T.C.

ALTINBAS UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

INCREASE ENERGY AWARE FOR WIRELESS SENSOR NETWORK USING LOWPAN

Zaid Ali Saeed AL-SARRAY

Master of Science

Supervisor

Asst. Prof. Dr. Abdullahi Abdu IBRAHIM

Istanbul, 2021

INCREASE ENERGY AWARE FOR WIRELESS SENSOR NETWORK USING LOWPAN

by

Zaid Ali Saeed AL-SARRAY

Electrical and Computer Engineering

Submitted to the Institute of Graduate Studies

in partial fulfillment of the requirements for the degree of

Master of Science

ALTINBAŞ UNIVERSITY

2021

The thesis titled “INCREASE ENERGY AWARE FOR WIRELESS SENSOR NETWORK USING LOWPAN” prepared and presented by “Zaid Ali Saeed AL-SARRAY” was accepted as a Master of Science Thesis in Electrical and Computer Engineering.

Asst. Prof. Dr. Abdullahi Abdu IBRAHIM

Supervisor

Thesis Defense Jury Members:

Asst. Prof. Dr. Abdullahi Abdu IBRAHIM	School of Engineering and Natural Sciences, Altinbas University	_____
Asst. Prof. Dr. Muhammad ILYAS	School of Engineering and Natural Sciences, Altinbas University	_____
Asst. Prof. Dr. A. Mohammed ABUBAKAR	Faculty of Business, Antalya Bilim University	_____

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Approval Date of Institute of Graduate Studies: ____/____/____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Zaid Ali Saeed AL-SARRAY

DEDICATION

I devote and pledge this research work to my supervisor who is salient for guiding me through whole research work as well as my family for always assisting me in my hard time.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my supervisor Asst. Prof. Dr. Abdullahi Abdu IBRAHIM for guiding and helping me along the way in writing this dissertation. Discussing my progress, problems, and ideas with my supervisor Asst. Prof. Dr. Abdullahi Abdu IBRAHIM a couple of times every week helped me tremendously in understanding the logic behind the research. It made me better realize the technical need for this research work. He helped me by looking outside of all the machine learning and network-based information, and considering the cryptocurrency-based knowledge from a more holistic perspective than just from the productivity point of view. He patiently explained to me a great number of technical details with regards to block-chain and cryptocurrency, for example how to deal with solving problems and to provide insight into the reliability of those results. Without his time and help none of this research would have been possible, and I'm grateful to him for giving me the opportunity to work on this interesting subject. I am also very thankful to my parents as well as my friends who always supported me through whole of this journey.

ABSTRACT

INCREASE ENERGY AWARE FOR WIRELESS SENSOR NETWORK USING LOWPAN

AL-SARRAY, Zaid Ali Saeed,

M.Sc., Electrical and Computer Engineering, Altınbaş University,

Supervisor: Asst. Prof. Dr.Abdullahi Abdu IBRAHIM

Date: Mar/2021

Pages: 60

There are many networks in remote areas to support all areas and applications. Networks That allow connectivity covering a range of square kilometers are critical for these remote deployments. The widely used star topology is not ideal for a rural environment as the coverage is limited by the central axis positioning which also contributes to being a single point of failure. It is clear that mesh networks are more attractive in this respect, but scalability has always been an issue for mesh networks, especially with regard to routing. Saving power very fundamental in remote IoT deployments, where devices can be left in isolated fields for an extended period of time. In this thesis we dealt with the steering problem of remote sensors by introducing reinforcement learning energy-aware routing algorithms. We determined the strength of the RL routing algorithm for remote sensing networks. This thesis also presents a step-by-step detailed analysis of the RL routing algorithm to To prove the effectiveness of the algorithm. We model the network operating in a region bounded by a finite number of randomly distributed nodes within the region in this algorithm. Hence, we have defined the service area of the target network assuming network limitations in the model.

Keywords: Wireless sensor network, Energy aware, LPWAN, IOT, Reinforcement Learning algorithm

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

1. INTRODUCTION

1.1 WIRELESS SENSOR NETWORK

A Wireless sensor network can be defined as a network of devices that can communicate the information gathered from a monitored field through wireless links. The data is forwarded through multiple nodes, and with a gateway, the data is connected to other networks like wireless Ethernet.

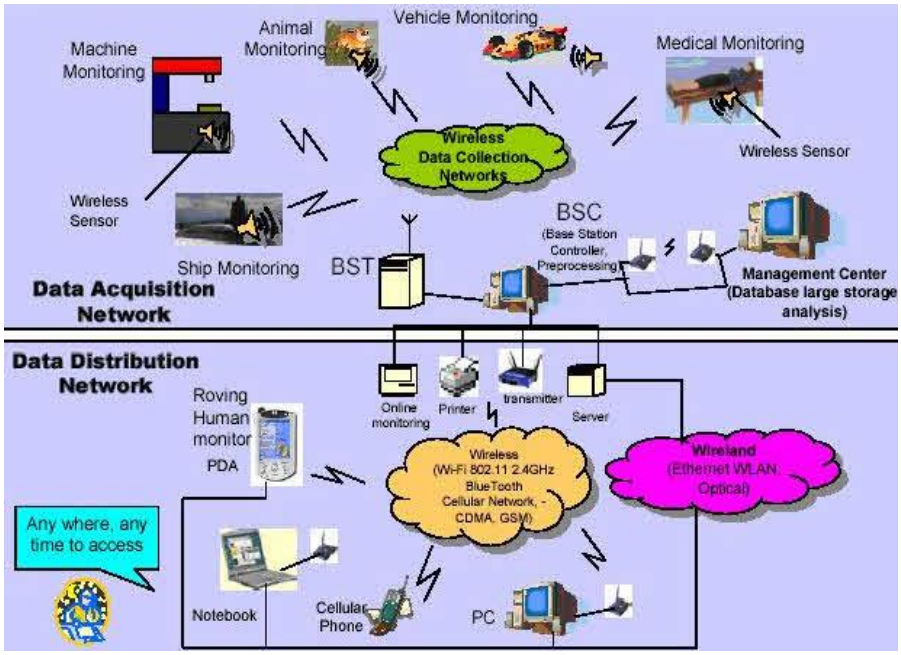

Figure 1.1: Wireless sensor network [1]

1.1.1 WSN Network Topologies

1. Star Topologies

Star topology is a communication topology, where each node connects directly to a gateway. A single gateway can send or receive a message to several remote nodes. Instar topologies, the nodes are not permitted to send messages to each other. This allows low-latency communications between the remote node and the gateway (base station).

Due to its dependency on a single node to manage the network, the gateway must be within the radio transmission range of all the individual nodes. The advantage includes the ability to keep the

remote nodes' power consumption to a minimum and simply under control. The size of the network depends on the number of connections made to the hub.

2. Tree Topologies

Tree topology is also called as a cascaded star topology. In tree topologies, each node connects to a node that is placed higher in the tree, and then to the gateway. The main advantage of the tree topology is that the expansion of a network can be easily possible, and also error detection becomes easy. The disadvantage with this network is that it relies heavily on the bus cable; if it breaks, all the network will collapse.

3. Mesh Topologies

The Mesh topologies allow transmission of data from one node to another, which is within its radio transmission range. If a node wants to send a message to another node, which is out of the radio communication range, it needs an intermediate node to forward the message to the desired node. The advantage of this mesh topology includes easy isolation and detection of faults in the network. The disadvantage is that the network is large and requires huge investment.

1.2 PROBLEM STATEMENT

Many studies have been published on the using and developing of ontologies in the security area authors claimed the importance of ontologies for classifying security threats. They provided a review of the most relevant papers on the topic of security ontologies and their applications and found that, although they offer a useful contribution to the community knowledge, ontologies proposed in the literature do not provide a comprehensive knowledge of the subject. An important contribution to the literature in the field was given above. Authors suggested a classification of ontologies in eight different security classes, namely web-oriented, taxonomies, requirement, risk-based, initial, general, and modelling. In particular, we are interested in the latter classification. Due to their extensibility, security ontological models can flexibly define concepts of a knowledge domain, spanning from a generic to detailed representation of facts. Moreover, their sharing enables the collaboration among system manager's/network administrators and cybersecurity

experts. As a benefit, they can improve in effective-ness and speed to respond to security threats. However, there are still some issues and challenges to be addressed in order to assess the semantic quality of security ontologies. Authors of explored the problem of quality assessment of ontologies and provided a statistical characterisation of "good ontologies". In [10], the authors described how a shared thesaurus can be exploited for the development of ontologies in many stages of their lifecycle. Authors claimed that the use and maintenance of a shared thesaurus may facilitate the development and interoperability of ontologies. A taxonomy can be considered as a simple variant of a thesaurus. Hence, instead of a thesaurus, it could be possible to use a shared taxonomy, able to organize words in a hierarchical structure, according to a similarity of meaning. In their analysis, the authors of [11]

stated that semantic reasoning (i.e., deriving information not explicitly made available by an ontology may be speeded-up by reducing the size of ontologies, limiting the number of independent paths and the degree of classes, and making the inheritance a tree-like graph. However, time constraints are not the only limiting factors for semantic reasoning systems. Indeed, semantic ac-curacy may influence the precision of the semantic inference tasks and, consequently, the output of reasoning systems. In it has been claimed that taxonomic features, namely number of classes, depth and breadth variances, are the best predictors of ontologies' semantic accuracy, even though this measure of accuracy strongly depends on the ontology size. This challenging issue was coped and overcome by defining an empirical aggregated measure of ontologies' semantic accuracy based on the variance computation of semantic dispersion of their taxonomic structures.

1.3 RESEARCH QUESTIONS AND/OR HYPOTHESES

Attacker may perform a selective packet dropping or change its behavior over time in order to deceive the underlying detection mechanism [12]. How can we exploit the evolution of a node during a time period to identify the nature of its behaviors? Although, the infrastructure resources could be shared among different network slice instances, every provider may use a specific control and cloud management system. Advanced orchestration and automation are required to release the configuration burden from users and to enable an integrated end-to-end solution. Confirmation of functions and systems and predictive analytics make it possible to effectively scale, change and

elastically manage the network service by mean of recursive structures. However, measurement of their performance in compliance with Service Level Agreements (SLAs) will be necessary for the dynamic slice instantiation and activation. The 5G network will be coping with the outstanding increasing information exchange throughout the whole system. Therefore, the security challenge in 5G will not be confined to guaranteeing reliable and trustworthy connectivity to end users.

1.4 THESIS CONTRIBUTION

The aim of this thesis is increase energy aware for wireless sensor network by using low power wireless area network that and consume less resources. By using RL the algorithm is able to benefits the experience of the entire network compared. By taking the Energy condition of the whole network into consideration, the RL routing algorithm has clarify enhancement in all measures including failure rates, energy efficiency that we used in the simulations over the benchmark algorithm. The thesis shows how energy awareness can play important role during deploying wireless sensor networks and has pointed out a new way of energy aware routing for these networks.

The framework should support understanding of how systems and services are tied together in Securing 5th Generation Network using Low-Power Wireless Personal Area Network in the Matlab environment.

The framework should be easy to apply to all industrial level organizations. Different advanced toolboxes in Matlab i.e. Antenna Toolbox, Machine Learning Toolbox, Wireless Toolbox.

1.5 THESIS OUTLINE

Chapter 1: Introduction

This section presents an overview of the thesis, as well as a short summary off each chapter.

Chapter 2: Theoretical Background

This chapter introduces the thesis further by giving the reader background information to wireless sensor networks using by using low power wireless area network

Chapter 3: Methodology

This chapter presents a theoretic overview of the method proposed in this thesis. It presents the structure of the method and the proposed framework for implementation and comparison, and suggests several sub-methods that can be used to implement it. A dataset of these will be used to train and evaluate the proposed method. This dataset will also be presented.

Chapter 4: Results

The results and lab practice are presented and compared in this chapter.

Chapter 5: Conclusion

The final chapter presents a summary and conclusion of the thesis. This chapter provides a discussion off the results, as well as the considerations and implications of the thesis, and a description of future research that may be conducted to further study the subjects presented.

Reference

2. RELATED WORK

2.1 LITERATURE REVIEW

The evolution of nowadays communication systems brings with her new opportuni-ties and will determine a profound modification of our lifestyle and human-to-systems interaction [13]. The 5G is a novel network paradigm that combines old and new tech-nologies and answer the calls for growing data demand due to an increasing number of entities accessing data communication services (see Figure 2.1) and novel, resource-consuming applications (e.g., 4k ultra-HD video streaming, virtual and augmented reality). In the vision of 5G Infrastructure Public Private Partnership (5G PPP), in future nations an enormous quantity of heterogeneous data and knowledge will be everywhere accessible to everyone and in real-time.Driven by new business use cases for the development and implementation of 5G, 5G PPP identified new actors/stakeholders that interact with each other to foster novel network services and applications. However, new challenging security prob-lems might emerge in this potentially untrustful environment.[14] As an example, if a provider of network services and applications suffers from security vulnerabilities, served stakeholders might be exposed to attacks to their security to court There-fore, accurately determining security vulnerabilities by considering interdependences among 5G actors might be of great interest.It is universally recognised that 5G should fill the gap in term of capacity, data

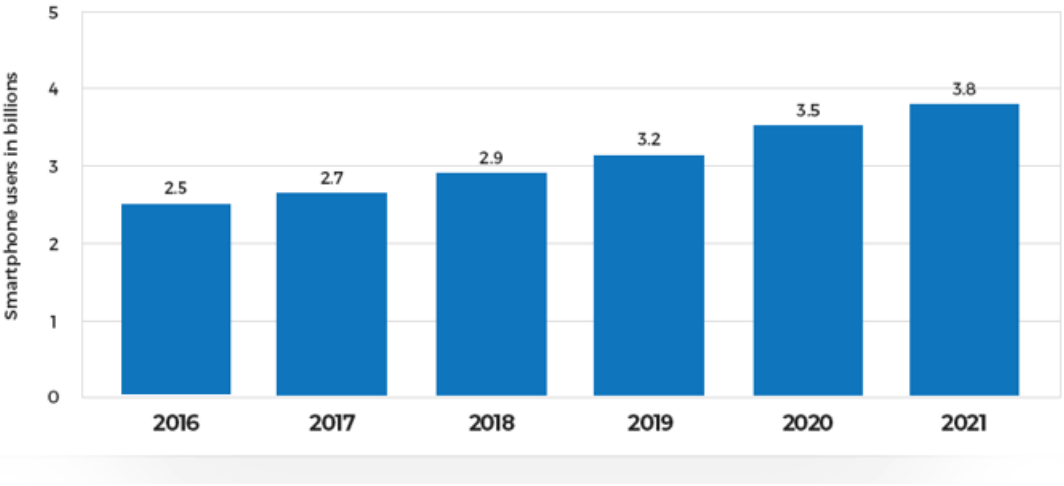

Figure 2.1: Global smarthphone users [15]

social, and health information can day-by-day be stored, manipulated, and analysed by service providers. However, although of the benefits that it can offer, information processing and transmission through networked systems could affect the security and privacy of their owners and subjects. Hence, the integrated, service-oriented network of the future, while ensuring both connectivity and privacy to end-users, should ad-dress the security on the network as a whole. However, studying and identifying privacy issues in the 5G is not straightforward. Indeed, 5G is a complex eco-system in which well-known vulnerabilities adds up to threats proper of the internet and software system.

