W are determined by the oscillator accuracy of the devices. High accuracy allows for smaller windows and higher device support capacity at the BS, while lower accuracy necessitates larger windows, reducing the overall capacity for device support. For clarity:

$$\text{Higher oscillator accuracy} \;\Rightarrow\; \text{smaller } W \;\Rightarrow\; \text{larger } N,$$
$$\text{Lower oscillator accuracy} \;\Rightarrow\; \text{larger } W \;\Rightarrow\; \text{smaller } N.$$

In order to showcase the advantages and limitations of the EDT+ concept, we designed several use cases, ranging from simple scenarios with perfect environmental conditions to dynamic time-window allocations. All of the scenarios use the following constants: a clock oscillator of ± 40 ppm (see

Section 2.5.4); one transmission at a time *(serialised UEs to isolate per-UE effects of the transmission procedures (Normal, C-IoT-Opt, EDT, EDT+) and to avoid contention)*; a 5 min simulation window with 100 transmissions/nodes; and an eight-transmission periodicity (p). Similar settings have been used by Pascal et.al. [28], and are reflected in the following scenarios:

- Traffic Meter - 30 minutes: Traffic monitoring systems often collect data at regular intervals to analyse traffic flow and congestion, helping in traffic management and planning.
- Electric Meter - 1 hour: Electric meters for residential or commercial properties typically record usage hourly to provide detailed usage data, aiding in energy management and billing.
- 2 hours: Air quality monitoring stations may update pollutant levels every 2 hours, providing data for environmental protection agencies to assess and respond to air quality issues.
- 6 hours: Weather stations might collect meteorological data every 6 hours to track weather patterns, which is crucial for forecasting and climate studies.
- 12 hour: Coastal tidal gauges might record sea level data every 12 hours to monitor tide levels, supporting maritime navigation and coastal management.
- 1 day: Some agricultural monitoring systems check soil moisture and other environmental conditions once a day to inform irrigation and farming decisions.
- 2 days: Groundwater monitoring wells might record water levels and quality metrics every 48 hours to track aquifer conditions and manage water resources.
- 7 days: Remote wildlife counting systems may log the species and number of specific animals on a weekly basis to study migration patterns, behaviour, and conservation status.

Chapter 4

NB-IoT Testbed and Simulation Environment

With the fast adoption of IoT, a demand for secure, robust and efficient communication technologies has emerged. LPWAN networks' primary objective is to facilitate this demand and push the boundaries of high connectivity. When considering LPWAN networks, it is worth mentioning that usually, they are split into two categories. First are the technologies that operate on an unlicensed spectrum, such as Sigfox, LoRaWAN, MIoTy, and others. These have benefited early from wide adoption due to their low cost, availability, and ease of use, which in turn developed a highly knowledgeable community that added again to the adoption rate.

On the other hand, the deployment of licence spectrum technology is gradually gaining momentum due to promising scalability, wide-coverage, availability, robustness, and security. Out of the license spectrum technologies NB-IoT has emerged as a pivotal standard, designed by 3GPP [59] with the aforementioned promises while also being built on legacy infrastructure. To achieve these objectives and to meet the demands of an interconnected world, **low cost** simulations and testbeds have to be developed. This approach will enable rigorous NB-IoT research and will play an important role in understanding and optimising the performance of the protocol.

Significance of Simulations and Testbeds

Due to the high complexity of telecommunication networks, simulations and testbeds serve as a foundational tool in network research, development, and deployment. Simulations offer researchers the opportunity to model and predict network behaviours under different scenarios, including various topologies, energy consumption models, and signal interference. They provide the ability to control the environment, test hypotheses, and understand the impact of different configurations without the need for real-world deployment, therefore reducing cost. Unfortunately for NB-IoT, publicly available simulation environments are limited to this day. Out of the handful, Matlab LTE Module focuses on signal generation and BLER [168], while srsRAN provides an open source downlink implementation up to SIB1-NB. Additionally, the srsRAN gives the opportunity to run the code in a simulation but also in the real world on Software Defined Radio (SDR)s, which we will discuss later. Lastly, the NS3 Lena NB-IoT Module provides an end-to-end simulation and, to this day, is one of the most complex simulation platforms available.

On the other hand, **testbeds** bring models into the real world. In the case of Narrowband Internet of Things (NB-IoT), this has proven to be particularly challenging due to the license spectrum nature of the protocol. Usually, testbeds that deploy an eNodeB need a license to operate, or they need to be contained in a Faraday cage. Another approach is to establish communication via wired connections using specialised equipment. To overcome all of this, one could shift the frequency to an unlicensed one and take into account the limitations that come with doing this. Overall NB-IoT testbeds bridge the gap between theoretical research and practical application. They offer evidence-based insights into the performance of the systems and facilitate the research and development of innovative solutions.

4.1 Simulation of NB-IoT Systems

4.1.1 Matlab

MATLAB is a powerful computational tool widely used across engineering disciplines. MATLAB's LTE Toolbox offers an extensive suite of functions and tools designed specifically for simulating, analysing, and testing LTE

communications systems. From academic research to industry R&D, the MATLAB LTE Toolbox has become an indispensable asset for anyone looking to delve into the nuances of LTE networks without the need for costly physical testbeds.

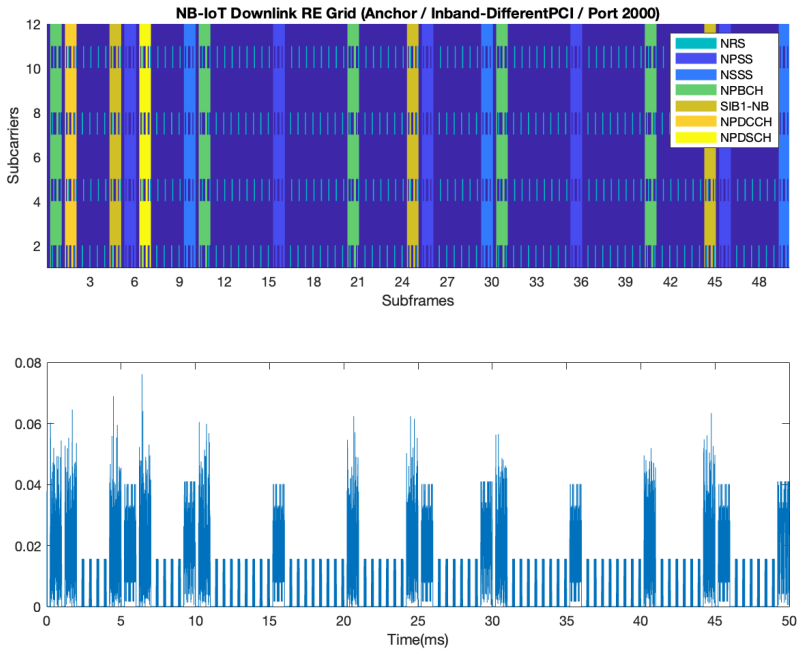


Figure 4.1: NB-IoT waveform produced by the simulation environment in Matlab. Each subframe's assigned channels and signal are shown in the upper representation. The identical signals and channels are allocated in a time-frequency domain, as seen in the lower figure.

It is important to note that the LTE Toolbox's rendition of the NB-IoT protocol does not extend to a fully reactive end-to-end simulation. Instead, its capabilities are more inclined towards the generation, modulation, demodulation, encoding, and decoding of the relevant waveform. This specific focus necessitates the pre-configuration of certain parameters within our simulation environment before initiating the simulator—for instance, settings like SIB2-NB maxPreambleTrans must be defined in advance. Illustratively, Figure 4.1 provides a visual representation of a simulated waveform detailing the distribution of allocated subframes across the spectrum of subcarriers. This approach allows for a nuanced exploration of device behaviour under various network conditions, although it inherently requires a more manual

setup process to accurately reflect the intended operational context of the NB-IoT devices under study.

In this research, the MATLAB software was used extensively for data analytics as well as simulating the NB-IoT channel. Furthermore, during simulation, three coupling losses were chosen, similar to the work done by Liberg et al. [55]. These settings represent a baseline for further specifications, such as power consumption and performance requirements.

Our UE current levels are grounded in vendor documentation for two representative NB-IoT chipsets and in independent measurements. The u-blox SARA-N3 datasheet lists PSM $\approx 3\,\mu A$, RX $\approx 23\,mA$, and TX $\approx 275\,mA$ at $3.8\,V$ [23], aligning with our choices $TX_{max} = 330\,mA$, $RX_{max} = 30\,mA$, $idle = 3\,mA$, and $deepsleep = 3\,\mu A$. Qualcomm's 212 LTE NB-IoT modem advertises sub-$1\,\mu A$ sleep current, supporting our deep-sleep selection [24]. Peer-reviewed measurements report UL power $\approx 716\,mW$ at $23\,dBm$ (i.e., $\approx 0.19\,A$ at $3.8\,V$), DL ≈ 213–$240\,mW$ (i.e., ≈ 56–$63\,mA$ at $3.8\,V$), and PSM $\approx 13\,\mu W$ (i.e., ≈ 3–$4\,\mu A$) [149]. Notably, these empirical DL/RX figures exceed vendor "typical" RX currents because they include end-to-end protocol activity and implementation losses (e.g., control-channel processing, clocking, front-end biasing), whereas datasheets often report steady-state currents under idealised conditions. To parameterise energy consumption, we used the published specifications from two widely deployed NB-IoT platforms [24, 23], which together cover the full set of vendor-reported operating currents. Preliminary experiments were conducted under near-ideal conditions to emphasise the causal effect of our intervention rather than the absolute values of device specifications.

GSMA/3GPP guidance codifies NB-IoT UE power classes $23/20/14\,dBm$ and frames a 10-year design target assuming $\sim 5\,Wh$ batteries [169, 170]; our battery choice $C = 1000\,mAh$ at $V_{nom} = 3.7\,V$ ($\approx 3.7\,Wh$) is therefore conservative relative to that reference practice [22]. This battery was preferred due to its popularity and availability on the market. It is worth mentioning that in real-world deployments, the UE 's lifespan will most likely be affected by battery degradation and other battery-related factors, such as temperature, humidity, fabrication quality and other environmental aspects, that were not included in our model.

Collectively, these sources substantiate our parameterisation across two mainstream modem families while remaining within published specifications

and empirical ranges.

4.1.2 NS3 Lena NB-IoT module

The ns-3 LENA (LTE-EPC Network Simulator) NB-IoT module is an advanced simulation environment dedicated solely to the research and analysis of NB-IoT technologies. The LENA NB-IoT module, which is part of the larger ns-3 simulation framework, is an excellent resource for researchers, developers, and network architects who wish to understand more about NB-IoT systems in depth.

The ns-3 LENA NB-IoT module is notable for its ability to simulate a wide range of NB-IoT scenarios, from basic signal transmission and reception to complex interactions within a fully deployed network. This module supports many aspects of the NB-IoT standard, including many operation modes (standalone, in-band, and guard-band), power-saving features like PSM (Power Saving Mode) and eDRX (Extended Discontinuous Reception), and extensive channel modelling. Furthermore, it allows for thorough configuration of network parameters such as bandwidth, transmission power, and coding schemes, resulting in a robust platform for conducting performance evaluations across a wide range of scenarios.

The ns3 architecture is designed to emulate the layered structure of the NB-IoT protocol stack, which consists of the physical (PHY), medium access control (MAC), radio link control (RLC), and packet data convergence protocol (PDCP) layers. This architecture enables a detailed analysis of protocol behaviour and interaction at each level, revealing potential bottlenecks and opportunities for improvement. Furthermore, the environment includes a realistic channel model that accounts for route loss, fading, and interference, all of which are important factors in wireless network performance.

The versatility of the ns-3 LENA NB-IoT module enables a wide range of applications, from basic research and protocol development to entire network design and optimisation. Researchers can leverage this module to assess the impact of different network configurations, analyse the effectiveness of power-saving mechanisms and explore the scalability of NB-IoT networks. Network architects and planners can leverage the “LENA” module to plan NB-IoT network deployment and analyse coverage, capacity and performance restraints of different deployment strategies.

However, this module has ample features, and it might come with a steep learning curve, as there are many configurable parts. Users should also be aware of the processing resources that would be required to simulate large-scale UE populations. Since this module strictly adheres to the NB-IoT protocol, it is vital to keep track of 3GPP standard updates and revisions to ensure an up-to-date simulation environment.

The ns-3 LENA NB-IoT module offers a reliable and comprehensive simulation environment for the NB-IoT ecosystem. It is a necessary tool to advance research, development and deployment of IoT devices. As NB-IoT evolves and expands, simulation environments like the ns-3 LENA module will be vital for navigating the complexities of this rapidly changing technical landscape.

4.1.3 srsRAN

srsRAN, formerly known as srsLTE, is an open-source software-defined radio (SDR) framework designed to facilitate the simulation, research, and real-world deployment of LTE and 5G wireless communication systems. Renowned for its comprehensive suite of tools and libraries, srsRAN is pivotal for developers, researchers, and educators in the field of wireless communications, providing a versatile and accessible platform for experimenting with the latest advancements in LTE and 5G technologies.

srsRAN offers an extensive array of features that cover the full stack of LTE and 5G NR (New Radio) protocols. This includes complete implementations of the eNodeB (LTE base station), UE (User Equipment), and EPC (Evolved Packet Core) for LTE networks, as well as support for NR base stations and devices for 5G simulations. The framework is compatible with MIMO (Multiple Input Multiple Output) configurations, sophisticated modulation schemes and numerous channel models to simulate real-world radio conditions as accurately as possible. On top of that, as an open-source 5G software suite, srsRAN is compatible with a variety of commercial and custom SDR setups.

An important aspect of srsRAN is that it is a modular design, which enables seamless integration of its components into various simulation and deployment scenarios. The framework is structured to allow for easy customisation and extension, catering to specific research needs or project requirements. Users can modify existing modules, such as PHY, MAC, RLC,

and PDCP layers, or integrate new functionalities to explore innovative communication concepts and technologies.

In addition to its simulation capabilities, srsRAN provides a solid foundation for the development and testing of real-world applications. It's been used in a wide range of contexts, from academic research to the development of commercial products and the optimisation of networks. The modular and open-source nature of the framework allows for the experimentation of new features of LTE and 5G networks, such as network slicing, optimisations for the Internet of Things and low-latency communication protocols. Furthermore, it can be used for research on security, analysing threats that may arise within networks or developing new ways to protect them.

While srsRAN presents a powerful solution for LTE and 5G simulations, users may encounter challenges related to its setup and operation. The requirement for compatible SDR hardware and the potential complexity of configuring real-world scenarios demand a certain level of technical expertise. Furthermore, as with any actively developed open-source project, keeping up-to-date with the latest updates and community contributions is essential to leverage the full potential of the framework.

srsRAN stands at the forefront of SDR technology, offering unparalleled opportunities for the exploration and implementation of LTE and 5G networks. Its comprehensive feature set, coupled with an open-source licensing model, makes it an ideal choice for the academic and research community, as well as industry professionals seeking a flexible and powerful tool for wireless communication development and testing. As the demand for advanced wireless communication solutions continues to grow, srsRAN will undoubtedly play a pivotal role in shaping the future of LTE and 5G technologies.

4.2 Testbed for NB-IoT Devices

One of the primary research goals is to analyse and study battery depletion attacks against NB-IoT protocol. Attack vectors such as Message Jamming (MJ) and Message Injection (MI), explained in 3.1, require a deep understanding of the NB-IoT environment and its behaviour, hence the necessity of constructing a physical testbed. Employing multiple SDRs that would act as the UE the eNodeB but also as a malicious entity provides the flexibility to target different aspects of the protocol. Due to the re-

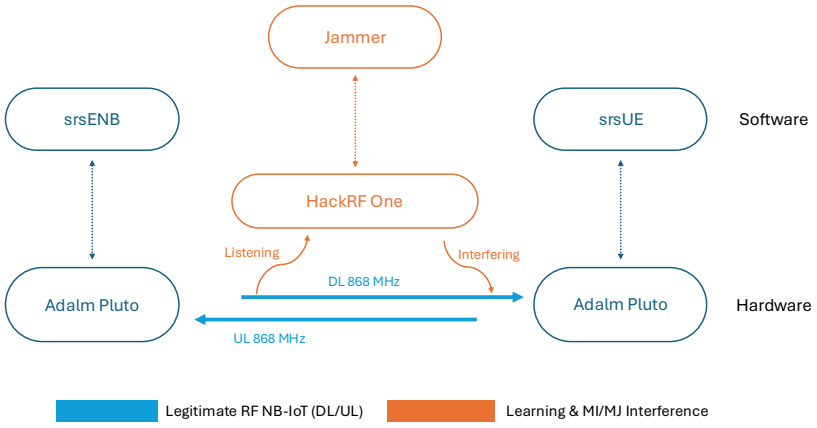


Figure 4.2: NB-IoT *emulation* testbed orchestration. Software roles (top) control SDR hardware (middle) to realise the RF link (bottom). Arrows show DL/UL paths and where message injection (MI) or message jamming (MJ) acts.

striction compelled by the licence spectrum, we chose to shift our testbed to an unlicensed frequency band. Furthermore, we extended the srsRAN open-source protocol and made it available on the public repository [26] for future research.

4.2.1 Hardware

In determining the appropriate hardware for the physical testbed, we took into consideration several factors:

- Availability: The hardware components needed to be readily available and avoid delays in procurement.
- Documentation and support: Comprehensive documentation and an active user community were essential for efficient setup and troubleshooting.
- Affordability: Cost-effectiveness was crucial to ensure the project remained accessible for future development.

- Ease of experiment replications: The hardware had to allow for straightforward replication of experiments to ensure consistency and reliability of results.

Taking all of this into consideration, we considered that HackRF One SDRs by Great Scott Gadgets [171] as well as ADALM-Pluto by Analog Devices [172] satisfies all of the previously mentioned requirements. The HackRF one is a SDR peripheral device operating between 1MHz and 6GHz. Along the open-source platform that it operates on, it can be used as a stand-alone device, or it can operate as a USB device capable of transmitting and receiving radio signals in a radius of 50 meters in open space. For the experiments presented in chapter 4.3, the devices were tuned to the open frequency of 868MHz with offset calibration for maximising the signal quality. The SDRs were set one meter apart in order to minimise the environmental interference.

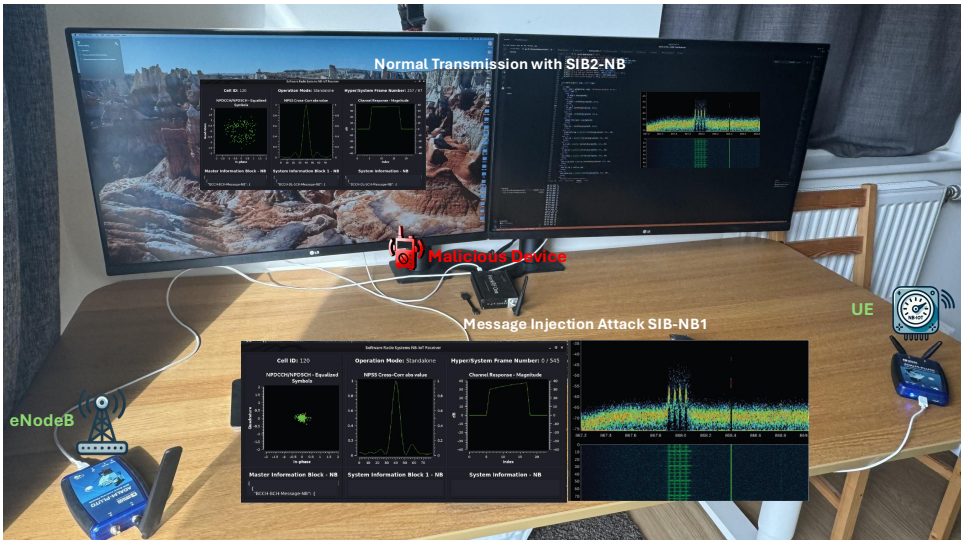


Figure 4.3: NB-IoT testbed utilising srsRAN software: The bottom left screen displays the eNodeB base station communicating with the UE in the bottom right. A malicious device in the centre executes a message injection attack on the SIB1-NB, while the central computer screen shows a standard connection scenario.

