# Managing Hybrid Industrial IoT Enterprise Wireless Networks

Yu Chen

Submitted in fulfilment of the requirements for the
Degree of Doctor of Philosophy

James Watt School of Engineering
College of Science and Engineering
University of Glasgow


March 2024

# Abstract

The advent of the Internet of Things has spurred the deployment of Low Power Wide Area Networks (LPWANs) to facilitate a myriad of commercial and private services. However, while LPWANs offer benefits such as low power consumption and wide coverage, their lower data rates and reliability have constrained their utility in industrial processes and high data rate multimedia applications. This thesis addresses these limitations by exploring the integration of LPWANs into the Fifth Generation (5G) cellular networks and enhancing the management of the hybrid network in terms of server offloading, data volume reduction, and scalability management.

The first part of the thesis surveys the challenges and solutions of LPWAN-5G integration, emphasizing hybrid architectures, security, mobility, interoperability, and coexistence with other wireless technologies. Building upon this, the second part of the thesis designs and implements a Long Range Wide Area Network (LoRaWAN)-5G integrated network with a collaborative radio access network and a converged core network. The integrated network has been deployed for heating monitoring, demonstrating the feasibility, flexibility, and cost-effectiveness of the hybrid network. The implemented LoRaWAN-5G integrated network has attracted new funding from the European Space Agency for a telemedicine project.

The third part of the thesis proposes a Long Range (LoRa) mesh-5G integrated network to address coverage gaps in railway operations, leveraging 5G for backhaul and computing while extending coverage with LoRa mesh. The integration of edge computing and a cloud-edge-terminal collaborative architecture enhances network efficiency and timeliness, as validated in a proof-of-concept deployment for trackside weather monitoring. The LoRa mesh-based trackside weather monitoring system has been adopted by Network Rail for potential widespread use.

Lastly, the fourth part of the thesis investigates the reliability and scalability

of the LoRa mesh-5G integrated network for monitoring linear infrastructure, proposing a deployment strategy and novel 5G-enabled routing algorithm to optimize node placement and enhance network performance within duty cycle regulations. Moreover, a simulation tool has been developed to validate these findings, offering insights into practical deployments.

Collectively, this thesis contributes to the understanding and advancement of LPWAN-5G integration, offering solutions for diverse industrial and infrastructure monitoring applications, e.g., trackside weather monitoring. This thesis serves as a comprehensive exploration of the integration and optimization of LPWAN technologies within 5G networks, paving the way for enhanced Internet of Things deployments in various domains.

# Contents

# List of Tables

# List of Figures

*To my parents.*
(献给我亲爱的父母)

# Acknowledgements


关山难越，谁悲失路之人；
(Mountains are hard to climb; who pities the lost?)
萍水相逢，尽是他乡之客。
(Meeting by chance in a distant place; all are expatriates.)
——王勃 (Bo Wang)

1) Pursuing a Ph.D. is akin to scaling a formidable mountain. Those who guide and support me serve as beacons of light along the arduous climb.

I would like to express my heartfelt appreciation to my esteemed supervisors, Dr. Yusuf Sambo, Dr. Oluwakayode Onireti, and Prof. Muhammad Ali Imran, whose invaluable assistance and unwavering support have played a pivotal role in shaping my journey through this endeavor. Dr. Sambo, serving as my principal supervisor, has provided meticulous guidance throughout my entire Ph.D. research, covering every facet of my study. His mentorship has been instrumental in transforming me from a student with no background in communication technology to a proficient Ph.D. candidate with expertise in wireless communication. Dr. Onireti has made significant contributions, particularly in enhancing my academic writing skills, aiding in the identification of compelling research topics, and refining my research methodology. Additionally, I am deeply grateful to Prof. Imran for his provision of research resources and invaluable opportunities for project involvement. Their collective support has been indispensable in my academic and professional growth, and I am profoundly grateful for their guidance and mentorship.

I would like to thank Dr. Guodong Zhao and Dr. Liying Li for recommending me to the Communication, Sensing, and Imaging (CSI) group at the University of Glasgow during my Ph.D. application process. Their endorsement helps integrate me into the group and foster a supportive environment. Additionally, I am thankful to my colleagues within the CSI group for their assistance and support. Moreover, I am

appreciative of the generous funding and support provided by Dr. Taner Dosluoglu and Ali Ertugrul from 5G3i Ltd. corporation for the satellites for digitalization of railways project. Furthermore, I would like to thank my thesis examiners and viva convener, Dr. Yao Sun, Dr. Charalampos Rotsos, and Dr. Carlos Nunez, for their valuable comments.

I would also like to extend my gratitude to Prof. Yijiu Zhao and Prof. Jianguo Huang from the University of Electronic Science and Technology of China. Although they served as my master's supervisors, their guidance, support, and care persisted beyond the completion of my master's degree.

Most importantly, I would like to acknowledge the love and support from my parents and girlfriend. Despite being thousands of miles away, the unwavering love and support from my parents traverse mountains and seas, accompanying me at all times. My girlfriend made the selfless decision to leave her job in China, part from her family, and join me overseas. Words cannot fully express my profound appreciation and love for her; instead, time will bear witness to my heart.

Additionally, I am grateful to my friends and other family members in China for their support. They have also played a significant role in encouraging me along this journey.

2) Gathering in Glasgow, friends from all corners of the globe bring me immense joy. The bonds of friendship forged with them resemble the rainbows adorning Glasgow's skies, offering delightful surprises and rendering the experience of living abroad truly beautiful.

I would like to express my gratitude to Dr. Yusuf Sambo once again. Not only has he been my supervisor, but he has also been a true friend who acquainted me with the environment, assisted me in settling down in the U.K., introduced me to new friends, helped me plan my career, and supported me in various aspects of life.

I would like to express my gratitude to David Wong and Nancy Wong. Their contribution played a pivotal role in helping me settle down in the U.K. Despite knowing each other for only two and a half years, they have become like family to me. They have offered valuable advice, assisted me in overcoming numerous challenges, celebrated important milestones with me, and accompanied me in various activities.

I would like to extend my gratitude to many other friends I met in Glasgow. Whether it was playing sports, dining together, engaging in conversations, sharing stories, or simply having fun, they have all contributed to making my time in Glasgow enjoyable and memorable.

**University of Glasgow**

College of Science & Engineering

**Statement of Originality**

**Name:** Yu Chen

**Registration Number:** xxxxxxxx

I certify that the thesis presented here for examination for a PhD degree of the University of Glasgow is solely my own work other than where I have clearly indicated that it is the work of others (in which case the extent of any work carried out jointly by me and any other person is clearly identified in it) and that the thesis has not been edited by a third party beyond what is permitted by the University's PGR Code of Practice.

The copyright of this thesis rests with the author. No quotation from it is permitted without full acknowledgment.

I declare that the thesis does not include work forming part of a thesis presented successfully for another degree.

I declare that this thesis has been produced in accordance with the University of Glasgow's Code of Good Practice in Research.

I acknowledge that if any issues are raised regarding good research practice based on review of the thesis, the examination may be postponed pending the outcome of any investigation of the issues.

**Signature:** _____

**Date:** 8th May 2024

# List of Abbreviations

| | |
|---|---|
| 2G | Second Generation |
| 3GPP | 3rd Generation Partnership Project |
| 4G | Fourth Generation |
| 5G | Fifth Generation |
| AES | Advanced Encryption Standard |
| AMF | Access and Mobility Management Function |
| ARIMA | Autoregressive Integrated Moving Average |
| AUSF | Authentication Server Function |
| BPSK | Binary Phase-Shift Keying |
| CSS | Chirp Spread Spectrum |
| DBPSK | Differential Binary Phase Shift Keying |
| DevEUI | Devices Extended Unique Identifier |
| DSSS | Direct Sequence Spread Spectrum |
| EC-GSM-IoT | Extended Coverage Global System for Mobile Communication IoT |
| eMBB | enhanced Mobile Broadband |
| eMTC | enhanced Machine Type Communication |
| EPC | Evolved Packet Core |
| ETSI | European Telecommunications Standards Institute |
| FSK | Frequency Shift Keying |
| GFSK | Gaussian Frequency Shift Keying |
| GMSK | Filtered Minimum Shift Keying |
| GSM | Global System for Mobile Communication |
| GSM-R | Global System for Mobile Communication-Railway |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |

| | |
|---|---|
| IoT | Internet of Things |
| IP | Internet Protocol |
| ISM | Industrial, Scientific and Medical |
| JoinEUI | Join Extended Unique Identifier |
| JWS | James Watt South |
| KPIs | Key Performance Indicators |
| LoRa | Long Range |
| LoRaWAN | Long Range Wide Area Network |
| LPWA | Low-Power Wide Area |
| LPWAN | Low-Power Wide Area Network |
| LPWANs | Low-Power Wide Area Networks |
| LTE | Long-Term Evolution |
| LTE-M | Long-Term Evolution for Machines |
| LTN | Low Throughput Network |
| M2M | Machine-to-Machine |
| MAC | Medium Access Control |
| MAE | Mean Absolute Error |
| MAPE | Mean Absolute Percentage Error |
| MEC | Multi-access Edge Computing |
| mMTC | massive Machine Type Communication |
| MNOs | Mobile Network Operators |
| MQTT | Message Queuing Telemetry Transport |
| NB-IoT | Narrowband–Internet of Things |
| NFV | Network Function Virtualization |
| NSA | Non-standalone Architecture |
| NSSF | Network Slice Selection Function |
| QPSK | Quadrature Phase Shift Keying |
| RAN | Radio Access Network |
| RMSE | Root Mean Square Error |
| RPMA | Random Phase Multiple Access |
| RSSI | Received Signal Strength Indicator |
| SDN | Software Defined Network |
| SMF | Session Management Function |
| SSL | Secure Sockets Layer |

| | |
|---|---|
| SUPI | Subscription Permanent Identifier |
| SVM | Support Vector Machines |
| TLS | Transport Layer Security |
| UDM | Unified Data Management |
| UDP | User Datagram Protocol |
| UDR | Unified Data Repository |
| UE | User Equipment |
| ueId | user equipment Identifier |
| UNB | Ultra Narrow Bandwidth |
| UPF | User Plane Function |
| URLLC | Ultra-Reliable and Low-Latency Communications |
| VM | Virtual Machine |

# List of Symbols

| | |
|---|---|
| $\alpha$ | Window length factor |
| $\Delta t$ | Observation interval |
| $\delta$ | The number of values |
| $\hat{d}$ | Average significant-change delay |
| $\hat{n}_i^{\mathrm{g}}$ | The estimated number of generated significant-change updates |
| $\hat{y}_i$ | $i^{th}$ predicted value |
| $\lambda$ | Node reliability |
| $\lceil \cdot \rceil$ | Ceiling function |
| $\mathbb{N}$ | Set of all natural numbers |
| $\mathbb{Z}$ | Set of all integers |
| $\mathbb{Z}^+$ | Set of all positive integers |
| $\Omega$ | The number of programmed preamble symbols |
| $\phi$ | Distance factor |
| $\Psi$ | Indicator of LoRa low data rate optimize |
| $\theta$ | Scalability factor determined by routing algorithm |
| $A_i$ | Theoretical value |
| $B_i$ | Simulated value |
| $BW$ | channel bandwidth |
| $c$ | Coverage extension ratio |
| $c^t$ | Time of the last update for air temperature |
| $c^w$ | Time of the last update for wind speed |
| $c_i$ | The number of significant-change updates between time $im$ and time $(i+1)m$ |
| $c^t_{\max}$ | Criteria of adverse weather about high air temperature |

| | |
|---|---|
| $c^w_{\max}$ | Criteria of adverse weather about high wind speed |
| $c^t_{\min}$ | Criteria of adverse weather about low air temperature |
| $CR$ | Coding rate |
| $D$ | Maximum duty cycle requirement |
| $d$ | Duty cycle |
| $d_G$ | Duty cycle of the gateway |
| $d_i$ | Duty cycle of sensor node $s_i$ |
| $E$ | Edge set of graph $G$ |
| $e_i$ | Delay occurring between time $im$ and $(i+1)m$ |
| $f(\cdot)$ | Number-conversion function |
| $F_i$ | Feature vector |
| $FN$ | False negative that a normal situation is incorrectly identified as an abnormality |
| $FP$ | False positive that an abnormality is incorrectly classed as normality |
| $G$ | Graph denoting the sub-network composed of $s_1, s_2, ..., s_{N+1}$ |
| $H$ | Indicator of explicit LoRa header |
| $H^t_{\max}$ | Threshold of maximum air temperature |
| $H^w_{\max}$ | Threshold of maximum wind speed |
| $H^t_{\min}$ | Threshold of minimum air temperature |
| $k$ | Vertex connectivity |
| $k(G)$ | Vertex connectivity of graph $G$ |
| $L_a$ | The length of acknowledgement packet |
| $L_d$ | The length of data packet |
| $l_i$ | Distance between $s_i$ and $s_{i+1}$ |
| $l_{i,j}$ | Distance between $s_i$ and $s_j$ |
| $m$ | Period of sending periodic updates |
| $N$ | The number of sensor nodes at one side of the gateway |
| $n_i$ | the number of sensor nodes whose data packets are relayed by $s_i$ |
| $n_{\mathrm{e}}$ | The number of values to be evaluated |
| $N_{\max}$ | The maximum number of sensor nodes |
| $n^{\mathrm{r}}_i$ | The number of received significant-change updates |
| $o_i$ | Packet loss indicator |

| | |
|---|---|
| $p$ | Packet rate |
| $p^{\mathrm{t}}_{\mathrm{max}}$ | Predicted maximum air temperature |
| $p^{\mathrm{w}}_{\mathrm{max}}$ | Predicted maximum wind speed |
| $p^{\mathrm{t}}_{\mathrm{min}}$ | Predicted minimum air temperature |
| $Pr$ | Sytem reliability |
| $r$ | Maximum communication distance of single-hop LoRa |
| $S$ | Vertex set of graph $G$ |
| $s_i$ | $i^{th}$ sensor node |
| $SF$ | LoRa spreading factor |
| $STD_i$ | Standard deviation |
| $T$ | Spanning tree |
| $t$ | Time |
| $T(t)$ | Temperature at the time $t$ |
| $t_a$ | Time on air of each acknowledgment packet |
| $t_c$ | Time on air of each routing discovery packet |
| $t_d$ | Time on air of each data packet |
| $t_r$ | Time on air of each routing quest packet |
| $TN$ | True negative that a normal situation is identified correctly |
| $TP$ | True positive that the loss of significant-change updates is successfully classed as an abnormality |
| $W(t)$ | Wind speed at the time $t$ |
| $w_i(\cdot)$ | Value of update on wind speed |
| $W_n$ | Received wind speed data |
| $X$ | Maximum delay integer for routing request |
| $Y$ | Maximum delay integer for routing discovery |
| $y_i$ | $i^{th}$ actual value |

# Chapter 1

# Introduction

## 1.1 Background

In the landscape of Industry 4.0, characterized by the integration of digital technologies into manufacturing processes, the demand for robust Internet of Things (IoT) solutions has surged. As industries transition towards this new paradigm, marked by automation, data analytics, and interconnectivity, the need for seamless connectivity and real-time data exchange becomes paramount. This paradigm shift in manufacturing aims to enhance efficiency, productivity, and predictive maintenance strategies. The adoption of Low-Power Wide Area Networks (LPWANs) has played a pivotal role in facilitating this transition, offering scalable, cost-effective connectivity solutions tailored for industrial applications. Low-Power Wide Area Network (LPWAN) technologies provide the backbone for deploying sensors, actuators, and other IoT devices across vast industrial environments, enabling remote monitoring, predictive maintenance, and resource optimization. However, LPWANs cannot meet the needs of all industrial applications such as process control due to its limitations like low data rate. To address this, it is anticipated that cutting-edge cellular communication technologies will have a crucial impact. However, as industrial IoT applications evolve and scale, the transition to advanced networking technologies such as Fifth Generation (5G) poses unique challenges. These challenges encompass compatibility issues, infrastructure adaptation, and cost considerations, underscoring the importance of a seamless migration strategy. Against this backdrop, the discussion shifts to explore the specific context of Long Range (LoRa)-based technologies within the realm of LPWANs,

highlighting its unique features and advantages in addressing the needs of Industry 4.0 applications. By delving into the interplay between LPWANs and 5G, this thesis argues that the integration and optimization of LPWANs and 5G will significantly enhance efficiency, productivity, and innovation within industrial manufacturing processes.

Industry 4.0 requires massive IoT connections to facilitate real-time data exchange, optimize production efficiency, and enable predictive maintenance strategies [1]. LPWANs have become the main driver for the growth of IoT connections globally and are expected to replace most Second Generation (2G) and third generation cellular IoT connections in the future [2]. Depending on spectrum license requirements, Low-Power Wide Area (LPWA) technologies can be classified into licensed LPWA technologies, such as Narrowband–Internet of Things (NB-IoT) and Long-Term Evolution for Machines (LTE-M), and unlicensed LPWA technologies, such as Long Range Wide Area Network (LoRaWAN) and Sigfox. The rise in IoT adoption has spurred the utilization of unlicensed LPWA technologies, both for commercial and private purposes, due to their cost-effectiveness and performance benefits. In contrast to licensed LPWA technologies, which operate on spectrum designated by regulators for exclusive use and seamlessly integrate with mobile networks, unlicensed LPWANs function as standalone networks with non-exclusive spectrum rights, necessitating specialized equipment and management systems. While unlicensed LPWANs offer advantages like low power consumption, extensive coverage, affordability, and scalability, they generally exhibit lower data rates and reliability, constraining their suitability for certain industrial applications such as process control and high-data-rate multimedia usage.

To address these limitations, industrial operators often employ a dual deployment approach, utilizing both licensed cellular networks like Long-Term Evolution (LTE) and the 5G cellular network alongside unlicensed IoT networks to accommodate diverse industrial needs. However, this deployment model poses challenges associated with complexity and cost management. Compared to previous generation cellular networks, 5G is a flexible, scalable, agile, and programmable communication system that can support integration with other technologies [3]. Thus, the integration of unlicensed LPWANs into 5G emerges as a promising method to avoid dual deployment and enhance network optimization. To ensure seamless integration, it is crucial to design a hybrid network architecture that can leverage the advantages of LPWANs and 5G. Moreover, optimizing the management of LPWANs by leveraging

the computational capabilities of 5G networks can significantly enhance efficiency and performance. For instance, offloading LPWAN management functions to 5G's robust core network, a potent platform for conducting complex calculations, can lighten the workload on LPWANs and improve overall system efficiency.

On the other hand, although unlicensed LPWANs, such as LoRaWAN and Sigfox, can provide extensive coverage with one-hop communication distances of up to tens of kilometers [4], their star network topology necessitates dense gateway deployment, especially in environments with many obstacles or when monitoring extensive infrastructure such as pipelines, roads, and railways. To address the high cost and management complexity induced by dense gateway deployment, mesh technologies have been introduced to unlicensed LPWANs. Mesh topologies offer increased flexibility, allowing end nodes to retransmit messages received from other nodes, thereby facilitating multi-hop communication. Due to these features, unlicensed mesh LPWANs, such as LoRa mesh, can achieve extended coverage without the need for densely deploying gateways. However, like unlicensed star-topology LPWANs, unlicensed mesh LPWANs also suffer from low scalability and reliability, which can also be improved through integration with 5G and careful design of the mesh network's routing algorithm.

This thesis investigates the integration of LoRaWAN, a promising unlicensed LPWAN, with 5G. To extend coverage further, a cloud-edge-terminal collaboration architecture is proposed to integrate LoRa mesh into a 5G network, along with a routing algorithm considering reliability and scalability. To mitigate the management burden of LPWANs, the LoRaWAN servers are offloaded to the 5G core network and a LoRa mesh server is designed and deployed within the 5G core network infrastructure.

## 1.2 Motivation and Objectives

This thesis integrates two promising unlicensed LPWA technologies, LoRaWAN and LoRa mesh, with 5G networks. The motivations behind the integration and optimization of the hybrid network are discussed as follows:

- The integration and optimization of LoRaWAN, LoRa mesh, and 5G networks stem from the pressing need to meet the requirements of massive IoT deployments, particularly in massive Machine Type Communication (mMTC)

scenarios. With an anticipated density of 1 million devices per square kilometer, traditional cellular technologies alone cannot fulfill the demands for low-cost, low-power, and wide-coverage connectivity. By leveraging LPWAN technologies, such as LoRaWAN and LoRa mesh, alongside 5G, the gap between current cellular limitations and the evolving needs of mMTC applications can be bridged.

- Despite the benefits of low power consumption, extensive coverage, and low end device cost, unlicensed LPWANs often suffer from drawbacks such as lower data rates and decreased reliability. As a complementary technology, 5G can realize reliable and high data rate communications, supporting the use cases that unlicensed LPWANs cannot support.

- Commercial 5G systems have been deployed progressively since 2018. Due to its boundary-stretching performance metrics, the 5G system can provide the backbone connectivity and management functions for unlicensed LPWANs, thereby significantly reducing complexity and costs while enhancing the resilience of unlicensed LPWAN deployment. Moreover, 5G networks can serve as a powerful computing platform for data processing and network optimization in unlicensed LPWANs.

- The dual deployment of unlicensed LPWANs and 5G requires two separate management systems. Integration enables unified management and optimization of both networks, including authentication, security, and mobility management, thereby improving overall efficiency.

This thesis focuses on addressing the challenges associated with architecture design, management function offloading, data volume reduction, and routing algorithm design. The Objectives of this thesis are

- To perform a thorough survey of unlicensed LPWAN-5G integration by examining state-of-the-art LPWA technologies, cellular technologies, and mesh technologies.

- To develop a hybrid architecture for integrating LoRaWAN with 5G core networks to facilitate the offloading of LoRaWAN servers.

- To integrate LoRa mesh technology into 5G networks, and propose a framework and algorithms for collaborative management of the LoRa mesh network via the 5G network.
- To design a routing algorithm for the LoRa mesh network to enhance network performance, focusing on the reliability, scalability, and coverage of the hybrid network.

## 1.3 Contributions and Research Outcome

Based on the objectives outlined earlier, this research aims to seamlessly integrate LoRaWAN and LoRa mesh into 5G networks and efficiently optimize the hybrid network. This section highlights the main contributions and research outcomes of this thesis.

### 1.3.1 Contributions

The major contributions of this thesis are summarised as follows:

- A comprehensive survey of state-of-the-art unlicensed LPWA technologies, 5G technologies, and mesh technologies is conducted. The survey also presents the LPWAN-5G integration challenges associated with hybrid architecture, security, mobility, interoperability between LPWANs, and coexistence of LPWANs with other wireless technologies. The potential solutions to address these challenges are discussed and evaluated. The outcome of this contribution is published in [P1].
- A LoRaWAN-5G integrated network with a collaborative Radio Access Network (RAN) and a converged core network is designed and implemented by utilizing the Glasgow 5G testbed. A LoRaWAN gateway, built using Raspberry Pi and a 5G modem, is developed with the ability to access the 5G new radio network wirelessly, functioning as a 5G User Equipment (UE). To the best of the author's knowledge, the gateway is the first LoRaWAN gateway that uses 5G as its backhaul technology. Moreover, the LoRaWAN servers are deployed on an edge server of the Glasgow 5G testbed, which is also the first set of LoRaWAN servers running within the core network

infrastructure of a 5G network. Furthermore, a prototype of a smart building heating management system is implemented, showcasing the feasibility of the hybrid network approach. The outcome of this contribution is published in [P2].

- A novel approach to integrate LoRa mesh into 5G networks is proposed, featuring the deployment of specially designed LoRa mesh servers within the 5G core network. A cloud-edge-terminal collaborative architecture with three algorithms, i.e., timely significant-change updates, packet loss detection, and adaptive threshold algorithms, is proposed, significantly reducing the data volume of the hybrid network. Using off-the-shelf components, the LoRa mesh-5G integrated network is implemented at the University of Glasgow campus. While initially designed for weather monitoring, its application extends as a prototype for low data rate sensing along extensive linear infrastructure. The outcome of this contribution is published in [P3].

- A deployment strategy is proposed for the LoRa mesh-5G integrated network in the context of linear infrastructure monitoring, aiming to reduce deployment complexity while ensuring the scalability and extended coverage of the network. The upper and lower bounds of the hybrid network's scalability and coverage extension ratio are derived, along with the conditions for reaching the upper bounds. A novel routing algorithm is proposed, achieving the upper bounds of the network's scalability and coverage extension ratio. Furthermore, a LoRa mesh simulator is developed to verify the system analysis and the proposed routing algorithm. This simulator is expected to make a valuable contribution to the field of LoRa mesh. The outcome of this contribution is published in [P4].

### 1.3.2 Research Outcome

The outcomes of this thesis have resulted in the following publications:

[P1] **Y. Chen**, Y. A. Sambo, O. Onireti, and M. A. Imran, "A survey on LPWAN-5G integration: main challenges and potential solutions," IEEE Access, vol. 10, pp. 32132-32149, 2022.

[P2] **Y. Chen**, Y. A. Sambo, O. Onireti, S. Ansari, and M. A. Imran, "LoRaWAN-5G integrated network with collaborative RAN and converged core network," in 2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). IEEE, 2022, PP. 1-5.

[P3] **Y. Chen**, G. Shi, M. Al-Quraan, Y. A. Sambo, O. Onireti, and M. A. Imran, "LoRa mesh-5G integrated network for trackside smart weather monitoring," IEEE Transactions on Vehicular Technology, 2024.

[P4] **Y. Chen**, G. Shi, Y. A. Sambo, O. Onireti, and M. A. Imran, "On the scalability and coverage of LoRa Mesh for monitoring linear infrastructure," submitted to IEEE Internet of Things Journal.

In addition, two prototypes have been implemented using the Glasgow 5G testbed. Firstly, a LoRaWAN-5G integrated network is deployed in the James Watt South (JWS) building of the University of Glasgow to upgrade the heating system. Secondly, a proof of concept for a trackside smart weather monitoring system based on a LoRa mesh-5G integrated network is deployed on the main campus of the University of Glasgow. Notably, the trackside smart weather monitoring system has been adopted by Network Rail, the largest railway operator in the UK. It is currently undergoing final trackside testing and has the potential to be widely used in UK railways.

Furthermore, a LoRa mesh simulator, called LoRaMeshSim[1], is developed for simulating signal collisions, routing behaviors, and duty cycles. Its open source is expected to facilitate the development of new routing algorithms and enable in-depth analysis of network reliability, scalability, and coverage.

## 1.4 Thesis Outline

The rest of this thesis is organized as follows:

Chapter 2 compiles an in-depth comparison of nine popular LPWA technologies, which are classified into licensed LPWANs and unlicensed LPWANs. Then, mesh technologies are surveyed, before transitioning to an exploration of the intricate architecture and enabling technologies of 5G networks. Finally, the challenges of

[1]Available at https://github.com/YuChenUoG/LoRaMeshSim

LPWAN-5G integration are identified, followed by the potential solutions for these challenges.

Chapter 3 describes the LoRaWAN-5G integrated network with collaborative RAN and converged core network. The implementation of the LoRaWAN gateway with a 5G UE module is presented, followed by a detailed discussion of offloading the LoRaWAN servers to a 5G edge server. Finally, a smart heating use case based on the hybrid network is presented.

Chapter 4 presents the network model and integration methods of the LoRa mesh-5G integrated network. It introduces the cloud-edge-terminal collaborative architecture, and elucidates three key algorithms about timely significant-change updates, packet loss detection, and adaptive thresholds. Additionally, a prototype based on the hybrid network for trackside weather monitoring is deployed on the University of Glasgow campus. Its experimental results are illustrated and analyzed.

Chapter 5 describes a deployment strategy and analyzes the performance of the hybrid network proposed in Chapter 4 in terms of reliability, scalability, and coverage. Based on the analysis, a novel LoRa mesh routing algorithm is proposed to achieve optimal scalability and coverage. Moreover, a LoRa mesh simulator is developed to verify the system analysis and the proposed routing algorithm.

Chapter 6 provides the conclusion. It summarizes the major findings of this thesis and discusses potential future directions to improve the performance of the unlicensed LPWAN-5G integrated networks.

# Chapter 2

# Literature Review

This chapter provides a comprehensive overview of the integration of unlicensed LPWAN with 5G. It begins by discussing popular LPWA technologies and providing a comparative analysis. Subsequently, it delves into mesh technologies and explores the advancements in 5G technologies. Following this, the chapter identifies the key challenges associated with LPWAN-5G integration and presents potential solutions to these challenges. Parts of the work in this chapter have been published in [P1].

## 2.1 LPWA Technologies

LPWAN [5] is a class of communication technologies characterized by low power consumption, low data rate, and wide-area coverage, which are perfectly suitable for most IoT applications such as smart cities, smart agriculture, connected industries, etc. As a promising solution for IoT and Machine-to-Machine (M2M) communication, LPWAN can provide billions of connections at a lower cost than conventional cellular systems.

LPWAN can be classified into two types: cellular LPWAN and non-cellular LPWAN. Cellular LPWA technologies, such as NB-IoT, enhanced Machine Type Communication (eMTC), and Extended Coverage Global System for Mobile Communication IoT (EC-GSM-IoT), are introduced by 3rd Generation Partnership Project (3GPP), operating in licensed cellular frequency bands. They are designed to seamlessly integrate with cellular networks and rely on the infrastructure of the cellular network. Unlike cellular LPWAN, non-cellular LPWA technologies, such as LoRaWAN, SigFox, and Random Phase Multiple Access (RPMA), are designed

independently of cellular systems. Working in unlicensed bands (mostly in sub-GHz ISM bands), non-cellular LPWA technologies are run by both public and private operators. In this section, nine popular LPWA technologies, including NB-IoT, eMTC, EC-GSM-IoT, LoRaWAN, SigFox, RPMA, DASH7, Weightless, and Telensa, are introduced and compared. The Key Performance Indicators (KPIs) of these technologies are listed in Table 2.1.

## 2.1.1 Licensed LPWAN

### 2.1.1.1 NB-IoT

NB-IoT [6] was standardized by 3GPP in Release 13 [7] in 2016. Based on LTE, NB-IoT is introduced to achieve M2M communication with the demand of low cost, low power, long-distance and massive capacity [8]. Due to these characteristics, NB-IoT can be classified as an LPWA technology. Facilitating radio network evolution and efficient coexistence with mobile broadband, NB-IoT can share the same infrastructure as LTE [9]. NB-IoT can be deployed in three operation modes including standalone mode, in-band mode, and guard band mode. In standalone mode, NB-IoT operates in a dedicated band re-farmed from the Global System for Mobile Communication (GSM) with a bandwidth of 200 kHz. In in-band mode, NB-IoT is allocated a LTE carrier with a bandwidth of 180 kHz. In guard band mode, NB-IoT utilizes the unused guard band (180 kHz) of LTE which is located at the edge of the LTE band. The collision and interference between LTE and NB-IoT may occur when NB-IoT operates in in-band mode or guard mode even though their power spectrum density is restricted [10]. NB-IoT is currently operated by many cellular operators in their Fourth Generation (4G) systems.

### 2.1.1.2 eMTC

In addition to NB-IoT, 3GPP Release 13 also introduces eMTC which is an amendment of the LTE-M [11] standard. Compared with machine-type communication in 3GPP Release 12, eMTC can provide extended coverage (less than 11 km) with lower device complexity and lower power consumption [12]. Compared with other LPWA technologies, eMTC can provide a comparatively high data rate of 1 Mbps at the cost of occupying a relatively wider frequency bandwidth of 1.08 MHz within LTE band. Utilizing power savings management and extended discontinuous

Table 2.1: Comparison of cellular and non-cellular LPWANs [15] [16] [17]

| | NB-IoT | eMTC | EC-GSM-IoT | LoRaWAN | SigFox | RPMA | DASH7 | WEIGHTLESS-W | WEIGHTLESS-N | WEIGHTLESS-P | TELENSA |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Licensed | YES | YES | YES | NO | NO | NO | NO | YES | NO | YES/NO | NO |
| Cellular | YES | YES | YES | NO | NO | NO | NO | NO | NO | NO | NO |
| Standardization group | 3GPP | 3GPP | 3GPP | LoRa Alliance | SigFox | Ingenu | DASH7 Alliance | Weightless SIP | Weightless SIP | Weightless SIP | Telensa |
| Frequency (MHz) | 700-900 | 700-900 | 800-900 | EU 868, EU 433, US 915, CN 490, AS 923, etc. | EU 868, EU 433, USA 915 | 2400 | 433, 868, 915 | TV whitespace (470-790) | EU 868, US 915 | Sub-GHz (169/ 433/ 470 /780/ 868/ 915/ 923MHz or licensed) | EU 868, US 915, Asia 430 |
| Bandwidth (Hz) | 180k or 200k | 1.08M | 200k | 125k, 250k, 500k | 200k (100k each) | 1M | 200k | 5M | 200 | 12.5k | 100k |
| Range (km) | 1 (urban), 10 (rural) | <11 | <15 | 2-5 (urban), 10-20 (rural) | 3-10 (urban), 30-50 (rural) | 5 (urban), 15 (rural) | 0-5 | 5 | 2 | 5 | 3 (urban), 8 (rural) |
| Security | 3GPP based | 3GPP based | 3GPP based | Two-layer AES-128b | AES-128b | AES-256b | AES-128b | AES-128b | AES-128b | AES-128b/256b | / |
| Modulation | BPSK, QPSK | QPSK, 16QAM | GMSK/ 8PSK | CSS | BPSK | DSSS for UL, FSK for DL | GFSK | 16-QAM, offset-BPSK | DBPSK | GMSK and offset-QPSK | UNB 2-FSK |
| Adaptive data rate | NO | NO | NO | YES | NO | NO | NO | NO | NO | NO | NO |
| Payload (bytes) | 1600 | / | / | 0-243 | 12 (UL), 8 (DL) | 6-10k | 20 | >10 | 20 | >10 | 65k |
| Data rate (bps) | 200k | 1M | 70k/240k | 300-50k | 100 or 600 | 20k | 200 | 1k-10M | 200-100k | 30-100k | 62.5 (UL), 500 (DL) |
| Network Topology | Star | Star | Star | Star | Star | Star/ Tree | Tree/ Star | Star | Star | Star | Star/Tree |
| Programmability | Depends on operators | Depends on operators | Depends on operators | High | Limited | Limited | Some | High | Moderate | Limited | Programmable |
| Open-source | Limited | Limited | Limited | Open specifications | Proprietary, no open-source | Proprietary, no open-source | Depends on project | Open specifications | Open specifications | Open specifications | Mix of proprietary and potentially open |

reception, the battery life of eMTC can be extended to over 10 years [13]. However, due to the relatively extended coverage and higher data rate, the cost of eMTC end devices is increased, making it have no price advantage [14].

#### 2.2.1.3 EC-GSM-IoT

The 2G cellular network is the first global digital mobile network that has extensive coverage in the world. So, utilizing GSM, 3GPP introduced EC-GSM-IoT [18] for IoT application. Operating in the GSM frequency band with a narrow bandwidth of 200 kHz, EC-GSM-IoT can provide long-range communication of up to 15 km. However, GSM is not specifically designed for IoT applications, resulting in the relatively higher power consumption of EC-GSM-IoT. The battery life of EC-GSM-IoT is shorter than other LPWA technologies due to the relatively high transmitting power of GSM end devices.

### 2.1.2 Unlicensed LPWAN

#### 2.1.2.1 LoRaWAN

LoRaWAN is one of the most popular LPWA IoT networks [19–22]. With regard to 5G mMTC use cases especially those without time-critical requirements, LoRaWAN is a potential complementary solution for the 5G network. It can achieve around 10% of the 5G mMTC connection density objective in the uplink [23]. LoRaWAN is a Medium Access Control (MAC) layer standard based on the LoRa Physical layer standard proposed by Semtech [24] and promoted by the LoRa Alliance [19]. LoRa operates in unlicensed Industrial, Scientific and Medical (ISM) bands with a bandwidth of 125 kHz. According to the Regional Parameters [25] proposed by LoRa Alliance, nine different ISM bands are specified for different regions. In the EU, there are two available bands including the EU 863-870MHz ISM band and the EU 433MHz ISM band. The key technology of LoRa is the Chirp Spread Spectrum (CSS) modulation which will generate a chirp signal for every single bit of data in the same time duration. This kind of modulation enables long-range end-to-end communication which can usually reach 2-5 km in urban areas and 15 km in suburban areas. In [26], the authors conduct a practical experiment using EU 868 MHz ISM band and 14 dBm transmit power, showing the maximum communication range of LoRa is 15 km on the ground and close to 30 km on water. However, due to the CSS

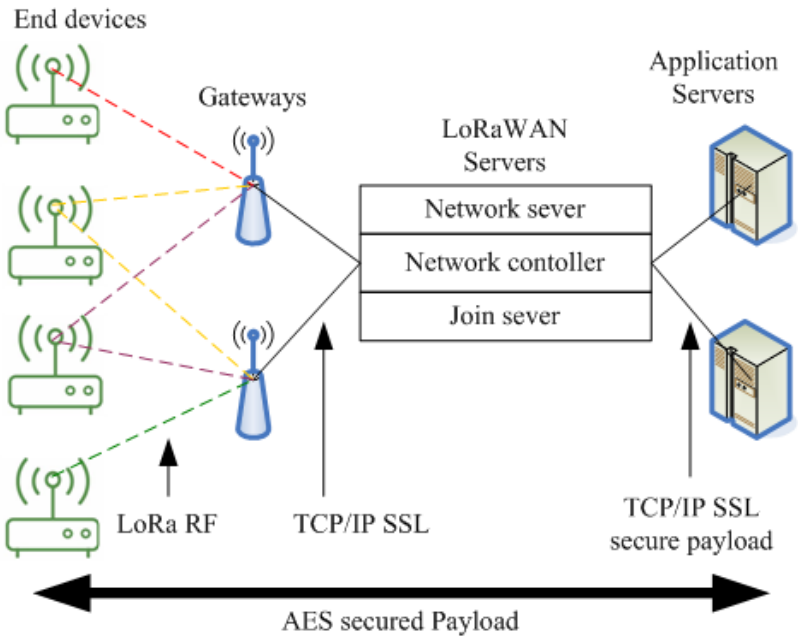



Figure 2.1: The architecture of LoRaWAN.

modulation, LoRa is only suitable for low data rate communication.

