On Reliable and Secure RPL (Routing protocol Low-power and Lossy Networks) based Monitoring and Surveillance in Oil and Gas Fields

Isam Wadhaj

A Thesis submitted in partial fulfilment of the requirements of Edinburgh Napier University, for the award of Doctor of Philosophy

August 2022

ABSTRACT

Different efforts have been made to specify protocols and algorithms for the successful operation of the Internet of things Networks including, for instance, the Low Power and Lossy Networks (LLNs) and Linear Sensor Networks (LSNs). Into such efforts, IETF, the Internet Engineering Task Force, created a working group named, ROLL, to investigate the requirement of such networks and devising more efficient solutions. The effort of this group has resulted in the specification of the IPv6 Routing Protocol for LLNs (RPL), which was standardized in 2012. However, since the introduction of RPL, several studies have reported that it suffers from various limitations and weaknesses including scalability, slow convergence, unfairness of load distribution, inefficiency of bidirectional communication and security, among many others. For instance, a serious problem is RPL's under-specification of DAO messages which may result in conflict and inefficient implementations leading to a poor performance and scalability issues. Furthermore, RPL has been found to suffer from several security issues including, for instance, the DAO flooding attack, in which the attacker floods the network with control messages aiming to exhaust network resources. Another fundamental issue is related to the scarcity of the studies that investigate RPL suitability for Linear Sensor Networks (LSN) and devising solution in the lieu of that.

Motivated by these observations, the publications within this thesis aim to tackle some of the key gaps of the RPL by introducing more efficient and secure routing solutions in consideration of the specific requirements of LLNs in general and LSNs as a special case. To this end, the first publication proposes an enhanced version of RPL called Enhanced-RPL aimed at mitigating the memory overflow and the under-specification of the of DAOs messages. Enhanced-RPL has shown significant reduction in control messages overhead by up to 64% while maintaining comparable reliability to RPL. The second publication introduces a new technique to address the DAO attack of RPL which has been shown to be effective in mitigating the attack reducing the DAO overhead and latency by up to 205% and 181% respectively as well as increasing the PDR by up to 6% latency. The third and fourth publications focus on analysing the optimal placement of nodes and sink movement pattern (fixed or mobile) that RPL should adopt in LSNs. It was concluded based on the results obtained that RPL should opt for fixed sinks with 10 m distance between deployed nodes.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
AODV	Ad hoc On-Demand Distance Vector (AODV)
BLE	Bluetooth Low Energy
CSMA	Carrier-Sense Multiple Access
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance
CTP	Collection Tree Protocol
DAG	Directed Acyclic Graph
DAO	Destination Advertisement Object
DAO-ACK	Destination Advertisement Object Acknowledgment
DIO	DODAG Information Object
DIS	DODAG Information Solicitation
DODAG	Destination Oriented Directed Acyclic Graph
DSR	Dynamic Source Routing
ELT	Expected Lifetime
ETX	Expected Transmission Count
HC	Hop Count
ICMPv6	Internet Control Message Protocol version 6
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IPv6	Internet Protocol version 6
LBR	LLNs Border Router
LLNs	Low-power and Lossy Networks
LoWPAN	Low Power Wireless Personal Area Network
MAC	Media Access Control
MP2P	MultiPoint-to-Point
MRHOF	Minimum Rank with Hysteresis Objective Function
OF	Objective Function
OF0	Objective Function Zero
PP	Preferred Parent
P2P	Point-to-Point
P2MP	Point-to-MultiPoint

PDR	Packet Delivery Ratio
QoS	Quality of Service
ROLL	Routing Over Low-power and Lossy networks
RPL	IPv6 Routing Protocol for Low-power and Lossy networks
APC	Average Power Consumption
TDMA	Time Division Multiple Access
UDGM	Unit Disk Graph Medium

ACKNOWLEDGMENT

First and foremost, I would like to thank and dedicate this thesis to my beloved Wife, Watfa, who has always believed in my capacity to achieve such a great project in the academic arena. Thank you for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without her support.

Furthermore, I would like to thank and acknowledge my director of studies Dr Baraq Ghaleb, who was always available whenever I ran into a trouble spot or had a question about my research or writing. He has allowed this thesis to be my own work, nevertheless steered me into the right direction whenever he thought I needed it. I thank you for your understanding, wisdom, patience, enthusiasm, and encouragement and for pushing me further than I thought I could go.

I am also thankful to my supervisor Prof Ahmed Al-Dubai for his very valuable comments and consistent guidance throughout the journey of this work.

Finally, I wish to express my heartfelt thanks and love to my children, Aqeel and Majeed for coping with the undue paternal deprivation during the course of my study.

DECLARATION

I, Isam Wadhaj, confirm that this thesis submitted for assessment is my own work and is expressed in my own words. Any uses made within it of the words of other authors in any form e.g., ideas, equations, figures, text, tables, programs, etc. are properly acknowledged. A list of references employed is included.

Name: Isam Wadhaj

Matriculation Number: 40454179

Signature: Date: 17/August/2022

LIST OF PUBLICATIONS

Peer-reviewed Conference, and Workshop Publications:

1. Ghaleb, B., Al-Dubai, A., Ekonomou, E., & **Wadhaj, I**. (2017). A new enhanced RPL based routing for Internet of Things. In 2017 IEEE International Conference on Communications, (1-6). https://doi.org/10.1109/ICCW.2017.7962723
2. **Wadhaj, I.,** Ghaleb, B., Thomson, C., Al-Dubai, A., & Buchanen, B. (2020). Mitigation Mechanisms Against the DAO Attack on the Routing Protocol for Low Power and Lossy Networks (RPL). IEEE Access, 8, 43665-43675. https://doi.org/10.1109/ACCESS.2020.2977476
3. **Wadhaj, I**., Ghaleb, B., Thomson, C. (2021). An RPL based Optimal Sensors placement in Pipeline Monitoring WSNs. International Conference on Emerging Technologies and Intelligent Systems (ICETIS 2021).
4. **Wadhaj, I**., Kristof, I., Romdhani, I., & Al-Dubai, A. (2015). Performance Evaluation of the RPL Protocol in Fixed and Mobile Sink Low-Power and Lossy-Networks. In Proceedings of the 14th IEEE International Conference on Ubiquitous Computing and Communications (IUCC 2015). , (1600-1605). https://doi.org/10.1109/cit/iucc/dasc/picom.2015.241
5. **Wadhaj, I**., Ghaleb, B., Thomson, C. (2021). Wireless Sensor Networks (WSN) in Oil and Gas Industry: Applications, Requirements and Existing Solutions. International Conference on Emerging Technologies and Intelligent Systems (ICETIS 2021).
6. **Wadhaj, I**., Gharebi, W., Al-Dubai, A., & Thomson, C. (2018). Performance Investigation of RPL Routing in Pipeline Monitoring WSNs. In 20th IEEE International Conference on High Performance Computing and Communications; 16th IEEE International Conference on Smart City; 4th IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2018. https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00178.
7. Thomson, C., **Wadhaj, I**., Romdhani, I., & Al-Dubai, A. (2017). Performance evaluation of RPL metrics in environments with strained transmission ranges. In 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA). https://doi.org/10.1109/aiccsa.2016.7945687.
8. Thomson, C., **Wadhaj, I**., Tan, Z., & Al-Dubai, A. (in press). A Mobility Aware Duty Cycling and Preambling Solution for Wireless Sensor Network with Mobile Sink Node. Wireless Networks.
9. Thomson, C., **Wadhaj, I**., Tan, Z., & Al-Dubai, A. (in press). Towards an Energy Balancing Solution for Wireless Sensor Network with Mobile Sink Node. Computer Communications, https://doi.org/10.1016/j.comcom.2021.01.011.
10. Thomson, C., **Wadhaj, I**., Tan, Z., & Al-Dubai, A. (2019). Mobility Aware Duty Cycling Algorithm (MADCAL) A Dynamic Communication Threshold for Mobile Sink in Wireless Sensor Network. Sensors, 19(22), https://doi.org/10.3390/s19224930.
11. Thomson, C., **Wadhaj, I**., Tan, Z., & Al-Dubai, A. (2019). Mobility Aware Duty Cycling Algorithm (MADCAL) in Wireless Sensor Network with Mobile Sink Node. In 2019 IEEE International Conference on Smart Internet of Things (SmartIoT). https://doi.org/10.1109/SmartIoT.2019.00037.
12. Thomson, C., **Wadhaj, I**., Al-Dubai, A., & Tan, Z. (in press). A New Mobility Aware Duty Cycling and Dynamic Preambling Algorithm for Wireless Sensor Network.

CHAPTER ONE: INTRODUCTION

Wireless sensor networks (WSNs) and Internet of Things (IoT) are among the top potential new technologies that dramatically alter the world and the way we live and work. Indeed, modern industry is becoming increasingly dependent on the need for real-time seamless transfer and manipulation of data for quick decision-making process. In line with those trends, the Oil and Gas industry is apparently looking towards WSNs and IoT to remotely monitor pipelines, natural gas leaks, corrosion, Hydrogen sulfide (H2S), equipment condition, and real-time reservoir status [3].

Indeed, most of the oil infrastructure, such as pipelines and refineries, require continuous monitoring of various parameters (pressure, temperature, vibration, etc.) in order to prevent accidents and malfunction, and to monitor the overall production system. Thus, the integration of IoT technologies with tiny wireless sensors represents one of the most promising routes toward realizing secure and reliable Oil and Gas monitoring systems. A multitude of wireless and IoT-based technologies can be deployed to facilitate the monitoring of Oil and Gas systems. One of these technologies is the 6LowPAN standard developed by the IETF standardization group that comprises several protocols including the IPv6 Routing Protocol (RPL) [1]. However, sensors in Gas and Oil networks are constrained in energy resources and are usually deployed in harsh environments where the replacement of depleted nodes will be a challenging task. Hence, RPL still has several restrictions that limits its applicability under Gas and Oil networks. These issues include the unbalanced topology that RPL builds, its scalability problem due to the sensor nodes memory limitations, the under-specification of how downward routes are built which may result in conflict, inefficient implementations leading to a poor performance and the ambiguity of how nodes placement strategies can affect the efficiency of the protocol [2] [3] [4] [5] [6] [7] [8] [9]. In addition, RPL still suffers from several security

issues which may limit its adoption in LLNs including Gas and Oil networks [10] – [20]. A vital security concern is the Destination Advertisement Object (DAO) attack in which an attacker may flood the network with DAO messages leading to network resource exhaustion [21] [22] [23].

1.1 MOTIVATION

Different efforts have been made to specify protocols for Low Power and Lossy Networks (LLNs) that include gas and oil networks. This need has been anticipated by the IETF and the ROLL working group has been created for this matter. The effort of this group resulted in the IPv6 Routing Protocol for Low-power and Lossy Networks (RPL) [1], which was standardized in 2012. However, since the introduction of RPL, several studies have reported that it suffers from various limitations and weaknesses including slow convergence, unfairness of load distribution, inefficiency of bidirectional communication and security among many others [24] [25] [26] [27] [28]. Thus, the aim of this dissertation is to address some of the key gaps of the RPL standard considering the specific requirements of LLNs and specifically Linear Sensor Networks (LSNs) and ultimately enabling widespread deployments of RPL on LLN applications and services in many different fields.

1.2 PROBLEM STATEMENT AND RESEARCH QUESTIONS

Efficient routing strategies are essential for efficient LLNs operations, and the poor performance of such networks severely affects the services that can be offered and supported hindering LLNs deployment in the future in multiple applications including the OIL and GAS monitoring applications. Despite the advantages brought out by the standardized routing protocol RPL, its efficiency in the context of LLNs as well as Oil and Gas networks has not been fully investigated, an objective that we aim to achieve in this dissertation. In addition,

many research studies have reported that the standard still suffers from several gaps that may harm its efficiency [29] - [40]. These gaps can be identified as follows:

First, RPL has been found to suffer from a scalability problem in its mechanism when constructing the reverse routes from the network's sink to the joined nodes (Downward routes). In addition, the scalability problem is magnified by the fact that the RPL specification does not allow for a node to look for another DAO parent when its current preferred parent runs out of memory. Even worse, RPL does not specify a mechanism to detect such a case. Another serious problem is RPL's under-specification of DAO timing, which may result in conflict and inefficient implementations leading to poor performance [8].

Second, a fundamental issue is that RPL is also restricted by the fact that Gas and Oil networks are envisaged to operate in a linearly distributed fashion along the pipeline and limited to a single path to transmit the data. Hence, the optimal placement of nodes under such scenarios has not been fully investigated raising the question about how efficient linear senor networks would be under different node placement strategies, when utilizing the RPL standard as the routing standard.

Third, a vital security concern is the Destination Advertisement Object (DAO) attack. This attack functions with the adversary node regularly advertising false DAO messages to its parent nodes, leading to network resource exhaustion as the parent will attempt to update the routing table by flooding the network with the received DAO messages. Thus, the attack will lead to an increase on processing power required to complete the routing table update and the DAOs transmission to parent nodes. Another factor that increases the effectiveness of the attack is that in RPL under storing mode, the transmission of DAO messages follows the upward direction towards the sink, and thus the scope of damage increases beyond area of the attacker node [21], [22]. These consequences downgrade the network performance with respect to

routing overhead, power consumption, latency and PDR, which significantly shorten the network lifetime [23].

Based on the mentioned observations, the following research questions are to be addressed:

- How may node placement strategies affect the efficiency of RPL under Linear Sensor Network (LSNs) in the context of oil and gas applications?
- In relation to metrics that govern the routing process in RPL, what would be the most efficient metric to be used in selecting optimal paths under multi-segment pipeline networks in the context of oil and gas applications?
- How will introducing mobility into network operations, in relation to the sink node, affect the perceived efficiency of RPL in terms Latency, Packet Delivery Ratio (PDR) and Energy Consumption in LLNs in general.
- Is the protocol able to maintain node connectivity within a Destination Oriented Directed Acyclic Graph (DODAG) under 'strained' transmission ranges?
- How to mitigate memory overflow and the under-specification of the downward route construction in a RPL network under the storing mode.
- How to better approach and develop efficient countermeasures for the DAO flooding attacks in RPL networks?

1.3 AIMS AND OBJECTIVES

The main aim of this thesis is to overcome the bottlenecks and gaps of the standardised routing protocol for LLNs, namely, RPL. Hence, several challenges related to the protocol operation have to be addressed including scalability, reliability, convergence efficiency, and security. The intended research work contains a group of objectives that will pave the way towards achieving the overall aim listed as follows:

- **Objective 1:** The first objective is to gain in-depth knowledge and master the state-of-the-art of specifications, requirements, applications and challenges of Low-power and Lossy Networks, of which WSNs are a particular type, especially in the context of the oil and gas industry.
- **Objective 2:** The second objective is to evaluate the performance of the RPL protocol under various scenarios including sink mobility, node placement strategies and routing metrics, so to gain insight into the suitability and the efficiency of the protocol in IoT networks including gas and oil applications.
- **Objective 3:** The third objective is to propose and implement new routing primitives that overcome the limitations of existing solutions with focus on enhancing IoT network scalability, energy efficiency, convergence time, load distribution and reliability.
- **Objective 4:** The fourth objective is to review existing security issues of RPL and introduce new mitigation techniques against the DAO flooding attacks.

1.4 CONTRIBUTIONS

In this thesis, I strive to push the boundaries of routing and secure routing in IoT networks beyond the state-of-the-art standardized solutions with the main aim to further enable widespread deployments of scalable, reliable, energy-efficient and secure networks in the context of IoT. To this end, and in addition to the literature review, the key contributions of this dissertation can be summarized as follows:

- **Wireless Sensor Networks (WSN) in Oil and Gas Industry: Applications, Requirements and Existing Solutions.**

The first contribution of this thesis focuses on surveying the provision of WSNs in the oil and gas industry, taking into account the specific requirements of the applications and challenges. Furthermore, a particular attention is given to the existing architectures of efficient

mechanisms that fulfil the requirements and overcome the challenges that arise when deploying a WSN in the Oil and Gas industry. The comparison of existing solutions is comprehensive and informative for the design and deployment of WSN-based sensor systems and particularly valuable for QoS perspectives such resilience, latency and energy-efficiency.

- **An evaluation of the RPL Protocol in Fixed and Mobile Sink Low-Power and Lossy-Networks.**

The second contribution of this thesis examines the challenges inherent when utilising a mobile sink node in IoT networks. Specifically, RPL was evaluated under fixed and mobile sink environments using several metrics including Latency, Packet Delivery Ratio (PDR) and Energy Consumption. Experimental results show that a Fixed-sink environment performs better in terms of average power consumption Latency and PDR. The contribution exposes some serious issues with sink mobility, where certain nodes have an excessively high-power consumption while several nodes were isolated.

- **An investigation of RPL metrics in environments with strained transmission ranges.**

The third major contribution of this thesis is the investigation of the applicability of RPL in the field of Oil and Gas monitoring systems in order to unleash the challenges and limitations that may appear as a result of such adoption. In particular, the performance of RPL routing mechanisms is evaluated in terms of Packet Delivery Ratio (PDR), latency and power consumption under constrained conditions, by using different topology types, different number of nodes and different transmission ranges. The performance evaluations of RPL have concluded that the RPL mechanisms used to build a topology may suffer from an excessive unbalanced traffic load. As a result, a part of the network may be disconnected, as the energy of the overburdened nodes will be drained much faster than other nodes.

- **A new enhanced RPL based routing for Internet of Things.**

The fourth contribution of this thesis is the development and implementation of a new algorithm that optimizes the Downward Routing Mechanism in RPL Storing Mode. The proposed algorithm is developed with the aim of tackling the issue associated with the scalability of downward routing presented in RPL. The result is an enhanced version of RPL, which successfully improves the original RPL in two aspects: mitigating the problem of storage limitation of the node's preferred parent and mitigating the issue of DAOs under-specification mechanisms.

- **An investigation of RPL Routing in Pipeline Monitoring WSNs.**

The fifth contribution of this thesis is the evaluation of the RPL standard under various routing metrics used for calculating the optimal routes in Multi Segment Linear Pipeline Monitoring IoT networks including ETX, Hop count and RSSI. This contribution has revealed that the ETX metric is the best metric to be used under applications that need high rates of success in delivering data packets, high reliability and low power consumption in the context of multi segment pipeline networks.

- **Mitigation Mechanisms Against the DAO Attack on the Routing Protocol for Low Power and Lossy Networks (RPL).**

The sixth contribution of this thesis regards enhancing the RPL protocol in the cybersecurity aspect. The work contributes to problem identification, development of the novel solution and evaluation of the new solution. It evaluates the effect of a DAO attack in the context of an RPL network. In particular, it identified the particular performance metrics and network resources that are most affected. Two effective mitigating mechanisms are developed to address the DAO insider attack in RPL: SecRPL1, which restricts the number of forwarded

DAOs per child; and SecRPL2, which restricts the entire number of forwarded DAOs by a specific node.

The simulation results have shown how the attack can damage the network performance by significantly increasing the overhead and power consumption. It also demonstrated that the DAO attack affects the reliability of the downward traffic under specific conditions.

- **An RPL based Optimal Sensors placement in Pipeline Monitoring WSNs.**

The seventh contribution of this thesis is related to investigating the linear placement of sensor nodes in LSNs, varying the distance and its impact on energy consumption, packet delivery ratio, end to end delay, throughput and the Destination Oriented Directed Acyclic Graph (DODAG) construction time.

The findings have shown that the increasing of the distance between nodes has important performance implication in terms of the studied quality of service metrics. The shorter the distance between nodes the better the performance is. It can be suggested with great confidence that a distance of 10m has achieved a significant level of performance and can be considered as the optimum solution for node placement in an LSN.

1.5 THESIS STRUCTURE

The remainder of thesis is organized into four chapters as follows:

- **Chapter Two: Wireless Sensor Networks (WSNs) in Oil and Gas Industry: Applications, Requirements and Existing Solutions.**

This chapter presents a thorough background to WSNs in Oil and Gas industry. It specifically provides an overview of the potential applications, existing standards and technical requirements of WSN deployment in the oil industry. It also elaborates on the techniques and solutions proposed in the literature.

- **Chapter Three: The IPv6 routing Protocol for LLNs (RPL): Basic Operations and security Features**

In this chapter, we present a comprehensive overview of the RPL standard including its topology, technical operations, limitations and drawbacks as reported in the literature related to its core operations (i.e. routing selection and optimization, routing maintenance operations and downward routing). This chapter provides the necessary background to the contributions made in this thesis. We have also provided an extensive survey and an in-depth analysis of research efforts aimed at addressing the limitations of RPL.

- **Chapter Four: Publications**

This chapter presents a critical evaluation of the publications considered for the PhD. All publications are co-authored publications with research colleagues. In five publications, I have acted as the principal researcher responsible for the research methodology, conceptualisation, simulation tools, investigation, resources, data curation, original draft preparation and presentation. Where I am the second author, I have contributed with formal analysis, validation and writing original draft preparation. The co-authors are willing to be contacted to address any concerns over co-authorship.

- **Chapter Five: Conclusion and Future Work**

This chapter concludes the dissertation by summarising its findings and outlining future research prospects and directions.

CHAPTER TWO: WIRELESS SENSOR NETWORKS (WSNS) IN OIL AND GAS INDUSTRY: APPLICATIONS, REQUIREMENTS AND EXISTING SOLUTIONS

Effective measurement and monitoring of certain parameters (temperature, pressure, flow etc.) is crucial for the safety and optimization of processes in the Oil and Gas Industry. Wired sensors have been extensively utilized for this purpose but are costly, not best suited for harsh environments and are difficult to deploy and maintain. Wireless Sensor Network Solutions is revolutionizing the Offshore Oil and Gas industry providing an evolving solution that introduces significant benefits in cost, ease of deployment, flexibility and convenience. The adoption of Wireless Sensor Networks is expected to be tremendous in industrial automation owing to a report that projected the deployment of 24 million wireless-enabled sensors and actuators worldwide by 2016.With limited literature on this specific subject matter, this chapter presents a critical survey into oil industry monitoring specifications, requirements and Wireless Sensor Network applications as it directly impacts the Oil and Gas Industry. An overview of Wireless Sensor Networks is presented, applications from literature are highlighted and finally challenges and existing solutions are discussed.

The chapter is organized as follows. In Section 2.1, the potential applications in oil and are identified. Then, in Section 2.2, existing standards for low-power wireless sensor networks are discussed. In section 2.3 the technical requirements of WSN deployments in oil industry are reviewed. In Section 2.4, we review techniques and solutions proposed in the literature. Finally, Section 2.5 concludes the chapter.

2.1 INTRODUCTION

The energy industry increasingly dependent on information technology. Although the oil and gas companies may have not invested the same percentage of money that is invested by other industrial sectors in information technology, such as the financial services sector, but that

there is a growing awareness of the role of this technology in shaping the future of the industry. Since the world economic growth depends largely on the oil and gas industry and the demand for energy resources increases, there is a need to adapt to intelligent technologies for the improvement of all areas of industrial practice in connection with the oil and gas processing stages including refining, exploration, extraction, transport and marketing of petroleum products [41] and thus increases the productivity while reducing costs.

In the light of the above mentioned phases, the harsh and intensive remote environments of oil and gas plants, required an adaptive monitoring system that is ideal for temporary installations, flexible, adaptable and in a position to reduce complexity and cut operational costs. In the last few years, oil and gas industries have used wired communications as a solution for applications monitoring. The installation, operation and maintenance of such a solution are usually costly and not appropriated for short-term installations and might not be easy to adapt in harsh environments [42] [4][3].

The major benefits of the sensor nodes lie not only in their small size and self-organising capabilities but also in their ability to provide reliable, fast, flexible, secure and cheap wireless communication. These features in WSNs have introduced a convenient alternative to the wired nodes [43] [44].

The technical capability of WSNs is still under ongoing exploration in science as its true potential has not been fully exploited. This chapter aims to provide WSN designers, oil and gas companies and researcher a critical review at the provision of WSN in the oil and gas industry taking into account the specific requirements of the applications and challenges. Furthermore, a particular attention is given to the existing architectures of efficient mechanisms that fulfil the requirements and overcome the challenges that arise when deploying WSNs in Oil and Gas industry.

2.2 WSN POTENTIAL APPLICATIONS IN OIL INDUSTRY

For Oil & Gas Industry, WSNs offer a large number of applications that are useful for the production of Performance Optimization [41] (monitor pipelines, gas detection, corrosion, H2S, equipment health [42] status, and real-time reservoir and process control, safety, maintenance.

This section presents a classification of WSN possible applications in oil and gas industry Figure 2-1 illustrates a classification for potential WSN applications in oil and gas industry.

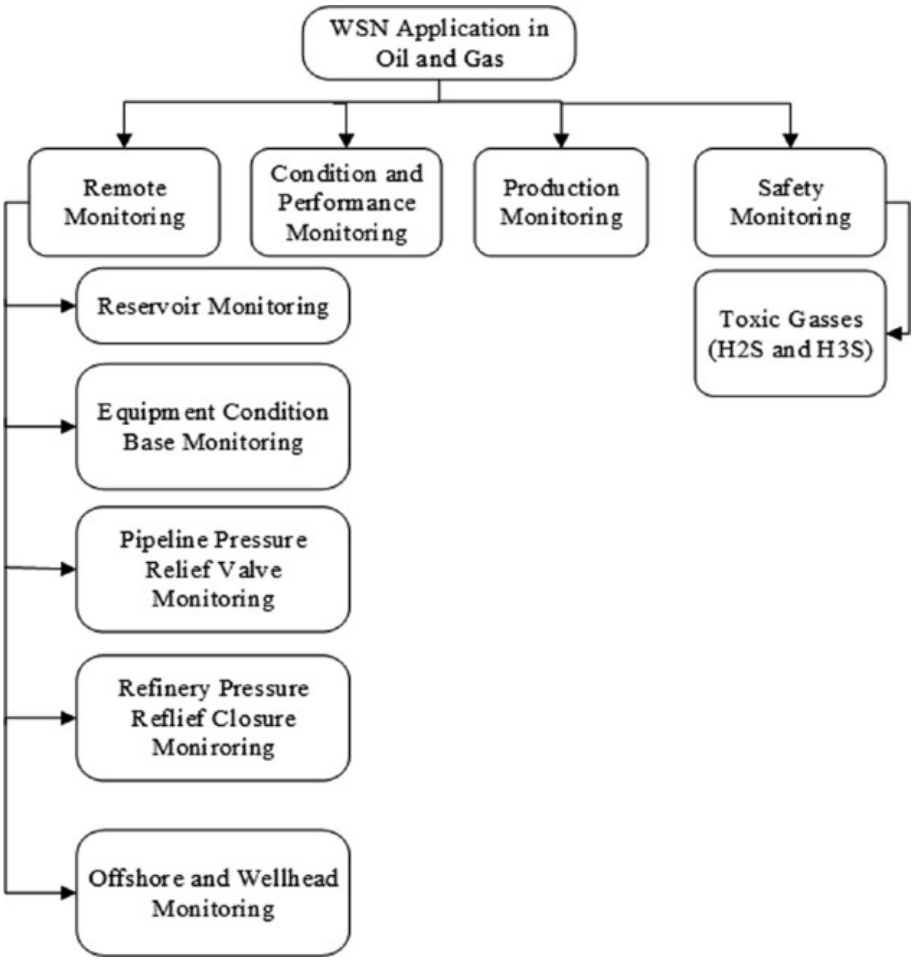


Figure 2-1. Classification of WSN Applications in Oil and Gas Industry [41]

2.2.1 REMOTE MONITORING

One of the main purposes of remote monitoring is to monitor pipelines for gas leakage and damages [45]. Remote monitoring is very beneficial for oil and gas industry in improving safety, enhancing operations, detecting problems, and reducing overall operational costs [41].

Hence sensor nodes are placed in numerous remote locations and hazardous environments such as in oil and gas pipelines can suffer from a variety of catastrophic events such as explosions due to high flammability [46]. This will result in serious environmental hazard and financial damage due loss of production. Therefore, it is crucial for the real time monitoring system to meet certain requirements to be able to predict possible failures before they occur.

In Pipelines monitoring, the unique long distance linear topology characteristics of the network infrastructure in which a large pool of sensor nodes are distributed linearly along the pipeline and limited to a single path to transmit the data, increases the challenges associated with network reliability, connectivity and an efficient energy management for sensors and actuators. Figure 2-2 illustrates the deployments of WSN in distributing and monitoring oil fields. The main requirements identified of WSNs applications for remote monitoring are delay, robustness, data reliability and security [47] [48].

2.2.2 CONDITION AND PERFORMANCE MONITORING

In oil and gas industry, monitoring of equipment and machinery plays an essential part in the overall operation. The aim monitoring is to provide fault diagnostics of different equipment and conduct machine health monitoring and temperature monitoring. Sensors can be used to detect vibration, temperature heat, dissolved gas, electromagnetic properties, power consumption [41], to gather information about the health status of machineries and provide fault diagnostics, that help identify the root cause of a problem, detect and even predict potential upcoming faults, thus the operation downtime, repair costs, damage and potential danger are minimized..

2.2.3 SAFETY MONITORING

The exploration and refinery procedures of oil is usually accompanied by several toxic gases that include ammonia (NH3), hydrogen sulphide (H2S), and sulphur dioxide [41] [47].

The leakage of such materials could have a serious impact on human beings and the environment. Therefore, the monitoring of the H2S considered important [40].

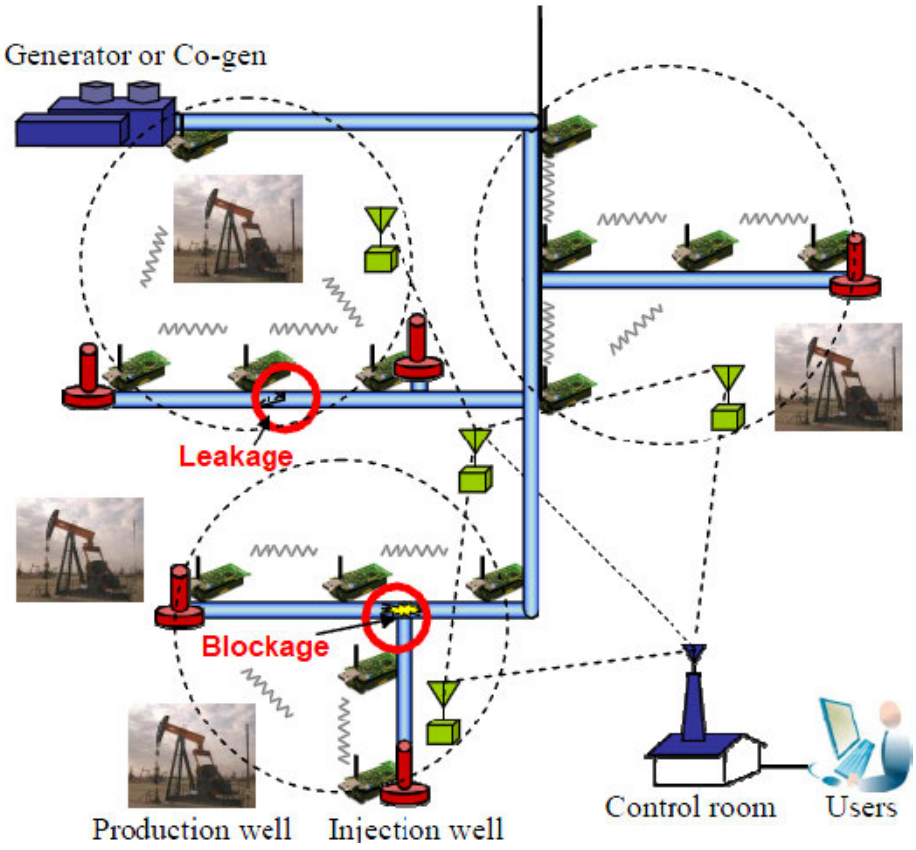


Figure 2-2. Oil Distribution and Monitoring using WSN [49].

2.3 WSN STANDARDS

As WSNs and their applications become more widespread in the oil and gas industry, companies are challenged with the decision of choosing between several emerging technologies and standards, such as IEEE802.15.4, ZigBee, ISA100.11a or WirelessHART. These standards are developed with the goal to provide high-level communication protocols and build the foundation of a complete network infrastructure taking into consideration the limited resources in terms of power, reliability, security, etc.

In this section we provide an overview of the existing standards. A detailed Comparison of WirelessHART, ISA100.11a and ZigBee for industrial applications is introduced in [51]. Figure 2-3 illustrates a classification of existing WSNs standards.

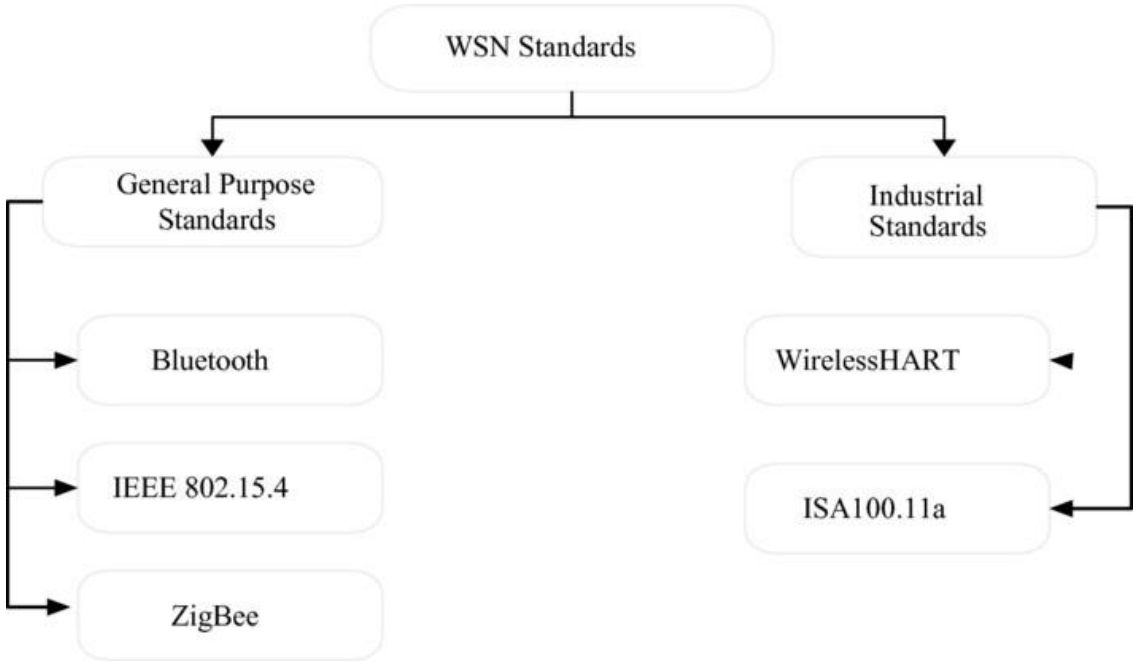


Figure 2-3. Classification WSN Standards [51]

2.3.1 BLUETOOTH

Bluetooth [52] is designed as an open wireless communication protocol to provide cost efficient services for devices that operate within short distance range with no longer than 10 meters with 2400 and 2483.5 MHz frequency range. Bluetooth support the communication between 1 master and more than 7 nodes per piconet [53]. In terms of energy consumption Bluetooth has limited battery lifetime. However, Bluetooth can be very beneficial for a wide range of application that are deployed in a short distance range such as Personal Area Network (PAN).

2.3.2 IEEE 802.15.4

The IEEE 802.15.4 [54] specifies the physical layer and Medium Access Control (MAC) for low data rate Wireless Personal Area Networks (WPANs). This standard uses a duty cycling

mechanism with which all participants nodes go into a sleep state in a regular interval so that energy can be saved. The standards use two modes: (1) non-beacon modes in which a Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) (2) and a beacon mode in which the PAN coordinator sends beacon frames to detect the PAN and starts node synchronisation. It also sends a super-frame structure that contains 16 time slots the so called guaranteed time slots (GTS) that can be assigned to nodes in each PAN, where only a maximum of seven GTS slots can be assigned to nodes contention free period (CFP). Other nodes can either transit into a contention access period (CAP) or inactive period of time during which the end-devices and coordinator transit into sleep state [55]

2.3.3 WIA-PA

The Chinese Industrial Wireless Alliance [56] has designed the Wireless Networks for Industrial Automation - Process automation (WIA-PA) that is based on IEEE 802.15.4 without modifications [57] with aim to provide a reliable, energy efficient, and multi-hop mesh network that adapt to frequent changes in the network. The standard uses a combination of CSMA, TDMA, and FDMA with a maximum of I6 channels under the 2.4 GHz band and frequency hopping [58]. It uses three types of frequency hopping mechanisms namely the Adaptive Frequency Switch, Adaptive Frequency Hopping, and Timeslot hopping. It can co-exist with other standards that are compliant with IEEE 802.15.4.

2.3.4 ZIGBEE

ZigBee [56] [59] is an open standard designed with the aim to provide an intelligent solution that meets wireless devices requirements in terms of cost, energy consumption, reliability, etc. ZigBee utilizes the upper layer of the IEEE 802.15.4 and supports mesh, star and tree topologies and is categorized into three device types, each has a specific role [60] as shown in **Figure 2-4**.

The main function of the Coordinator in all ZigBee networks is to set up the network, therefore it must be aware of all the constituent nodes and should be able to store information and manage communication and security keys of the network. Routers are the intermediaries which facilitate information flow between devices. The endpoint devices are required to perform a limited function of interacting with their parent nodes.

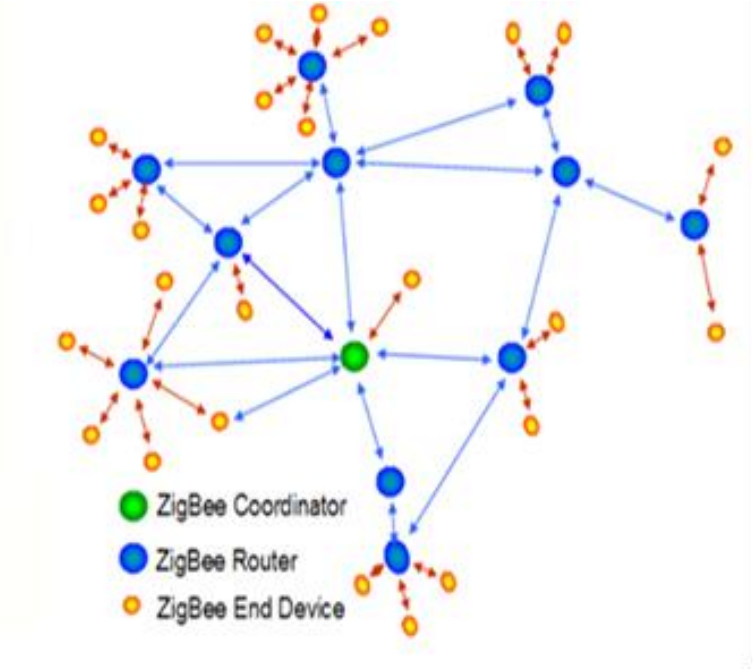


Figure 2-4. ZigBee network [60]

2.3.5 WIRELESSHART

The Highway Addressable Remote Transducer (HART) [56] is an industrial standard developed on the basis of IEEE 802.15.4 specification using up to 15 different channels and a frequency of 2.4 GHz [61]. WirelessHART was developed to support power efficiency, reliability and integrated security. It uses Time Division Multiple Access (TDMA) with Frequency Hopping Spread Spectrum (FHSS) to access different channels at different time slots, while blocking channels which experience interference with the signal by creating a Blacklisting. These mechanisms will result in less interference with the existing wireless systems and reduce noise impact [62] [63].

A typical WirelessHART network that the network manager can support are mesh, star and combination of both topologies and it consists of four components that are essential to provide a fully functional network as illustrated in **Figure 2-5** [60] [64] [63]

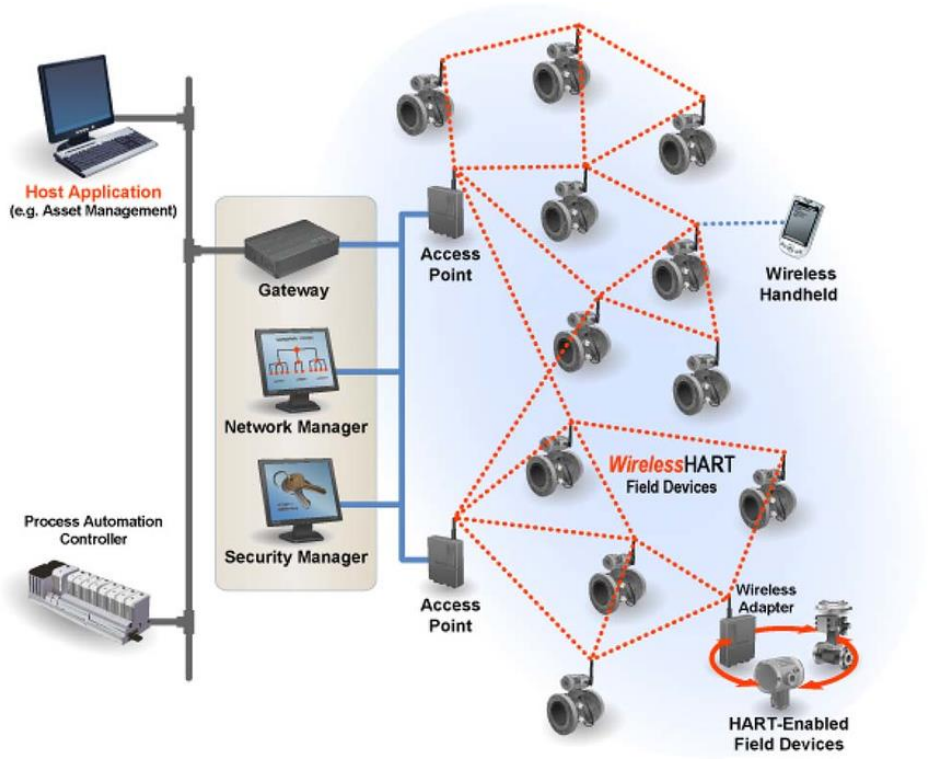


Figure 2-5. WirelessHART Network Architecture adapted from [60]

2.3.6 ISA100.11A

This standard is designed on the basis of the IEEE 802.15.4 with the aim to provide reliability to the wireless communications infrastructure for monitoring and control different types of applications [65] [66]. ISA100.11a like WirelessHART supports channel hopping and channel blacklisting to reduce interference and allows a device to coexist with other RF devices in the same band. It also benefits from TDMA mechanism that enables a device-to-device communication without delay in accessing an RF medium using the allocated time slot of 10 ms [62] [63]. At the network layer the standard facilitates the use of 6LoWPAN that is needed to handle IPV6 traffic and thus gives users the opportunity to connect to the internet. The ISA100.11a standard supports symmetric AES 128bit encryption.

An ISA100.11a network supports star, mesh and a combination of both and facilitates co-existence with WirelessHART [63] and it consists of different components that are essential to provide a fully functional network as illustrated in **Figure 2-6**.

