Artificial Intelligence Review (2024) 57:248
https://doi.org/10.1007/s10462-024-10907-y

RPL-based attack detection approaches in IoT networks: review and taxonomy

Nadia Alfriehat[1] · Mohammed Anbar[1] · Mohammed Aladaileh[2] · Iznan Hasbullah[1] · Tamarah A. Shurbaji[1] · Shankar Karuppayah[1] · Ammar Almomani[3,4,5]

Accepted: 6 August 2024 / Published online: 12 August 2024
© The Author(s) 2024

Abstract
The Routing Protocol for Low-Power and Lossy Networks (RPL) plays a crucial role in the Internet of Things (IoT) and Wireless Sensor Networks. However, ensuring the RPL protocol's security is paramount due to its susceptibility to various attacks. These attacks disrupt data transmission and can substantially damage network topology by depleting critical resources. This paper presents a comprehensive survey addressing several key components in response to this challenge. Firstly, it categorizes potential attacks targeting the RPL protocol based on their impact on network performance and explores effective mechanisms to secure the protocol against them. The study identifies the most destructive and problematic threats affecting RPL functionality. Furthermore, it provides valuable insights into the security challenges of the RPL protocol and discusses their real-world implications for deploying and maintaining IoT and sensor networks. To underscore the uniqueness of the survey, we offer a qualitative comparison with other surveys in the same field. While this study acknowledges certain limitations, such as intentionally focusing only on reviewing RPL-specific attacks, it is a valuable reference for future researchers seeking to comprehend and mitigate attacks targeting RPL. It also suggests areas for further research in this domain.

Keywords RPL · IoT networks · Intrusion detection system · Artificial intelligence

1 Introduction

The IoT transforms how people connect and engage with ordinary things, computer systems, and users (Makina et al. 2024). The IoT expanded the standard internet architecture to include the networking and communication of different IoT devices (Wisdom et al. 2024). To effectively manage IoT devices' special qualities and needs, specialized IoT architectures and routing protocols must be developed. Reliability Mayzaud et al. (2017), low power usage, scalability, and security are key challenges these systems and protocols must address. The distributed setup, where data processing occurs at edge

Mohammed Aladaileh, Iznan Hasbullah, Tamarah A. Shurbaji, Shankar Karuppayah and Ammar Almomani have equally contributed to this work.

Extended author information available on the last page of the article

devices or in a decentralized manner, and the centralized architecture, where all data is sent to a central server for processing, are two commonly used IoT architectures. Furthermore, various routing protocols have been developed specifically for IoT networks (Ahmed and Ko 2016).

Among these protocols is RPL, which is intended for IoT devices that have limited memory and processing capacity; the RPL is well-suited for IoT networks, designed specifically to optimize IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN). RPL is an essential protocol for Internet of Things networks because it allows devices with low power and computing capacity to communicate effectively and reliably. It is specially made to facilitate routing in situations with constraints Thungon et al. (2024), such as sensor networks, where devices might only have a small amount of memory, computing power, or battery life. RPL does this using a simple routing protocol that minimizes control overhead and adapts to the dynamic nature of these networks.

It establishes a hierarchical structure (Destination-oriented Directed Acyclic Graph, or DODAG) that facilitates efficient data routing between devices in an IoT network (Kamel and Elhamayed 2020). However, the resource-constrained nature of 6LoWPAN devices-limitations in battery power, processing capacity, memory, and bandwidth-can impact the performance and security of the RPL protocol. (Raza et al. 2013).

Another illustration is the lightweight publish/subscribe messaging protocol Message Queuing Telemetry Transport (MQTT), perfect for IoT applications with constrained connections and bandwidth. Moreover, other routing protocols, such as IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN) and Constrained Application Protocol (CoAP) Ferraz Junior et al. (2022), have been created to offer effective routing and communication in IoT networks. To facilitate the implementation of a wide range of IoT applications across industries like transportation, healthcare, agriculture, and smart homes Kamel and Elhamayed (2020), these protocols and architectures are essential for enabling seamless communication and data exchange between IoT devices.

Routing protocols and IoT design prioritize security, emphasizing the need for data transfer and inter-device connectivity protection. Encryption and authentication are essential security mechanisms to ensure data confidentiality and integrity, prevent unauthorized access, and preserve personal data. Specialist IoT architectures and routing protocols must efficiently manage the unique characteristics of IoT devices. IoT, 6LoWPAN, WSN, and routing protocols are interconnected Raza et al. (2013), forming the foundation for the Internet of Things. Understanding their roles is crucial for effective IoT solutions leveraging data to transform our lives. As depicted in Table 1. Security is paramount in IoT design and operation.

Table 1 summarizes key findings from previous studies on IoT routing protocols, highlighting the difference between IoT, 6LoWPAN, and WSN.

These surveys often lack comprehensive taxonomies of RPL detection mechanisms, fail to cover recent RPL-specific attack types, and lack clarity in their explanations. This survey paper addresses specific research gaps within the domain of RPL, attacks, and countermeasures, aiming to provide a detailed and comprehensive overview for experts and non-experts.

The contributions of this paper are as follows:

1. A comprehensive survey of potential attacks targeting the RPL protocol and its detection mechanisms.
2. A taxonomy of existing detection mechanisms for RPL-based attacks.

Table 1 Comparison of IoT, 6LoWPAN, WSN, and routing protocols

Feature	IoT	6LoWPAN	WSN	Protocol routing
Concept	A network of physical devices embedded with software, sensors, and actuators to collect and exchange data	An adaptation layer protocol that enables IPv6 communication on resource–constrained networks	A specific type of IoT network focused on collecting environmental data using sensor nodes	Protocols that define how data is routed between devices in a network
Purpose	Connect devices to the internet and enable communication between them	Adapts IPv6 for low–power networks	Enables communication between sensor nodes	Establishes paths for data flow in a network
Focus	Overall networking architecture for diverse devices	Efficient communication for low–power devices	Data collection and monitoring	Routing data packets between network nodes
Key Features	- Heterogeneous devices (sensors, actuators, smartphones) - Resource–constrained (limited processing power,memory, battery) - Integration with cloud platforms	- Enables IPv6 addressing on low–power networks– Header compression for smaller packets - Supports different types of devices	- Sensor nodes with limited resources - Focus on energy efficiency - Specialized data collection protocols	- Utilize various message formats (e.g., unicast, multicast) - Adapt to network conditions (dynamic routing) - Security considerations for data integrity and privacy
Communication Model	Varies depending on protocol (e.g., MQTT, CoAP)	Message–based (e.g., UDP)	Message–based (often custom protocols)	Varies depending on protocol (e.g., RPL, AODV)
Underlying Network	Can operate on various network technologies	Designed for low–power wireless networks (e.g., IEEE 802.15.4)	Often deployed in WSN	Provides routing functionality within a network
Example Applications	Smart homes, industrial automation, wearables	Environmental monitoring, building automation, agriculture	Industrial monitoring, structural health monitoring, precision agriculture	Traffic management, smart grids, industrial automation

3. A statistical analysis of RPL-based attack detection mechanisms to identify the most efficient methods.
4. A qualitative comparison between the proposed and existing surveys in the same field using statistical analysis and data visualization techniques to show the uniqueness of this survey.

The remainder of the paper consists of a concise introduction to the RPL protocol, a classification system of attacks specific to the RPL protocol (Sect. 2), and a proposal of a taxonomy for various defensive strategies against RPL attacks found in published works (Sect. 3). It also shows the outcome and talks about how it compares to other evaluations of RPL attack detection methods, pointing out how they are unique within the RPL protocol. Section 4, then discusses techniques to detect VNA against the RPL protocol Sect. 5. The paper ends with suggestions for future research trajectory (Sect. 6) and conclusions (Sect. 7).

2 Background

The background provides three key elements of the RPL protocol, starting with A brief overview of the RPL protocol (Sect. 2.1), followed by the terminology used in the RPL context (Sect. 2.2). Finally, we comprehensively review the primary security issues and attack classifications associated with the RPL protocol in Sect. 2.3.

2.1 Overview of RPL protocol

RPL is designed for IoT networks, focusing on low-power consumption and support for WSNs (Thubert et al. 2018). It operates proactively and constructs a DODAG topology using control packets. This topology enables efficient communication among resource-constrained devices Zhou (2024)in various environments. Table 2 provides an overview of the RPL routing protocol's primary characteristics (Simha et al. 2020).

2.2 RPL terminology

Understanding the RPL terminology is crucial to comprehend the intricacies of RPL-based attacks fully Agiollo et al. (2021). RPL relies on four fundamental ICMPv6 control messages. The four RPL-related ICMPv6 are as follows. as illustrated in Fig. 1.

