Secure Routing Protocol for Low Power and Lossy Networks Against Rank Attack: A Systematic Review

Laila Al-Qaisi, Suhaidi Hassan, Nur Haryani Binti Zakaria
InterNetWorks Research Lab, School of Computing
Universiti Utara Malaysia, Kedah Darul Aman, Malaysia

***Abstract*—The Internet of Things (IoT) is witnessing massive widespread along in almost all aspects of life. IoT is defined as a network of interconnected devices applied in various environments including smart cities, transportation, health, industries, military, and agriculture. Its main purpose is to simplify the exchange and collect data from and to deployment environments. Due to their small size and cost-effectiveness, Wireless Sensor Networks (WSN) form one of the core technologies deployed in IoT. Yet, things interconnected with each other and exchanging data are prone to different kinds of security attacks. As a result, it is possible to compromise data while transmitted from source to destination through nodes. Routing Protocol for Low Power and Lossy Networks (RPL) offers only slight protection against routing attacks, but having a network with limited energy sources, processors, and memory, besides being deployed in unattended nature and hostile environment requires more scalable security measures. This paper focuses on investigating the problem of security provisioning in RPL. As such, a Systematic Literature Review (SLR) of security mechanisms proposed for RPL will be discussed. An extensive search was conducted on various online databases, then findings were filtered by reviewing abstracts, introduction, and conclusion. Finally, a summary of recent research work is presented. This work is important to highlight various aspects of securing RPL and get an initial insight for studying them.**

Keywords—Wireless sensor networks; internet of things (IoT); routing security; RPL; objective function

I. Introduction

Internet of Things (IoT) emergence was led by the assistance of existing wireless communications along with Radio-Frequency Identification (RFID), Wireless Sensor Network (WSN) technologies besides new emerging technologies such as Information-Centric Network (ICN) and Named Data Networks (NDN) [1]. So, data is easily transmitted between various devices and associative things regardless of time and place through network standards and protocols. Every device and thing in IoT is assigned a unique Internet Protocol (IP) address, by which they can sense and collect data from the deployment environment for both processing and decision making. IoT is contributing significantly to various domains like smart cities, building, healthcare, and agriculture and has a vital impact on improving people’s daily life [2].

IoT architecture is presented in the literature as mentioned by [3]–[5] consisting of three main layers, namely, perception, network, and application layers. As a hot research topic, many researchers found the three layers architecture very basic and is suitable for defining the main terminology of IoT and cannot be used for research that digs into further components of IoT. This is when the five layers architecture was introduced as [3] explained, it included processing and business as additional layers. Fig. 1 shows both three- and five-layers architecture.

The network layer is responsible for communication and information exchange employing techniques, standards, and protocols to simplify the task such as Internet Protocol Version 4 (IPv4), Internet Protocol Version 6 (IPv6), Constrained Application Protocol (CoAP), Wireless Personal Area Network (WPAN), IPv6 over Low Power Wireless Personal Area Network (6LoWPAN), User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). Securing data transmitted between the perception layer and the application layer is facilitated by the network layer as well [6].

The Routing Protocol for Low-Power and Lossy Networks (RPL) was developed by the Internet Engineering Task Force (IETF) to fit into Wireless Sensor Networks (WSNs) and the Internet of Things (IoT) domains. As a simple networking protocol, RPL was designed as an interoperable protocol that handles resource-constrained devices connected via multi-hop networks. It enables efficient use of smart devices’ energy along with the establishment of flexible topology and routing of data [7].

Nevertheless, the RPL protocol since its inception suffers from a lack of security measures at the network layer as stated by [8]. RPL and its improved versions suffer from a severe performance gap towards network attacks especially ranking attacks [9]. Securing IoT routing should be studied considering WSN features as they are inherited into the IoT environment [10]. Moreover, other metrics in RPL should be taken into consideration such as power consumption as a major challenge facing IoT and controls network lifetime [11].

Cryptography, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), authentication, trust-based mitigation techniques, and much more, have all been introduced to solve security vulnerabilities in LLNs [12]. In the application, transport, network, and physical levels, IoT devices and traditional PCs share some similar protocols. The biggest impediment to LLN devices implementing existing security methods at IoT interfaces is their limited computational and energy resources [13]. LLN devices produce massive amounts of data, but they lack the resources to store and process it.

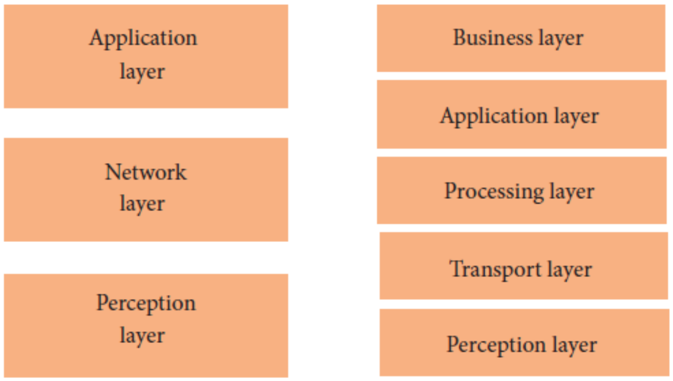

Fig. 1. IoT Architectures [3].

Since in IoT, RPL plays a vital and broad role in service providing, it's a clear target for attackers and a crucial candidate for defense as well. To overcome security issues and challenges in RPL routing, further research is required as per [14], and how intrusions on RPL can be detected is one facet of defense that must now be examined. As a result, this forms a starting point to investigate, propose, and implement mitigation mechanisms for network layer attacks [15].

The main goal of this study is to show the impact that rank attacks (RA) can have on RPL networks. Also, to study and compare the available research that support RPL security and counter the effect of these attacks in terms of the security techniques utilized and their performance. To point up the flaws in the available solutions suggested by existing studies. To suggest some potential methods to address the existing flaws and increase RPL security in IoT networks by limiting the effects of RA. Also, discuss some open challenges in this study area that require more attention.

This paper presents an SLR of security mechanisms proposed for RPL RA specifically being one of the most destructive attacks targeting RPL topology. Starting with RPL in-depth explanation. Followed by a discussion on RPL attacks along with a suitable taxonomy. A focus on rank attacks is presented afterward. Finally, a summary of the selected studies is presented. The remainder of this paper is organized as follows: Section 2 defines and explains preliminaries. Then, Section 3 identifies and explains the following SLR methodology. Section 4 discusses the results found thoroughly. Finally, Section 5 summarizes selected research papers and therefore compares the approaches used by the researchers.

II. Preliminaries

A. *Routing Protocol for Low-Power and Lossy Networks (RPL)*

Since Low-Power and Lossy Networks (LLN) consist of highly constrained devices in terms of memory, processing capabilities, and energy resources, RPL was designed as an IPV6 distance vector protocol to support communication among LLN devices such IoT. It was mentioned by [16] and [17] that such networks suffer from low data and packet delivery rates along with lossy connection which RPL was designed to be flexible enough for network conditions' adaptation and provide suitable alternative routes when default ones are not available for any reason at any time.