The HackRF One is classified as a half-duplex SDR. It can receive or transmit data at a single time. While most telecommunication UEs are half duplex, most eNodeB are full-duplex and can transmit and receive at

the same time. If we consider the exploits from 3.1, we can observe that the jammers need to respect a strict timing constraint. The HackRF One platform is not capable of switching between receiving and transmitting in real-time, thus limiting the capability of the jamming device. To overcome this, the jammer was configured each time by producing relevant signals for the specific experiment. It is worth mentioning that this limitation can be overcome with a more capable SDR. A testbed variant is illustrated in Figure 4.3.

4.2.2 Software

The srsRAN software is an open-source project developed to be used with in-house and third-party core network equipment. It includes protocol stacks for both the UE and the eNodeB and is capable of creating an end-to-end network solution [173]. While this ability is implemented for LTE and 5G networks, it lacks the full implementation of the NB-IoT protocol, allowing transmission up to SIB1-NB [174].

To conduct our experiment, we integrated the functionality of sending the SIB2-NB into srsRan. To reduce packet overlapping, we modified the existing code to account for the Hyper Frame Number (HFN) and to ensure the eNodeB was not concurrently transmitting other data. The primary configuration for the downlink channel to transmit the SIB2-NB was established as follows: *si_repetition_pattern* = 4 (every fourth frame); *si_window_length* = 960 transport block size *si_tb* = 440; window length; *si_periodicity* = 512.

All of the software implementation was developed on Linux using a standard CPU and the aforementioned radio equipment. The operating software was Kali Linux. We used the SDRAngel and the CubicSDR software for spectrum analysis, and we employed the HackRF One driver to interact with the SDRs.

4.3 Framework for Evaluating Jamming Vulnerabilities

To study the effectiveness of our attacks, we employed two evaluation scenarios designed for the specific testbed in which they were deployed. More precisely, a virtual simulation environment based on Matlab and LTE Tool-

box (see Section 4.1.1) [27] and a hardware simulation environment based on HackRF One and srsRAN (see Section 4.2) [27]. For simplicity reasons, in this chapter, we will distinguish between virtual and physical simulations.

4.3.1 Evaluation Scenario

Virtual Simulation

Following a common NB-IoT scenario similar to Liberg et al. [55], we assume that the eNodeB has the necessary bandwidth to receive any uplink transmission and that the UEs can communicate seamlessly with the eNodeB. Furthermore, a UE will wake up periodically every $t = 2h$, receiving a payload of $b_{up} = 60byte$ and transmitting $b_{up} = 200byte$ of data. These settings represent the baseline. This initial scenario is performed without any interference in order to establish a baseline for the energy usage of the UEs. Afterwards, the identical scenario is performed with interference, and the energy usage is compared to the baseline.

Physical Simulation

We used the testbed described in Section 4.2 to assess interference-based battery depletion attacks. Three HackRF One devices are positioned in a line approximately 1m apart. The jammer is placed between the targeted UE and the eNodeB. The eNodeB continuously broadcasts its downlink channel, while the UE is tasked with acquiring all the messages up to SIB2-NB inclusively as fast as possible. Due to the discrepancy in specification between a HackRF One and a real NB-IoT UE, in addition to the insufficient information regarding the specific moment when a UE should cease receiving corrupted messages, we chose not to calculate the exhausted energy. Instead, we highlighted our result in the active receiving time and delay caused by the UE per message when trying to acquire specific data.

4.3.2 Evaluation Metrics

Virtual Simulation

We employ two parameters to evaluate the effectiveness of an attack. The first parameter is Energy Depletion Rate (EDR), a metric proposed in this

work to quantify the extent to which an attack depletes a device's battery compared to the baseline scenario. We defined EDR as:

$$EDR = 1 - \frac{E_{baseline}}{E_{attack}} \tag{4.1}$$

$E_{baseline}$ represents the UE's average energy consumption under normal, interference-free operation, profiled through repeated measurements in controlled conditions using the same traffic pattern, configuration, and environmental parameters as in the attack scenario. E_{attack} refers to the energy consumption in an attack scenario. The EDR can have values between 0 and 1, where 0 represents a lack of efficiency, while 1 represents a highly effective attack. This metric is used for both the downlink and the uplink channel to determine whether the attack has a greater impact on upstream or downstream channels.

For capturing the percentage of time a malicious device is active, we calculated the Jammer Duty Cycle (JDC). JDC is given by:

$$JDC = \frac{T_{active}}{T_{total}} \tag{4.2}$$

T_{active} represents the time the jamming device is transmitting, while T_{total} denotes the total duration of the experiment. JDC measures the effort required by the attacker to achieve their objective. It also indicates how active the attacker is and how easily they might be detected.

Physical Simulation

To assess the success of a jamming attack using our physical testbed, we calculate the UEs additional receive time. The maximum additional time accomplished by an attack relies on the implementation characteristics of each UE and is not specified by the NB-IoT standard. For example, if the UE is designed to permit a repeat of 5 MIB-NB before the connection is declared invalid, an attack on the MIB-NB can extend UE receiving time up to four times while still not interrupting the communication. Some UE implementations may not specify a repetition counter, causing them to listen for the MIB-NB indefinitely. To test the efficacy of jamming attacks, we choose the additional receiving time T_R by interfering with the reception of one MIB-NB, SIB1-NB, or SIB2-NB. We calculate T_D as the additional

delay time necessary to wait for a retransmission. The Jammer goal is to remain undetectable while simultaneously using as little energy as possible to achieve its purpose. Therefore, it is helpful to assess the jamming duration. We choose T_J as the active jamming necessary in blocking one of the MIB-NB, SIB1-NB, or SIB2-NB. Depending on the attack form (MJ or MI) T_J may vary.

4.3.3 Jammer

Virtual Simulation

In our virtual setup, we simulated four jamming attacks.

- Decreasing the quality of service using a **simple** jammer: simple Degradation of Quality of Signal Attack (sDQS)
- Decreasing the quality of service using a MJ also known as an **intelligent** jammer: intelligent Degradation of Quality of Signal Attack (iDQS)
- Targeting the Random Access Procedure using an **intelligent** jammer: Random Access Procedure (RAP)
- Performing an iDQS followed by a RAP using an **intelligent** jammer: (iDQS + RAP)

As stated above, intelligent jamming and message jamming use the same techniques and procedures to find and exploit vulnerabilities. For virtual environments, we primarily use the term "intelligent jamming", whereas for physical environments, the term "message jamming" is employed. By using Matlab (see Section 4.1.1), we modelled the iDQS and the sDQS attacks to maximise the required resources for completing a communication cycle. Explicitly, both the number of repetitions as well as the transmission power were adjusted for an MCL of 164db [55]. The sDQS made use of an AWGN function for adding varying amounts of noise to a legitimate transmission. The noise levels were influenced by the transmission power. Furthermore, assuming that the intelligent jammer has already intercepted and learned the transmission pattern between the UE and the eNodeB, the iDQS is performed. This involves adding the same AWGN noise only to the targeted signals as described in Section 3.2.1.

In order to evaluate the RAP exploit (see Section 3.2.2), we only modelled the RAP on top of our baseline environment. After receiving and correlating the NPSS and the NSSS, the malicious device acquires the Master Information Block (MIB), which will provide all the necessary information to acquire the SIB1-NB and consequently the SIB2-NB. The SIB2-NB will provide an offset in the frequency, representing the band for the uplink channel. The jammer is now ready to listen and learn the transmission pattern of the targeted device. To perform an EDA, the intelligent jammer will start interfering with the uplink messages (in our specific scenario Random Access Preamble Transmission (Msg1)), which in turn will increase the number of retransmissions. An alternative way of finding the uplink channel is to find the NPSS and listen on a wider band for uplink transmissions. Usually, the uplink messages will have less power than the downlink ones due to the UEs limitations. This alternative is less complex and easier to implement by a malicious entity, but it lacks in terms of accuracy and efficiency.

We simulated the full attack in Matlab and calculated the jammer duty cycle and the depletion rate by increasing the number of repetitions to 120 out of 128 maximum. This attack was directed at the Msg1 on the uplink channel as well as the SIB2-NB on the downlink channel.

Physical Simulation

For the physical simulation testbed, we used the models presented in Section 3.1, specifically the MJ and the MI. The testbed composed of three SDRs enabled us to test the feasibility of the MJ and MI attacks.

When it comes to the MJ attack, we modulated noise using an 802.15.4 QPSK and transmitted it in a valid subframe slot on the downlink channel. The transmission power for the malicious HackRF One SDR was set to -38db, which, in our case, prevented the UE from decoding the subframe. The probability of success at this power level was above 99%.

On the other hand, the MI attack was performed by broadcasting a structurally valid message concurrently with the eNodeBs message. By setting the attacker's power level to -57db, the UE achieved a probability of 99% in decoding the malicious message instead of the real one.

We assumed that both the MJ and the MI jammer devices have a deep understanding of the protocol and are capable of eavesdropping and learning the communication patterns of the UE.

Chapter 5

Evaluation Results

5.1 Battery Depletion Results

5.1.1 Baseline

As illustrated in Figure 5.1, the battery lifetime of an NB-IoT UE is drastically impacted by the Maximum Coupling Loss (MCL). We believe that a transmission interval of $t = 2h$ with an uplink payload of $b_{up} = 200byte$ and a downlink payload $b_{down} = 60byte$ represents a realistic scenario. These baseline results are in line with other literature findings such as [55, 175, 176] and represent a good starting point in evaluating the attacks discussed in Section 3.1.

In NB-IoT, the MCL levels define the extent of coverage enhancement achievable under different conditions. NB-IoT supports three main coverage enhancement levels, each with specific MCL values:

- CE-0: This level has an MCL of 144 dB (good network coverage).
- CE-1: This level has an MCL of 155 dB (average network coverage).
- CE-2: This level has an MCL of 164 dB (bad network coverage).

These levels help to ensure that NB-IoT devices can maintain connectivity even in challenging environments such as deep indoor areas or basements. [177, 178]. Figure 5.1 illustrates the percentage used by the UE in different communication states (Active (TX/RX), Idle Sleep and Deep Sleep). In this scenario, we can observe that an MCL = 144db satisfies the minimum 10-year requirement specified by 3GPP [59], while a CE-1 and CE-2 fall short

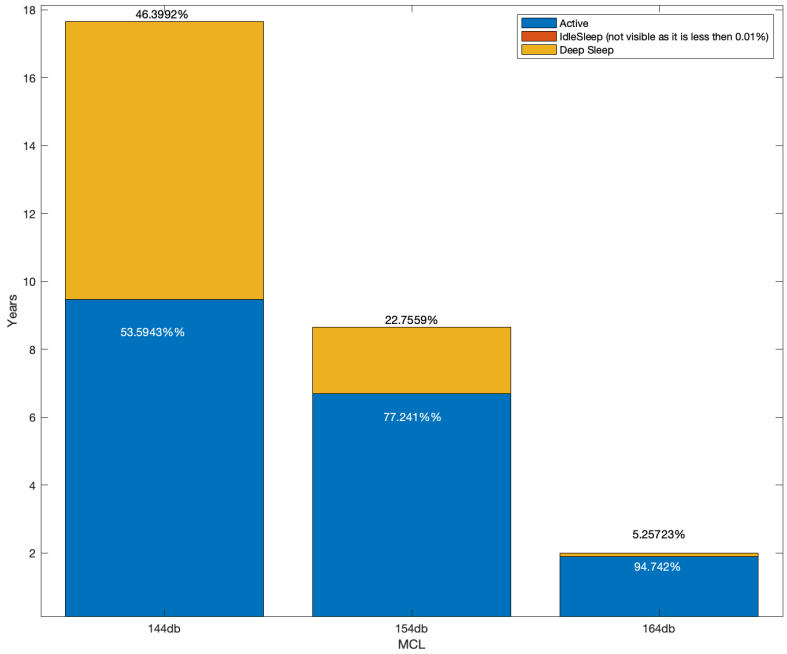


Figure 5.1: Battery lifetime of an NB-IoT node in the baseline scenario using communication parameters $t = 2h$, $b_{up} = 200byte$, and $b_{down} = 60byte$ under various MCL conditions.Baseline scenario: no bandwidth limit, perfect battery, no jamming attack.

of it. While a $t = 2h$ transmission interval might be deemed aggressive, there are a number of real-world applications (electric meters, water level meters, wildlife monitors and others) that require such a schedule. It is worth mentioning that the idle sleep mode is represented in Figure 5.1, but is less than 0.01%, making it difficult to visualise.

5.1.2 Jamming Attacks in Virtual Environment

Table 5.1 presents the results of our evaluation, which examines Energy Depletion Rate (EDR) and Jammer Duty Cycle (JDC) across different attack types, specifically sDQS, iDQS, RAP, and iDQS + RAP.

Type	EDR	JDC
1.Baseline	0	0
2.sDQS	0.41	1
3.iDQS	0.41	0.0026
4.RAP	0.76	0.0223
5.iDQS + RAP	0.85	0.0246

Table 5.1: EDR and JDC metrics for the different attack types evaluated (sDQS, iDQS, RAP, and iDQS + RAP).

Simple Jammer

When analysing a simpler jammer performing an sDQS attack, we can observe the lack of efficiency, having a Jammer Duty Cycle (JDC) of 1. This is expected as this type of malicious device is designed to always transmit and is not capable of analysing any communication patterns. When the interference power level is precisely set, the Energy Depletion Rate (EDR) attack is on par with the iDQS attack. However, this precision level is very hard to achieve in an uncontrolled environment, and setting it too high might block the transmission entirely, therefore forcing the UE into a cell reselection procedure. Similarly, setting the transmission power to low might have little to no effect for a QPSK encoded transmission. In practice, the sDQS attack benefits from its simplicity and ease of deployment but is limited by its need for precise power levels and a constant power supply, making it easy to detect.

Intelligent Jammer

Compared to the simple jammer, the intelligent jammer is highly effective with a JDC ranging from 0.0026 to 0.0246. This variation depends on the selected exploit (iDQS, RAP and iDQS + RAP), which also impacts the EDR. The most effective attack is the combination of iDQS + RAP, having an EDR of 0.85 and a joint energy effort of 0.0026 + 0.0223, representing the JDC of iDQS RAP attacks. When examining the overall results, we can see that while EDR can be doubled from the iDQS, JDC increases nearly tenfold.

Further on, we assess the efficacy of the intelligent jammer in greater

detail. We will consider varying payload sizes for both downlink and uplink (b_{down} and b_{up}) and separate the EDR results accordingly, as shown in Figure 5.2). Moreover, Figure 5.3 depicts the relationship between JDC and EDR in both uplink and downlink for various payload sizes.

Figure 5.2 depicts the EDR for sending and receiving different payload sizes. It plots the results of multiple simulations with incremental payload from 0 to 300 bytes for both uplink b_{up} and downlink b_{down}. An EDR of zero means that there is no interference with the communication channel and is equivalent to our baseline scenario. A value of one represents an attack that has a theoretical impact of 100% on the battery lifespan. The Energy Depletion Attacks (EDAs) targeting the downlink (receiving) channels are coloured in blue, while the EDAs directed towards the uplink (sending) channels are highlighted in orange. The iDQS is the least efficient attack for both uplink and downlink. However, its efficiency increases non-linearly with the payload size. As expected, the uplink channel is more susceptible to EDAs due to the increased power consumption needed for sending data. On the other hand, the RAP attack consistently impacts the channel, no matter the payload size, as it exclusively targets the Msg1 from the random access procedure.

When comparing the downlink and the uplink channels, we can observe a big difference in impact. For the downlink channel (receiving), the highest effect is the iDQS + RAP attack with a depletion rate of ≈ 0.55. Similarly, in the uplink (sending), the most impactful attack is also the iDQS + RAP, with a depletion rate of ≈ 0.9.

For a better understanding of the efficiency of each attack, Figure 5.3 plots the uplink EDR (blue) against the Jammer Duty Cycle (JDC) (orange). It is worth mentioning that the slight differences in results from Figure 5.2 are explained by the fine adjustment an intelligent jammer has to make in order to perform an EDA instead of an DoS attack (see Section 3.1). The highest EDR impact with the least effort (represented by a low JDC) is the iDQS. Additionally, it is evident that as the payload size increases, the EDR shows a much steeper incline compared to the JDC, making it more effective with larger payloads. The RAP attack is linear as the payload size does not influence it. Contrary to the iDQS, the combination of iDQS+RAP converses with a slight ascending trajectory for EDR over the payload size, while the JDC trajectory is steeper.

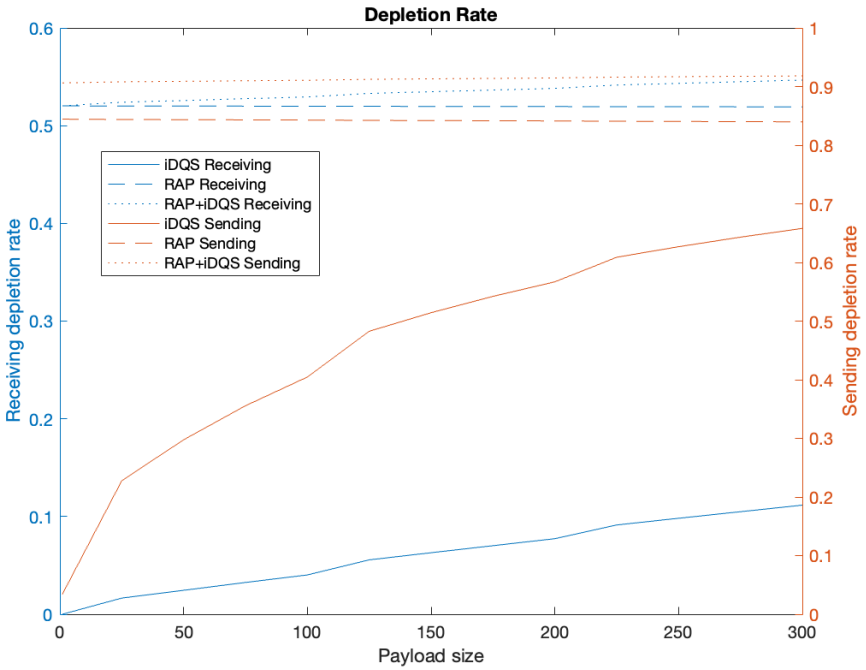


Figure 5.2: EDR for the receiving (downlink) and sending (uplink) channels for various attacks (iDQS, RAP, and iDQS + RAP). Communication parameters are set to $t = 2h$, $0 < b_{up} \leq 300$ bytes, and $0 < b_{down} \leq 300$ bytes.

5.1.3 Jamming Attacks in Physical Environment

We extended our research presented in Section 5.1.2 to a physical environment. We choose to focus on the downlink shared channel by using the testbed elaborated in Section 4.2. Moreover, targeting the MIB-NB, SIB1-NB and SIB2-NB by jamming or corrupting the messages forces the UE to drain its battery faster. This effect is explained as a result of the additional listening time T_R, a UE has to extend due to repeated attempts in decoding the corrupted messages or the time spent in reacquiring the jammed message. We used this T_R as a measurement of the effectiveness of the jamming attack. As explained in Section 4.3.2, the maximum T_R is not governed by the 3GPP specification and is dependent on the UE own implementation. Therefore, our T_R reflects only the acquisition of one Information Block message. We used T_D as the time delay the UE has to sustain before a retransmission of the targeted message is performed. This measurement is important as additional delays can pressure the overall performance

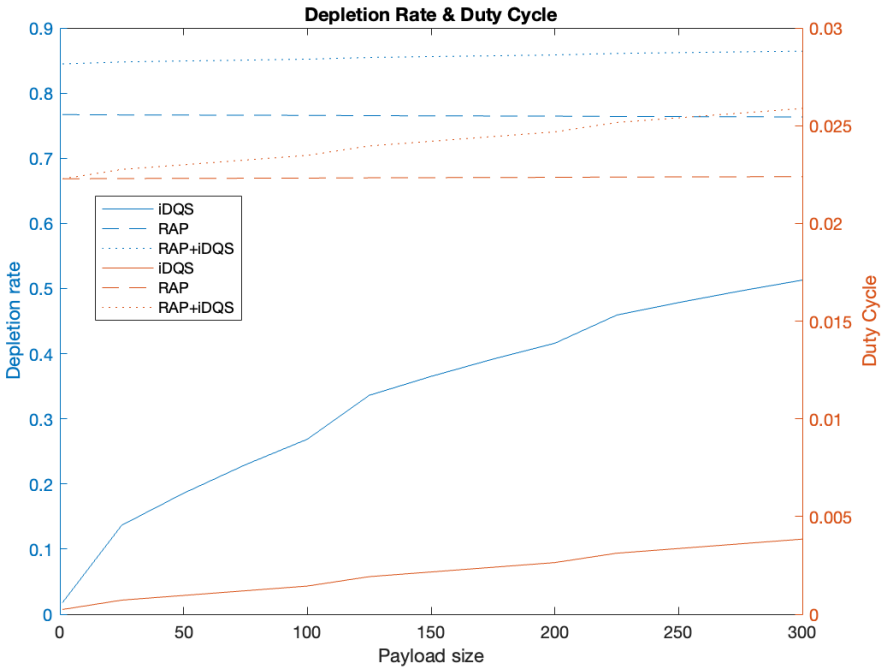


Figure 5.3: EDR (blue) and JDC (orange) relationship, for various attack types (iDQS, RAP, and iDQS + RAP). Communication parameters are set to $t = 2h$, $0 < b_{up} \leq 300$ bytes, and $0 < b_{down} \leq 300$ bytes.

of the network. For example, if we consider the transmission pattern of the MIB-NB (see Section 2.2.1), a $T_R = 64ms$ can be achieved by performing a MIB-NB attack, as described in Section 3.2.3. The delay will result in a $T_D = 640ms$ as the 64 CSBs containing the MIB-NB are allocated to every subframe 0 of an SFN. Comparably, performing a SIB1-NB attack (see Section 3.2.4) derives a $T_R = 32ms$ and $T_D = 2560ms$ while targeting the SIB2-NB (see Section 3.2.5) results in $T_R = 192ms$ and $T_D = 5120ms$. Table 5.2 summarises our findings. Both the T_R and the T_D are independent of the MJ or the MI attack technique.

