EAI Endorsed Transactions
on Internet of Things

Research Article **EAI.EU**

Fortifying RPL-Based 6LoWPAN in IoT: A Comprehensive Review of Emerging Attack Vectors and Defensive Mechanisms using Machine Learning

Unnam Sudha Rani[1], Kareemulla Shaik[1,*]

[1]School of Computer Science and Engineering, VIT-A.P University, Amaravati-522241, Andhra Pradesh, India

Abstract

Internet of Things (IoT) is a system of interconnected digital tools, including sensing elements and communication modules, that enables seamless data transfer over the Internet. These devices, though, run with resource limitations in terms of power, memory, and computational capabilities. Therefore, scientists created the IPv6 Over Low-power Wireless Personal Area Network (6LoWPAN) protocol, which allows for wireless communication among IoT devices while ensuring efficient use of resources. The Internet Engineering Task Force (IETF) has formally ratified 6LoWPAN, and its ROLL working group presented the Routing Protocol for Low-power and Lossy Networks (RPL), standardized as IETF RFC 6550, as a fundamental part of the 6LoWPAN stack. Although beneficial, RPL-based routing within IoT networks is particularly exposed to various security risks. This survey offers an in-depth overview of RPL-specific attacks and their defense mechanisms, as published in top-tier journals between 2015 and 2025. Based on a conceptual analysis of routing-based attacks in RPL, we introduce a new attack taxonomy that categorizes these attacks into 12 fundamental categories based on intrinsic features and behavior. Furthermore, we discuss the impact of every attack on network performance and describe actual cases in which these vulnerabilities have been targeted. Aside from attack classification, this survey proposes a novel taxonomy of defense mechanisms that categorizes them into 8 fundamental categories depending on their strategic method of routing attack mitigation. Every defense method is extensively studied concerning its applicability in actual IoT implementations. Furthermore, we critically study and evaluate different evaluation platforms, such as testbeds and simulators, used in investigating RPL-based security attacks and countermeasures, highlighting their applicability and usefulness in real-world environments. Lastly, we identify open research challenges by examining current literature gaps and outline future research opportunities for both researchers and practitioners. In addition, the survey notes a clear shift toward sequence-based and graph-driven learning models, supported by optimization with meta-heuristic techniques, which increasingly guide the design of modern IDS frameworks for RPL-enabled IoT networks. Our research is intended to offer valuable understanding and a strong platform for investigators to create more efficient security measures in response to evolving RPL-based attacks in the IoT environment.

Keywords: Routing Protocol for Low-power and Lossy Networks (RPL), Internet of Things (IoT), IPv6 Over Low-power Wireless Personal Area Network (6LoWPAN) protocol, Multiple Attacks, Security Mechanism, Routing Protocols.

Received on 10 July 2025, accepted on 17 August 2025, published on 16 December 2025

doi: 10.4108/eetiot.9694

*Corresponding author. Email: kareemulla.shaik@vitap.ac.in

1. Introduction

IoT is a revolutionary scientific innovation that allows seamless communication and data exchange between different physical objects, such as sensors, computing machines, and other digital objects, without human interaction. IoT operates as an ecosystem where sensors collect data, gateways enable data transfer, and the application layer (AL) analyzes the data to make smart decisions [1]. This technology has a broad range of applications in many different industries such as healthcare, agronomy, trade robotics, transport, smart home, and market operations. Many IoT architectures have been suggested with varying user points of view. Among the commonly used models are the three-layered architecture, middleware-based architecture, and modular services architecture [2]. The triple-layered model categorizes IoT devices into three major components: the perception layer, the network layer, and the application layer. The perception layer gathers and processes data from IoT devices, while the network layer guarantees secure data transmission between the perception and application layers. The AL hosts user interfaces and provides services to users of IoT [3]. Low-power lossy links are one of the principal complications in IoT networks, which determine the small throughput and high packet loss rate (PLR).

In response to such limitations, the IETF's ROLL working group proposed the RPL. Though RPL has been designed with security mechanisms, it is still susceptible to new cyber threats. Scientists have proposed many security solutions over a period of time to make RPL more secure; however, there is an ongoing requirement for more sophisticated and integrated defense mechanisms to resist newer modes of attack [4]. With the fast growth of IoT ecosystems, it is necessary to provide devices with unique identifiers, something that has been alleviated by the simulation of the IPv6 protocol. Reliable and efficient routing and protection from external threats are another essential component of IoT security. The 6LoWPAN protocol, facilitating the use of IPv6-based networking for low-power wireless personal area networks, is instrumental in solving both secure routing and unique device identification challenges [5].

RPL is an important element in IoT networking due to its ability to optimize routing for low-power devices, manage lossy links, and accommodate scalable deployments. Its main benefits add to the effectiveness and dependability of IoT systems in various ways. To begin with, RPL optimizes resource usage through power constraint adaptation of IoT devices while providing reliable communication over unstable links. This feature not only boosts network performance but also extends the battery life of energy-restrained devices. Moreover, the scalability of RPL enables it to effectually accomplish large-scale IoT deployments, supporting dynamic topology and guaranteed connectivity across numerous fields such as smart cities, industrial IoT, healthcare, and agriculture. Alternative important representative of RPL is its sustenance for optimizing routing decisions according to individual application needs, taking into consideration energy expenditure, latency, and link quality. This makes efficient data transfer possible and accommodates specialized applications such as firmware upgrades using multicast communication and group operations [6].

Additionally, RPL's flawless compatibility with IPv6, supported by its attainment of IETF standard status, makes it easy to combine into different IoT devices and systems and enjoys a tightly connected and standardized communication model [7]. Security is another major feature of RPL since it supports encryption mechanisms and secure key management schemes for safeguarding critical IoT data and applications. The security features further increase the credibility of IoT deployments by addressing probable vulnerabilities and cyber-attacks. RPL is generally a fundamental protocol in IoT communications that provides an all-around array of features optimizing performance, scalability, reliability, and security. Its ability to enable effective and secure IoT operations makes it a critical technology for the continued growth and development of connected systems [8].

The key contributions of the proposed survey can be summarized as follows:

- A **comprehensive taxonomy of RPL attacks** is introduced, covering 12 categories that include both conventional and emerging threats such as DAO induction, cross-layer, and hybrid attacks. This extends beyond earlier surveys that used narrower classifications.
- The **practical impact of routing attacks** on IoT performance (e.g., PDR, delay, energy) is assessed with support from real-world cases, whereas many prior reviews remained purely theoretical.
- A **novel taxonomy of defense mechanisms** is proposed with 8 categories, unifying IDS, ML/DL, cryptographic, trust-based, and blockchain-based strategies, unlike earlier works that considered them in isolation.
- A **critical review of testbeds, simulators, and datasets** is provided, an aspect largely overlooked in past surveys, to guide researchers in practical evaluation.
- **Research gaps and future directions** are identified, emphasizing unresolved challenges such as scalable hybrid-attack detection, lightweight AI defense mechanisms, and large-scale real-world validation.

The research questions of this comprehensive survey are formulated as:

- Which attacks have researchers identified as the most critical threats undermining the security of the RPL protocol?
- What network constraints are exaggerated by routing attacks, and how do these attacks affect routing choices?
  - What protection mechanisms have been designed to make the RPL protocol more secure against different security threats?
  - What are the most significant assessment metrics to measure the effectiveness of various defense mechanisms?
- What are the available simulators, datasets, and testbeds for research on RPL, and how well can researchers leverage them?
- Which attacks are not yet explored in the literature, and what new defense mechanisms need to be proposed to fill these gaps?

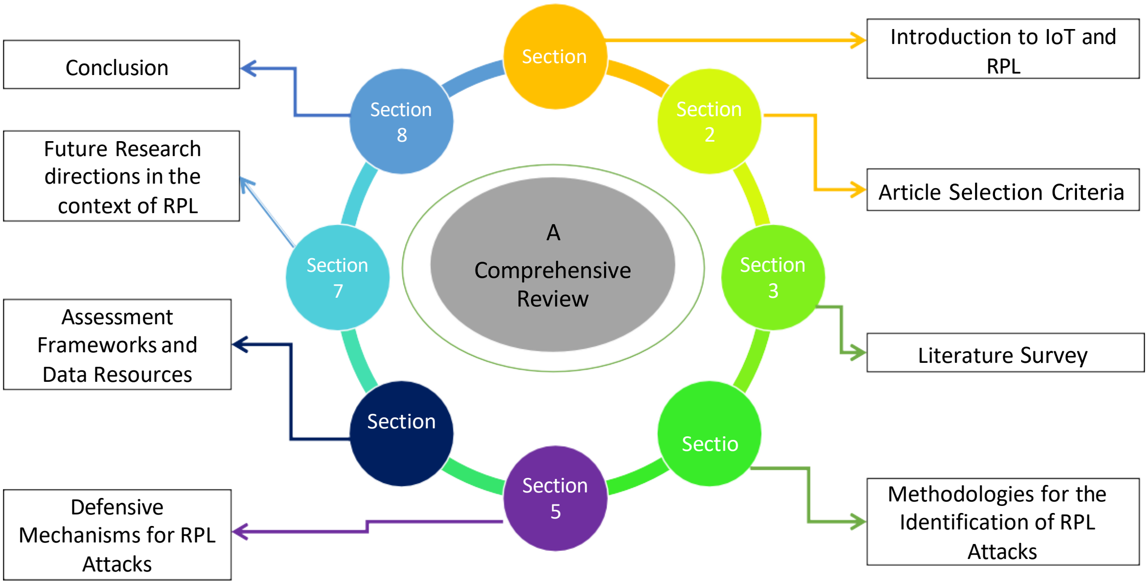
Conclusion
Section
Section 8
Section 2
Introduction to IoT and RPL
Future Research directions in the context of RPL
Article Selection Criteria
A Comprehensive Review
Section 7
Section 3
Literature Survey
Assessment Frameworks and Data Resources
Section
Sectio
Section 5
Methodologies for the Identification of RPL Attacks
Defensive Mechanisms for RPL Attacks

Figure 1: Outline of this survey are listed in this diagram.

The outline of this survey is designed as follows: Section 2 emphasizes the article selection criteria. Section 3 summarizes current surveys and relevant research, highlighting the novelty and importance of this research. Section 4 discusses RPL-based attacks, classification, and examines how they affect network performance. Section 5 deeply analyzes defense mechanisms developed to counter RPL attacks. Section 6 presents several evaluation tools and testbeds employed for measuring RPL security. Section 7 explains current research needs and delineates open problems waiting to be discovered in the future. Section 8 concludes the manuscript by recapping the important contributions and broad applicability of this survey. The Figure 1 outline the details representation and flow of this survey

2. Article Selection Criteria

To systematically identify, screen, and include relevant studies for this review, the PRISMA 2020 framework was rigorously followed. The identification phase began with a comprehensive search of multiple scientific databases and digital libraries, including IEEE Xplore, Springer, Elsevier (ScienceDirect), Wiley, MDPI, Taylor & Francis, Hindawi, and ACM Digital Library. A total of 312 records were initially identified through these electronic databases using relevant keywords and Boolean operators aligned with the review objectives. An additional 27 records were retrieved from other sources such as preprint servers, reference list checks, and grey literature databases, resulting in a combined total of 339 records.