1. DODAG Information Object (DIO) conveys information for nodes to locate an RPL instance Arış and Oktuğ (2020), Arış et al. (2019) that permits nodes to select a DODAG parent set and locate the RPL instance Fig. 1a.
2. During the upward transmission phase, nodes without children nodes send Destination Advertisement Object (DAO) Fig. 1b. messages to the root nodes. These DAO messages comprise the destination data's address and contribute to constructing an ascending route Ambarkar and Shekokar (2021). In a hierarchical network structure, the ascending route creates a path from the leaf nodes (without children) to the root node. This route is made through the exchange of DAO messages. However, the term "ascending route" may not be widely used or clearly understood in this context. It could be more precise

Table 2 RPL routing protocol's primary characteristics

Key	Description
Scalability	Designed to support large–scale networks with low power and lossy links, making it suitable for various IoT applications. Kiran et al. (2024)
Adaptive	RPL adapts to the changing network environment by adjusting routes based on link quality and energy Bokka and Sadasivam (2024)
Target network	LLN; IPv6/6 low PAN network
Routing type	Source–routing, Distance –Vector
Topology	Mesh/hierarchical based on DAGS
Traffic flows	MP2P,P2MP and P2P
Message update	Trickle timer
Control message	DIO,DAO, DIS Alfriehat et al. (2024)
Neighbor discovery	Like IPV6ND mechanisms
Transmission	Unicast and multicast
Metrics & constraints	Dynamic, based on OF and Rank
Modes	Storing and non–Storing Al–Mubarak and Conejo (2023)
Taxonomy of RPL attacks	Resource–based, Topology–based, and Traffic–based

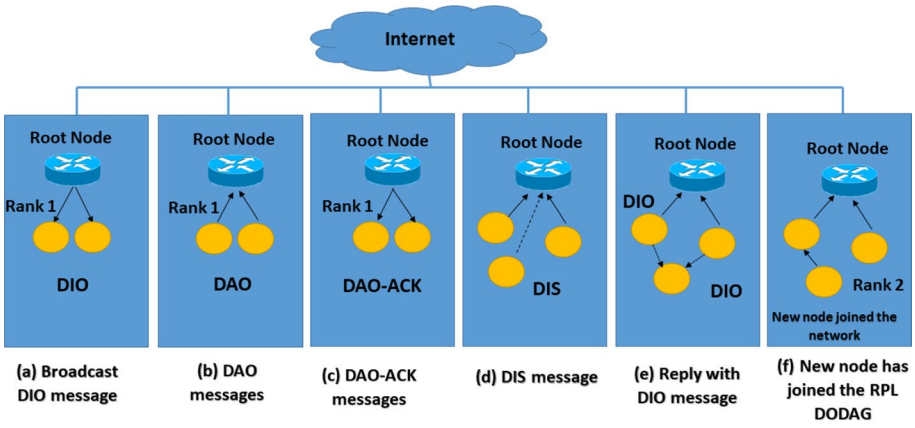

Fig. 1 DODAG control message structure

to describe this process as establishing a route from leaf nodes towards the root node to avoid confusion. During the upward transmission phase, nodes without children send DAO messages to the root nodes. These DAO messages contain the destination data's address and contribute to constructing a route from leaf nodes towards the root node in the hierarchical network structure.

3. Information Solicitation for DODAG (DIS): A node broadcasts a message to join the network, which can be exploited by malicious nodes for launching FAs Avila et al. (2020) Fig. 1d

4. Destination Advertisement Object Acknowledgement (DAO-ACK): A unicast message is sent from the recipient of a DAO message Abhinaya and Sudhakar (2021), typically the DODAG root node or parent node of the sender, back to the sender Fig. 1c. The purpose of the DAO-ACK message is to confirm that the recipient can forward packets to the sender and acknowledge the receipt of the DAO message. The DAO-ACK message is sent in response to DAO messages (Al-Amiedy et al. 2022). These messages facilitate DODAG formation and route establishment (Tasneem and Wahid 2021). When a node first joins an RPL instance, it sends out a DIO message to its neighbours to establish a new DODAG (Fig. 1a). DAO messages are returned by the child nodes (Fig. 1b). The DODAG is subsequently finished by the root node sending a DAO-ACK response (Fig. 1c). To connect to an active RPL instance, a node will send a DIS message to the DODAG root node (Fig. 1d). The new node can then join the network by receiving a DIS message from the nearest nodes (Fig. 1f). The network's single root node is ensured by this process. The network topology of an RPL network is the Internet-connected root node with the lowest rank and the leaf nodes with the highest rank values.

2.2.1 Communication modes

RPL supports two communication modes: storing mode and non-storing mode (Zhang et al. 2023). As shown in Table 3 In storing mode, intermediate nodes in the network store routing information, enabling efficient path discovery and maintenance. This mode is advantageous for networks with high traffic and frequent topology changes. However, storing mode requires more memory and processing power, making it less suitable for resource-constrained devices. On the other hand, the non-storing mode Rabet et al. (2024) does not require intermediate nodes to store routing information, reducing memory and processing requirements. This mode is advantageous for networks with limited resources but may result in increased overhead and longer end-to-end delays (Krentz and Voigt 2024).

2.2.2 Control message

Some control messages used in RPL include DIO and DAO. DIO messages distribute information about the network topology and the DODAG structure, allowing nodes to join and maintain the routing structure (Mayzaud et al. 2017). DAO messages are used to advertise and update routes to specific destinations. However, these control messages can be vulnerable to attacks. For example, an attacker can forge DIO messages to disrupt the network by causing nodes to join a malicious DODAG or inject false topology information. Similarly, DAO messages can be spoofed, propagating incorrect or malicious routes

Table 3 Comparison of storing mode and non-storing mode

Aspect	Storing mode	Non–storing mode
Routing	Stores routing information	Does not store routing information
Overhead	Higher control message overhead	Lower control message overhead
Memory usage	Requires more memory in nodes	Requires less memory in nodes
Scalability	Less scalable for large networks	More scalable for large network

throughout the network. It is essential to implement security measures, such as message authentication (MA), to prevent these vulnerabilities and ensure the integrity and authenticity of control messages.MA ensures that only authorized nodes can send control messages by validating the message's source. Cryptography techniques can verify the authenticity of the control message Oladipupo et al. (2023), preventing attackers from forging DIO or DAO messages. Additionally, implementing encryption mechanisms can further protect the confidentiality of the control messages, ensuring that only authorized nodes can access and interpret the information. These security measures are crucial for maintaining a secure and reliable routing protocol in WSN.

2.2.3 Establishment of DODAG

Describe how DODAGs are established in RPL, including the roles of root nodes and how nodes join and leave the DODAG. Discuss potential vulnerabilities during this process. DODAGs are established in RPL through DODAG formation. The root node initiates the formation by sending DIOs to neighboring nodes. These nodes then become parents (children) of the root node and start propagating their DIOs, forming the DODAG. Nodes join the DODAG by selecting a parent node based on various metrics, such as link quality or available resources (Almusaylim et al. 2020).

During the establishment of DODAGs, potential vulnerabilities can arise. One vulnerability is the risk of nodes joining a malicious DODAG controlled by an attacker. This can lead to unauthorized access and manipulation of control messages, compromising the security and integrity of the network. To mitigate this risk, authentication mechanisms can be implemented to ensure that only trusted nodes can join the DODAG. Another vulnerability is the possibility of nodes selecting unreliable or compromised parent nodes Alsukayti and Alreshoodi (2023), resulting in degraded network performance or complete network failure. This risk can be minimized using appropriate metrics and algorithms for parent selection, considering factors such as stability and trustworthiness. Overall, establishing and maintaining DODAGs requires careful consideration of security measures to ensure the robustness and efficiency of the network, (Omar et al. 2023), as shown in Fig. 2

RPL packets follow a specific format that includes various fields crucial for routing decisions and security. One critical field is the Destination IPv6 address, which indicates the intended recipient of the packet. Another important field is the DODAGID, which identifies the DODAG to which the packet belongs. This field helps determine the appropriate path for forwarding the packet. The RPL Control field also plays a vital role in routing decisions, containing information about the packet's rank, Objective Function (OF),

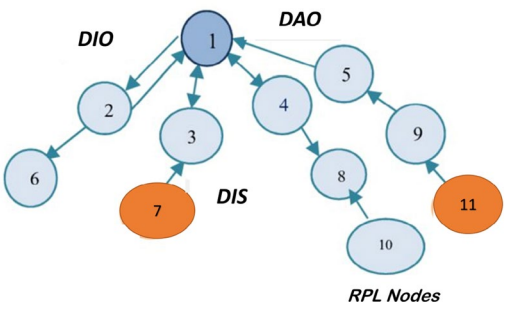

Fig. 2 DODAG structure

and routing method. Ensuring the security of these fields is essential to prevent unauthorized access and potential attacks on the network. Below is an overview of the typical RPL packet format (Omar et al. 2023):

1. RPL Header: Type (T) (1 byte): Specifies the type of RPL packet, such as control or data. Instance ID (IID) (1 byte): Identifies the RPL instance to which the packet belongs. Flags (1 byte): Contains various control flags, e.g., for multicast or security settings.
2. DIO: The DIO Base variable length (VL) contains information about the DODAG, including its rank, version, and OF. This is crucial for building and maintaining the DODAG structure. Routing Information:
3. Destination Address VL: Specifies the destination node or prefix for which routing information is provided.
4. Next Hop Address VL: Indicates the next hop towards the specified destination.
5. Routing Metrics (variable length): Contains routing metrics like hop count or Expected Transmission Count (ETX).
6. Payload: Data Payload VL: This section carries the application data for data packets. Neighbor Payload VL: Control packets may contain additional information required for network management and control. Optional Security Header:
7. Security Parameters VL: This section contains cryptographic information like keys and signatures if security is enabled. Trailer:
8. Checksum (CRC): A cyclic redundancy check or checksum is often included to ensure packet integrity. Additional TLVs (Type-Length-Value):
9. Optional TLVs VL: Additional Type-Length-Value fields may be included to convey specific information as required.

