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

ARTICLE HISTORY
Received 17 September 2024
Accepted 28 October 2024
Published 7 January 2025

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

LC. 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
North-West University
dept. Computer Science & Information Systems
Vaal Triangle, South Africa
Chris.Sejaphala@nwu.ac.za

Vusimuzi Malele
North-West University
dept. Computer Science & Information Systems
Vaal Triangle, South Africa
Vusi.Malele@nwu.ac.za

Francis Lugayizi
North-West University
dept. Computer Science & Information Systems
Mmabatho, South Africa
Francis.Lugayizi@nwu.ac.za

***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: https://doi.org/10.33333/lajc.vol12n1.03

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: https://doi.org/10.33333/lajc.vol12n1.03

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: https://doi.org/10.33333/lajc.vol12n1.03

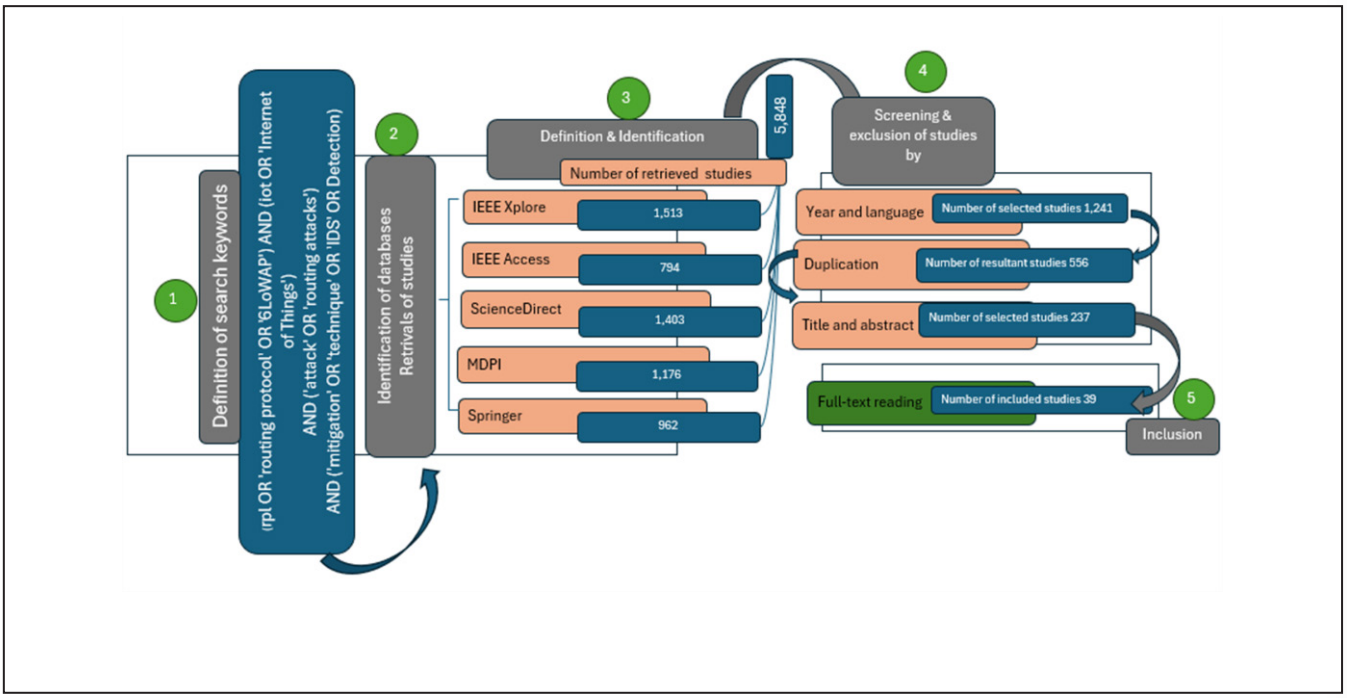

Fig. 1 Diagrammatic representation of SLR methodology steps

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.