Akin to the attacks presented previously, the secondary objective of the malicious entity is to remain undetected. T_J denotes the jamming time necessary in preventing the reception of a MIB-NB, SIB1-NB or SIB2-NB. Depending on the type of attack and the targeted message, the T_J varies. Therefore, for an MJ attack against the MIB-NB $T_J = 8ms$, while for SIB1-NB $T_J = 4ms$ and $T_J = 24ms$ for a SIB2-NB attack. In case of

Target	User Equipment Measurement		MJ	MI
	T_R	T_D	T_J	T_J
MIB-NB	64ms	640ms	8ms	1ms
SIB1-NB	32ms	2560ms	4ms	4ms
SIB2-NB	192ms	5120ms	24ms	24ms

Table 5.2: Evaluation of MIB-NB, SIB1-NB, and SIB2-NB based on Active Receiving Time (T_R), Delay Time (T_D), and Active Jamming/Injecting Time (T_J)

an MI a $T_J = 1ms$, $T_J = 4ms$ and $T_J = 24ms$ corresponding to MIB-NB, SIB1-NB and SIB2-NB can be achieved. An MI attack is preferable because it consumes less energy than jamming a subframe with an MJ attack, and its transmission footprint is indistinguishable from a legitimate one. Additionally, when targeting the MIB-NB, the MI attack only needs to replace a single subframe to trigger a failed CRC. All the results are presented in Table 5.2.

In terms of energy depletion, a typical NB-IoT transmission, as shown in Figure 2.6, would consume 23360 mW when using a Sara N3-NB-IoT chipset [23]. Listening for an additional 1 ms would require 80 mW. Assuming an allowance of 10 failed messages, an attack against the MIB-NB would lead to an increase in energy consumption of 297.2%, 198.6% for SIB1-NB, and 691.7% for SIB2-NB.

5.1.4 Evaluation Discussions

Virtual Environment

In our virtual environment, we presented two types of jamming devices: the simple jammer and the intelligent jammer (MJ). The simple jammer's main advantage is the ease of construction and use. It needs to be capable of transmitting noise at a precise frequency and power to degrade the quality of the signal. This can be achieved with *off the shelves* SDRs without any complex programming. However, because it needs to constantly transmit a jamming signal, no matter if a communication is happening or not, it requires a constant power supply. Moreover, due to its inability to observe the communication channel, it cannot react to frequency hopping or cell reselection procedures. Overall, the simple jammer is easy to use and has a fast deployment time, but it lacks the flexibility to remain undetected or to

handle changes in the transmission pattern.

On the other hand, an intelligent jammer is a complex device that requires a deep understanding of the NB-IoT protocol. It needs to observe and learn the communication pattern between an UE and the eNodeB, as well as time precisely its transmission. Furthermore, the low power consumption resulting from brief transmission periods enables the malicious device to operate on battery power. All of this creates an environment where an intelligent jammer can remain undetected for a longer period of time. As an example, when performing an iDQS attack (described in Section 5.1.2) for a scenario with $t = 2h$, $b_{up} = 200byte$ and $b_{down} = 200byte$ it results in a JDC of 0.0026. Utilising the same transmission chip and battery as the targeted UE, the intelligent jammer can operate for more than two years. This estimate follows from the known endurance of the UE in the baseline scenario (over two years) [75] and the fact that the jammer's transmissions, as reflected in the JDC value of 0.0026, occupy significantly less airtime per event than those of the UE. The reduced duty cycle directly lowers the average energy draw, meaning that—under equivalent hardware constraints—the jammer's operational lifetime would meet or exceed that of the UE[179, 180]. Moreover, when targeting the base scenario, depicted in Figure 5.1, it can deplete the battery from 17 years to just under two years when deploying an iDQS attack, six months for a RAP attack, and four months for iDQS + RAP

Physical Environment

The physical testbed described in Section 4.2 validated our presumption developed in the virtual environment. We have proven that by using an SDR such as the HackRF One, a bad actor can jam individual subframes (MJ attack) or even replace them (MI attack). We have also shown that an MI attack has higher efficiency than an MJ and can mask itself as a legitimate transmission. This, in turn, makes the jamming device very hard to discover and would require physical identification and removal to mitigate its effects. A variant of the MI attack has been proven by Yang et al. [156] against the legacy LTE called Physical Signal Overshadowing (SigOver) attack. It utilises the same capture effect vulnerability as this work. Furthermore, we believe that an MI device can exploit other attack opportunities beyond the battery depletion one. Such devices could potentially exploit various as-

pects of network vulnerability, leading to broader implications for network security and integrity. Consequently, it is crucial to further investigate and develop robust countermeasures to detect and mitigate these advanced jamming techniques, ensuring the resilience of future wireless communication systems.

5.2 EDT+ Impact and Evaluation

5.2.1 EDT+ Power Profiles

In NB-IoT devices, Power Saving Mode (PSM) (deep sleep) accounts for the bulk of energy consumption [181]. A device enters PSM between transmissions, and its length is dictated by the periodicity of transmissions p (every hour, twice a day, every week, etc.) minus the length of the transmissions procedures (usually between a couple of seconds, up to 20-30 sec). During the PSM, the UE tries to reduce the consumption as much as possible by stopping any communication. Optimising the energy consumption of the PSM becomes a hardware limitation, and it is directly correlated to the chip's efficiency during deep sleep.[180]. Moving forward, we will focus only on the transmission procedures when analysing energy efficiency and optimisation. The value in the real world varies significantly regarding the transmission length. The data below represent a simulation run in a perfect environment without data loss, with only one packet and no repetitions.

Figure 5.4 shows the power profile of a normal NB-IoT transmission during our NS3 simulation. It is worth mentioning that the simulation was done with near-perfect conditions, a data size of 49 bytes (chosen to guarantee a single NPUSCH transport block (no segmentation) under the evaluated settings), and only one repetition [28]. Figure 5.4 depicts only a snapshot of the profile, and in the real world, it can extend up to 30 seconds, similar to [181]. Here, we can see that once the device wakes up, it starts the synchronisation procedure by acquiring the NPSS, NSSS, MIB-NB and other information blocks required to send the NPRACH preamble in MSG1. The device is able to optimise its energy usage by switching from Receiving (RX) to IDLE mode because of the known index frame of the NPSS, NSSS, MIB and SIB1.

One of the main advantages of EDT+ is the reduced energy consumption

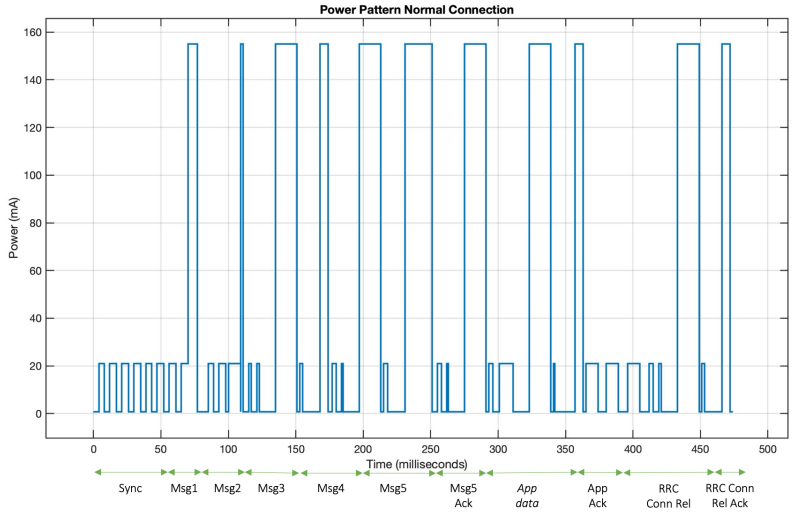


Figure 5.4: NS3 Power Profile Normal NB-IoT Data Transmission.

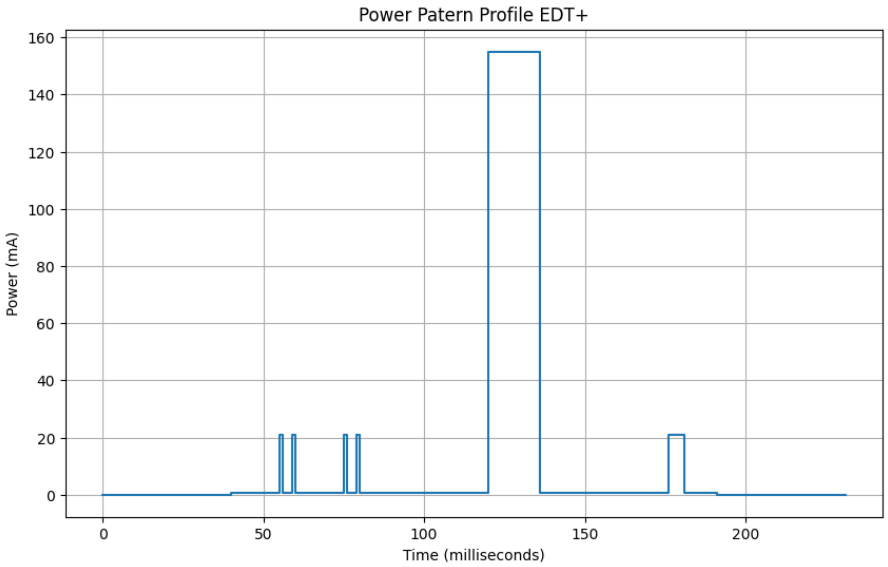
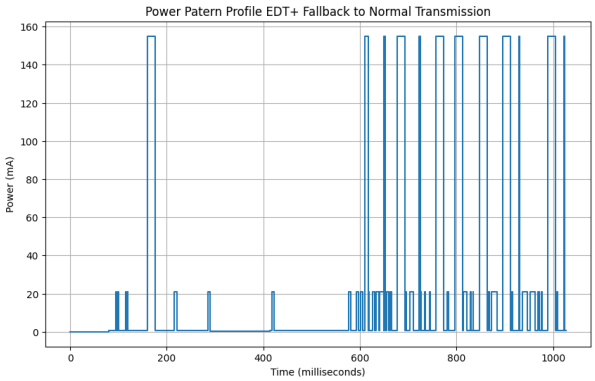


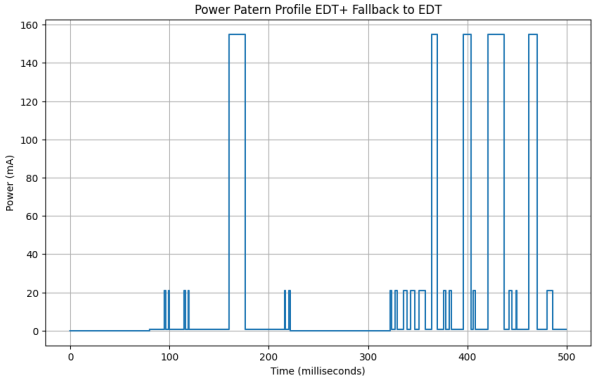
Figure 5.5: NS3 Power Profile EDT+ Data Transmission.

during transmission. In a successful transmission, the EDT+ protocol wakes up, acquires the NPSS and NSSS, and directly transmits its data, followed by receiving the ACK alongside the parameters for the following transmissions. All of this is reflected in the EDT+ power profile, Figure 5.5. The nature of the protocol allows fewer RX and Transmitting (TX) interactions, thus

minimising the time needed for the User Equipment (UE) to be active.



(a) Power Profile EDT+ Fallback Normal Transmission.



(b) Power Profile EDT+ Fallback EDT Transmission.

Figure 5.6: (a) Power Profile EDT+ Fallback Normal Transmission. (b) Power Profile EDT+ Fallback EDT Transmission.

On the downside, if the UE misses their allocated time windows, it needs to fall back to normal or EDT transmission mode. Meaning that it will waste both time in terms of latency and, more importantly, energy. Figure 5.6 illustrates the power profile for normal (a) and EDT fallback (b). Comparing the two of them from an efficiency perspective, it is clear that the EDT fallback is more efficient in terms of energy and latency *(latency measured per report as the elapsed time from UE wake-up to receipt of the downlink ACK/feedback on the NPDCCH, including random-access, scheduling, and UL transmission)*, thus arguing that it will be a better choice in case EDT+ fails.

In Table 5.3, the energy distribution is shown in a fully simulated environment between the deep sleep and the transmission modes over different

time intervals. This environment closely resembles the settings shown in the NS3 power profiles (Figures 5.4 and 5.5), which assume perfect conditions with a single packet transmission, no data loss, no repetitions, and most importantly, no inactivity timer. The percentages of energy used for deep sleep and transmission for the Normal, EDT, and EDT+ transmission modes across various time intervals are displayed in the table. Similar to previous findings and simulations cited therein, which is that a substantial amount of the device's energy is used up while it is in the Power Saving Mode (deep sleep). This thorough analysis makes it easier to understand how significantly the deep sleep period affects total energy efficiency. It also emphasises how successful the EDT+ protocol is in reducing active transmission and reception times, which maximises energy utilisation.

Periodicity	**Normal**		**EDT**		**EDT+**	
	Trans.%	**Sleep%**	**Trans.%**	**Sleep%**	**Trans.%**	**Sleep%**
30 min	76.15	23.85	48.98	51.02	28.29	71.71
1 hr	61.48	38.52	32.44	67.56	16.48	83.52
2 hrs	44.39	55.61	19.36	80.64	8.98	91.02
6 hrs	21.01	78.99	7.41	92.59	3.18	96.82
12 hrs	11.74	88.26	3.85	96.15	1.62	98.38
1 day	6.24	93.76	1.96	98.04	0.82	99.18
2 days	3.22	96.78	0.99	99.01	0.41	99.59
7 days	0.94	99.06	0.28	99.72	0.12	99.88

Table 5.3: Percentage of energy used for transmission and deep sleep across different periodicities for each transmission mode in a **perfect environment, no repetition, one packet, no data loss, no inactivity timer.**

We define the following variables in the context of evaluating the energy efficiency of EDT+ transmission schemes with possible fallback:

- $P_{\text{success, EDT+}}$: The success rate for EDT+ transmissions.
- $E_{\text{EDT+}}$: The energy used for EDT+ transmissions.
- E_{fallback}: $E_{\text{EDT+}}$ + the energy used for fallback transmissions.

The following is a mathematical expression for the generalised expected energy consumption, or E_{expected}, taking into account the dynamics of successful and fallback transmissions:

$$E_{\text{expected}} = P_{\text{success, EDT+}} \cdot E_{\text{EDT+}} + (1 - P_{\text{success, EDT+}}) \cdot E_{\text{fallback}} \quad (5.1)$$

Taking into account the trade-off between energy efficiency and dependability under various operating profiles and conditions, the formula 5.1 can help inform strategic decisions about whether and when to utilize EDT+. If we consider E_{expected} to be equal to the energy consumption of normal transmission or EDT, noted as E_{a}, we can calculate the success rate threshold under which EDT+ is no longer viable as follows:

$$S_{\text{threshold}} = \frac{E_{\text{normal}} - E_a}{E_{\text{EDT+}} - E_a} \tag{5.2}$$

When applying the formula to the ideal scenario (perfect environment, no repetition, one packet, no data loss, no inactivity timer), the calculated thresholds for reverting to either normal transmission or EDT due to inefficiencies in EDT+ are as follows:

- Success Rate Threshold for normal fallback = 12.32%
- Success Rate Threshold for EDT fallback = 41.09%

5.2.2 Impact of inactivity timer in real-world scenario

According to [59], the inactivity timer shows the amount of time that a UE is accessible from both uplink and downlink traffic. The RRC inactivity timer is reset, and the duration of this state is increased each time traffic is sent or received in RRC CONNECTED [75]. The inactivity timer's main purpose is to give the possibility for the UE to receive or send additional messages. It is set by the eNodeB, and usually, it is chosen as 10, 20 or 30 seconds. The UE can switch to a lower energy mode like extended Extended Discontinuous Reception (eDRX) or PSM after the inactivity period goes off in order to save energy. Because the inactivity timer controls how long a device stays in a higher energy consumption state before shifting to a more energy-efficient mode, its duration can have a major impact on the energy efficiency and battery life of NB-IoT devices [181]. Multiple research [181, 75, 182, 179] point out the shortcomings of the inactivity timer in terms of energy consumption. For instance, in the study carried out by Yang et al. [181] across various real-world settings, it was discovered that 75% to 91% of the energy consumed during data transmission was attributed to devices waiting for the 20-second inactivity timer to elapse, exceeding 3000 mJ per transmission no matter the ECL. It was shown that in a

typical deployment, such as a smart parking system [183], a device with poor coverage (ECL2) transmitting five packets per day lasted only 270 days on battery life. According to [181], reducing the inactivity timer to three seconds would increase the device lifetime to 440 days. Figure 5.7 showcases a simulation for a normal transmission, where the inactivity timer is set by the eNodeB to 10 seconds. Furthermore, the inactivity timer might be exploited in battery depletion attacks as presented in chapter 5.

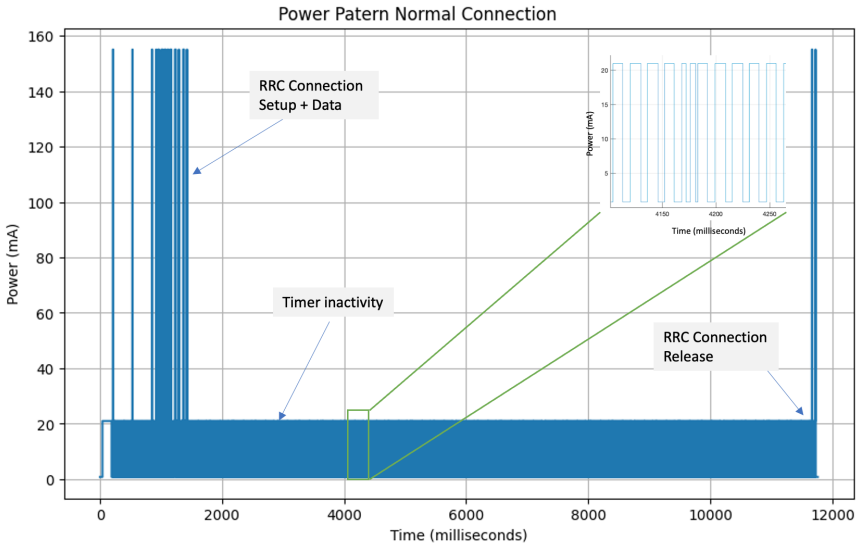


Figure 5.7: Power Profile for Normal Transmission with an inactivity timer of 10 sec.

To mitigate these challenges, 3GPP Release 14 [59] introduced an uplink message known as the Release Assistance Indication (RAI). This brief message, sent from the UE to the eNodeB, signals that the UE has no further uplink data to transmit and does not await additional downlink data. Consequently, it allows the eNodeB to close the RRC prematurely connection before the Inactivity Timer runs out. Unfortunately, as noted by [181], awareness and implementation of this feature remain limited, and few telecommunications networks/developers have implemented it to this day.