RPL can be defined as a proactive routing protocol that relies on the distance between nodes and sink node to form a topology. The following explanation of the RPL hierarchy is based on [18]–[21]:

1) Hierarchy: Using the distance vector procedure RPL exploits Directed Acyclic Graphs (DAG) mechanism to construct a structure tree or DODAG (Destination Oriented Directed acyclic graph) that controls available nodes' connections with each other. This will enable multi-hop communication via the closest nodes.

RPL methods for establishing connections include point-to-point (P2P), point-to-multipoint (P2MP), and multipoint-to-multipoint (MP2P) communications. While types of nodes for constructing topology are, the source that are responsible nodes for gathering information, leaf nodes that do not perform any task and sink nodes which are the most significant with capabilities of energy and processing to compile whole network information. Hence, two major terms are required here, Control Messages (CM) by which connections are initiated and maintained along with topology formation, and Objective Functions (OF) for routing decision making through the network.

Four types of CM are used to exchange information between nodes in RPL:

- DODAG Information Solicitation (DIS): it is used to request passing the DIO to network neighbors.
- DODAG Information Object (DIO): Stores pertinent information needed to build upward DODAGs route such as RPLInstanceID, configuration parameters, candidate parent information, DODAG maintenance, and more.
- Destination Advertisement Object (DAO): sends information to register every node visited on the downward route.
- Destination Advertisement Object Acknowledgement (DAO-ACK): confirms safe receipt of sent DAO message to the sender node.

2) Objective function (OF): OF was described as the basic element that is handling several vital definitions;(1) computing link cost, (2) parent node selection (when, who, and how many candidates), and (3) computing rank cost, fourth: advertising path cost. There are two defaults OF with RPL, MRHOF (Minimum Rank with Hysteresis Objective Function) and OF0 (Objective Function Zero), and the following are their definitions as per [22]–[24]:

- OF0: This OF adds a specifically predefined value to the previous rank. It takes hop count as a routing metric and selects the best parent node from available candidates based on that. While building the DODAG, nodes should consider hop count to get the shortest path for reaching the grounded root. The rank increases while going down from root to candidate nodes. However, reliance on node metrics will cause poor link quality. Also, selecting the shortest path in terms of minimum hop count may lead to more retransmissions along with increased packet loss if the path was unreliable. Additionally, this same shortest path may cause more node failure which will definitely decrease network lifetime.

- MRHOF: This OF was designed to overcome the shortcoming of OF0 which depends on a single node metric to compute rank and choose the best parent node. It relies on the expected transmission count (ETX) as a dynamic link metric to stabilize the rank. Still, it chooses the lowest-cost path and avoids network churn overflow using two mechanisms. First, choose a low-rank path, and second hysteresis mechanism ensures changing rank to a lower one only if there exists a rank that is less than the current one. Literature has two main implementations of MRHOF, one that relies on ETX and the other relies on energy.

3) Routing metrics: Routing metrics are essential to evaluate path cost and then choose the lowest cost path. There are too many implementations in literature for OF, some take a single metric to calculate rank, while others consider more than one metric. As a matter of fact, metrics can be categorized based on their characteristics into node and link, dynamic and static, quality and quantity routing nodes [25]. Both routing metrics and constraints are used to form a criterion to choose the optimal path. Yet, the main difference between them is that constraint is used to restrict options such as avoiding unreliable links, while metrics define a certain level of reliability to include links that give the optimal path. As a result, both metrics and constraints are used and deployed as per RPL implementation requirements [26]. Moreover, dynamicity is a vital characteristic of metrics, since RPL operating environment is rapidly changing which results in instability of both node and link metrics [27].

The following list summarizes metrics of both link and nodes (refer to Fig. 2):

- Link metrics:

a) RSSI and LQI: main radio link estimators are the Received Signal Strength Indicator (RSSI) and the Link Quality Indicator (LQI). The former indicates the level of power received by an antenna that is a high level of RSSI means a stronger radio signal which indicates a closer destination. While the latter measures the quality of the link using a range of values between 0 to 7.

b) ETX: Expected Transmission Count indicates the reliability of the network and gives the required number of transmissions for receiving acknowledgment from the destination.

- Node metrics:

a) Energy: represents the energy consumed by nodes through network operations.

b) Hop count: it is a measure of path link that is used extensively in wireless networks and the main drawback is to get the shortest path with the lowest hop count regardless of link quality.

c) End-to-end delay: a vital metric for building route in RPL and it indicates the needed time to deliver packets to the sink from sender nodes.

B. RPL Attacks Classification

RPL is vulnerable to various kinds of attacks and does not have a solid security measure that can prevent such attacks [28]. There are several taxonomies proposed for attacks targeting RPL in different studies, such as Almusaylim et al. [17] in which three main types of attacks were explained namely; against resources that consume nodes resources, topology in which try to cause damage in the construction process and traffic which aim at capturing as much traffic as possible. Also, Avila et al. [10] categorized attacks into passive and active attacks, where passive attacks aim to gather information after accessing the system and comprise confidentiality, and active ones sabotage the system by data alteration, disabling nodes, or giving access to unauthorized users. An interesting categorization was presented by Raoof et al. [29], in which attacks were classified based on their origin into RPL Specific and WSN inherited as Fig. 3 shows.

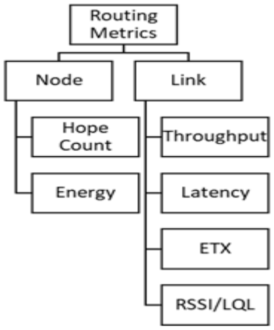

Fig. 2. Routing Metrics.

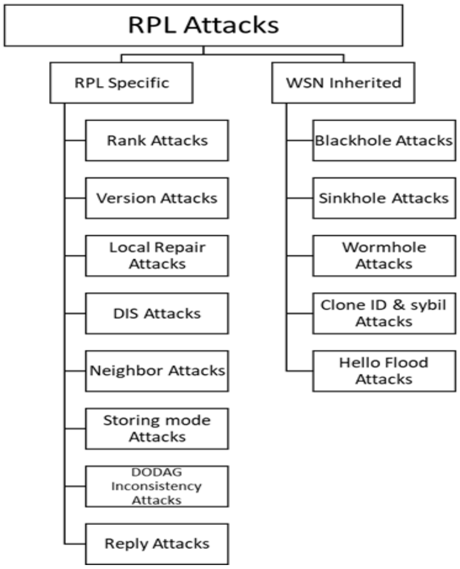

Fig. 3. RPL Attacks.

III. Methodology

This study employed the systematic literature review guidelines and standards proposed by Kitchenham [30]. This consists of a set of well-defined stages conducted in line with a predefined protocol. SLR consists of three phases: planning, conducting, and reporting the reviews according to Shaffril et al. [31]. These phases consist of the following processes: (1) identifying RQs; (2) developing a review protocol; (3) determining both exclusion and inclusion criteria; (4) selecting search strategy and study process; (5) quality assessment (QA); and (6) extracting and synthesizing data.