2.2 THE 5G ECO-SYSTEM

The 5G network represents the answer of wireless communication infrastructure to the proliferation of new businesses for industry and vertical markets. Present society is evolving towards a new model of human-to-human and human-to-device interac-tion, in which hyper-connected autonomic entities continuously exchange, store, and elaborate information in real-time. This communication network revolution leads the way towards design and implementation of new services and application, driven by novel emerging use cases, vertical markets and industries (e.g., e-health, smart city, connected cars, haptic communication, virtual and augmented reality).5G is envisioned to provide high-speed connectivity (1Gbps), low-latency (at max-imum 1 ms, to be successful for mission-critical application and systems) and support for low power devices (e.g., sensors) with lifespans up to several years

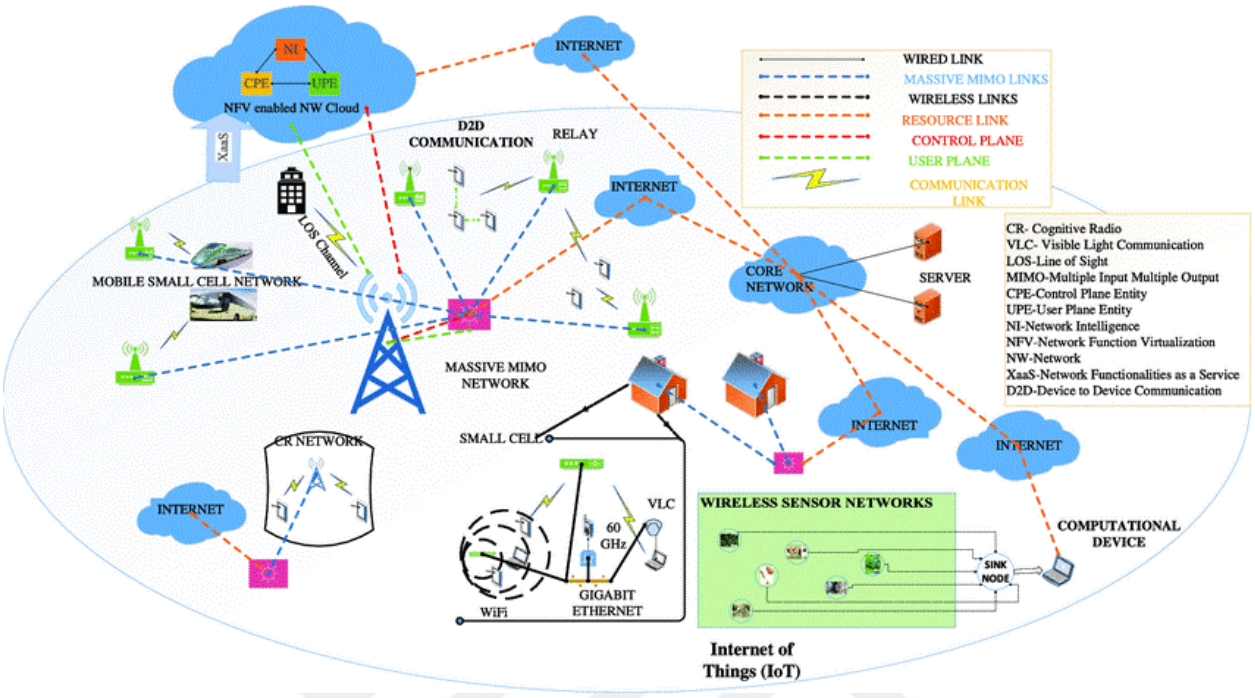

Figure 2.2: General 5G Network [16]

Soon, i.e., past 4G, a portion of the prime goals or requests that should be tended to are expanded limit, improved information rate, diminished dormancy, and better nature of administration. To fulfill these needs, exceptional upgrades should be made in cell network engineering. This paper presents the aftereffects of an itemized review on the fifth era (5G) cell network engineering and a portion of the key rising advancements that are useful in improving the design and satisfying the needs of clients. In this nitty gritty study, the prime spotlight is on the 5G cell network engineering, gigantic different info numerous yield innovation, and gadget to-gadget correspondence (D2D). Alongside this, a portion of the rising advances that are tended to In this paper, an overall plausible 5G cell network design is proposed, which shows that D2D, little cell passages, network cloud and the Internet of Things can be a piece of 5G cell network engineering. A definite review is incorporated with respect to ebb and flow research ventures being directed in various nations by research gatherings and foundations that are taking a shot at 5G advancements.

2.3 TECHNOLOGIES TO BE INCORPORATED INTO 5G AND RELATED WORK ON THEM

In this section we present an overview on three efficient spectrum reuse technologies to be incorporated into 5G that are studied in this dissertation

2.3.1 Device-to-Device (D2D)

Recently, the concept of D2D communication has emerged to cater the ever-increasing demand of data rate and system capacity. D2D enables UEs lying in close proximity, that intend to exchange information, to bypass the cellular BS and communicate in a peer-to-peer fashion. It is envisioned that D2D communication between UEs can improve the network performance in terms of spatial frequency reuse, latency, and energy consumption In other words, D2D communication replaces the conven-tional two-hop cellular link by a short-range, low-power, and direct D2D link which will improve the latency and power consumption. Further, while the conventional cellular association dictates a single link per channel per cell (thereby prohibiting intracell interference), D2D links aggressively reuse the same channel over the spa-tial domain with no restriction over the cell boundaries, which increases the spatial frequency reuse. Consequently, D2D communication introduces a new type of interfer-ence between the cellular mode and D2D mode UEs, which is denoted as cross-mode interference. The envisioned D2D gains come at the expense of more complicated network management. Choosing the mode of operation (i.e., cellular mode or D2D mode) and neighbor discovery are two new network functions that arise with D2D communication. Further, interference management between cellular and D2D links also needs to be taken into account. Despite the increased interference level imposed by D2D communication, non-trivial gains can be harvested if e cient interference coordination between D2D and cellular links is adopted. In addition to im-proving the spatial spectral utilization, D2D can potentially bring other performance gains for cellular networks, namely, lower power consumption, higher network capac-ity, and lower communication latency.

2.3.2 Full Duplex (FD)

FD communication involves a transceiver communicating such that it is simultane-ously transmitting and receiving on the same frequency channel. In the literature this has been, rightfully,

compared to \trying to hear a whisper while shouting at the top of your lungs" This is due to the overwhelming self-interference (SI) dominating the signal at the receive antenna from the message being transmitted by the transceiver itself. Consequently, FD communication was thought to not be possible for the longest time However, with recent advances in SI cancellation techniques, that mitigate the overwhelming SI, simultaneous transmission and recep-tion on the same time-frequency resource block has become possible; as a result, FD communication has become a reality.FD communication at a transceiver can be realized in two ways: 1) Bi-directional FD transmissions, and 2) the FD 3-node topology As the name suggests, bidirectional FD involves a pair of nodes transmitting to and receiving from each other in the same time-frequency resource block. On the other hand, in the FD 3-node topology, the transceiver that communicates via FD transmits to one HD node and receives from another HD node simultaneously on the same frequency channel.[17] As FD communication enables simultaneous transmission and reception on a link, it was envisioned that the technology has the potential to double the throughput. However, this is far from true as FD communication also dramatically increases the network interference.

communication also dramatically increases the network interference. Accordingly, several studies for FD communication in large networks have been conducted via stochastic geometry to include the impact of the increased network interference. FD communication is employed at the cellular link. When FD is employed at the cellular link, high rate improvement is observed for the downlink However, the authors in show that the downlink rate improvement may come at the expense of high degradation in the uplink rate due to the high disparity between the uplink and downlink transmit powers. An adhoc network is considered in and the authors report that FD communication o ers rate improvement in both the forward and the reverse links when both have equivalent transmit powers.

2.3.3 Non-Orthogonal Multiple Access (NOMA)

NOMA is advanced as one of the promising innovations to be received in 5G cellular systems. In differentiate to ordinary orthogonal different get to (OMA), NOMA is predicted to extend the organize capacity by progressing the spatial utilization of the rare range.Expectedly, transient, ghostly, and/or spatial orthogonal-ization are received to dodge intracell obstructions (i.e.,

obstructions among UEs within the same cell) in OMA[18]. This grants as it were one UE to be served per time-frequency resource-block per BS in OMA.In NOMA cellular systems, on the other hand, mul-tiple UEs can be clustered and at the same time served over the same time-frequency resource-block.

Especially, NOMA UEs share the same time-frequency assets by either having their messages superposed within the control space or within the code space.

NOMA is subsequently a uncommon case of superposition coding The shared intracell obstructions among the clustered UEs is overseen by legitimate asset allotment (e.g., transmission control and rate) in conjunction with progressive impedances cancellation (SuIC) Translating strategies utilizing SuIC for multiple-access channels have been examined from an information-theoretic point of view for a few decades and they were actualized on a program radio stage in Thus, UE clus-tering and asset assignment are pivotal for NOMA operation in arrange to play down the e ect of intracell impedances Persuaded by its potential to extend the capacity of cellular systems, the plan of NOMA transmission by means of UE clustering and asset allotment has gotten much consideration from the investigate community For occasion, the significance of control allotment for accomplishing transmission rate picks up in a single-cell NOMA downlink is emphasized The e ect of control assignment on transmission rate reasonableness among NOMA UEs is showed in UE clustering is considered inwhere determination methodologies are proposed based on the remove between the UEs and the BS. In it is appeared that having NOMA UEs with more unmistakable channels upgrades NOMA picks up in as ingle-cell downlink situation. The coexistence of a cognitive auxiliary NOMA framework with a essential OMA network.for occasion are not sufcient to attain the yearning execution prerequisite de ned for 5G net-worksTherefore,it is believed that the foreseen 5G performance will be ful lled by integrating several new technologies to the state of the art cellular system This implicitly requires more aggressive usage for the spectrum and more sophisticated in-terference management techniques. For instance, it is shown in that integrating massive MIMO with D2D communication increases the cellular transmissions per cell and mitigates the D2D-to-cellular interference, at the expense of increasing the cellular-to-D2D interference. This improves the network spectral efciency while providing sufcient protection to the conventional cellular users. However,the channel state information between all D2D transmitters and all antennas is required, which imposes high control

burden. integrated NOMA and FD transmission scheme is proposed in to reduce relaying delay and improve the end to end throughput. The BS broadcasts the superimposed message for the strong and weak users which is decoded by the strong user and a FD relay. No direct link between the BS and the weak user exists; the weak user's message is decoded by the relay and forwarded to it in a future time slot using FD. The authors in exploit FD relaying to improve the reliability of NOMA transmissions, in which the NOMA UE with the stronger channel simultaneously receives it own message and relays an older message designated to the UE with the weaker channel.

An adaptive multiple access scheme is also studied that switches between the proposed cooperative NOMA, conventional NOMA, and OMA according to the link quality and level of residual self interference.

2.3.4 On Physical Layer Security

As mentioned before, with the wide range of applications of wireless communication, secure information transmission has become very important. The focus now is on physical layer security. Various works have been done that focus on exploiting the nature of the wireless network to enhance security. In our work on physical layer security, we are particularly interested in the impact that interference has on achievable secure communication.Until recently, network interference has been considered an undesirable perfor-mance limiting parameter for wireless communication.This conception is changing with the emerging requirement for physical layer security where interference may help in increasing transmission secrecySecure information transmission opportu-nities on the legitimate link arise from the random uctuation of interference power at the receiver and eavesdropper. Particularly, exploiting the time intervals where the receiver (eavesdropper) experience low (high) interference powers, the transmitter can send information at a rate that is higher than the capacity of the eavesdrop-per link. This leads to the event of opportunistic secure spectrum access (OSSA) in which the eavesdropper cannot decode the message while the legitimate receiver can; transmission secrecy is therefore attained on the legitimate link.The efect of interference on transmission secrecy is mainly studied and quan-ti ed assuming independent interference at the legitimate-receiver and eavesdrop-per However, since the interference experienced at the receiver and eaves-dropper arises from the same set of transmitters, the network interference is spatially correlated Studying the impact of correlated

interference is important as it may degrade OSSA performance more than that anticipated for independent in-terference, in which the degradation becomes more prominent as the eavesdropper gets closer to the receiver.

Hence, the performance of OSSA should be character-ized in terms of the distance between the receiver and eavesdropper. To the best of our knowledge, this problem has not been investigated in the literature. Numerous works have considered the impact of correlated fading between the eavesdropper and receiver in small networks on the achievable secrecy however, our focus is on independent fading but correlated interference in a large network. This case is more practically relevant since the spacing between legitimate users and eavesdroppers cer-tainly exceeds the coherence length of the fading, while the interference is correlated over much larger distances.

2.3.5 NOMA for Large Networks

A number of the aforementioned NOMA studies are myopic in the sense that each BS independently utilizes the local information (e.g., channel state information (CSI), UE locations, target-rates, power constraints, etc.) to perform UE clustering and re-source allocation. Such myopic schemes ignore intercell interference (i.e., interference from other cells), which is a fundamental performance limiting parameter in cellular networks. In Chapter 5 we study NOMA for large networks where intercell interfer-ence is accounted for. To illustrate the e ect of intercell interference on NOMA rate, we show Fig.1.1 which plots guaranteed versus target UE rates for a two-UE xed-rate NOMA transmission in a large-scale downlink cellular network. The simulation environment considered to plot Fig.1.1 is detailed in AppendixAs shown in the gure, the guaranteed UE rate is always less than the target-rate due to transmis-sion outages, which occur when the fading, noise, and interference lead to a channel.

