# An intelligent security model for defence against routing attacks on the Internet-of-Things

**LC Sejaphala**

**orcid.org/0000-0003-1321-9557**

Thesis accepted in fulfilment of the requirements for the degree *Doctor of Philosophy in Computer and Information Sciences with Information Technology* at the North-West University

Promoter: Prof FL Lugayizi

Co-promoter: Prof V Malele

Graduation: May 2026

## ACKNOWLEDGEMENTS

I extend my sincere gratitude to the following:

- God in His trinity for health, favour and grace.

- My grandmother and mother, Maria and Matshidiso Sejaphala, friends, and colleagues, for their support during times when discouragement outweighed motivation

- The North-West University's Unit for Data Science and Computing that allowed me to pursue this study. I furthermore appreciate the nGAP programme for its support.

- Professor Francis Lugayizi and Vusumuzi Malele, my promoters, for all their guidance, support, tolerance and encouraging words during my doctoral journey.

## DECLARATION

I, Lanka Chris Sejaphala, declare that this thesis for the Doctor of Philosophy titled, "**An Intelligent Security Model for Defence against Routing Attacks on the Internet-of-Things**" is my own work, and any references to the sources I have cited or used are fully disclosed and acknowledged.

| Approval | Student | Promoter | Co-Promoter |
|---|---|---|---|
| Signature |  | |  |
| Date | 03 March 2026 | | 03 March 2026 |

## ABSTRACT

The Internet of Things (IoT) is fundamentally revolutionising diverse sectors such as agriculture, smart cities, and health, enabling critical applications such as environmental monitoring, military surveillance, and efficient waste management. These pervasive deployments often rely on Low-power and Lossy Networks (LLNs). The network caters for resource-constrained devices which rely on the Routing Protocol for Low-power and Lossy Networks (RPL) to facilitate efficient routing decisions. RPL is a widely used routing protocol designed for LLNs. Its operational integrity hinges on control messages like DODAG Advertisement Object (DAO), DODAG Information Object (DIO), and DODAG Information Solicitation (DIS) control messages, which collectively establish and maintain network topology. However, the limitations of IoT devices, including battery, processing capacity, and memory, as well as the complexities of RPL, make these networks particularly susceptible and vulnerable to various threats. Routing attacks pose a severe challenge to network stability and data integrity. Among these routing attacks, the DIS-flooding attack stands out as the most destructive and resource-consuming threat. The attack specifically exploits RPL's DIS mechanism by overwhelming the network with an excessive volume of DIS messages. Such a disruption can lead to severe resource exhaustion, network congestion, and ultimately, a denial-of-service condition, significantly undermining the reliability of IoT network operations. The urgent need to counteract these sophisticated routing attacks is paramount to safeguarding the functionality of modern RPL-based IoT networks.

Despite the proliferation of security models in the literature for general IoT environments, there remains a significant gap in the implementation of lightweight intelligent security models specifically tailored for RPL-based IoT. Existing solutions often struggle to balance detection efficacy with the stringent resource constraints of LLN devices. This research study’s primary objective is to address this critical gap by implementing a novel, lightweight and intelligent security model designed to effectively detect the DIS-flooding attack with a high detection rate, low false alarm and minimum program flash memory utilisation of the IoT devices. To achieve this, the study adopted a simulation-based quantitative approach. A robust experimental setup was created within the Cooja simulation tool, utilising nodes running the Contiki 3.x operating system. This environment

allowed for the precise implementation of the routing attacks that the study addresses and the generation of a comprehensive dataset under two distinct scenarios: a baseline normal operation and a DIS-flooding attack scenario. This dataset was then meticulously used to build, train, and test six(6) distinct machine learning (ML) algorithms, including Support Vector Machine (SVM), Random Forest (RF), Decision Tree (DT), Multilayer Perceptron (MLP), K-Nearest Neighbours (KNN), and Naive Bayes (NB).

This study contributes three key advancements to the field: a theoretical contribution highlighting the imperative for intelligent and resource-efficient security models in RPL-based IoT; a methodological contribution presenting a robust framework for implementing and evaluating routing attacks within the Cooja simulation environment; and a significant practical contribution underscoring the real-world applicability of the proposed DT-based lightweight and intelligent security model to detect anomalies in IoT networks.

The results of this study demonstrate that a tree-based algorithm, the Decision Tree model, performed significantly well as compared to other evaluated models, showcasing its higher performance with below threshold False Negatives (FN), and a remarkably small model size. Specifically, the DT model achieved an outstanding 98.21% Matthews Correlation Coefficient (MCC), 99.12% accuracy, 99.12% recall, and 98.86% precision, coupled with an exceptionally low 3.79% FN rate. Furthermore, the model required only 4.17 KB of program memory, confirming its suitability for deployment on resource-constrained IoT device.

The novelty of this study lies in the integrated implementation and evaluation of a memory-efficient intelligent detection model directly tailored to RPL-based IoT, validated within a realistic LLN simulation framework. Unlike prior approaches that prioritise detection performance without resource considerations, this work demonstrates that high detection accuracy and minimal memory footprint can be simultaneously achieved in RPL-based IoT environments. The findings provide a practical and scalable pathway toward securing LLNs against DIS-flooding attack, thereby enhancing the resilience of modern IoT networks.

**Key words**-DIS-flooding attack, IoT, LLNs, Machine Learning, & RPL.

# TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | |
|---|---|
| 3D | Three-Dimension |
| AI | Artificial Intelligence |
| ACM | Association for Computing Machinery |
| AODV | Ad-hoc On-Demand Distance Vector |
| AUC | Area Under Curve |
| BLR | Binary Logistic Regression |
| CART | Classification And Regression Tree |
| CoAP | Constrained Application Protocol |
| CIC | Customer In Cloud |
| CSV | Comma-Separated Values |
| DAE | Deep Auto Encoder |
| DANN | Deep Artificial Neural Network |
| DAO | DODAG Advertisement Object |
| DDoS | Distributed Denial of Service |
| DETONAR | Detection of Routing Attacks in RPL-Based IoT |
| DIO | DODAG Information Object |
| DIS | DODAG Information Solicitation |
| DL | Deep Learning |
| DODAG | Destination-Oriented Directed Acyclic Graph |
| DSR | Dynamic Source Routing |
| DS | Decision Tree |
| DV | Distance Vector |
| FN | False Negative |
| GRU | Grated Recurrent Unit |
| HTML5 | Hypertext Markup Language 5 |
| ICMPV6 | Internet Control Message Protocol version 6 |
| IETF | Internet Engineering Task Force |
| ILR | Integrative Literature Review |
| IDS | Intrusion Detection System |
| IEEE | Institute of Electrical and Electronics Engineers |

| | |
|---|---|
| IoT | Internet of Things |
| IPv6 | Internet Protocol Version 6 |
| LoWPAN | Low-Power Wireless Personal Area Networks |
| KNN | K-Nearest Neighbour |
| LAN | Local Area Network |
| LLNs | Low-powered and Lossy Networks |
| LSTM | Long Short-Term Memory |
| MCC | Mathews Coefficient Correlation |
| ML | Machine Learning |
| MLP | Multi-Layer Perceptron |
| NB | Naïve Bayes |
| OSPF | Open Shortest Path First |
| PCAP | Packet Capture |
| QoS | Quality of Services |
| RF | Random Forest |
| RFC | Request For Comments |
| RIP | Routing Information Protocol |
| RL | Reinforcement Learning |
| RO | Research Objective |
| ROLL | Routing Over Low Power and Lossy networks |
| ROC | Receiver Operating Characteristic |
| RPL | Routing Protocol for Low-Power and Lossy Networks |
| RUS | Random Under-Sampling |
| SLR | Systematic Literature Review |
| SMOTE | Synthetic Minority Over-Sampling Technique |
| SVM | Support Vector Machine |
| TPR | True Positive Rate |
| VN | Version Number |
| WSN | Wireless Sensor Networks |

# CHAPTER 1

# INTRODUCTION

## 1.1 BACKGROUND

The IoT network consists of smart connected devices that collect and exchange data with each other within an environment of deployment (Adebayo *et al.*, 2019). This network transmits data to the edge device or cloud application over the internet for further processing. The capabilities of IoT networks enable their adoption for various uses, not limited to smart home, smart grid monitoring and environmental monitoring, but extends to management, patient monitoring, and smart farming (Mosa *et al.*, 2024). One of the enablers of IoT applications is the LLNs. LLNs are made up of a collection of embedded resource-constrained devices, such as sensor-enabled microcontrollers. These microcontrollers have less processing and storage capabilities and are battery-powered, meaning that they have a limited lifespan (Medjek *et al.*, 2021). The LLN devices are crucial to the operations of industrial and environmental applications (Goel *et al.*, 2023). They communicate among themselves via lossy links to discover their neighbours, establish, choose and maintain optimal routes for application data transmission.

The resource-constrained nature of IoT devices renders protocols like Ad hoc On-Demand Distance Vector (AODV), Open Shortest Path First (OSPF), Dynamic Source Routing (DSR), and Routing Information Protocol (RIP), unsuitable (Ankam & Reddy, 2023), as they are not optimised for the resource limitations and unreliable links of IoT networks (Raghavendra *et al.*, 2022). Therefore, the Routing protocol for Low power and Lossy Networks (RPL) was designed and developed to address the limitations of the current routing protocol, similarly providing an efficient routing in the LLN IoT networks (Mali & Govinda, 2023). RPL is the widely adopted standardised distance vector routing protocol for most IoT networks running on resource-constrained devices. RPL ensures energy efficiency, reliability over lossy links, and efficient use of the limited memory and processing power of the network when routing traffic across the network (Alanazi *et al.*, 2025). It builds and maintains a Destination-Oriented Directed Acyclic Graph (DODAG) (Aydın *et al.*, 2024), a tree-like topology that allows child nodes to create routes by attaching themselves to the network through it by exchanging Internet Control Messages

Protocol Version six (ICMPv6) packets, that is, DODAG Information Solicitation (DIS), DODAG Object Advertisement (DOA), DODAG Information Object (DIO) packets (Medjek *et al.*, 2021). RPL can effectively facilitate routing in LLNs; it possesses vulnerable mechanisms that intruders can exploit. Furthermore, the widespread adoption of these networks is an invitation which cybercriminals would never decline. This vulnerability opens up the cyberattack space even more. Cyberattacks within the RPL-based IoT network spectrum target the network functionality layer (layer three), particularly the routing protocols; hence, vulnerabilities of RPL are exploited (A. Almusaylim *et al.*, 2020; Verma & Ranga, 2018).

The Distributed Denial of Service (DDoS) attacks in IoT networks are capable of rendering network nodes, communication channels, and links unavailable, disrupting the normal operations of the network, ultimately impacting the normal operations of the network (Momand *et al.*, 2021). Literature argues that flooding attacks, another type of DDoS, are among the active routing attacks intended to render services of systems unavailable, isolate the victim nodes from the entire network, and also target resources of network devices, such as the battery, by sending a large volume and congesting the network with malicious traffic (Koosha *et al.*, 2022; Nisha *et al.*, 2022). These resource-consuming attacks can be implemented by exploiting the vulnerabilities in the RPL routing protocol (Nisha *et al.*, 2022).

Securing the IoT has become a significant challenge and a crucial issue (Kamaldeep *et al.*, 2021; Mukhaini *et al.*, 2024). In the recent past, a number of mechanisms have been proposed to avert routing attacks in RPL IoT networks. Furthermore, comprehensive reviews such as (Ahmad & Alsmadi, 2021; Al-Amiedy *et al.*, 2022; Sejaphala *et al.*, 2025) provide a cross-sectional synthesis of the proposed techniques in literature, highlighting their strength and weaknesses, areas of improvement and suggesting directions for effective defence techniques suitable for LLN.

In the current era, some of these IoT devices are very small and inexpensive, yet security can be very expensive to deploy through such devices. Moreover, traditional defence techniques cannot provide adequate detection of attacks (Violettas *et al.*, 2021). Defence techniques such as Machine Learning (ML)-based techniques, Intrusion Detection

Systems (IDS), and secure-protocol techniques have been proposed in literature (Laiby & Subramanya, 2021). Trust-based protocols, cryptography, and key management, which are secure-protocol techniques, highlight a remarkably high detection rate, but can be resource-intensive for the network and devices (Rabhi *et al.*, 2023). As such, they fall behind in providing robust security for the LLNs. Traditional IDS (anomaly-based, signature-based, and specification-based) provides a different approach by specifying a network-level deployment to reduce load on the nodes (Pasikhan *et al.*, 2023). However, IDSs are prone to false alarms and require large storage to update a database of reference signatures (Pasikhan *et al.*, 2023) in the case of anomaly-based and signature-based, respectively. Machine Learning-based techniques promise an effective capability in defending IoT LLNs against routing attacks by leveraging network logs as data input (Ioulianou *et al.*, 2022) for classification and precise detection of routing attacks with less network resource consumption. ML-based techniques leverage network performance data for the effective analysis of the IoT network performance for attack detection and accurate predictions (Cakir *et al.*, 2020). Similarly, employing such capability in the security and performance of LLNs is a promising solution, given the nature and characteristics of both the devices and the network.

## 1.2 PROBLEM STATEMENT

The ongoing adoption of IoT networks in distinct use cases, not limited to smart home, smart farming, and environmental monitoring exerts an effect on the increase in cyberattacks which similarly continue to grow at an alarming rate. Cyberattacks disrupt operations and critical network functions (Nisha *et al.*, 2022), affecting the livelihood of persons, organisations and the state whose productivity and functionality rely on the efficient functioning of the network (Bediya & Kumar, 2020). Therefore, network disruptions may inflict compromised personal safety, financial loss and catastrophic implications in specific cases. As IoT networks are not secure in nature, research shows that routing attacks remain a serious risk to IoT networks with limited resources. Routing attacks are known to disrupt normal operations of the network, isolate network nodes, and congest communication channels with bogus traffic (Koosha *et al.*, 2022). This poses a negative impact, where the availability and reliability of these IoT networks are of paramount importance (Sanders & Yau, 2021). These attacks exploit vulnerabilities of

RPL to carry out malicious activities like flooding the network with DODAG Information Solicitation (DIS) packets, dropping data packets, and tampering with network topology to introduce end-to-end delay (Raoof *et al.*, 2019).

A DIS-Flooding attack is an active routing assault aimed at the resources of targeted nodes. The attack is implemented by flooding victim nodes and links with a large volume of DIS ICMPv6 packets. DIS control message packets are one of the ICMPv6 packets used by RPL to establish and maintain optimal routes for IoT applications using Low Power and Lossy Network (Medjek *et al.*, 2021). DIS packets are used for network discovery; a child node wishing to join a DODAG or to change a parent broadcasts DIS packets to neighbour nodes in its transmission range. Any node receiving a DIS broadcasted packet drops any activity and broadcasts DODAG Information Object (DIO) packets and resets its trickle timer (a node's clock mechanism to regulate how often it transmits control messages such as DIO packets). This mechanism presents a vulnerability which can be exploited by intruders who may use a node(s) to transmit large volumes of DIS packets to victim nodes in the network, launching a DIS flooding attack (Pongle & Chavan, 2015). This degrades the performance of the network, affecting the operations, which could potentially lead to harm or catastrophic situations in some cases. As such, this poses a security threat to IoT applications relying on LLNs.

As a result, the extensive use of IoT applications makes the security of their networks extremely vulnerable (Fatima tuz *et al.*, 2019). Numerous defence methods have been suggested in the literature to safeguard RPL-based IoT networks from routing attacks (Pasikhani, Clark, Gope*, et al.*, 2021). The defence techniques can be categorised into three groups: secure-protocol, conventional IDS and ML-based (Jamalipour & Murali, 2022). In recent years, studies incorporating artificial intelligence, especially machine learning, suggest that algorithms based on machine learning offer effective methods for countering attacks (Fatima tuz *et al.*, 2020). Nonetheless, limited focus has been directed towards their implementation in resource-limited IoT networks (Momand *et al.*, 2021).

Consequently, utilising network operational and traffic data to create an intelligent security framework for protecting IoT networks from routing attacks through the implementation of machine learning models becomes a feasible approach to addressing routing attacks.

Machine learning models are recognised for their capacity in identifying patterns in past data to forecast results. Furthermore, ML models promise to detect the presence of a routing attack (Raman *et al.*, 2023) with high accuracy and precision. However, as security is not a one-size-fits-all type of technology, there are identified open research opportunities in the security techniques against routing attacks. Consequently, this research suggests a machine learning approach to protect RPL-based IoT networks from routing attacks, showcasing elevated detection precision, minimal false negatives, and the least utilisation of device program flash memory. This study employs a decision tree classification model, which is a supervised machine learning method noted for its straightforward learning decision rule and low memory usage to identify a DIS-Flooding attack. The research utilises network simulation logs to create a dataset, constructs and trains a decision tree model to identify routing attacks with high detection precision, minimal false alerts, and reduced impact on the program flash memory of the network device.

## 1.3 RESEARCH QUESTION

How can an intelligent machine learning model effectively detect RPL DIS-Flooding attacks in IoT networks while maintaining fewer false alarms?

## 1.4 HYPOTHESIS

An intelligent model based on a decision tree detects DIS-Flooding attacks with over 95% accuracy and introduces less than a 10% false negatives while maintaining low program flash memory utilisation of the IoT devices.

## 1.5 RESEARCH AIM

The research sought to present a safeguard against routing attacks in RPL-based IoT by creating a lightweight intelligent security framework.

## 1.6 RESEARCH OBJECTIVES

i. Theoretical

- TO1: Explore routing attacks on RPL-based IoT to acquire a thorough understanding of their attributes, implementation, and theoretical effects.

- TO2: Review existing security mechanisms in RPL-based IoT to determine their applicability, strength, feasibility, and limitations in defending against routing attacks.

ii. Empirical

- EO1: To explore the influence of routing attacks on RPL-based IoT through experimental assessment of their effect on network performance and resource usage.
- EO2: Examine and evaluate supervised machine learning algorithms for identifying routing attacks in RPL-based IoT, then identify the most effective algorithm for deployment to protect against routing attacks
- EO3: Propose a smart, lightweight security model to combat routing attacks in RPL-based IoT and assess its efficiency and strength

## 1.7 DELIMITATION

This research focuses on the execution of DIS-Flooding attacks and assesses its effects on IoT networks through the Cooja simulation tool, and the development of a security model within a simulated environment for attack detection. Network performance is assessed using key indicators like Packet Delivery Ratio (PDR), End-to-End (E2E) delay, Beacon Interval, and energy usage, providing an assessment of the effects of the DIS-flooding attack. The system comprises sensors, a sink, sniffers, and an edge node. The sensor and sink communicate in a multi-hop mode, utilising the RPL protocol for packet routing, and sniffer nodes capture network traffic and transmit it to the edge device.

A crucial assumption in this study is that sniffers are resource-rich nodes that communicate their data to an edge device via a separate secured network for analysis. Furthermore, the research specifically uses a simulation-generated dataset to build, train, and test six classification machine learning models using the data collected. It is important to state that the identification of the DIS-flooding attack takes place offline following the simulation as the models are not designed for real-time detection. As such, models are evaluated using their size for memory utilisation evaluation rather than real-time RAM

usage, among other performance metrics. Additionally, this study does not include model deployment and mitigation strategies; study relied solely on simulations, and no real network or testbeds were utilised.

## 1.8 SIGNIFICANCE

A Distributed Denial of Service attack threatens the availability and reliability of systems and networks. DDS disrupts their operations by flooding the victims with a large volume of bogus packets. An attack directed at the smart IoT environmental monitoring network could lead to catastrophic outcomes. Literature establishes that the application of intelligent models in IoT networks as a defence technique against flooding attacks is feasible. It promises accurate detection, minimum false negatives and quick response to network threats. The benefits of adopting an intelligent model for IoT security and performance are:

i. Ensured network security
ii. Improved detection accuracy
iii. Reduced false negatives
iv. Reduced memory consumption

## 1.9 CONTRIBUTIONS

A PhD is awarded not for “doing research” alone, but for making an original contribution to knowledge. Contributions can be categorised into three classes: theoretical, methodological, and practical contributions

i. **Theoretical contribution**

   This dissertation shall be accepted in the university library as a contribution to the academic research community. Furthermore, six articles were developed from this study.

   - Five (5) journal articles
   - One (1) conference paper

   The study established that, though security is the main issue in IoT networks and an enormous amount of defence techniques (both conventional and intelligent) are

proposed in literature, there are still open challenges which are not addressed. Most published articles focus on detection accuracy, neglecting the resource consumption of the proposed techniques.

ii. **Methodological contribution**

This study developed an adoptable routing attack and baseline scenario implementation technique. Moreover, it offers a method to assess the effectiveness of machine learning models found in the literature by comparing their performance metric results.

iii. **Practical contribution**

A model based on decision trees can be trained on network operational and traffic data as a security technique with high detection accuracy and fewer false negatives, to realise its effectiveness in detecting routing attacks.

## 1.10 CHALLENGES

The study simulated two network scenarios: the first to mimic a DIS-Flooding attack and the other as a baseline scenario for comparison, collected network logs, transformed them into datasets, and developed an intelligent defence model against routing attacks. However, simulating a large network scenario for a longer time was not feasible. Consequently, the study focused on medium-sized network simulations. Moreover, it would be intriguing to evaluate the model on a testbed IoT network logs dataset. Access to an IoT testbed is still a major challenge among scholars in the area of security and performance of IoT networks. In this regard, several testbeds have been identified for future research.

## 1.11 STRUCTURE OF THE STUDY

This research study consists of six chapters: introduction, literature review and related works, methodology, results and discussion, cross-article and synthesis, and lastly the conclusion chapter.

**Chapter 1**

This introductory chapter highlights the importance of securing LLNs against routing attacks and the feasible adoption of intelligent models. The chapter outlines the problem statement of the study, the research aim, the research question and objectives, as well as the dissertation structure.

**Chapter 2: Literature Review and Related Work**

Extending from Chapter 1, this second chapter provides a summary of the IoT and its applications, a routing protocol suited for resource-constrained devices and routing attacks exploiting its vulnerabilities, potential machine learning algorithms and related work.

**Chapter 3: Methodology**

The chapter offers an overview of research methodology to place the study within the context of research design. This chapter presents the research paradigm, research design, and various research methods utilised.

**Chapter 4: Results and Discussion**

This chapter presents the findings of this study, which covers the exploration of different defence techniques in the literature, the design of an implementation framework and the development of an intelligent defence model against routing attacks in IoT.

**Chapter 5: Cross-article synthesis**

This chapter presents a cross-sectional synthesis of published work from this study. It amplifies a coherent flow of findings presented in the articles and further highlights the contributions and the alignment of the articles to the specific research questions of this research.

**Chapter 6: Conclusion**

The conclusion chapter, being the last chapter of this dissertation, terminates the research by summarising the study, encompassing the recommendations arising from the specific objectives of the study. This chapter further aggregates major findings and highlights the limitations of this research.

## 1.12 CHAPTER SUMMARY

This chapter provided an in-depth overview of the research, highlighting the IoT networks and applications, and a brief overview of the vulnerabilities of RPL that DIS-Flooding exploit to transmit a large volume of DIS packets. The chapter underscores the significance of addressing the security of the IoT networks, leveraging their operation and traffic data logs to create a technique utilising machine learning for identifying routing attacks to enhance the network's availability and dependability. The next chapter presents the overview of the study, diving deeper into IoT networks, the RPL protocol and related work.

# CHAPTER 2

# LITERATURE REVIEW AND RELATED WORK

## 2.1 INTRODUCTION

This literature review chapter evaluates the work done in recent years by experts in the domain of performance and security of the IoT network. It first presents an overview of the IoT paradigm, extending to its use and applications. Further, the chapter reviews the RPL protocol and its operations in ensuring efficient routing and routing attacks that can exploit vulnerabilities of the network to disrupt its normal operations. Lastly, the chapter reviews related works, highlighting strengths, weaknesses, and contributions of each study.

## 2.2 INTERNET OF THINGS OVERVIEW

These smart interconnected systems, highlighted in Section 1, include the IoT, which is described as resource-constrained tangible devices that are fitted with sensors, software, processing power, and additional technologies that allow them to link and share data with other devices via the internet (Rani *et al.*, 2022). IoT encompasses diverse applications, including transportation and logistics, smart farming, smart grids, and smart factories as illustrated by Figure 2-1.

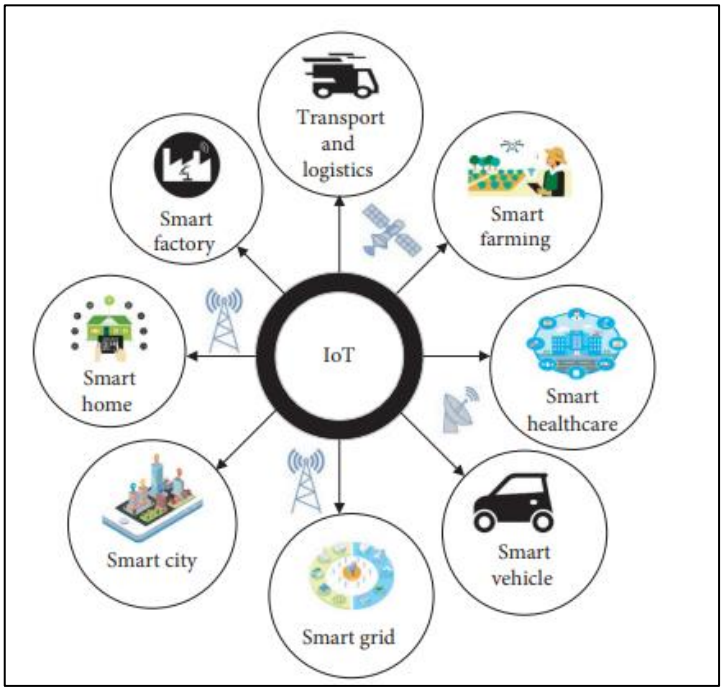


**Figure 2-1:** Applications enabled by IoT networks (Mehmood *et al.*, 2021)

IoT devices are expanding swiftly, directly impacting human lives, and assisting sectors such as manufacturing, logistics, and healthcare in making important decisions. The IoT sector is projected to exceed $2.4 trillion in annual revenue by 2027. This encompasses the increase in IoT devices from $8 billion in 2019 to $41 billion in 2027 (Ahmad & Alsmadi, 2021). The IoT has delivered considerable advantages to 21st century lives, communities, and sectors. Considering the uses of IoT, many IoT devices are limited in resources (minimal onboard memory, reduced energy, and low processing power) and are anticipated to run for extended durations; therefore, energy-efficient protocols are preferred.

In industrial and environmental monitoring, IoT is characterised by a large deployment of LLNs with communication connections that exhibit minimal throughput and significant packet loss. These features render cutting-edge routing protocols such as Ad-hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Open Shortest Path First (OSPF) unsuitable for LLNs. To address these limitations in the mentioned protocols in the LLNs, a set of standardised protocols is proposed, which includes Internet Protocol version 6 (IPv6) for Low-Power Wireless Personal Area Networks (IPv6LoPWAN) for the adaptation layer, IEEE 802.15.4 PHY/MAC for physical and Data Link Layer, Constrained Application Protocol (CoAP) for application layer, and RPL for network layer. In using the auto-configuration tendency of IPv6, new IoT devices can connect to existing networks easily through RPL, a network-layer routing protocol. This feature attracts attacks to hamper the network and disrupt its normal functionalities (Verma & Ranga, 2018).

## 2.3 ROUTING PROTOCOLS

Routing Protocols are sets of rules and algorithms used by network devices (such as routers or nodes in a wireless sensor network) to identify the best route for network traffic to traverse from an origin to a target. They enable the sharing of routing data among devices, supporting the construction and maintenance of routing tables that dictate how data packets should be forwarded. Routing protocols play a crucial role in guaranteeing effective, dependable, and scalable communication in wired and wireless networks, such as the internet and Local Area Networks (ANs), and wireless sensor networks (WSNs). Routing protocols are classified into three categories that is, the Distance Vector (DV),

Link State and Hybrid. DV are suited for simpler networks, allowing nodes to share their routing table with neighbours, using metrics like hop count and link quality. Link State, is suitable for larger networks; it allows nodes to share information about their directly connected links, building a complete network topology map. The Hybrid combines the two approaches with reactive and proactive capabilities.

Distance Vector (DV) protocols determine the best path for data transmission based on the distance (e.g., hop count or cost) to a destination, with each node sharing its routing information with its neighbours. In IoT mesh networks, particularly LLNs, routing protocols are adapted to address challenges such as energy efficiency, limited resources, and dynamic topologies. There are several routing protocols in the DV category that establish and maintain routes for application data traffic transmission and control message exchange in IoT applications running on mesh networks. This includes Ad-hoc Distance Vector Routing Protocol (AODV), and Routing Information Protocol (RIP)

## 2.4 RPL ROUTING PROTOCOL

The RPL is the de facto common network layer routing protocol for LLN IoT (Hachemi *et al.*, 2020). This RPL was standardised in 2012 as RFC 6550 by the Routing Over Low-power and Lossy Networks (ROLL), a working group of the Internet Engineering Task Force (IETF) (Verma & Ranga, 2018). The RPL has become widely recognised in both industry and the academy due to its capability to deliver effective routing among resource-limited smart IoT nodes with IPv6 support, QoS provision, and adaptability to various network structures. The RPL employs energy-efficient methods to facilitate self-organisation and self-healing in response to common node failures. Moreover, ensuring effective routing for IPv6 packets, these features of RPL promote its application in IoT solutions operating on the LLN framework.

The RPL uses Destination Oriented Directed Acyclic Graph (DODAG) to build a tree topology which consists of a parent and two child nodes. The RPL consists of three control messages: DODAG Information Solicitation (DIS), DODAG Information Object (DIO), and DODAG Advertisement Object (DAO). When a new node aims to join an RPL-based IoT network, it transmits a DIS to determine the availability of the DODAG. The root node regularly sends out DIO, and any node that wants to join the DODAG uses the

DIO information to calculate and establish its rank. The node adds the sender node to its parent list, and broadcasts the DIO. DAO is utilised to disseminate information needed to facilitate downward traffic toward offspring (Gawade & Shekokar, 2017). Nonetheless, the RPL is susceptible to routing assaults targeting IoT, including attacks like DIS-flooding, rank, sinkhole, and worst parent, among others. These attacks exploit the RPL protocol feature to disrupt the operations of the networks (Wallgren *et al.*, 2013).

## 2.5 ROUTING ATTACKS

Routing attacks target to disrupt functions of the network by exploiting some existing vulnerabilities in the network (Seth *et al.*, 2021). In RPL-based IoT, these attacks can be divided into three groups e.g., resource consumption, network traffic and topology attacks. Resource consumption attacks aim at consuming network resources such as energy, and bandwidth, whereas traffic attacks aim at eavesdropping and/ or dropping network traffic packets while topology attacks disrupt normal functionality of the RPL.

This study addresses the most destructive and catastrophic routing attack in RPL-based IoT - the DIS-flooding attack (Nisha *et al.*, 2022). This DIS-flooding attack affects the operations and functionality of the network, including resource consumption and potentially disrupting data traffic.

DIS-flooding attack: This takes advantage of the unlimited number of DIS that a node can send until it gets DIO. Malicious node(s) can exploit this vulnerability by repeatedly multicasting DIS control messages to its neighbour. The neighbours in the range immediately respond to the DIS and send DIO messages, thinking there is an inconsistency. The victim nodes also repeatedly reset their Tricker Timer after every DIS received, resulting in a rise in control message overhead and total energy usage (Garba, 2022). Furthermore, this results in the formation of loops, the use of an unoptimised path, a decrease in PDR, and an increase in E2E delay (Ioulianou *et al.*, 2022). This causes delays and routing loops in the IoT running the RPL routing protocol (Garba, 2022). Table 2-1 outlines the impacts of DIs-flooding attacks on IoT systems based on RPL.

Table 2-1: Features impacted by routing attacks in IoT networks.

| ***Attack*** | ***Data traffic*** | ***Delay*** | ***Network resource*** | ***Routing Delay*** | ***Packet Loss*** | ***Topology*** |
|---|---|---|---|---|---|---|
| *DIS-Flooding* | √ | √ | √ | √ | √ | √ |

## 2.6 MACHINE LEARNING

ML is a branch of Artificial Intelligence, which is recognised as the most suitable computational paradigm to have revolutionised the IoT environment (Hussain *et al.*, 2020). Variance of ML algorithms helps businesses and industries to grow by learning from model behaviour and utilises the models for classification or prediction without human intervention (Jahangeer *et al.*, 2023).

Machine learning algorithms can be grouped into four categories: supervised, unsupervised, semi-supervised and reinforcement learning algorithms. Supervised learning trains from labelled data; unsupervised learning uses unlabelled data; semi-supervised learning is used in cases where labels are not present in the majority of rows in the data. Reinforcement learning gets rewarded for correctly interacting with the environment. In IoT networks, machine learning can integrate intelligence into the system for multiple objectives. These include security, especially attack detection and mitigation (Zahra *et al.*, 2022). This study explores some of the supervised machine learning algorithms as security models against IoT routing attacks guided by the literature.

## 2.7 RELATED STUDIES

The network layer is tasked with delivering functionality by choosing an optimal route to target network packets for different types of systems, including IoT (Nisha *et al.*, 2022). Attacks in this layer are meant to disrupt the functionality of the network. Therefore, an intelligent and lightweight security model demonstrating high detection and minimum false alarms is of crucial in mitigating this. The work in (Gothawal & Nagaraj, 2023) proposes a lightweight and intelligent IDS model based on finite automata to reinforce the security of the RPL routing mechanism.

### 2.7.1 Works on DL and ML

(Ahmadi & Javidan, 2024) propose a trust-based technique using Long Term Short Term Memory (LSTM), a deep learning model, to detect blackhole, selective forwarding and rank attacks using a dataset generated from NetSim simulations with 16 nodes (Agiollo *et al.*, 2021). Furthermore, the work in (Al Sawafi *et al.*, 2023) also utilised a publicly available dataset, IoTR-DS, to evaluate the performance of supervised Deep Artificial Neural Network (DANN) and semi-supervised Deep AutoEncoder (DAE) in detecting DIS-flooding, rank and wormhole attacks. The proposed model achieves an accuracy of 98% and an F1-score of 95% which outperformed SVM, LSTM, KNN, and J48 (DT). However, in the two studies mentioned, the memory utilisation of the proposed models is not presented.

According to (Krari *et al.*, 2024), simple traditional models provide a quick response time. In their study, Krari and colleagues compared the performance of LSTM, DNN, and SVM using a dataset generated from a Cooja simulation scenario with 20 nodes to detect DIS-flooding attack. Their findings suggest that LSTM outperformed both SVM and DNN, achieving a 99.99% accuracy. These results highlight that SVM tops all models in terms of training time, which suggests its suitability. The two studies (Sharma & Yadav, 2024) and (Krari *et al.*, 2024), achieve high accuracy but the false alarm results of the suggested model are not shown. The models are contrary to this research, which presents the false negative outcomes of the models, among other performance metrics of the models. Aydin and colleagues evaluated the performance of eleven and two DL models in detecting four routing attacks (Aydın *et al.*, 2024). With bagging, a tree-based model outperforms all models, including a neural network DL model, achieving a 99% accuracy, precision, and recall. A study (Alanazi *et al.*, 2025) compared two DL models (GRU & LSTM) to detect five routing attacks using a Cooja simulation-generated dataset, where LSTM outperformed GRU by achieving 95% accuracy. The study also adopted the GRU DL model to detect seven routing attacks, including the DIS-Flooding attack (Bokka & Sadasivam, 2023). The model achieved 95% accuracy, 94% precision, and 81% recall. Though DL demonstrates acceptable results, however, according to literature (Sejaphala *et al.*, 2025), the benchmark for average accuracy, precision, and recall is 95% and above. DL's performance from the synthesised studies falls exactly at the threshold.

Moreover, FN and model sizes results are not presented, which, however, are significant performance metrics more especially in LLNs and the severity of having a compromised node in the IoT applications.

### 2.7.2 Works on ML models

The work in (Wakili *et al.*, 2024) evaluates and compares five (5) models and suggests RF as the best detection model to enhance RPL security and QoS, achieving an accuracy and precision of 99% each and a 92% F1-score. The study further adopts and integrates a Reinforcement Learning (RL) module into RPL for flexible and adjustable routing based on the outcomes of RF. The study (Sharma & Yadav, 2024) also utilised the IoTR-DS dataset to implement and compare the performance of RF, MLP, KNN, SVM and DT in terms of accuracy to detect DIS-flooding, and other disruptive routing attacks. The study then proposes RF with a higher accuracy of 98%. Though the model achieves desirable outcomes, the question of model size still stands.

(Abdulkareem *et al.*, 2024) propose an IDS adopting a tree-based algorithm that is RF, DT, & extra trees to build a stacking ensemble learning model. Using the IRAD dataset, the authors reported an accuracy, precision, and recall of 99%, demonstrating the effectiveness of ML in detecting DIS-flooding, VN, and decreased rank attacks. Demonstrating the superiority of ensemble learning models, Rabhi and colleagues furthermore compared and stacked SVM, NB and DT to implement an ensemble learning model, which achieved a 98% accuracy and precision with 0.006% FP (Rabhi *et al.*, 2022). RF and KNN ML models have been compared to detect four routing attacks, where the models achieved 99% & 98% accuracy, respectively (Mosa *et al.*, 2024). Furthermore, Wang and others, in their study, compared five ML models: KNN, NB, LR, DT and RF (Wang *et al.*, 2024). Where RF outperformed other models by achieving an 89% accuracy, the study further compared performance of their proposed model against publicly available datasets like IoT-Sentry, RLP-NIDDS17, and WSN-DS, and the model performed well with the simulation-generated dataset.

Studies demonstrate that traditional ML models, more especially RF, KNN, DT, SVM and NB, continue to dominate the integration of ML in the security of the IoT network to safeguard and detect routing threats. However, most of these studies do not display the

size of the models, which is a crucial metric, more especially when the model is intended for utilisation in IoT devices with limited resources.

Tables 2-2 and 2-3 present a comprehensive summary of the synthesised studies. Table 2-2 demonstrates the proposed technique, strengths and limitations, dataset source, tools used to collect the dataset, and size of the network, including the number of malicious nodes presented for each study.

Table 2-2 Summary of related work: Strengths and limitations

| **Ref** | **Technique** | **Model** | **Strength** | **Weakness** | **Dataset** | **Tool** | **NWS** |
|---|---|---|---|---|---|---|---|
| (Wakili *et al.*, 2024) | ML | RF | 99% accuracy | Memory utilisation is not presented | NA | NA | 50-x |
| (Ahmadi & Javidan, 2024) | DL | LSTM | Multiple attack scenarios | Memory utilisation is not presented | public | NetSim | 16-x |
| (Al Sawafi *et al.*, 2023) | DL | DANN | 98% accuracy | Memory utilisation is not presented | public | OMNET++ | 100-16 |
| (Sharma & Yadav, 2024) | ML | RF | 98% accuracy | FN & memory utilisation are not presented | public | NA | NA |
| (Krari *et al.*, 2024), | DL | LSTM | 99% accuracy | FN and memory are not presented | simulated | Cooja | 20-x |
| (Rabhi *et al.*, 2022) | ML | Ensemble | 98% accuracy | Model size not presented | Simulated | Cooja | 24-x |
| (Aydın *et al.*, 2024) | ML | Bagging | 99% accuracy | Model size is not presented | Public | ROUT-4-2023 | - |
| (Alanazi *et al.*, 2025) | DL | LSTM | 95% accuracy | FN & model size not presented | Simulated | Cooja | - |
| (Bokka & Sadasivam, 2023) | DL | GRU | 95% accuracy | Model size not presented | Simulated | NetSim | 20-2 |

Furthermore, Table 2-3 presents outcomes of the performance metrics derived from the synthesised studies. The results demonstrate that most studies did not display the MCC, FN and model size results, which, in contrast to this study, MCC, FN and model size results are presented.

Table 2-3 Summary of related models' performance metrics

| Ref | Accuracy | Precision | Recall | MCC | FN | Model size | Model |
|---|---|---|---|---|---|---|---|
| (Wakili *et al.*, 2024) | 99 | 99 | 100 | - | - | 10KB | RF |
| (Al Sawafi *et al.*, 2023) | 99 | 98 | 99 | - | - | - | DANN |
| (Sharma & Yadav, 2024) | 98 | 95 | 90 | - | - | - | RF |
| (Krari *et al.*, 2024) | 99 | - | - | - | - | - | LSTM |
| (Abdulkareem *et al.*, 2024) | 99 | 99 | 99 | - | - | - | Ensemble |
| (Rabhi *et al.*, 2022) | 98 | 98 | 98 | 98.5 | - | - | Ensemble |
| (Aydın *et al.*, 2024) | 99 | 99 | 99 | - | - | - | bagging |
| (Alanazi *et al.*, 2025) | 99 | - | - | - | - | - | LSTM |
| (Bokka & Sadasivam, 2023) | 95 | 94 | 81 | - | - | - | GRU |

### 2.7.3 More proposed techniques

A study (Ioannou & Vassiliou, 2020) proposed a local agent to accurately detect the sinkhole attack on the IoT. The research investigated the practicality of utilising local information and agents to identify malicious nodes. The proposed system utilised three types of local agents as anomaly detectors, namely support vector machines, binary logistic regression, and a threshold. In their finding, it was evident that the threshold-based detection approach performed poorly. However, SVM, which was implemented as a local agent and binary logistic regression within the node's operating system yielded favourable outcomes in identifying sinkhole attacks. Nevertheless, the research failed to show the network's scale and the quantity of malicious nodes(s). The proposed implementation of binary logistic regression in a resource-constrained network like LLN cannot be a viable solution in detecting the attack, as it utilises memory and introduces computation overhead. Contrary to their study, we use a packet sniffing tool and an IDS

to detect the network layer attacks, taking into consideration resource constraints on the network.

In RPL, the intruder's exploit is the rank attribute. The rank indicates a node's position in the network in relation to the root node. It serves as a key factor in selecting parents in RPL networks. (Choukri *et al.*, 2020) employed deep learning to identify the occurrence of rank attack in RPL. They suggested an IDS utilising the Multi-Layer Perceptron (MLP) neural network to authenticate and categorise normal and abnormal traffic. The proposed system achieved 94.57% in accuracy, 98% in F1 score, and 100% recall using a dataset of 852. Although the study demonstrates acceptable results in detecting, it is unclear what the outcomes would be in medium to large-sized network datasets. In this research, we consider a medium-sized network with more than four hostile nodes to assess the strength of our suggested algorithm.

Multiple attacks impact different elements of the network. Some attacks affect control traffic, while some other affect data traffic. There are other attacks that target the resources of nodes. It is desirable to use data from multiple layers to detect attacks in IoT. (Alam *et al.*, 2022) suggested a machine learning method to identify attacks in IoT, utilising multi-layer data. Authors utilise Python CICflowmeter in the architecture to extract features for every packet received by the root node. While features are being extracted, no new packet is sent to the CICflowmeter. This is time-consuming and could lead to a bottleneck on the root as it would be receiving a large volume of packets from the nodes in a medium-sized network. Although the approach seems feasible, it is clear that they have a very small network of 5 nodes. However, in a medium-sized network, the robustness of the proposed approach remains in question.

It is of great importance to identify appropriate feature selection methods to yield good performance metrics. (Nandhini *et al.*, 2022) proposed a comparative study for feature selection methods to classify RPL-based IoT attacks utilising ML models. The study evaluated the performance of KNN, Gaussian Naïve Bayes and SVM to classify RPL-based IoT attacks under different feature selection methods (including univariate selection, feature importance, recursive feature elimination and correlation). KNN

outperformed SVM and Gaussian Naïve Bayes and illustrated much better results when recursive feature elimination.

While the feature selection method is crucial, the quantity of features chosen significantly influences the effectiveness of the machine learning algorithm. (Sharma *et al.*, 2019) proposed a supervised machine learning algorithm to act against RPL attacks. These authors compared the performance of random forest, decision tree and Naïve Bayes under different numbers of features. Employing a feature reduction technique, namely the filter approach, to decrease the feature count from 58 to 21, they achieved a 36% reduction to conserve processing and communication power. The reduced feature random forest classifier achieved great results with an accuracy of 99.33%. Compatible with this paper, our study considers, among other feature reduction techniques, filter techniques, wrapper techniques, and embedded techniques to decrease the number of features in the bid of reducing processing and communication energy. However, the size of the proposed model is still a question even in this study.

Numerous network layer attacks exist for wireless sensor networks and RPL-based IoT. Extensive efforts have been made to identify practical solutions for detecting and alleviating these adversaries. It is, of course, significant to realise systems that can countermeasure large-scale attacks at a go. That process requires a dataset for such a large number of attacks. (Agiollo *et al.*, 2021) suggested an IDS for identifying numerous threats in IoT networks. But first, the authors generated a dataset that contains five simulations for 14 well-known routing attacks. To detect attacks, they developed DETONAR, an IDS that combines signature-based and anomaly-based rules to discover nefarious or abnormal behaviour in the network traffic. Their system's attack detection exceeded 80% for 10 attacks out of the 14 considered attacks, and maintained a type I error close to zero.

Reinforcement-Learning-based IDS for 6LoWAPN was proposed by (Pasikhani, Clark & Gope, 2021). The proposed IDS uses reinforcement learning to identify diverse assaults on RPL, encompassing numerous attacks that current research has not addressed. Moreover, it is capable of identifying even attacks and mobile intruders that have not been encountered before. In the research, the authors examined the effectiveness of various

machine learning algorithms, including (Decision tree, k-nearest neighbour, neural networks, reinforcement learning, and Support vector machine). An intelligent attack detection and mitigation technique is essential in security against routing attacks in RLP-based IoT. Most ML-based security methods primarily classify routing attacks and they have filled that gap (Momand *et al.*, 2021). Authors proposed the support vector machine, one of the supervised machine learning algorithms, as a detection and mitigation scheme to act against rank, version number and DoS attacks. Simulated in the Cooja simulator tool with 30 nodes, the proposed scheme achieved a Packet delivery ratio of 76.8% low control message overhead and less energy consumption. Although the research nearly fulfils the criteria for a novel security approach in RPL-based IoT, it does not provide the results for detection rates and false negatives, which are the two metrics utilised to assess the effectiveness of security techniques.