A. Identifying Research Questions (RQs)Text

To achieve the main objectives of this study, primary studies should be assessed and reviewed thoroughly. As a result, the following research questions are proposed based on Population, Intervention, Comparison, Outcomes, and Context (PICOC) as per [30]:

- RQ1: What is the impact of the rank attack and to which extent do they damage the network?
- RQ2: What are the proposed approaches that monitor the network to handle attacks targeting RPL?
- RQ3: What are the technical performance metrics of the research in this field?
- RQ4: What are the advantages and disadvantages of each proposed approach?

B. Developing a Review Protocol

A vital step that makes SLR different from traditional methods of reviewing the literature. Because it decreases study bias as discussed by Shaffril et al. [32]. The review protocol categorizes review background, search strategy, development of RQs, extraction of data, criteria for study selection, and data synthesis.

C. Search Strategy

The search strategy started with choosing E-digital libraries and online databases as the following list shows, taking into consideration selecting only high-impact-factor publications:

- IEEE Explore
- ACM Digital Library
- Science Direct
- Scopus
- Wiley Online Library

Afterward, the search string is required to conduct an in-depth search through selected E-digital libraries. The following steps were applied to define the used search string as per [30]:

- Define major keywords depending on identified research questions.
- Consider linguistic synonyms, alternatives, and interchangeable terms for each keyword.
- Use conjunction operators (AND, OR) when needed to produce the full search string.

As a result, keywords included for the search were “IoT” OR “Internet of Things” AND “RPL” OR “Routing Protocol for Low-Power and Lossy Networks” AND “rank attack detection” OR “mitigation”. All available papers relating to specified keywords 2022 were collected from digital libraries.

Afterward, a manual search was applied to the results of the automatic search by filtering each paper's title, abstract and content. This is to ensure that the selected paper supports answering the defined QAs and Fig. 4 illustrates the overall search phases.

D. Inclusion and Exclusion Criteria

Search results are filtered in terms of the following inclusion and exclusion criteria:

- Inclusion Criteria:

a) Written in English language.

b) The study's domain is RPL and responds to previously stated RQs.

c) Published in journal or conference.

d) Published date: 2017-2022.

- Exclusion Criteria:

a) Duplicates.

b) Unavailable full text.

c) Do not meet the inclusion criteria.

Afterward, a manual filtration process was conducted by reviewing the title, abstract, and conclusion to get papers that meet the set criteria of found papers. This eliminated the number of found papers from 1061 to 9 only, given that only papers published between 2017 to 2022 and studied RA in RPL only.

E. Applying Quality Assessment (QA)

The related studies' quality was assessed using QA as recommended by Kitchenham [30]. All found studies were assessed concerning every single research question. QA criteria used for the assessment process were as follows:

- QA1: Is the topic addressed in the paper related to securing RPL?
- QA2: Is there any mechanism proposed to detect rank attack detection in RPL?
- QA3: Is there a sufficient explanation of the background in which the study was performed?
- QA4: Is there a clear declaration concerning methods used to validate the applied mechanism?

The reliability of articles and studies found was tested through the four QA criteria and has three categories low, medium, and high as by Shaffril et al. [31] and [32]. Each QA had a score of 2 points and each paper that meets the defined QA earns a score of 2, 1 is earned when the paper partially meets the QA criteria and 0 when it does not satisfy the QA criteria at all. Papers scored more than 5 are discussed in the next section and are categorized based on the technique used and Table II summarizes the findings sorted by year of publication.

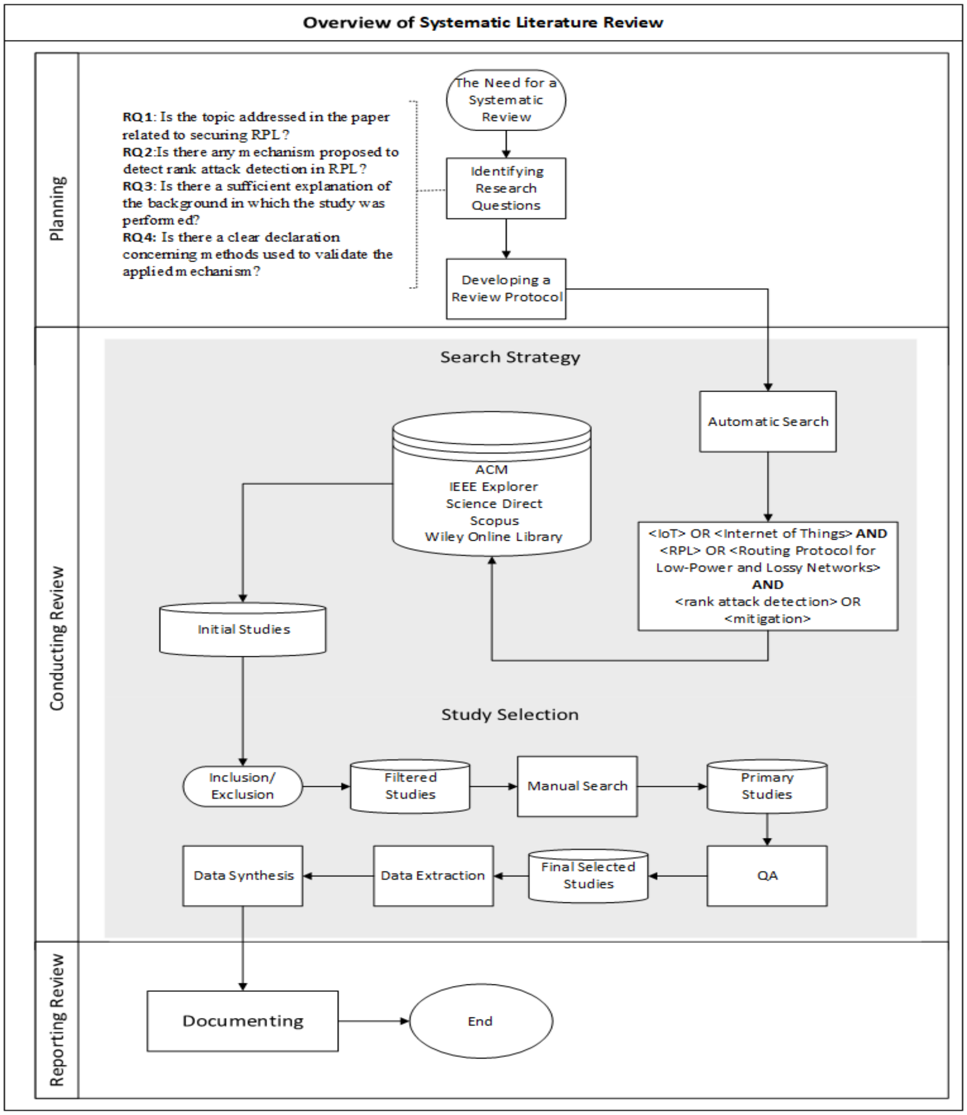
Overview of Systematic Literature Review
Planning
RQ1: Is the topic addressed in the paper related to securing RPL?
RQ2:Is there any mechanism proposed to detect rank attack detection in RPL?
RQ3: Is there a sufficient explanation of the background in which the study was performed?
RQ4: Is there a clear declaration concerning methods used to validate the applied mechanism?
The Need for a Systematic Review
Identifying Research Questions
Developing a Review Protocol
Conducting Review
Search Strategy
Automatic Search
ACM
IEEE Explorer
Science Direct
Scopus
Wiley Online Library
<IoT> OR <Internet of Things> AND
<RPL> OR <Routing Protocol for Low-Power and Lossy Networks>
AND
<rank attack detection> OR <mitigation>
Initial Studies
Study Selection
Inclusion/ Exclusion
Filtered Studies
Manual Search
Primary Studies
QA
Final Selected Studies
Data Extraction
Data Synthesis
Reporting Review
Documenting
End