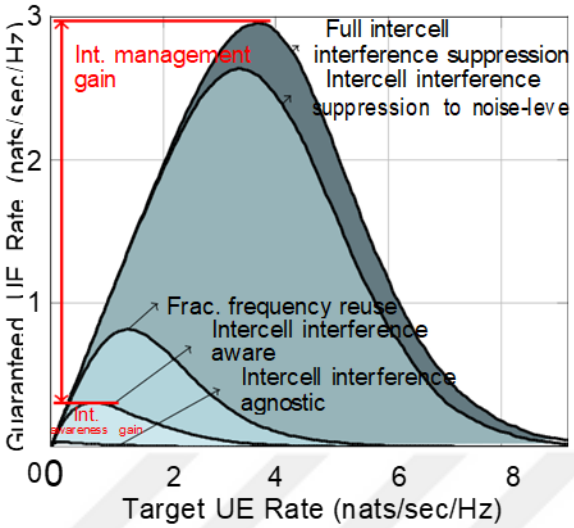

Figure 2.3: Downlink guaranteed-rates per UE for di erent levels of intercell interference in a NOMA setup with N = 2.

Here, the guaranteed-rate is the least e ective-rate of a UE within the setup, where the e ective-rate of a UE is the target-rate times the likelihood that no blackout occurs.capacity less than the xed-transmission rate. Too, we watch the presence of an ideal target-rate that equalizations the tradeo between blackout likelihood and channel utilization.

The gure appears that the guaranteed-rate gets to be signi cantly less than the target-rate for intercell obstructions skeptic NOMA plan. Be that as it may, intercell obstructions mindfulness and administration can signi cantly diminish blackouts and move forward the UE guaranteed-rate, which highlights the extreme e ect of intercell interference.Having highlighted the significance of interference-aware NOMA plan for 5G cellular systems, it remains to note that there are different challenges related with such plan such as:Interference's stochastic nature:

This is often due to a few sources of vulnerability such as channel picks up, organize geometry, transmission powers, tra c prerequisites, etc., which make impedances difficult to estimate.Location reliance: Impedances is profoundly subordinate on the area of Ues inside a BS's benefit region: UEs close the cell boundary involvement more intercell impedances.

2.3.6 Security, Privacy and Trust in 5G

The 5G system is expected to realise precise actions to cope with the increasing in-formation traffic and provide reliable connectivity and security to the entire network. Security challenges will involve confidentiality of communications, authorisation and access control (of UEs), accounting, integrity, availability, and authentication. The 5G system is required to cope with a significant number of potential classes of threats that can be originated by failures (both internal and external), malicious actions of stake-holders, and external entities. Authentication will be particularly challenging. Due to the time required for operations at remote servers (in the order of hundreds of milliseconds), current approaches to authentication will not be suitable anymore in 5G, which is inconsistent with the specification of latency (ideally equal to zero). In general, current security and privacy mechanisms are at odds with latency requirements as stronger approaches are both more computationally expensive and time-demanding. Moreover, the authentication issue will be worsened by the ultra-densification trend. Then, as to cope with the resulting rise in the number of handovers and continuous authentication of user equipment's over small cells, the ultra-dense setting will require novel mechanisms for transferring the security context. Although it might seem a good solution to detect intruders and secure the network, monitoring a large number of UEs served by 5G systems is not a trivial task. Since it does not require the execution of complex operations, the physical layer security might represent a viable solution to secure the 5G. Furthermore, it offers a valid alternative to the adoption of third-party security providers and cryptographic approach for authentication and information privacy [19]. New business models and applications highlight the role of cooperation and strong. Interdependence among several actors of 5G and the paramount value of the trust among them.

Delivery of services will require a synergistic action of multiple actors, that will try to ensure a given quality of service in agreement with the service level agreements (SLAs). Therefore, the trust among involved parties is the glue to build novel and evolved services. It and its model can track the reputation of actors as a function of their performance, thus promoting the birth of a chain of responsibilities for granting a proper level of service for the end-users and an optimal state for the network system. In the next generation network, it is expected to be a growing awareness of responsibilities, driven by the need of having a clear picture of risks. A metric to measure actors' reputation and trust might be founded on security measures they actually put in place, their

compliance to policies, and availability. Monitored resources might be both the physical and virtual ones required for the delivery of services. The 5G-ENSURE project exploited a comprehensive method of risks identification built on machine understandable models enforced with expert knowledge on potential risks for the system to be analysed. By using a machine-understandable model, this analysis direction can automatically identify and carefully every known way in which the network may be attacked or accidentally compromised, also reducing the probability that any vulnerabilities could be overlooked. In Chapter 3 we discuss the automated threat identification and provide some considerations in this vein.

2.4 PRIVACY METRICS

In this section we recall some important works and definitions of privacy. In general, we can distinguish two broad approaches to individual ‘s privacy. The first is focused on protecting identities, and the second trying to preserve their data. When the users ‘identity are protected, linking users ‘data must be unfeasible or very hard to obtain.

Most techniques that aim to protect user ‘s data are usually based on disclosing of modified versions of original dataset. In this manner, adversaries can access only to inaccurate information. In this direction, [20] introduced one of the most prominent privacy definitions, namely the k-anonymity. Using the notion of quasi-identifiers (that is, a set of information and attributes that cannot disclose real identity of individuals when taken singularly, but can do it if used in combination with other data sources), authors proved that hiding or reducing the granularity of the set, can make an individual indistinguishable from other k-1 subjects. That is, any combination of quasi-identifiers (attributes of individuals) could not disclose real identities of a target, but make it undistinguishable from other k-1 ones. In, authors defined the concept of differential privacy, which provides a condition on the public release of datasets.

It states that given two public release of dataset differing for only one record are differentially private if outputs from their querying are equally likely. Although k-anonymity and differential privacy were considered first in the context of statistical databases, they have been successfully applied in the field of location-based systems. The scientific community proposed other variants of k-anonymity over the years, such as l-diversity or t-closeness. The former variant requires that for each combination of non-sensitive information of individuals made public (e.g., present into

the released set) there must be at least l different and well-represented values released of each sensitive data. The latter principle imposes that the difference of the distribution of values of a sensitive attribute in an equivalence class must be no more than a threshold t with respect to the released set. Anyway, protecting the users 'identity might not be enough to protect their privacy. In fact, adversaries might disclose real identity of individuals by combining anonymised information with other publicly available dataset or data of their own. Location, together with financial and medical information, belongs to a long list of personal data that can be exploited as a starting point to derive new insightful and valuable information on individuals (e.g., data on personal life, religion and political beliefs, financial and professional information). Protecting location privacy, might mean quantify the error of the adversary trying to infer the real location of victims.

Privacy frameworks founded on definition of k-anonymity, differential privacy, or mix-zones can, although with limitations, preserve location privacy of individuals.

2.4.1 Security threats in Ultra-dense networks

Motivated by the forecast of wireless traffic in the years to come, network densification represents a viable solution to cope with scarce spectrum resources. The idea behind the network densification trend is that network performance in term of bandwidth, spectrum reuse, network capacity, and energy consumption can improve through proper access points deployment. Densification is fulfilled by positioning small cell access points indoors in buildings, and outdoors in public areas. Both small and macro cells coexist in a multi-tier, software-defined network architecture. In UDNs, small cells can be classified into pico and femto cells (i.e., fully-functioning base stations, capable of perform all the functions of the protocol stack within a limited coverage area) and macro-extensions access systems (such as Relays and Remote Radio Heads, that extends the signal coverage and can perform some or all physical layers functions of the protocol stack)[21]. Follows a brief overview of the characteristics and challenges of ultra-dense networks Users are surrounded by many small cells with a low power and small footprint. The inter-site distance is of the order at maximum of tens meters.

For the sake of interference and energy consumption reduction, small cells are not all active at the same time instant. In particular, small cells can be turned on and off depending on connectivity demand by users and in consideration of the aforementioned optimisations.

Drastic interference between neighbouring cells limits network densification. To this aim, strict interference management schemes are required to mitigate the inter-cell interferences.

Unfortunately, one of the main limits of k-anonymity-based approaches is that k-anonymity cannot be proved to be satisfied without considering adversary's auxiliary information. Recently, because of its independence from the prior knowledge of the adversary, differential privacy has gained momentum. Anyway, both differential privacy and its derived definitions (e.g., geo-indistinguishability) still appear impractical for protecting of spatiotemporal in-formation. Introduced the notion of anonymity which can be seen as a variation of -anonymity. It has been conceived to attain the uninformative principle, thus guaranteeing that an adversary cannot infer from eavesdropped information longer fragment of users' trajectories. However, since k-anonymity is a special case of anonymity and for the sake of simplicity, in this thesis we make use of k-anonymity as a metric for measuring location privacy [23].

2.4.2 Security and Privacy in the IOT

The concept of the IOT was introduced as long ago as 1999 with the diffusion of Wireless Sensor Network technologies and the spread of the Radio Frequency Identification techniques.

The IOT is a network of physical objects, smart and personal devices (such as smart-watches, smartphones), health monitors, vehicles, buildings, and appliances (and many other entities) that are revolutionising in many ways our daily lives. Devices can sense and send information to remote servers, communicate and cooperate with each other, and take decisions autonomously on our behalf. By elaborating and properly combining the acquired information, new smart entities such as smart homes, smart cities, healthcare and intelligent transport systems can spring into life [24]. The overwhelming growing rate of the number of interconnected devices was already discernible in early 2012, since yet then there were more than nine billion IOT devices active worldwide.

These impressive numbers were and will be propelled by the financial market and in various domains, such as healthcare, public services and transportation. In the near future, the number of

wirelessly connected devices will dramatically increase and hugely influence the design and requirements of next-generation cellular networks. However, the notable IOT diffusion and potential interaction among a huge number of entities might lead to worrying security issues.

This is further supported by the statements of the Defence Advance Research Project Agency (DARPA) on the difficulty to establish a general-purpose security strategy model for the IOT.

In addition, several challenges in term of scalability, latency, the reliability of messages delivery, management of intermittent transmission behaviour and support of multiple wireless technologies need to be addressed. Because of design trade-offs in term of cost, complexity, and energy consumption, many devices in the IOT are usually resource-limited. As to cope with unauthorised access, data theft, and eavesdropping's, devices should be provided with authentication, authorisation mechanisms, and data preservation capabilities, ensuring freshness, authenticity, confidentiality, and integrity of information. Privacy (i.e., unlikability, data secrecy, and anonymity) should be accurately preserved since personal and sensitive information could be stolen and abused by an adversary. In particular, sensitive data should be preserved by encryption before of being sent, since it prevents that transmitted data can be intercepted and easily read by passive adversaries [25]. Nevertheless, encrypting the information might re-quire using computationally expensive cryptographic primitives (e.g. pairing- based cryptography), which could not be executed by every IOT device. In order to identify suitable cryptographic approaches for the IOT, [25] measured the performance of the most used primitives (such as RSA, secure hashing algorithms and AES) on some of the most common micro-controllers (ARM, MSP430f X) equipping IOT devices. They found that while operations of hashing and symmetric ciphering take few milliseconds and can also run on very limited microcontrollers, stronger approaches, such as RSA asymmetric signing (by a 2048-bit private key), can cause delays into hundreds of milliseconds, which are intolerable in real-time IOT applications. Computationally complex operations could be carried out remotely or on communication gateways. Although they determine a reduction of both energy consumption and computation for devices, these approaches require trustful gateways and protected communications. Pseudonymization can hide the real identity of both devices and users. Hence, it could be a viable technique to protect entities from being traced. Anyway, as suggested in and in,

when they act within a sufficiently wide time window of observation, eavesdroppers might disclose real victims 'identifier. For ex-ample, as described later in this thesis, when they connect to an LTE-based network, IOT devices can decode messages broadcasted by E-UTRAN Node Bs (eNodeBs) to search for their (temporary or unique) identifier. A passive adversary could exploit decoded information to retrieve associations among temporary and unique identifier. Furthermore, colluding IOT users positioned in proximity of locations occasionally visited by the IOT target (i.e. the victim), even though protected by a pseudonym, might reveal to the attacker the target's real identity and its private activities[26].

In our knowledge of the IOT, confidentiality, trust, and privacy are main key issues to the development of IOT services and applications. Then, identifying and adopting a privacy framework for the IOT is of paramount importance Furthermore, since they are provided with internet connectivity, the IOT devices can be exposed to a long list of threats such as, to name a few, the Denial of Service (DOS), Distributed Denial of Service (DDOS), SYN Flood, and Smurfing attack. As to mitigate advanced persistent threats against the IOT, the authors of proposed the Network Attack and Defence Framework (NADF) and provided a quantitative evaluation of the effectiveness of their approach. Since NADF is built upon the ZF, it can manage the security problem from both microscopic and macroscopic point of view, involving management, technology, and strategies for security.

The IOT is a very complicated ecosystem, whose protection would require both a holistic and specialised approach and that should span from the software to the network side. Then, we envisage that the research direction described in is viable to assess security risk for the IOT. Anyway, this work does not study the IOT privacy problem, which is closely related to security, but most focuses on data protection and the right on data. The privacy issue in the IOT is discussed. In their work, authors provide a comprehensive overview of the IOT and on its privacy challenges, and draw our attention to the most important characteristics a privacy framework for the IOT should have, that is identity, temporal, location and query privacy in addition to interoperability, data minimisation, and accountability.

[27] call into question some past assumption about privacy-by-design strategies. In particular, authors claim that minimisation of data acquisition, storage, retention time, number of data source, and granularity in conjunction with encryption of data, communications, processing, and hiding of

routing and location information, could lessen the privacy risk in term of unauthorised access and misuse of data. Authors claimed that exploiting cryptographic approaches can guarantee the privacy in the IOT.