2.2.4 Routing process

The RPL routing process discovers routes through a proactive approach called DODAG formation. During this process, nodes exchange control messages to establish the network's topology. Routinely updating the DODAG structure and refreshing control messages are necessary for maintaining routes. Each node follows the DODAG structure when forwarding packets, selecting the next-hop neighbor based on the rank and OF. However, this routing process is susceptible to potential vulnerabilities and attack vectors. Adversaries can launch attacks such as spoofing control messages, injecting malicious control information Hannachi et al. (2024), or tampering with the rank calculation. These attacks can disrupt route discovery, misdirect packets, or cause network congestion.

Additionally, attacks on the RPL may compromise the entire network, allowing adversaries to gain unauthorized access to sensitive information or manipulate the network topology. Various security mechanisms can be employed to mitigate these threats, such as authentication and encryption of control messages, secure neighbor discovery protocols, and rank calculation algorithms that are resistant to tampering. Furthermore, continuous monitoring and anomaly detection techniques can help identify and respond to any suspicious activities in real-time, ensuring the integrity and availability of the routing process in the network. For example, in a large-scale IoT deployment Yang et al. (2024), an attacker may attempt to impersonate a legitimate device and inject false routing information into the network. To prevent this, the network can employ authentication mechanisms that verify each device's identity before accepting control messages. Additionally, encryption can be used to protect the confidentiality of control messages and prevent unauthorized access.

These security measures help ensure that only trusted devices can participate in the routing process and minimize the risk of tampering or unauthorized network manipulation.

2.3 RPL security issues and attacks classification

Due to the nodes' vulnerabilities, mobility, and resource constrained, the RPL protocol is susceptible to various internal and external attacks. Detecting and preventing these attacks is challenging because of node vulnerabilities, mobility, and resource constrained. Researchers have proposed RPL-specific security measures, such as security modes and control message encryption, to address these issues. Furthermore, RPL protocol attacks are categorized based on the Confidentiality, Integrity, Authentication, and Availability (CIAA) factors Mayzaud et al. (2017). These measures are effective against external attacks but inadequate against internal (insider) attacks. Insider attackers can bypass security measures and disrupt network functionality by manipulating RPL control messages, interfering with routing operations, and exploiting fault tolerance mechanisms to launch DoS attacks. Additionally, numerous RPL implementations omit these security measures due to incomplete specifications and concerns about overhead (Abhinaya and Sudhakar 2021).

The following sections comprehensively investigate RPL-based attacks targeting the protocol (Sharma et al. 2023). These attacks are categorized into resource-based, traffic-based, and topology-based groups, Verma and Ranga (2020), as depicted in Fig. 3.

2.3.1 Resource-based attacks

Resource-based attacks deplete nodes' resources by handing them meaningless tasks, targeting their storage Sharma and Verma (2021), energy use, and computing resources. These attacks impact the network lifetime by shortening it, and the network availability is affected by congesting the available links Mayzaud et al. (2016b), reducing the quality of service. Resource-based attacks can be direct, such as Hello flooding attacks (HFA) that overload the network with traffic, or indirect, such as attacks that exploit vulnerabilities in network protocols (Patil et al. 2022).

1. *Direct attacks* In direct attacks, malevolent nodes degrade the network by directly overwhelming it with traffic, rendering nodes and links inaccessible. The HFA is an example of a direct attack. HFA Jiang et al. (2024)is a form of attack that overloads a network by internal or external attackers, leading to the exhaustion of network resources in severe cases. Once a node has joined the network, it can launch this attack without violating security protocols. For instance, the HFA involves continuous broadcasting or unicasting of DIS solicitation messages that congest and saturate the link, leading to the resetting of trickle timers and responses with DIO messages.
2. *Indirect attacks*Indirect attacks occur when a malicious node manipulates other nodes to cause network congestion and increased Rank, DAG inconsistency, and VNAs. These attacks can cause substantial performance disruptions and compromise the system's security and integrity.

    (a) Version number attack (VNA): The VNA in RPL involves a malicious node elevating the root node's DODAG VN in DIO messages to deceive neighboring nodes. This causes DODAG rebuilds that are not needed and can cause loops in

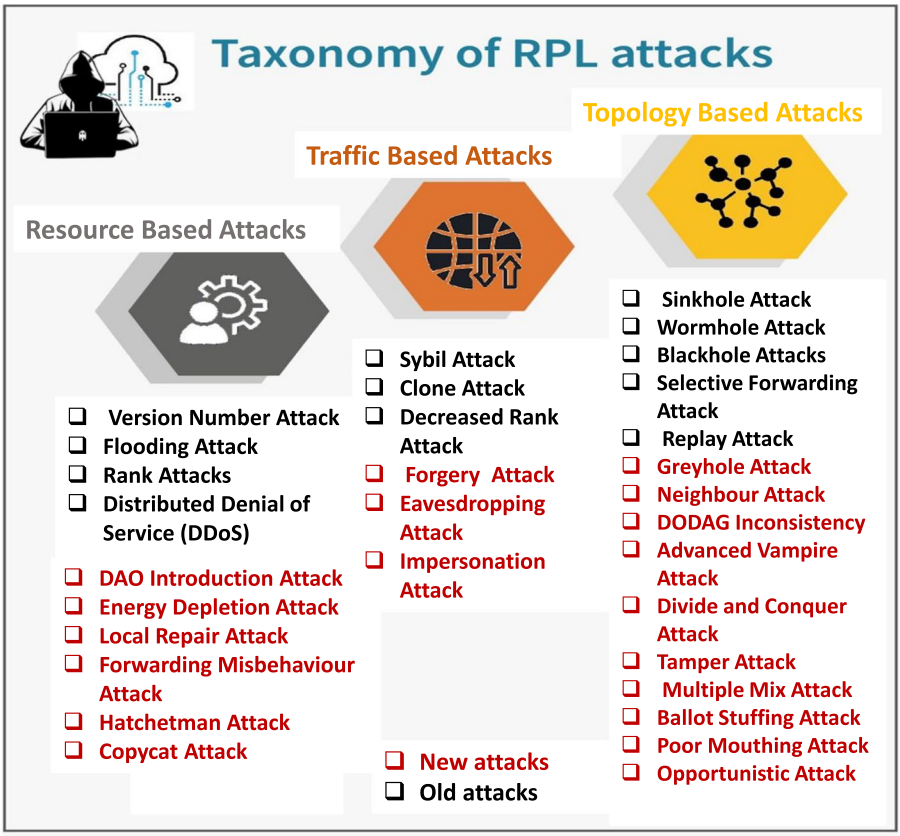

Fig. 3 Taxonomy of RPL attacks

the network topology Alfriehat et al. (2024). The attack breaks the network's functionality, uses more energy (EC), and interrupts communication(Sharma et al. 2023). Figure 4 shows VNAs. During a VNA, neighbor nodes reset their trickle timers and continuously broadcast updated DIO messages, leading to a twofold increase in network latency and more dropped packets. The attack exploits the global repair mechanism, triggered when the network faces issues. It causes the root to rebuild the DODAG by incrementing its VN. Mitigating the VNA requires implementing mechanisms to authenticate DIO messages and verify the integrity of VN (Verma and Ranga 2020). Detecting the attack is challenging due to the deceptive nature of malicious DIO packets Faraj et al. (2020), making it difficult to determine their origin. Communication between nodes is essential to tracing the attack's source.

(b) A flood attack (FA): is a type of cyberattack where a target system or network is inundated with an overwhelming volume of traffic or requests, making it inaccessible or unresponsive to legitimate users. Botnets, networks of compromised computers or devices, often orchestrate these attacks by flooding the target with many requests or data packets simultaneously (Suzuki et al. 2023). Due to the sheer scale of the traffic involved, FA can cause significant service disruptions that

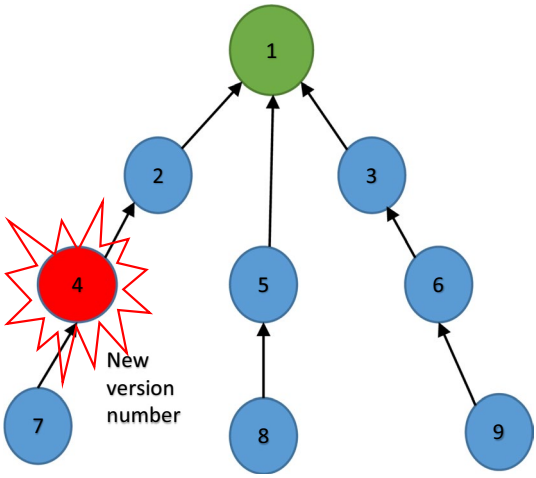

Fig. 4 Version number attack

are difficult to mitigate. These attacks can originate from individual compromised devices or large botnets, and the massive influx of traffic makes them challenging to defend against.