Benefiting from the feature of LoRa, LoRaWAN is designed at MAC layer level to achieve long-range, low power, and low data rate communication which is perfectly suitable for IoT networks. As shown in Figure 2.1, LoRaWAN has a star topology with multiple gateways supporting end devices, LoRaWAN servers, and application servers. The core services of a LoRaWAN network include the Join Server, Network Server, and Application Server. The Join Server facilitates the onboarding of new devices onto the network securely. The Network Server manages the communication between end devices and gateways, handling tasks such as routing, data rate control, and security enforcement. The Application Server processes and stores data received from end devices, enabling application-specific logic and functionality.

For the uplink, the packets from an end device should be received and forwarded by all the gateways that can receive the packets. The gateways then forward the packets to the LoRaWAN servers including the network server, the network controller, and the join server. These servers are responsible for controlling the network and determining the network parameters. Specifically, the adaptive data rate is a key function realized by these servers which specify a minimum transmitting power for each end node by adjusting its data rate in the range of 300 to 50k bps. In doing so, the lowest power consumption of the whole network can be achieved.

Finally, LoRaWAN servers also send the frame payloads of the message to application servers for a variety of use cases.

For the downlink, LoRa Alliance defines three kinds of end nodes including class A (baseline), class B (beacon), and class C (continuous) in the LoRaWAN specification [19]. Class A end devices can receive messages only in two short downlink receiving windows following every uplink transmission. Compared with class A, class B end devices can open an extra periodic receiving window for downlink message reception. Class C end devices keep the receiving window open all the time. The three kinds of end devices can be chosen for different use cases to achieve the lowest power consumption. A well-configured LoRaWAN end device powered by a battery of 2400 mAh can achieve a 6-year lifetime when communicating infrequently [27].

In terms of security, LoRaWAN adopts a message integrity code and two-layer Advanced Encryption Standard (AES) secured encryption. Each frame and each MAC layer message have a message integrity code to ensure the integrity of each packet. Further, the application session has a different encryption key from the network session. In doing so, the network operator cannot decrypt the payload data of each application, ensuring the privacy of application users.

LoRaWAN doesn't have a standardized programming API like some other networking protocols do. Instead, it operates on a set of specifications defined by the LoRa Alliance, which includes the physical layer (LoRa) and the MAC layer (LoRaWAN). To interact with LoRaWAN networks, developers typically use LoRaWAN libraries provided by hardware manufacturers or open-source communities. These libraries abstract away the low-level details of LoRa communication and provide higher-level functions for sending and receiving data over LoRaWAN networks.

#### 2.1.2.2 SigFox

SigFox [28] is a typical LPWA technology proposed by its operator, the company also known as SigFox. Based on Low Throughput Network (LTN) [29], SigFox has a similar star network architecture to LoRaWAN. The packets sent from objects, i.e., the end nodes of SigFox, can be received by any base station in the range. Then all the packets are forwarded to the SigFox Cloud to be processed and subsequently, the application payload would be transmitted to the corresponding application server. Unlike LoRaWAN in which the network infrastructure is operated by several

independent operators having joined the LoRa Alliance, the infrastructure of SigFox is operated by SigFox itself.

Operating in unlicensed bands such as EU 433 MHz, EU 868 MHz, and USA 915 MHz, SigFox adopts Binary Phase-Shift Keying (BPSK) [30] modulation in ultra-narrowband which is 100 Hz wide for each message. The message payload is confined within 12 bytes for uplink transmission and 8 bytes for downlink transmission, which is very limited but enough for many sensor data transmissions such as GPS location, temperature, and speed. Unlike the adaptive data rate of LoRaWAN, the data rate of SigFox is fixed to 100 or 600 bps depending on the region. Given that the bandwidth, payload size, and data rate are limited, SigFox can achieve long-distance communication [31] [32] and low power consumption [33]. In rural areas, SigFox can cover a range of 30-50 km while in urban areas the distance is reduced to 3-10 km. Due to low power consumption, the battery life can be significantly extended which is predicted to be over 10 years.

#### 2.1.2.3 RPMA

RPMA [34] is a proprietary LPWA technology proposed and operated by Ingenu which is an American company founded in 2008. Unlike other LPWA technologies that use different sub-GHz frequency bands in different regions, RPMA adopts a unified unlicensed 2.4 GHz ISM band all over the world, which is beneficial for roaming across regions. The bandwidth of RPMA reaches 1 MHz, which is also much wider than other LPWA technologies. In the physical layer, Direct Sequence Spread Spectrum (DSSS) is employed as the modulation method for uplink transmission and a single time slot can be shared by multiple transmitters [35]. In the downlink transmission, RPMA adopts the Frequency Shift Keying (FSK) modulation technique [36]. This physical layer standard has been made to comply with IEEE 802.15.4k, which is a low-power critical infrastructure monitoring networks standard. RPMA can cover a range of 15 km in rural areas and 5 km in urban areas with a payload size of up to 10 kB [37]. In terms of security, RPMA prioritizes data protection through robust encryption mechanisms. It employs AES-256b based encryption, ensuring that data transmitted over the network remains secure and protected from unauthorized access or tampering. This encryption standard is widely recognized for its strength and is commonly used in high-security applications, providing peace of mind for IoT deployments utilizing RPMA technology.

#### 2.1.2.4 DASH7

Stemming from the International Organization for Standardization 18000-7 Radio-frequency Identification [38], DASH7 [39] [40] is an open-source LPWAN standard proposed by DASH7 Alliance. With the modulation technique of Gaussian Frequency Shift Keying (GFSK) [41], DASH7 operates in the sub-GHz ISM bands including 433 MHz, 868 MHz, and 915 MHz. It is designed for ultra-low-power sensor-actuator applications where sensors can report data and actuators can receive commands typically within a latency of 1 second but only consuming 30 uA on average. Offering data rates up to 200 kbps, DASH7 can cover a range of 0-5 km.

#### 2.1.2.5 Weightless

Weightless [42] is an open LPWA technology operated in sub-GHz frequency bands. It is developed, standardized, and maintained by Weightless Special Interest Group. This technology consists of three types of standards including Weightless-W, which operates on licensed bands, and Weightless-N and Weightless-P which both operate on unlicensed bands. They have similar network architecture but the coverage and power consumption of the three stands are different to meet the demands of different use cases.

Based on LTN, Weightless-N [43] is the second standard released by Weightless Special Interest Group. With the Differential Binary Phase Shift Keying (DBPSK) modulation scheme, Weightless-N operates in ISM Sub-GHz bands including EU 868 MHz and US 915 MHz with an ultra-narrow bandwidth. To relieve spectrum collision, a special frequency hopping method is used by Weightless-N to randomly select a channel for each transmission [44]. Weightless-N can cover a range of 2 km with 20-byte payloads. The main disadvantage of Weightless-N is the one-way communication from nodes to the base station.

To conquer the disadvantage of Weightless-N, Weightless-P [45] is proposed to achieve bidirectional communication at the cost of consuming more energy. Adopting Gaussian Filtered Minimum Shift Keying (GMSK) and offset Quadrature Phase Shift Keying (QPSK) modulation scheme, Weightless-P operates in sub-GHz bands such as 433 MHz and 868 MHz or licensed bands with a bandwidth of 12.4 kHz.

#### 2.1.2.6 TELENSA

Telensa [46] provides LPWAN IoT solutions and infrastructure for smart city buildings, especially smart street lighting [47]. With the Ultra Narrow Bandwidth (UNB) 2-FSK modulation scheme, Telensa operates in unlicensed ISM bands including EU 868 MHz, US 915 MHz, and Asia 430 MHz. Although the source is not open, Telensa is trying to standardize its technology to comply with European Telecommunications Standards Institute (ETSI) LTN.

### 2.1.3 Summary of LPWA Technologies

In summary, the landscape of LPWA technologies offers a diverse array of options, each with its unique characteristics and advantages. Among them, unlicensed LPWAN technologies, such as LoRaWAN, emerge as compelling choices for IoT deployments. Unlicensed LPWANs provide distinct advantages over licensed counterparts, including lower regulatory burdens and deployment costs.

Within the realm of unlicensed LPWANs, LoRaWAN stands out for several reasons. Its long-range capability, robustness in challenging environments, and support for bi-directional communication and adaptive data rates make it suitable for a wide range of applications. Moreover, LoRaWAN benefits from a vibrant ecosystem and widespread adoption, fostering interoperability and innovation. Additionally, LoRaWAN's high programmability and adherence to open specifications provide opportunities for customization and innovation, further enhancing its appeal for IoT deployments.

Overall, the advantages of unlicensed LPWANs over licensed alternatives, coupled with the specific benefits of LoRaWAN, position these technologies as key enablers for IoT deployments, offering cost-effectiveness, reliability, adaptability, and scalability for various use cases.

## 2.2 Mesh Technologies

Mesh networks have emerged as a crucial solution for extending the coverage and scalability of IoT deployments, particularly in scenarios where densely deploying gateways is impractical or cost-prohibitive. Traditional LPWAN technologies, such as those employing a star topology like LoRaWAN, face limitations in monitoring

massive infrastructure like railways, where coverage extension becomes essential. Mesh technology addresses this challenge by allowing devices to communicate not only with gateways but also with each other, forming a self-healing and self-organizing network. In a mesh network, each node serves as a potential relay, enabling data to hop through multiple nodes until it reaches a gateway or its final destination. This approach not only extends the coverage area but also enhances network resilience and reliability. The next paragraph will review how mesh technologies have been applied to enhance the capabilities of LPWANs.

As the most promising unlicensed LPWAN, many efforts have been put to extend its coverage by using mesh technologies. Lundell *et al.* [48] proposed a routing protocol for LoRa mesh networks and validated it in both laboratory and field tests. Berto *et al.* [49] implemented a LoRa mesh network based on RadioHead packet radio library [50] which is a popular open-source LoRa mesh library for embedded microprocessors with very limited resources. Lee and Ke [51] evaluated the performance of LoRa mesh networks via a real experiment of monitoring large-area IoT sensors. Huh and Kim [52] proposed a LoRa mesh protocol and discussed its use cases including fire pipe freeze monitoring, street light smart control, and toxic gas monitoring. Ebi *et al.* [53] used a LoRa mesh network to monitor underground infrastructure. By evaluating the performance of two field tests, the authors in [53] proved that LoRa mesh networks have advantages over LoRa and LoRaWAN in terms of the coverage and reliability of packet delivery. Hong *et al.* [54] proposed a hierarchical-based energy-efficient routing protocol for LoRa mesh networks. They demonstrated that the proposed protocol outperforms conventional ad hoc on-demand distance vector routing methods in terms of energy efficiency and transmission delay. Tian *et al.* [55] developed LoRaHop which is an add-on protocol compatible with LoRaWAN to extend the coverage by a multi-hop mesh network. They evaluated its performance on an outdoor testbed demonstrating that LoRaHop can extend the coverage of a LoRaWAN network with improved reliability and reduced power consumption. Wu and Liebeherr [56] proposed a self-organizing communication protocol, called CottonCandy, to mitigate packet collisions during data collection.

## 2.3 5G Architecture

5G was initially standardized by 3GPP from Release 15 in 2018 [57] and shortly afterward, deployments by both public and private network operators commenced. For example, Verizon and AT&T released their first 5G service in the USA at the end of 2018. The early commercial systems of 5G are deployed in the Non-standalone Architecture (NSA) mode in which only the 5G New Radio is utilized and the 4G core network, Evolved Packet Core (EPC), remains as the core network. This architecture provides only enhanced Mobile Broadband (eMBB) service. However, subsequent Releases of 5G provide Ultra-Reliable and Low-Latency Communications (URLLC) service and mMTC service to support varieties of IoT applications. As shown in Figure 2.2, the requirements of the three application scenarios are distinct from each other. For eMBB, 5G is required to provide communication with a high data rate of up to 10 Gbps. For URLLC, 5G should provide mission-critical communication with a latency of less than 1 ms. For mMTC, 5G is expected to enable ultra-dense connection (1 million per $km^2$ [58]). The KPIs of the three application scenarios are too strict to be met simultaneously. Fortunately, most practical use cases do not require 5G to meet all the KPIs. For example, some mission-critical applications require URLLC to function properly but a lot of these applications have low data rate requirements.

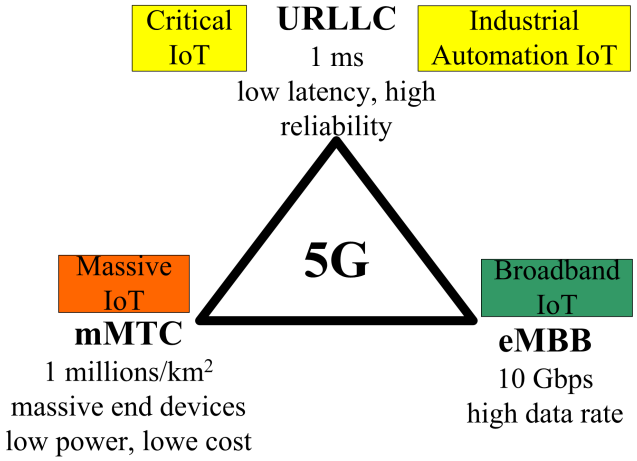



Figure 2.2: Applications scenarios of 5G.

5G has been designed with evolved network architecture and a set of enabling technologies, such as Software Defined Network (SDN), Network Function

Virtualization (NFV), and network slicing, are utilized to support its stringent requirements. Before 5G, cellular technologies are designed by the hardware-based method. SDN, a network paradigm evolved from work done at UC Berkeley and Stanford [59], can replace this method with a software-driven network design, which can make the network more flexible and programmable [60]. NFV can be the complement to SDN for 5G. It enables the functions of the 5G core to work in general-purpose hardware rather than dedicated hardware, which can reduce the operators' costs and make the network more scalable and agile. Due to the distinct scenarios that 5G should be applied to, a physical 5G network is expected to incorporate multiple logical networks with different quality of service. Network slicing can achieve this goal by providing different network topologies and parameter configurations for different services.

There are two methods to describe and visualize the architecture of 5G: reference point representation and service-based representation. In both representations, each network element is called a function. As shown in Figure 2.3, reference point representation is a traditional method that describes the logical interfaces between two functions. In 5G, the interaction between two functions is regarded as a service provisioning process in which one function serves as the service provider and the other one serves as the service user [61]. Thus, service-based representation, shown in Figure 2.4, can describe this notion better. Moreover, the control plane and user plane are completely separated in 5G. Compared with 4G, there are three noticeable features in the 5G network architecture. First, some 4G entities are separated into several logical functions in 5G. For example, the home subscriber server in 4G can achieve UE authentication while in 5G the subscription information stored in Unified Data Repository (UDR) [62] should be retrieved by Authentication Server Function (AUSF) through Unified Data Management (UDM). This kind of separation can simplify the deployment and management of the functions even when the network scales up in size. Second, new functions have been introduced to provide more services. For example, a network slicing Select Function is introduced to achieve network slicing. Third, unlike 4G, the entities in 5G are called functions because they are just logical functions that may run in the same physical general-purpose hardware by NFV.

In the realm of 5G networks, several key components play pivotal roles in enabling seamless connectivity and efficient data management. The Access and Mobility Management Function (AMF) oversees device authentication and mobility

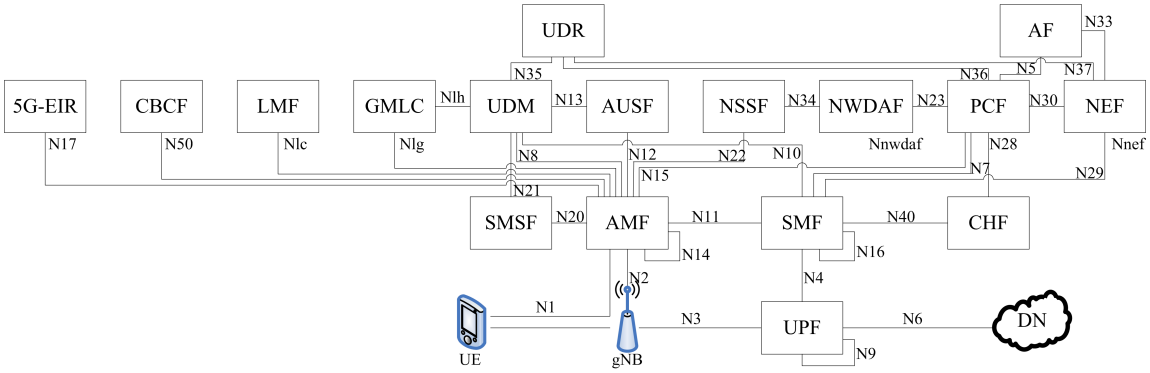



Figure 2.3: Reference-point network architecture of 5G [57].

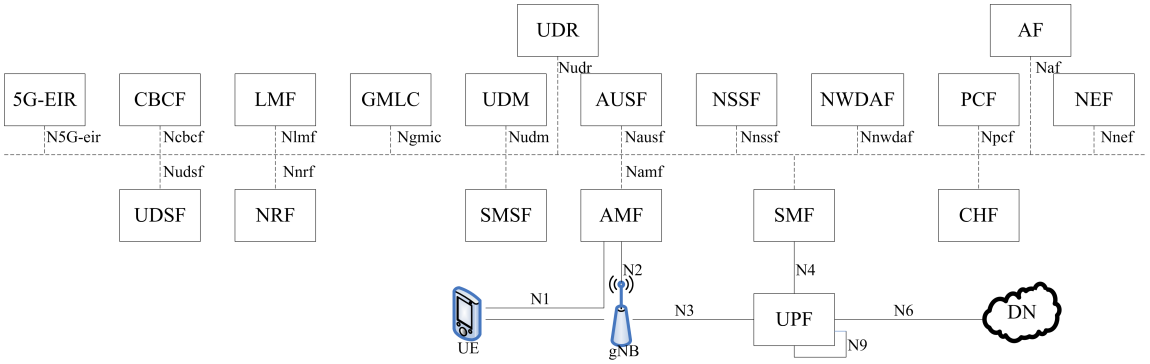



Figure 2.4: Service-based network architecture of 5G [57].

management, ensuring smooth transitions between network cells. The Session Management Function (SMF) handles session establishment and management, facilitating data flow between devices and applications. The User Plane Function (UPF) serves as the traffic anchor, managing data routing and forwarding across the network. AUSF authenticates users and devices, enhancing network security. The UDM and UDR collectively manage subscriber data, enabling personalized services and efficient resource allocation. Lastly, the Network Slice Selection Function (NSSF) dynamically selects and allocates network slices based on service requirements, optimizing network resources for diverse applications and user needs. Together, these components form the backbone of 5G infrastructure, empowering high-speed, low-latency connectivity and unlocking the potential of next-generation technologies.

It can be seen from Sections 2.2 and 2.3 that the requirements of the mMTC scenario can be met by LPWAN and with 5G being a flexible, scalable, agile, and programmable network platform, it is the opportunity to integrate LPWAN into 5G

network to create a hybrid ecosystem for IoT [60]. The authors in [63] introduce the 5G test network in Oulu, Finland, which has a highly heterogeneous architecture including IEEE 802.11, Bluetooth Low Energy, LoRa, NB-IoT, ultra-wideband and LTE evolution like LTE-M and LTE-U. The 5G test network demonstrates the feasibility of unlicensed LPWAN-5G integration, but there are still many challenges.

## 2.4 LPWAN-5G Integration

Cellular LPWA technologies are designed to be compatible with cellular networks, but they operate in licensed cellular bands, which results in significant initial capital investment. Non-cellular LPWA technologies, operating in unlicensed bands with low power consumption, wide coverage, low-cost, and scalability, are expected to complement 5G networks to support a variety of applications. By integrating unlicensed LPWAN into 5G, the capital and operational expenditures of the operator can be significantly reduced through a hybrid network with a unified management entity. However, there are several challenges to the integration of non-cellular LPWAN and 5G, including hybrid architecture, security, mobility, interoperability between LPWA technologies, and coexistence of LPWANs with other wireless technologies. In this section, all the identified challenges and potential solutions will be discussed as all of them are important aspects of LPWAN-5G integration. However, this thesis only focuses on addressing the challenge of hybrid architecture in the subsequent chapters. Other challenges will be tackled in my future work.

### 2.4.1 Challenges

#### 2.4.1.1 Hybrid Architecture

5G and unlicensed LPWAN have their own infrastructures which are different from each other. For operators that require both 5G and LPWAN, it could be costly and inefficient to deploy and manage two network infrastructures simultaneously. Thus, there is an urgent need for a hybrid architecture that can support and manage LPWAN end devices through 5G infrastructure. Unfortunately, it is challenging to design such hybrid architecture for both access and core networks. As shown in Figure 2.1, LoRaWAN has a simple architecture that is distinct from the much more complicated architecture of 5G shown in Figure 2.3. In terms of access networks,

LoRaWAN end devices transmit each packet over the air to all the gateways that can receive the signal, and then these gateways will forward the copies of the packet to the network server without processing. In contrast, 5G UE will select the best gNB to transmit packets, and then only the serving gNB will transmit the packets to the core network. Moreover, LoRaWAN and 5G have distinct radio access technologies that are only suitable for their own use cases and cannot be applied to each other.

In terms of core networks, emerging enabling technologies, including network slicing, NFV, and SDN, provide the possibility of implementing LoRaWAN servers within a 5G core network. The control plane and the user plane are separated entirely in the 5G core network for scalability and easy management [64]. By contrast, all the signals, including both signaling and user data, are transmitted to Network Server in LoRaWAN. Hence, LoRaWAN packet routing has to be carefully designed in the converged core network for seamless interoperability.

#### 2.4.1.2 Security

As expected, 5G and LPWAN adopt different security schemes. Compared with 5G, the security schemes of LPWAN are simplified due to the requirements of low cost and low power consumption of end devices. However, this results in three notable security challenges for LPWAN-5G integration, which are identity protection, key derivation and encryption, and unified authentication procedure. First, to protect UE identities, 5G adopts the subscription concealed identifier to conceal the permanent UE identifier, i.e. Subscription Permanent Identifier (SUPI), which is not transmitted over the air in plain text at any time [65]. By contrast, LPWANs do not meet the requirements of identity protection of 5G [66]. For example, LoRaWAN end devices will send a join-request, containing Devices Extended Unique Identifier (DevEUI) and Join Extended Unique Identifier (JoinEUI), to the gateways over the air without encryption [25]. DevEUI and JoinEUI are 64-bit MAC addresses that identify LoRaWAN end devices and Join Servers respectively. The Join-request in plain text would undermine the security of the LPWAN-5G integrated network [67]. In terms of the privacy of LPWAN users, their DevEUI could be captured by illegitimate gateways, resulting in position exposure and/or the crisis of replay attack [68]. In terms of the security of the integrated core network, JoinEUI would expose the address of the function dealing with the join-request, which could lead to denial-of-service [69]. Thus, identity protection is one of the challenges when

designing secure LPWAN-5G integrated networks.

Second, it is difficult to integrate the different key hierarchies and encryption methods of LPWANs and 5G. From the root key $K$ to the radio key $K_{gNB}$, 5G adopts a 6-level key hierarchy and AKA-based encryption. By contrast, LPWANs generally adopt a 2-level key hierarchy and AES-based encryption as shown in Table 2.1. To enhance the efficiency of the hybrid network and benefit from the integrated infrastructure, the keys of LPWANs can be derived from the keys of 5G. However, it is challenging to design an exchange mechanism to send 5G keys to LPWANs without posing any threats to the security of the 5G network.

Third, LPWANs adopt diverse authentication methods and it is difficult to design a unified authentication method for all kinds of LPWAN end devices in the hybrid network. 5G adopts three bidirectional authentication methods including the 5G-authentication and key agreement [70], extensible authentication protocol method for 3rd Generation authentication and key agreement [71] and extensible authentication protocol-transport layer security [72]. The extensible authentication protocol-transport layer security is used to provide key services in specific IoT circumstances [73]. Due to the constraints on end devices such as low power and low cost, LPWANs tend to adopt unidirectional authentication methods i.e., only end devices need to be authenticated by the network [74]. When different types of LPWAN end devices connect to the hybrid network, a network-independent authentication method should be used for these end devices to reduce network complexity and ease management. However, given the diversity of LPWANs and the requirement of compatibility with 3GPP's specifications, it is hard to design a unified authentication method for these LPWAN end devices. Hence, special care must be taken when designing an LPWAN-5G hybrid network to ensure that the security of both technologies is not compromised.

#### 2.4.1.3 Mobility

In most cases, both cellular and non-cellular LPWANs only consider fixed connected things and the mobility of end devices is not the strength of LPWANs, which limits the range of their suitable use cases [75]. For example, as two major drivers of the expected IoT growth in the next few years, smart transportation and logistics tend to adopt IEEE 802.11p-based technologies instead of LPWANs mainly due to their mobility [76]. Although roaming and high mobility are not supported by

most LPWAN standards, mobility is one of the key features of 5G systems [77]. In the hybrid network of LPWAN-5G integration, the mobility and roaming ability of LPWANs is expected to be significantly enhanced by virtue of the strong mobility and roaming ability of 5G. However, there are three challenges that should be addressed to enhance the mobility and roaming ability of LPWANs by 5G. First, the interface between the data management entities of LPWAN and 5G should be designed carefully. As shown in Figure 2.3, 5G adopts UDM to manage subscription data stored in UDR [62]. By contrast, LPWANs employ different entities to manage data. For example, as shown in Figure 2.1, Join Server is the the entity that manages the subscription information of LoRaWAN users [78]. The different data management entities need to communicate with each other through an interface when a 5G network is utilized to authenticate the roaming or moving end devices of LPWANs. The interface must be designed carefully as important data, such as encryption keys and subscription information, would be transmitted through it, which has an impact on network security and privacy.

Second, it is challenging to map from the 64-bit MAC address of LPWANs end devices to SUPI of 5G. According to 3GPP specifications, all the data of 5G, including subscription data, policy data, structured data for exposure, application data, and group ID mapping data, converged in an UDR, instead of multiple databases [79]. In the hybrid network of LPWAN-5G integration, the subscription data of LoRaWAN should be transferred to UDR for both mobility enhancement and compatibility with 5G standards. However, as shown in Figure 2.5, the user equipment Identifier (ueId) serves as the identifier to structure the subscription data in UDR for 5G. The ueId of 5G, referred to as SUPI, is no more than 15 digits consisting of mobile country code, mobile network code, and mobile subscription identification number. By contrast, LPWANs generally use 64-bit MAC addresses as the identifiers of their end devices. To keep UDR compliant with 3GPP, the long MAC addresses need to be mapped to the short SUPI, which is a challenge.

Third, designing a unified charging and billing policy for LPWANs in the 5G system needs to be considered. Emerging enabling technologies allow 5G networks to achieve multitenancy, multi-network slicing, and multi-level services, resulting in the increasing complexity of charging and billing systems [80]. From release 15, service-based charging and billing systems are introduced by 3GPP, merging the message commands, chargeable events, and charging information in the charging function [81]. On the other hand, the charging and billing policies of LPWANs usually depend on

the operators and are highly diverse. Thus, to enhance the mobility of the hybrid network, a hybrid core needs to be carefully designed to support both the highly diverse charging policies of LPWANs and the highly converged and complex charging policies of 5G.

Given the security challenges, the hybrid architecture design necessitates merging LPWAN servers into the 5G core network and offloading LPWAN databases to the UDR of 5G. This consolidation facilitates unified authentication procedures, crucial for managing diverse LPWAN end devices within the hybrid network. By centralizing authentication mechanisms and database management within the 5G infrastructure, security can be enhanced while ensuring seamless interoperability between LPWAN and 5G technologies.

#### 2.4.1.4 Interoperability between LPWA Technologies

In the Internet of Everything era, a single technology cannot meet the demands of all kinds of use cases. Multiple LPWA technologies may be deployed in the same area or even in the same hybrid ecosystem. However, most non-cellular LPWA technologies operate in unlicensed ISM frequency bands that are close to each other or even in the same bands, resulting in interference and collisions [82]. For example, both operating in EU 868 MHz and EU 434 MHz, LoRaWAN and SigFox may interfere with each other in Europe [83]. Thus, the main challenge of interoperability between LPWANs is to mitigate interference of radio signals. Moreover, although LPWANs have the advantages of wide coverage, low cost, and low power consumption, their weaknesses are also noticeable, such as low mobility, low reliability, and low security. It is important to overcome their weaknesses through interoperability between multiple LPWA technologies.

#### 2.4.1.5 Coexistence with Other Wireless Technologies

Although LPWANs have the advantages of low power consumption, wide-area coverage, low cost, and scalability, they generally have lower data rates, lower reliability, and higher latency, and can only meet the demands of mMTC. For other types of IoT requirements like URLLC, LPWANs are not suitable. In order to meet the demands of all kinds of use cases, a hybrid 5G-based ecosystem with various wireless technologies including but not limited to LPWANs is needed. Given the distinct features of these different wireless technologies, designing a coexistence

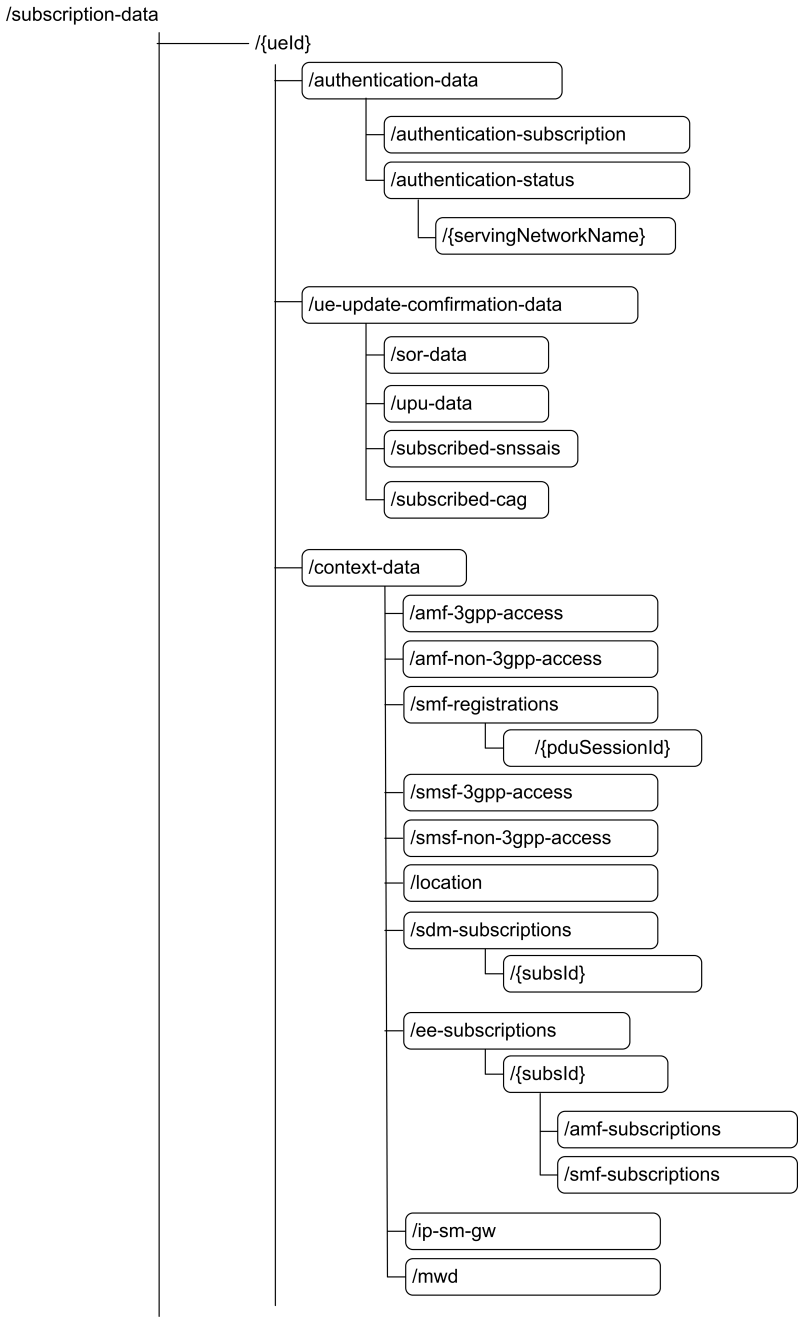



Figure 2.5: Architecture of subscription data in UDR (extracted from [79]).

scheme for the 5G-based ecosystem is a great challenge. Thus, the existence of LPWANs with other wireless technologies should also be considered when designing the scheme of LPWAN-5G integration.

As shown in Table 2.2, the challenges of LPWAN-5G integration are summarized and linked with corresponding potential solutions that will be discussed in the next section.

## 2.4.2 Potential Solutions

### 2.4.2.1 Architecture of Unlicensed LPWAN-5G Integrated Networks

The authors in [84] investigate how to seamlessly integrate LoRaWAN into 5G and propose four potential integration options, i.e. 1) via 3GPP access network, 2) via non-3GPP untrusted access network, 3) as a part of eNodeB, and 4) virtually as a part of the core network. In Option 1, the LoRaWAN gateway has access to eNodeB by installing the universal mobile telecommunications system subscriber identity module and Internet Protocol (IP) stack in the gateway. Then, by the eNodeB connected with EPC through the S1 interface, LoRaWAN can access the core of the cellular network. This option is easy to implement and has already been realized in the 5G Test Network of the University of Oulu, Finland in 2017 [84]. Moreover, currently, there are also available commercial LoRaWAN gateways in the market for this Option, like the Wirnet iFemtoCellevolution LoRaWAN gateway [85] produced by Kerlink. In Option 2, the LoRaWAN gateway is also required to have an IP stack. Moreover, the evolved packet data gateway configured in the 5G core network can create an Internet protocol security tunnel for untrusted non-3GPP access network [86], which makes it possible for the LoRaWAN gateway to be connected with the 5G core network through one non-3GPP technology like WiFi. Wi-Fi operates as an untrusted access network by providing open or password-protected connectivity to users, typically in public spaces or private environments. Users connect to Wi-Fi hotspots, which may lack stringent security measures, making them susceptible to various security threats such as eavesdropping and unauthorized access. In Option 3, the LoRaWAN gateway is incorporated into eNodeB which is expected to support multiple LPWA technologies in the future, enabling LPWAN end devices to have access to eNodeB directly. This will increase the complexity of eNodeB and at the stage of deployment, the operators have to modify many eNodeB that they have already deployed before. In Option 4, utilizing NFV and the OpenStack cloud

Table 2.2: Challenges and potential solutions

| Aspects | Challenges | General efforts | Potential solutions | Status[1] |
|---|---|---|---|---|
| Architecture | Access network design | Actility, Simfony | [84, 87–91], Kerlink | ✓ |
| | LoRaWAN packet routing in the converged core | | None | × |
| Security | Identity protection | 5G: [92–101] LPWANs: [102–110] Integration: [111] | None | × |
| | Key derivation and encryption | | [87], [88] | ✓ |
| | Unified authentication procedure | | [112, 113] | ✓ |
| Mobility | Interface design between data management entities | 5G: [103, 114–122] LPWANs: [123–129] Hybrid network: [130] | [88] | ✓ |
| | Mapping from MAC address to SUPI | | None | × |
| | Charging and billing policy design | | None | × |
| Interoperability between LPWANs | Interference between LPWANs | None | [83], [82] | ✓ |
| | Overcoming weaknesses by interoperability | | [130–132] | ✓ |
| Coexistence with other wireless technologies | designing a coexistence scheme for a hybrid 5G-based ecosystem | None | [10, 133–142] | ✓ |

[1] ✓denoting that the challenge has not yet been completely solved even though some work has been done, and × denoting that no work has been done to address the challenge

platform, the LoRaWAN server will be installed in the cloud as a part of the 5G core network and the LoRaWAN functionality will be available in some virtual instances.