Moreover, they stated that anonymous routing systems (e.g., TOR) is a viable direction to hide the routing traffic in the IOT. Even if assumptions in seems to be well-founded, this study they overlook the technological limitations that may affect IOT devices in their analysis of privacy requirements for the IOT, [28] question the need for embedding privacy engineering methods into IOT systems and applications. They underlined that apparently non-personal information, when linked together, may disclose personal and sensitive information on IOT users and their activities. They marked a distinction between a privacy framework and a privacy engineering framework. In particular, the latter extends the former providing reference to well-known privacy engineering fundamentals or concepts (i.e., privacy engineering and privacy-by-design, privacy objectives, and privacy properties to be protected), identifying actors (i.e., the stakeholders) and their roles within a system. Moreover, it includes protection of privacy engineering and common privacy engineering terminologies. In addition, made a distinction between privacy engineering for IOT subsystem and privacy engineering for IOT system. In particular, they defined a subsystem of the IOT as an independent entity upon which the IOT system is built. By integrating sub-systems together, it is possible to provide the IOT system with functionalities it needs. As an example, the LTE cellular network when providing wireless connectivity to devices is a subsystem for the IOT [28]. In general, suppliers of IOT subsystems are not aware of IOT-specific systems and applications requirements. Then, keen attention should be paid from the IOT system engineering perspective to prevent and manage security and privacy issues that can derive from heterogeneous system integration [29].

2.5 HETEROGENEOUS NETWORKS (HETNET)

Heterogeneous networks (HetNet) are critical towards low-cost, high-capacity 5G communication network deployment. The growth in data rate could only be met by making use of dense HetNet. Stringent latency requirements bring new challenges in secure handover and authentication in 5G HetNets. The frequency of handovers increases the challenge due to the dense nature of networks. SDN will play a major role in 5G networks. Centralized control over the network and the ability

to manage the network with high-level application programming interface (API) makes SDN a desirable technology in 5G. One of the main advantages of SDN is the deployment of policies on devices from the management layer. A low-level conjuration of each device is not required anymore, with the help of SDN controller the network API's can achieve this task easily. E client routing path can be created dynamically based on changing network tra c patterns. From a security perspective, SDN architecture could be leveraged to deploy security procedures more efficiently [30]. Our contribution is to provide a method, to perform secure handover authentication and key management using SDN, which can meet the requirements of a 5G network. Mobile data has been growing at fast rate. With the advent of new technologies, this trend is expected to continue. A recent survey concluded that the growth rate is projected to continue at 53% compound annual rate till 2020 and the monthly mobile track generated will reach 30 Exabyte by that time. 5G networks are expected to cope with the data. In addition to the data rate support, next generation networks are expected to be reliable, efficient, and secure [31].

Support of Heterogeneous networks (HetNet) will be a cornerstone in pursuing the goal of support for a higher data rate in 5G networks. In HetNets, a small cell such as microcell, femtocell, picocell and wi access points can be used to o oad a great share of the network tra c load. Network operator's operating expense and capital expenditure will be reduced by supporting HetNets. The study in highlights that 50% of the monthly mobile data tra c is being o oaded through femtocells or In 5G networks, HetNet will be increasingly used to complement the coverage and capacity of the conventional cellular network. Secure handovers, under the delay requirements, are one of the main challenges for a 5G HetNet.Some of the main features expected from 5G networks are to provide an uninterrupted connectivity, high-speed connection, and low latency [32]. The industry standard for the 5G networks are still in infancy stage, but the requirements and expectation for the 5G network have been laid down. Devices are expected to connect ubiquitously. Extremely low latency of 1 ms is expected from 5G Support for data rates in the order of 10-100 Gb per second is expected. Support for data volume 10Tb/s/Km2, reliability of 99.999%, connections up to 1M terminal/km2 and service deployment time of 90 minutes is expected from 5G A detailed survey of the 5G network has been presented in a multi-tiered architecture has been adopted for 5G networks where a macro base station covers many small cells inside it. The small cell will complement the coverage and capacity of the network. 5G HetNet will support the integration of different radio access technologies such as 3G, 4G, LTE, WiMAX, LTE-Unlicensed, LTE-

Advanced, mm-Wave Frequencies and Device to Device (D2D) communications' SDN will be one of the main technologies in 5G based LTE-Advanced networks. Low cost and ease of scalability are leading a shift towards SDN-based architecture. From a security perspective, SDN brings advantages as well as challenges [33]. Centralized control over the network means that it will be easier to monitor the network and gather trac statistics. SDN controller can run intrusion detection system to monitor for patterns of known attacks [34]. Once a pattern is detected it will be easier to isolate and x it. Such self-healing methods provide improved security as compared to traditional IP-based networks. SDN provides an improved resilience against denial-of-service attack (DoS attack) .

The forwarding device can be programmed to report a ow once it exceeds a certain tra c threshold within a period. A detailed survey on SDN security has been done. When a mobile device moves from the range of one base station to another base station, a handover takes place. First, the authentication process will occur where the user is identified and veri ed; next key establishment will take place [35]. At the end of key establishment process, both parties will have a shared key to communicate. The main entities involved are user equipment (UE), a base station (BS)/ eNodeB (eNB) and authentication servers such as AAA or HSS. For a secure handover, cryptographic messages are passed to establish new key between the destination BS and user equipment. Low latency requirements in 5G bring a challenge to perform this procedure within the latency requirement. A detailed survey of existing methods has been provided in chapter the existing methods of secure handover are unable to meet the latency requirements of 5G networks. There is a lack of a direct link in HetNet, so a secure communication channel is not available between source and destination AP. So far, the only solution for secure handover in SDN 5G has been presented.

2.6 SECURITY ANALYSIS

An informal analysis against a variety of attack is shown.

Mutual Authentication and Key Agreement.During the handover procedure, mutual authentication and key agreement will be es-tablished between UE and eNB. This has been proved through BAN analysis earlier. AVISPA simulation results given below also prove this security property.

User Anonymity

We use pseudo identity for UE and base stations. A new pseudo id will be assigned for each new session so the identity of any UE cannot be associated with a particular base station without the explicit mapping knowledge.

Non-Repudiation of Handover Request/Ack

This has been proved through BAN analysis. Handover Request and acknowledgment (Ack) are signed with the private keys which give a strong con rmation on the origin of the message. Nonce verifcation con rms the freshness of handover request and A

Parallel Session Attacks

Use of signature provides a veri cation on the origin of the message and it's integrity. Nonce generated during session are unique and as integrity of the message is veri ed, ipso facto information from one session will not be of use in another session. This type of attack is also tested through AVISPA simulation[36].

Binding Attack

Binding attack happens when an intruder tries to convince one of the base station on a compromised public key. Let's suppose eNBa wants to perform a handover procedure with eNBb, then in such an attack intruder I will try to convince eNBa that eNBb's public key is Ki. Certi cate timestamps will ensure the validity period of the certi cates. Forgery of a certi cate is non-feasible due to the computational complexity.

Replay Attack

Our scheme can withstand any replay attacks. The scheme uses random nonce for fresh-ness checking at the base stations and by authentication service. The nonce challenge will be rejected once a replayed message is returned[37].

Perfect Forward Secrecy

Perfect secrecy ensures that the adversary cannot compute the session keys even if the private keys of the participants are compromised. The session keys derivation uses a hash of security parameters

such as physical link properties, current location, direction, channel quality indicator[38]. The pseudo id's used are also per session based. Due to collision resistance property of the one way hash function, it will be computationally infeasible for an adversary to compute the session key.

Known Session Security Parameters

The proposed algorithm uses session security parameters for key derivations. Assuming a known adversary gets this information, he will still not be able to generate the key without knowledge of random nonce, ciphering and integrity keys.

Denial of Service Attack

DoS attacks can be handled through SDN based architecture. An intrusion detection service running at controller layer will detect if an unusual number of connections are requested during a time window through a speci c network node. The system can react by isolating the source and stopping the spread of tra c to other parts of the network. Furthermore, initial checking of security parameters could be performed at the source eNB without involving VAS so such a attack could be thwarted in the starting phase.

Typing Attack

In this type of attack, an intruder replaces a protocol message eld with another type. As we are sending hash of the message, any such change will result in a mismatch during hash veri cation. Furthermore the signatures will verify the integrity of messages. AVISPA simulation uses typed and un typed properties to verify such attacks.

Man-in-the-Middle Attack

The communication protocol uses signed messages and secret sharing. Without the secret, an intruder will not be able to impersonate.We conducted Literature review and extensive research and analysis of the environmental requirement for Securing 5G Network using low power wireless personal area network. We concluded that LPWANs with mesh topology were the choice for such tasks [38]. We then introduced artificial intelligence into the routing using machine learning in the algorithm to enable long-term energy awareness. Such energy awareness can be reflected on the routing decision made by the algorithm as the algorithm learning about the network. This thesis,

we proposed a reinforcement learning routing algorithm that can reduce the failure rate, improve energy efficiency and carrier band usage rate of wireless mesh networks for Securing 5G Network using low power wireless personal area network.

3. METHODOLOGY

The proposed reinforcement learning algorithm for increase the energy aware is designed for mesh topology from the ground up by the model of the network itself using low power personal area networks. We model the network operating in a region bounded by a finite number of randomly distributed nodes within the region in this algorithm. Hence, we have defined the service area of the target network assuming network limitations in the model. We then model the connection between the nodes in the network. In this model, we consider that any two nodes are adjacent when they are in a certain range and can establish an ad hoc connection between each other. This also models the connections in the network as we define the link as the connection between these nodes. However, not every two nodes in the range can establish a link between each other in this model because of the possible obstacle in between or zero battery power in either of the nodes. The model of the wireless channel as the network is set to be in the rural areas, we assume no coverage of all other kinds of wireless network services in the ISM band of choice. We also consider that the channel has certain interference (I) and background white noise (N). Hence, we can use the full capacity of the channel to reach the given rate of transmission. We can then calculate the maximum transmission rate (R) at the given Signal to Interference and Noise Ratio (SINR) of the channel based on Shannon–Hartley theorem and Shannon's noisy-channel coding theorem as shown in (3.1).

$$R = BW * log0(1 + SINR) \quad (3.1)$$

where BW represent the bandwidth of the carrier used in the transmission. In order to calculate the SINR of the transmissions, we modelled the channel as a fading channel with the path loss exponent α as well as the channel gain coefficient h.

3.1 THE MODEL OF THE LOW POWER WIRELESS AREA NETWORK

The networks show in this paper comprises of a specific number of nodes, with the connections between them. pre-defined gateway nodes, as we consider all nodes equivalent and the Internet

connection can be accessible at any nodes. Hence the elimination of a single point of failure

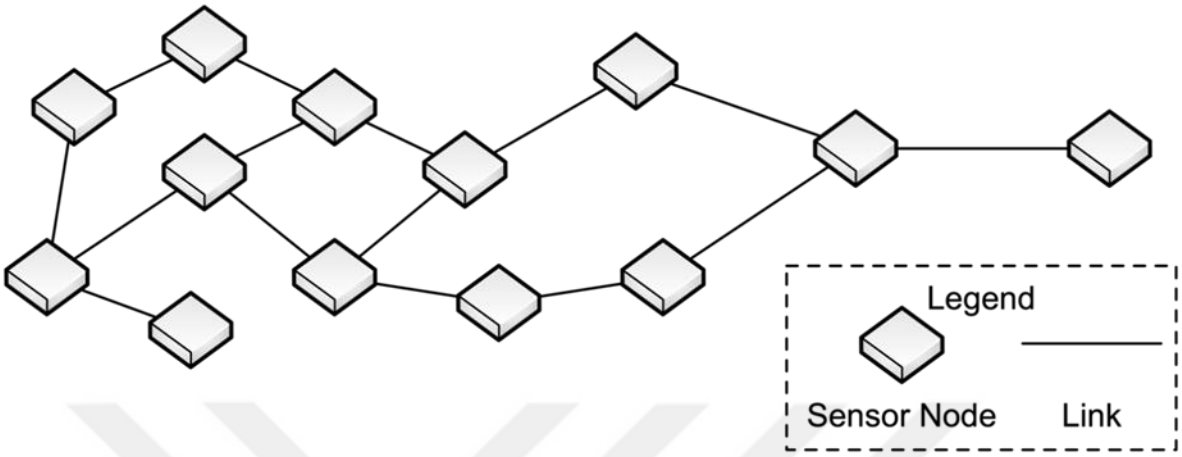

Figure 3.1: modelled network [39]

3.2 SENSOR NODES

In Figure 3.1 there is a simplified model of the sensor node structure as each sensor node contains an internal battery with constant capacity of Pmax,It is considered the only source of energy. At any point the remaining energy in the battery is considered as Pnow. For the sustainability of the node in the remote area. We consider that all nodes are connected to a solar charger. For the sake of simplicity of the model we emulate the charging process by resetting the Pnow to its maximum value (Pmax) after the period of a pre-defined charging cycle (CC) with the unit of time

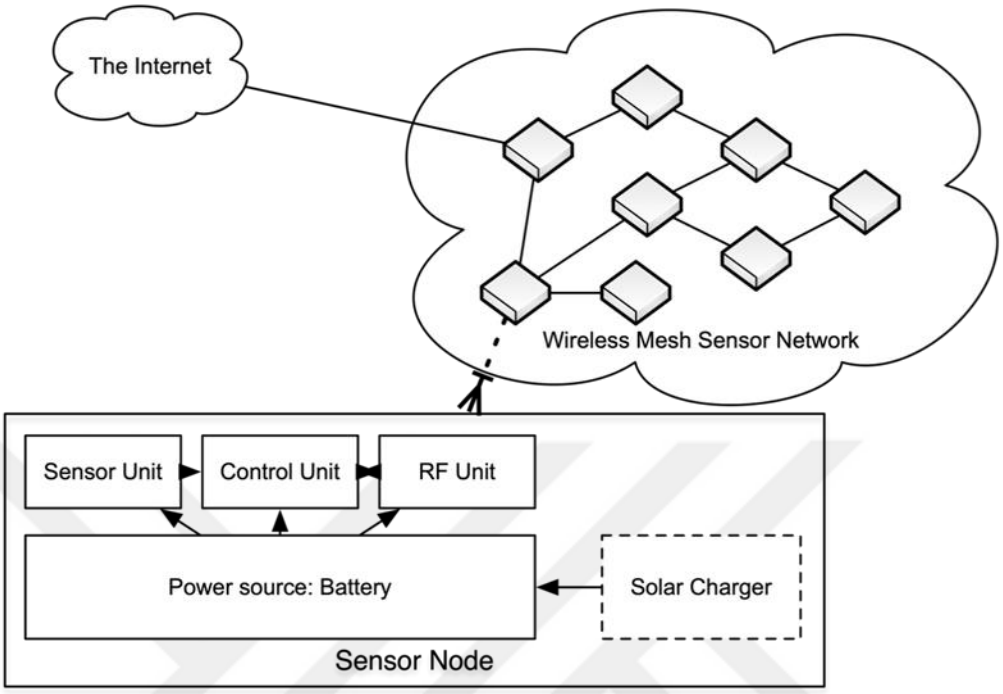

Figure 3.2: Structure of a sensor node [40]