(c) Rank attacks (RA): The RPL protocol is open to rank-based attacks because it does not have a way to check the validity of control messages and routing metrics from parent nodes (Verma and Ranga 2020). This means that subordinate nodes accept routing information from their parent nodes without checking to see if it is real, which means they can get malicious data. This vulnerability can lead to suboptimal network routing and a decline in overall network efficiency. An attacker can exploit this vulnerability by manipulating its rank value and executing an RA against a malicious node. By manipulating its rank value Sharma et al. (2023), the attacker can deceive neighboring nodes into selecting the malicious node as a parent, as they believe it provides the shortest path to the root node . Figure 5 depicts a RA scenario. Any node in the network can start an RA as long as it can manipulate the routing protocol. The node does not necessarily need to be connected to the network initially Verma and Ranga (2020), as it can exploit vulnerabilities in the network's routing algorithm to gain access and control over the network's traffic . Therefore, any node manipulating the routing protocol can

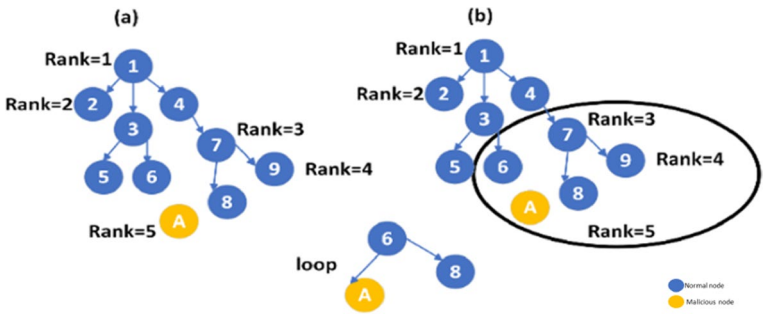

Fig. 5 Rank attack

generate an RA, regardless of its initial connection status or security measures (Sharma et al. 2023). Figure 5 depicts RA.

(d) A distributed denial of service (DDoS): DDoS attack is a deliberate effort to disrupt the normal operation of a network, system, or website by inundating it with an overwhelming amount of traffic from multiple sources (Hasan et al. 2023).These attacks can exhaust VoIP resources and block legitimate users from accessing services, rendering them particularly hazardous. The cybersecurity community has taken note of these attacks Shafi et al. (2024), leading to discussions about cybersecurity and the unpredictable nature of such threats.

(e) Decentralized autonomous organization (DAO) introduction attack: The DAO, a 2016 decentralized venture capital fund on the Ethereum blockchain, was hacked in June 2016, allowing an attacker to drain significant Ether into a "child DAO." This led to various hard forks in the Ethereum blockchain, splitting the blockchain into two separate entities: Ethereum (ETH) and Ethereum Classic (ETC) (Saurabh et al. 2024). The attack highlighted the risks of smart contract development and decentralized governance.

(f) DODAG inconsistency:

RPL uses data path validation to identify and correct rank-related anomalies, such as loops, in the DODAG. It detects network inconsistencies using identifiers within the RPL IPv6 header options of multi-hop data packets. If a data packet's direction flag does not precisely follow the sender/forwarder's rank relation, the "R" flag is set to 1 to conduct a topology repair. Any node that receives a packet with the "R" indicator set discards it and begins a local repair. However, an adversary can exploit these identifiers to execute a variety of DODAG Inconsistency attacks Dvir et al. (2011), such as Direct and Forced BH attacks. These attacks can disrupt the network's routing and cause communication failures by injecting false DIO messages into the network, leading neighboring nodes to form incorrect routing paths.

(g) Energy depletion attacks (EDA): An EDA aims to swiftly deplete the batteries of battery-operated devices, including smartphones or IoT gadgets. This may shorten the gadgets' lifespan or cause them to become non-functional. These attacks use weaknesses in devices to make them use more energy than they normally would Mottola et al. (2024), usually by delivering a lot of data or requests. Implementing security measures like encryption and device authentication is known as mitigation.

(h) Local repair attack (LRA): A node in RPL that loses the link to its preferred parent may start the local repair procedure by modifying the DODAG ID field to DIO or by updating its rank to infinite and disseminating the DIO to all neighbors, thereby accelerating network convergence. However, an adversary can force a node to perform superfluous local repairs while still connected to its parent. Any node in the network can start this attack, also known as the LRA, and it doesn't require a prior connection or security breach. RPL cannot confirm the validity of local repairs started by nearby nodes (Prathapchandran and Janani 2021). This results in increased EC and disruption of the routing process.

(i) Forwarding misbehavior attacks (FMA): In RPL-based IoT networks, FMA can have severe consequences. Nodes that misbehave by dropping or incorrectly forwarding packets can disrupt network operations, lead to data loss, and impact overall network efficiency. Any node in the RPL network, including internal and external nodes, can start these attacks. They can occur without the node needing to be initially connected

to the network or bypass security measures. To stop FMA in RPL networks, network administrators can do things like keep an eye on and audit network traffic, set up secure routing protocols that are only used in RPL Gowtham et al. (2024), and use access control to find and stop bad behavior.

(j) Hatchetman attack (HA): A HA is a recent DoS attack where a malignant node changes the source route header of the received packets, then generates and broadcasts many bogus packets with an error route to normal nodes. These malicious nodes interfere actively with the network's routing mechanisms by injecting fraudulent routing updates Sharma et al. (2022), deleting packets selectively, and causing routing loops. Using a simulation, a comprehensive study by Pu and Song (2018) reviewed and investigated Hatchetman attacks on LLN. The results show that HAs significantly increase packet delivery latency, ERC, and throughput while decreasing PDR significantly. For RPL networks to be safe from the bad changes HAs can make, they need strong authentication, behavior monitoring, and secure routing protocols. Any node in the network is capable of producing the HA, and neither a prior connection nor a security breach are necessary. This attack is a form of insider attack, where a compromised node intentionally disrupts the network by selectively dropping packets or sending false information. The goal of the HA is to degrade network performance or cause network nodes to choose suboptimal paths Pu and Song (2018), leading to inefficiencies in routing and potential disruptions in communication.

(k) Copycat attacks (CA): Usually, malevolent actors outside the network either human or automated systems-start CAs. These attackers seek to fool victims and exploit weaknesses by pretending to be trustworthy people or actions. Phishing, spoofing, and impersonation are just a few examples of the many shapes CAs may take. They don't always require the attacker to be connected to the network at first. To execute the attack, attackers could occasionally need to get past network security measures (Albinali and Azzedin 2024). All things considered, CAs pose a severe risk that businesses should mitigate by implementing security measures like network segmentation, multi-factor authentication, and user education.

2.3.2 Topology-based RPL attacks

Topology-based RPL attacks alter the network topology and can fall under sub-optimization or isolation categories:

1. *Sub-optimization*: When attackers purposely lower the network's optimal paths, they hurt its performance by stopping it from converging to its optimal form (i.e., optimal paths). This leads to poor performance, lower network throughput, and higher latency (Agiollo et al. 2021). Examples of sub-optimization attacks are as follows:

   (a) Sinkhole attack (SH): An attacker executes the SH in an RPL network by manipulating rank values and advertising false information, thereby unlawfully attracting a large volume of traffic before modifying or deleting it. Although the attacker's node performs inferior, the manipulated rank values deceive the neighboring nodes into selecting the attacker as the preferable parent. Therefore, the routes

cannot reach their optimal state Sehgal et al. (2014), the network's topology is altered, and its efficacy degrades. A BH attack is created if the attacker chooses to stop all traffic.

(b) Wormhole attack (WH): A WH attack in RPL compromises network privacy and security by allowing attackers to listen in on network traffic without detection. This attack can compromise private information exchanged between nodes Sehgal et al. (2014), including passwords and credentials. Protecting the integrity of the network requires effective countermeasures to detect and prevent WH attacks in RPL.

2. *Isolation:* Some topology-based attacks also isolate a node or group of nodes in the RPL network, resulting in their inability to communicate with their parents' nodes or the root (Verma and Ranga 2020). Examples of isolation attacks are as follows:

   (a) Blackhole attack (BH): A BH attack involves an intruder dropping all packets intended for forwarding on purpose. This can cause significant damage, particularly when joined with an SH attack Pishdar et al. (2022), resulting in a substantial quantity of traffic loss. This form of attack is a DoS attack. An attacker strategically positioned can isolate multiple nodes (Prakash and Swaroop 2016). Another example is the grey hole or SF attack, in which the perpetrator discards only the traffic of a subset of the network, (Verma and Ranga 2020).

   (b) Selective forwarding attack (SF): While capable of isolating a part of the network like the BA, it has less impact since it does not eliminate all received messages. Instead, it discards only a part of them . The magnitude of data loss caused by this attack is proportional to the number of packets the malicious node throws away (Deng et al. 2009).