Similar to option 3, the integrated architecture proposed by [87], named Option 5 in the survey, is to implement the virtual base station function of eNodeB protocol stacks into LoRaWAN gateways, which enables the gateway to deliver signaling and data messages through 5G core network. In both Option 3 and Option 5, the integration is achieved at the RAN level by incorporating LoRaWAN gateways with eNodeB, but their incorporating directions are opposite. In Option 5, only the LoRaWAN gateway needs to be modified, while the end device, LoRaWAN server, and 5G core network infrastructure remain standard. Consequently, both 5G and LoRaWAN security are maintained. Furthermore, from the cellular operators' perspective, Option 5 is better than Option 3 considering the cost of deployment as there is no need to modify a great number of eNodeB that have already been deployed before. Therefore, Option 5 has advantages over Option 3 in terms of security [87] and deployment costs.

In [88], the LoRa end device is equipped with components required in 5G UE, which consequently has the capability of 5G communication. The architecture is denoted as Option 6 in the survey. When adopting Option 6, the roaming end device can be authenticated in a visited LoRaWAN network by virtue of a 5G core network, which enhances the mobility and roaming ability of LoRaWAN. There are two authentication methods in Option 6. Method A does not require 5G coverage but deviates from the standard authentication procedures of 5G and LoRaWAN. By contrast, method B almost follows the standard authentication procedures of 5G and LoRaWAN but requires 5G coverage and pre-authentication. Although the roaming ability is enhanced, Option 6 is not suitable for many common use cases, especially in cases where the end device does not need roaming, making this option expensive since the end device has dual connection capability.

Other researchers employed architectures of these options to investigate other issues of cellular-LoRaWAN integration. Employing Option 1, an LTE-LoRaWAN integrated network is adopted in [89] to evaluate two use cases, i.e., terrestrial vehicular and unmanned aerial vehicles. Specifically, LTE serves as a backhaul network while LoRaWAN is used to deliver the data collected in sensors. In doing so, the cellular infrastructure that the operators have deployed can be employed to support the LoRaWAN network. With the architecture of Option 1, [90] utilizes LTE as the backhaul to deliver packets from the gateway to the network server,

and the LoRaWAN gateways are replaced by multiple intermediate gateways that can receive packets from end devices and then forward them to eNodeB. Copies of the same uplink packets from an end device are likely to be transmitted to multiple gateways and then to be forwarded to LTE. To reduce the load of LTE, [90] proposes a traffic management method to select a suitable eNodeB and a gateway for each uplink traffic. Also focused on traffic management, [91], however, adopts Option 5 instead of Option 1. It proposes a routing and packet scheduling mechanism in the integrated network, which allows multiple LoRa gateways to coexist and forward packets through EPC to the application server. Actility [143] and Simfony [144] announced in April 2021 that they will cooperate on developing a multi-technology IoT platform that can provide Mobile Network Operators (MNOs) and mobile virtual network operators an integrated solution for the management of LoRaWAN and Cellular IoT networks.

The hybrid architectures of the 6 options are illustrated in Figure 2.6, and the comparison among them is concluded in Table 2.3. Most of the options, including Option 1, 2, 3, and 5, are only considering access-level integration and only utilize cellular networks as backhaul. Although Option 6 works at the core network level, it is only suitable for very limited use cases due to the requirement of dual connection. Option 4 focuses on the core network for most use cases, but its authors do not provide any methods to achieve it.

#### 2.4.2.2 Authentication, Security and Privacy

Security is an important aspect of both 5G and LPWANs. Significant research [92–98] has been carried out to generally analyze 5G security including its technologies, challenges, threats, and solutions. Given that 5G provides substantial support for IoT, some research works, such as [99–101], focus on 5G security in IoT application scenarios. Although LPWANs simplify their security mechanism to achieve low cost, low complexity, and low power consumption, security is still an essential aspect especially when considering network integration. Some surveys [102–104] on LPWANs analyze the security mechanisms of LPWANs. Other works focus on one specific LPWA technology, such as [105] and [106] on NB-IoT, [107] and [108] on LoRaWAN, and [109] and [110] on SigFox.

In terms of LPWAN-5G integrated networks, there are also some published works aiming at addressing the security challenges. The work in [111] surveys the

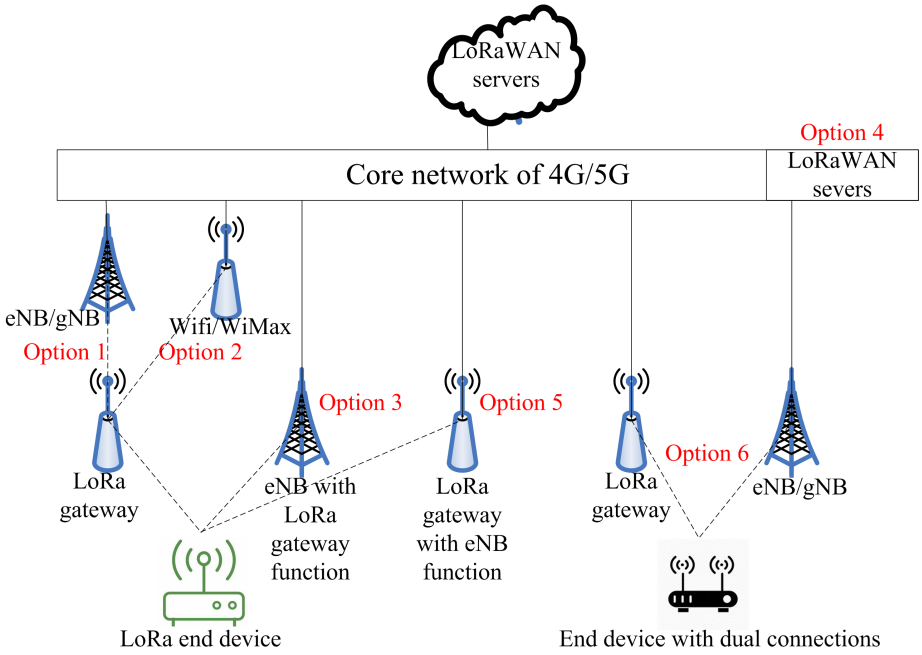



Figure 2.6: Six LoRaWAN-5G hybrid architectures.

Table 2.3: Comparison of six hybrid architectures

| | Option 1 | Option 2 | Option 3 | Option 4 | Option 5 | Option 6 |
|---|---|---|---|---|---|---|
| Papers | [84], [89], [90] | [84] | [84] | [84] | [87], [91] | [88] |
| Architecture | 3GPP access network | Non-3GPP untrusted access network | Part of eNodeB | Virtually as a part of core network | Incorporate eNodeB into LoRaWAN gateway | End device having dual connection |
| Applicable use cases | Most use cases | Most use cases | Most use cases | Most use cases | Most use cases | Roaming |
| Integration level | Access | Access | Access | Core | Access | Core |
| Deployment cost | Medium | Medium | High | Medium | Low | Low |
| Follow standard procedure | Many | Many | Almost all | Many | Almost all | Method A: little, Method B: Almost all |

security challenges of integrating LPWA technologies in 5G systems and analyzes the security requirements of LPWAN-5G integration. It can be seen from [111] that LPWAN-based security solutions need to be enhanced and adapted to meet the requirements of 5G. A secure LoRaWAN-cellular integration proposal is provided in [87], in which each LoRaWAN packet serves as the payload of a 4G message. In doing so, each LoRaWAN message ends up with two-layer encryption including AES-based encryption (LoRaWAN) and AKA-based encryption (4G). The security of both LoRaWAN and cellular networks can be ensured in this hybrid architecture. The solution proposed in [88] is to borrow 5G keys as the network session root key of LoRaWAN. Derived from the root key $K$, $CK$ and $IK$ are important 5G keys stored in both the universal mobile telecommunications system subscriber identity module and UDR to generate other derived keys. In this solution, $IK$ is used as $NwkKey$, the network session root key of LoRaWAN, when authenticating roaming LoRaWAN end devices. In further messages after authentication, $CK$ is used as $NwkKey$. This solution can improve the security of LoRaWAN and enhance the network efficiency as there is no need to store $NwkKey$ in LoRaWAN end devices or Join Server. However, in standard 5G systems, $IK$ or $CK$ is not allowed to leave UDM or UE. The key sharing proposed in [88] may have a negative impact on 5G security, which needs further analysis. Moreover, the importance of identity protection is also discussed in [88], but no potential solution is proposed to protect LoRaWAN identity in the integrated network.

Rather than designing a security method for a specific LPWA technology, the authors in [113] and [112] propose a network-independent solution for access authentication of LPWAN end devices integrated into 5G. This solution is designed for constrained devices which is suitable for many LPWA technologies, such as LoRaWAN, NB-IoT, and LTE-M. However, this solution is only for the secondary authentication of 5G. More research is expected to be carried out on the security aspect of LPWAN-5G integration.

#### 2.4.2.3 Mobility and Roaming

Mobility and roaming of 5G has been comprehensively studied in [114] and [115], covering architecture, services, drivers, key challenges, and solutions. Other surveys, including [103], [116], [117] and [118] , also analyze mobility and roaming of 5G. Moreover, distributed mobility management [119] [120] and blockchain-based

mobility management [121] [122] are expected to bring great evolution to 5G. Compared with 5G, mobility is the weakness of LPWANs. Thus, some efforts have been undertaken to enhance the mobility of LPWANs [123–126]. In terms of LoRaWAN, roaming is the main research direction recognized by LoRa Alliance to enhance mobility [76], and some research, such as [127–129], has been carried out to enhance its roaming ability. However, the author only found one paper focusing on addressing the roaming challenges of LPWAN-5G integrated networks [88]. In [88], two similar LoRaWAN-5G integration methods are proposed to enhance the mobility and roaming ability of LoRaWAN. By virtue of the 5G core network integrated with LoRaWAN, roaming end devices can be authenticated in a visited LoRaWAN network. In terms of interface designing, the S1AP interface is used to connect the Join Server with AUSF, and the S6a interface is used to connect the Join Server with UDM. Borrowing a standard interface can ensure security, but dedicated interfaces still need to be designed to improve the efficiency of data exchange. Although [88] provides the first roaming solution for LoRaWAN-5G integrated networks, the end devices in the methods are required to have dual connection ability which will significantly increase the cost of each end device. In most IoT use cases, a substantial number of end devices are needed to be deployed. It is obvious that including a 5G module in LoRaWAN end devices will significantly increase their cost. Instead of focusing on LPWAN-5G integrated network, the authors in [130] propose a media-independent solution for mobility management in heterogeneous LPWANs. Although they do not consider a 5G network, this IPv6-based solution can be potentially used for an LPWAN-5G integrated network when multiple LPWA technologies are integrated into a single 5G network.

#### 2.4.2.4 Enhancing Interoperability within LPWA Technologies

The interference between LPWANs has attracted attention from the research community. The authors in [83] measure and analyze the interference between LoRa and SigFox in the band of 863-870 MHz in Aalborg, Denmark. The results show that there is a 22-33% probability of interfering signals above -105 dBm in downtown Aalborg. Also focusing on interference measurement, the authors in [82] measure and analyze the interference between sub-Gigahertz technologies including LoRa, SigFox, Z-wave, and IO Home Control. The results show that there is a non-negligible loss of 12-20% when the interferer starts during the preamble and header time. Although

the interference between LPWANs has been measured and analyzed, to the best of the author's knowledge, there is no effective solution that has been proposed to eliminate the interference.

A single LPWA technology has some limitations such as low reliability, high latency, and low mobility. Adopting multiple LPWANs simultaneously could enhance their capabilities. To enhance reliability, the interoperability between NB-IoT and LoRaWAN is studied in [131], and the interoperability between NB-IoT and SigFox is studied in [132]. The prototype of a multi-RAT LPWAN device in smart cities via integrating LoRaWAN into NB-IoT has been demonstrated in [131]. The result shows the feasibility of interoperability between LoRaWAN and NB-IoT. Compared with a single LPWAN, the end devices with dual connections of both LoRaWAN and NB-IoT have higher flexibility, reliability, and dependability. To realize low cost and wide area coverage, most LPWA technologies work in the sub-GHz band, suffering from high data loss rate mostly due to the channel effects [145] [146]. Besides, the quest to keep the network in the low power mode negatively affects data packet delivery. As a result, it is difficult for LPWAN to support critical use cases that need high reliability or low latency. In [132], redundant LPWA technologies are used to provide improved resilience for critical use cases. Specifically, NB-IoT is implemented as the primary communication technology to send data while SigFox is chosen to be the secondary communication technology to provide a backhaul path. To enhance mobility, the handovers between LoRaWAN and NB-IoT are achieved in [130] by an IPv6-based solution. In conclusion, the works in [130], [131], and [132] demonstrate the benefits of interoperability between different LPWANs, but more solutions are needed to improve the efficiency of interoperability.

#### 2.4.2.5 Facilitating Coexistence with other Technologies

In the era of the Internet of Everything, billions of devices will be connected and varieties of wireless access technologies will coexist in the same area or even in the same ecosystem. When designing the LPWAN-5G integrated network, the coexistence of LPWAN with other wireless technologies should also be considered. The work in [133] surveys the potential of integrating cognitive radio into LPWAN for IoT-based applications. Given the heterogeneity and the requirements of IoT standardization, the authors in [134] propose an architecture of the integrated IoT application development platform that supports heterogeneous IoT end devices

including both long-distance and short-distance communication devices such as LoRa, ZigBee, and Bluetooth Low Energy. The options for the integration of LPWAN and low rate-wireless personal area networks are investigated in [135], and two technologies: NB-IoT and IEEE 802.15.4.g, are selected to implement the integration. The authors in [136] analyze the coexistence of 5G NR, LTE-A, and NB-IoT in the 700MHz band by an indoor experiment, showing an efficient spectrum sharing for the three wireless technologies.

Although NB-IoT is designed to comply with LTE and utilize the infrastructure of LTE, interference and collision may still happen due to their operating frequency bands that are the same or close to cellular bands [138]. [10] demonstrates that NB-IoT may interfere with LTE which is likely to affect the coexistence of NB-IoT with LTE. The authors in [139] analyze the interference between NB-IoT and LTE signals and propose a new algorithm for channel equalization to reduce the sampling rate mismatch between the NB-IoT user and LTE base station. To eliminate NB-IoT interference to LTE, machine learning is a potential solution, e.g., the block sparse Bayesian learning-based approach proposed in [140] and the sparse machine learning-based approach proposed in [141]. Based on the interference prediction, the authors in [142] propose a novel framework for radio resource management in NB-IoT systems. In addition to the NB-IoT, LoRa may also interfere with LTE if the LoRa transceiver, like SX1281 released by Semtech, operates in the 2.4GHz frequency band [137].

## 2.5 Summary

This chapter provides a survey and tutorial on LPWAN-5G integration for hybrid networks, focusing on main integration challenges and potential solutions. Firstly, a comparison is made among the leading nine popular LPWA technologies, which were classified into cellular LPWANs operating in licensed bands and non-cellular LPWANs operating in unlicensed bands. Mesh technologies are also presented, offering the potential to extend the coverage of the unlicensed LPWANs without the limitation of star topologies. Following this, the 5G network architecture is introduced as a flexible, scalable, agile, and programmable network platform to which other technologies can be integrated, along with the enabling technologies. Finally, the main challenges and potential solutions of LPWAN-5G integration are

discussed in detail. In summary, it is feasible to integrate LPWANs into 5G systems, but some key problems should be addressed including hybrid architectures, security, mobility, and interoperability between LPWANs, and coexistence with other wireless technologies. Moreover, LoRaWAN and LoRa mesh will be given priority when integrating non-cellular LPWA technologies into 5G given their popularity and open-source protocol. Furthermore, unlike previous work mainly focusing on access-level integration, more efforts will be undertaken to design a converged core network for LPWAN-5G integration. Thus, in the following chapters, the focus will be on integrating LoRaWAN and LoRa mesh into a 5G network, addressing the challenge of hybrid architecture, and enhancing network performance through the utilization of the 5G core network.

# Chapter 3

# LoRaWAN-5G Integrated Network with Collaborative RAN and Converged Core Network

This chapter proposes a LoRaWAN-5G integrated network with a collaborative RAN and a converged core network. The work presented in this chapter has been published in [P2].

## 3.1 Introduction

The 2021 United Nations climate change conference concluded with nearly 200 countries agreeing on the Glasgow climate pact [147] to keep the critical 1.5°C global warming goal alive. IoT technologies and their application to smart buildings, smart factories, smart transportation, etc., will contribute massively to achieving this goal. Due to various requirements, a single IoT technology can not provide ubiquitous coverage or address all the vertical IoT use cases. It is important to design an efficient hybrid network that many IoT technologies can be integrated into. 5G has been designed from the ground up to support a number of cellular IoT technologies.

Characterized by low cost, low data rate, low power consumption, and wide-area coverage, cellular LPWANs, such as NB-IoT, eMTC and EC-GSM-IoT, are an important class of cellular IoT technologies for massive IoT applications. Standardized by 3GPP, cellular LPWANs operate in licensed bands and are designed to co-exist with cellular networks. Unlike cellular LPWANs, non-cellular LPWANs,

such as LoRaWAN [148] and Sigfox, are designed independently of cellular networks, requiring end-to-end deployment of a dedicated access and core infrastructure. However, non-cellular LPWANs are also the main players capturing the LPWAN market mainly because of their advantages over cellular LPWANs in terms of battery lifetime, capacity, cost, and unlicensed frequency band [149].

LoRaWAN is the leading non-cellular LPWAN technology. ABI Research forecasts that LoRaWAN will account for over a one-fourth share of all LPWAN connections by 2026 [150]. To ease the deployment and management of LoRaWAN, some work has been done to integrate LoRaWAN into 4G/5G networks. The authors in [84] propose four integration options, i.e., 1) via 3GPP access network, 2) via non-3GPP untrusted access network, 3) as a part of eNodeB, and 4) virtually as a part of the core network. The authors in [87] propose to implement the virtual base station function of eNodeB protocol stacks into LoRaWAN gateways. Focusing on roaming scenarios, a core-level integration is proposed in [88] for end devices of dual connectivity of 5G and LoRaWAN. Adopting the 3GPP access network based integration option in [84], the authors in [89] evaluate two use cases of a long-term evolution (LTE)-LoRaWAN integrated network. The authors in [90] propose a traffic management method for LTE-LoRaWAN integration. Adopting the integrated architecture proposed in [87], the authors in [91] propose a routing and packet scheduling mechanism for the integrated network. In addition to the efforts in academia, the industry also takes action to facilitate LoRaWAN-5G integration. Kerlink [151] produced commercial LoRaWAN gateways with 4G backhaul, such as the indoor Wirnet iFemtoCell-evolution gateway and the outdoor Wirnet iStation gateway. Actility [143] and Simfony [144] announced in April 2021 that they will cooperate on developing a multi-technology IoT platform that can provide MNOs and mobile virtual network operators an integrated solution for LoRaWAN and cellular IoT networks management.

Cellular and LoRaWAN will co-exist in the form of hybrid networks in the 5G and beyond era. However, equipped with flexible, agile, and powerful core networks, 5G can serve as more than a backhaul network for LoRaWAN. The LoRaWAN-5G integration is expected to evolve from access networks to core networks like cellular LPWANs and fixed-mobile convergence that can communicate with the converged 5G core network efficiently. There are three motivations behind LoRaWAN-5G integration with a converged core network: 1) From the perspective of MNOs, to maximize the returns of infrastructure deployments by going beyond serving as only

backhaul providers in the big market of non-cellular LPWANs. Instead, they will evolve their cellular networks to expand their business [152]. With a converged core network, MNOs will have the capability of taking over the operation of LoRaWAN. 2) From the perspective of customers, the integration of LoRaWAN and 5G with a converged core is cost-effective as it avoids the dual deployment and management of LoRaWAN and 5G. 3) From a technical perspective, a converged core can enhance the capabilities of LoRaWAN, such as security, capacity, and roaming ability.

In this chapter, a LoRaWAN-5G integrated network with a collaborative RAN and a converged core network is implemented utilizing the Glasgow 5G testbed. A LoRaWAN gateway is built using Raspberry Pi and a 5G modem, capable of accessing the 5G new radio network over the air as a 5G UE. This implementation marks the first instance of a LoRaWAN gateway utilizing 5G as its backhaul technology, demonstrating the feasibility of LoRaWAN-5G integration. Additionally, the LoRaWAN servers deployed on an edge server of the Glasgow 5G testbed represent the first set of LoRaWAN servers operating within the core network of a 5G network. Furthermore, the viability of this hybrid network is demonstrated through its application in a smart building heating management system aimed at saving energy.

## 3.2 Motivation behind Converged Core Network

The survey presented in Chapter 2 highlights the predominant focus of existing research on access-level integration to leverage the backbone of 5G networks. This section delves into the motivations underpinning the design of converged core networks.

As shown in Table 2.3, all current research works on LPWAN-5G integration are based on 4G or NSA 5G with EPC serving as the core network. The main reason is that 5G network deployments started in 2018 with the non-standalone mode that employs EPC as the core network [153]. However, till March 2021, 68 operators in 38 countries globally have been investing in public 5G standalone networks with 5G core networks according to Global Mobile Suppliers Association [154]. With the advent of standalone 5G, 5G core networks are becoming available for both research and commercial deployments. Compared with EPC, a 5G core network can support more extensive and powerful functions by virtue of many enabling technologies like

NFV, SDN, and Network Slicing. Since the emergence of 5G core networks, fixed-mobile convergence [155] [156] has evolved gradually from access network level to core network level, which makes it possible to manage different access networks and UE by a converged 5G core network. Similarly, it is expected that more research will be done at the core network level for LPWAN-5G integration. There are three motivations behind core-level integration in the standalone 5G era.

First, enabling technologies such as SDN and NFV can considerably reduce the cost and complexity when new functions (like servers of LPWAN) need to be implemented into the core mainly by reusing the same hardware [157]. Furthermore, Network Slicing enables many networks with different features to be able to coexist in a single core network [158]. For instance, LPWAN is characterized by low data rate and non-time-critical applications, while a standard 5G core network supports URLLC. By using NSF, the 5G core network can be logically sliced into two distinct networks - one is characterized by a low data rate for LPWAN, while the other one is characterized by low latency for URLLC applications. Although logically separated, the two distinct networks still coexist in a converged 5G core network, which is beneficial for optimization of network resource configuration and the adoption of different security schemes.

Second, unified management and overall optimization can be achieved when integrating at the core level. If the integration is considered only at access networks such as Options 1, 2, 3, and 5 in Chapter 2, the cellular network only serves as a backhaul network from the LPWAN perspective and there is no interworking between the 5G core network and the servers of LPWAN, which makes the cellular network transparent. Consequently, it is impossible to manage the 5G network and the LPWAN in a converged core and the overall optimization of the hybrid network is also unlikely to be achieved.

Third, for operators, especially cellular network operators, the core level integration can massively reduce the cost of deployment, operation, management, and maintenance compared with operating two separate networks i.e. 5G core network and LPWAN servers. To expand the scope of their customer base, operators have integrated NB-IoT into their cellular networks [159] [160]. Thus, it can be predicted that more LPWAN networks would be integrated into operators' cellular networks and more integrations would be implemented at the core level in the future. However, the integrated access network is still valuable which could considerably reduce the cost of gateway deployment by utilizing the 5G access network which has

been already deployed. Therefore, rather than relying on a single option listed in Table 2.3, the prime integrated architecture is likely to be a hybrid of two options. For example, option 4 in Chapter 2 can be used to build an LPWAN-5G converged core network, and then option 5 in Chapter 2 can be used to get access to the converged core network for LoRaWAN end devices.

## 3.3 Integration Solution

In this section, the implementation of the LoRaWAN-5G integrated network characterized by a collaborative RAN and a converged core network will be introduced.

As shown in Figure 3.1, a private LoRaWAN is integrated into an NSA 5G network which is composed of gNB, eNB, and EPC+. The LoRaWAN gateway can communicate with gNB as a 5G UE by virtue of a 5G modem. The LoRaWAN servers are deployed on an edge server of EPC+. The hybrid network can support both 5G UE and LoRaWAN end devices at the same time. In terms of standard 5G UEs, the integration has no impact on their usage as there is no modification of the gNB or any entity of EPC+. In terms of LoRaWAN end devices, they can communicate with the LoRaWAN servers through the LoRaWAN gateway, gNB, and EPC+ in sequence. However, for LoRaWAN end devices, they can regard the network as a standard LoRaWAN network. The integration has two parts including the collaborative RAN and the converged core network.

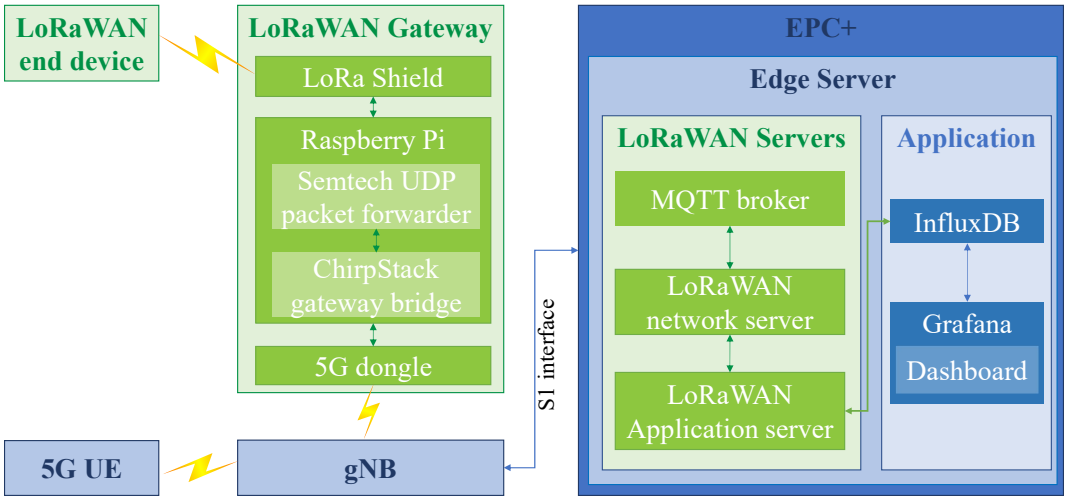



Figure 3.1: System diagram of the LoRaWAN-5G integrated network

At the RAN level, there are a number of potential solutions to the integration of LoRaWAN and cellular networks [4]. However, only two solutions have been implemented so far due to the state of the technology and the availability of commercial products. The first solution, which inserts a universal subscriber identity module card and an LTE UE module to the LoRaWAN gateway, was implemented in [84], [89] and [90]. By doing so, the gateway can access the cellular network to communicate with LoRaWAN servers in the cloud. The second solution incorporates the eNB stack in the LoRaWAN gateway and was implemented in [87] and [91]. By doing so, the gateway can access the EPC directly via the S1 interface. Given that the first solution has advantages over the second solution in terms of flexibility, the cost of deployment, and the complexity of the gateway, the first solution, i.e., building a LoRaWAN gateway with a 5G UE module, is adopted in this Chapter. However, there is a significant difference between the implementation and the related works [84, 87, 89–91], which are all based on the 4G cellular networks. Although the cellular network in [84] is a 5G test network, it uses eNodeB as RAN and EPC as the core network. In this chapter, the cellular network that the LoRaWAN is integrated into is a telco-grade NSA 5G network composed of gNB, eNB, and EPC+. With the ability to communicate with gNB over the air, the gateway can collaborate with gNB and access EPC+. Through the collaborative RAN, both 5G UE and LoRaWAN end devices can access the EPC+ at the same time.

At the core network level, all the LoRaWAN servers, including a Message Queuing Telemetry Transport (MQTT) server, a LoRaWAN network server, and a LoRaWAN application server, are deployed in a Virtual Machine (VM) on the edge server of the EPC+. The data generated in the LoRaWAN end devices goes through the LoRaWAN gateway and gNB to EPC+. The ChirpStack gateway bridge in the LoRaWAN gateway communicates with the MQTT broker in the LoRaWAN servers over a standard IP connection. In the EPC+, the serving gateway receives the LoRaWAN data and routes it to the edge server that resides within the operator's IP network. Within the edge server, the communication among LoRaWAN servers is also over a standard IP connection. In the whole process, the LoRaWAN data does not leave the EPC+, ensuring its security and privacy. Moreover, the converged core network with the integration of EPC+ and LoRaWAN servers can reduce the cost of deployment for those who need a 5G network and LoRaWAN at the same time as they only need to deploy one hybrid network. Furthermore, deploying LoRaWAN servers within EPC+ provides the possibility of interoperation between the 5G core

network and LoRaWAN servers. The interoperation is expected to improve the efficiency, security, mobility, and compatibility of the hybrid network [4].

The details of the implementation of the LoRaWAN gateway and the LoRaWAN servers will be discussed in the next two subsections.

### 3.3.1 LoRaWAN Gateway with 5G UE Module

As shown in Figure 3.2, the hardware of the gateway includes a Raspberry Pi, a LoRa shield, and a 5G dongle. The Raspberry Pi is Pi 4 model B with 4GB RAM powered by a 5.0V 3A adaptor. The LoRa shield is LoRaGO PORT [161] which is designed specifically for multi-channel LoRaWAN gateways. The 5G dongle is assembled at the University of Glasgow and can access the Glasgow 5G testbed. The 5G dongle and the LoRa shield are powered by the Raspberry Pi. The test demonstrates that the 5.0V 3A power adaptor can support the Raspberry Pi, the LoRa shield, and the 5G dongle at the same time. It makes the deployment of the gateway very straightforward, flexible, and cost-effective, as the gateway only needs to be simply placed anywhere under the coverage of the 5G network and provide it with the power supply. Except a cable for the power supply, the gateway does not need any other cables.

In terms of the software, as shown in Figure 3.1, the Semtech user User Datagram Protocol (UDP) packet forwarder [162] and the ChirpStack gateway bridge [163] are deployed in the Raspberry Pi with the Raspberry Pi OS. The Semtech UDP packet forwarder forwards the radio frequency packets received by the LoRa shield to the ChirpStack gateway bridge in the format of UDP packets. The ChirpStack gateway bridge converts the UDP packets to JSON and Protobuf which are the required data formats of ChirpStack LoRaWAN servers. Then, through the 5G dongle, gNB, and EPC+, the bridge transmits the JSON and Protobuf packets to the specified MQTT server which is deployed on the edge server of EPC+. To ensure the successful registration and communication of the ChirpStack gateway bridge with the MQTT server, it is necessary to include the IP address of the VM hosting the LoRaWAN servers in the configuration file of the gateway bridge. The 5G dongle and the LoRa shield have their own firmware and drivers, and there is no need to deploy extra software on them. The logs of the packet forwarder, the bridge, and the 5G dongle are displayed in Figure 3.2. The log of the packet forwarder shows its status. The log of the bridge shows the uplink and downlink communications between the bridge

and the MQTT server. The log of the 5G dongle shows the packet data network session established in the EPC+ for the gateway.


Figure 3.2: The LoRaWAN gateway with 5G dongle

### 3.3.2 LoRaWAN Servers in 5G Edge Server

In the 5G edge server, a VM is created by Proxmox for the LoRaWAN network and its applications. Ubuntu 18.04 is selected as the operating system of the VM. ChirpStack LoRaWAN server solution [164] is chosen for the network. As shown in Figure 3.1, the LoRaWAN servers include an MQTT server, a LoRaWAN network

server, and a LoRaWAN application server. All the three servers are deployed in the VM. The MQTT server forwards the packets received from the ChirpStack gateway bridge to the ChirpStack LoRaWAN network server. The network server plays the vital roles in the authentication of end devices, de-duplication of the LoRaWAN frames received by the LoRaWAN gateway, and processing of the downlink and uplink LoRaWAN MAC-layer message. Moreover, the network server sends the processed messages to the ChirpStack LoRaWAN application server. Figure 3.3 shows the interface of the VM and the dashboard of the application server. The dashboard illustrates that all the end devices and the gateway are active and working well. The "Device data-rate usage" indicates "DR5" which means that the sampling factor is 7 and the bandwidth is 125 kHz according to the LoRaWAN regional parameters [25]. As the LoRa shield has a global positioning system module, the dashboard of the application server also illustrates the location of the gateway, which is at the JWS building at the University of Glasgow.

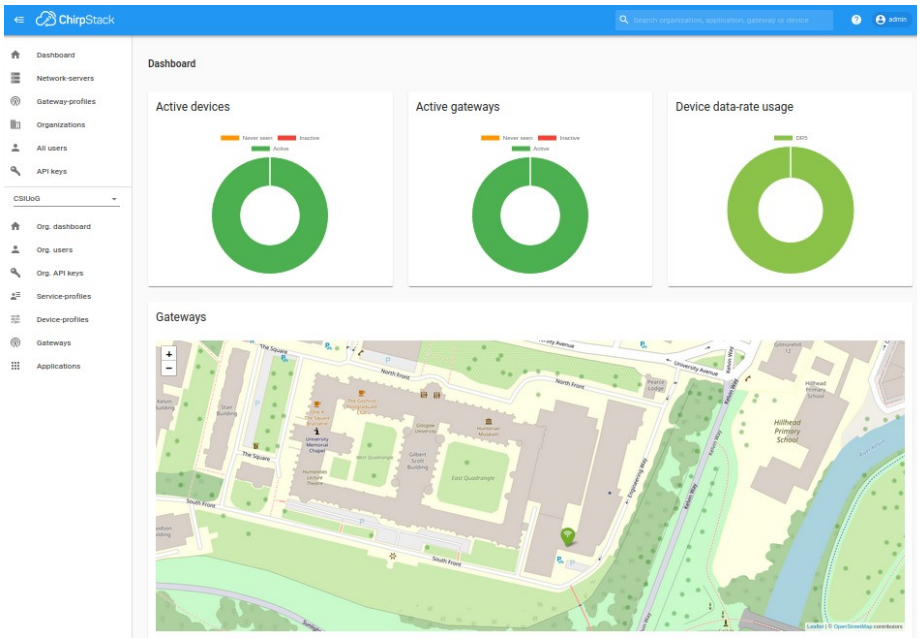



Figure 3.3: The LoRaWAN servers deployed in the 5G edge server

## 3.4 Use Cases

Compared with standard LoRaWAN, the LoRaWAN-5G integrated network has many advantages in terms of flexibility, deployment cost, security, and privacy. With

these advantages, the integrated network is expected to have many use cases, e.g., smart factories, smart transportation, and smart buildings. In this section, the smart heating project developed to digitize and upgrade the heating system of the JWS building at the University of Glasgow is introduced.

The energy shortage and climate change are two severe problems that all human beings are facing. According to the heating report of IEA [165], heating is the world's largest energy end use, accounting for almost half of global final energy consumption in 2021. However, the heating system of the JWS building is traditional and old-fashioned. The management team of the building knows little about the temperature, people activity, or the status of heating (on or off) in each room. Moreover, there is the possibility that the heating radiators keep on for a long time with nobody in the room, resulting in energy wastage. The LoRaWAN-5G network proposed in this chapter can be used to upgrade the heating system and solve the problem at a very low cost. The LoRaWAN-5G gateway is deployed in Room 468 of the JWS building and three sensors with built-in LoRaWAN modules in Room 468 (a), Room 468 (b), and Room 534 of the JWS building. The reason why two sensors are deployed in Room 468 is that the room is too large to be measured precisely by one sensor. The selected sensors are TEKTELIC PIR (passive infrared sensor) smart room sensors that can capture the temperature, humidity, and human activity, etc. Furthermore, the sensors support LoRaWAN specification 1.0.2 and can send data to the LoRaWAN servers deployed in the edge server of 5G via the LoRaWAN gateway and gNB.

As shown in Figure 3.1, in addition to LoRaWAN servers, some applications are also deployed in the VM including InfluxDB and Grafana. InfluxDB is a time series database that can store the data directly from the ChirpStack application server via the application programming interface designed by ChirpStack. Grafana is a dashboard platform that can read data from InfluxDB and do some simple data processing. The Grafana dashboard of the smart heating system is shown in Figure 3.5. In the first row, the current temperature, humidity, and the sensor battery voltage are displayed. The second row illustrates the human activity in each room, which is perceived by the PIR detector integrated into the smart room sensor. The last row illustrates the historical data on temperature and humidity in each room. The time range of the historical data can be adjusted as needed. By the dashboard, the building management team can remotely monitor the temperature and human activity level of each room, and then determine when to switch on or off the radiator.


Figure 3.5: Dashboard of the smart heating system

As shown in Figure 3.4, the speed and latency of the 5G network are measured using LibreSpeed. The download and upload speeds are 950.62 and 28.18 Mbit/s, respectively, and the latency is 17.10 ms, which significantly meets the requirements of LoRaWAN communication of the hybrid network.