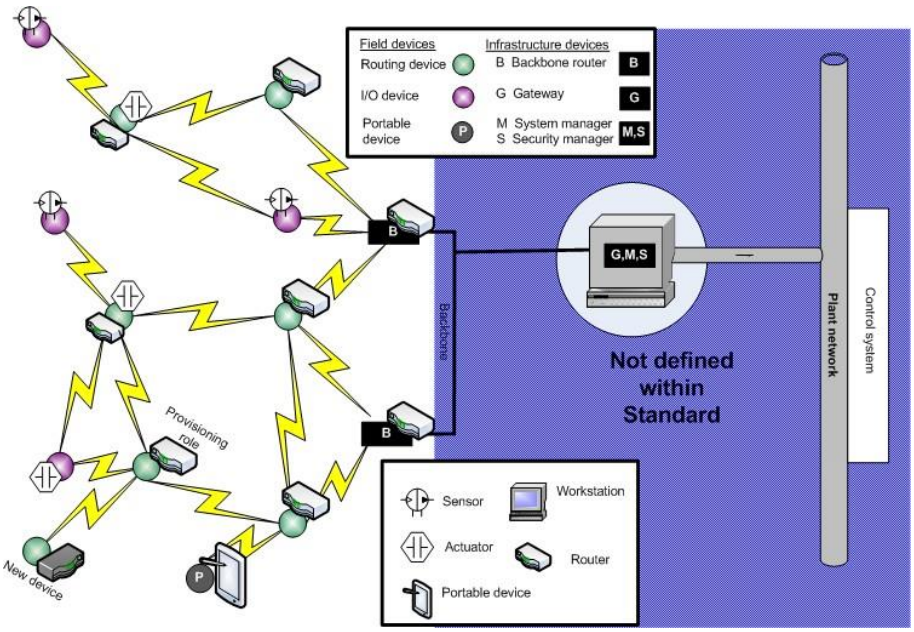


Figure 2-6. ISA.100 Network Architecture adapted from [67]

The authors in [70] have conducted study comparing WirelessHART and ZigBee in terms of some quality of services metrics such as robustness, coexistence and security. The outcome of the study showed that WirelessHART is a better choice for industrial applications compared to ZigBee in some quality of services terms. The authors in [57] (Liang, et al., 2011) have performed a comparative study on the WSN standards (WirelessHART, ISA100.11a and WIA-PA). **Figure 2-7** illustrates the protocol stacks of ISA100.11 a, WirelessHART, IEEE802.15.4, and ZigBee.

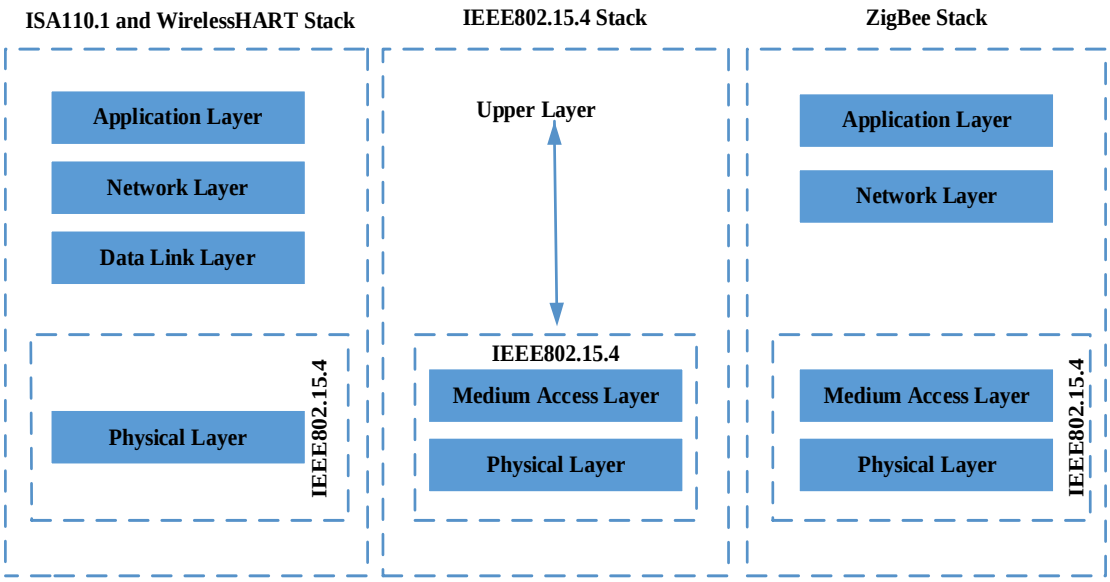


Figure 2-7. Protocol Stacks of ISA100.11 A, WIRELESSHART, IEEE802.15.4, AND ZIGBEE [68]

2.3.7 DISCUSSION

Based on the above review on WSN standards, we can conclude that WirelessHART and ISA100.11a both are suitable for industrial and large scale deployment, while ZigBee technology is suitable for general applications due to the limitation on radio range of 100 meter. WIA-PA is relatively new, and it is still not widespread deployed.

WirelessHART and ISA100.1 both standards define the radio on the basis of the IEEE 802.15.4 standard for low-rate wireless personal area networks (L-R WPAN). WirelessHART also uses unmodified IEEE802.15.4-2006 MAC, while ISA100.11a uses a modified, flexible IEEE802.15.4-2006 MAC. Both use the same mechanisms for establishing the wireless network and exchange data between network devices. Both standards deploy energy saving mechanisms that offer batteries longer lifetime. Both standards survive the interference caused by the presence of other network system by combining channel-hopping and direct-sequence, spread spectrum (DSSS).

The TDMA-based mesh topology used by WirelessHART and ISA100.1 provide a centralized infrastructure, that is required for large scale deployment. This makes both

standards preferred over ZigBee with its tree topology. Table 2-1 presents the comparisons among the three technologies.

Table 2-1. A comparison between WSN Standards [65] [42] [69]

Features	ZigBee	WirelessHART	ISA100.1
Underlying Standard	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.15.4
Security	High Symmetric	High Symmetric	High Symmetric/ Asymmetric
Scalability	Yes	Yes	Yes
Power Consumption	High	Low	Low
Latency	Low	High	High
Co-Existence	NO	Yes	Yes
Application	Commercial	Industrial	Industrial
Bandwidth	20-250 Kbps		
Transmission Range	2.4GHz and 868/915MHz	2.4GHz	2.4GHz Free Band
Network Size	65,000	Up to 250 nodes on a network	above 250 nodes per network
Topology	Mesh	Mesh and Star	Mesh and Star
Radio Channel	CSMA-CD	TDMA	TDMA / CSMA-CD
Network Routing Strategy	AODV/ Tree Routing	Graph/Source/Superframe Routing	Addressing; Routing

2.4 Requirements Of WSNs

There are certain requirements that are essential for a successful deployment of WSNs in the oil, gas and resources industries. In this section, the major requirements are discussed. In **Figure 2-8**, we propose a taxonomy of the requirements of WSN in the oil and gas industry.

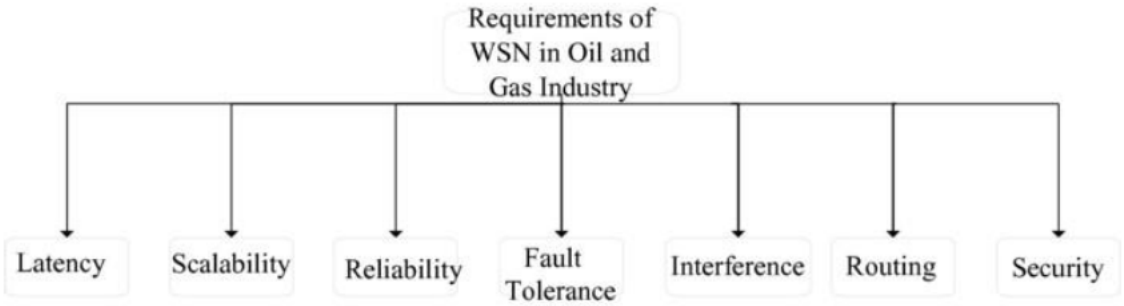


Figure 2-8. Taxonomy of Requirements of WSN in the Oil and Gas Industry

2.4.1 LATENCY

Latency is a measure of delay in time [71] that requires a data packet to successfully reach the receiving node and acknowledged. The probability of a successful transmission depends largely on the quality of transmission media, which is influenced by the signal-to-noise ratio in the RF domain. The number of hops from source to destination can also affect the latency [69].

2.4.2 SCALABILITY

Scalability is the ability of the network to cope with the growth in number of the sensor nodes which vary from a few to several thousands. Different requirements of applications in oil and gas industry require protocols and standards that are scalable and able to adapt new functionalities such as adding and removing numerous sensor nodes without impacting the quality of service (QoS) performance metrics [58] [69].

2.4.3 FAULT TOLERANCE AND RELIABILITY

Fault tolerant is described as the capability of the network to operate in a reliable fashion and adapt any topological changes that might occur as a result of node failures and link failures. Many factors [62] can affect the performance of a sensor node and cause frequent failures, such as energy depletion, harsh physical locations and other environmental conditions [72].

Reliability is the measure of the amount of data that is delivered from source and accurately received by the destination with minimum possible packet loss [69] [73] [74]. Usually, the reliability in each layer of the communication stack [58] has various requirements and definition of error rates, error burst, delay, error concealment techniques, etc.

2.4.4 CO-EXISTENCE AND INTERFERENCE

WSNs transmit on low-power signals are extremely sensitive to noise, which makes the radio signal subject to interference and multi-path distortion with other wireless networks and communication systems operating under the same radio-frequency (RF) medium. WSN

standards should be able to function efficiently and co-exist in the occurrence of interference [58] [75] [76] [77].

2.4.5 ROUTING

An essential design criteria is the capability to deliver packets from source to destination consuming the least amount of energy possible. There are various constraints that must be taken into account when designing a routing protocol for WSNs, such as node deployments, energy, scalability and other quality of services necessary metrics for reliable data delivery. It is therefore important to overcome these challenges before efficient communication and reliable monitoring system for oil and gas industrial applications can be achieved in WSNs [78].

2.4.6 SECURITY

One of the major benefits of WSNs is the ability to place sensor nodes in an environment without any supervision. This can provide security drawbacks to the network and backend system if the sensor nodes are located in harsh environments or in an unsecured manner while being readily accessible to people. Therefore, there is a need for security system that protect access and privacy [62].

2.4.7 POWER CONSUMPTION

The Oil & Gas Industry urges longer battery lifetimes that lasts over years for wireless sensors as a long term solution for the enormous effort required to maintain the network when replacing depleted batteries. In WSNs, rechargeable batteries are the main source of power for, and a regular replacement of the batteries is complex due to the number of several thousand sensors per plant, therefore nodes need to adapt an energy-aware mechanism in order to rationalize the consumption of energy and thus ensure a longer lifetime of the network [65].

2.5 EXISTING SOLUTIONS

In this subsection, an overview of the existing solutions that tackle the challenges and enhance the deployments of WSNs in oil and gas industry are discussed.

2.5.1 PIPELINE MONITORING

In [80], the authors proposed a magnetic-induction based pipeline monitoring system (MISE-PIPE) that is intended to provide real time leak detection in both under-ground and above ground pipeline. A performance evaluation test showed precise results in detecting and localizing leakages. In [81], a framework that aimed to provide cost-effectiveness, security and reliability in monitoring pipeline structures is proposed. However, the work does not provide neither technical design details nor performance tests. A crude oil leak detection and location monitoring system has been proposed by the authors in [82]. In [83], the authors discussed the reliability of using wave as a solution to detect leakages in pipelines. A wired PLC-5 programmable controller and wireless 1785-KE card were used to provide connectivity to the internet. It has proven its stability and reliability by detecting a leak that is larger than 2% of the total flow in 180 seconds, and accurate position that is less than 2% of the length of the pipeline. The authors in [84] introduced a heterogeneous network for underwater monitoring of oil and gas production to detect oil and gas leakages and to improve the flow and well production. A combination of ultrasonic and optical networks is used in additions to wires, to provide redundancy. Results showed that, connecting Tmote nodes with Micro- Electro-Mechanical Sensors (MEMS) to other Tmotes in the network using frequency (RF) communication or ultrasound or light connection improve the device flexibility.

A system that provides an early detection and warning ahead in time of failures and unexpected events has been proposed by the authors in [85]. The aims of the system are to meet the requirement of a real time monitoring in terms of the time delay between discovering a failure, examining the cause and preventing damage. The results show that 80% of messages

received in less than 1ms, where 90% have an average of 10ms latency. The authors in [86] have proposed an online monitoring and inventory management system (TOTE INVENTORY MANAGEMENT) based on Radio Frequency Identification (RFID) and WS that helps monitor production activities in oil and gas plants. The results show that the system will improve the operation, however the proposed system might face several challenges such as power consumption and interference with other in plant existing system.

The authors in [87] have tackled the problem of the safety in gas fields by introducing a multi-sensor gas monitoring platform that detects possible gas leakage in reliable manners and provides an accurate positioning of the source. The authors in [88] have addressed the moisture problem related to LPG, LNG pipeline in oil and gas production plant by introducing a monitoring system that is equipped with RFIDs sensor to detect the level of the received signal energy in a certain amount of time and thus the existence of moisture in the pipeline is determined.

2.5.2 LATENCY

The authors in [89] designed and deployed a WSN in a petroleum facility at College of North Atlantic, Cove Campus, and Newfoundland. The study focused on investigating the data rates and latency as important requirements of building a heterogeneous sensor network in an industrial area. An analysis of environmental noise in an industrial plant has also been conducted. The results showed that sensor networks for an industrial environment have stable supplies of latency, throughput and channel access. They have also concluded that the usage of pure CSMA-CD or TDMA might not be the optimal solution for some of the sensor or actuator points in the petroleum plant.

2.5.3 FAULT TOLERANCE AND CO-EXISTENCE AND INTERFERENCE

The authors in [90] proposed a WSN application to monitor shipboard PdM aboard an operating oil tanker. They have conducted an experiment using a mesh topology with three Intel Mote clusters and three Mica2 Mote clusters were used to investigate the fault tolerance problem. A fault tolerance solution, called FTSHM (fault-tolerance in SHM is proposed in [91] the authors aim is to predict the node or link failure and repair them before they occur. The authors in [92] have proposed a network infrastructure that combines the features of both wired and WSNs. The wired network devices act as a primary connection and the wireless network sensors providing a backup in the presence of network failures. They tackled the fault tolerance and power constraint by designing a network system in which the connection between nodes is performed through wireless transceiver and wired links, while the wireless transceiver is turned off for future backup activities the communication occurs using the wired links. The power is provided through wired Devices. The authors in [93] [94] carried out research about the technical possibility of implementing WSN in oil and gas industry environments. For they used WSN standards (WirelessHART, ISAl00.11, ZigBee) as solutions for applications monitoring. The results showed that all three studied standards function efficiently in the presence of other network systems and are able to survive the interference and noise issues.

2.5.4 RELIABILITY

In [71] the authors deployed a WSN at the Gullfaks offshore oil and gas facility in the North Sea to forecast production stops caused by pressure drops in well pipes. For this an ATEX version of the DUST wireless communications protocol with a wireless temperature sensor network was selected to forecast the loss of flow from a well. The result of this study demonstrated that the WSN allowed fast, relatively inexpensive and reliable detection of lost flows, therefore enabling quick action to re-establish flow. The WSN has provided almost 100% reliability with an acceptable latency (<2 Sec). These results show that WSNs are

completely capable of strong and reliable connection in the severe environment of offshore platforms.

2.5.5 ROUTING, ENERGY CONSUMPTION AND SECURITY

An enhanced version of the original AODV routing protocol has been proposed by the authors in [42]. In the M-AODV, the HELLO and ERR messages exchanged by the neighbor's device in the original AODV to announce their presence and update the routing table are eliminated and thus flooding the network with unnecessary broad-casts is avoided. The results obtained from the comparative study between M-AODV against AODV and HERA protocol showed the A-AODV outperformed both protocols in terms of delay but has similar performance to HERA in terms of stability and collision. It is also found that M-AODV has a higher transmission that reaches 99% in 3 minutes time interval 4 times faster as the original protocol. A study of Sensor lifetime maximization with respect to sensor placement along a pipeline under different power model, ideal power model and Tmote power model has been investigated by the authors in [95]. For their study, they distributed a set of Tmote Sky sensors with low power MCU MSP430, TI CC1101 transceiver chip. The sensors were distributed uniformly with equal distance. It is found that an increasing in the number of nodes under the equal distance scheme will result in decreasing the lifetime. The authors in [96] have tackled the security issues faced when deploying WSNs to control and monitor the safety of crude oil pipelines in industrial automation, specifically the Niger Delta region of Nigeria. They proposed a security solution that could protect oil and gas facilities from Vandalism by enabling a reliable and fast detection and re-porting of possible security breaches.

Table 2-2 provides a summary of the existing solutions that tackle the challenges and enhance the deployments of WSNs in oil and gas industry.

Table 2-2. Summary of the existing solutions that tackle the challenges and enhance the deployments of WSNs in oil and gas industry

Study	Technical Requirements	Technology used	Types of Motes	Network Type
[42]	Energy consumption and Reliability,	WirelessHART	N/A	Mesh and a SensiNet network
[45]	Reliability, power consumptions and fault tolerance	Multi-hop routing algorithm	N/A	Linear Infrastructure
[46]	Gas leaks in pipeline localization	ZigBee protocol	Temperature sensor	Linear Infrastructure
[47]	Gas leaks, corrosion, H2S	CDMA/GPRS	Temperature, pressure, motor current and voltage	Redundant Multi-hop Topology
[71]	Reliability	ATEX version of DUST Wireless Networks	N/A	N/A
[78]	Stability and Reliability	M-AODV (modified AODV)	N/A	Mesh Topology
[79]	Gas pipeline pressure, temperature	Optical Fiber	Pressure and temperature	Distributed
[80]	Gas Pipeline Leakage	Pressure, acoustic and soil property sensors	N/A	Magnetic induction-based wireless sensor networks
[81]	Pipeline Monitoring Scalability	N/A	MicaZ mote,RF Chipcon and CC2420 transceiver	N/A
[82]	Stability and reliability in Gas leakage detection	MODEM, GPS and wireless 1785-KE card	Pressure, flow and temperature	N/A
[83]	Leakage detection reliability	Wave	N/A	N/A
[84]	Redundancy in underwater gas Leakage monitoring	Ultrasonic and optical networks	Moteiv Tmote Sky Type) with TinyOS	Heterogeneous
[85]	Time delay in Gas Leakage detection	SOAP and MQTT	N/A	N/A
[86]	Monitoring and management inventory system	WirelessHART and RFID	N/A	Mesh topology
[87]	Safety in Oil and Gas Field	GPS\FRID,STM32F10 3 and µC/OS-II	Gas sensors	N/A
[88]	Moisture in LPG, LNG pipeline	Pico-RFID and Agilent's PSA E4440A	N/A	N/A.
[89]	Latency and Data rates	N/A	Tmote sky devices, MIMO access AGN1200 and TS-3300 board	Heterogeneous
[90]	Fault-tolerance,	N/A	Intel Mote and Mica2 Mote	. Mesh topology
[91]	Reliability, energy consumption and interference	backup sensor placement (BSP)	N/A	N/A
[92]	Fault-Tolerance	N/A	N/A	Wired/Wireless Sensor Network
[93]	Interference	WirelessHART, ISA100.11, ZigBee	N/A	N/A
[94]	Interference	WirelessHART, ISA100.11, ZigBee	N/A	N/A
[95]	Energy consumption	N/A	Tmote Sky sensors with low power MCU MSP430, TI CC1101	Uniformly Distributed Nodes

[96]	Security	Cyber Physical Systems (CPS), Wireless Fidelity (Wi-Fi) and low-cost digital Close Circuit Television (CCTV) cameras	N/A	N/A

CHAPTER THREE: THE IPV6 ROUTING PROTOCOL FOR LLNS (RPL): BASIC OPERATIONS AND SECURITY FEATURES

RPL is an IPv6-based proactive routing protocol designed by the IETF community to fulfil the routing requirements of a wide range of LLN applications [97]. RPL is optimized particularly for data gathering applications (i.e., MP2P traffic pattern), and it also provides a reasonable support for the P2MP traffic pattern, while providing an indirect support for the P2P pattern [97] [98]. In this chapter, an overview of RPL's operations, routing selection and optimization mechanisms, routing maintenance, is presented. In addition, a thorough analysis of RPL's limitations and security concepts is presented.

3.1 AN OVERVIEW OF RPL

The lossy nature of an LLN means that links can go down and then come back up quite regularly therefore it would be highly inefficient to send messages with this information on every occurrence. There would also be consideration of the low-power nature of Wireless Sensors, where various energy saving techniques can be utilised such as sensors going to sleep until required, in order to conserve valuable battery power. With it firmly established that no existing protocol provided the solution to these issues, in 2008 the IETF ROLL working group [7] was established with the purpose of creating a standardised routing solution for LLNs. This resulted in the standardisation in 2012 of the IPv6 Routing Protocol for Low-power and Lossy Networks (RPL) [99]. RPL is basically a proactive distance-vector based routing protocol that organizes a physical network into a form of Directed Acyclic Graph (DAG) [101] [102] [103].

3.1.1 RPL TOPOLOGY

The main concept of RPL is that the nodes are able to self-organize themselves by forming a hierarchical tree-like topology with a root at the top named the Destination-Oriented Directed Acyclic Graph (DODAG) as illustrated in **Figure 3-1**. RPL networks carry two types of traffic:

upward and downward traffic. Upwards traffic to the sink can be described as multipoint-to point from the nodes to the DODAG root, while downwards can be described as point-to-multipoint from the DODAG root to the nodes [104][105]. Considering energy consumption, the protocol uses a proactive approach to construct and maintain the topology and a reactive approach for resolving routing conflicts.

A DODAG is built according to an Objective Function (OF) [106] that can utilise several different metrics and constraints and plays a significant role in the building of a DODAG instance.

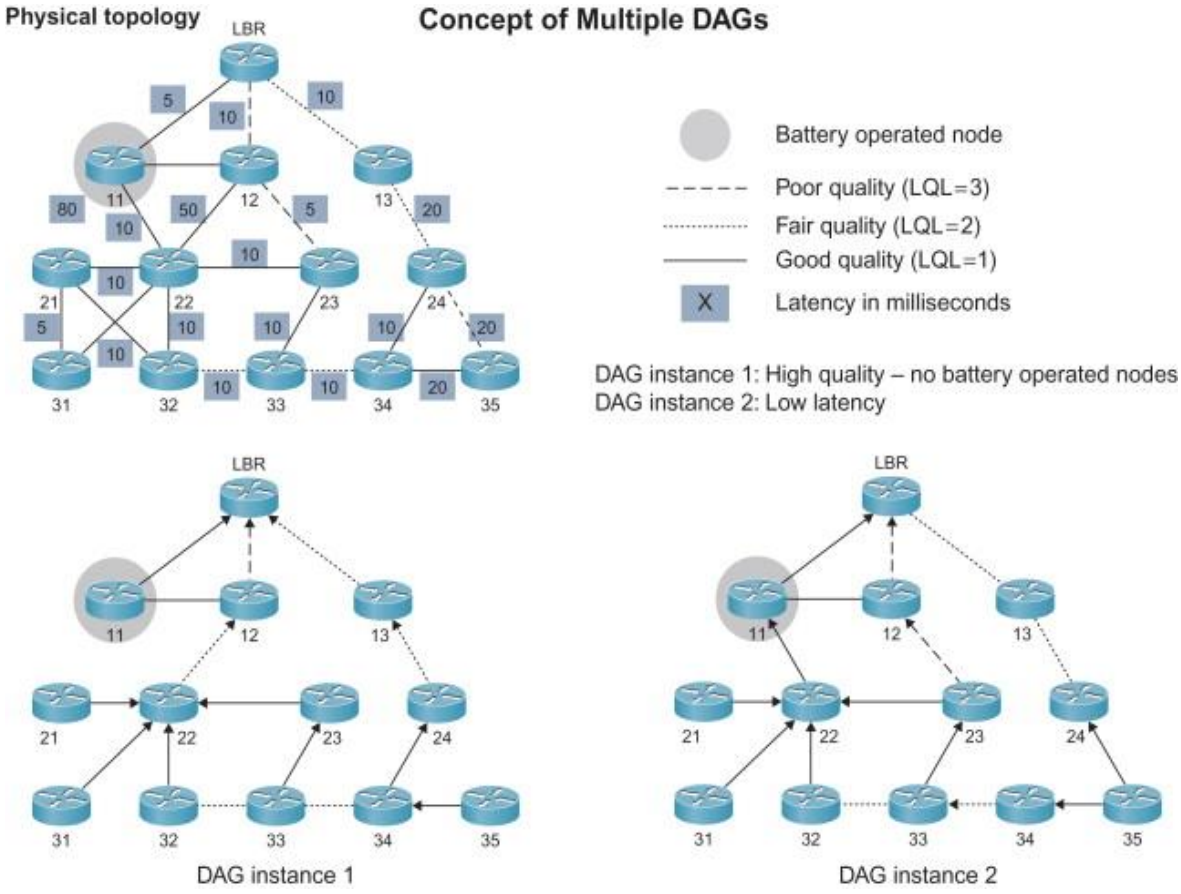


Figure 3-1. Example of Multiple DODAG Instances [39]

3.1.2 RPL OBJECTIVE FUNCTION

The construction of a DODAG is performed in accordance with an Objective Function (OF) and may use one or more metrics for the aim of optimizing a specific routing goal [106].

A metric is more relevant to the cost of the path in regard to a routing destination. For example, RIP uses hop-count as metric, the path- cost being the number of hops to a destination [107]. In the case of RPL the use of constraints and metrics is combined into a routing objective. For example, the routing objective could specify a constraint such that the OF should prune any paths with nodes below a certain memory capacity or could specify a metric such as hop-count [39] [106].

3.1.2.1 The Objective Function Zero (OF0)

The Objective Function Zero (OF0) [105] is the default OF for RPL. The standard does not specify a specific metric to be used under this OF so it can be used with any metric with goal, for instance, to minimize the number of hops along the constructed routes or maximize the reliability. In other words, a node will always select the closest node (shortest path) to the DODAG as its next hop for routing and will always switch to the shortest path when a new one is available [105].

3.1.2.2 The Minimum Rank with Hysteresis Objective Function (MRHOF)

The Minimum Rank with Hysteresis Objective Function (MRHOF) [106] again seeks to reduce the distance to the DODAG root. However, unlike OF0, introduces the concept of Hysteresis which favours stability over switching to the shortest path that does not meet a pre-specified threshold called the “Hysteresis”. In the case of MRHOF it determines the shortest path using the metrics or constraints carried within the metric container advertised in the DAG container option in DIO messages [1]. If no metric is advertised in the DIO messages, then MRHOF will default to the ETX metric [106]. However, MRHOF can use any of the metrics

defined in “RFC6551: [40] such as Hop Count, Link Latency, ETX, RSSI, Node Energy, Throughput.

3.1.3 RPL ROUTING METRICS

Several metrics have been proposed for RPL with the following are the most popular.

3.1.3.1 Minimum Hop Count (Minimum Hop Count)

The most used metric to create paths in the context of WSNs is the hop-count between sender and receiver, as protocols like the DSDV and AODV assume that all connections between nodes are either 100% reliable or do not work at all which is unrealistic approach. Due to the dynamic nature of the channels, especially in networks of reduced power and performance in terms of binary output, the communications undergo variations related to interference and concrete characteristics of each application such as line-of-sight factors. The hop-count metric also undergoes network-level performance failures, especially in dense networks. Minimizing the number of hops increases the distance of each jump, minimizing RSSI and the loss rate. And even if the best routing is the one that keeps the fewest jumps, there may be other possible routing, with better performance and better quality of service. Therefore, the choice of routing with the least number of hops will not always be the best routing possible [40] [108].

3.1.3.2 Expected Transmission (ETX)

The solution proposed in [109] for creating paths is the Expected Transmission (ETX) metric [107] which can be defined as the number of transmissions and retransmits of a packet until arriving at the destination. Because the resulting ETX assigns a cost to bidirectional connections by the rate of losses they have on downlinks and upstream links, the choice of routers with high bit rate is forced. The basic calculation of this quotient can simply be inferred by the number of transmissions, t of p data packets successfully delivered between the node x and the node y [109].

$$g(x , y) = t/p \quad (1)$$

The ETX makes an indirect count of the number of hops. For example, if the connection between two nodes (one-hop only) has a success rate of 50%, the ETX will equal 2.

3.1.3.3 Received Signal Strength Indicator (RSSI)

Whilst the use of hop-count and ETX are common approaches in the utilisation of the RPL routing protocol, the use of Received Signal Strength Indicator (RSSI) [110] is less so. In the most basic terms, RSSI is the measurement of the strength of a signal at the point of reception. As such, a higher RSSI indicates a stronger and more powerful signal transmission. In the case of routing, this involves utlising this measurement in order to determine the best path to a destination based on signal strength.

3.1.4 TRICKLE TIMER

One of the key design principles of RPL protocol is minimizing the routing control overhead and signaling data as a mechanism to reduce energy consumption and enhance the reliability of the protocol. To this end, RPL has adopted Trickle algorithm [111] to govern transmission of the signaling traffic used to construct and maintain the DODAG topology. The basic idea behind Trickle is to adjust the frequency of message transmission based on network conditions. In this regards, Trickle relies on two main simple principles or mechanisms to efficiently disseminate routing information. The first mechanism is to adaptively change the signaling rate according to conditions currently present in the network. Trickle increases the transmission rate when a change in routing information of the network is discovered (inconsistency is detected) as a mean to rapidly populate the network with the up-to-date information. As the network stabilises, Trickle exponentially reduces the transmission rate in order to limit the number of transmissions when there is no update to propagate. The second mechanism used by Trickle is the suppression mechanism in which a node suppresses the

transmission of its control packet if detected that enough number of its neighbors have transmitted the same piece of information and by that limiting the number of redundant submissions. The adaptive signaling rate in addition to suppressing redundant information enables the network to use its available resources efficiently and as consequently save energy and bandwidth.

3.1.5 RPL OPERATIONS

As with other routing protocols RPL uses the exchange of ICMP messages to build a topology. In the case of RPL the messages are ICMPv6 and the three message types used are:

- DODAG Information Object (DIO). Used for DODAG discovery, sent to advertise a DODAG in the 'Down' direction to build 'upward' routes to the DODAG root. Advertises routing metrics and constraints [40].
- Destination Advertisement Object (DAO). Used to establish 'downward' routes therefore sent in the 'Up' direction. Can optionally be acknowledged by the destination node with a Destination Advertisement Acknowledgement (DAO-ACK) message. RPL specifies two kinds of nodes for downward routing. Storing nodes effectively use their own routing tables to determine the next-hop for a packet whereas non- storing nodes do not have routing tables for downward routes. The route the packet must take is populated in the packet by the DODAG root.
- DODAG Information Solicitation (DIS). Used to solicit DIO messages from nodes, much like a router solicitation message in a traditional network [1] [39].

The structure of a DODAG is initialized by the DODAG root by multicasting DIO messages to other nodes [111] [1].

Upon receiving DIO message from the DODAG root, a node calculates a value called the Rank that reflects its distance from the DODAG root, selects the root as its parent, and then multicasts the DIO to other neighboring node updated with its calculated rank. [39]. If a node

receives DIOs from multiple neighbors, it will select the node with smallest rank as its own parent considering any constraints set by the used objective function.

3.2 RPL LIMITATIONS AND DRAWBACKS

3.2.1 RPL WITHIN A MOBILE ENVIRONMENT

When referring to mobile nodes within an LLN, in regard to the use of RPL, there are two distinct possibilities. One is the issue of a regular node being mobile, gathering data to then send back to the sink node. This is generally where issues arise in regard to parentage and the node becoming part of the DODAG, as seen in **Figure 3-2**. The second possibility is that of the sink node itself being mobile. Within either of these possibilities there are common issues in regard to the detection of mobility, such as the velocity of the node, is the pattern predictable or random and the context in which the mobile node is being utilised. With regard to mobile sink nodes further issues arise such as how the sink node is advertised, whether the DODAG should be constantly rebuilt and again the pattern of movement. But in this case whether it is by design or reactive, possibly moving away from energy depleted nodes. **Figure 3-3** shows a sink node moving from its initial position, with the issue of DODAG build clearly visible. It is feasible that the rank of every other node could change as the sink node moves. But the rate this occurs would depend on the Trickle timer [10]. By mobilising the sink node, the aforementioned issues regarding hotspots and bottlenecks inherent in the use of static sink nodes can be negated.

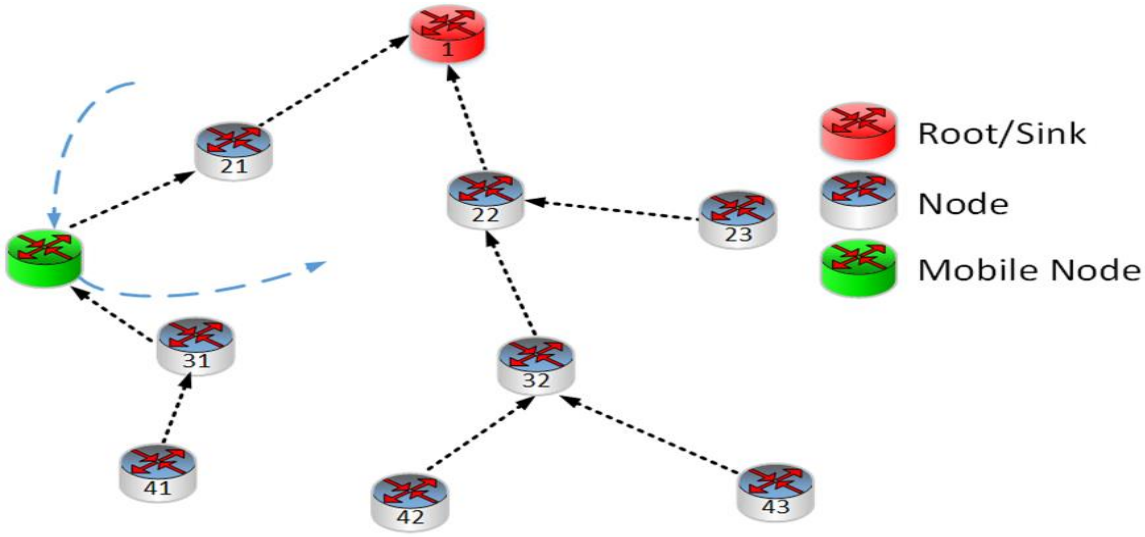


Figure 3-2. Static WSN with Mobile Node

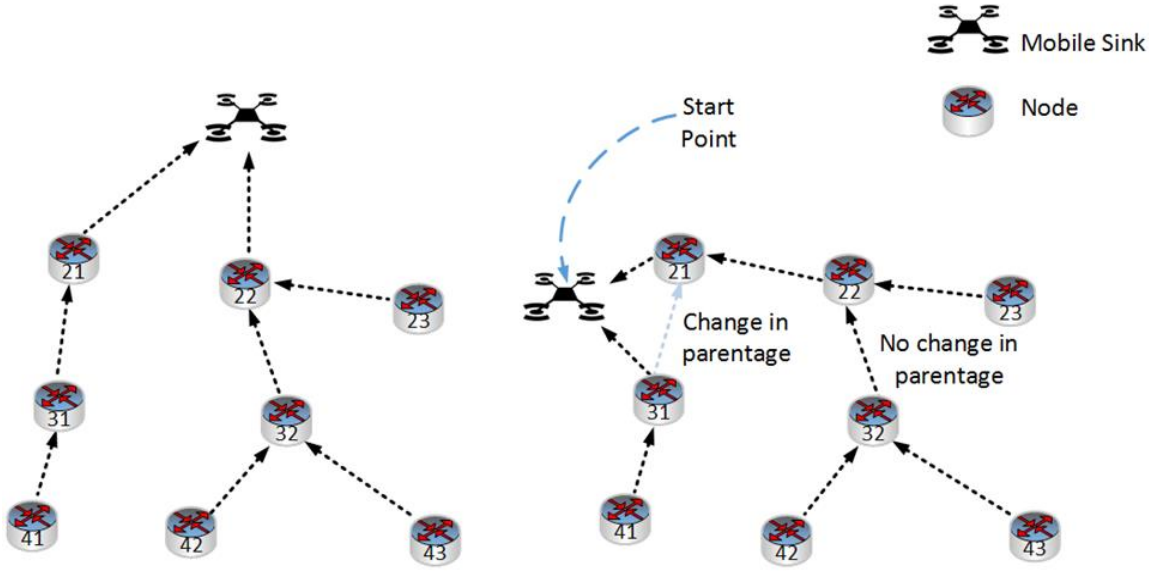


Figure 3-3. WSN with Mobile Sink Node

3.2.2 UNDER-SPECIFICATION OF METRICS COMPOSITION

RPL is a flexible and adaptive protocol, specifically designed with the propensity for packet losses in WSNs in mind. These packet losses are expected in WSNs with the potential for environmental factors coming into play, which could cause interference and therefore extreme link-instability, resulting in high levels of packet loss. In this case different principles

must apply. RPL cannot overreact to packet loss by immediately recalculating routes, due to the limited power and data transfer rates available [106].

In regard to the establishment of the best route to a destination in RPL and as discussed earlier, RFC specifies building a destination oriented directed acyclic graph (DODAG). A DODAG is a logical topology placed over a physical network of which there can be several and of which a node can be a member of multiple occurrences. The characteristics of a DODAG will reflect Quality of Service (QoS) or constrained-based routing requirements in such that each DODAG 'instance' has a particular role to provide regarding routing across the physical network. A DODAG is built according to an Objective Function (OF) [40], which can utilise several different metrics and constraints to build the DODAG topology.

RPL may also utilise constraint- based routing, which looks at restrictions on nodes such as energy-saving, CPU levels and memory capacity [40]. As such an OF may include or exclude routes depending on these requirements. A metric is more relevant to the cost of the path in regard to a routing destination. In the case of RPL, the use of constraints and metrics is combined into a routing objective. For example, the routing objective could specify a constraint such that the OF should prune any paths with nodes below a certain memory capacity or could specify a metric such as hop-count. The values, however, are not exclusive and can be used as either constraint or metric in that a hop-count could also be used as a constraint to only use paths above or below a certain number of hops [9][11].

3.2.3 SUITABILITY OF RPL FOR LINEAR SENSOR NETWORKS (LSN)

Recently, the use of Linear Sensor Networks (LSNs) has emerged as an area of interest in many several applications. An LSN becomes pertinent in situations where sensors are required to be lined up due to the particular application. This may be the monitoring of roads and bridges, however, the most obvious use is in pipelines [81] [145] [146]. This may involve the monitoring of oil, gas or water, or sensors gathering information on the pipeline itself regarding

temperature, water or oil flow, leakages, fire or pressure [81]. A driving factor behind the use of LSNs as opposed to wired networks is in the security of transmission and being less prone to failure or sabotage [81].

Despite the obvious need for research in the application of LSNs, the difficulties inherent in improving these networks has resulted in a dearth of related work. As such, whilst the less complex implementation of a linear network topology may first indicate a simple implementation, this is not always the case. Whereas a complex network topology presents many different opportunities to improve the different facets of network performance, the same cannot be said for an LSN. An LSN presents little room for maneuver with regard to different combinations of Layer 3 metrics and algorithms to improve network performance. In areas such as data delivery and energy consumption.

In simplistic terms, if the transmission range of any node only puts one node within range, as in **Figure 3-4**, then this node will always be the next hop, whatever routing metric is utilised. This then puts a vast amount of strain on nodes nearest the sink node, which will be the recipient of every single transmission in the network. This issue can be negated by increasing the transmission range (TX) of nodes, as in **Figure 3-5**, enabling neighbouring nodes in the linear structure to be hopped over. Whilst also bringing the possibility of utilising other metrics such as ETX or residual node energy. However, the cost of this pay-off is in increased energy consumption by each node. This occurs as radio signals are increased in order to improve said TX [9]. The challenges inherent in improving performance levels in LSNs have been overviewed in serval studies. What is clear is that there is little consensus on how best to approach the issue of routing in LSNs. However, given the recent standardization of the IPv6 Routing Protocol for Low-power and Lossy Networks (RPL) [1], there is a requirement to evaluate the performance of this protocol in LSNs and to improve it where possible especially in relation to the optimal placement of nodes in such networks.

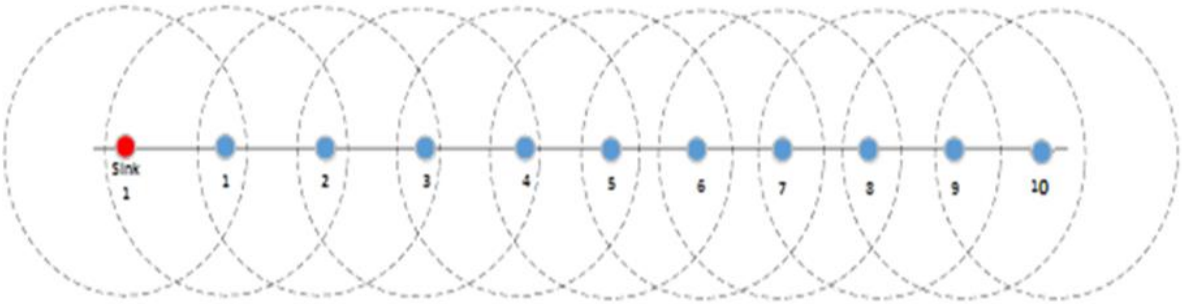


Figure 3-4. One-hop Transmission range

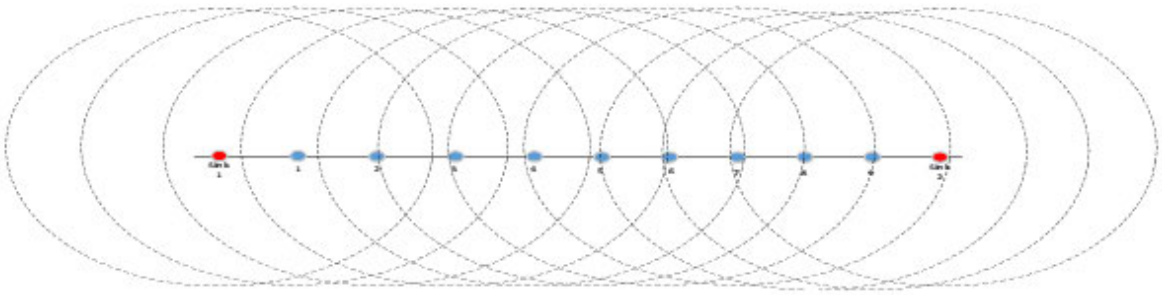


Figure 3-5. Multi-hop Transmission Range

The obvious benefits in the application of LSNs has driven the need for research in this area. However, related work is sparse which may be due to the difficulties inherent in improving data delivery in LSNs. Whilst the lack of complexity in physical layout of a LSN over other WSNs may at first give the impression of a simple implementation, the opposite is commonly the case. This is due to the lack of 'wiggle room' when seeking to make improvements in network performance. Whereas in more complex network structures the opportunity will exist to develop combinations of metrics to ensure an optimal combination of efficient data delivery and energy consumption, this is not generally possible in an LSN.