   (c) Rank inconsistency (RI): When neighbouring nodes in a network have different ranks, it's referred to as RI in the context of the RPL protocol used in IoT networks. A rank measure is utilised in RPL to calculate a node's location in the network topology concerning the root node (Nandhini et al. 2023b). Various factors, including node movement, malicious attacks, and changes in network structure, might result in RI. A hostile node may modify its rank value or the rank values of other nodes in an RI attack to interfere with network functionality or launch further attacks (Cao et al. 2020).

   (d) Replay attacks (REA): These attacks occur when an attacker records data, intercepts it, and then retransmits it to trick a system into believing it to be authentic (Li et al. 2023). This kind of attack takes advantage of holes in data transfer security, such as insufficient authentication procedures or poor encryption (Quintero et al. 2023). These attacks include the attacker capturing data packets, such as encrypted or authenticated messages and replaying them later. If the destination system lacks security measures to identify and reject replayed packets, it may mistakenly accept the retransmitted data, opening the door to unwanted access or other security lapses.

   (e) Greyhole attacks (GH): One cyberattack that targets peer-to-peer (P2P) file-sharing networks is called a "GH attack." This attack involves a malicious node on the network posing as the owner of an entire copy of a file and accepting download requests from other nodes (Maheswari et al. 2022). However, the malicious node "swallows" the file requests by sending partial or damaged data instead of the

legitimate file. The name "GH" describes the misleading aspect of the attack, in which a hostile node poses as a legitimate member of the network yet engages in malevolent behaviour by omitting or presenting false information (Javed et al. 2023).

(f) Neighbour attacks (NA): A hostile node in a network tries to breach the security or interfere with the operation of neighbouring nodes in an attempt known as an "NA." This attack usually happens in decentralised networks, such as (P2P) or WSNs, where nodes communicate and coordinate by exchanging information with other nodes (Mattern et al. 2023). A malicious node may pretend to be a trustworthy neighbouring node, listen in on conversations between trustworthy nodes, or alter the data shared between nodes in a neighbor attack. An attacker can also interfere with network operations, steal private data, or start new attacks by jeopardising the integrity of nearby nodes.

(g) DAO inconsistency: To regulate structural mechanisms, RPL employs IPv6 hop-by-hop option variables. Down 'O' denotes packet direction, while Rank-Error 'R' indicates a topology rank error and Forwarding-Error 'F' indicates the node's incapacity to forward the packet (Al-Amiedy et al. 2023b). A DAO inconsistency occurs when a node's offspring can forward data based on erroneous routing information learned from a spoofed DAO message. To regulate topological mechanisms, RPL uses IPv6 hop-by-hop option variables. Down 'O' indicates packet direction, Rank-Error 'R' indicates a topological rank error, and Forwarding-Error 'F' indicates the node's inability to forward the packet. A DAO inconsistency occurs when a node's offspring can forward data based on erroneous routing information learned from a spoofed DAO message (Sharma et al. 2023). An attacker can exploit this vulnerability by setting the "F" flag in the packets to 1 and transmitting them back to the parent, forcing the parent to ignore reliable routes, increasing latency, achieving a poor topology, and isolating nodes (Pongle and Chavan 2015).

(h) Advanced vampire attack (AVA): The AVA is a stealthy hazard that targets RPL-based networks. Malicious nodes use nearby nodes' energy resources in a planned way in this advanced attack. Unlike traditional vampire attacks Al-Amiedy et al. (2023a), advanced version picks high-priority targets with smart methods, which is very dangerous for the network's energy-efficient operation. By depleting the energy of crucial nodes, this attack can disrupt network communication, causing delays and possibly rendering it inoperable. To protect RPL networks from the debilitating effects of the AVA, energy-efficient routing algorithms Juneja and Dinkar (2023), secure network monitoring and EC strategies are vital.

(i) Divide and conquer attack (DAC): Malevolent actors use a "DAC" attack as a deliberate strategy to compromise a system's security by breaking it down into smaller, more prone components. With this approach, it is simpler for attackers to obtain unauthorised access or interfere with the system's proper functioning by concentrating their efforts on targeting vulnerabilities in specific components (Hemalatha et al. 2024). This attack involves the attacker identifying the target system and breaking it into smaller parts called subsystems. They then attack every section, taking advantage of weaknesses to seize control or interfere with the system's operation. Once a segment or segments are penetrated, the attacker can use these breaches to get greater access to the system and accomplish their objectives.

(j) Tamper attack (TA): Tampering, another name for a TA, is an act in which the attacker tries to alter hardware, software, or data to interfere with or jeopardise a

system's security or effectiveness (Chen et al. 2024). Several system types, such as computers, networks, and electrical devices, are susceptible to these attacks. An attacker may attempt to tamper with data in transit or change a system's functioning to accomplish their nefarious objectives. An attacker may, for instance, alter data to affect a process's outcome or interfere with software to include a backdoor (Palani and Loganathan 2024).

(k) Multiple mix attack (MMA): This attack sends internet data via many intermediary nodes, or mixes, to obfuscate its source before it reaches its intended destination. This procedure improves privacy and anonymity by making it impossible for other parties to determine the source of the traffic (Lin et al. 2020). an additional attack that uses several mixed nodes to target or exploit weaknesses in a system.

(l) Ballot stuffing attack (BSA): One way to conceptualise a malicious effort to corrupt or disrupt the routing process inside an RPL-based network is as a BSA based on RPL. Similar to how ballot boxes could be stuffed with fictitious votes Agarwal et al. (2024), the phrase BSA in this context may be used metaphorically to describe an attack in which nodes in the network are inundated with malicious or misleading routing information. An attacker may use BS on an RPL-based network to sway other nodes' routing decisions by injecting bogus routing messages, forging routing data, or changing the rank values of individual nodes. If the network is overloaded with traffic, this might result in DoS, unstable networks, or less-than-ideal routing routes (Xiang et al. 2024).

(m) Poor mouthing attack (PMA): A PMA in the context of RPL could entail hostile nodes disseminating inaccurate or misleading information about other network nodes or the performance of the network as a whole. By tricking nodes into choosing less-than-ideal routes or instilling suspicion in genuine nodes Lewis et al. (2023), this attack can potentially interfere with the routing process. In bad-mouthing, a malicious node might deceitfully assert its optimal path to a destination node, causing other nodes to route their traffic via the malicious node. Increased latency, packet loss, or network congestion might come from this.

(n) Opportunistic attack (OA): These attacks could exploit vulnerabilities or weaknesses in the protocol to disrupt or compromise network communication. One possible OA in RPL could involve a malicious node exploiting insecure authentication mechanisms to gain unauthorized access to the network. Once inside, the attacker could manipulate routing information, inject false data, or disrupt the routing process, causing network congestion or DoS (Li et al. 2024).

2.3.3 Traffic-based RPL attacks

Traffic-based attacks aim at RPL network communication and encompass eavesdropping and impersonation attacks. Examples of traffic-based attacks are as follows:

1. Eavesdropping: The prevalence of RPL networks may facilitate the deployment of malicious nodes, enabling them to engage in surveillance activities such as network traffic interception and analysis through a sniffing attack (SA) (Wang et al. 2023). An SA is a type of network security threat where the attacker listens to and collects packets transmitted over a network, compromising the confidentiality of communication. This attack is typical in wired and wireless networks, whether involving a hacked device in wired networks or the direct capture of traffic in wireless networks. In RPL networks,

sniffing control messages can reveal information about the network configuration, while sniffing data packets can provide insights into packet content and the local network topology. Detecting and preventing this attack is challenging, as it can only be mitigated by encrypting messages when the attacker is external. However, the technical details for encryption are not available in the specification document Verma and Ranga (2020), RFC 6550.