Fig. 4. Systematic Literature Review (SLR).

F. Data Extraction and Synthesis

For accurate data extraction and synthesis, a form was developed to conduct this step. Details of each study related to the reference, year of publication, methodology, and comments were extracted. A tabular form was used to register this information about each study. Table I illustrates the details registered for each paper.

TABLE I. TABLE TYPE STYLES

Extracted Data	Description
Study ID	paper DOI
Year	Publication Date
Type	Journal or conference
Methodology	e.g., trust, cryptography, IDS
Performance Measure	e.g., ACC, PR, RE

IV. RESULTS

This section discusses rank attacks against RPL and analyzes the application of detection and mitigation techniques towards it. The methods analyzed herein are ones that were proposed to secure RPL against RA. The goal is to present their performance in terms of the chosen performance metrics which will be discussed here as well.

A. Rank Attack (RA) (RQ1)

This attack aims at attracting network traffic to a specified node. Ul Hassan et al. [34] defined RA as an attack that occurs when the malicious node sends information of a lower range, to be closer than others to the root. This scenario will have a consequence that makes malicious nodes able to capture as much traffic as possible. Hashemi and Aliee [35] mentioned that RA is considered the most destructive attack among other types, this is because it intentionally aims at downgrading the network performance by tampering with the rank. By which a rank is decreased to make the malicious node closer to the chosen parent, so a massive amount of passing packets through it may be manipulated.

RA workflow starts when a malicious node sends a fake rank through an RPL control message or advertises a fake route across the root node to mislead close nodes to make them transmit packets through it [36]. In other words, RA exposes ranks of child nodes in the RPL network topology, then modifies the way of processing DIO messages by neighboring nodes. The worst part will occur when a malicious node with a fake rank is chosen as the preferred parent node while operating, which will result in creating more traffic for data packets to go through the malicious node as un-optimized routing occurs due to network topology OF is not completely achieved as discussed [37].

Mishra and Pandya [38] added another scenario for rank attacks by which an attacker node advertises a better routing metric to other neighboring nodes although it's fake, it misleads network flow to be passing through it. Besides, this may lead to significant increasing latency and decreasing throughput in the network. Fig. 5 illustrates an example of RA.

RA may affect the network and causes several issues as discussed by Nandhini and Mehtre [39]: first, form an unoptimized route. The second is unrecognized loop formation. Third, RPL network topology never uses the optimized route. Fourth, the decreased packet delivery ratio affects the delay increase. Fifth, network topology changes rapidly causing DIO messages number to increase. Some network restricted resource properties would be affected such as energy consumption, throughput, latency, and data rate.

As a result, RPL security forms a major concern that should be considered and further investigated, especially when RA is the topic. This is because routed data shouldn’t be accessed by a third party or attacker.

B. *RPL Rank Attack (RA) Countermeasures (RQ2)*

Many papers categorized countermeasures deployed to secure RPL against attacks, Raoof et al. [29] classified detection and mitigation mechanisms into Acknowledgment-based which depends on sending and receiving acknowledgment messages to prevent any suspicious alteration, and Trust-based depending on the node to monitor neighboring nodes by rating them and consider a ratio to accept, Location-based considering physical location of nodes and Statistical/Mathematical-based by which a mathematical calculation is considered to detect attacks.

Further classification is presented by Verma and Ranga [37] added to the above mentioned, Intrusion Detection Systems (IDS) that consists of signature-based IDS, anomaly-based IDS, and specification-based IDS. It is defined by [40] as, a complete system that may be deployed either in a stand-alone computer system or a network. Its main role is to monitor activities and analyze them to specify any incident which targets security policies integrity, availability, or confidentiality and report it as unauthorized or malicious activity.

Muzammal et al. [41] also mentioned IDS as a significant method that is used to mitigate attacks of RPL in addition to all previously stated ones. Besides many alterations to OF by combining various previously explained link and nodes metrics with adopting additional methods such as fuzzy logic.

Moreover, Tasneem and Wahid [42] classified proposed defense methods for RPL into reactive approaches that include cryptography-based, trust-based, and threshold-based methods, and proactive approaches which consist of time-based and energy-based methods.