The inactivity timer behaviour does not impact the EDT+ protocol as we do not utilise the RRC connection procedure nor the same logic for releasing the connection. In case the UE needs to receive additional downlink messages, the eNodeB will transmit the number of expected downlink messages

together with the data ACK. On the other hand, in case the UE needs to change the number of uplink messages, it needs to fallback to normal transmission or EDT and ask the eNodeB for a new EDT+ configuration. This approach, while successfully mitigating the energy expenditure during the inactivity timer, limits the UE in terms of flexibility. It will receive the additional downlink messages only on the next transmission. It will reset all its parameters learned by the eNodeB and risk denial of EDT+ access.

5.2.3 EDT+ Preliminary Study

In our preliminary study [29], we wanted to compare a simplified EDT+ framework against the C-IoT-Opt and EDT modes. This study provided the necessary baseline data to evaluate the performance and resource efficiency of the EDT+. Additionally, it offered insights into its potential benefits and limitations within the context of static NB-IoT UEs.

In the simplified version of EDT+, we employed the scenarios presented in Table 5.4. The goal was to cover a wide range of applications and conditions to ensure a comprehensive analysis and robustness of real-world use cases. For this reason, the scenarios leverage parameters such as payload size and device density.

Application	**No. of Devices in a Single Cell**	**Reporting Interval Uplink**	**Uplink payload [bytes]**
High Density	172800	1/day	49
Water metering	37500	1/day	200
Gas metering	37500	4/day	100
Parking management	8000	1/hour	100
Watering	200	2/day	100

Table 5.4: Evaluation Scenarios Summary highlighting Data Volume for Uplink Communications, Application Type, Device Density, and Reporting Interval.

For the High-Density Scenario, we reference the work of Pascal et al. [28] to act as a benchmark, enabling a direct comparison with the established EDT transmission. It reproduces the environment in Pascal's study by deploying 172,800 UEs for a single eNodeB, transmitting daily a payload of 49-byte. The other scenarios are drawn from real-world deployments as described by Fattah et al. [56] and represent practical utility management systems with different reporting intervals and device densities. The corresponding uplink payload per report is set to 100–200 bytes at the appli-

cation layer (excluding RLC/MAC/PHY overhead), reflecting typical meter identifiers, timestamps, consumption counters, and alarm flags in such deployments [56]. Furthermore, to simulate real-world conditions, a non-ideal physical channel model was used, incorporating three distinct ECL as described in Section 2.4.3.

In this study [29], we tested our assumption of improved battery lifetime, network capacity and latency by leveraging the simplified payload transmission process of the EDT+.

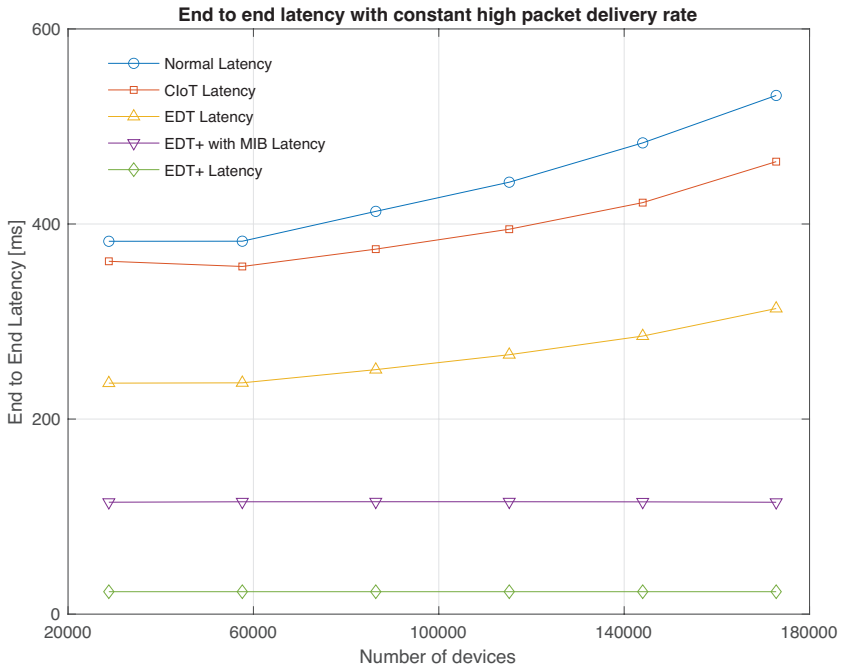


Figure 5.8: End-to-end latency, assuming the device has a small CFO drift for "EDT+ with MIB" and a minimum drift for "EDT+", that allows reaching its designated window. The simulation assumes that SIB1 and SIB2 have already been received in non EDT+ transmissions.

In Figure 5.8, the end-to-end latency (the elapsed time from UE wake-up to receipt of the downlink ACK on the NPDCCH, including random-access, scheduling, and UL transmission) is measured in ms for the different modes of operations. Similar to the values achieved by [28], the Normal and the CIoT values start just under 400ms while the EDT starts at around 230ms. For all of these transmissions, we can observe an increase in latency once

there are more than 60000 devices active daily. The increase can be explained by the limited processing power of the eNodeB and timer expiration on the UE side. Even though small, we've also observed package collisions (around 50) during the random access procedure in more challenging situations with over 100000 active devices. These are due to multiple UEs selecting the same NPRACH preamble and saturation of the RAR window, so some contenders are not served in that occasion. The same behaviour has been observed by Pascal et. al. [28]. On the other hand, the EDT+ and EDT+ with MIB-NB acquisition latency remains constant no matter the number of active UEs. This consistency is achieved by allowing the eNodeB to schedule the UE transmissions. There is a small variation (not visibly discernibly on the graph) for the EDT+ with MIB-NB acquisition due to how MIB-NB is transmitted. In the ideal scenario where the UE CFO is minimal, or the UE is capable of compensating for it, the latency is just 23ms as the device wakes up from PSM and immediately transmits data. In a more realistic scenario where the UE has a small CFO and needs to acquire the MIB-NB in order to determine the SFN, the latency peaks at around 127ms, with lows close to 109ms, depending on the timing of the wake up in relation to the subframe number.

In Fig. 5.9, it is evident that the Normal and CIoT transmissions exhibit very similar power consumption in the High-Density scenario, which is also reflected in the battery lifetimes. Consistent with the findings of Pascal et al. [28], EDT demonstrates better energy efficiency compared to Normal and CIoT transmissions, extending battery lifetime to just over 20 years. When considering EDT+ transmission, there is a notable power reduction to as low as 4.2 W/s, compared to 5 W/s for EDT. This reduction is attributed to the lower number of messages that need to be sent with EDT+. Consequently, energy consumption improvements translate to an approximate 20% increase in battery lifetime compared to EDT, using the same NS3 battery configurations as described by Pascal et al. [28].

To simulate more realistic scenarios, we examined gas meter, water meter, parking, and watering scenarios as previously outlined. Fig.5.10 shows the daily energy utilisation for the scenarios presented in Table 5.4. Although hourly transmission may seem aggressive, energy harvesting technologies such as solar and wind [184] can support such settings. For contexts that do not require frequent transmissions and high payload sizes, innovative

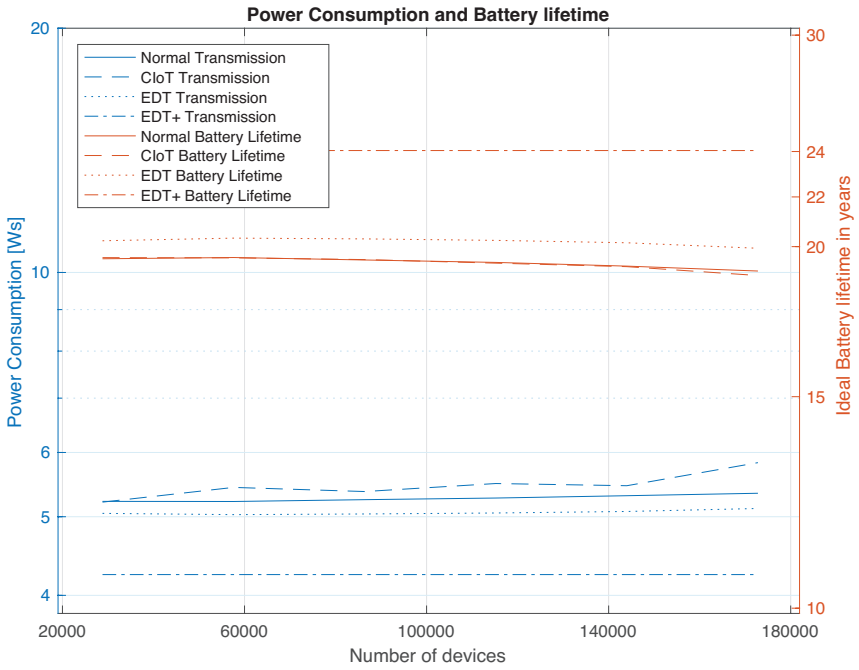


Figure 5.9: Ideal battery lifetime and power consumption for High-Density scenario with minimum CFO drift. Inactivity timer present.

approaches such as piezoelectric or thermoelectric solutions, as discussed by [185], could allow UEs to become energy independent.

5.2.4 Static Time Window

Further on, we will focus on a more advanced implementation of the EDT+, and we will be using the scenario presented in Section 3.3.7. These use cases will assist in analysing various techniques for connecting and transmitting payloads in EDT+ mode.

Static time window equally distributed

To calculate a static time window w, equally distributed within a t simulation time (5 minutes), we will need to divide t by the number of devices n (100 devices), as shown in 5.3, resulting in $w_{\text{static and equal}} = 3$ seconds.

$$w_{\text{static and equal}} = t/n \tag{5.3}$$

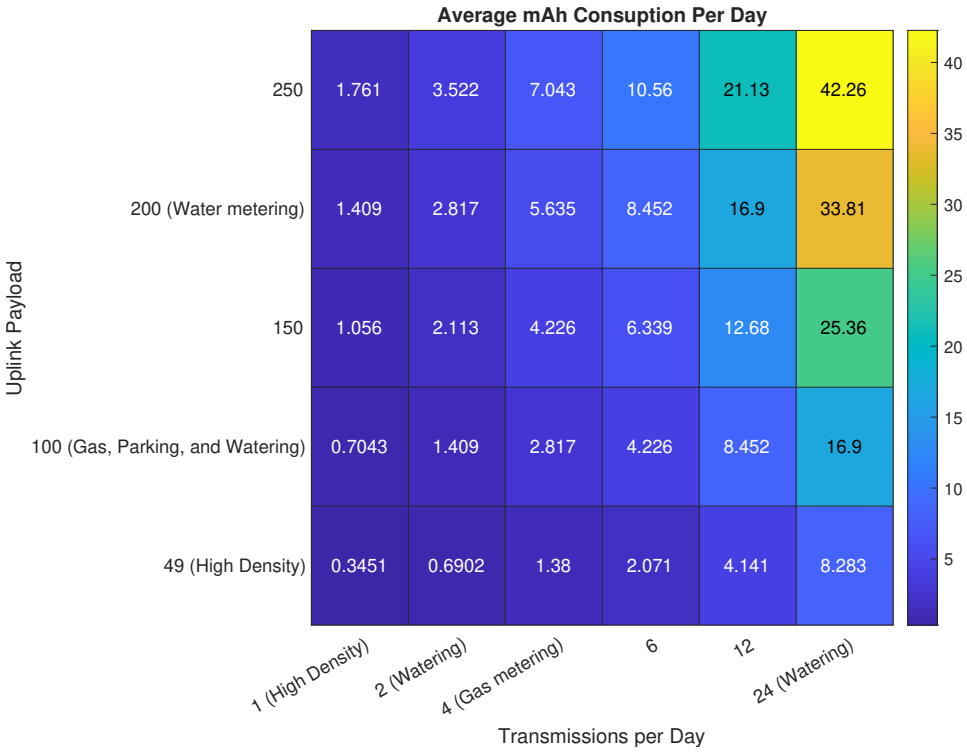


Figure 5.10: Average energy used per day, factoring in the size of the uplink payload and the number of transmissions occurring daily.

In the first static scenario, we considered perfect environment conditions and an upload data size of 49 bytes transmitted within a single packet. For a time window of 3 seconds

Figure 5.11 show the above-mentioned scenario. We can clearly see that a time window of 3 seconds is more than enough for a periodicity of up to 6 hours. For a periodicity of 12 hours, the success rate falls to around 85%. This accuracy still provides benefits when we consider the efficiency calculated from in 5.2. On the other hand, if we consider periodicity of one day or more, we can see that a three-second time window is not viable in case the UE is cable of transmitting in EDT, but still suitable in case the eNodeB accepts only normal fallback.

Static time window correlated to periodicity

The logic function to calculate the time window, given a fixed clock accuracy and periodicity, can be represented as follows:

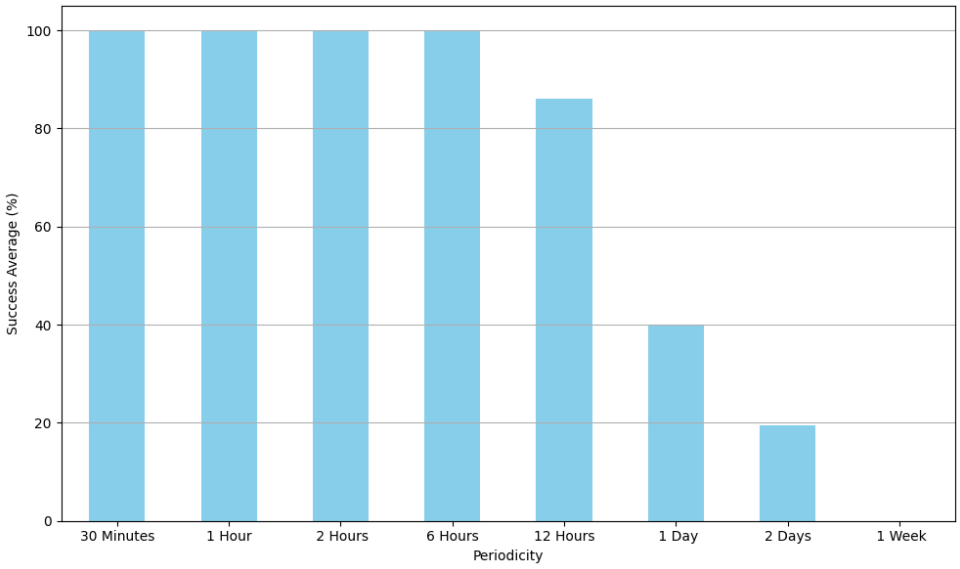


Figure 5.11: Success Rate Variation for 100 devices across Different Periodicity, for a time window size of 3 seconds, 49 bytes, perfect environmental conditions, no clock drift variation.

$$w = \frac{a}{10^6} \times p \tag{5.4}$$

- a represents the clock accuracy in PPM
- p represents the periodicity in milliseconds.
- w represents the time window in milliseconds.

Considering that a is usually represented as a range $\pm a$ (i.e., ± 40 PPM), a becomes $\max a$ and we need to double the window size, in order to account for $-a$ and $+a$. Giving the following:

$$w = 2 \times (\frac{a}{10^6} \times p) \tag{5.5}$$

We also need to make sure that the start of the time window is offset by minus $-a$ and round it up to the nearest 0.5 milliseconds for uplink time-slots compliance.

In Figure 5.12, we considered the correlation between the length of the time window and the periodicity of each transmission scenario. We conducted 1400 transmissions and averaged the results for every 100 entries.

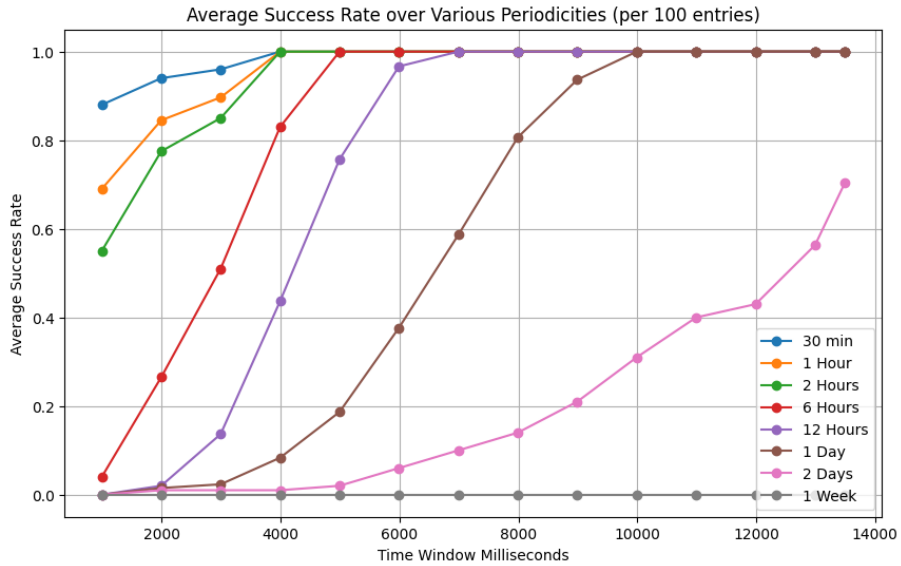


Figure 5.12: Success Rate Variation across Different Periodicity, for incremental time window, 49 bytes, and perfect environmental conditions, 1400 transmission/periodicity.

The success rate fluctuation can be explained due to the value of a, which was set to ±40 PPM. While the time window always considered the $\pm \max a$, the UE might have a lower clock drift than the absolute $\pm \max a$, which made it eligible for a shorter time window allocation. Once the time window exceeds the absolute $\pm \max a$, the success rate starts to converge to 1. The limitation of this approach is that the algorithm is not flexible enough to account for UE that have clock accuracy better than the maximum drift specified. For a periodicity p of one week, the time window would need to be $\approx$ 48 seconds

5.2.5 Environmental impact on clock accuracy using EDT+

According to Marco et al., [186] and Haapala et al.[97], temperature and especially temperature variation greatly affect clock accuracy. Marco et al. showed that within one day, the difference could be 56.6 °C, and within one hour, it can be as high as 34.9 °C. [186]. Both studies have shown that the clock oscillators tend to run faster with lower temperatures, while higher temperatures will have the opposite effect and slow down, thus accumulating delays. Oscillators use crystal cuts to resonate as close to the

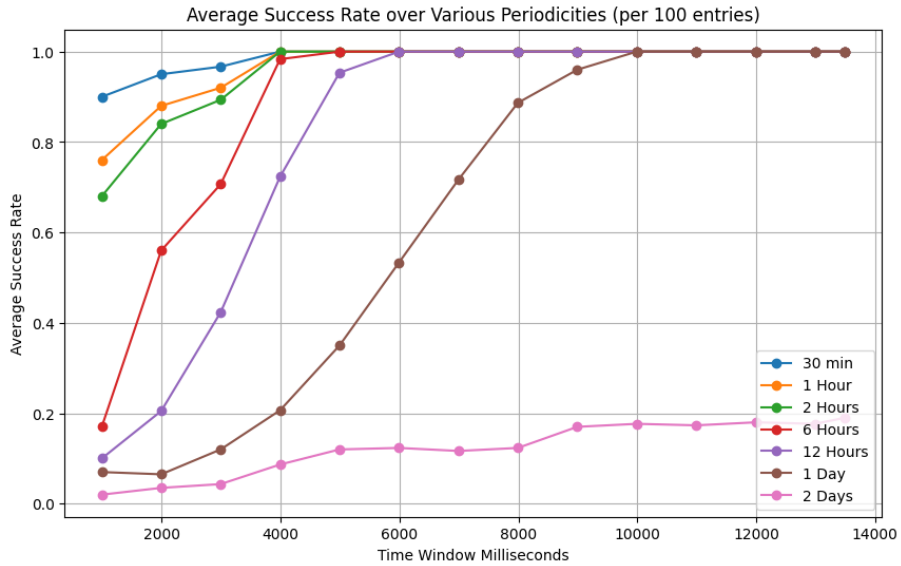


Figure 5.13: Success Rate Variation across Different Periodicity, for incremental time window, 49 bytes, with temperature variation, 1400 transmission/periodicity.

target frequency at room temperature. A multitude of crystal cuts (i.e., CT, DT, XY, BBT.) frequency offset can be described using a quadratic or cubic function in the case of the common AT cut. However, in practice, manufacturers often use different batches with different cuts without specifying the type of cut used in the data sheet [186]. Considering all of this, we decided to model our simulator by averaging the results found by Marco et al. at ± 1.244 ppm/°C for a random range of ± 28.3 °C resulting in the previously mention variation of 56.6 °C in a single day and ± 17.95 °C which represent the maximum fluctuation in a single hour [186]. Figure 5.13 quantifies this effect: to achieve a success rate of ≥ 0.95, short periodicities ($\leq$2 h) require windows of ≈3–4 s, 12 h requires ≈5–6 s, and daily reporting ≈9–10 s; multi-day periodicities are more sensitive and require substantially longer windows to reach the same threshold.