2. impersonation: An impersonation attack occurs when the adversary takes on the identity of a trusted entity in a network to mimic a legitimate device or user to gain unauthorized access to the network or data. The impersonator can obtain control over the patient's wearable device and access sensitive medical information. The attacker can exploit the device for harmful purposes, such as manipulating an insulin pump, leading to an overdose of insulin, and potentially causing hypoglycemia or even diabetic shock in severe cases (Maikol et al. 2021). Additionally, RPL is vulnerable to common assaults in Wireless Sensor Networks, such as HF, SA, WA, BA, SF, Sybil, and Clone ID, substantially disrupting the network's performance and shortening its lifetime. The attacks are categorized based on whether insiders or outsiders carry them out, what is required to effectuate them, and how they impact network performance (Mayzaud et al. 2017).
3. Decreased rank attack (DR): A DR attack involves malicious nodes manipulating their rank values to deceive neighboring nodes into choosing them as parents. This attack aims to disrupt the network's routing process and can lead to suboptimal routing decisions, increased latency, and reduced network efficiency (Nandhini et al. 2023a). In a DR attack, a malicious node artificially reduces its rank value to appear more attractive to neighboring nodes as a potential parent. Hence, This can cause neighboring nodes to select the malicious node as a parent, believing it provides a shorter path to the network's root. By doing so, the attacker can manipulate the network topology, potentially leading to increased EC, data loss (Sharma et al. 2023), or network congestion.
4. Clone attack (CA): a CA involves creating a duplicate copy of a legitimate RPL node to impersonate that node and gain unauthorized access to the network. For example, an attacker could clone the identity of a legitimate RPL node and then use the cloned node to inject false routing information into the network. This could disrupt the routing process Roberts and Ramasamy (2023), cause nodes to route their traffic through the cloned node (potentially allowing the attacker to eavesdrop on or manipulate the traffic), or even cause nodes to become isolated from the rest of the network.
5. Forgery attack (FA): To interfere with the network's functionality, hostile nodes fake or fabricate routing information. This is known as a forgery attack. This attack can result in inadequate routing choices, network congestion, and possible DoS. A malicious node may create and send bogus routing messages, such as DAO or DIO messages Islam et al. (2020), using altered or faked data in a forgery attack. By doing this, the attacker can affect other nodes in the network's routing decisions, leading them to choose less-than-ideal routes or isolate themselves from the rest of the network .
6. Sybil attack: A Sybil attack is a deceptive attack on network integrity in which a malicious entity establishes multiple false identities or nodes to obtain unauthorized influence or control. This malicious strategy in RPL networks entails impersonating multiple nodes to deceive legitimate network participants. These deceitful nodes may appear trustworthy due to their fabricated attributes Platt and McBurney (2023), causing their neighbors to trust them erroneously. Once an adversary has gained access to the network's trust circle, they can manipulate routing paths, inject fraudulent information, and disrupt network operations, resulting in routing inefficiencies and wasted resources. To keep RPL networks safe and reliable, Sybil attacks need to be found and stopped. This

is usually done through authentication, behaviour monitoring, and trust-based routing methods (Hassan et al. 2023). Figure 6 shows the various categories of RPL attacks and their effects on the efficiency of a network (Ashrif et al. 2023).The information above can be summarized in the following Table 4

In addition to the above, Table 4 provides a comprehensive overview of various attacks and their corresponding defense mechanisms, ranging from simple to complex attacks, and the measures needed to mitigate them. There are specific examples of defense mechanisms for each attack category and a range indicating the level of defense mechanism required.

1. High (DDoS, FA, Sybil Attack, VNA): These attacks require comprehensive defense mechanisms due to their ability to overwhelm networks with traffic, fake identities, or manipulate rankings.
2. Medium (Most attacks): Many attacks in this category exploit specific vulnerabilities or involve modifying data. A combination of proactive and reactive defenses is often needed.
3. Low (WH attack): WH attacks are less common and exploit specific protocol weaknesses. However, patching vulnerabilities and network monitoring are still crucial. This classification helps prioritize defense strategies based on the severity and complexity of the attacks, ensuring that resources are allocated effectively to mitigate potential threats.

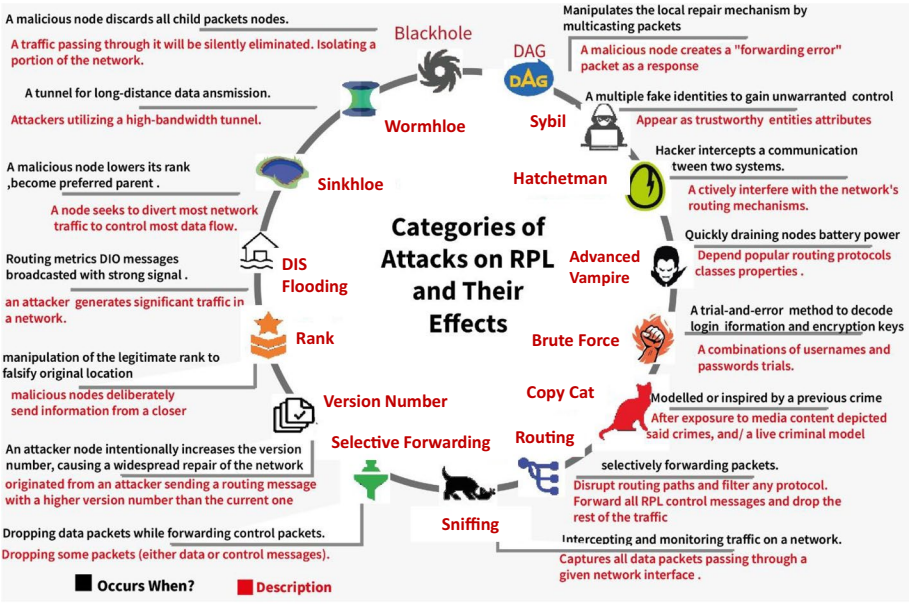

Fig. 6 Categories of attacks on RPL and their effects on the network's performance

Table 4 Attack and defense mechanisms

Attacks	Defense mechanism range	Examples of defense mechanisms
Flooding attacks (FA)	High	- Traffic filtering, rate limiting, anomaly detection, IDS, and firewalls
Replay attacks (RA)	Medium	- Secure protocols and timestamping are necessary. Further actions can be required based on the particular network
Sinkhole attacks (SH)	Medium	- Route validation, reputation systems, blacklisting, traffic redirection,and IDS
Wormhole attacks (WH)	Low	- Protocol patching, secure routing protocols, network monitoring, and IDS prevent exploitation
Denial–of–Service (DoS) Attacks	High	- Traffic filtering, rate limiting, resource monitoring, IDS, firewalls, load balancing
Spoofing attacks (SA)	Medium	- IP address validation, MAC address filtering, data authentication (e.g., digital signatures), secure protocol
Tampering Attacks	Medium	- Data encryption, MA codes (MACs), digital signatures, IDS, data integrity checks
Hatchetman Attack (HA)	Medium	- Secure reputation systems, DAO membership filtering
Sybil attack	High	- Proof–of–stake consensus mechanisms, CAPTCHAs, identity verification
Energy depletion attacks (EDA)	medium	- Low–power communication protocols
Decentralized Autonomous Organization (DAO)	Medium	-Secure coding practices, smart contract audits, DAO voting mechanisms
Forwarding Misbehavior attacks (FMA)	Medium	- Secure routing protocols, anomaly detection systems (ADS)
Copycat attacks (CA)	Medium	- Secure communication protocols (e.g., TLS/SSL), digital signatures
Clone attack	medium	-Device authentication (e.g., MAC address filtering), ADS
DECREASE rank attack (DR)	Medium	- Secure ranking algorithms, reputation systems
Greyhole attacks (GH)	Medium	-Traffic analysis, ADS
Neighbour attacks (NA)	Medium	- Neighbor discovery protocols, ADS
Eavesdropping	Medium	- Data encryption (e.g., AES)
Rank inconsistency (RI)	Medium	- Secure ranking algorithms, reputation systems
Advanced Vampire Attack (AVA)	Medium	- A complex attack that combines multiple techniques. A combination of defense mechanisms against Sybil attacks, DoS attacks, and resource depletion attacks is needed..
Version Number Attack (VNA)	High	- Secure RPL implementations, ADS

3 Related works

The best way to guarantee the sustainability of secure IoT systems is to defend against malicious attacks before they occur. Therefore, detecting and preventing malicious attacks is vital to protecting IoT systems from attacks. Attack detection is possible using a signature-based or predictive approach. However, signature-based methods have difficulty identifying routing attacks that significantly alter their behavior or attack patterns. In addition, anomaly-based detection techniques are more accurate in detecting previously unknown attacks than signature-based ones.

This section reviews the existing research on detecting routing attacks. These studies are classified into two categories, as illustrated in Fig. 7: secure protocol-based and IDS-based mechanisms. The tables in this section also compare performance parameters related to the secure protocol-based and IDS-based mechanisms for securing the RPL protocol.

Detecting and mitigating attacks is paramount in cybersecurity. Various performance metrics are employed to evaluate the effectiveness of detection algorithms, aiding in developing robust security solutions. These metrics help measure the success rate of attack detection, identify false alarms and missed attacks, and assess overall system performance. as shown in Table 5 below.

Researchers frequently use metrics in Table 5 to evaluate proposed systems, helping measure the success rate of attack detection, identify false alarms and missed attacks, and assess overall system performance. These metrics provide a comprehensive assessment of a system's ability to detect and respond to security threats, facilitating the development of effective security solutions.

3.1 Secure protocol-based

This section provides an overview of defense strategies that use secure protocols to safeguard the RPL protocol from routing attacks.

3.1.1 Rule-based mechanism

There are numerous studies on rule-based routing protocol threat detection for IoT. Raza et al. Raza et al. (2013) compared Node IDs and rankings to assign values to look for anomalies. It raises the alarm if a malicious node is found. However, rule-based detection is ineffective for complicated systems and undiscovered attacks since it necessitates many rules, making rule administration challenging. Furthermore, since administrators create regulations based on pre-determined system configurations and known attacks, they must introduce new rules to address different attacks. Meanwhile, Almusaylim et al. (2020) created SRPL-RP, a routing protocol with better security. Its main goal was to find and stop VNA, RPL rank, and VNA by isolating them and adding them to a block list. The detection process involves comparing the ranking mechanism with an alternative one. Their analysis of the protocol's effectiveness shows a 99.92% success rate in detecting routing attacks and a high PDR of 98.48%.