While past research findings confirm the significance of the problem and have proposed an algorithm to detect and classify routing attacks, there are still RPL-based security open concerns which must be addressed for the end-to-end functioning of IoTs in real-world deployments.

## 2.8 CHAPTER SUMMARY

The chapter provided the literature review connected to this research. It presented the IoT overview, highlighting its use case and applications, extending to the routing protocol designed for IoT networks with limited resources, and further discussed the most common research routing attacks in the IoT networks. It finally reviewed related work, highlighting the strengths and weaknesses of some of the proposed works in the literature. The literature provides evidence that machine learning algorithms promise to be an effective detection technique with a high detection rate and a minimum of false alarms. Moreover, it was observed through literature that as much as ML algorithms can be effective, there is a limit to their integration in RPL-based IoT simulated in the Cooja simulator with minimum false alarms and high detection rate. Additionally, the adoption of mitigation techniques after detection is still a challenge. However, mitigation is not within the scope of this study. The following chapter outlines the methodology utilised in this research.

# CHAPTER 3

# RESEARCH METHODOLOGY

## 3.1 INTRODUCTION

This chapter outlines the techniques utilised in this research to fulfil its objectives and tackle the research gap highlighted in Chapter 1. The chapter presents a smart model to protect against routing assaults in IoT applications that uses mesh LLNs as its backbone. This is an experimental study, which depends on the network simulations for data collection. The chapter discusses research the paradigm, research methods, and data collection methods that align with studies in computing and information systems. The chapter furthermore demonstrates how this study fits into the selected concepts from a broader view. As this is an article-based PhD, several methods were adopted to accomplish the study's goal; therefore, the techniques used for each article are examined separately in the chapter.

## 3.2 RESEARCH METHODOLOGY OVERVIEW

### 3.2.1 Research paradigm

Based on Rehman, (2016: 240), a research paradigm refers to a philosophical view of the world that guides how research is approached, including beliefs regarding reality, understanding, and methods for gathering and analysing data. Four paradigms are dominant and relevant to computing and information systems research: interpretivism, common in studies involving user behaviours and culture in society; pragmatism, often used in studies where both technical performance and user experience are relevant particularly in studies developing models and/or artefacts; lastly, positivism, which is the basic paradigm of this study, relevant in studies where models and algorithms are tested using measurable metrics (Davies, 2018: 263).

This research adopts a positivist philosophy because it investigates objective reality where model performance metrics exist independently of the researcher. The study is designed to test hypotheses regarding the relationship of cause and effect between routing attacks and network performance, along with the detection efficacy of the suggested intelligent model. This is accomplished by gathering only quantitative data from controlled simulation experiments of network and model performance metrics,

allowing for the statistical validation of results and the establishment of generalisable conclusions.

### 3.2.2 Research design

A methodology is an organised and systematic strategy for carrying out research and a way to gather data (Davies & Fisher, 2018; Rehman & Alharthi, 2016). It is a framework that guides the entire approach to gathering and analysing data (Rehman & Alharthi, 2016). Rather than just being a single technique (a "method"), methodology defines:

- **The theoretical basis** for the research approach.
- **The overall strategy** for the study that determines what kind of data is needed.
- **The rationale** for choosing specific data collection tools (e.g., experiments, simulations, surveys, logs).

In essence, methodology entails the critical process of designing how a research question is investigated. The structure for executing research is referred to as the research design. This also details the approaches and methods employed for gathering and examining the data (Sileyew, 2019). The research design is determined by the researcher's understanding of the subject and the objectives for reviewing and interpreting the data (Myers *et al.*, 2013).

This study adopted a positivist paradigm, which, according to (Mbanaso *et al.*, 2023) influences the selection of the methodology. A study can be quantitative, qualitative, or mixed methods. Quantitative research methodology means the research depends on quantifiable or measurable information. Qualitative research approaches mean that the study is based on individual narratives or records that elaborate how individuals react or perceive reality within a community. Mixed research approaches utilise both quantitative and qualitative research methodologies (Apuke, 2017). This study adopted a quantitative research methodology for data collection since it is an experimental-based study (Bacon-Shone, 2013).

Figure 3-1 illustrates a three-phased research design employed in this study, that is, the literature review, empirical, and validation and contribution phases. The literature review phase establishes the theoretical elements of this study that directed this research.

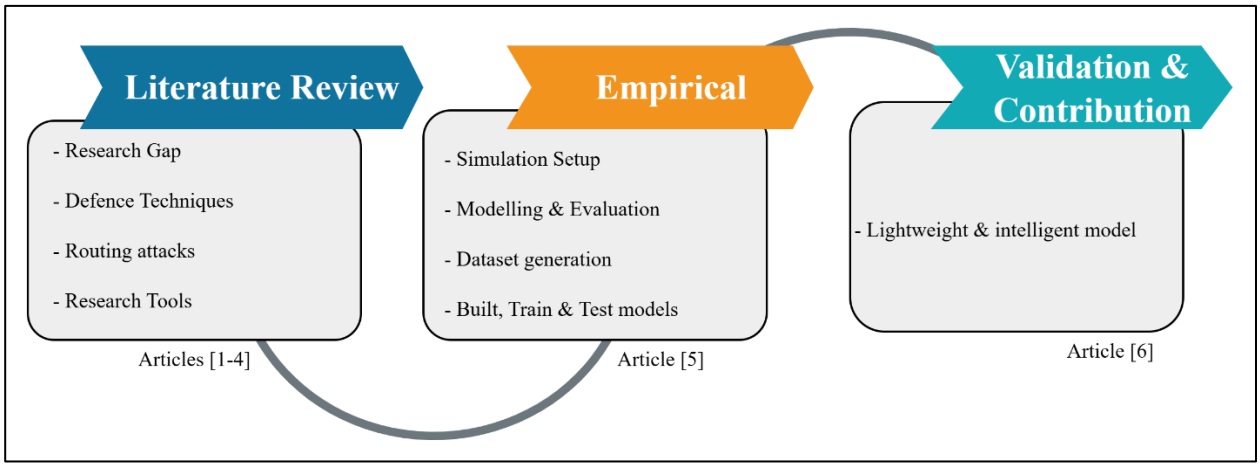


**Figure 3-1:** Research Approach utilised for this study

The empirical phase utilises the findings from the literature review phase to set up simulations, model attack and baseline scenarios, evaluating the simulation results to examine the effect of the adversary on the network. Furthermore, the study utilises the simulation network logs to generate a dataset which is then used to build, train, test and compare different supervised machine learning models. Lastly, the validation and contributions phase authenticates and proposes a decision tree-based lightweight and intelligent model.

### 3.2.3 Research tools

In network security and performance, network operational logs are leveraged to build and train models for the classification and detection of routing attacks. This study utilised the following tools to achieve its aim:

- Cooja simulation tool to conduct IoT mesh network simulation scenarios using two network topologies. It is an open-source simulation tool with comprehensive formal documentation and an extensive collection of tutorials for experimental use.
- Visual Studio, using Python programming language libraries to preprocess the dataset, build, train, and test models.
- Draw.io was used to design the figures of this study. Draw.io is a free online, cross-platform graph visualisation software created using HTML5 and JavaScript.

## 3.3 DATA COLLECTION AND ANALYSIS

This study combined three complementary methods for data collection - Integrative Literature Review (ILR), Systematic Literature Review (SLR), and experimental, displayed in Figure 3.2 - aligning with specific Research Objectives (ROs) and contributing progressively to the final defence model.

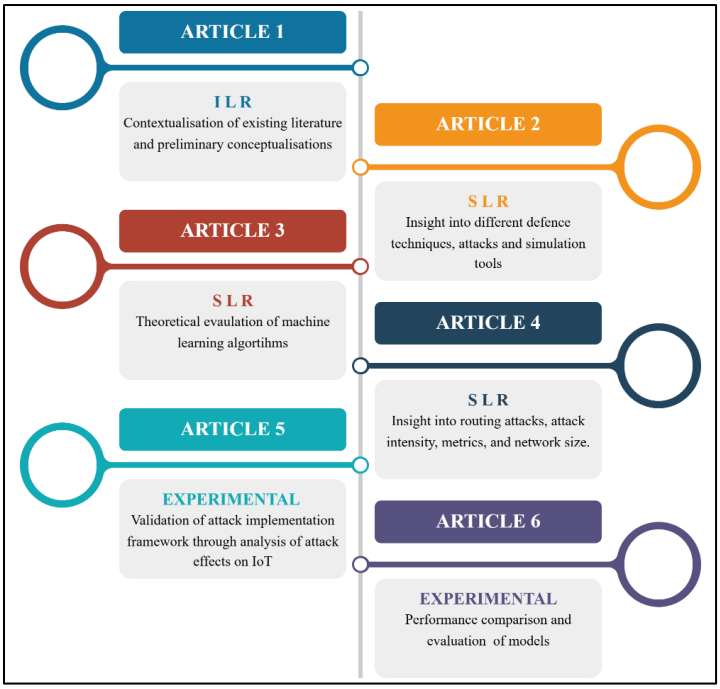


**Figure 3-2:** Articles: cross-sectional data collection methods

Articles 1 through 4 utilised literature review as methods of data collection. Specifically, article 1 adopted an integrative literature review, and articles 2,3 & 4 adopted a systematic literature review for data collection. Articles 5 & 6 utilised simulations for data collection through experimental setups.

### 3.3.1 Methods

#### 1. Integrative Literature Review

An integrative literature review research approach was adopted to critique and synthesise existing literature and contextualise current knowledge. The aim here is to provide an overview of the knowledge framework, analyse critically and possibly reframe, and thereby enhance the theoretical basis of the topic as it evolves. For newly emerging

subjects, the goal is to develop initial or preliminary conceptualisations and theoretical frameworks instead of assessing existing models (Snyder, 2019).

(i) Purpose of this study

This is designed to examine the literature's knowledge base and to pinpoint research deficiencies, develop a problem statement, and outline the study's goal and objectives.

(ii) Design adopted

Article 1 reviewed the literature in the field of defence mechanisms in RPL-based IoT networks.

(iii) Data collection

Different academic databases, e.g., IEEE, Science Direct, etc., were consulted to collect several published studies that are relevant to this study.

(iv) Data analysis

Qualitative analysis was adopted to identify the research gaps this study aimed to address.

(v) Contribution to overall research

This study established the research gap, justified for developing an intelligent defence model and a conceptual framework for deployment of the defence model.

**2. Systematic Literature Review**

A Systematic Literature Review (SLR) is a procedure for locating and thoroughly evaluating pertinent research. A systematic review seeks to locate all empirical evidence that meets predefined inclusion criteria to address a specific research question or hypothesis (Snyder, 2019). Furthermore, it was created as a method to combine research results in a systematic, clear, and replicable manner and it has been termed the gold standard for reviews (Snyder, 2019).

(i) Purpose of this study

To identify, evaluate, and synthesise existing publications on routing attacks and defence mechanisms in IoT LLNs.

(ii) Design adopted

Article 2 reviewed defence techniques (secure-protocol, IDS, and AI-based). Furthermore, article 3 dived deep into machine learning defence models. Lastly, article 4 employed the design to conduct a review of routing attacks and theoretical implementation guidelines.

(iii) Data collection

The publications were sourced from academic databases, e.g., IEEE, ACM, Scopus, and these were screened using inclusion/exclusion criteria, and analysed following the defined SLR flow. Furthermore, each of the three articles that adopted SLR has its own subsequent collected data.

(iv) Data analysis

Qualitative thematic analysis was used to categorise types of defence techniques and routing attacks. Furthermore, quantitative analysis was conducted to assess the effectiveness of machine learning algorithms found in the literature regarding accuracy, precision, recall, F1-score, and false positive rate. Lastly, the analysis culminated in mapping network size and attack intensity.

(v) Contribution to overall research

The study established the research gap and justification for developing an intelligent defence model.

## 3. Experimental

(a) Simulations: Article 5

(i) Purpose of this study

To simulate and verify the effects of routing attacks on network performance

(ii) Design adopted

Article 5 implemented DIS-Flooding attacks (see appendix 1)and baseline simulations in Cooja/Contiki and validated the effect of the adversary on the performance of the network compared to the baseline scenario.

(iii) Data collection

Network performance logs were captured during simulation runs. These logs contain data that includes the time packets are sent, received, the number of successful packets, the type of packet, the beacon interval, and energy consumption.

(iv) Data analysis

This entails comparative analysis of DIS-Flooding attack and baseline results based on the selected metrics to quantify attack severity. PDR, E2E delay, beacon interval, and energy consumption evaluation metrics were derived to assess the effect of the adversary on the network compared to the normal operations of the network.

(v) Contribution to overall research

The study provided experimental evidence of vulnerabilities and the effect of DIS-flooding on network efficiency.

(b) Simulations: article 6

(i) Purpose of this study

To build, train, and test ML-based defence models against routing attacks and optimise the best-performing model.

(ii) Design adopted

Article 6 evaluated four machine learning models on simulation datasets and optimised the best-performing model as the intelligent defence model.

(iii) Data collection

This was derived from simulation dataset (CSV) generated from simulations (attack and baseline scenarios) and pre-processed into feature vectors suitable for Machine Learning input.

(iv) Data analysis

Data analysis was undertaken through model training, testing, and cross-validation; performance assessed through accuracy, precision, recall, F1-score, false negatives and ROC-AUC.

(v) Contribution to overall research

This study ultimately contributes to the facilitation and creation of a smart defence model that combines precise identification and efficient resource consumption, forming the core practical contributions of this study.

Different methods were adopted in this study because of its article-based format. Table 3-1 below summarises the methods employed in the research, emphasising their objectives, data gathering, and analysis techniques and overall contribution to this study.

**Table 3-1:** Summary of adopted methods used in this study

| | **ILR** | **SLR** | **Experimental** |
|---|---|---|---|
| Articles | Article 1 *(Conceptual framework)* | Article 2 *(Defence Mechanisms),* Article 3 *(ML Techniques),* and Article 4 *(Routing Attacks)* | Article 5 (*Validation and Implementation of Routing Attacks and Baseline Scenarios in LLNs*)<br><br>Article 6 (*Comparison of ML Models for Routing Attack Detection*), (*Optimised Defence Model Proposal*) |
| Purpose | Identify a research gap | Explore the research study in depth and identify key elements for this study | Assess the efficacy of the suggested framework and establish the effectiveness of the suggested mode |
| Data Collection | Articles from academic databases, including IEEE, ACM, Scopus, etc. | Articles from IEEE, ACM, Scopus; screened via a defined inclusion/exclusion criterion | Simulation logs (PDR, delay, energy consumption) and attack and baseline datasets (CSV) generated from simulations; pre-processed into features |
| Data analysis | Qualitative synthesis of existing research | Synthesis of existing research: Qualitative synthesis; thematic categorisation of routing attacks & defences. Quantification of performance metrics, network size, Number of attacks and attacking nodes | Statistical comparison of attack vs. baseline scenarios Model training/testing; cross-validation; metrics: accuracy, precision, recall, F1,false negatives |
| Contribution | Research gap identification Conceptualisation of knowledge and development of a conceptual framework | Identification of routing attacks<br>Explore existing defence techniques<br>Identification of simulation tools and performance metrics<br>Theoretical framework | Provision of empirical evidence of vulnerabilities of RPL and validation of the framework.<br>Assess the effectiveness of the suggested defence model. |

## 3.4 SYSTEM MODEL

In this study, a decision tree-based lightweight and intelligent defence model for DIS-Flooding attack is proposed to accurately detect the attacks with a demonstration of low false alarm and program flash memory utilisation. An implementation diagram of the design and the structure of the suggested model is articulated in this section. This study utilises the Cooja tool to simulate a baseline and DIS-Flooding attack scenarios for dataset generation.

Two datasets are generated: baseline_dataset.csv and disflooding_dataset.csv and these are concatenated to create a binary class dataset employed to educate and evaluate the models. The resulting dataset underwent data preprocessing stages in readiness for model fitting and classification. Figure 3-3 demonstrates the system architecture adopted in this study to achieve its aim.

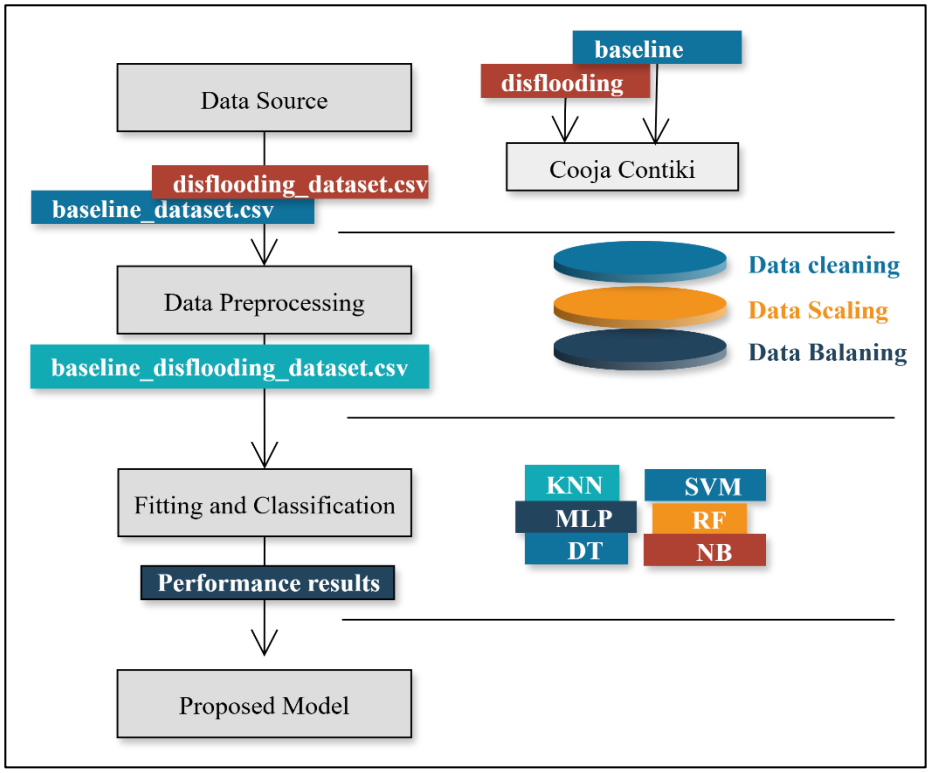


**Figure 3-3:** System architecture flow diagram

### 3.4.1 Data source

Using the Cooja simulator, a 25-sensor-node wireless sensor IoT network with 1 sink node was simulated for an hour as a baseline scenario. Then DIS-Flooding attack nodes were added to create a DIS-Flooding attack scenario, which also ran for an hour. In both scenarios, network logs (see appendix 2) were collected, and the Python programming language was utilised to extract valuable information from the network logs and generate Comma-Separated Values (CSV) files from both scenarios (see appendix 3), that is, baseline_dataset.csv and disflooding_dataset.csv.

### 3.4.2 Preprocessing

Data preprocessing involves applying several strategies to the data, including data cleaning, transformation, balancing, and splitting. The objective is to make the data suitable for supervised machine learning classification models. This study cleaned and organised data for analysis by handling missing values, efficiently scaling data and balancing the binary class dataset. This procedure guarantees that the data is precise, uniform, and prepared for modelling.

#### 3.4.2.1 Data cleaning

It was observed that some columns and rows in the data files had missing values. The basic strategy of dealing with missing values would be discarding the entire rows and or columns, but that would result in data loss. Imputation was adopted to deal with the missing values. Univariate feature imputation was utilised to impute missing values with the statistical mean of each column. Furthermore, for each data file, a column ‘target’ was created with entries of 0s and 1s for baseline and DIS-Flooding, respectively, further concatenated into one base_disflooding data frame.

#### 3.4.2.2 Data scaling

Normalisation and data standardisation techniques were applied as this is a requirement for many machine learning models, and it was observed with the Support Vector Machine and Multilayer Perceptron in this study. The mentioned models performed poorly with

unscaled data, which demonstrated the importance of scaling data for improved classification.

#### 3.4.2.3 Data balancing

The binary class dataset of this study has 1475 and 1162 entries representing baseline (0) and DIS_Flooding (1) classes, respectively. Though the imbalance is not significant, for better classification, the Synthetic Minority Oversampling Technique (SMOTE) was adopted to create synthetic data points to balance the dataset, so as to improve model generalisation and performance by reducing bias towards the majority class.

### 3.4.3 Fitting and classification

Upon preprocessing the dataset, supervised machine learning algorithms were created, trained, assessed, and analysed. The selection of the models and performance metrics was guided by the literature and the SLRs (Article 3) conducted in this study. In this subsection, we outline the training and selection techniques employed in our research.

In this study, the dataset was divided into a training set and a testing set, with 70% allocated for training and 30% for testing the detection capability of the model given the dataset. Moreover, the research utilised six machine learning models: SVM, RF, MLP, KNN, DT, and NB.

These are classification models for supervised learning that can learn from labelled data and forecast the class of unknown data. The models were selected based on guidance from the literature, their effectiveness in classification tasks, and their capability to reflect performance and quality regarding accuracy, precision, recall, false negatives, and Matthews Correlation Coefficient (MCC). This study evaluates and analyses the performance results of the 6 models to determine the best-performing one.

### 3.4.4 Decision tree-based lightweight and intelligent defence model

A Decision Tree is a supervised machine learning model that is non-parametric and used for both classification and regression tasks. It separates the data instances in its processes and generates decision rules based on data characteristics to predict the target variable's value.

The decision-making process of this paradigm can be represented as a tree, facilitating user interpretation. Decision nodes and leaves are the core components of decision trees. In the decision node, data is partitioned according to a specific parameter, while the leaves yield the outcomes or decisions (Wang *et al.*, 2022) as depicted in Figure 3-4.

In this experimental work, the splitting criterion employed was Gini, which quantifies the impurity of the split. It exhibits how well a split divides the total samples of binary classes into a specific node $t$. Mathematically, it can be expressed as in (1).

$$Gini(t) = 1 - \sum_{i=1}^{k} p_i^2 \quad (1)$$

where, $t$ is the node, $k$ is the number of possible classes, and $i$ represents the class.

$p_i^2$ proportion of samples belonging to the class $i$ in node $t$

Then the prediction for the input $x$ can be expressed as in (2)

$$\hat{y}(x) = \arg\max_{i \in C} p(i|x \in leaf) \quad (2)$$

where, $c$represents a class, either baseline or DIS-Flooding. $C$ is a set of classes {*baseline, DIS-Flooding*}

$p(i|x \in leaf)$ the probability of the class $i$ given that $x$ ends up in that leaf node, $\arg max$ chooses the class with the maximum probability

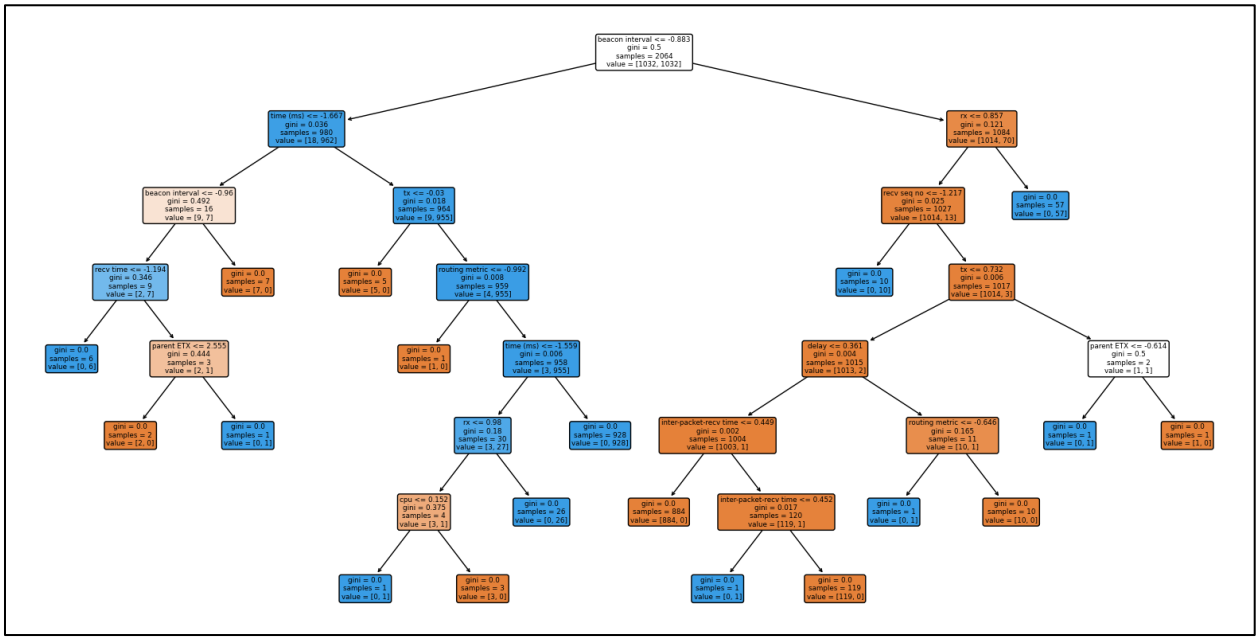


**Figure 3-4:** Proposed decision tree classifier architecture

## 3.5 ETHICAL CONSIDERATIONS

An examination of ethical concerns during research activities is essential to avoid ethical breaches (Kamiri & Mariga, 2021). Although this study is a no or low risk ethical one, the study followed the ethics process as defined in the FNAS document of the North-West University. The researcher signed the North-West University code of conduct, committing to uphold honesty, accountability, professional civility and good stewardship, and received ethical approval for the project. The risk application was scrutinised by the committee and ethical clearance number was approved (NWU-01333-24-A9),see appendix 4, ethical clearance. Beyond procedural clearance, additional ethical dimensions were considered. With respect to data privacy, the dataset utilised in this study was generated within a controlled Cooja simulation environment and did not involve human participants, personal data, or identifiable information. Consequently, no personal privacy risks were present. Nevertheless, secure storage practices and controlled access to the generated datasets were maintained to preserve research integrity and prevent unauthorised manipulation.

It is worth noting that the experimental setup, simulation parameters, attack implementation methodology, feature extraction process, and model evaluation procedures were systematically documented. This approach mitigates reproducibility

risks and promotes methodological transparency, thereby supporting verification and replication by other researchers in the field. While this study involves the implementation of routing attacks within a simulation environment, such implementation was conducted strictly for defensive and evaluative purposes. The objective is to strengthen the resilience of RPL-based IoT networks rather than to facilitate malicious exploitation.

## 3.6 CHAPTER SUMMARY

In conclusion, a positivist paradigm was adopted because it assumes reality exists independent of humans, which aligns with the philosophical orientation of this study. A positivist paradigm assumes several methods, including quantitative, qualitative and mixed methods. However, this study adopted only a quantitative strategy, further utilising review and experimental methods for examining data. The following chapter presents the findings and analysis of this research.

# CHAPTER 4

# RESULTS AND DISCUSSION

## 4.1 INTRODUCTION

This section presents the results of this research. It emphasises the findings and discussion of every article in this study in the "*articles from the research study"* section. For each article, the chapter presents purpose, methods employed to conduct the research, results and discussion, conclusion, and the full paper submitted for publication. Lastly, it presents a chapter summary of the findings of this chapter and introduces the next chapter.

## 4.2 ARTICLES DEVELOPED FROM THE STUDY

### 4.2.1 Article 1

#### 1. Article publication details

Title: High-Level Defence Model against Routing Attacks on the Internet-of-Things

Status: Published

#### 2. Article synthesis

(i) Purpose

This article is a theoretical study extracted from the initial proposal of this research. It aims facilitate the creation of a streamlined smart defence framework against a routing adversary in LLNs. Building on established findings from the literature, this article proposes a high-level end-to-end conceptual framework for the implementation and deployment of a lightweight and smart security model to protect against routing attacks in resource-limited IoT networks with limited memory, processing power, and energy.

(ii) Methods

An integrative literature review research approach was adopted to critique and synthesise existing literature and contextualise existing knowledge.

(iii) Results and Discussion

As a conceptual study, this article does not only present empirical results but discusses findings based on the literature review. It highlights that there is still a research gap to exploit in the adoption of ML techniques as security models in IoT networks against routing attacks, further establishing that Edge computing is a feasible option for deploying models, taking into account the limited resources of IoT networks.

(iv) Conclusion

Though this article does not provide empirical results, through an integrative review, it presents a comprehensive conceptual model aimed at protecting IoT networks of resource-constrained devices against routing attacks, meaning that the field of adoption of machine learning algorithms still needs to be explored further.

## 3. Full paper

**Indonesian Journal of Computer Science**
ISSN 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam No. 1, Padang, Indonesia
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

# High-Level Defence Model against Routing Attacks on the Internet-of-Things

**Lanka Chris Sejaphala[1], Vusumuzi Malele[2] , Francis Lugayizi[3]**
chris.sejaphala@nwu.ac.za, vusi.malele@nwu.ac.za, francis.Lugayizi@nwu.ac.za
North-West University, South Africa

**Article Information**

Submitted : 1 Feb 2024
Reviewed: 11 Feb 2024
Accepted : 27 Feb 2024

**Keywords**

Internet of Things, RPL, Machine learning,

**Abstract**

This paper aims to answer the following research question: "To what extent can an intelligent security model effectively defend against routing attacks in RPL-based Internet of Things (IoT) with a demonstration of less network resource consumption, high detection rate, and minimal false negatives?" To answer this question, this paper proposes a high-level conceptual framework to defend the IoT against routing attacks. In recent works, mitigation techniques have been proposed to act against routing attacks, however conceptual defence or mitigation framework is not presented as a set of steps to follow to develop an effective and robust intelligent security model. This paper aims to present a high-level conceptual defence framework against routing attacks; specifically, sinkhole, rank, DIS-Flooding, and worst parent. The four mentioned routing attacks are capable of disturbing IoT network functions and operations, and consuming network resources such as memory and power.

## A. Introduction

In recent years, technology has evolved significantly, leading to distinct generations characterised by major advancements and innovations. The current generation of technology is characterised by the proliferation of the internet users, IoT, Artificial Intelligence (AI), cloud computing, etc. It encompasses the third and fourth industrial revolutions [1]. The third industrial is referred to as the digital revolution characterised by the advent of the internet and digital technology. This revolution gave rise to the integration of Information Technology into various industries and transformed how people communicate, work, and access information.

The current phase of the industrial revolution, the 4th Industrial Revolution (4IR) is characterised by the convergence of physical, digital, and biological technologies, involving advancements in Internet-of-Things (IoT), Machine Learning, Three-Dimensional (3D) printing, Nanotechnology, and Biotechnology to name a few. The 4th Industrial Revolution aims to create "smart" and interconnected systems that can enhance efficiency and productivity across various sectors, including transportation, manufacturing, mining, agriculture, health, and energy [2].

The IoT is a paradigm of interconnected devices that collect and exchange data with each other from the environment of deployment and share the data over the Internet to achieve a particular goal (see Figure 1). This paradigm is used in a wide range of applications including home security management, industrial automation, smart energy monitoring and management, surveillance and military, smart cities, and farming, to name a few.

The IoT applications are growing rapidly, bringing significant differences in human lives, and helping industries like manufacturing, logistics, and health make critical decisions. The IoT market is estimated to grow over $2.4 trillion annually by 2027. This includes the growth of IoT devices from 8 billion in 2019 to 41 billion in 2027 [3]. The IoT has brought very significant benefits to our lives, society, and industries. Given the applications of IoT, most of the IoT devices are resource-constrained (small on-board memory, less energy, and low computation capabilities) and are expected to operate for a long period; thus, low power-consuming protocols are desired. Due to its resource constraint (energy, memory, computation) nature, IoT devices use standardised Routing Protocol for Low-power and Lossy networks (RPL) to communicate their routing information among themselves and route their observed data to the sink node.

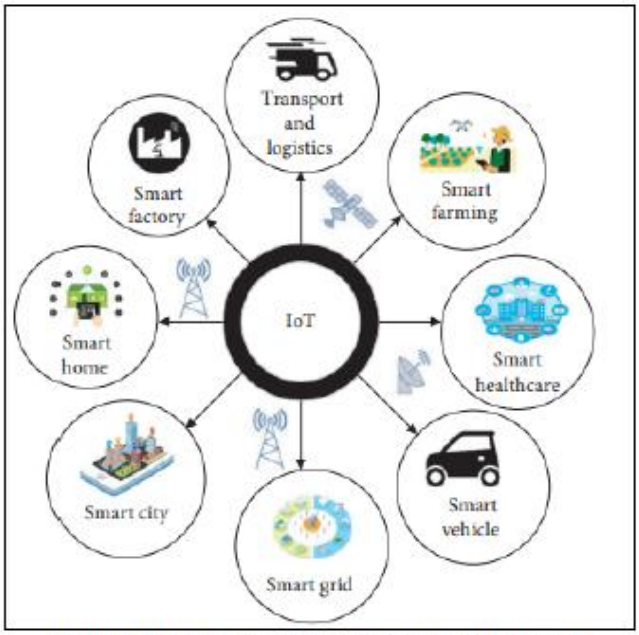


**Figure 1.** Applications of the Internet of Things [4]

RPL is the only DeFacto standardised network layer routing protocol for Low-power and Lossy Network (LLN) IoT [5]. Standardised in 2012 as RFC 6550 by Routing Over Low Power and Lossy Networks (ROLL) which is a working group of the Internet Engineering Task Force (IETF) [6]. The RPL has gained much popularity in the industry and academia because of its capability to provide efficient routing among resource-constrained smart IPv6-enabled IoT nodes, Quality of Services (QoS) support, and flexibility in adapting to different network topologies. The RPL uses low energy-consuming techniques to support self-organisation and self-healing for handling frequent node failure. Furthermore, providing efficient routing for IPv6 packets, these capabilities of RPL favours its usage in the IoT applications running on LLN infrastructure.

While IoT opens doors to the realisation of the connected world and new networking possibilities, it is vulnerable to routing attacks. The most common types of attacks in IoT running RPL are routing attacks since all nodes in the network partake in packet forwarding for the whole network [7]. These attacks cause massive data theft and system susceptibility [8]. Moreover, an increase in connected IoT devices and their insecure nature gives adversaries more options to gain access to the devices and use them to launch further large-scale catastrophic attacks like DDoS [9]. The popularity of RPL in IoT applications renders the security of this protocol of paramount importance. In other words, the deployment of RPL-based IoT has caused critical security vulnerabilities simultaneously, as such it has become crucial to address these vulnerabilities in RPL-based IoT [10]. The RPL as a widely deployed routing protocol in IoT is susceptible to routing attacks such as DIS-

flooding, sinkhole, rank, and worst parent attacks to name a few. Routing attacks pose a great threat to IoT running RPL as a routing protocol; and may affect its performance and functionalities [11].

In recent years, traditional techniques have been proposed; however, in literature, it is reported that Machine Learning techniques are more effective in terms of analysing IoT network traffic and making accurate predictions [12]. As such Machine Learning algorithms are utilised to monitor the behaviour of the network, classify network traffic, detect and mitigate network attacks, etc. However, these intelligent security models impose memory and computational power challenges in the IoT network, they require large memory and computational power to carry out their functions. In this study, edge computing is realised as a suitable solution to the challenges faced by intelligent model deployments.

This paper aims to propose a high-level conceptual framework that will contribute towards the development of a defence model that will effectively defend against routing attacks in RPL-based IoT with a demonstration of less network resource consumption, high detection rate, and minimal false negative. Taking advantage of the memory and computational capability of edge computing, as its use in model deployment to defend against routing attacks in IoT remains limited. Despite this introduction, this paper comprises of the following sections: literature review, methodology, proposed model, and conclusion and future studies.

## B. Research Method

In this section, experimental setup and methods of data collection and analysis are presented. However, prior to the latter, this section will discuss both network and adversary modelling as a subsection of the experimental setup.

- **Experimental setup**

To run different simulation scenarios, the study utilises NetSim V13.2 installed on an HP laptop running a 64-bit Windows 10 Pro Operating System and 16GB RAM. MATLAB R2023 is utilised for performance metrics visualisation, the edge computing device is simulated as an HP PC running Linux OS with 16 GB memory.

- **Network Modelling**

We conduct extensive simulation experiments using NetSim to model IoT running RPL. Where IoT nodes are uniformly distributed in a defined network area, with a single DODAG root. The communication range of each node is 50m with a normal data rate of 250Kbps, and 802.15.1 MAC/PHY operates with a default configuration.

- **Adversary Model**

The attack model is followed to capture the performance of the network under different numbers of attacking nodes defined as percentages and to evaluate the robustness of the proposed scheme. The paper defines 5%,10%, and 15% for each network size (e.g., 25,36, and 64) as attacking nodes as a mechanism to evaluate the performance of the proposed scheme. As presented in Table 3 below, a network size of 25 IoT devices provides 1 attacking node at 5% attack, and a network size of 36 IoT devices provides 5 devices attacking nodes, and so on.

**Table 1**. Attack percentage distribution

| | Attack % | | |
|---|---|---|---|
| **Network Size** | 5% | 10% | 15% |
| **25** | 1 | 3 | 4 |
| **36** | 2 | 4 | 5 |
| **64** | 3 | 6 | 10 |

- **Evaluate performance**

To evaluate the performance of the proposed model, the paper considers the following performance metrics accuracy, precision recall, and area under ROC. These metrics are most used to evaluate the performance of Machine Learning algorithms. Furthermore, the paper utilises network performance metrics to evaluate the performance of the network during a network attack, no attack, and after the mitigation of the attack. Metrics that are considered are packet delivery ratio, energy consumption, detection rate, false negative, control message overhead, and end-to-end delay.

- **Assumptions and Limitations**

The network can only maintain one DODAG instance. The security of edge device is not the scope of this work, as such, the paper assumes that the edge device is secured.

- **Data Collection and Analysis**

Wireshark as a packet sniffing application is utilised as a data collection tool. Wireshark has the capability to capture network packets and display them at a granular level [25]. It can be used for real-time or offline analysis to assist with network analysis and ultimately network security. Collected data is analysed using a graphical representation. Both MATLAB and/or Microsoft Excel applications are utilised for the presentation of data.

### C. Result and Discussion

This paper proposes a high-level conceptual framework to defend against routing attacks in IoT running RPL routing protocol. The framework utilises edge computing technology to deploy the Intelligent Security Model at the edge of the network. The high-level conceptual framework is depicted in Figure 2 and details of each component are described in the following subsections.

- **High-level conceptual framework**

The proposed framework implements ensemble learning, where multiple supervised machine learning algorithms are integrated into one model for the classification of network traffic data, detection of attacks, and identification of malicious nodes. A list of malicious nodes list is forwarded to the 6LowPWAN Border Gateway (6BG), which then multicast the malicious node list to the legitimate nodes with an instruction of selective-forwarding. As depicted in Figure 2, a proposed conceptual defence framework is presented. Edge computing technology is utilised to deploy the Intelligence Security Model, the framework uses packet

sniffing devices to forward the network traffic as a pcap file to the model deployed at ML-enabled edge device for analysis.

The output from the ML-enabled edge device is a list of malicious nodes identified in the network and is sent to the 6BG for mitigation. During mitigation, legitimate IoT nodes are instructed to drop control message packets from the malicious node list as a mitigation mechanism. While MATLAB is used to capture and display the performance of the network and the Intelligent Security Model.

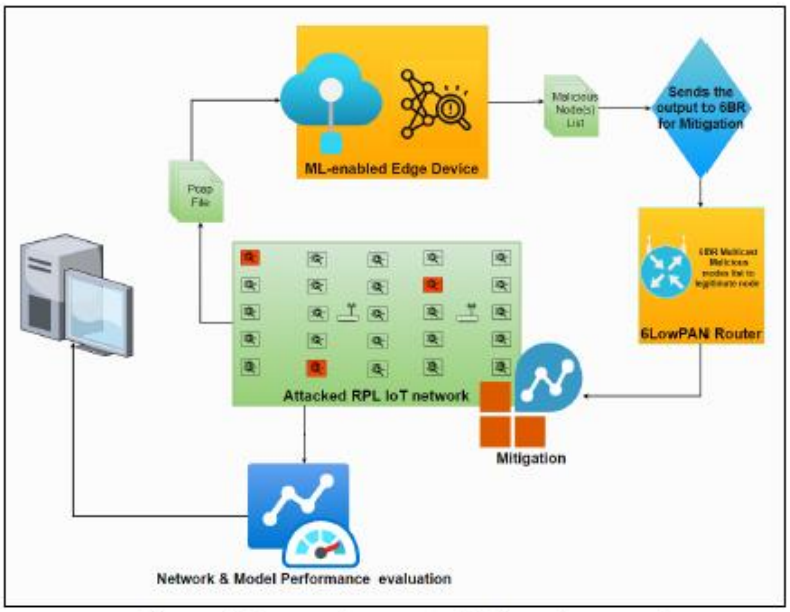


**Figure 1.** Proposed conceptual defence framework.

- **High-level conceptual framework: Literature Contribution**

It is fundamental to develop security techniques that detect and mitigate routing attacks with less or close to zero network overhead. Current state-of-art security solutions use traditional techniques (e.g., trust-based, rule-based, signature-based, encryption, and key-management, etc.) trying to ensure the security of the RPL-based IoT [13]. While securing the network, these techniques introduce heavy mechanisms at the expense of IoT devices and the overall network performance. To launch an attack, cybercriminals generally modify an existing attack code to replicate an attack. This is where the power of edge-enabled intelligent mitigation techniques proves to be an ideal solution because they rely on past learning rather than signature and rules which can be changed easily [14] while the computations are done on the edge of the network instead of at the IoT device level.

The fact that a large amount of data is acquired from IoT devices with limited resources such as computing, has rendered conventional techniques ineffective leading to the emergence of intelligent systems [12]. In recent years, research work

in the integration of artificial intelligence particularly machine learning as a security solution has been conducted [15]. It is evident that machine learning-based methods promise to be a viable solution against routing attacks, but little attention has been given to IoT [16]. It is expected that machine learning algorithms promise to produce desired results in efficient and effective mitigation approaches to address some of routing attacks in RPL-based IoT networks [17]. In the context of networks, the most used machine learning techniques from literature are supervised learning [18], they achieve high-performance metrics percentage in classifying several attacks. However, most of the proposed machine learning-based security techniques in RPL-based IoT only classify attacks without mitigation. It is known that RPL-based IoT has adopted some spectrum of wireless sensor network attacks [19]. In their study, they proposed a machine learning class, ensemble learning-based intrusion detection system for RPL-based IoT to detect against selected seven network layer attacks which use four different classifiers. The four classifiers e.g., boosted trees, subspace discriminant, RUS boost tree and bagged tree were trained and tested. Boosted tree achieved the highest accuracy of 94.5% and RUS boosted tree achieved a better area under ROC of 98%. However, their proposed system only classifies normal and attack traffic it does not neither identify malicious nodes nor mitigate them. Their system model does not offer an end-to-end mitigation mechanism.

Although in the recent past, some works have been done on traditional techniques aiming at securing RPL, showing acceptable results [20]. However, although these conventional techniques promise to mitigate routing attacks in RPL-based IoT, most of them do not evaluate resource utilization and communication overhead during detection and mitigation [21]. Furthermore, with conventional techniques, it is also not feasible to address multiple attacks with only one technique [22]. Moreover, these conventional techniques either introduce communication overhead, computation performance issues, and/or energy consumption in these LLNs. A conventional end-to-end mitigation technique to act against Network Isolation Attacks in defending RPL [23]. Unlike [19] and [23], [24] not only employed an intelligent security model to identify anomalies in the IoT but also realised and utilised fog computing for model deployment. In ensuring that the proposed model does not contribute much to IoT device resource consumption. They allowed expensive computation of the detection model to be handled by a fog device equipped with computational power and memory. However, as far as [19] realised the power of the intelligent model, they could only identify attacks, without mitigation. But [23] implemented end-to-end detection and mitigation technique. Whereas [24] integrated methods in [19] and [23] into fog computing to realise an end-to-end defence against one type of attack, DDoS, by classifying network traffic. This paper then proposes the integration of an intelligent security model into an edge device to defend against multiple routing attacks. Furthermore, evaluate both the performance of the model and network under different performance metrics.

In the IoT environment given its large-scale deployment, applications, and wide uses it is vital to develop an intelligent security model against routing attacks aiming at disrupting network functionality. The security model must be able to achieve a high detection rate, and almost close to zero false negative while mitigating the attacks with close to zero network overhead. Furthermore, the model

must consider the resource-limitation nature of the RPL-based IoT networks. To the best of our knowledge through literature, such an intelligent security model has not yet been developed. The work illustrated in Table 2 presents the theoretical contribution that our proposed model promises to close the gap.

**Table 2.** Theoretical gap contribution

| Studies | | Open issues | | | | |
|---|---|---|---|---|---|---|
| | | Effects of attacks on the network | Proposed technique Resource consumption | Spectrum of attacks | Mitigation | Network performance metrics |
| Existing Research work | Conventional based | Not addressed | Addrresed | Difficult to address multiple attacks | Techniques are able to mitigate and isolate malicious nodes from the network | Presented |
| | Intelligent Security based | Not addressed | Partially addressed | Able to address mutliple attacks at once | Techniques only attacks they do not provide mitigation mechanism | Not addressed, only machine learning metrics evaluation are presented |
| Proposed Study | Intelligent security Model | Will be addressed | Will be addressed, computations to be done on edge device | Mutliple attacks will be addressed | Malicious nodes will be identified, isolated and attacks will be mitigated | Both machine learning and network performance metrics will be presented |

This paper attempts to close the gap of the need for a supervised machine learning mitigation model to act against routing attacks, to secure the network, and maximise its performance. As such, the paper contributes an intelligent security model as a defence mechanism against routing attacks in IoT running RPL as a routing protocol. The model will integrate best-performing supervised algorithms for the classification of network traffic, detection of attacks, and identification of malicious nodes. The model will take advantage of the edge computing technology and have all the computations done on the edge device, not the IoT device level.