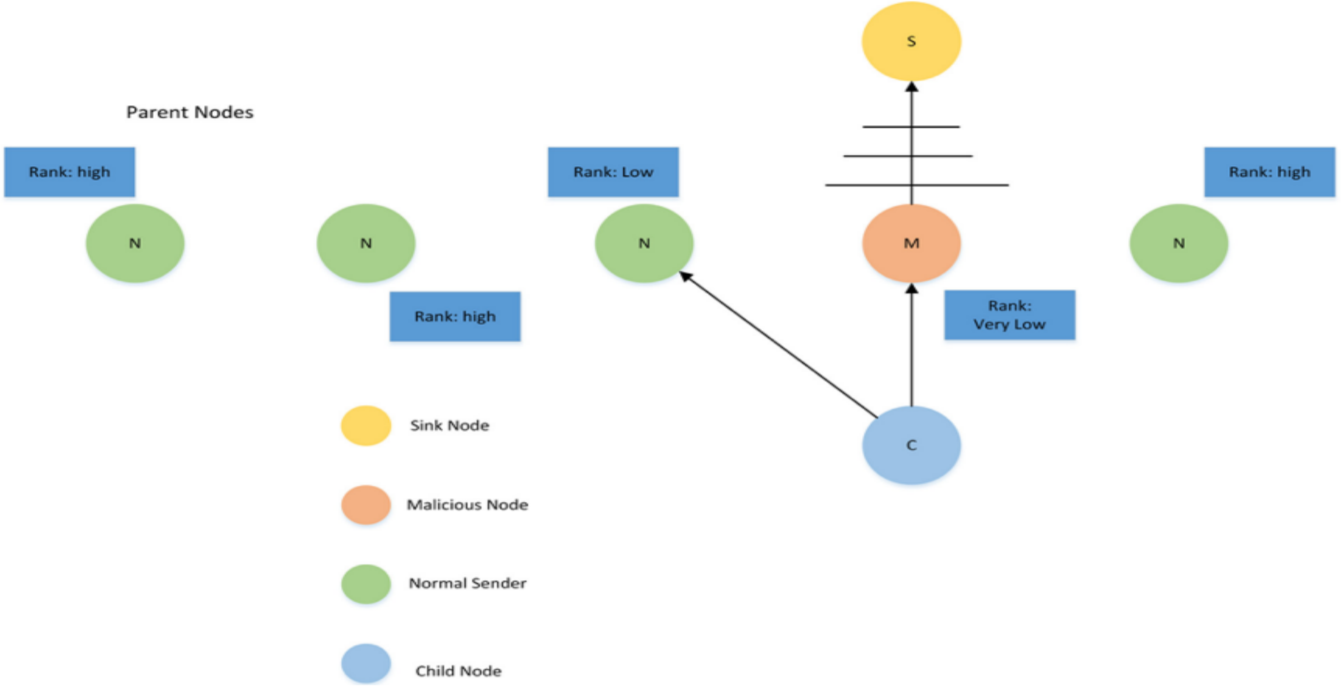

Fig. 5. RA Example, [33].

Finally, countermeasures proposed for RPL against RA were classified by Almusaylim et al. [17] into modification techniques by which some alterations may be applied to a certain component of RPL such as DODAG, OF, or ranking policies and IDS.

C. Performance Metrics (RQ3)

Various metrics were used for measuring the performance of the proposed methods. Yet, many studies like [7], [9], and [14] mentioned using node and link metrics discussed previously such as power consumption, ETX, and PDR. In addition, accuracy metrics including True Positive Rate (TPR), False Positive Rate (FPR), and Detection Rate (DR) were mentioned to be used as well, and below are their formulas as per [43]–[47]:

- Detection Rate (DR): Refers to the ability of the model to rank patterns, and its ability to select a threshold in the ranking used to classify patterns as normal if above the threshold and abnormal if below. It is calculated using Equation 1 below:

$$DR = \frac{TPR}{TPR+FNR} * 100\% \qquad (1)$$

where All = TPR + TNR + FPR + FNR

- TPR: Also called sensitivity and it measures the truly predicted positive and were correctly identified. It is calculated as in Equation 3:

$$\mathrm{TPR} = \frac{TPR}{TPR+FNR} * 100\% \qquad (2)$$

Where FNR is calculated as follows:

$$FNR = \frac{TPR+TNR}{TPR+FPR} * 100\% \qquad (3)$$

- FPR: Refers to the probability of a False Alarm. That is, the percentage of actual abnormal flows predicted as normal flows and it is calculated as in Equation 4:

$$\mathrm{FPR} = \frac{FPR}{FPR+TNR} * 100\% \qquad (4)$$

Where TNR is calculated as follows:

$$TNR = \frac{TNR}{FPR+TNR} * 100\% \qquad (5)$$

D. Summary of Shortlisted Studies (RQ4)

This section discusses thoroughly found nine studies that proposed techniques to detect and mitigate RA targeting RPL and strictly meet the criteria defined in the SLR methodology section along with a summary presented in Table II.

A Secure RPL Routing Protocol (SRPL-RP) for rank and version number attacks was proposed by Almusaylim et al. [48] in which a timestamp is added to ensure the legitimacy of sending nodes. A monitoring table is included through the process of constructing DODAG which collects all information about existing nodes. A blacklist and alert tables were added to simplify the procedures of mitigating and isolating both types of studied attacks. Several conditions were added to control the current rank of nodes and parent nodes to maintain a safe network. Simulations were conducted using the Cooja simulator and results showed that the proposed SRPL-RP had a higher PDR and a lower control message value compared to methods previously proposed in literature along with 95% accuracy in all kinds of tested network topologies.

Shafique et al. [49] proposed a novel sink-based IDS (SBIDS) by which a timespan is added to the DAO message for ensuring its freshness. Then several detection steps are followed to detect any violence in rank, especially a rule that compares node current rank (NCR) to node parent rank NPR. Simulations were conducted using the Cooja simulator and performance metrics were percentage of accuracy, TP, TN, FP, FN, and confidence interval (CI) under mobility conditions. Results showed that SBIDS had 100% detection accuracy under normal circumstances, yet it decreased with the number of nodes with mobility increased.

TABLE II. FINAL SELECTED PAPERS FOR SECURING RPL AGAINST RA

Ref	Paper Information			
	Year	**Type**	**Methodology**	**Performance Measure**
Almusaylim et al. [48]	2020	Journal	SRPL-RP based on rank strategy	PDR, Acc
Shafique et al. [49]	2018	Journal	Sink-based IDS (SBIDS)	Acc, TPR, TNR, FPR, FNR, and confidence interval (CI)
Boudouaia et al. [50]	2021	Journal	Rank property + DIO messages with 2 rank thresholds	DR, average network hops, and global energy consumption.
Nair and BJ [51]	2021	Conference	SCF and Dijkstra's algorithm	Throughput and PDR
Karmakar, Sengupta and Bit [52]	2021	Conference	DODAG modification with adding Authentication Code (HMAC-LOCHA)	DR, FPR, FNR, and energy consumption
Zarzoor [53]	2021	Journal	Layering mechanism	Latency, energy consumption, and DR
Stephen and Arockiam [54]	2018	Conference	Node energy based E2V architecture with IDS	Network convergence delay, energy consumption, and attacker identification delay
Seth et al. [55]	2020	Conference	Round trip time (RTT) based detection and isolation mechanism	Acc
Althubaity, Gong, and Raymond [56]	2020	Conference	Specification-based IDS (FORCE)	DR and overheads incurred on the nodes' resources

Boudouaia et al. [50] proposed a security scheme that uses a rank property to choose a preferred parent in RPL topology, so any malicious behavior in terms of rank may be detected. Afterward, when the DIO message arrives two values will be calculated to indicate the minimum rank threshold and maximum rank threshold depending on the neighboring rank. As a result, nodes that do not match threshold criteria are blacklisted and the selection process will be held upon legitimate nodes only. Experiments were done using the cooja simulator, 4 scenarios, and performance evaluations were conducted in terms of successful detection rate, the average network hops, and the global energy consumption.

Another solution was proposed by Nair and BJ [51] in which both spatial correlation function (SCF) and Dijkstra's algorithm were applied to select the preferred parent nodes using proactive routing in terms of throughput and energy as selection parameters. For experiments, the NS-2 simulator was used, and performance evaluation was based on throughput and PDR.

An interesting study by Karmakar, Sengupta, and Bit [52] combined several methods to secure RPL against RA. First, the algorithm forming DODAG was modified to be able to detect RA during building and maintaining the topology. Second, two modules were added, distributed at all nodes, and centralized at the sink node. Third, the DAO control message was modified to lower overhead levels and a lightweight Message Authentication Code (HMAC-LOCHA) was used to verify exchanged message's integrity and authenticity. Cooja simulator was used to conduct experiments and multiple test case scenarios were applied. detection accuracy, false positive/negative rate, and energy consumption.