In the next step, duplicate records were carefully removed using automated tools and manual validation, leading to the exclusion of 86 duplicates, thus retaining 253 unique records for screening. During the screening phase, the titles and abstracts of all 253 articles were independently reviewed to evaluate their weight to the predefined inclusion criteria. 149 articles were excluded at this stage for reasons such as irrelevance to RPL-based security, lack of technical contribution, or generality beyond the scope of IoT and 6LoWPAN networks.

Subsequently, 104 full-text articles were evaluated for suitability based on more detailed inclusion criteria, such as the presence of a defined security framework, attack mitigation strategy, or trust management scheme within RPL-enabled IoT environments. During this eligibility phase, 56 full-text articles were excluded due to reasons such as inadequate methodological rigor, absence of experimental validation, or duplication in reporting the same study across conference and journal versions.

Finally, 48 studies met all eligibility criteria and were included in the qualitative synthesis of this review. These selected studies span a publication period from 2015 to 2025, encompassing contributions from SCI-indexed journals, IEEE Access, Elsevier's *Computer Networks*, *Computers & Security*, Springer's *Cluster Computing*, Wiley's *IJCS*, and other high-impact venues.

The included references collectively represent diverse methodological approaches such as lightweight authentication schemes, hybrid trust-based intrusion detection systems, game-theoretic models, machine learning-based RPL enhancements, blockchain-integrated security frameworks, and fuzzy-logic-powered attack mitigation protocols. Each step of the selection procedure is clearly illustrated using the PRISMA 2020 diagram to maintain openness and reproducibility of the review methodology.

3. Literature Survey

Several studies have been published on intrusion detection systems (IDS) and strategies for mitigating RPL routing attacks in IoT ecosystem. These works have primarily emerged since 2010, and the field is still in its developmental stages.

In [9], a systematic literature review on IPv6 RPL classified IDS techniques and identified research gaps. However, it did not evaluate the practical effectiveness of these methods in real-world settings. In [10], RPL protocol attacks and solutions were reviewed, but it did not test the responsiveness and load adaptability of these solutions under different network conditions. In [11], RPL's advantages and disadvantages in IoT applications were discussed, along with a comparison of RPL-based protocols. The review, however, focused narrowly on RPL and overlooked other IoT routing protocols that could offer better alternatives.

In [12], a systematic review of 53 studies on RPL attack mitigation identified key strategies, with network monitoring being the most common. However, the review lacked a critical evaluation of the effectiveness of these strategies in various IoT scenarios. In [13], the review on load balancing in RPL evaluated various routing metrics. The drawback was the insufficient consideration of scalability and long-term performance in large-scale networks. In [14], a review study was conducted to examine 6LoWPAN packet formatting, security methods, available tools, and challenges in IoT, given its widespread use in wireless networks. The review highlighted that despite recent research advancements, key security challenges in 6LoWPAN networks remained unresolved. The drawback of this study was its limited exploration of practical, effective solutions for addressing these security issues. Table 1 indicates the relative analysis of RPL attacks and security schemes.

Table 1: Relative Analysis of RPL Attacks and Security Schemes

Ref	Review Focus	Range	Coverage	Demerits
[16]	A systematic review of IPv6 RPL and IDS techniques	103 papers from several sources	Classification of IDS methods and identification of research gaps	Did not analyze the practical impact or real-world applicability of IDS methods
[17]	Overview of RPL protocol attacks and countermeasures	Various studies on RPL protocols	Review of available solutions for RPL protocol attacks	Did not consider scalability or performance in diverse network scenarios

[18]	Examination of RPL's pros and cons in IoT applications	107 papers from several sources	Advantages, disadvantages, and RPL-based protocol comparison	Focused only on RPL, ignoring other potentially better IoT routing protocols
[22]	RPL attack mitigation strategies	53 studies reviewed	Key mitigation techniques; network monitoring commonly used	No critical evaluation of strategy effectiveness across diverse IoT scenarios
[23]	Load balancing in RPL through routing metrics	96 papers from several sources	Analysis of routing metrics for balanced load	Limited consideration of scalability and long-term performance in large-scale networks
[24]	6LoWPAN packet formatting, tools, security techniques, and IoT challenges	35 various studies on RPL protocols	Security aspects and tool support in 6LoWPAN for IoT	Limited exploration of practical and effective security solutions despite highlighting unresolved issues
Present Survey	The study reviews RPL attacks and defense strategies, analyzing routing datasets, testbeds, and simulation tools, while offering key insights for future research directions.	128 various studies on RPL protocols	This work introduces a new classification for RPL bouts and security, with influence breakdown, and explores relevant datasets, simulators, and real-time testbeds.	-

Several surveys on RPL-based IoT security have been published, yet each suffers from limitations that restrict their applicability. For instance, some studies provided a systematic review of IDS techniques for IPv6 RPL but did not evaluate their practical effectiveness in real-world environments. Similarly, other reviews identified key mitigation strategies such as network monitoring but lacked a critical assessment of their performance under diverse IoT scenarios. Earlier surveys either focused narrowly on specific attack classes (e.g., rank or repair attacks) or discussed RPL’s advantages without systematically analyzing defense mechanisms. Moreover, most prior studies were limited in scope, covering works only up to 2019 or 2020, and did not address emerging hybrid or cross-layer attacks. In contrast, our survey makes four distinct contributions. First, it introduces a comprehensive taxonomy of RPL-specific attacks, categorizing them into 12 families that capture both traditional and emerging threats (e.g., Sink-Clone, DAO induction, cross-layer, and hybrid attacks). This extends beyond the narrower classifications used in earlier works. Second, it proposes a novel taxonomy of defense mechanisms, organizing 8 strategic categories that unify IDS, ML, DL, cryptographic, and blockchain-based approaches, which prior reviews have only treated in isolation. Third, unlike existing surveys, this paper provides a systematic evaluation of testbeds, datasets, and simulators, highlighting their strengths and limitations for real-world deployment. Finally, this study covers a broader time span (2015–2025) and synthesizes 48 high-impact references, ensuring both state-of-the-art and future research directions are captured. Overall, by bridging gaps in prior reviews and extending the scope to practical evaluation platforms and advanced AI-driven defense strategies, our work offers a more comprehensive and practically relevant foundation for researchers and practitioners seeking to fortify RPL-based IoT networks against evolving security threats.

4. Methodologies for the Identification of RPL Attacks

Based on our systematic overview of the review, we introduce a more nuanced taxonomy to better categorize RPL-based routing attacks. In contrast to other efforts which categorized attacks by purpose; origin point; CIA security attributes; and RPL control messages our nomenclature is made using the inherent nature and behavior of the attacks themselves. By contrast, our nomenclature includes all the recent threats described in the literature, such as advanced ones like Induced Blackhole (BH), Coordinated BH, Buffer Reservation, DAO Induction, Multicast, Spam DIS Flooding, Dropped DAO, Energy Depletion, Hatchetman, Novel Partitioning, Divide and Conquer, Hybrid Attacks (e.g., Copycat and Sink-clone), and Cross-Layer Attacks (e.g., Rank Manipulation and Drop Delay).

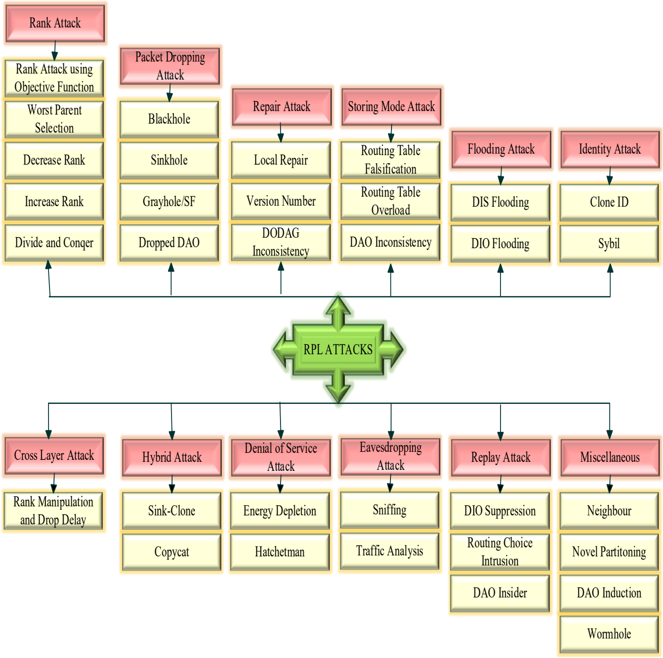

Figure 2: Nomenclature for RPL Attack Classification

The taxonomies proposed here, which have evolved to include 33 distinct attack types under 12 higher-level categories, as shown in Figure 2, better capture the essence of the more sophisticated attacks seen in recent times. Older surveys usually categorize attacks by their primary targets, e.g., network resources, topology, or data flow. While this method provides a high-level view of attack patterns, it fails to encapsulate the richness of newer threats. Most contemporary attacks on RPL target more than one component at a time; for instance, hybrid attacks tend to target both the topology and system resources. There are also cases where different attacks look almost the same, for instance, DAO insider, Dropping DAO, and DAO induction attacks, hence making it challenging to classify them based on conventional frameworks. To rise above these shortcomings, we present a novel nomenclature that classifies attacks based on their fundamental mechanisms, for example, whether or not they leverage rank manipulation or the local repair processes of RPL. The hierarchy also differentiates attacks based on techniques such as denial-of-service (DoS), flooding, replay, PL, or eavesdropping. We also extend our categorization by adding individual classes for hybrid, identity-based, storing-mode, and miscellaneous attacks. This new framework provides a more realistic model of how these threats work and hopes to assist researchers by offering a clearer and more applicable model for researching RPL security.

Conventional Studies Addressing RPL-Based Routing Attacks

Following the development of a refined nomenclature for RPL-based routing attacks, it is essential to examine how existing research has addressed these threats. Although the literature on RPL security is extensive and diverse, this review highlights only the most influential and methodologically significant studies across major attack categories, ensuring analytical clarity and avoiding redundancy. These representative works illustrate the evolution of RPL security solutions—from lightweight mitigation and collaborative defense mechanisms to advanced machine-learning-driven intrusion detection approaches—while also reflecting the growing focus on countering sophisticated, multi-vector threats that exploit multiple components of the protocol simultaneously. Taken together, these studies provide a concise yet comprehensive foundation for understanding current defense strategies and for identifying research gaps that motivate further investigation. The key representative studies for each attack category are summarized below.

Nandhini *et al.* [15] have formulated a rate-limiting approach to regulate the generation of DODAG Information Object (DIO) packets and utilized DODAG Information Solicitation (DIS) messages to separate potential rank attackers. In cases where an attacker evaded these initial measures, detection was achieved through a consistency check of the hash values within the Destination Advertisement Object (DAO) messages. Once an attacker was identified, an alarm was triggered. This alarm was embedded within the control message itself rather than sent as a separate packet. Osman *et al.,* [16] have determined the artificial neural network (ANN) model to detect decreased rank attacks, structured into three main phases: data pre-processing, feature extraction (FE) using a random forest (RF) classifier, and detection through the ANN model. The model was evaluated under both multi-class and binary classification scenarios using the IRAD dataset. In cases of data imbalance or limited diversity in attack patterns, the detection accuracy may decrease, potentially leading to misclassification or overlooked threats. Table 2 indicates the Analysis of Conventional Studies Related to Rank Attacks.