5.2.6 Dynamic Time window

Given a clock accuracy, a uniformly distributed over a range of $[-x, x]$ parts per million (PPM), the goal is to analyse the impact of this variation on clock drift and, consequently, on determining a sufficient time window. To

capture the event within the clock's accuracy range, we consider both the length and the start offset of the time window.

Further, we will explain the concepts of Exponential Moving Average (EMA) and target success rate in the context of clock drift and temperature variation simulations for NB-IoT devices. We also discuss how these parameters are adjusted using a Proportional-Integral-Derivative (PID) controller to meet desired performance criteria.

The EMA is a moving average that places weight and significance on the most recent data points. It is helpful in this simulation because it helps to smooth out short-term fluctuations and highlight longer-term trends in clock accuracy affected by temperature variations.

In our context, the EMA is calculated iteratively for each transmission of a device. The formula used is:

$$\text{EMA}_t = \alpha \cdot x_t + (1 - \alpha) \cdot \text{EMA}_{t-1}$$

Where:

- EMA_t is the EMA at the current time step.
- α is the smoothing factor, also known as the decay factor.
- x_t is the current value of clock accuracy adjusted by temperature.
- EMA_{t-1} is the EMA calculated at the previous time step.

The initial EMA (EMA_0) is set to the adjusted clock accuracy of the first transmission. Typically, a normal transmission is where the device asks for permission to transmit in EDT+, as explained in 3.3.4. By always storing the clock accuracy of each device, the base station is able to adjust the window offset for each transmission precisely and also take into consideration the clock ageing drift. Taking this into consideration, the only factors that can impact the accuracy are the environmental factors, in our case, temperature.

Target Success Rate

To properly evaluate the performance of the dynamic window, we developed an algorithm that calculates the necessary time window for a desired success

rate. The target success rate refers to the proportion of successful transmissions where the clock drift remains within acceptable bounds. The success rate is influenced by the accuracy of the clock and the effects of temperature variations over time.

To achieve a specific target success rate, the code uses a Proportional-Integral-Derivative (PID) controller to adjust the parameters dynamically. The PID controller aims to minimise the error between the current success rate and the target success rate by adjusting three parameters:

- K_p (Proportional gain): Determines the reaction to the current error. In the code, $K_p = 0.001$.
- K_i (Integral gain): Determines the reaction based on the sum of all past errors. In the code, $K_i = 0.001$.
- K_d (Derivative gain): Determines the reaction to the rate of change of the error. In the code, $K_d = 0.005$.

The PID controller adjusts the α, *success_factor*, and *failure_factor* parameters to achieve the desired success rate.

The adjustment process involves:

1. Calculating the current success rate based on the EMA and the required time window for each transmission.
2. Computing the error as the difference between the target success rate and the current success rate.
3. Updating the parameters using the PID controller formula:

$$\text{adjustment} = K_p \cdot \text{error} + K_i \cdot \sum \text{error} + K_d \cdot \frac{d(\text{error})}{dt}$$

4. Modifying EMA's α, *success_factor*, and *failure_factor* to reduce the error in subsequent iterations.

Figure 5.14 to 5.16 depict the dynamic time window adjustment for one device over 1400 transmissions. The figures illustrate the variation in the time window and success rate for different periodicities, specifically 0.5 hours, 1 hour, 2 hours, 6 hours, 12 hours, and 24 hours.

In each figure, the blue line represents the adjusted time window, the red line indicates the average success rate and the green dashed line marks the average window size. The target success rate is set at 85%.

- Figure 5.14 illustrates the scenario for a periodicity of 0.5 hours, with an average window size of 15.2ms.
- Figure 5.15 illustrates the scenario for a periodicity of 1 hour with an average window size of 54.9 ms.
- Figure 5.17a illustrates the scenario for a periodicity of 2 hours with an average window size of 114.4ms.
- Figure 5.17b illustrates the scenario for a periodicity of 6 hours with an average window size of 334.3ms.
- Figure 5.17c illustrates the scenario for a periodicity of 12 hours with an average window size of 1125.9ms.
- Figure 5.16 illustrates the scenario for a periodicity of 24 hours with an average window size of 2284ms.

In our dynamic window sizing algorithm, the first window size is big enough to accommodate a successful transmission. In the case it fails, as seen in 5.14 and 5.15, it will aggressively increase its value in order to get the first successful transmission. We design the algorithm in this way so that we can quickly find a successful set of parameters and optimise them for future transmission. In our study, we choose to implement a target success rate that will force the algorithm to find specific parameters for increasing and decreasing the window size to achieve the desired success rate. Setting a target to 100% with an error tolerance of 0.001 will result in a window size close to the static one. On the other hand, as explained in 5.5, setting a target of just 41% would provide little to no benefit in terms of energy saving. Through multiple experiments, we found that a target success rate between 95% and 85% yields the optimum ratio between successful transmission and window sizing. For all scenarios, the parameter configurations to reach the desired target were 19 iterations.

Upon analysing all of the scenarios, we can observe more similarities than differences. It becomes apparent that the first transmission's success

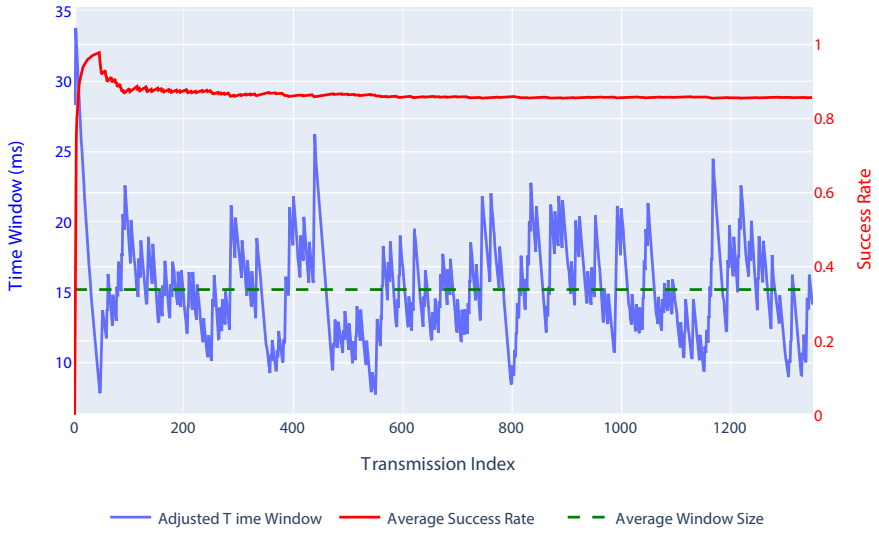


Figure 5.14: Dynamic time window for one device, 1400 transmission, with a target success rate of 85% for a periodicity of 0.5 hours.

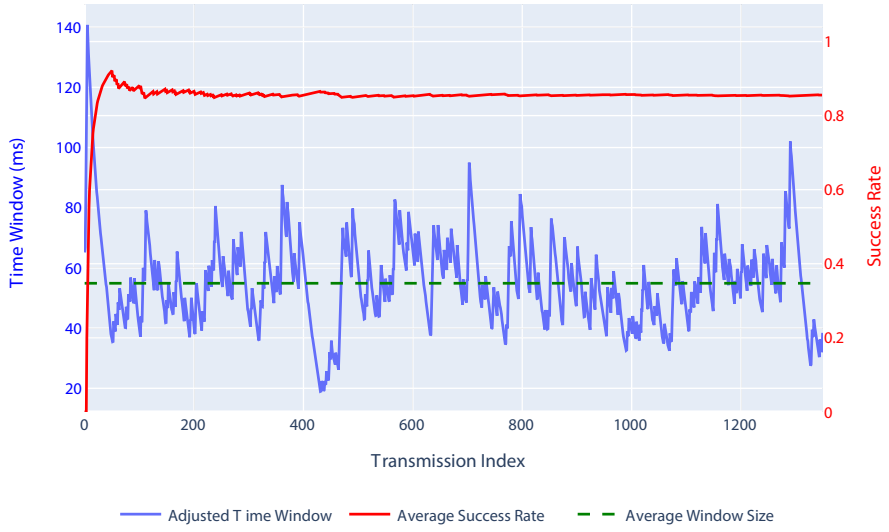


Figure 5.15: Dynamic time window for one device, 1400 transmission, with a target success rate of 85% for a periodicity of one hour.

rate tends to be close to 100% and then starts to average down and becomes stable once the parameters adjustment reflects the desired target. On the other hand, the window size keeps fluctuating due to environmental factors.

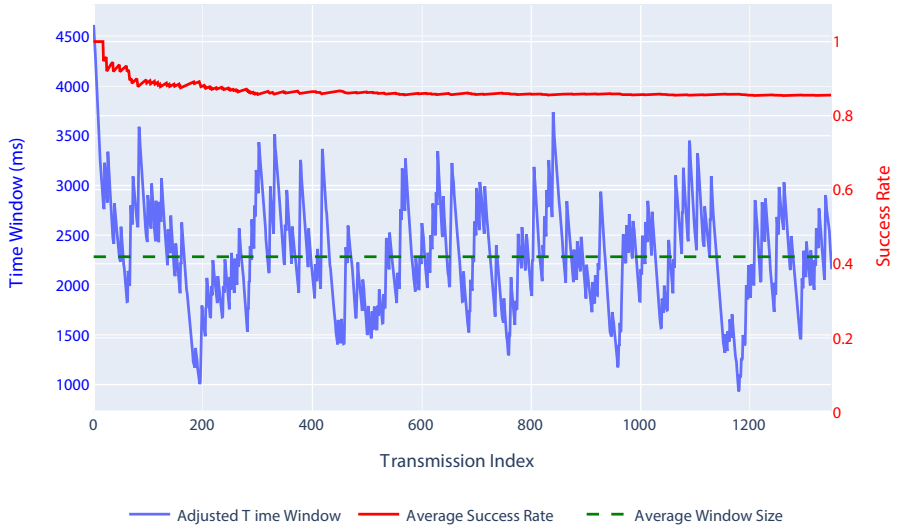
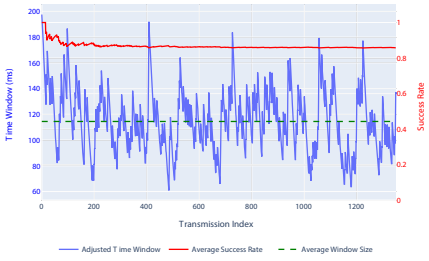
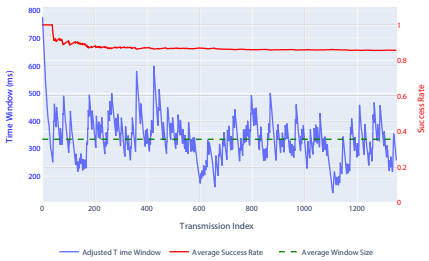


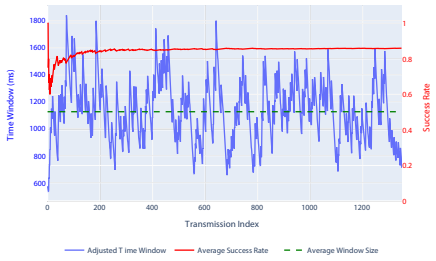
Figure 5.16: Dynamic time window for one device, 1400 transmission, with a target success rate of 85% for a periodicity of 24 hours.



(a) 2-hour periodicity (target 85%).



(b) 6-hour periodicity (target 85%).



(c) 12-hour periodicity (target 85%).

Figure 5.17: Dynamic window behaviour for 2 h, 6 h, and 12 h periodicities (target success 85%). Panels arranged with 2/6 h on the top row and 12 h centred beneath.

Consistent with this trend, Figure 5.17 compares 2,h, 6,h, and 12,h periodicities. The controller maintains the 85% target while the window scales with the sleep period p: the average window increases from 114.4,ms (2 h) to 334.3,ms (6 h) and 1125.9,ms (12 h). At 2 h the window stays around 60–200,ms with rapid recovery after occasional misses; at 6 h both the mean and spread grow as clock error and temperature drift accumulate; at 12 h larger windows are selected to preserve the target. Even so, the overall energy overhead remains limited because the device opens a receive window only once per period.

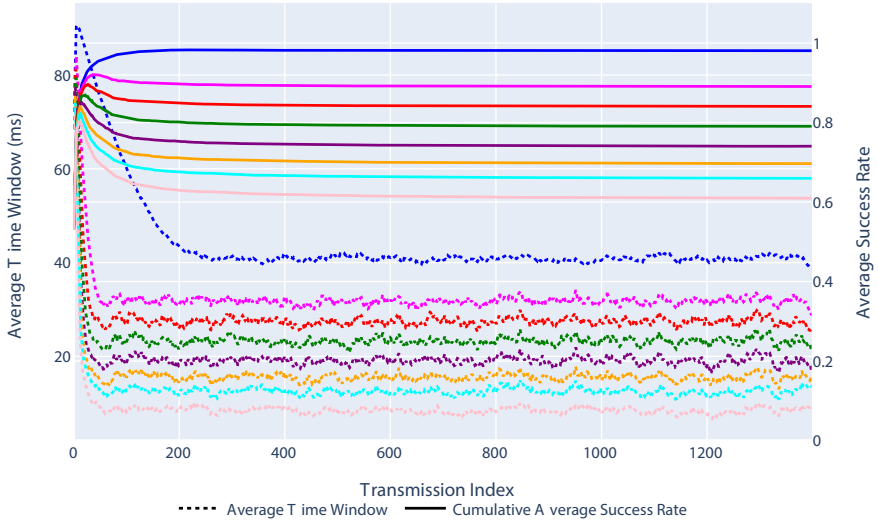


Figure 5.18: Dynamic time window for 100 devices, 1400 transmission, with a target success rate of 85% for a periodicity of one hour.

When we analyse the overall picture as seen in Figure 5.18 and 5.19, we can observe consistent behaviour within multiple success targets with time window sizing being somewhat equally divided when correlated with the intended success rates. The only outlier is the 99%, which, as expected, needs a higher margin of error. The average time window sizes can be seen in Table 5.5. Despite the fact that we developed the model around more extreme cases (see Section 5.2.5), the similarities shared across the scenarios make this approach predictable, which by itself provides benefits like device management, resource allocation, robustness, and energy harvesting capabilities. Overall, these figures demonstrate the system's ability to dynamically

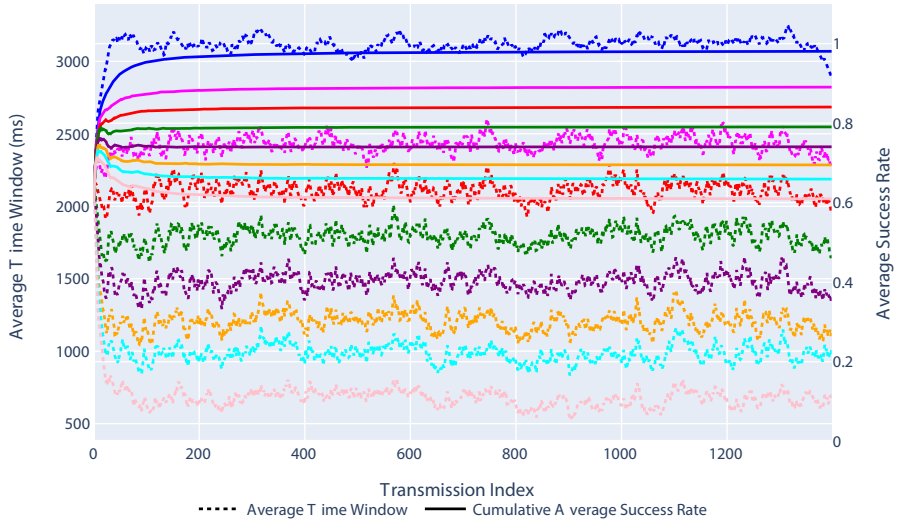


Figure 5.19: Dynamic time window for 100 devices, 1400 transmission, with a target success rate of 85% for a periodicity of 24 hours.

Periodicity	99%	90%	85%	80%	75%	70%	65%	60%
0.5 hours	22.27	16.35	14.08	11.97	9.92	8.17	6.71	4.63
1 hour	44.33	32.59	28.09	23.83	19.71	16.19	13.15	9.07
2 hours	88.82	65.08	56.10	47.81	39.47	32.16	26.19	18.27
6 hours	266.61	196.12	169.66	143.29	118.37	96.86	78.41	54.43
12 hours	530.89	390.60	336.67	284.83	236.12	193.61	158.97	109.55
24 hours	3114.13	2418.90	2081.33	1766.82	1458.88	1178.99	960.15	660.81

Table 5.5: Average Time Window Sizes (ms) for Different Target Success Rates.

adjust the transmission time window to achieve a consistent success rate across different periodicities. The adjustments are more frequent and have a larger amplitude for shorter periodicities, while they are less frequent but more substantial for longer periodicities.

5.2.7 Potential security vulnerabilities of EDT+

A first residual concern is *capability and pattern leakage* arising from the expanded RRC Msg3 used to request EDT+. If the "EDT+" flag and sizing hints (e.g., `transmissionPeriodicity`, `payloadSize`) are conveyed before confidentiality is active, a passive observer could fingerprint device classes or infer traffic profiles from the mere presence and length of these information

elements.

A second residual risk is *system-level resource-reservation abuse*. A compromised/ rouged fleet can issue repeated EDT+ requests or keep changing parameters, causing the eNodeB to reserve large listening windows or many repetitions that are then under-used. This wastes scheduler capacity and reduces cell availability, independent of any per-link cryptographic protection. Practical controls are straightforward: apply per-UE admission and rate limits to EDT+ requests; cap the per-cell budget of concurrent EDT+ windows/repetitions; enforce *used-vs-granted* checks with automatic downgrade to EDT or Normal on persistent underuse; and raise alerts on abnormal request patterns [30, 29].

5.3 Battery Depletion Attacks Mitigation

One of the main vulnerabilities identified in the attack analysis (Chapter 5) is the deterministic nature of NB-IoT devices, where their transmission times are generally fixed and occur at regularly spaced intervals. UEs typically transfer data at fixed intervals, often with a consistent timestamp (for instance, every 12 hours or daily at 10:30 am). This determinism generates two key issues.

The first one is network overcrowding and performance degradation. The simultaneous transmission of numerous devices leads to network congestion, which increases latency and energy consumption. In turn, this limits the device density that an eNodeB can support and also reduces the network's overall performance. The second one deals with exploitation by Smart Jammers. As shown in Section 3.1, jamming attacks exploit any predictable transmission patterns. Smart jammers can learn the transmission schedules of NB-IoT devices, therefore saving their energy by becoming active only when NB-IoT devices are transmitting. In other words, smart jammers can transmit intermittently, with periods of idleness in between, which could allow them to remain undetected for a long period of time and even elude detection by any RF spectrum-sensing software. This could lead to severe network security issues for the communication protocol, resulting in an increased risk of unreliable performance of the devices that rely on that network.

5.3.1 Mitigating Predictability with Dynamic Scheduling

Scope. The scheduling mechanism is implemented and evaluated in simulation in this work; however, it has not been tested under adversarial (jamming) conditions, so the security effects discussed here are inferred rather than measured.

These vulnerabilities can be mitigated by using a dynamic transmission scheduling where the eNodeB determines the next transmission time based upon the expected communication pattern preferred by the UE (e.g., every day, twice a day, every week) and a pseudo-random slot allocation that takes into consideration the predictive load of the cell. Using this strategy, the transmission schedule will become less deterministic, making it also less predictable for potential adversaries. The expected benefits follow.