3.2.4 RPL DOWNWARD ROUTES

Pertaining to the storing mode of operation and as depicted in **Figure 3-6**, each RPL router must store a routing state for each reachable destination in its own sub-DODAG. As a result, a router may run out of memory easily resulting in the newly received DAOs being ignored. This

means that several downward routes or destinations would remain undiscovered impacting negatively the application reliability and scalability [9]. Although an RPL router may have multiple parents (multiple candidate parents in addition to its preferred parent), RPL's router is allowed to advertise prefixes, belong to its sub-DODAG, to only its preferred parent. This hinders the protocol from exploiting the additional storage that might be available in other candidate parents which further harms the protocol scalability and reliability. The current proposed solutions for mitigating this issue have concentrated on combining both storing and non-storing modes of RPL or mixing the storing mode of RPL with multicast forwarding. However, as the non-storing mode has its own disadvantages, these disadvantages would be inherited in the hybrid approach. In addition, these mechanisms only allow destination advertisements to be unicasted to the preferred parent.

To further get insight into this issue, let us assume that we have a network of six nodes with a routing capacity of two entries per node excluding the root A which has no capacity limit. Given that after the DODAG is constructed, we ended up with the topology depicted in **Figure 3-6a**. In this topology, the node D has one preferred parent B and another candidate parent C. It also has two children E and F. For constructing the downward routes, each node should announce its prefix to the root via its preferred parent. For instance, in **Figure 3-6b**, E transmits its prefix in a DAO message to its parent D, which stores it in its routing table and forwards it, in turn, to its preferred parent B and finally to the root A. The routing tables of the nodes until before the node F announces its prefix would look as depicted in **Figure 3-6c**. However, because the B routing table is limited to two entries, the prefix of destination F cannot be stored in its routing table. As for RPL, although an optional Destination Advertisement Object Acknowledgement (DAO-ACK) has been defined to signal the rejection or acceptance of the advertised destination, RPL does not specify how to handle this case. Thus, the state of the prefix F will not be forwarded up the network, even though, another candidate parent, C,

might be willing to perform the task as depicted in **Figure 3-6d**. In this study, we argue that there is still a window for enhancing the operation of RPL storing mode by exploiting a feature in RPL that allows for multiple DAO parents before one can resort to other developed techniques.

Another key issue when constructing downward routes in RPL is that the timing of DAOs emission is not explicitly specified [1] [31]. The under-specification of DAOs timing may lead to conflict and inefficient implementations resulting in a poor performance. For instance, the study in [10] has opted to periodically transmit DAO messages, increasing significantly the control overhead in comparison with ContikiRPL [11] implementation which transmits the DAO messages based on the Trickle timers of DIOs. Although it managed to lower the overhead, ContikiRPL is still relatively inefficient. This is because ContikiRPL associates (couples) a node's DAO transmission with the DIO transmission of its preferred parent. In other words, a node should unicast a DAO to its preferred parent each time it receives a DIO from this parent which deems to be unnecessary. This is because receiving a new DIO from the parent does not necessarily mean that an update is needed. Thus, sending a DAO would be just a waste of resources. Furthermore, although an optional control message (DAO-ACK) with rejection status code has been defined by the standard to inform the DAO sender of the recipient incapacity to accept the new routing entry, RPL does not specify how the DAO sender should handle or react to this rejection. Therefore, the target advertised by the rejected DAO would remain unknown to all routers higher in the DODAG, including the root, rendering the partially built route useless. This would leave the DODAG root with no option but to drop all the data-plane messages destined to unknown prefix [7].

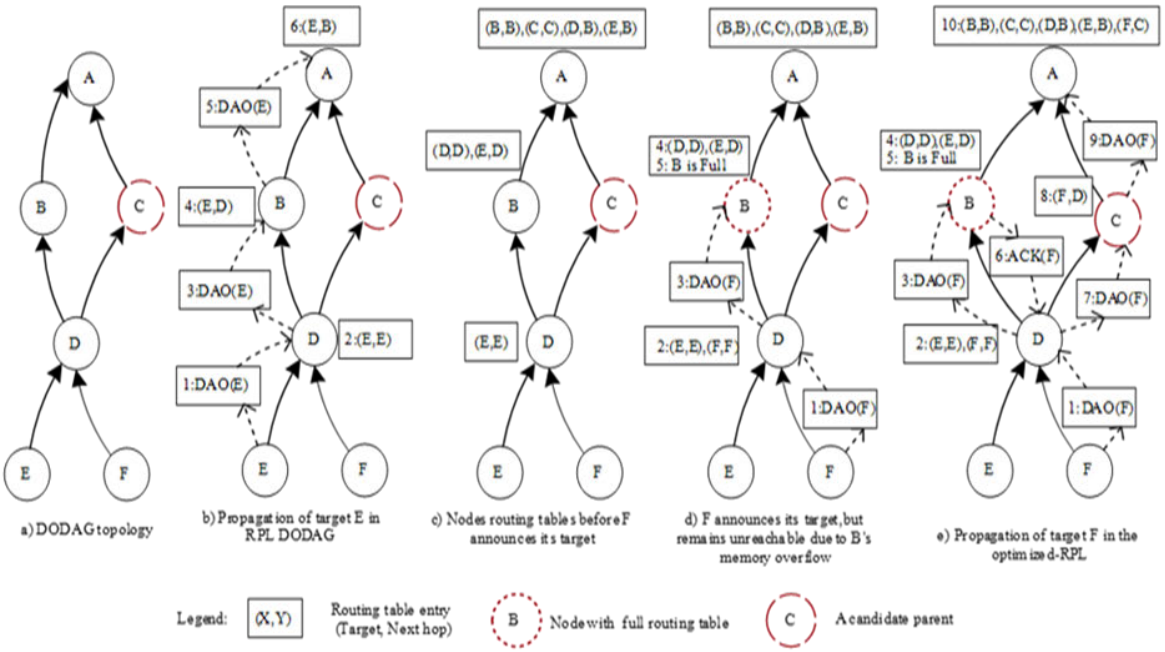


Figure 3-6. Operations of RPL and the Enhanced-RPL

3.2.5 RPL SECURITY LIMITAIONS

Vulnerable components in LLNs include the routing information that is exchanged and stored, as well as the available resources of the nodes and the processes running on them [112]. Routing information is exchanged in LLNs using wireless communication at the control layer and partially cached on the reprocessing nodes. The resources on the nodes consist of their computing power, available memory, available energy, and the bandwidth available to communicate with their neighbors. The routing processes of the node summarize services that generate and maintain routes in the topology. Among the potential attacks in the immediate area of the topology is the possibility to attack the RPL nodes from a distance through the Internet. This is made possible by the fact that RPL is designed for use on low-resource nodes, allowing communication and interaction with nodes from other IPv6-based networks [13] [14].

To protect against attacks, RPL defines optional cryptographic protections that enable secure communication using secret keys [113].

RPL attacks can be categorized into three types of attacks:

3.2.5.1 TOPOLOGY ATTACKS

Attacks that can be used to manipulate the orientation of the paths of a DODAG (Direction-Oriented Directed Acyclic Graph). For this purpose, the attacker attempts to deform the DODAG in a targeted manner, so that the paths on which messages are exchanged are directed specifically into certain sections of the DODAG or the message exchange on the affected branches is disturbed. In the Storing Mode of Operation (MOP), the attacker can advertise paths to non-existent sub-DODAG nodes by tampering with DAOs, fictitious prefixes. The information about the advertised prefixes of the DAO propagates upward to the root of the DODAG. All parent nodes in the relevant branch enter the advertised prefixes in their routing tables, and potentially cannot enter and serve sub-DODAGs of other children. Nodes whose downward prefixes cannot be operated in the affected branch will only be able to advertise their prefixes in other branches if available. If the nodes migrate their paths to the alternate parent nodes, their downward routes are pushed out of the affected upward branch of the attacker, resulting in a degeneration of the original DODAG. If a child with its sub-DODAG incorrectly joins a parent node that cannot operate the sub-DODAG with messages in the direction of the child, the prefixes are not advertised upward and remain unknown on the downward path to the affected parent node [114] [115] [159].

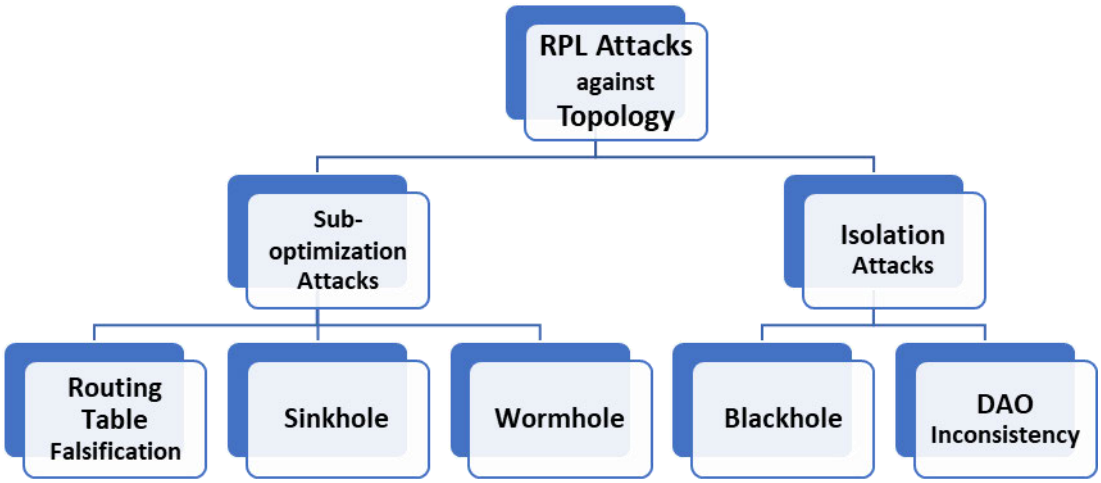


Figure 3-7. RPL Attacks against Topology

3.2.5.1.1 ROUTING TABLE FALSIFICATION

This attack targets nodes operating in storing mode. The malicious node modifies or forges DIO control messages to advertise the false downward route to a destination. The target nodes then add the false routes to their routing table despite the routes inducing delay, packet drops and congestion. Receiving different routes to the same destination can indicate this attack is occurring [116].

3.2.5.1.2 SINKHOLE

In the sinkhole attack the attacking node first advertise to its neighbours falsified information about beneficial path in order to attract as much as possible nearby devices to route their traffic through itself. Then it modifies the original traffic executing selecting forwarding or dropping packets. This attack is not completely disruptive for the topology but, because of its falsified path advertisement, degrades the network performance and can create more damage when combine with other attacks [116] [117].

The authors in [118] proposed a method using Multi-sinks in IoT (SDMSI) to detect sinkhole and rank attack in RPL topology. The method utilises a link latency threshold in the root nodes that must not exceed specific value. If the link becomes silent for a period higher

than the latency threshold the malicious node is then added to a blacklist. The authors tested the proposed solution using Cooja simulator. The result shows efficiency in terms of, traffic congestion, communication, and resource consumption. However, there is an increase in the overhead.

The authors in [119] presented a trust-based lightweight solution to detect the sinkhole attack. The RFTrust proposed model utilises Random Forest (RF) and Subjective Logic (SL) machine-learning algorithm to calculate the trust metrics for every node in the network. Nodes with high packet delivery ratio and low latency are classified as trusted, and nodes with high packet delivery ratio, high delay and honesty neighbour are trusted. Nodes with high packet delivery ratio, high delay and dishonest neighbour are classified as malicious, and nodes with low packet delivery ratio and dishonest as malicious. The authors used the Contiki 3.0 OS and the Cooja simulator to test the proposed model. The results show the effectiveness of the RFTrust model in terms of PDR, throughput, delay and low energy consumption.

3.2.5.1.3 WORMHOLE

In wormhole attack two or more malicious nodes in the topology can pose the network to a serious security breach, especially if combined with other attacks. For example, two attacker nodes can create a tunnel and transmit a part or all traffic through it, disrupting the network topology and the traffic flow. Wormhole nodes are not necessarily malicious, but rather can be used to, for example, send critical messages faster [120].

In [121] the authors have proposed a framework that mitigate against rank and wormhole attacks using machine learning approach.

The authors in [122] have proposed recurrent neural network (RNN), deep learning model using confusion matrix to detect and classify the wormhole attack. Contiki OS and the Cooja

simulator was used to evaluate the proposed model. The results show an accuracy of 96% and a precision score F1 score of 0.96 in detecting and classifying the wormhole attacks.

In [123] the authors presented a Deep Learning based approach for the anomaly-based intrusion-detection model. The approach used deep belief network (DBN) for detection of malicious nodes in the IoT network demonstrating the feasibility of using Deep Learning algorithms for effective anomaly detection in IoT environments.

3.2.5.1.4 BLACKHOLE

In the blackhole attack, a malicious node drops all the packet that essentially triggering a Denial of Service (DoS). This attack can be categorised as a Topology- isolation attack. The attack can be implemented by making the node maliciously advertising itself as the shortest path to the destination during the path-discovering mechanism. As a result, the DODAG graph will be sub-optimised or and part of the network would be completely isolated [116].

In [124] the authors have addressed the impact of both rank and blackhole attacks, when combined, and proposed a trust-based security framework (SRF-IoT) to detect and isolate malicious attackers with the help of an external intrusion detection system (IDS). For the evaluation of the framework, they have used the Whitefield framework that combines both the Contiki-NG and the NS-3 simulator. The results show increase in term of packet delivery ratio (PDR), decrease in term of packets dropped, number of parent changes and minimal overhead.

In [125] a UDP-based heartbeat detection method for greyhole and black-hole attacks. The idea is to send ICMPv6 echo requests from a dedicated node to the rest of the nodes in the network. If the sender of the ICMPv6 echo request does not receive a response, this may indicate that there is an ongoing blackhole attack and further investigation will follow. Moreover, if a node goes down for some reason, this mechanism should be able to detect that.

The authors in [126] have proposed an intrusion detection mechanism to mitigate blackhole attacks. Their proposed method uses a watchdog module (Local Detection) and a BR module (Global Detection and Eviction). To detect a malicious node the watchdog performs local detection by monitoring each node behavior by collecting the DAO, DIO, DIS, and DAO-ACK and data packets exchanged by the nodes. Then it sends the obtained results to the BR, which performs the global detection by aggregating the classification results using Dempster-Shafer theory of evidence. To evaluate the proposed IDS, the Contiki OS 3.0 were used. The simulation results showed an increase in the true positive rate (TPR) and packet delivery ratio (PDR) and decrease the false-positive rate (FPR) and end-t-end-delay (EED).

In [127] the authors have introduced a mechanism for the detection of black holes attacks. Their model consists of two steps to detect a malicious node a suspicion and verifications step. In the suspicion step, each child node starts a timer once the connection to a parent is established. The timer is restarted each time the child node receives packets from its parent node. If no packets have been received within the time threshold, the node is declared as a potential black hole node and a verification process is initiated. In the verification process the child node broadcast a verification packet to all neighbours. If the verification fails, the node is assumed to be malicious and the initiator node changes its parent.

The proposed model was implemented using the Contiki-NG operating system. The simulation results shows that the model was able to detect and isolate black holes effectively with low false positives and false negatives and a high true positive.

3.2.5.1.5 DAO INCONSISTENCY

In this attack a malicious node attempts to drop the received packets and sets a forwarding error flag in packets forwarded to its parent nodes. As a consequence, parent nodes remove

valid downward routes effectively sub-optimising the topology and isolating the malicious nodes' sub-DODAG [128].

An intelligent lightweight IDS model named RAIDER has been proposed in [129] to mitigate against four different attacks namely rank attack, DAO inconsistency attack, sinkhole attack, and DoS attack on RPL. The model introduces an automata-based lightweight intrusion detection methodology called RAIDER with a context-aware decision-making model. The proposed RAIDER mechanism utilizes a finite automata model for detecting intrusions in the network. The use of different state transitions helps in avoiding false detection of normal nodes as attacker nodes. Contiki OS and the Cooja simulation results show the enhanced performance of RAIDER with an 88% reduction in delay and 25% better energy consumption than the SecTrust protocol.

3.2.5.2 RESOURCE ATTACK

Attacks that increase the energy consumption of RPL nodes. The attacker attempts to load a node with computationally intensive operations and frequently consumes its memory. The motivation behind the attacks is to weaken the performance of the entire topology and thereby disrupt the operation in the DODAG [130] [131].

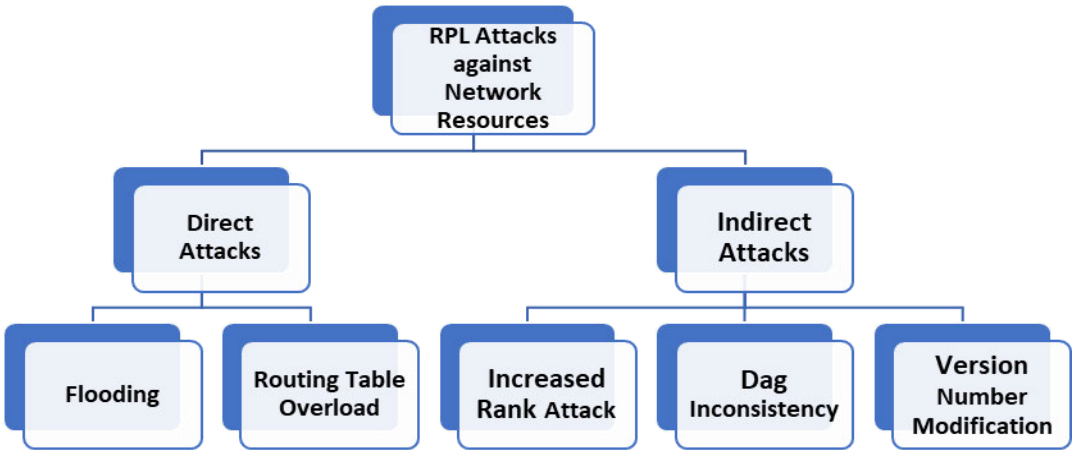


Figure 3-8. RPL Attack against Network Resources

3.2.5.2.1 FLOODING

In RPL, nodes willing to join the DODAG broadcast DIS messages to request DIO messages from neighboring nodes. A malicious node may exploit this case to flood the network by periodically transmitting DIS messages to its parent node.

The authors in [132] have addressed the DIS flooding attacks by proposing a Secure-RPL mitigation mechanism that restricts unnecessary trickle timer resets and DIO transmissions caused by DIS flooding attack. The Contiki operating system was used to evaluate the performance of the proposed mechanism. The simulation results shown significant improvement in terms of control packet overhead and power consumption.

3.2.5.2.2 ROUTING TABLE OVERLOAD

In this attack a malicious node operating under storing mode announces fake routes using DAO messages to saturate the routing table of the targeted nodes. The attack prevents the legitimate nodes to create legitimate routes thus reducing network availability and causing memory overflow [133].

The authors [133] in have presented a solution to the routing table overhead attack by introducing STIR, an RPL protocol modification that permit parent nodes only to store as many routing table entries as it has children or sub-DODAGs. This in return will prevent a malicious child node to add new routing table entries for an unknown or forged nodes. They have used Cooja to evaluate the performance of the proposed solution. The results show improvement in terms of the routing table size metric, however adding additional control messages has reduced the performance of the network.

3.2.5.2.3 INCREASED RANK

RANK is a basic parameter of the RPL protocol which indicates the position of a node in the DODAG relative to the root node. In a rank attack, the attacking node falsely advertises a

either higher or lower rank to its neighbours. Then it selects a preferred parent that was previously in its sub-DODAG leading to routing loops. Due to the attack the rank rule is broken sub-optimised path will be created in the network, decreasing the overall network performances in terms of packet delivery ratio, power consumption and topology optimization. [134].

3.2.5.2.4 DAG INCONSISTENCY

In DAG inconsistency attack a malicious node manipulates the data path validation mechanism by altering the header flags on the forwarded packet forcing the receiving nodes to reset the trickle timers, causing flooding. A malicious node may isolate other nodes by adding a forwarding error flag in the forwarded packets to its neighbor forcing them causing them to drop it [135].

3.2.5.2.5 VERSION NUMBER MODIFICATION

In version number attack the attacking nodes advertise a higher version number of the DODAG graph. When nodes receive the new higher version number DIO message, they start rebuilding of the DODAG tree. This unnecessary rebuilds increases the convergence time, creating inconsistences in the topology and inevitably decreasing all network performances [135].

In [136], a Version Number Attack Detection System (VeNADet) is proposed that puts certain conditions on the nodes to updates their Version Number. Any node that does not meet theses condition is considered as an attacker and is isolated from the network. The Cooja simulation results shows that 94.4% of Version attacks were efficiently detected.

3.2.5.2.6 THE DAO MESSAGES

DAO messages are used in RPL networks to create the routing paths that will carry the downward traffic from the DODAG root to the respective nodes. The specification of RPL does

not define how often and/or when such messages are to be transferred. Therefore, different implementations of the protocol may opt to propagate DAOs messages differently. For example, the implantation of RPL in [22] have chosen to transmit DAOs periodically with a pre-specified interval while they have been propagated in the Contiki RPL implementation [137] based on the timing of DIO messages. In Contiki RPL, a child node will usually send a DAO to its preferred parent in three occasions: 1) after receiving a DIO from its own parent; 2) when changing the preferred parent; and 3) in the detection of some specific errors. A critical issue here is that a DAO sent by a child node will lead to the transmission of several DAOs equivalent to the number of parents up to the DODAG root. A malicious node may exploit this case to drain the network resources by judiciously and repeatedly transmitting DAO messages to its parent node. One approach to perform this attack is by replaying a DAO sent by a legitimate node by an outsider malicious attacker [20]. RPL's security services deployed by layers underneath such as the cryptographic challenge-response handshake and link layer encryption can be used to mitigate this attack [20]. However, an insider attacker can easily bypass such security mechanisms triggering the need for more efficient solutions [20].

3.2.5.3 TAFFIC ATTACKS

The aim of traffic attacks is to capture and attract traffic inside an RPL network.

They are categorised into two groups: eavesdropping and misappropriation attacks. Eavesdropping attack are aiming to gather and examine network traffic. Misappropriation attacks involve stealing the identity of a legitimate node or overclaiming its performance.

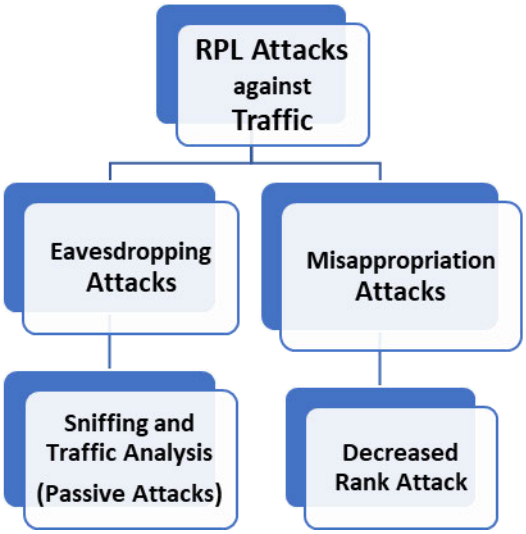


Figure 3-9. RPL Attacks against Traffic

3.2.5.3.1 SNIFFING AND TRFAFFIC ANALYSIS

The attacks aim to capture traffic from a shared communication media. The captured packets can contain important information such as the DODAG structure and data content that can be used to gain unauthorized access to the network. The information gained breaks the routing confidentiality of the network and can also be used to launch more severe attacks [138].

In [138] the authors have developed an Intrusion Detection System (IDS) to detect multiple attacks on RPL network. The proposed IDS DETector of rOutiNg Attacks in Rpl (DETONAR) identifies malicious behavior in the traffic using signature and anomaly-based rules. Netsim simulation was used to evaluate the performance of the proposed model against 14 well-known routing attacks. The simulation results show that the IDS successfully detects 8 out of 14 attacks with 100% accuracy and no RPL overhead.

3.2.5.3.2 DECREASED RANK ATTACK

In decreased rank attack, the attacking node falsely advertises a lower rank to its neighbours. The attack is fairly easy to implement by making a malicious node advertise crafted

DAG values, hence the node is advertising a lower rank and overclaiming its performances and proximity to the sink [139].

The authors in [139] have addressed the decreased rank attack in RPL using an artificial neural network model named multi-layer RPL (MLRPL). Their proposed model attack detection is composed of three modules that work together to perform the detection of the attacks. The performance of the proposed model was conducted using the IRAD dataset and evaluated in terms of accuracy, detection rate (DR), precision and F1 score. The test results show 97.14% accuracy, 97.03% precision, 0.36%, false positive rate, and 98% AUC-ROC.

Table 2-2 provides a summary of the recent works that have been carried out to tackle RPLs security challenges and enhance the overall network performances.

Table 3-1. The summary of the recent mitigation mechanism against attacks on RPL

Study	Year	Attack	Mitigation Mechanism
[118]	2020	Sinkhole	Proposed a method using Multi-sinks in IoT (SDMSI) to detect sinkhole and rank attack in RPL topology. The method utilises a link latency threshold in the root nodes that must not exceed specific value. If the link becomes silent for a period higher than the latency threshold the malicious node is then added to a blacklist.
[119]	2021	Sinkhole	Proposed a trust-based lightweight solution to detect the sinkhole attack. The RFTrust proposed model utilises Random Forest (RF) and Subjective Logic (SL) machine-learning algorithm to calculate the trust metrics for every node in the network.
[121]	2020	Wormhole and Rank	Proposed a framework that mitigate against rank and wormhole attacks using machine learning approach.
[122]	2022	Wormhole	Proposed recurrent neural network (RNN), deep learning model using confusion matrix to detect and classify the wormhole attack
[123]	2019	Sinkhole and Wormhole	A deep belief network (DBN) for detection of malicious nodes in the IoT network demonstrating the feasibility of using Deep Learning algorithms for effective anomaly detection in IoT environments
[124]	2022	Blackhole and Rank	A trust-based security framework (SRF-IoT) to detect and isolate malicious attackers with the help of an external intrusion detection system (IDS).
[125]	2020	Greyhole and Blackhole	UDP-based heartbeat detection method for greyhole and black-hole attacks. The idea is to send ICMPv6 echo requests from a dedicated node to the rest of the nodes in the network. If the sender of the ICMPv6 echo request does not receive a response, this may indicate that there is an ongoing blackhole
[126]	2021	Blackhole	An intrusion detection mechanism that uses a watchdog module (Local Detection) and a BR module (Global Detection and Eviction). To detect a malicious node the watchdog performs local detection by monitoring each node behavior by collecting the DAO, DIO, DIS, and DAO-ACK and data packets exchanged by the nodes.
[127]	2022	Blackhole	Their model consists of two steps to detect a malicious node a suspicion and verifications step. In the suspicion step, each child node starts a timer once the connection to a parent is established. The timer is restarted each time the child node receives packets from its parent node. If no packets have been received within the time threshold, the node is declared as a potential black hole node and a verification process is initiated

[129]	2021	DAO Inconsistency	An automata-based lightweight intrusion detection methodology called RAIDER with a context-aware decision-making model. The proposed RAIDER mechanism utilizes a finite automata model for detecting intrusions in the network.
[132]	2020	DIS Flooding	A Secure-RPL mitigation mechanism that restricts unnecessary trickle timer resets and DIO transmissions caused by DIS flooding attack.
[133]	2021	Routing Table Overhead	STIR, an RPL protocol modification that permit parent nodes only to store as many routing table entries as it has children or sub-DODAGs. This in return will prevent a malicious child node to add new routing table entries for an unknown or forged node.
[136]	2021	Version Number	A Version Number Attack Detection System (VeNADet) is proposed that puts certain conditions on the nodes to updates their Version Number. Any node that does not meet theses condition is considered as an attacker and is isolated from the network.
[138]	2021	Sniffing and Traffic Analysis	An Intrusion Detection System (IDS) to detect multiple attacks on RPL network. The proposed IDS DETector of rOutiNg Attacks in Rpl (DETONAR) identifies malicious behavior in the traffic using signature and anomaly-based rules. Netsim simulation was used to evaluate the performance of the proposed model
[139]	2021	Decreased Rank	An artificial neural network model named multi-layer RPL (MLRPL). Their proposed model attack detection is composed of three modules that work together to perform the detection of the attacks.

3.3 RPL's Implementations and Research Tools

Having discussed and analyzed the literature review related to the LLNs and RPL's concepts, limitations, it is important to shed light on the different implementations of RPL and tools that can be employed to develop and evaluate new contributions. Hence, several vendor and open-source RPL's tools and implementations are exist in the literature as follows:

3.3.1 Open-Source Tools

3.3.1.1 ContikiOS

Contiki [137] [140] is a lightweight and open-source operating system designed specifically for the low-power resource-constrained IoT devices [141]. Contiki features a highly optimized networking stack including several IoT standards such as 6LoWPAN and IPv6. It also features an implementation for the RPL standard fundamental mechanisms within a library called ContikiRPL. Both the OF0 and the MRHOF are implemented within the library with the OF0 uses the hop-count as its routing metric and the MRHOF uses the ETX. In addition, the latest version of ContikiRPL includes both the storing and the non-storing modes of RPL.

In 2017, the authors of Contiki started a new fork of the Contiki operating system named Contiki-NG [142], which features two different implementations of RPL: RPL-classic, and RPL-light. RPL-classic has a code size of 227 KB whereas RPL-light has a relatively smaller code footprint of 204 KB. The main difference between the two implementations is that RPL-light do not implement some features that seems unnecessary such as the storing mode and the existing of multiple instances (e.g., only one instance has been supported that uses the MRHOF and ETX metric). However, all Contiki-based implementations of RPL do not include any of its security features.

3.3.1.2 The Object Oriented Network Simulator OMNET++

OMNeT++ is a discrete event-oriented simulator that simulate many applications and areas such as modeling of the wired and wireless networks, protocols, queue management, multi-processors and other distributed hardware systems. It is not specialized to specific networks but provides an infrastructure and tools to create any event simulations. A fundamental part of framework is the architectural components for the simulation models. These components can be used diversely and for several models re-used. However, OMNET++ does not fulfill our study requirements completely in terms of studying the performance of routing protocol for low power and lossy networks (RPL) as there is no proper implementation of this protocol. This limitation encouraged us to extend OMNET++ simulation platform by adding other platforms with more functionalities namely MiXiM [143], in particular in relation to the simulation of IEEE 802.15.4 networks. MiXiM provides additional components such as detailed protocol layers, signal propagation and power consumption. In addition to this MiXiM supports different mobility models necessary to test the behavior of the sink node in WSNs in a mobility situation [144].

3.4 SUMMARY

This chapter has outlined the main concepts related to RPL operations, objective functions and routing metrics, security concepts and elaborated on the key limitations of the protocol.

Having overviewed existing RPL's limitations and identified the gaps, the chapter concludes that novel solutions need to be developed to address the identified gaps.

The first identified gap is that RPL was mainly developed for static networks without mobility, however, the increased demand for mobility in our everyday life raises the question how RPL would perform in networks with a mobile sink. In response, an evaluation of RPL in mobile and fixed sink environments under different scenarios focusing on Latency, Packet Delivery Ratio (PDR) and Energy Consumption metrics has been carried out in chapter 4.

The second identified gap concern the problem of the under-specification of metrics composition of the RPL standard. In response, an evaluation of RPL routing mechanisms in terms of Packet Delivery Ratio (PDR), latency and power consumption under constrained conditions by using different topology types, different number of nodes and different transmission ranges has been conducted in chapter 4.

The third identified gap is also concern the problem of the under-specification of metrics composition of the RPL standard. In response, an evaluation of the RPL standard under various routing metrics used for calculating the optimal routes in Multi Segment Linear Pipeline Monitoring IoT networks including ETX, Hop count and RSSI has been conducted in chapter 4.

The fourth identified gap is that RPL suffers from scalability problem in its mechanism for constructing the reverse routes from the network's sink to the joined nodes (Downward routes). In addition, the scalability problem is magnified by the fact that the RPL specification does not allow for a node to look for another DAO parent when its current preferred parent runs out of memory. Even worse, RPL does not specify a mechanism to detect such a case.

Another serious problem is RPL's under-specification of DAOs timing which may result in conflict and inefficient implementations leading to a poor performance. In response, an enhanced version of RPL called Enhanced-RPL has been introduced as explained in Chapter 4.

The fifth gap being identified is that RPL is also restricted by the fact that Gas and Oil network is envisaged to operate in a linearly distributed fashion along the pipeline and limited to a single path to transmit the data. In response, an RPL based optimal sensor placement scheme has been presented in Chapter 4.

The sixth identified gap concerns the lack of the standard for a security mechanism that addresses the Destination Advertisement Object (DAO) attack. In response, a new mitigation technique has been proposed as illustrated in chapter 4.

CHAPTER FOUR: THE PUBLICATIONS

4.1 INTRODUCTION

This chapter outlines and critically evaluates the author publications for a PhD by published works. As summarised in Table 4-1 on the next page, the selected papers demonstrate contributions in relation to the Routing protocol for Low-power and Lossy Networks (RPL) that is envisaged to be used for Monitoring and Surveillance in Oil and Gas networks. In this thesis, I strive to push the boundaries of routing in LLNs beyond the state-of-the-art standardized solutions with the main aim is to further enable widespread deployments of scalable, reliable, energy-efficient and secure LLNs in the context of internet of things. To this end, and in addition to the literature review, the key contributions is to address seven research questions, which can be summarized as follows:

Table 4-1. The Contributions of the published papers

Area	Detailed contributions
I. What is the state of art of IoT and LLNs concepts?	An extensive state-of-the-art survey on related and ongoing projects found in the literature under the umbrella of controlling and monitoring systems.
II. How and to which extend can routing in LLNs be scalable and reliable under various patterns whilst taking into account the limitations of such networks?	Development and implementation of a new algorithm that optimizes the Downward Routing Mechanism in RPL Storing Mode. The new proposed algorithm was developed with the aim to tackle the issue associated with the scalability of downward routing presented in RPL.
III. To which extend can RPL to secured against the DAO (Destination Advertisement Object) attack?	Development and implementation of a new algorithm that mitigates against the DAO (Destination Advertisement Object) attack on RPL.
IV. Shall RPL be within stationary WSNs there must also be regard paid to mobile implementations?	Examination of the challenges inherent in utilising a mobile sink node by studying the behaviour of RPL in fixed and mobile sink environments.

Area	Detailed contributions
V. Is the protocol able to maintain motes within a DODAG under 'strained' the transmission ranges of motes?	An extensive performance evaluation for RPL routing protocol in LLNs under constrained conditions considering all existing objective functions and metric with regard to energy efficiency, PDR and latency. This allowed to evaluate the suitability of RPL protocol for oil and gas networks in order to discover the limitations of RPL protocol in oil and gas networks
VI. How the Placement of the nodes LSN based on RPL as a routing protocol would affect the performance metrics such as energy efficiency, network lifetime, coverage and connectivity?	An extensive investigation of the linear placement of sensor nodes along oil and gas pipeline with respect to distance and its impact on energy consumption, packet delivery ratio, end to end delay and throughput.
VII. What is the behaviors and performances of the protocol routing metric for calculating the cost of downstream routing for the RPL protocol in a multi segment pipeline?	Identified problems at the level of routing in WSN, and a study of specific metrics used to calculate the forwarding cost between nodes in a Multi Segment Linear Pipeline Monitoring WSNs.

A self-critical summary for each publication, in terms of strengths and weaknesses, is presented in Table 4-2, which provides a conceptual framework to frame analysis and discussion including the research theoretical point-of-departure, Empirical data collection and Contribution to knowledge in the field.

All publications are co-authored publications with research colleagues. In five publications, I have acted as the principal researcher responsible for the research methodology, conceptualisation, simulation tools, investigation, resources, data curation, writing original draft preparation and presentation. Where I am the second author, I have contributed with formal analysis, validation and writing original draft preparation. The co-authors are willing to be contacted to address any concerns over co-authorship. The co-authors have written and signed a letter related to this, a copy of which is presented in Appendices.

Table 4-2. The Publications, including Theoretical point-of-departure, Empirical data collection and Contribution to knowledge

Publication	Theoretical point-of-departure	Empirical data collection	Contribution to knowledge
Performance Evaluation of the RPL Protocol in Fixed and Mobile Sink Low-Power and Lossy-Networks.	The paper is based on a theoretical underpinning by the RPL protocol.	Empirical study is the focus of the paper. The evaluation is in a large-scaled simulation environment and covers different network metrics such as latency, packet delivery ratio and energy consumption.	The findings from the evaluation have its unique value in guiding networks designers and operators to achieve better performance (green networks) in the networks design and operations, largely in the sense of energy consumption.
Performance evaluation of RPL metrics in environments with strained transmission ranges.	The focus of the paper is not direct theoretical breakthrough. The findings from the evaluation have non-trivial value in guiding researchers and designers to generate novel theoretical concepts or system protocols or models for better networks, which will bring up new types of mobile networks.	The evaluation engages fours tests in appraising the network metrics from diverse aspects. The tests are developed systematically, and the scale, the data collected, and the findings from the analysis of the test results have non-trivial impact on the future networks design.	The findings from the evaluation represent a guideline with non-trivial value for researchers and designers to generate novel theoretical concepts or system protocols or models for better networks.
A new enhanced RPL based routing for Internet of Things.	The work innovatively extends the current theory of IPv6 routing protocol with two underpinning advances: enhanced storing mode, and downward routes maintenance.	The impact of the two proposed theoretical advances have been verified and evaluated with a series of simulation-based tests. The results and analysis are convincing in confirming the value of the advances and meanwhile suggest for further refinement and improvement.	The proposed enhanced storing mode has been fully defined and developed. The process of the downward routes maintenance is developed.
Performance Investigation of RPL Routing in Pipeline Monitoring WSNs.	The performance investigation is based on a theoretical underpinning by the RPL protocol.	The paper presents another solid evaluation work on the strength and drawbacks of RPL, covering the behaviors and performances of three routing metric for calculating the cost of downstream routing for the RPL protocol in a multi segment pipeline.	The findings from the evaluation provide the guidance with non-trivial value for researchers and designers to create novel theoretical concepts or system protocols or models for better networks.

Mitigation Mechanisms Against the DAO Attack on the Routing Protocol for Low Power and Lossy Networks (RPL).	The paper contributes to the current state of art with a theoretical advance, i.e. the mitigating security mechanisms against DAO attacks.	The paper evaluates the effect of the DAO attack in the context of an RPL IoT network. In particular, it identified the particular performance metrics and network resources that are most affected. The simulation results have shown how the attack can damage the network performance by significantly increasing the DAO overhead and power consumption. It also demonstrated that the DAO attack affects the reliability of the downward traffic under specific conditions.	Two effective mitigating mechanisms are developed to address the DAO insider attack in RPL: SecRPL1, which restricts the number of forwarded DAOs per child; and SecRPL2, which restricts the entire number of forwarded DAOs by a specific node.
An RPL based Optimal Sensors placement in Pipeline Monitoring WSNs	The RPL protocol acts as the theoretical underpinning of the work presented in this paper.	With simulations, the paper analyses and evaluates the impact of node placement in a linear sensor network (LSN) by placing the nodes uniformly a long a pipeline. The evaluation is in-depth, and the conclusions are convincing.	The findings from the evaluation provide the guidance with non-trivial value for researchers and designers to create novel theoretical concepts or system protocols or models for better sensor networks.
Wireless Sensor Networks (WSN) in Oil and Gas Industry: Applications, Requirements and Existing Solutions.	The protocol and routing mechanisms of WSN are the theoretical foundation of the study presented by this paper.	The findings from the survey will benefit the design and development of effective WSN sensor networks with unique guidelines and information.	The paper contributes to the current knowledge at the application level substantially. The comparison of existing solutions is comprehensive and informative for the design and deployment of WSN-based sensor systems, particular valuable for the QoS perspectives such resilience, latency and energy-efficiency.

4.2 PERFORMANCE EVALUATION OF RPL PROTOCOL IN FIXED AND MOBILE SINK LOW-POWER AND LOSSY-NETWORKS

4.2.1 BACKGROUNAD

Low-Power and Lossy-Network (LLN) represents a class of networks comprising tiny sensors nodes that have limited resources and interconnected by wired or wireless lossy links [103]. Such nodes have the capability of sensing the environment then sending the collected data hop by hop to the central node (i.e., sink) using low power and short range transceivers. Hence, the network lifetime strongly depends on the routing protocol, which is responsible for finding the best path to the sink considering different routing metrics. The consequences of incorrect routing decisions mean more retransmissions will occur across the network which may results in poor performance related to the power consumption or reliability of the networks. One of the promising routing protocols is the one developed by the IETF standardization body, namely, RPL (the Routing Protocol for Low-Power and Lossy-Networks). This protocol was mainly developed for static networks without mobility, however, the increased demand for mobility in our everyday life **raises the question how RPL would perform in networks with a mobile sink**. Hence, the aim of this paper is to evaluate RPL in mobile and fixed sink environments under different scenarios focusing on Latency, Packet Delivery Ratio (PDR) and Energy Consumption metrics. The experimental results show that RPL does not perform well under mobile-sink environments exposing serious issues with sink mobility, such as certain nodes had an excessively high APC and several nodes were isolated which requires the research community to enhance the protocol further.

4.2.2 CRITICAL REVIEW OF RELATED WORK

There have been several studies conducted to evaluate the performance of RPL using different simulation frameworks, different scenarios and for different performance metrics. In [6] the authors evaluated RPL with respect to several metrics of interest such as path quality,

end-to-end delay, constraints on nodes and the ability to cope with unstable situations. A scenario of an outdoor network topology with 45 nodes has been used with no mobile scenarios has been considered, an issue that we aim to investigate in our study.

The performance of RPL over IEEE 802.15.4 and the impact of the MAC on the network layer was investigated also in [145] in terms of delay and latency, however, mobility has not been considered in this study.

In [26], the author explored the performance of RPL-enabled broadcast with respect to Classic Flooding, MultiPoint Relay Flooding (MPRF), Parent Flooding (PF MPRF) and Preferred Parent MPR Flooding (PPMPRF) using the Ns2 network simulator and again with no consideration of mobility. The same goes for the study in [146] which presents a critical analysis of RPL and evaluated the performance of upward traffic using Ns2 simulations. In [147] the author presents a simulation-based design and implementation of RPL inside the uIPv6 stack. The research paper focuses on the power efficiency and the implementation complexity of ContikiRPL by constructing a WSN with 41-node and a small-scale 13-node Tmote Sky to simulate in an office environment. The results reported that IPv6 routing with ContikiRPL is both lightweight and power-efficient, providing a lifetime of several of years for both leaf nodes and routing nodes using the Contiki operating system [137].

The authors in [148] have also evaluated the performance of the RPL protocol with real power line communication networks (PLC) using COOJA under two case studies, mobile sink nodes and PLC nodes. Energy consumption was analysed with respect to network lifetime, residual energy and packet overhead. The simulation results reported that RPL provides interesting capabilities for mobility management to improve WSN lifetime by managing the sink mobility and offers logical routing in LLN heterogeneous platforms with wireless and PLC WSN. Although there are several studies and implementations that focused on the evaluation of the performance of RPL, there is still a lack of a comprehensive comparative

study of the behaviour of the RPL protocol in fixed and mobile sink environments where different network metrics such as latency, packet delivery ratio (PDR) and energy consumption are considered which has been addressed in this chapter.

4.2.3 PERFORMANCE ANALYSIS AND EVALUATION

In this subsection, we describe the simulation environment, the simulation parameters used to mimic different real-life scenarios to evaluate RPL in fixed and mobile sink environment focusing on Latency, PDR and Energy Consumption. The performance is carried out through extensive simulation experiments under different scenarios and operation conditions.