Albinali *et al.,* [17] have constructed the simulations across various network topologies, including grid and binary structures, to estimate the effect of local repair attacks on RPL protocol performance. The findings revealed that such attacks significantly degraded the protocol's efficiency. The binary topology experienced a noticeable reduction in PDR, while the grid topology was affected by a considerable increase in end-to-end delay. The evaluation focused on static topologies, which may not fully reflect the behavior of RPL under dynamic or mobile scenarios.

Rouissat *et al.,* [18] have established a modified edition of the flooding attack, known as the Destination Advertisement Object Flooding (DAOF), a lightweight solution was implemented, leveraging a straightforward collaborative mechanism among RPL nodes. This method was designated as DAOF-Secure RPL (DAOF-SRPL) and aimed to enhance the protocol's resilience against such flooding behavior. While the collaborative mechanism effectively addressed the flooding issue, it may introduce synchronization challenges with high node mobility or frequent topology changes.

Canbalaban *et al.,* [19] have emphasized the IDS leveraging neural networks to identify targeted attacks against the RPL protocol. In addition to utilizing features derived from the routing layer, the influence of link layer-related attributes on the effectiveness of IDS was also examined. Despite demonstrating promising detection capabilities, the system showed limitations in handling large-scale networks with high traffic variability, which impacted its scalability and detection accuracy under complex conditions.

Azzedin *et al.,* [20] have considered the effects of two energy depletion attacks—hello flooding and version number modification on the RPL protocol were analyzed, with a focus on their impact on network performance. A trust-based behavioral defense mechanism was developed to mitigate these threats. An extensive evaluation was conducted to assess how these attacks influenced radio energy consumption as the network scaled up in terms of nodes. Despite the mitigation strategy, the solution's effectiveness was influenced by factors such as potential delays in detecting malicious behavior.

Kim *et al.,* [21] have presented the fuzzy logic (FL)-based IDS, named FLSec-RPL, aimed at enhancing the security of the RPL protocol against specific attacks. The approach consisted of three main phases: first, it monitored activity-related variables to identify suspicious behavior; second, it applied fuzzy logic techniques to detect potentially malicious neighboring nodes; and third, it incorporated a screening and blocking procedure to accurately isolate both confirmed and suspected attacker nodes from the network.

Al-Sarawi *et al.,* [22] have established the Passive Rule-based Approach (PRBA) to identify sinkhole (SH) nodes in IoT networks operating with RPL. This method utilized three behavioral indicators: bi-directional (BD) behavior, BD frequent behavior, and power ingesting behavior. Despite its effectiveness, the approach may encounter limitations in dynamic network conditions or with energy-constrained devices.

Krari *et al.,* [23] have addressed the critical need for safeguarding IoT networks against routing table falsification attacks using the SecureGuard scheme. It uses Graph Neural Networks (GNNs) to perform adaptive analysis of dynamic network topologies. It was trained on labeled datasets comprising both benign and malicious instances, enabling it to identify subtle indicators of routing table manipulation effectively. However, its performance may be influenced by the quality and diversity of training data in large-scale deployments.

Morales-Molina *et al.,* [24] have employed rarely addressed identity-based threats known as the Clone ID attack, which targeted the RPL network. A Dense Neural Network (DNN) was simulated to enhance deep feature representation, aiming to improve the accuracy of classifying and identifying counterfeit attempts. However, the framework's performance may be influenced by the diversity and quality of the training data, potentially limiting detection under varied network conditions.

Mirshahjafari *et al.,* [25] have elucidated the hybrid attack combining SH and CloneID tactics, referred to as the "Sink-Clone" attack to assess its impact on the RPL network. The influence of this combined threat was analyzed and tested against a detection strategy that drew inspiration from existing identification mechanisms. While the detection method demonstrated potential, its efficiency may be affected by factors such as attacker behavior variation and network topology complexity, presenting a limitation in certain deployment scenarios.

Verma *et al.,* [26] have introduced the IDS known as CoSec-RPL to address the impact of non-spoofed copycat attacks on RPL networks. Its detection mechanism primarily relied on Outlier Detection (OD) to identify anomalous behavior. CoSec-RPL effectively reduced the negative influence of such attacks on holistic network capability. However, the approach may face limitations in handling adaptive or evolving attack strategies over time. Table 11 indicates the Analysis of Conventional Studies Related to hybrid Attacks.

Chinnakali *et al.,* [27] have emphasized the simulated network traffic generated through the Cooja Simulator for Sniffing attacks. Both benign and malicious scenarios were modeled to collect relevant data. This dataset underwent pre-processing before being applied to various ML algorithms. Feature selection was performed using the Chi-squared (chi2) method to reduce dimensionality and enhance model performance and ML-based classification models were implemented. However, the performance may vary with different feature selection methods or larger-scale networks.

Goel et al., [28] have determined the enhancement to the prevailing mitigation scheme (ERPL) to integrate a more operative detection mechanism for the Negative Acknowledgment Path Attack (NPA). The method authenticated DAO-ACK packets transmitted from PNs to client nodes to ensure their legitimacy. This improved approach, referred to as SecRPLNPA, was integrated and evaluated to assess its performance in securing RPL networks. However, its effectiveness might be reduced in highly dynamic topologies or the presence of multiple simultaneous attack types.

Table 2: Summary Table of Conventional Representative RPL Attack Studies

Ref	Category	Year	Scope	Attack Focused	Method Used	Performance assessment	Merits
[15]	Rank Attack	2023	RPL IoT networks	RA	E-RAD using DIO/DIS filtering and hash consistency in DAO	Energy utilized-1356J, PD delay-775ms, PDR-95.5%, accuracy-97.2%, packet overhead-1023	Early detection and isolation
[16]	Repair Attack	2023	RPL-based 6LoWPAN networks	Local Repair Attack	Simulation across grid and binary topologies	PDR-80%, end to end delay-2.2s, power utilized-40%	multi-topology testing
[17]	2023	RPL-based 6LoWPAN networks	Local Repair Attack	Simulation across grid and binary topologies	PDR-80%, end to end delay-2.2s, power utilized-40%		multi-topology testing
[18]	Flooding Attack	2025	RPL-based IoT networks	DAOF	DAOF-SRPL	PDR-98%, latency-0.92s, energy utilized-53.51J	Enhanced protocol resilience
[19]	Cross-Layer Attack	2020	RPL-IoT networks	Targeted routing and link-layer attacks	neural networks	Detection rate-97.06%, FPR-0.61%	Effective detection of complex intrusions
[20]	DoS Attack	2023	RPL-IoT	Hello flooding & Version Number Modification (Energy depletion attacks)	Trust-based behavioral defense mechanism	Average energy consumed-3.45%	Reduced radio energy drain
[21]	Replay Attack	2024	RPL-IoT	DIO Neighbor Suppression Attack	FLSec-RPL	EED (varying percentage of attacker nodes)-130–670ms, PDR-91–99%, First-time-detection-31-110s, detection accuracy-96–99%, average power consumption-3.17-4.09mW	allows nuanced threat evaluation

[22]	Packet Dropping	2023	RPL-IoT	SH attack	PRBA	Power utilized-0.90mW, detection accuracy-99%	Lightweight and passive
[23]	Storing Mode	2024	IoT networks with dynamic topologies	Routing Table Falsification	GNN trained on labeled datasets	Detection accuracy-97%	identifies subtle attack signatures
[24]	Identity Attack	2021	RPL-IoT	Clone ID Attack	DNN trained to detect counterfeit node identities	Accuracy-99.6%, F-score-99.6%	Enhances deep feature extraction
[25]	Hybrid Attack	2022	RPL-IoT	Sink-Clone (SH + Clone ID) Attack	Combined detection strategy based on ID-based threat identification mechanisms	TPR-90%, energy utilized-0.187mJ, power consumed-6.25 e -5	Enables detection of complex hybrid threats
[26]	Hybrid Attack	2023	RPL	Non-spoofed Copycat Attack	CoSec-RPL IDS with OD	average AE2ED-1.27s, PDR-0.97, accuracy-94%	Minimizes performance degradation
[27]	Eavesdropping	2024	6LoWPAN RPL Networks	Sniffing Attack	ML-based classification with chi2	Latency-3.1s, accuracy-0.97, precision-0.98, sensitivity-0.97, f-measure-0.97	Improved detection accuracy via dimensionality reduction
[28]	Miscellaneous	2024	RPL	Negative Acknowledgment Path Attack (NPA)	SecRPLNPA	Accuracy-98%, PDR-97%	Improved packet legitimacy validation

5. Defensive Mechanisms for RPL Attacks

The primary objective of this review was to provide an inclusive overview of RPL-based routing attacks and their corresponding defense mechanisms in IoT environments. Although limited studies have proposed organized classifications or taxonomies for countermeasures against RPL-based routing attacks, most current work has focused on IDS-based solutions. On the contrary, some high-profile surveys have emphasized general attack mitigation approaches more than IDS-specific methods. Within the framework of RPL security studies, various mitigation techniques, aside from IDS, have been considered. This has culminated in a rich taxonomy that divides defense approaches based on the inherent strategy into trust-based, specification-based, cryptographic, threshold-based, machine intelligence-driven, statistical, IDS-related, and miscellaneous categories. These general categories were then more specifically defined as mechanisms that the sources emphasized.

5.1. ML based Defensive Mechanisms

The defense approach was implemented using machine intelligence-based computational methods. These methods offered the advantage of rapid processing speeds, enabling quicker identification of potential attacks. This section outlines various defense strategies that utilize ML schemes to enhance network security:

Azzaoui *et al.,* [29] have presented the IDS with the RPL routing protocol by utilizing selected PNs as dispersed detection agents. A lightweight ANN model was embedded within these agents to identify malicious traffic while operating in coordination with a centralized monitoring system. Based on the topology established by the RPL, parent nodes were automatically designated as IDS agents. However, the federal coordination could pose a scalability concern and might become a bottleneck in large or densely connected networks. Kannan *et al.,* [30] have established the classification method using a combination of neural networks and genetic algorithms (NGCA). This NGCA effectively identified nodes responsible for RPL and other forms of attacks, thereby enhancing security within IoT networks. Experimental evaluation using the NSL-KDD dataset demonstrated that NGCA achieved higher detection accuracy compared to conventional classifiers. However, its performance might vary under different network conditions and datasets. effectively identified nodes responsible for RPL and other forms of attacks, thereby enhancing security within IoT networks.

Osman *et al.,* [31] have elucidated the Ensemble Learning-based IDS (ELG-IDS) utilizing assembling and rigorous parameter tuning to identify three specific RPL interior attacks: version number manipulation, decreased rank exploitation, and DIS flooding. The system incorporated advanced feature extraction methods along with genetic algorithm-based feature selection to enhance detection accuracy. Despite its improved performance, the approach may face challenges when applied to larger-scale or resource-constrained IoT environments.