### D. Conclusion

In this paper, we proposed a high-level conceptual framework to defend against routing attacks in IoT running RPL. The framework displays the use of edge computing technology to store and execute the defence model, as edge computing technology is capable of integrating high-performing (in terms of memory storage and computational power) devices closer to the IoT end-devices. The framework demonstrates high-level end-to-end mitigation.

This paper aims to contribute towards the development of an effective and efficient Intelligent Security Model to defend against routing attacks in IoT networks running RPL. As such, the primary contribution of this paper is to propose a high-level conceptual framework for defence against routing attacks. The secondary contribution of the paper is the identification of a theoretical gap in the literature to utilise edge computing integrated intelligent security model to defend IoT against routing attacks. Limitations of the study are that the simulation tool can only simulate homogeneous IoT device networks.

In future work, routing attacks defence is intended to be addressed by developing an intelligent security model to defend IoT against routing attacks. Furthermore, future work will enhance the performance of the Intelligent Security Model by providing feedback on its performance and suggestions to improve its performance metrics. In such a way that the model will not only defend against the routing attacks, but its poor performing metrics will be improved from performance feedback.

## E. References

[1] P. Ross, and K. Maynard, "Towards a 4th industrial revolution", Intelligent Buildings International, 13, (3), pp. 159-161, 2021.

[2] A.O. Adebayo, M.S. Chaubey, and L.P. Numbu, "Industry 4.0: The fourth industrial revolution and how it relates to the application of internet of things (IoT)", Journal of Multidisciplinary Engineering Science Studies (JMESS), 5, (2), pp. 2477-2482, 2019.

[3] R. Ahmad, and I. Alsmadi, "Machine learning approaches to IoT security: A systematic literature review", Internet of Things, 14, pp. 100365, 2021.

[4] M.Y. Mehmood, A. Oad, M. Abrar, H.M. Munir, S.F. Hasan, H.A.U. Muqeet, and N.A. Golilarz, "Edge Computing for IoT-Enabled Smart Grid", Security and Communication Networks, pp. 5524025, 2021.

[5] F.E. Hachemi, M. Mana, and B.A. Bensaber, "Study of the Impact of Sinkhole Attack in IoT Using Shewhart Control Charts", in Editor (Ed.)^(Eds.): 'Book Study of the Impact of Sinkhole Attack in IoT Using Shewhart Control Charts' (edn), pp. 1-5, 2020.

[6] A. Verma, and V. Ranga, "Analysis of routing attacks on RPL based 6LoWPAN networks", International Journal of Grid and Distributed Computing, 11, pp. 43-56, 2018.

[7] M. Koosha, B. Farzaneh, and S. Farzaneh, "A Classification of RPL Specific Attacks and Countermeasures in the Internet of Things", in Editor (Ed.)^(Eds.): 'Book A Classification of RPL Specific Attacks and Countermeasures in the Internet of Things' (edn.), pp. 1-7, 2022.

[8] R. Raman, B. Mandaloju, D. Singh, V. Tripathi, U.H. Maginmani, and J.L.A. Gonzáles, "An Experimental Study of Sink Hole Attacks and Distributed

Denial of Service (DDS) on IoT network-based Healthcare Applications", in Editor (Ed.)^(Eds.): 'Book An Experimental Study of Sink Hole Attacks and Distributed Denial of Service (DDS) on IoT network based Healthcare Applications' (edn.), pp. 990-993, 2023.

[9] A.K. Bediya, and R. Kumar, "Real Time DDoS Intrusion Detection and Monitoring Framework in 6LoWPAN for Internet of Things", in Editor (Ed.)^(Eds.): 'Book Real Time DDoS Intrusion Detection and Monitoring Framework in 6LoWPAN for Internet of Things' (edn.), pp. 824-828, 2020.

[10] Z. Fatima, N. Jhanjhi, S.N., Brohi, and N.A. Malik, "Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning", in Editor (Ed.)^(Eds.): 'Book Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning' (edn.), pp. 1-9, 2019.

[11] A. Jahangeer, S.U. Bazai, S. Aslam, S., Marjan, M., Anas, and S.H. Hashemi, "A Review on the Security of IoT Networks: From Network Layer's Perspective", IEEE Access, 11, pp. 71073-71087, 2023.

[12] S. Cakir, S., Toklu, and N. Yalcin, "RPL Attack Detection and Prevention in the Internet of Things Networks Using a GRU Based Deep Learning", IEEE Access, 8, pp. 183678-183689, 2020.

[13] M. Hasan, M.M., Islam, M.I.I. Zarif, and M.M.A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches", Internet of Things, 7, pp. 100059, 2019.

[14] I.F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study", Computer Networks, 188, pp. 107840, 2021.

[15] A.M. Pasikhani, J.A. Clark, P. Gope, and A. Alshahrani, "Intrusion Detection Systems in RPL-Based 6LoWPAN: A Systematic Literature Review", IEEE Sensors Journal, 2021, 21, (11), pp. 12940-12968, 2021.

[16] M.D Momand, M.K. Mohsin, M.K., and I-ul-Haq: 'Machine Learning-based Multiple Attack Detection in RPL over IoT', in Editor (Ed.)^(Eds.): 'Book Machine Learning-based Multiple Attack Detection in RPL over IoT' (2021, edn.), pp. 1-8

[17] F. Zahra, N.Z. Jhanjhi, S. Brohi, N.A. Malik, and M. Humayun, "Proposing a hybrid RPL protocol for rank and wormhole attack mitigation using machine learning". Proceedings of the 2nd International Conference on Computer and Information Sciences (ICCIS). 2020. https://doi.org/10.1109/ICCIS49240.2020.9257607

[18] A, Jamalipour, and S. Murali, "A Taxonomy of Machine-Learning-Based Intrusion Detection Systems for the Internet of Things: A Survey", IEEE Internet of Things Journal, 9, (12), pp. 9444-9466, 2022.

[19] A. Verma, and V. Ranga, "ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things", in Editor (Ed.)^(Eds.): 'Book ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things' (edn.), pp. 1-6, 2019.

[20] B. Chen, Y. Li, and D. Mashima, "Analysis and enhancement of RPL under packet drop attacks", in Editor (Ed.)^(Eds.): 'Book Analysis and enhancement of RPL under packet drop attacks' (edn.), pp. 167-174, 2018.

### 4.2.2 Article 2

#### 1. Article publication details

**Title:** A Systematic Literature Review on Defence Techniques against Routing Attacks in the Internet of Things

Status: Published

#### 2. Article synthesis

(i) Purpose

This article provides a robust and comprehensive analysis by synthesising existing research on routing attacks and the defence techniques in IoT RPL-based networks. It achieves this by investigating the secure-protocol, conventional IDS and ML-based IDS techniques. The article identifies their effectiveness, deployment, and application in predicting and alleviating routing attacks and offers insights into the state of RPL security. The article also identifies shortcomings in existing research and suggests avenues for future investigations to enhance IoT network security.

(ii) Methods

The study utilised a SLR research methodology to collect and analyse 39 relevant published studies between 2021 and 2024. Publications were extracted using search keys from scholarly databases like IEEE, Scopus, ScienceDirect, and MDPI.

(iii) Results and Discussion/ Findings

The review is structured into two main sections: a cross-sectional comprehensive analysis of defence techniques (article distribution, simulation tools, and configurations) and a synthesis of related studies highlighting the scope of work, strengths, and challenges. Key findings include the prominence of ML-based IDS, constituting 43.59% of the selected publications, flooding attacks topping the attack category, appearing 22 times over 122 attack instances. It is established that commonly used simulation tools include Cooja Contiki OS, MATLAB, NetSim,

OMNeT++, and NS3, with varying simulation configurations. Subsequently, Cooja contributes 76% usage in the publications. The study further presents metrics for assessing the efficacy of defence strategies, demonstrating that detection accuracy is the most prominent metric for the evaluation of the technique. The review concludes with recommendations for improving defence techniques and addressing challenges like energy efficiency in low-power IoT devices.

(iv) Conclusion

This article presents a comprehensive systematic review of defence techniques against attacks on routing in LLNs. Defensive strategies can be classified into secure-protocol, conventional IDS, and ML-based IDS. Moreover, ML-based IDSs are the most researched between 2021 and 2024, demonstrating their adoption as a defence technique to identify bogus network traffic for IoT networks.

## 3. Full paper

# A Systematic Literature Review on Defense Techniques Against Routing Attacks in Internet of Things

ARTICLE HISTORY

Received 17 September 2024
Accepted 28 October 2024

Lanka Chris Sejaphala
dept. Computer Science and Information Systems
North-West University
Vaal Triangle, South Africa
Chris.Sejaphala@nwu.ac.za
ORCID: 0000-0003-1321-9557

Vusimuzi Malele
dept. Computer Science and Information Systems
North-West University
Vaal Triangle, South Africa
Vusi.Malele@nwu.ac.za
ORCID: 0000-0001-6803-9030

Francis Lugayizi
dept. Computer Science and Information Systems
North-West University
Mmabatho, South Africa
Francis.Lugayizi@nwu.ac.za
ORCID: 0000-0002-5666-4805

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025



L.C. Sejaphala, V. Malele, and F. Lugayizi,
"A Systematic Literature Review on Defense Techniques Against Routing Attacks in Internet of Things",
Latin-American Journal of Computing (LAJC), vol. 12, no. 1, 2025.

# A Systematic Literature Review on Defense Techniques Against Routing Attacks in Internet of Things

Lanka Chris Sejaphala
*dept. Computer Science & Information Systems*
North-West University
Vaal Triangle, South Africa
Chris.Sejaphala@nwu.ac.za
ORCID: 0000-0003-1321-9557

Vusimuzi Malele
*dept. Computer Science & Information Systems*
North-West University
Vaal Triangle, South Africa
Vusi.Malele@nwu.ac.za
ORCID: 0000-0001-6803-9030

Francis Lugayizi
*dept. Computer Science & Information Systems*
North-West University
Mmabatho, South Africa
Francis.Lugayizi@nwu.ac.za
ORCID: 0000-0002-5666-4805



***Abstract***— The proliferation of the Internet of Things (IoT) has attracted different sectors such as agriculture, manufacturing, smart cities, transportation, etc. to adopt these technologies. Most IoT networks utilize Routing Protocol for Low Power and Lossy Networks (RPL) to exchange control and data packets across the network. However, RPL is susceptible to routing attacks such as rank attacks, DIS-flooding, etc. In recent years, different defense techniques have been proposed to act against these attacks i.e., Secure-Protocol, conventional Intrusion Detection Systems (IDS), and Machine Learning (ML)-based. This systematic literature review explores 39 published papers in the domain of defense techniques against routing attacks in RPL-based IoT. The findings of this study suggest that most Secure-Protocol can detect and mitigate routing attacks utilizing distributed placement, ML-based can detect most attacks but lack mitigation mechanisms, and conventional IDS technique utilizes a hybrid approach in detection and placement strategies. Additionally, this study reveals that India publishes more research papers in ML-based and Secure-Protocol. Furthermore, flooding attacks are the most discussed attacks in the selected studies. Finally, Cooja Contiki is the most used simulation tool.

***Keywords***—*Defense technique, RPL, Routing attacks, IoT*

## I. Introduction

The Internet of Things (IoT) emerges with different innovations including smart agriculture, environmental monitoring, and smart grids, to name a few [1]. However, the broad adoption of IoT faces challenges in terms of security due to some of its characteristics, i.e., direct access to devices from the internet, the communication nature of wireless media, and potential unattended operations of relevant deployment. One of the significant enablers of IoT technology is the Low-power and Lossy Networks (LLNs) which comprise interconnected devices with low computational capabilities and less storage and are often operating on batteries such as sensor nodes and actuators [2]. Communication technologies in LLNs are subjected to limitations such as short communication range, high packet loss, low data rate, dynamically changing topology and frame size limitations. Such limitations render the development of efficient routing protocols for LLNs of significant importance. Routing is one of the fundamental driving forces of LLNs, it provides connectivity to various applications and enables seamless communication among IoT devices [3]. LLNs run on resource-constrained devices like radio transceivers and ultra-low powered micro-controllers as such, traditional routing protocols like Ad hoc On-Demand Distance Vector (AODV), Open Shortest Path First (OSPF), Dynamic Source Routing (DRS) are not suitable to facilitate data transmission between such devices due to network and device characteristics[4].

To overcome the limitations of traditional routing protocols in LLNS, the Internet Engineering Task Force (IETF) group for Routing Over Loss-power and Lossy Networks (ROLL) has introduced and standardized the IPv6 Routing Protocol for low-power and Lossy Networks (RPL) to meet various requirements of applications and obligations [5]. Moreover, it satisfies the routing necessities of LLNs [6]. It is worth noting that, the RPL as a prominent infusion to routing limitations in IoT is vulnerable to many network layer attacks, particularly routing attacks [7]. Some examples are DIS Flooding, Rank, Sinkhole, and Worst Parent attacks. These attacks exploit the vulnerabilities inherent in RPL-based IoT systems by consuming device power, causing topology inconsistencies, dropping data packets, and creating delays in packet delivery.

Recent review works demonstrate that RPL is susceptible to many routing attacks, additionally, several researchers have proposed defense techniques [8-10] to defend the IoT from those routing attacks. However, these studies do not discuss the three techniques this study covers i.e., Secure-Protocol,

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: 10.5281/zenodo.14449371

conventional Intrusion Detection Systems (IDS), and Machine Learning (ML)-based defense techniques in one paper. To the best of our knowledge this is the first review to discuss traditional and advanced defense techniques and to provide a link between publication country of origin, adopted defense technique, academic library, and year of publication. The contributions of our study are as follows 1) provide a comprehensive SLR method relevant to different RPL defense techniques, 2) formulate a set of research questions pertinent to various defense techniques, distributions of publications, statistics of network simulation tools, configurations setups, and discussed attacks. 3) provide a link between the publications of the origin country, defense techniques adopted, academic library, and year of publication.

The rest of the paper is organized as follows, section II provides related work of the study, Section III discusses the methodology used to conduct this SLR study, a discussion of results is presented in Section IV, and lastly, the conclusion in Section V.

## II. Related works

The advent of IoT networks and their applicability in different sectors has ignited significant academic and industrial interest, especially in RPL security. This section provides a review of related work in the domain of security techniques in RPL-based IoT. We rigorously identify and evaluate four existing systematic review and traditional review papers that are pertinent to the critical aspects of our domain of interest.

Authors of [11] conducted a comprehensive traditional review comparing the Secure-Protocol and IDS security solutions. They, furthermore, gave an analysis of the RPL-specific attacks and their countermeasures highlighting essential attributes i.e., topology, resources, and traffic affected by these attacks. The study [8] provides an analysis of machine learning-based techniques to secure IoT following the SLR methods. The study presents a comprehensive review of different machine learning detection models and their pros and cons. However, the study is focused on application layer attacks.

The study [10] presents an extensive review of several routing attacks. In addition, it further provides an in-depth description of IDS and its different detection strategies that can be adopted for the detection of routing attacks. However, the study lacks an analysis of Secure-Protocol defense techniques. Authors of the study [9] demonstrated the significance of the Secure-Protocol as a defense technique against routing attacks. They further provide a distribution of publications; however, the study lacks a relationship between the publication year, country of origin, academic library, and defense techniques.

Table I below provides a summarized analysis of the related work.

TABLE I. SUMMARY OF RELATED STUDIES

| Study | Scope of work | Strength | Similarity with our study | Limitation |
|---|---|---|---|---|
| [11] | A review of comparison of Secure-Protocol and IDS, RPL-specific attacks and their countermeasures, attack taxonomy, and cross-layer security solution for RPL | The study provides an in-depth analysis of RPL-specific attacks and their countermeasures. | Overview of security solutions for RPL | The study lacks a review of Machine learning as a potential security solution |
| [8] | SLR on machine learning and deep learning-based techniques to detect large-scale attacks | The paper presents a comprehensive review of machine learning and deep learning-based techniques | Overview of machine learning techniques | The paper lacks a review of traditional solutions i.e., Secure-Protocol and their attack focus is not routing attacks. |
| [10] | SLR on RPL and its existing threats, and classification of IDS techniques. | The study presents an extensive review of RPL threats and the classification of relevant IDS techniques. | Overview of IDS techniques | The research paper lacks a review of Secure-Protocol and machine-learning defense techniques |
| [9] | SLR on attacks defense mechanisms in RPL-based 6LoWPAN | The review provides a comprehensive in-depth analysis of various RPL security mechanisms, challenges, key issues, and recommends future research directions. | Overview of secure-protocol techniques | The study lacks a review of both IDS and machine learning-based defense techniques |

## III. Research methodology of SLR study

To gain an insight into which studies have been publishing in the sphere of defense techniques against routing attacks in LLN, the Systematic Literature Review (SLR) method was adopted in this article. This section of the article covers each step of SLR methodology in detail. In sections B, C, and D, the paper gives an explanation of key concepts of the SLR protocol, followed by Section E which explains the validation results of collected and synthesized publications

### *A. Research questions and SLR protocol*

This paper aims to evaluate studies between 2018 and 2023 in the domain of defense techniques against routing attacks in RPL-based IoT have been conducted. To achieve this goal, it is required an understanding of RPL and different routing attacks that are threats to the RPL-based IoT. Secondly, we investigate different defense techniques which are proposed in the year range. This includes compiling findings, outlining weaknesses and strengths, and presenting empirical evidence in detecting and mitigating routing attacks.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: 10.5281/zenodo.14449371

Lastly, give recommendations, challenges, and future research areas. To meet the objectives, we formulated several research questions as follows:

- RQ1: What is the distribution of studies into defense techniques in RPL-based IoT regarding country of origin, year of publication, type of defense technique, and academic library?
- RQ2: Which simulation tools are mostly used, and which configurations are mostly used particularly simulation area, simulation time, transmission range, and interference range?
- RQ3: Which attributes can be used to evaluate the robustness of defense techniques?
- RQ4: Which types of detection and placement strategies demonstrate the capability of addressing most attacks?
- RQ5: Which routing attacks are mostly addressed by the proposed defense techniques?
- RQ6: Which proposed techniques are capable of detecting and mitigating routing attacks?
- RQ7: Which performance metrics are commonly used to evaluate the performance of defense techniques?
- RQ8: What are the best defense techniques, detection and placement strategies, challenges, and future research areas?
-

### *B. Identification of academic databases and Search keywords*

In this step, we explored academic information sources, and four databases were exploited to extract and collect publications for inclusion in the subsequent extraction and synthesis procedure. In this article, a set of search keywords is declared by the union of specific and broad keywords to achieve a reasonable number of publications that are suitable to the research topic. From background section 2.1, RPL is a standardized routing protocol for IoT specifically LLN networks, However, the 'IoT' keyword is implicit in most publications, and 'RPL' is in the title abstract and keyword sections. So, we used two sets of keywords relevant to IoT and RPL subjects to collect publications. But, because we want an insight into defense techniques, we added two more sets of keywords 'mitigation technique', 'security model', 'defense strategy', 'detection scheme'; and 'routing attacks', and 'network layer attacks' to have two groups of keywords. It is worth mentioning that we eliminated keywords that were not relevant to the scope of this article.

### *C. Publications selection criterion*

This step outlines the publication selection criteria used to retrieve publications aligned with the scope of this article. We used five factors to select and include publications that are aligned with our article, namely: publication year, language, duplications, type of publication, and availability of full text. First, we defined a publication year filter from 2018 to 2024 to include studies. Secondly, we only included publications that are published in the English language. This was done manually by screening the title and abstract of the studies. Thirdly, manually checking whether there are no duplicated publications from multiple databases. Fourthly, we determined the type of publication. In this procedure, we only considered studies that are conference proceedings, journal articles, and/or book chapters. And lastly, we only considered publications from which we could get their full-text reading. Table II below presents a summary of inclusion and exclusion elements considered in this study.

TABLE II. LIST OF PUBLICATIONS SELECTION CRITERIA

| Inclusion | Exclusion |
|---|---|
| Published between 2018 & 2024 | A study is a duplicate |
| Written in the English language | Published in a language other than English |
| A study remains within the borders of routing attacks in RPL | Not relevant to the scope of this article |
| A study is a journal article, a book chapter, and a conference proceeding | It is a grey literature |
| Full-text reading is available | Full-text reading is not available |

### *D. Extraction of articles and synthesis*

In this step, we explain how the final set of selected publications was produced from the initial set of retrieved publications. We explored the titles and abstracts of the selected publications to identify those that are relevant to RPL or LLN research and excluded those that are not. We further used the full-text read to include publications that focus on the prevention, mitigation, and detection of routing attacks in RPL.

### *E. Validation results*

In the last step of our SLR study, we present three broad steps used to select studies. Refer to Fig. 1. The selected four databases of digital libraries produced 5,848 results with 1,513 from IEEE Xplore, 1,403 from ScienceDirect, 1,176 from MDPI, 962 from Springer, and 794 from IEEE Access. We then applied the publication year range and studies written in English exclusion criteria which reduces the results to 1,241. Excluding 685 duplicate studies the returned results were then reduced to 556.

To select relevant RPL-based studies within our scope, we screened their titles and abstracts, resulting in the exclusion of 319 and the inclusion of 237. The final set of studies which formed part of this SLR was a result of the conducted full-text reading and it was discovered that only 39 studies were relevant to the scope of this study.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: 10.5281/zenodo.14449371

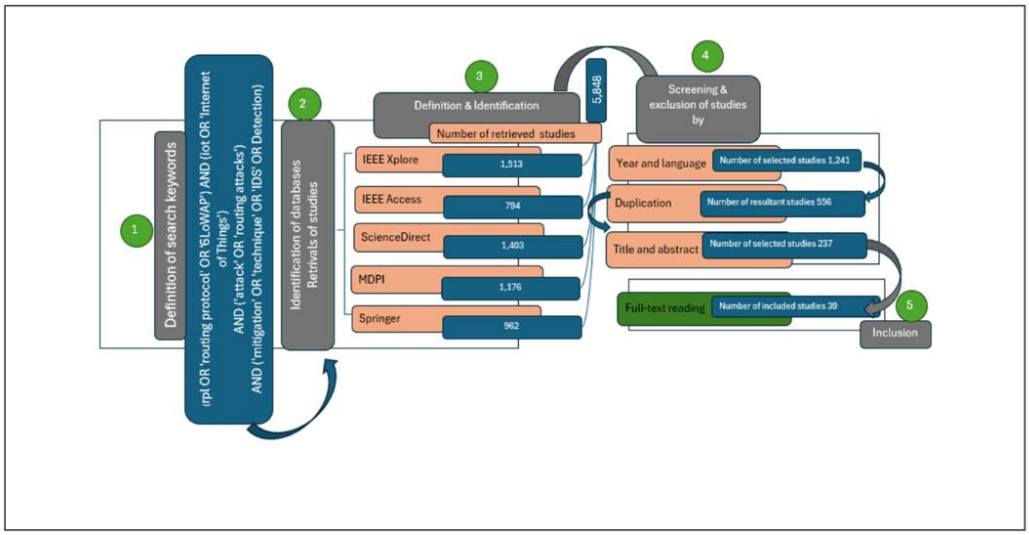


Fig. 1 Diagrammatic representation of SLR methodology steps

## IV. Results and Discussion

This paper focuses on reviewing proposed defense techniques and determining the most suitable technique to defend RPL-based IoT against routing attacks. Thus, 39 publications proposing defense techniques are selected and critically evaluated to answer the research questions provided in the methodology section and achieve the objective of this paper.

*1) RQ1: What is the distribution of studies into defense techniques in RPL-based IoT regarding country of origin, year of publication, academic library, and type of defense technique?*

It is important to understand the distribution of publications, including academic sources, year of publication, defense technique, and country of origin. This information gives an insight into the spread of publications across countries, years, and academic libraries.

Fig. 2 presents the percentages of distribution of the selected studies across the four academic databases mentioned in section 4. Most of the studies were found in the IEEE Xplore and Science Direct constituting 44% and 23% respectively.

Furthermore, Fig. 3 depicts that most of the selected publications were published in 2022, 2021, and 2023 with 11, 9, and 8 publications, respectively.

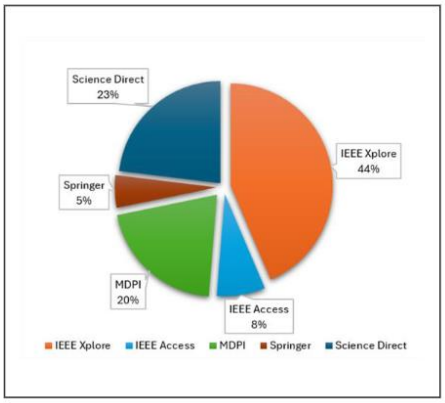


Fig 2 Contribution of Academic Libraries

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: 10.5281/zenodo.14449371

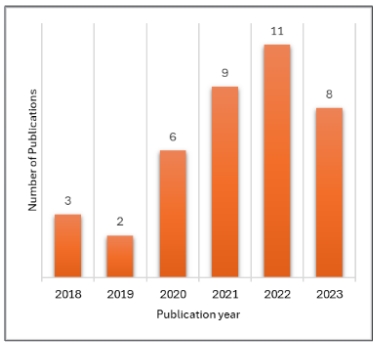


Fig. 3 Distribution of publications by year

It is also important to note that most of the selected publications proposed Machine Learning-based IDS as their defense techniques. As depicted in Fig. 4, ML-based IDS is the first largest proposed defense technique amounting to 17 publications; 11 are traditional Machine Learning, 4 are Deep Learning (DL), and 2 are Reinforcement Learning(RL). The second largest defense is Secure-Protocol with 14 publications in total and a threshold-based detection strategy is proposed in 5 studies followed by specification and trust-based detection strategies proposed in 3 studies each. Furthermore, Conventional Intrusion Detection Systems (IDS) constituted 8 publications. Four techniques were found in IDS studies i.e., anomaly, specification, signature, and hybrid. Anomaly and Hybrid detection strategies are each proposed in 3 studies.

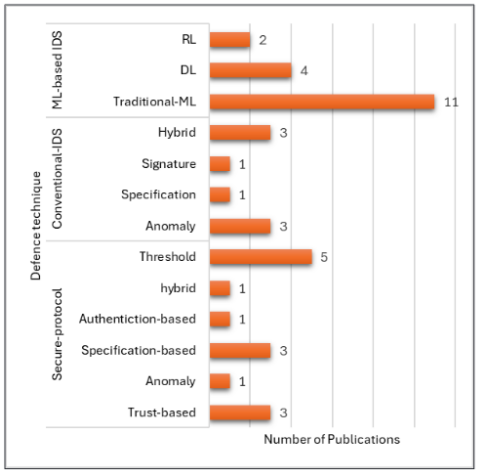


Figure 4 Distribution of different defense techniques and the adopted detection strategies

Fig. 5 presents the country of origin of the selected studies. Most of the selected publications are written by authors from India which are 12 in total followed by the UK with 6 publications. Furthermore, Saudi Arabia, Canada, Algeria, Malaysia, and Turkey, each has 2 papers from the selected studies.

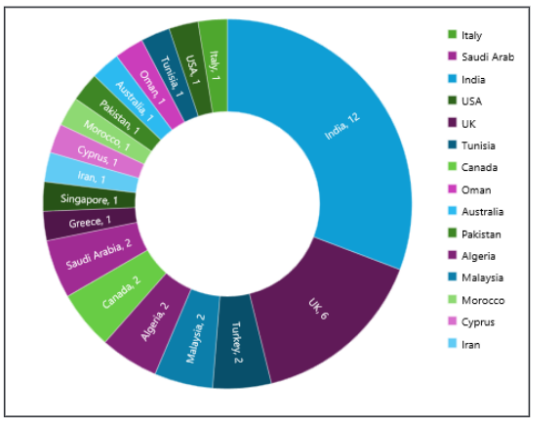


Fig. 5 Contribution by Country of origin

However, the information presented in Fig. 2,3,4 & 5 does not tell us the story as there is no link between them. Most of the SLR studies do present this information without including the link [9] we saw this as a loophole in most SLR and traditional literature review studies. We then developed a way to present the link between the distribution information of publications in Table III which presents the link between the distribution factor of publications.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: 10.5281/zenodo.14449371

TABLE III. DISTRIBUTION OF DEFENSE TECHNIQUES IN ACADEMIC LIBRARY, COUNTRY OF ORIGIN AND YEAR OF PUBLICATIONS

| | | Defense Techniques | | |
|---|---|---|---|---|
| | | **Secure-Protocol** | **Conventional IDS** | **ML-based IDS** |
| **Academic Libraries** | **IEEE Xplore** | Canada[1 \| 2022]<br>India[1 \| 2021]<br>USA[1 \| 2018]<br>Singapore[1 \| 2018] | Turkey [1 \| 2021]<br>India[1 \| 2022; 1 \| 2018]<br>Italy[1 \| 2021] | India[2 \| 2021; 1 \| 2022; 1 \| 2019]<br>Canada[1 \| 2023]<br>UK[1 \| 2022; 1 \| 2021]<br>Cyprus[1 \| 2020]<br>Morocco[1 \| 2020] |
| | **IEEE Access** | Saudi Arabia[1 \| 2022]<br>UK[1 \| 2020] | | Turkey[1 \| 2020] |
| | **MDPI** | Saudi Arabia[1 \| 2020]<br>Algeria[1 \| 2023] | UK[2 \| 2022] | Oman[1 \| 2023]<br>Malaysia[2 \| 2022]<br>Australia[1 \| 2023] |
| | **Springer** | India[1 \| 2021] | | Tunisia[1 \| 2023] |
| | **Science Direct** | Algeria[1 \| 2021]<br>Iran[1 \| 2022]<br>Pakistan[1 \| 2020]<br>India[1 \| 2022; 1 \| 2023] | Greece[1 \| 2021]<br>India[1 \| 2019] | UK[1 \| 2023]<br>India[1 \| 2022] |

The table gives an insight into the distribution of publications. It also demonstrates which defense techniques are most proposed in which countries and academic libraries e.g. ML-based IDS is mostly published in IEEE Xplore with 9 publications of which 5 are from India followed by the UK with 2 publications. Malaysia published 2 ML-based IDS studies with MDP. However, the second country to publish the most ML-based IDS is the UK with 3 followed by Malaysia across our academic libraries. It can also be seen that India, and the UK are the leading countries to propose Conventional IDS as a defense technique against routing attacks with 2 studies each. Between 2021 and 2023 it appears that Secure-Protocol has been proposed mostly in India, constituting 4 publications followed by Saudi Arabia with 2 in 2020 and 2022.

*2) RQ2: Which simulation tools are mostly used, and which configurations are used particularly simulation area, simulation time, transmission range, and interference range?*

It is observed that studies conduct their simulations using Cooja Contiki OS, MATLAB, NetSim, OMNET++, and NS3. From the selected studies 28 used Cooja Contiki OS, then 6 used MATLAB and NetSim equally, furthermore, 2 used OMNET++ and lastly, only one study was found to have used NS3 and Cooja Contiki OS. Fig. 6 presents a graphical presentation of the used simulation tools.

It is also identified that two studies did not disclose the simulation tools that they used in their experiments [12] & [13]. It is likewise noted that the selected studies choose simulation environments ranging from 100x100m to as large as 1000x1000m except for studies [14] & [15] that choose 70x70m and 5x5m, respectively. Furthermore, the transmission range of nodes in the network was also seen from the selected studies, and it was deduced that 9 of the selected studies used a transmission range configuration of 50m, whereas only one study [16] opted for a transmission range of 100m, however, the simulation area is not presented in that study.

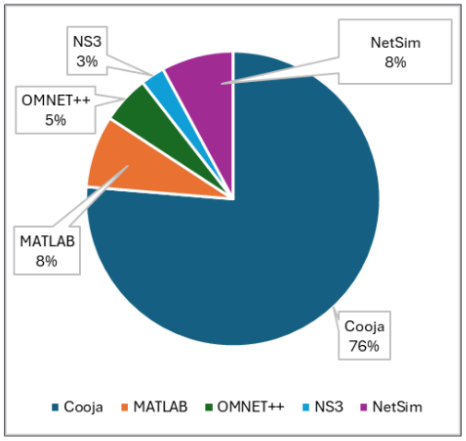


Fig. 6 Percentage of usage of simulation tools

Table IV below shows the technical configurations of the simulation area as well as adopted defense techniques, detection, and placement strategies. It is used to answer RQ2, RQ3, and RQ4.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: 10.5281/zenodo.14449371

TABLE IV. TECHNICAL ANALYSIS OF PROPOSED DEFENCE TECHNIQUES

| Study | Defense Technique | Detection strategy | Placement strategy | Network Size | malicious nodes | Mobility | Tools | No of Attacks | Simulation Area (m) | Trans Range (m) | Inter Range (m) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| [2] | Secure-Protocol | Threshold-based | Distributed | 50 | 2,5,10 | Yes | Cooja | 1 | 300x200 | - | - |
| [5] | Secure-Protocol | Trust-based | Distributed | 50, 100, 150 | 10% | Yes | MATLAB | 1 | 100x100 | - | - |
| [17] | Secure-Protocol | Threshold-based | - | 20,40 | - | - | Cooja | 4 | 20x20 | - | - |
| [1] | Secure-Protocol | Threshold-based | - | 25 | - | Yes | Cooja | 1 | 100x100 | 30 | 25 |
| [3] | Secure-Protocol | Trust-based | Decentralized | 35 | 3 | Yes | Cooja | 1 | - | 50 | - |
| [4] | Secure-Protocol | Authentication-based | Distributed | 18, 28 | 3 | Yes | Cooja | 1 | 200x200 | 50 | - |
| [18] | Secure-Protocol | Trust-based | Distribution | 28 | 2 | No | Cooja | 3 | 210x150 | - | - |
| [6] | Secure-Protocol | Hybrid (thresh-spec) | Distributed | 30 | 5 | No | Cooja | 1 | - | 50 | - |
| [19] | Secure-Protocol | Threshold-based | Distributed | 100 | 30 | No | OMNeT++ | 1 | 200x200 | 30 | - |
| [20] | Secure-Protocol | Anomaly-based | Distributed | 50 | 1 | No | Cooja | 1 | 280x150 | 50 | 70 |
| [21] | Secure-Protocol | Specification-based | Distributed | 50 | 10 | No | Cooja | 1 | 100x100 | 30 | 25 |
| [22] | Secure-Protocol | Specification-based | Distributed | 25,40,65 | - | No | Cooja | 1 | 300x300 | 25 | 50 |
| [23] | Secure-Protocol | Specification-based | Distributed | 13 | 1 | No | Cooja | 1 | 200x200 | 50 | 100 |
| [24] | Secure-Protocol | Threshold-based | Distributed | 20 | 4,1 | No | Cooja | 2 | 100x100 | 50 | 100 |
| [25] | Conventional-IDS | Anomaly-based | Hybrid | 8,16,24 | 12 | No | Cooja | 1 | - | - | - |
| [26] | Conventional-IDS | Anomaly-based | Hybrid | 10 | 1 | No | Cooja | 1 | - | - | - |
| [27] | Conventional-IDS | Hybrid | Centralized | 16 | 1 | No | NetSim | 14 | - | - | - |
| [28] | Conventional-IDS | Specification-based | Distributed | 10,20,30,40,50,60 | - | - | MATLAB | 2 | 1000x1000 | - | - |
| [14] | Conventional-IDS | Anomaly-based | Distributed | 36 | 6 | No | Cooja, NS3 | 2 | 70x70 | - | - |
| [29] | Conventional-IDS | Hybrid(Sig-Spe) | Hybrid | 12 | 1 | - | Cooja | 6 | - | - | - |
| [30] | Conventional-IDS | Signature-based | Central | 30 | 20% | - | Cooja | 4 | - | - | - |
| [31] | ML-Based | Supervised-learning | Distributed | 30 | - | - | Cooja | 3 | 100x100 | - | - |
| [32] | ML-Based | Supervised-Learning | Centralized | 10,20,40,100 | 2,4,8, 10 | No | Cooja | 5 | - | - | - |
| [16] | ML-Based | Reinforcement-Learning | Centralized | 30 | 1 | No | Cooja | 1 | - | 100 | 30 |
| [12] | ML-Based | Deep-Learning | - | - | - | - | - | 1 | - | - | - |
| [33] | ML-Based | Supervised-learning | Decentralized | 16,32,64,128 | 10%, 20%, 30% | Yes | NetSim | 10 | 250x250 | 50 | - |
| [34] | ML-Based | Supervised-Learning | Centralized | - | - | - | Cooja | 4 | - | - | - |
| [35] | ML-Based | Supervised-Learning | - | 25 | 1 | - | Cooja | 3 | 200x200 | - | - |
| [13] | ML-Based | Supervised-Learning | - | 30 | 6 | | - | 2 | - | - | - |
| [36] | ML-Based | Deep-Learning | - | 10 | 2 | No | Cooja | 1 | - | - | - |
| [15] | ML-Based | Supervised-Learning | - | 25 | - | No | Cooja | 1 | 5x5 | - | - |
| [37] | ML-Based | Supervised-Learning | Centralized | - | - | No | MATLAB | 7 | - | - | - |
| [38] | ML-Based | Reinforcement-Learning | Decentralized | 16,32,64,128 | 10%, 20%, 30% | Yes | NetSim | 8 | 850x850 | 50 | - |
| [39] | ML-Based | Deep-Learning | Centralized | 6,11,16 | 1,1,3 | No | Cooja | 1 | - | 50 | - |
| [40] | ML-Based | Deep-Learning | - | 100 | 6 | - | OMNeT++ | 3 | 500x500 | 60 | - |
| [41] | ML-Based | Supervised-Learning | - | 50 | 2 | Yes | Cooja | 2 | - | - | - |
| [42] | ML-Based | Supervised-Learning | - | 11 | 3 | - | Cooja | 7 | 200x200 | - | - |
| [43] | ML-Based | Supervised-Learning | - | 20,50 | - | - | Cooja | 2 | - | 50 | 100 |

*3) RQ3: Which attributes can be used to evaluate the robustness of defense techniques?*

In most IoT applications, devices are deployed in large numbers. Hence, network size and number of malicious nodes in a network, play a vital role in testing the robustness of security solutions in IoT environments.

The authors of the study [2] considered a network size of 50 nodes against 10 malicious nodes to test the robustness of their proposed scheme. Similarly, authors of the study [5] implemented three scenarios in their study, where they have 50, 100 & 150 network sizes with 10% of each network size as the malicious nodes. However, they only considered one type of attack in their study. In contrast, the study [18] despite

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: 10.5281/zenodo.14449371

having a smaller network size of 28 nodes and less number of malicious nodes of two nodes as compared to the studies [2] & [5], they tested the robustness of their proposed scheme by having multiple types of attacks in their study. It is relevant to consider multiple types of attacks when developing a defense scheme for networks such as IoT because these types of networks are susceptible to different types of attacks. In [30], the authors tested the robustness of their proposed scheme in a 30-node network size with 10% of them as malicious nodes where they implemented 4 different types of attacks in their scenarios. This ensures that the defense scheme can address multiple attacks. Furthermore, there are studies that considered a larger number of different types of attacks but only one malicious node was considered [7] & [27]. The former implemented two scenarios with 25 & 50 nodes in their network, while the latter only had 16 nodes in their simulation. However both studies considered a large number of attacks. Although, the robustness of their defense scheme might be jeopardized because of the number of malicious nodes considered and the network size. The study [33] demonstrated a desirable robustness test. By implementing scenarios of 16,32,64, & 128 network sizes and 10%,20%, & 30% as malicious nodes in each scenario. The study addressed eight different routing attacks. Though network size and the number of malicious nodes can be used to evaluate the robustness of the defense techniques, multiple attacks can also add a cherry on top.

*4) RQ4: Which types of detection and placement strategies demonstrate the capability of addressing most attacks?*

In this study, we demonstrated that three types of defense techniques can be employed to defend IoT networks against routing attacks, i.e., Secure-Protocol, conventional IDS, and ML-based IDS. However, the effectiveness of these techniques depends on the adopted detection strategy i.e., threshold, trust-based, signature-based, anomaly-based, hybrid, supervised-learning-based, etc., and placement strategy i.e., distributed, centralized, and hybrid. An adopted detection strategy that can address more than two attacks could be very effective in defense against routing attacks.

Authors of [17], adopted a threshold-based detection strategy to address four types of attacks. Althought they did not present their placement strategy it can be assumed to be distributed. Whereas authors in [18], adopted a trust-based strategy to detect three types of routing attacks. Studies by [7] & [29] adopted a hybrid strategy for both detection and placement in their proposed IDS techniques. The former can detect thirteen attacks, while the latter addresses six attacks. Moreover, they [27] adopted a hybrid detection strategy and utilized a centralized placement strategy to act against fourteen routing attacks. Authors of [30] adopted a signature-based detection strategy which is centralized to detect four attacks in their IDS. Studies that employ ML-based defense techniques appear to address more attacks than both IDS and Secure-protocol, where a centralized supervised learning-based detection strategy is realized [32], [34] & [37]. However, in [33], although they utilized supervised-learning-based detection the placement strategy used is decentralized, and their proposed technique addresses a total of eight attacks. Centralized placement of detection strategy appears to be effective, especially in a network of resource-constrained devices like LLNs. However, to consider mitigation of the attacks nodes in the network must participate; therefore, a hybrid placements strategy can be very effective in detecting and ensuring mitigation of routing attacks in RPL-based IoT networks, while both hybrid and supervised learning-based detection strategies demonstrate their effectiveness in addressing multiple attacks.

*5) RQ5: Which routing attacks are mostly addressed by the proposed defense techniques?*

Routing attacks can be divided into three categories according to their impact on the network i.e., traffic, network device resource, and topology impacting attacks. Traffic-impacting attacks such as Sinkholes, Wormhole, Blackhole, Grayhole, etc. are considered the most detrimental attacks in IoT [9, 27, 44]. However, flooding attacks seem to top the list of most investigated attacks in the selected studies. Flooding attacks exhaust the resources of network devices in the case of RPL-based IoT, particularly the energy of the devices, since most of the IoT devices are battery-powered. Furthermore, DIS-flooding attacks prevent nodes from participating in the transmission of both data and control messages. Fig. 7 below presents the distribution of investigated attacks in the selected studies.

It is found that 22 flooding attacks were investigated in the selected studies, followed by 16 rank attacks, which are resources and topology-impacting attacks, respectively.

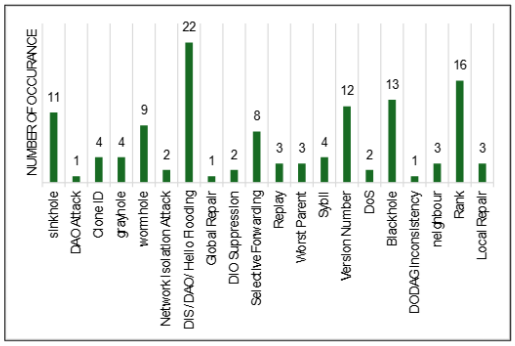


Fig. 7 Distribution of discussed attacks in the selected studies

Moreover, the hole-family attacks i.e., Blackhole, Sinkhole, and Wormhole which are traffic-impacting attacks were found to be 13,11, & 9, respectively. Version Number attacks impact topology and, therefore, affect end-to-end delay and it appears 12 times in the selected studies as one of the most investigated attacks. To this end, it is evident that Flooding attacks, Rank attacks, Blackhole attacks, Version Number attacks, and Sinkhole attacks appear to be investigated most in the literature.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: 10.5281/zenodo.14449371

*6) RQ6: Which proposed techniques are capable of mitigating routing attacks?*

Applications of IoT span multiple sectors including manufacturing, agriculture, health, smart homes and cities [45] as such their security is of great importance. However, in the case of attacks in the network, it is significant to detect and mitigate those attacks to allow normal functionality of the network. When developing defense techniques against attacks, more especially routing attacks mechanisms must be in place to then mitigate the attacks. Most of the Secure-Protocol techniques in the selected publications demonstrate the capability to mitigate the routing attacks that is 11 out of 13 proposed techniques mitigate the attacks. However, in studies that proposed IDS as their defense technique only 2 studies out of 8 can mitigate the attacks. Additionally, while ML-based defense techniques demonstrate a high detection rate, they lack mitigation mechanisms. Of the selected studies that employ ML as their defense only one study presented that their proposed technique could mitigate the attacks. The Secure-Protocol defense techniques demonstrate the results of attack mitigation.

*7) RQ7: Which performance metrics are commonly used to evaluate the performance of defense techniques?*

To evaluate the performance of RPL-based IoT networks several performance metrics can be used such as Packet Delivery Ratio (PDR), Control Message Overhead (CMO) which represents the number of control messages generated during an attack, throughput, End-to-End Delay (E2E), Energy Consumption (EC), Packet Loss Ratio (PLR) indicating the number of packets lost relative to the packets transmitted, etc. Fig. 8 depicts the distribution of evaluation performance metrics used in the selected studies.

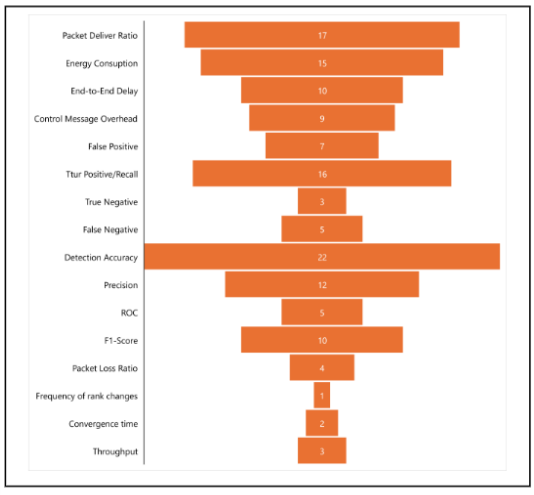


Fig. 8 Occurrence of evaluation metrics in selected studies

These metrics can also be used to measure the impact of routing attacks and the effectiveness of defense techniques on network performance. However, to evaluate the performance of the defense techniques, metrics such as Detection Rate (DR), Accuracy, True Negative (TN), False Positive (FP), False Negative (FN), True Positive (TP)/ Recall, etc., can be used. The most used evaluation metric for the defense techniques is detection / Accuracy which appeared 22 times in the selected studies. This metric is used to measure the number of detected malicious compared to the overall number of malicious nodes. To evaluate the effects of defense techniques we expect PDR to increase and PLR to decrease. However, most studies opted for PDR instead in which it appears 17 times and PLR only appeared 4 times in the selected studies.