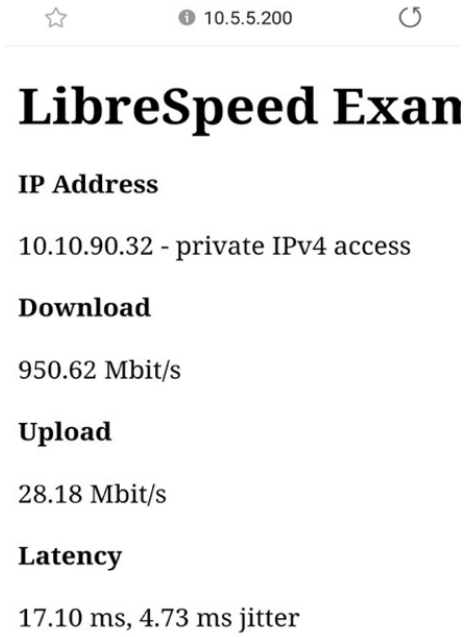



Figure 3.4: The measurements of the network

## 3.5 Summary

In this chapter, a LoRaWAN-5G integrated network has been designed with a collaborative RAN and a converged core network. With the 5G UE module, the LoRaWAN gateway can collaborate with gNB to communicate with the LoRaWAN servers deployed in the edge server of EPC+. The integrated network has been implemented on the Glasgow 5G testbed to upgrade the heating system of the JWS building at the University of Glasgow. The use case demonstrates that the integrated network can work efficiently and stably. Building a 5G modem in the LoRaWAN gateway makes the deployment very straightforward, flexible, and cost-efficient. Deploying the LoRaWAN servers in the core network of 5G enhances the security and privacy of LoRaWAN data. Because of these benefits, the proposed solution of LoRaWAN-5G integration is expected to be widely adopted in the 5G

and beyond era.

However, to cover an extensive area, this solution also needs to densely deploy the LoRaWAN gateways. To address the challenge, the integration of LoRa mesh into 5G will be investigated in the following chapters.

# Chapter 4

# Cloud-Edge-Terminal Collaboration of LoRa Mesh-5G Integrated Network

This chapter proposes a LoRa mesh-5G integrated network by developing a LoRa mesh server that operates within a private cloud of the 5G network and designing a could-edge-terminal collaborative architecture. The work presented in this chapter has been published in [P3].

## 4.1 Introduction

Since the 19th century, the railway has become one of the main transportation methods all over the world. According to the International Union of Railways [166], the total length of railway tracks in the world was more than 855,726 km in 2022. The cost of maintaining such a vast infrastructure is very high, especially if traditional periodic maintenance methods are used, i.e., sending the crew and equipment to walk along railways to check the status of the infrastructure regularly. With the development of IoT and data analysis technologies, predictive maintenance has become a promising method to reduce costs. Due to the long length of railway tracks, a massive number of sensors deployed alongside railway tracks is needed to monitor the status of the infrastructure and transmit it to the cloud for making policies. The crew and equipment are sent out to specific locations only when maintenance status is triggered by the system. On the other hand, bad weather

causes damage to the infrastructure and poses a threat to the safety of passengers and staff [167]. Specifically, a high temperature poses the risk of buckling to rails and a low temperature freezes rails. High wind can blow objects onto rails blocking the railway, while heavy rain makes rails slippery and continuous rain would result in landslides or flooding. To reduce the damage and threat, railway operators need to monitor the trackside weather and predict the weather in the future. With the information, they can take action before adverse weather happens, such as reducing the speed limit, rescheduling routes, and sending special fleets to maintain the rails. However, the general weather forecast from organizations like the MET Office in the UK cannot offer precise weather measurements and forecasts for railways in rural areas since they lack weather stations along the railways, relying mainly on satellite images for their measurements and predictions. Thus, railway operators need a dedicated system to monitor and predict trackside weather. Both predictive maintenance and weather monitoring need a mMTC network to gather data from sensors throughout the whole railway network. The main requirements of the network are as follows.

1. Wide coverage: The communication network should cover the whole railway network which is characterized by several long linear tracks.

2. Supporting massive end devices: Given the long length of railway tracks, a massive number of sensors and end devices need to be deployed to monitor the whole railway network.

3. Low-cost communication infrastructure: High investment in the infrastructure is hard to be paid back as many railways are located at remote sites without other connectivity requirements.

4. Low-power and low-cost end devices: Given the massive number of end devices, their power consumption and cost have a great impact on the overall cost.

Unfortunately, current trackside networks do not satisfy the requirements. As a traditional mobile communication system of railways, the Global System for Mobile Communication-Railway (GSM-R) is widely used globally, especially in Europe [168]. Based on the second-generation cellular network, GSM-R is already outdated and suffers from many issues such as high interference, low capacity, and limited capability. Hence, GSM-R cannot support massive end devices for predictive

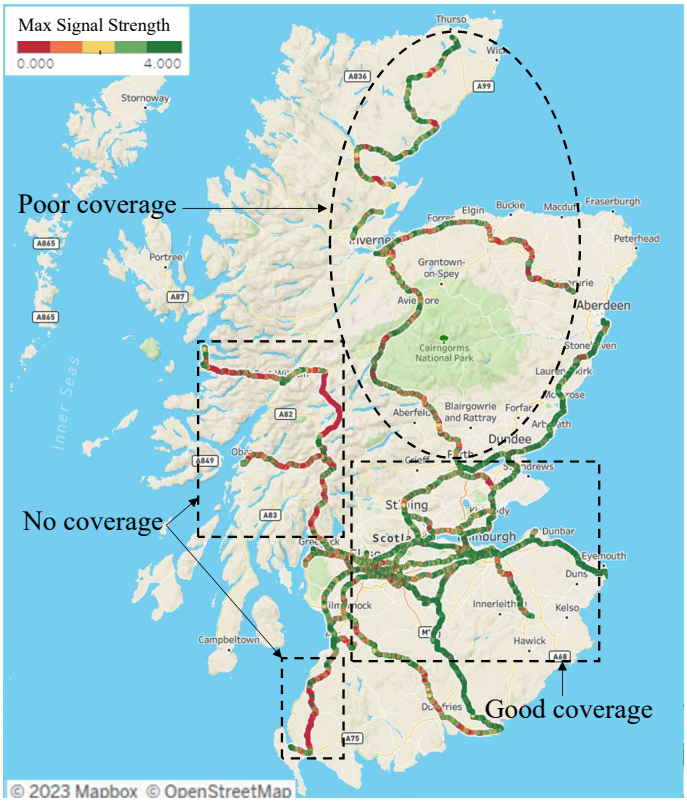



Figure 4.1: 4G signal strength of Scotland railways (based on [170]).

maintenance or weather monitoring. With the sunset of the second and third-generation cellular networks, GSM-R is being replaced by LTE for railways which is based on the 4G cellular network. Although operators have started deploying 4G since 2009, they do not cover the whole railway network due to the low rate of return in remote and rural areas. Taking Scotland as an example, Ofcom, the regulator for communication services in the United Kingdom, measured the 4G signal strength in the railways of Scotland [169]. As shown in Figure 4.1, the railways near main cities have good signal strength, whereas coverage in rural areas is poor, especially the lines in the highland and west coast which are remote sites with low population density. Thus, the current 4G does not provide the coverage required by railway networks. With wide deployment in recent years, the 5G cellular network is expected to facilitate railway digitalization. However, 5G faces the same challenges as 4G, and might even require a denser deployment based on their operating frequency bands. Therefore, the biggest issue of 4G and 5G for widespread railways is that they cannot provide wide coverage at a low cost.

Regarded as one of the most popular low-power wide-area technologies, LoRaWAN, based on LoRa, is an important supplement to cellular networks in rural areas [4,84,87,171]. With a star topology, the messages from LoRaWAN end devices aggregate at the LoRaWAN gateway which forwards them to the LoRaWAN server on the cloud by backhaul networks. Although LoRaWAN has wide coverage, it is not suitable for linear rail lines as many LoRaWAN gateways have to be deployed alongside the lines at a certain distance. Each gateway requires access to a backhaul connection, which significantly increases the deployment cost. Instead of using one-hop communication, LoRa mesh can extend the coverage of LoRaWAN with no need to densely deploy gateways. It allows trackside end devices to relay messages from other end devices until they arrive at a gateway that is deployed at locations with access to a backhaul network. Thus, LoRa mesh is a potential network providing wide coverage for railways.

Motivated by the trackside sensing requirements, the coverage status of existing trackside networks, and the wide coverage of LoRa mesh, in this chapter, a LoRa mesh-based network is proposed to monitor trackside weather. LoRa mesh is a self-organized network lacking a centralized server for management, e.g., node registration. To overcome this challenge, the integration of LoRa mesh into a 5G network is proposed, which provides the LoRa mesh with a private cloud for network management and intelligent data processing. Moreover, 5G networks can provide a reliable and flexible backhaul for LoRa mesh and reduce the deployment cost by utilizing existing cellular infrastructure. On the other hand, collaborating with the terminal and cloud, edge computing is integrated to reduce the volume of data transmitted in the network. The proposed network is suitable for trackside low data rate sensing applications including both predictive maintenance and weather monitoring. Moreover, due to its low cost and extensive coverage, the proposed network can be utilized in various scenarios, including infrastructure monitoring in remote areas, environmental monitoring in agricultural settings, and the development of IoT-based smart cities. In this chapter, it is implemented as a proof of concept for weather monitoring.

The rest of this chapter is structured as follows. In Section 4.2, the network model and integration methods of the LoRa mesh-5G integrated network are presented. Section 4.3 proposes the cloud-edge-terminal collaborative architecture, along with three algorithms concerning timely significant-change updates, packet loss detection, and adaptive thresholds. Section 4.4 and Section 4.5 present the implementation and

experimental results, respectively. Finally, Section 4.6 concludes the chapter.

## 4.2 LoRa Mesh-5G Integrated Network

In this section, a system model and an integration approach of the LoRa mesh-5G integrated network for trackside smart monitoring will be introduced.

### 4.2.1 System Model

As shown in Figure 4.2, a LoRa mesh network is deployed alongside a railway track to monitor the weather. It consists of two kinds of nodes, i.e., gateway and sensor nodes denoted as $s_i$ where $i$ is an integer. The gateway is deployed in the middle of the railway line, receiving packets from sensors deployed on either side of the railway line. The coverage area of the gateway is equivalent to that of a single-hop LoRa network, depicted as a light green ellipse in Figure 4.2. It is assumed that there are $N$ sensor nodes at both sides of the gateway, where $N$ are integers. To simplify the notation in the following analysis, the gateway is denoted as $s_{N+1}$ even though it does not have sensors. Some nodes, such as $s_1, s_2, s_N, s_{N+2}, s_{2N-1}$ and $s_{2N+1}$, are equipped with weather stations. They can read the weather station data and send it to the gateway in the form of LoRa mesh packets. Besides, they also relay packets from other nodes. Other nodes do not have weather stations, such as $s_3$ and $s_{2N}$, and only relay packets. They are used to extend the coverage of the LoRa mesh network when network operators do not want to densely deploy weather stations. The relaying of sensor nodes significantly extends the coverage of the LoRa mesh network, as depicted by the light blue ellipse in Figure 4.2. All the packets containing weather data are transmitted to the gateway via one-hop or multi-hop LoRa communication. Depending on the distances between nodes, one sensor node can have one or multiple routes to the gateway. When joining the network or finding that the existing route is no longer valid by not receiving the expected acknowledgment message after sending data message, a sensor node tries to discover a valid route to the gateway automatically, achieving self-organization and self-healing [49, 172]. Moreover, to achieve remote and smart control, downlink communication is enabled, allowing the gateway to send commands like resetting to sensor nodes.

After aggregating at the gateway, all the trackside data needs to be transmitted to

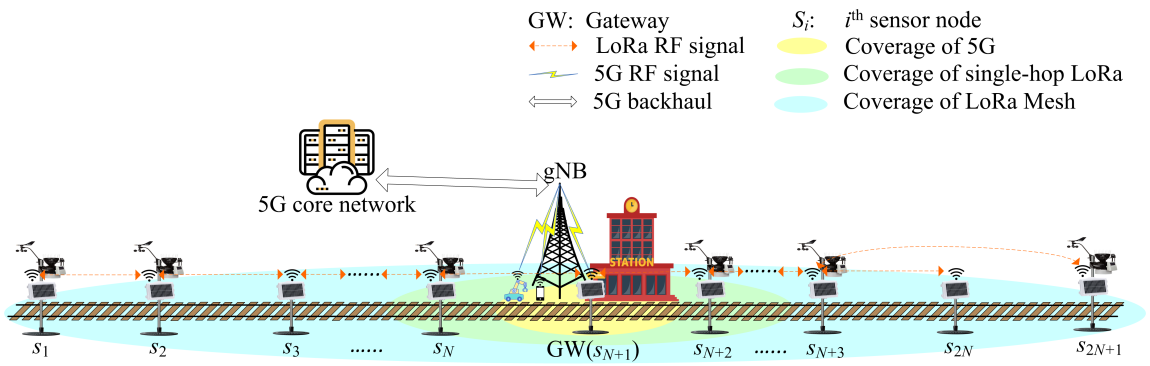



Figure 4.2: System model of the LoRa mesh-5G integrated network.

the cloud through a backhaul connection. To leverage existing cellular infrastructure, the gateway is deployed in areas with 5G coverage, e.g., a train station. As shown in Figure 4.2, a 5G base station (gNB) is deployed near a train station providing connections for various users, such as automated guided vehicles, smartphones, and the LoRa mesh network. Compared with LoRa and LoRa mesh, the 5G network offers relatively shorter coverage, illustrated by the yellow ellipse in Figure 4.2. In the 5G network, the gateway acts as an UE that can communicate with the gNB directly. Then, through the 5G backhaul, the weather data can securely arrive at the 5G core network in the cloud. It is clear from Figure 4.2 that the LoRa mesh-5G integrated network has a significantly extended coverage compared with 5G networks and single hop LoRa-5G integrated networks.

### 4.2.2 Integration Approach

Although LoRa mesh networks benefit from flexible deployment and coverage extension, they lack a centralized server, resulting in difficulties in management. Leveraging the existing 5G network, a LoRa mesh server is proposed to be deployed within the 5G core network to provide efficient management. To allow the LoRa mesh nodes to access the 5G network, a 5G dongle is integrated into the LoRa gateway.

The functions of the LoRa mesh server are 1) sensor node registration, 2) network parameter management, e.g., the update frequency of sensor nodes, 3) data storage, 4) cloud data processing for application, and 5) providing a user interface. As shown in Figure 4.3, the LoRa mesh server is deployed in one of the virtual machines within the 5G network cloud. Based on the 5G-Multi-access Edge Computing (MEC)

integration method proposed by ETSI [173], the cloud is deployed within the 5G core network as an MEC server and connects to the UPF via N6 interface in the user plane. Although it is a MEC server, it serves as a cloud for the LoRa mesh network. Based on Hypertext Transfer Protocol Secure (HTTPS), transmission control protocol, and IP, the user interface bridges the LoRa mesh server and external networks. Through the user interface, the network status and the processed application data are displayed to users in a dashboard. Moreover, the interface allows authorized users to change the parameters of the network and reset specific sensor nodes or the gateway. To enable the gateway to access the LoRa mesh server within the 5G core network, the protocol stack of 5G UE is installed in the gateway. As shown in Figure 4.3, the gateway has both the LoRa mesh protocol stack and the 5G UE protocol stack. When receiving LoRa mesh packets from sensor nodes, the gateway decapsulates them like a usual LoRa mesh node. Then, acting as a 5G UE, the gateway encapsulates the data as 5G packets and transmits them to gNB over the air via NR-Uu interface. Through the gNB and UPF, the packets arrive at the LoRa mesh server securely as the transmission is protected by 5G security mechanisms.

In terms of the application layer protocol for the session between the gateway and the LoRa mesh server, the choice is MQTT [174], which is a lightweight open messaging transport protocol. Based on a publish-subscribe model, an MQTT broker listens to MQTT publishers and retransmits the received messages to specific MQTT subscribers. The messages are published on topics. In the LoRa mesh-5G integrated network, an MQTT broker is deployed in the LoRa mesh server to retransmit messages with two topics including uplink data and downlink commands. Regarding uplink data, an MQTT publisher and an MQTT subscriber are deployed in the gateway and the LoRa mesh server, respectively. Regarding downlink commands, an MQTT publisher and an MQTT subscriber are deployed in the LoRa mesh server and the gateway, respectively. By doing so, bidirectional communication between the gateway and the LoRa mesh server is achieved. Designed for restricted environments such as machine-to-machine communication and IoT, MQTT has many advantages including a small footprint, limited network bandwidth, fast message delivery, and easy deployment. In the LoRa mesh-5G integrated network, compared with Hypertext Transfer Protocol (HTTP) [175], MQTT can reduce the consumption of the gateway resource, especially the required 5G radio frequency bandwidth. However, security is the main drawback of MQTT [176]. Without built-in encryption, MQTT usually uses Transport Layer Security (TLS)/Secure Sockets

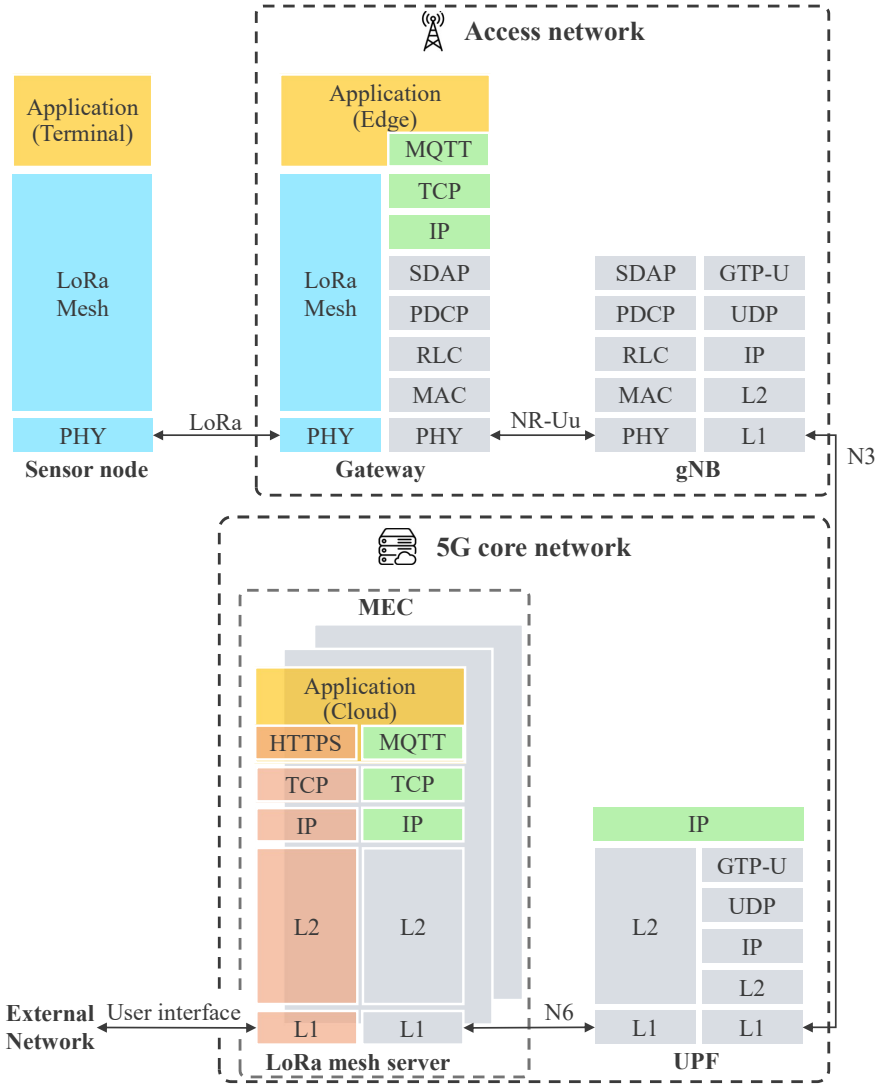



Figure 4.3: Protocol stacks of LoRa mesh-5G integrated network.

Layer (SSL) for security encryption, deviating from its design aim as TLS/SSL is not a lightweight protocol. By virtue of the 5G security mechanisms, there is no need to use TLS/SSL as MQTT data is encapsulated as a 5G payload protected by 5G authentication and encryption. Thus, the drawback of MQTT on security is overcome in the LoRa mesh-5G integrated network.

According to the above description, the integration of LoRa mesh and 5G is achieved at both the core network level and access network level. The core-level integration helps manage the LoRa mesh network and provides a user interface for observation and control. The access-level integration keeps the deployment flexibility

of the LoRa mesh network. Collecting data from a mesh network requires one or more nodes to have a backhaul connection to upload the data to the cloud. The backhaul connection is usually via wire-based networks like Ethernet or short-range wireless networks like WiFi, posing restrictions on the deployment location of one or more nodes. With the capability of communicating with gNB, the gateway is required to be deployed within the coverage of gNB which is a relatively large area and has no impact on the deployment flexibility of LoRa mesh networks. Thus, the LoRa mesh-5G integrated network benefits from both the management capability of the 5G network and the coverage extension of LoRa mesh networks with no impact on the deployment flexibility.

## 4.3 Cloud-Edge-Terminal Collaboration

In addition to enhancing communication capability, the integration of LoRa mesh and 5G also provides a three-level computing architecture, i.e., terminal computing at sensor nodes, edge computing at the gateway, and cloud computing at the 5G core network. Through cloud-edge-terminal collaboration, the packet rate and data volume of the integrated network can be reduced significantly, which is beneficial to enhancing the scalability of the LoRa mesh network, reducing the required 5G radio frequency bandwidth, and easing the backhaul workload.

### 4.3.1 Cloud-Edge-Terminal Collaboration Architecture

As shown in Figure 4.4, terminal devices, i.e., sensor nodes, measure air temperature and wind speed, and the observations are sent to the edge, i.e., the gateway, periodically. Despite operating in license-free bands, LoRa suffers from duty cycle limitation which results in lower packet rates to connect more end devices [177]. So, it is necessary to reduce the frequency of periodic updates to support more sensor nodes. However, a low update frequency increases the delay between a significant change in an observation happening and the railway track manager knowing it. The delay further increases the response time to adverse weather or extreme weather. To address the issue, besides sending periodic updates at a low frequency, terminal devices send significant-change updates to the gateway edge immediately when detecting a significant change between the current observation and the last update. The detection is easy to achieve so that the complexity and resource consumption of

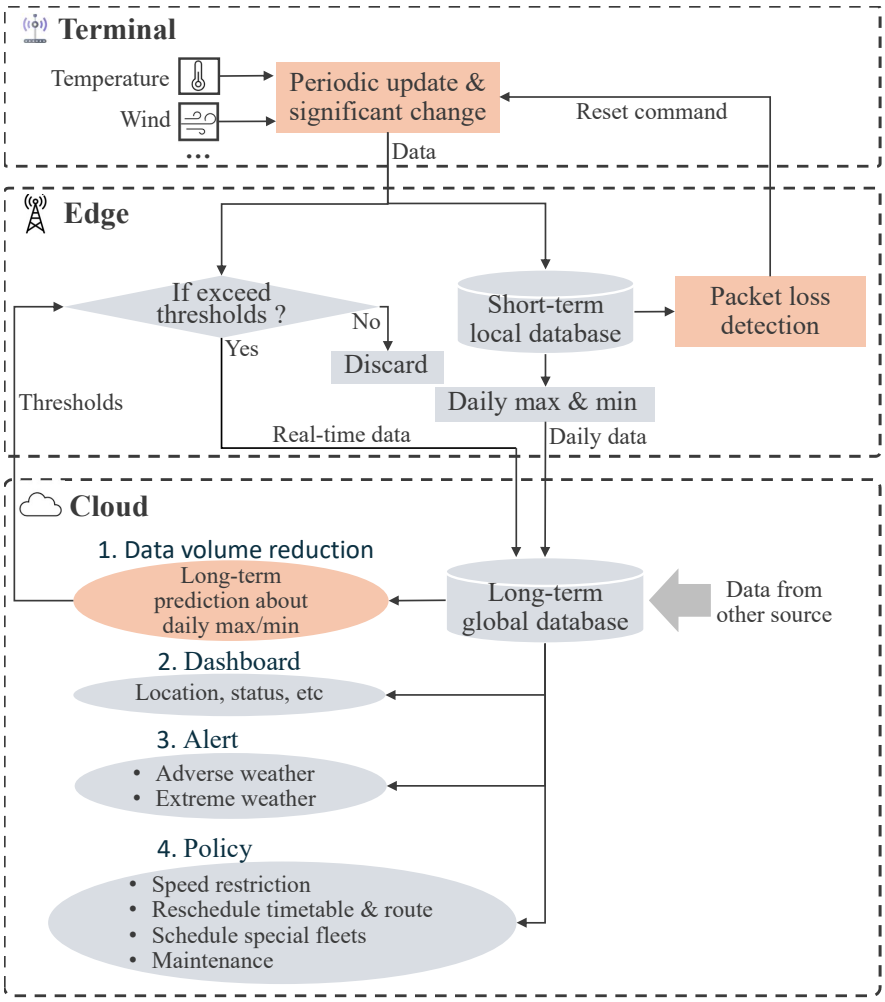



Figure 4.4: Data flow chart of cloud-edge-terminal collaboration.

terminal devices is not increased. As shown in Figure 4.4, after receiving data from terminal devices, the gateway edge stores it on a local database. Given the storage capability of the gateway edge device, the retention time of the data is limited.

Operating in license-free bands, LoRa suffers from packet loss due to reasons such as signal collision [178]. With more hops and dynamic routes, LoRa mesh is more likely to lose packets. If packet loss continues for a specific sensor node, there is a high probability that the sensor node has malfunctioned or its route to the gateway has issues, e.g., some intermediate nodes are too busy to relay packets for it. Routing-related issues can be solved by remote resetting the sensor node as this will initiate route discovery again. If there are multiple potential routes to the gateway, the new route is very likely to be different from the old one as the

busy intermediate nodes are also too busy to process the route discovery request from it. The issues with the sensor node can be classified into two categories. The first category is those that can be solved remotely, e.g., the periodical updates of two sensor nodes collide with each other as they transmit periodical updates at the same time due to the same period and start time. Remote resetting can solve the issue by changing the start time of the sensor node. It is also expected to solve many other issues of the first category. The second category is those that cannot be solved remotely such as hardware issues. Although they cannot be solved remotely, a remote resetting command is also helpful to verify this kind of issue as the sensor node cannot transmit an acknowledgment back to the gateway for the remote resetting command in this situation. Thus, it is necessary to design a packet loss detection algorithm to trigger remote reset commands to heal the network or verify the issues that cannot be solved remotely. In this chapter, as shown in Figure 4.4, a method of packet loss detection is designed for the gateway edge. It reads data from the local database and automatically sends a reset command to the specific sensor node when detecting continuous packet loss. On receiving a reset command, the sensor node resets itself, discovers a route to the gateway again, and sends an acknowledgment to the gateway. The reason why packet loss detection is deployed at the gateway edge instead of the cloud is that it is based on the most recently received data that is not necessarily fully sent to the cloud. To reduce the backhaul 5G network requirement, the edge filters data before sending it to the cloud. The filtering policy is based on thresholds calculated in the cloud. Besides filtering the real-time data, the edge also calculates the maximum air temperature, minimum air temperature, and maximum wind speed of a day, which are sent to the cloud on a daily basis for calculating the thresholds of the filtering.

The computation tasks of the cloud are application-oriented. In the case of trackside weather monitoring, track and/or train operators are concerned about bad weather that is likely to pose a danger to passengers, trains, or infrastructures. Network Rail [167], the biggest track manager in the United Kingdom, discloses their definitions of adverse weather and extreme weather in winter, i.e., temperature below -3 °C or wind speed above 60 miles per hour (mph) as adverse weather, and temperature below -7 °C or wind speed above 70 mph as extreme weather. In summer, high temperature also has an adverse impact on the track or train. In adverse weather or extreme weather, the operator must take action promptly such as imposing a speed restriction for trains, rescheduling timetables and/or routes, and

scheduling special fleets like snowploughs. Thus, historical daily maximum and/or minimum weather values are used to predict the maximum and/or minimum weather values of the next day as the thresholds of real-time data filtering. As shown in Figure 4.4, the thresholds are sent to the edge. If weather values are within the thresholds, they are discarded in the edge. Otherwise, they are sent to the cloud immediately. There are two advantages of the adaptive thresholds. First, the operator can master the trend of the weather with reduced data volume from the edge to the cloud. Second, if weather values are outside of the predictions, the operator is informed of the unexpected values immediately which are likely to change to adverse or extreme weather. So, the operator can get an early warning of adverse weather and extreme weather. By employing the adaptive thresholds, the operator obtains the data with lower delays. In the meantime, the data volume from the edge to the cloud is significantly reduced.

As shown in Figure 4.4, besides data volume reduction, the cloud runs a dashboard that shows the location of LoRa mesh nodes, the status of the LoRa mesh network, and the weather status and values. Moreover, the cloud sends alerts to corresponding staff when adverse or extreme weather is likely to happen. Combined with data from other sources such as atmosphere, passenger, train, and route information, weather data can also be used to make intelligent policies such as speed restrictions, timetables, routes, scheduling special fleets, and maintenance.

### 4.3.2 Periodic and Significant-Change Updates

Sensor nodes send periodic updates with the period $m$. In addition, they send significant-change updates when the change from the last update is bigger than $c^{\mathrm{t}}$ for air temperature or $c^{\mathrm{w}}$ for wind speed. The parameters $t_{\mathrm{u}}^{\mathrm{t}}$ and $t_{\mathrm{u}}^{\mathrm{w}}$ denote the time of the last update for air temperature and wind speed, respectively. Let $T(t)$ and $W(t)$ denote temperature and wind speed at the time $t$, respectively. Assume that sensor nodes check observations at intervals of $\Delta t$, where $m/\Delta t \in \mathbb{N}$. Then, the time of sending periodic and significant-change updates can be described by Algorithm 1.

### 4.3.3 Packet Loss Detection

As mentioned earlier, there are two kinds of packets from the terminal to the edge, i.e., periodical updates and significant-change updates. Since packet loss is easy to

**Algorithm 1** Periodic and significant-change updates

**Input:** $c^{\mathrm{t}}$, $c^{\mathrm{w}}$, $m$
**Initialization:** Time $t = 0$, $t_{\mathrm{u}}^{\mathrm{t}} = 0$, $t_{\mathrm{u}}^{\mathrm{w}} = 0$
**Repeat:**
  IF $t/m \in \mathbb{N}$ THEN
    send $T(t)$ and $W(t)$ in one packet
    $t_{\mathrm{u}}^{\mathrm{t}} = t$, $t_{\mathrm{u}}^{\mathrm{w}} = t$
  ELSE IF $|T(t) - T(t_{\mathrm{u}}^{\mathrm{t}})| \geq c^{\mathrm{t}}$ THEN
    send $T(t)$
    $t_{\mathrm{u}}^{\mathrm{t}} = t$
  ELSE IF $|W(t) - W(t_{\mathrm{u}}^{\mathrm{w}})| \geq c^{\mathrm{w}}$ THEN
    send $W(t)$
    $t_{\mathrm{u}}^{\mathrm{w}} = t$
  END IF
  $t = t + \Delta t$

detect for periodic updates, this chapter only focuses on the detection for significant-change updates. Given that the characteristics of air temperature and wind speed are different, different methods are used to detect packet loss for them.

Trackside air temperature varies continuously and is unlikely to fluctuate greatly within a short duration. Given that the period of the periodical updates is relatively short, it is assumed that air temperature varies monotonically within a period. So, when $\Delta t$ approaches 0, i.e., the checking for significant changes is continuous, the estimated number of generated significant-change updates between time $im$ and time $(i+1)m$ where $i \in \mathbb{N}$ is

$$\hat{n}_i^{\mathrm{g}} = \begin{cases} 0, & \text{for } T(im) = T((i+1)m) \\ \left\lceil \frac{|T((i+1)m) - T(im)|}{c^{\mathrm{t}}} \right\rceil - 1, & \text{for } T(im) \neq T((i+1)m) \end{cases} \tag{4.1}$$

where $\lceil \cdot \rceil$ is the ceiling function. Packet loss of significant-change updates on air temperature between time $ip$ and time $(i+1)m$ happens when

$$n_i^{\mathrm{r}} < \hat{n}_i^{\mathrm{g}}, \tag{4.2}$$

where $n_i^{\mathrm{r}}$ is the number of received significant-change updates between time $im$ and time $(i+1)m$. As deterministic formulas, (4.1) and (4.2) can be used to detect packet loss for air temperature easily.

Unlike air temperature, wind speed fluctuates greatly. Moreover, even within

a short time, it is likely to change so dramatically that it is regarded as a discrete variable. Thus, it is difficult to derive a deterministic formula for packet loss detection on wind speed. Since packet loss is an abnormal behavior, data-driven anomaly detection methods are suitable for the detection. The received data on wind speed between time 0 and time $(n+1)m$ where $n \in \mathbb{N}$ can be denoted as

$$\begin{aligned} W_n = \{&w_0(0), w_1(0), ..., w_{c_0}(0), \\ &w_0(m), w_1(m), ..., w_{c_1}(m), \\ &..., \\ &w_0(nm), w_1(nm), ..., w_{c_n}(nm)\}, \end{aligned} \tag{4.3}$$

where $w_0(im)$ with $i \in [0, n] \cap \mathbb{N}$ is the value of the periodic update at time $im$, $w_j(im)$ with $j \in [1, c_i] \cap \mathbb{N}$ is the value of one significant-change update between time $im$ and time $(i+1)m$, and $c_i \in \mathbb{N}$ is the number of significant-change updates between time $im$ and time $(i+1)m$. Packet loss happens when the number of generated packets is not equal to the number of received packets. Since the number of generated packets is related to the changes in the readings, five features are selected, denoted by a feature vector

$$F_i = [c_i, STD_i, \max_{j \in [0,c_i]} w_j(im), \min_{j \in [0,c_i]} w_j(im), w_0(im)]^{\mathrm{T}}, \tag{4.4}$$

where $STD_i$ is the standard deviation of $\{w_0(im), w_1(im), ..., w_{c_i}(im)\}$. By slicing the received data by windows with the length of $\alpha m$ where $\alpha \in \mathbb{Z}^+$, the data set can be structured as

$$W'_n = [(I'_1, o_1), (I'_2, o_2), ..., (I'_{n-\alpha+1}, o_{n-\alpha+1})], \tag{4.5}$$

where $I'_i = [F_i^{\mathrm{T}}, F_{i+1}^{\mathrm{T}}, ..., F_{i+\alpha-1}^{\mathrm{T}}]^{\mathrm{T}}$, and the binary variable $o_i$ is the output of the $i^{th}$ window. The parameter $o_i = 1$ when there is packet loss during the time window, and 0 otherwise. Finally, Support Vector Machines (SVM) [179], a typical anomaly detection method, is used to process the data set for packet loss detection.

### 4.3.4 Long-Term Prediction for Adaptive Thresholds

Predicting the daily maximum temperature, daily minimum temperature, and daily maximum wind speed based on historical data is a typical time-series prediction problem. [180–182]. There are many popular methods, such as Artificial Neural Networks, Exponential Smoothing, Lasso, and Autoregressive Integrated Moving Average (ARIMA) [183]. Given that the collected data is limited, Artificial Neural Networks are not suitable here as they typically require a large volume of data for effective training. Exponential Smoothing, Lasso, and ARIMA have been tested, and the results indicate that ARIMA performs the best. Processing the three kinds of values separately, ARIMA is used to predict the maximum air temperature, minimum air temperature, and maximum wind speed of the next day based on historical daily maximum air temperature, minimum air temperature, and maximum wind speed respectively.

Let $p^{\mathrm{t}}_{\mathrm{min}}$, $p^{\mathrm{t}}_{\mathrm{max}}$, and $p^{\mathrm{w}}_{\mathrm{max}}$ denote the predicted minimum air temperature, maximum air temperature, and maximum wind speed of the next day, respectively. The thresholds of minimum air temperature, maximum air temperature, and maximum wind speed are calculated respectively as

$$H^t_{\mathrm{min}} = \max(p^{\mathrm{t}}_{\mathrm{min}}, c^t_{\mathrm{min}} + v^t_{\mathrm{min}}), \tag{4.6a}$$

$$H^t_{\mathrm{max}} = \min(p^{\mathrm{t}}_{\mathrm{max}}, c^t_{\mathrm{max}} - v^t_{\mathrm{max}}), \tag{4.6b}$$

$$H^{\mathrm{w}}_{\mathrm{max}} = \min(p^{\mathrm{w}}_{\mathrm{max}}, c^{\mathrm{w}}_{\mathrm{max}} - v^{\mathrm{w}}_{\mathrm{max}}), \tag{4.6c}$$

where $c^{\mathrm{t}}_{\mathrm{min}}$, $c^{\mathrm{t}}_{\mathrm{max}}$, and $c^{\mathrm{w}}_{\mathrm{max}}$ are the criteria of adverse weather about low air temperature, high air temperature, and high wind speed, respectively, and $v^{\mathrm{t}}_{\mathrm{min}}$, $v^{\mathrm{t}}_{\mathrm{max}}$, and $v^{\mathrm{w}}_{\mathrm{max}}$ are the fixed values determined by the operator for early warning of adverse weather. $H^{\mathrm{t}}_{\mathrm{min}}$, $H^{\mathrm{t}}_{\mathrm{max}}$, and $H^{\mathrm{w}}_{\mathrm{max}}$ are sent back to the edge and only data outside of the thresholds is sent to the cloud.