Current solar panels are small enough and capable of powering up the sensor nodes. Here we provide a commercial example of such solar panel that is accessible as well as affordable for such networks. The size of this panel can be fitted onto most enclosures of the sensor nodes and the power output of the panel (Pcharge) is sufficient to charge the nodes consistently. There are many better solar panels in the industry, but such one can serve as a reference for evaluating the charging cycle. The battery gets recharged tcharge hours each day. Nowadays, most mobile devices use Li-ion batteries which have a very high charging efficiency and have a small discharge loss. We consider that the discharge loss is 0 because it is relatively small when compared with the operational discharge. We denote efficiency of the charging circuit as charge. We then can calculate the CC in the unit of days using

$$CC = \frac{P_{max}}{P_{charge} \times t_{charge} \times \eta_{PQRSTU}}$$

During the operation of the nodes, there may have several possible phases that consume the battery power:

1. Data collection;
2. Data processing;
3. Sleeping;
4. Transmitting;
5. Receiving;

The data collection phase means the sensor is working to collect the data needed for securing 5g. However, due to the huge possible variety of sensor applications can be used in the remote monitoring network, it is difficult to precisely model the power consumption of this phase. Besides, the transmission power is much greater than the working power consumption of the sensors. For example, LoRa radio chip SX1278 requires a typical supply current in transmitting mode of 120mA when the RF gain is 20 dBm, while in the receiving mode, it requires 11.5mA. Where an example of this total dissolved solids (TDS) water quality sensor has a working current of the entire module, including the probe, is 3-6 mA. Moreover, most of the time, the sensor will be in the sleeping phase to conserve battery, and the power consumption is minimal. Thus, we consider mainly the transmitting power when calculating the cost of each point-to-point transmission in the algorithm. However, we do factor the percentage of remaining power of the node (the ratio of Pnow / Pmax) into the cost function of the algorithm. Anyway, it is possible to include the power consumption of the sensors in the data collection phase in the calculation to reflect the cases of high-power sensor consumption when necessary. However, we put the focus of this paper on the more dominate transmission power in the present stage to have a better understanding of the impact of the decision of routing on the operation of the network.

Each node has a routing table stored in its control unit. The routing table keeps track of all the possible routes from that node to all possible nodes in the mesh network. It starts of the destination column and also has a next node column as oppose to gateway column in the traditional IP routing tables. The node keeps track of all its adjacent nodes using the next node column. As the network is not subdivided into subnets, there’s also no need for a netmask column where can be found in IP routing tables. The Routing Metric (RM) values of each route can be found in the next column.

The RM values indicate the likeliness of selecting the next node in the same row when routing to the designation node. Here we use the likeliness instead of the possibility of selection is because we use the Boltzmann exploration process to balance exploration and exploitation behaviour for the best result of the Low power wireless area network of this chapter. A visited column keeps track of how many times the node being visited, and this information is also used in the reinforcement learning process. An example of a Routing table of node 1 is presented in Table 3.1.

Table 3.1: An example of the routing table

Destination	Possible Next Node	Routing Metric	Times Visited
3	4	1	131
4	3	1.42	22
4	5	1.71	31
4	6	3.18	80
5	4	2.13	68
5	6	0.13	2
6	4	4.98	186
6	5	0.05	3

3.3 THE ROUTING DECISION PROCESS

The routing decision process of the algorithm is illustrated in the flowchart in Figure 3.3. All the routing process happens with in one single node in the network. This local decision process makes the algorithm totally distributed. With this nature of the algorithm, each individual node learns the network individually and when one of more nodes becomes offline, the rest of the nodes in the network still have their own information about the network and will eventually learn the changes that happened in the network. This eliminated not only the problem of having a single point of failure in the star networks but also makes the network more adaptive. The process begins from the SN choosing an NN from the routing table using the Boltzmann exploration. Then the SN will be added to the visited variable in the packet header.

If the chosen NN is the DN, the transmission is successful as the data has been delivered to the DN, and the feedback and updating process will occur Otherwise, all the nodes in the visited

variable in the header will be removed from the routing table of NN before it selects its next NN. The process will continue repeating itself with new NNs until the DN has been selected or when one of the NN's routing tables has no available nodes to select. When there are no more available nodes to be selected as the new NN, the algorithm will calculate the number of retries (NR) and compare it to the maximum allowed retry count (NRmax). If NR is smaller than NRmax, the algorithm will go back to the previous node and retry the process and 1 will be added to NR. If the NR is equal to or larger than NRmax, the routing will be considered failed. Once the routing process is finished, regardless of success or failure, feedback with the value calculated in (3.8a) will be transmitted to the nodes involved during the process.

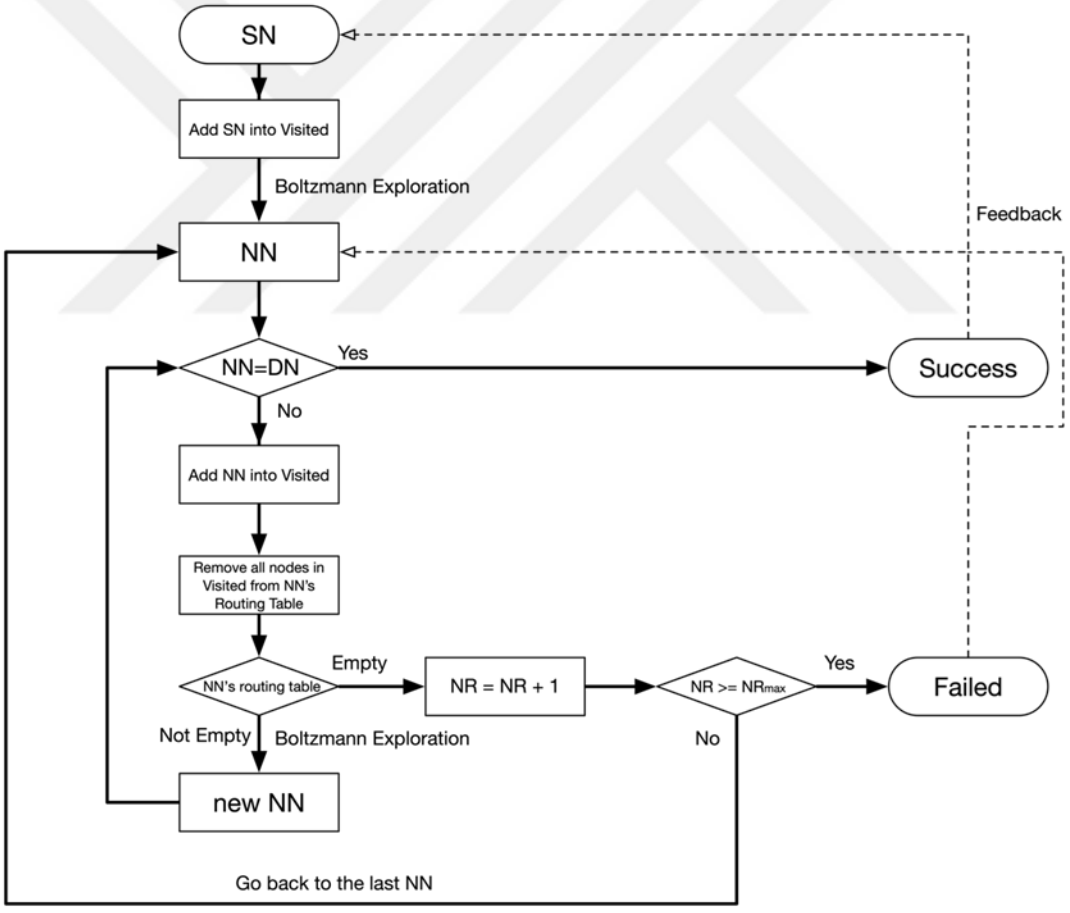

Figure 3.3: RL routing process

3.3.1 Feature Scaling

When training networks, it is considered to be the best practice to scale the data. Otherwise different problems can be encountered such as degraded performance, unpredictable behavior of optimization algorithm and exploding gradient. There are different ways to scale the data, some of them rely on knowing the maximum and minimum values for the distribution, and as the data is not in some predefined range like, e.g. pixel value data, the standardization method is chosen, that relies on computing the mean and variance of the train set.

3.3.2 Feature Selection

Some features of the data may be more important than others. This has been reflected by the works studying dimensionality reduction for botnet attack detection. By selecting a smaller number of features we will enable this work to be compared to other works and additionally demonstrate how neural network performance changes when applied to varying number of inputs.

3.4 TRAINING, VALIDATION, AND TESTING SETS

All of the data is divided for the different purposes in this segment in which the portion of the data for the training will draw direct conclusions from the validation data. But If the accuracy of the validation set drops below the results of the training data, the network is starting to memorize the data it knows rather than generalizing on the concept.

This subset that will go through the process of testing is called testing data. In contrast to the validation set, it's only used once in the very end, to give a final score. The idea is that by building a model based on the validation results a certain amount of information bleed occurs, where the network will implicitly learn from the validation data. In order to avoid bad results, testing data is normally used as a reference for the performance.

- Training Set: 72% of the data
- Validation Set: 15% of the data
- Test Set: 13% of the data

3.5 EVALUATION MATRICS

For the task of more accurate values, we can apply a two-class confusion matrix to evaluate our results as in Table 3.2.

Table 3.2: Confusion matrix classes for predicting normal or predicting 5g attack.

	Predicted normal	**Predicted attack**
Actual normal	True Negative (TN)	False Positive (FP)
Actual attack	False Negative (FN)	True Positive (TP)

Accuracy can then be defined as (4).

$$ACC = \frac{TP+TN}{TP+TN+FP+FN} \quad (4)$$

And precision as (5).

$$PR = \frac{TP}{TP+FP} \quad (5)$$

False positive rate will be defined as (6).

$$FPR = \frac{FP}{FP+TN} \quad (6)$$

Similarly, accuracy can be computed for more than 2 classes. Also, for our machine learning models, we can also measure how long does the training take in seconds to achieve good accuracy and how complex the model is, meaning how many parameters does it contain and how much does it weight when saved to disk.

4. RESULTS

To evaluate the performance of the reinforcement learning for increase energy aware for wirless sensor networks using low power wireless area network, we established a series of simulations with different learning variables to assess the performance of the reinforcement learning against the two benchmark LPWANs. Different advanced toolboxes in Matlab i.e. Antenna Toolbox, Machine Learning Toolbox, Wireless Toolbox is used. First, we established a simulation environment that is based on that of the remote Low power wireless area network model. We started by defining the characteristics of the channel used in the simulations. When determining the path loss exponent. We considered the network as a far- field communication scenario. Given that the network is being remotely deployed, the typical value between of 2.7 to 3.5 was selected for describing the open area mobile radio environment. In the simulations in this paper, we assumed the empirical value of 2.8 for the environment of the remote monitoring network's low multi-path channel. Similarly, the network is likely to have little fluctuation due to the infrequent human activities in the place where it is operational, we also assumed a fixed channel gain h of 2. The ambient noise (N) of the channel was assumed at the level of -110 dBm for the same reason. Besides, having a clear radio spectrum means that the adjacent- channel interference (ACI) does not exist, and the only interference can happen is co-channel interference (CCI) when two or more transmissions arrived at the same node at the same time. We can also utilize non-overlapping channels for simultaneous transmissions, this assumption is technically feasible. We also understand that these assumptions may not best describe the practical dynamic communication environment, therefore further detailed study of these specific parameters will be performed in the future work. In this paper, we focus more on the failure rate, energy efficiencies and carrier band usage rate (CBUR) serving as the foundation for the future work. We set up a series of simulations to compare the performance of the reinforcement learning LPWAN against the lower bound benchmark, i.e. the random LPWAN and the upper bound benchmark, i.e. the centralized shortest path first LPWAN.

The computer we used for the simulation the experiment is carried using Matlab R2019a Windows environment on 32GB RAM and 2.9 GHz Intel Core i9. After carrying out several experiments using the artificial neural network, we have come to present all our findings here. We carried out artificial neural network algorithms on our data-set. The results are described in the table. We have

done the test procedure with 25 percent data which is equal to 13889 data. All tests were run on a dual 12 core AMD Magny Cours equipped with a NVIDIA Tesla C2050 GPU with 14 Streaming Processors (32 cores each). The artificial neural network was created and trained on all 115 features. Default Keras optimization hyper-parameters were used. Training was limited to 100 epochs with additional condition of early stopping, using functionality provided by Keras. This ensures that the model is trained only until the score on validation set is not getting worse – this in turn helps to avoid overfitting the training set.For each parameter we investigated, we ran the simulations over 3 different scales of networks with 7, 20, 50 nodes within an area of 20*20 km2 space to represent different scales of networks on the computer with the specification. The choice of such area and scale was considering the accessibility of the internet from either cable or mobile networks in remote areas so that the data collected by the nodes can be uploaded. The 3 different scales of nodes represented low, medium, and high density of node coverage in that area. These 3 densities can be considered small, medium and large scale of the network, as the complexity of the network increases as more nodes are involved. Each simulation consisted of 52560 timeslots of 10 minutes each to simulate the one- year total operational time of the network. We executed each simulation of each scale of network for 5 times and averaged the results of these simulations for better precision. The transmissions happen randomly, with a 20% chance to initiate in any timeslot. Each timeslot was capped with initiating 3 maximum transmissions. This made a total approximate number of 31,500 transmissions in each simulation. The difference the maximum transmission range of each node in the simulation. However, in all other simulations, we fixed the range to 10km. We also studied the performance of the network under different charging cycles to reflect different weather conditions. In all other simulations, a fixed charging cycle of 5 days (720 timeslots) is implemented.