4.2.4 PERFORMANCE ANALYSIS

4.2.4.1 Simulation Environment and Parameters

The major component of the simulation environment is Instant Contiki 2.7. It is important not to mix up with Contiki OS, which is an operating system for IoT nodes. Instant Contiki is a freeware Ubuntu Linux-based virtual machine which provides a framework for developers and includes all tools and compilers necessary for Contiki software and hardware developments [148].

For our simulation, we have deployed the Unit Disk Graph Model (UDGM) to simulate lossy networks. Taking two range parameters, one for transmission (TX range = 70 *m*) and one for interference (INT range = 90 *m*) with other radios as depicted in **Figure 4-1**. The larger green inner circle indicates the transmission range of node 1 whereas the grey outer circle shows the interference with other radios. The percentages show the reception ratio of transmission between node 1 and other nodes.

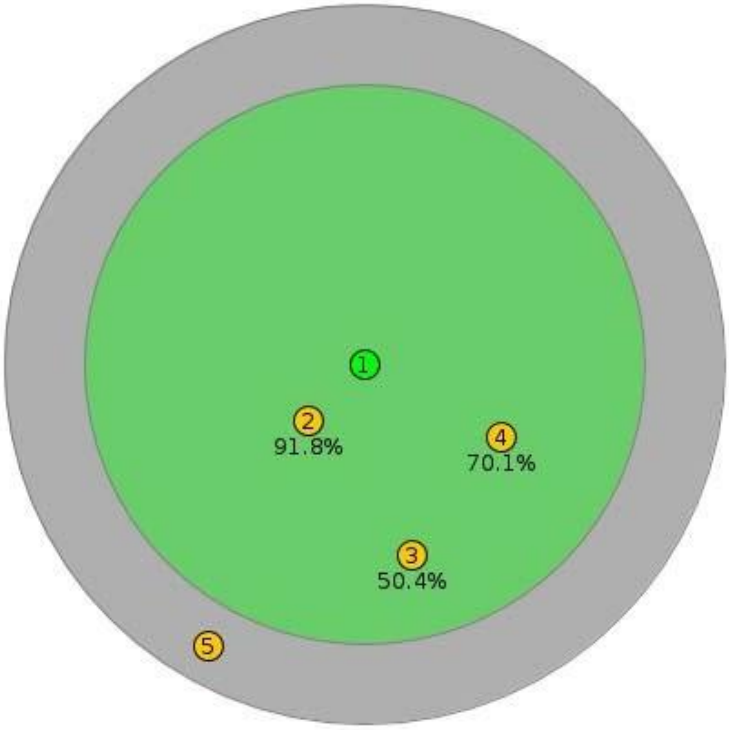


Figure 4-1. UDMG Model in COOJA

The simulation time is set to 10 minutes and 15 minutes, with 10 tests have been carried out. Each scenario consists of a sink node which collects data from 24 randomly distributed sender nodes with each node sends on UDP packet each minute. The nodes are evenly distributed to preserve the same node density for each scenario because that affects routing capabilities in mesh networks. A script runs alongside the simulation to calculate Latency and PDR. Table 4-3 summarizes the simulation setups in Cooja.

Table 4-3 Simulation Parameters Setup

Parameter Name	**Values**
Wireless Channel Mode	Unit Disk Graph Medium (UDGM)
Mote Type	Tmote Sky
Mac Layer	non-slotted CSMA + ContikiMAC
Transport Protocol	UDP
Simulation time	10 min, 15 min
Radio Channel Check Rate	8 H z
Radio Interface	CC2420 2.4 *GH z* (IEEE 802.15.4)
INT range	90 m
TX Range	70 m
Node	25
Mobility Type	Random Way Point
Mobile Sink Speed	$4 - 6$ *km/h*

4.2.4.2 Simulation Scenarios

In order to evaluate how RPL can handle mobile sinks, 5 different scenarios have been created as illustrated in **Figure 4-2**. Two scenarios consider fixed sinks and three others consider mobile sinks. In each mobility scenario, we consider different paths for the sink node. In the first one the sink passes near a sensor field. In the second case, the path goes diagonally across the sensor field and in the third one, the sink circulates around a sensor field. To control the movement of nodes for each scenario we have used a mobility script (DAT file) that describes the movement pattern. Literally it is a pre-constructed table which has node ID, time in seconds, X and Y coordinate fields. The speed of a mobile sink is fixed to (6 km/h) for each scenario which is an average speed of an adult. Table 4-4 shows the content of a DAT file.

Table 4-4. Mobility Parameters

Node ID	Time (S)	X	Y
0	0	389.98	17.09
1	1	389.93	19.19
2	2	389.84	21.28
3	3	389.71	23.37
4	4	389.54	25.46
5	5	389.34	27.54

The calculation of coordinates for linear movements achieved by calculating the distance between the start and end points, then calculating time with a formula where time equals to distance divided by velocity. Velocity is 6 km/h which is an average speed of an adult. We have applied the same mechanism for calculating the circular motion for Scenario 5 by.

1) Calculating the circumference with a radius of 120 m that is 753.98 m.

2) Calculating the time in seconds which is necessary to take this distance with a velocity of 6 km/h. That is 452 seconds. The coordinates given in every second, therefore the time can be used as 452 steps.
3) Calculating the angle for each step and converted them into radian.

   360 / 452 = 0.796 degree for each step. (0.01390 rad).
4) Using the following formulas to calculate X and Y

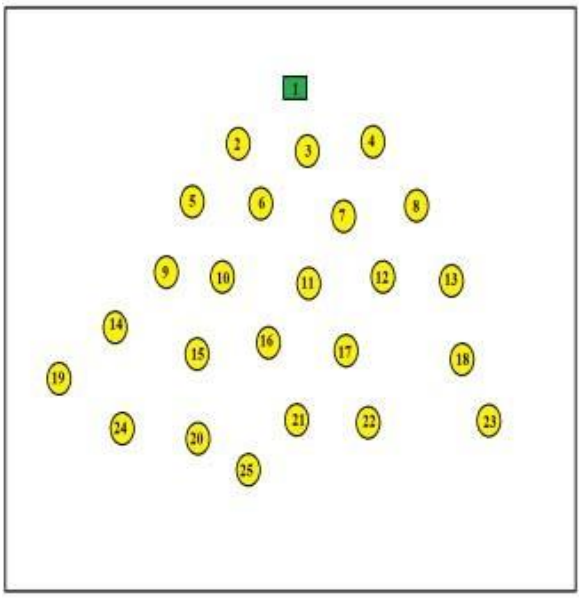
   Coordinates for each step:

$$x = c \cdot x + r \cdot \cos(a) \quad (2)$$

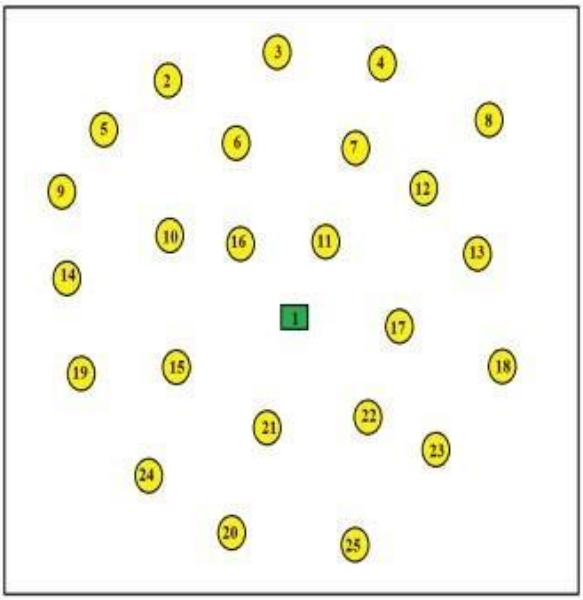
$$y = c \cdot y + r \cdot \sin(a) \quad (3)$$

   where c · x is (270 m) the X and cy is (15 m) the Y coordinate value of the circle centre point and a is the angle in radian.

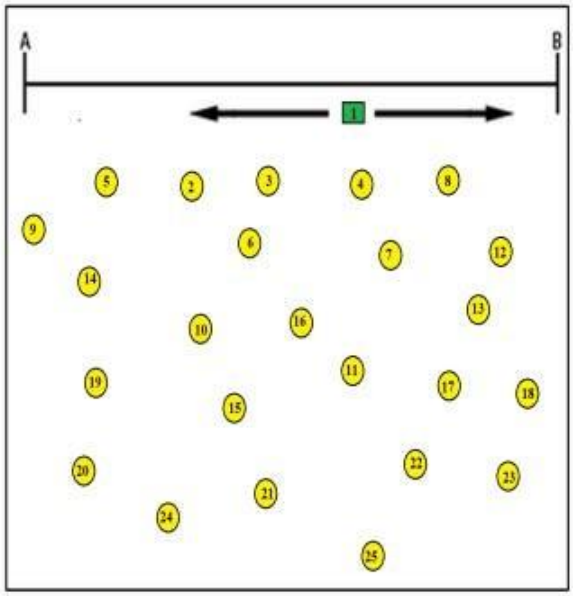
The figures below represent the 5 simulation scenarios created to evaluate the performance of RPL.



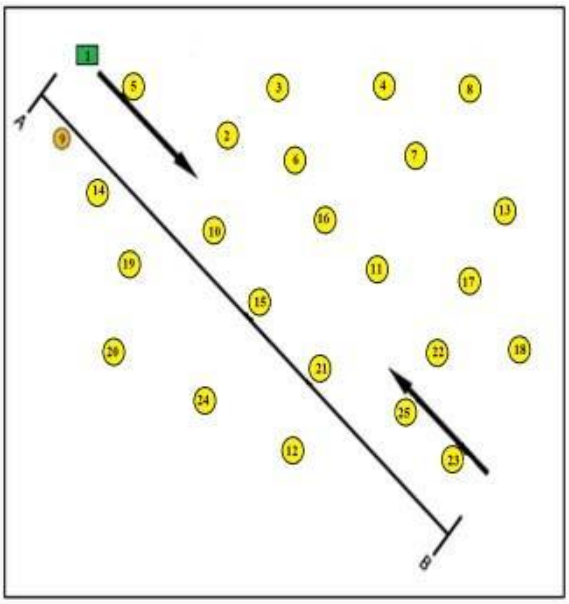
(a) Tree Topology



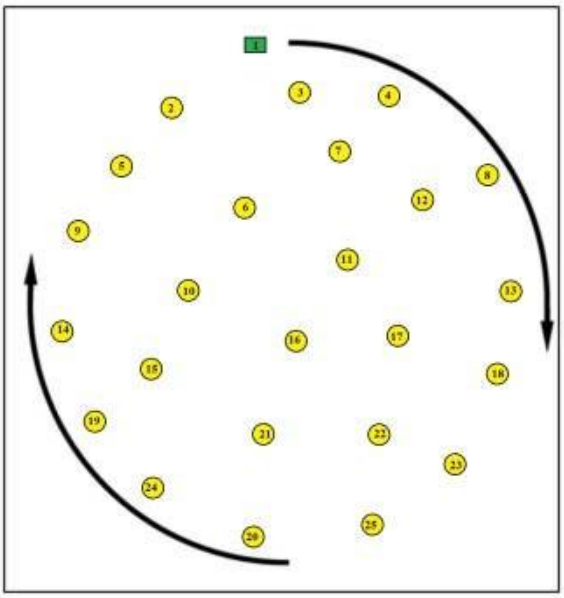
(b) Fixed Sounded Sink



(c) Sink moves in front



(d) Sink moves across



e) Sink moves around

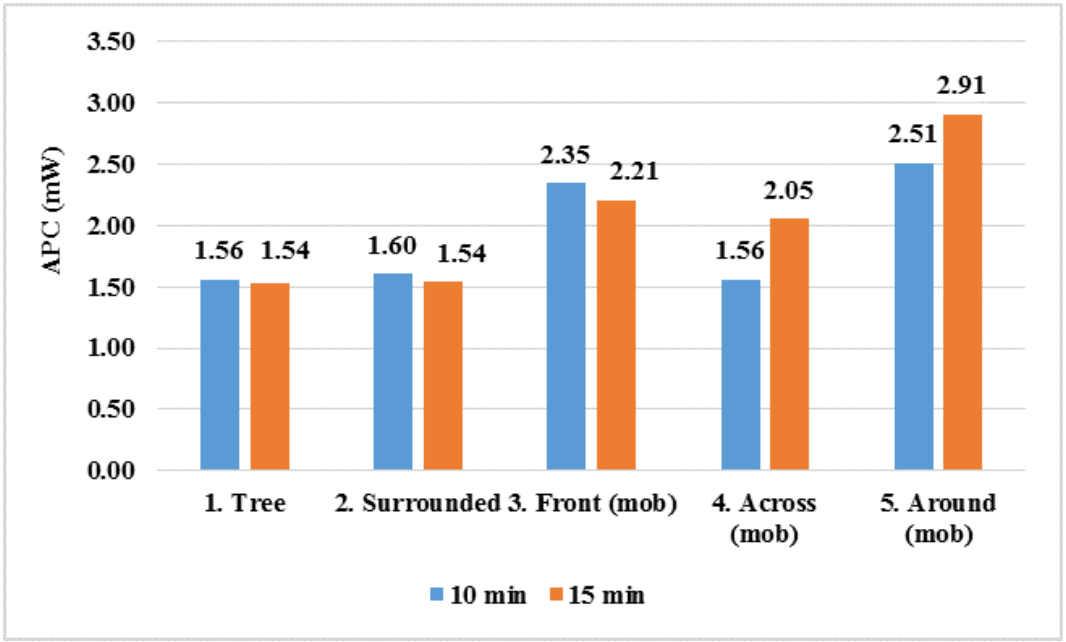
Figure 4-2. Simulation scenarios

4.2.4.3 Simulation Experiments

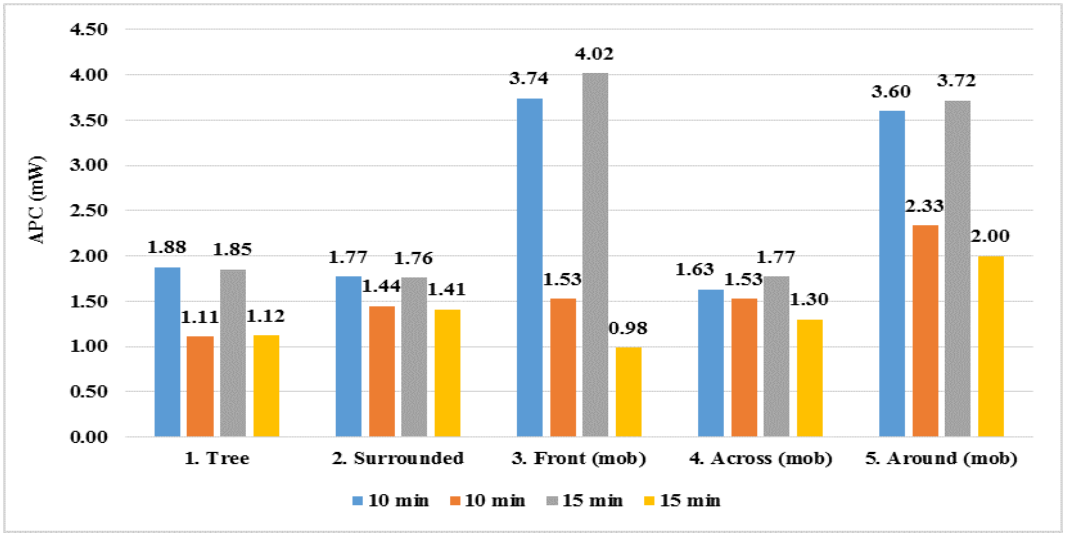
This subsection analyses the outcomes of the experiments and compares the results of the different scenarios in both time frames (10 minutes and 15 minutes) with respect to power consumption, latency and packet delivery ratio.

4.2.4.4 Power Consumption

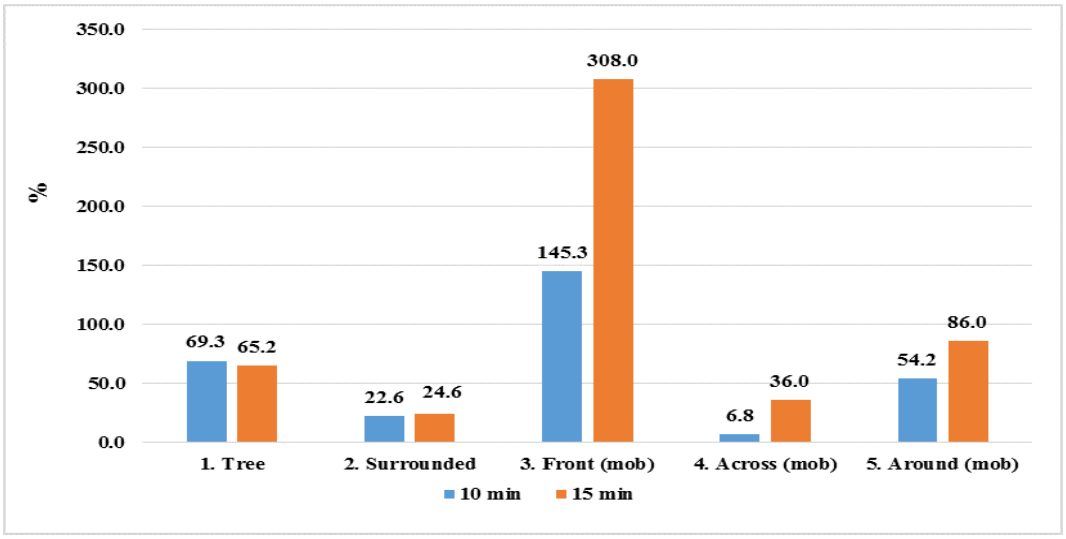
Figure 4-3 presents The APC (Average Power Consumption) for all scenarios. According to **Figure 4-3a,** mobile sink scenarios appear to consume more power compared to stationary ones. The consumption for fixed sink scenarios is constant in both time frames reached a maximum of 1.6 mW. The results for mobile sink scenarios varying more and the majority of the values is over 2 mW. Scenario 3 topped at 2.35 mW for 10 minutes time frame and slightly lower 2.21 mW on 15-minute time frame. Both values are therefore very close to each other. Scenario 4 where the sink moves across a sensor field performed the best between all the mobile scenarios and measured similar value of 1.56 mW as recorded in a fixed sink environment on 10-minute time frame. Although 2.05 mW on 15-minute time frame is nearly 25% more than the 10-minute results. In the fifth scenario where the sink moves around a sensor field it consumes the highest power with 2.51 mW on 10 minutes and 2.91 mW on the 15-minute time frame. This is nearly the double of energy required by fixed sink scenarios.



(a) APC for all scenarios



(b) 1-hop and further nodes APC



(c) APC difference between 1-hop and further nodes in %

Figure 4-3. Average Power Consumption

Figure 4-3b provides a detailed picture behind the APC results and shows the 1-hop and further nodes APC for each scenario in both time frames. We can observe that the 1-hop nodes have consumed more power than the further nodes.

Figure 4-3c displays the difference between 1-hop and further nodes in percentage from which we can notice that for the two fixed sink scenarios the overall consumption is nearly the

same. However, the distribution is more balanced in scenario 2 because the difference between 1-hop and further nodes is only 22 − 24% compared to 69 − 65% in Scenario 1. The gap is smaller because 1 hop values decreased slightly and the further node values remarkably increased. From the mobile sink scenarios, a higher gap between 1-hop and further nodes for Scenario 3 and Scenario 5 is observed. Scenario 3 results are excessive, 1-hop nodes consume almost 1.5 times more on 10 minutes and 3 times more on then15 minute time frame. Scenario 5 achieved a difference of 54% in10 minutes and 86% on the 15-minute time frame which about 20% higher than Scenario 1. Scenario 4 performed the best within a mobile sink environment with a 6.8% difference in 10 minutes and 36% difference on 15-minute time frame. Literally much better than Scenario 1 and slightly worse than Scenario 2 on the higher time frame. Also, the APC of Scenario 4 makes it competitive compared to the fixed sink environments.

Focusing on the APC of 1-hop and further nodes the experiments clearly show that scenarios where the number of 1-hop nodes is low such as Scenario 1 and 3, the difference of APC between these two groups is higher because only a few nodes will interact directly with the sink and forward packets from the rest of the network. Also, scenarios with more 1-hop nodes shows a more balanced picture e.g., Scenario 1, 4 and 5.

In the APC calculation process, it is discovered that one or two nodes had excessively high-power consumption in each mobile sink scenario. This excessively high value means 2-4 times more than the network average. The following table displays these nodes in both time frames.

Focusing on the APC of 1-hop and further nodes the experiments clearly show that scenarios where the number of 1-hop nodes are low such as Scenario 1 and 3, the difference of APC between these two groups is higher because only a few nodes interacting directly with the

sink and forwarding packets from the rest of the network. Also, scenarios with more 1-hop nodes showing a more balanced picture e.g., Scenario 2, 4 and 5.

In the APC calculation process it is discovered that one or two nodes had excessively high-power consumption in each mobile sink scenario. This excessively high value means 2-4 times more than the network average. Table 4-5 displays these nodes in both time frames.

Table 4-5. Nodes with excessively high PC

Scenario	**Node ID**	**APC in 10 min in (mW)**	**APC in 15 min in (mW)**
3. Front (mob)	5	5.39	5.39
4. Across (mob)	5	-	3.28
	9	-	5.05
5.Around(mob)	1	12.36	9.19

The common in these nodes are that when the simulation starts the sink interacts first with them. This area is the starting point of the sink path, and these nodes get the highest rank when the DODAG is built for the first time. When the sink moves out of the transmission range the DODAG repairing process does not react quickly to implement changes in the routing table and the other nodes of the network still assuming that these nodes are 1-hop away from the sink and keep sending the packets to them. Overall, these nodes waste a large amount of energy to retransmit the packets and find the correct path to the sink. Other 1 hop nodes having similar APC values like in fixed scenarios. A quicker repair mechanism of the DODAG could overcome on this issue.

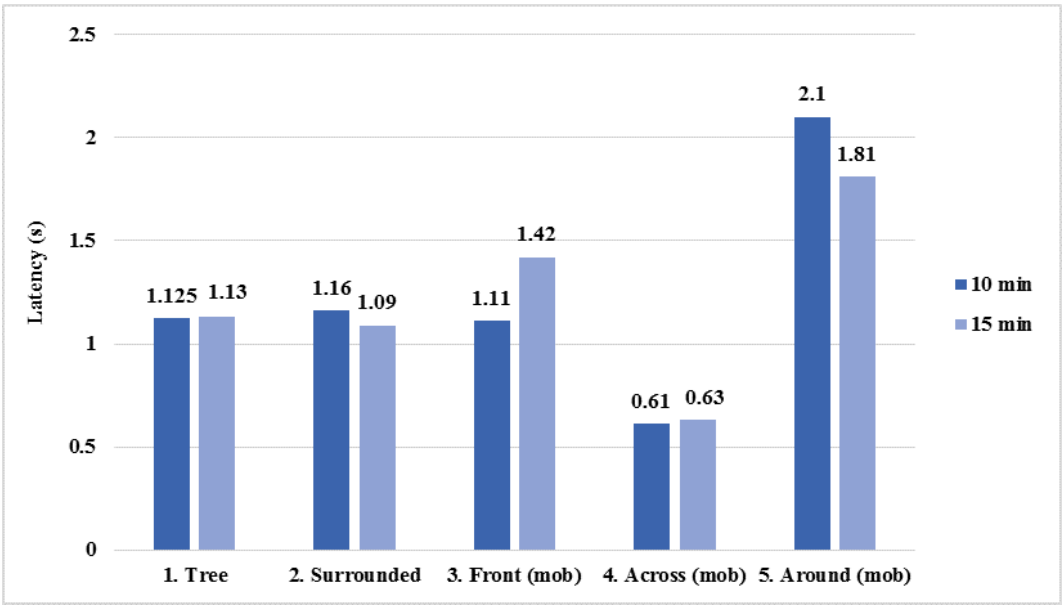
During the experiments, it is observed that some nodes were not managed to connect to the DODAG, and this was confirmed by the Cooja Collect View plugin. The plugin was not able to display results from several isolated nodes in each mobile sink scenario because the sensor data was dropped on the way to the sink. Which means these nodes and some of the

intermediate nodes had outdated routing information about the position of the sink. The isolated nodes were typically at the edge of the topology.

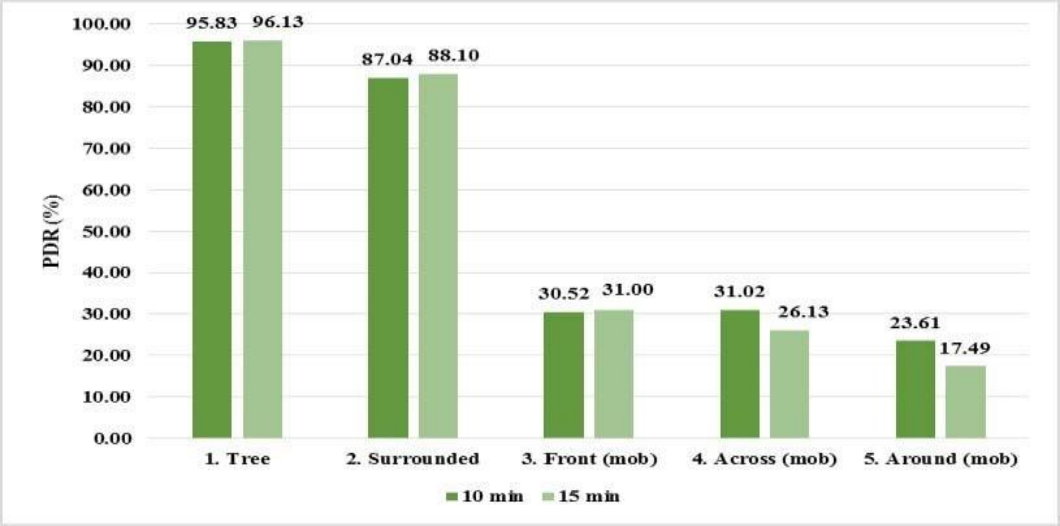
4.2.4.5 Latency and PDR

This subsection provides the results obtained from the evaluated latency and packet delivery ratio for all 5 scenarios. **Figure 4-4** presents the Latency and the PDR for all scenarios in both time frames.

From **Figure 4-4a,** it can be observed that the Fixed sink scenarios outperformed mobile sink scenarios in terms of reliability. Both scenarios (1 and 2) achieved very similar Latency, which is just over 1 second in both time frames and the PDR values around 96% and 88% which are excessively higher than mobile sink networks. These Latency and PDR values are acceptable for LLN networks



(a) Latency of different scenarios



(b) PDR of different scenarios

Figure 4-4. Latency and Packet Delivery Ratio

The Latency results in mobile sink scenarios are varying between 0.61 seconds and 2.1 seconds. Scenario 3 performed the best with 0.61 seconds on the 10 minutes and 0.63 seconds on 15 minutes time frame. These results are surprisingly better than fixed sink results. Scenario 3 got very similar values than the fixed sink scenarios with 1.11 seconds on 10 and 1.42 seconds on the 15-minute time frame. The worst performed scenario was number 5 with 2.1 seconds on the10 minutes and 1.81 seconds on the 15-minute time frame. These are roughly 3 times higher values compared to the best performed Scenario 4.

The PDR values shown in **Figure 4-4b** for mobile sink LLNs are surprisingly low compared to the fixed sink. Scenario 3 and 4 achieved around 30% and Scenario 5 have lower values with 23.6% in 10 minutes and 17.5% on the 15-minute time frame.

According to the evaluation results it can be observed that RPL performs much better in the fixed sink environment because achieved 3 times better PDR results with a very competitive Latency and the best APC. The difference between fixed sink LLNs is less. As previously stated in the Literature Review RPL is a hierarchical protocol where the ranks are very important and the protocol building a tree-like topology also called DODAG. That is the reason why is so

competitive in Scenario 1 in terms of reliability. However, in case of a real-life scenario where changing the battery of sensor nodes is feasible Scenario 2 would be slightly better because drains the power source in a more equable manner between 1-hop and further nodes. This could be explained with Scenario 2 having more 1-hop nodes, which distributes the traffic much better from the edges of the DODAG and the deepness of the topology is lower. Furthermore, another possible solution to decrease the 65% APC difference is to create a diamond-like topology with 2 sinks, one at the top and another at the bottom. The sinks would operate alternately and swap their operation after a period of time. So, when the other sink takes over, the 1-hop nodes becoming edge nodes and able to conserve power, besides the edge nodes becoming 1-hop nodes. The drawback is every time when the other sink takes over the DODAG needs to be rebuilt again and that increases the number of control messages (DIO), nevertheless this solution would benefit from the reliability of Scenario 1 and the equable power distribution of Scenario 2.

The low performance of RPL in mobile sink scenarios was unexpected and according to the results, the protocol was not able to cope with topology changes in a reasonable manner. Furthermore, mobile sink LLNs consumed remarkably more power in two scenarios and also the difference between 1-hop and further node APC were significant in these two scenarios. Scenario 4 performed the best amongst mobile sink LLNs but the low ratio of packet delivery still not sufficient in real life conditions.

4.2.5 THEORETICAL POINT-OF-DEPARTURE

The paper presents theoretical perspectives around the topic of Internet of Things (IoT) more specifically the Routing Protocol for Low-power and Lossy Networks. The theoretical point of departure was to look at how RPL behaves under such mobility conditions and report any observed issues.

4.2.6 EMPIRICAL DATA COLLECTION METHOD

The evaluation is in a large-scaled simulation environment and covers different network metrics such as latency, packet delivery ratio and energy consumption. The paper has a solid research methodology with an empirical data collection method utilizing simulation experiments using one of the well-known simulators for IoT networks, namely, cooja

4.2.7 CONTRIBUTION TO THE KNOWLEDGE

In this paper, an in-depth performance evaluation of the RPL protocol was conducted to better understand its behaviour under different mobility scenarios. This evaluation demonstrated that there are major performance differences not only between fixed and mobile sink environments but also between mobility patterns. Fixed sink LLNs performed better in terms of APC, latency and PDR, which confirms that RPL is suitable for fixed environments. The evaluation exposed also some serious issues with sink mobility and revealed that some sensor nodes had an excessively high APC while other were isolated. These issues will be further investigated in future by taking into consideration different mobility models, different network density probabilities and higher number of sinks. The findings from the evaluation have its unique value in guiding networks designers and operators to achieve better performance (green networks) in the networks design and operations, largely in the sense of energy consumption.

As of the 16th of September 2021, the article has been read a total of 844 times and citied 14 times.

4.3 Performance Evaluation of RPL Metrics in Environments with 'Strained' Transmission Ranges

4.3.1 Background

RPL is a flexible and adaptive protocol, specifically designed with the propensity for packet losses in WSNs in mind. These packet losses are expected in WSNs with the potential for environmental factors coming into play, which could cause interference and therefore extreme link-instability, resulting in high levels of packet loss. In this case different principles must apply. RPL cannot overreact to packet loss by immediately recalculating routes, due to the limited power and data transfer rates available [106].

Recent studies aimed at evaluating the performance of RPL, with regard to the different OFs and metrics therein, have tended to focus on performance based on Packet Delivery Ratio (PDR), energy consumption and latency. Simulations are generally designed to organise the nodes within a WSN in the most effective way with regard to transmission ranges. This study, however, aims to take a completely different approach, in that the network topologies utilised within the simulations performed as part of this study have been designed in that the nodes are located at distances aimed to'strain' their transmission ranges. The performance of the network in relation to RPL metrics is based on the ability to maintain nodes as part of the network after a set period of time. This is seen as of great importance given the 'real- world' implementations of WSNs and the possibility of inhospitable environments.

4.3.2 Critical Review of Related Work

There have been a variety of studies into the performance of RPL, as well as different ways of implementing the protocol. The study in simulated RPL on the Contiki OS [140], by exploration of the area each node inhabits to manage their neighbour tables. Also employed is link estimation [149]. This results in considerably better delivery rates and highlights the need for novel approaches to routing in the IoT in general. With regard to energy-saving, this is the

one area affected by all others. Poor data delivery, as previously commented upon, will result in heavy energy consumption. The non-avoidance of loops is another area of concern as this can also lead directly to high energy consumption when not implemented correctly. The study in [149] uses simulation to test the effects of combining primary and composite routing metrics and proposes a set of complex formulae to implement this. The result is a successful convergence to optimal loop-free paths within an LLN using the RPL protocol.

A fairly early thesis detailing an implementation of RPL in a WSN and examining the Hop Count Object and Node Energy Object metrics [150], utilised the OMNeT++ simulation model [151]. OMNeT++ is not a simulator in the traditional sense but more a modular platform on which simulations can be built. This is based around scripts written in C++, is extremely flexible and particularly suitable for simulating mobile protocols such as Destination-sequenced Distance Vector (DSDV) [152] [153][154] [155].

The study in [156] proposed improvements to RPL by implementing multipath routing in the form of three different schemes. Those being Energy Load Balancing (ELB), Fast Local Repair (FLR) and a combination of both (ELB-FLR). What is explored in this paper is the consideration of a node of the same rank in the event of a parent node going down, or a "sibling" in the case of FLR. This can subsequently result in more efficient redundancy as it opens up a far greater choice of alternative routes than would previously have been available. In the case of ELB residual energy of nodes is used in calculating their rank as well as in routing. This means that the energy level is then an integral part of the decision making process when it comes to assigning parents, as higher residual energy will contribute to a lower rank. The ELB-FLR approach seeks to combine these two methods to result in a proposed new protocol, with high levels of redundancy and the always important issue of energy levels also accounted for [157].

One of the earlier studies to utilise ContikiRPL in the Cooja simulator was “Simulation and Performance Evaluation of DAG Construction with RPL” [158]. This study differed from others at the time in that it was directed more at the actual construction of the network rather than individual variables. In this regard the ability to simulate large networks was of high importance. An evaluation of ContikiRPL found that general implementation was less complex. Also, it was proven that a battery lifetime of several years was possible, as well as a high packet delivery ratio. By the standard of more recent studies the results of this particular study are not hugely revealing, in that they prove that power consumption of a DODAG increases in relation to the number of nodes and that a node consumes more energy depending on its position within the DODAG, regarding the number of neighbours it has. Thus, the more routing the node must perform the more energy it consumes. It was also shown how the Average Hop Distance, Convergence Time and the size of each node’s routing table could be directly related to the size of the network and the position of the DODAG root.

With regard to Objective Function the study demonstrated that OF0, which builds a DODAG based on Rank, which merely reduces the number of hops, is more effective with regard to hop-count reduction and power consumption than MRHOF. Which uses the ETX metric in DODAG construction. However, with OF0 not considering network throughput the possibility is raised of studies into further Objective Functions [159]. Studies of the performance of RPL have become more complex since this study took place in 2012, however, it demonstrates the constraints which were in place before the advent of ContikiRPL.

The conference paper “Performance Evaluation of RPL Objective Functions” [159] was one of the first studies to investigate the impact of the two Objective Functions in combination with particular topologies and Packet Reception Ratio (RX). This study demonstrated that performance can be optimised depending on the topology used, in this case random or grid, and that MRHOF can provide slightly better results in regard to Packet Delivery Ratio (PDR)

and energy consumption. However, there is clearly room for further study with regard to different topologies and different metrics and constraints used with MRHOF. Some of the ideas within this paper are built on within the testing performed as part of this study.

Bringing research completely up to date and again demonstrating how Cooja is now seen as the logical choice for the simulation of RPL networks, comes a study of "Proactive Maintenance in RPL for 6LowPAN" [157]. This study proposes a proactive version of RPL, namely Pro-RPL. This based on what is defined as a "suffering index" [157] which is defined by RPL nodes' tendency to fail. With the aim being to predict the likelihood of failure, and therefore circumnavigate the issues that then follow. Among those being the buffering of data within a node until a link is re- established and the change of parentage within the DODAG. The operation of pro-RPL is thus, utilising information from DIO messages (used by RPL to build upward routes from leaf nodes to sink nodes) received from neighbouring nodes, the suffering index of each node's parent is calculated "based on the path cost from the parent to the root, the parent's neighbouring index, energy consumption and its number of alternative parents" [157]. This study is typical of many current studies to be found with regard to RPL and how to improve routing within WSNs. More novel approaches are now being taken to address many of the inherent problems with RPL, and routing in WSNs in general. This would certainly appear to indicate the recent standardisation of RPL by the IETF should be seen as a baseline to build from, rather than a defined endpoint in the development of this area [105].

4.3.2.1 Summary

The diversity of studies into the performance of RPL makes a direct comparison across all paper's problematics. However, several observations can be made. Firstly, regarding the use of a particular simulator, in using the actual code utilised in real nodes, Cooja would appear to be the most realistic choice currently available. In terms of the performance of metrics, whilst both OF0 and MRHOF have both been utilised, only the ETX metric is used with MRHOF in any

of the studies summarised. Finally, when measuring the performance of RPL no consideration is given to the physical layout of the network other than all nodes should be well within range. This in order to measure metrics such as PDR, Latency and Energy Consumption. As such this led to the conclusion that a gap exists in research where the effect on a network where transmission ranges between nodes are 'strained' is examined. It was concluded that this study should utilise the Energy metric in Cooja, as well as hop count and ETX. Finally, the performance metric should be that of the ability to retain nodes as part of the DODAG build.

4.3.3 PERFORMANCE ANALYSIS AND EVALUATION

Testing as part of this study is implemented using the Cooja simulator within Instant Contiki 2.7, not to be confused with the Contiki OS which is an actual operating system for use within real Wireless Sensors. As such, although the tests in this study are performed on simulation software, the nodes, or motes as referred to within Cooja, used within each simulation are compiled with the actual firmware used within physical versions of said motes [128]. Resultantly, each mote should behave as if in a real implementation of a WSN. Secondly, the performance of each mote is within the physical parameters of that mote type. In the case of the testing to be performed as part of this document, the simplest of the motes available for use within Cooja shall be used, that being the Tmote Sky sensor [160]. The Sky mote has integrated sensors as well as radio, antenna, microcontroller and programming capabilities. From the point of view of testing within this document one of the most important features is "Integrated onboard antenna with 50m range indoors / 125m range outdoors" [160].

4.3.3.1 Performance Analysis

Several routing metrics for achieving load balancing in RPL networks have been proposed in the literature including number of children, throughput and queue utilization factor with each has its own shortcomings. In our study, we opt to use the number of children metric for the purpose of load-balancing for two primary reasons. First, it can be measured easily based on

the data-plane traffic without incurring an extra overhead in the control-plane, especially in periodic applications as discussed next. Second, in the vast majority of applications, it reflects the actual network load.

Testing within this document shall build on previous studies with the primary focus on the two Objective Functions, OF0 and MRHOF. Within Contiki the use of OF0 effectively results in the use of Hop-count as a metric. In the case of MRHOF the ETX metric and another metric where the remaining Energy level of nodes is used are available in Cooja and both shall be utilised. As previously stated, this study approaches testing from a different angle from other studies. In this regard, the novel approach shall be taken of utilising 'strained' transmission ranges within topologies. This is with the intention of analysing the best performing OFs and metrics therein. From the analysis of the data recorded, the positives and negatives of each OF shall be discussed, as well as conclusions drawn as to potential future developments.

4.3.3.2 Simulation Environment and Parameters

As has been clearly illustrated, RPL has been tested in various scenarios. The approach taken in the testing within this document was to utilise all metrics available with regard to building a DODAG. In this regard both Objective Functions have been used – OF0 [40] and MRHOF [25]. A particular OF will utilise the metric advertised in DIO messages, with OF0 using rank which essentially results in the use of Hop-count and MRHOF defaulting to ETX. For the purpose of this testing the use of OF0 shall be referred to as using Hop-count. The use of MRHOF raises the possibility of utilising other metrics which may be within the Metric Container of a DIO. The Cooja simulator in the Instant Contiki OS [161] facilitates the use of the Energy metric when building a DODAG instance, taking into account the energy level of motes. Therefore, this allows the use of three different metrics with the possibility to compare the results across these.

Within the parameters of each metric the tests in this section utilise two different network layouts. Those being a tree formation with a sink mote at the top and a circular formation with the sink mote in the middle. These formations shall be utilised with both 25 motes and 50 motes with the location of the motes aimed to test the ability of RPL to build a DODAG under certain conditions. That being that the range between motes shall be random and often not ideal in order to attempt to replicate possible issues in a physical environment. Previous testing has tended to control density of networks in order to keep control of scenarios and thus more easily compare results in regard to power consumption, Packet Delivery Ratio (PDR) and latency. The testing performed as part of this dissertation deliberatively takes the approach of utilising less than perfect scenarios in order to 'strain' the networks in regard to transmission range. Therefore, in this regard the first factor examined within testing shall be the number of motes lost in regard to taking any part in the DODAG build. This allows the effect of each metric to be examined with regard to mote loss, and to determine if the metric and OF are significant factors in affecting the ability to build and maintain a DODAG instance when the distance between motes is at and beyond the limits of the transmission range. In particular this allows the comparison of the performance of the Energy metric to Hop-count and ETX when considering these factors. Each scenario is run over 10 and 20 minutes to examine the effect of each metric as time passes. Finally, each scenario is run with two different transmission ranges. Firstly, a transmission range of 70m and an interference range of 90m, secondly a transmission range of 50m and an interference range of 100m.

In addition to these parameters more specific observations will be made regarding power levels of particular nodes and what can be observed from the particular scenario.

The parameters for testing are shown in Table 4-6. Four tests are performed, with each test utilising a particular topology and number of motes. These topologies are utilised using two different transmission and interference range combinations, all of which is illustrated in Table

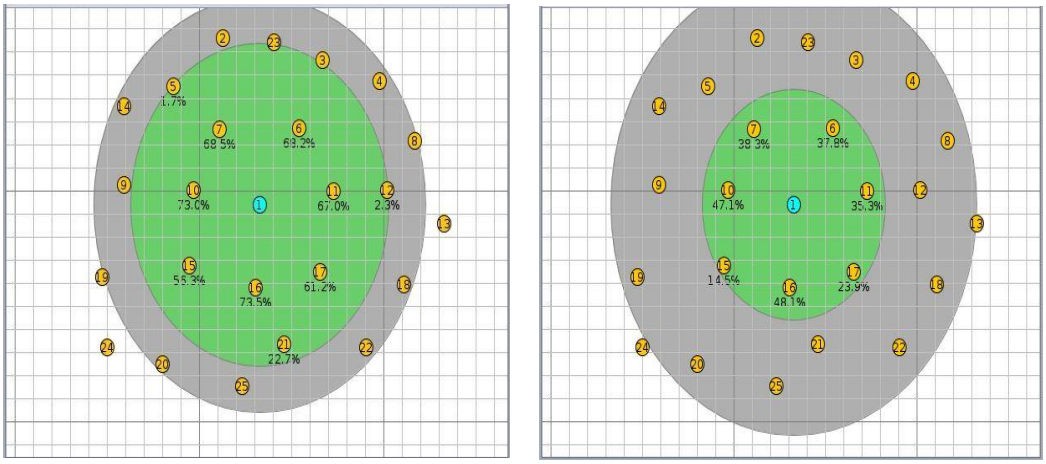
4-6. Tests 1 and 2 comprise of 1 sink and 24 senders, whereas Tests 3 and 4 comprise of 1 sink and 49 senders, with all tests performed over 10 and 20 minutes. All topologies are designed with the intention of 'straining' these transmission ranges in that communication between motes should not be optimal. The main difference in the topologies is that in Tests 1 and 3 a tree topology is utilised, whereas in Tests 2 and 4 a circular topology is in use. The 10m grid demonstrates the distance between motes of between 30m and 50m, as can be observed in **Figures 4-5**.