The third most used metric is TP/Recall which measures the correct prediction of positive outcome by the defense technique. We mostly observe this metric in ML-based defense techniques. EC metric in RPL-based IoT is a crucial metric to consider because of the nature of the LLN devices we do not want to implement heavy techniques that harvest the energy of the nodes. The fifth most utilized metric is precision, especially for ML-based, which appears 12 times followed by E2E and F1-Score which both appear 10 times each. Functionality of RPL depends on Control messages exchanged between the nodes, hence CMO is an important metric to be considered in an RPL environment, it appears 9 times in the selected publications.

TABLE V presents the actual results obtained by the proposed defense techniques against routing attacks in RPL-based IoT. These are, however, the standard evaluation metrics commonly utilized to measure the performance of the network and the proposed defense techniques

It is recommended that the performance of a defense technique achieve at least 90%, more especially detection/accuracy, however, there are proposed techniques that obtained less than 90% detection/accuracy [27] in an IoT environment, this cannot be accepted because it implies that the technique can leave out more than 10% of the attacking nodes in the network which can still have a great impact on the performance of the network. Moreover, PDR is also an important metric to consider, and we must always strive for higher PRD, which evaluates the performance of the network under attacks and after attack i.e., upon mitigation of routing attacks. the proposed techniques in [39] obtained 69% of PDR, which means over 30% of packets are lost during network operation. Moreover, the technique in [31] achieved 76% of PDR which is still low same as [16] which produces 80% PDR indicating that 20% of packets are lost.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: 10.5281/zenodo.14449371

TABLE V. STANDARD PERFORMANCE METRICS RESULTS OF SELECTED STUDIES

| Study | Packet Delivery Ratio % | Energy Consumption | End-to-End delay | CMO | False Positive % | True Positive /Recall % | True Negative % | False Negative % | Detection \ Accuracy % | Precision % | ROC % | F1-Score % | PLR % | Frequency of rank changes % | Convergence time (s) | Throughput kbps |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| [2] | - | ~2,4 mW | | -50% | - | - | | - | -- | - | - | 91 | - | - | - | - |
| [5] | - | - | - | - | - | - | - | - | - | - | - | - | -27,6 | 59.5 | 60 | - |
| [17] | 98.4 | | | | | 94.67 | | 0.59 | 93.18 | - | - | - | - | - | - | - |
| [1] | 91 | 30% | 0.883s | 32 | - | - | | - | - | - | - | - | - | - | - | 191 |
| [3] | ~93 | 2,3 mW | 70s | +16 % | - | - | | - | 90 | - | - | - | - | - | - | - |
| [4] | +66 | 2,31 mW | 0,12 s | 4439 | 0 | 100 | 100 | 0 | 100 | 100 | - | - | 25 | - | - | - |
| [18] | 98 | 6.75 mW | 10s | - | - | - | - | - | -- | - | - | - | - | - | - | - |
| [6] | 97 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| [19] | ~80 | 2,9mW | ~2,2 s | - | - | - | - | - | ~94 | - | - | - | - | - | - | - |
| [20] | - | - | - | - | - | - | - | - | - | - | - | - | ~10 | - | - | - |
| [21] | 95 | 2,4mW | 0,9s | - | - | - | - | - | - | - | - | - | - | - | - | - |
| [22] | 97,9 | 6,5mW | 149.85 | 950 | - | - | 99.3 | 1.48 | 99.0 | - | - | - | - | - | 20 | 512.4 |
| [23] | 100 | 12.15mW | 0.29 s | 865 | - | - | - | - | - | - | - | - | - | - | - | - |
| [24] | 98.2 | 12.38mW | - | 1043 | - | - | - | - | 95.64 | - | - | - | - | - | - | - |
| [7] | - | +1.54% | - | 94.7 % | - | - | - | - | - | - | - | - | - | - | - | - |
| [25] | - | - | - | - | - | 87.9 | - | - | - | - | - | - | - | - | - | - |
| [26] | 96.3 | >5% | 0.03 ms | - | - | - | - | - | - | - | - | - | - | - | - | 98.45 |
| [27] | - | - | - | - | ~14 | - | - | - | 85.71 | - | - | - | - | - | - | - |
| [28] | - | - | - | - | - | 50-96 | - | - | - | - | - | - | - | - | - | - |
| [14] | 92.8 | - | - | - | - | - | - | - | - | - | - | - | 8.2 | - | - | - |
| [29] | High | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| [30] | - | 5.3% | - | - | 0.53 | - | - | - | 99 | - | - | - | - | - | - | - |
| [31] | 76 | 8.776mW | - | 1474 | - | 96 | - | - | 92 | 98 | - | 96 | - | - | - | - |
| [32] | - | - | - | - | - | 99.3 | - | - | 99.3 | 99.2 | - | 99.3 | - | - | - | - |
| [16] | 80 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| [12] | - | - | - | - | - | - | - | - | 97.76 | - | - | - | - | - | - | - |
| [33] | - | 3.50 mW | - | - | 3.55 | 90.6 | - | - | 94.1 | 94.6 | - | 94.1 | - | - | - | - |
| [34] | - | - | - | - | - | - | - | - | 98 | - | - | - | - | - | - | - |
| [35] | - | - | - | - | - | 98.9 | - | 0.6 | - | 98.9 | 100 | 98.9 | - | - | - | - |
| [13] | - | - | - | - | - | 93.3 | - | - | - | 93.3 | 92 | 93.3 | - | - | - | - |
| [36] | - | - | - | - | 24 | 100 | - | - | 96 | 100 | 100 | 86 | - | - | - | - |
| [15] | - | - | - | - | - | 99.68 | - | - | 99.99 | 100 | - | - | - | - | - | - |
| [37] | - | - | - | - | - | - | - | - | 94.4 | - | 93.4 | - | - | - | - | - |
| [38] | - | - | - | - | 4.5 | 97.5 | 95.5 | 2.5 | 96.6 | 96.7 | - | 96.6 | - | - | - | - |
| [39] | 69 | - | 0.9s | - | - | - | - | - | 99.95 | - | - | - | - | - | - | - |
| [40] | - | - | - | - | - | 92 | - | - | 98 | 92 | 100 | 92 | - | - | - | - |
| [41] | - | - | - | - | - | 99.8 | - | - | 99.8 | 99.7 | - | - | - | - | - | - |
| [42] | | | | | 0.78 | 97.1 | | | 97.1 | | | 97.1 | | | | |
| [43] | - | - | - | - | - | 98.1 | - | - | 99.7 | 99 | - | - | - | - | - | - |

There are, furthermore, other uncommon evaluation metrics used to measure the performance of the proposed techniques. These metrics are presented in Table VI below. We used a table to track the frequency of occurrence of these

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: 10.5281/zenodo.14449371

metrics. Other researchers can explore this table and use some of these metrics to evaluate their proposed techniques.

TABLE VI. UNCOMMON PERFORMANCE EVALUATION METRICS USED IN THE SELECTED PUBLICATIONS

| Evaluation metric | occurrence | Evaluation metric | occurrence |
|---|---|---|---|
| No of Device detached | 1 | CPU | 1 |
| Single-hop Average Trip Time | 1 | Data Packet overhead | 1 |
| Isolation Latency | 1 | Average reward | 1 |
| Avg routing packets per min | 1 | Average Packet Delivery Time | 1 |
| No of DAO forwarded | 1 | Kappa | 3 |
| Attack Identification | 1 | MCC | 4 |
| Attack detection delay | 1 | Cross Entropy | 2 |
| Preferred parent change rate | 2 | Expected Transmission Count | 1 |
| Network overhead | 1 | RAM & ROM | 1 |

*8) RQ8: What are the best defense techniques, detection and placement strategies, challenges, and future research areas?*

Three defense techniques were discovered i.e., Secure-Protocol, Conventional IDS, and ML-based technique. Amongst the three, Secure-Protocol appears to detect and mitigate routing attacks though it is limited to not more than 4 attacks. however, from the selected publications most of the ML-based techniques only detect attacks with high accuracy but lack mitigation mechanisms. This was discovered to be the limitation of most of the ML-based studies. One of the reasons for this lack of mitigation is the lack of pipeline development and deployment of the ML technique. Additionally, most of the Secure-Protocol techniques utilize a decentralized placement strategy to implement their defense techniques, while conventional IDS takes advantage of a hybrid placement approach utilizing both centralized and decentralized placement.

The future research direction the authors of this study will take is to investigate and set up a simulation environment for routing attacks in RPL-based IoT to measure their impact on the network. Furthermore, implement an ML-based defense technique that can detect and mitigate the investigated routing attacks. Taking into consideration the placement strategy; it was discovered that hybrid placement proves to be an efficient strategy that guarantees centralized detection and distributed mitigation implementation. Moreover, some secure-protocol detection strategies can be deployed to mitigate the attacks. In conclusion, integration of ML-based IDS and Secure-Protocol appears to be an effective approach to defend RPL-based IoT against routing attacks.

## V. Conclusion

The Internet of Things (IoT) emerges with different innovations including smart agriculture, environmental monitoring, and smart grids, to name a few. One of the significant enablers of IoT technology is the Low-power and Lossy Networks (LLNs) which comprise interconnected devices with low computational capabilities and less storage and are often operating on batteries such as sensor nodes and actuators. However, the broad adoption of IoT faces challenges in terms of security due to some of its characteristics, i.e., direct access to devices from the internet, the communication nature of wireless media, and potential unattended operations of relevant deployment. This study has conducted a Systematic Literature Review on the defense techniques against routing attacks in RPL-based IoT; as such 9 research questions were formulated to assist the researcher in gaining an insight into the defense techniques that can be implemented to defend the RPL-based IoT against routing attacks that take advantage of vulnerabilities of RPL protocol to affect traffic, topology, and resources of the network. However, the defense techniques in the studies demonstrate the effectiveness in detecting the attacks. With proper implementation and strategic placement of the techniques and integration into a hybrid defense technique, the technique can be effective in detection and mitigation, efficient to the network resources consumption and robust to address and cope under a large number of attacks.

## References


[1] Ankam, S., and Reddy, D.N.S.: 'A mechanism to detecting flooding attacks in quantum enabled cloud-based lowpower and lossy networks', Theoretical Computer Science, 2023, 941, pp. 29-38

[2] Medjek, F., Tandjaoui, D., Djedjig, N., and Romdhani, I.: 'Multicast DIS attack mitigation in RPL-based IoT-LLNs', Journal of Information Security and Applications, 2021, 61, pp. 102939

[3] Bang, A.O., and Rao, U.P.: 'A novel decentralized security architecture against sybil attack in RPL-based IoT networks: a focus on smart home use case', The Journal of Supercomputing, 2021, 77, (12), pp. 13703-13738

[4] Goel, S., Verma, A., and Jain, V.K.: 'CRA-RPL: A Novel Lightweight challenge-Response authentication-based technique for securing RPL against dropped DAO attacks', Computers & Security, 2023, 132, pp. 103346

[5] Seyfollahi, A., Moodi, M., and Ghaffari, A.: 'MFO-RPL: A secure RPL-based routing protocol utilizing moth-flame optimizer for the IoT applications', Computer Standards & Interfaces, 2022, 82, pp. 103622

[6] 6 Seth, A.D., Biswas, S., and Dhar, A.K.: 'Mitigation Technique against Network Isolation Attack on RPL in 6LoWPAN Network', in Editor (Ed.)^(Eds.): 'Book Mitigation Technique against Network Isolation Attack on RPL in 6LoWPAN Network' (2021, edn.), pp. 68-73

[7] Violettas, G., Simoglou, G., Petridou, S., and Mamatas, L.: 'A Softwarized Intrusion Detection System for the RPL-based Internet of Things networks', Future Generation Computer Systems, 2021, 125, pp. 698-714

[8] Ahmad, R., and Alsmadi, I.: 'Machine learning approaches to IoT security: A systematic literature review ', Internet of Things, 2021, 14, pp. 100365

[9] Al-Amiedy, T.A., Anbar, M., Belaton, B., Bahashwan, A.A., Hasbullah, I.H., Aladaileh, M.A., and Mukhaini, G.A.L.: 'A systematic literature review on attacks defense mechanisms in RPL-based 6LoWPAN of Internet of Things', Internet of Things, 2023, 22, pp. 100741

[10] Pasikhani, A.M., Clark, J.A., Gope, P., and Alshahrani, A.: 'Intrusion Detection Systems in RPL-Based 6LoWPAN: A Systematic Literature Review', IEEE Sensors Journal, 2021, 21, (11), pp. 12940-12968

[11] Verma, A., and Ranga, V.: 'Security of RPL Based 6LoWPAN Networks in the Internet of Things: A Review', IEEE Sensors Journal, 2020, 20, (11), pp. 5666-5690

[12] L, A.R., S, B., and G. S, C.: 'An Effective Detection of Version Number Attacks in the IoT using Neural Networks', in Editor (Ed.)^(Eds.): 'Book An Effective Detection of Version Number Attacks in the IoT using Neural Networks' (2022, edn.), pp. 1-7

[13] Ioulianou, P.P., Vassilakis, V.G., and Shahandashti, S.F.: 'ML-based Detection of Rank and Blackhole Attacks in RPL Networks', in Editor


ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: 10.5281/zenodo.14449371

(Ed.)^(Eds.): 'Book ML-based Detection of Rank and Blackhole Attacks in RPL Networks' (2022, edn.), pp. 338-343

[14] Ioulianou, P.P., Vassilakis, V.G., and Shahandashti, S.F.: 'A Trust-Based Intrusion Detection System for RPL Networks: Detecting a Combination of Rank and Blackhole Attacks', in Editor (Ed.)^(Eds.): 'Book A Trust-Based Intrusion Detection System for RPL Networks: Detecting a Combination of Rank and Blackhole Attacks' (2022, edn.), pp. 124-153

[15] Ioannou, C., and Vassiliou, V.: 'Accurate Detection of Sinkhole Attacks in IoT Networks Using Local Agents', in Editor (Ed.)^(Eds.): 'Book Accurate Detection of Sinkhole Attacks in IoT Networks Using Local Agents' (2020, edn.), pp. 1-8

[16] Moreira, C.M., and Kaddoum, G.: 'QL vs. SARSA: Performance Evaluation for Intrusion Prevention Systems in Software-Defined IoT Networks', in Editor (Ed.)^(Eds.): 'Book QL vs. SARSA: Performance Evaluation for Intrusion Prevention Systems in Software-Defined IoT Networks' (2023, edn.), pp. 500-504

[17] Qureshi, K.N., Rana, S.S., Ahmed, A., and Jeon, G.: 'A novel and secure attacks detection framework for smart cities industrial internet of things', Sustainable Cities and Society, 2020, 61, pp. 102343

[18] Raoof, A., Lung, C.H., and Matrawy, A.: 'Securing RPL Using Network Coding: The Chained Secure Mode (CSM)', IEEE Internet of Things Journal, 2022, 9, (7), pp. 4888-4898

[19] Pu, C., and Hajjar, S.: 'Mitigating Forwarding misbehaviors in RPL-based low power and lossy networks', in Editor (Ed.)^(Eds.): 'Book Mitigating Forwarding misbehaviors in RPL-based low power and lossy networks' (2018, edn.), pp. 1-6

[20] Chen, B., Li, Y., and Mashima, D.: 'Analysis and enhancement of RPL under packet drop attacks', in Editor (Ed.)^(Eds.): 'Book Analysis and enhancement of RPL under packet drop attacks' (2018, edn.), pp. 167-174

[21] Wadhaj, I., Ghaleb, B., Thomson, C., Al-Dubai, A., and Buchanan, W.J.: 'Mitigation Mechanisms Against the DAO Attack on the Routing Protocol for Low Power and Lossy Networks (RPL)', IEEE Access, 2020, 8, pp. 43665-43675

[22] Alsukayti, I.S., and Singh, A.: 'A Lightweight Scheme for Mitigating RPL Version Number Attacks in IoT Networks', IEEE Access, 2022, 10, pp. 111115-111133

[23] Rouissat, M., Belkheir, M., Alsukayti, I.S., and Mokaddem, A.: 'A Lightweight Mitigation Approach against a New Inundation Attack in RPL-Based IoT Networks', in Editor (Ed.)^(Eds.): 'Book A Lightweight Mitigation Approach against a New Inundation Attack in RPL-Based IoT Networks' (2023, edn.), pp.

[24] A. Almusaylim, Z., Jhanjhi, N.Z., and Alhumam, A.: 'Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP', in Editor (Ed.)^(Eds.): 'Book Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP' (2020, edn.), pp.

[25] Deshmukh-Bhosale, S., and Sonavane, S.S.: 'A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things', Procedia Manufacturing, 2019, 32, pp. 840-847

[26] Manne, V.R.J., and Sreekanth, S.: 'Detection and Mitigation of RPL Routing Attacks in Internet of Things', in Editor (Ed.)^(Eds.): 'Book Detection and Mitigation of RPL Routing Attacks in Internet of Things' (2022, edn.), pp. 481-485

[27] Agiollo, A., Conti, M., Kaliyar, P., Lin, T.N., and Pajola, L.: 'DETONAR: Detection of Routing Attacks in RPL-Based IoT', IEEE Transactions on Network and Service Management, 2021, 18, (2), pp. 1178-1190

[28] Choudhary, S., and Kesswani, N.: 'Detection and Prevention of Routing Attacks in Internet of Things', in Editor (Ed.)^(Eds.): 'Book Detection and Prevention of Routing Attacks in Internet of Things' (2018, edn.), pp. 1537-1540

[29] Garcia Ribera, E., Martinez Alvarez, B., Samuel, C., Ioulianou, P.P., and Vassilakis, V.G.: 'An Intrusion Detection System for RPL-Based IoT Networks', in Editor (Ed.)^(Eds.): 'Book An Intrusion Detection System for RPL-Based IoT Networks' (2022, edn.), pp.

[30] Yılmaz, S., Aydogan, E., and Sen, S.: 'A Transfer Learning Approach for Securing Resource-Constrained IoT Devices', IEEE Transactions on Information Forensics and Security, 2021, 16, pp. 4405-4418

[31] Momand, M.D., Mohsin, M.K., and Ihsanulhaq: 'Machine Learning-based Multiple Attack Detection in RPL over IoT', in Editor (Ed.)^(Eds.): 'Book Machine Learning-based Multiple Attack Detection in RPL over IoT' (2021, edn.), pp. 1-8

[32] Kamaldeep, Malik, M., Dutta, M., and Granjal, J.: 'IoT-Sentry: A Cross-Layer-Based Intrusion Detection System in Standardized Internet of Things', IEEE Sensors Journal, 2021, 21, (24), pp. 28066-28076

[33] 33 Pasikhan, A.M., Clark, J.A., and Gope, P.: 'Incremental hybrid intrusion detection for 6LoWPAN', Computers & Security, 2023, 135, pp. 103447

[34] Raghavendra, T., Anand, M., Selvi, M., Thangaramya, K., Santhosh Kumar, S.V.N., and Kannan, A.: 'An Intelligent RPL attack detection using Machine Learning-Based Intrusion Detection System for Internet of Things', Procedia Computer Science, 2022, 215, pp. 61-70

[35] Rabhi, S., Abbes, T., and Zarai, F.: 'IoT Routing Attacks Detection Using Machine Learning Algorithms', Wireless Personal Communications, 2023, 128, (3), pp. 1839-1857

[36] Choukri, W., Lamaazi, H., and Benamar, N.: 'RPL rank attack detection using Deep Learning', in Editor (Ed.)^(Eds.): 'Book RPL rank attack detection using Deep Learning' (2020, edn.), pp. 1-6

[37] Verma, A., and Ranga, V.: 'ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things', in Editor (Ed.)^(Eds.): 'Book ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things' (2019, edn.), pp. 1-6

[38] Pasikhani, A.M., Clark, J.A., and Gope, P.: 'Reinforcement-Learning-based IDS for 6LoWPAN', in Editor (Ed.)^(Eds.): 'Book Reinforcement-Learning-based IDS for 6LoWPAN' (2021, edn.), pp. 1049-1060

[39] Cakir, S., Toklu, S., and Yalcin, N.: 'RPL Attack Detection and Prevention in the Internet of Things Networks Using a GRU Based Deep Learning', IEEE Access, 2020, 8, pp. 183678-183689

[40] Al Sawafi, Y., Touzene, A., and Hedjam, R.: 'Hybrid Deep Learning-Based Intrusion Detection System for RPL IoT Networks', in Editor (Ed.)^(Eds.): 'Book Hybrid Deep Learning-Based Intrusion Detection System for RPL IoT Networks' (2023, edn.), pp.

[41] Zahra, F., Jhanjhi, N.Z., Brohi, S.N., Khan, N.A., Masud, M., and AlZain, M.A.: 'Rank and Wormhole Attack Detection Model for RPL-Based Internet of Things Using Machine Learning', in Editor (Ed.)^(Eds.): 'Book Rank and Wormhole Attack Detection Model for RPL-Based Internet of Things Using Machine Learning' (2022, edn.), pp.

[42] Alazab, A., Khraisat, A., Singh, S., Bevinakoppa, S., and Mahdi, O.A.: 'Routing Attacks Detection in 6LoWPAN-Based Internet of Things', in Editor (Ed.)^(Eds.): 'Book Routing Attacks Detection in 6LoWPAN-Based Internet of Things' (2023, edn.), pp.

[43] Zahra, F., Jhanjhi, N.Z., Khan, N.A., Brohi, S.N., Masud, M., and Aljahdali, S.: 'Protocol-Specific and Sensor Network-Inherited Attack Detection in IoT Using Machine Learning', in Editor (Ed.)^(Eds.): 'Book Protocol-Specific and Sensor Network-Inherited Attack Detection in IoT Using Machine Learning' (2022, edn.), pp.

[44] Garba, F.: 'A Comprehensive Review of Routing for Low Power and Lossy Network (RPL) Protocol Challenges and Proposed Improvements' (2022. 2022)

[45] Adebayo, A.O., Chaubey, M.S., and Numbu, L.P.: 'Industry 4.0: The fourth industrial revolution and how it relates to the application of internet of things (IoT)', Journal of Multidisciplinary Engineering Science Studies (JMESS), 2019, 5, (2), pp. 2477-2482

[46] A. Almusaylim, Z., Jhanjhi, N.Z. & Alhumam, A. 2020. Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP. Sensors, 20(21), 10.3390/s20215997

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: 10.5281/zenodo.14449371

# AUTHORS

## Lanka Chris Sejaphala

Lanka Chris Sejaphala serves as a Computer Networks Lecturer at North-West University and previously worked as an integration engineer for a telecommunication company. He brings a strong professional background in mobile cellular networks, integrating his field expertise with dedicated research. Mr Sejaphala holds a master's degree in Computer Science from the University of Limpopo and is currently pursuing his PhD at North-West University. His research focuses on critical areas including the application of machine learning in IoT security, and network performance optimization, all aimed at enhancing network security and efficiency.

## Vusimuzi Malele

A senior researcher and Postgraduate supervisor at North West University. An experienced engineer, teacher, research professional and manager with more than 25 years of experience in the ICT industry.

# AUTHORS

## Francis Lugayizi

Francis Lugayizi is an accomplished Associate Professor in Computer Science with a strong background in higher education and a specialization in Computer Networking and Database Systems. Earning his Ph.D. in Computer Science from North-West University/ Noordwes-Universiteit, Prof. Lugayizi has focused his academic and research efforts on the evolving fields of Quality of Service (QoS) and Quality of Experience (QoE) within Next Generation Computer and Communication Networks. His work emphasizes optimizing both network and application layers to improve end-user experiences, a crucial area within Information and Communication Technology (ICT). With a commitment to advancing academic rigor and innovation, Prof. Lugayizi aims to lead curriculum and research initiatives that refine existing optimization techniques and foster the development of new approaches to enhance QoS in Next Generation Networks. Through his academic journey and dedication to ongoing ICT advancements, he continues to contribute as an independent researcher and educator, advancing knowledge and solutions in network performance and end-user experience.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025

### 4.2.3 Article 3

#### 1. Article publication details

**Title:** Machine Learning Algorithms to Defend against Routing Attacks on the Internet of Things: A Systematic Literature Review

Status: Published

#### 2. Article synthesis

(i) Purpose

This article aims to theoretically evaluate the performance of traditional and advanced machine learning algorithms through a systematic literature review to determine the most effective algorithm for simulating the detection of routing attacks in IoT networks. The paper examines and consolidates current research to assess the efficiency of machine learning algorithms in identifying routing attacks in IoT networks that use RPL as the routing protocol.

(ii) Methods

This article employs an SLR methodology to review 17 published studies from 2018 to 2023, sourced from databases like IEEE Xplore and ScienceDirect, focusing on ML-based detection techniques. Data was collected from the selected studies' algorithm performance metrics such as precision, accuracy, F1-score, recall and FPR.

(iii) Results and Discussion/Findings

Traditional ML Algorithms Random Forest (RF) outperformed others, achieving 99.3% accuracy, precision, recall, and F1-score, followed by SVM with 95.3% accuracy. Naïve Bayes demonstrated the best FPR of 0.87%. On average, traditional algorithms achieved 91.67% accuracy and 2.75% FPR. In contrast, advanced ML Algorithms, such as Reinforcement Learning, led with over 98% in accuracy, precision, recall, and F1-score. Despite its high performance in detection,

it displays a poor FPR of 8% while Neural Networks achieved 97.88% accuracy, and Multi-Layer Perceptron achieved 98% F1-score. Advanced algorithms averaged 96.03% accuracy and 4.79% FPR. The article establishes that there is a lack of public datasets. As such, most studies employ self-created datasets to train and evaluate their suggested models. It is further noted that some published studies do not address resource consumption, attack mitigation, or model placement strategies. The results suggest that while advanced ML algorithms excel in accuracy, traditional algorithms like RF, DT, and Naïve Bayes offer lower false alarms, making them suitable for IoT environments with very low fault-tolerance. RF's superior performance across metrics highlights its potential as the most effective algorithm for detecting RPL attacks.

(iv) Conclusion

This article conducted a comparative analysis study using a systematic literature review to compare traditional and advanced machine learning models.
Performance metrics of the algorithms were collected from the selected studies to draw a conclusion on which algorithm category and individual models perform better according to the literature.

## 3. Full article

Journal of Information Systems and Informatics
Vol. 6, No. 3, September 2024 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v6i3.828 Published By DRPM-UBD

# Machine Learning Algorithms to Defend Against Routing Attacks on the Internet of Things: A Systematic Literature Review

**Lanka Chris Sejaphala[1], Vusimuzi Malele[2], Francis Lugayizi[3]**

[1,2]Department of Computer Science and Information Systems, North West University, Vanderbijlpark, South Africa
[3] Department of Computer Science and Information Systems, North West University, Mmabatho, South Africa
Email: [1]chris.sejaphala@nwu.ac.za, [2]vusi.malele@nwu.ac.za, [3]francis.lugayizi@nwu.ac.za

**Abstract**

The Internet of Things (IoT) has become increasingly popular, opening vast application possibilities in different fields including smart cities, healthcare, manufacturing, agriculture, etc. IoT comprises resource-constrained devices deployed in Low Power and Lossy Networks (LLNs). To satisfy the routing requirements of these networks, the Internet Engineering Task Force (IETF) created a standardised Routing Protocol for low-power and Lossy Networks (RPL). However, this routing protocol is vulnerable to routing attacks, prompting researchers to propose several techniques to defend the network against such attacks. Machine learning approaches demonstrate effective ways to detect such attacks in large quantities. Therefore, this paper systematically synthesised 17 publications to compare the performance of traditional and advanced machine learning algorithms to identify the best algorithm for detecting RPL-based IoT routing attacks. The findings of this paper show that machine learning algorithms are capable of effective detection of many routing attacks with high accuracy and a low False Positive Rate. Furthermore, the results demonstrate that on average, advanced machine learning algorithms can achieve an accuracy of 96.03% compared to traditional machine learning algorithms which achieved 91.67%. Traditional machine learning algorithms demonstrated the best performance on average False Positive Rate by achieving 2.75% compared to their counterparts which gained 4.79%. However, Random Forest showed the best performance and outperformed all the algorithms in the selected publications by achieving over 99% accuracy, precision and recall.

**Keywords:** RPL, IoT, LNNs, Machine learning, routing attacks

## 1. INTRODUCTION

The IoT is a paradigm of interconnected devices which collect and exchange data with each other from an environment of deployment and share the data over the

internet to achieve a particular goal [1]. This paradigm is used in a wide range of applications including home security management, industrial automation, smart energy monitoring and management, surveillance and military, smart cities, and farming, etc.

Due to its characteristics and nature, IoT has limitations regarding energy, memory, and computational capabilities, which traditional routing protocols cannot satisfy[2]. The Internet Engineering Task Force (IETF) working group designed and standardised Routing protocol for low-power and Lossy networks (RPL) to satisfy the routing needs of Low Power and Lossy Networks (LLNS) and to enable the resource-constrained devices to communicate their routing information among themselves and route their observed data to the root node[3, 4]. However, RPL as the DE facto routing protocol in IoT is susceptible to different routing attacks (i.e. flooding, sinkhole, worst parent attacks, etc) [5]. Routing attacks pose a great threat to the RPL-based IoT and can affect its performance and functionalities [4].

Different defence techniques against routing attacks in RPL-based IoT have been studied in the recent past, including the secure protocol, IDS and machine learning-based [6-8]. Machine learning techniques are currently new and more effective techniques used to deal with routing attacks in RPL as compared to traditional approaches [9]. Machine learning helps to analyse the IoT attack data and make accurate predictions in detecting routing attacks. This paper presents the findings of the Systematic Literature Review (SLR) method which is employed to identify the best-performing machine-learning algorithm to detect routing attacks in RPL-based IoT. Several SLR studies have been conducted in the past to try and find gaps in the machine learning-based detection techniques in RPL-based IoT[10-12]. Unlike in [13] in which authors highlighted strengths and limitations of machine learning algorithms, our study's primary objective is to use the SLR method to identify the best-performing machine learning algorithms. However, authors in [14] highlighted that most studies use private or self-generated datasets, which is one of the fundamental drives of our study. The selected studies used network simulation tools to generate their training and testing datasets, because of lack of publicly available datasets[13] .

The primary objective of this paper is to use a systematic literature review method to identify the best machine learning algorithm for the detection of routing attacks in RPL-based IoT. Contributions of this paper are that the study uses the SLR method to select and screen publications for inclusion and exclusion, Furthermore, provides a compressive summarised review of studies which proposed machine learning algorithms to act against routing attacks in IoT, Lastly, the study identifies the best-performing machine learning algorithm from the included publications

The rest of the paper is organised as follows: Section 2 presents a critical review literature in this area. Section 3 we propose our robust SLR methodology including inclusion and exclusion criteria followed to achieve relevant publications. Section 4 gives insight into the findings and analysis. Last, Section 5 concludes this paper by highlighting a summary of findings, limitations of the study, recommendations and scope of future work.

## 2. METHODS

This paper adopts the Systematic Literature Review (SLR) methodology to systematically source, analyze, and synthesize data into insightful information, with the aim of addressing the research question and presenting the findings in a comprehensive manner. The research design followed for the SLR is illustrated in Figure 1, outlining the structured process undertaken to achieve the objectives of this study. The design encompasses stages 2-5, which are essential for the selection and inclusion of relevant publications for the review.

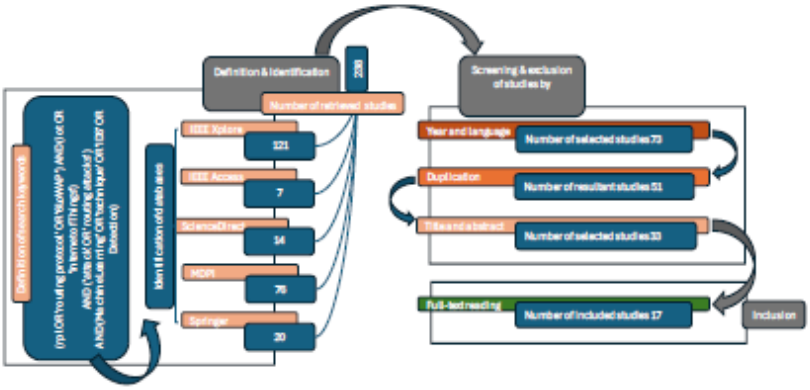


**Figure 1.** The adopted SRL research design.

The SLR approach employed in this paper consists of six critical stages. These stages ensure a rigorous review process, allowing for a systematic collection and evaluation of relevant literature. The stages are as follows:

1. **Stage 1**: Formulating the key research question. The research question that guides this study is: *Which machine learning algorithm, based on the synthesized publications, demonstrates the best performance in terms of accuracy, precision, and recall?*
2. **Stage 2**: Defining search keywords. This stage involves selecting specific keywords to narrow down relevant studies within the scope of machine learning in RPL (Routing Protocol for Low-power and Lossy Networks) and IoT (Internet of Things).

3. **Stage 3**: Identifying academic databases. Relevant academic libraries were identified to source publications, including reputable databases such as IEEE Xplore, ScienceDirect, MDPI, and Springer. These sources provide a wide range of high-quality peer-reviewed articles.
4. **Stage 4**: Screening and inclusion of studies (as detailed in Table 1). This stage involved the selection process, where studies were screened based on predefined criteria. A total of 73 studies initially met the year and language criteria, but after screening, 22 duplicate studies were excluded, 18 studies were dismissed due to irrelevant titles or abstracts, and 16 were excluded due to the unavailability of full texts. As a result, 17 studies were ultimately included for analysis.
5. **Stage 5**: Data extraction and synthesis. In this stage, data were meticulously extracted from the selected studies, and the relevant information was synthesized to ensure meaningful insights were drawn.
6. **Stage 6**: Presentation of findings. The final stage involves presenting the synthesized findings derived from the SLR process, which will be discussed in detail in the subsequent section of this paper.

**Table 1.** List of Publications selection criteria

| No | Inclusion | Exclusion |
|---|---|---|
| 1 | Published between 2018 & 2023 | A study is a duplicate |
| 2 | Written in the English language | Published in a language other than English |
| 3 | A study remains within the borders of machine learning in RPL and/or IoT | Not relevant to the scope of this article |
| 4 | A study is a journal article, a book chapter and a conference proceeding | Is a grey literature |
| 5 | Full-text reading is available | Full-text reading is not available |

## 3. RESULTS AND DISCUSSION

### 3.1 SLR Results

This section presents the findings of the Systematic Literature Review conducted in this paper. The main objective of this paper is to compare the performance results of machine learning algorithms from different studies in detecting routing attacks in RPL-based IoT. The selected studies used self-generated datasets from different simulation tools (e.g., Cooja, MATLAB, NetSim and OMNeT++) to develop and fit their selected machine-learning algorithms. However, some of the findings of this paper are that most studies that try to defend IoT using machine learning algorithms do not:

1. Demonstrate the impact of the observed attacks
2. Energy consumption of the proposed models is not well addressed
3. The placement strategy of the detection model is not presented
4. The proposed techniques only classify or detect the attacks, they do not identify intruders nor mitigate the attacks.

In this paper, we have summarised the findings of different studies comparing traditional and advanced machine learning algorithms in Tables 2 and Table 3 respectively. Table 3 displays a comparison results of different traditional machine learning algorithms from synthesised studies. Only one study from the selected studies had fitted Random Forest (RF) in their generated dataset.

**Table 2.** Performance metrics of traditional machine learning algorithms

| | RF | DT | KNN | Naïve Bayes | Google AutoML | SVM |
|---|---|---|---|---|---|---|
| Accuracy | 99.30 | 92.69 | 95.12 | 75.95 | - | 95.30 |
| Precision | 99.20 | 88.03 | 90.90 | 96.40 | 93.30 | 92.91 |
| Recall | 99.30 | 80.10 | 86.60 | 89.35 | 93.30 | 94.31 |
| F1-Score | 99.30 | 84.75 | 87.15 | 96.10 | 93.30 | 94.13 |
| FPR | - | 1.82 | 5.40 | 0.87 | - | 2.91 |

From the results, it appears that RF outperformed all the selected algorithms achieving an accuracy of 99.30% followed by SVM which achieved an accuracy of 95.30%. However, Naïve Bayes outperformed both RF and SVM in terms of precision and FPR achieving 96.40% and 0.87% respectively; followed by DT which achieved an FPR of 1.82%. Though Naïve Bayes' accuracy is the lowest it displayed exceptional results following RF though its FPR is not known. Figure 2 presents a graphical representation of Table 2. It displays averages of the evaluated performance metrics of traditional machine-learning algorithms.

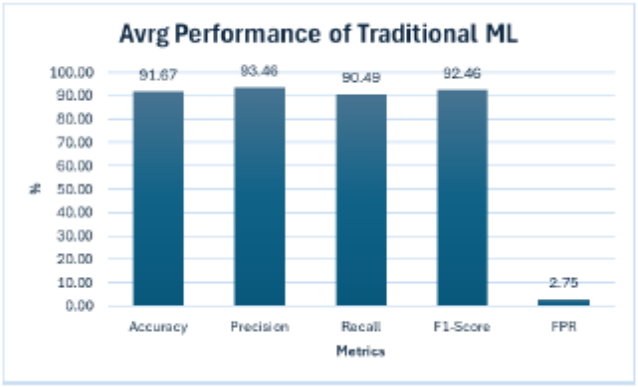


**Figure 2.** Performance metrics of traditional machine learning algorithms

On average the traditional machine learning algorithms achieved an accuracy of 91.67% and an FPR of 2.75%. This is however acceptable given their ability to produce such a low FRP and a precision of 93.46%.

Table 3 presents the results of advanced machine learning algorithms. As presented below Reinforcement learning algorithms outperformed all the algorithms in terms of accuracy, precision, Recall and F1-Score; in its performance, it achieved more than 98% in all the performance metrics but incurred a higher FPR of 8% which is still good but not acceptable. Followed by Neural Network (NN) which achieved an accuracy of 97.88% but ensembled achieved a higher precision and recall of 96.70% and 96.52% respectively. Moreover, Multi-Layer Perceptron (MLP) achieved the lowest FPR and second highest F1-Score of 98%.

**Table 3.** Performance metrics of different advanced machine learning

| Metrics | NN | MLP | Ensembled | Log Regression | Reinforcement |
|---|---|---|---|---|---|
| Accuracy | 97.88 | 91.11 | 96.50 | 96.18 | 98.50 |
| Precision | 92.00 | 96.00 | 96.70 | 95.65 | 98.60 |
| Recall | 92.00 | 93.85 | 96.25 | 93.44 | 98.00 |
| F1-Score | 92.00 | 98.00 | - | 90.80 | 98.50 |
| FPR | - | 1.16 | - | 5.20 | 8.00 |

Advanced machine learning algorithms appear to have achieved over 94% on all the performance metrics i.e., accuracy, precision, recall, and f1-score and below 5% of FPR as displayed in Figure 3.

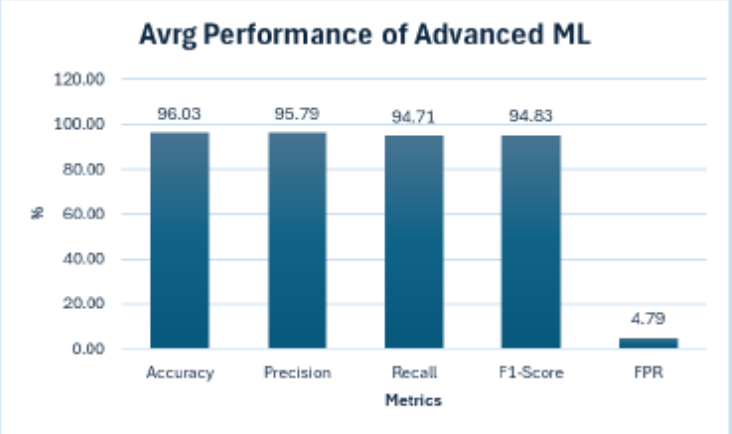


**Figure 3.** Performance metrics of advanced machine learning algorithms

From the results in Figure 2 and Figure 3, it is evident that advanced machine learning algorithms yield significant performance in detecting routing attacks. However, they turn out to incur a higher false alarm as compared to traditional machine learning algorithms. However, results in Table 3 and Table 4 demonstrate that Random Forest achieves significantly higher accuracy and precision, Recall and F1-Score. However, Naïve Bayes demonstrated a very low False alarm percentage of 0.87%. Furthermore, Reinforcement learning achieved higher accuracy, precision and recall percentages followed by ensembled learning then MLP coming second in F1-Score. From the presented results, on average, it can be concluded that traditional machine learning algorithms seem to excel in maintaining a very low FPR while advanced machine learning algorithms are good at producing higher accuracy and precision. However, individual algorithms demonstrate that Random Forest yields the best result as compared to all the algorithms presented in this paper.

### 3.2 Discussion

As recent works suggest, intelligence defense techniques are prominent solutions to defend against attacks in IoT [14, 15], particularly machine learning as it improves the attack detection rate using efficient learning techniques [16]. In their study [16], the authors proposed a machine learning-based technique to detect version number, rank, and DoS attacks. The technique employs a Support Vector Machine (SVM) integrated into each node of an RPL-based IoT.

In 2021, a Random Forest classifier [17] was proposed to defend IoT against five types of attacks. Although the proposed technique achieves a high detection rate, it does not mitigate the attacks. The authors in [18] proposed a reinforcement learning model for Software-Defined IoT networks to combat rank attacks. Their experimental results demonstrated that a State Action Reward State Action (SARSA) model is more effective in facilitating the implementation of Intrusion Prevention Systems.

The study [19] compared the performance of four supervised-learning algorithms, namely Logistic Regression, SVM, Gaussian Naive Bayes, and Neural Networks, to detect version number attacks. The Neural Network outperformed traditional machine learning algorithms and achieved an accuracy of 97.76%. Another study [20] proposed a distributed One-Class SVM (OCSVM) to detect outliers related to 10 types of attacks. The results of the OCSVM are communicated to a hybrid centralized IDS. However, the OCSVM adds energy consumption overhead.

To address blackhole, sinkhole, decreased rank, and selective forwarding attacks, the study [21] proposed a fuzzy KNN classifier. The authors in [22] proposed an ensembled classifier consisting of SVM, Naïve Bayes, and a Decision Tree to

detect blackhole, hello flooding, and version number attacks. The results show that using the ensembled method yields higher performance than a single classifier. The authors in [23] compared the performance of Microsoft Azure SVM, Decision Tree, and Google AutoML to detect rank and blackhole attacks. Google AutoML achieved a higher precision of 93.3% and outperformed Microsoft Azure's SVM and Decision Tree based on other evaluation metrics. In [24], the authors proposed an Artificial Neural Network using Multi-Layer Perceptron (MLP) to detect rank attacks in RPL-based IoT. The proposed technique produced a precision of 100% and an accuracy of 96%. However, the technique does not mitigate the attack, and no placement strategy was provided.

The study [25] compared the performance of SVM and Binary Logistic Regression (BLR) to detect sinkhole attacks in IoT. The results indicated that BLR outperformed SVM, and it was implemented for detection. However, the energy consumption of the proposed BLR was not presented, though it is reported to be lightweight. The study [26] proposed an ensembled method to detect seven routing attacks in RPL-based IoT. This study utilized the RPL-NNIDS17 dataset to train and test the proposed technique.

The authors in [27] proposed a Reinforcement-learning technique to defend against eight routing attacks in RPL-based IoT. The technique combines homogeneous machine learning algorithms, such as SVM, Decision Tree (DT), KNN, K-Means, and Logistic Regression. To achieve optimum performance, they used Deep Q-Network (DQN) and Double DQN (DDQN) to approximate the Q function for value-action selection.

The work in [28] investigated the performance of SVM, Logistic Regression (LR), and Gated Recurrent Unit (GRU)-based Deep Learning to defend against hello flooding attacks in RPL-based IoT. Their results indicated that GRU outperformed both SVM and LR, yielding higher accuracy and PDR. The proposed technique, implemented with Recurrent Neural Networks architecture, is used to classify malicious nodes and mitigate hello flooding attacks.

The authors in [29] proposed a hybrid Deep Learning Artificial Neural Network (DANN) to classify network traffic. The performance of the proposed technique was compared with J48, SVM, KNN, and Long Short-Term Memory (LSTM), with DANN achieving 98% accuracy and a 92% F1-Score. To detect rank and wormhole attacks, the authors in [30] proposed a Machine Learning Lightweight Gradient Boost Machine Model (ML-LGBM) to classify rank, wormhole, and normal attacks. In their study, they compared the performance of GRU-DL, SVM, Gradient Boost (GB), and Extended Gradient Boost (XGB), with the proposed technique showing better performance in terms of accuracy and precision.

The study [9] proposed a stacking ensembled method that combines the results of C4.5 and SVM. This technique was integrated into a Hybrid IDS to detect seven routing attacks in IoT. The study compared C4.5, MLP, SVM, and Naïve Bayes, with the experimental results showing that the ensemble of C4.5 and SVM outperformed other individual techniques in terms of accuracy and false alarms. The study [31] proposed the ProSenAD model to detect rank and wormhole attacks. The proposed technique optimizes LGBM for multiclass classification to detect protocol-specific and sensor network attacks. The authors compared several machine learning algorithms, but the ProSenAD model outperformed them in terms of classification accuracy.

Table 4 summarises the findings of this paper, outlining the strengths and limitations of the study and proposed defence technique, names and number of attacks addressed, and whether the study demonstrates the impact of the studied attacks or not; furthermore, demonstrates if the proposed technique mitigates the attacks or not. Lastly, the machine learning algorithms were investigated, and the size of the dataset used in the study.