Zarzoor [53] proposed a security mechanism that relies on the layering principle. It consists of three main phases: first, nodes are categorized into layers. Second, calculate the trust value for the path. Third, detect and mitigate the RA. For implementation Cooja simulator was used and performance evaluation was conducted based on latency, nodes' energy consumption, and accuracy of malicious node detection.

A further three-phase mechanism called E2V was proposed by Stephen and Arockiam [54] which starts with rank calculation, substantiation, and elimination. Where the malicious node is detected at the substantiation phase by the defined IDS. Then, in the elimination phase, malicious nodes will be eliminated by either local repair or global repair. The Cooja simulator is used for implementation purposes and evaluation in terms of network parameters such as network convergence delay, energy consumption, and attacker identification delay.

Seth et al. [55] used round trip time (RTT) to detect verify and isolate malicious nodes from the network in RPL. Cooja simulator was used for implementation and performance was evaluated in terms of accuracy where the proposed scheme was found to be better than previous ones.

Althubaity, Gong, and Raymond [56] proposed a fully distributed specification-based IDS (FORCE). The type of node forms a significant issue for FORCE, yet it was designed so that every single node can analyze and receive control messages and in case of any attack detection an alert will be generated directly. Evaluation metrics used were detection rates and overheads incurred on the nodes' resources and experiments were conducted using the Cooja simulator.

V. Discussion

The main goal of this part is to understand the obstacles and current research for detecting RA in RPL routing protocols, as well as several flaws that require more research. RPL routing protocols provide for more efficient use of smart devices, resources, and data routing. Because of the characteristics that distinguish this network from others, developing secure routing algorithms for IoT networks is a difficult task. Secure routing techniques for IoT devices have received a lot of attention in recent years. However, they all rely on traditional cryptographic operations, which deplete device resources and have a significant impact on the performance of limited IoT devices. They are vulnerable to a wide range of security threats. The absence of infrastructure, inconsistent links, resource limits, poor physical security, and changing topology of PRLs make them vulnerable to attacks and difficult to defend against.

A. Limitations

Based on reviewed studies it was found that current security features of RPL may be defined but not actually used either in real applications or in research as they are marked as optional features. This puts security as a significant concern of RPL especially since it's being deployed and used widely in IoT environments which are witnessing massive growth globally.

As RPL is vulnerable to several attacks, RA is one of the major attacks that were found to compromise RPL, yet a lower amount of research conducted to specifically target it. Also, these studies had several shortcomings which should be addressed to overcome their consequences.

As a result, it was found from this review: that first, most studies considered either selection or mitigation, but only a few of them investigated both schemes. Second, mainly one type of network topology was selected to test and measure the performance of the proposed scheme. Third, most research studies tend to evaluate their proposed schemes by taking small IoT Networks (<100 nodes) which are considered impractical because the impact of network size on both attacks and security mechanisms remains unknown. Fourth, many schemes encountered an increased number of control messages for acknowledgment purposes which may cause both complexities and increased overhead and are considered inefficient.

B. Comparison

Based on provided review and summery in Table II, it can be concluded that most chosen metrics for performance evaluation were DR and energy consumption as in [50], [52], [53] and [56]. As DR indicated to which extent the proposed mechanism was able to detect threats and energy consumption represented a measure of keeping devices resources available. IDS was chosen as a detection solution in three papers [49], [54] and [56], while the rest choose to modify the main protocol policies and add certain solutions to improve its security measures. None of found studies tented to combine IDS with protocol policy improvements. Also, none of them included integration with other recently hot fields such as fuzzy logic as a solution.

Studies discussed securing RPL against RA were 5 conference papers to 4 journal papers within period 2017 to 2022, which means this kind of attacks require more powerful solutions are to be proposed in order to provide efficient solution.

Finally, experiments of all founded papers showed that the Cooja simulator usage is dominant in RPL studies where all of them implemented proposed solutions using it.

VI. Conclusion

This paper studied applied methods for RA detection in RPL thoroughly to address limitations in this field. An SLR was conducted to determine the required studies to be conducted for improving security measures deployed in this regard. Definitions of required terms starting from IoT, RPL architecture, and security attacks, to detection and mitigation techniques, are presented to help researchers have a brief explanation of them. Also, a summary of recent studies is presented. It was found that many of the currently applied mechanisms in literature have weak points, cryptographic-based methods may provide security, but it definitely consumes nodes' restricted resources. While trust-based may solve the resource restrictions, it may cause other issues regarding network performance such as latency. IDS, it's considered the most effective solution among all proposed ones, but it requires collaboration, and many aspects in this regard should be taken into consideration such as placement. Finally, a hybrid IDS is highly recommended as a solution for securing RPL as it is used by IoT and keeping it safe will definitely be reflected in the overall IoT environment.

VII. Future Work

Future research aims at extending this review to examine and build better detection and mitigation measures for RPL. This will primarily be addressing RPL rank vulnerabilities.

Acknowledgment

This research was supported by the Ministry of Higher Education (MoHE) of Malaysia through The Fundamental Research Grant Scheme (FRGS/1/2020/ICT07/UUM/01/1).

References

[1] A. Abrar, A. S. B. C. M. Arif, and K. B. M. Zaini, “Producer Mobility Support in Information-Centric Networks: Research Background and Open Issues,” Int. J. Commun. Networks Distrib. Syst., vol. 28, no. 1, p. 1, 2022, doi: 10.1504/ijcnds.2022.10044469.

[2] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, “A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions,” Electron., vol. 9, no. 7, 2020, doi: 10.3390/electronics9071177.

[3] P. Sethi and S. R. Sarangi, “Internet Of Things: Architecture,Issues and Applications,” Int. J. Eng. Res. Appl., vol. 07, no. 06, pp. 85–88, 2017, doi: 10.9790/9622-0706048588.

[4] R. Mondal and T. Zulfi, “Internet of Things and Wireless Sensor Network for Smart Cities,” Int. J. Comput. Sci. Issues, vol. 14, no. 5, pp. 50–55, 2017, doi: 10.20943/01201705.5055.

[5] H. Babbar and S. Rani, “Software-defined networking framework securing internet of things,” in Integration of WSN and IoT for Smart Cities, Springer, 2020, pp. 1–14.

[6] D. B.D. and F. Al-Turjman, “A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks,” Ad Hoc Networks, vol. 97, p. 102022, Feb. 2020, doi: 10.1016/j.adhoc.2019.102022.

[7] M. Zaminkar and R. Fotohi, “SoS-RPL: Securing Internet of Things Against Sinkhole Attack Using RPL Protocol-Based Node Rating and Ranking Mechanism,” Wirel. Pers. Commun., vol. 114, no. 2, pp. 1287–1312, Sep. 2020, doi: 10.1007/s11277-020-07421-z.