Increased Energy Expenditure for Malicious Entities:

Randomising transmission times within that window means that any smart jammer would have to stay active longer before it had any chance of capturing, let alone jamming, any communications. This wastes more of its energy reserves, limiting the ability of any smart jammers to attack effectively.

Higher Detection Probability and Complexity for Attackers:

Requiring the jammer to be active for extended periods increases the likelihood that the network's monitoring systems will detect the jammer. Moreover, the jammer might have to use alternative power sources to fuel prolonged jamming activities, further increasing the cost and complexity of the attack. Increased complexity raises the potential for detection and mitigation of jamming attacks.

5.3.2 The Benefits of Dynamic Transmission Scheduling

Implementing dynamic transmission scheduling involves several techniques to ensure effective mitigation. First, transmission times are randomised within a window. For example, the device might have been commanded to transmit at 10:30 am daily. Using EDT+, the transmission would be chosen randomly between 10:00 am and 11:00 am by the eNodeB. This randomness makes it harder to time an attack because the correct target time

now becomes unpredictable. Second, the network can easily adopt adaptive scheduling for EDT+ UEs. This means the eNodeB dynamically adjusts the transmission schedules based on network conditions and historical information. During a period of high traffic, transmission intervals might be tweaked to spread the traffic load out more evenly and, therefore, lessen the probability that the network gets congested and slows down. Third, a priority-based scheduling could become viable. Some data are more important or urgent and so have to be beamed through at unpredictable or more secure times, while other data can support very high latencies. Prioritising these streams is possible due to evenly spread traffic. It could make the jammer's task more complex, as it would have to classify or target particular types of communication.

Overall, the predictability of NB-IoT devices' transmissions leads to systematic vulnerabilities, congestion of the network, and vulnerability and exposure for malicious entities to exploit. Our proposed dynamic transmission scheduling approach, where the eNodeB allocates the times for transmission, reduces these susceptibilities by increasing the attacker's energy consumption and detection probability. It can improve network performance through evenly distributed traffic at different times and frequencies, and it also improves system security and robustness against targeted attacks on NB-IoT devices. In the future, with further advancements in machine learning, collaborative scheduling and more powerful security protocols, we envision a more secure and robust NB-IoT protocol.

Chapter 6

Conclusion

6.1 Summary of Key Findings

The primary objectives of this research were threefold. Firstly, we wanted to analyse the effects of Energy Depletion Attack (EDA) against Narrowband Internet of Things (NB-IoT) devices, focusing on how they would impact the energy expenditure as well as the lifespan and viability of NB-IoT operations. Secondly, we wanted to develop and enhance existing NB-IoT simulation testbeds in order to establish a framework for future research. Lastly, we proposed a new communication mode called EDT+ that significantly improves the lifespan of an NB-IoT UE by taking advantage of the static nature of NB-IoT devices. Additionally, it reduces the impact of a battery depletion attack and smart interfering techniques.

6.1.1 Key Results

In Section 4, we detailed the development and utilisation of several NB-IoT testbeds and demonstrated their use in assessing the NB-IoT protocol. For analysing the efficiency and impact of Energy Depletion Attack (EDA) against NB-IoT devices, we based our primary testbed on the HackRF One SDR and srsRAN software suite. This allowed us to conduct experiments on the MJ and MI adversarial attacks, providing insights into their effects on device energy consumption and lifespan. Additionally, we used the MATLAB LTE module to set up a controlled environment for simulating and assessing simple and smart jamming techniques against NB-IoT UEs. Moreover, we employed the LENA-NB-IoT module in NS3, which provided us with the

necessary framework to develop the new EDT+ communication mode and assess its efficiency. With these tools, we offer a comprehensive set of results, including the vulnerability of NB-IoT devices to battery depletion attacks and the efficacy of our EDT+ mode. We have made the source code for our testbeds publicly available in the hope that it will cater to future NB-IoT research.

The NB-IoT simulations employed in this paper have shown that the energy use of an NB-IoT device can be compromised by various types of jamming attacks, leading to more than 90% of its energy depleted, which would reduce the device lifetime from 17 years to approximately four months. Additionally, by utilising MJ or MI techniques (see Section 4.3.3) against poorly configured UEs, we predict that a malicious entity can prevent an NB-IoT device from entering sleep mode, therefore, degrading the lifespan from years to days. Considering all of this, we conclude that a jamming device using the attacks described in this work can jeopardise the commercial viability of any NB-IoT deployment.

Furthermore, this research introduces a new communication mode Improved Early Data Transmission (EDT+). It is a novel approach designed to improve the energy efficiency of static NB-IoT devices. We have demonstrated that an EDT+ device utilises significantly less energy compared to normal or EDT transmission. Our results show a minimum of 20% improvement in battery lifespan with the inactivity timer still active, which can have an impact between 75% and 91% on the energy consumed during transmission. Additionally, in certain favourable scenarios—such as one-hour periodicity, with no repetition, no data loss, and no inactivity timer—EDT+ can reduce the transmission cost drastically. Specifically, it can lower the battery percentage used for normal transmission over the device's lifetime from approximately 61.5% to as little as 16.48%.

6.1.2 Implications of Results

We believe that the implications of this research results should impact the deployment and maintenance of NB-IoT technologies. The susceptibility of NB-IoT devices to jamming attacks requires careful evaluation of the security risk before wide deployment. These vulnerabilities should be addressed before any operation or financial losses occur. Therefore, we consider that it is imperative for stakeholders to adopt effective countermeasures and design

strategies to minimise the consequences of such jamming attacks.

The optimisation by EDT+ leads to substantial energy savings, which is an important factor in making long-term deployments viable. Additionally, it can motivate the investigation of energy-harvesting technologies for NB-IoT devices. In the case of static nodes – which is often the case in NB-IoT applications such as smart meters, in-field agricultural sensors, or environmental monitoring - EDT+ yields substantial energy savings and can help mitigate smart jamming techniques.

6.2 Limitations of the Study

This work addresses several technological and methodological limitations, focusing on the evolution of the NB-IoT protocol. Following are the limitations and constraints that we have identified and acknowledged in our study.

Technological Constraints: This research encompasses a snapshot of the evolution of the NB-IoT protocol from the fall of 2019 until early 2024. At the beginning of the study, resources were limited, and the technology was scarcely available in Europe. Work such as Cellular Internet of Things written by Olaf et al. [55] represented a ground stone in the start of this research, explaining the procedures used by NB-IoT. However, the rules and regulations imposed by the licensed spectrum, as well as the high cost of running telecommunication equipment inside a Faraday cage, limited our experimentation to simulation environments. By extending the capabilities of the proven simulations which reflect the real world [187], such as LTE-Toolbox and NS3, we were able to conduct virtual simulations in a safe and affordable manner. Furthermore, by shifting the spectrum to an unlicensed one with the help of SDRs, the research managed to test and validate our theoretical findings in the physical world.

Limitation of Threats: The cyber threats presented in this work focus on Energy Depletion Attack (EDA). Even though some of the techniques employed to perform EDA make use of other types of attacks, such as eavesdropping, DoS, or MITM, this research is limited to understanding and mitigating battery depletion vulnerabilities. It is important to acknowledge that IoT security, including CIoT, is a multifaceted domain involving a multitude of potential threats beyond EDA. For instance, physical tam-

pering can compromise device integrity, while advanced cyber-attacks such as MAC or IMSI cloning (in the context of CIoT) can impact the whole network. Therefore, different IoT communication protocols are exposed to different types of cyber threats, and while some overlap, others are specifically designed to target a particular protocol or, more granularly, a specific use case. Consequently, this study provides an insight into EDA specifically targeted towards NB-IoT devices. Nevertheless, it does not cover the entire spectrum of cyber attacks an NB-IoT device might be vulnerable to.

Limitation of Energy Model: Although many battery simulation models try to encompass all aspects of a battery, including but not limited to State of Charge (SOC), degradation, and lifespan, we opted to utilize a perfect battery model in all our simulations. This decision was made to provide a clear understanding of our theoretical premises and to validate them effectively. Furthermore, in real-world deployments, we expect a slight impact in our estimations from the batteries' physical differences, the battery types, the environment contrasts, and the configurations of the network and the User Equipment (UE)

Simulation vs. Real-World Deployment: We acknowledge the inherent limitations of the simulation tools used, such as hardware imperfections and the lack of varied environmental interference that have an impact on the performance of the NB-IoT protocol. One example where real-world deployment might influence the results found in this research is the accuracy of the internal oscillator. This accuracy can have a big influence on the enhancement of the protocol presented in Chapter 3.3. While we tried to the best of our knowledge to model the simulation for a suit of extreme use cases, we understand that each deployment varies from one to another in terms of environment, hardware, deployment modes and available infrastructure. Consequently, these limitations can influence the effectiveness of proposed solutions in practice. Even though the results presented in this study may not perfectly reflect the behaviour seen in commercial deployments, we regarded them as close enough to be worth considering.

Dynamic Nature of IoT Security: NB-IoT security and procedures evolve with new 3GPP releases. Our analysis is version-locked to the specifications and software used during 2019–2024. We provide the models and parameter sets so that results can be re-run and compared as releases change; the vulnerabilities in Chapter 5 should be re-validated, as well as the EDT+

evaluation in Chapter 3.3 against their target release and vendor stack.

Generalisability: While the findings described in this work might offer insight into the NB-IoT security and might be applicable to other communication protocols as well, we advise caution against overgeneralising the results across the whole LPWAN landscape. For reference, one of the exploits described in Chapter 5 makes use of the high repetition number of up to 128 for the uplink channel [55]. This feature is specifically designed into the NB-IoT protocol, and while the same approach might be adjusted for other communication protocols, the results will differ.

To conclude, acknowledging the limitations of this research is essential for providing a realistic and clear context of the research findings. The focus of improving the NB-IoT's robustness and efficiency through gaining knowledge into battery depletion attacks as well as proposing EDT+ operation mode highlights notable progress. However, the simulation constraints, environmental diversity, network configurations, and manufacturing differences underscore the necessity for continuous caution and adaptation against new exploits.

6.3 Recommendations

We believe that the NB-IoT technology will play a crucial role in the ever-growing world of interconnected devices. It offers clear advantages to other LPWAN technologies, such as single-hop communication, superior security, scalability, utilisation of existing infrastructure and many others. At the time of writing (2025), NB-IoT adoption remains strongest in **Asia** (especially China) while being widely available across Europe. China reported 1.8 billion licensed cellular–IoT connections in 2022 [188]. In the **EU**, commercial NB-IoT networks are broadly deployed and cross-border NB-IoT roaming has been live since 2020, later expanded across roughly twenty countries [189, 190, 191].In the **UK**, low-cost NB-IoT tariffs exist (e.g., 1NCE "€10 for 10 years," 500,MB included) [192]. Prototyping hardware such as the DFRobot Arduino NB-IoT Expansion Shield cost around £48 at UK distributors [193]. The often-quoted US$5 device target stems from Release-13 cost/complexity goals in 3GPP and industry documents [4, 194, 2]. Licensed spectrum improves reliability but restricts open experimentation, requiring specialised equipment and permissions. Given these factors and our results,

we propose the following recommendations for advancing NB-IoT:

For widespread adoption and innovation, NB-IoT deployments need to be more cost-effective. This is true not only for the data plans but also for the hardware required for development and testing. Such a reduction would also be more in line with the 3GPP target and could make the technology available to a much wider base of users and researchers. Taking into consideration the phasing-out of the GSM spectrum, we believe that it could be a perfect medium for the NB-IoT network while at the same time maximising the spectrum utilisation.

Furthermore, we believe that the development of end-to-end simulation tools as well as equipment for deploying private NB-IoT networks will be important for academic and industrial research. Improved and open-source tools that allow researchers to create, configure and test private NB-IoT networks for experimental purposes will help to lower the cost of entry and encourage innovation. Given the importance of security in NB-IoT networks, developing and implementing jamming detection algorithms such as the ones presented by Morillo et al. [21, 195] is essential. These approaches could enable the distinguishing of the actual occurrences of jamming and unintentional interference. The ability of NB-IoT to scale up to a reliable, secure platform depends on these pathways being mapped and incorporated into the system.

Besides interference detection, there is a need for smart jamming mitigation without human interference. Design such as the EDT+ can help in minimising the malicious effect. Similar strategies will increase the robustness and reliability of the NB-IoT networks, especially in large-scale deployment scenarios such as urban areas or places with high device density. Moreover NB-IoT deployments are often static. Optimising protocol efficiency in these installations can lead to considerable increases in energy efficiency, data throughput, spectrum efficiency, and network performance. Adopting EDT and EDT+ configurations would improve network efficiency and sustainability for cellular IoT.

These recommendations seek to address the current challenges and limitations faced by NB-IoT networks. Implementing them will help to develop more efficient and cost-effective NB-IoT solutions. Additionally, it will encourage more research opportunities and a wider adoption of this promising technology in the future.

Acronyms

3GPP 3rd Generation Partnership Project

ACK Acknowledgement

AWGN Additive White Gaussian Noise

BLER Block Error Rate

BS base station

C-IoT-Opt Cellular Internet of Things Optimization

CE Coverage Enhancement

CFO Clock Frequency Offset

CIoT Cellular IoT

CRC Cyclic Redundancy Check

CSB Code Sub-Block

DoS Denial of Service

DQS Degradation of Quality of Signal

ECL Extended Coverage Level

EDA Energy Depletion Attack

EDR Energy Depletion Rate

eDRX Extended Discontinuous Reception

EDT Early Data Transmission

EDT+ Improved Early Data Transmission

EMA Exponential Moving Average

eNodeB Evolved Node B

GSM Global System for Mobile Communication

H-SFN Hyper System Frame Number

H-SFN Hyper-System Frame Number

HFN Hyper Frame Number

iDQS intelligent Degradation of Quality of Signal Attack

IoT Internet of Things

JDC Jammer Duty Cycle

LoRaWAN Long Range Wide Area Network

LPWAN Low Power Wide Area Network

LSB Least Significant Bit

LTE Long-Term Evolution

MCL Maximum Coupling Loss

MCS Modulation and Coding Scheme

MI Message Injection

MIB-NB Narrowband Master Information Block

MIB Master Information Block

MITM Man in the Middle Attack

MJ Message Jamming

mMTC machine-type communication

MSB Most Significant Bit

Msg1 Random Access Preamble Transmission

Msg2 Random Access Response

NB-IoT Narrowband Internet of Things

NF Noise Figure

NPBCH Narrowband Physical Broadcast Channel

NPDCCH Narrowband Physical Downlink Control Channel

NPDSCH Narrowband Physical Downlink Shared Channel

NPRACH Narrowband Physical Random Access Channel

NPSS Narrowband Primary Synchronization Signal

NPUSCH Narrowband Physical Uplink Shared Channel

NRS Narrowband Reference Signal

NSSS Narrowband Secondary Synchronization Signal

OFDM Orthogonal Frequency-Division Multiplexing

PCID Physical Cell Identity

PCIDs Physical Cell Identities

PI Interference amount

PLMN Public Land Mobile Network

PN Thermal Noise

PNeff Effective Noise Floor

PRACH Physical Random Access Control Channel

PRB Physical Resource Block

PRXmin Receiver Sensitivity

PSM Power Saving Mode

PTX Power Level at the Antenna Connector

PUR Preconfigured Uplink Resources

QoS Quality of Signal

QPSK Quadrature Phase Shift Keying

QPSK Quadrature Phase Shift Keying

RAI Release Assistance Indication

RAP Random Access Procedure

RAR Random Access Response

RB Resource Block

RE Resource Element

RRC Radio Resource Control

RSRP Reference Signal Received Power

RSRQ Reference Signal Received Quality

RSSI Received Signal Strength Indicator

RU Resource Unit

RX Receiving

SC-FDMA Single-Carrier Frequency-Division Multiple Access scheme

sDQS simple Degradation of Quality of Signal Attack

SDR Software Defined Radio

SFN System Frame Number

SI System Information

SIB System Information Block

SIB System Information Block

SIB1-NB Narrowband System Information Block 1

SIB2-NB Narrowband System Information Block 2

SigOver Physical Signal Overshadowing

SINR Signal-to-Interference and Noise Ratio

SNR Signal-to-Noise Power Ratio

SNRmin Minimum Signal-to-Noise Power Ratio

TAO Time-of-Arrival Offset

TBS Transport Block Size

TCTS Temperature Compensated Time Synchronization

TCXO Temperature Compensated XO

TOP Timing Offset Propagation

TTI Transmission Time Interval

TX Transmitting

UE User Equipment

UNB Ultra Narrowband

WLAN Wireless Local Area Networks

XO Uncompensated Crystal Oscillator

BLE Bluetooth Low Energy

TDOA Time Difference of Arrival

AoA Angle of Arrival

CNI Critical National Infrastructure

IT Information Technology

OT Operational Technology

IIoT Industrial Internet of Things

SDN Software-Defined Networking

NS Network Slicing

MEC Multi-access Edge Computing

5GC 5G Core

UPF User Plane Function

SLA Service-Level Agreement

URLLC Ultra-Reliable Low-Latency Communications

mMTC massive Machine-Type Communications

5GS 5G System

EPS Evolved Packet System

AI Artificial Intelligence

NS Network Slicing

NPN Non-Public Network

UPF User Plane Function

APN Access Point Name

MEC Multi-access Edge Computing

RAN Radio Access Network

IT Information Technology

OT Operational Technology

SNOW3G SNOW 3G stream cipher

AES Advanced Encryption Standard

ZUC ZUC stream cipher

PKI Public Key Infrastructure

CA Certification Authority

CNI Critical National Infrastructure

NAC Network Access Control

MNO Mobile Network Operator

WLAN Wireless Local Area Network

SDN Software-Defined Networking

IIoT Industrial Internet of Things

TSN Time-Sensitive Networking

QoS Quality of Service

SLA Service-Level Agreement

5GC 5G Core

URLLC Ultra-Reliable Low-Latency Communications

LTE-M Long Term Evolution for Machines

MME Mobility Management Entity

AKA Authentication and Key Agreement

NAS Non-Access Stratum

AS Access Stratum

USIM Universal Subscriber Identity Module

EARFCN E-UTRA Absolute Radio Frequency Channel Number

GBA Generalised Bootstrapping Architecture

Bibliography

[1] C. Lundqvist, A. Keränen, B. Smeets, J. Fornehed, C. R. B. Azevedo, and P. von Wrycza, "Key technology choices for optimal massive iot devices," Ericsson Technology Review, January 9, 2019, 2019. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/key-technology-choices-for-optimal-massive-iot-devices

[2] Ericsson, "Nb-iot: A sustainable technology for connecting billions of devices," Ericsson Technology Review, 2016. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/nb-iot-a-sustainable-technology-for-connecting-billions-of-devices

[3] GSMA, "Mobile iot in a 5g future," GSMA, White paper, October 2024. [Online]. Available: https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/wp-content/uploads/2024/10/Mobile-IoT-in-a-5G-Future-Final.pdf

[4] *3GPP Low Power Wide Area Technologies*, 3GPP, 2016.

[5] S. Sinha, "LPWAN market 2024: Licensed technologies boost their share among global 1.3 billion connections as LoRa leads outside China," feb 2024. [Online]. Available: https://iot-analytics.com/lpwan-market/

[6] Y.-P. E. 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," vol. 55, no. 3, pp. 117–123, 2017-03-13. [Online]. Available: http://arxiv.org/abs/1606.04171

[7] 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," 2019.

[8] ISO/IEC, *ISO/IEC 27001:2022 Information security management systems — Requirements*, Std., 2022. [Online]. Available: https://www.iso.org/standard/27001

[9] ThreatLocker, "Zero Trust Moves from Reactive to Proactive Security: "Assume Breach" Mindset," Magazine PDF, May 2025. [Online]. Available: https://static.threatlocker.com/magazine/_TL_Issue1_doublepage-view.pdf?11c68ba5_page=2

[10] S. H. Hall and H. L. Heck, *Advanced signal integrity for high-speed digital designs*. John Wiley & Sons, 2011.

[11] 3GPP, "3gpp system architecture evolution (sae); security architecture," 3GPP / ETSI, Technical Specification TS 33.401 V18.3.0, April 2025. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/133400_133499/133401/18.03.00_60/ts_133401v180300p.pdf

[12] S. F. Tan and A. Samsudin, "Recent technologies, security countermeasure and ongoing challenges of industrial internet of things (iiot): A survey," *Sensors*, vol. 21, no. 19, p. 6647, 2021. [Online]. Available: https://doi.org/10.3390/s21196647

[13] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," 2016.