Table 4-6. Simulation Parameters Setup

Test Parameters	**Values**		
Objective Functions	O	MRHOF	
Metrics	Hop-	ETX	Energy
TX Range/INT Range	70m/90m, 50m/100m		
Topologies	Tree (Sparse), Circle (Sparse)		
Simulation Times	10 minutes, 20 minutes		
Number of Nodes	25, 50		
Mote Type	Tmote Sky		
Wireless Channel Model	UDGM		

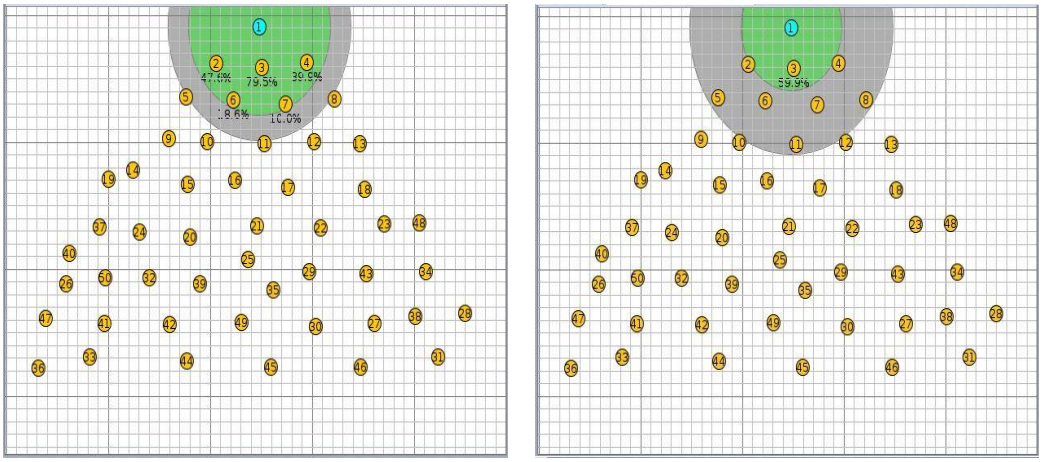
(a) Test 1 with 70m, 90m (b) Test 1 with 50m, 100m

Figure 4-5. Test 1 Transmission, Interference



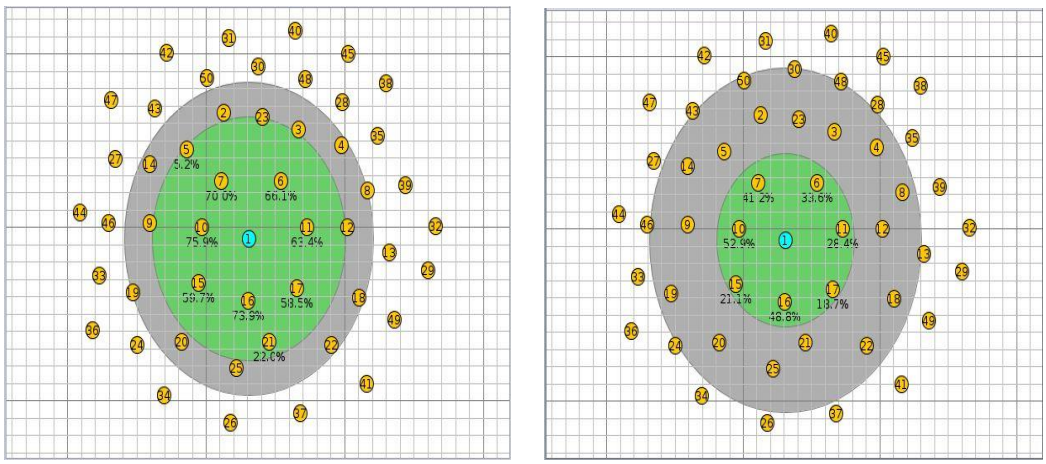
(a) Test 2 with 70m, 90m (b) Test 2 with 50m, 100m

Figure 4-6. Test 2 Transmission, Interference



(a) Test 3 with 70m, 90m (b) Test 3 with 50m, 100m

Figure 4-7. Test 3 Transmission, Interference



(a) Test 4 with 70m, 90m (b) Test 4 with 50m, 100m

Figure 4-8. Test 4 Transmission, Interference

4.3.3.3 Simulation Experiments

4.3.3.3.1 TEST 1

The results in relation to Mote Loss are compared across the four different test runs as part of Test 1. The results can be observed in **Figure 4-9**. What is immediately clear is that the change to a transmission/interference range of 50m/100m from 70m/90m has a major effect on the ability of RPL to build and maintain a DODAG instance. What this demonstrates is that when motes are only within the interference range of each other it causes great difficulty in exchanging messages to a degree that a DODAG can be maintained. In regard to the different metrics in use it can be observed that the Energy metric loses the greatest number of motes in all scenarios, losing over 70% of motes in the 50m/100m scenario over 20 minutes. What can be observed regarding the Hop-count and ETX metrics is that both perform better over greater periods of time, with mote loss decreasing in the 20 minute scenarios. Even for the more challenging 50m/100m scenario, by the time the scenario has been running for 20 minutes, RPL using MRHOF with the ETX metric has 76% of the motes making up the DODAG.

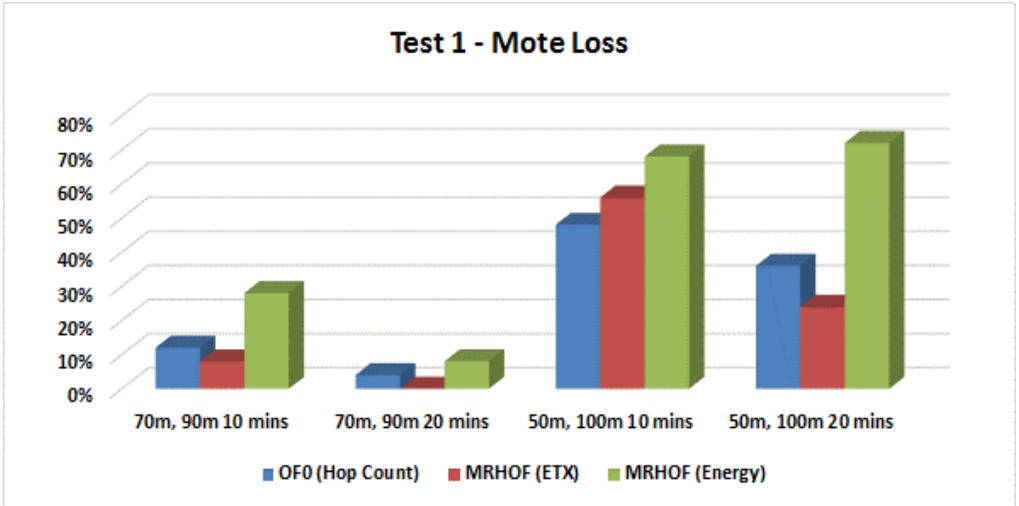


Figure 4-9. Test 1 MOTE Loss

4.3.3.3.2 TEST 2

The results in relation to Mote Loss are compared across the four different test runs as part of Test 2. The results can be observed in **Figure 4-10**. What should be considered firstly is that the scale of this graph is far smaller than in Test 1, with no scenario suffering mote loss above 30% for any of the metrics used. Again, the change to a transmission/interference range of 50m/100m from 70m/90m has an effect on the ability of RPL to build and maintain a DODAG instance, but not to the extent of the tree topology utilised in Test 1. This demonstrates the greater variety of routes available to the sink mote in this topology, even when the transmission range is reduced. Regarding the different metrics in use, the only relevance is in regard to the 50m/100m scenario as there is no loss of motes whatsoever at the end of both runs of the 70m/90m scenario. Regarding the 50m/100m scenario again it is the Energy metric which performs worst, although to a lesser degree than in Test 1. Again, both ETX and Hop-count perform well the longer the scenario runs for. Hop-count in particular has no loss of motes at all after 20 minutes.

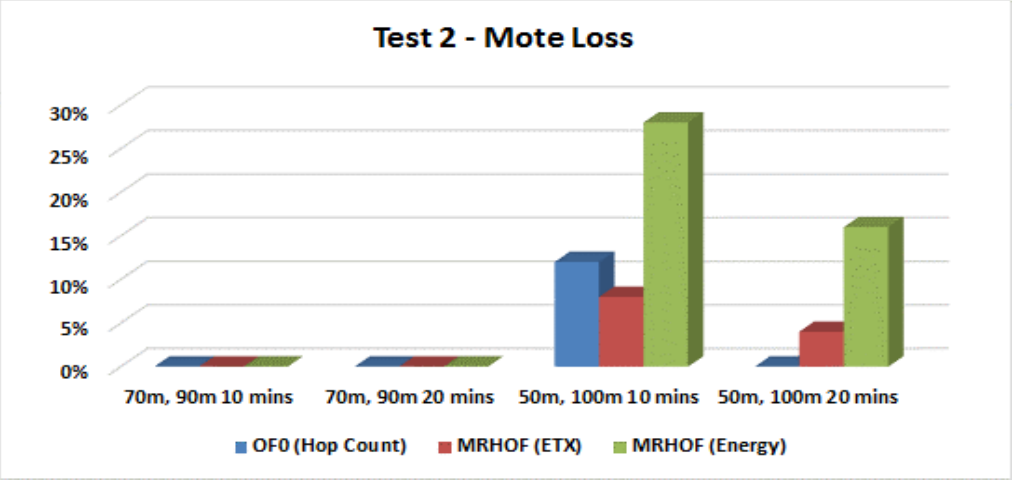


Figure 4-10. Test 2 MOTE Loss

4.3.3.3.3 TEST 3

The results in relation to Mote Loss are compared across the four different test runs as part of Test 3. The results can be observed in **Figure 4-11**. What can be immediately observed

regarding the topology is that the 50m/100m suffers catastrophic mote loss irrespective of the timeframe, to the point where it can be concluded that this scenario is not viable. This scenario would have to be improved with regard to mote density regardless of which metric is utilised. Alternatively, the 70m/90m scenario performs slightly better initially, although the Energy metric again suffers from major loss of motes. As the time progresses from 10 minutes to 20 minutes the Energy metric does improve slightly but the ETX metric improves greatly.

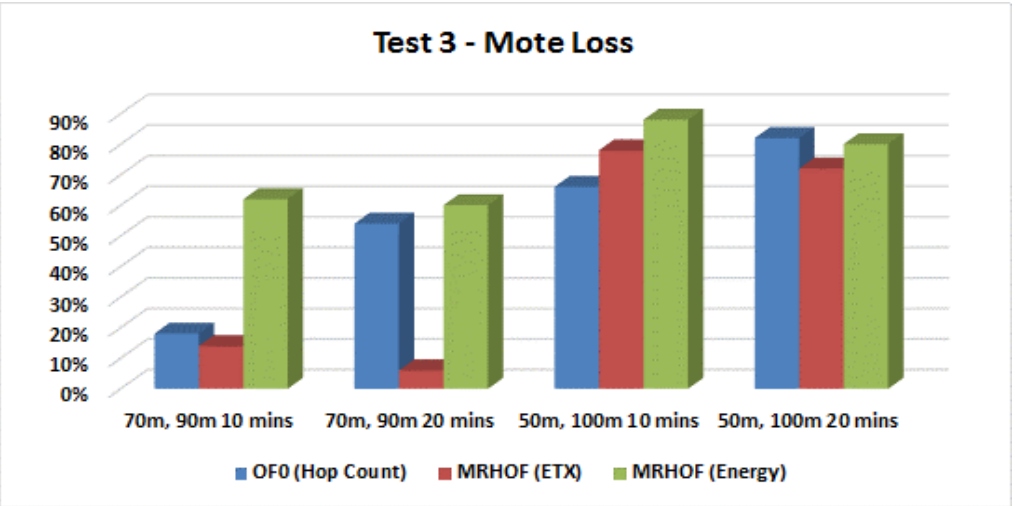


Figure 4-11. Test 3 MOTE Loss

4.3.3.3.4 TEST 4

The results in relation to Mote Loss are compared across the four different test runs as part of Test 4. The results can be observed in **Figure 4-12**. It could be argued that this scenario demonstrates most effectively the difference in performance with regard to mote loss across the three different metrics used. Again, the poor performance of the Energy metric is clear, even in the almost ideal 70m/90m scenario where ETX and Hop-count lose very few motes by the end of the 20 minute test. Moving to the 50m/100m scenario there is a catastrophic loss of motes when utilising the Energy metric. However, whereas the Hop-count metric still endures losses of 32% reducing to 24%, the ETX metric sees losses move from 14% to only 6% in a less than ideal network scenario.

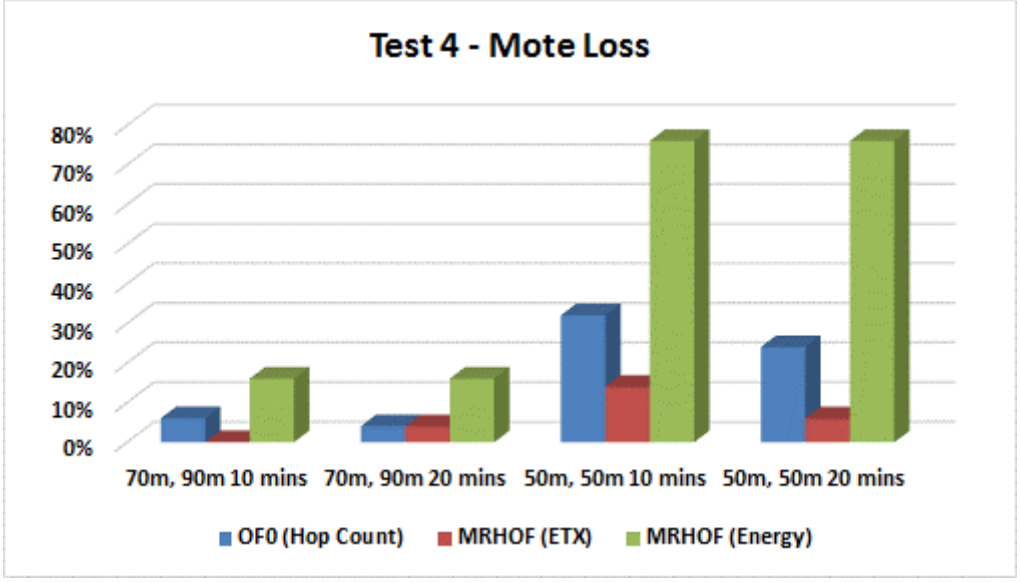


Figure 4-12. Test 4 MOTE Loss

The third step towards realizing an efficient load-balancing objective function is answering the question on how to combine the load-balancing metric with another metric without effecting negatively other performance metrics and how to select the preferred parent based on such a composite metric. Hence, we proposed that the new OF should lexically combines a primary metric (e.g., hop count or ETX) with the number of children load-balancing metric of a specific parent (NoCH) with the goal of building a balanced topology. To select the preferred parent based on such metric, the primary metric is used by a node to calculate its rank and select a set of candidate parents toward the DODAG root. Once the candidate parent set has been selected, the load-balancing metric is used to break ties among selected parents if there is more than one in the parent set. The details of the parent selection process is illustrated in Algorithm 2.

4.3.3.4 Evaluation

The topologies utilised within this study have been designed with the aim of 'straining' the transmission ranges of motes.

In this regard the evaluation concerns the ability to maintain motes within a DODAG under these conditions. The main parameters to evaluate are the performance of the use of Energy as

a metric as part of MRHOF, in comparison to the use of the more commonly used ETX within MRHOF and Hop-count as part of OF0. The effectiveness and requirements of the particular topologies shall also be examined. Observing the performance of the Energy metric across all tests it is immediately apparent that in terms of maintaining motes within a DODAG, it is far less effective than Hop-count or ETX. When considered logically this should not be surprising. The motes utilised within the networks are battery-powered and as time passes the power levels will decrease. If the sole metric used to determine the best path to the sink mote is one which utilises the remaining energy levels within motes, then issues would appear unavoidable. The 1-hop motes, and any other which may be the parent mote in a bottleneck situation, will obviously use more energy than others due to the higher levels of processing involved. This clearly then causes issues when considering energy levels in order to establish parentage and therefore establish the optimum path to the sink mote. In this regard it can be concluded that the Energy metric is not effective when used alone. Some results would render the network virtually useless, and this only worsens over time.

Contrastingly, the other metric utilised by MRHOF, that of ETX, performs very well in regard to sustaining motes within a network of strained transmission ranges. This is particularly true versus the use of OF0 and Hop-count over longer periods. This again would seem logical in this scenario given that the ETX metric seeks to avoid the lowest quality links in the network rather than taking a blunt-force approach of merely utilising the shortest path to the sink mote. In conclusion, in a topology where the transmission ranges of motes are strained, a metric of energy levels of motes is ineffective on its own. Over a longer period of time it would appear any network utilising this metric in these conditions would eventually be rendered useless. Of interest going forward would be to comprise testing where Energy and ETX are used together. It may be that this could be best achieved by utilising Energy as a constraint rather than a metric. Greater depth of investigation is required in this area as the Cooja simulator would

appear to provide a more simplistic use of metrics than that described in “RFC 6719: The Minimum Rank with Hysteresis Objective Function” [25] and “RFC6551: Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks” [162]. Cooja also does not provide a facility to utilise constraints within MRHOF as a matter of course, therefore some manipulation of code would be required. This would also be the case in regard to combining the Energy and ETX metrics.

With regard to the topological layout of the tests within this paper, it can be concluded that a circular layout results in better performance in regard to maintaining the number of motes. It is clear that a tree layout puts considerably greater strain on first-hop motes and can also cause other bottlenecks within the network. In conclusion, node density is extremely important in a tree formation and should be given careful consideration as part of the initial design.

4.3.4 THEORETICAL POINT-OF-DEPARTURE

The paper has a good theoretical background which could be utilized around the Routing Protocol for Low-power and Lossy Networks and Linear Sensor Networks. The focus of the paper is not direct theoretical breakthrough. The findings from the evaluation have non-trivial value in guiding researchers and designers to generate novel theoretical concepts or system protocols or models for better networks, which will bring up new types of mobile networks.

4.3.5 EMPIRICAL DATA COLLECTION METHOD

This paper provides an empirical study around the Routing Protocol for Low-power and Lossy Networks (RPL) and Linear Sensor Networks utilizing one of the well-known simulators in the field to conduct experiments and collecting data that uncover some issues of the standard under few scenarios. The evaluation engages fours tests in appraising the network metrics from diverse aspects. The tests are developed systematically, and the scale, the data collected, and

the findings from the analysis of the test results have non-trivial impact on the future networks design.

4.3.6 CONTRIBUTION TO THE KNOWLEDGE

In this paper, a series of tests differ from previous work in regard to RPL in two regards. Firstly, there is no concerted effort to ensure the appropriate density of the network topologies with the intention of straining the limits of the transmission ranges.

Secondly, the use of an Energy metric with MRHOF to bring a comparison with OF0 and MRHOF using ETX. When considering a sparse, strained network topology it can be concluded that the optimum metric for use with RPL in terms of maintaining the maximum number of motes, is the MRHOF with ETX. In regard to the Energy metric, it can be concluded that it is highly ineffective in this environment. It may be that there are benefits to be gleaned from using this metric in a more controlled environment. Aims to determine the optimal Packet Reception Ratio (RX) when using OF0 and MRHOF with ETX. It could be of interest to repeat these tests with the Energy metric to determine any possible benefit.

As of the 16th of September 2021, the article has been read a total of 334 times and citied 11 times.

4.4 AN RPL BASED OPTIMAL SENSORS PLACEMENT IN PIPELINE MONITORING WSNS

4.4.1 BACKGROUND AND PROBLEM STATEMENT

The unique long distance linear topology characteristics of the network infrastructure in which a large pool of sensor nodes is distributed linearly along the pipeline and limited to a single path to transmit the data, increases the challenges associated with network reliability, connectivity and an efficient energy management for sensors and actuators. It is therefore important to overcome these challenges before efficient communication and reliable monitoring system for oil and gas applications can be achieved in WSNs. This paper aims to investigate the linear placement of sensor nodes along oil and gas pipeline with respect to distance and its impact on energy consumption, packet delivery ratio, end-to-end delay and throughput. The study is carried out using a uniform topology, where nodes are distributed linearly along the pipeline with increased distance, while the sink is placed at the end of the pipeline. In addition to this the paper fulfils the requirement of evaluating the performance of IPv6 Routing Protocol for Low-power and Lossy Networks (RPL) in LSNs and to improve it where possible. There are very few works related to node placement in LSN, they mainly focus on placement of sinks in overall LSN deployment. Whereas focus of our work is mainly on placement of sensors because they have limited energy resources and have higher impact on network performance. Moreover, these studies do not analyse the impact of nodes location in term of quality of service metrics other than network lifetime, which we do in this work. In addition to this, the performance evaluation in this study carried out based on RPL as a routing protocol, which add more uniqueness to our work

4.4.2 RELATED WORK

Strategic placement of nodes is extremely crucial to satisfy contemporary performance metrics such as energy efficiency, network lifetime, coverage and connectivity. This issue is highlighted in [9], which proposes the routing protocol Minimum Energy Relay Routing

(MERR) for LSNs. Within this study, the authors admit to seeing optimal routing as the least important metric in determining the efficiency of the protocol. With the minimum use of energy seen as the highest bound. In return, this also highlights another potential issue, with the previous study assuming uniform node placement. It is unlikely that this will always be the case. The study in [163] divided LSNs into groups based on density and the types of nodes in the network. Also seeking to inspire development of routing protocols which are more pointed in the direction of LSNs. The authors in [164] attempt to negate some of the issues presented by LSNs by utilising unmanned aerial vehicles (UAVs) in data collection from the sink nodes. What is clear is that there is little consensus on how best to approach the issue of routing in LSNs in relation to the optimal node placement strategy.

4.4.3 System Model And Problem Description

As a system model a pipeline monitoring sensor network that contain N number of nodes and a sink is considered as illustrated in **Figure 4-13.**

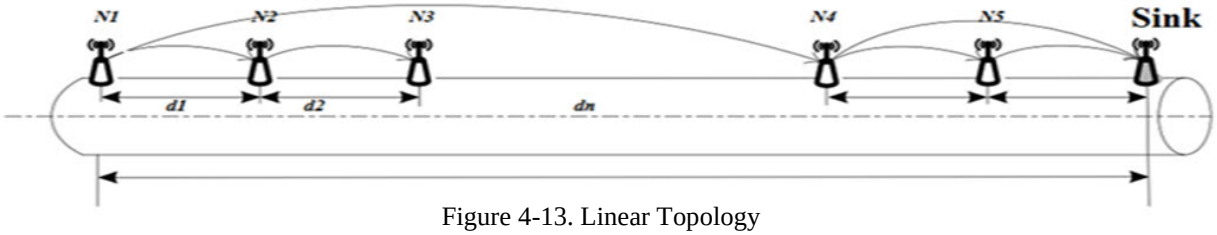


Figure 4-13. Linear Topology

The nodes are responsible for detecting, collecting and processing the monitored information and send it to the sink for further processing. The sink is located in one end of the pipeline.

Let *N* be the number of sensor nodes along the pipeline and *di* be the distance between node *i* and (*i*+1), *i = 1,.., n.*

The length of the pipeline is

$$\sum_{i=1}^{N} d1 = L \quad (4)$$

The nodes communicate in multi-hop fashion with the same transmission range. For the data forwarding between individual nodes and the sink RPL with Expected Transmission Count (ETX) as an objective function is employed as a routing protocol. The use of the Expected Transmission Count (ETX) metric in RPL over LSN will help the nodes to use more reliable paths that is based on minimum transmissions of a packet to reach the sink.

Assuming different distance *di* between nodes, nodes placed at a larger distance from sink might suffer from additional overhead and overload in transmitting the packets, which in return might lead to performance implications in throughput, reliability issues and energy consumption.

4.4.4 PERFORMANCE EVALUATION AND DISCUSSION

In this subsection the simulation and metrics and the performance evaluation are presented.

The Simulated topology consists of 24 sensor nodes and 1 sink positioned along the pipeline of length 1000m in a linear sequential manner. The sink is positioned at the edge of the pipeline. The experiment is carried out so that an optimal spacing between nodes under uniform and linearly sensor placement schemes with increasing distance can be provided. In addition to this the performance of RPL under the same conditions can also evaluated.

The evaluation has been carried out using a customized version of Omnet++ network simulator that includes an implementation of the RPL routing protocol designed by the authors. The transmission and an interference range are set to be of 100 meters. The Expected Transmission Count (ETX) [108] [165] [169] is used for calculating the node ranks and selecting the preferred parent, so that stability in the network topology is built. Further parameters are provided in Table 4-7.

Table 4-7. Simulation Parameters Setup

Parameter Name	Values
Simulation area	1000 x 1000 m
Number of nodes	First Scenario 25
Number of nodes	Second Scenario 200, 300, 400, 500
Simulation time	300s
UDP Packet	60 byte
Mac/Adaptation Layer	IEEE8015.4/6LoWPAN
Radio Model	CC2420
Transmission/Interference Range(m)	30, 25 m
Routing Protocol	RPL
Mote Type	Tmote Sky Mote
Mode Of Operation	Non-Storing mode
Rank Metric	ETX
Nominal Capacity	1000mAh
Battery Capacity	1000mAh
Voltage	3 V
Node Distribution	Linear Distribution

4.4.4.1 Distance Variation

In the simulation scenario the distance between nodes starts at a value of 10 meters then varied by 5m meters to a maximum of 40 meters. UDP packet of 60 bytes is sent by all nodes to the sink. To generate accurate results an average value of 10 runs with different seed values over a simulation duration of 300 seconds is taken. Following metrics were used:

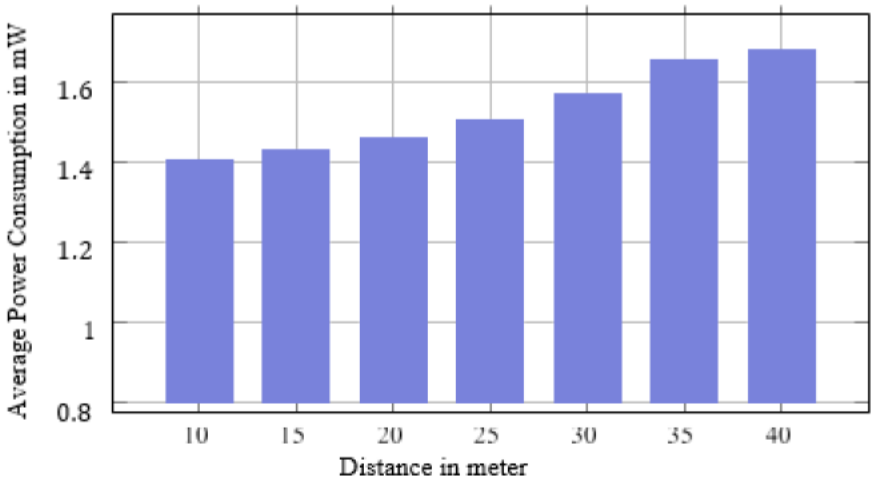


Figure 4-14. The Average Mean Power Consumption in mW

Figure 4-14 presents the average mean power as a function of the distance between nodes. It can be observed that increasing the distance will result in an increase in the power consumption. The figure indicates that placing the node in 10 meters distance from each other

leads to the least amount of consumed power and the longer the distance between nodes is the more power is consumed. The power consumption reaches the highest level at a distance of 40m. This increase is due to the fact that the transmitting from a larger distance to the sink might lead to overhead and overload in delivering data packets.

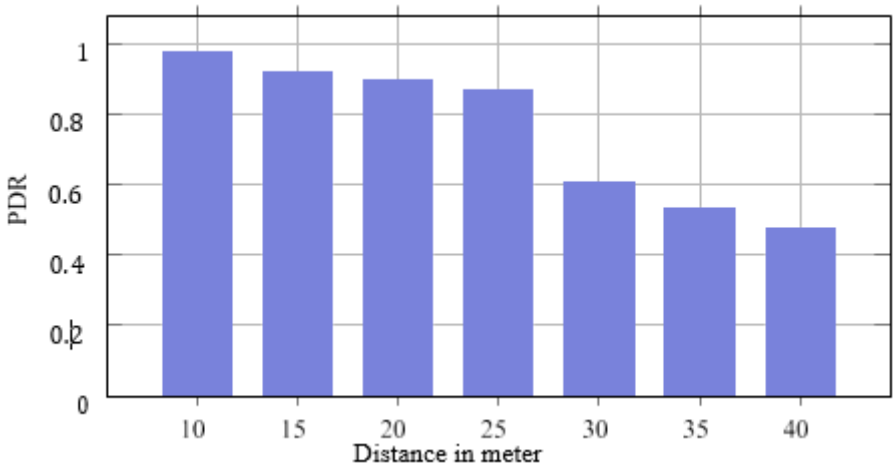


Figure 4-15. Packet Delivery Ratio vs distance

Figure 4-15 illustrates the PDR as a function of distance between nodes along the pipeline. The delivery ratio of 98% in 10 meter distance has achieved the highest level compared to the other distances followed by a delivery ratio of 92%, 89% and 87% for 15m, 20m and 25m respectively. While at distance of 30m and 35m the PDR has dropped to 60% and 53% respectively. At a distance of 40m the PDR has registered the lowest value of 48% only.

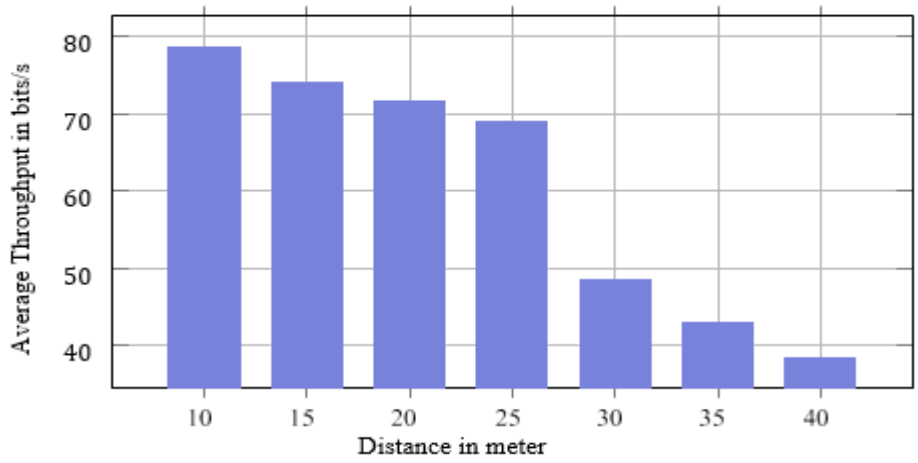


Figure 4-16. The Average Throughput vs Distance in bits/s

Figure 4-16 shows the results obtained for the throughput as a function of distance in bit/s. From which it can be observed that the distance of 10m has achieved the highest throughput of 78.72 bit/s surprisingly the throughput at 15m has shown significant drop. At distance of 20m, 25m and 30m the average throughput increases outperforming 15m, 35m and 40, but still less than the throughput in 10m distance. It can be concluded that placing the node at 10m distance from each other is the optimum in terms of throughput.

Referring to **Figure 4-17** the average end to end delay in packet transmission as a function of distance is presented. It can be observed that at a distance at 10m the end-to-end delay has recorded the lowest level. Starting at a distance of 15m the end-to-end delay increases gradually till it reaches its highest value at 40m.

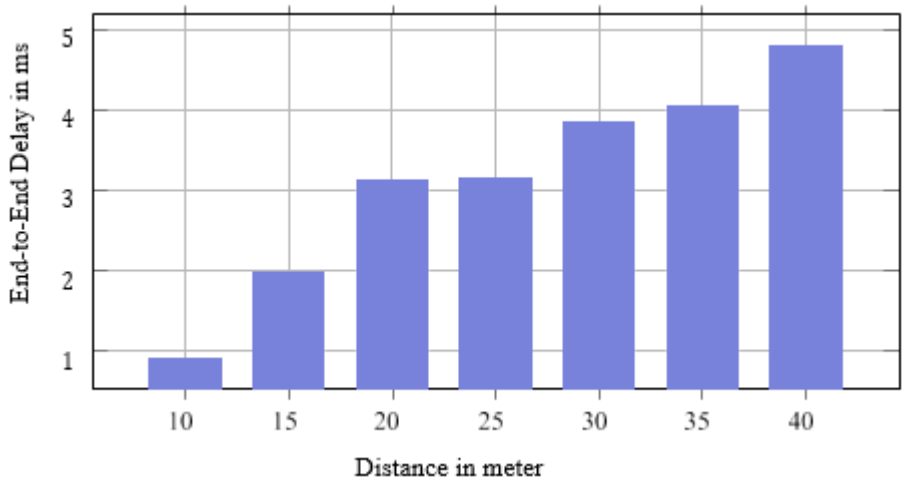


Figure 4-17. The End-to-End Delay vs Distance in m/s

4.4.4.2 Network Density

In the second scenario we have increased the number of nodes starting from 100 to a maximum of 500 nodes. This required also increasing the length of the pipeline to 20000 meters to accommodate the number of nodes. The simulation time is set to 1 hour to enable enough time for all node to join the DODAG. The distance between each node starts at a value of 10 meters then varied by 5m meters to a maximum of 40 meters. UDP packet of 60 bytes is sent by all nodes to the sink. To generate accurate results an average value of 10 runs with different

seed values. This scenario should help in studying the impact of the number of nodes and distance would affect the energy consumption, PDR, throughput and delay in a linear pipeline.

Figure 4-18 represents the power consumption for different distances and increasing number of nodes. It can be observed that in a distance of 10 meters the power consumption is the lowest. The power consumed is increased by increasing the distance and the number if nodes. This happens because the number of hops needed to reach the destination is increased by increasing distance, and hence the average power dissipated is decreased, but this is valid up to an optimum value, which is here the distance of 10m.

It is clear from the **Figure 4-22** that there is an inverse relationship between the distance and the power consumption while there is a direct relationship with the delay and DODAG construction time. Indeed, the lesser is the minimum DIO interval, the higher is the energy consumption.

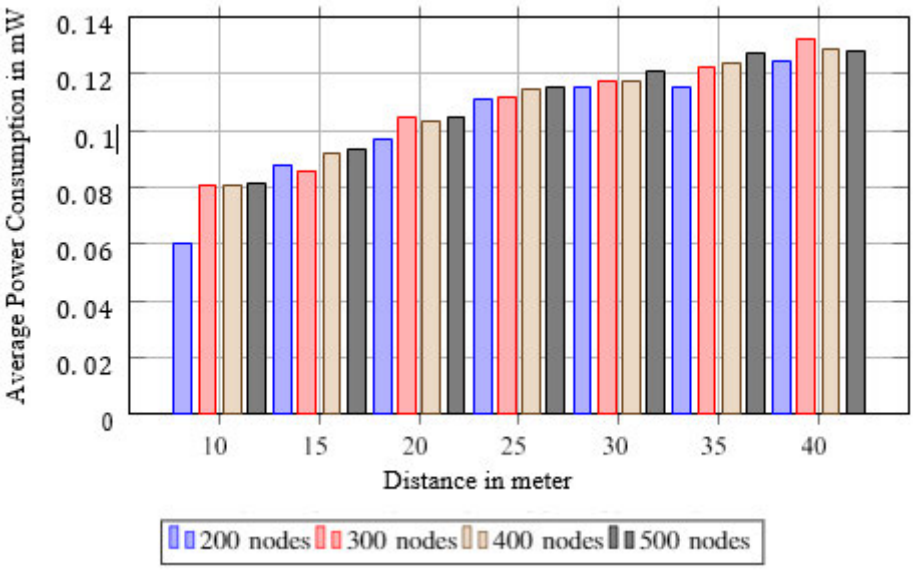


Figure 4-18. Power Consumption vs Distance for Different Node Number in mW

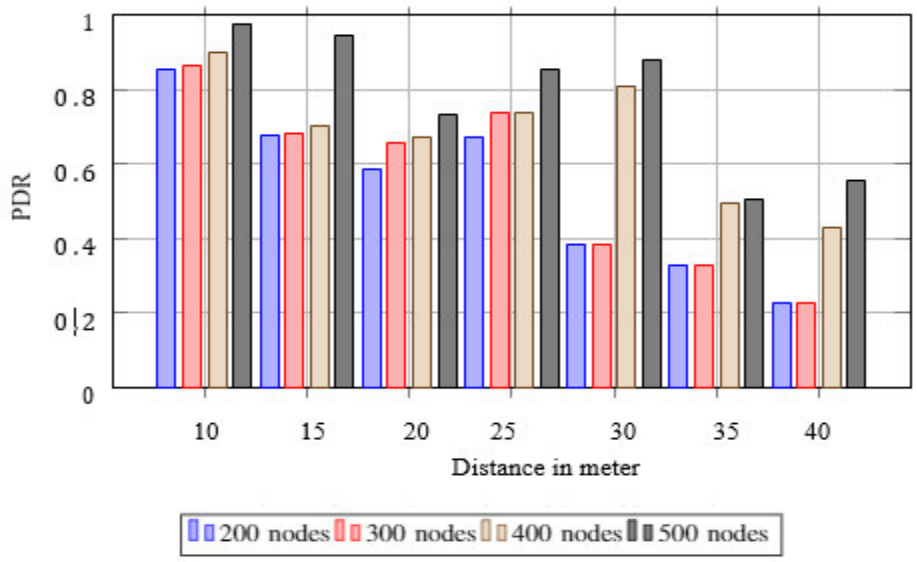


Figure 4-19. PDR vs Distance for Different Node Number

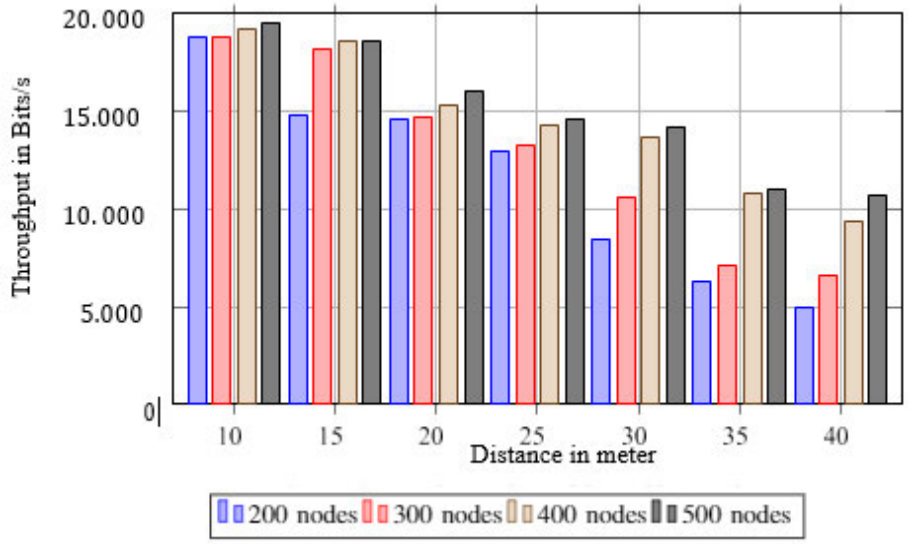


Figure 4-20.The Throughput vs Distance for Different Node Number

From **Figures 4-19** and **4-20** the packet delivery ratio and throughput decrease with increasing the distance and increase as the number of nodes increases. Here also we can conclude that 10 m distance is an optimal distance that can accommodate up to 500 nodes. This also can be justified by considering **Figures 4-22**, where it shows shorter the distance the less time it takes for nodes to join the DODAG. As consequence immediate packet transmission can start.

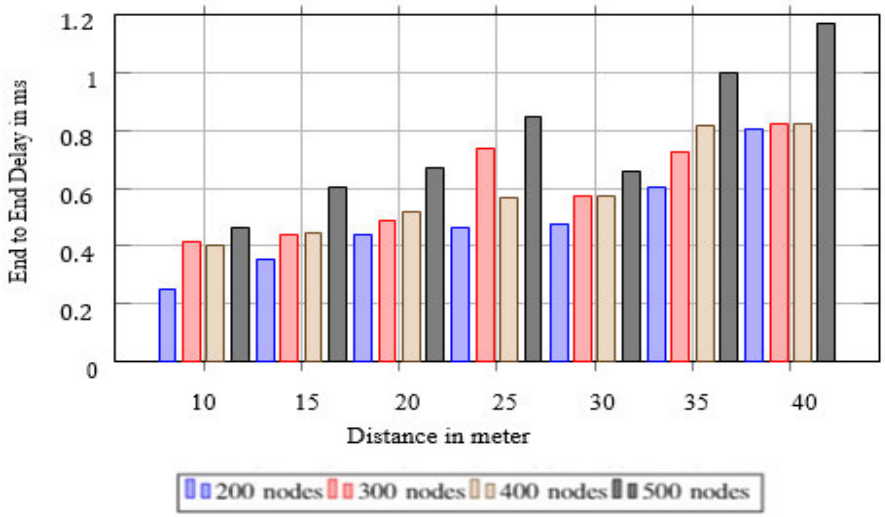


Figure 4-21. The End-to-End Delay vs Distance vs for Different Node Number

A Poor packet delivery rate is an ingrained problem. It may be caused by many reasons, such as interferences, collisions, signal attenuation etc. **Figure 4-21** illustrates the delivery ratio according to different distance and node density that are classified to their Euclidian distance from each other and from their sinks. The path cost selection is based on the OF with ETX metric, which unsurprising gives the best overall results in terms of power consumption, PDR and throughput. However, this comes at the cost of increased delay due to the probing packets required to calculate the ETX metric. But also, the results shown in **Figure 4-22** is applicable to justify the poor delay when the distance increases.

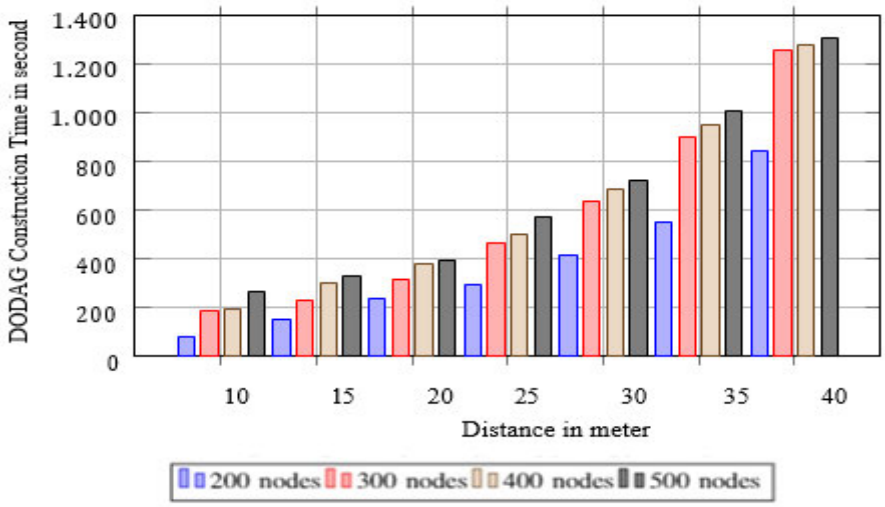


Figure 4-22. DODAG Construction Time vs Distance for Different Node Number

4.4.5 THEORETICAL POINT-OF-DEPARTURE

The RPL protocol acts as the theoretical underpinning of the work presented in this paper.