## 4.4 Implementation

Given the safety and efficiency implications in railway operations as highlighted in Section 4.1, a proof of concept has been implemented on the University of Glasgow campus for validation purposes. In this proof of concept, a LoRa mesh-5G integrated network is deployed utilizing the Glasgow 5G testbed. As shown in Figure 4.5(a),

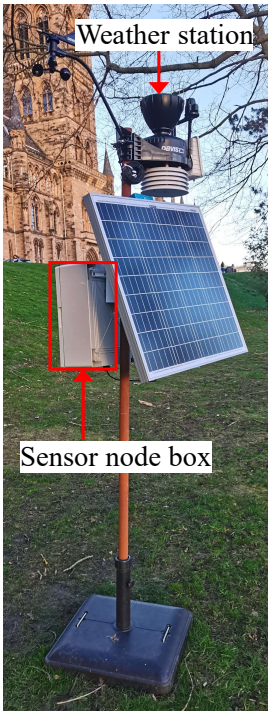
a gateway is deployed within the coverage of the 5G testbed and it connects to the network using its 5G module. In addition, three sensor nodes i.e., $s_1$, $s_2$, and $s_3$ are deployed such that sensors $s_2$ and $s_3$ can communicate with the gateway directly. However, due to blockage by the main building of the University of Glasgow, $s_1$ can communicate with neither gateway nor $s_3$ directly. Instead, the packets of $s_1$ must be relayed by $s_2$ to arrive at the gateway. Thus, the topology of the LoRa mesh network is illustrated by blue dash lines in Figure 4.5(a).

$s_1$ and $s_3$ are sensor nodes connected to a weather station. As shown in Figure 4.5(b), they consist of a weather station produced by Davis Instruments[2] and a sensor node box that has a weather envoy, a Raspberry Pi, and an Arduino board inside. The weather envoy reads real-time data from the weather station using WiFi and transmits it to the Raspberry Pi using a data logger. The Raspberry Pi is connected to the Arduino board using a universal serial bus cable. Data processing is realized using the Raspberry Pi. When periodic updates or significant-change updates need to be sent to the gateway, the Raspberry Pi transmits the update to the Arduino board where a LoRa mesh client runs. Given the requirement of low power consumption and low costs, the LoRa mesh clients in the network are based on the RadioHead packet radio library [50]. On receiving data from Raspberry Pi, the LoRa mesh client encapsulates the data as a LoRa mesh packet and sends it over the air to the LoRa mesh client of the gateway directly or through other sensor nodes. Unlike $s_1$ and $s_3$, as shown in Figure 4.5(c), $s_2$ consists of only an Arduino board and a power system. Without weather stations, $s_2$ only relays LoRa mesh packets.

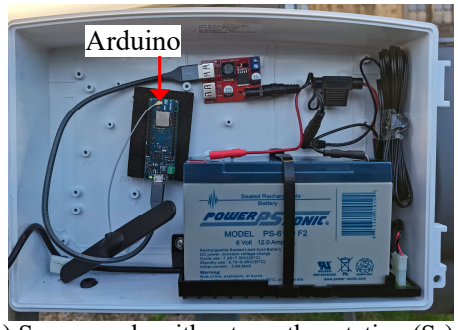
As shown in Figure 4.5(d), the gateway consists of an Arduino board, a Raspberry Pi, and a 5G dongle. Running on the Arduino board, the LoRa mesh client of the gateway receives LoRa mesh packets, decapsulates them, and forwards them to the Raspberry Pi. All the data processing tasks of the edge shown in Figure 4.4 are realized in the Raspberry Pi. Moreover, an MQTT subscriber and an MQTT publisher are implemented in the Raspberry Pi using Node-RED[3] which is a programming tool providing a wide range of nodes with various functions. The 5G dongle is assembled at the University of Glasgow and can access the Glasgow 5G testbed. By the 5G dongle, the LoRa mesh gateway can communicate with the LoRa mesh server deployed in the 5G core network.

[2]https://www.davisinstruments.com/
[3]https://nodered.org/

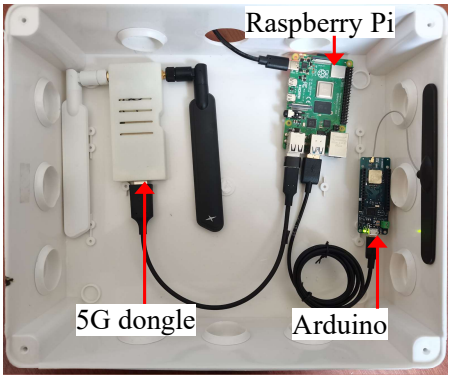

(a) Deployment locations (based on Google Map)




(b) Sensor node with weather station ($S_1$ & $S_3$)




(c) Sensor node without weather station ($S_2$)




(d) Gateway (GW)

Figure 4.5: Implementation at the campus of the University of Glasgow. $s_1$ and $s_3$ are sensor nodes with weather stations shown in (b). $s_2$ is a sensor node without a weather station shown in (c). GW is a gateway shown in (d).

Glasgow 5G testbed is equipped with an on-premises private cloud. A VM instance is created on the cloud to implement the LoRa mesh server. In the implementation, only the functions of data volume reduction and dashboard are realized as the functions of alert and policy are out of the scope of this thesis. For bidirectional communication with the gateway, an MQTT broker, an MQTT subscriber, and an MQTT publisher are implemented on the server also using Node-RED. Moreover, Node-RED is used to process the received data and store it in

Table 4.1: Experiment setting

| Parameters | Value |
|---|---|
| Bandwidth | 125 kHz |
| Coding Rate | 4/5 |
| Spreading Factor | 11 |
| Preamble Length | 8 |
| Frequency band | 868 MHz |
| Transmission Power | 20 dBm |

the long-term global database which is realized by InfluxDB[4]. For data volume reduction, Python is used to read data from InfluxDB, make predictions, and store the results. i.e., thresholds, in InfluxDB again. Node-RED monitors InfluxDB for the thresholds and sends them to the gateway. Grafana[5] is used to directly read from InfluxDB, process data, and display data on a dashboard. Grafana provides an HTTP-based user interface by which users can access the dashboard from external networks easily. Besides, another user interface is implemented for changing the parameters of the network such as the update frequency of LoRa mesh sensor nodes. By deploying HTTP end-points on the Node-RED, the LoRa mesh server provides HTTP-based web services that users can call from external networks to change parameters. With the two user interfaces, authorized users can monitor the network and change parameters easily.

## 4.5 Experimental Results

In this section, the experimental results of periodic and significant-change updates, packet loss detection, and adaptive thresholds will be presented. The experiment setting is listed in Table 4.1.

### 4.5.1 Periodic and Significant-Change Updates

To investigate the benefits of timely significant-change updates, data in a sensor node from May 01, 2023, to May 17, 2023, is recorded, with $\Delta t = 1$ second. By doing so, the results of different $m$, $c_{\mathrm{t}}$, and $c_{\mathrm{w}}$ can be calculated from one data set.

[4]https://www.influxdata.com/
[5]https://grafana.com/

To quantify the delay between a significant change in an observation happening and the track manager knowing it, the average delay between time 0 and time $(n+1)m$ where $n \in \mathbb{N}$ is defined as

$$\hat{d} = 1440 \cdot \frac{\sum_{i=0}^{n} e_i}{(n+1)m}, \tag{4.7}$$

where the constant number 1440 is for transforming the unit of $\hat{d}$ to minutes per day and $e_i$ is the delay occurring between $im$ and $(i+1)m$, such that $e_i = 0$ if $|T(t) - T(im)| < c^{\mathrm{t}}$ and $|W(t) - W(im)| < c^{\mathrm{w}}$ for $\forall t \in (im, (i+1)m)$. Otherwise, $e_i = \max\left((i+1)m - t\right)$ where $t$ satisfies $|T(t) - T(im)| \geq c^{\mathrm{t}}$ or $|W(t) - W(im)| \geq c^{\mathrm{w}}$. With the definition, the average delay is illustrated in Figure 4.6. For sending only periodic updates, the average delay increases significantly with the increase of $m$, $c^{\mathrm{t}}$, and $c^{\mathrm{w}}$. However, as shown in Figure 4.7, increasing $m$ can significantly reduce the number of packets. Thus, periodic updates cannot achieve low packet rates and low average delay at the same time. Adding significant-change updates solved the problem. The green line in Figure 4.6 illustrates the average delay in sending periodic and significant-change updates. Regardless of $m$, $c^{\mathrm{t}}$, and $c^{\mathrm{w}}$, it approaches zero as sensor nodes send updates once a significant change is detected. On the other hand, its number of packets also reduces significantly with the increase of $m$. Compared with periodic updates, adding significant-change updates increases the number of packets very slightly, e.g., using significant-change updates with $c^{\mathrm{t}} = 2$ °C and $c^{\mathrm{w}} = 20$ mph only increases about 3 packets per day when $m$ is between 5 and 5.08 minutes. Therefore, it is beneficial to use periodic updates and significant-change updates to reduce packet rates and average delay at the same time.

### 4.5.2 Packet Loss Detection

Data is directly collected from sensor nodes, including generated periodical updates and significant-change updates, from December 14, 2022, to January 20, 2023, with $m = 15$ minutes, $c^{\mathrm{t}} = 2$ °C, and $c^{\mathrm{w}} = 12$ mph. Assume that all the periodical updates are received by the gateway.

In terms of air temperature, $n_{\mathrm{t}}^{\mathrm{g}} = \hat{n}_{\mathrm{t}}^{\mathrm{g}}$ for 99.97% of the data, which means the estimation of (4.1) has the accuracy of 99.97%. In this situation, the result of packet loss detection is correct no matter whether there is a packet loss or not.

In terms of wind speed, given that there are not enough lost packets during this time to do the training and test of SVM, 30% of the significant-change updates

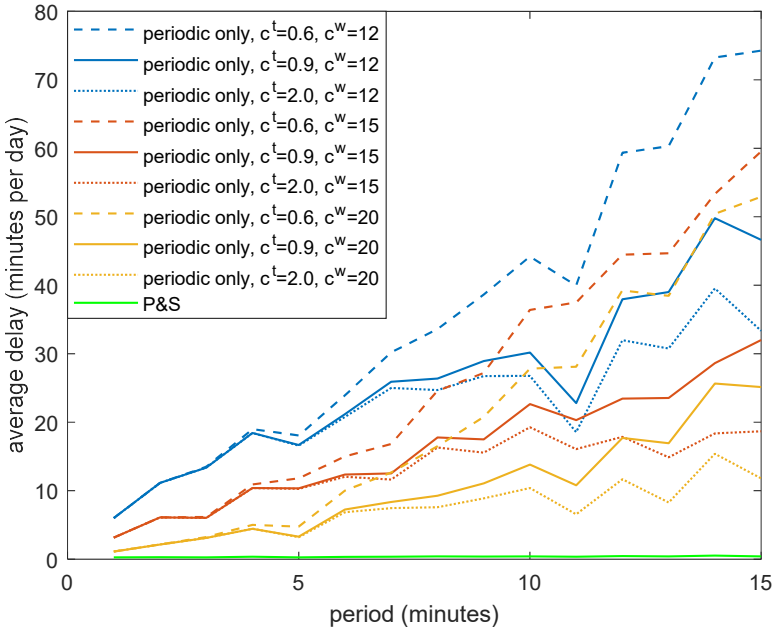



Figure 4.6: Average delay with different periods and significant-change criteria. $c^{\mathrm{t}}$ and $c^{\mathrm{w}}$ are in °C and mph, respectively. "P&S" denotes that sensor nodes send periodic and significant-change packets.

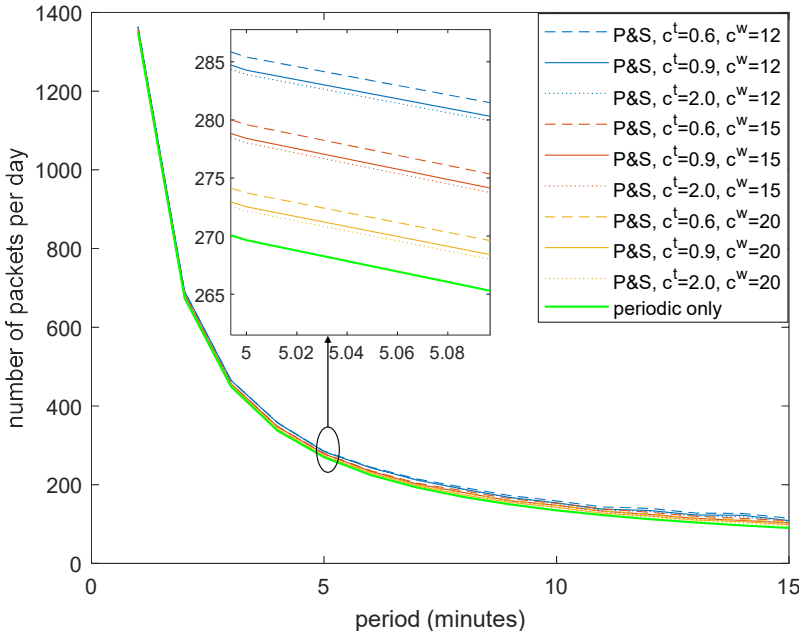



Figure 4.7: The number of packets with different periods and significant-change criteria. $c^{\mathrm{t}}$ and $c^{\mathrm{w}}$ are in °C and mph, respectively. "P&S" denotes that sensor nodes send periodic and significant-change packets.

are randomly deleted. Subsequently, samples with features are generated using the moving window method, as described in (4.4) and (4.5). The samples with deleted significant-change updates are labeled as abnormal, or otherwise normal. Then, 80% of the samples are randomly selected to train the SVM algorithm, and the remaining 20% of the samples are utilized to evaluate the performance. Since packet loss detection is a supervised anomaly detection problem, four common performance metrics are selected including *precision*, *recall*, $F1score$, and *accuracy* which are defined as

$$precision = \frac{TP}{TP + FP}, \tag{4.8a}$$

$$recall = \frac{TP}{TP + FN}, \tag{4.8b}$$

$$accuracy = \frac{TP + TN}{TP + FP + FN + TN}, \tag{4.8c}$$

$$F1score = \frac{2 * precison * recall}{precison + recall}, \tag{4.8d}$$

where $TP$ denotes true positive that the loss of significant-change updates is successfully classed as an abnormality, $TN$ denotes true negative that a normal situation is identified correctly, $FP$ denotes false positive that an abnormality is incorrectly classed as normality, and $FN$ denotes false negative that a normal situation is incorrectly identified as an abnormality. To obtain the optimal window length, the experiments are repeated with different window lengths. As shown in Figure 4.8, the x-axis, i.e., window length, is the length of the moving window described in (4.4) and (4.5). With the window length increasing, *recall* and *accuracy* drop when the window length is less than 1 hour and become stable when the window length is bigger than 2 hours. *precision* and $F1score$ increase with the window length increasing and become stable when the window length is bigger than 15/4 hours. Therefore, the window length should be set bigger than 15/4 hours for high performance of the packet loss detection algorithm. Given computation complexity and storage requirement, the window length is set as 15/4 hours which also serves as the retention time of the local database in the edge.

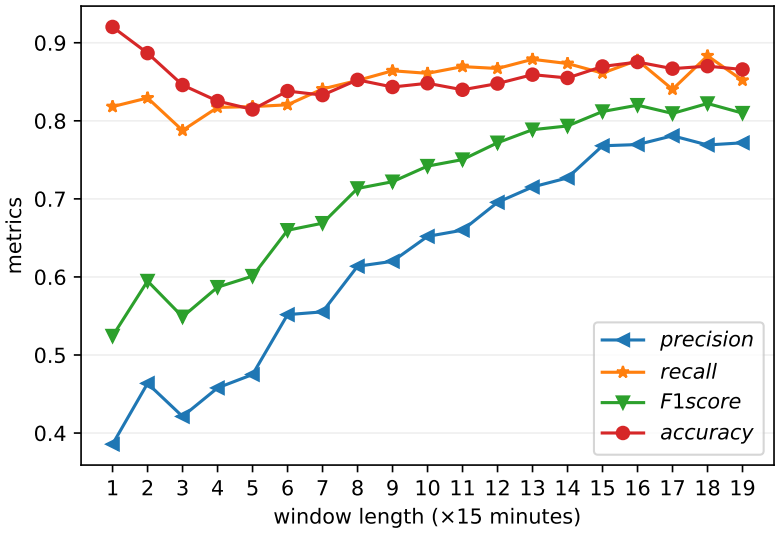



Figure 4.8: Result of packet loss detection.

### 4.5.3 Adaptive Thresholds

The data collected from the implemented network between December 14, 2022, and January 20, 2023, is also used for the adaptive threshold algorithm. ARIMA model is fit by the data from December 14, 2022, to January 10, 2023. The remaining data is used to evaluate the prediction performance by Root Mean Square Error (RMSE) and Mean Absolute Error (MAE) which are defined as

$$RMSE = \sqrt{\frac{1}{n_e}\sum_{i=1}^{n_e}(y_i - \hat{y}_i)^2}, \tag{4.9a}$$

$$MAE = \frac{1}{n_e}\sum_{i=1}^{n_e}|y_i - \hat{y}_i|, \tag{4.9b}$$

where $y_i$ is the $i^{th}$ actual value, $\hat{y}_i$ is the corresponding predicted value, and $n_e$ is the total number of the values to be evaluated. As shown in Table 4.2, the RMSE of the prediction for the maximum air temperature, minimum air temperature, and maximum wind speed of the next day is 1.906 °C, 1.231 °C, and 6.997 mph, respectively. The MAE of the prediction about the maximum air temperature, minimum air temperature, and maximum wind speed of the next day is 1.544 °C, 0.983 °C, and 6.097 mph, respectively. With the prediction accuracy, the data reduction rates from edge to the cloud for air temperature and wind speed are 72.23% and 97.96%, respectively.

Table 4.2: Results of adaptive thresholds.

| Prediction objective | RMSE | MAE | Data reduction rate |
|---|---|---|---|
| Max air temperature | 1.906 °C | 1.544 °C | 72.23% |
| Min air temperature | 1.231 °C | 0.983 °C | |
| Max wind speed | 6.997 mph | 6.097 mph | 97.96% |

## 4.6 Summary

In this chapter, a LoRa mesh-5G integrated network has been proposed for trackside smart weather monitoring. Firstly, the network model is presented and the LoRa mesh network is integrated into a 5G network, which significantly reduces the cost of deploying communication infrastructure for wide and remote coverage. The proposed network is employed for weather monitoring and a cloud-edge-terminal collaborative architecture is designed to bring artificial intelligence to the IoT network. Utilizing three intelligent algorithms, i.e., timely significant-change updates, packet loss detection, and adaptive thresholds, the proposed architecture reduced the data volume and achieved self-detection for packet loss. With reduced data volume, the network can support more end devices and provide wider coverage. Based on the Glasgow 5G testbed, a proof of concept was implemented using low-power and low-cost off-the-shelf hardware. The experimental results demonstrated the feasibility of the proposed integrated network and cloud-edge-terminal collaborative architecture. The proposed LoRa mesh-5G integrated network satisfies all the identified trackside sensing requirements, i.e., wide coverage, supporting massive end devices, low-cost communication infrastructure, and low-power and low-cost end devices.

However, the possibility of signal collision and interference could rise with an increase in the deployed end devices, posing a threat to network reliability. Moreover, duty cycle regulation [184] on the frequency bands utilized by LoRa could constrain its scalability. In the following chapter, these aspects of the network will be analyzed and novel LoRa mesh routing algorithms will be introduced to address the potential challenges associated with reliability and scalability.

# Chapter 5

# Linear LoRa Mesh Reliability and Scalability Management

This chapter analyzes fault tolerance, reliability, scalability, and coverage of the LoRa mesh-5G integrated network, and proposes a novel routing algorithm to achieve optimal scalability and coverage. Part of the work presented in this chapter has been submitted to the IEEE Internet of Things Journal.

## 5.1 Introduction

Linear infrastructure, such as pipelines, roads, railways, mines, and international borders, constitutes a vital and extensive network characterized by its linear configuration. The efficient monitoring of linear infrastructure plays a pivotal role in ensuring the safety, reliability, and optimal performance of these critical systems [185]. Moreover, enabled by remote monitoring, predictive maintenance has become a promising method for maintaining extensive infrastructure given the high cost of traditional periodic maintenance approaches. However, substantial parts of these infrastructures are located in remote areas without terrestrial network coverage which makes deployment slow and expensive [169]. Given the linear nature of these infrastructures, wireless networks with star topology are not well-suited for such monitoring. This is because deploying numerous gateways with backbone connections is necessary alongside the linear infrastructure, resulting in high deployment and management costs. Instead, mesh topology offers a promising method for linear infrastructure monitoring due to their multi-hop communication

technologies [186]. Although the topology of the infrastructure is linear, the topology of the mesh network is not necessarily linear.

The advent of LPWA technologies, exemplified by LoRa [187] communication, has revolutionized the field of remote monitoring. Given the low-power, long-range, and low-cost capabilities, LoRa is well-suited for applications in remote areas such as smart agriculture [188] and smart farming [189]. However, the star topology limits the use of LoRa in extensive linear infrastructure monitoring applications. In this context, the implementation of LoRa mesh [53] networks has emerged as a notable advancement. Unlike traditional single-hop LoRa setups, LoRa mesh offers extended coverage and improved reliability through its self-organizing capabilities, making it an appealing choice for large-scale linear infrastructure monitoring deployments. More significantly, LoRa mesh nodes can be deployed alongside linear infrastructure and form multi-hop communication paths, eliminating the need for densely deploying gateways and significantly reducing the deployment cost.

Compared with single-hop LoRa, LoRa mesh has two key features: multi-hop routing and self-organization, which act as a double-edged sword influencing its fault tolerance and reliability. On the one hand, multi-hop paths increase vulnerability to node failure, as the failure of any intermediate node may cause communication interruptions for the remaining nodes. On the other hand, the self-organization mechanism enables the network to self-heal in the event of node failure, provided that alternative routes exist. Thus, it is imperative to investigate fault tolerance and reliability when developing a self-organized network like LoRa mesh [190].

Monitoring extensive linear infrastructure requires numerous devices connected to a single network, which poses the network scalability challenge. In LoRa and LoRa mesh, scalability is constrained by 1) internal signal collisions, and 2) duty cycle regulations. The duty cycle of LoRa refers to the maximum amount of time a LoRa device can transmit data within a specific time window while adhering to regulatory constraints, ensuring fair use of the radio spectrum. For the first constraint, internal signal collisions refer to the collision caused by concurrent signal transmission from multiple nodes of the network. With the increase in the number of nodes, the possibility of internal signal collisions increases, thereby constraining network scalability [54] [56] [55]. This limitation can be eliminated or mitigated by properly scheduling data collection and transmission. In addition, signals from external devices may also collide with internal signals, as LoRa and LoRa mesh operate in license-free frequency bands. To mitigate interference among networks,

regulators impose restrictions on the maximum duty cycle, i.e., the second constraint. For example, in Europe, LoRa operates in the frequency bands 433.05-434.79 MHz or 863-870 MHz, where ETSI limits the duty cycle under 0.1%, 1%, or 10% [184] depending on the sub-band. To avoid network congestion, LoRa Alliance specifies 1% as the maximum duty cycle for LoRa in the bands where ETSI requires 10% [25]. These duty cycle regulations impose limitations on the scalability of LoRa-based networks [191]. However, existing research on the scalability of LoRa mesh focuses on the constraint of internal signal collisions, ignoring the constraint of duty cycle regulations. On the other hand, since the coverage extension ratio of LoRa mesh, compared to LoRa, is related to the number of nodes that can be deployed in the network [52], duty cycle regulations also constrain the coverage extension ratio. Investigating the coverage extension ratio is also crucial for monitoring linear infrastructure, given the considerable length of the infrastructure.

In Chapter 4, LoRa mesh was integrated with a 5G network for trackside weather monitoring, and a cloud-edge-terminal collaborative architecture was proposed to reduce the network data volume. This chapter investigates the challenges associated with fault tolerance, reliability, scalability, and coverage of linear LoRa mesh. Firstly, a deployment strategy is proposed for a LoRa mesh network designed for monitoring linear infrastructure. The strategy not only ensures fault tolerance, reliability, scalability, and extensive coverage but also introduces deployment adaptability by allowing flexibility in the distances between proximate nodes. Secondly, the fault tolerance, reliability, scalability, and coverage of the LoRa mesh network are analyzed. In terms of the constraints on scalability and coverage, the focus is on duty cycle regulations instead of internal signal collisions. In terms of coverage, the focus is on the coverage extension ratio of the LoRa mesh compared to single-hop LoRa instead of absolute coverage. The upper and lower bounds for scalability and coverage extension ratio are derived. It is observed that the values of these metrics depend on the routing algorithm. Thirdly, a novel routing algorithm is proposed that leverages the 5G core network and considers the minimum number of hops and the Received Signal Strength Indicator (RSSI) to achieve maximum scalability and coverage. Lastly, with the lack of a suitable LoRa mesh simulator for the research community, a simulator called LoRaMeshSim is developed to verify the system analysis and the proposed routing algorithm.

The remainder of this chapter is organized as follows: Section 5.2 presents the system model of the linear LoRa mesh network and introduces the proposed

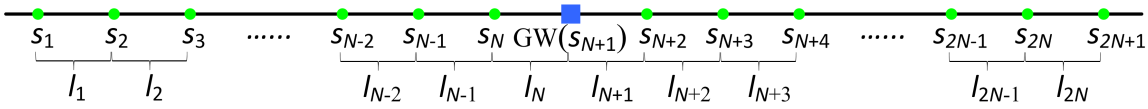



Figure 5.1: System model of LoRa mesh network on linear infrastructure.

deployment strategy for LoRa mesh. Section 5.3 details the system analysis on fault tolerance, reliability, scalability, and coverage. In Section 5.4, the novel routing algorithm is introduced. Section 5.5 describes the validation using the LoRa mesh simulator. Finally, Section 5.6 concludes the chapter.

## 5.2 System Model

The system model of the proposed LoRa mesh-5G network was previously introduced in Figure 4.2. In this chapter, depicted in Figure 5.1, the system model is redrawn, eliminating the diagrammatic elements and aspects related to 5G, to emphasize the positioning of each node. As shown in Figure 5.1, a linear infrastructure can be modeled as a straight line with LoRa mesh nodes deployed alongside it. A LoRa mesh gateway is deployed in the middle of the line with $N$ sensor nodes at both sides of the gateway. The $i^{th}$ sensor node from left to right is denoted as $s_i$ for $i \in [1, N] \cap \mathbb{Z}$ and $s_{i+1}$ for $i \in [N+1, 2N] \cap \mathbb{Z}$, respectively. To simplify the notation in the following analysis, the gateway is denoted as $s_{N+1}$ even though it does not have sensors. Sensor nodes collect data and transmit it to the gateway by encapsulating it as LoRa mesh packets. The gateway has access to the Internet via different technologies such as Ethernet, WiFi, satellite communication, and cellular networks [192, 193]. When receiving LoRa mesh packets, the gateway uploads data to the cloud via the Internet for further processing.

Unlike single-hop LoRa networks, most of the sensor nodes are outside of the coverage of the gateway, thus requiring other sensor nodes to relay packets. The selection of a relayer node depends on the routing algorithm, while the number of relayer candidates for each node is determined by its distance from other nodes. It is assumed that nodes are placed in a two-dimensional plane with the gateway located at coordinates (0,0). The distance between $s_i$ and $s_{i+1}$ is denoted as $l_i$ for $i \in [1, 2N] \cap \mathbb{Z}$. Then, each sensor node $s_i$ is placed at coordinates $(\sum_{j=i}^{j=N} -l_j, 0)$ for $i \in [1, N] \cap \mathbb{Z}$ and coordinates $(\sum_{j=N+1}^{j=i-1} l_j, 0)$ for $i \in [N+2, 2N+1] \cap \mathbb{Z}$. The maximum communication distance of single-hop LoRa depends on the frequency

band, the transmit power, the spreading factor, and the terrain [26]. this chapter considers a fixed value, $r$ for the distance since the focus is on the coverage extension ratio of LoRa mesh compared to LoRa, instead of the absolute coverage. Traditional research methods of linear infrastructure monitoring usually assume that sensors are deployed evenly [194] [195], i.e., all the $l_i$ equal to a fixed value. In a real deployment, it is difficult to realize given the practical environment, terrain, and available deployment locations. To address these challenges, a more adaptable deployment strategy is proposed, introducing flexibility in the node-to-node distances denoted by $l_i$. Specifically, a positive integer is defined, denoted as the distance factor $\phi$. With this parameter, flexible deployment distances can be expressed as follows:

$$l_i \in \left( \frac{r}{\phi + 1}, \frac{r}{\phi} \right) \text{ for } i \in [1, 2N] \cap \mathbb{Z}, \tag{5.1}$$

The parameter $\phi$ plays a pivotal role in defining the spacing between two proximate nodes, thus directly shaping the overall deployment density of the network. Since the system model is symmetric, only the sensor nodes on the left side of the gateway are considered in the following analysis. The results will also be applicable to the sensor nodes on the right side of the gateway. Let $l_{i,j}$ denote the distance between $s_i$ and $s_j$, i.e., $l_{i,j} = \sum_{\mu=i}^{\mu=j-1} l_\mu$, where $i, j \in [1, N+1] \cap \mathbb{Z}$. Then, according to (5.1),

$$l_{i,j} \begin{cases} < r, & \text{for } j - i \in [1, \phi] \\ > r, & \text{for } j - i > \phi. \end{cases} \tag{5.2}$$

Thus, $\forall i, j \in [1, N+1] \cap \mathbb{Z}$, $s_i$ and $s_j$ can directly communicate with each other only when $|j - i| \in [1, \phi]$. For instance, if $\phi = 1$, the distance between two proximate nodes can be any value between $r/2$ and $r$. $s_1$ can directly communicate with $s_2$ as $l_{1,2} = l_1 < r$. $s_1$ cannot directly communicate with $s_3$ as $l_{1,3} = l_1 + l_2 > r$.

The sensor nodes that can directly communicate with the gateway are referred to as adjacent nodes. According to (5.2), the number of adjacent nodes on the left side of the gateway, consisting of $s_i$ for $i \in [N-\phi+1, N] \cap \mathbb{Z}$, equals the distance factor, $\phi$. All the sensor nodes outside of the coverage of the gateway, i.e., $s_i$ for $i \in [1, N-\phi] \cap \mathbb{Z}$, are referred to as remote nodes and need adjacent nodes to relay data packets. Based on (5.2), the sub-network composed of $s_1, s_2, ..., s_{N+1}$ can be denoted as a graph $G = (S, E)$, where $S = s_1, s_2, ..., s_{N+1}$ and $E = \{(s_i, s_j) \mid s_i, s_j \in S \text{ and } j - i \in [1, \phi]\}$.

## 5.3 System Analysis

In this section, the fault tolerance, reliability, scalability, and coverage extension ratio will be analyzed.

### 5.3.1 Fault Tolerance and Reliability

Fault tolerance of a system assesses its capability to function with faulty components [196]. Most of the studies on fault tolerance in mesh networks use the vertex connectivity ($k$) of a graph as the metric of fault tolerance [197], which is defined as the smallest number of vertices whose deletion separates the graph [198]. In the linear LoRa mesh network, with the assumption of $|S| > \phi + 1$, the vertex connectivity can be derived as

$$k(G) = \phi, \tag{5.3}$$

where $\phi$ is the same positive integer in (5.1) denoting the deployment density of the sensor nodes. Proof: See Section A of the Appendix. Thus, the fault tolerance of the mesh network is determined by the deployment density of sensor nodes. According to (5.3), when the number of malfunctioning nodes is less than $\phi$, the network is still connected and each remaining sensor node has at least one feasible route to the gateway. With self-healing routing algorithms, a sensor node can automatically find a new feasible route to the gateway when its current route is no longer valid due to the malfunctions of the relay nodes.

Based on the fault tolerance, the system reliability of the LoRa mesh network can be analyzed, which is defined as the probability of the LoRa mesh network being connected [199]. According to (5.3), the following theorem can be further derived:

**Theorem 1** *$\forall V \subset S$, the graph $G - V$ is connected if $\forall i \in [1, N - \phi + 2], \{s_i, s_{i+1}, ..., s_{i+\phi-1}\} \nsubseteq V$.*

Proof: See Section B of the Appendix. Theorem 1 shows that the network is still connected if the number of continuously located malfunctioning nodes is less than $\phi$. On the other hand, if $\{s_1, s_2, ..., s_i\} \subseteq V$ where $i \in [\phi, N]$, $G - V$ may remain connected despite the existence of $\phi$ consecutive failed sensor nodes. The reason is that the set $\{s_1, s_2, ..., s_i\}$ where $i \in [\phi, N]$, located at the left end of the network, has no impact on the connectivity of the remaining network if all nodes in the set fail. Thus, assuming that the gateway never fails and each sensor node has a reliability

of $\lambda$ (with a failure rate of $1-\lambda$), the system reliability can be calculated as

$$Pr = h(\lambda, \phi, N) + \sum_{i=1}^{N-1} (1-\lambda)^i \lambda h(\lambda, \phi, N-i-1) + (1-\lambda)^N, \tag{5.4}$$

where $h(\lambda, \phi, N)$ is the probability of the nonexistence of $\phi$ consecutive failed sensor nodes. Chiang and Niu [199] derive a recursive formula to calculate $h(\lambda, \phi, N)$ when analysing consecutive-$\phi$-out-of-$N$:F systems, shown as

$$h(\lambda, \phi, N) = \sum_{i=1}^{N-\phi+1} \sum_{j=i+1}^{i+\phi-1} h(\lambda, \phi, N-j) \lambda^i (1-\lambda)^{j-i} + \lambda^{N-\phi+1}$$

$$h(\lambda, \phi, \eta) = \begin{cases} 1, & 0 \leq \eta < \phi \\ 0, & \eta < 0. \end{cases} \tag{5.5}$$

### 5.3.2 Scalability

This subsection will investigate the impact of duty cycle regulations on the scalability of the LoRa mesh network—specifically, examining the maximum number of sensor nodes that the network can support under the set duty cycle requirement.

Mesh networks require an acknowledgment message for each data message as each node needs to know the validity of its routes to the destination nodes. It is assumed that all the data messages have the same packet length denoted as $L_d$ bytes, all the acknowledgment messages have the same packet length denoted as $L_a$ bytes, all the sensor nodes transmit data at the same packet rate denoted as $p$ packets per second per node, and each node selects only one route to transmit a data packet to the gateway. With these assumptions, the duty cycle of sensor node $s_i$ can be expressed as

$$d_i = (n_i + 1) p t_d + n_i p t_a, \tag{5.6}$$

where $n_i$ is the number of sensor nodes whose data packets are relayed by $s_i$. Here, the term 'relayed' includes not only the initial relay but also subsequent relays, given that a data packet may need to be relayed multiple times before reaching the gateway. $t_d$ and $t_a$ are the time on air of each data packet and each acknowledgment packet,

respectively, which can be calculated by [200]

$$t_d = (\Omega + 4.25 + 8 + n_d^p)\frac{2^{SF}}{BW}, \tag{5.7}$$

$$t_a = (\Omega + 4.25 + 8 + n_a^p)\frac{2^{SF}}{BW}, \tag{5.8}$$

where

$$n_d^p = \max\left[\left\lceil\frac{8L_d - 4SF + 28 + 16 - 20H}{4(SF - 2\Psi)}\right\rceil(CR + 4), 0\right], \tag{5.9}$$

$$n_a^p = \max\left[\left\lceil\frac{8L_a - 4SF + 28 + 16 - 20H}{4(SF - 2\Psi)}\right\rceil(CR + 4), 0\right], \tag{5.10}$$

where $\lceil\cdot\rceil$ is the ceiling function. The explanation of the variables in (5.7), (5.8), (5.9), and (5.10) is listed:

- $\Omega$ is the number of programmed preamble symbols.
- $SF$ is the spread factor from 7 to 12.
- $BW$ is the channel bandwidth.
- $H = 1$ indicates the LoRa header is explicit and 0 otherwise.
- $\Psi = 1$ indicates low data rate optimize can be enabled and 0 otherwise.
- $CR$ is the coding rate from 1 to 4.

According to the duty cycle regulation, $\forall i \in [1, N] \cap \mathbb{Z}, d_i \leq D$, where $D$ is the maximum duty cycle requirement. Combining (5.6), to comply with the regulation, the following must hold

$$n_i \leq \frac{D - pt_d}{p(t_d + t_a)}, \forall i \in [1, N] \cap \mathbb{Z}. \tag{5.11}$$

To relieve the relaying burden, sensor nodes on one side of the gateway are presented from relaying packets from the sensor nodes on the other side by allocating different identification addresses to them. Thus, $n_i \leq N - 1$. Since $d_i$ is positively correlated with $n_i$ according to (5.6), $\exists i \in [1, N] \cap \mathbb{Z}, n_i = N - 1$ is the worst case where all the packets on the left side are relayed by one sensor node.