[14] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir, and R. Brooks, "The sleep deprivation attack in sensor networks: Analysis and methods of defense," *International Journal of Distributed Sensor Networks*, vol. 2, no. 3, pp. 267–287, 2006. [Online]. Available: https://doi.org/10.1080/15501320600642718

[15] V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, "Energy depletion attacks in low power wireless networks," *IEEE Access*, vol. 7, pp. 51 915–51 932, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8691738/

[16] J.-K. Lee, Y.-R. Choi, B.-K. Suh, S.-W. Jung, and K.-I. Kim, "A survey on energy drainage attacks and countermeasures in wireless sensor networks," *Applied Sciences*, vol. 15, no. 4, p. 2213, 2025.

[17] V. Kumar, R. K. Jha, and S. Jain, "Nb-iot security: A survey," *Wireless Personal Communications*, vol. 113, no. 4, pp. 2661–2708, 2020.

[18] K. O. A. Alimi, K. Ouahada, A. M. Abu-Mahfouz, and S. Rimer, "A survey on the security of low power wide area networks: Threats, challenges, and potential solutions," *Sensors*, vol. 20, no. 20, p. 5800, 2020.

[19] G. Stanco, A. Navarro, F. Frattini, G. Ventre, and A. Botta, "A comprehensive survey on the security of low power wide area networks for the Internet of Things," *ICT Express*, vol. 10, no. 3, pp. 519–552, jun 2024. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2405959524000274

[20] T. Bani-Yaseen, A. Tahat, K. Kastell, and T. A. Edwan, "Denial-of-sleep attack detection in nb-iot using deep learning," *Journal of Telecommunications and the Digital Economy*, vol. 10, no. 3, pp. 14–38, 2022.

[21] G. Morillo, U. Roedig, and D. Pesch, "Detecting targeted interference in nb-iot," in *2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*. IEEE, 2023, pp. 475–482.

[22] V. Ionescu and U. Roedig, "Battery depletion attacks on nb-iot devices using interference," in *Computer Security. ESORICS 2021 International Workshops*, S. Katsikas, C. Lambrinoudakis, N. Cuppens, J. Mylopoulos, C. Kalloniatis, W. Meng, S. Furnell, F. Pallas, J. Pohle, M. A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. Maestre Vidal, and M. A. Sotelo Monge, Eds. Cham: Springer International Publishing, 2022, pp. 276–295.

[23] u blox, "Sara-n3 series data sheet," https://content.u-blox.com/sites/default/files/SARA-N3_DataSheet_UBX-18066692.pdf, 2018.

[24] Qualcomm, "Qualcomm 212 lte modem," https://www.qualcomm.com/products/technology/modems/qualcomm-212-lte-modem, 2024.

[25] S. Liu, L. Xiao, Z. Han, and Y. Tang, "Eliminating nb-iot interference to lte system: A sparse machine learning-based approach," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6919–6932, 2019.

[26] V. Ionescu, "https://github.com/ionescuvlad12/srsran-nb_iot." [Online]. Available: https://github.com/ionescuvlad12/srsRan-NB_IOT

[27] V. Ionescu and U. Roedig, "Nb-iot battery depletion via malicious interference," in *Proceedings of the 2022 INTERNATIONAL CONFERENCE ON EMBEDDED WIRELESS SYSTEMS AND NETWORKS*, ser. EWSN '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 244–249.

[28] C. W. Pascal Jörke, Tim Gebauer, "From lena to lena-nb: Implementation and performance evaluation of nb-iot and early data transmission in ns-3," *WNS3 2022*, 2022. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/3532577.3532600

[29] V. Ionescu, I. Wassel, and U. Roedig, "Edt+: Energy consumption optimization of nb-iot," in *Proceedings of the 11th International Workshop on Energy Harvesting & Energy-Neutral Sensing Systems*, ser. ENSsys '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 37–43. [Online]. Available: https://doi.org/10.1145/3628353.3628548

[30] V. Ionescu and U. Roedig, "Reception window selection in edt+ for energy efficient nb-iot," in *Proceedings of the 13th International Workshop on Energy Harvesting and Energy-Neutral Sensing Systems*, ser. ENSsys '25. New York, NY, USA: Association for Computing Machinery, 2025, p. 8–14. [Online]. Available: https://doi.org/10.1145/3722572.3727927

[31] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low Power Wide Area Networks: An Overview," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 855–873, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7815384/

[32] J. P. Shanmuga Sundaram, W. Du, and Z. Zhao, "A Survey on LoRa Networking: Research Problems, Current Solutions,

and Open Issues," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 371–388, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8883217/

[33] F. Gu, J. Niu, L. Jiang, X. Liu, and M. Atiquzzaman, "Survey of the low power wide area network technologies," *Journal of Network and Computer Applications*, vol. 149, p. 102459, jan 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1084804519303194

[34] N. S. Chilamkurthy, O. J. Pandey, A. Ghosh, L. R. Cenkeramaddi, and H.-N. Dai, "Low-Power Wide-Area Networks: A Broad Overview of Its Different Aspects," *IEEE Access*, vol. 10, pp. 81 926–81 959, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9848798/

[35] M. Bembe, A. Abu-Mahfouz, M. Masonta, and T. Ngqondi, "A survey on low-power wide area networks for IoT applications," *Telecommunication Systems*, vol. 71, no. 2, pp. 249–274, jun 2019. [Online]. Available: http://link.springer.com/10.1007/s11235-019-00557-9

[36] M. C. Bor, U. Roedig, T. Voigt, and J. M. Alonso, "Do LoRa Low-Power Wide-Area Networks Scale?" in *Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*. Malta Malta: ACM, nov 2016, pp. 59–67. [Online]. Available: https://dl.acm.org/doi/10.1145/2988287.2989163

[37] B. S. Chaudhari, M. Zennaro, and S. Borkar, "LPWAN Technologies: Emerging Application Characteristics, Requirements, and Design Considerations," *Future Internet*, vol. 12, no. 3, p. 46, mar 2020. [Online]. Available: https://www.mdpi.com/1999-5903/12/3/46

[38] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "Overview of cellular LPWAN technologies for IoT deployment: Sigfox, LoRaWAN, and NB-IoT," in *2018 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2018*, 2018.

[39] J. Petajajarvi, K. Mikhaylov, A. Roivainen, T. Hanninen, and M. Pettissalo, "On the coverage of LPWANs: range evaluation

and channel attenuation model for LoRa technology," in *2015 14th International Conference on ITS Telecommunications (ITST)*. Copenhagen, Denmark: IEEE, dec 2015, pp. 55–59. [Online]. Available: http://ieeexplore.ieee.org/document/7377400/

[40] R. El Chall, S. Lahoud, and M. El Helou, "LoRaWAN Network: Radio Propagation Models and Performance Evaluation in Various Environments in Lebanon," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2366–2378, apr 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8672452/

[41] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview of enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 855–873, 2017.

[42] Radiocrafts, "Rc1692hp-sig-dk demonstration kit," https://partners.sigfox.com/products/rc1692hp-sig-dk, 2025.

[43] G. G. L. Ribeiro, L. F. D. Lima, L. Oliveira, J. J. P. C. Rodrigues, C. N. M. Marins, and G. A. B. Marcondes, "An Outdoor Localization System Based on SigFox," in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*. Porto, Portugal: IEEE, jun 2018, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/8417853/

[44] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT system for m2m communication," in *2016 IEEE Wireless Communications and Networking Conference Workshops, WCNCW 2016*, 2016.

[45] M. Chen, Y. Miao, Y. Hao, and K. Hwang, "Narrow band internet of things," vol. 5, pp. 20 557–20 577, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/8038776/

[46] B. Buurman, J. Kamruzzaman, G. Karmakar, and S. Islam, "Low-Power Wide-Area Networks: Design Goals, Architecture, Suitability to Use Cases and Research Challenges," *IEEE Access*, vol. 8, pp. 17 179–17 220, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8963911/

[47] R. S. Sinha, Y. Wei, and S.-H. Hwang, "A survey on LPWA technology: LoRa and NB-IoT," vol. 3, no. 1, pp. 14–21, 2017-03. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2405959517300061

[48] D. Ismail, M. Rahman, and A. Saifullah, "Low-power wide-area networks: opportunities, challenges, and directions," in *Proceedings of the Workshop Program of the 19th International Conference on Distributed Computing and Networking*. Varanasi India: ACM, jan 2018, pp. 1–6. [Online]. Available: https://dl.acm.org/doi/10.1145/3170521.3170529

[49] N. Laili Ismail, M. Kassim, M. Ismail, and R. Mohamad, "A Review of Low Power Wide Area Technology in Licensed and Unlicensed Spectrum for IoT Use Cases," *Bulletin of Electrical Engineering and Informatics*, vol. 7, no. 2, pp. 183–190, jun 2018. [Online]. Available: https://beei.org/index.php/EEI/article/view/1174

[50] 3GPP, "3gpp system architecture evolution (sae); security architecture," 3GPP / ETSI, Technical Specification TS 33.401 V18.0.0, 2024. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/133400_133499/133401/18.00.00_60/ts_133401v180000p.pdf

[51] O. Liberg, M. Sundberg, Y.-P. E. Wang, J. Bergman, J. Sachs, and G. Wikström, "NB-IoT," in *Cellular Internet of Things*, 2020.

[52] J. Xu, J. Yao, L. Wang, Z. Ming, K. Wu, and L. Chen, "Narrowband internet of things: Evolutions, technologies, and open issues," 2018.

[53] A. Adhikary, X. Lin, and Y. P. Eric Wang, "Performance evaluation of NB-IoT coverage," in *IEEE Vehicular Technology Conference*, 2016.

[54] Y. D. Beyene, R. Jantti, K. Ruttik, and S. Iraji, "On the performance of narrow-band internet of things (NB-IoT)," in *IEEE Wireless Communications and Networking Conference, WCNC*, 2017.

[55] O. Liberg, M. Sundberg, Y.-P. E. Wang, J. Bergman, J. Sachs, and G. Wikström, *Cellular internet of things: from massive deployments to critical 5G applications*. Academic Press, 2020.

[56] H. Fattah, *5G LTE Narrowband Internet of Things (NB-IoT)*, 09 2018.

[57] 3GPP, "3gpp specification details for specification reference 22.125." [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3545

[58] 3GPP, "3gpp release 16." [Online]. Available: http://www.3gpp.org/release-16

[59] ——, "Evolved universal terrestrial radio access (e-utra); physical layer; measurements." [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2428

[60] A. P. Matz, J.-A. Fernandez-Prieto, J. Cañada-Bago, and U. Birkel, "A systematic analysis of narrowband IoT quality of service," vol. 20, no. 6, p. 1636, 2020-03-14. [Online]. Available: https://www.mdpi.com/1424-8220/20/6/1636

[61] Nokia, "Nokia siemens network. rf measurements quantities and optimization." [Online]. Available: https://www.academia.edu/8902974/Soc_Classification_level_1_Nokia_Siemens_Networks_Presentation_Author_Date_RF_measurements_quantities_and_optimization_Soc_Classification_level_2_Nokia_Siemens_Networks_Presentation_Author_Date_Content?auto=download

[62] 3GPP, "Specification details for specification reference 22.887." [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4309

[63] X. Lin, A. Adhikary, and Y.-P. Eric Wang, "Random access preamble design and detection for 3gpp narrowband IoT systems," vol. 5, no. 6, pp. 640–643, 2016-12. [Online]. Available: http://ieeexplore.ieee.org/document/7569029/

[64] W. S. Jeon, S. B. Seo, and D. G. Jeong, "Effective frequency hopping pattern for toa estimation in nb-iot random access," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 10, pp. 10 150–10 154, oct 2018.

[65] H. Chougrani, S. Kisseleff, and S. Chatzinotas, "Efficient preamble detection and time-of-arrival estimation for single-tone frequency hop-

ping random access in nb-iot," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7437–7449, 2021.

[66] R. Harwahyu, R.-G. Cheng, W.-J. Tsai, J.-K. Hwang, and G. Bianchi, "Repetitions versus retransmissions: Tradeoff in configuring NB-IoT random access channels," vol. 6, no. 2, pp. 3796–3805, 2019-04. [Online]. Available: https://ieeexplore.ieee.org/document/8605340/

[67] N. Mangalvedhe, R. Ratasuk, and A. Ghosh, "NB-IoT deployment study for low power wide area cellular IoT," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, 2016.

[68] "E-UTRA; physical channels and modulation (3gpp ts 36.211) release 17," ETSI, Tech. Rep. TS 136 211 V17.2.0, 08 2022. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/136200_136299/136211/17.02.00_60/ts_136211v170200p.pdf

[69] "E-UTRA; physical layer procedures (3gpp ts 36.213) release 18," ETSI, Tech. Rep. TS 136 213 V18.3.0, 02 2025. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/136200_136299/136213/18.03.00_60/ts_136213v180300p.pdf

[70] "E-UTRA; multiplexing and channel coding (3gpp ts 36.212) release 18," ETSI, Tech. Rep. TS 136 212 V18.1.0, 01 2025. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/136200_136299/136212/18.01.00_60/ts_136212v180100p.pdf

[71] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near shannon limit error-correcting coding and decoding: Turbo-codes," in *Proc. IEEE International Conference on Communications (ICC)*, Geneva, Switzerland, 1993, pp. 1064–1070. [Online]. Available: https://mat.hjg.com.ar/tic/img/Near%20Shannon%20Limit%20Error.pdf

[72] H. G. Myung, J. Lim, and D. J. Goodman, "Single carrier fdma for uplink wireless transmission," *IEEE Vehicular Technology Magazine*, vol. 1, no. 3, pp. 30–38, 2006. [Online]. Available: https://doi.org/10.1109/MVT.2006.307304

[73] K. Dev, P. K. R. Maddikunta, T. R. Gadekallu, S. Bhattacharya, P. Hegde, and S. Singh, "Energy Optimization for Green Communication in IoT Using Harris Hawks Optimization," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 2, pp. 685–694, jun 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9684544/

[74] R. Hernowo, A. Suharjono, B. Supriyo, M. Mukhlisin, S. S. Hidayat, E. D. Wardihani, and S. Beta K.K, "Power Consumption Optimization for Flood Monitoring System using NB-IoT," in *2022 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*. Yogyakarta, Indonesia: IEEE, dec 2022, pp. 58–63. [Online]. Available: https://ieeexplore.ieee.org/document/10052891/

[75] F. Michelinakis, A. S. Al-Selwi, M. Capuzzo, A. Zanella, K. Mahmood, and A. Elmokashfi, "Dissecting Energy Consumption of NB-IoT Devices Empirically," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1224–1242, jan 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9159902/

[76] A. K. Sultania, C. Blondia, and J. Famaey, "Optimizing the Energy-Latency Tradeoff in NB-IoT With PSM and eDRX," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12 436–12 454, aug 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9367281/

[77] R. K. Singh, P. P. Puluckul, R. Berkvens, and M. Weyn, "Energy Consumption Analysis of LPWAN Technologies and Lifetime Estimation for IoT Application," *Sensors*, vol. 20, no. 17, p. 4794, aug 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/17/4794

[78] Z. E. Ahmed, R. A. Saeed, A. Mukherjee, and S. N. Ghorpade, "Energy optimization in low-power wide area networks by using heuristic techniques," in *LPWAN Technologies for IoT and M2M Applications*. Elsevier, 2020, pp. 199–223. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/B9780128188804000119

[79] G. Hu, Z. Yi, L. Lu, Y. Huang, Y. Zhai, J. Liu, and B. Yang, "Self-powered 5g nb-iot system for remote monitoring applications," *Nano Energy*, vol. 87, p. 106140, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2211285521003967

[80] P. Das, S. Ghosh, S. Chatterjee, and S. De, "Energy harvesting-enabled 5g advanced air pollution monitoring device," in *2020 IEEE 3rd 5G World Forum (5GWF)*, 2020, pp. 218–223.

[81] A. Haridas, V. S. Rao, R. V. Prasad, and C. Sarkar, "Opportunities and challenges in using energy-harvesting for nb-iot," *SIGBED Rev.*, vol. 15, no. 5, p. 7–13, nov 2018. [Online]. Available: https://doi.org/10.1145/3292384.3292386

[82] S. Khan, M. Alam, Y. Le Moullec, A. Kuusik, S. Pärand, and C. Verikoukis, "An empirical modeling for the baseline energy consumption of an nb-iot radio transceiver," *TechRxiv*, 2020. [Online]. Available: https://figshare.com/articles/preprint/An_Empirical_Modelling_for_the_Baseline_Energy_Consumption_of_an_NB-IoT_Radio_Transceiver/12738725/2/files/27573026.pdf

[83] M. Zeinali and J. Thompson, "Impact of compression and small cell deployment on nb-iot devices coverage and energy consumption with a realistic simulation model," *Sensors*, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/19/6534/pdf?version=1632994128

[84] T. Xie, X. Zhang, and J. Liu, "Energy consumption delay evaluation of nb-iot terminal based on markov model," *Research Square*, 2021. [Online]. Available: https://www.researchsquare.com/article/rs-1036939/latest.pdf

[85] A. Höglund, D. P. Van de Putte, 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. [Online]. Available: https://ieeexplore.ieee.org/document/8325482

[86] "E-UTRA; NAS; Protocol for Control Plane and User Plane for EPS (3GPP TS 24.301) Rel-13," Technical Specification, 3GPP, Tech. Rep., 2016. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=417

[87] D. Liu, B. Chen, J. An, C. Li, G. Liu, J. Shao, W. Tang, C. Zhang, and Z. L. Wang, "Wind-driven self-powered wireless environmental sensors for internet of things at long distance," *Nano Energy*, vol. 73, p. 104819, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2211285520303761

[88] K. Skiadopoulos, A. Tsipis, K. Giannakis, G. Koufoudakis, E. Christopoulou, K. Oikonomou, G. Kormentzas, and I. Stavrakakis, "Synchronization of data measurements in wireless sensor networks for IoT applications," *Ad Hoc Networks*, vol. 89, pp. 47–57, jun 2019. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1570870518308825

[89] T. Schmid, Z. Charbiwala, J. Friedman, Y. Cho, and M. Srivastava, "Exploiting manufacturing variations for compensating environment-induced clock drift in time synchronization. sigmetrics," vol. 36, 06 2008, pp. 97–108.

[90] B. Sundararaman, U. Buy, and A. D. Kshemkalyani, "Clock synchronization for wireless sensor networks: a survey," *Ad Hoc Networks*, vol. 3, no. 3, pp. 281–323, may 2005. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1570870505000144

[91] D. Bankov, E. Khorov, A. Lyakhov, and E. Stepanova, "Clock Drift Impact on Target Wake Time in IEEE 802.11ax/ah Networks," in *2018 Engineering and Telecommunication (EnT-MIPT)*. Moscow, Russia: IEEE, nov 2018, pp. 30–34. [Online]. Available: https://ieeexplore.ieee.org/document/8757473/

[92] J. Elson, L. Girod, and D. Estrin, "Fine-grained network time synchronization using reference broadcasts," *ACM SIGOPS Operating Systems Review*, vol. 36, no. SI, pp. 147–163, dec 2002. [Online]. Available: https://dl.acm.org/doi/10.1145/844128.844143

[93] S. K. Mani, R. Durairajan, P. Barford, and J. Sommers, "An architecture for IoT clock synchronization," in *Proceedings of the 8th International Conference on the Internet of Things*. Santa Barbara California USA: ACM, oct 2018, pp. 1–8. [Online]. Available: https://dl.acm.org/doi/10.1145/3277593.3277606

[94] S. Gachhadar and K. Ruttik, "Clock Error Impact on NB-IoT Radio Link Performance."