[8] M. Pishdar, Y. Seifi, M. Nasiri, and M. Bag-Mohammadi, “PCC-RPL: An efficient trust-based security extension for RPL,” Inf. Secur. J. A Glob. Perspect., vol. 31, no. 2, pp. 168–178, Mar. 2022, doi: 10.1080/19393555.2021.1887413.

[9] S. Y. Hashemi and F. Shams Aliee, “Fuzzy, Dynamic and Trust Based Routing Protocol for IoT,” J. Netw. Syst. Manag., vol. 28, no. 4, pp. 1248–1278, Oct. 2020, doi: 10.1007/s10922-020-09535-y.

[10] K. Avila, D. Jabba, and J. Gomez, “Security Aspects for Rpl-Based Protocols: A Systematic Review in IoT,” Appl. Sci., vol. 10, no. 18, p. 6472, 2020, doi: 10.3390/app10186472.

[11] G. Soni and R. Sudhakar, “A L-IDS against Dropping Attack to Secure and Improve RPL Performance in WSN Aided IoT,” in 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN), Feb. 2020, pp. 377–383, doi: 10.1109/SPIN48934.2020.9071118.

[12] T. Park, N. Abuzainab, and W. Saad, “Learning How to Communicate in the Internet of Things: Finite Resources and Heterogeneity,” IEEE Access, vol. 4, pp. 7063–7073, 2016, doi: 10.1109/ACCESS.2016.2615643.

[13] D. Midi, A. Rullo, A. Mudgerikar, and E. Bertino, “Kalis — A System for Knowledge-Driven Adaptable Intrusion Detection for the Internet of Things,” in 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Jun. 2017, pp. 656–666, doi: 10.1109/ICDCS.2017.104.

[14] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, “Trust-aware and cooperative routing protocol for IoT security,” J. Inf. Secur. Appl., vol. 52, p. 102467, Jun. 2020, doi: 10.1016/j.jisa.2020.102467.

[15] E. Fernandes, A. Rahmati, K. Eykholt, and A. Prakash, “Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges?,” IEEE Secur. Priv., vol. 15, no. 4, pp. 79–84, 2017, doi: 10.1109/MSP.2017.3151346.

[16] D. B. Gothawal and S. V. Nagaraj, “Intrusion Detection for Enhancing RPL Security,” Procedia Comput. Sci., vol. 165, pp. 565–572, 2019, doi: 10.1016/j.procs.2020.01.051.

[17] Z. A. Almusaylim, A. Alhumam, and N. Z. Jhanjhi, “Proposing a Secure RPL based Internet of Things Routing Protocol: A Review,” Ad Hoc Networks, vol. 101, p. 102096, Apr. 2020, doi: 10.1016/j.adhoc.2020.102096.

[18] A. Arena, P. Perazzo, C. Vallati, G. Dini, and G. Anastasi, “Evaluating and improving the scalability of RPL security in the Internet of Things,” Comput. Commun., vol. 151, pp. 119–132, Feb. 2020, doi: 10.1016/j.comcom.2019.12.062.

[19] M. A. Boudouaia, A. Ali-Pacha, A. Abouaissa, and P. Lorenz, “Security Against Rank Attack in RPL Protocol,” IEEE Netw., vol. 34, no. 4, pp. 133–139, Jul. 2020, doi: 10.1109/MNET.011.1900651.

[20] A. M. Pasikhani, J. A. Clark, P. Gope, and A. Alshahrani, “Intrusion Detection Systems in RPL-Based 6LoWPAN: A Systematic Literature Review,” IEEE Sens. J., vol. 21, no. 11, pp. 12940–12968, 2021, doi: 10.1109/JSEN.2021.3068240.

[21] A. K. Rana and S. Sharma, “Contiki Cooja Security Solution (CCSS) with IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) in Internet of Things Applications,” 2021, pp. 251–259.

[22] H. Lamaazi and N. Benamar, “A comprehensive survey on enhancements and limitations of the RPL protocol: A focus on the objective function,” Ad Hoc Networks, vol. 96, p. 102001, Jan. 2020, doi: 10.1016/j.adhoc.2019.102001.

[23] A. Paul and A. S. Pillai, “A Review on RPL Objective Function Improvements for IoT Applications,” ACCESS 2021 - Proc. 2021 2nd

Int. Conf. Adv. Comput. Commun. Embed. Secur. Syst., no. September, pp. 80–85, 2021, doi: 10.1109/ACCESS51619.2021.9563294.

[24] S. M M and D. P. I. Basarkod, "A Comprehensive Survey on RPL: Evolution and Challenges," SSRN Electron. J., 2019, doi: 10.2139/ssrn.3510063.

[25] G. Violettas, G. Simoglou, S. Petridou, and L. Mamatas, "A Softwarized Intrusion Detection System for the RPL-based Internet of Things networks," Futur. Gener. Comput. Syst., vol. 125, pp. 698–714, Dec. 2021, doi: 10.1016/j.future.2021.07.013.

[26] H. Lamaazi and N. Benamar, "RPL enhancement using a new objective function based on combined metrics," in 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Jun. 2017, pp. 1459–1464, doi: 10.1109/IWCMC.2017.7986499.

[27] S. Sennan and S. Palanisamy, "Composite Metric Based Energy Efficient Routing Protocol for Internet of Things," Int. J. Intell. Eng. Syst., vol. 10, no. 5, pp. 278–286, Oct. 2017, doi: 10.22266/ijies2017.1031.30.

[28] J. Karlsson, L. S. Dooley, and G. Pulkkis, "Secure Routing for MANET Connected Internet of Things Systems," in 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), Aug. 2018, pp. 114–119, doi: 10.1109/FiCloud.2018.00024.

[29] A. Raoof, A. Matrawy, and C. H. Lung, "Routing Attacks and Mitigation Methods for RPL-Based Internet of Things," IEEE Commun. Surv. Tutorials, vol. 21, no. 2, pp. 1582–1606, 2019, doi: 10.1109/COMST.2018.2885894.

[30] B. Kitchenham, "Procedures for performing systematic reviews," Jun. 2004, [Online]. Available: http://www.elizabete.com.br/rs/Tutorial_IHC_2012_files/Conceitos_RevisaoSistematica_kitchenham_2004.pdf.

[31] H. A. Mohamed Shaffril, S. F. Samsuddin, and A. Abu Samah, "The ABC of systematic literature review: the basic methodological guidance for beginners," Qual. Quant., vol. 55, no. 4, pp. 1319–1346, 2021, doi: 10.1007/s11135-020-01059-6.

[32] H. A. M. Shaffril, A. A. Samah, and S. F. Samsuddin, "Guidelines for developing a systematic literature review for studies related to climate change adaptation," Environ. Sci. Pollut. Res., vol. 28, no. 18, pp. 22265–22277, May 2021, doi: 10.1007/s11356-021-13178-0.