The paper has a good theoretical grounding around the RPL standard and its suitability under the scenario of Pipeline Monitoring WSNs, a type of IoT networks highlighting some issues in relation to node placement and investigating what would the optimal node placement in this regard.

4.4.6 EMPIRICAL DATA COLLECTION METHOD

The paper analyses and evaluates the impact of node placement in a linear sensor network (LSN) by placing the nodes uniformly a long a pipeline. It utilizes OMNeT++ to conduct experiments and collect the results to investigate the optimal node placement under Pipeline Monitoring WSNs and the RPL standard.

4.4.7 CONTRIBUTION TO KNOWLEDGE

This study has highlighted research carried out to investigate the impact of node placement in a linear sensor network (LSN) by placing the nodes uniformly a long a pipeline. The study based on increasing the distance between nodes, while placing the one sink at the end of the pipeline. The nodes communicate in multi-hop fashion with the same transmission range. For the data forwarding between individual nodes and the sink, RPL with Expected Transmission Count (ETX) as an objective function is employed as a routing protocol. The study evaluates the performance in terms of power consumption, throughout, PDR and end to end delay.

The findings have shown that the increasing of the distance between nodes has important performance implication in terms of the studied quality of service metrics. The shorter the distance between nodes the better the performance is. It can be suggested with great confidence that a distance of 10m has achieved a significant level of performance and can be considered as the optimum solution for node placement in an LSN. In the future it is planned to look at linear network from a routing perspective in LSN by conducting further study on RPL

performance compared to the traditional standards, but also within RPL itself by using different objective functions to determine the best path.

The findings from the evaluation provide the guidance with non-trivial value for researchers and designers to create novel theoretical concepts or system protocols or models for better sensor networks.

The paper has been selected as the best paper in the of International Conference on Emerging Technologies and Intelligent Systems and published as a book chapter in the International Conference on Emerging Technologies and Intelligent Systems, Book Subtitle ICETIS 2021 Volume 2, ISBN978-3-030-85989-3.

4.5 Performance Investigation of RPL Routing in Pipeline Monitoring WSN

4.5.1 Background and problem Statement

As discussed earlier, the need for LSNs arises when use of sensor networks are required in areas such as the monitoring of roads and bridges, but perhaps most pertinently, in pipelines [81] [163] [164]. There are many benefits to be gained by utilising sensors in the monitoring of pipelines, with many of these dependent on the purpose of the particular pipeline. This could involve oil, gas or possibly water [81]. The environment in which the pipeline is located may also be monitored via sensors in order to detect leakages or fire, with the possibility of also relaying camera images via sensors. The use of wireless sensors in these situations also improves upon cabled networks in that they are less prone to failure. With security, also a concern in some areas, wireless sensors remove the possibility of deliberate damage being inflicted to cabling [81]. One of the candidate protocols to be used in such networks is the 6LoWPAN stack. The 6LoWPAN adaption layer enables the IPv6 addresses assignment with low levels of overhead. To facilitate maximum efficiency of WSN, integrated with IoT, the routing protocol RPL was developed to be compatible with 6LoWPAN networks. However, it was found that there are no research studies that investigate the feasibility of using the RPL protocol under such networks. Hence, the main contribution of this paper is on identifying problems at the level of routing in OIL and GAS monitoring network, and a study of specific metrics used to calculate the forwarding cost between nodes in a Multi Segment Linear Pipeline Monitoring WSNs. The RPL protocol was implemented on OMNeT++ simulator with the objective of analysing the behaviors of ETX, HOP-COUNT and RSSI routing metrics.

4.5.2 Performance Evaluation and Discussion

In this section, a simulation approach is considered to analyze three routing metrics discussed previously ETX, HOP-COUNT and RSSI. The simulations were performed through the OMNeT ++ simulator [150]. The focus of the simulations and analysis performed is the

creation and maintenance of upstream routing from the data-generating nodes to aggregator node, the sink node. Thus, only the strategy for the sharing of the DODAG Information Object (DIO) packets and the calculation of the descending rank is described and analyzed.

The simulations and subsequent studies are based on the acquisition of reference metric values to understand the level of quality and efficiency of the networks in question, such as energy consumption, packet delivery ratio, end-to-end delay and throughput. A second objective of the simulations is to provide a link quality assessment of the metrics within the scope of convergence time and the number of preferred parents.

For the simulation, a hierarchical multi segment LSN is considered that consists of 9 segments as shown in **Figure 4-23**. Each segment contains number of sensor nodes placed uniformly and evenly at equal distance of 10 meters in a linear sequential manner along the segments. The sink is positioned at the edge of the pipeline. The nodes communicate in multi-hop fashion with a transmission range of 100m as shown in Table 4-8.

Table 4-8. Simulation Parameters Setup

Parameter Name	Values
Simulation Area	1000 × 1000 m
Number of nodes	39 and 1 Sink
Simulation time	600s
Mac/Adaptation Layer	IEEE802.15.4/6LoWPAN
Radio Model	CC2420
Transmission Range(m)	100
Routing Protocol	RPL
Mode Of Operation	Non-Storing mode
Rank Metric	ETX/ Hop Count/ RSSI
Nominal Capacity	1000mAh
Battery Capacity	1000mAh
Voltage	3 V

4.5.2.1 Increasing The Packet Size

In the first scenario, the default RPL parameters are used. The performance is measured by varying the UDP packet size, starting at 40 byte and increased by 20 to a maximum 140 byte. To generate accurate results an average value of 10 runs with different seed values.

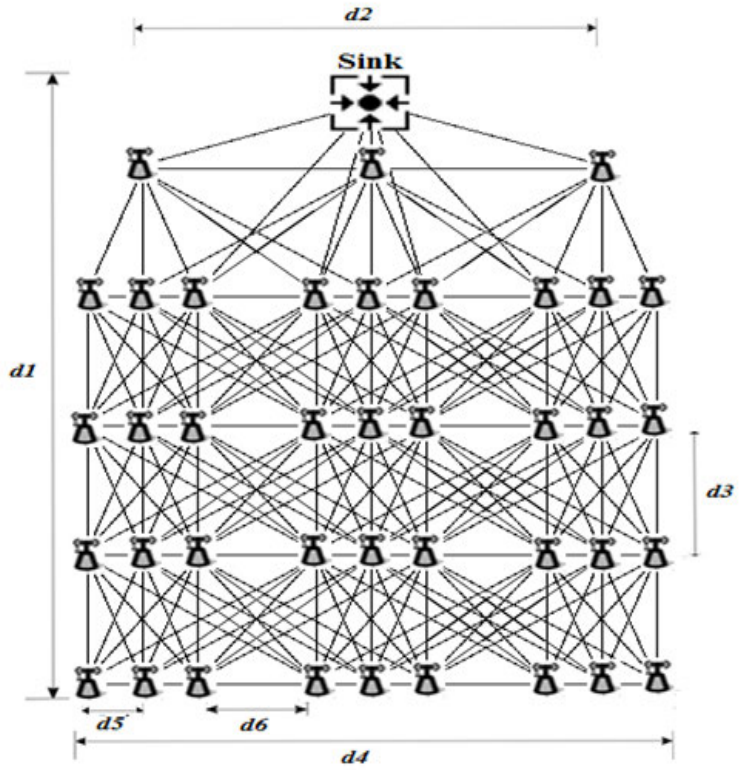


Figure 4-23. A Multi Segment Linear WSN

Figures 4-24, 4-25, 4-26 and **4-27** present comparisons between the Hop-Count, ETX and RSSI in terms of the average power consumption, average packet delivery ratio (PDR), the throughput, and average End-to-End delay respectively as a function of the packet size.

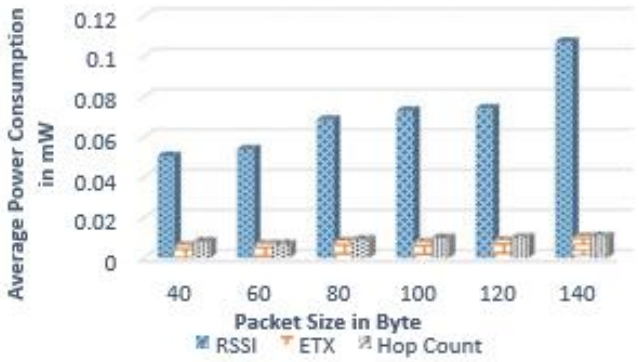


Figure 4-24. The Average Power Consumption vs Packet Size in mW

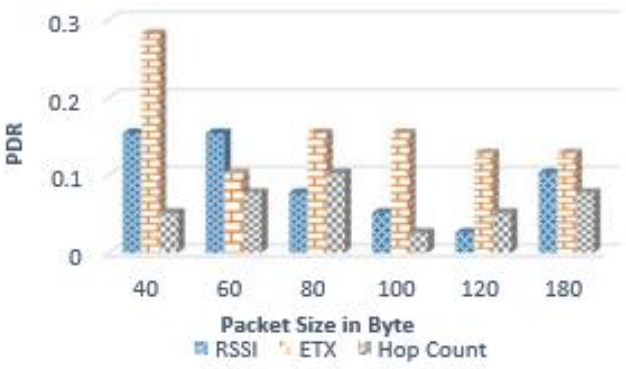


Figure 4-25. The Average Packet Delivery Ratio vs Packet Size

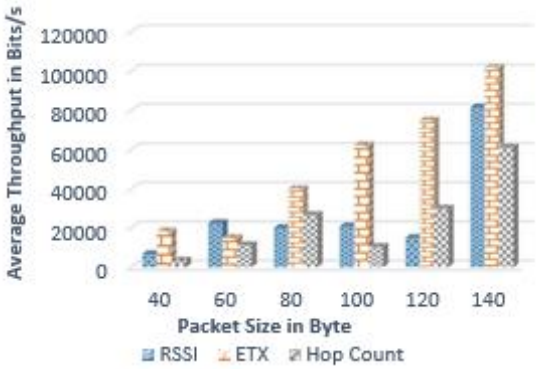


Figure 4-26. The Average Throughput vs Packet Size

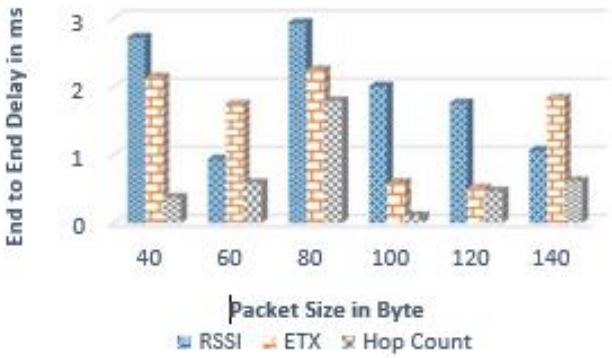


Figure 4-27. The Average End-to-End Delay vs Packet Size

As shown in **Figure 4-24**, RPL with RSSI metric has the worst performance in terms of power consumption while the ETX metric has least power consumption rate. The superiority of ETX can be attributed to the metric capacity in finding optimal routes towards the DODAG root thus lessen the number of retransmissions needed to transmit a specific packet. In turn, this has resulted in less amount of energy expenditure. The same justification is applicable for

the superiority of ETX in terms of PDR and throughput as depicted in **Figure 4-25** and **Figure 4-26** respectively. **Figure 4-27** shows that the hop-count metric has the best performance in terms average end-to-end delay. This can be explained by the fact that hop-count metric tends to select the path with fewer hops toward the root compared to RSSI and ETX. This resulted in packets being transmitted over shorter paths leading to minimizing the average delay. It is unsurprising that ETX gives the best overall results in terms of power consumption, PDR and throughput. However, this comes at the cost of increased delay due to the probing packets required to calculate the ETX metric.

4.5.2.2 DIO Minimum Interval

In the second scenario, the performance of the three routing metrics is evaluated against DIO Minimum interval. This is the minimum possible interval value in the original Trickle algorithm. The first set of comparison simulations involved varying the value of DIO Minimum value from 9 to 15.

These values determine the minimum interval length using,

$$2^x \text{ Milliseconds} \quad (5)$$

Where x is the chosen DIO Minimum value.

Table 4-9 displays the equivalent DIO minimum interval obtained from (2).

Table 4-9. DIO Minimum Interval

DIO Minimum Interval	Equivalent Value in Seconds
8	0.256s
9	0.512s
10	1.024s
11	2.048s
12	4.096s
13	8.192s
14	16.384s
15	32.768s

This scenario runs for 600s sending 60 bytes of packets from source nodes to the sink.

Figures 4-28, 4-29, 4-30 and 4-**31** present comparisons between the Hop-Count, ETX and RSSI in terms of the average power consumption, End-to-End delay, and average preferred parent change and convergence time in Seconds respectively as a function of the DIO minimum interval.

Figure 4-28. The Average Power Consumptions vs DIO Minimum Interval in mw

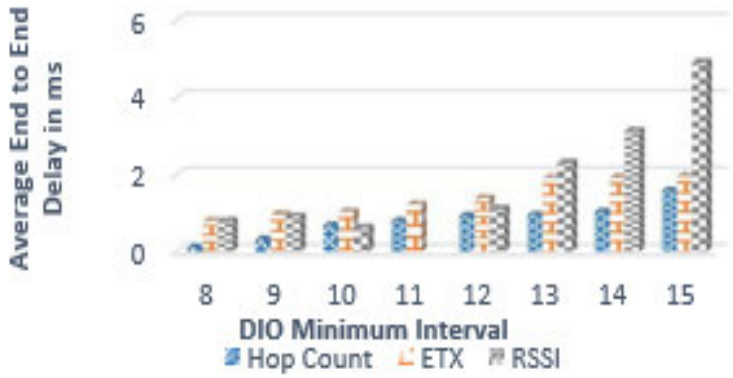


Figure 4-29. The Average End-to-End Delay vs DIO Minimum Interval

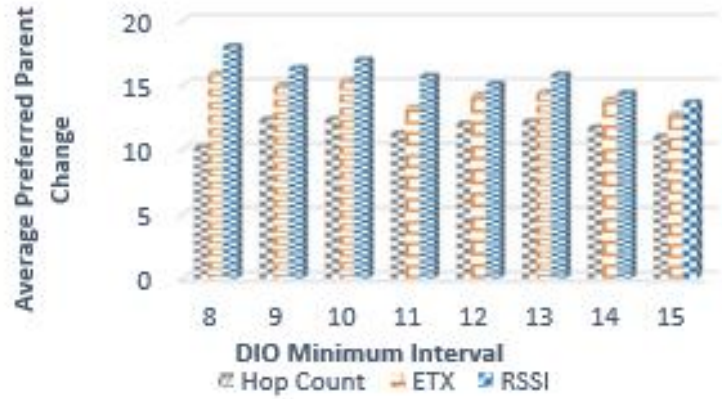


Figure 4-30. The Average Preferred Parent Change vs DIO Minimum Interval

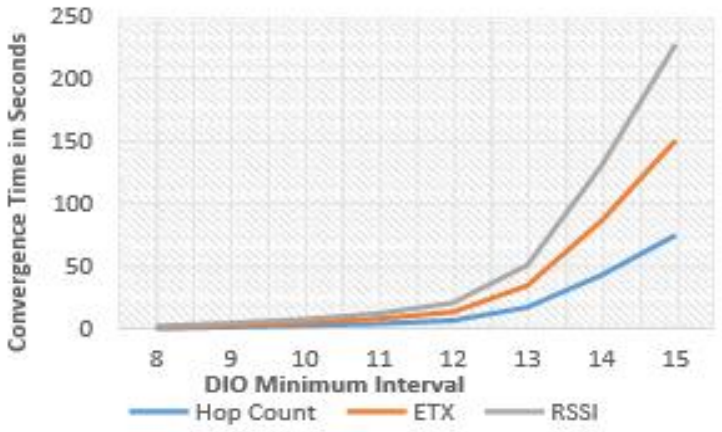


Figure 4-31. The Convergence Time vs DIO Minimum Interval

It is clear from the figures that there is an inverse relationship between the minimum DIO interval and the power consumption while there is a direct relationship with the delay and the convergence time (i.e., the time at which the protocol has finished building the topology or restructured it). Indeed, the lesser is the minimum DIO interval, the higher is the energy consumption. This is due to that the protocol makes more DIO transmissions per time unit as the DIO interval gets smaller. More control overhead in the form of more DIOs transmissions will surlily results in higher energy consumption rates. On the other hand, when the minimum DIO interval gets bigger, the time needed to construct the topology and responding to topology changes is minimized and hence the low average delay and the faster convergence time. In general, a small DIO minimum interval results in a higher energy consumption but a lower delay/convergence time and vice versa. Therefore, there is a need to balance between both cases unless the particular context requires one or the other. For example, in the case of application that detects the problem in a pipeline, which may be essential to avoid disaster like a crack in the infrastructure. In such a case, the energy consumption is of less concern than the speed of the delivery. Thus, the application should opt to set the minimum DIO interval to the least possible value. **Figure 4-31** shows the average churn of the network with varying the minimum DIO interval between 9 and 15. The figure shows that, in general, the churn is not affected by the value of minim interval.

4.5.3 THEORETICAL POINT-OF-DEPARTURE

The performance investigation is based on a theoretical underpinning by the RPL protocol. In addition to that the paper provides a theoretical context around the suitability of RPL for Linear Sensor Networks (LSN) such as the Gas and Oil pipeline networks.

4.5.4 EMPIRICAL DATA COLLECTION METHOD

The paper presents another evaluation work on the strength and drawbacks of RPL, covering the behaviors and performances of three routing metric for calculating the cost of upstream routing for the RPL protocol in a multi segment pipeline. The data collection appears to have been robustly performed with strong practical implementation utilizing OMNET++.

4.5.5 CONTRIBUTION TO KNOWLEDGE

In this paper, the behavior and performance of three routing metric for calculating the cost of routing for the RPL protocol in a multi segment pipeline were evaluated. The study is conducted after the implementation of the RPL protocol in the OMNeT ++ simulator Framework. For the ETX, HOP-COUNT and RSSI metrics, two scenarios have been created by varying the size of packet in the network and the DIO minimum interval. The performance evaluation shows that the ETX metric, has the best performance in terms, of energy consumptions, PDR and throughput in both scenarios. It can be concluded that the ETX is the appropriate metric for applications that need high rates of success in delivering data packets, high reliability and low power.

HOP-COUNT has shown adequate performance in most of the results obtained. It outperformed both ETX and RSSI in terms of delay showing significant delay reduction and faster convergence and thus routing stability is provided. RSSI metric reveals poor results at all levels.

The findings from the evaluation uncover some limitations for the standard under such scenarios provide the guidance with non-trivial value for researchers and designers to create novel theoretical concepts or system protocols or models for better networks.

As of the 16th of September 2021, the article has been read a total of 50 times and recommended 1 time.

4.6 A NEW ENHANCED RPL BASED ROUTING FOR INTERNET OF THINGS

4.6.1 BACKGROUND

As mentioned previously in chapter 3, one of the main issues in relation to the RPL storing mode is that this mode is restricted by storage limitations in the routers along the downward path. In fact, unreachable destination problem may be easily encountered when a router fails, due to memory overflow, to store a routing entry for a target in its associated sub-network. In addition, the under-specification of Downward Advertisement Objects (DAOs) represents another serious issue in RPL. The timing of when and how often DAOs should be emitted is not fully addressed which may lead to inefficient implementations. Motivated by these observations, this study presents an enhanced version of RPL called Enhanced-RPL. In the proposed enhancement, to mitigate the problem of memory overflow of the node's preferred parent, a node is allowed to distribute prefixes belong to its sub-network among multiple parents. In addition, a more cautious approach for emitting DAOs is proposed to mitigate the issue of DAOs under-specification mechanisms. Our simulation experiments demonstrate that the proposed Enhanced-RPL outperforms the RPL standard by an average of up to 64% in terms of control-plane overhead and 30% regarding the packet delivery ratio.

4.6.2 RELEATED WORK

The interest in enhancing RPL mechanisms and operations has grown rapidly since the protocol standardization by IETF community. Despite this growing interest, only a few research studies have focused on enhancing the process of constructing and maintaining the downward routes. For instance, the study in [4] has pointed that maintaining the downward routes is costly in terms of storage utilization and overhead. To mitigate this issue, it was proposed to integrate the reactive query mechanism of The Lightweight On-demand Ad hoc Distance-vector Routing Protocol - Next Generation (LOADng) [5] protocol with the proactive

mode of RPL for maintaining the downward routes. In this case, a network can opt either to use the reactive mode or the proactive mode according to the application requirements.

The work in [6] has proposed an RPL extension, namely, MERPL for enhancing the storing mode scalability. They propose that a node whose routing entries reach a pre-determined factor N should opt to delegate one or more of its children to work as a storing node. The routing entries in the node whose next hop is the selected child should be then deleted from the node's routing table. Also, a DAO containing the destinations reachable by this selected child should be sent to the LBR. Finally, a hybrid approach of storing and non-storing operations is employed when routing the data from the LBR to the other sensor nodes. Another enhancement of RPL called Bounding-Degrees RPL (BD-RPL) is reported in [9]. DB-RPL tries to enhance memory utilization by limiting in-advance the number of next-hop children that a parent can accept to up of k children. A child who has been denied by its preferred parent should select another parent as its new preferred parent.

A totally different mechanism for mitigating the storage limitation problem in RPL storing mode is introduced in [7]. In their proposed scheme, they integrate the multicast dissemination with the storing mode of operation in RPL. All junction nodes (a junction node is a node whose preferred parent has reached its memory limit) should join a special multi-cast group instead so that the LBR would use this multicast address for communicating with the unreachable destinations. The study in [166] has highlighted the problem of interoperability between RPL's storing and non-storing modes of operation. They pointed that the co-existence of the two modes in one physical domain may result in unreachable destination leading to packet forwarding failures. To address this issue, two major changes for RPL standard are introduced. First, they propose that source routing headers should be attached to all nodes configured with storing mode so that they have the capability of working in the non-storing mode when needed [170]. Second, they suggest that all nodes running the non-storing mode of RPL should

advertise their prefixes hop-by-hop rather than the currently used end-to-end approach [170]. Hence, a storing node in the middle of the network would be able to store the routing state of all nodes in its sub-graph. These studies have focused on combining both storing and non-storing modes of RPL or mixing the storing mode of RPL with multicast forwarding. However, as the non-storing mode has its own disadvantages, those would be inherited in the hybrid approach. Moreover, it is worth indicating that none of them has described a mechanism for the timing of the control-plane messages.

4.6.3 THE PROPOSED SOLUTION

In this subsection, the proposed enhancements to downward routing in RPL are presented. In the proposed solution, we consider an LLN where the LBR (DODAG root) is assumed to be unconstrained in terms of memory and computing resources, which is not the case in the associated nodes. Thus, the DODAG root can maintain the routing state for all nodes in its DODAG whereas other nodes can only have up to k routing entries in their routing tables.

4.6.3.1 An Enhanced Storing Mode

The next steps present in detail how the proposed solution builds the upward and downward routes in RPL networks:

1) The upward routes construction goes as specified in the original protocol which is explained in the previous sections. As a result of this process, each node will end up with one preferred parent and probably a list of candidate parents.
2) Each node willing to participate in the downward routing process should sort ascendingly its candidate parents, including the preferred parent, according to their ranks. If two parents have the same rank, then the parents would order based on their announcement order.

3) Once the ordered list of parents has been created, the node should send a DAO to the first feasible parent, which is the parent that still has a capacity to store children in the ordered list advertising its own prefix.
4) Once a parent receives a DAO from one of its children, this parent should either: (i) store the announced prefix in its routing table along with the DAO sender address as the prefix's next hop, and acknowledge the DAO sender with a status of zero to signal the acceptance of this prefix, and finally forward this prefix in turns to the first feasible parent in its own ordered parent list. Alternatively, (ii) it should reject the announced prefix and acknowledge the DAO sender with a status of one to signal the rejection of this prefix.
5) If the prefix announced by a node has been rejected by a specific parent, this node should: (i) lock that parent so that no more prefixes will be directed towards this parent, (ii) select another feasible parent from the ordered list and resend the DAO to this new parent. This process must be repeated until acceptance acknowledgment is received or no more feasible parents in the ordered list are left.

According to the previous steps and as depicted in **Figure 3-6e**, once the DAO announcing the destination F reaches the node B whose routing table is already full, it will send back a rejection DAO-ACK regarding the prefix F to the node D. Upon receiving such a DAO-ACK, D looks for another feasible parent from its candidate parent list, which is the node C in this scenario. Finally, C will forward the received DAO from D regarding the prefix F up the DODAG and to the root A which, in turn, will add it to its routing table.

4.6.3.2 Downward Routes Maintenance

This process begins after constructing the downward routes in the previous stage in order to keep the network state up to date. In fact, at the end of this stage, each node would have one

DIO preferred parent for the upward routing, and one or more a DAO parents for the downward routing (the parent of the node's prefix itself and the parents of prefixes of the node's children). Here, we refer to the parent of the node's prefix as the DAO direct parent, which may or may not be the same as the node's DIO preferred parent. In order to improve the efficiency of the downward routing maintenance process, we opted to limit the number of DAO update transmissions to only few cases which are listed as follows:

1) A node should unicast a DAO message advertising its own prefix to the first feasible parent in its candidate parent list when first joining the DODAG. This parent is referred to as the DAO direct parent, as has been mentioned previously.
2) Until receiving a DAO-ACK, a node should unicast a DAO each time it receives a DIO from its DAO direct parent.
3) A node may use other candidate parents as an alternative option for storing prefixes belonging to its sub-DODAG. Thus, when this node receives a DAO from one of its children, it should forward the received DAO to that children's DAO parent. It should also continue forwarding this DAO each time it receives a DIO until a DAO-ACK is received.
4) When a node changes its DAO direct parent, it should send a DAO to its previous DAO direct parent announcing that it is no more reachable through this parent. It should also keep sending a DAO to its new direct parent each time it receives a DIO from this parent until receiving an acknowledgement.

4.6.4 PERFORMANCE EVALUATION AND DISCUSSION

In this section, a performance evaluation of the proposed scheme is presented in comparison with the standard RPL routing protocol in terms of Packet Delivery Ratio (PDR), energy consumption and control-plane overhead. In this study, the control-plane overhead is defined as the number of DAOs and DAO-ACKs messages that have been transmitted by the

nodes. In RPL, the transmission of DAO-ACKs would be useless as RPL does not specify a mechanism for how to handle their reception. Therefore, we choose to entirely disable the emission of them. In this case, the control-plane overhead would refer only to the number of DAOs transmissions. The evaluation has been carried out by means of Cooja network simulator for Contiki operating system [161], which is the de-facto simulator of IoT devices. Contiki is selected because it has a basic implementation of the RPL routing protocol within ContikiRPL library which has been used as a ground for our enhancements. This allows us to evaluate the exactly executable code that runs on real sensor motes such as Sky motes. The Cooja feature of Unit Disk Graph Model (UDGM) with a transmission range of 25 meters is used to simulate propagation model. Although, using the UDGM may not precisely reflect the real network behavior, the model is still enough to showcase the advantage of the proposed scheme in comparison with RPL as the focus is on efficient storage utilization and not on how efficient the messages are delivered. The Objective Function Zero (OF0) [105] is used for computing the ranks of the sensor nodes and selecting the preferred parent in order to build more stable topology. The MAC and underlying duty-cycling layers are set to the CSMA and ContikiMac protocols respectively. For data model, every node is setup to send an application data packet every minute to the root at random time with a maximum data length of 30 bytes. For each message received at the root, the root should instantly send an acknowledgment reply to the source node. For each setup, we have run 10 experiments with different seeds in order to get statistically solid results with a simulation time of 20 virtual minutes for each experiment.

4.6.4.1 Grid (uniform) Topology

In the first set of experiments, the Enhanced version and the RPL standard are compared in a grid topology where nodes are spread over 100x100m area using a uniform distribution. The LLN border router (LBR) is placed in the middle of the network. **Figures 4-32, 4-33** and 4-**34** present comparisons between the two protocols in terms of the average Packet Delivery

Ratio (PDR), the average control overhead, and the average power consumption respectively as a function of the routing capacity. Here, the routing capacity refers to the number of routing entries that a node can hold in its routing table. As can be observed from **Figure 4-32**, both protocols achieve similar PDR rates when the routing capacity is large enough to accommodate all entries in a node's sub-DODAG. As the routing capacity decreases, also both protocols show degradation in their respective PDR. However, the degradation is more noticeable in the case of the original RPL. For instance, in the worst case scenario (a routing capacity of 4 routing entries), the Enhanced-RPL registered a PDR rate of 0.74%, while RPL has registered a PDR of 0.57 which is much more less than that of the Enhanced version. This is because the nodes in RPL are only allowed to advertise prefixes to only one DAO parent which is its DIO preferred parent. Thus, when that parent runs out of routing entries, it has no choice but to silently drop the new associated children leaving them unreachable from the root point of view.

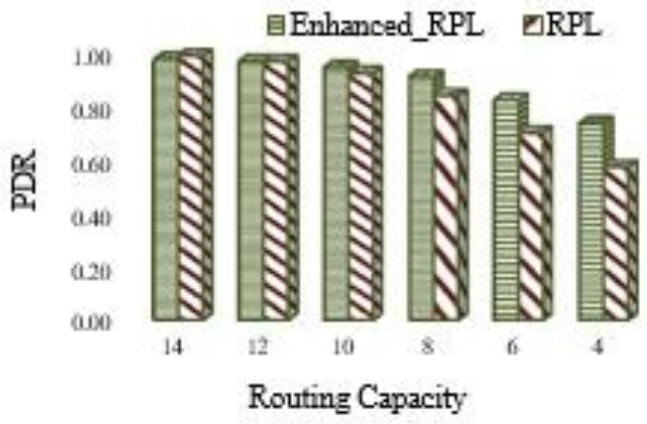


Figure 4-32. The Packet Delivery Ratio of RPL and Enhanced-RPL in Grid Topology

Although Enhanced-RPL delivers more data-plane messages than RPL, this does not result in higher power consumption as depicted in **Figure 4-33**. This can be attributed to the fact that the Enhanced-RPL has lower signaling rates in comparison with RPL. In fact, the Enhanced-RPL has limited the number of cases in which the protocol should send DAOs to only four cases: i) when the node joins the DODAG, ii) when the node receives a DIO from its direct

parent providing that it has recently received no DAO-ACK, and iii) when the node needs to change its DAO direct parent for the purpose of removing the old parent and associating itself to a new one, iv) for forwarding purposes. These enhancement steps have resulted in significantly reducing the number of control-plane messages (DAOs) by up to 64% as shown in **Figure 4-34**. The significant decline in the control-plane overhead has compensated for the energy consumed in delivering more data packets and, hence, the approximately similar curves of power consumption.

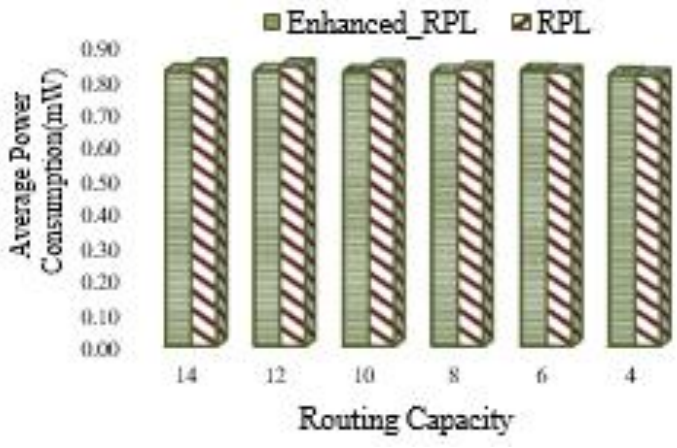


Figure 4-33. The Average Power Consumption of RPL and Enhanced-RPL in Grid Topology

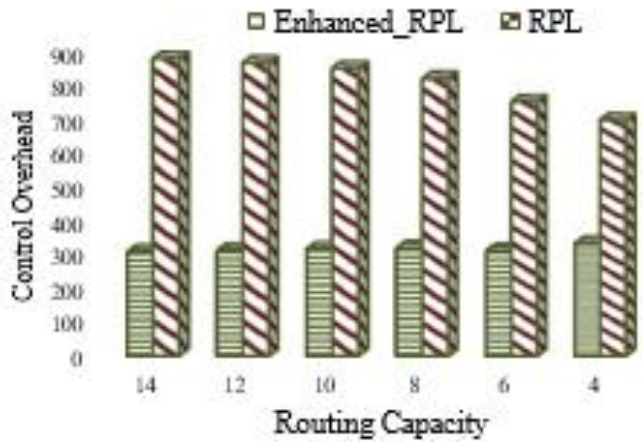


Figure 4-34. The Control Overhead of RPL and Enhanced-RPL in Grid Topology

4.6.4.2 Random Topology

Here, we also evaluate the Enhanced-RPL in a harsher environment where the nodes are distributed randomly over the simulation area. Ten random topologies are also created with different seeds. We verified the case that each node should have at least one parent (neighbor) so that the created topology would be connected, and the two paradigms of communication (sensor-to-root and root-to-sensor) are applicable. Again, both protocols are compared in terms of PDR, control-plane overhead and power consumption which are illustrated in **Figures 4-35**, **4-36** and **4-37**, respectively. It is also clear from **Figure 4-3** that the Enhanced-RPL still has better PDR rates in comparison with RPL, however, not as efficient as the case with the uniform distribution. In the uniform distribution of nodes, a node is guaranteed to have more than one DAO parent at a time, which is exploited by the Enhanced-RPL to distribute its children prefixes among them. However, in a random topology, there are several times where a node ends up with only one DAO parent rendering the node unable to exploit the features of the Enhanced-RPL.

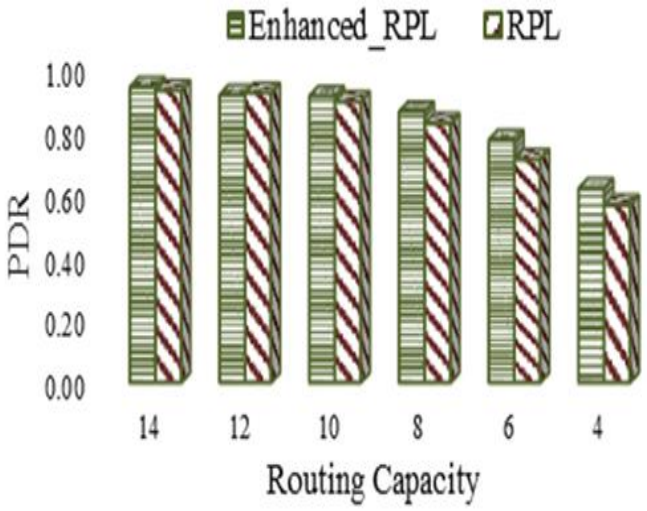


Figure 4-35. The Packet Delivery Ratio of RPL and Enhanced-RPL in Random Topology

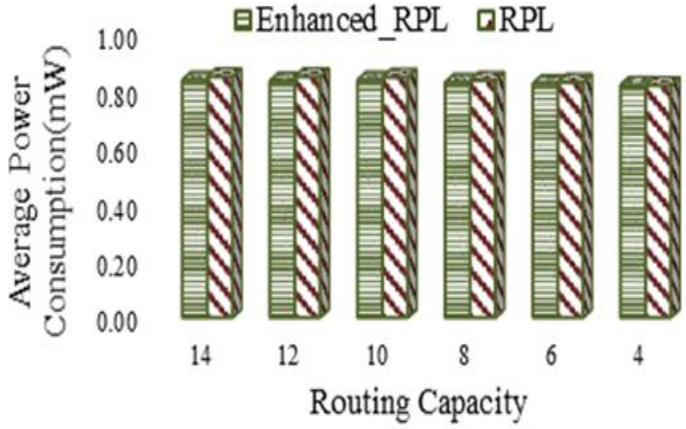


Figure 4-36. The Average Power Consumption of RPL and Enhanced-RPL in Random Topology

Therefore, the efficiency of the Enhanced-RPL in terms of PDR depends mainly on the node distribution and network topology. A network where there is a high probability for a node to have multiple DAO parents will benefit greatly from the Enhanced-RPL and vice versa. This fact does not apply to the control-plane overhead and power consumption as the Enhanced-RPL still shows better results compared to RPL which is justified similar to the case in the uniform distribution.

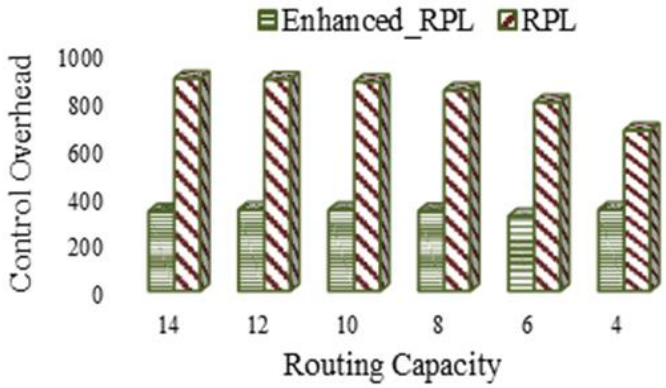


Figure 4-37. The Control Overhead of RPL and Enhanced-RPL in Random Topology

4.6.5 THEORETICAL POINT-OF-DEPARTURE

The paper has a theoretical underpinning that covers the state of art around the limitations of RPL protocol standard highlighting gaps existed in the current solutions and proposing a solution that overcome several reported issues. The work extends the current theory of IPv6 routing protocol with two underpinning advances: an enhanced storing mode, and an enhanced downward route maintenance.

4.6.6 EMPIRICAL DATA COLLECTION METHOD

This paper uses a scientifically solid data collection method, and again through simulation experiments with a rigour methodological approach utilizing a popular OS and simulator, namely Contiki and Cooja to prove the efficiency of the proposed solution with a focus on enhancing IoT networks scalability, energy efficiency, convergence time, load distribution and reliability. The impact of the two proposed theoretical advances have been verified and evaluated with a series of simulation-based tests. The results and analysis confirming the value of the advances and meanwhile suggest for further refinement and improvement.

4.6.7 CONTRIBUTION TO KNOWLEDGE

In this paper, an enhancement of RPL protocol called Enhanced-RPL is proposed that tackles these two specific problems and extensive simulation experiments have been carried out for both protocols comparing their performance in terms of data-plane reliability, control-plane overhead and power consumption. The results demonstrated the validity of the Enhanced-RPL and showed that new mechanism has promoted the reliability of RPL. In the future, we aim at validating the proposed extension efficiency in real testbeds and in networks with different densities.

As of the 16th of September 2021, the article has been read a total of 649 times, citied 11 times and recommended 8 times.

4.7 MITIGATION MECHANISMS AGAINST THE DAO ATTACK ON THE ROUTING PROTOCOL FOR LOW POWER AND LOSSY NETWORKS (RPL)

4.7.1 PROBLEM STATEMENT

The security features of RPL have been investigated extensively in research, indicating that there are some security issues that must be addressed to enable wider adoption of the protocol [8] [14] – [20]. A vital security concern is the DAO (Destination Advertisement Object) attack. This attack functions with the adversary node regularly advertising false DAO messages to its parent nodes, leading to network resource exhaustion as the parent will attempt to update the routing table by flooding the network with the received DAO messages. Thus, the attack will lead to an increase in processing power required to complete the routing table update and the DAOs transmission to parent nodes. Another factor that increases the effectiveness of the attack is that in RPL under storing mode the transmission of DAO messages follows the upward direction towards the sink, and thus the scope of damage increases beyond area of the attacker node [21] [22]. These consequences downgrade the network performance with respect to routing overhead, power consumption, latency and PDR, which significantly shorten the network lifetime [23].

To address this issue, we propose two mitigation techniques and evaluate their efficiency compared to the unsecured version of RPL under wider simulation environments and parameters. The obtained results have demonstrated that our proposed solutions are very effective in mitigating the DAO attack and can upgrade the network performance significantly with respect to power consumption, routing overhead and the packet delivery ratio.

4.7.2 THE DAO ATTACK

DAO messages are used in RPL networks to create the routing paths that will carry the downward traffic from the DODAG root to the respective nodes. The specification of RPL does not define how often and/or when such messages are to be transferred. Therefore, different

implementations of the protocol may opt to propagate DAOs messages differently. For example, the implantation of RPL in [22] have chosen to transmit DAOs periodically with a pre-specified interval while they have been propagated in the Contiki RPL implementation [137] based on the timing of DIO messages. In Contiki RPL, a child node will usually send a DAO to its preferred parent in three occasions: 1) after receiving a DIO from its own parent; 2) when changing the preferred parent; and 3) in the detection of some specific errors. A critical issue here is that a DAO sent by a child node will lead to the transmission of several DAOs equivalent to the number of parents up to the DODAG root. A malicious node may exploit this case to drain the network resources by judiciously and repeatedly transmitting DAO messages to its parent node. One approach to perform this attack is by replaying a DAO sent by a legitimate node by an outsider malicious attacker [20]. RPL's security services deployed by layers underneath such as the cryptographic challenge-response handshake and link layer encryption can be used to mitigate this attack [20]. However, an insider attacker can easily bypass such security mechanisms triggering the need for more efficient solutions [20].

4.7.3 PROPOSED SOLUTION

In order to address the DAO insider attack in RPL, two mitigation mechanisms have been proposed, named SecRPL1 and SecRPL2. These schemes need to be activated at the beginning of the network operations. In SecRPL1, we restrict the number of forwarded DAOs per child. This is achieved by having each parent node count the number of DAOs received from each child node in the parent sub-DODAG. Then the parent node will stop forwarding the child's DAOs when their number exceeds a pre-specified threshold. Hence, during a specific time slot, a node will forward up any received DAO initiated by a specific child until it reaches a pre-specified limit. When reaching that limit, no further DAOs from that child will be forwarded until the end of that time slot. The start and the end of time slot is controlled by the Trickle

timer of DIO messages. In other words, the length of each time slot is equivalent to the length of DIO current interval.

To guarantee that no DAOs will be discarded due to the time factor, we reset the DAO counter at every DIO interval specifically, at the time a parent sends out a DIO message.

In the second scheme (SecRPL2), we restrict the entire number of forwarded DAOs by a specific node regardless of the child node who initiated the DAO. Hence, during a specific time slot, a node will forward up any received DAO until it reaches a pre-specified limit (DAO_FORWARD_MAX). When reaching that limit, no further DAOs will be forwarded until the end of that time slot.