**Table 4.** Summarised findings from the included publications

| Study | ML-algorithms | Dataset | No of Attacks | Strength | Limitation | Attacks | Impact of attacks |
|---|---|---|---|---|---|---|---|
| [17] | SVM | Generated - NA | 4 | the proposed technique achieves more than 90% accuracy and consumes less energy as compared to base RPL | Though the proposed technique achieves acceptable performance results, the number of malicious nodes is not mentioned | Version Number, Rank, DoS Attack | Yes |
| [16] | Random Forest Classifier | Generated - NA | 6 | Achieves 99.46% detection rate | The technique does not mitigate the attacks | UDP Flooding, Selective Forwarding, Blackhole, DIS Flooding, ICMPv6 Flooding | Yes |
| [18] | State Action Reward State Action | Generated - NA | 1 | It is said the proposed technique | Only one malicious | Rank | No |

| Study | ML-algorithms | Dataset | No of Attacks | Strength | Limitation | Attacks | Impact of attacks |
|---|---|---|---|---|---|---|---|
| | | | | effectively prevents rank attack's harmful effects | node is considered | | |
| [19] | Logistic Regression, SVM, Gaussian Naïve Bayes, Neural Network | Generated -103839 | 1 | The proposed technique achieves 97.76% accuracy | The placement strategy of the proposed technique is not presented | Version number attack | No |
| [20] | SVM | Generated - NA | 10 | The proposed technique can detect malicious activities with a 99.74% TPR | The proposed technique adds energy consumption overhead | Sinkhole, Blackhole, Grayhole, DIS Flooding, Increase Rank, Wormhole, DIO Suppression, Worst Parent, Version Number, Neighbour Attack | No |
| [21] | Fuzzy KNN Classifier | Generated - NA | 4 | The proposed technique achieves an accuracy of more than 98% | The proposed technique cannot mitigate the detected attacks | Decreased Rank, Blackhole, Sinkhole, Selective Forwarding | No |
| [22] | SVM, Naïve Bayes, Decision Tree | Generated - NA | 3 | The proposed technique achieves more than 98% accuracy, precision, recall, TPR, F-measure and MCC. | The proposed technique cannot mitigate the detected attacks. only one malicious | Blackhole, Hello Flooding, Version Number | No |

| Study | ML-algorithms | Dataset | No of Attacks | Strength | Limitation | Attacks | Impact of attacks |
|---|---|---|---|---|---|---|---|
| | | | | | was considered. | | |
| [23] | Azure SVM, Azure Decision Tree, Google AutoML. | Generated - NA | 2 | The evaluation show that ML techniques can be effective in detecting rank and blackhole attacks achieving a precision of 93.3% | The proposed technique cannot mitigate the detected attacks. | Rank, Blackhole | No |
| [24] | MLP ANN | Generated - NA | 1 | Achieves 100% precision | The study considered a small network size with only 2 malicious nodes | Rank | No |
| [25] | BLR & SVM | Generated - NA | 1 | The proposed Binary Logistic Regression achieves higher accuracy and precision | The energy consumption of the proposed technique is not presented | Sinkhole | No |
| [26] | Boosted Trees, Bagged Trees, Subspace Discriminant, & RUS Boosted Trees. | Generated -175077 | 7 | The proposed ensembled achieved 94.5% and 93.4% accuracy and AUC respectively. | The proposed technique cannot mitigate the detected attacks. | Sinkhole, blackhole, Sybil, Clone ID, Selective Forwarding, Hello Flooding, & Local Repair | No |

| Study | ML-algorithms | Dataset | No of Attacks | Strength | Limitation | Attacks | Impact of attacks |
|---|---|---|---|---|---|---|---|
| [27] | Decision Tree, K-NN, K-means, SVM, & Logistic Regression | Generated -80000 | 8 | The proposed RL technique achieves 96.6% and 96.7% accuracy and precision respectively | The proposed technique cannot mitigate the detected attacks. | Sinkhole, Blackhole, Grayhole, DIS Flooding, Increased Rank, Wormhole, DIO Suppression, Replay | No |
| [28] | GRU, SVM, LR | Generated -10519 | 1 | The proposed GRU produces an accuracy of 99.95% with higher PDR | The energy consumption of the proposed GRU-based DL is not presented | Hello-Flooding | Yes |
| [29] | DANN, J48, KNN, SVM, LSTM | Generated -380732 | 3 | The proposed DL technique shows exceptional results performance against supervised learning algorithms achieving 98% and 92% accuracy and F1-score respectively | The proposed technique cannot mitigate the detected attacks. | DIS-Flooding, Rank & Wormhole | No |
| [30] | LGBM, GRU-DL, SVM, GB, XGBoost | Generated -31062 | 2 | The proposed technique achieved an accuracy of 99.8% which is higher than all other algorithms in the study | The proposed technique cannot mitigate the detected attacks. | Rank & Wormhole | No |

| Study | ML-algorithms | Dataset | No of Attacks | Strength | Limitation | Attacks | Impact of attacks |
|---|---|---|---|---|---|---|---|
| [31] | C4.5, SVM, MLP, & Naive Bayes | Generated -3190 | 8 | The proposed technique produces a high TP of 97.1% and FP of almost 1% | Only one malicious node is considered in the study | Flooding, Dos, Wormhole, Rank, blackhole, Version number, & Sinkhole | No |
| [9] | GAN-C, ML-LGBM, LGBM, GB, XGBoost | Generated - NA | 2 | The proposed technique demonstrated a high level of accuracy and precision in detecting rank and wormhole attacks | The number of attacking nodes is not mentioned and the model can only classify, it does not identify nor mitigation | Rank & Wormhole | No |

From Table 4 presented the evident that machine learning algorithms are capable of addressing several routing attacks where we see over only 5 studies out of 17 addresses only one attack. However, most of the studies we synthesised did not disclose their dataset size which also affect the performance of the machine learning algorithms.

## 4. CONCLUSION

In conclusion, machine learning algorithms display an effective and efficient way to detect routing attacks. From the studies that were synthesised, it is evident that machine learning algorithms can detect many routing attacks with high accuracy and precision while also displaying a significantly low False Positive Rate. This paper investigated the performance of different machine-learning algorithms from 17 publications that met the inclusion criteria of this paper, and it was discovered that between traditional machine learning and advanced machine-learning algorithms, on average advanced machine learning demonstrated the best performance over traditional machine-learning algorithms. However, this paper aims to identify the best machine learning algorithm from the synthesises publications. It was then discovered that Random Forested demonstrated the best results in terms of accuracy, precision, Recall and F1-Score. Although dataset size, feature engineering techniques used, number of features selected, number of attacks, and training time are some of the factors that are to be considered,

however, they are not within the scope of this paper but are to be considered. In future, the authors intend to generate datasets of different attacks and legitimate traffic using one of the simulation tools described in the literature to compare the performance of machine learning algorithms. The authors will train and test the algorithms on the same dataset and consider all factors mentioned, furthermore, propose the best-performing model for implementation to defend IoT against routing attacks.

## REFERENCES

[1] A. O. Adebayo, M. S. Chaubey, and L. P. Numbu, "Industry 4.0: The fourth industrial revolution and how it relates to the application of internet of things (IoT)," *Journal of Multidisciplinary Engineering Science Studies (JMESS)*, vol. 5, no. 2, pp. 2477-2482, 2019.

[2] A. J. Witwit and A. K. Idrees, "A comprehensive review for RPL routing protocol in low power and lossy networks," in *Proc. Int. Conf. New Trends Inf. Commun. Technol. Appl.*, Cham, Switzerland: Springer International Publishing, Sep. 2018, pp. 50-66.

[3] F. Garba, "A Comprehensive Review of Routing for Low Power and Lossy Network (RPL) Protocol Challenges and Proposed Improvements," 2022.

[4] A. Jahangeer, S. U. Bazai, S. Aslam, S. Marjan, M. Anas, and S. H. Hashemi, "A Review on the Security of IoT Networks: From Network Layer's Perspective," *IEEE Access*, vol. 11, pp. 71073-71087, 2023.

[5] J. Rani, A. Dhingra, and V. Sindhu, "A Detailed Review of the IoT with Detection of Sinkhole Attacks in RPL based network," in *Proc. A Detailed Review of the IoT with Detection of Sinkhole Attacks in RPL based network*, 2022, pp. 1-6.

[6] A. Agiollo, M. Conti, P. Kaliyar, T. N. Lin, and L. Pajola, "DETONAR: Detection of Routing Attacks in RPL-Based IoT," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1178-1190, 2021.

[7] H. Alam, M. S. Yaqub, and I. Nadir, "Detecting IoT Attacks using Multi-Layer Data Through Machine Learning," in *Proc. Detecting IoT Attacks using Multi-Layer Data Through Machine Learning*, 2022, pp. 52-59.

[8] A. U. Gawade and N. M. Shekokar, "Lightweight Secure RPL: A Need in IoT," in *Proc. Lightweight Secure RPL: A Need in IoT*, 2017, pp. 214-219.

[9] A. Alazab, A. Khraisat, S. Singh, S. Bevinakoppa, and O. A. Mahdi, "Routing Attacks Detection in 6LoWPAN-Based Internet of Things," in *Proc. Routing Attacks Detection in 6LoWPAN-Based Internet of Things*, 2023.

[10] R. Ahmad and I. Alsmadi, "Machine learning approaches to IoT security: A systematic literature review," *Internet of Things*, vol. 14, pp. 100365, 2021.

[11] T. A. Al-Amiedy, M. Anbar, B. Belaton, A. H. Kabla, I. H. Hasbullah, and Z. R. Alashhab, "A Systematic Literature Review on Machine and Deep Learning Approaches for Detecting Attacks in RPL-Based 6LoWPAN of Internet of Things," in *Proc. A Systematic Literature Review on Machine and Deep Learning Approaches for Detecting Attacks in RPL-Based 6LoWPAN of Internet of Things*, 2022.

[12] A. M. Pasikhani, J. A. Clark, P. Gope, and A. Alshahrani, "Intrusion Detection Systems in RPL-Based 6LoWPAN: A Systematic Literature Review," *IEEE Sensors Journal*, vol. 21, no. 11, pp. 12940-12968, 2021.

[13] T. A. Al-Amiedy, M. Anbar, B. Belaton, A. A. Bahashwan, I. H. Hasbullah, M. A. Aladaileh, and G. A. L. Mukhaini, "A systematic literature review on attacks defense mechanisms in RPL-based 6LoWPAN of Internet of Things," *Internet of Things*, vol. 22, pp. 100741, 2023.

[14] G. A. L. Mukhaini, M. Anbar, S. Manickam, T. A. Al-Amiedy, and A. A. Momani, "A systematic literature review of recent lightweight detection approaches leveraging machine and deep learning mechanisms in Internet of Things networks," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 1, pp. 101866, 2024.

[15] H. Xu, Z. Sun, Y. Cao, and H. Bilal, "A data-driven approach for intrusion and anomaly detection using automated machine learning for the Internet of Things," *Soft Computing*, vol. 27, no. 19, pp. 14469-14481, 2023.

[16] M. D. Momand, M. K. Mohsin, and Ihsanulhaq, "Machine Learning-based Multiple Attack Detection in RPL over IoT," in *Proc. Machine Learning-based Multiple Attack Detection in RPL over IoT*, 2021, pp. 1-8.

[17] Kamaldeep, M. Malik, M. Dutta, and J. Granjal, "IoT-Sentry: A Cross-Layer-Based Intrusion Detection System in Standardized Internet of Things," *IEEE Sensors Journal*, vol. 21, no. 24, pp. 28066-28076, 2021.

[18] C. M. Moreira and G. Kaddoum, "QL vs. SARSA: Performance Evaluation for Intrusion Prevention Systems in Software-Defined IoT Networks," in *Proc. QL vs. SARSA: Performance Evaluation for Intrusion Prevention Systems in Software-Defined IoT Networks*, 2023, pp. 500-504.

[19] A. R. L., B. S., and C. S. G., "An Effective Detection of Version Number Attacks in the IoT using Neural Networks," in *Proc. An Effective Detection of Version Number Attacks in the IoT using Neural Networks*, 2022, pp. 1-7.

[20] A. M. Pasikhani, J. A. Clark, and P. Gope, "Incremental hybrid intrusion detection for 6LoWPAN," *Computers & Security*, vol. 135, pp. 103447, 2023.

[21] T. Raghavendra, M. Anand, M. Selvi, K. Thangaramya, S. V. N. Santhosh Kumar, and A. Kannan, "An Intelligent RPL attack detection using Machine Learning-Based Intrusion Detection System for Internet of Things," *Procedia Computer Science*, vol. 215, pp. 61-70, 2022.

[22] S. Rabhi, T. Abbes, and F. Zarai, "IoT Routing Attacks Detection Using Machine Learning Algorithms," *Wireless Personal Communications*, vol. 128, no. 3, pp. 1839-1857, 2022.

[23] P. P. Ioulianou, V. G. Vassilakis, and S. F. Shahandashti, "ML-based Detection of Rank and Blackhole Attacks in RPL Networks," in *Proc. ML-based Detection of Rank and Blackhole Attacks in RPL Networks*, 2022, pp. 338-343.

[24] W. Choukri, H. Lamaazi, and N. Benamar, "RPL rank attack detection using Deep Learning," in *Proc. RPL rank attack detection using Deep Learning*, 2020, pp. 1-6.

[25] C. Ioannou and V. Vassiliou, "Accurate Detection of Sinkhole Attacks in IoT Networks Using Local Agents," in *Proc. Accurate Detection of Sinkhole Attacks in IoT Networks Using Local Agents*, 2020, pp. 1-8.

[26] A. Verma and V. Ranga, "ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things," in *Proc. ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things*, 2019, pp. 1-6.

[27] A. M. Pasikhani, J. A. Clark, and P. Gope, "Reinforcement-Learning-based IDS for 6LoWPAN," in *Proc. Reinforcement-Learning-based IDS for 6LoWPAN*, 2021, pp. 1049-1060.

[28] S. Cakir, S. Toklu, and N. Yalcin, "RPL Attack Detection and Prevention in the Internet of Things Networks Using a GRU Based Deep Learning," *IEEE Access*, vol. 8, pp. 183678-183689, 2020.

[29] Y. Al Sawafi, A. Touzene, and R. Hedjam, "Hybrid Deep Learning-Based Intrusion Detection System for RPL IoT Networks," in *Proc. Hybrid Deep Learning-Based Intrusion Detection System for RPL IoT Networks*, 2023.

[30] F. Zahra, N. Z. Jhanjhi, S. N. Brohi, N. A. Khan, M. Masud, and M. A. AlZain, "Rank and Wormhole Attack Detection Model for RPL-Based Internet of Things Using Machine Learning," in *Proc. Rank and Wormhole Attack Detection Model for RPL-Based Internet of Things Using Machine Learning*, 2022.

[31] F. Zahra, N. Z. Jhanjhi, N. A. Khan, S. N. Brohi, M. Masud, and S. Aljahdali, "Protocol-Specific and Sensor Network-Inherited Attack Detection in IoT Using Machine Learning," in *Proc. Protocol-Specific and Sensor Network-Inherited Attack Detection in IoT Using Machine Learning*, 2022.

### 4.2.4 Article 4

#### 1. Article publication details

**Title**: A Review of Routing Attacks in RPL-based IoT Networks

Status: Accepted

#### 2. Article synthesis

(i) Purpose

This article uses SLR to identify suitable simulation tools for modelling RPL-based routing attacks, determine network performance metrics that might suggest the presence of routing attacks, and highlight gaps in existing literature regarding attack implementation details and the effects of routing attacks on the stability of networks, available resources, and traffic behaviours. In synthesising existing literature, the article seeks to provide a comprehensive understanding of routing attack characteristics, implementation details, and their impacts on network topology, resources, and traffic, ultimately identifying gaps for future research.

(ii) Methods

The study employs an SLR research approach to synthesise 38 published articles from different academic databases (IEEE Access, ScienceDirect, Springer, and MDPI) published between 2021 and 2024. Quantitative data collection was done on network size, simulation tools, number of attack nodes, attack intensity, and network performance metrics.

(iii) Results and Discussion/Findings

The article identifies Cooja running ContikiOS as the preferred simulation tool, highlights key performance metrics (throughput, packet delivery ratio, energy consumption, end-to-end delay, and control message overhead), and highlights vulnerabilities of RPL exploited by routing attacks. It outlines attack characteristics, defines attack intensity levels for impact adjustment and further provides a network

size and attack intensity mapping, which can be enablers of robust and effective defence models as far as a comprehensive training dataset is concerned. Lastly, it outlines implementation details (e.g., modification of RPL scripts (rpl-private.h, rpl-timers.c) to implement DIS-Flooding by setting DIS transmission intervals to zero).

(iv) Conclusion

The review provides a foundation for understanding routing attacks and their impacts, identifying gaps in implementation details and mitigation strategies. Additionally, the study provides a synthesised, readable network size and attack intensity mapping, and performance metrics. Ultimately, the article further emphasises the need for standardised simulation frameworks.

## 3. Full paper

This paper seeks to address questions regarding suitable simulation tools, factors impacted by routing attacks (such as performance metrics and attack intensity for realistic simulation), and implementation details, including attack descriptions, characteristics, and steps to simulate routing attacks in Low-power and Lossy IoT Networks. Sinkhole, rank, DIS-flooding, and Worst parent attacks are only some of the novel internal threats to RPL, which are considered in this study. While there exist publications pertaining to routing attacks in LLNs, a comprehensive review is missing in highlights the characteristics, implementation, and algorithms of routing attacks. The edge behind this research paper is to gather all the necessary tools for an in-depth understanding and implementation of routing attacks in a single volume.

Based on the literature search findings, a structured analysis of the description, characteristics, and algorithms of routing attacks needs to be conducted to identify research gaps and implementation of these routing attacks for academic experimental purposes. This research paper aims to address the issues related to the implementation of routing attacks with the following research questions:

- Which simulation tool is suitable for implementing RPL-based routing attacks?
- Which network performance metrics may demonstrate the presence of routing attacks?
- What percentage of malicious nodes significantly impact the network's performance proportional to legitimate nodes?
- What key steps or framework can be adopted to implement routing attacks?

As such, the contributions of this paper are as follows: The paper lays a thorough foundation of descriptions and characteristics of the selected routing attacks; dissects related work and provides a synthesised summary highlighting the contributions and limitations of the selected works. Furthermore, it brings forth the implementation structure and algorithms of the addressed routing attacks.
Looking ahead: The synthesised related work is presented in Section II, Section III lays out the RPL overview and operations, Section IV provides a comprehensive discussion of the routing attacks in question, the adopted methodology is presented in Section V, Section VI discusses the findings of this research paper, and Section VII concludes it.

## II. Related Work

In recent years, resource-constrained networks have gained popularity in academic and industrial research areas, from network performance optimisation to security threat detection and mitigation. With the rapid growth of RPL-based IoT applications, the provision of attack review is of great importance. Thus, the focus of this study is to conduct a review of the RPL-based IoT network's security threat, particularly the routing attacks.

Jahangeer in their study [1] conducted a review of the security of IoT networks from the perspective of the network layer. The study reviewed state-of-the-art works, including machine learning-based algorithms and techniques, and evaluated performance parameters such as energy consumption and throughput. Authors of the study [7] they conducted a detailed review of the detection of sinkhole attacks in RPL-based networks. The authors presented the characteristics and description of the sinkhole attacks. However, they did not factor in the implementation of the addressed attack. An overview of the RPL network and security features is presented in [8]. The study presents a detailed review of rank and blackhole attacks, and security solutions against these attacks for RPL-based networks. However, implementations of the attacks are not presented. Furthermore, it is not evident as to which factors their focus attacks affect.

Nish et al [6] presents a DIS-flooding attack overview, demonstrating that there are two types of such attacks, namely, unicast and multicast DIS-flooding attacks. The study further notes that the attacks affect the resources of LLN nodes, particularly energy. Authors of the study [9] provides a comprehensive survey of fourteen RPL-specific attacks and their mitigation techniques. The study further demonstrated the impact of the attacks on the resources, traffic, and topology of the network. The study [10] provides a various number of routing attacks affecting RPL. Additionally, the study categorises these attacks in terms of affected factors such as topology, resources, and traffic flow. The study, furthermore, highlighted subdivisions within each category of affected factors to demonstrate the effects of routing attacks in their taxonomy of RPL routing attacks.
Table I exhibits a comprehensive summary of synthesised related work, highlighting the description of the paper, major contribution, and the number of attacks addressed. It further highlights whether or not the study presents implementation of attacks, and affected factors (topology, traffic, & resources); lastly, the limitations of the studies.

TABLE I SUMMARY OF SYNTHESISED RELATED WORK

| Reference | Description | Major Contribution | Number of attacks | Implementation | Affected Factors (Topology, traffic & Resources) | Limitation |
|---|---|---|---|---|---|---|
| [1] | A review of the security of IoT networks at the network layer perspective | The study reviews routing attacks, existing detection approaches, and evaluation parameters | 7 | No | No | Implementation of attacks is not presented |

select a node with the minimum rank value as its preferred parent [4].

## IV. LLNS ATTACKS OVERVIEW

In this section, the study presents an overview of Rank, Sinkhole, Worst Parent, and DIS-flooding attacks that negatively affect the network from optimal convergence, excessively consume network resources, and greatly affect the overall performance of the LLNs. We outline the characteristics and description of the routing attacks, vulnerabilities of RPL that these routing attacks can exploit, and the affected factors and performance metrics.

LLNs are susceptible to various attacks, including routing attacks. These attacks are detrimental to network topology, resources and traffic, intending to destabilise the network's quality of services [18]. An attacker may intentionally violate one or more of the notions of the rank property mentioned in Section 2 to instigate various routing attacks that may disrupt network traffic, deplete network resources or sub-optimise the LLN's performance.

### *A. Dis Flooding Attacks*

In normal RPL operations, a new node(s) or node(s) who loses connection with its parents sends a DIS control packet to solicit DIO packets from its neighbour nodes. One way to transmit the DIS packets is to broadcast them such that they reach any node in the radio range of the sender. Upon receipt of the DIS packet, the trickle timer of the receiver is reset, and the node then broadcasts its DIO packet. An attacker can exploit the multicast solicitation technique of RPL to launch a DIS-flooding attack [25, 26]. An attacker frequently transmits DIS packets to the victim node in its transmission range [27] and ignores any DIO packets sent by neighbour nodes. Unicast or broadcast DIS control packets increase control message overhead and energy consumption. Furthermore, it causes the unavailability of legitimate nodes, link channels, etc. Multicast DIS control packets cause a frequent reset of the trickle timer of the receiving nodes to its minimum value and abort the scheduled emission of DIO packets. The frequent trickle timer resets due to massive DIS received and massive DIO transmitted by victim nodes increase the control packet overhead [15, 28]. The DIS Flooding attacks are resource-affecting attacks. Thus, a rapid increase in control packets increases the energy consumption of the affected nodes, resulting in a shortened network lifespan and, additionally, reducing the availability of communication links [6] and degrading the efficiency of the network.

To implement the DIS-flooding attacks, *rpl-private.h* and *rpl-timers.c* scripts can be modified and are found in this path *contiki/core/net/rpl/*. The script *rpl-private.h* contains DIS operation constant. The DIS transmission interval is different from one RPL's implementation to another [17]. The interval is handled by *RPL_DIS_INTERVAL* and *RPL_DIS_START_DELAY* constants [15]. To accelerate DIS packets dispatched by the malicious node, these constants may be set to zero (0).

### *B. Sinkhole attacks*

The attack attracts and intercepts a significant portion of the network traffic, effectively disrupting the network's routing services [13]. In this attack, a malicious node disseminates faulty routing information to fabricate itself as a better route [29, 30] it does that by decreasing its OF metric which is used to calculate the rank value [31]. So that all the neighbour traffic in the network is directed through the malicious node [2]. A sinkhole attack may selectively drop received packets or may completely drop all packets, altering the communication stream, and performing packet modification [2]. These attacks may affect topology and data traffic; furthermore, affecting end-to-end delay, packet delivery ratio, and throughput [3].

The script to modify to implement the sinkhole attacks is *rpl_mrfhof.c* found in the path *contiki/core/net/rpl/*. This function *calculate_rank(rpl_parent_t *p, rpl_rank_t base_rank)* is used to calculate the rank value of its target node.

### *C. Rank attacks*

The Rank attacks can occur by manipulating link parameters. The attacker advertises either a lower or a higher rank value in case of a decreased rank attack and an increased rank attack, respectively [32]. In the case of decreased rank attacks, legitimate nodes will choose a lower-ranked node as the preferred parent, resulting in data traffic routed to the malicious node. The rank attack is a data traffic flow-affecting attack that causes energy depletion, and loop creation, decreases the packet delivery ratio and increases end-to-end delay [33]. The rank attack exploits the inability of RPL to verify the rank values of nodes in the network. The malicious node disseminates DIO packets with a significantly lower rank value than its actual value to deceive the neighbour nodes that it provides the lowest cost path to the root node. This is done by initialising these constants RPL_CONF_MIN_HOPRANKINC and RPL_MAX_RANKINC to zero (0) [34].

The scripts that need modification to implement rank attacks are *rpl-private.h and rpl_mrfhof.c* can be found in the path *contiki/core/net/rpl/*. The *rpl-private.h* script stores Contiki RPL implementation declarations such as mode of operation, ICMP control packets default values, DAG routing tables, timings, and other essential information[15]. Moreover, this script *rpl_mrfhof.c* stores a function *calculate_rank(rpl_parent_t *p, rpl_rank_t base_rank)* that is used to calculate the rank value of its target node.

### *D. Worst parent attack*

RPL does not offer a mechanism to monitor node behaviour, it believes that every node is dependable and that it adheres to the protocol's standard policy[35]. In Worst Parent Attacks, an adversary would choose a reverse policy of RPL and choose an optimal route to the sink node by selecting a parent with a higher rank value [4, 9]. The attacker modifies the OF to choose the worst rank node as a parent [24].. This delays packet transmission and raises the ETX of all descended nodes of the malicious node [19]. The WPA is a network data traffic affecting attack causing an End-2-End Delay (E2E) and a reduction in the packet delivery ratio. Furthermore, it prevents the network from optimal convergence and isolates

| | | | | | | |
|---|---|---|---|---|---|---|
| [7] | A review of the detection of sinkhole attacks in RPL-based networks | The research reviewed sinkhole attack and detection techniques | 1 | No | No | Implementation of attacks is not presented |
| [8] | A review of secure routing challenges in LLNs | Review of blackhole and rank attacks | 2 | No | No | Implementation of attacks is not presented |
| [6] | The study reviews DIS-flooding attacks | A detailed overview of RPL and DIS-flooding attack | 1 | No | Yes | Implementation of attacks is not presented |
| [9] | A comprehensive survey exclusive of RPL-based attacks | Provides a review of 14 routing attacks | 14 | No | Yes | Implementation of attacks is not presented |
| [10] | A study of RPL attacks and defense mechanisms in IoT | Provides a review of 17 routing attacks and categorise them according to affected factors | 17 | No | Yes | Implementation of attacks is not presented |

In the related work, it has been discovered that many previous studies do not consider a structured implementation method for routing attacks, however, our study offers a unique perspective on the implementation of the routing attacks in the RPL network. Ultimately, it provides a comprehensive description of routing attacks, effects and factors impacted, and implementation of routing attacks in LLNs. It further presents attacking percentages that can be adopted to mimic operations of the networks under routing attacks.

## III. RPL Overview And Operations

This section briefly overviews the Routing Protocol for Low-power and Lossy Networks (RPL) and its operations. It also outlines the control packets used by RPL to construct and maintain the network topology to ensure efficient communication and optimal delivery of data packets.

RPL is a distance vector source routing protocol which supports unicast and multicast data transfer methods [11]. It employs a Destination-Oriented Directed Acyclic Graph (DODAG) to construct a tree-like topology [12]. The DODAG comprises a sink or root node and leaf nodes [13]. It has three primary traffic flows, namely, upward, downward, and non-root routing: multipoint-to-point, point-to-multipoint, and point-to-point, respectively [14]. RPL is an IPv6 routing protocol that allows transmitter nodes to create, find, and choose a packet transmission path to the destination root [15].

DODAG root utilises four Internet Control Message Protocol version 6 (ICMPv6) to create and maintain the topology of the LLNs, namely, DODAG Information Object (DIO), DODAG Object Advertisement (DAO), DODAG Information Solicitation (DIS), and DODAG Object Advertisement-Acknowledgement (DAO-ACK). To start a new DODAG, the sink node transmits a DIO to disseminate the latest routing information among DODAG nodes [16]. These include RPLinstanceID, its rank value, DODAG ID, Objective Function Code, and version number. Upon receiving a DIO packet, the node processes it and chooses a preferred parent based on the received rank value. Then, a unicast packet, DAO, is used to disseminate a child node's details to a parent node and to connect the child to the parent node. Upon receiving the DAO packet, the parent node will unicast a DAO-ACK to acknowledge the child-parent communication to the child node. DIS packets are dispatched either unicast or multicast by new nodes or nodes that lost their parents to solicit DIO packets from neighbour nodes and to join the established DODAG structure [17]. When receiving a multicast DIS packet, the receiver resets its trickle timer (which defines the interval of sending DIO) and multicast DIO packets. Any receiver of DIO packets processes them and unicast a DAO packet to the preferred parent. Furthermore, it is observed that a rise in DAO and DIO packets signals an unstable network topology, which may give rise to end-to-end delay, decrease packet delivery ratio and network throughput, and degrade the network's efficiency [18].

In RPL routing protocol operations, nodes await DIO messages from neighbouring nodes before joining the tree topology. These DIO packets are transmitted on an interval basis by each node using the trickle algorithm [19]. Trickle timer intervals are longer and shorter when the network is stable and unstable, respectively [20]. Moreover, when the network is unstable, the trickle timer is reset to send DIO packets more frequently [21]. A node may receive several DIO packets from neighbour nodes within its transmission range; it then chooses a preferred parent based on the rank value calculated using the Objective Function (OF) mechanism encapsulated in the DIO packets. Metrics used to define OF's incremental factor include link reliability, Hop count, energy consumption, ETX, etc. [22]. The IETF describes two objective function standards to calculate the rank value. namely, Objective Function Zero (OF0) and Minimum Rank with Hysteresis Objective Function (MRHOF), the former employs the hop count metric to dictate the shortest path to the sink, and the latter employs the Expected Transmission Count (ETX) metric to assess link quality and dictate routes with the lowest cost [23]. The rank value signifies a node's position relative to the sink, it increases moving down the DODAG tree from root to leaf nodes [24]. The rank value ensures optimal topological formation, network resources utilisation and quality traffic paths to the DODAG root [4, 12]. The notions of the rank property are that rank strictly increases from root to leaf nodes in DODAG, a child node must have a greater rank value than its parent, and lastly, a child node must

several nodes from the entire network [24]. WPA is a sub-optimal attack, it does not increase packet loss nor consume network resources [4]. Furthermore, it is noted that it is tedious to detect such malicious nodes since they do not demonstrate abnormal behaviour but only choose a worst-rank parent. The script for modification to implement the WPA *rpl-mrhof.c* is found in the path *contiki/core/net/rpl*.

Table II presents a synthesised overview of the attacks investigated in this research study. It exhibits the affected factors of each attack, the impact on network performance including affected performance metrics, and lastly, the exploited vulnerabilities of the RPL protocol.

TABLE II. ATTACKS IMPACT AND EXPLOITATION

| Attacks | Affected Factor | Impact on network | Performance Metrics | RPL Vulnerability |
|---|---|---|---|---|
| Rank | Topology | Stability | PM2 | Lack of verification of Rank Value |
| Sinkhole | Data traffic | Reliability | PM4, PM5 | High data loss |
| Worst Parent | Data traffic | Stability | PM2, PM4 | Lack of restriction on parent selection |
| DIS-Flooding | Resources | Availability | PM1, PM3, PM5 | Lack of restrictions on the number of DIS dissemination |
| **PM1**- Control Message Overhead, **PM2**- Delay, **PM3**-Energy Consumption, **PM4**-Packet Delivery Ratio, **PM5**-Troughput | | | | |

These attacks compromise the availability, stability, and security of the LLNs, allowing adversaries to intercept or disrupt communication between legitimate nodes [36]. RPL builds its topology using its control packets; modification in the contents of the packets gives rise to routing attacks [33]. These attacks cause loop creation, decrease packet delivery ratio and energy depletion, increase packet delivery latency, and low throughput. Ultimately, they affect network efficiency and reliability by degrading its performance. However, it is important to be able to implement network scenarios that mimic real-world routing attacks for the simulation of network resiliency and the development of defence techniques.

## V. METHODS

This paper aims to synthesise reviews on routing attacks in RPL-based IoT networks. The authors observed that it is necessary to understand the routing attacks in the protocol in question, the RPL. They then adopted the Systematic Literature Review (SLR) presented in [37]. The adopted method consists of five steps:

### *A. Definition of search keywords:*

They defined an array of keywords to query academic databases for relevant studies, such as "RPL"

### *B. Identification of academic databases:*

The authors identified databases to query their structure keywords array. They queried IEEE Access, ScienceDirect, Springer, and MDPI. These are major academic databases.

### *C. Query and Retrieval of Studies:*

The study retrieved 931 studies published in the years from 2021 to 2024. To filter the results, the authors defined screening and exclusion criteria, which enabled them to get the relevant studies from the query

### *D. Screening & exclusion of studies*

The authors excluded publications without full-text access, those that fall outside the borders of the review of RPL attacks, routing attacks in RPL, LLN routing attacks, or routing attacks in IoT, and duplicates.

### *E. Inclusion of studies*

The study then ended up reviewing 38 studies that are relevant and fall within the borders of this study.

To select relevant review RPL-based attacks publications within our scope, the authors of this paper screened titles and abstracts, resulting in the exclusion of 858 and the inclusion of 73. The final set of publications, which were considered in this review, was a result of the conducted full-text reading. The study then found that 38 publications were relevant and included in the study.

TABLE III. PUBLICATION SELECTION CRITERIA

| No | Inclusion | Exclusion |
|---|---|---|
| 1 | Published between 2021 & 2024 | A study is a duplicate |
| 2 | English language | Non-English |
| 3 | A publication remains within the borders of this study | Not relevant |
| 4 | Full-text reading is available | Is a grey literature |

## VI. DISCUSSION

The goal of this section is to present the outcomes of this study. The study answers questions related to the suitable simulation tools, discussion of factors affected by routing attacks, including performance metrics, attacking percentage for better attack simulation, and lastly, implementation, which includes descriptions of the routing attacks, characteristics, and implementation of routing attack-like simulation.

### A. *Which simulation tool is suitable for implementing RPL-based routing attacks?*

Several simulation tools, such as NetSim, MATLAB, Cooja, etc., may be used to simulate IoT networks. Different studies utilise different tools for their simulation experiments depending on their intended scenarios, topology, use cases, etc. However, as per the reviewed literature, most researchers prefer the Cooja running ContikiOS for their RPL-based IoT simulations [2, 18]. According to [36], simulations conducted using the Cooja platform have proven to be quite accurate; Cooja presents ideal real-world scenarios. Cooja is a Java open-source, portable, and multitasking operating system for IoT, particularly LLNs running the RPL protocol [32]. This tool simulates the binary code of actual sensor devices operating on the Contiki OS. It offers several modes to replicate real-world environments and includes auxiliary tools to help measure various metrics that assess system performance [28].

### B. *Which network performance metrics may demonstrate the presence of routing attacks?*

The synthesised publications highlight metrics that can be evaluated to determine the presence of the routing attack(s) in the IoT networks [16], namely, throughput, packet delivery ratio, energy consumption, end-to-end delay and control message overhead. Throughput is the measure of the amount of useful data that can be transmitted per unit of time and is expressed in Mbps. The higher the throughput, the better it is for the network. Among network performance metrics, throughput is the most critical one for evaluation [13]

Packet Delivery Ratio is the percentage of source-transmitted packets that reach their destination [15].It assists in calculating network reliability. Energy Consumption refers to the amount of energy consumed by network nodes throughout the network lifetime. It can be computed by summing the power consumed during node sleep mode, for processing, receiving data, and transmitting data [18]. End-to-end Delay is the measure of time a packet travels from source to destination through the network [29]. It is a common concept in Internet Protocol (IP) networks. It is different from Round-Trip Time (RTT), which defines time from source to destination and back to source. Control Message Overheard denotes the number of control packets transmitted during the network runtime to construct and maintain the network topology. In a case of network instability, control packets are generated by the nodes to optimise the routing topology [16] ultimately stabilising the network. An increase in control packets demonstrates network instability. The presented metrics may be used to identify discrepancies in the network, which would potentially indicate the presence of routing attacks.

### C. *What percentage of malicious nodes significantly impact the network's performance in proportion to legitimate nodes?*

The percentage of malicious nodes in the network may have a significant impact on the performance of the network; thus, to mimic the effect of routing attacks, one needs to consider the number of malicious nodes against the network size. The higher the attack intensity, the greater the impact can be observed on the network performance. Bokka et al in their study [13] evaluated the effect of 2 malicious nodes in a network of 20 nodes. It was observed that the impact was moderate but higher than what was observed in [32]; where they considered 1 malicious node out of 22 nodes, which yielded a low impact that one would mistake for one of the characteristics of LLNs, namely, low data rate, and lossy links. However, the studies [14, 18, 34] considered 7%, 8%, & 8% attacking nodes in their network simulations, respectively. It was observed that their attack intensity demonstrates a moderate impact with a significant decline in PDR and throughput, an increase in control message overhead, and energy consumption. High impact is observed in Nandhini et al study [33] where they measured the impact of the attack at 14% of malicious nodes, we observed a large number of packets being dropped and the presence of significant delay and energy consumption. Table III presents the attack percentage, network size and attack percentage, and level of attack impact and performance metrics per publication.

TABLE IV. ATTACK PERCENTAGE AND IMPACTED METRICS PER STUDY

| Ref | Simulation | Size | Attack | Impact | Attack % | Performance metrics |
|---|---|---|---|---|---|---|
| [13] | NetSim | 20 | 2 | M | 10% | Throughput, E2ED, CMO |
| [29] | NetSim | 5 | 1 | H | 20% | Throughput, E2ED, PDR, EC, |
| [14] | Cooja | 13 | 1 | M | 7% | EC, PDR, Radio Duty Cycle |
| [15] | Cooja | 16 | 3 | H | 19% | EC, CMO, PDR |
| [23] | Cooja | 20 | 1 | M | 10% | Delay, CMO, Throughput, |
| [32] | Cooja | 22 | 1 | L | 5% | Radio Duty Cycle, EC |
| [16] | NetSim | 16 | 2 | M | 13% | PDR, CMO, Throughput, E2ED |
| [18] | Cooja | 12 | 1 | M | 8% | E2ED, PC, |
| [25] | Cooja | 21 | 1 | L | 5% | PC, PLR, |
| [34] | Cooja | 12 | 1 | M | 8% | PC, Throughput |
| [3] | NS2 | 122 | 32 | H | 26% | Throughput, E2ED, PDR |
| [38] | Cooja | 100 | 50 | H | 50% | E2ED, Throughput, EC, PDR |
| [33] | Cooja | 70 | 10 | H | 14% | PDR, CMO, E2ED, EC |

Low-L, Medium-M, high-H, Energy Consumption-EC, end-to-end delay- 2ED, Packet Delivery Ratio-PDR, Control Message Overhead-CMO, Packet Loss Ratio-PLR

To propose effective detection and mitigation techniques, 5% attacking nodes could be used as a minimum attack percentage, as it is closer to the characteristics of LLNs; so the techniques should be able to detect such a small number of attacks, as they can have a significant impact in the long run. Secondly, 7-13% demonstrate moderate impact, and anything above and including 14% can be used for high-impact analysis.

### *D. What key steps or framework can be adopted to implement routing attacks?*

To analyse the performance of the network under routing attack, generate attack datasets, develop detection and mitigation techniques, etc., it is vital for researchers to develop scenarios that mimic real-world routing attacks. Many works, including [14-16], presents simulation results demonstrating the presence of routing attacks in the network. However, a structured implementation is never presented, which in many cases limits the comparison of simulation scenarios and defence techniques among researchers. This study, however, identified high-level steps that were observed to occur in the synthesised literature [25, 33] as Ad-hoc methods. The paper observed that it is significant for researchers to adopt a structured method to implement routing attacks, which would potentially fuel cooperation among them.

The study. The potential key steps which may be adopted in the implementation of routing attacks in LLNs include cloning of Contiki project file, modifying the operations of the RPL protocol by modifying the core files, including the header and source scripts to mimic the routing attack of interest, compiling the edited scripts and correcting errors, loading the compiled scripts into the firmware of the selected mote, and lastly, logs collection which involves collecting network operation data, including packets sent, received, time, power consumption, etc.

## VII. CONCLUSION

This paper explores four routing attacks—DIS flooding, sinkhole, rank, and worst-parent attacks—alongside network metrics that indicate their presence. It also identifies key steps for the structured implementation of these attacks in Low-power and Lossy IoT Networks. It was discovered that these four attacks have an impact on network topology, resources, and data traffic. Moreover, they affect the performance of the network in terms of packet delivery ratio, end-to-end delay, control message overhead, throughput, and energy consumption. It is observed that having a structured implementation would potentially allow ease of comparative analysis of studies, algorithms, adoption of defence techniques, etc. An ideal minimum attack intensity is observed to be 5%, which provides a low to moderate impact on the network, and 15% demonstrates a high impact on network performance. Attack intensity is a very important metric to evaluate the robustness and effectiveness of defence techniques.

The focus of future research will explore an ad-hoc implementation framework, then propose and adopt a structured implementation framework for routing attacks that can be adopted to allow easy comparison of proposed defence techniques, scenarios in literature, and collaborations among researchers. Furthermore, propose attacks and network logs modules. Another future direction is exploring machine learning algorithms to determine the best-performing model based on network data collected using the implementation framework to be proposed.