Wakili *et al.* [32] have devised a machine-learning-based framework that unites Random Forest traffic classification, reinforcement learning-assisted adaptive routing, and an altered RPL objective function. Their method has revealed considerable enhancements in the metrics of QoS like latency reduction, throughput boost, and packet delivery ratio increase, while simultaneously identifying Rank, Sinkhole, and Wormhole attacks with a small number of false positives and quick reactions. Such a design of multiple layers not only secures RPL but also fosters a highly operationally efficient IoT-supported wireless sensor networks.

Lmkaiti *et al.* [33] present a metaheuristic optimization framework that incorporates PSO, MILP, ARS2A, and simulated annealing for the sake of securing RPL routing subject to Blackhole, Sinkhole, and Wormhole attacks. Their results showcased that ARS2A and MILP together brought down ETX (1.28), latency (0.12 ms), and energy consumption (0.85 J) to a significant extent, thus providing a balanced trade-off between real-time adaptiveness and computational efficiency. Also, the use of hybrid optimization in a secure and scalable IoT was brought into focus by the study. Table 14 indicates the Analysis of Conventional Studies Related to ML Defensive Mechanisms.

Table 3: Analysis of Conventional Studies Related to ML Defensive Mechanisms

Ref	Year	Scope	Attack Focused	Method Used	Performance assessment	Merits
[29]	2024	RPL-IoT	General malicious traffic	ANN with distributed parent node IDS agents	Energy utilized-2400J	Efficient detection with minimal resource usage
[30]	2024	IoT	RPL and generalized attacks	NGCA	ADR-99%, FPR-0.56	adaptive classification
[31]	2024	IoT	VN Manipulation, DR Exploitation, DIS Flooding	EL with stacking and GA	Average accuracy-97.90%	High precision via hybrid learning
[32]	2024	RPL-IoT	Rank, Sinkhole, Wormhole	Random Forest + Reinforcement Learning + Modified RPL Objective Function	High detection rate, reduced false positives, improved throughput and latency	Three-layer ML integration improves QoS and security simultaneously
[33]	2025	RPL-IoT	Blackhole, Sinkhole, Wormhole	Metaheuristics (PSO, MILP, ARS2A, SA)	ETX – 1.28, Latency – 0.12 ms, Energy – 0.85 J	Hybrid optimization provides security–performance balance

5.2. DL based Defensive Mechanisms

Berguiga *et al.,* [34] have contemplated the hybrid DL-IDS for boosting the shield of the RPL protocol in Internet of Medical Things (IoMT) networks. Referred to as HIDSRPL, the model integrated CNNs for extracting significant features with LSTM networks, which were commonly utilized for processing sequential data. The detection capability of this hybrid system was assessed using the CIC-DDoS2019 benchmark dataset. Despite its promising accuracy, the model showed certain limitations in terms of processing time and adaptability across heterogeneous IoMT environments. Ahmadi *et al.,* [35] have planned to address the susceptibility of the RPL protocol to various known routing attacks by introducing a trust-based identification framework. The expected behavior of network nodes was estimated using a learning framework trained on historical routing patterns, leveraging recurrent neural networks (RNNs). This approach enabled the identification of attacks with notable accuracy and precision. However, its performance may vary under dynamic network conditions and with limited historical data, indicating potential constraints in real-time adaptability.

KRARI et al., [36] have manipulated the innovative method for identifying the critical RPL VN attack within IoT networks by leveraging LSTM networks and DNN. Through training the LSTM and DNN models on this dataset, complex behavioral patterns linked to the attack were captured to enhance detection accuracy. Despite its effectiveness, the approach may encounter challenges in handling real-time constraints or adapting to evolving attack strategies without frequent retraining. Al Sawafi et al., [37] have formulated the integration of supervised and semi-supervised Deep Autoencoder–DLNN (DAE-DLNN) techniques to classify network traffic exhibiting both known and unknown abnormal behaviors within IoT environments. Although the model demonstrated promising classification performance, its adaptability to real-time traffic and broader attack variations remains a potential limitation. Kowsalyadevi, and Balaji [38] have encompassed the IoBTSec-RPL to recognize and classify numerous routing attacks in RPL-based networks. The framework followed four main stages: data preprocessing using min-max normalizer and imputation, feature selection via an enhanced pelican optimizer, class balancing with an auxiliary classifier gated adversarial network, and final classification using a combined LSTM and DBN. The model effectively captured complex attack patterns and demonstrated strong detection capabilities. However, scalability and real-time performance in large-scale dynamic IoT environments remained a challenge. Dey and Ghosh [39] have come up with iTRPL, an intelligent trust-aware RPL protocol that employs Multi-Agent Reinforcement Learning (MARL). Through this framework, parent nodes get to assign trust scores to their children, monitor their actions, and let the root know the scores for optimized DODAG reconfiguration. The experiments showed that iTRPL learns the best routing paths on its own, taking care of internal threats that regular authentication-based techniques overlook. Shivanajappa *et al.* [40] put forward a GNN-based IDS that utilizes GCNConv layers and was trained on the RADAR dataset to recognize RPL routing attacks. The model is capable of detecting both nodes. Table 15 indicates the Analysis of Conventional Studies Related to DL Defensive Mechanisms.

Table 4: Analysis of Conventional Studies Related to DL Defensive Mechanisms

Ref	Year	Scope	Attack Focused	Method Used	Performance assessment	Merits
[34]	2025	RPL-IoMT	General RPL Attacks	CNN + LSTM	Precision-98.5%, accuracy-99.7%, F1-score- 98.5%	captures spatial and temporal patterns
[35]	2024	IoT	General Routing Attacks	Trust-based RNN framework	Accuracy-99%, precision-99.2%	Accurately predicts abnormal behavior
[36]	2023	IoT	VN attack	LSTM + DNN	MAE-0.0072, MSE-0.0072, RMSE-0.085, R^2-0.96	Captures complex behaviors
[37]	2023	RPL-IoT	Known & Unknown Traffic Anomalies	Supervised + Semi-supervised DAE-DLNN	DR-98%, F-score-92%	good generalization
[38]	2023	Battlefield IoT	Multiple Routing Attacks	IoBTSec-RPL using LSTM + DBN; feature	Sensitivity-98.93%, accuracy-	Four-phase detection pipeline

				selection with Pelican Optimizer	98.1%, precision-98.46%	
[39]	2024	RPL-IoT	Insider attacks in DODAG	Trust-based Multi-Agent Reinforcement Learning (iTRPL)	Learns optimal decisions over time	Soft-security integration prevents insider threats
[40]	2024	RPL-IoT	General routing attacks	Graph Neural Network (GCNConv-based IDS)	High accuracy, precision, recall on RADAR dataset	Captures node/edge feature dependencies for improved detection

5.3. Trust based Defensive Mechanisms

Trust-oriented defense strategies function by building trust relationships among neighboring nodes using assigned trust values to counteract routing attacks. This section provides a comprehensive summary of such trust-based defense methodologies:

Remya *et al.,* [41] have outlined the Trust-IDS for RPL (TIDSRPL) was introduced in this study. This approach shifted the burden of complex trust evaluation tasks to the root node, which analyzed trustworthiness based on observed network activities. Such delegation effectively minimized the risk of resource exhaustion at individual nodes by conserving their energy, memory, and processing capabilities. However, reliance on a single root node may lead to a potential bottleneck failure under high traffic or targeted attacks. Mbarek *et al.,*[42] have presented a trust detection method to counter replication attacks in IoT environments, wherein multiple cloned nodes were deliberately added to evaluate the trustworthiness and reaction of witness nodes. However, the method's performance may vary depending on network density, and its reliance on witness node integrity may present limitations in highly compromised environments. Table 15 indicates the Analysis of Conventional Studies Related to DL Defensive Mechanisms.

Table 5: Analysis of Conventional Studies Related to Trust-based Defensive Mechanisms

Ref	**Year**	**Scope**	**Attack Focused**	**Method Used**	**Performance assessment**	**Merits**
[41]	2024	LLNs	General RPL Attacks	TIDSRPL: Hybrid Trust-based IDS with root node-based trust analysis LSTM	Accuracy-98.29%	Reduces node resource consumption
[42]	2024	6LoWPAN-IoT	Replication (Clone) Attacks	Trust evaluation via witness node monitoring and proactive trust scheme	Detection probability-90%, average run time-60s	Targets replication threats

5.4. Authentication and Encryption based Defensive Mechanisms

The subsequent sections explore defense mechanisms that rely on authentication techniques: Goel *et al.,*[43] have established the ightweight Challenge-Response Authentication-based method was developed to strengthen RPL protocol security against DDAO attacks. This mechanism, referred to as CRA-RPL, incorporated challenge-response pairs into modified control messages for authenticating DAO-ACK communications. Although it preserved the efficiency of resource-limited nodes, potential limitations may arise in large-scale deployments due to increased control message complexity. Zaminkar *et* *al.,* [44] have introduced the hybrid encryption was utilized to address security challenges in the RPL-LLNs. The method, referred to as Detection of SH in RPL (DSH-RPL), involved four key stages. Initially, it established a reliable RPL structure. Subsequently, it identified sinkhole attacks within the network. The third stage involved isolating the compromised node, followed by the final phase where data transmission occurred with encryption for added security. While the approach strengthened protection against sinkhole threats, its performance could vary depending on dynamic topology changes and energy constraints. Table 16 indicates the Analysis of Conventional Studies Related to DL Defensive Mechanisms.

Table 6: Analysis of Conventional Studies Related to Authentication and Encryption-based Defensive Mechanisms

Ref	Year	Scope	Attack Focused	Method Used	Performance assessment	Merits
[43]	2024	LLNs	General RPL Attacks	TIDSRPL: Hybrid Trust-based IDS with root node-based trust analysis LSTM	Control packet overhead-4100, average power consumed-4.6mW	Reduces node resource consumption
[44]	2024	6LoWPAN-IoT	Replication (Clone) Attacks	Trust evaluation via witness node monitoring and proactive trust scheme	DR-96%, FNR-10.98%, FPR-13.6%, PDR-98%	Targets replication threats

5.5. Threshold based Defensive Mechanisms

Threshold defense mechanisms relied on either static or dynamic threshold values to identify abnormal network behavior. This subsection outlines various approaches that employed threshold-based strategies for IDS and mitigation:

Rajasekar et al., [45] have formulated the Adaptive Threshold-based IDS to counter selective forwarding attacks (SFAs) in the RPL 6LoWPAN scenario. The architecture included four core modules: Pre-emptive analysis, acquisition module, interpreter, and attack handler, each comprising sub-modules. It employed sub-tree monitoring, adaptive threshold calculation based on environmental factors, and dissimilarity metrics (θ, β, δ). Limitations included potential complexity in dynamic environments and added latency in group analysis. Kharrufa et al., [46] have interpreted the game-theoretic scenario in which nodes competed selfishly for network components to transmit their data packets to the sink node. An optimized protocol, referred to as Game-Theory-Based Mobile RPL (GTM-RPL), was executed and evaluated across various scenarios with differing component necessities suitable for IoT applications. However, the non-cooperative nature of the model might not effectively capture collaborative behavior in certain network environments, limiting its applicability in some real-world deployments. Table 17 indicates the Analysis of Conventional Studies Related to DL Defensive Mechanisms.