Algorithm 1 DAO Attack Countermeasure 1

```
1:  procedure Initilization
2:      set DAO_For_MAX_PerChild
3:  end procedure
4:  procedure DIO Transmitted
5:      for Each child in the childern list do
6:          child_DAO_Counter = 0
7:      end for
8:  end procedure
9:  procedure Child's DAO Received
10:     if child_DAO_Counter < DAO_For_MAX_PerChild
    then
11:         forward the DAO
12:         child_DAO_Counter ++
13:     else
14:         discard the DAO
15:     end if
16: end procedure
```

Algorithm 2 DAO Attack Countermeasure 2

```
1:  procedure Initilization
2:      set DAO_For_MAX
3:  end procedure
4:  procedure DIO Transmitted
5:      DAO_Counter = 0
6:  end procedure
7:  procedure Child's DAO Received
8:      if DAO_Counter < DAO_For_MAX then
9:          forward the DAO
10:         DAO_Counter ++
11:     else
12:         discard the DAO
13:     end if
14: end procedure
```

4.7.4 Performance Evaluation and Discussion

In this section, we show the effect of the attack on the performance of the network in terms of several metrics, and to demonstrate how our proposed mechanisms can mitigate the DAO attack. A set of experiments have been carried out based on the well-known Contiki, the operating system for IoT devices [137]. Contiki has implementations for IoT communication stack including the standards of RPL, 6LoWPAN, CoAP, and IPv6.

Cooja simulator [140] which emulates exactly the binary on real IoT devices is used in our study to conduct the experiments. This has been exploited to emulate the MSPsim [171] of the Tmote sky platform, a well-known IoT sensor device with a low power IEEE 802.15.4 compliant CC2420 radio chip. The radio protocol (UDGM), Unit Disk Graph Radio Medium, is used to simulate the propagation model. For Link layer, we used the CSMA/CA whereas the ContikiMAC was used as the radio duty cycling (RDC) proto- col. The attack itself (i.e., DAO attack) has been implemented based on the ContikiRPL library within Contiki operating system. In particular, the attack was mounted by having an insider attacker send DAO messages periodically at pre- specified interval to its parent. The number of attackers in our simulation is set to three nodes and the rest of simulation prameters are set according to Table 4-10.

Table 4-10. Simulation Parameters Setup

Parameter Name	Values
Simulation Area	1000 × 1000 m
Number of nodes	50
Simulation time	1800s
Mac/Adaptation Layer	IEEE802.15.4/6LoWPAN
Radio Model	CC2420
Transmission Range (m)	30 m
Interference Range (m)	25 m
Routing Protocol	RPL
Mode Of Operation	Storing mode
Rank Metric	MRHOF
Nominal Capacity	1000mAh
Battery Capacity	1000mAh
Voltage	3 V
Packet Interval	60s
Node Distribution	Uniform Distribution

A periodic data gathering application where sensor nodes send their readings to the DODAG root every minute was simulated at the application layer where the DODAG root sends a reply for each received message as a downward traffic. We simulated a stationary network with 50 nodes, the predominant pattern that you will find in a typical home network. The nodes in our simulation were distributed uniformly in an area of 100m x 100m while the DODAG root is positioned outside the deployment area. The simulation is timed out to end in 30 minutes for each simulated scenario.

The protocols evaluated for each scenario are RPL, RPL with attack (InsecRPL), RPL under attack with first proposed solution (SecRPL1), and RPL under attack with second proposed solution (SecRPL2). In terms of the following metrics:

1) The average number of DAO messages forwarded by the parents in the network (Number of DAOs For- warded).
2) The average power consumption in the network in milliwatts (Power Consumption (mW)).
3) The Packet Delivery Ratio (PDR) of the upward traffic (i.e., from nodes to the DODAG root)
4) The PDR of downward direction (i.e., from the DODAG root to nodes)
5) The average end-to-end delay from nodes to the DODAG root in seconds (i.e., latency of the upward traffic)
6) The average end-to-end delay from the DODAG root to nodes in seconds (i.e., latency of the downward traffic)

4.7.4.1 The Effect of the DAO Attack Frequency

In the simulated scenario, three nodes located at the edge of the deployment area farther away from the DODAG root were selected to run as the attacker nodes as this will ensure covering the vast majority of forwarding paths, a phenomenon that an attacker will prefer to

maximize the damage in the network. The maximum number of DAOs allowed to be forwarded for each child by a parent is set to 10 empirically (i.e., DAOMax threshold). The attack interval, the rate in milliseconds at which the malicious nodes transmit DAOs, is chosen between 250 and 10000 milliseconds. Five runs were conducted for each simulated scenarios under different random seeds for getting statistically solid results which are depicted in the following graphs.

The performance of the network under the simulated scenarios in terms of Forwarded DAO messages and under different attacking intervals is depicted in **Figure 4-38** where the DAOMax threshold per child is set to ten. **Figure 4-38** shows that the overhead of forwarded DAOs in InsecRPL, SecRPL1 and SecRPL2 is higher than that of normal model (i.e., RPL) regardless of the attacking interval value. However, we can also that SecRPL2 has performed better, especially under attack interval of 250 milliseconds, in terms of DAOs overhead compared to other models apart from normal RPL. The same can be said in relation to the power consumption as demonstrated in **Figure 4-39**. This better performance in terms of overhead and power consumption is easily justified by having the parent restricts the number of forwarded messages per child as proposed in our mechanism.

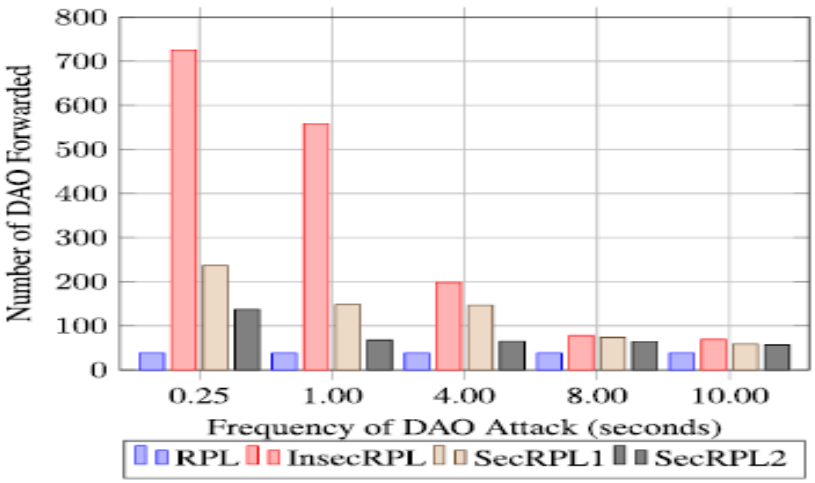


Figure 4-38. DAO's Forwarding Overhead vs Attack Intervals

It can be observed in **Figure 4-39** that the insecure version of RPL has suffered heavily in relation to average power consumption due the attackers being able to flood the network with

large amount of DAOs with no defense mechanism in place. This has been mitigated in both SecRPL1 and SecRPL2 applying the idea of threshold-based security with SecRPL1 showing relatively better performance compared to SecRPL2.

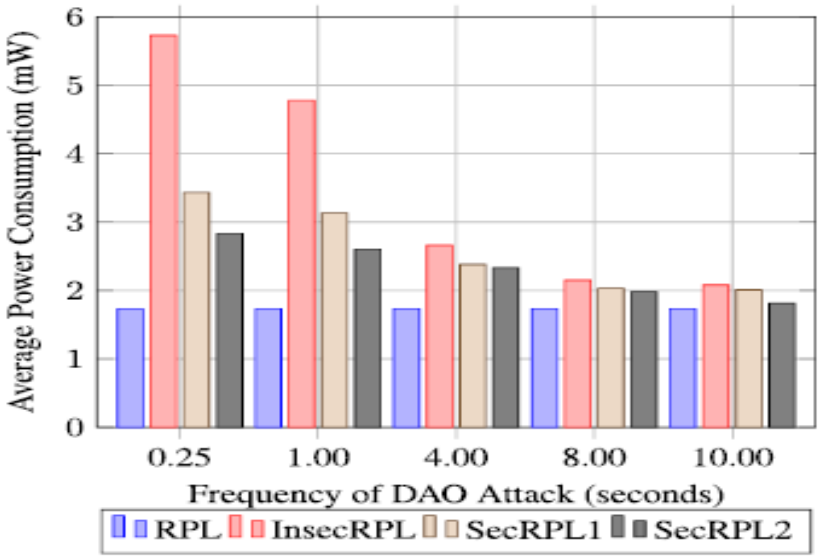


Figure 4-39. Power Consumption vs Attack Intervals

Indeed, the amount of power consumed is calculated in Contiki by adding up the power consumed in four of states of the nodes which are: power consumed in the listening state, power consumed in the idle state, power consumed in the transmission state and power consumed in the running state. Hence, the high overhead in terms of DAOs will surely lead to an increase in the power consumed in the transmission and listening states of the forwarder nodes along the path to the DODAG root, consequently increasing the average power consumption of the network.

The performance of the network in terms of upward latency is shown in **Figure 4-40**, whereas upward latency is depicted in **Figure 4-41**. Similarly, it is evident from figures that the latency in both downward and upward traffic has been adversely affected by the DAO attack. This again can be attributed to high overhead at the forwarder nodes that induces a higher congestion. In the same context, this degradation in the network performance in terms

of latency has been mitigated by applying our mitigation mechanism (i.e., SecRPL1 and SecRPL2) specifically under heavy attacking intervals.

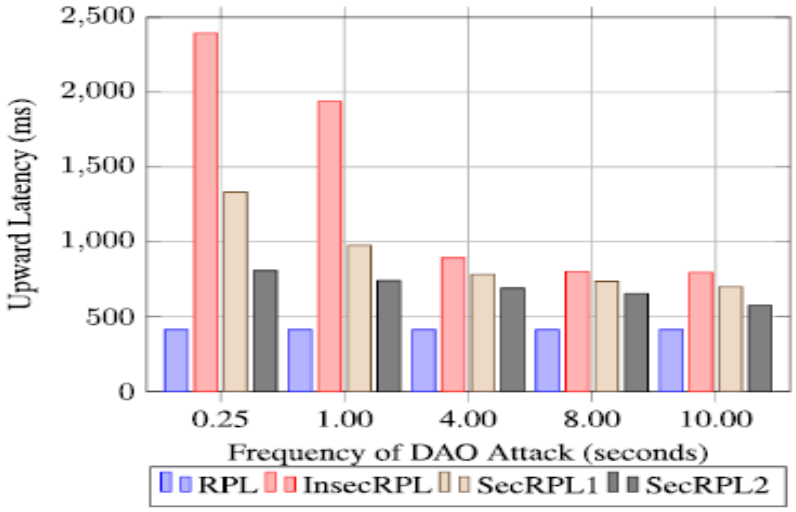


Figure 4-40. Upward Latency vs Attack Intervals

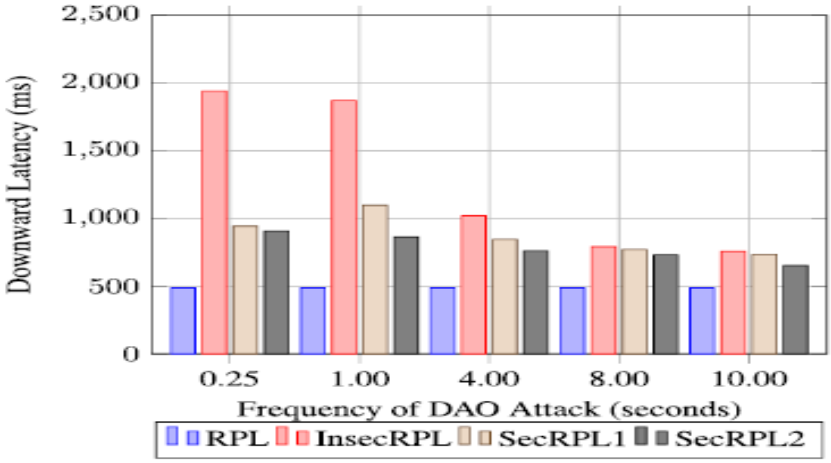


Figure 4-41. Downward Latency vs Attack Intervals

The PDRs of the upward traffic and downward traffic are shown in **Figure 4-42** and **Figure 4-43** respectively. It is again evident from both figures that the PDR in both directions suffer heavily when running the attack under a high attack interval. Note, however, that this may not hold true when mounting the attack under different data rates or topologies. This degradation can be mainly justified by the congestion incurred due to the high overhead at the forwarder nodes under the effect of the attack which again has been alleviated applying our proposed mitigation mechanisms. Both RPLSec1 and RPLSec2 have shown comparable PDR rates in both directions to that of the reference model. The insecure version of RPL (i.e.,

InSecRPL) has experienced the worst results in terms of PDR, with 7% lower than that of the reference model of RPL. Both SecRPL1 and SecRPL2 have managed to enhance the performance in terms of PDR by up 4% and 6% respectively.

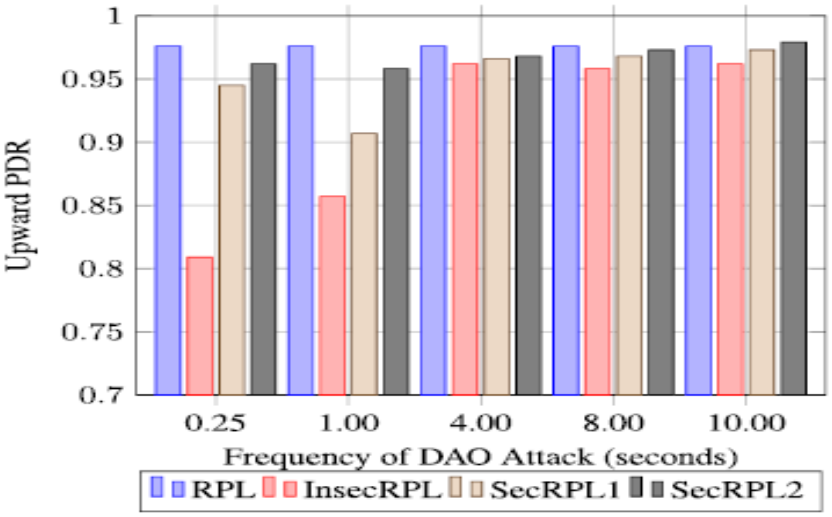


Figure 4-42. Upward PDR vs Attack Intervals

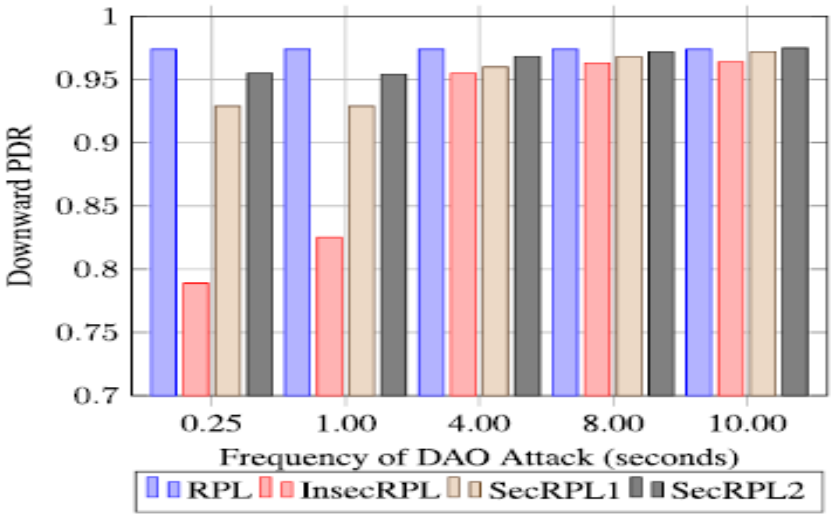


Figure 4-43. Downward PDR vs Attack Intervals

4.7.4.2 The Effect of Increasing the Number of Attackers

In this scenario, the attack will be implemented by increasing the number of attackers, starting with two attackers and incrementing it by two to a maximum of 10. The value of DAOMax threshold in all cases was fixed to 10 in both RPLSec1 and RPLSec2.

The DAO overheads in terms of the average number of forwarded messages per node with different attacking intervals is depicted in **Figure 4-44**. The figure demonstrates that InsecRPL have increased the DAO overhead in comparison with SecRPL2 and RPL. In fact, SecRPL1, SecRPL2 have managed to mitigate the effect of the DAO attack, especially in the case under ten attacking nodes with 76.36% and 205% respectively decrease in the DAO overhead compared to the InsecRPL.

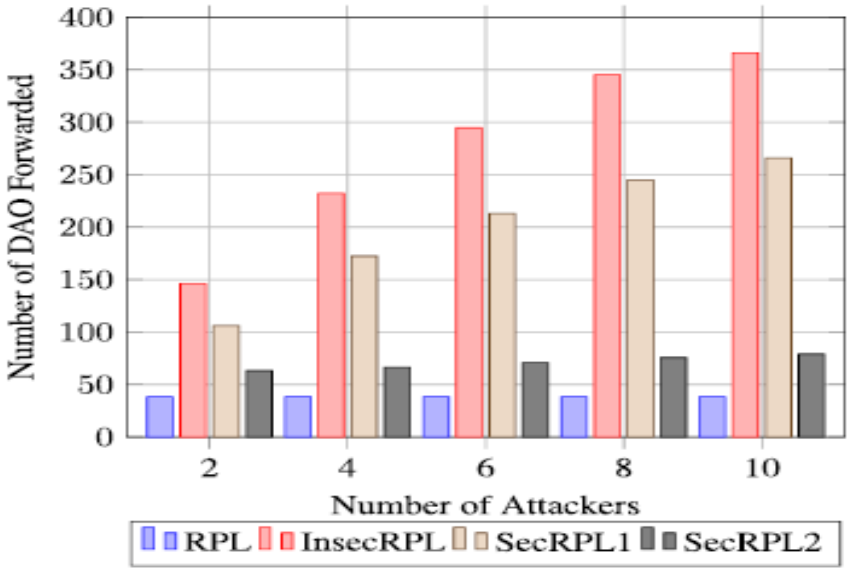


Figure 4-44. DAO Forwarding Overhead vs Number of Attackers

The superior performance of SecRPL2 over SecRPL1 is related to the value of the DAOMax chosen as SecRPL2 can only forward up to 10 DAOs in total in a given interval while SecRPL1 can forward 10 DAOs per destination, hence, the superiority of SecRPL2 over SecRPL1. This has been translated into a decrease in the power consumption under the proposed schemes as depicted in **Figure 4-45** which can be easily justified by the capacity of secure versions of RPL (i.e., SecRPL1 and SecRPL2) to restrict the number of forwarded DAOs per child due to the attack. Both mitigation schemes SecRPL1 and SecRPL2 were able to reduce the effect of the attack by 24% and 87% respectively; however, both consumed more power than the reference network (RPL).

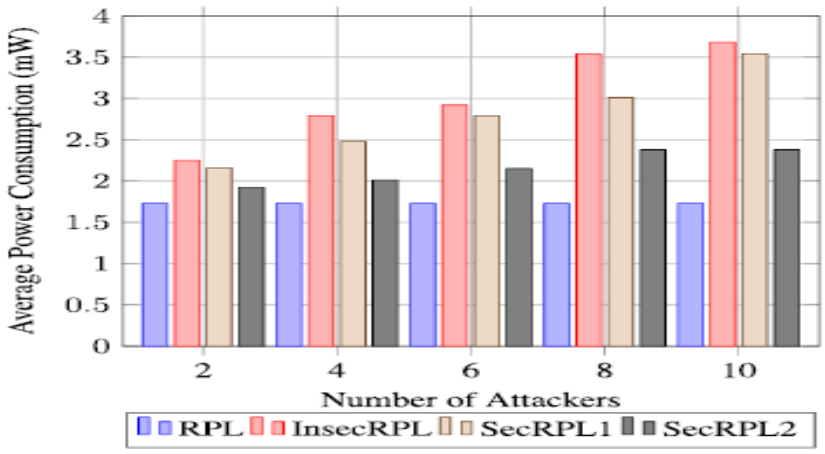


Figure 4-45. Average Power Consumption vs Number of Attackers

Figures 4-46 and 4-47 demonstrate the latency of the upward and downward traffic respectively for protocols under comparison. Similarly, it is evident that the latency has suffered significantly under the attack for both traffic patterns as a result of the significant congestion at the forwarder nodes. SecRPL1 has improved the upward latency by 65.88% and the downward latency by 181.19%. With SecRPL2 both upward and downward latency are greatly reduced outperforming SecRPL1 which can be attributed again to the DAO threshold chosen.

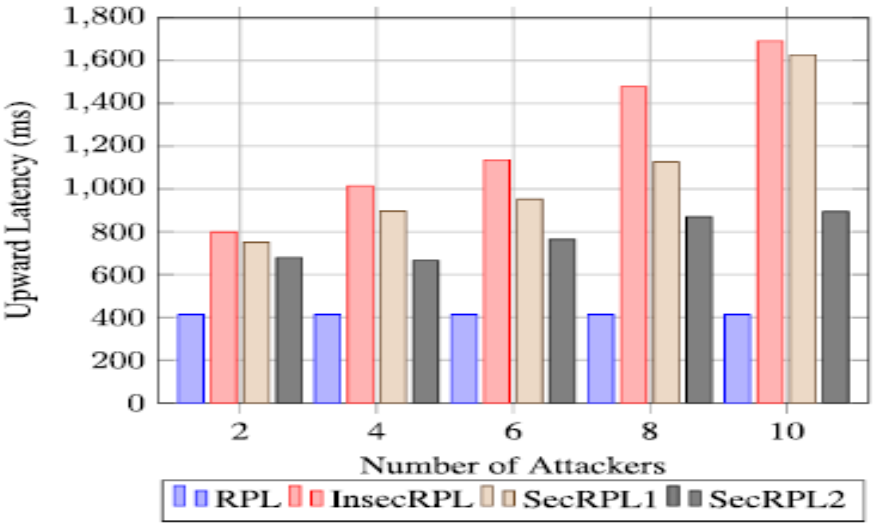


Figure 4-46. Upward Latency vs Number of Attackers

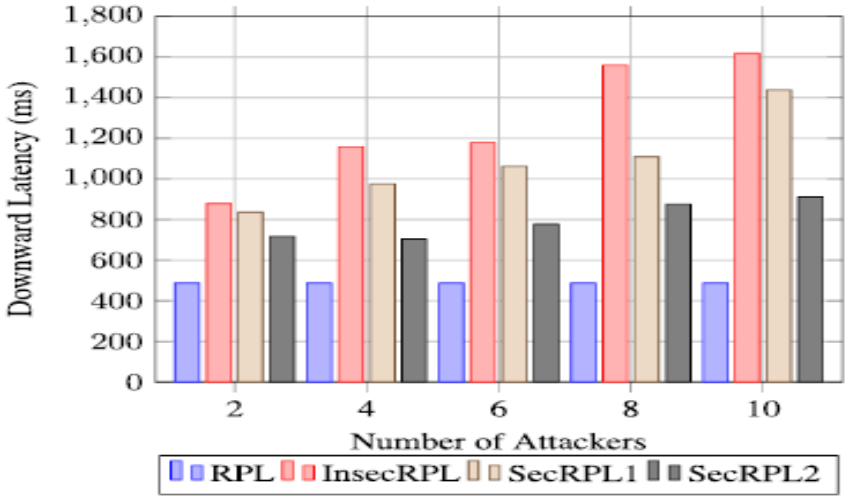


Figure 4-47. Downward Latency vs Number of Attackers

The PDRs of upward and downward traffic for the four models are depicted in **Figure 4-48** and **Figure 4-49** respectively. The figures again demonstrate that the PDRs of both traffic patterns have been affected negatively and the amount of the affect is proportional to the number of the attackers in the net- work, which can be attributed to the congestions experienced by the forwarder nodes. The degradation in the PDR rate has been overcome by the proposed solutions, in which we almost restore the same efficiency of the reference model. From **Figure 4-48 and Figure 4-49**, we can conclude that SecRPL1 has slightly improved PDR over InsecRPL with a 2% increase. SecRPL2, however shows an increase of 3% indicating best performance comparable to the reference model with 3% difference.

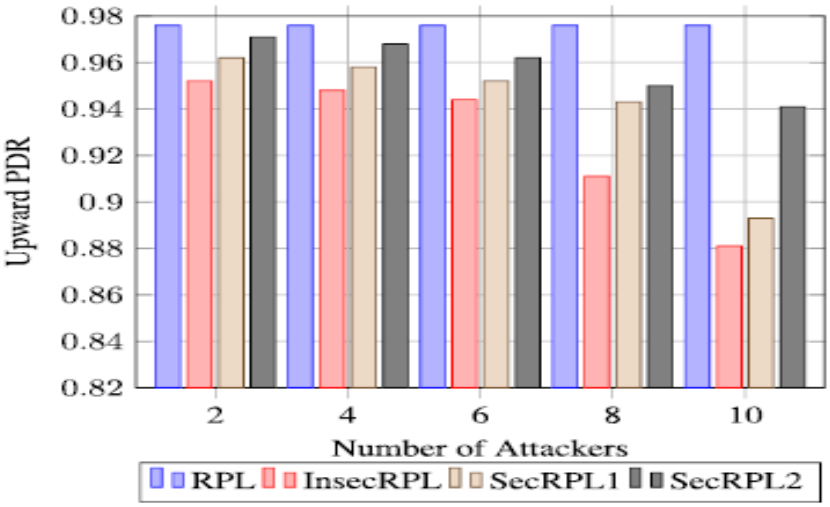


Figure 4-48. Upward PDR Number of Attackers

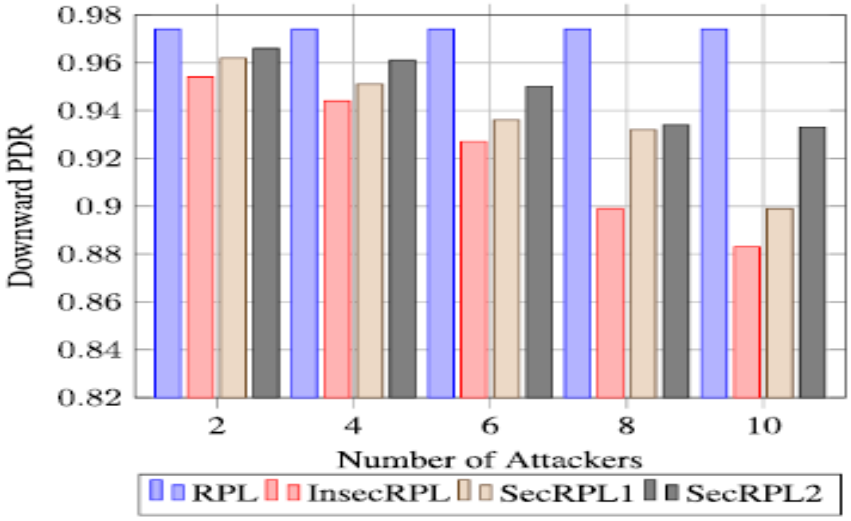


Figure 4-49. Downward PDR vs Number of Attackers

4.7.4.3 The Effect of the Threshold Parameter (DAO-Max)

We also investigated the effect of the threshold value (i.e., DAO threshold Max) on the network reliability in terms of PDR. Intuitively, the smaller the value of the threshold, the lower the DAO overhead and power consumption but at the expense of network reliability. We have depicted how setting the threshold value can affect the performance of the network in terms of mentioned metrics in **Figure 4-50 and Figure 4-51**. It is clear from the figures that selecting a very small value for the threshold has reduced the control overhead and power consumption in both mitigation mechanisms with SecRPL2 again being more efficient in overcoming the effect of the attack, reducing the DAO overhead and the power consumption to up to 48.5% and 18% respectively compared to SecRPL1.

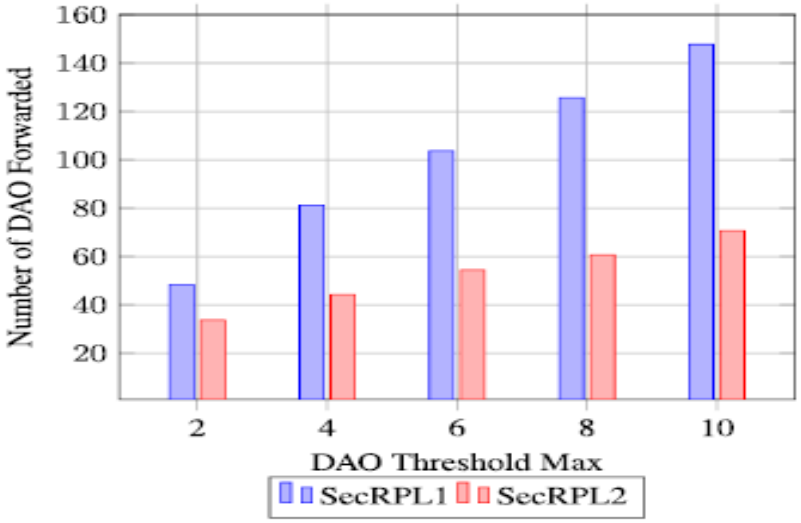


Figure 4-50. DAOs Forwarding under Various DAO Threshold

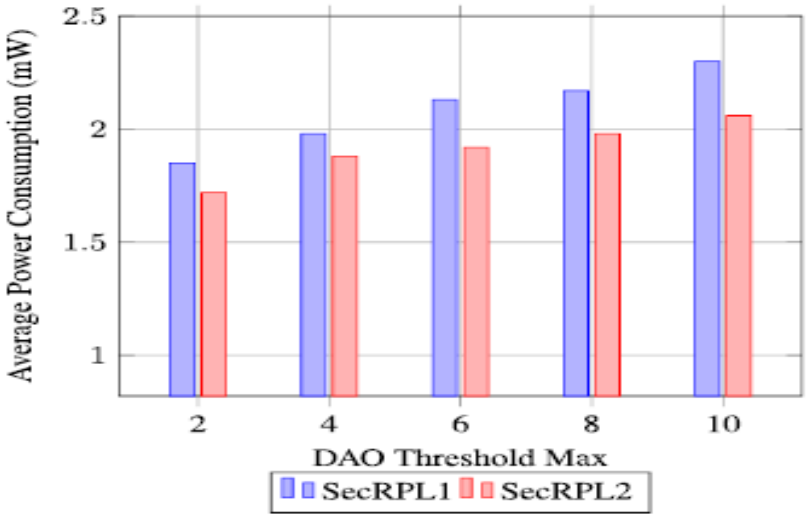


Figure 4-51. Power Consumption under Various DAO Threshold

However, this has impacted the PDR of the downward traffic negatively as illustrated in **Figures 4-52 and 4-53**. This holds true for any value of the threshold less than four. This can be explained easily by the fact that the small value of the threshold will lead into preventing the forwarding of critical DAO messages necessary to build more efficient downward routing paths, hence, the lower PDR of the downward traffic. The figures show also that SecRPL2 performs better than SecRPL1 under both traffic patterns in terms of PDR as the DAO threshold are only restricted partially.

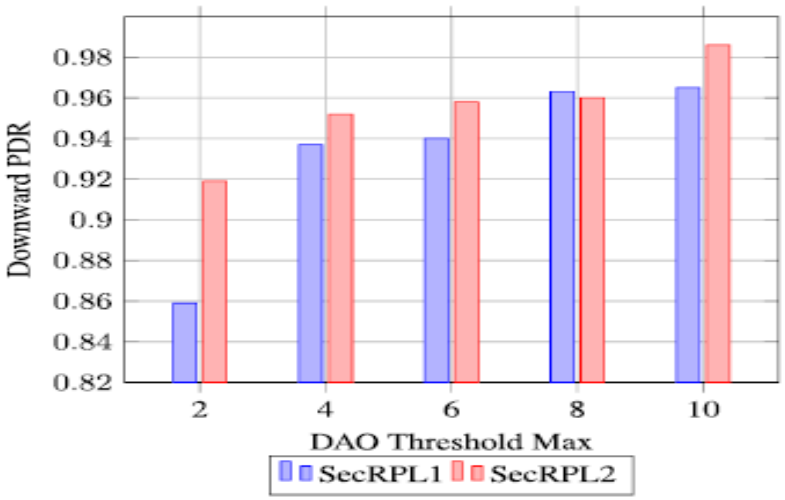


Figure 4-52. Downward PDR under Various DAO Threshold

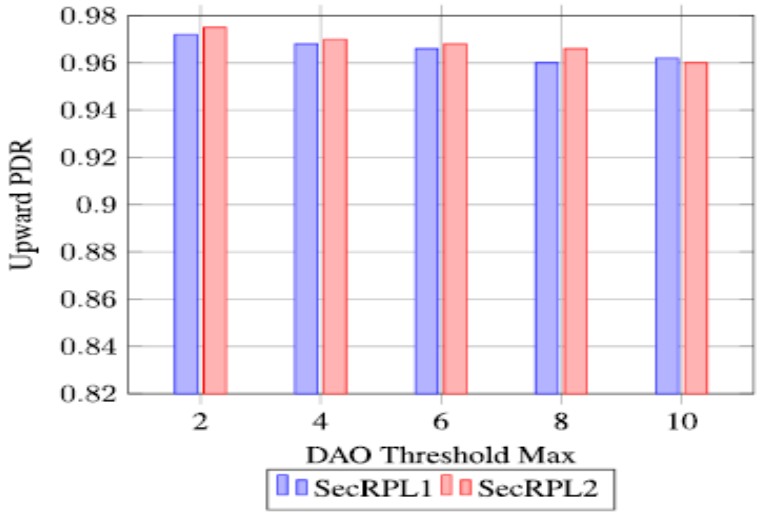


Figure 4-53. Upward PDR under Various DAO Threshold

Figures 4-54 and 4-55, show the effect of both mechanisms on downward and upward latency. It indicates that assigning lower threshold values will reduce the latency. SecRPL2 was able to overcome the effect of the attack, decreasing upward and downward latency much better by 53.57% and 53.71%, respectively in comparison to SecRPL1.

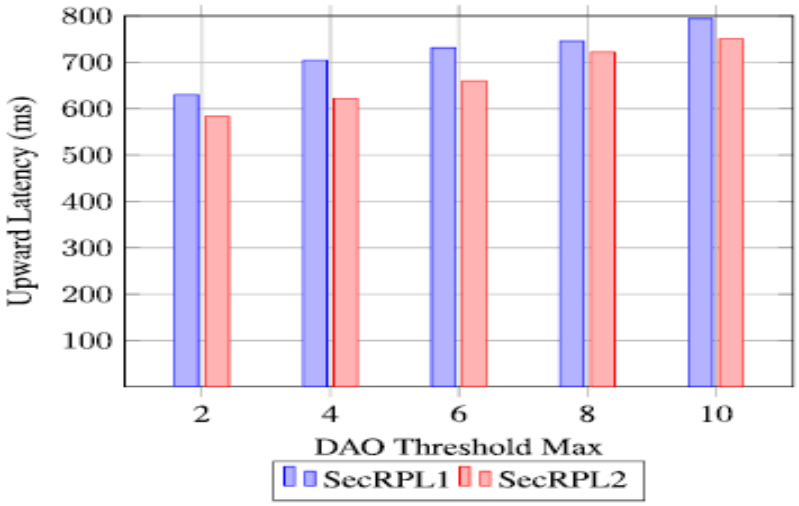


Figure 4-54. Upward Latency under Various DAO Threshold

Figure 4-55. Downward Latency under Various DAO Threshold

4.7.5 CONCLUSION

This paper evaluates the effect of the DAO flooding attack on the network performance in terms of power consumption, packet delivery ratio and latency under different scenarios and operating conditions. The DAO attack can be mounted in IoT networks by having an attacker node transmitting periodically DAO messages to its preferred parent which in turn will forward the received DAOs to its own parent and so on until the DAOs reach the destination, which is the DODAG root. The DAOs in the context of the RPL protocol are transmitted in end-to-end approach (i.e., from sensors to the sink) which makes them different from other RPL's flooding attacks including the DIO and DIS attacks. Hence, not only the immediate neighbors of the

attackers will get affected and harmed by the attack, but also all forwarding nodes to the DODAG root. In fact, an attacker node located at the network edge and transmitting a DAO message will prompt all other nodes in the forwarding path to the DODAG root to forward such a message. The simulation results have shown how the attack can damage the network performance by significantly increasing the DAO overhead and power consumption. The results have also demonstrated that the DAO attack may moderately affect the reliability of the downward traffic under specific conditions. To overcome the effect of the attack, two mitigation mechanisms have been proposed and evaluated showing a good capacity in restoring the optimal performance of the network in terms of the respective metrics.

4.7.6 THEORETICAL POINT-OF-DEPARTURE

The paper contributes to the current state of art with a theoretical advance, i.e., the mitigating security mechanisms against DAO attacks. The paper also has a good theoretical underpinning around reviewing existing security concepts of RPL and the main security issues.

4.7.7 EMPIRICAL DATA COLLECTION METHOD

The paper shows a strong empirical work that has been undertaken here utilizing Cooja and Contiki emulation tools to conduct experiments and collect the results that prove first, the adverse impact of the reported attack on the network and also the efficiency of the proposed solution in mitigating the impact of such an attack.

4.7.8 CONTRIBUTION TO KNOWLEDGE

The paper represents a successful effort in enhancing the RPL protocol in the cybersecurity aspect. The work contributes in problem identification, development of the novel solution, and evaluation of the new solution. It introduces a new mitigation technique against the DAO Attack on the Routing Protocol for Low Power and Lossy Networks (RPL) and evaluates their efficiency compared to the unsecured version of RPL. The obtained results have demonstrated

that the proposed solutions are very effective in mitigating the DAO attack and can upgrade the network performance significantly with respect to power consumption, routing overhead and the packet delivery ratio. This adds a significant contribution to the body of knowledge in this domain.

As of the 16th of September 2021, the article has been read a total of 178 times, and citied 8 times and recommended 7 time.

CHAPTER FIVE CONCLUSION AND FUTURE WORK

This chapter summarises the problems addressed in this thesis, briefly discussing the contributions achieved and their limitations, as well as highlighting the potential avenues for future research.

5.1 THESIS SUMMARY

As the de-facto standard for routing in WSNs, the IPv6 Routing Protocol for Low-power and Lossy networks (RPL) is a promising routing solution that has been advised by the recent studies to be adopted in Gas and Oil networks as they share the same routing requirements and challenges that RPL was standardized for. Thus, this thesis aimed to tackle some of the key gaps of the RPL standard by introducing more efficient and secure routing solutions considering the specific requirements of LLNs as well investigating the most efficient strategies to deploy RPL in LSN.

Guided by the literature review introduced in Chapter 2 and Chapter 3, we have identified three major gaps related to the RPL standard in the context of IoT networks summarized as follows:

1) RPL suffer from scalability problem in its mechanism for constructing the reverse routes from the network's sink to the joined nodes (Downward routes). In addition, the scalability problem is magnified by the fact that the RPL specification does not allow for a node to look for another DAO parent when its current preferred parent runs out of memory. Even worse, RPL does not specify a mechanism to detect such a case. Another serious problem is RPL's under-specification of DAOs timing which may result in conflict and inefficient implementations leading to a poor performance
2) RPL is also restricted by the fact that Gas and Oil network is envisaged to operate in a linearly distributed fashion along the pipeline and limited to a single path to transmit

the data. This restricts the number of hops in the source header to no more than 8 hops. Thus, the challenges associated with network reliability, connectivity and an efficient energy management for sensors is increased

3) The third identified limitation concerns security features of RPL indicating that there are some security issues that must be addressed to enable secure adoption of the protocol. The Destination Advertisement Object (DAO) attack will lead to an increase on processing power required to complete the routing table update and the DAOs transmission to parent nodes. And downgrade the network performance with respect to routing overhead, power consumption, latency and PDR, which significantly shorten the network lifetime.

Chapter 2 presents first contribution of this thesis focused on surveying the provision of WSNs in the oil and gas industry considering the specific requirements of the applications and challenges. Furthermore, a particular attention is given to the existing architectures of efficient mechanisms that fulfil the requirements and overcome the challenges that arise when deploying a WSN in Oil and Gas industry. The comparison of existing solutions is comprehensive and informative for the design and deployment of WSN-based sensor systems, particular valuable for the QoS perspectives such resilience, latency and energy-efficiency.

Chapter 3 presents an overview of RPL's operations, routing selection and optimization mechanisms, routing maintenance. In addition, a thorough analysis of RPL's limitations and security concepts is presented.

Chapter 4 outlines and critically evaluate the contribution of the thesis. In particular, the second contribution that examine the challenges inherent in utilising a mobile sink node by studying the behaviour of RPL in fixed and mobile sink environments by comparing the performance of different scenarios focusing on Latency, Packet Delivery Ratio (PDR) and Energy Consumption. Furthermore, I investigated the extent of average power consumption

between 1 hop and further nodes. Experimental results show major performance differences be- tween fixed and mobile sink environments. Fixed sink LLNs performed better in terms of APC, Latency and PDR therefore it can be stated that RPL designed for fixed environments. The tests exposed some serious issues with sink mobility, such as certain nodes had an excessively high average power consumption, and several nodes were isolated.

The chapter also highlights the third major contribution that investigates the applicability of RPL in the field of Oil and Gas monitoring systems to unleash the challenges and limitations that may appear as result of such adoption. In particular, I evaluate the performance of RPL routing mechanisms in terms of Packet Delivery Ratio (PDR), latency and power consumption under constrained conditions by using different topology types, different number of nodes and different transmission range. The performance evaluations of RPL have concluded that RPL's mechanisms that are used to build topology may suffer from an excessive unbalanced traffic load. As a result, a part of the network may be disconnected, as the energy of the overburdened nodes will be drained much faster than other nodes.

The fourth contribution of this thesis investigates the impact of node placement in a linear sensor network (LSN) by placing the nodes uniformly a long a pipeline. The study based on increasing the distance between nodes, while placing the one sink at the end of the pipeline. The nodes communicate in multi-hop fashion with the same transmission range. For the data forwarding between individual nodes and the sink RPL with Expected Transmission Count (ETX) as an objective function is employed as a routing protocol. The study evaluates the performance in terms of power consumption, throughout, PDR, end to end delay and the Destination Oriented Directed Acyclic Graph (DODAG) construction time. The findings have shown that the increasing of the distance between nodes has important performance implication in terms of the studied quality of service metrics. The shorter the distance between nodes the better the performance is.

The chapter also presents the fifth contribution that identifies the problems at the level of routing in WSN, and a study of specific metrics used to calculate the forwarding cost between nodes in a Multi Segment Linear Pipeline Monitoring WSNs. The performance investigation is based on a theoretical underpinning by the RPL protocol. It presents another solid evaluation work on the strength and drawbacks of RPL, covering the behaviors and performances of three routing metric for calculating the cost of downstream routing for the RPL protocol in a multi segment pipeline.

The sixth major contribution address the issue associated with the scalability of downward routing presented in RPL. An enhancement of RPL protocol called Enhanced-RPL is proposed that tackles these two specific problems and extensive simulation experiments have been carried out for both protocols comparing their performance in terms of data-plane reliability, control-plane overhead and power consumption. The results demonstrated the validity of the Enhanced-RPL and showed that new mechanism has promoted the reliability of RPL.

Finally, Chapter 4 presents major seventh contribution, which addresses the problem of the DAO (Destination Advertisement Object) attack on RPL and its impact on the network performance with respect to routing overhead, power consumption, latency and PDR, which significantly shorten the network lifetime. Two effective mitigating mechanisms are developed to address the DAO attack, SecRPL1, which restricts the number of forwarded DAOs per child; and SecRPL2, which restricts the entire number of forwarded DAOs by a specific node.

The simulation results have shown how the attack can damage the network performance by significantly increasing the DAO overhead and power consumption. It also demonstrated that the DAO attack affects the reliability of the downward traffic under specific conditions. A performance evaluation of the proposed mechanism in comparison with the RPL standard has been also reported demonstrating its efficiency concerning average routing entries, packet delivery ratio and energy consumption.