## REFERENCES


[1] Jahangeer, A., Bazai, S.U., Aslam, S., Marjan, S., Anas, M., and Hashemi, S.H.: 'A Review on the Security of IoT Networks: From Network Layer's Perspective', IEEE Access, 2023, 11, pp. 71073-71087

[2] Al-chikh Omar, A.A.R., Soudan, B., and Ala, A.: 'A comprehensive survey on detection of sinkhole attack in routing over low power and Lossy network for internet of things', Internet of Things, 2023, 22, pp. 100750

[3] Bilal, A., Hasany, S.M.N., and Pitafi, A.H.: 'Effective modelling of sinkhole detection algorithm for edge-based Internet of Things (IoT) sensing devices', IET Communications, 2022, 16, (8), pp. 845-855

[4] Sahay, R., Geethakumari, G., and Mitra, B.: 'Mitigating the worst parent attack in RPL based internet of things', Cluster Computing, 2022, 25, (2), pp. 1303-1320

[5] Miranda, C., Kaddoum, G., Boukhtouta, A., Madi, T., and Alameddine, H.A.: 'Intrusion Prevention Scheme Against Rank Attacks for Software-Defined Low Power IoT Networks', IEEE Access, 2022, 10, pp. 129970-129984

[6] Nisha, Dhingra, A., and Sindhu, V.: 'A Review of DIS-Flooding Attacks in RPL based IoT Network', in Editor (Ed.)^(Eds.): 'Book A Review of DIS-Flooding Attacks in RPL based IoT Network' (2022, edn.), pp. 1-6

[7] Rani, J., Dhingra, A., and Sindhu, V.: 'A Detailed Review of the IoT with Detection of Sinkhole Attacks in RPL based network', in Editor (Ed.)^(Eds.): 'Book A Detailed Review of the IoT with Detection of Sinkhole Attacks in RPL based network' (2022, edn.), pp. 1-6

[8] Tasneem, B., and Wahid, M.: 'A Review of Secure Routing Challenges in Low Power and Lossy Networks', in Editor (Ed.)^(Eds.): 'Book A Review of Secure Routing Challenges in Low Power and Lossy Networks' (2021, edn.), pp. 120-125

[9] Koosha, M., Farzaneh, B., and Farzaneh, S.: 'A Classification of RPL Specific Attacks and Countermeasures in the Internet of Things', in Editor (Ed.)^(Eds.): 'Book A Classification of RPL Specific Attacks and Countermeasures in the Internet of Things' (2022, edn.), pp. 1-7

[10] Dhingra, A., and Sindhu, V.: 'A Study of RPL Attacks and Defense Mechanisms in the Internet of Things Network', in Editor (Ed.)^(Eds.): 'Book A Study of RPL Attacks and Defense Mechanisms in the Internet of Things Network' (2022, edn.), pp. 1-6

[11] Karmakar, S., Sengupta, J., and Bit, S.D.: 'LEADER: Low Overhead Rank Attack Detection for Securing RPL based IoT', in Editor (Ed.)^(Eds.): 'Book LEADER: Low Overhead Rank Attack Detection for Securing RPL based IoT' (2021, edn.), pp. 429-437

[12] Ghaleb, B., Al-Dubai, A., Hussain, A., Ahmad, J., Romdhani, I., and Jaroucheh, Z.: '(POSTER) Resolving the Decreased Rank Attack in RPL's IoT Networks', in Editor (Ed.)^(Eds.): 'Book (POSTER) Resolving the Decreased Rank Attack in RPL's IoT Networks' (2023, edn.), pp. 65-67

[13] Bokka, R., and Sadasivam, T.: 'Simulation-based Analysis of RPL Routing Attacks and Their Impact on IoT Network Performance', Journal of Electronic Testing, 2024, 40, (2), pp. 259-273

[14] Kumar, D., Sinha, N., Mishra, A.K., and Tripathy, A.K.: 'An Experimental Comparison and Impact Analysis of Various RPL-Based IoT Security Threats Using Contiki Simulator', in Editor (Ed.)^(Eds.): 'Book An Experimental Comparison and Impact Analysis of Various RPL-Based IoT Security Threats Using Contiki Simulator' (2024, edn.), pp. 111-116

[15] Gupta, H., Bhardwaj, S., and Dave, M.: 'Security Analysis of RPL-Based IoT Networks: Evaluating the Impact of Attacks on Performance Parameters', in Editor (Ed.)^(Eds.): 'Book Security Analysis of RPL-Based IoT Networks: Evaluating the Impact of Attacks on Performance Parameters' (2024, edn.), pp. 1-8

[16] Bokka, R., and Sadasivam, T.: 'DIS flooding attack Impact on the Performance of RPL Based Internet of Things Networks: Analysis', in

Editor (Ed.)'(Eds.): 'Book DIS flooding attack Impact on the Performance of RPL Based Internet of Things Networks: Analysis' (2021, edn.), pp. 1017-1022

[17] Medjek, F., Tandjaoui, D., Djedjig, N., and Romdhani, I.: 'Multicast DIS attack mitigation in RPL-based IoT-LLNs', Journal of Information Security and Applications, 2021, 61, pp. 102939

[18] Rajasekar, V.R., and Rajkumar, S.: 'A Study on Impact of DIS flooding Attack on RPL-based 6LowPAN Network', Microprocessors and Microsystems, 2022, 94, pp. 104675

[19] Subhash, P.: 'rankIMPACT: A Study of Rank Attacks impact over RPL based Internet of Things Networks', in Editor (Ed.)'(Eds.): 'Book rankIMPACT: A Study of Rank Attacks impact over RPL based Internet of Things Networks' (2023, edn.), pp. 1-5

[20] Yoshida, M., Uchida, R., and Noguchi, T.: 'Rank Attack Avoidance Method based on Neighbor Node Rank Variation in RPL Network', in Editor (Ed.)'(Eds.): 'Book Rank Attack Avoidance Method based on Neighbor Node Rank Variation in RPL Network' (2023, edn.), pp. 353-357

[21] Aljufair, G., Mahyoub, M., and Almazyad, A.S.: 'On Mitigating DIS Attacks in IoT Networks', in Editor (Ed.)'(Eds.): 'Book On Mitigating DIS Attacks in IoT Networks' (2023, edn.), pp. 104-109

[22] Mishra, A.K., Puthal, D., and Tripathy, A.K.: 'A Secure RPL Rank Computation and Distribution Mechanism for Preventing Sinkhole Attack in IoT-based Systems', in Editor (Ed.)'(Eds.): 'Book A Secure RPL Rank Computation and Distribution Mechanism for Preventing Sinkhole Attack in IoT-based Systems' (2023, edn.), pp. 1-6

[23] Nejad, F.V., Sadeghi, M.M.G., and Rezvani, M.H.: 'Analysis of Decreased Rank Attack on RPL-Based IoT Networks', in Editor (Ed.)'(Eds.): 'Book Analysis of Decreased Rank Attack on RPL-Based IoT Networks' (2024, edn.), pp. 40-45

[24] Kiran, U.: 'IDS To Detect Worst Parent Selection Attack In RPL-Based IoT Network', in Editor (Ed.)'(Eds.): 'Book IDS To Detect Worst Parent Selection Attack In RPL-Based IoT Network' (2022, edn.), pp. 769-773

[25] Kiran, U., Maurya, P., and Sharma, H.: 'Investigating Routing Protocol Attacks on Low Power and Lossy IoT Networks', SN Computer Science, 2024, 5, (4), pp. 393

[26] Sejaphala, L.C., Malele, V., and Lugayizi, F.: 'High-Level Defence Model against Routing Attacks on the Internet-of-Things', Indonesian Journal of Computer Science, 2024, 13, (1), pp. 669-679

[27] Ankam, S., and Reddy, D.N.S.: 'A mechanism to detecting flooding attacks in quantum enabled cloud-based lowpower and lossy networks', Theoretical Computer Science, 2023, 941, pp. 29-38

[28] Guo, G.: 'A Lightweight Countermeasure to DIS Attack in RPL Routing Protocol', in Editor (Ed.)'(Eds.): 'Book A Lightweight Countermeasure to DIS Attack in RPL Routing Protocol' (2021, edn.), pp. 0753-0758

[29] Mohapatro, M., and Snigdh, I.: 'An Experimental Study of Distributed Denial of Service and Sink Hole Attacks on IoT based Healthcare Applications', Wireless Personal Communications, 2021, 121, (1), pp. 707-724

[30] Sejaphala, L.C., and Velempini, M.: 'The Design of a Defense Mechanism to Mitigate Sinkhole Attack in Software Defined Wireless Sensor Cognitive Radio Networks', Wireless Personal Communications, 2020, 113, (2), pp. 977-993

[31] Yadollahzadeh Tabari, M., and Mataji, Z.: 'Detecting Sinkhole Attack in RPL-based Internet of Things Routing Protocol', Journal of AI and Data Mining, 2021, 9, (1), pp. 73-85

[32] Ambarkar, S.S., and Shekokar, N.: 'Impact Analysis of RPL Attacks on 6Lo WPAN based Internet of Things network', in Editor (Ed.)'(Eds.): 'Book Impact Analysis of RPL Attacks on 6Lo WPAN based Internet of Things network' (2021, edn.), pp. 1-5

[33] Nandhini, P.S., Kuppuswami, S., Malliga, S., and DeviPriya, R.: 'Enhanced Rank Attack Detection Algorithm (E-RAD) for securing RPL-based IoT networks by early detection and isolation of rank attackers', The Journal of Supercomputing, 2023, 79, (6), pp. 6825-6848

[34] Sharma, S., and Verma, V.K.: 'Security explorations for routing attacks in low power networks on internet of things', The Journal of Supercomputing, 2021, 77, (5), pp. 4778-4812

[35] Chaitanya, K., Y, K., Kumari, N., Ch, R., and K, E.: 'Rank Attack (RA) Detection in RPL Protocol based on Network Characteristics', in Editor (Ed.)'(Eds.): 'Book Rank Attack (RA) Detection in RPL Protocol based on Network Characteristics' (2023, edn.), pp. 465-470

[36] Sridhar, K., Kumar, B.A., Devi, S.A., Raju, V.P., Soni, A., Singh, P., and Deore, S.S.: 'Enhancing Security in IoT Networks Through RDAD for Attack Detection in RPL-Enabled Environments', SN Computer Science, 2024, 5, (7), pp. 864

[37] Sejaphala, L.C., Malele, V., and Lugayizi, F.: 'A Systematic Literature Review on Defense Techniques Against Routing Attacks in Internet of Things', Latin-American Journal of Computing, 2025, 12, (1), pp. 35 - 49

[38] Prathapchandran, K., and Janani, T.: 'A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest – RFTRUST', Computer Networks, 2021, 198, pp. 108413

### 4.2.5 Article 5

#### 1. Article publication details

**Title**: Design and Validation of an Adaptable Framework for Implementing Routing Attacks in Low-Power and Lossy Networks

Status: In the pipeline

#### 2. Article synthesis

(i) Purpose

The purpose of this article is to evaluate the effects of the assault on the IoT. It addresses the lack of structured methodologies for implementing and simulating routing attacks, as well as for generating datasets, and ensuring simulation and experiment reproducibility for comparative analysis among studies. And lastly, the article proposes a methodical strategy for the execution and simulation of routing attacks to allow collaboration among researchers, enable consistent scenario comparisons, and support the development of robust and effective defence mechanisms against routing attacks, leveraging the generated datasets.

(ii) Methods

A quantitative methodological choice was adopted for data generation and collection following an experimental strategy and deductive research approach. Cooja ContikiOS was utilised to simulate two scenarios, the first with 25 sensor nodes and 1 sink node, and the other scenario with 15% attack intensity of DIS-Flooding nodes. Data was collected from network performance metrics, that is, beacon interval, PDR, End-to-End Delay, CPU and energy consumption.

(iii) Results and Discussion/Findings

The simulation results validated the framework's effectiveness in implementing a DIS-Flooding attack and baseline scenarios. Furthermore, they statistically demonstrated the effect of the attack on network performance metrics, demonstrating that attacked nodes exhibited a reduced beacon interval of less than 50,000 ms. This result confirms heightened activity stemming from frequent

responses to DIS packets. The DIS-Flooding attack forced the attacked nodes to consume 0.75 mW compared to 0.5 mW in the baseline scenario, representing a 20% increase that underscores the elevated processing demands during the attack. The attack scenario, furthermore, resulted in an average power consumption of 7.6 mW, compared to 3.2 mW in the baseline - a 4.5 mW rise that confirms the resource-intensive nature of DIS-flooding. PDR declined by up to 50%, with certain nodes dropping as low as 25%, primarily because nodes prioritised processing DIS packets and consequently discarded data packets. End-to-end delays also surged dramatically, reporting over 9,000 ms under attack versus less than 1,000 ms in the baseline. The discussion emphasises that this framework effectively induced network degradation, thereby validating its utility for implementing attacks. These results align closely with prior studies, reinforcing the critical need for standardised frameworks to enable reproducibility and facilitate comparative analysis.

(iv) Conclusion

This framework represents an adaptable framework for implementing routing attacks in LLNs, addressing the lack of standardised methodologies. The framework's structured approach (cloning, modification, building, flashing, logging) enables reproducible experiments and fosters collaboration among researchers. It demonstrates the framework's effectiveness via Cooja ContikiOS simulations, showing significant network degradation in DIS-Flooding attacks. This article provides a logical basis for generating standardised datasets and developing intelligent detection models, with plans to use collected logs for this purpose.

## 3. Full article

Journal of Information Systems and Informatics
Vol. 6, No. 3, September 2024 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v6i2.759 Published By DRPM-UBD

# Design and Validation of an Adaptable Framework for Implementing Routing Attacks in Low-Power and Lossy Networks

**Abstract**

Low-power and Lossy Networks (LLNs) are an emerging technology that modernises how IoT devices communicate and transmit network traffic. The capability of LLNs to allow IoT resource-constrained devices to communicate makes them suitable for adoption in IoT applications such as environmental monitoring, military surveillance, etc. Given their well-vested suitability in IoT, LLNs are susceptible to routing attacks, which pose threats to the degradation of resources, traffic, and topology of the network. It is vital to defend the network from routing attacks. To defend against routing attacks, a standard framework for routing attack implementation should be adopted, which allows ease of scenario comparison, defence techniques adoption, and fosters collaboration among researchers in the field of routing attacks in LLNs. Many studies demonstrate the impact of routing attacks, but only a few present the frameworks for implementing routing attacks. This study proposes an adaptable framework for routing attack implementation that fosters collaboration and allows for easy comparison studies, and potentially contributes to the design of robust defence techniques against routing attacks. In addition, the paper presents a comprehensive review of existing works and a methodology for the reproducibility of this study. The study utilised the proposed framework to implement and simulate a DIS-Flooding attack and baseline scenarios for comparison. The Simulations were conducted on Cooja Conitki to evaluate the framework's effectiveness. Results indicate significant degradation 30% in packet delivery ratio, and increased control message overhead, end-to-end delay, and increased 20% energy consumption, demonstrating the framework's utility for routing attack implementation.

**Keywords**: RPL, LLNs, Routing Attacks, DIS-Flooding attack

## 1. INTRODUCTION

The RPL is crucial to IoT as it optimises resource consumption and ensures reliable data transmission in a resource-constrained environment [1]. Its ability to establish communication paths between sensor nodes makes it indispensable for IoT applications, including smart agriculture and smart cities. However, the

increase in adoption of connected devices expands the attack terrain, making it crucial to address vulnerabilities and protect sensitive information from potential threats [2].

Most works on RPL attacks are concentrated on the impact of attacks in network performance analysis and/or dataset collection for intelligent detection techniques under attacks, with minimal reference to how operating system modules may be modified to effectively launch such attacks [3]. Furthermore, malicious nodes cannot be altered during simulation.

The importance of security system development within IoT ecosystems holds immense significance [4]. However, a robust routing attack implementation is indispensable to ensure a structured security system design, reproducible experiments, and comparative analysis of research works in the field of routing attacks on RPL. The discovery of this study is expected to lay the groundwork for the current and future academic and industrial works in relation to routing attacks in LLNs.

The motivation of the study stems from three primary observations i.e. RPL introduces intricate mechanisms that create multiple attack vectors, current approaches to routing attack research lack standardized attack implementation and often rely on ad-hoc and inconsistent methodology, making comparative analysis a challenge. Furthermore, a structured framework enables systematic exploration of potential network vulnerabilities and facilitates more robust security designs. The study contributes a comprehensive framework for routing attack implementation in LLNs, enabling reproducible experiments, as well as a structured and systemized methodology for routing attack impact analysis. The study, furthermore, provides simulation-based validation demonstrating the effectiveness of the adopted methodology and proposed framework using Cooja ContikiOS to assess attack impact on RPL networks, and quantitative analysis of attack effect on the network key performance metrics i.e. Control Message Overhead (CMO), power consumption, and Packet Delivery Ratio (PDR).

### 1.1 RPL Overview

LLN devices force a reduced transmission range; as a result, the network uses the sensors as intermediate nodes for efficient data transmission to the sink. Furthermore, the network suffers from low packet data rate, packet losses, resource-constrained devices, and offers a Maximum Transmission Unit (MTU) of 127 bytes. Therefore, the transmission of data in such low-power and lossy networks requires a routing protocol that can address these challenges. RPL promises to address the challenges faced by the LLNs. RPL aims to facilitate Protocol Data Units (PDUs) between sensor devices with low latency and reliability while minimising the power utilisation of devices. he RPL protocol, a proactive routing mechanism, establishes and maintains a routing topology known

as a Destination-Oriented Directed Acyclic Graph (DODAG) through the periodic exchange of control messages. DODAGs are hierarchical structures at the node level to ensure efficient data transmission [2].

RPL defines four control messages to carry out its responsibilities i.e. Destination Information Solicitation (DIS), Destination Information Object (DIO), Destination Advertisement Object (DAO), and DAO-Acknowledgement (DAO-ACK). DIS packets are used by new sensors or those that lost their parents to solicit DIO packets from nodes connected to the DODAG to connect or update their DODAG structure. DIS packets can be multicast or broadcast. Upon receiving a multicast or broadcast, the receiver assumes that the network is unstable, then resets its trickle timer and multicasts a DIO packet [5]. A Trickle algorithm is used to facilitate transmission intervals of DIO messages. RPL utilises this algorithm to manage the rate at which DIO packets are transmitted to increase the chance of the DIS sender joining the DODAG.

DIO packets are used to transmit information about the current DODAG topology, such as the Objective function used, DODAGID, RPLInstanceID, Version number and configuration metrics, and the rank value of the sender node. DIO packets are used by receiving nodes to choose a preferred parent and join a DODAG. Upon receiving a DIO, a node then selects a preferred parent based on the used routing metric (rank value, hop count, or expected transmission count) and unicast a DAO packet to its preferred parent. DAO packets are unicasted by a child node to provide its parent with a downward route, and DAO-ACK is used by the parent node to acknowledge receipt of a DAO. Broadcasting DIS packets forces nodes to reset their trickle timer.

### 1.2 DIS-Flooding Attacks

Attackers transmit large volumes of packets to the network to consume communication resources or render target devices unavailable [2, 6]. A technique for transmitting DIS packets involves broadcasting them to all nodes within the sender's radio transmission range. Upon receiving a DIS packet, the receiving node's trickle timer is reset, triggering the broadcast of its DIO packet. An attacker can exploit the multicast solicitation mechanism of the RPL protocol to initiate a DIS-flooding attack [7].
The attacker either broadcasts or multicasts DIS packets to the victim nodes [8]. Upon receiving DIS packets, victim nodes reset their trickle timer and multicast DIO packets throughout the network [5]. An attacker persistently sends DIS packets to a target node within its transmission [9], disregarding DIO packets transmitted by neighbouring nodes. The use of multicast or broadcast DIS control packets elevates control message overhead and energy consumption. This disrupts

the availability of legitimate nodes, communication channels, and other network resources [10]. Broadcast and DIS packets trigger frequent resets of the trickle timer in receiving nodes to its minimum value, interrupting the scheduled transmission of DIO packets. These repeated trickle timer resets, caused by a high volume of received DIS packets and excessive DIO transmissions from victim nodes, significantly increase control packet overhead [6, 11]. DIS-flooding attacks, as resource-intensive attacks, rapidly escalate the energy consumption of affected nodes, leading to a reduced network lifespan, diminished availability of communication links [5] and degraded network efficiency.

## 2. LITERATURE REVIEW

In this section authors present reviews of existing works that present the routing attacks implementation framework and/or adopted simulation methodology for RPL Networks. Publications included in this section demonstrated that they can implement routing attacks in RPL-based networks, it is essential to investigate and synthesise the methodologies employed for implementing routing attacks.

The study [3] introduces the implementation of known routing attacks using Contiki-NG. It further proposes a framework to facilitate the simulation experiment of multiple RPL attacks under distinct setups in terms of severity and duration. Using C preprocessor instructions to command which attack code to execute during build. However, the proposed reference implementation is the automation of attack launch, as they used Boolean variables to manage the timing and activation of a routing attack. The authors of the paper [10] demonstrated the impact of sinkhole attacks on the RPL network. However, the paper uses an ad-hoc methodology which does not guarantee the reproducibility of their work. Work in [12] demonstrated the impact of six routing attacks. Their adopted ad-hoc framework embeds attacker code on each sensor node in the network, wherein a node must check if it is an attacker or not. This increases the margin of error and does not demonstrate feasibility. Furthermore, attacking nodes are hard coded which hinders attack density alterations. Przemyslaw and Jaroslaw in their study [8] implemented four routing attacks aiming to assess the network's performance under routing attack conditions. An individual attack was simulated and logged. However, a clear framework that was followed is not presented, though the results demonstrate the impact of the simulated attacks.

The study [4] like [8] evaluated the impact of multiple routing attacks. Though their results illustrate the expected impact of each attack on the network, the method of attack implementation is not presented. This hinders reproducibility and ease of comparison. The authors of the work [13] evaluated the performance of DIS-Flooding attacks using the NetSim simulation tool. In their implementation of the attack, the malicious code is integrated into every sensor node's source code and for every network event, each node checks if it is a malicious node or not. If it is a malicious node, it transmits and drops DIS and

DIO packets respectively. Though the authors provided implementation steps; however, it does not guarantee reproducible experiments. The same can be observed from the work in [13], where ad-hoc methods are used to implement and analyse the impact of routing attacks in LLNs. The use of ad-hoc methods is also observed in the work [14]. The paper demonstrates the impact of the DAO flooding attack and further proposes a secure protocol as a measure against the attack using ad-hoc methods, which would be an obstacle for the research community.Modification of routing protocol logic appears to be a viable way to implement routing attacks. The study [15] adopted such an approach to implement DIS-Flooding attacks. The study proposes a modification of protocol logic files in Cooja's core folder to implement routing attacks. The modified files are then part of the Cooja core project directory. The works [6, 7] adopted the methodology presented in the work [15] to analyse the impact of six and four routing attacks on network performance, respectively. It is, however, not clear which protocol logic files normal and attacking nodes use in both studies. Furthermore, it appears that the proposed framework cannot implement multiple attacks in a single simulation scenario.

The studies [6, 7] illustrate that having a structured implementation of routing attacks could potentially influence reproducible experiments, improve comparative analysis of proposed studies, and, as such, foster the generation of standardised datasets and ultimately the development of robust and effective security mechanisms against routing attacks.

## 3. METHODS

This section focuses on the adopted methodology to reach the objectives of this paper. It is essential to note that this paper aims to propose a routing attack implementation framework on Routing Protocol over Low-power and lossy networks (RPL), which is a widely used routing protocol for resource-constrained IoT devices due to its scalability and energy efficiency. The significance of the framework is to foster reproducible experiments, comparative analysis studies, and research collaborations.

Furthermore, given the adoption of machine learning in the fight against routing attacks, as suggested in the work [16]. The systemised methodology (see Fig. 1) adopted promises the generation of standard IoT routing attack datasets and ultimately the design and development of robust and effective security techniques.

Journal of Information Systems and Informatics
Vol. 6, No. 3, September 2024
p-ISSN: 2656-5935 http://journal-isi.org/index.php/isi e-ISSN: 2656-4882

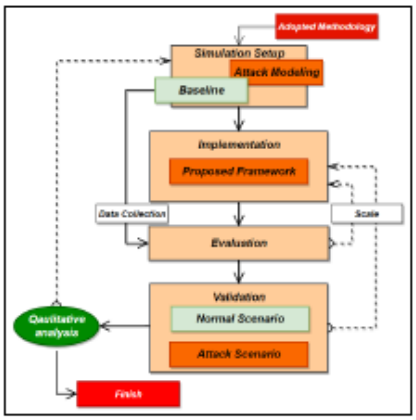


**Figure 1.** Proposed methodology for routing attacks simulation

### 3.1 Simulation Setup

Simulation Environment

Cooja serves as a desirable and widely used simulation platform designed explicitly for the ContikiOS [7], an enabler of the low-power IoT space [17]. Cooja, with its concentration on wireless sensor simulations, offers researchers and developers a powerful ability to simulate their ContikiOS-based applications before deployments. The Cooja is a widely adopted simulation tool in both academic as well as in industrial simulation setups. It is an open-source platform that fosters community-driven contributions and improvements, ensuring its ongoing relevance and efficacy within the low-power and lossy IoT ecosystem

The environment supports a whole range of features, such as simulation of ContikiOS operable devices and emulation of limited resources devices [18] that enables the creation and virtualisation of RPL-based network setups and topological structures. Furthermore, it allows multiple node simulations, which enables researchers to evaluate the performance of protocols and networks in a controlled virtual environment.

Simulation Parameters

To evaluate the effectiveness of the proposed framework, a simulation setup was designed following the framework of routing attacks implementation in IoT using the Cooja simulation platform. The following Table 1 highlights the simulation setup where a network simulation area of 100 m x 100 m was set up, comprised of 25 sensor nodes, 1 sink, and 4 attacker nodes. The simulation utilised the Sky mote and employed the UDP as the transport protocol, along with the IEEE 802.15.4 standard for the PHY and MAC layers. The Tmote Sky is a widely used wireless mote designed for research and experimentation in Low-power and Lossy

Networks (LLNs). It is equipped with 92kb flash memory and 16 MHz CPU, which makes it suitable for field deployment, implementation of IDS and routing protocols with logging, amongst others.

**Table 1.** Simulation setup

| Settings | Values |
|---|---|
| Simulation tool | Cooja ConitkiOS |
| Mote type | Sky Mote |
| Dimension area | 100 m x 100 m |
| Transmission range | 50 m |
| Sensor nodes | 25 |
| Sink node | 1 |
| Attacker nodes | 4 |
| Radio Medium | Unit Disk Graph Medium |
| Data rate | 256kbps |

The study defines a 15% attack intensity to simulate the network attack scenario. It is worth noting that, though the number of malicious nodes does affect the performance of the network, however, the number of attacked nodes can ultimately yield desirable and realistic results. One can have 10 malicious nodes, for example, which only attack 12% of the network, as compared to a smaller number of malicious nodes strategically placed to attack a larger number of legitimate nodes. As such, this study adopts the attack model and intensity distribution proposed in the work [16] as presented in Table 2, however, it only focuses on 25 network sizes with a 15% attack intensity. The attack intensity denotes the number of attacking nodes. As presented in Table 2 below, a network size of 25 nodes has 15% of attacking nodes.

**Table 2.** Attack intensity distribution

| NETWORK SIZE | ATTACK INTENSITY | | |
|---|---|---|---|
| | 5% | 10% | 15% |
| 25 | 1 | 3 | 4 |
| 36 | 2 | 4 | 5 |
| 64 | 3 | 6 | 10 |

### 3.2 Baseline Scenario

The IoT simulation environment for the baseline scenario (see Fig. 2) is for comparison with the network attack scenario. In the baseline scenario, we consider a total of 25 sensors, 1 sniffer and 1 sink node. The logs collected from the baseline

scenario because a benchmark for comparison and evaluation of results obtained in the attacked network.

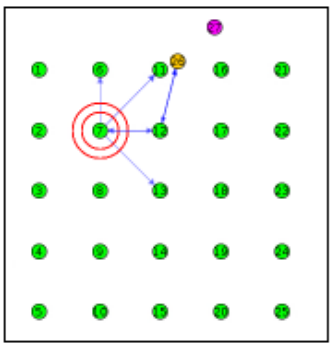

**Figure 2.** Baseline scenario simulation area

### 3.3 Attack Modelling

This step involves attack definition, profiling, and definition of attack triggers. The study modelled two routing attacks such as. DIS-Flooding and Sinkhole attacks. DIS-Flooding attack, the attacker node broadcasts DIS packets to sensor nodes in its transmission range, forcing victim nodes to transmit DIO packets and remain actively listening to incoming packets, thus consuming their energy and creating instability and suboptimisation of the network. The sinkhole attacker, on the other hand, transmits and manipulates the routing metric (rank value) of the RPL protocol to appear as the preferred parent to its neighbours, then drops UDP packets transmitted on its way. Attacks are triggered once attacking nodes are placed in the simulation environment.

### 3.4 Implementation

It is worth noting that in the third-last step of our methodology, we adopt the proposed framework presented in Section 4. In this step, we implement the five steps defined in the proposed framework, that is, cloning, modification, building and compiling, code flashing and logging.

### 3.5 Evaluation

Routing attacks are severe and result in network performance degradation. In this work, we evaluated the network performance during attack simulations and considered the most responsive and essential network performance metrics such as Power consumption, End-to-End Delay, Packet Delivery Ratio, Control Message Overhead, and beacon interval.

Packet Delivery Ratio (PDR) presents the proportion of data packets successfully received at a root node to those transmitted by the sensor nodes.

$$PDR = \frac{\sum_{j=1}^{r} Pr_j}{\sum_{i=1}^{s} Ps_i} * 100 \quad (1)$$

It is computed using equation 1, where *Ps* denotes the quantity of transmitted data packets and *Pr* denotes those that are successfully received at the root.
The end-to-end delay presents the average of different delays associated with each packet sent and received by sensor nodes and sink node, respectively, computed by equation (2), where *Ts* and *Tr* denote the time when each packet is sent by sensor nodes and received by sink node, respectively.

$$Delay = \frac{\sum_{i=1}^{pr}(Tr_i - Ts_i)}{pr} \quad (2)$$

Energy consumption is one of the crucial network performance metrics to consider in the LLNs, it affects network performance in various ways. It refers to the amount of operating power consumed by each sensor node in a network lifetime, computed by equation (3)

$$PC\ (mW) = \frac{(CPU*0.5+LPM*0.0005+Tx*17.4+Tx*18.8)*3v}{32768} \quad (3)$$

*CPU* denotes active mote power consumption during computations, *LPM* denotes power consumption during standby mode, and *Tx* and *Rx* denote power consumed during transmission and listening respectively.
Control Message Overhead (CMO) represents the number of control packets i.e. DIS, DIO, and DAO transmitted during the network's runtime. Where *nrt* denotes the network runtime, DIS, DIO, and DAO denote the respective control packets. CMO is computed using equation (4)

$$CMO = \sum_{i=1}^{nrt}(DIS_i + DIO_i + DAO_i) \quad (4)$$

### 3.6 Validation

To validate the effectiveness of the proposed framework, the authors of this work compared the outcomes of the attack and baseline scenarios. An attack within the network can be identified by a decline in network performance, which can be viewed on the selected network performance metrics.

This section presents the methodology which was adopted to conduct this study. Highlighting the network simulation setup, which includes the simulation environment and parameters. Further, presenting a baseline scenario and attack modelling.

### 3.7 Proposed Framework

The literature demonstrates that attacks, particularly routing attacks in Routing over Low-Power and Lossy Networks, have been investigated and evaluated [8, 15]. However, the current literature does not present a comprehensive framework for the implementation of routing attacks. As such, this paper proposes an adaptable framework to implement and launch routing attacks in Cooja ContikiOS for academic purposes, as shown in Figure 3, and furthermore, insinuates the structured attack implementation and impact analysis, which will subsequently enable standardised detection and mitigation techniques implementations for adoption in real-world IoT applications.

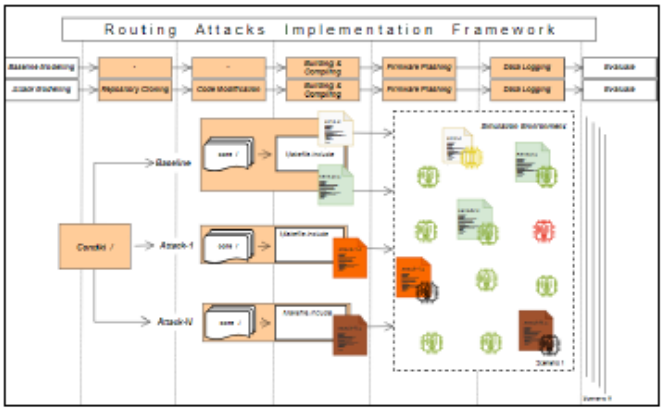


**Figure 3.** Routing attacks implementation framework

Our proposed framework follows five steps of implementation, which are cloning, modification, building, flashing, and logging:

**Repository Cloning**-Clone Contiki files to several attack types (N) you want to implement. Rename the cloned folders to the names of the attacks investigated for simplicity, that is, attack-1, attack-2, …, attack-N. This approach not only separates attack and legitimate core folders but also ensures modification of the logical operations of the legitimate and attack routing (see Fig. 3). It further allows the implementation of multiple attacks, as most implementations in the literature consider individual attacks triggered when their simulation starts [3].

**Code Modification-** Exploit the routing protocol's logic as part of implementing the attack(s). This can be done by modifying specific (*.h* and *.c* extension) files in the *core folder* of the project for each attack. Then modify the PROCESS_THREAD() function in the *attack-1.c*, …, *attack-N.c* script(s) for the malicious node to execute during the attack. Modification of protocol logic enables the implementation of different routing attacks with different logical characteristics. Some of the scripts to modify the logic of the protocol are:
*rpl-private.h* stores private declarations of RPL, such as default values for ICMP packets, mode of operation, timings, etc.
*rpl-timer.c* handles all timing-related operations of the RPL protocol. The script uses a tickler timer algorithm to adapt the sending rate of control packets such as DIS, DAO and DIO based on network stability.
*rpl-mrhof.c* implements the minimum Rank with Hysteresis Objective Function (MRHOF), the default OF used by child nodes to select parent nodes. It calculates rank value based on Expected Transmission Count (ETX) or latency metrics, and it further helps to facilitate the selection of the preferred parent node based on the rank value contained in a DIO packet

*rpl-icmp6.c* implements the ICMPv6 functionalities specific to RPL by handling the encoding and decoding of the RPL ICMPv6 control messages. Encoding means constructing the message, i.e. filling in the current types, fields, and payload.

**Building and Compiling-** The source codes of *sensor.c* and *sink.c* scripts in the original Contiki folder (*Normal*) and *attack-1.c*, …, *attack-N.c.* from the cloned folders (*Attack-1*, …, *Attack-N*) are built using their respective *makefile.include*, as shown in Figure 4. The *Makefile.include* is a configuration file that defines hardware-specific settings, compiler options, paths to the libraries, header files and sources directories needed during compilation, and rules that are essential for building the firmware correctly for a specific target device. The compiler then generates a binary firmware image file.

```
1 CONTIKI = ../../..
2 APPS = powertrace collect-view
3 CONTIKI_PROJECT = sensor sink
4 PROJECT_SOURCEFILES += collect-common.c
5
6 ifdef PERIOD
7 CFLAGS+=-DPERIOD=$(PERIOD)
8 endif
9
10 all: $(CONTIKI_PROJECT)
11
12 CONTIKI_WITH_IPV6 = 1
13
14 include $(CONTIKI)/Makefile.include
```

a. Legitimate makefile.include

```
1 CONTIKI = ../../..
2 APPS = powertrace collect-view
3 CONTIKI_PROJECT = dis_flooding
4 PROJECT_SOURCEFILES += collect-common.c
5
6 ifdef PERIOD
7 CFLAGS+=-DPERIOD=$(PERIOD)
8 endif
9
10 all: $(CONTIKI_PROJECT)
11
12 CONTIKI_WITH_IPV6 = 1
13 include $(CONTIKI)/Makefile.include
```

b. Attack makefile.include

**Figure 4.** Snippets of makefile.include files for sensor and sink nodes (a), and a malicious node (b)

**Firmware Flashing**- After a successful compilation, the binary firmware is then flashed or loaded onto the microcontroller(s) of the target node(s). In this case, the *sink.c*, *sensor.c*, and *attack-1.c*, …, *attack-N.c* are flashed onto the microcontrollers of the root node, sensor node(s) and malicious node(s) respectively.

**Data Logging**- The simulation environment is instructed to log key events such as protocol messages, data packets, node behaviour, resource consumptions, etc., during simulation. The proposed framework utilises a sniffing module to log and collect network statistics.

## 4. RESULTS AND DISCUSSION

In this section, a comparison of baseline and DIS flooding attack scenarios is presented to evaluate the effectiveness of the proposed framework. Five LLNs performance metrics are used to demonstrate the presence of a DIS Flooding attack in the RL-based IoT network. The DIS Flooding attack is a resource consumption attack, where a malicious node(s) broadcasts DIS packets to nodes within its transmission range. Upon receipt of DIS packets, nodes drop whatever activity it was processing and transmit a DIO packet to the sender of DIS packets—in our case, the malicious node. Because a large volume of DIS packets is transmitted, this triggers the transmission of DIO and DAO packets.

A comparison of the beacon interval between the two scenarios, shown in Figure 5. During the DIS Flooding attack, it is observed that some motes report a very low beacon interval, demonstrating that these motes are actively transmitting DIO and DAO packets in response to the DIS broadcast packets.

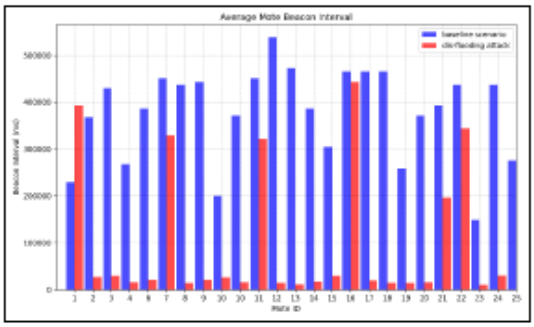

**Figure 5.** Comparison of average beacon interval in milliseconds

Low beacon interval demonstrates that nodes are active and transmitting packets at a very high speed. It is observed that modes under attack reported an average beacon interval of less than 50000ms

The average CPU and power consumption of the attacked motes demonstrate the presence of DIS flooding attacks in the network. As a DIS flooding attack is a resource consumption attack, it is vital to present these metrics as they indicate an ongoing attack. It can be observed, as shown in Figure 6 and Figure 7; that attacked motes consume more power in an attack scenario as compared to a baseline scenario.

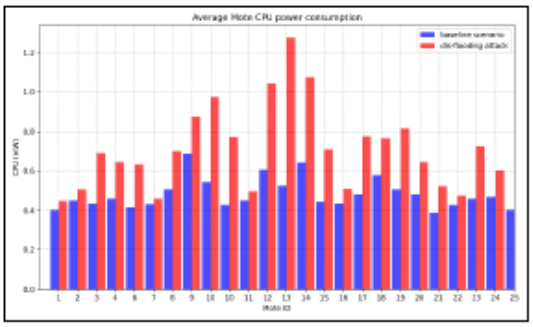


**Figure 6.** Comparison of average mote CPU consumption

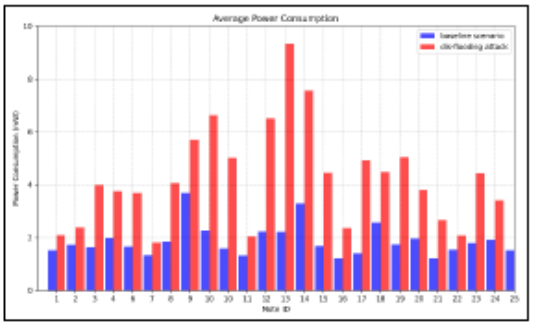


**Figure 7.** Average mote's power consumption

It can be observed that attacked motes consume their processing power (CPU) as they try to process the incoming DIS packets and transmit DIO packets as they respond to the DIS packets, as shown in Figure. 8. On average, baseline and DIS flooding attack scenarios demonstrate CPU consumption of 0.5 mW and 0.75

mW, respectively; attack scenarios consume over 20% more of the total CPU power than the baseline scenario. Further, on average power consumption, these include CPU, LPM, Tx, and Rx; the proposed framework demonstrated its effectiveness in attack implementation, as we see an increase in average power consumption. The presence of the attack can be witnessed as it consumes, on average, 7.6 mW, and the baseline scenario consumes only 3.2 mW; that is, the attack consumes 4.5 mW more average power than the baseline scenario.

We furthermore observed that the presence of the attack also affects packet delivery ratio and end-to-end delay, as exhibited respectively, as shown in Figure 8 and Figure 9.

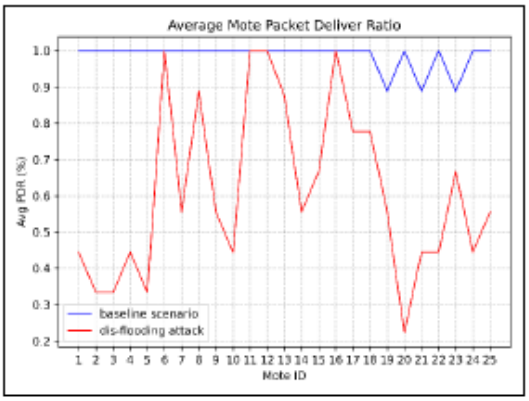


**Figure 8.** Average Packet Delivery Ratio (PDR)

The implemented DIS flooding attack demonstrates a drop in packet delivery ratio as low as 25% for mote 20. This is because attacked nodes drop any activity when they receive DIS packets, which include data packets of the deployed environment. We observed a 30% decrease in PDR in the presence of the attack. It can be seen that the attack also increases end-to-end delay, as shown in Figure. 9.

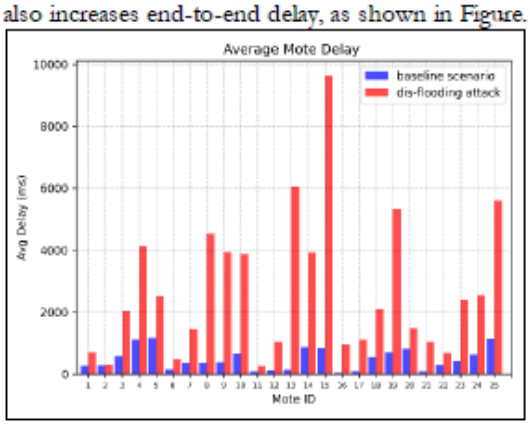

**Figure 9.** Average End-to-End Delay

Node 15 suffers a great delay as the attack scenario recorded a delay of over 9000 ms as compared to the baseline scenario that recorded a delay of just less than 1000 ms.

The proposed framework demonstrates its effectiveness in implementing and launching attacks in RPL-based network simulations. It is observed that the attack was successfully implemented and launched, and the degradation of the network performance subsequently proves the effectiveness of the proposed framework.

## 5. CONCLUSION

This study proposes an adoptable routing attack implementation framework to foster collaboration among researchers in the field of routing attacks in RPL-based IoT and smooth comparison of scenarios from different publications. It was abstracted from literature that researchers in the frilled of routing attacks in RPL-based networks use ad-hoc methodologies to implement routing attacks, which can have a great impact when it comes to comparison of scenarios and experiments, and collaboration amongst researchers. The study painted a vivid picture of the importance of a structured framework for implementing routing attacks to influence the reproducibility of experiments and comparative analysis of attack scenarios, and subsequently, comparative analysis of proposed detection techniques.

The study proposed a routing attack implementation framework, which demonstrated its effectiveness by yielding network degradation results when the framework was implemented. It is explicitly clear that the performance of the network degrades in terms of PDR, CMO, Delay and beacon interval upon adoption of the proposed framework. Future direction, the authors of this work are going to use the logs collected in this study to generate a network dataset, which can be used to build and propose an intelligent model to detect the routing attack in the RPL-based networks.

## REFERENCES

[1] Ajayy, V., and Ranga, V.: 'Performance analysis of RPL protocol in different nodes positioning using Contiki Cooja', *International Journal of Information Technology*, 2024, 16, (6), pp. 3683-3689

[2] Aydın, B., Aydın, H., Görmüş, S., and Mollahasanoğlu, E.: 'Detection of RPL-based Routing Attacks Using Machine Learning Algorithms', *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi*, 2024, 15, (4), pp. 783-796

[3] Algahtani, F., Tryfonas, T., and Oikonomou, G.: 'A Reference Implemenation for RPL Attacks Using Contiki-NG and COOJA', in Editor (Ed.): '*Book A Reference Implemenation for RPL Attacks Using Contiki-NG and COOJA*' (2021, edn.), pp. 280-286

[4] Giri, A., Hegde, A.S., and Mendhiratta, A.: 'Analyzing the Impact of RPL Routing Attacks on the Smart City Ecosystems', in Editor (Ed.): '*Book Analyzing the Impact of RPL Routing Attacks on the Smart City Ecosystems*' (2023, edn.), pp. 1-6

[5] Nisha, Dhingra, A., and Sindhu, V.: 'A Review of DIS-Flooding Attacks in RPL based IoT Network', in Editor (Ed.): '*Book A Review of DIS-Flooding Attacks in RPL based IoT Network*' (2022, edn.), pp. 1-6

[6] Gupta, H., Bhardwaj, S., and Dave, M.: 'Security Analysis of RPL-Based IoT Networks: Evaluating the Impact of Attacks on Performance Parameters', in Editor (Ed.): '*Book Security Analysis of RPL-Based IoT Networks: Evaluating the Impact of Attacks on Performance Parameters*' (2024, edn.), pp. 1-8

[7] Kiran, U., Maurya, P., and Sharma, H.: 'Investigating Routing Protocol Attacks on Low Power and Lossy IoT Networks', *SN Computer Science*, 2024, 5, (4), pp. 393

[8] Maciejko, p., and Krygier, J.: 'Performance of RPL-based Wireless Sensor Networks Subjected to Selected Attacks', 2025

[9] Ankam, S., and Reddy, D.N.S.: 'A mechanism to detecting flooding attacks in quantum enabled cloud-based lowpower and lossy networks', *Theoretical Computer Science*, 2023, 941, pp. 29-38

[10] Bin, M.L.W., Kamis, N.H., Razak, S.F.A., Yogarayan, S., Yassin, S.M.W.M.S.M.M., and Abdullah, M.F.A.: 'Impact of Sinkhole Attacks on IoT Network Efficiency using Cooja', in Editor (Ed.): '*Book Impact of Sinkhole Attacks on IoT Network Efficiency using Cooja*' (2024, edn.), pp. 401-406

[11] Guo, G.: 'A Lightweight Countermeasure to DIS Attack in RPL Routing Protocol', in Editor (Ed.): '*Book A Lightweight Countermeasure to DIS Attack in RPL Routing Protocol*' (2021, edn.), pp. 0753-0758

[12] Bokka, R., and Sadasivam, T.: 'Simulation-based Analysis of RPL Routing Attacks and Their Impact on IoT Network Performance', *Journal of Electronic Testing*, 2024, 40, (2), pp. 259-273

[13] Bokka, R., and Sadasivam, T.: 'DIS flooding attack Impact on the Performance of RPL Based Internet of Things Networks: Analysis', in Editor (Ed.): '*Book DIS flooding attack Impact on the Performance of RPL Based Internet of Things Networks: Analysis*' (2021, edn.), pp. 1017-1022

[14] Rouissat, M., Alsukayti, I.S., Belkheir, M., Alreshoodi, M., Mokaddem, A., and Ziani, D.: 'A Simple Approach for Mitigating a New Flooding Attack in RPL-Based IoT Networks', *IEEE Access*, 2025, 13, pp. 5342-5358

[15] Rajasekar, V.R., and Rajkumar, S.: 'A Study on Impact of DIS flooding Attack on RPL-based 6LowPAN Network', *Microprocessors and Microsystems*, 2022, 94, pp. 104675

[16] Sejaphala, L.C., Malele, V., and Lugayizi, F.: 'High-Level Defence Model against Routing Attacks on the Internet-of-Things', *Indonesian Journal of Computer Science*, 2024, 13, (1), pp. 669-679

[17] Hkiri, A., Alqurashi, S., Ben Bahri, O., Karmani, M., Faraj, H., and Machhout, M.: 'Performance Evaluation of Mobile RPL-Based IoT Networks under Hello Flood Attack', in Editor (Ed.): '*Book Performance Evaluation of Mobile RPL-Based IoT Networks under Hello Flood Attack*' (2024, edn.), pp.

[18] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M.: 'Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications', *IEEE Communications Surveys & Tutorials*, 2015, 17, (4), pp. 2347-2376

### 4.2.6 Article 6

#### 1. Article publication details

**Title**: A lightweight Intelligent Model against Routing Attacks in IoT-based LLN

Status: Developing

#### 2. Article synthesis

(i) Purpose

This article proposes a lightweight intelligent model to detect DIS-Flooding attacks with a demonstrated high detection accuracy, low false negatives, and less program flash memory utilisation. The latter ensures feasible adoption in resource-constrained IoT devices. Furthermore, the model ensures openness and accessibility to allow ongoing research support in RPL-based IoT studies simulated on Cooja by making the dataset publicly available. Moreover, this article demonstrates the practical implications of the adoption of machine learning models as a defence mechanism in IoT networks.

(ii) Methods

For this article, a quantitative methodological choice was adopted for data generation and collection following an experimental strategy and deductive research approach. Cooja ContikiOS was utilised for the simulation of two network scenarios, where each scenario was simulated three times in each of two selected network topologies (random and linear). Additionally, Visual Studio was utilised to preprocess datasets and simulate selected machine learning models in terms of training, testing and validating the optimised model. Lastly, data was collected from the performance metrics of the models, that is, MCC, recall, false negatives, and program flash memory utilisation.

(iii) Results and Discussion/Findings

The findings of this article demonstrate that a decision tree is a suitable lightweight intelligent model to detect DIS-Flooding attacks, achieving a 4.17KB of program flash memory model utilisation, 3.79% of false negatives, and 98.21% of Matthews

Correlation Coefficient. It satisfies the predefined threshold values defined in the methodology of this article. Though models like support vector machine and multi-layer perceptron achieved higher MCC, precision and accuracy, they score the same percentage of 99.14% recall, which defines the specificity of the model. However, the decision tree's performance, grounded in the combination of the chosen performance metrics, meets the criteria.