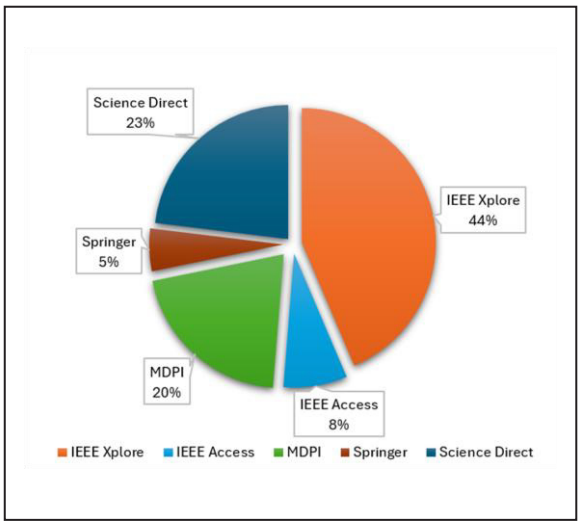

Fig 2 Contribution of Academic Libraries

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: https://doi.org/10.33333/lajc.vol12n1.03

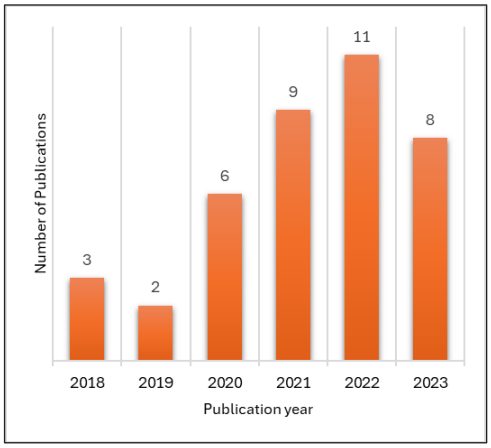

Fig. 3 Distribution of publications by year

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.

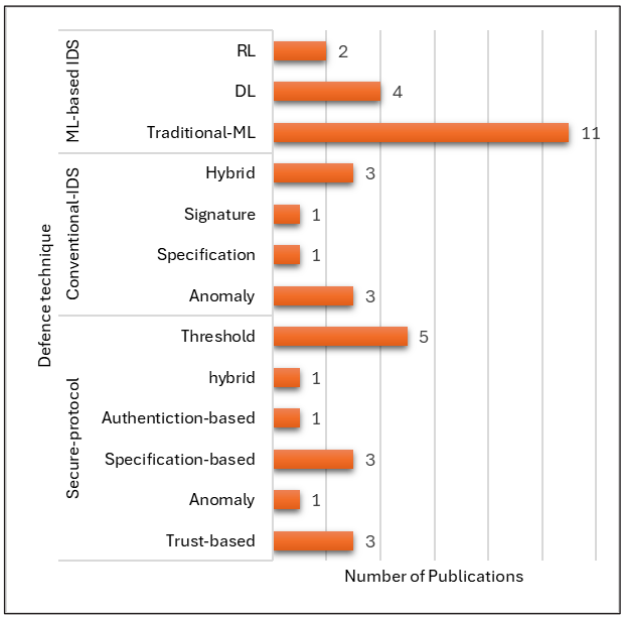

Figure 4 Distribution of different defense techniques and the adopted detection strategies

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.

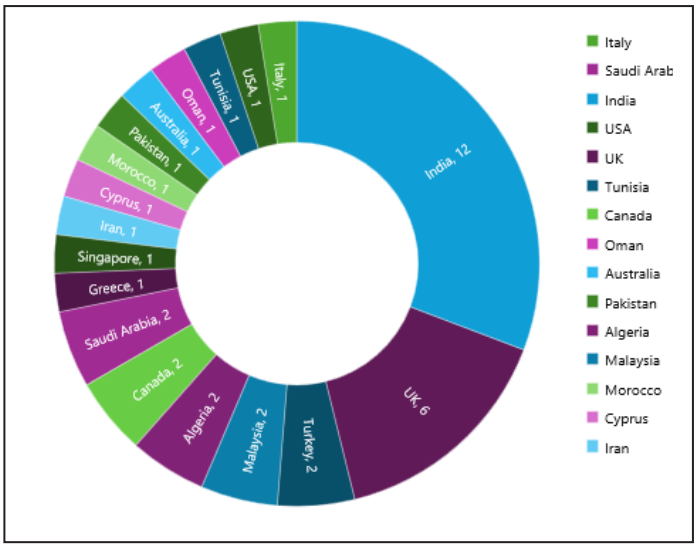

Fig. 5 Contribution by Country of origin

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: https://doi.org/10.33333/lajc.vol12n1.03

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] India[1 | 2021] USA[1 | 2018] Singapore[1 | 2018]	Turkey [1 | 2021] India[1 | 2022; 1 | 2018] Italy[1 | 2021]	India[2 | 2021; 1 | 2022; 1 | 2019] Canada[1 | 2023] UK[1 | 2022; 1 | 2021] Cyprus[1 | 2020] Morocco[1 | 2020]
	IEEE Access	Saudi Arabia[1 | 2022] UK[1 | 2020]		Turkey[1 | 2020]
	MDPI	Saudi Arabia[1 | 2020] Algeria[1 | 2023]	UK[2 | 2022]	Oman[1 | 2023] Malaysia[2 | 2022] Australia[1 | 2023]
	Springer	India[1 | 2021]		Tunisia[1 | 2023]
	Science Direct	Algeria[1 | 2021] Iran[1 | 2022] Pakistan[1 | 2020] India[1 | 2022; 1 | 2023]	Greece[1 | 2021] India[1 | 2019]	UK[1 | 2023] 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.