Table 7: Analysis of Conventional Studies Related to Threshold-based Defensive Mechanisms

Ref	Year	Scope	Attack Focused	Method Used	Performance assessment	Merits
[45]	2024	RPL-based 6LoWPAN	Selective Forwarding Attack	DSAT-IDS	TPR-99.12%, PDR-99.52%, throughput-99.1%, FPR-1.05%, FNR-2.16%, average energy consumed-19000mJ	Adaptive detection with sub-tree monitoring and environmental thresholds

[46]	2018	Mobile RPL for IoTs	Resource Misuse	GTM-RPL	Delay-5.8s, energy consumed-55mJ/packet	strategic behavior modeling for resource efficiency

5.6. GINI Index and Attack Graph based Defensive Mechanisms

The subsequent sections explore defense mechanisms that rely on the Gini index and attack graph-based techniques:

Hassan *et al.,* [47] have established the fog-enabled trust mechanism based on the Gini index, referred to as GITM, to counter Sybil attacks by analyzing the advancing comportment of legitimate nodes. This method effectively identified and isolated a greater number of malicious nodes within the network associated with similar techniques, all within a comparable time frame. However, the accuracy of GITM relied heavily on consistent forwarding patterns, which could be influenced by network congestion or topology changes. Sahay *et al.,* [48] have elucidated the construction of an Attack Graph for the susceptibilities of the rank property in the RPL protocol. This graph was developed by analyzing various potential threats associated with the manipulation of rank values. Several key observations were also presented to support the development of methods aimed at preventing the exploitation of rank-related vulnerabilities. However, implementing preventive measures based on these observations could introduce additional overhead and may require frequent updates to remain effective against evolving threats. Table 18 indicates the Analysis of Conventional Studies Related to the Gini index and attack graph-based Defensive Mechanisms.

Table 8: Analysis of Conventional Studies Related to Gini Index and Attack Graph-Based Defensive Mechanisms

Ref	Year	Scope	Attack Focused	Method Used	Performance assessment	Merits
[47]	2023	RPL-AMI	Sybil Attack	GITM	Power utilized-4.10mW	Effectively isolates more malicious nodes with minimal delay
[48]	2018	RPL-6LoWPAN	Rank Property Attacks	Attack Graph	Isolation latency-4s, number of control messages-12100, energy utilized-0.07mJ	Identifies rank manipulation threats

5.7. Learning Automata and BC-based Defensive Mechanisms

The subsequent sections explore defense mechanisms that rely on learning automata and BC-based techniques:

Homaei *et al.,* [49] have propounded the DDSLA-RPL decision system by evaluating qualitative parameters. Child nodes were informed of their potential links to these available parents. In the routing process, a learning automata-based decision system was utilized to energetically adjust and upgrade the weights of influential routing parameters. However, it relied heavily on real-time parameter estimation, which could be affected by unstable network conditions. Additionally, the computational complexity of learning automata might introduce latency in low-power IoT devices. Abdulkareem *et al.,* [50] have presented the BC with the VGG16 scheme to ensure data privacy and secure message transmission. Initially, network fabrication was carried out to optimally position the Mr. Fixit nodes and adapt to network dynamics using the Bettered Remora Algorithm (Be-Remo). Following this, the RPL topology was registered at the Dutiful Advisor (DA) by submitting relevant parameters, after which the DA issued secret keys to nodes via the Boosted CHACHA algorithm (B-CHACHA). The root node in the RPL then propagated DIO messages, allowing each node to choose its parent based on various optimal metrics through the Be-Remo mechanism. These requirements may limit deployment in resource-constrained IoT environments, and real-time responsiveness could be affected under high network load or frequent topological changes. Table 19 indicates the

Analysis of Conventional Studies Related to learning automata and BC-based Defensive Mechanisms .

Table 9: Analysis of Conventional Studies Related to Learning Automata and BC-based Defensive Mechanisms

Ref	Year	Scope	Attack Focused	Method Used	Performance assessment	Merits
[49]	2021	RPL-QoS Routing	Not attack-specific	DDSLA-RPL	Throughput-0.89, PDR-0.99, control overhead-510, energy utilized-47.8J	Adaptive routing via dynamic weight updates
[50]	2024	RPL-BC-IoT	Hybrid & Collaborative Attacks	Blocollab: VGG16 + Blockchain + Be-Remo + B-CHACHA	Energy utilized-35%, latency-1300ms, accuracy-99%, number of DIO received-27	Enhances privacy and secure routing via optimized topology

6. Assessment Frameworks and Data Resources

This section describes the tools, simulators, and datasets that are generally used to assess security mechanisms in RPL-based networks.

6.1. RPL Attack Datasets

Multiple datasets have been constructed to facilitate RPL-based security threat research. These include synthetic or typical (i.e., publicly shared for research purposes) datasets representing diverse attack scenarios. Table 20 provides prominent RPL attack datasets along with key parameters such as dataset name, type (synthetic or typical), including attacks, a record number (benign and malicious), and a simulation platform utilized to generate the dataset.

Table 10: RPL Attack Datasets

Year	Dataset Name	Attack Types Addressed	Record Count	Attributes	Sample Count (Benign / Malicious)
2018	IRAD	VN, Decreased rank, and HF	9520795	116	3,395,601 / 6,125,194
2019	RPL-ND2017	Clone ID, Local repair, HF, Selective forwarding, SH, BH	465318	22	431,083 / 34,235
2019	IoT-RPL	HF and VN	-	14	-
2021	2-Class/multi-class	Clone ID, SH, Selective forwarding, HF, RA	106122796	91	-
2020	Routing Attack Dataset for IoT	Version number, Hello flood, Wormhole	27	-	-
2020	IoT-DDoS	Selective forwarding, SH, Flooding	4198537	16	-
2020	IoT-ID	Decreased path rank, Selective forwarding, SH	-	24	-
2021	RADAR	BH, SH, Clone ID, Hello flood, Rank manipulation, Wormhole, Version, etc.	-	-	15
2021	IDC and EDC	Hello flood, Rank, Version number	4029537	206	-
2021	DDoS Dataset	Clone ID	1279213	-	812,702 / 466,511

2021	RPL Attack Dataset	Version number	1279213	17	812,702 / 466,511
2021	IRA-IoT	SH, BH, Clone ID, Rank attack, DoS, DIO suppression, etc.	1023336	35	503,173 / 520,163
2023	RPL-IoT2023	SH, DoS, Flooding, BH, etc.	380772	23	-
2023	ROLTA-2023	BH, Rank decrease, Flooding, DoS	1639992	16	-
2024	DA-RPLRouting	Hello flood, Rank decrease, DoS, SH, Version number	536000	16	-
2024	UOS_IOTSH_2024	SH	1771860	14	59,370 / 1,712,490

Dataset Characteristics in Existing Studies

Recently, there have been advancements in RPL-based IoT datasets that have not only been more sophisticated but also have shifted the focus from simple packet traces to flow-level behavioral characteristics [51]. One of the most frequently cited datasets is the IoT-RPL 2021 Cyber-Attack Dataset. This dataset was produced with the Cooja simulator in a 6LoWPAN setup and comprises imitation routing-layer threats such as Blackhole, Flooding, Version Number manipulation, and Decreased Rank attacks. The dataset also offers a systematic basis for testing traditional machine-learning models [52].

The dataset driven by the simulation is capable of capturing behavioral representation that is richer than what the packet-level datasets are providing, allowing the use of models like autoencoders, graph attention networks, and reinforcement-learning frameworks to learn complex attack patterns. At the same time, large-scale and realistic datasets such as UOS_IOTSH_2024 [53] and the RPL-IDS Behavior Dataset are coming up that provide multi-topology scenarios, and routing-layer anomalies that contain DIS flooding, rank manipulation, and selective forwarding as well. Recent studies have cited benchmark datasets like ROUT-4-2023 [54], which keep on providing the evaluation of classical ML-based RPL intrusion detection. All of the above datasets signify a distinct shift from the small, attack-specific packet datasets to the more realistic, behavior-rich flow-level datasets that are crucial for today's ML/DL-based IDS research in RPL-enabled IoT environments.

6.2. IoT Simulation Environments

IoT testbeds are real-time environments that provide the facility to develop, deploy, debug, and test IoT applications. IoT testbeds provide researchers the ability to run solutions on actual hardware, supporting end-to-end monitoring of IoT device behavior and performance analysis of target systems. Table 21 provides a comparative summary of the most notable IoT testbeds for RPL-based applications. It indicates main parameters like types of access, user interfaces, number of nodes, supported hardware, programming languages, and operating systems.

Table 11: IoT Simulation Environments for RPL-based Applications

Testbed Name	User Interface	No. of Nodes	Programming Language	Hardware Used
WISEBED	GUI, CLI	550+	C	MicaZ, iSense
LOG-a-TEC	Web	200+	Java, C	VESNA ARM Cortex
FIT IoT-LAB	Web, REST, CLI	2728+	C	M3 ARM Cortex
NetSeCof	CLI	-	Python	Raspberry Pi
INDRIYA2	CLI	95	C	TelosB
TUTORNET	GUI	-	C, Perl, PHP	SunSPOT, MicaZ

CCI IoT	GUI	-	-	Raspberry Pi, ARM Cortex A53

6.3. Performance Indicators

Some commonly used metrics to evaluate RPL-based IoT networks, especially in the context of security and defense mechanisms are deliberated as follows:

End-to-End Delay (EED)

EED measures the average time taken for a data packet to travel from the source to the destination across the network. It reflects the responsiveness and latency of the network.

$$EED = \frac{\sum_{i=1}^{N}\left(T^{i}_{arrival} - T^{i}_{sent}\right)}{N} \quad (1)$$

Here, $T^{i}_{arrival}$ represents the time at which the i^{th} packet arrives at the destination, T^{i}_{sent} manipulates the time at which the i^{th} packet was sent, and N symbolizes total number of successfully received packets.

Energy Consumption (EC)

It quantifies the amount of energy used by a node or the entire network over a specific duration, especially relevant in low-power IoT environments.

$$EC = \sum_{i=1}^{n} P_i \times t_i \quad (2)$$

Here, P_i manipulates the power consumption of the node during i^{th} activity, t_i contemplates the duration of the activity, and n signifies the number of distinct energy-consuming operations.