(iv) Conclusion

This article proposes a decision tree as a lightweight intelligent model against routing attacks. It further establishes the practical implications of the adoption of a decision tree algorithm as a lightweight and intelligent model to defend IoT LLNs against routing attacks.

## 3. Full article

# A lightweight Intelligent Model Against Routing Attacks in IoT-based LLN

*Abstract*—**Low-power and Lossy Networks (LLNs) play a significant role in IoT applications running on resource-constrained devices—devices with limited program flash memory, computing capability, and battery life. To route traffic data of the IoT applications, LLNs utilize RPL, the de facto routing protocol that is designed to create and maintain routes for data transmission efficiently. LLNs are widely used in a wide range of IoT applications, including environmental monitoring, agriculture, surveillance, waste management, etc. However, the rapid growth of IoT networks has also attracted a significant number of routing attacks, like DIS-Flooding attacks, that exploit vulnerabilities of RPL. DIS-Flooding attack is a form of Denial-of-Service attack that exploits the RPL mechanism and floods the network with DIS packets with the aim to deplete network resources, render some channels and nodes unavailable, and furthermore, disrupt operations of the network, which could lead to catastrophic situations in some extreme cases. This study proposes a lightweight intelligent model against DIS-Flooding attacks in LLNs. Using a simulation-generated dataset, the study evaluated the performance of six machine learning algorithms based on detection accuracy, false negatives, and program flash memory. The findings of the study demonstrated that the decision tree achieved a detection accuracy of 99.18% and a false negative rate of 3.79% with a 4.17KB program flash memory (ROM) requirement.**

***Keywords—IoT, flooding attack, intelligent model, LLNs, RPL***

## I. INTRODUCTION

The proliferation of IoT applications has found a diverse adoption in different sectors, from military surveillance, environmental monitoring, including agriculture and industrial, to healthcare and transportation[1]. Most IoT monitoring applications are implemented on smart devices with limited processing capability, limited program flash memory, and battery life. These smart devices use Low-power and Lossy Networks (LLNs), a network for resource-constrained devices to communicate amongst themselves and transmit their monitoring data on a hop-to-hop basis to the base station (sink node) [2]. However, such communication of IoT devices requires a routing protocol specially designed for resource-constrained devices. A working Group for the Routing Protocol of Low-power and Lossy Networks (ROLL), the International Engineering Task Force (IETF) designed and developed a Routing Protocol for Low-power and Lossy Networks (RPL), the de facto routing protocol for LLNs [3].

RPL is a distance vector routing protocol that facilitates routing and node interaction in a mesh topology with the aim to meet the requirements of the LLN [4]. Moreover, the protocol provides an efficient routing solution tailored to LLNs to address the LLNs' resource-constrained nature [5]. However, it was designed primarily to optimize the performance of LLNs without prioritizing security requirements [6]. The protocol builds a Destination-Oriented Direct Acyclic Graph (DODAG), a hierarchical tree-like topology that comprises a single destination (sink/ root node), leaves (child and parent nodes). RPL uses four ICMPv6 packets (DIS, DIO, DAO, DAO-ACK) to create and maintain a DODAG for dynamic parent selection and ultimately optimal route selection [7]:

- DODAG Information Solicitation (DIS) packet – used by nodes to solicit DODAG information and to join the network, or by node(s) already in the network that need to change their parent. The DIS packet can be broadcast in the node's transmission range. Any node receiving the broadcast DIS packet stops any process it was executing, resets its trickle time, and unicasts a DODAG Information Object (DIO) packet to the DIS sender [8].
- DODAG Information Object (DIO) packet – a unicast or multicast packet from a parent node to a child node with DODAG configurations including DODAG version number, RPLInstance, routing metric to calculate rank value, and parent node's rank metric.
- DODAG Object Advertisement (DAO) – is a unicast packet sent by the child node to the selected parent.
- DAO-Acknowledgement (DAO-ACK)- Upon receiving a DAO, the parent node then unicast a DAO-ACK.

Attacks on IoT networks are escalating rapidly due to the widespread use of LLNs in different sectors [6]. The design vulnerabilities of RPL make it susceptible to a range of sophisticated routing attacks that can exploit network security and performance [4]. Though RPL has security modes for

control messages, attacks that interrupt routing paths and drain resources can still be launched [5]. As such, there is minimum security mechanism in the RPL protocol for routing attacks [9].

Routing attacks are network functionality disruptors that aim to deplete network resources, affect data packet delivery, introduce delays, and interfere with normal operations of the network. An example of such an attack is the Distributed Denial of Service attacks exploiting the DIS packet mechanism to flood nodes with DIS packets intended to deplete network resources, disrupt communication between nodes and deem other nodes unavailable [1]. DIS-flooding attacks degrade network performance by consuming battery power of the network, additionally, rendering devices unavailable, decreasing packet delivery ratio, and subsequently increasing end-to-end delay and control message overhead.

Detection techniques have been proposed in the literature to try to defend the LLNs against routing attacks, as suggested in these comprehensive reviews [10, 11]. Different techniques, from secure-protocol, Intrusion Detection Systems (IDS) to AI-based, have been proposed, tested and evaluated, with strengths and weaknesses highlighted in the work [12, 13]

Traditional techniques for protecting IoT are no longer effective because of emerging vulnerabilities in the LLNs [5]. IDS demonstrates its ability to detect routing attacks using techniques like signature-based, anomaly-based, specification-based and hybrid-based. However, these techniques have limitations [6]. However, each one of them has its own challenges; signature-based, it depends on a database or patterns found in earlier attacks discovered. However, this database must be updated regularly. Anomaly-based: system behaviour is observed for a certain time, and a profile that includes all system operations is created. Hybrid: combines both techniques[14].

Recent advancements in machine learning (ML) provide a promising alternative for adaptive, data-driven attack detection systems. ML detection mechanisms leverage network data to autonomously distinguish between normal and abnormal network operations, demonstrate a higher detection rate, and provide adequate adaptability and generalization over traditional mechanisms [4].

To accurately detect DIS-Flooding attacks with low false negatives, this study proposed a decision tree-based lightweight intelligent defense model against DIS-Flooding attacks for IoT monitoring applications running on LLNs, with a demonstration of efficacy on the program flash memory of the nodes. The main contributions of this work are as follows:

- A program flash memory was introduced as a new evaluation metric for ML, intended for resource-constrained devices
- Dataset derived from simulation network operation, packets, sent time, received time, inter-packet time, beacon, interval, cpu, tx, rx, to name a few.
- Decision tree, as a lightweight yet powerful classification algorithm, was adjusted to optimise its performance.
- Dataset. By ensuring openness and accessibility, our dataset ensures long-term availability and ongoing support for research. It can be accessed from the following link. https://github.com/lankachris/RPL_Attack_Dataset

This paper is organized as follows: Section I provides literature and related work on intelligent models, Methodology is discussed in Section III, which explains details of the methods adopted to conduct the study, Section IV shows the performance results with detailed discussion, and lastly, the conclusion is in Section V, which reflects on the findings, and points at a future research direction.

## II. LITERATURE REVIEW

### A. *Supervised machine learning algorithms*

#### *1) Decision tree*

Decision Tree (DT) is a classic supervised learning model that utilises a tree-like graph to represent a flow-chart-like structure for making decisions. The algorithm has proven to be a highly successful general-purpose method for both classification and Io features. Decision trees are considered interpretable due to their straightforward, easy-to-understand computation process. The construction of a decision tree typically involves two conceptual phases: growing and pruning. The learning process commonly uses recursive partitioning, where a dataset is repeatedly split based on selected tests until no further partitioning is needed or possible.

#### *2) Random forest*

Random Forest (RF) is a powerful machine learning algorithm which has become a standard data analysis tool in various fields, including anomaly detection. It operates as an ensemble learning method that combines the output of multiple random decision trees to arrive at a single, more robust result [6]. Each tree in a Random Forest is built from a random sample of the training data with replacement (bootstrap aggregating or bagging), and during the tree construction, only a random subset of features is considered for each split. Furthermore, the final prediction is typically determined by averaging the predictions of individual trees for regression or by a majority vote for classification. Additionally, this ensemble approach enhances predictive accuracy and helps mitigate overfitting, a common issue with individual decision trees. Random Forests are known for their simplicity, effectiveness, and ability to handle high-dimensional data, making them popular in both industry and academia [15].

#### *3) Support Vector Machine*

Support Vector Machine (SVM) is primarily used for classification, regression, and outlier detection problems [15]. Rooted in statistical learning theory, SVM aims to find an optimal hyperplane that best separates different classes in a high-dimensional feature space. it is worth noting that the core principle involves maximising the margin, which is the distance between the hyperplane and the closest data points (support vectors) from each class. SVM can effectively handle both linear and non-linear classification tasks by employing the "kernel trick," which implicitly maps input data into higher-dimensional spaces where a linear separation might be possible [16] .SVM

has been widely adopted in various fields due to its strong mathematical foundation and excellent performance.

*4) K-Nearest Neighbor*

K-Nearest Neighbor (KNN) is a non-parametric, supervised learning classifier used for both classification and regression tasks [15]. When classifying a new data point, KNN identifies the 'K' closest data points (neighbors) in the training dataset based on a distance metric, such as Euclidean distance. The class of the new data point is then determined by the majority class among its 'K' nearest neighbors. Furthermore, KNN is considered a "lazy learning" algorithm because it does not build a generalised model during the training phase but rather stores the entire training dataset and performs computations only when a prediction is requested [17]. The performance of KNN is significantly influenced by the choice of 'K' and the distance metric used.

*5) Multi-Layer Perceptron*

A Multi-Layer Perceptron (MLP) is a type of artificial neural network composed of multiple layers: an input layer, one or more hidden layers, and an output layer. Inspired by the structure and function of biological neural networks, MLPs are designed to receive, process, and transmit data [1].It is a feedforward neural network, meaning that information flows in only one direction, from the input layer through the hidden layers to the output layer [1]. MLPs are capable of learning relationships between both linear and non-linear data and are known as good non-linear approximators. The most common training algorithm for MLPs is backpropagation, which involves adjusting the connection weights between neurons to minimise the difference between the network's output and the desired output. MLPs are widely used for tasks such as pattern classification and function regression.

*6) Naïve Bayes*

Naïve Bayes (NB) is a probabilistic classification algorithm based on Bayes' theorem, which makes a "naive" assumption of independence between features given the class. Despite this strong independence assumption, which is often not met in real-world data, Naïve Bayes classifiers have demonstrated remarkable effectiveness and efficiency in various applications. It is a generative learning algorithm that models the distribution of inputs for a given class[15]. The algorithm calculates the probability of a given data point belonging to a particular class based on the probabilities of its features. The algorithm is distinguished by its computational speed and efficiency in prediction operations. It is particularly well-suited for tasks like text categorisation, spam filtering, and sentiment analysis.

*B. Related work*

Several recent works have made significant efforts to enhance the security of LLNs against various routing attacks. They further demonstrated the feasibility of adopting machine learning models for higher accuracy and precision in routing attack detection while minimising false alarms[13].

A study evaluated the performance of five models using a Cooja simulation-generated dataset [4]. The study compared the performance of KNN, Naïve Bayes, Logistic Regression, Decision Tree, and Random Forest to detect three routing attacks (blackhole, flooding, and version number attacks). The study proposes random forest as the best-performing model, achieving an accuracy of 89.99%.

The study [9] employed a deep learning-based Gated Recurrent Unit model to distinguish between normal and abnormal network behaviour on RPL. The model is trained on a simulated dataset generated using NetSim with 20 nodes and achieved an accuracy of 95%, 94% precision, 81% recall, and 87% F1-score.

Demonstrating the applicability of deep learning models, the study [5] proposed GRU and LTSM to detect five routing attacks in RPL. The models were trained and tested on the Cooja simulation-generated dataset of 10845 data samples of the five attacks. The models achieved 90% and 95% accuracy, respectively. The findings prove that the suggested technique performs well in identifying multiple threats but faces challenges in a resource-constrained environment.

Authors of the study in [6] evaluated four machine learning models on a ROUT-4-2023 dataset. The study demonstrated that random forest achieved 99% accuracy while KNN achieved 98%. A multiclass dataset comprising 16 features and 1639975 instances representing three attacks and normal network traffic classes. Contrary to our study, the study did not present the false negative results and memory requirements of the model. The study [1] utilised the same dataset as [6] to train and test random forest, decision tree and bagging models to detect blackhole, version number, flooding, and decreased rank attacks. Using 5-fold cross-validation iterations, the decision tree achieved 99% accuracy.

Using the WEKA feature selection tool for optimal model performance, a study in [7] utilised the Cooja simulated dataset to train and evaluate the performance of SVM, Decision Tree, ensembled learning, and Naïve Bayes models. The results suggest ensembled learning demonstrates higher detection accuracy of 988% while the decision tree and Naïve Bayes achieved 94% accuracy; furthermore, SMV is the lowest performer, achieving 95% accuracy.

The study [18]proposes an ensemble learning model to detect various routing attacks. The study integrates random forest, decision tree, and extra trees algorithms to build an ensembled model. Authors of the study further compared their proposed model against some models proposed in the literature using the IRAD dataset. Their proposed model demonstrated that it is effective in detecting the routing attack in question by achieving 99% accuracy, precision, and recall. Nevertheless, the model demonstrates high recall; the study lacks the memory requirements of the model.

TABLE I. SUMMARY OF RELATED WORK

| REF | MODELS | ATTACKS | DATASET | FEATURES | MOTE | N SIZE | MODEL SIZE |
|---|---|---|---|---|---|---|---|
| [4]. | 4 | 3 | simulation | 24 | Z1 | 11 | NA |
| [9] | 1 | 6 | Simulation | 21 | Netsim motes | 20 | NA |
| [5] | 2 | 5 | Simulation | NA | Cooja | NA | NA |
| [1] | 3 | 4 | ROUT-4-2023 | 16 | NA | NA | NA |
| [7] | 4 | 3 | Simulation | NA | NA | 24 | NA |
| [18] | 3 | 3 | IRAD | 18 | NA | NA | NA |

Existing works demonstrate the power of machine learning and deep learning models in accurately detecting various routing attacks in LLNs. However, most of these studies neglect the size of the model as a contributing factor for the selection of the best-performing model for LLN microcontrollers with limited program flash memory

## III. METHODOLOGY

While the ideal approach for data collection involves gathering from real-world IoT network devices, which entails technical complexity and cost, we find it feasible to adopt a simulation-based methodology to create an RPL-based IoT network and collect simulation data from it. To ensure the relevance of our simulation, we calibrated the simulation parameters based on empirical data and theoretical models that closely resemble those found in actual IoT networks. The ability to simulate an IoT network scenario and maintain high fidelity to real-world conditions enables the creation of effective and applicable datasets for research and development purposes in the field of RPL security and performance.

### *A. 3.1 Simulation setup*

This paper utilizes the Cooja Contiki simulation tool, which furnishes nodes with identical CPU and memory configurations as real IT devices, facilitating the extraction of simulated network messages.

The simulation network comprised 25 sensors, 1 sink, and 2 sniffer Sky Tmotes as depicted in Fig. 1.

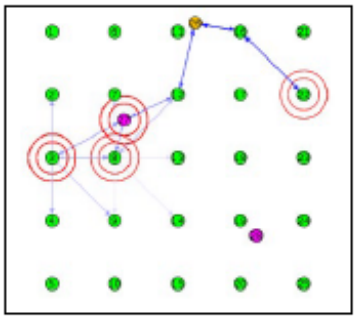

Fig. 1. Simulation environment of 25 sensors, a sink and 2 sniffer nodes

Attack intensity increases from 1 to 3, then 5 dis-flooding attacking nodes. Furthermore, two (2) different Cooja default topologies were simulated ( linear and random); each topology consists of three (3) 10-minute simulations for the baseline scenario and three (3) 10-minute simulations for the attack scenario. That is, two hours of simulation runtime excluding simulation preparations and finalization. The simulation parameters are stated in Table II.

TABLE II. SIMULATION PARAMETERS

| PARAMETERS | VALUES |
|---|---|
| No. of simulations | 12 |
| Simulation tool | Cooja Contiki3.X |
| Area | 100m X 100m |
| Simulation time | 10 minutes |
| Mote type | Sky Tmote |
| Mote ROM&RAM | 48Kb & 10Kb |
| Radio Medium | UDGM |
| Transmission range | 50 M |
| Data packet size | 127 Bytes |
| IEEE standard | Contiki MAC 801.15.4 |

### *B. Dataset*

Datasets containing both categorical and numerical features were extracted from network logs. The dataset comprises data traffic logs, mote operation time, protocol-level metrics, and power consumption. Two datasets were derived from the two scenarios, that is, baseline.csv with 1476 instances and disflooding.csv representing the minority class with 1164. These two datasets are then concatenated to form one binary class dataset with 2640 data points or entries and 24 features.

### *C. Data Preprocessing*

Our dataset consists of 2 classes: baseline and DIS-flooding. To ensure the best results of the selected models, we applied several data processing techniques to the dataset. Label encoding was used to convert the target columns' names to numerical binary values. The number of normal traffic is 12% more than that of the DIS-flooding attack data points, which declares the dataset imbalance.

- *Feature engineering* is the process of extracting relevant information from existing data. This step is critical as the characterization ability of the feature set directly influences the accuracy and generalization of the detection algorithms [19]. Ten (10) relevant features were selected using the SelectBest Python library.
- *Data Scaling:* The selected features underwent scaling using StandardScaler to normalize their ranges, which is crucial for algorithms sensitive to feature magnitudes [20].
- *Resampling:* To ensure a balanced dataset, the Synthetic Minority Over-sampling Technique (SMOTE) was adopted. Its power is observed from its capabilities to generate synthetic data samples for minority classes by

adopting k-nearest neighbors to randomly select data points from each minority class sample and creating synthetic points along the line segments joining these neighbors [21].

*4) Train-Test Split:* The dataset was split between training and test data points, with 70% training and 30% testing using stratified sampling.

*D. 3.3 Model Selection*

Six (6) supervised machine learning algorithms were chosen, backed by literature as the most researched and suited algorithms for LLNs considering their resource-constrained nature. In different studies, each of the selected algorithms demonstrates the ability to detect attacks with high accuracy and low false alarms.

- Decision tree: Is considered interpretable due to its straightforward, easy-to-understand computation process
- Random forest: They are known for their simplicity, effectiveness, and ability to handle high-dimensional data, making them popular
- Support Vector Machine: has been widely adopted in various fields due to its strong mathematical foundation and excellent performance
- Multi-layer Perceptron are widely used for tasks such as pattern classification and function regression
- K-Nearest Neighbor is significantly influenced by the choice of 'K' and the distance metric used
- Naïve Bayes is distinguished by its computational speed and efficiency in prediction operations. It is particularly well-suited for tasks like text categorization, spam filtering, and sentiment analysis

*E. Evaluation Metrics*

The algorithms were assessed against the following performance metrics: accuracy, precision, recall, F1-score, Area Under the Receiver Operating Characteristic (AUC-ROC), Area Under the Precision-Recall Curve (AUC-PR), Matthews Correlation Coefficient (MCC), False Negative Rate, False Positive Rate, and memory requirements for resource-constrained devices to evaluate their effectiveness in detecting Dis-flooding attacks.

Accuracy: represents the proportion of correctly classified instances out of the total instances [22] given in (1).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

Precision: is the ratio of correctly predicted positive observations to the total predicted positive observations [22] in (2).

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

Recall: measures the proportion of actual positive instances that were correctly identified [23] in (3).

$$Recall = \frac{TP}{TP+FP} \quad (3)$$

F1-Score: is the harmonic mean of precision and recall, providing a single metric that balances both precision and recall [23] in (4)

$$F1\text{-}Score = 2*\frac{Precision*Recall}{Precision+Recall} \quad (4)$$

Matthews Correlation Coefficient (MCC): is a measure of the quality of binary classifications that considers true and false positives and negatives, providing a balanced measure even if the classes are of very different sizes [21] in (5)

$$MCC = \frac{TP*TN-FP*FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \quad (5)$$

*F. Model selection*

Memory requirements of the model play a crucial role in determining the best model for LLNs devices with constrained resources, especially memory, processing, and power. Guided by the literature, the best model was selected based on the satisfaction of the following thresholds:

- Detection accuracy over 95%
- False negative below 10%
- Memory Requirements below 15KB

Memory requirement is a crucial metric for evaluating the feasibility of deploying models on resource-constrained LLN devices

*G. Decision tree defense model*

A Decision Tree is a non-parametric supervised machine learning model utilized for classification and regression applications. It consistently divides the data based on a particular attribute. It derives decision rules from the data properties. Utilizing those rules, it forecasts the value of the target variable

The decision-making process of this paradigm can be represented as a tree, facilitating user interpretation. Decision nodes and leaves are the core components of decision trees. In the decision node, data is partitioned according to a specific parameter, while the leaves yield the outcomes or decisions[22].

*1) Modelling*

In this experimental work, the splitting criterion employed was Gini, which quantifies the impurity of the split. It reveals how well a split divides the total samples of binary classes in a specific node $t$. Mathematically, it can be expressed as in (6)

$$Gini(t) = 1 - \sum_{i=1}^{k} p_i^2 \quad (6)$$

Where, $t$ is the node, $k$ is the number of possible classes, and $i$ represents the class.

$p_i^2$ proportion of samples belonging to the class $i$ in node $t$

Then the prediction for the input $x$ can be expressed as in (7)

$$\hat{y}(x) = \arg\max_{i \in c} p(i|x \in leaf) \quad (7)$$

Where, $c$represents a class, either baseline or DIS-Flooding. $C$ is a set of classes $\{baseline, DIS\text{-}Flooding\}$

$p(i|x \in leaf)$ the probability of the class $i$ given that $x$ ends up in that leaf node, arg $max$ chooses the class with the maximum probability

*2) Hyperparameter tuning*

To optimize the decision tree classifier for distinguishing baseline RPL traffic from DIS flooding attacks in low-power and lossy networks (LLNs), we performed hyperparameter tuning using grid search with 5-fold cross-validation on the training dataset. The search focused on key parameters to balance model complexity and generalization: max_depth (explored values: 5, 10, 15, None) and min_samples_split (explored values: 2, 5, 10). The Gini impurity criterion was fixed, as it provided efficient splits aligned with the binary classification task. The optimal configuration, yielding the highest Matthews Correlation Coefficient (MCC) of 0.98 on validation data, was max_depth=10 and min_samples_split=5. This setup resulted in a tree with moderate depth to capture subtle attack patterns without overfitting to noise in simulated traffic traces.

## IV. Results and Discussion

As it is stated in Section I, this paper is aimed at proposing an intelligent defense model to act against resource-consuming routing attacks known as DIS-flooding attacks. As such, the paper trained and tested six supervised machine learning algorithms on the dataset generated from simulations. This section presents the results of the performance of the models and provides a cross-cutting findings discussion.

### A. Results

The four models were evaluated in terms of accuracy, precision, F1-score, and false positives. These performance metrics are categorised as baseline performance metrics, as they do not really present the robustness of the models; however, they present the ability of the model to correctly classify the unseen data.

*1) Detection Ability*

Depicted in Fig. 1 is the models' performance comparison in terms of baseline metrics.

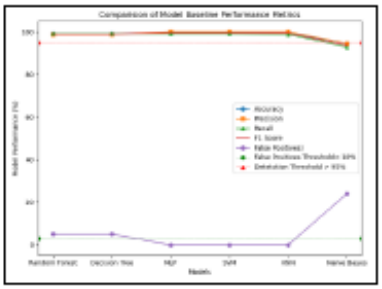

Fig. 2. Detection accuracy of the models and false positive performance

With the defined threshold of 95% detection, Naïve Bayes appears to fall below the threshold by achieving 94% accuracy and precision, 93% F1-Score, and high false positives above the threshold of 10%. In contrast, other models have their detection ability above the threshold, with specific emphasis on SVM, KNN, and MLP achieving 99% accuracy and F1-Score, 100% precision, and zero (0) false positives; and random forest and decision tree, though they demonstrate the ability to correctly classify the binary labels with performance over the threshold, moreover, they seem to lack in terms of false alarms were both models achieved 5% false positive which is above threshold of 3%.

Fig. 2 displays the confusion matrix demonstrating the total number of correctly and incorrectly classified baseline entries, and correctly and incorrectly classified attack entries. The results demonstrate the continuing high performance of SVM, KNN and MLP, and random forest and decision tree being the second performing models class, then Naïve Bayes being the worst performing out of all six models.

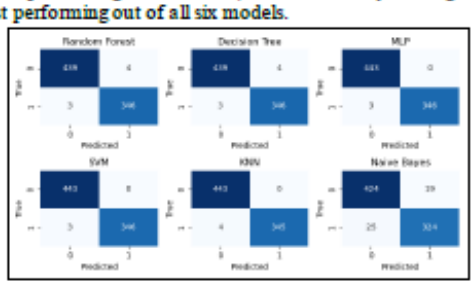


Fig. 3. Confusion matrix

*2) The Area Under the Curve (AUC)*

Curves are useful especially in a general classification problem like anomaly detection, spam detection or performance detection. This subsection presents the Area Under the Curve of the Receiver Operating Characteristic Curve (AUC-RCO) and Precision-Recall Curve (AUC-PRC), demonstrating the performance of the models across all possible thresholds, and the trade-off between precision and recall, respectively.

Fig. 3 depicts an AUC-ROC curve of the models. The curves indicate the best five performing models (SVM, MLP, KNN, random forest, and decision tree) still demonstrate their effectiveness in detecting Dis-flooding attack with a value of 99% while Naïve Bayes achieved 98%.

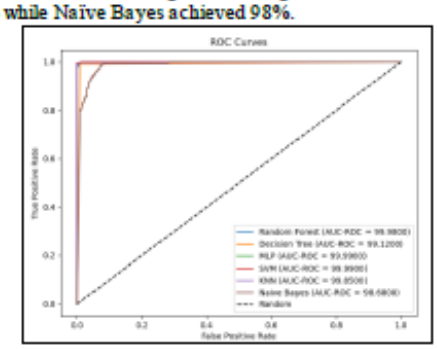


Fig. 4. AUC ROC curves

While Fig. 4 demonstrates the trade-off between precision and recall, that is, as precision increases, recall decreases and vice versa. However, the best five models achieved a performance of 99% each for AUC-PRC and Naïve Bayes, achieving 98%.

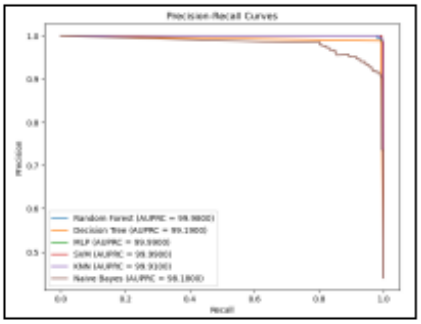


Fig. 5. AUC PRC curves

The AUC value of 99% demonstrates that the models can differentiate the Dis-flooding attacks class from the normal network operations class by almost 100%. This is a clear indication of the effectiveness of machine learning models in IoT for security and performance, leveraging the network traffic data and logs generated by IoT networks.

*3) Results of Robust Performance*

Fig. 4 demonstrates the robustness of the models to correctly classify almost all instances, with an excellent balance between sensitivity and specificity. The results show that the models are almost perfect, with few errors across all categories of the confusion matrix, that is, high TP and TN, and low FP and FN. SVM and MLP obtained 99%, random forest, decision tree, and KNN achieved 98% and Naïve Bayes achieved 88%, which suggests that Naïve Bayes is the worst performer compared to the other five models with different challenges.

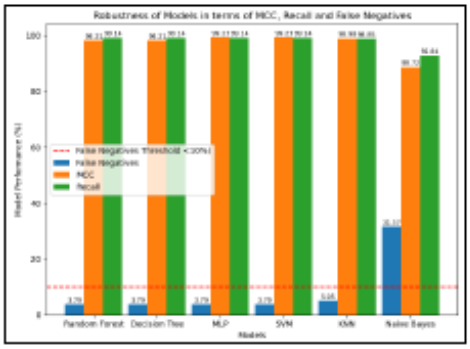


Fig. 6. MCC, Recall and false negative

In contrast, the performance of SVM and MLP appears to have the same false negative value of 3% as the random forest and decision tree, while KNN reported a value of 5% and Naïve Bayes reported 31% false negatives.

In the quest for the adoption of intelligent models for LLNs' security and performance, it is worth noting the storage implications of the model on resource-constrained IoT devices with limited ROM and RAM on their microcontrollers. For that reason, model size is also used as part of the selection criteria, with more value as models appear to perform well in other performance metrics. Moreover, models can be tuned over time and against until desirable results are obtained. However, model size plays a significant role in the context and embedded deployment. Fig. 6 presents the model file size in Kilobytes (KB).

Naïve Bayes classification models are so simple that their size is 1.32Kb compared to KNN, with a size of 307Kb. KNN can be memory-intensive if the entire training dataset needs to be stored for prediction, which might be a limitation for very large datasets on resource-constrained devices.

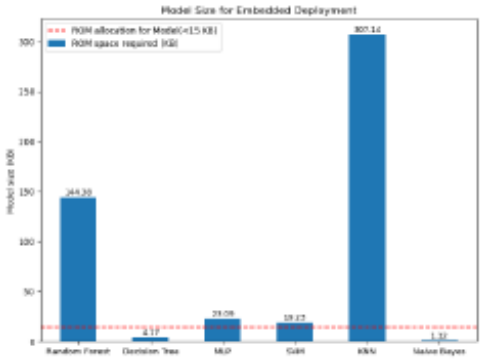


Fig. 7. Program flash memory requirements

The random forest classifier with 50 trees has the second largest space requirement of 144Kb. While SVM and MLP models' memory space requirements (19.23 and 23.09, respectively) are just above the threshold. Additionally, the decision tree taking up less than 50% of the available ROM is remarkable.

TABLE III SHOWS THE PERFORMANCE SUMMARY OF THE MODELS.

| Model | Acc | Prec | Recall | F1- | ROC | PRC | MCC | FN | ROM |
|---|---|---|---|---|---|---|---|---|---|
| RF | 99.12 | 98.86 | 99.14 | 99 | 99.98 | 99.98 | 98.21 | 3.79 | 144.38 |
| MLP | 99.62 | 100 | 99.14 | 99.57 | 99.99 | 99.99 | 99.23 | 3.79 | 23.09 |
| SVM | 99.62 | 100 | 99.14 | 99.57 | 99.99 | 99.99 | 99.23 | 3.79 | 19.23 |
| KNN | 99.49 | 100 | 98.85 | 99.42 | 99.85 | 99.91 | 98.98 | 5.05 | 307.14 |
| NB | 94.44 | 94.46 | 92.84 | 93.64 | 98.68 | 98.18 | 88.72 | 31.57 | 1.32 |
| DT | 99.12 | 98.86 | 99.14 | 99 | 99.12 | 9.19 | 98.21 | 3.79 | 4.17 |

### B. Discussion

A lightweight and effective intelligent defense mechanism in detecting anomalies in the LLNs for IoT applications is as important as the applications running on the LLNs, to ensure the availability, reliability and potentially to gain insight into the network performance. The accurate detection of potential threats and resource-efficient (particularly, required memory size for model deployment into resource-constrained devices) are the key indicators of the best performing model to defend the LLNs with close to zero false negatives. Both SVM and MPL demonstrated a high precision percentage of 100% and 0% false positives, indicating their superiority over the decision tree and random forest, with 98% and 5% false positives, which still fall within the FP and FN thresholds. The robustness of SVM and MLP is observed on the Matthews Correlation Coefficient (MCC), both achieving 99.23% while random forest and decision tree achieved 98.21%. However, decision trees and Naïve Bayes appear to have very low ROM memory requirements for LLN devices: 4.17Kb and 1.32Kb, respectively. Naive Bayes models are generally considered lightweight in terms of memory, as they primarily store probability distributions.

Based on the performance of the models in terms of MCC, false negatives and resource efficiency, particularly memory efficiency of the models, decision trees appear to be a suitable fit to be integrated into the lightweight intelligent defense model for the resource-constrained IoT devices using LLNs for communications, ensuring effective attack detection and low memory utilisation on already constrained devices for security and performance optimisation. The decision trees insist on low memory requirements and detection accuracy well above the threshold of 95% and with fewer and the same false negatives as SVM and MLP of about 3%. Additionally, it demonstrates that it requires 79.42% and 81.9% less memory compared to SVM and MLP, respectively. As such, this study proposes decision trees as the intelligent defense model against Dis-flooding attacks; given its lightweight nature and less complexity, the decision tree is the best model. It promises effectiveness, efficiency and robustness in detecting routing attacks and network anomalies for performance optimisation.

## V. Conclusion

The aim of the paper is to propose a lightweight and effective intelligent defense model to act against Dis-flooding attacks, a type of Distributed Denial of Service attack targeting vulnerabilities of the Routing Protocol for Low Power and Lossy Networks. This study demonstrated that machine learning models, particularly the decision tree, can be effectively used to detect routing attacks in network traffic data, taking into consideration the resource-constrained nature of LLN devices, particularly program flash memory (ROM) utilization.

After comparative analysis of the models in MCC, recall, false negatives and memory requirements, the decision tree was demonstrated to be the best and proposed model that satisfies the aim of the paper. The tuned model achieved superior performance over untuned baselines, with a test MCC of 0.98 and minimal false positives for DIS flooding detection, ensuring lightweight deployment feasibility on resource-constrained nodes like Tmote Sky.

Future Work of this paper is to look into the IoT Testbeds for network simulation and collection of datasets that are close to real-world, and evaluate the performance of the proposed model even further. Further, extending the dataset to cover more attack types.

## References


[1] Aydın, B., Aydın, H., Gömüş, S., and Mollahasanoğlu, E.: 'Detection of RPL-based Routing Attacks Using Machine Learning Algorithms', Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi, 2024, 15, (4), pp. 783-796

[2] Goel, S., Verma, A., and Jain, V.K.: 'CRA-RPL: A Novel Lightweight challenge-Response authentication-based technique for securing RPL against dropped DAO attacks', Computers & Security, 2023, 132, pp. 103346

[3] Agiollo, A., Conti, M., Kaliyar, P., Lin, T.N., and Pajola, L.: 'DETONAR: Detection of Routing Attacks in RPL-Based IoT', IEEE Transactions on Network and Service Management, 2021, 18, (2), pp. 1178-1190

[4] Wang, X., Yang, W., Hou, C., and Luo, H.: 'Routing Attack and Detection Methods in the RPL-based Internet of Things', in Editor (Ed.)' (Eds.): 'Book Routing Attack and Detection Methods in the RPL-based Internet of Things' (2024, edn.), pp. 127-130

[5] Alanazi, S.G., Alsirhani, A., and Alanazi, N.S.: 'IoT Network Security Framework to Classify RPL Attacks Using Deep Learning Algorithms', in Editor (Ed.)' (Eds.): 'Book IoT Network Security Framework to Classify RPL Attacks Using Deep Learning Algorithms' (2025, edn.), pp. 276-282

[6] Mosa, H., Saleh, A., and Alkasassbeh, M.: 'RPL Routing Attacks Detection for IoT Networks Using Machine Learning', in Editor (Ed.)' (Eds.): 'Book RPL Routing Attacks Detection for IoT Networks Using Machine Learning' (2024, edn.), pp. 169-175

[7] Rabhi, S., Abbes, T., and Zarai, F.: 'IoT Routing Attacks Detection Using Machine Learning Algorithms', Wireless Personal Communications, 2023, 128, (3), pp. 1839-1857

[8] Raman, R., Mandaloju, B., Singh, D., Tripathi, V., Maginmani, U.H., and Gonzales, J.L.A.: 'An Experimental Study of Sink Hole Attacks and Distributed Denial of Service (DDS) on IoT network based Healthcare Applications', in Editor (Ed.)' (Eds.): 'Book An Experimental Study of Sink Hole Attacks and Distributed Denial of Service (DDS) on IoT network based Healthcare Applications' (2023, edn.), pp. 990-993

[9] Bokka, R., and Sadasivam, T.: 'Securing IoT networks: RPL attack detection with deep learning GRU networks', Int. J. Recent Eng. Sci, 2023, 10, (2), pp. 13-21

[10] Pasikhani, A.M., Clark, J.A., Gope, P., and Alshahrani, A.: 'Intrusion Detection Systems in RPL-Based 6LoWPAN: A Systematic Literature Review', IEEE Sensors Journal, 2021, 21, (11), pp. 12940-12968

[11] Mukhaini, G.A.L., Anbar, M., Manickam, S., Al-Amiedy, T.A., and Momani, A.A.: 'A systematic literature review of recent lightweight detection approaches leveraging machine and deep learning mechanisms in Internet of Things networks', Journal of King Saud University - Computer and Information Sciences, 2024, 36, (1), pp. 101866

[12] Al-Amiedy, T.A., Anbar, M., Belaton, B., Bahashwan, A.A., Hasbullah, I.H., Aladaileh, M.A., and Mukhaini, G.A.L.: 'A systematic literature review on attacks defense mechanisms in RPL-based 6LoWPAN of Internet of Things', Internet of Things, 2023, 22, pp. 100741

[13] Sejaphala, L.C., Malele, V., and Lugayizi, F.: 'A Systematic Literature Review on Defense Techniques Against Routing Attacks in Internet of Things', Latin-American Journal of Computing, 2025, 12, (1), pp. 35 - 49

[14] Zahra, F., Jhanjhi, N.Z., Khan, N.A., Brohi, S.N., Masud, M., and Aljahdali, S.: 'Protocol-Specific and Sensor Network-Inherited Attack Detection in IoT Using Machine Learning', in Editor (Ed.)' (Eds.): 'Book Protocol-Specific and Sensor Network-Inherited Attack Detection in IoT Using Machine Learning' (2022, edn.), pp.

[15] Gill, K.S., Anand, V., and Gupta, R.: 'Website Classification Through Exploratory Data Analysis Using Naive Bayes, Random Forest, and Support Vector Machine Classifier', in Editor (Ed.)' (Eds.): 'Book Website Classification Through Exploratory Data Analysis Using Naive

Bayes, Random Forest, and Support Vector Machine Classifier' (2023, edn.), pp. 1-5

[16] Al-Amiedy, T.A., Anbar, M., Belaton, B., Kabla, A.H., Hasbullah, IH., and Alashhab, Z.R.: 'A Systematic Literature Review on Machine and Deep Learning Approaches for Detecting Attacks in RPL-Based 6LoWPAN of Internet of Things', in Editor (Ed.)^(Eds.): 'Book A Systematic Literature Review on Machine and Deep Learning Approaches for Detecting Attacks in RPL-Based 6LoWPAN of Internet of Things' (2022, edn.), pp.

[17] Kilincer, I.F., Ertam, F., and Sengur, A.: 'Machine learning methods for cyber security intrusion detection: Datasets and comparative study', Computer Networks, 2021, 188, pp. 107840

[18] Abdulkareem, O.A., Kontham, R.K., and Mahmood, F.E.: 'Securing Smart Grids: Machine Learning-Driven Ensemble Intrusion Detection for IoT RPL Networks', International Journal of Safety & Security Engineering, 2024, 14, (5)

[19] Yang, J., Wang, H., and Lu, Y.: 'Web Attack Detection through Network-Traffic-Based Feature Engineering and Machine Learning', in Editor (Ed.)^(Eds.): 'Book Web Attack Detection through Network-Traffic-Based Feature Engineering and Machine Learning' (2020, edn.), pp. 103-108

[20] Zhang, Y., and Wang, Z.: 'Feature Engineering and Model Optimization Based Classification Method for Network Intrusion Detection', in Editor (Ed.)^(Eds.): 'Book Feature Engineering and Model Optimization Based Classification Method for Network Intrusion Detection' (2023, edn.), pp.

[21] Li, M., and Chen, P.: 'A Hybrid Nearest Neighbor Based SMOTE Oversampling Algorithm', Proceedings of the 2023 3rd International Conference on Big Data, Artificial Intelligence and Risk Management, 2023

[22] Wang, Y., Zhang, J., and Zhang, L.: 'Theory of decision tree models in classification problems', in Editor (Ed.)^(Eds.): 'Book Theory of decision tree models in classification problems' (2022, edn.), pp.

[23] Dhahir, Z.S.: 'A Hybrid Approach for Efficient DDoS Detection in Network Traffic Using CBLOF-Based Feature Engineering and XGBoost', Journal of Future Artificial Intelligence and Technologies, 2024

## 4.3 CHAPTER SUMMARY

In conclusion, routing attacks are still an enormous threat in IoT networks, and as such, defending against them is of paramount importance to ensure dependability and effectiveness of the networks. Furthermore, it was established that machine learning algorithms promise accurate detection of DIS-Flooding attacks leveraging network traffic data. This study proposed the decision tree as a lightweight and efficient intelligent security model to defend IoT networks from routing attacks. The next chapter presents the cross-article analysis and synthesis, which includes key findings, contributions and research questions and contributions mapping.

# CHAPTER 5

# CROSS-ARTICLE ANALYSIS AND SYNTHESIS

## 5.1 INTRODUCTION

The research articles developed from this study were detailed in Chapter 4, aimed at achieving the theoretical and empirical research objectives. This chapter provides a cross-article analysis and synthesis across the six articles produced in this study to comprehensively address the defined research problem. Firstly, the chapter integrates key findings across the articles; secondly, it establishes the contributions, and lastly, it presents a coherent mapping of research questions and the articles. In a PhD by article format, this chapter serves a vital function of consolidating the results of each article into a unified body, all contributing to the full study's primary objective.

## 5.2 INTEGRATION OF KEY FINDINGS ACROSS ARTICLES

The findings from the individual articles are integrated in this section to illustrate how this study collectively addressed the overarching aim of developing an efficient intelligent security model to defend IoT networks from routing attacks with a demonstration of high detection accuracy, low false negatives by leveraging network logs. The integration across the six articles confirms a coherent progression in addressing the research problem formulated to achieve the aim of this study, as presented in Figure 5-1.

The review articles of this study confirmed, theoretically, that IoT routing protocols, particularly RPL, are widely adopted in IoT networks with limited resources and are highly prone to various routing attacks, notably DIS-Flooding, sinkhole, and rank attacks as highlighted in related studies such as (Al-Amiedy *et al.*, 2023), (Verma & Ranga, 2020), and (Pasikhani, Clark, Gope*, et al.*, 2021). The articles further highlight that limited studies have addressed the lack of efficient intelligent models in RPL-IoT, as in (Kilincer *et al.*, 2021). The finding provided the empirical basis for exploring the implementation of DIS-flooding attacks and the development of an intelligent model.

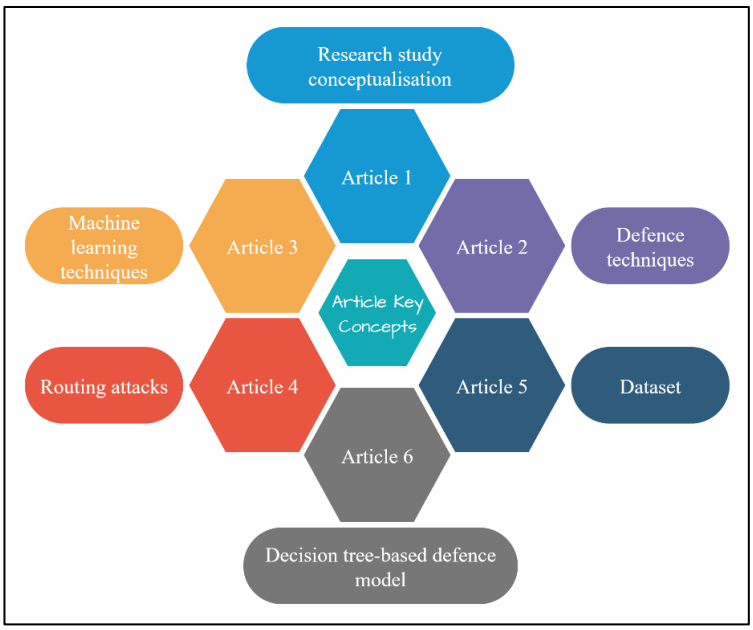


**Figure 5-1:** Key concepts towards the proposed technique

Article 1 of this study highlights that security remains an ongoing challenge in IoT networks, despite various proposed solutions in existing literature. However, limitations are what keep the research gaps open. Furthermore, research studies in “the security techniques for IoT networks” are active and quite prominent in the European and Asian countries, with less footprint in African countries, South Africa in particular. India and the UK demonstrate dominance in proposing defence techniques for IoT networks. It is noted that defence techniques can be categorised into three categories: secure-protocol, IDS, and ML-based, and they demonstrate their effectiveness in detecting routing attacks. However, what sets them apart is their method of detection and footprint in the network resource consumption. Through Article 2, this study highlighted that machine learning techniques, particularly traditional machine learning, have been researched the most since 2021, constituting 64.7% of ML-based techniques. Moreover, the ML-based technique constitutes 44% of the total defence techniques, followed by secure-protocol, with 35% and intrusion detection, constituting 21%. Furthermore, selected publications investigated 124 instances of routing attacks and flooding attacks appeared 22 times, making them the most researched attack, representing 18% followed by the rank attack with 13%.

Flooding attacks are proactive routing attacks that flood the network and victim nodes with a large volume of bogus traffic, impacting data packet delivery, increasing delay and network operational time, and consuming resources of the network and nodes (Koosha *et al.*, 2022). It is noted that flooding attacks have similarities with most disruptive routing attacks, which suggests that learning patterns of flooding attacks for detection could potentially lead to the detection of other routing attacks. However, this would require an intelligent technique that can leverage network data to learn network behaviour in the presence of flooding attacks.