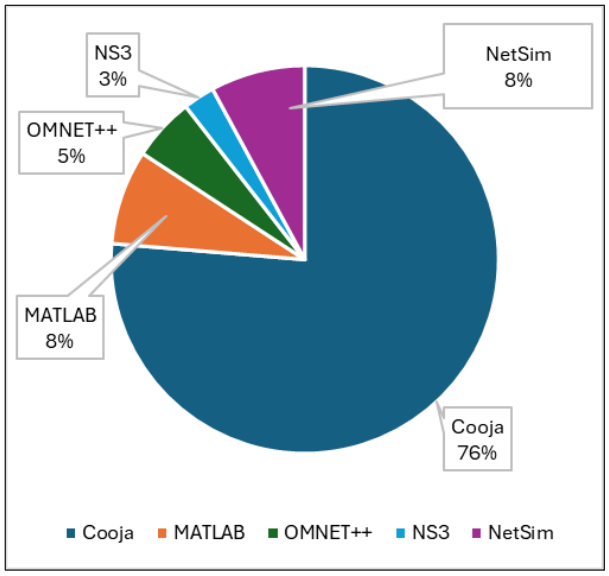

Fig. 6 Percentage of usage of simulation tools

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: https://doi.org/10.33333/lajc.vol12n1.03

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: https://doi.org/10.33333/lajc.vol12n1.03

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.

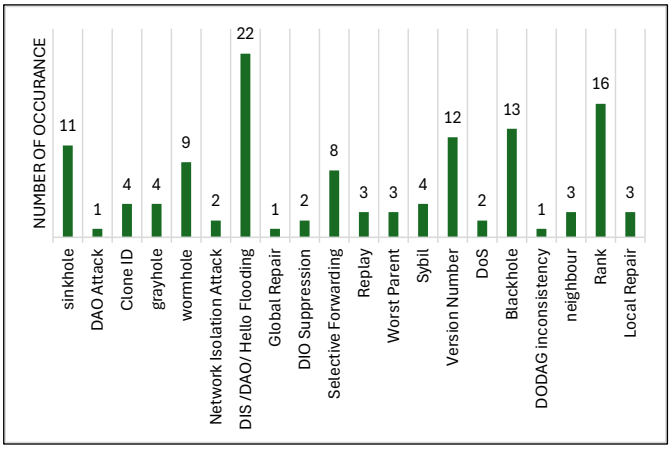

Fig.7 Distribution of discussed attacks in the selected studies

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: https://doi.org/10.33333/lajc.vol12n1.03

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.

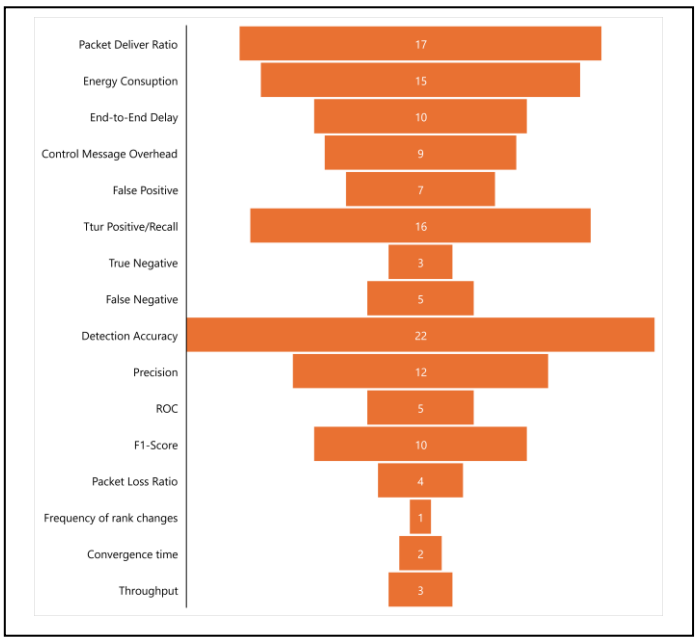

Fig. 8 Occurrence of evaluation metrics in selected studies

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: https://doi.org/10.33333/lajc.vol12n1.03

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

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: https://doi.org/10.33333/lajc.vol12n1.03

(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

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 MaleleTharmini

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.

LC. 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.