The proposed adaptive threshold (AT) mechanism Dvir et al. (2011) functions by discarding incoming packets that surpass a predefined threshold of 20, triggering a reset of the trickle timer. However, a sophisticated adversary can systematically undermine network performance by transmitting 20 malformed packets per hour. To address this

Table 5 Define performance parameters and metrics

Term	Definition	Interpretation
Lightweight	- A security solution or algorithm that has low computational or resource requirements	- Low: Indicates a low computational or resource overhead. - High: Indicates the opposite
True positive rate (TPR)	- Measures the model's ability to identify TP. For example, a TPR of 95% indicates that 95% of actual attacks were correctly identified with the remaining 5% potentially being false alarms	- High: Indicates a high percentage of attacks correctly detected. - Low:Indicates the opposite
False positive rate (FPR)	- This metric represents the proportion of negative cases that the model incorrectly classified as positive (Measures the model's tendency to generate false alarms.). A high FPR indicates the model produces many false alarms	- High: Indicates a high rate of false alarms. - Low: Indicates the opposite
False negative rate (FNR)	- The percentage of missed attacks or undetected attacks	- N/A
Precision	- The proportion of TP detections out of all positive detections	- N/A
Recall	- This metric measures the proportion of actual positive cases that the model correctly classified as positive. A TPR of 95% signifies that the model identified 95% of the TP in the data	- High: Indicates a high proportion of actual positives correctly identified. - Low: Indicates the opposite
F1–Score	- A combined measure of precision and recall , offering a balanced evaluation of the detection system's performance	- High: Indicates a balanced performance in terms of precision and recall. - Low: Indicates the opposite
Packet delivery ratio (PDR)	- PDR is defined as the proportion of packets that are effectively delivered from their source to the destination	- High: Indicates a high proportion of packets successfully delivered. - Low: Indicates the opposite
Detection accuracy (ACC)	- The percentage of accurately detected attacks out of all attacks	- High: Indicates a high percentage of accurately detected attacks. - Low: Indicates the opposite
Overhead	- Refers to the extra resource consumption, such as energy and processing power, induced by the security approach	- High: Indicates a high resource consumption. - Low: Indicates the opposite

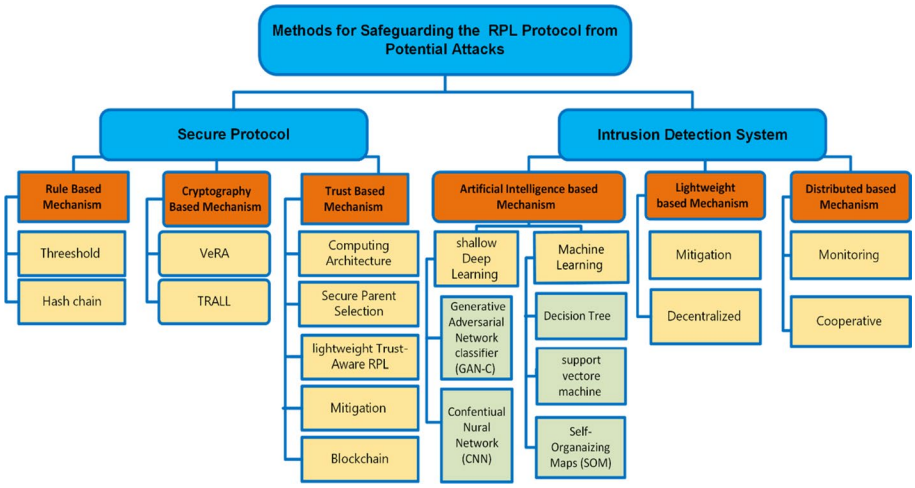

Fig. 7 Taxonomy of methods for safeguarding The RPL protocol from potential attacks

issue, the AT mechanism dynamically adjusts the threshold based on the reception rate, reducing it when the attacker sends packets rapidly and increasing it during periods of inactivity. Nonetheless, this approach requires calculating configuration parameters in advance and not considering node mobility. In a previous study, Mayzaud et al. used an entirely dynamic threshold (DT) mechanism to cut down on DODAG inconsistencies (Mayzaud et al. 2015). Unlike the AT mechanism, which relies on pre-calculated configuration parameters, DT considers the network's dynamic characteristics to establish a threshold for mitigating DODAG inconsistency attacks. It collects all the necessary information directly from the network, including the convergence time of the RPL network. As a result, DT effectively prevents unnecessary resets of the trickle timer, reducing the number of DIO transmissions. DT surpasses AT in packet delivery ratio (PDR), energy efficiency, and end-to-end latency. Furthermore, the DT mechanism proves highly effective in mitigating the forced BH problem.

To defend against many attack types, including SA, BA, SFA, and RAs, the writers Almusaylim et al. (2020) of SRPL designed it. It accomplishes this by starting the attack, confirming it, and then updating the rank in three steps. Every node in the network computes its rank, threshold values, and matching hashed values during the beginning phase. Parents or other nodes confirm the hashed ranks and thresholds during verification. Ultimately, the rank update happens when a node wants to modify its rank. To make sure that any rank revisions are permitted, this adjustment is cross-checked against historical data.

The authors Remya et al. (2024) of "Enhancing Security in LLNs Using a Hybrid Trust-Based IDS for RPL" discuss the security challenges prevalent in LLNs that extensively utilize the Routing Protocol for LLNs (RPL). Their system, TIDSRPL, delegates intricate trust calculations to the root node, mitigating resource exhaustion and conserving energy, storage, and computational capabilities. Through experimentation, TIDSRPL performs better in identifying and isolating malicious nodes, diminishing the average packet loss ratio, and enhancing energy efficiency. These outcomes contribute significantly to the progression of security within IoT networks.

Table 6 Summary of rule-based approaches

References	Attacks	Mechanism	Pros	Cons	Summary and result
Remya et al. (2024)	SH, Sf, Sybil attacks	TIDSRPL	TIDSRPL outperforms MRHOF–RPL in detecting and isolating malicious nodes, reducing packet loss, achieving greater energy efficiency, and enhancing security in LLNs	- The proposed system introduce additional overhead due to the offloading of trust computations to the root node	–NA
Kamel and Elhamayed (2020)	spoofed, SH, and SF	SVELTE	- Less computational overhead. (e.g., processing time< 10ms)	- High false detection TPR (> 10%) - Do not consider the mobility of nodes based	TPR is not (100%)
Raza et al. (2013)	Rank and VNA	Threshold (SRPL–RP)	- The SRPL–RP offers enhanced security and efficiency in terms of network performance and ACC	The proposed solutions do not consider internal rank attackers, and they also overlook the aspect of node mobility	TPR = 99.92% PDR = 98.48%
Mayzaud et al. (2016a)	VNA	Threshold	Potentially locates the attacker	One drawback of this approach is that it relies on high–order devices for monitoring, resulting in increased overhead costs. Additionally, it incurs high deployment costs, which further adds to the method's drawbacks	It presents excellent TPR, And the performance results show a high ACC F1 score (98%)

Table 6 (continued)

References	Attacks	Mechanism	Pros	Cons	Summary and result
Mayzaud et al. (2015)	DODAG inconsistency and Blackhole	Threshold	The suggested approach uses less energy, making it an appropriate option for securing the IoTs network	- The approach did not consider mobility	PDR (99%) Overhead (between 20 to 50%)
Dvir et al. (2011)	Increased rank, SH, and VNA	Threshold/ hash chin SRPL	Mobile supported Through the periodic update of the initial thresholds and their associated hash values	- The thresholds impose additional overhead on both malicious and non–malicious nodes indiscriminately. - Only one attacker is assumed	PDR for the: - single attacker; decreased from (0.97) to (0.26) - multiple attackers; it fell from (0.83) to (0.42). Control overhead:(1330) Energy resources:(0.93)

Table 6 lists secure rule-based solutions defense solutions that secure the RPL protocol, including the pros and cons of each proposed mechanism in providing the desired level of security for IoT networks.

In summary, within the rule-based defense solutions for securing the RPL protocol, only a few works Raza et al. (2013), Mayzaud et al. (2016a) have employed threshold-based approaches. Also, the solutions suggested in these papers only work on a few types of attacks, like DODAG inconsistency, forced BH Mayzaud et al. (2015), and DAO falsification attacks. This leaves a big hole in the research field. Also, the solutions suggested by Kamel and Elhamayed (2020), Raza et al. (2013), and Mayzaud et al. (2015) do not think about how nodes can move around Remya et al. (2024), which could slow down the system (Dvir et al. 2011). Applying such solutions to address other routing attacks is challenging, as determining the optimal thresholds or parameters while considering the network environment poses a significant challenge in designing threshold-based solutions. Some methods have a high rate of false detection because they only look at certain types of attacks Mayzaud et al. (2016a) and do not consider node mobility Mayzaud et al. (2015) or Kamel and Elhamayed (2020) Moreover, the most significant limitation of SRPL Raza et al. (2013) lies in its computationally expensive processes, which consume significant node resources.