Regarding the fixed parameters about the node, we assumed that the battery size of each node (Pmax) was 20 Wh. We chose this value based on the constraint of the size of the sensor node. The battery capacity of a smartphone with good a battery life, such as Huawei Mate 20 Pro, was used as a reference here. That smart phone has a typical battery capacity of 4200 mAh, operating at 3.7V, the energy it stores can be calculated by 4200mAh*3.7V = 15. 54Wh.We also chose the transmission bandwidth (BW) to be 125 kHz as it is the minimum transmission bandwidth of LoRa to reflect the extreme case. We also chose a fixed transmission rate (R) of 5 kbps for all the transmissions in the simulations. The choice of this transmission rate is in line with the LoRa

network with spread factor 7 in 125 kHz bandwidth. In order to avoid looping and infinite retries when finding routes, we also have defined the maximum number of retry NRmax = 10 in all simulations. We also fixed the weight (W1, W2 and W3) used in the cost function (3.6) to emphasize on the transmitting power first and then the remaining power of the receiver, before the power of the sending node. This will lead the algorithm to pick a route with less chance of failure, as the receiver has more power left for forwarding the packet on. We used these numbers based on our previous trials on the algorithm. All the empirical fixed parameters used in the simulation can be found in Table 4.1:

Table 4.1: Fixed parameters used in the simulation

BW (kHz)	N (dBm)	α	h	I	R (kbps)
115	-110	2.8	2	0	5
P_{max} (Wh)	NR_{max}	W_1	W_2	W_3	
20	10	1	0.1	0.3	

we used the exact same method to randomly generate networks for the simulations of each scale. The number of transmissions for the small-scale 7- node networks was 31611, for mid-sized 20-node networks was 31497, where for the large-scale 50-node networks was 31605. These simulations were also performed with 5 different values (0.1, 0.2, 0.5, 0.8 and 1).

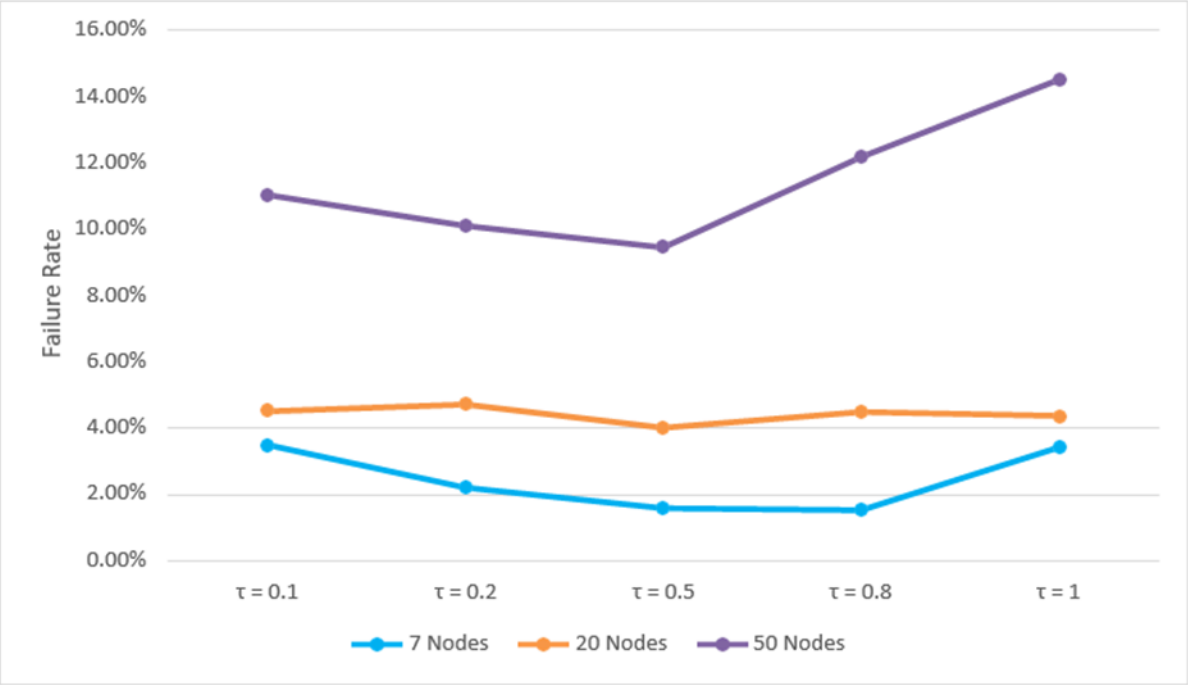

Figure 4.1: Average failure rates

Figure 4.1 shows the results of the average failure rate using the same set of topologies and transmission settings with different Boltzmann exploration hyper- parameter (τ) values. We averaged all the failure rates results of a series of 5 simulations. As shown in Figure 4.1, the average failure rate of the transmissions was raised as the number of nodes increased. The result of the failure rate of 50- node large scare networks is much higher than the smaller scale networks. This phenomenon was expected as more nodes in the network will result in more legs in each transmission. Hence, there is a higher chance of generating route loops, which leads to failed transmissions. However, among all 3 different scale networks with the values we tested, we found that the optimum τ value was 0.5. It resulted in the lowest average failure rate in all 3 scales of networks. As the τ value controls the spread of possibility, this result can be explained with a small value of τ the algorithm will be more exploitive of the learnt information, more likely to rely on the same route. This may exhaust the battery of the nodes on that route and is less responsive to the changes in the network. In contrast, a large τ value will even out the different of the likeliness routing metrics stored in the routing table. This will result in a more explorative behavior, making the route selection more random rather than taking advantage of learnt information about the network. We found that the τ value of 0.5 strikes the best balance both exploration and exploitation

in the tested networks with the best result. With the algorithm in place, all the failure rates met the target we set in the beginning part of this chapter, which is lower than 5% for the 7-node and 20-node network and 10% for the 50-node network. We then compare the reinforcement learning LPWAN with the value of 0.5 against the upper bound CSPF and lower random routing benchmarks in all 3 scales of networks. The results are shown in Figure 4.2.

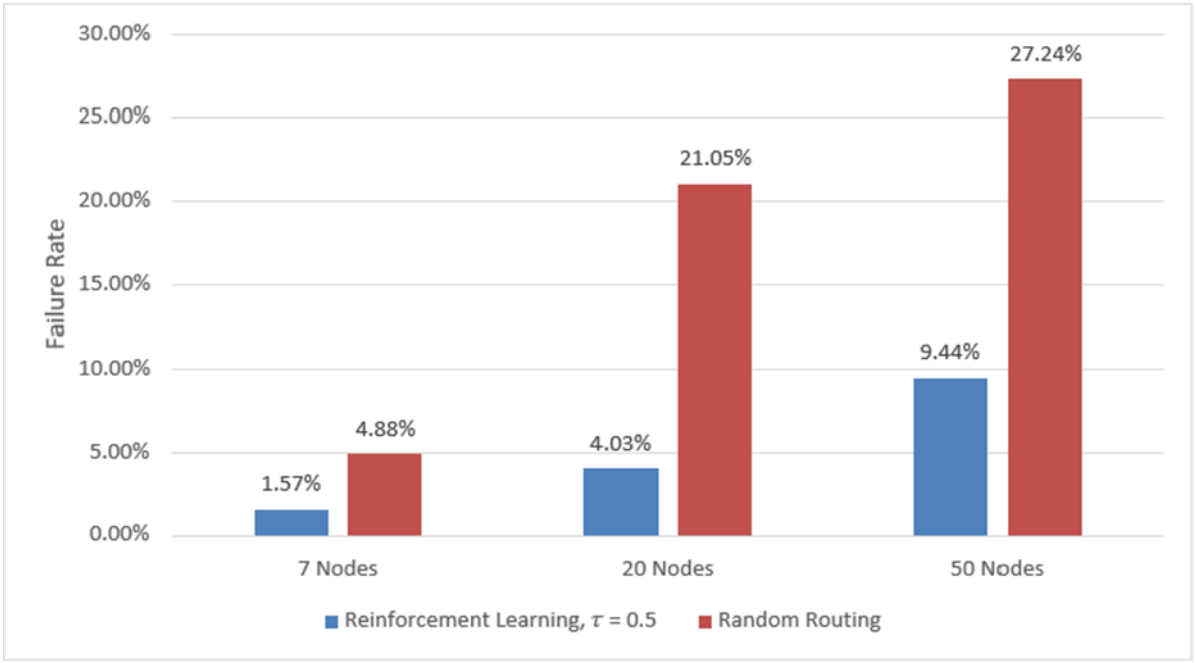

Figure 4.2: Average failure rates using RL, random LPWANs

Figure 4.2 shows the comparison of the average failure rate between the RL and LPWAN with the τ value of 0.5 against the random LPWAN. The result of the CSPF algorithm for securing 5g networks was omitted here as it scored a constant 0% failure rate at all times. We found that the average failure rate of reinforcement learning LPWAN is much lower than that of the random low power wireless area network in both situations of all 3 scales of networks, only at only around 1/5 for the 20-node networks and 1/3 for the 7-node and 50-node networks. This is because of the learning algorithm use the learnt information to avoid lower powered nodes as the RM values are updated with the cost function (3.6) where the remaining power of both nodes are also taken into account. The possibility of selecting the low powered route is reduced. Especially with a reasonable τ value to balance exploration and exploitation to take advantage of possible alternative routes. Without this knowledge of the network, random routing can only randomly pick the route,

resulting in a higher failure rate. The CSPF algorithm eliminated the failed transmissions as it manages the entire network, and the best available route is always utilised. Figure 4.2 also shows the change the RL algorithm brings to the result by making the network meet the failure rate target. Figure 4.3 shows the result of average energy efficiency of the series of τ values (0.1, 0.2, 0.5, 0.8 and 1) in the same set of simulations, where Figure 4.4 illustrates the comparisons between when the best result of $\tau = 0.5$ from Figure 4.3 and 4.4 are applied to the RL LPWAN against benchmark algorithms in the simulations of networks with different scales.

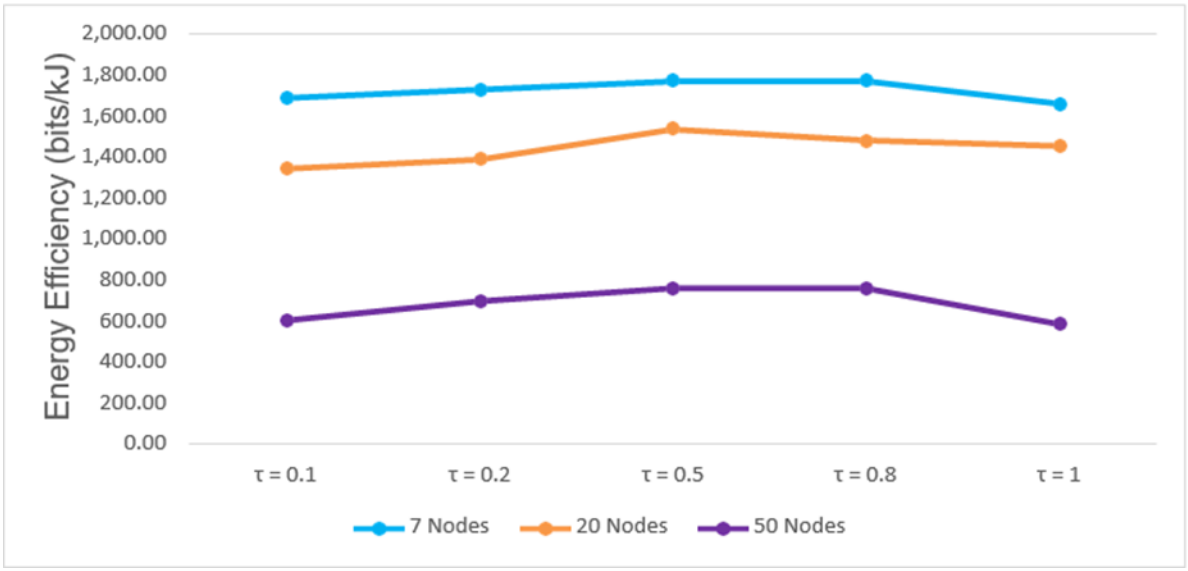

Figure 4.3: Average efficiencies.

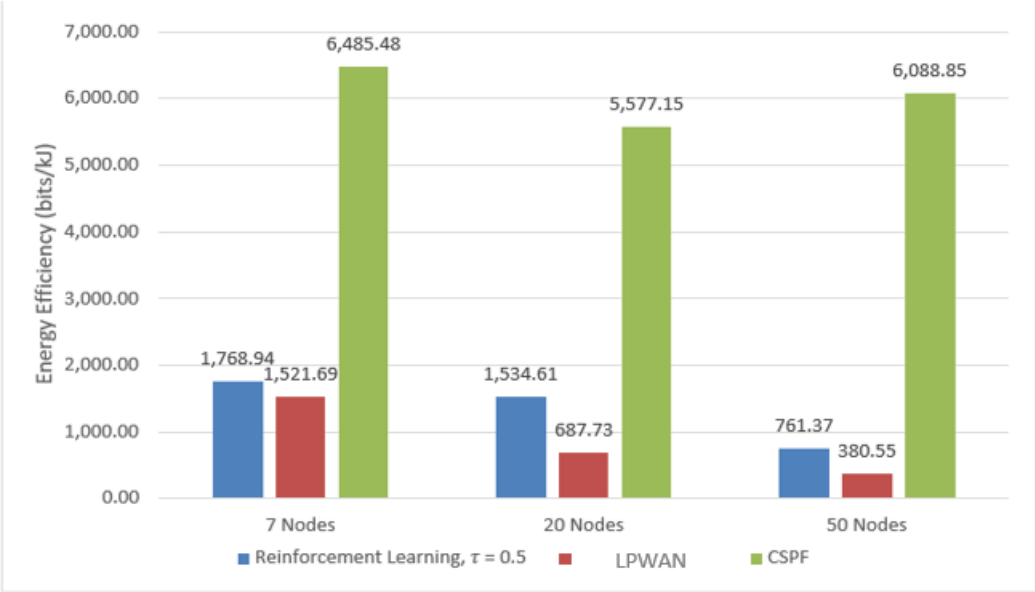

Figure 4.4: Average efficiencies using reinforcement learning, LPWAN and CSPF algorithms.

The results were similar to what can be found in the average failure rates. The upper bound benchmark CSPF algorithm had a significant advantage due to the ability to pick the best energy-efficient route at all time. This route may usually be the shortest route available and the lack of trial and learn progress from the RL algorithm, hence the much higher efficiency. Whilst the random LPWAN, being the lower bound benchmark, was trailing behind both other algorithms. The difference between the random LPWAN and the reinforcement learning LPWAN was less prominent in the 7-node network.