[33] M. Karthik, VK Pushpalatha, "Addressing Attacks and Security Mechanism in the RPL based IOT," Int. J. Comput. Sci. Eng. Commun, vol. 5, no. 5, pp. 1715–1721, 2017.

[34] T. ul Hassan, M. Asim, T. Baker, J. Hassan, and N. Tariq, "CTrust - RPL : A control layer - based trust mechanism for supporting secure routing in routing protocol for low power and lossy networks - based Internet of Things applications," Trans. Emerg. Telecommun. Technol., vol. 32, no. 3, Mar. 2021, doi: 10.1002/ett.4224.

[35] S. Y. Hashemi and F. Shams Aliee, "Dynamic and comprehensive trust model for IoT and its integration into RPL," J. Supercomput., vol. 75, no. 7, pp. 3555–3584, 2019, doi: 10.1007/s11227-018-2700-3.

[36] A. Rehman, M. M. Khan, M. A. Lodhi, and F. B. Hussain, "Rank attack using objective function in RPL for low power and lossy networks," in 2016 International Conference on Industrial Informatics and Computer Systems (CIICS), Mar. 2016, pp. 1–5, doi: 10.1109/ICCSII.2016.7462418.

[37] A. Verma and V. Ranga, "Security of RPL Based 6LoWPAN Networks in the Internet of Things: A Review," IEEE Sens. J., vol. 20, no. 11, pp. 5666–5690, 2020, doi: 10.1109/JSEN.2020.2973677.

[38] N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," IEEE Access, vol. 9, pp. 59353–59377, 2021, doi: 10.1109/ACCESS.2021.3073408.

[39] P. S. Nandhini and B. M. Mehtre, "Intrusion Detection System Based RPL Attack Detection Techniques and Countermeasures in IoT: A Comparison," Proc. 4th Int. Conf. Commun. Electron. Syst. ICCES 2019, no. Icces, pp. 666–672, 2019, doi: 10.1109/ICCES45898.2019.9002088.

[40] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," J. Netw. Comput. Appl., vol. 84, pp. 25–37, 2017, doi: 10.1016/j.jnca.2017.02.009.

[41] S. M. Muzammal, R. K. Murugesan, and N. Z. Jhanjhi, "A Comprehensive Review on Secure Routing in Internet of Things: Mitigation Methods and Trust-Based Approaches," IEEE Internet Things J., vol. 8, no. 6, pp. 4186–4210, 2021, doi: 10.1109/JIOT.2020.3031162.

[42] B. Tasneem and M. Wahid, "A Review of Secure Routing Challenges in Low Power and Lossy Networks," in 2021 International Conference on Communication Technologies (ComTech), Sep. 2021, pp. 120–125, doi: 10.1109/ComTech52583.2021.9616966.

[43] P. Ruckebusch, J. Devloo, D. Carels, E. De Poorter, and I. Moerman, "An Evaluation of Link Estimation Algorithms for RPL in Dynamic Wireless Sensor Networks," 2016, pp. 349–361.

[44] P. Sanmartin, A. Rojas, L. Fernandez, K. Avila, D. Jabba, and S. Valle, "Sigma Routing Metric for RPL Protocol," Sensors, vol. 18, no. 4, p. 1277, Apr. 2018, doi: 10.3390/s18041277.

[45] H. Lamaazi and N. Benamar, "OF-EC: A novel energy consumption aware objective function for RPL based on fuzzy logic.," J. Netw. Comput. Appl., vol. 117, pp. 42–58, Sep. 2018, doi: 10.1016/j.jnca.2018.05.015.

[46] X. Liu, Z. Sheng, C. Yin, F. Ali, and D. Roggen, "Performance Analysis of Routing Protocol for Low Power and Lossy Networks (RPL) in Large Scale Networks," IEEE Internet Things J., vol. 4, no. 6, pp. 2172–2185, Dec. 2017, doi: 10.1109/JIOT.2017.2755980.

[47] O. Gaddour, A. Koubâa, and M. Abid, "Quality-of-service aware routing for static and mobile IPv6-based low-power and lossy sensor networks using RPL," Ad Hoc Networks, vol. 33, pp. 233–256, Oct. 2015, doi: 10.1016/j.adhoc.2015.05.009.

[48] Z. A. Almusaylim, N. Jhanjhi, and A. Alhumam, "Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP," Sensors, vol. 20, no. 21, p. 5997, Oct. 2020, doi: 10.3390/s20215997.

[49] U. Shafique, A. Khan, A. Rehman, F. Bashir, and M. Alam, "Detection of rank attack in routing protocol for Low Power and Lossy Networks," Ann. Telecommun., vol. 73, no. 7–8, pp. 429–438, Aug. 2018, doi: 10.1007/s12243-018-0645-4.

[50] M. A. Boudouaia, A. Abouaissa, A. Ali - Pacha, A. Benayache, and P. Lorenz, " RPL rank based - attack mitigation scheme in IoT environment," Int. J. Commun. Syst., vol. 34, no. 13, Sep. 2021, doi: 10.1002/dac.4917.

[51] D. S. Nair and S. K. BJ, "Identifying Rank Attacks and Alert Application in WSN," in 2021 6th International Conference on Communication and Electronics Systems (ICCES), Jul. 2021, pp. 798–802, doi: 10.1109/ICCES51350.2021.9489034.

[52] S. Karmakar, J. Sengupta, and S. Das Bit, "LEADER: Low Overhead Rank Attack Detection for Securing RPL based IoT," in 2021 International Conference on COMmunication Systems & NETworkS (COMSNETS), Jan. 2021, pp. 429–437, doi: 10.1109/COMSNETS51098.2021.9352937.

[53] A. R. Zarzoor, "Securing RPL Routing Path for IoT against rank attack via utilizing layering technique," Int. J. Electr. Eng. Informatics, vol. 13, no. 4, pp. 789–800, 2021, doi: 10.15676/ijeei.2021.13.4.2.

[54] R. Stephen and L. Arockiam, "E2V: Techniques for Detecting and Mitigating Rank Inconsistency Attack (RInA) in RPL based Internet of Things," J. Phys. Conf. Ser., vol. 1142, no. 1, 2018, doi: 10.1088/1742-6596/1142/1/012009.

[55] A. D. Seth, S. Biswas, and A. K. Dhar, "Detection and Verification of Decreased Rank Attack using Round-Trip Times in RPL-Based 6LoWPAN Networks," Int. Symp. Adv. Networks Telecommun. Syst. ANTS, vol. 2020-Decem, pp. 3–8, 2020, doi: 10.1109/ANTS50601.2020.9342754.

[56] A. Althubaity, T. Gong, K. K. Raymond, M. Nixon, R. Ammar, and S. Han, "Specification-based Distributed Detection of Rank-related Attacks in RPL-based Resource-Constrained Real-Time Wireless Networks," Proc. - 2020 IEEE Conf. Ind. Cyberphysical Syst. ICPS 2020, pp. 168–175, 2020, doi: 10.1109/ICPS48405.2020.9274726.