On the other hand, comparing the duty cycle of adjacent nodes and remote nodes, the following lemma holds for the sensor nodes in the LoRa mesh network:

**Lemma 1** *Among the sensor nodes, the node with the highest duty cycle, when*

*compared to all other sensor nodes, is an adjacent node.*

Proof: See Section C of the Appendix. Based on Lemma 1, the best case is that the $\phi$ adjacent nodes evenly share the relay tasks for the $N-\phi$ remote nodes, which can be formulated as $n_i = (N-\phi)/\phi = N/\phi - 1$ for $i \in [N-\phi+1, N] \cap \mathbb{Z}$. Thus, in the best case, $n_i \leq N/\phi - 1$ for $\forall i \in [1, N] \cap \mathbb{Z}$. Given the worst and best cases, the following derivations can be made:

$$\begin{cases} \forall i \in [1, N] \cap \mathbb{Z}, & n_i \leq \frac{N}{\theta - 1} \\ \exists i \in [1, N] \cap \mathbb{Z}, & n_i = \frac{N}{\theta - 1}, \end{cases} \tag{5.12}$$

where $\theta \in [1, \phi]$. $\theta = 1$ indicates that the network is in the worst status while $\theta = \phi$ indicates the best status in terms of duty cycle. The value of $\theta$ is determined by the routing algorithm which will be discussed in Section 5.4. If $N$ is configurable, to satisfy (5.11), the following must hold

$$\begin{aligned} \frac{N}{\theta} - 1 &\leq \frac{D - pt_d}{p(t_d + t_a)}, \\ N &\leq \theta \frac{D + pt_a}{p(t_d + t_a)}, \theta \in [1, \phi]. \end{aligned} \tag{5.13}$$

In terms of the gateway, although it does not send any data packets, it sends out an acknowledgment packet for each data packet from any sensor node. Thus, its duty cycle $d_{\mathrm{G}} = 2Npt_a$. As the gateway also complies with the duty cycle regulation,

$$\begin{aligned} 2Npt_a &\leq D, \\ N &\leq \frac{D}{2pt_a}. \end{aligned} \tag{5.14}$$

Combining (5.13) and (5.14),

$$N \leq \min\left(\frac{D}{2pt_a}, \theta \frac{D + pt_a}{p(t_d + t_a)}\right), \theta \in [1, \phi]. \tag{5.15}$$

As $N$ is an integer, the maximum number of sensor nodes on the left side of the gateway is derived as

$$N_{\max} = \min\left(\left\lfloor \frac{D}{2pt_a} \right\rfloor, \left\lfloor \theta \frac{D + pt_a}{p(t_d + t_a)} \right\rfloor\right), \theta \in [1, \phi], \tag{5.16}$$

where $\lfloor \cdot \rfloor$ is the floor function. Since the network is symmetric, the maximum total number of sensor nodes is $2N_{\max}$. As indicated in (5.16), $\phi$ determines the upper bound of $N_{\max}$, and when $\theta = \phi$, the network can reach this upper bound.

### 5.3.3 Coverage Extension Ratio

In addition to scalability, coverage is another important aspect of the LoRa mesh network. For the linear LoRa mesh network, the coverage extension ratio is used as the metric which is defined as

$$c = \frac{l_{1,N+1}}{r} = \frac{\sum_{i=1}^{N} l_i}{r}. \tag{5.17}$$

As $l_i < r/\phi$ for $\forall i \in [1, N] \cap \mathbb{Z}$,

$$c < \frac{\sum_{i=1}^{N} \frac{r}{\phi}}{r} = \frac{N\frac{r}{\phi}}{r} = \frac{N}{\phi} \leq \frac{N_{\max}}{\phi}. \tag{5.18}$$

Thus, combining (5.16) and (5.18),

$$c < \min\left(\frac{1}{\phi}\left\lfloor \frac{D}{2pt_a} \right\rfloor, \frac{1}{\phi}\left\lfloor \theta \frac{D + pt_a}{p(t_d + t_a)} \right\rfloor\right), \theta \in [1, \phi]. \tag{5.19}$$

Similar to scalability, $\phi$ determines the upper bound of $c$, and when $\theta = \phi$, the network can reach this upper bound.

## 5.4 Routing Algorithm

In this section, the network topology required for achieving the upper bounds of $N_{\max}$ and $c$ will be derived first. Subsequently, a routing algorithm utilizing a 5G core network to achieve this network topology will be presented.

### 5.4.1 Required Topology

As indicated by (5.16) and (5.19), both the maximum number of sensor nodes and the maximum coverage extension ratio are functions of $\theta$. The upper bounds for the number of sensor nodes and coverage extension ratio can be obtained when $\theta = \phi$. As analyzed, $\theta = \phi$ when $\phi$ adjacent nodes evenly share the relay tasks for

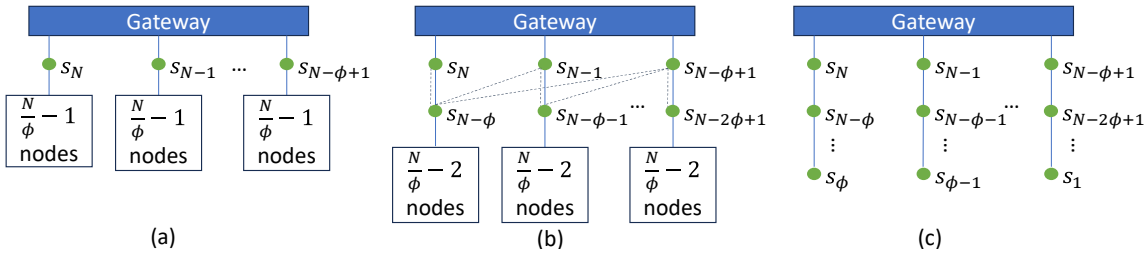



Figure 5.2: Network topology derivation process and routing discovery process

$N-\phi$ remote nodes. Routing algorithms determine the relay relationship and enable self-organization in the topology of a spanning tree of the graph $G$ [56]. If a node in a tree is designated as the root, the nodes in the tree are hierarchical based on the length of the path from the node to the root, which is termed as the level. The root is at level zero, while nodes directly connected to the root are at level one, nodes connected to them are at level two, and so on. The topology required for $\theta = \phi$ will be discussed level by level.

First, as illustrated in Figure 5.2 (a), the gateway is designated as the root. At level one, the $\phi$ adjacent nodes, i.e., $s_i$ for $i \in [N-\phi+1, N] \cap \mathbb{Z}$, serve as the children of the gateway and each adjacent node becomes the root of a sub-tree with $N/\phi$ nodes. This arrangement is necessary because each adjacent node needs to relay data packets from $N/\phi - 1$ remote nodes to achieve $\theta = \phi$.

Second, at level two, as illustrated in Figure 5.2 (b), the candidates include $s_i$ for $i \in [N-2\phi+1, N-\phi] \cap \mathbb{Z}$, determined based on their distances to the nodes at level one. Each node at level one must select at least one node as its child until the number of its descendants reaches $N/\phi - 1$. Consequently, among these candidates, $s_{N-\phi}$ must serve as the child of $s_N$ as only $s_{N-\phi}$ can communicate with $s_N$ directly. Once $s_{N-\phi}$ is selected, the process repeats, and $s_{N-\phi-1}$ becomes the child of $s_{N-1}$ as only $s_{N-\phi-1}$ in unselected candidates can communicate with $s_{N-1}$ directly. This derivation continues iteratively, assigning each candidate a parent node, i.e., $s_i$ as the parent node of $s_{i-\phi}$ for $i \in [N-\phi+1, N] \cap \mathbb{Z}$. The result is illustrated in Figure 5.2 (b) where the solid lines denote selection and the dashed lines denote that the two nodes can communicate with each other directly.

Finally, by iteratively progressing from level one to level two, and continuing this process until reaching from level $N/\phi - 1$ to level $N/\phi$, the complete topology of the spanning tree can be derived, denoted as $T = (S, E_t)$ where $S = s_1, s_2, ..., s_{N+1}$ and $E_t = E'_t \cup E''_t$. $E'_t = \{(s_i, s_j) \mid s_i, s_j \in S \text{ and } j - i = \phi \text{ for } j \leq N\}$ and

$E_t'' = \{(s_i, s_j) \mid s_i, s_j \in S \text{ and } j - i \leq \phi \text{ for } j = N + 1\}$. As illustrated in the Figure 5.2 (c), for $i \in [N - \phi + 1, N] \cap \mathbb{Z}$, $s_i$ relays data packets from $N/\phi - 1$ remote nodes, which consists of $s_{i-j\phi}$ for $j \in [1, N/\phi - 1] \cap \mathbb{Z}$. Thus, the topology achieves the requirement of $\theta = \phi$. Furthermore, it is evident from the derivation process that the topology is uniquely determined, signifying that there exists only one possible topology, i.e., $T$, for $\theta = \phi$.

### 5.4.2 Routing

To achieve the topology of $T$, a routing algorithm considering RSSI and the number of hops is proposed, using a 5G core network. Since $T$ is a spanning tree, each sensor node only has one parent node towards the gateway. So, the aim of the routing algorithm is to equip each sensor node with a routing table that contains only one piece of information, i.e., the identifier of the next-hop node towards the gateway. The routing process consists of two stages, i.e., routing request and routing discovery.

At stage one, when a node, called an initializer, wants to join the network or its routing table is no longer valid (known by acknowledged packets), it broadcasts a routing request to the network. Any node in the network receiving this request unicasts it to the gateway using the routing table of the node. Since multiple nodes may receive the broadcasted request, the gateway would receive the request from the same initializer multiple times. To mitigate the calculation and storage burden, the gateway sends the request to a 5G core network by the method proposed in Chapter 4. The 5G core network stores these requests and decides which request should receive a response. To avoid message congestion in the LoRa mesh network, only the first request from an initializer within a specific time is responded to. The 5G core network sends a downlink message with the decision to the gateway, informing it to respond by initializing a routing discovery process.

At stage two, after receiving a routing request, the gateway broadcasts a routing discovery message with the identifier of the initializer. When a sensor node receives the message, it checks whether a routing discovery message for the same initializer has been received. If yes and the number of hops of the new message is bigger than the previous one, it discards the message. Otherwise, it updates its routing table using the identifier of the sender of the message, rebroadcasts the message, and records the message for future route checking purpose. However, if the number of hops of the new routing discovery message is equal to the previous one, the node

compares their RSSI and chooses the worst one. The worst RSSI in this scenario would typically imply the longest distance between the transmitter and the receiver as RSSI is negatively correlated with the communication distance [201].

Figure 5.2 is used again to illustrate the broadcasting process of the routing discovery message as it is similar to the network topology derivation process. As shown in Figure 5.2 (a), when the gateway broadcasts the routing discovery message, adjacent nodes receive it and update their routing tables. Then, as shown in Figure 5.2 (b), the adjacent nodes rebroadcast the message, and the nodes at level two receive them. Some nodes at level two receive the message multiple times with the same number of hops, but $s_i$ chooses $s_{i+\phi}$ for $i \in [N - 2\phi + 1, N - \phi] \cap \mathbb{Z}$ based on the criterion of worst RSSI. In addition to the nodes at level two, nodes at the lower levels also receive the rebroadcasted message, but they discard it as the number of hops is bigger than the message they received before. By doing so, the nodes at level two have the correct routing tables specified by the topology of $T$. Finally, by iteratively progressing from level one to level two, the whole network shapes the topology of $T$.

Given the complexity of the routing discovery process, an example with $N = 4$ and $\phi = 2$ is used for clearer illustration. As shown in Figure 5.3 (a), there are four sensor nodes placed according to (5.1). The potential routes based on their location are shown with dash lines. As shown in Figure 5.3 (b), $s_4$ and $s_3$ receive the routing discovery message broadcasted from the gateway. After receiving the message, they update their routing table, select gateway as their next-hop node, and rebroadcast the message. As shown in Figure 5.3 (c), the rebroadcast messages arrive at the gateway and are subsequently discarded. $s_4$ discards the message rebroadcasted from $s_3$ as its hops exceed the hop of the message that $s_4$ has received from the gateway. $s_3$ discards the message rebroadcasted from $s_4$ as $s_4$ is spatially closer to $s_3$ than the gateway which has sent routing discovery message to $s_3$. Additionally, $s_2$ receives the rebroadcasted messages from both $s_4$ and $s_3$. $s_2$ selects $s_4$ as its next-hop node because $s_4$ is spatially further to it. $s_1$ receives the rebroadcasted messages from $s_3$, updates its routing table, and selects $s_3$ as its next-hop node. As shown in Figure 5.3 (d), both $s_2$ and $s_1$ rebroadcasts the message after they updates their routing tables. However, the rebroadcasted messages are discarded by other nodes due to either having more hops or being closer in location. Finally, the selected routes are shown in Figure 5.3 (e), achieving the topology of $T$ shown in Figure 5.2 (c).

Although signal collisions are out of the scope of this thesis, signal collisions

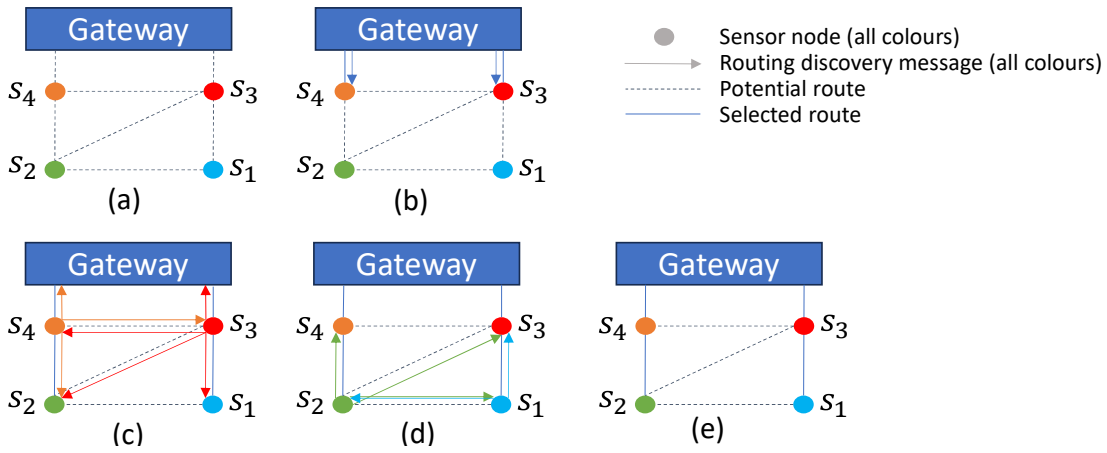



Figure 5.3: Example of routing discovery process with $N = 4$ and $\phi = 2$

arising from broadcasts during the routing process must be addressed, as they significantly affect the success rate of routing. When a node broadcasts a message, multiple nodes may receive it at the same time. If they retransmit it immediately after receiving it, any node within the coverage of two or more transmitters cannot receive any messages due to signal collisions. In the proposed routing algorithm, there are two kinds of broadcasts, i.e., initial routing request broadcast and routing discovery broadcast. Their signal collisions can be addressed using random delay. When a node receives a broadcasted routing request message, it delays unicasting the message by $it_r$, where $t_r$ denotes the time on air of the routing request message and $i$ is randomly chosen in $[0, X] \cap \mathbb{Z}$. When a node receives a routing discovery message, it delays rebroadcasting the message by $it_c$, where $t_c$ denotes the time on air of the routing discovery message and $i$ is randomly chosen in $[0, Y] \cap \mathbb{Z}$. The determination of the values of the two integers, $X$ and $Y$, referred to as the maximum delay integer for routing request and routing discovery, respectively, will be discussed in Section 5.5 through experiments. The routing algorithm is outlined in Algorithm 2.

## 5.5 Verification

Simulation is important for analyzing LoRa mesh performance and developing routing algorithms. However, despite the existence of several LoRa simulators, such as NS-3 [202] [203] and LoRaSim [204] [205], there is currently no dedicated LoRa

**Algorithm 2** Routing Algorithm

```
IF the node is initializer
  WHEN joining the network or routing table no longer valid
      WHEN routing discovery not received
          Broadcast routing request
          Wait for routing discovery message
      Update routing table
ELSE IF the node is the gateway
  WHEN routing request received
      IF not received from the initializer before
          Record the message
          Delay by (X + N)t_r
          Broadcast a routing discovery
ELSE
  WHEN routing request received
      IF it is a broadcast
          Delay by it_r, i randomly chosen in [0, X]
      Unicast to the next hop
  WHEN routing discovery received
      IF received before
          IF new hops < old hops
              Delay by it_c, i randomly chosen in [0, Y]
              Update routing table
              Record the message
              The hops of the message + 1
              Rebroadcast
          ELSE IF new hops = old hops
              IF new RSSI < old RSSI
                  Delay by it_c, i randomly chosen in [0, Y]
                  Update routing table
                  Record the message
                  The hops of the message + 1
                  Rebroadcast
```

mesh simulator available. LoRa mesh simulators face the challenge of handling concurrent transmissions from numerous nodes and managing their interactions. Existing LoRa simulators fall short in addressing this challenge as they do not incorporate signal relaying and routing in their design process. Thus, to validate the analysis and the proposed routing algorithm and to support the research

Table 5.1: The values of fixed parameters in the simulations.

| **Parameter** | **Value** |
|---|---|
| simulation time | 24 (hours) |
| $L_a$ | 5 (bytes) |
| $\Omega$ | 8 |
| $SF$ | 7 |
| $BW$ | 125 (kHz) |
| $H$ | 0 |
| $\Psi$ | 0 |
| $CR$ | 1 |

and development of LoRa mesh, a LoRa mesh simulator called LoRaMeshSim[5] is developed based on LoRaSim and SimPy (a discrete event simulator) [206]. In LoRaMeshSim, in accordance with the deployment strategy formulated in (5.1), $N$ independent random numbers are generated for $l_i$ where $i \in [1, N] \cap \mathbb{Z}$, utilizing a uniform distribution with the open interval $(\frac{r}{\phi+1}, \frac{r}{\phi})$. All the nodes including sensor nodes and the gateway are activated at the same time. After activation, each sensor node independently collects data continuously at intervals that follow an exponential distribution with a rate parameter equal to the packet rate, $p$. The data is then transmitted to the gateway in the form of a data packet if the sensor node has a valid routing table. Otherwise, the sensor node initializes a routing process by broadcasting a routing request to the network. Although signal collisions (except the ones caused by broadcast) are not considered in this thesis, they are simulated in the LoRaMeshSim. Specifically, in the simulator, a node cannot transmit or receive a packet if it is transmitting or receiving another packet. When multiple signals persist simultaneously in the surroundings of a node for a while, it cannot receive any of them. By doing so, a more practical LoRa mesh network is simulated. LoRaMeshSim will be used to validate the following aspects of the network in this section: 1) reliability, 2) routing success rate, and 3) scalability and coverage extension ratio. The values of fixed parameters in the simulations are listed in Table 5.1.

[5]Available at https://github.com/YuChenUoG/LoRaMeshSim

### 5.5.1 Reliability Verification

To verify the system reliability $Pr$, sensor nodes are not required to collect data or send packets. After placing all the nodes, whether a sensor node fails is determined by the probability of $1 - \lambda$. If a sensor node fails, it is deleted from the network. Then, the connectivity of the left network is determined using the depth-first search algorithm [207], one of the popular methods for checking the connectivity of undirected graphs. The values for $\lambda$, $N$, and $\phi$ vary, and the simulation is repeated 10,000 times for each set of these parameters to obtain the simulated probability of network connectivity. As shown in Figure 5.4, when $\phi$ is fixed at 2 and $N$ takes values in the set $\{4, 9, 14, 19\}$, $Pr$ increases either with the increase of $\lambda$ or with the decrease of $N$. With the increase of $N$, newly deployed nodes are positioned farther from the gateway. Consequently, the failure of any nearby nodes could disrupt the connectivity of the newly added nodes to the network, leading to a decrease in $Pr$. For $N = 4$, $Pr$ reaches 0.8, a relatively high value, when $\lambda > 0.6$. By contrast, for $N = 9, 14$ or 19, $Pr$ reaches 0.8 when $\lambda$ roughly exceeds 0.85. As shown in Figure 5.5, when $N$ is fixed at 10 and $\phi$ takes values in the set $\{1, 2, 3, 4\}$, $Pr$ increases either with the increase of $\lambda$ or with the increase of $\phi$. Noticeably, the line corresponding to $\phi = 1$ is significantly lower than the others as the failure of any sensor node, except $s_i$, results in the disconnection of the network when $\phi = 1$. Figure 5.4 and Figure 5.5 also demonstrate that the simulated results align well with the theoretical predictions from (5.4), thus confirming its correctness.

### 5.5.2 Routing Success Rate Investigation

The routing process consists of the routing request and the routing discovery. To investigate their success rates affected by the signal collisions arising from packet broadcast, sensor nodes are not required to collect data or send data packets.

To investigate the routing discovery success rate, after placing all the nodes, the routing discovery process is triggered from the gateway assuming that the gateway receives a routing request successfully. Then, whether the routing discovery is successful is determined by comparing the routing tables of all the nodes with the ideal topology of $T$. The values for $\phi$, $N$, and maximum delay integer for routing discovery $Y$ vary, and the simulation is repeated 10,000 times for each set of these parameters to obtain the success rate. As shown in Figure 5.6, when $\phi$ is fixed at 2 and $N$ takes values in the set $\{2, 6, 10, 14, 18\}$, the success rate increases either

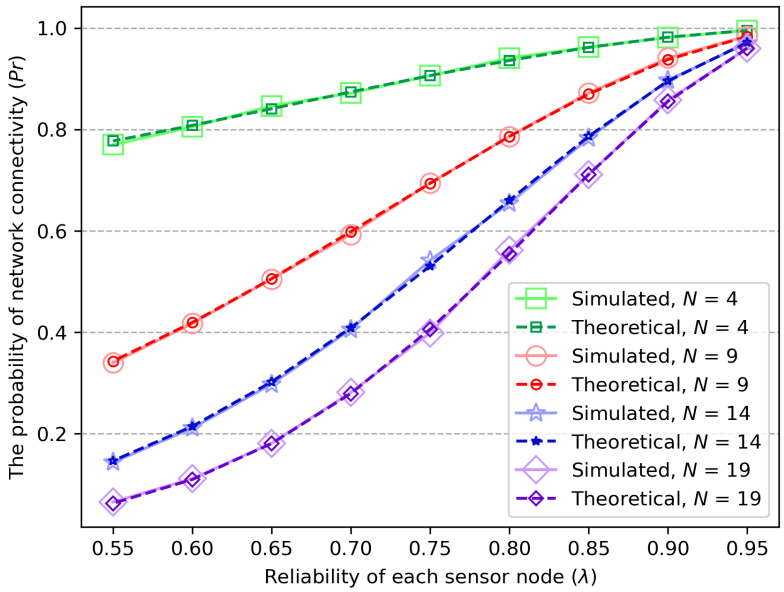



Figure 5.4: The probability of network connectivity with different $N$ when $\phi = 2$

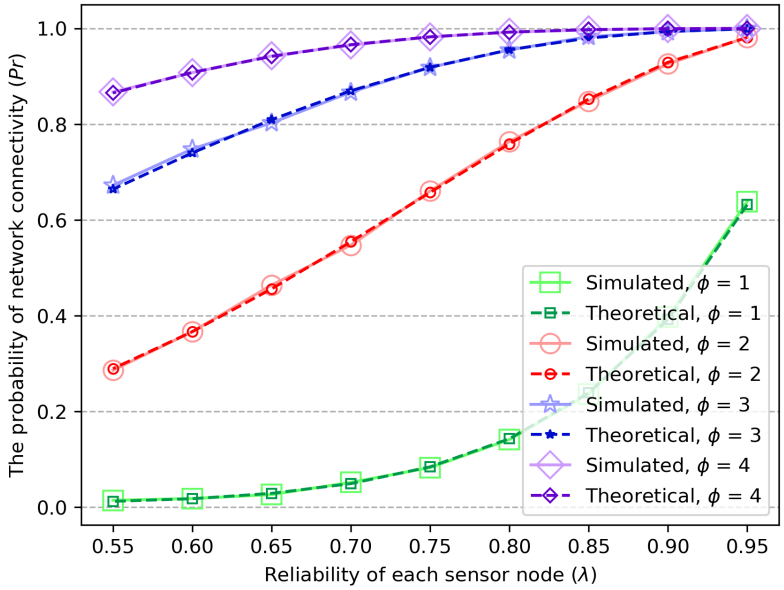



Figure 5.5: The probability of network connectivity with different $\phi$ when $N = 10$

with the increase of $Y$ or with the decrease of $N$. When $N = 2$, the success rate is always 100% regardless of the rebroadcast delay. The reason is that rebroadcast is not required as all the sensor nodes can receive the broadcasted routing discovery message from the gateway directly when $N = 2$ and $\phi = 2$. As shown in Figure 5.7, when $N$ is fixed at 8 and $\phi$ takes values in the set $\{1, 2, 3, 4\}$, the success rate

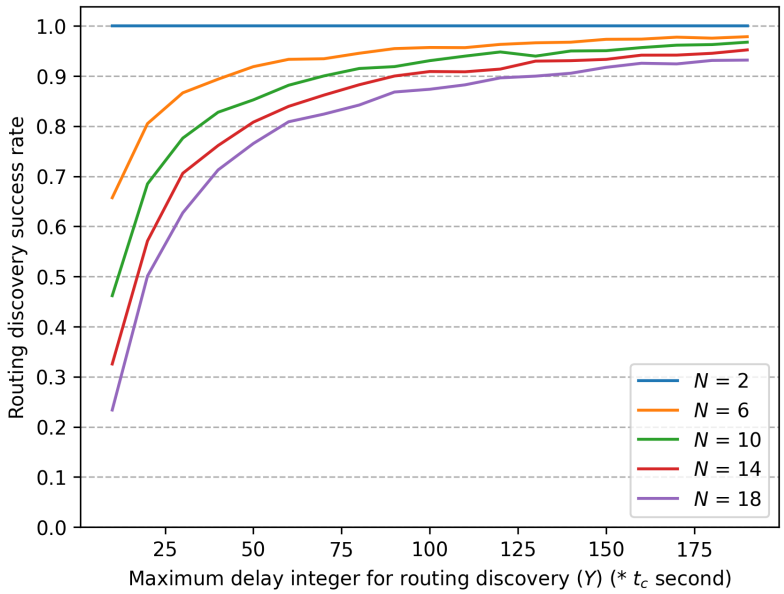



Figure 5.6: Routing discovery success rate with different $N$ when $\boldsymbol{\phi} = 2$

increases either with the increase of $Y$ or with the decrease of $\phi$. When $\phi = 1$, the success rate is always 100% regardless of the rebroadcast delay. The reason is that only one node broadcasts or rebroadcasts a routing discovery message at a time when $\phi = 1$. This is because only one sensor node receives each broadcasted or rebroadcasted routing discovery message, except for another sensor node that has previously received a discovery message with fewer hops and thus discards the current one. In both Figure 5.6 and 5.7, with the increase of $Y$, the success rate exceeds 90%, a high success rate. It can be observed that the worst case is when $\phi = 4$ and $N = 8$. In this case, the minimum $Y$ to achieve the success rate of 90% is around 175 corresponding to a delay of $175t_c$ seconds. The routing discovery packet contains four pieces of information: the initializer identifier, the sender identifier, the number of hops, and the message identifier. If adopting the size allocation method of RadioHead, each piece of information occupies one-byte space. Then, based on (5.7) and (5.9), $t_c = 0.036$ seconds. Thus, $175t_c = 6.318$ seconds which is the maximum delay to obtain a high routing discovery success rate in the worst case.

To trigger a routing discovery process, the gateway needs to receive at least one routing request message. Thus, a routing request process is considered successful if the gateway receives at least one routing request message from the initializer after the initialization of the routing request process. To investigate the routing request

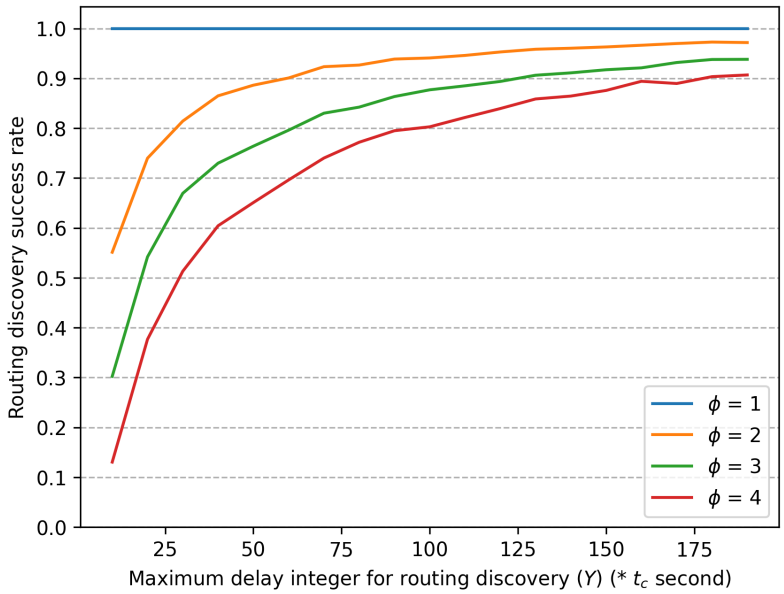



Figure 5.7: Routing discovery success rate with different $\boldsymbol{\phi}$ when $N = 8$

success rate, after placing all the nodes, a node is deleted and a routing discovery process is triggered from the gateway for the left nodes. Note that the topology of the network cannot be the topology of $T$ since one node is deleted. Thus, in this case, the routing discovery process is considered successful if the routing tables of all the sensor nodes follow the rules of minimum hops and worst RSSI which was discussed in Section 5.4. After the routing discovery process, the deleted sensor node is placed back at its previous location and initializes a routing request process. Then, the gateway is observed to determine if the routing request process is successful. In this simulation, $N$ is fixed at 20 since the signal collision arising from the routing request broadcast is only relevant to the nodes receiving the broadcast request and is independent of the total number of sensor nodes. The values for $\phi$ and $X$ vary, and the simulation is repeated 50,000 times for each set of these parameters to obtain the routing request success rate. The results are classified into two groups according to if the routing discovery is successful. As shown in Figure 5.8, if the routing discovery is successful, the routing request success rate is 100% regardless of the maximum delay integer for routing request $X$ and $\phi$. If the routing discovery fails, the routing request success rate decreases with the increase of $\phi$. For $\phi = 1$, the routing request success rate is 100% regardless of the random delay value. For $\phi \in \{2, 3, 4, 5\}$, the routing request success rate increases with the increase of $X$.

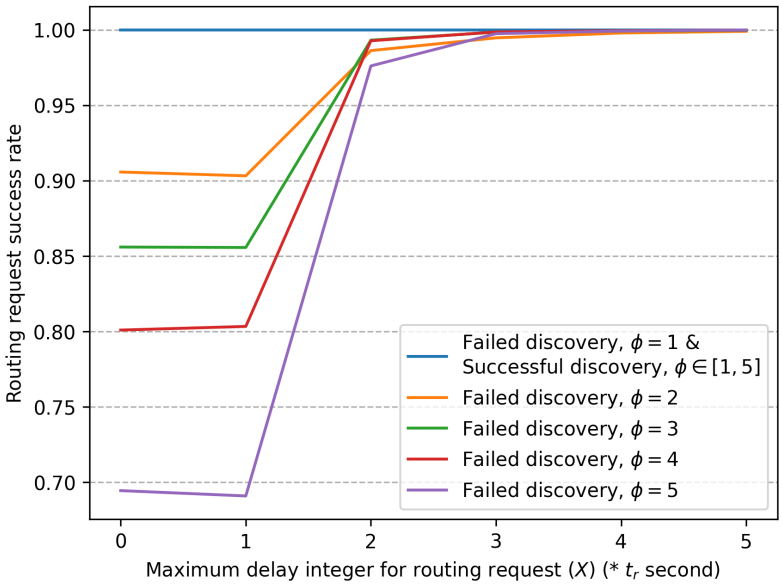



Figure 5.8: Routing request success rate with different $\phi$ when $N = 20$

When $X \geq 3$, the routing request success rate approaches 100% regardless of $\phi$ and the routing discovery result. Thus, a very small random delay can resolve the signal collision arising from the routing request broadcast.

Note that only the case with successful routing discovery is considered in the following subsection.

### 5.5.3 Scalability and Coverage Extension Ratio Verification

This subsection will evaluate the duty cycle of the LoRa mesh network, and verify the performance of the proposed routing algorithm and the bounds of scalability and coverage extension ratio.

#### 5.5.3.1 Duty Cycle Evaluation

Before demonstrating the scalability and coverage extension ratio of the network, LoRaMeshSim is utilized to analyze the duty cycle of each node and evaluate how it affects the scalability and coverage extension ratio. The parameters $\phi$ and $L_d$ are fixed at 2 and 50, respectively. The values for $N$ vary and the simulation is conducted only once, with a duration of 24 hours for each value of $N$. The duty cycle of each node is calculated and the results are shown in Figure 5.9. The simulation validates Lemma 1, i.e., one of the adjacent nodes has the maximum duty cycle in the sensor

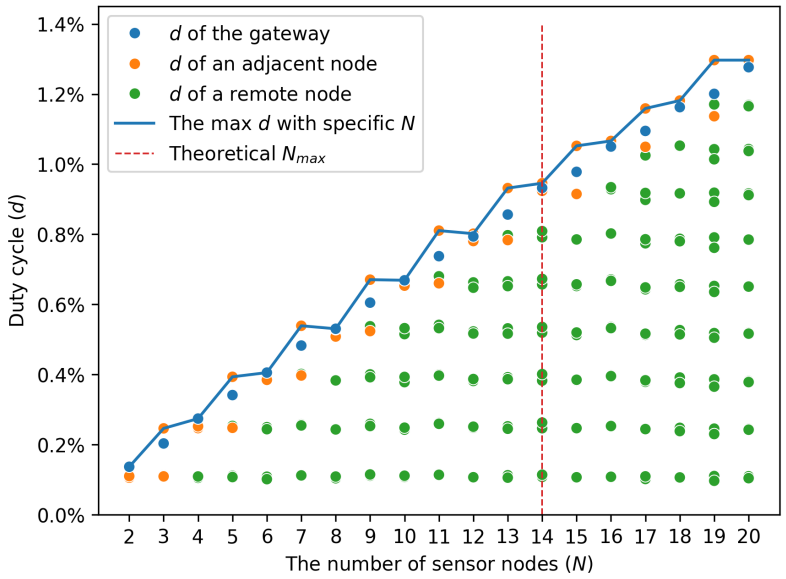



Figure 5.9: Duty cycle and the maximum number of sensor nodes of the proposed routing algorithm

nodes. Moreover, either the gateway or an adjacent node has the maximum duty cycle in the network. Since the proposed routing algorithm evenly allocates the relay burdens to the two adjacent nodes, their duty cycles are close to each other. With the increase of $N$, the maximum duty cycle of the network increases. It does not exceed 1.0% until $N$ exceeds 14. Thus, to comply with the duty cycle regulation, the maximum number of sensor nodes is 14, aligning with the theoretical $N_{\max}$ given in (5.16). By contrast, using Andrei Broder and David Alduous algorithm [208] [209], a random spanning tree of the graph $G$ is generated as the topology of the network to replace the proposed routing algorithm. As shown in Figure 5.10, the simulation with the topology of a random spanning tree is repeated. In this case, Lemma 1 still holds. However, the gap between the duty cycles of the two adjacent nodes significantly expands due to the unevenly allocated relay burden. Consequently, there is a significant increase in the duty cycle of an adjacent node, resulting in a significant increase in the maximum duty cycle of the network. To comply with the duty cycle regulation, the maximum number of sensor nodes drops to 7. In the following simulations on scalability, $N_{\max}$ is determined by conducting an experiment with $N = 2$ and then increasing $N$ until the maximum duty cycle exceeds 1%.