Packet Delivery Ratio (PDR)

PDR is the ratio of the number of packets successfully delivered to the destination to the number of packets sent by the source.

$$PDR = \left(\frac{packet\ recieved}{packets\ sent}\right) \times 100 \quad (3)$$

Packet Loss Ratio (PLR)

PLR indicates the proportion of packets that fail to reach their destination due to network failures, attacks, or congestion.

$$PLR = \left(\frac{packet\ lost}{packets\ sent}\right) \times 100 \quad (4)$$

Throughput

Throughput is the rate at which data is successfully transmitted over the network, usually measured in bits per second (bps).

$$Throughput = \left(\frac{\text{Total data received (in bits)}}{Total\ transmission\ time\ (in\ seconds)}\right) \times 100 \quad (5)$$

Detection Rate (DR)

In the context of attack detection, this metric indicates the proportion of actual attacks that are correctly identified by the security mechanism.

$$DR = \left(\frac{T_p}{T_p + F_n}\right) \times 100\% \quad (6)$$

False Positive Rate (FPR)

The rate at which legitimate actions are incorrectly identified as malicious by the IDS framework.

$$FPR = \left(\frac{F_p}{F_p + T_n}\right) \times 100\% \quad (7)$$

Power Utilization (PU)

It represents the average power consumed per node over the network's lifetime, crucial for energy-constrained IoT deployments.

$$PU = \frac{Total\ energy\ consumed}{time\ \ duration} \quad (8)$$

Control Packet Overhead

This metric refers to the proportion of control packets (e.g., RPL DIO, DAO, DIS) to total packets transmitted, impacting network efficiency.

$$Control\ \ overhead = \left(\frac{\text{Number of Control Packets}}{\text{total packets sent}}\right) \times 100\% \quad (9)$$

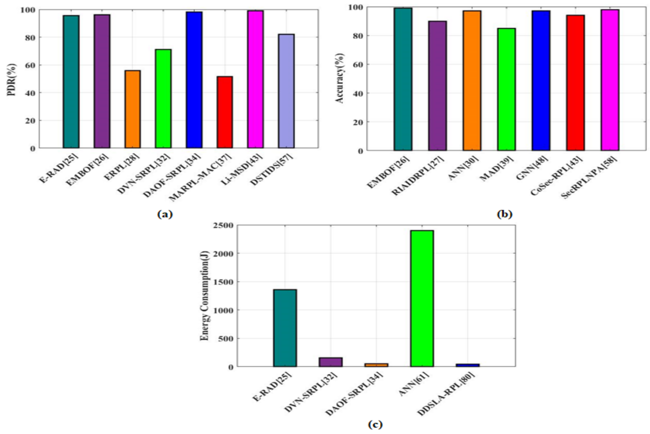

Figure 4: Comparative illustration of (a) PDR, (b) Accuracy, and (c) EC

The outcomes depicted in Fig. (a) illustrate that the greater part of the enhanced RPL schemes get very high PDR, with a number of methods getting nearly 100%. As shown in Fig. (b), the assessed intrusion-detection and secure-routing methods are still very strong in terms of accuracy, being the least 85-95%. The analysis shown in Fig. (c) points out the energy consumption in the drastic way where the lightweight optimization-based models consume way less energy than the heavier ANN-based ones. Simply, all three figures give testimony that even though a good number of RPL enhancements are still very reliable and accurate, their power consumption varies with the degree of their computational complexity.

6.4. Modeling Tools

Simulators are one of the important tools of research and development that provide a simulated version of reality to support experimentations and training without requiring actual deployment. In RPL-based IoT networks, various influential network simulators have been utilized by researchers for performance analysis, protocol testing, and attacking simulations. Table 22 provides a comparative summary of top RPL simulators, including information regarding simulator type, licensing schemes, RPL conformity, programming language, supported operating systems, and available interfaces.

Cooja is undoubtedly the go-to RPL simulator for many researchers, with more than 90% of them relying on it [27]. It is a Java simulator that comes with Contiki-NG and allows for real mote emulation (like Z1 [55]), supports major RPL modes, and allows for the use of objective functions such as OF0 and MRHOF. NetSim [56], a simulator that is licensed by TETCOS, can simulate up to 500 sensor nodes in wired, wireless, and mobile scenarios. It also allows users to configure it through a GUI, to integrate it with MATLAB [57], to animate packets, and to make trace logs of the communication. However, the RPL support in this simulator is limited and does not offer features such as DODAG repair, energy profiling, and memory analysis. NS-3 [58] is a powerful simulation platform that is open-source and has an RPL module that is capable of handling IPv6 routing, OF0, and MRHOF, but it does not have much support for energy models, mobility and custom objective functions by default. It is kept up to date with developments in standards such as 802.15.4 and 6LoWPAN. OMNeT++ [59] provides simulations that can be scaled according to the INET framework with RPL functionalities like handling the parent table and source routing being the only ones offered, though, still, there is confusion about the configuration and instability at times. TinyRPL [60], which uses TinyOS and BLIP, is evidence of the early support for RPL with OF0 and MRHOF, but it only works with upward routing, one instance ID, and no GUI and no scalability.

6.4.1 Critical Evaluation of Simulators

Each of the simulators has its distinct strengths and weaknesses on various dimensions, as outlined below:
Cooja has comprehensive documentation, GUI support, and mobility and energy analysis functions, but it is sluggish with big networks, and there are no built-in attack scenarios. NetSim, on the other hand, has a polished interface and internal monitoring; nevertheless, it is a paid product with limited RPL functionalities and no energy, memory, and attack simulation features. NS-3 is the most prominent in scalability and open-source with sophisticated logging, but on the other hand, it has a steep learning curve and limited default support for mobility, energy, and attack modules. OMNeT++ is another option that is flexible and scalable but requires great effort in the manual configuration process and still faces the challenge of an immature RPL implementation without physical-layer or attack modeling. TinyRPL is offering the very basics of the early RPL technology that has very limited functionalities and no GUI, scalability, and support for attacking or real-world modeling at all.

The future IoT simulator's attack libraries must be modular (with attacks like Rank, Sybil, Sinkhole) and hybrid scalability should be for both small and large networks. They should also provide detailed profiling of power, memory, delay, throughput, and PLR along with realistic IoT environments that consist of heterogeneous devices, channel noise, mobility, obstacles, and the emerging technologies like 5G, LoRaWAN, and NB-IoT.

Besides, both GUI and CLI interfaces must be provided to meet the needs of users at all levels thus making RPL research more accurate, scalable, and security-focused.

Table 12: RPL Modelling Tools

Ref	Simulator Type	Licensing	Programming Language	User Interface
[27]	Discrete-event	Open source	C language	GUI and CLI
[56]	Research-based	Licensed	C language	GUI
[58]	Discrete-event	Open source	C++ and Python	GUI and CLI
[59]	Discrete-event	Open source	C++ and NED	GUI
[60]	–	Open source	C language	–

6.5. Research Challenges

In spite of the many defense measures evolved to mitigate RPL-based routing attacks, some open challenges persist as a result of the characteristic confines of RPL and the limited nature of IoT settings. These limitations, such as limited power, memory, and processing power, necessitate that any security process needs to be lightweight and non-intrusive to prevent causing protocol performance degradation. Future research shall consider these shortcomings while formulating stronger and better security frameworks. Two important lines of research discussed below are as follows:

6.5.1 Unaddressed Security Features of RPL

The RPL protocol, defined in RFC 6550 [61], specifies three operating security modes: unsecured, preinstalled, and authenticated. Yet, these security modes are typically viewed as optional, and to this day, there has not been a complete implementation or field testing of all these modes in any study. Most works so far avoid using the built-in security modes and instead use external means for threat detection or prevention. This absence of usage and testing creates a knowledge gap regarding how effectively RPL's own security architecture fares under real-world conditions. Accordingly, future effort should be spent on completely installing and benchmarking these in-built security features on actual deployments and studying their influence on network efficiency, scalability, and resilience against different attacks.

6.5.2 Security in RPL-Based Mobile Networks

The majority of current RPL defense mechanisms have been developed with static or little dynamic networks. Yet, most current IoT applications involve mobile nodes, e.g., in smart transport, healthcare, or industrial automation, where the movement of devices greatly complicates the maintenance of secure and dependable communication. Node mobility may result in frequent disconnections of links, higher packet collisions, and lower PDR, all of which render the environment unpalatable to both routing and attack detection. Additionally, mobility brings special attack possibilities and renders classical intrusion detection methods less efficient because of changing topologies at all times. Hence, there is a vital necessity for security explanations that are vigorous in mobile environments, dynamic in adapting to changes in the network and tuned for sustaining the performance and integrity of mobile RPL deployments.

6.6. Emerging Technology-Based Security Solutions

As IoT networks grow in size and complexity, emerging technologies such as machine learning (ML), software-defined networking (SDN), blockchain (BC), and next-generation communication systems are being explored to enhance the security of RPL-based environments. However, their application against RPL-specific routing attacks remains limited.

ML: ML is increasingly used in IoT security but introduces new vulnerabilities, such as adversarial attacks that manipulate input or poison datasets to deceive models. Future security solutions should explore Generative Adversarial Networks (GANs) and self-supervised learning to build robust models capable of detecting and mitigating AI-based attacks. Integration of explainable AI is essential to ensure transparency in dataset handling, model decisions, and algorithm behavior, thereby fostering trust in ML-based security.

SDN: SDN enables centralized management and network programmability, making it suitable for intrusion detection in RPL networks. Scalable SDN-based frameworks can dynamically enforce security policies and detect RPL routing or anomaly attacks in large-scale IoT deployments.

BC: Blockchain provides a decentralized and tamper-evident approach to managing trust and security in IoT networks. Combining BC with deep learning and smart contracts allows attack-related data to be stored securely and anomalies to be detected intelligently. Future work can focus on optimizing BC scalability and integrating lightweight cryptography suitable for resource-constrained IoT devices.

6G-Based RPL Networks: Integrating RPL with 6G communication frameworks offers ultra-reliable, low-latency, and high-throughput networks with energy efficiency for low-power IoT devices. Key challenges include ensuring secure and efficient data transmission. Research directions may include secure communication protocols, energy harvesting methods, and data security mechanisms specifically designed for 6G-enabled RPL systems.

Metaverse Applications: Metaverse environments rely on extensive IoT sensors and devices to create immersive virtual worlds, where RPL is critical for connectivity. Security threats such as Sybil attacks can generate false digital avatars and disrupt interactions. Investigating RPL-specific defenses for Metaverse IoT networks is an important area for future research.

Smart Factories and Industry 4.0: In smart factories, RPL supports communication among sensor nodes for monitoring, cloud-based analytics, and automated decision-making. Security breaches in RPL can cause operational failures, downtime, or physical damage. Future work should focus on designing robust RPL defense mechanisms to ensure high availability, reliability, and safety in industrial environments.

6.7. New RPL Routing Attack Dimensions

The investigation of various RPL routing attacks has been done but there are still new ones and less studied attacks that give room to significant research work:

Unexplored Attacks: There are still some M2M-layer attacks and some of the RPL-exclusive attacks like the existing unavailability due to BH attacks, DIO flooding, Hatchetman attacks, DIO suppression, DAO insider, and routing table falsification that have not been fully researched hence the need to come up with detection and mitigation strategies specifically tailored to them to be effective in practice.

Coordinated Attacks: The activation of a coordinated attack can come from a well-planned arrangement of the compromised nodes within the entire network, and this can lead to getting rid of some large sections of the network. Coordinated attacks understanding and developing countermeasures that are adaptable are key.

Hybrid Attacks: At the same time, solutions like Copycat and Sink-Clone are considered to emulate the normal behavior while doing the attacks. Thus, the hybrid attacks in future will expose shortcomings in the present defenses and will aid in developing the future security with more immunity.

Cross-layer Attacks: Cross-layer attacks, which take advantage of weaknesses across the whole system from the application down to the physical layer, are a major threat. The existing few studies on this are an indication of the urgency of developing global attack prevention, detection, and classification systems that can handle the multi-layer threat.