This is due to the less available links between nodes leads to a lack of choice for the routes for the RL LPWAN to learn from. For the larger scale networks, the reinforcement learning LPWAN had outperformed the lower benchmark. Among the different τ values in the reinforcement learning LPWAN, the energy efficiency of both $\tau = 0.5$ and $\tau = 0.8$ were consistently higher than all other τ values. In the 7-node network scenario, the performance of all τ values were quite comparable, the same reason as the lack of choice mentioned when compared with random routing. In the large 50-node network simulation. $\tau = 0.1$ and $\tau = 1$ were much lower than other values as too much exploration may behave like random routing while too much exploitation will also exhaust nodes along a certain route, leading to worse results. Generally, from the result of this simulation the performance of all five simulations of reinforcement learning LPWAN were better than the random routing benchmark in average energy efficiency.

4.1 THE IMPACT OF THE CHARGING CYCLE OF THE NODES

We also assumed no other power consumption such as power leakage in the process for the ease of calculation in the simulation. Throughout a year, the average hour of sunlight in the Turkey is 3.76 per day, and 6.00 per day during the longest sunlight month (May), while only 1.32 per day when it is the shortest month (December). We can then use this data to calculate the charging cycle (CC) in the unit of days we use in the simulation for the environment of the Turkey using the equation Where CCdays stands for charging cycles measured in days, Pmax was 20Wh for each node in the simulations in this thesis, Pcharge was 1W in the case of the example solar panel mentioned earlier, charge for the charging efficiency, which was 0.8 in this case. We then

calculated the charging cycle of the average, best case and worse case for the simulation is 3.125, 4.98 and 14.20 days respectively.

To roundup for the ease of representation, we choose 3 days, 5 days and 15 days in the simulation. This selection of charging cycles represented the actual climate conditions in the context of deployment of remote monitoring devices for the rural areas in the Turkey. We then converted the CCdays into CCtimeslots that can be used in the simulation

$$CC_{\text{timeslots}} = CC_{\text{days}} \times N_{\text{timeslot per day}}$$

where Ntimeslot per day represents the number of timeslots per day, and in this simulation is 144 for the 10 minute-timeslot. Hence, the CCtimeslots is 432, 720 and 2160 for the best, average and worst climate scenario, respectively. We then used these CCtimeslots in the simulation with optimal learning parameters. We plotted the results of the comparison between failure rates of reinforcement learning routing and random routing under different charging cycles in Figure

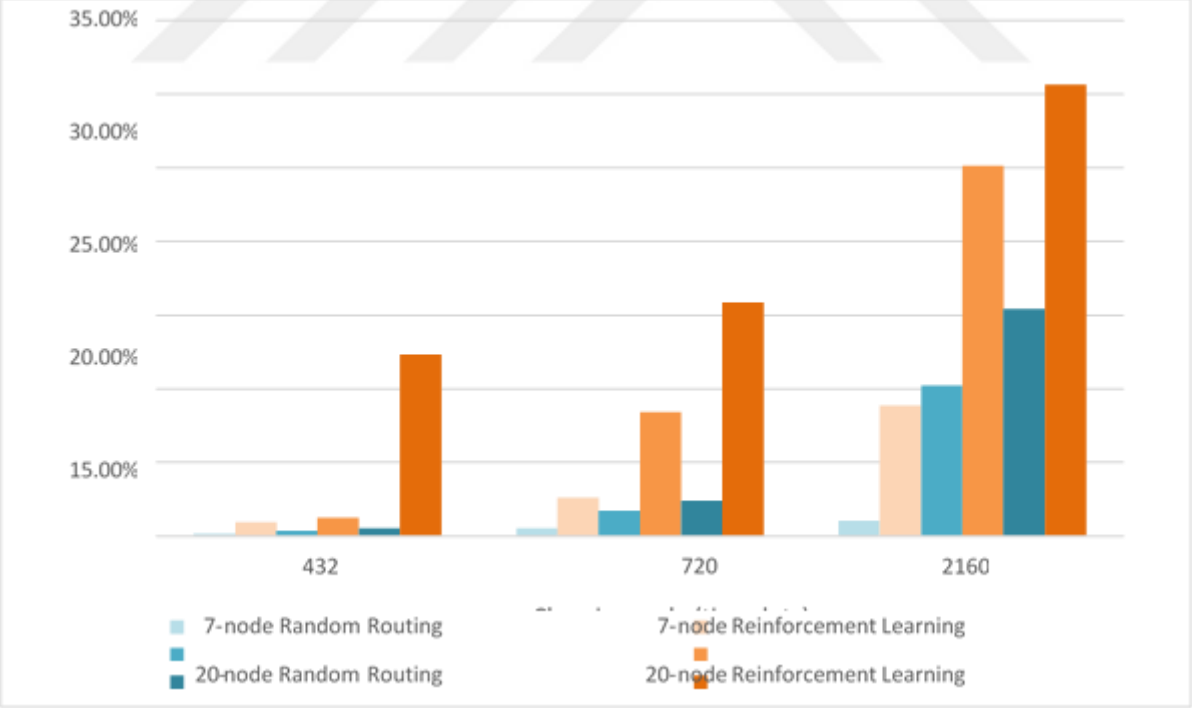

Figure 4.5: Average failure rates under different charging cycles

As shown in Figure 4.5, with the increase of the charging cycle, the failure rate of both the random routing and the reinforcement learning routing algorithm increased accordingly. However, the

random routing algorithm suffered a greater impact on the 50-node network with more than 30 percent transmission failed with the 2160-timeslot charging cycle. It also failed 12.33% and 15.86% of all transmissions even with the 432 and 720-timeslot charging cycle respectively on the 50-node network. In the smaller networks, the failure rates were lower for the random routing, but with the 2160-timeslot charging cycle, it still had a 25.13% failure rate on the 50-node network. This made random routing unusable when the network is large and charging cycle is long, such as a large-scale monitoring network in the unpredictable climate of the rural areas. The same trend can also be found for the reinforcement learning routing algorithms as well, however, the reinforcement learning routing algorithm was significantly more resilient to such extension of the charging cycle. The worst result appeared in the 50-node network with a 2160-timeslot charging cycle. 15.4% of failure rate for the size of the network and the length of the charging cycle was much more usable than the random routing. In this case, the network become quite unusable as the failure rate is 50% higher than the target we set in the earlier part of this chapter. However, given the fact that 2160 timeslots are equivalent of 15 days, this failure rate is not that bad as the number suggested. The entire month of December has only 2 of this 15-day charging circles. Just like previous simulations, the CSPF algorithms always kept 0 failure of all simulation because of the up-to-date knowledge of the network which has been omitted in this figure. The results here demonstrated the advantage of the reinforcement learning routing over the traditional random routing for the remote monitoring IOT networks in the context of the climate of the Turkey.

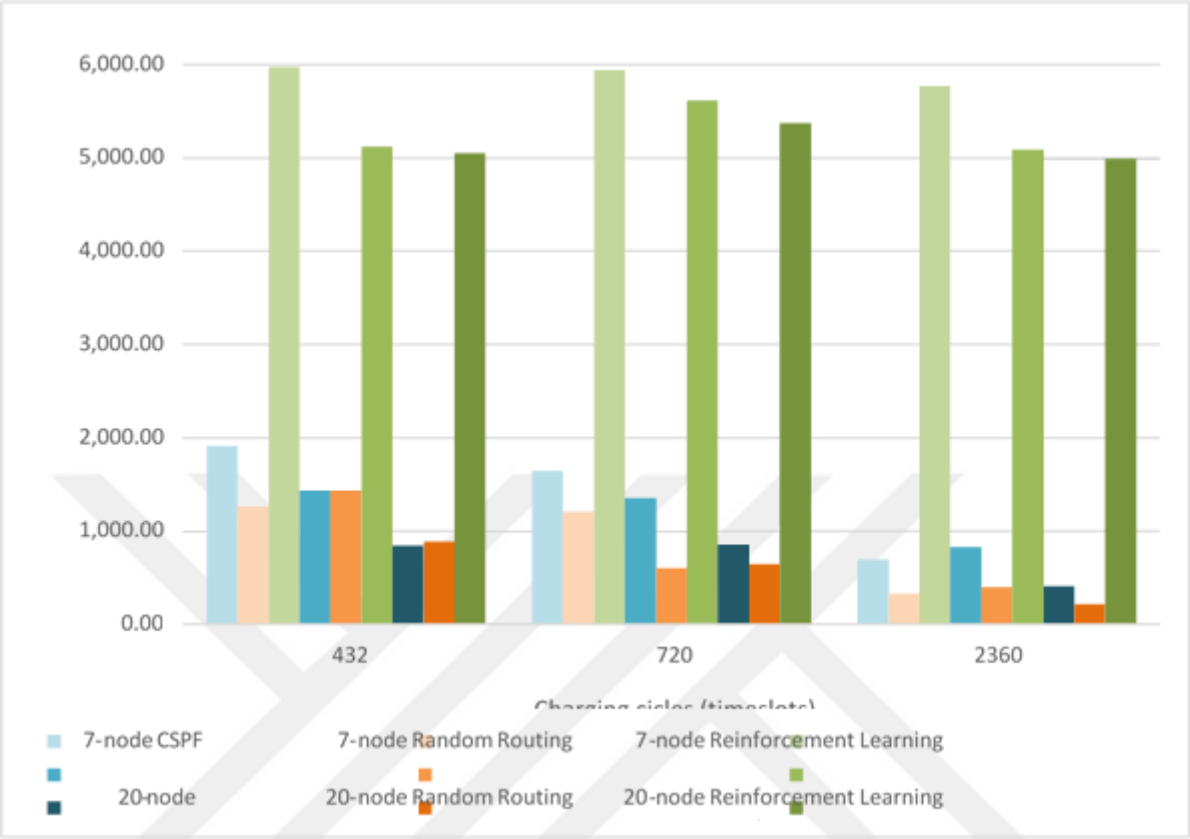

Figure 4.6: Average of the efficiency under different charging cycles

We then looked into the impact of charging cycles on the energy efficiency of the network with different routing options in different network scales. As can be seen on Figure 4.6, the effect of the charging cycles on the CSPF algorithm was minimal. As it is based on the centralized information, the CSPF can always work out the efficient route at any time. The energy efficiency has dropped with the increasing of the number of nodes. This is the same trend we observed, the increase of complexity of the network will make the route longer for each transmission, hence, the decrease of the energy efficiency. However, it can also be observed that the impact of the extended charging cycle impairs the random routing more than the reinforcement learning routing algorithm. When the charging cycle changed from 432 to 720 timeslots, the average energy efficiency of the random routing had dropped 31.6% while the reinforcement learning routing had only 8.1%. The decrease from the 720-timeslot and the 2360-timeslot were 62.4% and 50.1% respectively. The biggest decrease of the random routing was more than 58.4% from 432 to 720 timeslots in the 20-node network and 66.3% from 720 to 2360 timeslots in the 50-node network whilst for the reinforcement learning routing algorithm was only 15% from 432 to 720 timeslots in the 7-node

network and 58.2% from 432 to 720 timeslots in the 7- node network. It is notable that the RL routing algorithm only better than the random routing marginally in 7-node network simulations, because of the lack of availability of selection of routes. The difference between the random routing and reinforcement learning routing algorithm in the larger networks and with longer charging cycles were much more significant when the learnt information is able to put into use. It is also noticeable that in case the 432-timeslot, 50-node network that the random routing has slightly better performance than the RL routing for Securing 5G Network using low power wireless personal area network. This can be explained when the charging circle is so short and the network work is so simple, the network has not much information to be learned from.

Nodes are mostly at its maximum power states and the routes are very simple. This resulted in this singularity. Except that, this general trend proves the benefit deploying RL routing over the random routing. The much less overhead RL routing brings about in comparison to the huge required computational power of the CSPF stated in Chapter 5 also proves the value of RL routing algorithm for the realistic remote monitoring sensing scenarios.

5. DISCUSSION

Privacy has been a talking point in previous technologies and continues to be one in 5G, as it is one of the subjects that everyone can chime in on. From the point of view of the users, the concerns arise from identity, data and location of your personal information. Many of the mobile phone applications these days require you to give them some sort of personal information before you can even download it.. It is not often mentioned how and where the data is stored or for what purpose it is used. This gives users a veil of shadow and uncertainty considering their own personal information. The location privacy can be leaked on the physical layer level because of the access point selection in 5G. If a malicious station is selected, the user's privacy is compromised. Attacks targeted at IMSI are threats as well. They aim to reveal the identity of the owner of the device that is targeted by this catching attack.

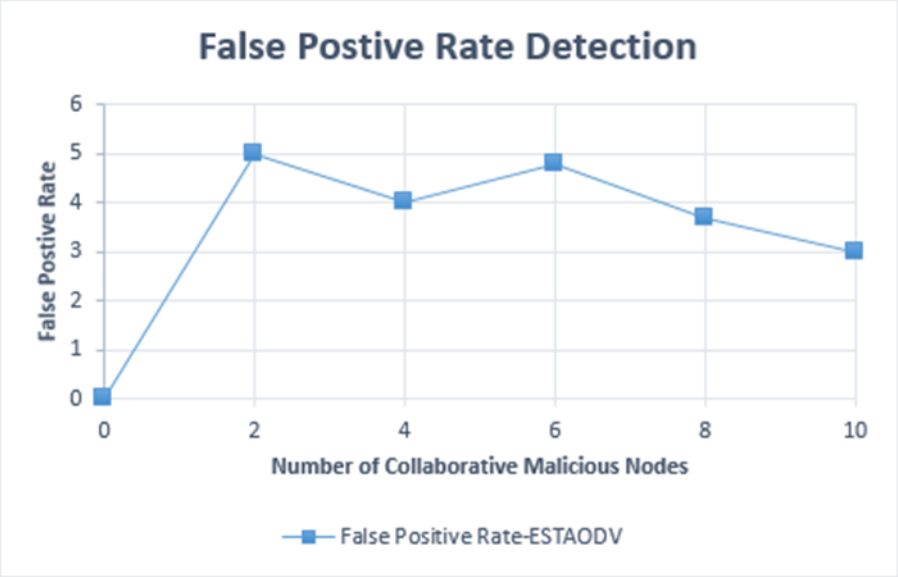

Figure 5.1: False Positive Rate for different Collaborative Malicious nodes

From the above figures, it is represented that the framework is having an identifiable difference in detecting collaborative malicious nodes. This can be seen in above figure, when collaborative node size is two there is a drop in the True Positive Rate[41]. This may be due to the dynamic change of the TrVs or the dynamic behaviour of the collaborative malicious nodes. Time to time the behaviour of the collaborative nodes can be changed. For some of the nodes it is going to act as trustworthy nodes and for some of the nodes, it reacts as a malicious node. In the spiral model

there is a way to track their dynamic behaviour and through that, it can suspect it is a collaborative node[42].