5.2 FUTURE DIRECTIONS

While the contributions in this thesis have addressed some of the key limitations of the RPL standard, there are still a variety of challenges that need to be addressed. Below are some instructions that are not fully covered in the literature and that could advance the RPL.

5.2.1 MOBILE DAO ATTACKER INVESTIGATION

In this study, we have evaluated the effect of the DAO flooding attack on the network performance in terms of power consumption, packet delivery ratio and latency under different scenarios and operating conditions. To overcome the effect of the attack, two mitigation mechanisms have been proposed and evaluated showing a good capacity in restoring the optimal performance of the network in terms of the respective metrics.

A consideration for future work under such a contribution would be to use a mobile DAO attacker that traverse the network randomly and then investigating whether the developed mitigation mechanisms can still be successful in restoring the normal operation of the network in comparison to the static mobile attacker.

5.2.2 REAL TESTBEDS EXPERIMENTATIONS

The use of simulations to validate the efficiency of network protocols have several advantages over the testbed experiments. For instance, simulations can be easily controlled and configured making it easier to conduct several experiments in a shorter window of time [172]. In addition, simulations enable the modeling of large-scale networks, a task that is very expensive, if not impossible, using real testbeds experimentations [172]. However, simulations do have their own limitations with the main limiting factor is their incapacity to reflect all aspects of real-world scenarios casting some doubts on the trustworthiness of the results obtained. Hence, as a direction for future work, we aim to validate the efficiency of our proposed solutions in this thesis under real testbeds, such as the FIT IoT-LAB testbed [173], with different densities and under a wide range of operating conditions.

5.2.3 DOWNWARD ROUTING EVALUATION UNDER VAROIUS OBJECTIVE FUNCTIONS

The Objective Function Zero (OF0) is used for computing the ranks of the sensor nodes and selecting the preferred parent when evaluating the performance of the downward routing of RPL in this thesis. In addition, the MAC and underlying duty-cycling layers were set to the CSMA and ContikiMac protocols respectively. As a future work, it might be interesting to see the how the downward routing of RPL will be affected by varying the objective functions used such the MRHOF and/or the underlying MAC protocols.

REFERENCE

[1] T. Winter, P. Thubert, A. Brandt, T. Clausen, J. Hui, R. Kelsey, P. Levis, K. Piaster, R. Strike and J. Vasseur," RPL: IPv6 Routing Protocol for Low power and Lossy Networks", RFC 6550, IETF ROLL WG, March 2012.

[2] G. Omprakash, F. Rodrigo, J. Kyle, M. David, L. Philip "Collection Tree Protocol", in Proc. of the 17th ACM Conference on Embedded Networked Sensor Systems (SenSys), Berkeley, California, USA, Nov. 2009.

[3] R. Ma, L. Xing, and H. E. Michel, "Fault-Intrusion Tolerant Techniques in Wireless Sensor Networks," in Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium, 2006.

[4] S. Dawson-Haggerty, A. Tavakoli, and D. Culler, "Hydro: A hybrid routing protocol for low-power and lossy networks," in Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, 2010, pp. 268–273.

[5] T. Clausen, A. C. de Verdiere, J. Yi, A. Niktash, Y. Igarashi, and U. Herberg, "The Lightweight On-demand Ad hoc Distance-vector Routing Protocol - Next Generation (LOADng)," IETF, Draft, Oct 2012.

[6] W. Gan, Z. Shi, C. Zhang, L. Sun, and D. Ionescu, "MERPL: A more memory-efficient storing mode in RPL," in Networks (ICON), 19th IEEE International Conference on, 2013, pp. 1–5.

[7] C. Kiraly, T. Istomin, O. Iova, and G. P. Picco, "D-RPL: Overcoming memory limitations in RPL point-to-multipoint routing," in Local Computer Networks (LCN), 2015 IEEE 40th Conference on, 2015, pp. 157–160.

[8] T. Clausen, U. Herberg, and M. Philipp, "A critical evaluation of the IPv6 routing protocol for low power and lossy networks (RPL)," in Wireless and Mobile Computing, Networking and Communications (WiMob), 2011 IEEE 7th International Conference on, 2011, pp. 365–372.

[9] M. Zimmerling, W. Dargie, and J. M. Reason, “Energy-Efficient Routing in Linear Wireless Sensor Networks,” in 2007 IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems, 2007, pp. 1–3.

[10] T. Clausen, U. Herberg, and M. Philipp, ``A critical evaluation of the IPv6 routing protocol for low power and lossy networks (RPL)," in Proc. IEEE 7th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob), 589 Oct. 2011, pp. 365 372.

[11] J. Vasseur and D. Culler, Routing over Low Power and Lossy Networks 591 (roll), document, IETF Working Group, 2008. AQ: 3.

[12] A. Dvir, T. Holczer, and L. Buttyan, ``VeRA Version number and rank authentication in RPL," in Proc. IEEE 8th Int. Conf. Mobile Ad-Hoc Sensor Syst., Oct. 2011, pp. 709 714.

[13] L.Wallgren, S. Raza, and T. Voigt, ``Routing attacks and countermeasures in the RPL-based Internet of Things," Int. J. Distrib. Sensor Netw. vol. 9, no. 8, Jan. 2013, Art. No. 794326.

[14] M. Landsmann, M. Wahlisch, and T. Schmidt, ``Topology authentication in RPL," in Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), Apr. 2013, pp. 73 74.

[15] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, ``Mitigation of topological inconsistency attacks in RPL-based low-power lossy networks," Int. J. Netw. Manage. vol. 25, no. 5, pp. 320 339, Jun. 2015.

[16] A. Mayzaud, R. Badonnel, and I. Chrisment, ``Detecting version number attacks in RPL-based networks using a distributed monitoring architecture," in Proc. 12th Int. Conf. Netw. Service Manage. (CNSM), Oct. 2016, pp. 127 135.

[17] F. Ahmed and Y.-B. Ko, ``Mitigation of black hole attacks in routing protocol for low power and lossy networks," Secur. Commun. Netw. vol. 9, no. 18, pp. 5143 5154, Oct. 2016.

[18] A. Aris, S. F. Oktug, and S. B. O. Yalcin, ``RPL version number attacks: In-depth study," in Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS), Apr. 2016, pp. 776 779.

[19] D. Airehrour, J. Gutierrez, and S. K. Ray, ``Secure routing for Internet of Things: A survey," J. Netw. Comput. Appl., vol. 66, pp. 198 213, May 2016.

[20] P. Perazzo, C. Vallati, G. Anastasi, and G. Dini, ``DIO suppression attack against routing in the Internet of Things," IEEE Commun. Lett. vol. 21, 620no. 11, pp. 25242527, Nov. 2017.

[21] J. Hui and J. Vasseur, The Routing Protocol for Low-Power and Lossy 58 Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams, document RFC 6553, Mar. 2012.

[22] U. Herberg and T. Clausen, ``A comparative performance study of the routing protocols LOAD and RPL with bi-directional traffic in low power and lossy networks (LLN)," in Proc. 8th ACM Symp. Perform. Eval. Wireless Ad Hoc, Sensor, Ubiquitous Netw. (PE-WASUN), 2011, pp. 73_80.

[23] D. Sharma, I. Mishra, and S. Jain, ``A detailed classification of routing attacks against rpl in Internet of Things," Int. J. Advance Res., Ideas Innov. Technol., vol. 3, no. 1, pp. 692_703, 2017. 628

[24] J. Tripathi, J. de Oliveira and JP. Vasseur, Ed., "Performance Evaluation of the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6687, Oct. 2012.

[25] E. Ancillotti, R. Bruno and M. Conti, "RPL routing protocol in advanced metering infrastructures: An analysis of the unreliability problems," in Sustainable Internet and ICT for Sustainability (SustainIT), Pisa, 2012, pp. 1-10.

[26] T. Clausen, H., and U. Herberg. (2010). Comparative Study of RPL-Enabled Optimized Broadcast in Wireless Sensor Networks, INRIA, and Tech. Rep. 7296.

[27] J. Yi, T. Clausen and Y. Igarashi, "Evaluation of routing protocol for low power and Lossy Networks: LOADng and RPL," in the IEEE Conference on Wireless Sensor (ICWISE), Kuching, 2013, pp. 19-24.

[28] C. Cobârzan, J. Montavont and T. Noël, "Analysis and performance evaluation of RPL under mobility," in the IEEE Symposium on Computers and Communications (ISCC), Funchal, June 2014, pp. 1-6.

[29] S. Elyengui, R. Bouhouchi and T. Ezzedine, "A comparative performance study of the routing protocols RPL, LOADng and LOADng-CTP with bidirectional traffic for AMI

scenario," in the IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Sept. 2015, pp. 561-568.

[30] E. Ancillotti, R. Bruno and M. Conti, "The role of the RPL routing protocol for smart grid communications," in the IEEE Communications Magazine, vol. 51, no. 1, pp. 75-83, Jan. 2013.

[31] T. Clausen and U. Herberg, “Some considerations on routing in particular and lossy environments,” in 1st IAB Interconnecting Smart Objects with the Internet Workshop, Mar. 2011.

[32] A. Parasuram, “An Analysis of the RPL Routing Standard for Low Power and Lossy Networks,” Master’s thesis, EECS Department, University of California, Berkeley, May 2016.

[33] O. Afonso, and T. VazÃ£o. “Low-Power and Lossy Networks under Mobility: A Survey.” in Computer Networks, vol. 107, no. 2, pp. 339–352, Oct. 2016.

[34] H. S. Kim, J. Ko, D. E. Culler and J. Paek, "Challenging the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL): A Survey," in IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2502-2525, Fourthquarter 2017.

[35] X. Liu, Z. Sheng, C. Yin, F. Ali and D. Roggen, "Performance Analysis of Routing Protocol for Low Power and Lossy Networks (RPL) in Large Scale Networks," in IEEE Internet of Things Journal, vol. 4, no. 6, pp. 2172-2185, Dec. 2017.

[36] O. Iova, P. Picco, T. Istomin and C. Kiraly, "RPL: The Routing Standard for the Internet of Things... Or Is It?" in IEEE Communications Magazine, vol. 54, no. 12, pp. 16-22, Dec. 2016.

[37] D. Airehrour, J. Gutierrez, and S. K. Ray, “Secure routing for Internet of Things: A survey,” in Journal of Network and Computer Applications, vol. 66, pp. 198–213, May 2016.

[38] N. Saputro, K. Akkaya, and S. Uludag., “A survey of routing protocols for smart grid communications”, in Computer Networks, vol. 56, no. 11, pp. 2742–2771, Jul. 2012.

[39] J.-P. Vasseur and A. Dunkels, “RPL Routing in Smart Object Networks,” in Interconnecting Smart Objects with IP, 2010, pp. 111–116.

[40] M. Kim, D. Barthel, J. Vasseur, and et al, “RFC6551: Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks,” 2012.

[41] M. R. Akhondi, A. Talevski, S. Carlsen and S. Petersen, “Applications of Wireless Sensor Networks in the Oil, Gas and Resources Industries,” in 24th IEEE International Conference on Advanced Infor-mation Networking and Applications, Perth, (2010).

[42] P. S., S. Doyle, C. Vatland, T. Aasland, T. Tman and D. Sjong, “Requirements, Drivers and Analysis of Wireless Sensor Network Solutions for the Oil & Gas Industry,” in the IEEE Conference on Emerging Technologies and Factory Automation, Patras, (2007).

[43] A. Talevski, S. Carlsen and S. Petersen, “Research Challenges in Applying Intelligent Wireless Sensors in the Oil, Gas and Resources Industries,” in 7th IEEE International Conference on Industrial Informatics, Perth, (2009).

[44] [J. A. GUTIERREZ, “IEEE STD. 802.15.4 - Enabling pervasive wireless sensor networks,” in EATON Corporation, (2005).

[45] I. Jawhar, N. Mohamed, M. Mohamed and J. Aziz, “A routing protocol and addressing scheme for oil, gas, and water pipeline monitoring using Wireless Sensor Networks,” in 5th IFIP International conference on Wireless and Optical Communication Networks, (2008).

[46] S. Husnain, A. Salman, R. Sidra, S. Qaisar and F. Emad, “Reliable monitoring of oil and gas pipelines using wireless sensor network (WSN) — REMONG,” in 9th International Conference System of Systems Engineering (SOSE), (2014).

[47] M. R. Akhondi, A. Talevski, S. Carlsen and S. Petersen., “The role of wireless sensor networks (WSNs) in industrial oil and gas condition monitoring,” in 4th IEEE International Conference, the Digital Eco-systems and Technologies (DEST), April, (2010).

[48] T. Rault, A. Bouabdallah and Y. Challal, “Energy efficiency in wireless sensor networks: A top-down survey,” in Computer Networks, Elsevier, (2014).

[49] A. C. Azubogu, V. E. Idigo, S. U. Nnebe, S. Oguejiofor Obinna and E. Simon, “Wireless Sensor Net-works for Long Distance Pipeline Monitoring,” international Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, (2013).

[50] X. Chao, D. Waltenegus and G. Lin, “Energy model for H2S monitoring wireless sensor network,” in 11th IEEE International Conference on Computational Science and Engineering DOI 10.1109/CS, (2008).

[51] T. Lennvall, S. Svensson and F. Hekland, “A Comparison of WirelessHART and Zigbee for Industrial Applications,” in IEEE International Conference Workshop Factory Communication System, (2008).

[52] 09 2017. [Online]. Available: www.bluetooth.com/Pages/low- energy.aspx.

[53] T. Alhmiedat, “A Survey on Environmental Monitoring Systems using Wireless Sensor Networks,” JOURNAL OF NETWORKS, vol. 10, no. 11, (2015).

[54] 09 2017. [Online]. Available: http://www.ieee802.org/15/pub/TG4.html.

[55] L. CHAARI and L. KAMOUN, “PERFORMANCE ANALYSIS OF IEEE 802.15.4/ZIGBEE STANDARD UNDER REAL TIME CONSTRAINTS,” International Journal of Computer Networks & Communications (IJCNC), vol. 3, no. 5, 9 (2011).

[56] J. J. Q. Wang, “Comparative Examination on Architecture and Protocol of Industrial Wireless Sensor Network Standards,” IEEE Communications Surveys & Tutorials, vol. PP, no. 99, p. pp. 1 – 1, (2016).

[57] W. Liang, X. Zhang, Y. Xiao, F. Wang, P. Zeng and H. Yu, “Survey and experiments of WIA-PA specification of industrial wireless network,” Wireless Communications and Mobile Computing, vol. 11, no. 8, p. 1197–1212, (2011).

[58] S. A Ajith Kumar, K. Øvsthus and L. M. Kristensen, “An Industrial Perspective on Wireless Sensor Networks - A Survey of Requirements, Protocols and Challenges,” IEEE Communications surveys and Tutorials, vol. 16, no. 3, pp. 1391 -1412, (2014).

[59] 09 2017. [Online]. Available: http://www.zigbee.org.

[60] J. Vandana and A. K. Verma, “The Underlying technologies in WSNs: ZigBee vs. Wireless HART,” in 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), (2015).

[61] 09 2017. [Online]. Available: http://www.hartcomm.org.

[62] P. Radmand, A. Talevski, S. Petersen and S. Carlsen, “Comparison of industrial WSN standards,” in 4th IEEE International Conference of the Digital Ecosystems and Technologies (DEST), (2010).

[63] F. Labeau, A. Agarwal and B. Agba, “Comparative study of Wireless Sensor Network standards for application in Electrical Substations,” in Computing, Communication and Security (ICCCS), International Conference, (2015).

[64] A. Remke and W. X, “WirelessHART modeling and performance evaluation,” in 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN, (2013).

[65] T. Rault, A. Bouabdallah, and Y. Challal, Energy efficiency in wireless sensor networks: A top-down survey. Computer Networks, Elsevier, .67, pp. 104-122. (2014).

[66] 09 2017. [Online]. Available: http://www.isa.orgISA100.

[67] J. Werb, “ISA100 wireless applications, technology, and systems A Tutorial white paper.” (2014).

[68] T. Alhmiedat. A Survey on Environmental Monitoring Systems using Wireless Sensor Networks. JOURNAL OF NETWORKS, 10(11), (2015).

[69] A. Nechibvute and C. Mudzingwa, “Wireless Sensor Networks for SCADA and Industrial Control Systems,” International Journal of Engineering and Technology, vol. 3, no. 12, 12 (2013).

[70] T. Lennvall, S. Svensson, and F. Hekland. A Comparison of WirelessHART and Zigbee for Industrial Applications. IEEE International Conference Workshop Factory Communication System, (pp. 85 - 88). (2008).

[71] S. Carlsen, N. StatoilHydro ASA, A. Skavhaug, S. Petersen and P. Doyle, “Using wireless sensor net-works to enable increased oil recovery,” in IEEE International Conference on Emerging Technologies and Factory Automation, (2008).

[72] R. Ma, L. Xing and H. E. Michel, “Fault-Intrusion Tolerant Techniques in Wireless Sensor Networks,” in Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium, (2006).

[73] L. Zhu, B. Zou, H. Zhang, Z. Wang and M. Jiang, “Design of multi-sensor wireless monitoring system and its application in natural gas purification plant,” in IEEE International Conference on Mechatronics and Automation (ICMA), (2015).

[74] B. Deb, S. Bhatnagar and B. Nath, “ReInForM: reliable information forwarding using multiple paths in sensor networks,” in 28th Annu. IEEE Int. Conf. on Local Computer Netw, (2003).

[75] J. Werb and V. B. S. L. D. S. a. M. L. M. Newman, ““Improved quality of service in IEEE 802.15. 4 mesh networks,” in Int. Workshop on Wireless and Industrial Automation, (2005).

[76] A. Willig, K. Matheus and Wolisz A., “Wireless technology in industrial networks,” in IEEE, (2005).

[77] A. Willig, K. Matheus and Wolisz A., “Wireless technology in industrial networks,” in IEEE, (2005).

[78] S. Ivanovitch, L. G. Affonso and V. Francisco, “A new AODV-based routing protocol adequate for monitoring applications in oil & gas production environments,” in 8th IEEE International Workshop of the Factory Communication Systems (WFCS), (2010).

[79] D. Alan, “Optical Fiber Sensors for Permanent Downwell Monitoring Applications in the Oil and Gas Industry,” IEICE Transaction on Electronics, Vols. E83-C, no. 3, pp. 400-404.

[80] S. Zhi, W. Pu, C. V. Mehmet, A. R. Mznah, M. A. D. Abdullah and F. A. Ian, “MISE-PIPE: Magnetic induction-based wireless sensor networks for underground pipeline monitoring,” Ad Hoc Networks, vol. 9, no. 3, pp. 218-227, (2011).

[81] I. Jawhar, N. Mohamed and K. Shuaib, “A framework for pipeline infrastructure monitoring using wire-less sensor networks,” in Wireless Telecommunications Symposium, (2007).

[82] S. Pakzad, G. Fenves, S. Kim and D. Culler, “Design and Implementation of Scalable Wireless Sensor Network for Structural Monitoring,” in New Sensors, Instrumentation, and Signal Interpretation, (2008).

[83] W. Li and Y. Zhu, ““Analysis on leakage detection and location techniques for long transmission Pipe-line,” IEEE Computer Society, vol. 7, no. 3, March (2006).

[84] D. Covas, H. Ramos and A. de Almeida, “Standing Wave Difference Method for Leak Detection in Pipeline Systems,” Journal of Hydraulic Engineering, 13, p. 1106–1116, (2012).

[85] M. Dalbro, E. Eikeland, A. in’t Veld, S. Gjessing, T. Lande, H. Riis and O. Sørasen, “Wireless sensor networks for off-shore oil and gas installations,” in Second International Conference on Sensor Technologies and Applications IEEE (SENSORCOMM), (2008).

[86] M. Hill, M. Campbell, Y. Chang and V. Iyengar, “Event detection in sensor networks for modern oil fields,” in second international conference on Distributed event-based systems, ACM, (2008).

[87] S. Vellingiri, A. Ray and M. Kande, “Wireless infrastructure for oil and gas inventory management,” in 39th Annual Conference of the IEEE Industrial Electronics Society, IECON, (2013).

[88] L. Zhu, B. Zou, H. Zhang, Z. Wang and M. Jiang, “Design of multi-sensor wireless monitoring system and its application in natural gas purification plant,” in IEEE International Conference on Mechatronics and Automation (ICMA), (2015).

[89] A. Nasir, B. H. S. and K. A. Qaraqe, “RFID in-pipe moisture sensing system for oil and gas quality monitoring in Qatar,” in 19th IEEE International Conference on Networks (ICON, (2013).

[90] I. Johnstone, I. Nicholson, B. Shehzad and J. Slipp, “Experiences from a wireless sensor network deployment in a petroleum environment,” in International conference on Wireless communications and mobile computing (IWCMC), New York, USA, (2007).

[91] L. Krishnamurthy, R. Adler, P. Buonadonna, J. Chhabra, M. Flanigan, N. Kushalnagar, L. Nachman and M. Yarvis, “"DesDesign and deployment of industrial sensor networks: experiences from a semi-conductor plant and the North Sea,” in 3rd International Conference on the Embedded Networked Sen-sor Systems (SenSys), ACM, New York, (2005).

[92] M. Z. A. Bhuiyan, G. Wang, J. Cao and J. Wu, “Deploying Wireless Sensor Networks with Fault-Tolerance for Structural Health Monitoring,” IEEE Transactions on Computers, vol. 64, no. 2, pp. 382 - 395, (2015).

[93] N. Mohamed and I. Jawhar, “A Fault Tolerant Wired/Wireless Sensor Network Architecture for Moni-toring Pipeline Infrastructures,” in Second International Conference of the Sensor Technologies and Applications (SENSORCOMM, (2008).

[94] A. Skavhaug, B. Myhre, D. Sjong, M. E., J. Hendrik, D. P. S. M., S. Carlsen and S. .. Petersen, “A Survey of Wireless Technology for the Oil and Gas Industry,” in Intelligent Energy, RAI. Society of Petroleum Engineer, Amsterdam, (2008).

[95] Y. Guo, F. Kong, D. Zhu, A. Şaman Tosun and Q. Deng, “Sensor placement for lifetime maximization in monitoring oil pipelines,” in 1st ACM/IEEE International Conference on Cyber-Physical Systems (ACM), (2010).

[96] C. Obodoeze, F. Ozioko, C. Mba, F. Okoye and S. Asogwa, “Wireless sensor networks (WSNs) in industrial automation: Case study of Nigeria oil and gas industry,” International Journal of Engineering Research and Technology (IJERT), vol. 2, no. 3, pp. 1 - 7, (2013.

[97] K. Pister, P. Thubert, S. Dwars, and T. Phinney, "Industrial Routing Requirements in Low-Power and Lossy Networks", RFC 5673, October 2009.

[98] M. Dohler, T. Watteyne, T. Winter, and D. Barthel, “Routing Requirements for Urban Low-Power and Lossy Networks", RFC 5548, May 2009.

[99] T. Winter et al., “RFC6550: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks,” 2012. [Online]. Available: https://datatracker.ietf.org/doc/rfc6550/.

[100] “IEEE 802.15.4,” 2016. http://www.ieee802.org/15/pub/TG4.html (accessed Mar. 22, 2016).

[101] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, “RFC4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks,” 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4944.txt.

[102] E. J. Hui and P. Thubert, “RFC6282: Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks,” 2011.

[103] J.-P. Vasseur and A. Dunkels, “The 6LoWPAN Adaptation Layer,” in Interconnecting Smart Objects with IP, 2010, pp. 231–250.

[104] IETF, “Routing over Low power and Lossy networks (roll) -.” [Online]. Available: http://datatracker.ietf.org/wg/roll/charter/. [Accessed: 16-Oct-2015].

[105] P. Thubert, “Objective function zero for the routing protocol for low-power and lossy networks (RPL),” RFC 6552, Internet Engineering Task Force (IETF), 2012.

[106] O. Gnawali and P. Levis, “The Minimum Rank with Hysteresis Objective Function”, IETF RFC 6719, Sep. 2012.

[107] G. S. Malkin, “RIP Version 2,” 1998. 10.

[108] S. Douglas J. De Couto, Daniel Aguayo, John Bicket, Robert Morris, “A High Throughput Path Metric for Multi-Hop Wireless Ruting”, in Proc. Of the 9 Annual International Conference on Mobile Computing and Networking (MobiCom), San Diego, Californa, USA, Sept. 2003.

[109] Di Wang, Zhifeng Tao, Jinyun Zhang, Alhussein Abouzeid, “RPL Based for Advanced Metering infrastructure in Smart Grid”, in Proc. of IEEE International Conference on Communications Workshops (ICC), Cape Town, South Africa, May 2010.

[110] L. J. García Villalba, A. L. Sandoval Orozco, A. Triviño Cabrera, and C. J. Barenco Abbas, “Routing Protocols in Wireless Sensor Networks,” Sensors, vol. 9, no. 11, pp. 8399–8421, Oct. 2009.

[111] P. Levis, T. H. Clausen, J. W. Hui, O. Gnawali, and J. Ko, “RFC6206: The Trickle Algorithm,” 2011.

[112] B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani, and L. Mackenzie, ``Addressing the DAO insider attack in RPL's Internet of Things networks," IEEE Commun. Lett. vol. 23, no. 1, pp. 68-71, Jan. 2019.

[113] S. M. Bellovin and R. Housley, ``Guidelines for cryptographic key management," in Proc. Symp. Res. Secur. Privacy, 2005, pp. 1-7.

[114] A. Perrig, J. Stankovic, and D. Wagner, ``Security in wireless sensor networks," Commun. ACM, vol. 47, no. 6, pp. 53-57, Jun. 2004.

[115] A. Le, J. Loo, Y. Luo, and A. Lasebae, ``the impacts of internal threats towards routing protocol for low power and lossy network performance," in Proc. IEEE Symp. Comput. Commun. (ISCC), Jul. 2013, pp. 000789-000794.

[116] A. Kamble, V. S. Malemath and D. Patil, "Security attacks and secure routing protocols in RPL-based Internet of Things: Survey," 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI), 2017, pp. 33-39, doi: 10.1109/ETIICT.2017.7977006.

[117] F. -E. Hachemi, M. Mana and B. A. Bensaber, "Study of the Impact of Sinkhole Attack in IoT Using Shewhart Control Charts," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 2020, pp. 1-5, doi: 10.1109/GLOBECOM42002.2020.9322603.

[118] M. M. Iqbal, A. Ahmed and U. Khadam, "Sinkhole Attack in Multi-sink Paradigm: Detection and Performance Evaluation in RPL based IoT," 2020 International Conference on Computing and Information Technology (ICCIT-1441), 2020, pp. 1-5, doi: 10.1109/ICCIT-144147971.2020.9213797.

[119] K. Prathapchandran, T. Janani. A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest–RFTRUST. Computer Networks. 2021 Oct 24; 198:108413.

[120] A. Sharma, K. Gautam, S. Gurung, R. Bera. Analysis of Wormhole Attack on Network Based on RPL. InAdvanced Computational Paradigms and Hybrid Intelligent Computing 2022 (pp. 607-617). Springer, Singapore.

[121] NZ .Jhanjhi, SN. Brohi, NA. Malik, M. Humayun. Proposing a hybrid RPL protocol for rank and wormhole attack mitigation using machine learning. In2020 2nd International Conference on Computer and Information Sciences (ICCIS) 2020 Oct 13 (pp. 1-6). IEEE.

[122] T. Thiyagu, S. Krishnaveni, R. Arthi. (2022). Deep Learning Approach for RPL Wormhole Attack. In: Hemanth, D.J., Pelusi, D., Vuppalapati, C. (eds) Intelligent Data Communication Technologies and Internet of Things. Lecture Notes on Data Engineering and Communications Technologies, vol 101. Springer, Singapore. https://doi.org/10.1007/978-981-16-7610-9_23.

[123] G. Thamilarasu and S. Chawla, "Towards deep-learning-driven intrusion detection for the Internet of Things," Sensors, vol. 19, no. 9, p. 1977, Apr. 2019.

[124] PP. Ioulianou, VG. Vassilakis, SF. Shahandashti. A Trust-Based Intrusion Detection System for RPL Networks: Detecting a Combination of Rank and Blackhole Attacks. Journal of Cybersecurity and Privacy. 2022 Mar 9; 2(1):124-53.

[125] EG. Ribera, BM. Alvarez, C. Samuel, PP. Ioulianou, VG. Vassilakis. Heartbeat-based detection of blackhole and greyhole attacks in RPL networks. In2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP) 2020 Jul 20 (pp. 1-6). IEEE.

[126] C. Prajisha, AR. Vasudevan. An Intrusion Detection System for Blackhole Attack Detection and Isolation in RPL Based IoT Using ANN. InInternational Advanced Computing Conference 2021 Dec 18 (pp. 332-347). Springer, Cham.

[127] DK. Sharma,SK. Dhurandher, S. Kumaram, KD.Gupta, PK.Sharma. Mitigation of black hole attacks in 6LoWPAN RPL-based Wireless sensor network for cyber physical systems. Computer Communications. 2022 May 1; 189:182-92.

[128] F. Azzedin, H. Albinali. Security in Internet of Things: RPL Attacks Taxonomy. InThe 5th International Conference on Future Networks & Distributed Systems 2021 Dec 15 (pp. 820-825).

[129] DB. Gothawal, SV. Nagaraj. An intelligent and lightweight intrusion detection mechanism for RPL routing attacks by applying automata model. Information Security Journal: A Global Perspective. 2021 Sep 6:1-20.

[130] A. Mayzaud, R. Badonnel, I. Chrisment, and I. G. Est-Nancy, ``A taxonomy of attacks in RPL-based Internet of Things," Int. J. Netw. Secur., vol. 18, no. 3, pp. 459-473, May 2016.

[131] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schonwalder, ``Using the RPL protocol for supporting passive monitoring in the Internet of Things," in Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS), Apr. 2016, pp. 366-374.

[132] A. Verma, V. Ranga. Mitigation of DIS flooding attacks in RPL-based 6LoWPAN networks. Transactions on emerging telecommunications technologies. 2020 Feb;31(2):e3802.

[133] Duroyon, Marin. "STIR: Preventing Routing Table Overload Attacks in RPL-based IoT Networks." (2021).

[134] R. Stephen and L. Arockiam, “RIAIDRPL: Rank increased attack (RIA) identification algorithm for avoiding loop in the RPL DODAG,” Int. J. Pure Appl. Math., vol. 119, no. 16, pp. 459–473, 2018.

[135] AP. Bang, UP. Rao, P. Kaliyar, M. Conti. Assessment of Routing Attacks and Mitigation Techniques with RPL Control Messages: A Survey. ACM Computing Surveys (CSUR). 2022 Jan 18; 55(2):1-36.

[136] AA. Anitha, L. Arockiam. VeNADet: version number attack detection for RPL based Internet of Things. Solid State Technology. 2021 Feb 12; 64(2):2225-37.

[137] A. Dunkels, B. Gronvall, and T. Voigt, ``Contiki-a lightweight and flexible operating system for tiny networked sensors," in Proc. 29th Annu. IEEE Int. Conf. Local Comput. Netw., Nov. 2004, pp. 455-462.

[138] A. Agiollo, M. Conti, P. Kaliyar, TN. Lin, L. Pajola. DETONAR: Detection of routing attacks in RPL-based IoT. IEEE Transactions on Network and Service Management. 2021 Apr 26; 18(2):1178-90.

[139] M. Osman, J. He, F. Mahiuob, M Mokbal, N. Zhu. Artificial neural network model for decreased rank attack detection in RPL based on IoT networks. Int. J. Netw. Secur. 2021 May 1; 23 (3):496-503.

[140] A. Dunkels et al (2006), Contiki-os [Online], Available: https://github.com/ contiki-os/ contiki/tree/master/core/net/rpl.

[141] N. Tsiftes, J. Eriksson, and A. Dunkels, "Low-Power Wireless IPv6 Routing with ContikiRPL," in 9th ACM/IEEE International Conference on Information Processing in Sensor Networks, Apr. 2010, pp. 406-407.

[142] G. Oikonomou et al (2006), contiki-ng [Online], Available: https://github.com/contiki-ng/contiki-ng/tree/develop/os/net/routing.

[143] A. Varga and OpenSim Ltd. OMNeT++ User Manual Version 4.1, 2010. ix, 13, 14, 16.

[144] A. Varga, and R. Hornig. (2008). An overview of the OMNeT++ simulation environment, in Int Conf on Simulation Tools (ICST).

[145] M. Nuvolone. (2010). Stability analysis of the delays of the routing protocol over low power and lossy networks, Master's thesis, Sweden Royal Institute of Technology.

[146] T. Clausen, T. H., and U. Herberg. (2010).” Multipoint-to-Point and Broadcast in RPL,” INRIA, Tech. Rep. 7244.

[147] L. Saad, C. Chauvenet and Tourancheau, B. (2011). ” Simulation of the RPL Routing Protocol for IPv6 Sensor Networks: two cases studies,” In: SENSORCOMM 2011: The Fifth International Conference on Sensor Technologies and Applications. IARIA, pp.128 - 133.

[148] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne and T. Voigt, "Cross-Level Sensor Network Simulation with COOJA," Proc. of the 31st IEEE Conference on Local Computer Networks, Tampa, FL, Nov. 2006, pp. 641-648.

[149] P. Karkazis, P. Trakadas, H. C. Leligou, L. Sarakis, I. Papaefstathiou, and T. Zahariadis, “Evaluating routing metric composition approaches for QoS differentiation in low power and lossy networks,” Wirel. Networks, vol. 19, no. 6, pp. 1269–1284, 2013. S. Hammerseth,

"Implementing RPL in a mobile and fixed wireless sensor network with OMNeT++." pp. 1–101, 2012.

[150] "OMNeT++ Discrete Event Simulator," 2015. [Online]. Available: https://omnetpp.org/. [Accessed: 09-Jan-2016].

[151] G. He, "Destination-sequenced distance vector (DSDV) protocol," Netw. Lab. Helsinki Univ. Technol., pp. 1–9, 2002.

[152] C. Perkings, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector.

[153] [Castalia, "Castalia - Wireless Sensor Network Simulator." [Online]. Available:

[154] https://castalia.forge.nicta.com.au/index.php/en/. [Accessed: 16-Jan-2016].

[155] "MiXiM," Sourceforge.net. [Online]. Available: http://mixim.sourceforge.net/. [Accessed: 18-Jan-2016].

[156] Q. Le, T. Ngo-Quynh, and T. Magedanz, "RPL-based multipath Routing Protocols for Internet of Things on Wireless Sensor Networks," in 2014 International Conference on Advanced Technologies for Communications (ATC 2014), 2014, pp. 424–429.

[157] N. Khelifi, S. Oteafy, H. Hassanein, and H. Youssef, "Proactive maintenance in RPL for 6LowPAN Proactive Maintenance in RPL for 6LowPAN," in Wireless Communications and Mobile Computing Conference (IWCMC, 2015, no. 2015 International, pp. 993–999.

[158] O. Gaddour, A. Koubaa, S. Chaudhry, M. Tezeghdanti, R. Chaari, and M. Abid, "Simulation and performance evaluation of DAG construction with RPL," in 3rd International Conference on Communications and Networking, ComNet 2012.

[159] H. Altwassi, M. Qasem, M. B. Yassein, and A. Al-dubai, "Performance Evaluation of RPL Objective Functions," in IEEE International Conference on Ubiquitous Computing and Communications, 2015, no. October.

[160] Moteiv Corporation, "Moteiv: tmote sky low power wireless sensor module," Tmote Sky Datasheet,2006.[Online].Available:http://www.eecs.harvard.edu/~konrad/projects/shimmer /reference s/tmote-sky-datasheet.pdf. [Accessed: 13-Feb-2016].

[161] Contiki, “Contiki: The Open-Source Operating System for the Internet of Things,” 2015. [Online]. Available: http://www.contiki-os.org/. [Accessed: 09-Nov-2015].

[162] J. Vasseur, M. Kim, K. Pister, N. Dejean, and D. Barthel, “Routing metrics used for path calculation in low-power and lossy networks,” in RFC 6551, pp. 1–30, IETF, (2012).

[163] I. Jawhar, N. Mohamed, J. Al-Jaroodi, and S. Zhang, “Data communication in linear wireless sensor networks using unmanned aerial vehicles,” in 2013 International Conference on Unmanned Aircraft Systems (ICUAS), pp. 492– 499, IEEE, (2013).

[164] I. Jawhar, N. Mohamed, and D. P. Agrawal, “Linear wireless sensor networks: Classification and applications,” Journal of Network and Computer Applications, vol. 34, no. 5, pp. 1671–1682, (2011).

[165] B. Ghaleb, A. Y. Al-Dubai, E. Ekonomou, I. Romdhani, Y. Nasser and A. Boukerche, "A Novel Adaptive and Efficient Routing Update Scheme for Low-Power Lossy Networks in IoT," in IEEE Internet of Things Journal, vol. 5, no. 6, pp. 5177-5189, Dec. 2018.

[166] J. Ko, J. Jeong, J. Park, J. A. Jun, O. Gnawali, and J. Paek, “DualMOP-RPL: Supporting Multiple Modes of Downward Routing in a Single RPL Networks,” in ACM Transactions on Sensor Networks (TOSN), vol. 11, no. 2, pp. 1–20, Feb. 2015.

[167] T. Winter, P. Thubert, A. Brandt, T. Clausen, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, and J. Vasseur, “Rpl: Ipv6 routing protocol for low power and lossy networks. draft-ietf-roll-rpl-19,” tech. rep., Internet Draft, March, (2011).

[168] J. Vasseur and A. Dunkels, “Interconnecting Smart Objects with IP: The Next Internet”, 1st ed., Burlington, MA, Morgan Kaufmann Publishers/Elsevier, Jun. 2010, pp. 1-432.

[169] B. Ghaleb et al., "A Survey of Limitations and Enhancements of the IPv6 Routing Protocol for Low-Power and Lossy Networks: A Focus on Core Operations," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1607-1635, Second quarter 2019.

[170] J. Ko, J. Jeong, J. Park, J. A. Jun, and N. Kim, “Towards full RPL interoperability: addressing the case with downwards routing interoperability,” in Proc. of the 10th ACM Conference on Embedded Network Sensor Systems, Nov. 2012, pp. 353–354.

[171] J. Eriksson, A. Dunkels, N. Finne, F. ¨ Osterlind, and T. Voigt, “Mspsim an extensible simulator for msp430-equipped sensor boards,” in Proceedings of the European Conference on Wireless Sensor Networks (EWSN ’07), Delft, The Netherlands, 2007.

[172] K. Tan, D. Wu, A. Chan and P. Mohapatra, "Comparing simulation tools and experimental testbeds for wireless mesh networks," 2010 IEEE International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Montrreal, QC, 2010, pp. 1-9.

[173] C. Adjih et al., "FIT IoT-LAB: A large scale open experimental IoT testbed," 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Dec. 2015, pp. 459-464.

APPENDICES

7.1 PUBLICATION FOR PHD

Paper[1]	Individual Statement
[1] **Wadhaj, I.,** Kristof, I., Romdhani, I., & Al-Dubai, A. (2015). Performance Evaluation of the RPL Protocol in Fixed and Mobile Sink Low-Power and Lossy-Networks. In Proceedings of the 14th IEEE International Conference on Ubiquitous Computing and Communications (IUCC 2015). ,(1600-1605). https://doi.org/10.1109/cit/iucc/dasc/picom.2015.241	I have acted as the principal researcher responsible for the research methodology, conceptualization, simulation tools, investigation, resources, data curation, writing original draft preparation and presentation
[2] Thomson, C., **Wadhaj, I.,** Romdhani, I., & Al-Dubai, A. (2017). Performance evaluation of RPL metrics in environments with strained transmission ranges. In 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA). https://doi.org/10.1109/aiccsa.2016.7945687.	Isam made a significant contribution to the simulation tools utilized, the analysis of the implementation and the validation of results. As well as supporting the original paper draft and subsequent revised editions.
[3] Ghaleb, B., Al-Dubai, A., Ekonomou, E., & **Wadhaj, I.** (2017). A new enhanced RPL based routing for Internet of Things. In 2017 IEEE International Conference on Communications. , (1-6). https://doi.org/10.1109/ICCW.2017.7962723	I have contributed into the evaluation and writing the paper.
[4] **Wadhaj, I.,** Gharebi, W., Al-Dubai, A., & Thomson, C. (2018). Performance Investigation of RPL Routing in Pipeline Monitoring WSNs. In 20th IEEE International Conference on High Performance Computing and Communications; 16th IEEE International Conference on Smart City; 4th IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2018. https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00178.	I have acted as the principal researcher responsible for the research methodology, conceptualisation, simulation tools, investigation, resources, data curation, writing original draft preparation and presentation
[5] **Wadhaj, I.,** Ghaleb, B., Thomson, C., Al-Dubai, A., & Buchanen, B. (2020). Mitigation Mechanisms Against the DAO Attack on the Routing Protocol for Low Power and Lossy Networks (RPL). IEEE Access, 8, 43665-43675. https://doi.org/10.1109/ACCESS.2020.2977476.	I have acted as the principal researcher responsible for the solution formulation, research methodology, conceptualisation, simulation tools, investigation, resources, data curation, writing original draft preparation and presentation
[6] **Wadhaj, I.,** Ghaleb, B., Thomson, C. (2021). An RPL based Optimal Sensors placement in Pipeline Monitoring WSNs. International Conference on Emerging Technologies and Intelligent Systems (ICETIS 2021).	I have acted as the principal researcher responsible for the research methodology, conceptualisation, simulation tools, investigation, resources, data curation, writing original draft preparation and presentation
[7] **Wadhaj, I.,** Ghaleb, B., Thomson, C. (2021). Wireless Sensor Networks (WSN) in Oil and Gas Industry: Applications, Requirements and Existing Solutions. International Conference on Emerging Technologies and Intelligent Systems (ICETIS 2021).	I have acted as the principal researcher responsible for the research methodology, conceptualisation, simulation tools, investigation, resources, data curation, writing original draft preparation and presentation

7.2 Co-authorship Declaration

Co-authorship Declaration

25th May 2021

Proposal for PhD by Published Works Co-authorship declaration

Title: On Reliable and Secure RPL (Routing protocol Low-power and Lossy Networks) based Monitoring and Surveillance in Oil and Gas Fields.

Authorship

Authorship of publications is co-authorship with Ghaleb, B., Thomson, C, Al-Dubai, A. In these co-authored publications where I (Isam Wadhaj) am the first-author, I have acted as the principal researcher responsible for the research methodology, conceptualisation, simulation tools, investigation, resources, data curation, writing original draft preparation and presentation. Where I am the second and fourth author, I have significantly contributed with formal analysis, validation and writing original draft preparation. The co-authors are willing to be contacted to address any concerns over co-authorship. They have signed this letter to demonstrate their agreement.

Signed: 

Mr. Isam Wadhaj (School of Computing, I.wadhaj@napier.ac.uk)

Dr Baraq Ghaleb (School of Computing, B.Ghaleb@napier.ac.uk)

Dr Craig Thomson (School of Computing, C.Thomson3@napier.ac.uk)

Prof Ahmed Al-Dubai (School of Computing, A.Al-Dubai@napier.ac.uk)