It is very important to focus on these new forms of attack so that RPL IoT networks remain resilient, secure and trustworthy.

7. Prominent Future Research Directions in the Context of RPL

This section emphasizes a few of the largest areas of future research in RPL (Routing Protocol for Low-power and Lossy Networks) with the hope of mitigating forthcoming challenges in IoT and sensor-based systems. These paths strive to make the protocol more efficient, dependable, and adaptable in dynamic resource-scarce environments.

Energy Efficiency and Resource Optimization: Develop routing metrics that are sensitive to energy usage and power consumption with consideration of battery status, network density, and traffic load. Control radio duty cycles and Trickle timers so as to have a good mix of responsiveness and energy usage.

Enhanced Security: Create easy-to-implement cryptographic algorithms, trust-based routing, and data integrity procedures that can prevent RPL from succumbing to such attacks as ranking spoofing and DODAG inconsistency.

Mobility Support: A seamless running for mobile IoT applications (like drones, self-driving cars, and wearables) will be possible by means of the application of mobility-aware metrics, route stability, and quick DODAG reconfiguration.

RPL in 6G and Next-Generation Networks: Modify RPL to take advantage of ultra-low latency, high throughput, network slicing, and edge computing in 6G, hence, improving the performance of the heterogeneous network.

Context-Aware and Adaptive RPL: Apply machine learning and adaptive metrics to route dynamically based on factors such as node energy, network traffic, and environment.
Renewable Energy Integration: Nodes that have solar, wind, or ambient energy sources shall be given priority and prediction of energy availability will be done so as to prolong the network's lifetime and sustainability.

Time-Sensitive Applications: Routing and switching of the traffic will be done in a controlled manner and multi-channel communication will be made more effective to cope with industrial automation and healthcare requirements that are very sensitive to latency.

Data Aggregation and Compression:
Communication will be made less costly and energy will be saved while bandwidth usage will be improved by the implementation of data aggregation and compression mechanisms.

Sequence-Based Deep Learning and Optimization: Temporal patterns in control messages of routing protocol for low-power and lossy networks (RPL) will be captured, routing optimized, and attacks like VM manipulation, DR exploitation, and DIS flooding detected by the use of LSTM, LSTM-DBN and hybrid ensemble frameworks along with metaheuristic feature selection techniques (e.g., PSO, MILP, ARS2A).

Graph-Based and Reinforcement Learning Models: Topology-aware intrusion detection, adaptive policy optimization, DODAG stabilization, and context-aware mitigation in dynamic networks will be done using graph neural networks (GAT, GCNConv) and reinforcement learning.

Integration of Hybrid Methodologies: The combination of sequence-based, graph-learning, and reinforcement-driven approaches will result in better energy efficiency, robustness, and large-scale RPL security, thus providing a coherent methodological foundation for future IoT-RPL research.

Together, these directions will not only make RPL more resilient and scalable but also energy-efficient and secure in the face of increasingly complex IoT environments.

8. Integration of prior Works into Methodological Foundations

A careful review of existing literature indicates that the methodological basis of this survey draws primarily from two major research directions, each representing a distinct stream of prior work that informs the foundations of RPL-based intrusion detection and attack classification.

Sequence-Based Deep Learning and Optimization-Driven Feature Engineering
The initial methodological direction is formed through research that uses deep learning models for temporal pattern extraction plus meta-heuristic feature-selection techniques. Studies such as Krari et al. [36], which applies LSTM architectures for depicting sequential routing behavior, and the combined LSTM–DBN framework suggested by Kowsalyadevi and Balaji [38], emphasize the significance of discovering temporal relations in RPL control-message sequences. In addition, optimization-focused defense measures such as the metaheuristic-based secure routing architecture proposed by Lmkaiti et al. [33], are able to show the potential of Particle Swarm Optimization (PSO), MILP, ARS2A, and Simulated Annealing in attacking scenarios by means of minimization of ETX, latency, and energy consumption. These trends highlight the importance of feature selection, routing in constrained resources, and large-scale optimization in the implementation of RPL networks. Similarly, Osman et al. [31]demonstrated that hybrid ensemble learning with GA-based feature selection can effectively detect VN manipulation, DR exploitation, and DIS flooding with high accuracy.

Collectively, these works establish the methodological base for:

- Selecting salient RPL features
- Handling large-scale, high-dimensional traffic logs
- Improving classification robustness under constrained IoT resources.

- Integrating temporal modelling with optimized preprocessing pipelines.

Graph-Based Learning and Adaptive Reinforcement-Driven Decision Models

A second methodological stream emerges from studies using graph learning paradigms and reinforcement-driven adaptation. Graph Attention Network (GAT)–based frameworks (e.g., Wang et al.,[62]) demonstrate strong capability in capturing the relational dependencies embedded in RPL's hierarchical topology and multi-hop parent–child structure. Simultaneously, the GCNConv-based intrusion detection models proposed by Shivanajappa et al. [40] provide additional support for the effectiveness of graph neural networks in learning the interactions between edges/nodes in multi-hop IoT routing.

Moreover, the mechanisms powered by reinforcement learning—such as the one by Wakili et al. [32], which combines Random Forest classification with adaptive RL-based routing, and iTRPL by Dey & Ghosh [39], which employs multi-agent RL with trust evaluation—illustrate the importance of reward-driven decision systems that dynamically stabilize DODAG structures and alleviate insider routing threats. These contributions inform modern detection architectures by enabling:

- Topology-aware intrusion modelling through graph embeddings
- Online and adaptive policy optimization
- Improved energy efficiency and context-aware mitigation
- resilient detection performance under dynamic routing changes.

By situating the current review within these two dominant methodological streams, the paper identifies how emerging research trends connect sequence-based deep learning, meta-heuristic feature engineering, graph-learning paradigms, and reinforcement-driven adaptation providing a coherent academic foundation for subsequent model development in IoT-RPL security research.

8.Conclusion

This survey provides an in-depth groundwork for RPL-based security solution design in IoT networks. It provides a systematic categorization of attacks and defense mechanisms, a complete overview of RPL-based routing threats, their impact on real-world applications, and an overview of related datasets, testbeds, and simulators. The survey categorizes attacks according to their exploitation techniques and strategic impact, which provides key RPL protocol vulnerabilities. Among the listed threats, the VN attack was the most disruptive with respect to the severity of energy and routing stability. Rank increase attacks, on the contrary, had rather a low impact, especially on the PDR. Most defense mechanisms are based on RPL specification modifications, while cryptographic methods are not so frequent owing to resource constraints and high overhead in constrained environments. PDR, energy consumption, and detection rate were identified by the survey as the first three performance metrics that are utilized to measure defense measures. IRAD, RADAR, and RPL-NIDDS17 are some of the most widely used datasets that have been expansively exploited for security evaluation based on ML and DL. CICIOT and FIT-IoT LAB are also widely used testbeds familiar to provide high functionality and ease of access for testing purposes concerning RPL. The COOJA simulator is still the most used tool for testing defense mechanisms because of its open nature and full RPL compliance. Hybrid attacks, cross-layer attacks, and other so-called untapped or untapped threats are recent areas of interest. More attention is being drawn to the creation of AI-powered security solutions to facilitate real-time threat detection and adaptive defense techniques. The research problems identified and directions outlined in this article are a good point of reference for future work in the development of improved and scalable defense for RPL in the emerging IoT environment. Last, while this survey provides a good theoretical framework, the absence of experimental proof-of-concept demonstration and verification of RPL-based attacks and defense is a limitation. Compared with existing reviews, this survey offers a broader scope and deeper analysis. Unlike prior studies that either focused on limited attack classes or overlooked evaluation platforms, our work provides a unified taxonomy of 12 RPL attack families and 8 defense categories, coupled with a systematic assessment of testbeds, datasets, and simulators.

Additionally, our study reveals that two methodological streams sequence-based deep learning with optimization with meta-heuristic techniques, and graph-learning with reinforcement-driven adaptation are increasingly shaping advancements in RPL security. Future IDS models may become more resilient, context-aware, and more adapted to the hierarchical structure of RPL by incorporating findings from these methods. This connection between methodological advances and protocol challenges provides a clear foundation for developing next-generation RPL security solutions. The future work shall focus on real-world experimentation to bridge this gap and make the proposed solutions more reliable.

References

[1] H. Albinali and F. Azzedin, "Replay attacks in RPL-based Internet of Things: Comparative and empirical study," *Comput. Networks*, vol. 257, p. 110996, 2025.

[2] A. K. Prajapati, E. S. Pilli, R. B. Battula, V. Varadharajan, A. Verma, and R. C. Joshi, "A comprehensive survey on RPL routing-based attacks, defences and future directions in Internet of Things," *Comput. Electr. Eng.*, vol. 123, p. 110071, 2025.

[3] N. A. Alfriehat, M. Anbar, S. Karuppayah, S. D. A. Rihan, B. A. Alabsi, and A. M. Momani, "Detecting version number attacks in low power and lossy networks for internet of things routing: review and taxonomy," *IEEE Access*, vol. 12, pp. 31136–31158, 2024.

[4] H. Albinali and F. Azzedin, "Toward RPL attacks and mitigation taxonomy: Systematic literature review approach," *IEEE Trans. Netw. Serv. Manag.*, vol. 21, no. 5, pp. 5215–5238, 2024.

[5] A. Bang and U. P. Rao, "Impact analysis of rank attack on RPL-based 6LoWPAN networks in Internet of Things and aftermaths," *Arab. J. Sci. Eng.*, vol. 48, no. 2, pp. 2489–2505, 2023.

[6] 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, 2020.

[7] N. Alfriehat *et al.*, "RPL-based attack detection approaches in IoT networks: review and taxonomy," *Artif. Intell. Rev.*, vol. 57, no. 9, p. 248, 2024.

[8] 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.

[9] 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.

[10] K. Mittal and P. K. Batra, "A Study on Intrusion Detection System for RPL Protocol Attacks in Internet of Things," in *Network Optimization in Intelligent Internet of Things Applications*, Chapman and Hall/CRC, 2024, pp. 173–193.

[11] H. Kharrufa, H. A. A. Al-Kashoash, and A. H. Kemp, "RPL-based routing protocols in IoT applications: A review," *IEEE Sens. J.*, vol. 19, no. 15, pp. 5952–5967, 2019.

[12] 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.

[13] D. Pancaroglu and S. Sen, "Load balancing for RPL-based Internet of Things: A review," *Ad Hoc Networks*, vol. 116, p. 102491, 2021.

[14] M. M. Mazlan, N. A. Zakaria, and Z. Z. Abidin, "Security challenges in 6lowpan protoco l for internet of things: a review," *J. Theor. Appl. Inf. Technol*, vol. 98, no. 23, pp. 3898–3908, 2020.

[15] P. S. Nandhini, S. Kuppuswami, S. Malliga, and Rjtj. DeviPriya, "Enhanced Rank Attack Detection Algorithm (E-RAD) for securing RPL-based IoT networks by early detection and isolation of rank attackers," *J. Supercomput.*, vol. 79, no. 6, pp. 6825–6848, 2023.