[95] C. DSP, "Nb-iot dragonfly system and method for radio cell synchronization," 2018. [Online]. Available: https://www.ceva-dsp.com/wp-content/uploads/2018/02/NB-IoT_Dragonfly_System_and_Method_for_Radio_Cell_Synchronization_WhitePaper_V1.0.pdf

[96] R. S. Thomas Schmid, Zainul Charbiwala, "Temperature compensated time synchronization," *IEEE Embedded Systems Letters*, 2009. [Online]. Available: https://ieeexplore.ieee.org/document/5170185

[97] T. Haapala, A. Liscidini, and K. A. I. Halonen, "Temperature compensation of crystal references in nb-iot modems," *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS–I: REGULAR PAPERS*, vol. 67, no. 7, pp. 2467–2479, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9007638

[98] *SARA-N2 / SARA-N3 Series NB-IoT Modules: System Integration Manual*, u-blox AG, 2021. [Online]. Available: https://content.u-blox.com/sites/default/files/SARA-N2-N3_SysIntegrManual_UBX-17005143.pdf

[99] *BC66 Hardware Design*, Quectel Wireless Solutions Co., Ltd., 2021. [Online]. Available: https://evelta.com/content/datasheets/027-Quectel_BC66_Hardware_Design_V1.4.pdf

[100] GEYER Electronic, "Crystal or tcxo based design: Technical break-even," Application note, 2025. [Online]. Available: https://www.geyer-electronic.de/wp-content/uploads/2025/04/TCXO-technical-break-even_GEYER_Electronic_04_2025.pdf

[101] M. Haenggi and R. K. Ganti, "Interference in Large Wireless Networks," *Foundations and Trends in Networking*, vol. 3, no. 2, pp. 127–248, 2008. [Online]. Available: http://www.nowpublishers.com/article/Details/NET-015

[102] Z. Haider, M. Saleem, and T. Jamal, "Analysis of Interference in Wireless Networks."

[103] M. Lauridsen, B. Vejlgaard, I. Z. Kovacs, H. Nguyen, and P. Mogensen, "Interference Measurements in the European 868 MHz ISM Band with Focus on LoRa and SigFox," in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*. San Francisco, CA, USA: IEEE, mar 2017, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/7925650/

[104] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovacs, P. Mogensen, and M. Sorensen, "Interference Impact on Coverage and Capacity for Low Power Wide Area IoT Networks," in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*. San Francisco, CA, USA: IEEE, mar 2017, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/7925510/

[105] G. J. Gonzalez, F. H. Gregorio, and J. Cousseau, "Interference Analysis in the LTE and NB-IoT Uplink Multiple Access with RF impairments," in *2018 IEEE 23rd International Conference on Digital Signal Processing (DSP)*. Shanghai, China: IEEE, nov 2018, pp. 1–4. [Online]. Available: https://ieeexplore.ieee.org/document/8631794/

[106] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, nov 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8401919/

[107] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9072101/

[108] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT Security: Ongoing Challenges and Research Opportunities," in *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*. Matsue, Japan: IEEE, nov 2014, pp. 230–234. [Online]. Available: http://ieeexplore.ieee.org/document/6978614/

[109] I. Yaqoob, E. Ahmed, M. H. U. Rehman, A. I. A. Ahmed, M. A. Al-garadi, M. Imran, and M. Guizani, "The rise of ransomware and emerging security challenges in the Internet of Things," *Computer Networks*, vol. 129, pp. 444–458, dec 2017. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1389128617303468

[110] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. De Alvarenga, "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, apr 2017. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1084804517300802

[111] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8688434/

[112] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, oct 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8796409/

[113] 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, oct 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7562568/

[114] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, jan 2015. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1389128614003971

[115] *System Architecture for the 5G System (5GS)*, 3GPP Std. TS 23.501, 2024.

[116] *Security Architecture and Procedures for 5G System*, 3GPP Std. TS 33.501, 2024.

[117] C. Bockelmann, N. Pratas, H. Nikopour *et al.*, "Massive machine-type communication in 5g: Physical and mac-layer solutions," *IEEE Communications Magazine*, vol. 54, no. 9, pp. 59–65, 2016.

[118] Y. Liu, Z. Zhang, Y. Chen *et al.*, "Vision, requirements, and technology trends for 6g wireless," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 1546–1577, 2021.

[119] H. Birkholz, D. Thaler, M. Richardson, N. Smith, and W. Pan, "Remote attestation procedures (rats) architecture," RFC 9334, 2023.

[120] M. Pritikin, M. Richardson, M. Behringer, T. Eckert, and F. Brockners, "Bootstrapping remote secure key infrastructure (brski)," RFC 8995, 2021.

[121] *IEEE Standard for Local and Metropolitan Area Networks—Secure Device Identity*, IEEE Std. IEEE Std 802.1AR-2018, 2018.

[122] "Study on security aspects of network slicing," Tech. Rep. TR 33.811, 2018.

[123] *Management and Orchestration; Concepts, Use Cases and Requirements*, 3GPP Std. TS 28.530, 2024.

[124] *Service Requirements for the 5G System (5GS)*, 3GPP Std. TS 22.261, 2024.

[125] *Multi-access Edge Computing (MEC); Framework and Reference Architecture*, ETSI Std. GS MEC 003, 2022.

[126] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to industrial control systems (ics) security," NIST, Tech. Rep. SP 800-82 Rev. 3, 2022.

[127] *Industrial communication networks – IT security for networks and systems – Part 3-3: System security requirements and security levels*, IEC Std. IEC 62 443-3-3, 2013.

[128] R. K. Jha, Puja, H. Kour, M. Kumar, and S. Jain, "Layer based security in narrow band internet of things (NB-IoT)," vol. 185, p. 107592, 2021-02. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1389128620312299

[129] Y. Lin, F. Jiang, Z. Wang, and Z. Wang, "Research on PUF-Based Security Enhancement of Narrow-Band Internet of Things," in *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*. Krakow, Poland: IEEE, may 2018, pp. 702–709. [Online]. Available: https://ieeexplore.ieee.org/document/8432308/

[130] R. Tengshe and E. Akanksha, "Security in LP-WAN Technologies: Challenges and Solutions," in *2023 IEEE 8th International Conference for Convergence in Technology (I2CT)*. Lonavla, India: IEEE, apr 2023, pp. 1–4. [Online]. Available: https://ieeexplore.ieee.org/document/10126493/

[131] 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)*. Aarhus, Denmark: IEEE, jun 2019, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/8766430/

[132] M. Mlongeni, A. M. Abu-Mahfouz, and G. P. Hancke, "Towards Building a Secure NB-IoT Environment on 5G Networks: A User and Device Access Control System Review," in *IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society*. Brussels, Belgium: IEEE, oct 2022, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/9968879/

[133] C. Zakaret, N. Peladarinos, V. Cheimaras, E. Tserepas, P. Papageorgas, M. Aillerie, D. Piromalis, and K. Agavanakis, "Blockchain and secure element, a hybrid approach for secure energy smart meter gateways," *Sensors*, vol. 22, no. 24, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/24/9664

[134] Y. Shen, T. He, Q. Wang, J. Zhang, and Y. Wang, "Secure Transmission and Intelligent Analysis of Demand-Side Data in Smart Grids: A 5G NB-IoT Framework," *Frontiers in Energy Research*, vol. 10, p. 892066, may 2022. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fenrg.2022.892066/full

[135] V. A. Desnitsky, I. V. Kotenko, and N. N. Rudavin, "Protection Mechanisms against Energy Depletion Attacks in Cyber-Physical Systems," in *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. Saint Petersburg and Moscow, Russia: IEEE, jan 2019, pp. 214–219. [Online]. Available: https://ieeexplore.ieee.org/document/8656795/

[136] T. Bhattasali, R. Chaki, and S. Sanyal, "Sleep Deprivation Attack Detection in Wireless Sensor Network," *International Journal of Computer Applications*, vol. 40, no. 15, pp. 19–25, feb 2012. [Online]. Available: http://research.ijcaonline.org/volume40/number15/pxc3877374.pdf

[137] X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen, "Ghost-in-ZigBee: Energy Depletion Attack on ZigBee-Based Wireless Networks," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 816–829, oct 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7377010/

[138] M. H. R. Khouzani and S. Sarkar, "Maximum Damage Battery Depletion Attack in Mobile Sensor Networks," *IEEE Transactions on Automatic Control*, vol. 56, no. 10, pp. 2358–2368, oct 2011. [Online]. Available: http://ieeexplore.ieee.org/document/5978191/

[139] H. Ruotsalainen, G. Shen, J. Zhang, and R. Fujdiak, "Lorawan physical layer-based attacks and countermeasures, a review," *Sensors*, vol. 22, no. 9, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/9/3127

[140] J. Šabić, T. Perković, D. Begušić , and P. Šolić , "Practical realization of reactive jamming attack on long-range wide-area network," *Sensors*, vol. 25, no. 8, 2025. [Online]. Available: https://www.mdpi.com/1424-8220/25/8/2383

[141] A. Dossa, A. Burg, and E. M. Amhoud, "Impact of reactive jamming attacks on lorawan: a theoretical and experimental study," 2025. [Online]. Available: https://arxiv.org/abs/2501.18339

[142] V. Shakhov and I. Koo, "Depletion-of-battery attack: Specificity, modelling and analysis," *Sensors*, vol. 18, no. 6, 2018. [Online]. Available: https://www.mdpi.com/1424-8220/18/6/1849

[143] O. Osanaiye, A. S. Alfa, and G. P. Hancke, "A statistical approach to detect jamming attacks in wireless sensor networks," *Sensors*, vol. 18, no. 6, 2018. [Online]. Available: https://www.mdpi.com/1424-8220/18/6/1691

[144] H. Soy, "Coverage analysis of lora and nb-iot technologies on lpwan-based agricultural vehicle tracking application," *Sensors*, vol. 23, no. 21, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/21/8859

[145] E. Rastogi, N. Saxena, A. Roy, and D. R. Shin, "Narrowband internet of things: A comprehensive study," vol. 173, p. 107209, 2020-05. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1389128619313593

[146] M. Pennacchioni, M. G. Di Benedette, T. Pecorella, C. Carlini, and P. Obino, "NB-IoT system deployment for smart metering: Evaluation of coverage and capacity performances," in *2017 AEIT International Annual Conference: Infrastructures for Energy and ICT: Opportunities for Fostering Innovation, AEIT 2017*, 2017.

[147] PCB Online, "Nb-iot smart water meter: How does it work and a real project," PCB Online Blog, November 28, 2024. [Online]. Available: https://www.pcbonline.com/blog/nb-iot-water-meter.html

[148] 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.

[149] M. Lauridsen, R. Krigslund, M. Rohr, and G. Madueno, "An empirical nb-iot power consumption model for battery lifetime estimation," in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*. IEEE, 2018, pp. 1–5.

[150] P. Andres-Maldonado, P. Ameigeiras, J. Prados-Garzon, J. J. Ramos-Muñoz, J. Navarro-Ortiz, and J. M. Lopez-Soler, "Analytic analysis

of narrowband iot coverage enhancement approaches," in *2018 Global Internet of Things Summit (GIoTS)*. IEEE, 2018, pp. 1–6.

[151] E. M. Migabo, K. D. Djouani, and A. Kurien, "The narrowband internet of things (nb-iot) resources management performance state of art, challenges, and opportunities," *IEEE Access*, 2020.

[152] E. Staddon, "Attack categorisation for iot applications in critical infrastructure," *Applied Sciences*, vol. 11, no. 16, p. 7228, 2021.

[153] F. T. Zahra, "Security of wireless iot in smart manufacturing," in *Secure and Smart IoT*, ser. Lecture Notes in Computer Science. Springer, 2024, vol. X, pp. XX–XX.

[154] D. TORRIERI, "Frequency hopping with multiple frequency-shift keying and hard decisions," *Communications, IEEE Transactions on*, vol. 32, pp. 574 – 582, 06 1984.

[155] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," *INFCOM*, pp. 2526 – 2530, 06 2007.

[156] H. Yang, S. Bae, M. Son, H. Kim, S. M. Kim, and Y. Kim, "Hiding in plain signal: Physical signal overshadowing attack on LTE," in *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, aug 2019, pp. 55–72. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/yang-hojoon

[157] H. Kim, J. Lee, E. Lee, and Y. Kim, "Touching the untouchables: Dynamic security analysis of the lte control plane," in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 1153–1168.

[158] S. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "Lteinspector: A systematic approach for adversarial testing of 4g lte," *Network and Distributed Systems Security (NDSS) Symposium 2018*. [Online]. Available: https://par.nsf.gov/biblio/10055689

[159] J. Morillo and U. Roedig, "Jamming of nb-iot synchronisation signals," Technical report / preprint, 2019. [On-

line]. Available: https://cora.ucc.ie/server/api/core/bitstreams/163399c7-16d3-4c7c-9787-4db5cd2815ef/content

[160] M. Lichtman, V. Marojevic, J. H. Reed, and T. C. Clancy, "Lte/lte-a jamming, spoofing, and sniffing: Threat assessment and mitigation," *arXiv preprint arXiv:1611.02428*, 2016. [Online]. Available: https://arxiv.org/abs/1611.02428

[161] N. Chakrapani, "Nb-iot uplink receiver design and performance study," arXiv preprint, 2019. [Online]. Available: https://arxiv.org/abs/1906.07096

[162] R. P. Jover, J. Lackey, and A. Raghavan, "Enhancing the security of LTE networks against jamming attacks," vol. 2014, no. 1, p. 7, 2014-12. [Online]. Available: https://jis-eurasipjournals.springeropen.com/articles/10.1186/1687-417X-2014-7

[163] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed. McGraw-Hill, 2007.

[164] S. Martiradonna, G. Piro, and G. Boggia, "On the evaluation of the NB-IoT random access procedure in monitoring infrastructures," vol. 19, no. 14, p. 3237, 2019-07-23. [Online]. Available: https://www.mdpi.com/1424-8220/19/14/3237

[165] M. Agiwal, M. K. Maheshwari, and H. Jin, "Power efficient random access for massive NB-IoT connectivity," vol. 19, no. 22, p. 4944, 2019-11-13. [Online]. Available: https://www.mdpi.com/1424-8220/19/22/4944

[166] A. Hoglund, G. A. Medina-Acosta, S. N. K. Veedu, O. Liberg, T. Tirronen, E. A. Yavuz, and J. Bergman, "3gpp release-16 preconfigured uplink resources for lte-m and nb-iot," *IEEE Communications Standards Magazine*, vol. 4, no. 2, pp. 50–56, 2020.

[167] S. Popli, R. Jha, and S. Jain, "A survey on energy efficient narrowband internet of things (nbiot): Architecture, application and challenges," *IEEE Access*, 2018.

[168] A. M. Abbas, K. Y. Youssef, I. I. Mahmoud, and A. Zekry, "Nb-iot optimization for smart meters networks of smart cities: Case study,"

Alexandria Engineering Journal, vol. 59, no. 6, pp. 4267–4281, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1110016820303598

[169] GSMA, "NB-IoT deployment guide to basic feature set requirements (v3)," GSMA, Tech. Rep., 2019, summarises UE power classes 23/20/14 dBm. [Online]. Available: https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/wp-content/uploads/2019/07/201906-GSMA-NB-IoT-Deployment-Guide-v3.pdf

[170] 3GPP, "3gpp standards for the internet-of-things," Presentation, 2016, common 10-year life design target with ∼5 Wh battery. [Online]. Available: https://www.3gpp.org/images/presentations/3gpp_standards_for_iot.pdf

[171] Great Scott Gadgets, "HackRF One Hardware," https://hackrf.readthedocs.io/en/latest/hackrf_one.html, 2025.

[172] A. Devices, *ADALM-PLUTO Evaluation Board*, 2024. [Online]. Available: https://www.analog.com/en/resources/evaluation-hardware-and-software/evaluation-boards-kits/adalm-pluto.html

[173] I. Gomez-Miguelez, A. Garcia-Saavedra, P. Sutton, P. Serrano, C. Cano, and D. Leith, "srslte: an open-source platform for lte evolution and experimentation," 10 2016, pp. 25–32.

[174] A. Puschmann, "Release srslte 20.04 · srsran/srsran." [Online]. Available: https://github.com/srsran/srsRAN/releases/tag/release_20_04

[175] M. Lukic, S. Sobot, I. Mezei, D. Danilovic, and D. Vukobratovic, "In-depth real-world evaluation of nb-iot module energy consumption," 2020. [Online]. Available: https://arxiv.org/abs/2005.13648

[176] A. Sørensen, H. Wang, M. J. Remy, N. Kjettrup, R. B. Sørensen, J. J. Nielsen, P. Popovski, and G. C. Madueño, "Modeling and experimental validation for battery lifetime estimation in nb-iot and lte-m," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9804–9819, 2022.

[177] "Sun, *Media Access Control for Narrowband Internet of Things: A Survey.* Cham: Springer International Publishing, 2018, pp. 1–4. [Online]. Available: https://doi.org/10.1007/978-3-319-32903-1_161-1

[178] "Narayanan, "Performance analysis of nb-iot random access channel," in *"Internet of Things*, "Auer, Ed. Cham: Springer International Publishing, 2021, pp. 1118–1128.

[179] B. Martinez, F. Adelantado, A. Bartoli, and X. Vilajosana, "Exploring the performance boundaries of nb-iot," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5702–5712, 2019.

[180] A. K. Sultania, P. Zand, C. Blondia, and J. Famaey, "Energy modeling and evaluation of nb-iot with psm and edrx," in *2018 IEEE Globecom Workshops (GC Wkshps)*, 2018, pp. 1–7.

[181] D. Yang, X. Huang, J. Huang, X. Chang, G. Xing, and Y. Yang, "A first look at energy consumption of nb-iot in the wild: Tools and large-scale measurement," *IEEE/ACM Transactions on Networking*, vol. 29, no. 6, pp. 2616–2631, 2021.

[182] M. T. Abbas, J. Eklund, K.-J. Grinnemo, A. Brunstrom, and . Alfredsson, "Guidelines for an energy efficient tuning of the nb-iot stack," in *2020 IEEE 45th LCN Symposium on Emerging Topics in Networking (LCN Symposium)*, 2020, pp. 60–69.

[183] J. Shi, L. Jin, J. Li, and Z. Fang, "A smart parking system based on nb-iot and third-party payment platform," in *2017 17th International Symposium on Communications and Information Technologies (ISCIT)*, 2017, pp. 1–5.

[184] R. Morais, S. G. Matos, M. A. Fernandes, A. L. Valente, S. F. Soares, P. Ferreira, and M. Reis, "Sun, wind and water flow as energy supply for small stationary data acquisition platforms," *Computers and Electronics in Agriculture*, vol. 64, no. 2, pp. 120–132, 2008. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0168169908001257

[185] K. Calautit, D. S. Nasir, and B. R. Hughes, "Low power energy harvesting systems: State of the art and future challenges,"

Renewable and Sustainable Energy Reviews, vol. 147, p. 111230, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1364032121005177

[186] "Zúñiga, *Report on Environmental and Platform Models.* ., 2013.

[187] R. Gupta, B. Bachmann, R. Ford, S. Rangan, N. Kundargi, A. Ekbal, K. Rathi, M. I. Sanchez, A. de la Oliva, and A. Morelli, "ns-3-based real-time emulation of lte testbed using labview platform for software defined networking (sdn) in crowd project," in *Proceedings of the 2015 Workshop on Ns-3*, ser. WNS3 '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 91–97. [Online]. Available: https://doi.org/10.1145/2756509.2756516

[188] GSMA Intelligence, "The mobile economy china 2023," https://www.gsma.com/mobileeconomy/wp-content/uploads/2023/03/The-Mobile-Economy-Report-China-2023.pdf, 2023.

[189] GSMA, "Mobile iot commercial launches (lte-m & nb-iot)," https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/mobile-iot-commercial-launches/, July 2025.

[190] Deutsche Telekom AG, "Mobile iot roaming goes live across europe," https://www.telekom.com/en/media/media-information/archive/mobile-iot-roaming-goes-live-across-europe-598700, April 2020.

[191] ——, "In action: Networks for the internet of things," https://www.telekom.com/en/media/media-information/archive/in-action-networks-for-the-internet-of-things-620682, March 2021.

[192] 1NCE GmbH, "Iot sim card for europe — 1nce iot lifetime flat (500 mb & 250 sms, 10 years)," https://www.1nce.com/en-us/1nce-connect/features/sim-cards/iot-sim-europe, 2025.

[193] RS Components, "Dfrobot arduino nb-iot expansion shield (dfr0763), rs stock no. 247-3226," https://uk.rs-online.com/web/p/shields-for-arduino/2473226?gb=s, 2025.

[194] 3GPP, "Tr 45.820: Cellular system support for ultra-low complexity and low throughput internet of things (ciot), release 13," https://www.

3gpp.org/dynareport/45820.htm, 3rd Generation Partnership Project, Tech. Rep., 2016.

[195] G. Morillo, U. Roedig, and J. Stankovic, "Technology independent targeted interference detection for wireless iot," in *2024 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, 2024, pp. 44–50.