Building on this foundation, Article 3 demonstrated that ML algorithms promise to enhance the detection of routing attacks, but with distinct percentages of detection accuracy and false alarms. By systematically synthesising published studies, the article compared the performance results of different machine learning algorithms. The results suggest that traditional machine learning techniques continue to excel in their integration in the security and performance analysis of IoT networks (also suggested in (Laiby & Subramanya, 2021), with better performance, of course, as compared to advanced ML models with regard to false alarms. This, however, demonstrates the superiority of machine learning techniques in leveraging network data for analysis and further detection of routing attacks.

In Article 5, this study adopted and implemented a framework for the implementation of the routing attacks theoretically presented in Article 4. Subsequently, a DIS-Flooding attack scenario was implemented and its impact on the network performance metrics presented in Articles 2 and 4 was analysed, taking into account power, data transmission success, and network operation time. The study further generated data from network operation and traffic logs, motivated by the findings of Article 3 about a lack of publicly available datasets and the wide use of datasets generated from individual research study simulations and experiments (Sharma *et al.*, 2019; Xu *et al.*, 2023).

Finally, Article 6 aggregates the cumulative findings of previous articles into a unified research study that proposes an intelligent technique, which integrates both high detection accuracy with low false negatives and efficient network resource consumption into a lightweight intelligent model to defend IoT LLNs against RPL routing protocols. The

article establishes that among the models which were compared (SVM, RF, DT, MLP, KNN, and NB), DT emerged as a suitable defence technique for resource-constrained IoT networks. It achieved an accurate detection performance (accuracy, precision, recall, and MCC) of over 95% threshold, with a false alarm of 3.79% which is below a 10% threshold and program flash memory utilisation of 4KB, suggesting its efficiency in terms of node storage utilisation.

The integration across articles of this study is ultimately represented in a thematic model as follows:

- ***Theme 1:*** *Vulnerabilities in IoT networks (Articles 1, 2 & 4)*
- ***Theme 2****: Feasibility of an intelligent detection approach (Article 3)*
- ***Theme 3:*** *Towards an intelligent model for IoT security (Articles 5 & 6)*

The findings further demonstrate a clear development from identifying the research gap to synthesising literature, modelling and simulations, and finally to the implementation and analysis of a lightweight and intelligent detection technique for IoT network security. Table 5-1 summarises these cumulative findings, converging towards the conclusion that robust IoT network security requires effective, intelligent, and resource-aware defence mechanisms.

**Table 5-1:** Cross-article building blocks

| | **Article 1** | **Article 2** | **Article 3** | **Article 4** | **Article 5** | **Article 6** |
|---|---|---|---|---|---|---|
| **Building blocks of this study** | Research gap | Defence techniques | Machine learning techniques | Routing attacks | Validation of the framework | Comparison of models |
| | Research question | Routing attacks | Data sources | Network size and attack intensity | Impact of the attack | Detection model |
| | Simulation setup | Simulations tools | Performance metrics | Network performance analysis metrics | Network logs generation | |

## 5.3 CONTRIBUTIONS OF THE RESEARCH STUDY

The contributions are articulated across theoretical, methodological, and practical dimensions as follows:

### 5.3.1 Theoretical contributions

To propose a resource-efficient intelligent security defence model, the authors of this dissertation deemed it necessary to conduct an ILR on existing literature to gain insight into various defence techniques and routing attacks in LLNs. These serve as the backbone of IoT applications running on resource-constrained devices.

A thorough review of this study has advanced theoretical understanding of routing attacks further, providing a clear understanding of their impact, suitable simulation methods, and attack intensity, and suitable performance metrics, among other factors, which potentially lead to the utilisation of a widely adopted and supported simulation tool to implement and analyse routing attack scenarios. This lays a foundation for contextualisation of routing attacks and points in a clear direction for implementing attack scenarios. This study produced an article whose strength lies in its rich knowledge of understanding routing attacks and commonly used simulation tools, as it is important to select a suitable simulation tool for a research study. It highlights both the RPL scripts for modification to mimic an ongoing attack and performance metrics that can be observed to determine the successful implementation of the DIS-flooding attacks.

This research study conducted an SLR to synthesise thirty-nine research articles that were published between the years 2018 and 2023. The article's findings paint a picture demonstrating that RPL has vulnerabilities that are exploited by routing attacks, as suggested in Al-Amiedy *et al.*, (2023); Mukhaini *et al.*, (2024). Moreover, secure-protocol techniques continue to present detection and mitigation of routing attacks; nevertheless, their feasibility in resource-constrained IoT networks is limited. The study established that there is a rise in the integration of machine learning algorithms as defence models for LLNs. Furthermore, findings established that most proposed machine learning-based techniques only detect attacks by classifying network traffic, without further implementing mitigation mechanisms. This established knowledge presents an open issue in the adoption of machine learning algorithms as defence techniques. It is further verified that

integration of secure-protocol and machine learning techniques could potentially provide a more efficient and robust intelligent security defence model to secure resource-constrained IoT networks. The study provides a clear picture of how defence techniques in IoT networks can be distinguished and visualised by firstly categorising defence techniques into three distinct classes (secure-protocol, conventional IDS, and ML-based IDS techniques), further presenting their adoption and effectiveness, and then their strengths and weaknesses to clarify which defence techniques are suitable for RPL-based IoT networks.

Furthermore, this study adds that the Cooja simulation tool is widely adopted and suitable for the simulation of IoT networks with resource limitations. The model established that flooding attacks are the most destructive and researched routing attacks, and further notes that integration of machine learning and secure-protocol techniques could provide both detection and mitigation capabilities. The study also adds to the knowledge that there are limited publicly available RPL-based IoT networks datasets, further extending that most research studies still utilise simulation tools to collect and generate datasets for training and testing of their machine learning algorithms. The study further argues that supervised machine learning algorithms are mostly integrated for defence due to their lightweight nature and shorter training time, as well as their ability to train on small-scale datasets

### 5.3.2 Methodological contributions

Methodology, as defined by (Goundar, 2012), is a collective term for the structured process of conducting research, encompassing the steps and procedures that guide a study. In the context of this study, methodological contributions extend beyond the adoption of standard approaches; they involve the development and validation of routing attack implementation frameworks and systematic processes to benchmark proposed techniques based on the findings in the literature.

Seventeen (17) articles were systematically collected for review from a pool of machine learning based defence techniques in IoT studies published between 2018 and 2023. The aim was to analyse and results from the selected studies to identify the best-performing machine learning model for adoption as a detection technique for IoT networks against

routing attacks. Models were grouped into two groups: traditional machine learning and advanced ML for comparison. Furthermore, performance metrics (accuracy, precision, recall, F1-score and false negative rate) results were collected for each machine learning model appearing in the selected studies. Averages were calculated for each model and compared between the two groups and within each group to dictate the best-performing algorithm in accordance with the literature. This method of comparing the same models from different studies may be utilised to benchmark the minimum acceptable performance results of ML models in detecting routing attacks.

Part of this study's methodological contributions is in proposing a routing attack implementation framework to model attacks and baseline simulation scenarios. The technique defines five (5) steps to the implementation of both scenarios, that is, repository cloning (clone baseline repository to create an attack repository for modification), code modification (modification of attack repository's core RPL logical scripts to mimic a routing attack), building and compiling (clearing errors script), firmware flashing (involves loading the compiled file onto the flash memory of the microcontroller), and data logging (collection of network operation data or logs when simulations starts). This method ensures a structured, replicable implementation of scenarios, creating a logical platform for collaboration and ease of comparison studies among researchers and practitioners utilising simulation tools for IoT routing attack analysis studies.

### 5.3.3 Practical contributions

This study proposed a lightweight and intelligent model to defend against DIS-flooding attacks on LLNs. The study demonstrates the practical implications of the adoption of the decision tree model as a detection technique for routing attacks in IoT networks. The study first demonstrates that operation and traffic data logs of networks can be leveraged as an enabler to build, train and test machine learning models for adoption as detection techniques. Furthermore, the proposed routing attack implementation as a logical platform for collaboration can be adopted by academics and industry practitioners working in the same research area to ease collaboration on studies.

## 5.4 RESEARCH OBJECTIVE-ARTICLE MATRIX -THE GOLDEN THREAD

This study established five (5) research objectives as building blocks to achieve its aim. Six articles developed from this study were strategically aligned to reach the overarching objective of the study, answer the research question, and ultimately address the need for a lightweight intelligent security model to counter DIS-flooding attacks in RPL-based IoT networks.

Article 1 identifies a research gap and establishes a research question: the robustness and effectiveness of a defence model in detecting routing attacks with minimum false negatives, further demonstrating less network resource consumption. It then proposes a high-level conceptual framework, which contributed towards the implementation and development of the proposed model of this research, tapping into almost all RO, with an emphasis on the simulation parameters and setup and model deployment in RO3 and RO5, as this research study integrates machine learning into the security of LLNs.

Articles 2 and 3 address the foundations and exploration objectives (RO1 and RO2). Article 2, on the other hand, establishes a firm Systematic Literature Review (SLR) and comprehensively synthesises security techniques, including conventional techniques (trust-based, cryptography), conventional IDS (signature-based, specification), and ML-based (traditional ML, DL and RL). Spanning across the five ROs, Article 2 presents the author of the study with a comprehensive, detailed analysis of performance metrics to consider for network and intelligent model evaluation, and placement of the model (node-level, network-level, or hybrid placement)

Article 3 explores published works related to the integration of ML as a security model in LLNs. Extending its impact, it presents an empirical approach, presenting a theoretical comparison of different machine learning algorithms to point the research in the right direction of the best performing model in literature, and which models to include in RO4.

Article 4 directly presents an in-depth review of routing attacks to address RO1. Using the SLR method adopted in articles 2 & 3, this article demonstrates that there is a lack of a standard implementation framework for routing attacks. It further gives a brief overview

of the most used simulation tools, network size and attack intensity to assist this research study in formulating an effective simulation setup, baseline and attack modelling.

Article 5 extends from the findings of Article 4. It designs and validates an implementation framework addressing RO3. The article further synthesises the DIS-Flooding attacks and empirically simulates two scenarios, the first mimicking the presence of DIS-Flooding attacks and the second as a baseline. Empirical simulation presented in the article generated a dataset used to train, test different ML algorithms in RO4 and RO5.

Finally, Article 6 (in the pipeline) consolidates the findings of all preceding articles to propose a lightweight, robust intelligent defence model (RO5). This model integrates detection and efficiency, focusing on accurate detection, minimum false negatives and efficient program flash memory utilisation. The model is grounded in the theoretical, methodological, and empirical insights generated throughout this study.

The articles' contributions to the intelligent model's development and the collective knowledge base are mapped against the research objectives in Table 5-2.

**Table 5-2:** Research Objectives and Articles Mapping

| Research Objectives | Article 1: ILR | Article 2: SRL | Article 3: SRL | Article 4: SRL | Article 5: simulation | Article 6: modelling |
|---|---|---|---|---|---|---|
| **RO1: Review of RPL and routing attacks** | Partial | **Points to the most researched and destructive attacks** | Partial | **In-depth taxonomy of routing attacks** | Synthesis of DIS-Flooding routing attack | Discusses DIS-Flooding attacks |
| **RO2: Review of security techniques** | Identifies research gaps in existing studies proposing security techniques for IoT | **Comprehensive synthesis of defence techniques in the literature** | **Demonstrates the applicability and usability of ML in defending against routing attacks** | | | A brief review of existing studies adopting Machine learning models |
| **RO3: Evaluation of attacks** | **Simulation setup and parameters** | Presents metrics for performance evaluation | Presents factors targeted by attacks | **Demonstrate a lack of an implementation framework** | **Design and validate the routing attack implementation framework** | Simulated attack scenario and baseline to |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | generate a dataset |
| **RO4: Evaluation of ML models** | | Presents the usability of ML in IoT for security | **Theoretical comparison of ML and established dataset sources** | | **Contributes to the dataset generation** | **Empirical validation of ML performance** |
| **RO5: Development of an intelligent model** | **Establishes a high-level conceptual framework for the intelligent defence model system** | Strategic deployment of the defence model for effective defence | Points to the promising model to develop and optimise | | **Contributes to the dataset generation** | **Development of an optimised intelligent model** |

## 5.5 CHAPTER SUMMARY

This chapter introduced a coherent flow of discoveries emerging from the articles produced from this study. It provides “the golden thread” that cuts across the articles, additionally mapping the aims of the articles with the research objectives formulated in Chapter 1. Furthermore, three categories of contributions are presented, that is, theoretical, methodological and practical. The chapter highlights the contributions of this study, fitting into the three classes of research contributions. The next chapter concludes this study, overall discussion, challenges, and points to future research directions.

# CHAPTER 6

# CONCLUSION AND FUTURE WORK

## 6.1 INTRODUCTION

This dissertation strove to address the growing challenge of routing attacks in LLNs, a critical network adopted by the IoT. By combining SLR, simulation-based experimentation, and machine learning modelling, the study highlighted its three classes of contributions. This chapter provides an overall discussion of the research environment, summarises the contributions, highlights the challenges and proffers future directions and recommendations.

## 6.2 OVERALL STUDY CONCLUSION

The study achieved key milestones aligned with the research objectives defined in the first chapter. First, this study, through the systematic literature review, identified a taxonomy of routing attacks and existing countermeasures (including secure-protocol-based, traditional IDS, and machine learning-based IDS), thereby highlighting the research gaps with regards robust and effective IoT security techniques against routing attacks. Second, by implementing and validating DIS-Flooding attacks in the Cooja/Contiki simulation tool, the study provided practical evidence of their impact on network performance metrics such as PDR, E2E delay, and power consumption. Third, the research applied classification machine learning models to a dataset derived from simulation network logs, comparing the performance of different classifiers concerning accuracy, recall, FN, and model size, as the model is intended for resource-constrained devices, and selecting the most optimal for DIS-Flooding attack detection. Finally, a lightweight and intelligent defence model was proposed, with practical implications for the accurate detection of a DIS-Flooding attack with minimum false alarms, and feasible deployment in resource-constrained IoT devices, as far as the program flash memory of devices is concerned.

## 6.3 CHALLENGES

Some of the challenges experienced in developing an intelligent security model to act opposed to the DIS-flooding attacks exploiting vulnerabilities of the RPL routing protocol are:

i. Limited access journals that the university where this study is registered does not have a subscription to.
ii. Fewer network logs as a default setting of the simulation tool
iii. Inability of the simulation tool to simulate large networks for an extended period.
iv. Lack of access to IoT Testbeds and / or real devices.

These challenges, however, open avenues that this study plans to exploit in its future research directions.

## 6.4 RECOMMENDATIONS AND FUTURE RESEARCH DIRECTIONS

Security is still a challenge in the current digital world. Now, with the advancement of generative AI for automation, hackers take advantage of this technology without ethical considerations to compromise IoT systems. The study recommends that researchers continue to develop advanced security models to act against attacks. They could also contemplate collaborations and partnerships with governmental Research and Innovation (R&I) hubs and private institutions within the discipline of IoT network performance and security.

The study is envisaged to transition into a post-doctoratal study as it takes a different direction, integrating testbeds or real-world IoT networks, delving deeper into the practicality of its nature. The study could establish some viable collaboration with researchers in government research institutions working on the integration of machine learning models to improve the security and performance of RPL-based LLNs. Getting access to IoT Testbeds would be beneficial to this study, transitioning into a post-doctoratal study. Several testbeds have been identified, including:

- FIT IoT-LAB (https://iot-lab.github.io/docs/boards/overview/),
- w-iLab.t (https://doc.ilabt.imec.be/ilabt/wilab/overview.html)

- NITOS (https://nitlab.inf.uth.gr/NITlab/ )

These testbeds could be explored in the future to investigate their usability as the underlying networks for the IoT applications, and investigate their security vulnerabilities, especially routing, for those that use RPL as their routing protocol.

## 6.5 CHAPTER SUMMARY

This study provides theoretical, methodological and practical advances toward securing LLNs against DIS-flooding attacks. By bridging the gap between literature synthesis, experimental validation, and intelligent modelling, the study demonstrates a coherent path toward the implementation of an effective, resilient, and lightweight smart security model to defend IoT networks against DIS-flooding attacks. For future endeavours, the study, in addition to contributing to academic knowledge, offers actionable insights for practitioners aiming to secure IoT infrastructures. Both IoT network security academics and engineers will find the body and findings of this study significant to their research work.

## REFERENCES


A. Almusaylim, Z., Jhanjhi, N.Z. & Alhumam, A. 2020. Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP. *Sensors*, 20(21), 10.3390/s20215997

Abdulkareem, O.A., Kontham, R.K. & Mahmood, F.E. 2024. Securing Smart Grids: Machine Learning-Driven Ensemble Intrusion Detection for IoT RPL Networks. *International Journal of Safety & Security Engineering*, 14(5),

Adebayo, A.O., Chaubey, M.S. & Numbu, L.P. 2019. Industry 4.0: The fourth industrial revolution and how it relates to the application of internet of things (IoT). *Journal of Multidisciplinary Engineering Science Studies (JMESS)*, 5(2):2477-2482.

Agiollo, A., Conti, M., Kaliyar, P., Lin, T.N. & Pajola, L. 2021. DETONAR: Detection of Routing Attacks in RPL-Based IoT. *IEEE Transactions on Network and Service Management*, 18(2):1178-1190. 10.1109/TNSM.2021.3075496

Ahmad, R. & Alsmadi, I. 2021. Machine learning approaches to IoT security: A systematic literature review *Internet of Things*, 14:100365. https://www.sciencedirect.com/science/article/pii/S2542660521000093 https://doi.org/10.1016/j.iot.2021.100365

Ahmadi, K. & Javidan, R. 2024. A novel RPL defense mechanism based on trust and deep learning for internet of things. *The Journal of Supercomputing*, 80(12):16979-17003.

Al-Amiedy, T.A., Anbar, M., Belaton, B., Kabla, A.H., Hasbullah, I.H. & Alashhab, Z.R. 2022. A Systematic Literature Review on Machine and Deep Learning Approaches for Detecting Attacks in RPL-Based 6LoWPAN of Internet of Things. *Sensors*, 22(9), 10.3390/s22093400

Al-Amiedy, T.A., Anbar, M., Belaton, B., Bahashwan, A.A., Hasbullah, I.H., Aladaileh, M.A. & Mukhaini, G.A.L. 2023. A systematic literature review on attacks defense mechanisms in RPL-based 6LoWPAN of Internet of Things. *Internet of Things*, 22:100741. https://www.sciencedirect.com/science/article/pii/S2542660523000641 https://doi.org/10.1016/j.iot.2023.100741

Al Sawafi, Y., Touzene, A. & Hedjam, R. 2023. Hybrid Deep Learning-Based Intrusion Detection System for RPL IoT Networks. *Journal of Sensor and Actuator Networks*, 12(2), 10.3390/jsan12020021

Alam, H., Yaqub, M.S. & Nadir, I. 2022. Detecting IoT Attacks using Multi-Layer Data Through Machine Learning. In. 2022 Second International Conference on Distributed Computing and High Performance Computing (DCHPC). pp. 52-59.

Alanazi, S.G., Alsirhani, A. & Alanazi, N.S. 2025. IoT Network Security Framework to Classify RPL Attacks Using Deep Learning Algorithms. In. 2025 4th International Conference on Computing and Information Technology (ICCIT). pp. 276-282.

Ankam, S. & Reddy, D.N.S. 2023. A mechanism to detecting flooding attacks in quantum enabled cloud-based lowpower and lossy networks. *Theoretical Computer Science*, 941:29-38.

https://www.sciencedirect.com/science/article/pii/S0304397522004923
https://doi.org/10.1016/j.tcs.2022.08.018

Apuke, O.D. 2017. Quantitative research methods: A synopsis approach. *Kuwait Chapter of Arabian Journal of Business and Management Review*, 33(5471):1-8.

Aydın, B., Aydın, H., Görmüş, S. & Mollahasanoğlu, E. 2024. Detection of RPL-based Routing Attacks Using Machine Learning Algorithms. *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi*, 15(4):783-796. https://doi.org/10.24012/dumf.1490367 Date of access: 2024. 10.24012/dumf.1490367

Bacon-Shone, J. 2013. *Introduction to quantitative research methods*. Graduate School, The University of Hong Kong.

Bediya, A.K. & Kumar, R. 2020. Real Time DDoS Intrusion Detection and Monitoring Framework in 6LoWPAN for Internet of Things. In. 2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON). pp. 824-828.

Bokka, R. & Sadasivam, T. 2023. Securing IoT networks: RPL attack detection with deep learning GRU networks. *Int. J. Recent Eng. Sci*, 10(2):13-21.

Cakir, S., Toklu, S. & Yalcin, N. 2020. RPL Attack Detection and Prevention in the Internet of Things Networks Using a GRU Based Deep Learning. *IEEE Access*, 8:183678-183689. 10.1109/ACCESS.2020.3029191

Choukri, W., Lamaazi, H. & Benamar, N. 2020. RPL rank attack detection using Deep Learning. In. 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT). pp. 1-6.

Davies, C. & Fisher, M. 2018. Understanding research paradigms. *Journal of the Australasian Rehabilitation Nurses Association*, 21(3):21-25.

Fatima tuz, Z., Jhanjhi, N., Brohi, S.N. & Malik, N.A. 2019. Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning. In. 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS). pp. 1-9.

Fatima tuz, Z., Jhanjhi, N., Brohi, S.N., Malik, N.A. & Humayun, M. 2020. Proposing a Hybrid RPL Protocol for Rank and Wormhole Attack Mitigation using Machine Learning. In. 2020 2nd International Conference on Computer and Information Sciences (ICCIS). pp. 1-6.

Garba, F. 2022. *A Comprehensive Review of Routing for Low Power and Lossy Network (RPL) Protocol Challenges and Proposed Improvements*.

Gawade, A.U. & Shekokar, N.M. 2017. Lightweight Secure RPL: A Need in IoT. In. 2017 International Conference on Information Technology (ICIT). pp. 214-219.

Goel, S., Verma, A. & Jain, V.K. 2023. CRA-RPL: A Novel Lightweight challenge-Response authentication-based technique for securing RPL against dropped DAO attacks. *Computers & Security*, 132:103346. https://www.sciencedirect.com/science/article/pii/S0167404823002560 https://doi.org/10.1016/j.cose.2023.103346

Gothawal, D.B. & Nagaraj, S.V. 2023. An intelligent and lightweight intrusion detection mechanism for RPL routing attacks by applying automata model. *Information Security Journal: A Global Perspective*, 32(1):1-20. https://doi.org/10.1080/19393555.2021.1971803 10.1080/19393555.2021.1971803

Goundar, S. 2012. Research methodology and research method. *Victoria University of Wellington*, 1(1):1-47.

Hachemi, F.E., Mana, M. & Bensaber, B.A. 2020. Study of the Impact of Sinkhole Attack in IoT Using Shewhart Control Charts. In. GLOBECOM 2020 - 2020 IEEE Global Communications Conference. pp. 1-5.

Hussain, F., Hussain, R., Hassan, S.A. & Hossain, E. 2020. Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Communications Surveys & Tutorials*, 22(3):1686-1721. 10.1109/COMST.2020.2986444

Ioannou, C. & Vassiliou, V. 2020. Accurate Detection of Sinkhole Attacks in IoT Networks Using Local Agents. In. 2020 Mediterranean Communication and Computer Networking Conference (MedComNet). pp. 1-8.

Ioulianou, P.P., Vassilakis, V.G. & Shahandashti, S.F. 2022. ML-based Detection of Rank and Blackhole Attacks in RPL Networks. In. 2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP). pp. 338-343.

Jahangeer, A., Bazai, S.U., Aslam, S., Marjan, S., Anas, M. & Hashemi, S.H. 2023. A Review on the Security of IoT Networks: From Network Layer's Perspective. *IEEE Access*, 11:71073-71087. 10.1109/ACCESS.2023.3246180

Jamalipour, A. & Murali, S. 2022. A Taxonomy of Machine-Learning-Based Intrusion Detection Systems for the Internet of Things: A Survey. *IEEE Internet of Things Journal*, 9(12):9444-9466. 10.1109/JIOT.2021.3126811

Kamaldeep, Malik, M., Dutta, M. & Granjal, J. 2021. IoT-Sentry: A Cross-Layer-Based Intrusion Detection System in Standardized Internet of Things. *IEEE Sensors Journal*, 21(24):28066-28076. 10.1109/jsen.2021.3124886

Kilincer, I.F., Ertam, F. & Sengur, A. 2021. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks*, 188:107840. https://www.sciencedirect.com/science/article/pii/S1389128621000141 https://doi.org/10.1016/j.comnet.2021.107840

Koosha, M., Farzaneh, B. & Farzaneh, S. 2022. A Classification of RPL Specific Attacks and Countermeasures in the Internet of Things. In. 2022 Sixth International Conference on Smart Cities, Internet of Things and Applications (SCIoT). pp. 1-7.

Krari, A., Hajami, A., Jarmouni, E. & Errakha, K. 2024. Neural Network-Based Detection Mechanism Against RPL DIS Flooding Attacks in IoT Networks. *International Journal on Technical and Physical Problems of Engineering (IJTPE)*, (59):175-184.

Laiby, T. & Subramanya, B. 2021. Machine Learning and Deep Learning Techniques for IoT-based Intrusion Detection Systems: A Literature Review. *International Journal of Management, Technology and Social Sciences (IJMTS)*, 6(2):296-314.

https://supublication.com/index.php/ijmts/article/view/649 Date of access: 2024/07/31. 10.47992/IJMTS.2581.6012.0172

Mali, S.D. & Govinda, K. 2023. A study on network routing attacks in IoT. *Materials Today: Proceedings*, 80:2997-3002. https://www.sciencedirect.com/science/article/pii/S2214785321049440 https://doi.org/10.1016/j.matpr.2021.07.092

Mbanaso, U.M., Abrahams, L. & Okafor, K.C. 2023. Research Philosophy, Design and Methodology. In: Mbanaso, U.M., Abrahams, L. & Okafor, K.C., eds. *Research Techniques for Computer Science, Information Systems and Cybersecurity*. Cham: Springer Nature Switzerland. pp. 81-113.

Medjek, F., Tandjaoui, D., Djedjig, N. & Romdhani, I. 2021. Multicast DIS attack mitigation in RPL-based IoT-LLNs. *Journal of Information Security and Applications*, 61:102939. https://www.sciencedirect.com/science/article/pii/S2214212621001563 https://doi.org/10.1016/j.jisa.2021.102939

Mehmood, M.Y., Oad, A., Abrar, M., Munir, H.M., Hasan, S.F., Muqeet, H.A.u. & Golilarz, N.A. 2021. Edge Computing for IoT-Enabled Smart Grid. *Security and Communication Networks*, 2021:5524025. https://doi.org/10.1155/2021/5524025 10.1155/2021/5524025

Momand, M.D., Mohsin, M.K. & Ihsanulhaq. 2021. Machine Learning-based Multiple Attack Detection in RPL over IoT. In. 2021 International Conference on Computer Communication and Informatics (ICCCI). pp. 1-8.

Mosa, H., Saleh, A. & Alkasassbeh, M. 2024. RPL Routing Attacks Detection for IoT Networks Using Machine Learning. In. 2024 International Jordanian Cybersecurity Conference (IJCC). pp. 169-175.

Mukhaini, G.A.L., Anbar, M., Manickam, S., Al-Amiedy, T.A. & Momani, A.A. 2024. A systematic literature review of recent lightweight detection approaches leveraging machine and deep learning mechanisms in Internet of Things networks. *Journal of King Saud University - Computer and Information Sciences*, 36(1):101866. https://www.sciencedirect.com/science/article/pii/S1319157823004202 https://doi.org/10.1016/j.jksuci.2023.101866

Myers, J.L., Well, A.D. & Lorch Jr, R.F. 2013. *Research design and statistical analysis*. Routledge.

Nandhini, P.S., Kuppuswami, S., Harish, M., Gomanishwaran, S. & Bharani, S. 2022. A Comparison on Feature Selection Methods using Machine Learning Algorithms for improving the Performance Parameters of RPL-BASED IoT Attacks Classification. In. 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA). pp. 981-986.

Nisha, Dhingra, A. & Sindhu, V. 2022. A Review of DIS-Flooding Attacks in RPL based IoT Network. In. 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT). pp. 1-6.

Pasikhan, A.M., Clark, J.A. & Gope, P. 2023. Incremental hybrid intrusion detection for 6LoWPAN. *Computers & Security*, 135:103447. https://www.sciencedirect.com/science/article/pii/S0167404823003577 10.1016/j.cose.2023.103447

Pasikhani, A.M., Clark, J.A. & Gope, P. 2021. Reinforcement-Learning-based IDS for 6LoWPAN. In. 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). pp. 1049-1060.

Pasikhani, A.M., Clark, J.A., Gope, P. & Alshahrani, A. 2021. Intrusion Detection Systems in RPL-Based 6LoWPAN: A Systematic Literature Review. *IEEE Sensors Journal*, 21(11):12940-12968. 10.1109/JSEN.2021.3068240

Pongle, P. & Chavan, G. 2015. A survey: Attacks on RPL and 6LoWPAN in IoT. In. 2015 International Conference on Pervasive Computing (ICPC). pp. 1-6.

Rabhi, S., Abbes, T. & Zarai, F. 2022. IoT Routing Attacks Detection Using Machine Learning Algorithms. *Wireless Personal Communications*, 128(3):1839-1857. https://doi.org/10.1007/s11277-022-10022-7 10.1007/s11277-022-10022-7

Rabhi, S., Abbes, T. & Zarai, F. 2023. IoT Routing Attacks Detection Using Machine Learning Algorithms. *Wireless Personal Communications*, 128(3):1839-1857. https://doi.org/10.1007/s11277-022-10022-7 10.1007/s11277-022-10022-7

Raghavendra, T., Anand, M., Selvi, M., Thangaramya, K., Santhosh Kumar, S.V.N. & Kannan, A. 2022. An Intelligent RPL attack detection using Machine Learning-Based Intrusion Detection System for Internet of Things. *Procedia Computer Science*, 215:61-70. https://www.sciencedirect.com/science/article/pii/S1877050922020786 10.1016/j.procs.2022.12.007

Raman, R., Mandaloju, B., Singh, D., Tripathi, V., Maginmani, U.H. & Gonzáles, J.L.A. 2023. An Experimental Study of Sink Hole Attacks and Distributed Denial of Service (DDS) on IoT network based Healthcare Applications. In. 2023 International Conference on Artificial Intelligence and Smart Communication (AISC). pp. 990-993.

Rani, J., Dhingra, A. & Sindhu, V. 2022. A Detailed Review of the IoT with Detection of Sinkhole Attacks in RPL based network. In. 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT). pp. 1-6.

Raoof, A., Matrawy, A. & Lung, C.H. 2019. Routing Attacks and Mitigation Methods for RPL-Based Internet of Things. *IEEE Communications Surveys & Tutorials*, 21(2):1582-1606. 10.1109/COMST.2018.2885894

Rehman, A.A. & Alharthi, K. 2016. An introduction to research paradigms. *International journal of educational investigations*, 3(8):51-59.

Sanders, K. & Yau, S.S. 2021. An Effective Approach to Protecting Low-Power and Lossy IoT Networks Against Blackhole Attacks. In. 2021 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics). pp. 65-72.

Sejaphala, L.C., Malele, V. & Lugayizi, F. 2025. A Systematic Literature Review on Defense Techniques Against Routing Attacks in Internet of Things. *Latin-American Journal of Computing*, 12(1):35 - 49. https://lajc.epn.edu.ec/index.php/LAJC/article/view/417 doi.org/10.5281/zenodo.14449371

Seth, A.D., Biswas, S. & Dhar, A.K. 2021. Mitigation Technique against Network Isolation Attack on RPL in 6LoWPAN Network. In. TENCON 2021 - 2021 IEEE Region 10 Conference (TENCON). pp. 68-73.

Sharma, H. & Yadav, G.S. 2024. Binary and Multi-Class Classification of RPL-Based Routing Attacks: An Experimental Study. In. 2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC). pp. 1-5.

Sharma, M., Elmiligi, H., Gebali, F. & Verma, A. 2019. Simulating Attacks for RPL and Generating Multi-class Dataset for Supervised Machine Learning. In. 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). pp. 0020-0026.

Sileyew, K.J. 2019. Research design and methodology. *Cyberspace*:1-12.

Snyder, H. 2019. Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104:333-339. https://www.sciencedirect.com/science/article/pii/S0148296319304564 https://doi.org/10.1016/j.jbusres.2019.07.039

Verma, A. & Ranga, V. 2018. Analysis of routing attacks on RPL based 6LoWPAN networks. *International Journal of Grid and Distributed Computing*, 11:43-56. 10.14257/ijgdc.2018.11.8.05

Verma, A. & Ranga, V. 2020. Security of RPL Based 6LoWPAN Networks in the Internet of Things: A Review. *IEEE Sensors Journal*, 20(11):5666-5690. 10.1109/JSEN.2020.2973677

Violettas, G., Simoglou, G., Petridou, S. & Mamatas, L. 2021. A Softwarized Intrusion Detection System for the RPL-based Internet of Things networks. *Future Generation Computer Systems*, 125:698-714. https://www.sciencedirect.com/science/article/pii/S0167739X21002752 https://doi.org/10.1016/j.future.2021.07.013

Wakili, A., Bakkali, S. & Alaoui, A.E.H. 2024. Machine learning for QoS and security enhancement of RPL in IoT-Enabled wireless sensors. *Sensors International*, 5:100289. https://www.sciencedirect.com/science/article/pii/S2666351124000111 https://doi.org/10.1016/j.sintl.2024.100289

Wallgren, L., Raza, S. & Voigt, T. 2013. Routing Attacks and Countermeasures in the RPL-Based Internet of Things. *International Journal of Distributed Sensor Networks*, 9(8):794326. https://doi.org/10.1155/2013/794326 Date of access: 2023/09/08. 10.1155/2013/794326

Wang, X., Yang, W., Hou, C. & Luo, H. 2024. Routing Attack and Detection Methods in the RPL-based Internet of Things. In. 2024 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). pp. 127-130.

Wang, Y., Zhang, J. & Zhang, L. 2022. Theory of decision tree models in classification problems. In. International Conference on Statistics, Applied Mathematics, and Computing Science (CSAMCS 2021). pp. 463-468.

Xu, H., Sun, Z., Cao, Y. & Bilal, H. 2023. A data-driven approach for intrusion and anomaly detection using automated machine learning for the Internet of Things. *Soft Computing*, 27(19):14469-14481. https://doi.org/10.1007/s00500-023-09037-4 10.1007/s00500-023-09037-4

Zahra, F., Jhanjhi, N.Z., Brohi, S.N., Khan, N.A., Masud, M. & AlZain, M.A. 2022. Rank and Wormhole Attack Detection Model for RPL-Based Internet of Things Using Machine Learning. *Sensors*, 22(18), 10.3390/s22186765

# APPENDIX 1

## DIS-FLOODING ATTACK CODE

```
/*--------------------DIS FLOODING ATTACK PROCESS----------------------------*/
PROCESS_THREAD(dis_attacker_process, ev, data) {
    PROCESS_BEGIN();
    PROCESS_PAUSE();

    set_global_address();

    printf("[DIS ATTACK] Malicious node started.\n");

    print_local_addresses();
 /* new connection with remote host */
  client_conn = udp_new(NULL, UIP_HTONS(UDP_SERVER_PORT), NULL);
  udp_bind(client_conn, UIP_HTONS(UDP_CLIENT_PORT));

  PRINTF("Created a connection with the server ");
  PRINT6ADDR(&client_conn->ripaddr);
  PRINTF(" local/remote port %u/%u\n",
  UIP_HTONS(client_conn->lport), UIP_HTONS(client_conn->rport));

uip_create_linklocal_allnodes_mcast(&dest_addr);    // Set the destination to all RPL nodes (broadcast)

  while(1){

     etimer_set(&attack_timer, CLOCK_SECOND * 1);  // wait 1 second before executing the process

     PROCESS_YIELD();
  dis_output(NULL);                               // Send the DIS packet

    }

    PROCESS_END();
}
/*---------------------------------------------------------------------------*/
```

# APPENDIX 2

# COLLECTED NETWORK LOGS

```
356 119442  ID:24   DATA send at 119140 ms | IPT: 0 ms with sequence no: 1 from node : aaaa::212:7418:18:1818
357 119447  ID:24   fe80::212:7418:18:1818
358 119939  ID:26   DATA recv at 118976 ms | IPT: 1750 ms with sequence no : 1 from node : aaaa::212:7412:12:1212
359 119954  ID:26   30 0 118 0 4626 1 2 0 22 15199 0 6849 53810 1325 1444 3084 263 963 8 131 252 1 189 182 65535 65535 0 0 0 0
360 120255  ID:25   Parent ETX: 2.176 | Routing Metric: 1759 | Number of Neighbors: 3 | Beacon Interval: 131 ms
361 120265  ID:25   DATA send at 119523 ms | IPT: 0 ms with sequence no: 1 from node : aaaa::212:7419:19:1919
362 120268  ID:25   fe80::212:7419:19:1919
363 120691  ID:27   time 15365 ,CPU: 3.1% ,LPM: 95.0% ,TX:  0.7% ,RX:  0.9% ,Avg: 99.7%
364 121153  ID:15   Parent ETX: 2.113 | Routing Metric: 1531 | Number of Neighbors: 5 | Beacon Interval: 131 ms
365 121164  ID:15   DATA send at 120429 ms | IPT: 33273 ms with sequence no: 2 from node : aaaa::212:740f:f:f0f
366 121167  ID:15   fe80::212:740f:f:f0f
367 121668  ID:17   Parent ETX: 0.128 | Routing Metric: 512 | Number of Neighbors: 8 | Beacon Interval: 131 ms
368 121679  ID:17   DATA send at 120601 ms | IPT: 7570 ms with sequence no: 2 from node : aaaa::212:7411:11:1111
369 121682  ID:17   fe80::212:7411:11:1111
370 121814  ID:26   DATA recv at 120851 ms | IPT: 1875 ms with sequence no : 2 from node : aaaa::212:7411:11:1111
371 121828  ID:26   30 0 120 0 4369 2 1 0 22 15435 0 5697 56193 25 822 6682 128 512 8 131 194 1 131 180 65535 65535 0 0 0 0
372 122160  ID:26   DATA recv at 121203 ms | IPT: 351 ms with sequence no : 1 from node : aaaa::212:7418:18:1818
373 122175  ID:26   30 0 121 0 6168 1 3 0 22 15248 0 6173 54685 1267 1162 4626 526 1357 5 131 252 1 189 182 65535 65535 0 0 0 0
374 124046  ID:26   DATA recv at 123085 ms | IPT: 1882 ms with sequence no : 1 from node : aaaa::212:7419:19:1919
375 124061  ID:26   30 0 123 0 6425 1 4 0 22 15298 0 5646 55411 1178 930 6168 688 1759 3 131 252 1 133 182 65535 65535 0 0 0 0
376 124420  ID:26   DATA recv at 123460 ms | IPT: 375 ms with sequence no : 2 from node : aaaa::212:740f:f:f0f
377 124434  ID:26   30 0 123 0 3855 2 4 0 22 15413 0 5682 62317 624 815 3598 625 1531 5 131 173 1 110 159 65535 65535 0 0 0 0
378 127919  ID:22   Parent ETX: 1.128 | Routing Metric: 1484 | Number of Neighbors: 4 | Beacon Interval: 131 ms
379 127930  ID:22   DATA send at 126992 ms | IPT: 41593 ms with sequence no: 2 from node : aaaa::212:7416:16:1616
380 127933  ID:22   fe80::212:7416:16:1616
381 128007  ID:26   DATA recv at 127046 ms | IPT: 3585 ms with sequence no : 2 from node : aaaa::212:7416:16:1616
```

# APPENDIX 3

## DATA EXTRACTION  MAIN FUNCTION

```
    # Compare sent and received packets NOTE RECV OMITS THE LAST ENTRY OF THE EXTRACTED_RECV_DATA
    for sent_pkt in extracted_sent_data:
        status = 0
        for recv_pkt in extracted_recv_data:
            # Check if sequence numbers and source IDs match
            if (sent_pkt.get('send seq no') == recv_pkt.get('recv seq no') and
                    sent_pkt.get('source ID') == recv_pkt.get('recv source ID')):
                status = 1
                recv_pkt['status'] = status  # Add status marker
                recv_pkt['recv_packet ID'] = recv_packet_id
                recv_pkt['delay'] = abs(int(sent_pkt['send time'] ) - int(recv_pkt['recv time']))
                recv_time = int(recv_pkt['recv time'])
                recv_pkt['inter-packet-recv time'] = abs(recv_time - current_time)
                updated_recv_data.append(recv_pkt)
                current_time = recv_time
                recv_packet_id += 1

                break
        if not status:
           r_pkt = {'status': 0,'recv_packet ID': 0,'delay': 0,
                    'recv source ID':0, 'recv time':0,
                    'inter-packet-recv time':0,'recv seq no':0}
           updated_recv_data.append(r_pkt)
    return updated_recv_data

def txt_file_open(input_file):
    sent = sent_data(input_file)
    parent = pd.DataFrame(parent_data(input_file))
    power = pd.DataFrame(power_data(input_file,sent))#.to_csv('power_dataframe.csv', index=False,na_rep='NULL')
    recv = pd.DataFrame(recv_data(input_file,sent))#.to_csv('recv_dataframe.csv', index=False,na_rep='NULL')
    sent = pd.DataFrame(sent)#.to_csv('sent_dataframe.csv', index=False,na_rep='NULL')

    network_data_dataframe = (pd.concat((sent,recv,parent,power), axis=1)).to_csv(output_file, index=False,na_rep='NULL')
    return network_data_dataframe

#DIS FLOODING NETWORK LOGS EXTRACTION AND CONVERT TO DATAFRAME AND CSVz
output_file = 'disflood_data.csv'
input_file = 'Difla/framework-disflood-moteoutput.txt'
txt_file_open(input_file)

#BASELINE NETWORK LOGS EXTRACTION AND CONVERT TO DATAFRAME AND CSV
output_file = 'baseline_data.csv'
input_file = 'Baseline/framework-baseline-moteoutput.txt'
txt_file_open(input_file)
```

# APPENDIX 4

# ETHICAL CLEARANCE

NWU®
NORTH-WEST UNIVERSITY
NOORDWES-UNIVERSITEIT
YUNIBESITI YA BOKONE-BOPHIRIMA

Private Bag X1290, Potchefstroom
South Africa 2520

Tel: 018 299-1111/2222
Fax: 018 299-4910
Web: http://www.nwu.ac.za

**Senate Committee for Research Ethics**
Tel: 016 910 3446
Email: Feziwe.Mseleni@nwu.ac.za

**ETHICS APPROVAL LETTER OF STUDY**

Based on the review by the **Faculty of Natural and Agricultural Sciences Ethics Committee (FNASREC)**, the Committee hereby clears your study as no ethical risk. This implies that the FNASREC grants permission that, provided the general conditions specified below are met, the study may be initiated, using the ethics number below.

**Study title: An Intelligent Security Model for Defence against Routing Attacks on the Internet-of-Things**
**Study Leader/Supervisor: Prof F Lugayizi**
**Student: LC Sejaphala**

**Ethics number:** N W U | - | 0 | 1 | 3 | 3 | 3 | - | 2 | 4 | - | A | 9
Institution | Study Number | Year | Status

Status: S = Submission; R = Re-Submission; P = Provisional Authorisation; A = Authorisation

**Application type: Single** **Risk Category:** **No Risk**

**Commencement date: 23/05/2024**
**Expiry date: 23/08/2025**

**General conditions:**
*The following general terms and conditions apply:*

- *The commencement date indicates the date when the study may be started.*
- *In the interest of ethical responsibility, the NWU-SCRE and FNASREC reserves the right to:*
  - *request access to any information or data at any time during the course or after completion of the study;*
  - *to ask further questions, seek additional information, require further modification or monitor the conduct of your research or the informed consent process;*
  - *withdraw or postpone approval if:*
    - *any unethical principles or practices of the study are revealed or suspected;*
    - *it becomes apparent that any relevant information was withheld from the FNASREC or that information has been false or misrepresented;*
    - *submission of the annual (or otherwise stipulated) monitoring report, the required amendments, or reporting of adverse events or incidents was not done in a timely manner and accurately; and / or*
    - *new institutional rules, national legislation or international conventions deem it necessary.*
- *FNASREC can be contacted for further information or any report templates via Roelof.Burger@nwu.ac.za 018 299 4269*

The FNASREC would like to remain at your service as scientist and researcher, and wishes you well with your study. Please do not hesitate to contact the FNASREC or the NWU-SCRE for any further enquiries or requests for assistance.

Yours sincerely,

Prof Roelof Burger
Chairperson Faculty of Natural and Agricultural Sciences Ethics Committee (FNASREC)

File reference: 9.1.5.4.2 Page 1 of 1

# APPENDIX 5

## CERTIFICATE OF LANGUAGE EDITING

NWU®
NORTH-WEST UNIVERSITY
NOORDWES-UNIVERSITEIT
UNIBESITI YA BOKONE-BOPHIRIMA

Office: 0183892451

FACULTY OF EDUCATION

Cell: 0729116600

Date: 23rd November, 2025

CERTIFICATE OF EDITING

I, **Muchativugwa Liberty Hove**, confirm and certify that I have read and edited the entire thesis, **An intelligent security model for defence against routing attacks on the Internet-of-Things**, submitted by **Lanka C. Sejaphala, orcid.org/0000-0003-1321-9557**, in fulfilment of the requirements for the degree *Doctor of Philosophy in Computer and Information Sciences with Information Technology* at the **North-West University**.

**Lanka C. Sejaphala** was promoted by **Prof F.L. Lugayizi**, with co-promoter **Prof V. Malele**.

I hold a PhD in Literature and Language Education and am competent to edit and advise on research practices, specifically coherence, cohesion and grammatical concord.

Yours sincerely

**Professor M.L. Hove (PhD, MA, PGDE, PGCE, BA Dual Honours; C2 NRF Rated Researcher; 2024 Visiting Scholar-University of London, SOAS)**

NWU®
NORTH-WEST UNIVERSITY
NOORDWES-UNIVERSITEIT
UNIBESITI YA BOKONE-BOPHIRIMA