To illustrate the coverage extension ratio, the simulation of Figure 5.9 is repeated 100 times, given that the sensor nodes are randomly located. To reduce the

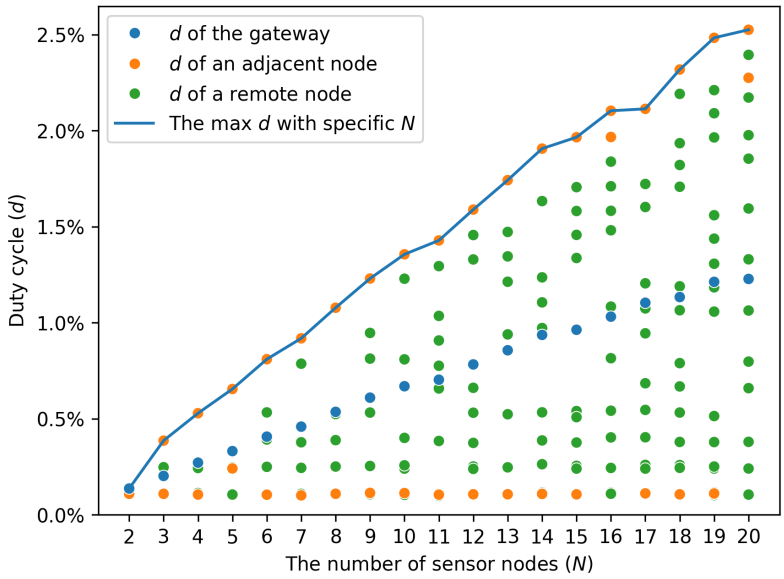



Figure 5.10: Duty cycle and the maximum number of sensor nodes of a random spanning tree

number of repeats required to find the maximum coverage extension ratio, $c$, beta distribution with parameters $\alpha = 0.005$ and $\beta = 0.018$ is employed, instead of uniform distribution, to place the sensor nodes. As shown in Figure 5.11, $c$ varies in a range for a specific $N$. The maximum $c$ increases with the increase of $N$ and the maximum duty cycle does not exceed 1.0% until $N$ exceeds 14. Thus, the maximum $c$ of the network is the maximum $c$ when $N = 14$. The value of the maximum $c$ aligns with the theoretical maximum $c$ given in (5.19). In the following simulations on the coverage extension ratio, the same beta distribution will be used for sensor node placement to reduce the number of repeated experiments. Moreover, unlike in this simulation, the maximum $c$ is determined by first identifying $N_{\max}$ and then repeating the experiment only for $N = N_{\max}$.

#### 5.5.3.2 Routing Performance Verification

The simulation will verify that the proposed routing algorithm enables the network to reach the upper bounds of $N$ and $c$. To obtain simulated $N_{\max}$, the values for $p$, $L_d$, and $\phi$ vary, and the simulations are conducted by increasing $N$ for each set of these parameters. As shown in Figure 5.12, when $\phi$ is fixed at 2, $N_{\max}$ decreases either with the increase of $p$ or with the increase of $L_d$. There is a sharp drop of $N_{\max}$ when $p$ increases from 1 to 10. For better display in simulations, the unit of $p$

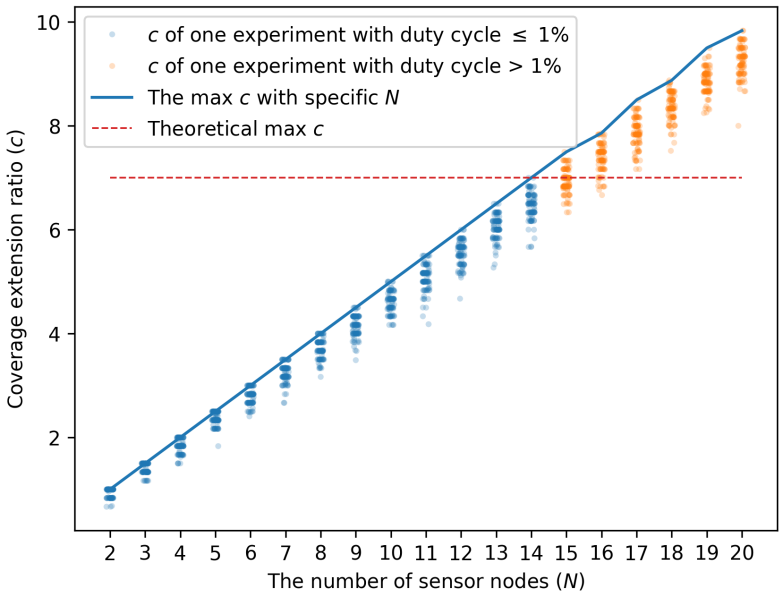



Figure 5.11: Duty cycle and the coverage extension ratio of the proposed routing algorithm

is set as packets per hour per node, which differs from packets per second per node in Section 5.3.

Given that the differences in $N_{\max}$ between different $L_d$ values become smaller when $p$ exceeds 10, this part is zoomed in for a clearer display. As shown in Figure 5.13, when $L_d$ is fixed at 60, $N_{\max}$ decreases with the increase of $p$, following the same trend of Figure 5.12. $N_{\max}$ increases with the increase of $\phi$ until $\phi$ reaches 4. The theoretical $N_{\max}$ when $\phi = 3$ exactly matches the one when $\phi = 4$.

After obtaining the simulated $N_{\max}$, they are used to search for the simulated maximum coverage extension ratio, $c$. As shown in Figure 5.14, when $\phi$ is fixed at 2, the maximum $c$ decreases either with the increase of $p$ or with the increase of $L_d$. As shown in Figure 5.15, when $L_d$ is fixed at 60, the maximum $c$ decreases with the increase of $p$, following the same trend of Figure 5.14. The maximum $c$ increases with the decrease of $\phi$ until $\phi$ drops to 1. The theoretical maximum $c$ when $\phi = 1$ closely matches the one when $\phi = 2$, with any differences attributed to the floor function in (5.16).

From these figures, it is evident that the simulated results closely match the theoretical results, proving that the network attains the upper bounds of $N$ and $c$. To measure the difference, the Mean Absolute Percentage Error (MAPE) metric is

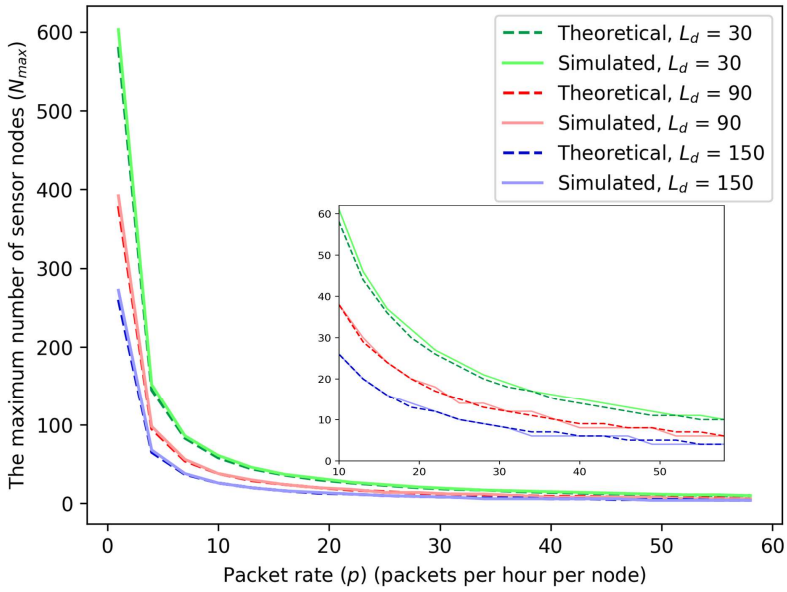



Figure 5.12: The maximum number of sensor nodes with different $L_d$ when $\phi = 2$

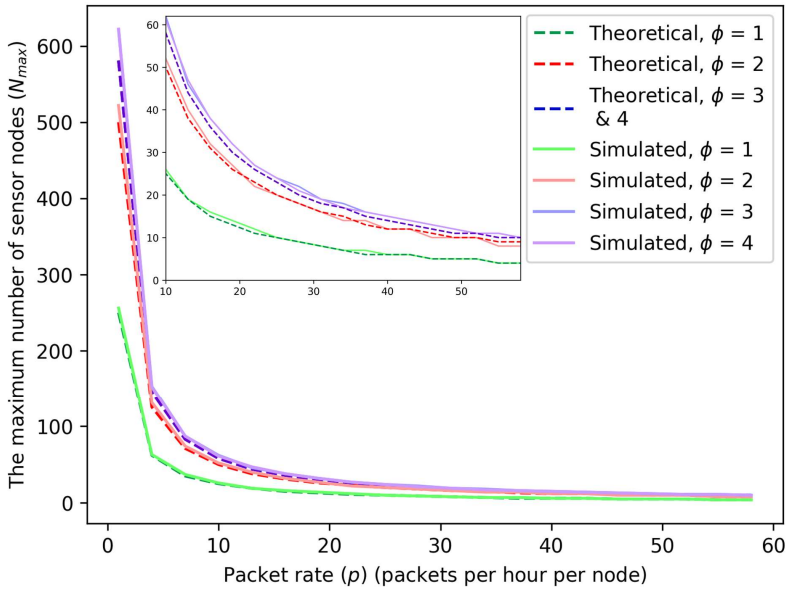



Figure 5.13: The maximum number of sensor nodes with different $\phi$ when $L_d = 60$

employed, which is defined as:

$$MAPE = \frac{1}{\delta}\sum_{i=1}^{\delta}\left|\frac{A_i - B_i}{A_i}\right| \tag{5.20}$$

where $A_i$ is the theoretical value, $B_i$ is the simulated value, and $\delta$ is the number

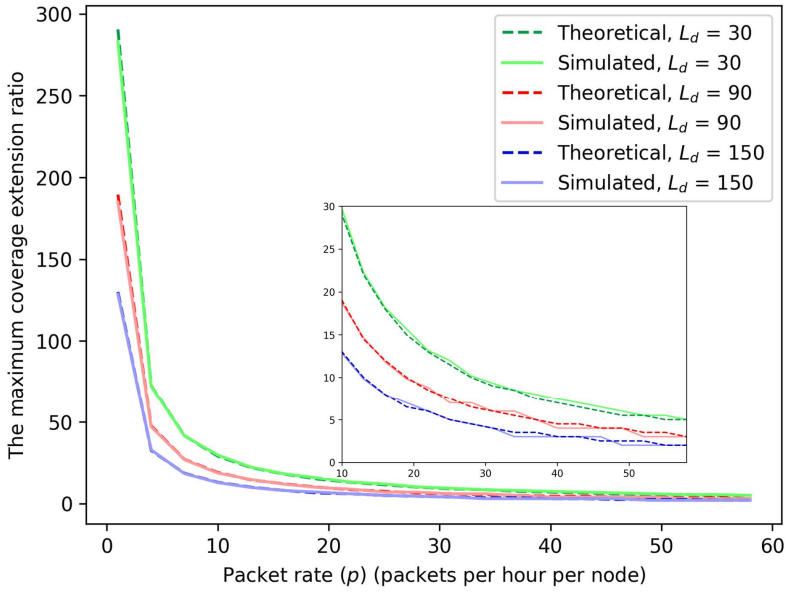



Figure 5.14: The maximum coverage extension ratio with different $L_d$ when $\phi = 2$

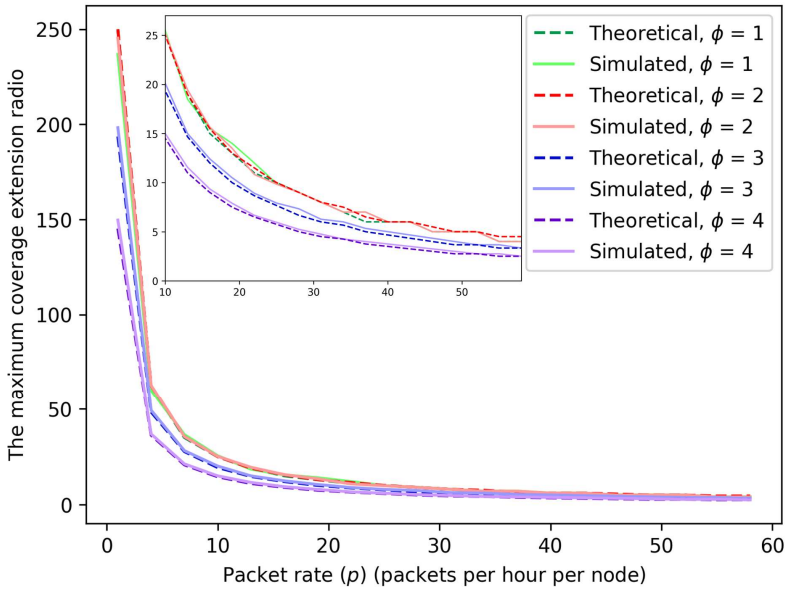



Figure 5.15: The maximum coverage extension ratio with different $\phi$ when $L_d = 60$

of values. MAPE between theoretical values and simulated values in Figure 5.12, 5.13, 5.14, and 5.15 is listed in Table 5.2. The error arises from two aspects: 1) The simulation duration of 24 hours may not be sufficient to eliminate the randomness in the data collection of each sensor node. 2) Signal collisions are not considered when deriving theoretical $N_{\max}$ and $c$, but they are simulated in LoRaMeshSim.

Table 5.2: MAPE between theoretical values and simulated values.

| | Figure 5.12 | Figure 5.13 | Figure 5.14 | Figure 5.15 |
|---|---|---|---|---|
| $L_d = 30$ | 5.0% | / | 3.6% | / |
| $L_d = 90$ | 4.7% | / | 4.4% | / |
| $L_d = 150$ | 5.4% | / | 5.1% | / |
| $\phi = 1$ | / | 2.7% | / | 2.8% |
| $\phi = 2$ | / | 4.0% | / | 3.2% |
| $\phi = 3$ | / | 6.0% | / | 4.8% |
| $\phi = 4$ | / | 5.4% | / | 4.5% |

#### 5.5.3.3 Bounds Verification

In (5.16), $N_{\max}$ has a upper bound and a lower bound when $\theta = \phi$ and 1, respectively. This implies that the values of $N_{\max}$ are between the two bounds regardless of the routing algorithms. To verify it, a straightforward method is to exhaust the possible topologies, i.e., all the spanning trees of graph $G$. However, the number of spanning trees grows exponentially with the increase of $N$. For example, according to Kirchhoff's theorem [210], when $\phi = 2$, the number of spanning trees of graph $G$ is 6,765 and 102,334,155, respectively, for $N = 10$ and $N = 20$. On the other hand, to determine the maximum duty cycle for each spanning tree, it is necessary to set the simulation time to at least several hours—a task that takes seconds for code execution. Thus, the exhaustive search method is impossible to realize. Alternatively, a random search method is proposed using the Andrei Broder and David Alduous random spanning tree generation algorithm. As shown in the Algorithm 3, to obtain the upper bound, an incremental search is conducted starting from $N = 2$ until a maximum duty cycle of less than 1% is no longer found. To obtain the lower bound, a decremental search is conducted starting from $N$ equal to the upper bound until a maximum duty cycle of greater than 1% is no longer found. To reduce the execution time, the simulation time is reduced from 24 hours to 5 hours and 12 hours for the upper bound and lower bound, respectively. As shown in Figure 5.16, the simulated bounds match the theoretical bounds with tolerable errors listed in Table 5.3. Moreover, simulations with the proposed routing algorithm and RadioHead are also conducted. In the simulation of RadioHead, collisions of routing broadcasts are intentionally disregarded to minimize interference from other factors. As shown in Figure 5.16, $N_{\max}$ of RadioHead lies on the lower bound due to uneven relay task assignments. By contrast, the proposed routing algorithm achieves the

**Algorithm 3** Random Search for the Bounds of $N_{\max}$

```
IF search for upper bound
  INPUT: search times = 2000
  INITIALIZATION: N = 2, i = 0
      WHEN i < search times
          Generate a random spanning tree
          Conduct a simulation using the tree
          If the maximum duty cycle ≤ 1%
              N+ = 1, i = 0
          ELSE
              i+ = 1
  OUTPUT: N − 1
ELSE IF search for lower bound
  INPUT: search times = 1000
  INITIALIZATION: N = the upper bound, i = 0
      WHEN i < search times AND N > 0
          Generate a random spanning tree
          Conduct a simulation using the tree
          If the maximum duty cycle > 1%
              N− = 1, i = 0
          ELSE
              i+ = 1
  OUTPUT: N
```

upper bound of $N_{\max}$, highlighting its advantage over other routing algorithms.

After verifying the bounds of $N_{\max}$, the simulated $N_{\max}$ is used to verify the bounds of the maximum $c$ indicated in (5.19). To obtain the lower bound of the maximum $c$, the simulated lower bound of $N_{\max}$ is set as $N$ and the simulation is repeated 100 times with random spanning trees as the topology. For the upper bound, the simulated upper bound of $N_{\max}$ is set as $N$ and the simulations with random spanning trees are repeated until a topology is found with a maximum duty cycle less than 1%. Employing the found topology, the simulation is repeated 100 times to obtain the upper bound of the maximum $c$. Moreover, simulations with the proposed routing algorithm and RadioHead in terms of the maximum $c$ are also conducted. As shown in Figure 5.17, the simulated lower bound matches the theoretical lower bound and RadioHead also lies on the theoretical lower bound due to uneven relay task assignments. By contrast, the simulated upper bound and the proposed routing algorithm match the theoretical upper bound. The errors are also listed in Table 5.3. This demonstrates the correctness of the theoretical bounds for

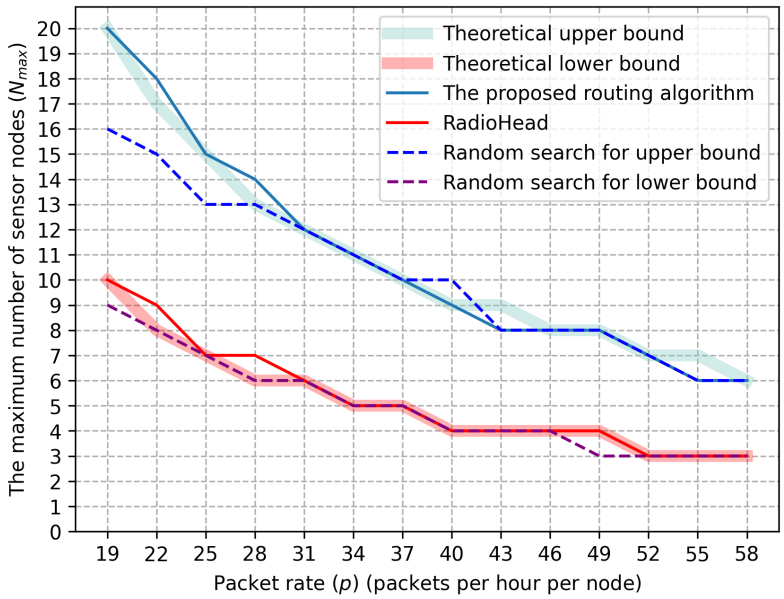



Figure 5.16: The bounds of $N_{\max}$

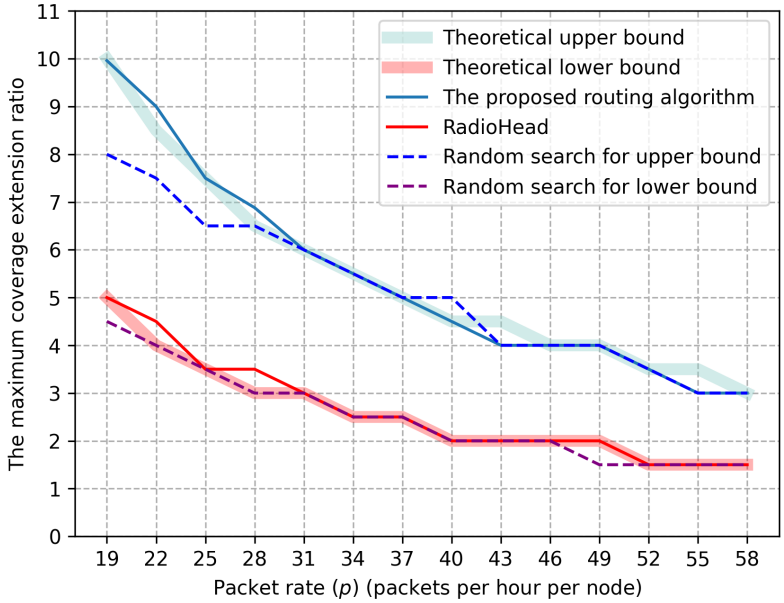



Figure 5.17: The bounds of the maximum $c$

the maximum $c$ and underscores the advantage of the proposed routing algorithm over others in terms of the maximum $c$.

Table 5.3: MAPE between theoretical bounds and simulated bounds.

| | | Theoretical Upper Bound | Theoretical Lower Bound |
|---|---|---|---|
| $N_{\max}$ | Proposed Routing Algorithm | 2.7837% | / |
| | Random Search for Upper bound | 5.8290% | / |
| | RadioHead | / | 2.0833% |
| | Random Search for lower bound | / | 2.5000% |
| maximum $c$ | Proposed Routing Algorithm | 2.6813% | / |
| | Random Search for Upper bound | 5.8293% | / |
| | RadioHead | / | 2.0833% |
| | Random Search for lower bound | / | 2.5000% |

## 5.6 Summary

This chapter contributes to the understanding of deploying LoRa mesh networks for monitoring linear infrastructure, offering insights into fault tolerance, reliability, scalability, and coverage extension. The proposed deployment strategy optimizes the placement of nodes, ensuring effective and reliable coverage along linear infrastructure while adhering to duty cycle regulations. The system analysis also reveals the impact of duty cycle limitations on network scalability and coverage extension ratio. Moreover, their bounds are derived with the condition to reach the upper bounds. The proposed routing algorithm demonstrates its efficacy in achieving maximum scalability and coverage extension ratios. The developed LoRa mesh simulator validates the proposed system analysis and routing algorithm, providing a valuable tool for further research and practical implementation. This work facilitates the design and deployment of robust LoRa mesh networks for monitoring linear infrastructure, addressing the challenges associated with scalability and coverage extension.

# Chapter 6

# Conclusions and Future Works

In this chapter, the contributions of this thesis are summarized. Moreover, some concluding remarks and future research directions are discussed.

## 6.1 Thesis Summary

Based on the comprehensive exploration and experimentation presented in the preceding chapters, the integration of unlicensed LPWA technologies, particularly LoRaWAN and LoRa mesh networks, into the 5G ecosystem emerges as a promising avenue with vast implications for various applications, such as smarting building, trackside weather monitoring, and linear infrastructure monitoring. The research journey embarked upon in this thesis has been multifaceted, tackling integration challenges, proposing novel architectures, developing a routing algorithm, and addressing practical considerations in deployment and operation, especially reliability, scalability, and coverage.

In addressing the first objective described in Section 1.2, a thorough survey of unlicensed LPWAN-5G integration was conducted in Chapter 2. It compares nine popular LPWA technologies, including both cellular and non-cellular LPWANs, while also highlighting the significance of mesh technologies in extending coverage. Through comparison, LoRaWAN and LoRa mesh are the most promising technologies and have the potential to integrate into a 5G network. Additionally, the chapter underscored the imperative of addressing key challenges such as hybrid architectures, security, mobility, and interoperability, all of which are vital for seamless integration.

The second objective, centered around the development of a hybrid architecture for LoRaWAN-5G integration, was effectively realized in Chapter 3. By leveraging collaborative RAN and converged core network architectures, the chapter demonstrated the efficacy of the proposed solution in real-world scenarios. Notably, the deployment on the Glasgow 5G testbed and the application in upgrading the heating system underscored the viability and benefits of the integration approach.

Expanding upon this foundation, Chapter 4 introduced a LoRa mesh-5G integrated network tailored for trackside smart weather monitoring, addressing the third objective about the framework and algorithms for LoRa mesh-5G integration. This innovative approach not only reduced communication infrastructure costs but also facilitated the integration of artificial intelligence through a cloud-edge-terminal architecture. The chapter's emphasis on intelligent algorithms and proof of concept experimentation reinforced the robustness and applicability of the proposed solution.

Chapter 5 further extended the discourse by focusing on the deployment of LoRa mesh networks for monitoring linear infrastructure. Through meticulous analysis and algorithmic design, the chapter elucidated strategies for optimizing coverage, reliability, and scalability while adhering to regulatory constraints, addressing the fourth objective about the routing algorithm design and network performance enhancement. The proposed routing algorithm and simulation framework provided valuable insights for practical deployment and scalability assessment.

Collectively, these chapters constitute a comprehensive exploration of LPWAN-5G integration, encompassing technological, architectural, and practical dimensions. They successfully address all the objectives outlined in Section 1.2. The findings underscore the immense potential of such integration in enabling diverse applications spanning smart cities, linear infrastructure monitoring, and beyond. While challenges remain, the insights gleaned from this research serve as a robust foundation for future advancements in the realm of hybrid industrial IoT enterprise wireless networks.

Through the course of this research, two valuable lessons have been gleaned. Firstly, the importance of interdisciplinary collaboration cannot be overstated, as the successful integration of diverse technologies requires expertise spanning multiple domains. Additionally, such complex integration work involves numerous aspects, e.g., architecture, security, and mobility. While it's impractical for researchers to address all of these aspects comprehensively within a single study, it's crucial to recognize their interrelation. Moving forward, leveraging these lessons will be

paramount in driving further innovation and realizing the full potential of hybrid wireless networks in the era of Industry 4.0 and beyond.

## 6.2 Future Work

In this section, future research directions aimed at enhancing the design and management of the proposed hybrid networks in this thesis are discussed.

### 6.2.1 Unified Data Management

As discussed in Chapter 2, 5G and LPWANs employ different databases and data management methods, which has a negative impact on the efficiency, mobility, and security of LPWAN-5G integrated networks. Developing a unified database and corresponding management method holds promise for storing subscription information of both 5G UE and LPWAN end devices. Unlike Option 6 in Table 2.3 requiring dual connectivity, unified data management enables LPWAN end devices without a 5G module to be authenticated as if the LPWAN gateway receiving the join request is connected to a network server residing in the 5G core network, which can retrieve the subscription information of the end device stored in the UDR. End devices roaming in a visited LPWAN network whose gateways have access to the same 5G core network can also be authenticated without the need for a 5G module. Moreover, unified data management can enhance the security of the LPWAN-5G integrated network as it reduces the risk of data exposure when two independent data management entities interact with each other.

### 6.2.2 LoRa Mesh Authentication and Encryption

The LoRa mesh-5G integrated networks proposed in Chapters 4 and 5 overlook the critical aspects of authenticating LoRa mesh nodes and encrypting LoRa mesh packets. However, authentication and encryption are indispensable for ensuring secure communication within a network. Hence, the development of advanced authentication and encryption methods emerges as a crucial avenue for future research to enhance LoRa mesh-5G integrated networks. Regarding authentication, adopting a unified data management approach within the 5G network, as outlined in Section 6.2.1, presents a promising strategy. In terms of encryption methods,

incorporating lightweight techniques and leveraging the encryption systems inherent in 5G represents another viable approach.

### 6.2.3 LoRa Mobility Enhancement

As discussed in Chapter 2, the integration of LoRa and 5G would potentially enable LoRa devices to benefit from the higher bandwidth, lower latency, and seamless handover capabilities offered by 5G networks, while still leveraging the long-range and low-power advantages of LoRa technology. Two key challenges about mobility enhancement will be addressed in future work: 1) Mobility Management: Designing mobility management protocols and algorithms tailored to the characteristics of LoRa devices, such as their intermittent connectivity and low data rate transmissions. This includes optimizing handover decision-making processes, managing mobility-related signaling overhead, and minimizing energy consumption in mobile LoRa devices. 2) Network Slicing: Exploring the concept of network slicing in 5G networks to allocate dedicated resources and network slices for LoRa devices with specific mobility requirements. This could involve dynamically adjusting network parameters such as modulation schemes, transmission power, or data rates based on the mobility patterns of LoRa devices.

# Appendices

## A Proof of Equation (5.3)

According to the definition of the vertex connectivity, $k(G) = \phi$ is equivalent to

$$\text{For } |V| = \phi, \exists V \subset S, G - V \text{ is not connected} \tag{1a}$$

$$\text{For } |V| = \phi - 1, \forall V \subset S, G - V \text{ is connected} \tag{1b}$$

Let $G'(S', E')$ denote the graph $G - V$, where $S^{'} = S - V$ and $E' = \{(s_i, s_j) \mid s_i, s_j \in S' \text{ and } j - i \in (0, \phi]\}$. For $|V| = \phi$, a set $V = \{s_2, s_3, ..., s_{\phi+1}\}$ can be found, making $\forall s_j \in S', (s_1, s_j) \notin E'$ as $j - 1 \notin (0, \phi]$. This means that there is no route between $s_1$ and other nodes, i.e., $G'$ is not connected. Equation (1a) is proved.

For $|V| = \phi - 1, V = \{s_i \mid i \in U\}$ where $U = \{u_i \mid i \in [1, \phi - 1] \cap \mathbb{Z} \text{ and } u_i \in [1, N + 1] \cap \mathbb{Z}\}$. Renumber the nodes in $G'$ by defining a number-conversion function

$$f(i) = \begin{cases} i + |U_{1,i}|, & \text{for } i + 1 \notin U \\ i + |U_{1,i}| + 1, & \text{for } i + 1 \in U \text{ and } i + 2 \notin U \\ i + |U_{1,i}| + 2, & \text{for } i + 1, i + 2 \in U \text{ and } i + 3 \notin U \\ ... & \\ i + |U_{1,i}| + \phi - 1, & \text{for } i + 1, i + 2, ..., i + \phi - 1 \in U \\ & \text{and } u_{i+\phi} \notin U, \end{cases}$$

where $U_{i,j} = \{u_k \mid u_k \in U \cap [i, j]\}$. The graph $G'$ is equivalent to graph $G''(S'', E'')$, where $S'' = \{s''_i \mid i \in [1, N - \phi + 2] \cap \mathbb{Z}\}$ and $E'' = \{(s''_i, s''_j) \mid i, j \in [1, N - \phi + 2] \cap$

$\mathbb{Z}$ and $f(j) - f(i) \in (0, \phi]\}$. $\forall i \in [1, N - \phi + 1] \cap \mathbb{Z}$,

$$f(i+1) - f(i) = \begin{cases} |U_{i+1,i+1}|, & \text{for } i+1 \in U \\ 1 + |U_{i+1,i+1}|, & \text{for } i+1, i+2 \notin U \\ 1 + |U_{i+1,i+1}| + 1, & \text{for } i+1, i+3 \notin U \text{ and } i+2 \in U \\ 1 + |U_{i+1,i+1}| + 2, & \text{for } i+1, i+4 \notin U \text{ and } i+2, i+3 \in U \\ ... & \\ 1 + |U_{i+1,i+1}| + \phi - 1, & \text{for } i+1, i+\phi+1 \notin U \text{ and } i+2, i+3, ..., i+\phi \in U, \end{cases}$$

$$= \begin{cases} 1, & \text{for } i+1 \in U \\ 1, & \text{for } i+1, i+2 \notin U \\ 2, & \text{for } i+1, i+3 \notin U \text{ and } i+2 \in U \\ 3, & \text{for } i+1, i+4 \notin U \text{ and } i+2, i+3 \in U \\ ... & \\ \phi, & \text{for } i+1, i+\phi+1 \notin U \text{ and } i+2, i+3, ..., i+\phi \in U, \end{cases}$$

i.e., $f(i+1) - f(i) \in (0, \phi]$. Thus, $\forall i \in [1, N - \phi + 1] \cap \mathbb{Z}, (s''_i, s''_{i+1}) \in E''$. Then, $G''$ is connected as $\forall s''_i, s''_j \in S''$ and $i < j$, there is at least one connected route between them, i.e., $s_i, s_{i+1}, ..., s_j$. Equation (1b) is proved. Therefore, equation (5.3) is proved.

# B Proof of Theorem 1

Assuming $|V| = \phi$ where $\phi \in [1, N+1) \cap \mathbb{Z}$. Then, $V = \{s_i \mid i \in U\}$ where $U = \{u_i \mid i \in [1, \phi] \cap \mathbb{Z} \text{ and } u_i \in [1, N+1] \cap \mathbb{Z}\}$. $\forall i \in [1, N-\phi] \cap \mathbb{Z}$,

$$f(i+1) - f(i) = \begin{cases} 1, & \text{for } i+1 \in U \\ 1, & \text{for } i+1, i+2 \notin U \\ 2, & \text{for } i+1, i+3 \notin U \text{ and } i+2 \in U \\ 3, & \text{for } i+1, i+4 \notin U \text{ and } i+2, i+3 \in U \\ ... & \\ \phi+1, & \text{for } i+1, i+\phi+1 \notin U \text{ and } i+2, i+3, ..., i \\ & +\phi+1 \in U. \end{cases}$$

If $\phi + 1 \leq \phi$, then $f(i+1) - f(i) \in (0, \phi]$. According to the proof of (5.3), G-V is connected. In the case of $\phi + 1 > \phi$, if $\forall i \in [1, N-\phi+2]$, $\{s_i, s_{i+1}, ..., s_{i+\phi-1}\} \nsubseteq V$, then

$$f(i+1) - f(i) = \begin{cases} 1, & \text{for } i+1 \in U \\ 1, & \text{for } i+1, i+2 \notin U \\ 2, & \text{for } i+1, i+3 \notin U \text{ and } i+2 \in U \\ 3, & \text{for } i+1, i+4 \notin U \text{ and } i+2, i+3 \in U \\ ... & \\ \phi, & \text{for } i+1, i+\phi+1 \notin U \text{ and } i+2, i+3, ..., i+\phi \\ & \in U, \end{cases}$$

i.e., $f(i+1) - f(i) \in (0, \phi]$. According to the proof of (5.3), It can be derived again that G-V is connected. Therefore, Theorem 1 is proved.

# C Proof of Lemma 1

The lemma can be proved using a proof of contradiction. Assume that a remote node has the maximum duty cycle in the sensor nodes, denoted as $\max(d_i)$. According to (5.6),

$$\max(d_i) = [\max(n_i) + 1]pt_d + \max(n_i)pt_a, \tag{2}$$

where $\max(n_i)$ denotes the number of sensor nodes whose data packets are relayed by the remote node. The data packets of the remote node have to be relayed by an

adjacent node to reach the gateway. All the nodes whose data packets are relayed by the remote nodes also require the adjacent node to relay data packets subsequently. Additionally, the adjacent node also relays the data packets generated in the remote node. Thus, the adjacent node relays data packets for at least $\max(n_i) + 1$ nodes and its duty cycle is not less than $[\max(n_i) + 2]pt_d + [\max(n_i) + 1]pt_a$ which is bigger than $\max(d_i)$. This contradicts the assumption, so Lemma 1 holds.

# Bibliography


[1] L. S. Dalenogare, G. B. Benitez, N. F. Ayala, and A. G. Frank, "The expected contribution of Industry 4.0 technologies for industrial performance," *International Journal of Production Economics*, vol. 204, pp. 383–394, 2018.

[2] "LPWAN Market Report 2021-2026," IoT Analytics, Oct. 2021. Accessed: Mar. 4, 2024. [Online], available: https://iot-analytics.com/product/lpwan-market-report-2021-2026/.

[3] F. Z. Yousaf, M. Bredel, S. Schaller, and F. Schneider, "NFV and SDN—Key technology enablers for 5G networks," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2468–2478, 2017.

[4] Y. Chen, Y. A. Sambo, O. Onireti, and M. A. Imran, "A survey on LPWAN-5G integration: Main challenges and potential solutions," *IEEE Access*, vol. 10, pp. 32 132–32 149, 2022.

[5] 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, 2020.

[6] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT system for M2M communication," in *2016 IEEE Wireless Communications and Networking Conference*. IEEE, 2016, pp. 1–5.

[7] "Evolved universal terrestrial radio access (E-UTRA); NB-IoT; technical report for BS and UE radio transmission and reception," Standard TR 36.802, Release 13, 3GPP, 2016.

[8] A. Adhikary, X. Lin, and Y.-P. E. Wang, "Performance evaluation of NB-IoT coverage," in *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*. IEEE, 2016, pp. 1–5.

[9] S. Landström, J. Bergström, E. Westerberg, and D. Hammarwall, "NB-IoT: A sustainable technology for connecting billions of devices," *Ericsson Technology Review*, vol. 4, pp. 2–11, 2016.

[10] J. Oh and H. Song, "Study on the effect of LTE on the coexistence of NB-IoT," in *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE, 2018, pp. 610–612.

[11] R. Ratasuk, N. Mangalvedhe, A. Ghosh, and B. Vejlgaard, "Narrowband LTE-M system for M2M communication," in *2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall)*. IEEE, 2014, pp. 1–5.

[12] R. Ratasuk, D. Bhatoolaul, N. Mangalvedhe, and A. Ghosh, "Performance analysis of voice over LTE using low-complexity eMTC devices," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*. IEEE, 2017, pp. 1–5.

[13] P. Jörke, R. Falkenberg, and C. Wietfeld, "Power consumption analysis of NB-IoT and eMTC in challenging smart city environments," in *2018 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2018, pp. 1–6.

[14] K. Xu, J. Liu, and J. Lu, "Research and Realization on Smart City Applications Based on eMTC wireless communication technology," in *Journal of Physics: Conference Series*, vol. 1757, no. 1. IOP Publishing, 2021, p. 012178.

[15] J. Finnegan and S. Brown, "A comparative survey of LPWA networking," *arXiv preprint arXiv:1802.04222*, 2018.

[16] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT express*, vol. 5, no. 1, pp. 1–7, 2019.

[17] 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)*. IEEE, 2018, pp. 197–202.

[18] S. Lippuner, B. Weber, M. Salomon, M. Korb, and Q. Huang, "EC-GSM-IoT network synchronization with support for large frequency offsets," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2018, pp. 1–6.