According to the mechanism in the spiral model if one node going to evaluate another node it is going to consider direct trust and the recommendations getting from the neighbours[43]. In that case, if those two values are more different from each other we can suspect some neighbours giving fake recommendations because of the malicious collaboration among those nodes with that particular node]. The aim of this thesis is to secure 5g network using by using low power wireless area network that secure 5g network and consume less resources[44]. As the 5G network security is a large subject, the focus will be on the new technologies coming with 5G. Among the new technologies are terms such as SDN, NFV and mobile cloud. Privacy aspect of 5G is also discussed, as it is an interesting subject for the customers. Same time this can be due to their interactions count or the knowledge with the node which is going to evaluate. By considering all these factors collaborative malicious node detection is challengeable, and it can be changed time to time as we can see it in above figure.

5.1 PERFORMANCE ANALYSIS

5G networks are poised to support a transmission rate of upto 10 Gb/sec. At such high data rates, the bulk of the authenticated handover time will be taken by cryptographic operations rather than the transmission time[45]. For performance analysis, we have looked into the time taken by cryptographic operations. The time used by handover execution has been measured using OpenSSL Libray.To evaluate the performance of the reinforcement learning routing algorithm, we established a series of simulations with different learning variables to assess the performance of the reinforcement learning routing algorithm against the two benchmark routing algorithms

6. CONCLUSION & FUTURE WORK

This chapter explains the conclusion of the research work and show some future directions for the research.

6.1 CONCLUSION

This thesis, we suggested a reinforcement learning routing algorithm that improve energy aware for wireless sensor networks using low power wireless personal area network that can decrease the failure rate and increase efficiency for Remote areas. This sort of network addresses the need for a network that can provide connection in effective way in remote areas Without the need to build a prior infrastructure. by introducing reinforcement learning, the algorithm has the ability to learn from the feedback data from each transmission and compare and store the data of the environment and the usage form of the power for better future routing decisions. we conducted comprehensive research and analysis of the environmental requirement for the remote monitoring networks and the available wireless sensor technologies. We understand that lowpan with wireless sensor network were the choice for such tasks. We then inserted artificial intelligence into the routing by using machine learning in the algorithm in order to enable the energy aware. Such energy awareness can be affected on the routing decision made by the algorithm as the algorithm learning about the network. Furthermore, we modelled the wireless sensor networks with of the key components including the channel, the nodes, the links, the transmissions, and the feedback that used for the machine learning. We likewise talked about and actualized the implemented the reinforcement learning method used in the algorithm. We likewise characterized a few key boundaries to be concentrated in the further examination. At long last, we directed a series of simulations to look at the impacts of the critical boundaries on the adequacy of the calculation.

We also compared the performance of the reinforcement learning routing algorithm with an upper bound and a lower bound benchmark. We proved the effectiveness of the algorithm by setting the performance target for algorithms to meet. We found that the RL routing has successfully met the target, whereas the benchmark algorithm has failed to meet the target. We gathered a set of parameters with the best performance for the RL algorithm under the simulated environment. We found that the RL routing algorithm with these selected parameters to have a substantial improvement over the benchmark in all three criteria we studied. In summary, we concluded that

the result has indicated that the proposed RL routing algorithm has addressed the need for the network. a comprehensive literature review was conducted for related fields including wireless networks and machine learning We identified the need for new directive algorithms specifically designed for remote sensing networks

Furthermore, we modelled the remote monitoring networks with attributes of the key components including the channel, the nodes, the links, the transmissions, and the feedback that used for the machine learning. We also discussed and implemented the reinforcement learning method used in the algorithm. We also defined some key parameters to be studied in the future works. This thesis gives data about the new technologies, and their security challenges and potential solutions. This research should also give some level of understanding of who is in charge of the implementation and what sort of hierarchy exists in terms of standardizing network security. Different advanced toolboxes in Matlab i.e. Antenna Toolbox, Machine Learning Toolbox, Wireless Toolbox used in this thesis.

6.2 FUTURE WORK

In light of the research directed in this thesis, there are a few suppositions that can be concentrated further later on. The suppositions incorporate the interference, the channel parameters, charging cycles and transmission patterns. With the contemplations on these suppositions, a more extensive model of the organization can be fabricated. Consequently, more indicated steering techniques can be created and actualized for additional investigates. Right off the bat, future works can think about the incorporation of both inside and outer obstructions. The obstruction has been viewed as zero in the reproductions of this proposition, yet in the genuine organization circumstances, it exists. Inside Co-channel Interference can be concentrated to take reproduction transmissions in adjoining hubs into thought. The calculation can redirect the course choice to improve utilize the space in the organization and even the energy utilization between all the hubs. Furthermore, outside Adjacent-Channel Interference ought to likewise be thought of. In spite of the fact that the steering calculation ought to be viewed as physical-layer innovation free, the presence of clog of the range the basic physical-layer innovation will affect the energy utilization and execution of transmissions in the organization. The learning cycle can consider that for more precise channel forecast for the determination of course.

REFERENCES

[1] MAlsharif, H.; Nordin, R.; Abdullah, N.F.; Kelechi, A.H. How to make key 5G wireless technologies environmental friendly: A review. Trans. Emerg. Telecommun. Technol. 2018, 29, e3254.

[2] Ericsson Mobility Report 2018. November 2018. Available online: https://www.ericsson.com/assets/local/

mobility-report/documents/2018/ericsson-mobility-report-november-2018.pdf

[3] Yaqoob, I.; Hashem, I.A.T.; Ahmed, A.; Kazmi, S.A.; Hong, C.S. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. Future Gener. Comput. Syst. 2019, 92, 265–275.

[4] Sah, D.K.; Kumar, D.P.; Shivalingagowda, C.; Jayasree, P. 5G Applications and Architectures. In 5G Enabled Secure Wireless Networks; Springer: New York, NY, USA, 2019; pp. 45–68.

[5] Alsharif, M.H.; Nordin, R. Evolution towards fifth generation (5G) wireless networks: Current trends and challenges in the deployment of millimetre wave, massive MIMO, and small cells. Telecommun. Syst. 2017, 64, 617–637. [CrossRef]

[6] Abrol, A.; Jha, R.K.; Jain, S.; Kumar, P. Joint power allocation and relay selection strategy for 5G network: A step towards green communication. Telecommun. Syst. 2018, 68, 201–215.

[7] Lloret, J.; Sendra, S.; Macias-Lopez, E. Advances in Green Communications and Networking. Mob. Netw. Appl. 2019, 1–4.

[8] Mowla, M.M.; Ahmad, I.; Habibi, D.; Phung, Q.V. A green communication model for 5G systems. IEEE Trans. Green Commun. Netwo. 2017, 1, 264–280.

[9] Hasan, Z.; Boostanimehr, H.; Bhargava, V.K. Green cellular networks: A survey, some research issues and challenges. IEEE Commun. Surv. Tutor. 2011, 13, 524–540.

[10] Ismail, M.; Zhuang, W.; Serpedin, E.; Qaraqe, K. A survey on green mobile networking: From the perspectives of network operators and mobile users. IEEE Commun. Surv. Tutor. 2015, 17, 1535–1556.

[11] Abdoos, Monireh & Esmaeili, Ahmad & Mozayani, Nasser. (2012). Holonification of a Network of Agents Based on Graph Theory. 7327. 379-388. 10.1007/978-3-642-30947-2_42.

[12] Behera, T. & Mohapatra, S K & Samal, U.C. & Khan, Mohammad Shoeb. (2019). Hybrid Heterogeneous Routing Scheme for Improved Network Performance in WSNs for Animal Tracking. Internet of Things. 6. 10.1016/j.IOT.2019.03.001.

[13] E. Catania, A. Di Stefano, E. Guardo, A. La Corte, S. Pagano, M. Scatà. Energy Awareness and the Role of "Critical Mass" in Smart Cities, International Refereed Journal of Engineering and Science (IRJES), Volume 4, Issue 7, July 2015, pp. 38-43. ISSN: 2319-183X (online); 22319-1821 (print).

[14] Gupta, Akhil. (2015). A Survey of 5G Network: Architecture and Emerging Technologies.Access, IEEE. 3. 1206-1232. 10.1109/ACCESS.2015.2461602.

[15] https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

[16] P. Motta, E. Catania, E. Guardo, A. La Corte, S. Pagano. Benefits of nanosatel-lite network for smart metering technological infrastructure in wide areas, Tartu Conference on Space Science and Technology Tartu, Estonia, 22-24 September 2014, poster & invited talk

[17] Khan, Rabia & Kumar, Pardeep & Jayakody, Dushantha Nalin & Liyanage, Madhusanka. (2019). A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions. IEEE Communications Surveys & Tutorials. 10.1109/COMST.2019.2933899.

[18] Akpakwu, G.A.; Silva, B.J.; Hancke, G.P.; Abu-Mahfouz, A.M. A survey on 5G networks for the Internet of Things: Communication technologies and challenges. IEEE Access 2017, 6, 3619–3647. [CrossRef]

[19] Riazul Islam, S.M.; Zeng, M.; Dobre, O.A.; Kwak, K.S. Non-Orthogonal Multiple Access (NOMA): How It Meets 5G and Beyond. arXiv 2019, arXiv:1907.1000.

[20] Thubert, P.; Pelov, A.; Krishnan, S. Low-power wide-area networks at the IETF. IEEE Commun. Stand. Mag. 2017, 1, 76–79. [CrossRef]

[21] Chacko, S.; Job, M.D. Security mechanisms and Vulnerabilities in LPWAN. IOP Conf. Ser. Mater. Sci. Eng. 2018, 396, 012027. [CrossRef]

[22] Thoen, B.; Callebaut, G.; Leenders, G.; Wielandt, S. A Deployable LPWAN Platform for Low-Cost and Energy-Constrained IOT Applications. Sensors 2019, 19, 585. [CrossRef]

[23] Key technology choices for optimal massive IOT devices, Ericsson Technology Review. Available online: https://www.ericsson.com/en/ericsson-technology-review/archive/2019/key-technology-choices-foroptimal-massive-IOT-devices.

[24] Rubio-Aparicio, J.; Cerdan-Cartagena, F.; Suardiaz-Muro, J.; Ybarra-Moreno, J. Design and Implementation of a Mixed IOT LPWAN Network Architecture. Sensors 2019, 19, 675. [CrossRef]

[25] Chen, M.; Miao, Y.; Jian, X.; Wang, X.; Humar, I. Cognitive-LPWAN: Towards intelligent wireless services in hybrid low power wide area networks. IEEE Trans. Green Commun. Netw. 2018, 3, 409–417. [CrossRef]

[26] SIGFOX. Available online: www.sigfox.com.

[27] Awadallah, S.; Moure, D. Torres-González, an Internet of Things (IOT) Application on Volcano Monitoring. Sensors 2019, 19, 4651.

[28] Centenaro, M.; Vangelista, L.; Zanella, A.; Zorzi, M. Long-range communications in unlicensed bands: The rising stars in the IOT and smart city scenarios. IEEE Wirel. Commun. 2016, 23, 60–67.

[29] Ingenu RPMA. Available online: http://www.ingenu.com/technology/rpma/

[30] Peña, Q.A.; Gia, J.T.N.; Zou, Z.; Tenhunen, H.; Westerlund, H. Comparative study of LPWAN technologies on unlicensed bands for M2M communication in the IOT: Beyond LoRa and LoRaWAN. Procedia Comput. Sci. 2019, 155, 43–350.

[31] Finnegan, J.; Stephen, B. A comparative survey of LPWA networking. arXiv 2018, arXiv:1802.04222.

[32] QOWISIO. Available online: www.qowisio.com.

[33] Hamza, Z.; Baddi, Y.; Hasbi, A. Ehealth smart application of WSN on WWAN. Proc. 2nd Int. Conf. Netw. Inf. Syst. Secur. 2019, 1–8.

[34] NWAVE. Available online: www.nwave.io.

[35] Pham, T.L.; Nguyen, H.; Bui, V.; Jang, Y.M. Low Power Wide Area Network Technologies for Smart Cities Applications. IEEE Int. Conf. Inf. Commun. Technol. Converg. (ICTC) 2019, 501–505.

[36] Semtech. LoRa Modulation Basics. AN1200.22. Available online: http://wiki.lahoud.fr/lib/exe/fetch.php? media=an1200.22.pdf.W

[37] Croce, D.; Gucciardo, M.; Mangione, S.; Santaromita, G.; Tinnirello, I. Impact of LoRa imperfect orthogonality: Analysis of link-level performance. IEEE Commun. Lett. 2018, 22, 796–799.

[38] LoRa Alliance. Available online: https://www.lora-alliance.org.

[39] Abdoos, Monireh & Esmaeili, Ahmad & Mozayani, Nasser. (2012). Holonification of a Network of Agents Based on Graph Theory. 7327. 379-388. 10.1007/978-3-642-30947-2_42.

[40] Behera, T. & Mohapatra, S K & Samal, U.C. & Khan, Mohammad Shoeb. (2019). Hybrid Heterogeneous Routing Scheme for Improved Network Performance in WSNs for Animal Tracking. Internet of Things. 6. 10.1016/j.iot.2019.03.001.

[41] Sharma, S.S.; Wang, X. Towards massive machine type communications in ultra-dense cellular IOT Netw. IEEE Commun. Surv. Tutor. 2019. [CrossRef]

[42] Weyn, M.; Ergeerts, G.; Wante, L.; Vercauteren, C. Hellinckx, Survey of the DASH7 alliance protocol for 433 MHz wireless sensor communication. Int. J. Distrib. Sens. Netw. 2013, 870430. [CrossRef]

[43] Polonelli, T.; Brunelli, D.; Marzocchi, A.; Benini, L. Slotted ALOHA on LoRaWAN-Design, Analysis, and Deployment. Sensors 2019, 19, 838. [CrossRef]

[44] Bembe, M.; Abu-Mahfouz, A.; Masonta, M.; Ngqondi, T. A survey on low-power wide area networks for IOT applications. Telecommun. Syst. 2019, 71, 249. [CrossRef]

[45] Lippuner, S.; Weber, B.; Salomon, M.; Korb, M.; Huang, Q. EC-GSM-IOT network synchronization with support for large frequency offsets. IEEE Wirel. Commun. Netw. Conf. 2018, 1–6.