[16] M. Osman, J. He, F. Mahiuob, M. Mokbal, and N. Zhu, "Artificial neural network model for decreased rank attack detection in RPL based on IoT networks," *Int. J. Netw. Secur.*, vol. 23, no. 3, pp. 496–503, 2021.

[17] H. Albinali, R. Alghofaili, and F. Azzedin, "Analytical study of local repair attack on RPL-based 6LoWPAN networks in internet of things," in *Proceedings of the 7th international conference on future networks and distributed systems*, 2023, pp. 641–646.

[18] M. Rouissat, I. S. Alsukayti, M. Belkheir, M. Alreshoodi, A. Mokaddem, and D. Ziani, "A Simple Approach for Mitigating a New Flooding Attack in RPL-Based IoT Networks," *IEEE Access*, 2025.

[19] E. Canbalaban and S. Sen, "A cross-layer intrusion detection system for RPL-based Internet of Things," in *International conference on Ad-hoc networks and wireless*, Springer, 2020, pp. 214–227.

[20] F. Azzedin, "Mitigating denial of service attacks in rpl-based iot environments: trust-based approach," *IEEE Access*, vol. 11, pp. 129077–129089, 2023.

[21] C. Kim, C. So-In, Y. Kongsorot, and P. Aimtongkham, "FLSec-RPL: a fuzzy logic-based intrusion detection scheme for securing RPL-based IoT networks against DIO neighbor suppression attacks," *Cybersecurity*, vol. 7, no. 1, p. 27, 2024.

[22] S. Al-Sarawi, M. Anbar, B. A. Alabsi, M. A. Aladaileh, and S. D. A. Rihan, "Passive rule-based approach to detect sinkhole attack in RPL-based Internet of Things networks," *IEEE Access*, vol. 11, pp. 94081–94093, 2023.

[23] A. Krari and A. Hajami, "RPL-shield: A deep learning GNN-based approach for protecting IoT networks from RPL routing table falsification attacks," in *International Conference on Digital Technologies and Applications*, Springer, 2024, pp. 117–127.

[24] C. D. Morales-Molina *et al.*, "A dense neural network approach for detecting clone id attacks on the rpl protocol of the iot," *Sensors*, vol. 21, no. 9, p. 3173, 2021.

[25] S. M. H. Mirshahjafari and B. S. Ghahfarokhi, "Sinkhole+ CloneID: A hybrid attack on RPL performance and detection method," *Inf. Secur. J. A Glob. Perspect.*, vol. 28, no. 4–5, pp. 107–119, 2019.

[26] A. Verma and V. Ranga, "CoSec-RPL: detection of copycat attacks in RPL based 6LoWPANs using outlier analysis," *Telecommun. Syst.*, vol. 75, no. 1, pp. 43–61, 2020.

[27] N. Chinnakali, "Sniffing Attack Detection in 6LoWPAN RPL Networks Using Machine Learning Algorithms," 2024.

[28] S. Goel, A. Verma, and V. K. Jain, "Design and Implementation of a Lightweight Mitigation Solution for Addressing Network Partitioning Attack Against RPL Protocol," *Wirel. Pers. Commun.*, vol. 139, no. 4, pp. 2027–2050, 2024.

[29] H. Azzaoui, A. Z. E. Boukhamla, P. Perazzo, M. Alazab, and V. Ravi, "A lightweight cooperative intrusion detection system for rpl-based iot," *Wirel. Pers. Commun.*, vol. 134, no. 4, pp. 2235–2258, 2024.

[30] A. Kannan, M. Selvi, S. V. N. Santhosh Kumar, K. Thangaramya, and S. Shalini, “Machine learning based intelligent rpl attack detection system for iot networks,” in *Advanced Machine Learning with Evolutionary and Metaheuristic Techniques*, Springer, 2024, pp. 241–256.

[31] M. Osman, J. He, N. Zhu, and F. M. M. Mokbal, “An ensemble learning framework for the detection of RPL attacks in IoT networks based on the genetic feature selection approach,” *Ad Hoc Networks*, vol. 152, p. 103331, 2024.

[32] A. Wakili, S. Bakkali, and A. E. H. Alaoui, “Machine learning for QoS and security enhancement of RPL in IoT-Enabled wireless sensors,” *Sensors Int.*, vol. 5, p. 100289, 2024.

[33] M. Lmkaiti, M. Lachgar, I. Larhlimi, H. Moudni, and H. Mouncif, “Secure Optimization of RPL Routing in IoT Networks: Analysis of Metaheuristic Algorithms in the Face of Attacks.,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 16, no. 4, 2025.

[34] A. Berguiga, A. Harchay, and A. Massaoudi, “HIDS-RPL: A Hybrid Deep Learning-Based Intrusion Detection System for RPL in Internet of Medical Thing Networks,” *IEEE Access*, 2025.

[35] K. Ahmadi and R. Javidan, “A novel RPL defense mechanism based on trust and deep learning for internet of things,” *J. Supercomput.*, vol. 80, no. 12, pp. 16979–17003, 2024.

[36] A. Krari, A. HAJAMI, and E. JARMOUNI, “Detecting the RPL version number attack in IoT Networks using Deep Learning Models,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 10, 2023.

[37] Y. Al Sawafi, A. Touzene, and R. Hedjam, “Hybrid deep learning-based intrusion detection system for RPL IoT networks,” *J. Sens. Actuator Networks*, vol. 12, no. 2, p. 21, 2023.

[38] K. Kowsalyadevi and N. Balaji, “IoBTSec-RPL: A novel RPL attack detecting mechanism using hybrid deep learning over battlefield IoT environment,” *Int. J. Comput. Netw. Appl*, vol. 10, pp. 637–650, 2023.

[39] D. Dey and N. Ghosh, “iTRPL: An intelligent and trusted RPL protocol based on Multi-Agent Reinforcement Learning,” *Ad Hoc Networks*, vol. 163, p. 103586, 2024.

[40] M. H. Shivanajappa, R. M. Seetharamaiah, B. V. Sai, A. J. Siddegowda, and V. K. Rajuk, “An intrusion detection system againstRPL-based routing atacks for IoT networks,” *Indones. J. Electr. Eng. Comput. Sci*, vol. 34, pp. 1324–1335, 2024.

[41] S. Remya, M. J. Pillai, C. Arjun, S. Ramasubbareddy, and Y. Cho, “Enhancing security in LLNs using a hybrid trust-based intrusion detection system for RPL,” *IEEE Access*, vol. 12, pp. 58836–58850, 2024.

[42] B. Mbarek, M. Ge, and T. Pitner, “Proactive trust classification for detection of replication attacks in 6LoWPAN-based IoT,” *Internet of Things*, vol. 16, p. 100442, 2021.

[43] S. Goel, A. Verma, and V. K. Jain, “CRA-RPL: A Novel Lightweight challenge-Response authentication-based technique for securing RPL against dropped DAO attacks,” *Comput. Secur.*, vol. 132, p. 103346, 2023.

[44] M. Zaminkar, F. Sarkohaki, and R. Fotohi, “A method based on encryption and node rating for securing the RPL protocol communications in the IoT ecosystem,” *Int. J. Commun. Syst.*, vol. 34, no. 3, p. e4693, 2021.

[45] V. R. Rajasekar and S. Rajkumar, “DSAT-IDS: Dissimilarity and Adaptive Threshold-based Intrusion Detection system to mitigate selective forwarding attack in the RPL-based 6LoWPAN,” *Cluster Comput.*, vol. 27, no. 9, pp. 12029–12068, 2024.

[46] H. Kharrufa, H. Al-Kashoash, and A. H. Kemp, “A game theoretic optimization of RPL for mobile Internet of Things applications,” *IEEE Sens. J.*, vol. 18, no. 6, pp. 2520–2530, 2018.

[47] M. Hassan *et al.*, “Gitm: A gini index-based trust mechanism to mitigate and isolate sybil attack in rpl-enabled smart grid advanced metering infrastructures,” *IEEE Access*, vol. 11, pp. 62697–62720, 2023.

[48] R. Sahay, G. Geethakumari, and K. Modugu, “Attack graph—Based vulnerability assessment of rank property in RPL-6LOWPAN in IoT,” in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, IEEE, 2018, pp. 308–313.

[49] M. H. Homaei, S. S. Band, A. Pescape, and A. Mosavi, “DDSLA-RPL: dynamic decision system based on learning automata in the RPL protocol for achieving QoS,” *IEEE Access*, vol. 9, pp. 63131–63148, 2021.

[50] O. A. Abdulkareem, R. K. Kontham, and I. T. Aziz, “Blocollab: A Blockchain-aided Deep Learning Model for Hybrid and Collaborative Routing Attack Detection and Mitigation in RPL.,” *Int. J. Intell. Eng. Syst.*, vol. 17, no. 4, 2024.

[51] E. Aydogan, S. Yilmaz, S. Sen, I. Butun, S. Forsström, and M. Gidlund, “c,” in *2019 15th IEEE International Workshop on Factory Communication Systems (WFCS)*, IEEE, 2019, pp. 1–5.

[52] salah dhifallah, walid; tarhouni, mounira; moulahi, tarek; zidi, “IoT-RPL 2021: Cyber Attack Dataset Based on RPL Routing for IoT.”

[53] A. A. R. A. Omar, B. Soudan, and A. Altaweel, “UOS_IOTSH_2024: A Comprehensive network traffic dataset for sinkhole attacks in diverse RPL IoT networks,” *Data Br.*, vol. 55, p. 110650, 2024.

[54] B. Aydin, H. Aydin, S. G. Örmüş, and E. M. Ollahasanoğlu, “Detection of RPL-based Routing Attacks Using Machine Learning Algorithms,” vol. 4, pp. 783–796, 2024, doi: 10.24012/dumf.1490367.

[55] Z. Z. Motes, “GitHub.” [Online]. Available: https://github.com/contiki-os/contiki/wiki/Zolertia-z1-motes

[56] TETCOS LLP, “NetSim Simulator.” [Online]. Available: https://www.tetcos.com/iot-wsn.html

[57] C. F. Higham and D. J. Higham, “Deep learning: An introduction for applied mathematicians,” *Siam Rev.*, vol. 61, no. 4, pp. 860–891, 2019.

[58] L. Bartolozzi, T. Pecorella, and R. Fantacci, “ns-3 RPL module: IPv6 routing protocol for low power and lossy networks,” in *Proceedings of the 5th international ICST conference on simulation tools and techniques*, 2012, pp. 359–366.

[59] H. Hosseini, E. Rojas, and D. Carrascal, “Implementation of RPL in omnet++,” *arXiv Prepr. arXiv2107.02551*, 2021.

[60] J. Ko *et al.*, “Contikirpl and tinyrpl: Happy together,” in *Workshop on Extending the Internet to Low Power and Lossy Networks (IP+ SN)*, 2011.

[61] T. Winter *et al.*, “RPL: IPv6 routing protocol for low-power and lossy networks,” 2012.

[62] Y. Wang, J. Lei, Y. Li, and F. Shang, “GATR: a graph attention deep reinforcement learning approach with variance-sensitive rewards for rpl routing

optimization," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 37, no. 9, pp. 1–18, 2025.