[19] "LoRaWAN specification 1.1," LoRa Alliance, 2017.

[20] J. Haxhibeqiri, E. De Poorter, I. Moerman, and J. Hoebeke, "A survey of LoRaWAN for IoT: From technology to application," *Sensors*, vol. 18, no. 11, p. 3995, 2018.

[21] D. Bankov, E. Khorov, and A. Lyakhov, "On the limits of LoRaWAN channel access," in *2016 International Conference on Engineering and Telecommunication (EnT)*. IEEE, 2016, pp. 10–14.

[22] J. P. S. 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, 2019.

[23] S. Böcker, C. Arendt, P. Jörke, and C. Wietfeld, "LPWAN in the context of 5G: Capability of LoRaWAN to contribute to mMTC," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. IEEE, 2019, pp. 737–742.

[24] "LoRa Technology: Ecosystem, Applications and Benefits," Semtch. Accessed: Mar. 17, 2022. [Online], available: https://info.semtech.com/ecosystem_benefits_white_paper_download.

[25] "LoRaWAN 1.1 regional parameters," LoRa Alliance, 2017.

[26] 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)*. IEEE, 2015, pp. 55–59.

[27] L. Casals, B. Mir, R. Vidal, and C. Gomez, "Modeling the energy performance of LoRaWAN," *Sensors*, vol. 17, no. 10, p. 2364, 2017.

[28] "Sigfox," Sigfox. Accessed: Mar. 4, 2024. [Online], available: http://www.sigfox.com.

[29] "Low throughput networks (LTN); functional architecture," ETSI GS LTN 002 V1.1.1, ETSI , 2014.

[30] A. Mathur, M. R. Bhatnagar, and B. K. Panigrahi, "On the performance of a PLC system assuming differential binary phase shift keying," *IEEE Communications Letters*, vol. 20, no. 4, pp. 668–671, 2016.

[31] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovács, P. Mogensen, and M. Sorensen, "Coverage and capacity analysis of Sigfox, LoRa, GPRS, and NB-IoT," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*. IEEE, 2017, pp. 1–5.

[32] M. Lauridsen, H. Nguyen, B. Vejlgaard, I. Z. Kovacs, P. Mogensen, and M. Sorensen, "Coverage comparison of GPRS, NB-IoT, LoRa, and SigFox in a 7800 $km^2$ area," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*. IEEE, 2017, pp. 1–5.

[33] C. Gomez, J. C. Veras, R. Vidal, L. Casals, and J. Paradells, "A Sigfox energy consumption model," *Sensors*, vol. 19, no. 3, p. 681, 2019.

[34] "RPMA," Ingenu Tech. Accessed: Mar. 4, 2024. [Online], available: https://www.ingenu.com/technology/rpma/.

[35] T. J. Myers, D. T. Werner, K. C. Sinsuan, J. R. Wilson, S. L. Reuland, P. M. Singler, and M. J. Huovila, "Light monitoring system using a random phase multiple access system," Jul. 2 2013, uS Patent 8,477,830.

[36] Q. Tang, L. Yang, G. B. Giannakis, and T. Qin, "Battery power efficiency of PPM and FSK in wireless sensor networks," *IEEE Transactions on wireless Communications*, vol. 6, no. 4, pp. 1308–1319, 2007.

[37] W. Hassan, M. Føre, J. B. Ulvund, and J. A. Alfredsen, "Internet of Fish: Integration of acoustic telemetry with LPWAN for efficient real-time monitoring of fish in marine farms," *Computers and Electronics in Agriculture*, vol. 163, p. 104850, 2019.

[38] H. Saleem, M. Z. A. Khan, and S. Afzal, "Review of various aspects of radio frequency IDentification (RFID) technology," *IOSR Journal of Computer Engineering (IOSRJCE)*, vol. 8, no. 1, p. 6, 2012.

[39] "Alliance protocol specification v1.2," DASH7. Accessed: Mar. 4, 2024. [Online], available: https://www.dash7-alliance.org/product/dash7-alliance-protocol-specification-v1-2/.

[40] M. Weyn, G. Ergeerts, L. Wante, C. Vercauteren, and P. Hellinckx, "Survey of the DASH7 alliance protocol for 433 MHz wireless sensor communication," *International Journal of Distributed Sensor Networks*, vol. 9, no. 12, p. 870430, 2013.

[41] X. Chen, A. Alghaihab, Y. Shi, D. S. Truesdell, B. H. Calhoun, and D. D. Wentzloff, "A crystal-less BLE transmitter with clock recovery from GFSK-modulated BLE packets," *IEEE Journal of Solid-State Circuits*, vol. 56, no. 7, pp. 1963–1974, 2021.

[42] "Weightless," Weightless. Accessed: Mar. 4, 2024. [Online], available: http://www.weightless.org/.

[43] "Weightless-N system specification v1.0," Weightless, 2015, Cambridge, UK.

[44] R. A. Abbas, A. Al-Sherbaz, A. Bennecer, and P. Picton, "A new channel selection algorithm for the weightless-n frequency hopping with lower collision probability," in *2017 8th International Conference on the Network of the Future (NOF)*. IEEE, 2017, pp. 171–175.

[45] "Weightless-P system specification v1.0," Weightless, 2015, Cambridge, UK.

[46] "Telensa," Telensa. Accessed: Mar. 4, 2024. [Online], available: http://www.telensa.com/.

[47] "Global smart street lighting smart cities: Market forecast (2019 – 2028)," Telensa. Accessed: Mar. 4, 2024. [Online], available: https://info.telensa.com/market-forecast-2019-2028.

[48] D. Lundell, A. Hedberg, C. Nyberg, and E. Fitzgerald, "A routing protocol for LoRa mesh networks," in *2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*. IEEE, 2018, pp. 14–19.

[49] R. Berto, P. Napoletano, and M. Savi, "A LoRa-based mesh network for peer-to-peer long-range communication," *Sensors*, vol. 21, no. 13, p. 4314, 2021.

[50] "RadioHead," AirSpayce. Accessed: Mar. 4, 2024. [Online], available: https://www.airspayce.com/mikem/arduino/RadioHead/.

[51] H.-C. Lee and K.-H. Ke, "Monitoring of large-area IoT sensors using a LoRa wireless mesh network system: Design and evaluation," *IEEE Transactions on Instrumentation and Measurement*, vol. 67, no. 9, pp. 2177–2187, 2018.

[52] H. Huh and J. Y. Kim, "LoRa-based mesh network for IoT applications," *IEEE 5th World Forum on Internet of Things (WF-IoT)*, vol. 2019, pp. 524–527, 2019.

[53] C. Ebi, F. Schaltegger, A. Rust, and F. Blumensaat, "Synchronous LoRa mesh network to monitor processes in underground infrastructure," *IEEE access*, vol. 7, pp. 57 663–57 677, 2019.

[54] S. Hong, F. Yao, Y. Ding, and S.-H. Yang, "A hierarchy-based energy-efficient routing protocol for LoRa-mesh network," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22 836–22 849, 2022.

[55] P. Tian, C. A. Boano, X. Ma, and J. Wei, "LoRaHop: Multi-hop support for LoRaWAN uplink and downlink messaging," *IEEE Internet of Things Journal*, 2023.

[56] D. Wu and J. Liebeherr, "A low-cost low-power lora mesh network for large-scale environmental sensing," *IEEE Internet of Things Journal*, vol. 10, no. 19, pp. 16 700–16 714, 2023.

[57] "System architecture for the 5G system," Standard TS 23.501 v17.1.1, Release 17, 3GPP, 2021.

[58] J. Liu, M. Sheng, L. Liu, and J. Li, "Network densification in 5G: From the short-range communications perspective," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 96–102, 2017.

[59] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: enabling innovation in campus networks," *ACM SIGCOMM computer communication review*, vol. 38, no. 2, pp. 69–74, 2008.

[60] F. Z. Yousaf, M. Bredel, S. Schaller, and F. Schneider, "NFV and SDN—Key technology enablers for 5G networks," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2468–2478, 2017.

[61] "5G system; principles and guidelines for service definition," Standard TS 29.501 v17.1.0, Release 17, 3GPP, 2021.

[62] "5G system; unified data repository services," Standard TS 29.504 v17.2.0, Release 17, 3GPP, 2021.

[63] A. Pouttu, O. Liinamaa, and G. Destino, "Demo/poster abstract: 5G test network (5GTN)—Environment for demonstrating 5G and IoT convergence during 2018 Korean Olympics between Finland and Korea," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2018, pp. 1–2.

[64] M. W. Kang and Y. W. Chung, "An efficient energy saving scheme for base stations in 5G networks with separated data and control planes using particle swarm optimization," *Energies*, vol. 10, no. 9, p. 1417, 2017.

[65] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196–248, 2019.

[66] R. Fujdiak, K. Mikhaylov, M. Stusek, P. Masek, I. Ahmad, L. Malina, P. Porambage, M. Voznak, A. Pouttu, and P. Mlynek, "Security in low-power wide-area networks: State-of-the-art and development toward the 5G," in *LPWAN Technologies for IoT and M2M Applications*. Elsevier, 2020, pp. 373–396.

[67] S.-Y. Gao, X.-H. Li, and M.-D. Ma, "A malicious behavior awareness and defense countermeasure based on LoRaWAN protocol," *Sensors*, vol. 19, no. 23, p. 5122, 2019.

[68] W.-J. Sung, H.-G. Ahn, J.-B. Kim, and S.-G. Choi, "Protecting end-device from replay attack on LoRaWAN," in *2018 20th International conference on advanced communication technology (ICACT)*. IEEE, 2018, pp. 167–171.

[69] I. Butun, N. Pereira, and M. Gidlund, "Security risk analysis of LoRaWAN and future directions," *Future Internet*, vol. 11, no. 1, p. 3, 2018.

[70] "Security architecture and procedures for 5G System," Standard TS 33.501 V15.5.0, Release 15, 3GPP, 2021.

[71] J. Arkko, V. Lehtovirta, and P. Eronen, "Improved extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA)," No. rfc5448, 2009.

[72] D. Simon, B. Aboba, and R. Hurst, "The EAP-TLS authentication protocol," No. rfc5216, 2008.

[73] J. Zhang, L. Yang, W. Cao, and Q. Wang, "Formal analysis of 5G EAP-TLS authentication protocol using proverif," *IEEE access*, vol. 8, pp. 23 674–23 688, 2020.

[74] S. Chacko and M. D. Job, "Security mechanisms and Vulnerabilities in LPWAN," in *IOP conference series: materials science and engineering*, vol. 396. IOP Publishing, 2018, p. 012027.

[75] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prévotet, "Internet of mobile things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs standards and supported mobility," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1561–1581, 2018.

[76] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of LoRaWAN," *IEEE Communications magazine*, vol. 55, no. 9, pp. 34–40, 2017.

[77] M. Lauridsen, L. C. Gimenez, I. Rodriguez, T. B. Sorensen, and P. Mogensen, "From LTE to 5G for connected mobility," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 156–162, 2017.

[78] "Lorawan network server demonstration: Gateway to server interface definition," SEMTECH. Accessed: Mar. 4, 2024. [Online], available: https://www.thethingsnetwork.org/forum/uploads/default/original/1X/4fbda86583605f4aa24dcedaab874ca5a1572825.pdf.

[79] "5G system; usage of the unified data repository services for subscription data," Standard TR 29.505 v17.1.1, Release 17, 3GPP, 2021.

[80] S. Wong, N. Sastry, O. Holland, V. Friderikos, M. Dohler, and H. Aghvami, "Virtualized authentication, authorization and accounting (V-AAA) in 5G networks," in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 2017, pp. 175–180.

[81] R. Törnkvist and C. Shan, "Charging and billing architecture for 5G network," *Journal of ICT Standardization*, pp. 185–194, 2019.

[82] J. Haxhibeqiri, A. Shahid, M. Saelens, J. Bauwens, B. Jooris, E. De Poorter, and J. Hoebeke, "Sub-gigahertz inter-technology interference. How harmful is it for LoRa?" in *2018 IEEE International Smart Cities Conference (ISC2)*. IEEE, 2018, pp. 1–7.

[83] 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)*. IEEE, 2017, pp. 1–6.

[84] R. Yasmin, J. Petäjäjärvi, K. Mikhaylov, and A. Pouttu, "On the integration of LoRaWAN with the 5G test network," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, 2017, pp. 1–6.

[85] "Wirnet iFemtoCell-evolution LoRaWAN gateway," Kerlink. Accessed: Mar. 4, 2024. [Online], available: https://www.kerlink.com/product/wirnet-ifemtocell-evolution/.

[86] "Core network dynamics," CND. Accessed: Mar. 17, 2022. [Online], available: http://www.corenetdynamics.com/products/openepc/.

[87] J. Navarro-Ortiz, S. Sendra, P. Ameigeiras, and J. M. Lopez-Soler, "Integration of LoRaWAN and 4G/5G for the industrial Internet of things," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 60–67, 2018.

[88] E. M. Torroglosa-Garcia, J. M. A. Calero, J. B. Bernabe, and A. Skarmeta, "Enabling roaming across heterogeneous IoT wireless networks: LoRaWAN meets 5G," *IEEE Access*, vol. 8, pp. 103 164–103 180, 2020.

[89] D. Carrillo and J. Seki, "Rural area deployment of Internet of things connectivity: LTE and LoRaWAN case study," in *2017 IEEE XXIV International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*. IEEE, 2017, pp. 1–4.

[90] M. Taneja, "LTE-LPWA networks for IoT applications," in *2016 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2016, pp. 396–399.

[91] C. C. Zhang, K. K. Nguyen, C. Pham, and M. Cheriet, "Routing and packet scheduling in LORAWANs-EPC integration network," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*. IEEE, 2020, pp. 1–6.

[92] P. Schneider and G. Horn, "Towards 5G security," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1. IEEE, 2015, pp. 1165–1170.

[93] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 2017, pp. 193–199.

[94] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE access*, vol. 6, pp. 4850–4874, 2017.

[95] X. Ji *et al.*, "Overview of 5G security technology," *Science China Information Sciences*, vol. 61, no. 8, p. 081301, 2018.

[96] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A comprehensive guide to 5G security*. Wiley Online Library, 2018.

[97] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.

[98] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3682–3722, 2019.

[99] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8169–8181, 2019.

[100] D. Schinianakis, "Alternative security options in the 5G and IoT era," *IEEE Circuits and Systems Magazine*, vol. 17, no. 4, pp. 6–28, 2017.

[101] H. Rahimi, A. Zibaeenejad, P. Rajabzadeh, and A. A. Safavi, "On the security of the 5G-IoT architecture," in *Proceedings of the International Conference on Smart Cities and Internet of Things*, 2018, pp. 1–8.

[102] Q. M. Qadir, T. A. Rashid, N. K. Al-Salihi, B. Ismael, A. A. Kist, and Z. Zhang, "Low power wide area networks: A survey of enabling technologies, applications and interoperability needs," *IEEE Access*, vol. 6, pp. 77 454–77 473, 2018.

[103] 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.

[104] 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, pp. 249–274, 2019.

[105] V. Kumar, R. K. Jha, and S. Jain, "NB-IoT security: A survey," *Wireless Personal Communications*, vol. 113, pp. 2661–2708, 2020.

[106] A. U. Mentsiev and T. R. Magomaev, "Security threats of NB-IoT and countermeasures," in *IOP Conference Series: Materials Science and Engineering*, vol. 862, no. 5. IOP Publishing, 2020, p. 052033.

[107] M. Eldefrawy, I. Butun, N. Pereira, and M. Gidlund, "Formal security analysis of LoRaWAN," *Computer Networks*, vol. 148, pp. 328–339, 2019.

[108] I. Butun, N. Pereira, and M. Gidlund, "Analysis of LoRaWAN v1. 1 security," in *Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects*, 2018, pp. 1–6.

[109] R. Fujdiak, P. Blazek, K. Mikhaylov, L. Malina, P. Mlynek, J. Misurec, and V. Blazek, "On track of sigfox confidentiality with end-to-end encryption," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018, pp. 1–6.

[110] L. Ferreira, "(In) security of the radio interface in Sigfox," *Cryptology ePrint Archive*, 2020.

[111] J. Sanchez-Gomez *et al.*, "Integrating LPWAN technologies in the 5G ecosystem: A survey on security challenges and solutions," *IEEE Access*, vol. 8, pp. 216 437–216 460, 2020.

[112] D. Garcia-Carrillo, J. Sanchez-Gomez, R. Marin-Perez, and A. Skarmeta, "EAP-based bootstrapping for secondary service authentication to integrate IoT into 5G networks," in *International Symposium on Mobile Internet Security*. Springer, 2019, pp. 13–22.

[113] J. Sanchez-Gomez, D. Garcia-Carrillo, R. Marin-Perez, and A. F. Skarmeta, "Secure authentication and credential establishment in narrowband IoT and 5G," *Sensors*, vol. 20, no. 3, p. 882, 2020.

[114] I. Shayea, M. Ergen, M. H. Azmi, S. A. Çolak, R. Nordin, and Y. I. Daradkeh, "Key challenges, drivers and solutions for mobility management in 5G networks: A survey," *IEEE Access*, vol. 8, pp. 172 534–172 552, 2020.

[115] N. Akkari and N. Dimitriou, "Mobility management solutions for 5G networks: Architecture and services," *Computer Networks*, vol. 169, p. 107082, 2020.

[116] D. D. Olatinwo, A. Abu-Mahfouz, and G. Hancke, "A survey on LPWAN technologies in WBAN for remote health-care monitoring," *Sensors*, vol. 19, no. 23, p. 5268, 2019.

[117] H. Zhang, N. Liu, X. Chu, K. Long, A.-H. Aghvami, and V. C. Leung, "Network slicing based 5G and future mobile networks: Mobility, resource management, and challenges," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 138–145, 2017.

[118] P. Fan, J. Zhao, and I. Chih-Lin, "5G high mobility wireless communications: Challenges and solutions," *China Communications*, vol. 13, no. 2, pp. 1–13, 2016.

[119] F. Giust, L. Cominardi, and C. J. Bernardos, "Distributed mobility management for future 5G networks: overview and analysis of existing approaches," *IEEE Communications Magazine*, vol. 53, no. 1, pp. 142–149, 2015.

[120] T.-T. Nguyen, C. Bonnet, and J. Harri, "SDN-based distributed mobility management for 5G networks," in *2016 IEEE Wireless Communications and Networking Conference*. IEEE, 2016, pp. 1–7.

[121] H. Lee and M. Ma, "Blockchain-based mobility management for 5G," *Future Generation Computer Systems*, vol. 110, pp. 638–646, 2020.

[122] N. Weerasinghe, T. Hewa, M. Dissanayake, M. Ylianttila, and M. Liyanage, "Blockchain-based roaming and offload service platform for local 5G operators," in *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2021, pp. 1–6.

[123] W. Ayoub, F. Nouvel, A. E. Samhat, M. Mroue, and J.-C. Prévotet, "Mobility management with session continuity during handover in lpwan," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6686–6703, 2020.

[124] Y. Moon, S. Ha, M. Park, D. Lee, and J. Jeong, "A methodology of NB-IoT mobility optimization," in *2018 Global Internet of Things Summit (GIoTS)*. IEEE, 2018, pp. 1–5.

[125] L. Oliveira, J. J. Rodrigues, S. A. Kozlov, R. A. Rabêlo, and V. Furtado, "Performance assessment of long-range and Sigfox protocols with mobility support," *International Journal of Communication Systems*, vol. 32, no. 13, p. e3956, 2019.

[126] R. Brotzu, P. Aru, M. Fadda, and D. Giusto, "Urban SigFox-based mobility system," in *2021 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*. IEEE, 2021, pp. 1–4.

[127] F. Flammini, A. Gaglione, D. Tokody, and D. Dohrilovic, "LoRa WAN roaming for intelligent shipment tracking," in *2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT)*. IEEE, 2020, pp. 01–02.

[128] W. Ayoub, M. Mroue, A. E. Samhat, F. Nouvel, and J.-C. Prévotet, "SCHC-based solution for roaming in LoRaWAN," in *Advances on Broad-Band Wireless Computing, Communication and Applications: Proceedings of the 14th International Conference on Broad-Band Wireless Computing, Communication and Applications (BWCCA-2019) 14*. Springer, 2020, pp. 162–172.

[129] L. Vangelista and M. Centenaro, "Worldwide connectivity for the Internet of things through LoRaWAN," *Future Internet*, vol. 11, no. 3, p. 57, 2019.

[130] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, H. Jradi, and J.-C. Prévotet, "Media independent solution for mobility management in heterogeneous LPWAN technologies," *Computer Networks*, vol. 182, p. 107423, 2020.

[131] K. Mikhaylov, M. Stusek, P. Masek, V. Petrov, J. Petajajarvi, S. Andreev, J. Pokorny, J. Hosek, A. Pouttu, and Y. Koucheryavy, "Multi-RAT LPWAN in smart cities: Trial of LoRaWAN and NB-IoT integration," in *2018 IEEE International Conference on Communications (ICC)*. IEEE, 2018, pp. 1–6.

[132] K. D. Ballal, L. Dittmann, S. Ruepp, and M. N. Petersen, "IoT devices reliability study: Multi-RAT communication," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*. IEEE, 2020, pp. 1–2.

[133] A. J. Onumanyi, A. M. Abu-Mahfouz, and G. P. Hancke, "Low power wide area network, cognitive radio and the Internet of Things: Potentials for integration," *Sensors*, vol. 20, no. 23, p. 6837, 2020.

[134] Y. Li, "An integrated platform for the Internet of things based on an open source ecosystem," *Future Internet*, vol. 10, no. 11, p. 105, 2018.

[135] J. P. García-Martín and A. Torralba, "On the combination of LR-WPAN and LPWA technologies to provide a collaborative wireless solution for diverse IoT," in *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2019, pp. 1–4.

[136] L. C. Alexandre, A. L. De Souza Filho, and A. C. Sodré, "Indoor coexistence analysis among 5G new radio, LTE-A and NB-IoT in the 700 MHz band," *IEEE Access*, vol. 8, pp. 135 000–135 010, 2020.

[137] L. Polak and J. Milos, "LTE and LoRa in the 2.4 GHz band: Adjacent channel interference issues," in *2020 30th International Conference Radioelektronika (RADIOELEKTRONIKA)*. IEEE, 2020, pp. 1–4.

[138] R. Ratasuk, N. Mangalvedhe, and D. Bhatoolaul, "Coexistence analysis of LTE eMTC and 5G new radio," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2019, pp. 1–6.

[139] L. Zhang, A. Ijaz, P. Xiao, and R. Tafazolli, "Channel equalization and interference analysis for uplink narrowband Internet of Things (NB-IoT)," *IEEE Communications Letters*, vol. 21, no. 10, pp. 2206–2209, 2017.

[140] S. Liu, F. Yang, J. Song, and Z. Han, "Block sparse Bayesian learning-based NB-IoT interference elimination in LTE-advanced systems," *IEEE Transactions on Communications*, vol. 65, no. 10, pp. 4559–4571, 2017.

[141] 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.

[142] H. Malik, M. M. Alam, H. Pervaiz, Y. Le Moullec, A. Al-Dulaimi, S. Parand, and L. Reggiani, "Radio resource management in NB-IoT systems: Empowered by interference prediction and flexible duplexing," *IEEE Network*, vol. 34, no. 1, pp. 144–151, 2019.

[143] "Actility," Actility. Accessed: Mar. 4, 2024. [Online], available: https://www.actility.com/.

[144] "Simfony," Simfony. Accessed: Mar. 4, 2024. [Online], available: https://www.simfony.com/.

[145] P. J. Marcelis, V. Rao, and R. V. Prasad, "DaRe: Data recovery through application layer coding for LoRaWAN," in *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, 2017, pp. 97–108.

[146] I. Ismail, N. A. Latiff, and N. Aziemah, "Performance analysis of data recovery via application layer for LPWAN," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*. IEEE, 2019, pp. 1–5.

[147] "Glasgow Climate Pact," United Nations, Novermber 2021. Accessed: May 4, 2022. [Online], available: https://unfccc.int/sites/default/files/resource/cma2021add1adv.pdf.

[148] M. A. Ertürk, M. A. Aydın, M. T. Büyükakkaşlar, and H. Evirgen, "A survey on LoRaWAN architecture, protocol and technologies," *Future Internet*, vol. 11, no. 10, p. 216, 2019.

[149] G. Kaur, S. H. Gupta, and H. Kaur, "Optimizing the LoRa network performance for industrial scenario using a machine learning approach," *Computers and Electrical Engineering*, vol. 100, p. 107964, 2022.

[150] A. Krishnan, "LoRaWAN and Multi-RAN Architecture connecting the next billion IoT Devices," ABI Research, February 2021. Accessed: Mar. 4, 2024. [Online], available: https://info.semtech.com/abi-research-white-paperhttps://info.semtech.com/abi-research-white-paper.

[151] "Kerlink," Kerlink. Accessed: Mar. 4, 2024. [Online], available: https://www.kerlink.com/.

[152] A. Zaidi, A. Bränneby, A. Nazari, M. Hogan, and C. Kuhlins, "Cellular IoT in the 5G era," *Communications*, vol. 4, p. 6, 2020.

[153] G. Liu, Y. Huang, Z. Chen, L. Liu, Q. Wang, and N. Li, "5G deployment: Standalone vs. non-standalone from the operator perspective," *IEEE Communications Magazine*, vol. 58, no. 11, pp. 83–89, 2020.

[154] "5G standalone global market status," GSM, March 2021. Accessed: Mar. 4, 2024. [Online], available: https://gsacom.com/paper/5g-standalone-2021-summary/.

[155] J. Ha and N. Park, "Unified control architecture for 5G convergence network," in *2017 International Conference on Circuits, Devices and Systems (ICCDS)*. IEEE, 2017, pp. 226–230.

[156] M. Condoluci, S. H. Johnson, V. Ayadurai, M. A. Lema, M. A. Cuevas, M. Dohler, and T. Mahmoodi, "Fixed-mobile convergence in the 5G era: From hybrid access to converged core," *IEEE Network*, vol. 33, no. 2, pp. 138–145, 2019.

[157] M. S. Bonfim, K. L. Dias, and S. F. Fernandes, "Integrated NFV/SDN architectures: A systematic literature review," *ACM Computing Surveys (CSUR)*, vol. 51, no. 6, pp. 1–39, 2019.

[158] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 80–87, 2017.

[159] "TR-470, 5G Wireless Wireline Convergence Architecture," Broadband Forum. Accessed: Mar. 4, 2024. [Online], available: https://www.broadband-forum.org/technical/download/TR-470.pdf.

[160] T. Mamouni, J. A. T. Gijón, P. Olaszi, and X. Lagrange, "Universal AAA for hybrid accesses," in *2015 European Conference on Networks and Communications (EuCNC)*. IEEE, 2015, pp. 403–407.

[161] "LoRaGO PORT gateway," LoRaGO. Accessed: Mar. 4, 2024. [Online], available: https://sandboxelectronics.com/?product=lorago-port-multi-channel-lorawan-gateway.

[162] "Semtech UDP packet forwarder," Semtech. Accessed: Mar. 4, 2024. [Online], available: https://github.com/Lora-net/packet_forwarder.

[163] "ChirpStack Bridge," ChirpStack. Accessed: Mar. 4, 2024. [Online], available: https://www.chirpstack.io/gateway-bridge/.

[164] "ChirpStack LoRaWAN Servers," ChirpStack. Accessed: Mar. 4, 2024. [Online], available: https://www.chirpstack.io/network-server/.

[165] "Heating," IEA, Paris, 2021. Accessed: Mar. 4, 2024. [Online], available: https://www.iea.org/reports/heating.

[166] "Railway statistics synopsis 2022," International Union of Railways (UIC), Paris, France. Accessed: Jun. 14, 2023. [Online], available: https://uic.org/IMG/pdf/uic-railway-statistics-synopsis-2022.pdf.

[167] "Winter weather can present some real challenges for the railway – here's how we respond," Network Rail. Accessed: Jun. 14, 2023.

[Online], available: https://www.networkrail.co.uk/running-the-railway/looking-after-the-railway/delays-explained/snow-and-ice/.

[168] P. Fraga-Lamas, T. M. Fernández-Caramés, and L. Castedo, "Towards the Internet of smart trains: A review on industrial IoT-connected railways," *Sensors*, vol. 17, no. 6, p. 1457, 2017.

[169] "Mobile signal strength measurement data from Network Rail's engineering trains," Ofcom. Accessed: Mar. 4, 2024. [Online], available: https://www.ofcom.org.uk/research-and-data/multi-sector.

[170] R. Rowson, "GB railway mobile phone network 4G coverage," *Tableau Public*, vol. 4, Jun. 2023. [Online]. Available: https://public.tableau.com/app/profile/richard.rowson/viz/lte/RailwayGsignalstrength

[171] H. Jradi, F. Nouvel, A. E. Samhat, J.-C. Prévotet, and M. Mroue, "A seamless integration solution for LoRaWAN into 5G system," *IEEE Internet of Things Journal*, vol. 10, no. 18, pp. 16 238–16 252, 2023.

[172] A. W.-L. Wong, S. L. Goh, M. K. Hasan, and S. Fattah, "Multi-hop and mesh for LoRa networks: Recent advancements, issues, and recommended applications," *ACM Computing Surveys*, vol. 56, no. 6, p. 136, 2024.

[173] S. Kekki, "MEC in 5G networks," ETSI, Sophia Antipolis, France, 2018. Accessed: Jun. 14, 2023. [Online], available: https://www.etsi.org/images/files/ETSIWhitePapers/etsiwp28mecin5GFINAL.pdf.

[174] "Information technology — Message queuing telemetry transport (MQTT) v3.1.1," ISO/IEC 20922:2016. Accessed: Mar. 4, 2024. [Online], available: https://www.iso.org/standard/69466.html.

[175] T. Yokotani and Y. Sasaki, "Comparison with and MQTT on required network resources for IoT," in *2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)*. IEEE, 2016, pp. 1–6.

[176] D. Dinculeană and X. Cheng, "Vulnerabilities and limitations of MQTT protocol used between IoT devices," *Applied Sciences*, vol. 9, no. 5, p. 848, 2019.

[177] O. Georgiou and U. Raza, "Low power wide area network analysis: Can LoRa scale?" *IEEE Wireless Communications Letters*, vol. 6, no. 2, pp. 162–165, 2017.

[178] G. Ferré, "Collision and packet loss analysis in a LoRaWAN network," *European Signal Processing Conference (EUSIPCO)*, vol. 2017, no. 25, pp. 2586–2590, 2017.

[179] M. Hosseinzadeh, A. M. Rahmani, B. Vo, M. Bidaki, M. Masdari, and M. Zangakani, "Improving security using SVM-based anomaly detection: issues and challenges," *Soft Computing*, vol. 25, pp. 3195–3223, 2021.

[180] Z. Karevan and J. A. Suykens, "Transductive LSTM for time-series prediction: An application to weather forecasting," *Neural Networks*, vol. 125, pp. 1–9, 2020.

[181] A. Paniagua-Tineo, S. Salcedo-Sanz, C. Casanova-Mateo, E. Ortiz-García, M. Cony, and E. Hernández-Martín, "Prediction of daily maximum temperature using a support vector regression algorithm," *Renewable Energy*, vol. 36, no. 11, pp. 3054–3060, 2011.

[182] T. L. Thorarinsdottir and T. Gneiting, "Probabilistic forecasts of wind speed: Ensemble model output statistics by using heteroscedastic censored regression," *Journal of the Royal Statistical Society: Series A (Statistics in Society)*, vol. 173, no. 2, pp. 371–388, 2010.

[183] N. Shivhare, A. K. Rahul, S. B. Dwivedi, and P. K. S. Dikshit, "ARIMA based daily weather forecasting tool: A case study for Varanasi," *Mausam*, vol. 70, no. 1, pp. 133–140, 2019.

[184] "ETSI EN 300 220-2 v3.2.1 (2018-06)," ETSI, Sophia Antipolis, France, Rep. REN/ERM-TG28-535, 2018. Accessed: Jan. 22, 2024. [Online], available: https://www.etsi.org/deliver/etsi_en/300200_300299/30022002/03.02.01_60/en_30022002v030201p.pdf.

[185] P. D'Aranno, A. D. Benedetto, M. Fiani, and M. Marsella, "Remote sensing technologies for linear infrastructure monitoring," *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. 42, pp. 461–468, 2019.

[186] R. M. Liaqat, P. Branch, and J. But, "LoRa based linear network applications, design considerations and open challenges: A review," in *Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems*, 2022, pp. 913–917.

[187] J. P. S. 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, 2019.

[188] A. Pagano, D. Croce, I. Tinnirello, and G. Vitale, "A survey on LoRa for smart agriculture: Current trends and future perspectives," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3664–3679, 2022.

[189] B. Citoni, F. Fioranelli, M. A. Imran, and Q. H. Abbasi, "Internet of things and LoRaWAN-enabled future smart farming," *IEEE Internet of Things Magazine*, vol. 2, no. 4, pp. 14–19, 2019.

[190] A. Shrestha and L. Xing, "A performance comparison of different topologies for wireless sensor networks," in *2007 IEEE Conference on Technologies for Homeland Security*. IEEE, 2007, pp. 280–285.

[191] A. Mahmood, E. Sisinni, L. Guntupalli, R. Rondón, S. A. Hassan, and M. Gidlund, "Scalability analysis of a LoRa network under imperfect orthogonality," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1425–1436, 2018.

[192] Y. Chen, G. Shi, M. Al-Quraan, Y. Sambo, O. Onireti, and M. Imran, "LoRa mesh-5G integrated network for trackside smart weather monitoring," *IEEE Transactions on Vehicular Technology*, 2024.

[193] Y. Chen, Y. A. Sambo, O. Onireti, S. Ansari, and M. A. Imran, "LoRaWAN-5G integrated network with collaborative RAN and converged core Network," in *2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2022, pp. 1–5.

[194] V. J. Hodge, S. O'Keefe, M. Weeks, and A. Moulds, "Wireless sensor networks for condition monitoring in the railway industry: A survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 3, pp. 1088–1106, 2014.

[195] A. M. Obeid, F. Karray, M. W. Jmal, M. Abid, S. M. Qasim, and M. S. BenSaleh, "Towards realisation of wireless sensor network-based water pipeline monitoring systems: a comprehensive review of techniques and platforms," *IET Science, Measurement & Technology*, vol. 10, no. 5, pp. 420–426, 2016.

[196] K. Azhar, S. Zafar, A. Kashif, A. Aljaedi, and U. Albalawi, "Fault-tolerant partition resolvability in mesh related networks and applications," *IEEE Access*, vol. 10, pp. 71 521–71 529, 2022.

[197] A. Sen, B. H. Shen, L. Zhou, and B. Hao, "Fault-tolerance in sensor networks: A new evaluation metric," in *INFOCOM 2006: 25th IEEE International Conference on Computer Communications*, 2006, p. 4146923.

[198] M. R. Henzinger, S. Rao, and H. N. Gabow, "Computing vertex connectivity: New bounds from old techniques," *Journal of Algorithms*, vol. 34, no. 2, pp. 222–250, 2000.

[199] D. T. Chiang and S.-C. Niu, "Reliability of consecutive-k-out-of-n: F system," *IEEE Transactions on Reliability*, vol. 30, no. 1, pp. 87–89, 1981.

[200] T. Bouguera, J. F. Diouris, J. J. Chaillout, R. Jaouadi, and G. Andrieux, "Energy consumption model for sensor nodes based on LoRa and LoRaWAN," *Sensors*, vol. 18, no. 7, p. 2104, 2018.

[201] K. H. Lam, C. C. Cheung, and W. C. Lee, "RSSI-based LoRa localization systems for large-scale indoor and outdoor environments," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 12, pp. 11 778–11 791, 2019.

[202] "NS-3 network simulator," Accessed: Mar. 4, 2024. [Online], available: https://www.nsnam.org/.

[203] F. Van den Abeele, J. Haxhibeqiri, I. Moerman, and J. Hoebeke, "Scalability analysis of large-scale LoRaWAN networks in NS-3," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2186–2198, 2017.

[204] 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*, 2016, pp. 59–67.

[205] T. Voigt and M. Bor, "LoRaSim," Version 0.2.1, 2017. Accessed: Mar. 4, 2024. [Online], available: https://mcbor.github.io/lorasim/.

[206] "SimPy - Event discrete simulation for Python," Accessed: Mar. 4 2024. [Online], available: https://simpy.readthedocs.io/.

[207] R. Tarjan, "Depth-first search and linear graph algorithms," *SIAM Journal on Computing*, vol. 1, no. 2, pp. 146–160, 1972.

[208] A. Z. Broder, "Generating random spanning trees," *FOCS*, vol. 89, pp. 442–447, 1989.

[209] D. J. Aldous, "The random walk construction of uniform spanning trees and uniform labelled trees," *SIAM Journal on Discrete Mathematics*, vol. 3, no. 4, pp. 450–465, 1990.

[210] D. B. West, *Introduction to graph theory*. Upper Saddle River: Prentice hall, 2001, vol. 2.