3.1.2 Cryptography-based mechanism

Ambarkar and Shekokar Ambarkar and Shekokar (2021) underscored the vulnerability of IoT devices to frequent DoS attacks due to their relatively weaker security measures. They recommend an upgrade to the framework along with the implementation of attack prevention and detection methods to mitigate such attacks. Although the authors recommend using cryptography to protect IoT networks, they are aware of the difficulty that arises from the limited computational power of IoT devices, which can make encryption a resource-intensive process for each data transmission. As an alternative, they propose a hybrid solution that combines IDS with essential security software to ensure low EC by IoT devices. The authors of the proposed solution stress how well their IDS algorithm works at quickly finding attacks and stopping them from doing more damage to the system (Sharma et al. 2023). This mechanism involves trusted third parties and designated nodes responsible for accessing the IEEE 802.15.4 network. However, the system's attack susceptibility stems from the lightweight hash generation method, which does not rely on trusted third parties.

Dvir et al. (2011) introduced a security measure known as VN and Rank Authentication (VeRA) to counter potential attacks by adversaries during routing via RPL using encryption. RPL establishes a DAG with the root located at any gateway and updates the VN when creating a new destination-oriented DAG version. The rank determines the route quality to the final sink node, and an attacker can reduce the node's rank value to eavesdrop on the root. VeRA employs various techniques to verify the authenticity of ranks and VNs, including the SHA hash function, HMAC MAC function, and RSA digital signature. Moreover, RPL calculates a node's rank value based on its preferred parent's rank, which is then broadcast to other nodes. According to the RPL standard, a parent node must have a lower rank than its children. Unfortunately, the research lacks an analysis of network performance.

Landsmann et al. (2013) introduced the Trust Anchor Interconnection Loop (TRAIL) security mechanism to counteract decreasing rank attacks. Their proposed solution employs a chain of nested encryption to prevent attackers from altering hash chains via

multicast, thereby safeguarding rank integrity. To improve topology authentication in RPL, Perrey et al. (2013) improved the TRAIL system to find and stop topological problems. This method enables each node to verify its upstream routing path to the root and identify rank forgery without relying on encryption chains. Additionally, TRAIL can identify and eliminate unauthorized network nodes.

It's worth noting that VeRA is also susceptible to hash chain forgery and replay attacks Dvir et al. (2011), making it more computationally demanding for nodes with constrained resources and more vulnerable to these types of attacks. However, VeRA and TRAIL require maintaining the node's state, leading to memory latency issues for nodes with limited resources (Iuchi et al. 2015). Table7 lists cryptography-based defense solutions that secure the RPL protocol, including the pros and cons of each proposed mechanism in providing the desired level of security for IoT networks.

As shown in Table 7, attackers can exploit replay and rank forgery attacks to undermine certain defense strategies Ambarkar and Shekokar (2021), as demonstrated in. However, some security measures have the drawback of significantly increasing memory and processing resource requirements, making them impractical for real-world IoT networks, as highlighted in (Dvir 2017; Dvir et al. 2011; Perrey et al. 2013). Thus, further research is essential to deepen our understanding of IoT constraints and develop effective, tailored security solutions for IoT networks. Additionally, exploring lightweight cryptography solutions, as discussed in Ambarkar and Shekokar (2021), could provide valuable insights into enhancing IoT system security.

The RPL is crucial for efficient communication in low-power wireless network environments. While cryptographic-based security solutions are commonly used for secure communication, there is a need for non-cryptographic-based security solutions specifically tailored for RPL. This need arises due to several reasons:

1. Avoiding the overhead of cryptographic operations: - Cryptographic security solutions use complicated calculations and algorithms Raeini (2024), which can make it much harder for devices in RPL networks that do not have a lot of resources to communicate and do computations. - The constraints on message authentication (MA) codes make them unsuitable for RPL. MA codes generate a tag or checksum using cryptographic techniques to confirm a message's integrity and legitimacy. Nevertheless, MA codes have limits in the case of RPL networks. First, the RPL network devices have constrained memory and processing capacities. Therefore, they cannot perform cryptographic tasks that demand high processing power, such as generating and validating MA codes.
2. Limitations of Mac-based Solutions for RPL: -Limited Protection: MACs primarily verify data integrity, ensuring messages are untampered during transmission. They do not provide encryption or strong replay protection. In RPL, attackers could capture and replay valid messages Banerjee and Samantaray (2019), disrupting routing. -Resource Consumption: MACs are less resource-intensive than cryptographic solutions but add computational overhead. For highly constrained devices in LLNs, even this overhead can be significant. Non-cryptographic solutions can be designed to be even lighter. -Potential Workarounds: With sufficient resources, attackers could forge MACs if they access the secret keying material. Non-cryptographic solutions, though not flawless, can make such attacks more challenging or computationally expensive.
3. In Summary: Non-cryptographic security solutions are crucial for RPL due to LLNs' resource limitations and scalability challenges. While MACs ensure some data integrity, their lack of confidentiality, replay protection, and resource efficiency makes them less

Table 7 Summary of cryptography approach

References	Attacks	Mechanism	Pros	Cons	Summary and Result
Raza et al. (2013)	DoS and VNA	Cryptography	The proposed algorithm can detect attacks faster, preventing further damage to the system	The system may not guarantee data confidentiality, integrity, and availability	Power consumption (77%), TPR (90%), and FPR (11%)
Agiollo et al. (2021)	VNA and DR	Hashchain /VeRA (SRPL–RP)	- Low–time overhead - mechanisms are implementable in the real scenario	The proposed solution is complex, causing node overhead, resource consumption, and inefficiency. Additionally, the researchers did not evaluate network performance or discuss the implementation of their paper	VeRA effectively detects attacking nodes by utilizing a one–way hash chain
Prakash and Swaroop (2016)	VNA and DR	Enhanced VeRA	- Solving some issues discovered in VeRA	The issue with TRAIL is that a child node can choose an attacking node as its parent, leading to extra overhead when using the Trail method to create a tree in RPL	TRAIL evaluation concerning energy or resource consumption is missing
Deng et al. (2009)	VNA, DR, and RRA	Hashchain /TRALL	Less complicated computations when compared to VeRA	– RRPs are a risk, and the young nodes may choose a danger as their parent. It also adds memory overhead	NA

suitable for RPL security. Ongoing research aims to develop efficient non-cryptographic security mechanisms for RPL Moreira and Kaddoum (2023), ensuring data integrity, confidentiality, and availability in resource-constrained environments

3.1.3 Trust-based mechanism

Many researchers employ trust-based methods, models, and authentication schemes to address attacks in RPL (Muzammal et al. 2022). Examples include research using Random Forest (RF) and subjective logic to identify SH attacks and IDS to solve fabricated parent-change vulnerabilities. Meanwhile, there is also work on a trust-based authentication scheme that mitigates rank, Sybil, BH, and man-in-the-middle attacks. In other research based on trust, a simple defense against the DIS attack was proposed Guo (2021). It also suggested a way to balance the load to stop DIS and HF attacks Avila et al. (2020) and improve the candidate parent nodes in RPL (Sahay et al. 2022).

Trusted Computing Architecture (TCA) Seeber et al. (2013) provides to establish trust and secure key exchange between nodes using a trusted platform module (TPM). The author used low-cost TPMs to add security to nodes that did not have a lot of resources. This was done to protect against node tampering, DoS attacks, and routing attacks that try to break integrity and availability. The TPM is essential to this design because it supplies the keys for safe communication between authenticated nodes. However, it also acts as a single point of failure, and if it is tampered with or breaks down, it may cause security lapses and a decline in network performance. Unfortunately, the work lacks a detailed simulation or review to verify its performance or effectiveness. Iuchi et al. Iuchi et al. (2015) suggested a secure parent selection strategy based on trust and threshold to defend against rank attacks in RPL. Through this process, each node in the network chooses its desired parent because genuine nodes are assumed to have far greater ranks than those that are not legitimate. The nodes compute their neighbors' maximum and average ranks and exclude nodes with ranks below the threshold to prevent forwarding packets to illegitimate nodes. While this method enhances parent selection security, it does have two limitations. Firstly, it may result in suboptimal routes since legitimate nodes may not always be selected as parents. Secondly, it is susceptible to Sybil and BH attacks, which undermine its effectiveness.

Mayzaud et al. Mayzaud et al. (2016a) When most nodes are near the root node and have a higher rank, a trust-based technique was suggested for minimizing VNA by altering the VN. Sahay et al. Sahay et al. (2020a) proposed a Blockchain-based framework to enhance the security of the RPL routing process by defending against rank and VNA. In their research, the authors investigated RPL vulnerabilities and proposed a Blockchain-powered attack detection module for IoT networks. The framework establishes a secure and reliable data connection between the RPL network and an attack detection module based on machine learning. It implements an eXtreme Gradient Boosting (XGBoost) classifier on a private Blockchain network to detect rank and VNA attempts effectively. Table8. shows a summary of trust-based mechanisms.

In summary, the analysis of secure protocol-based mechanisms presented in Table8 reveals several significant limitations. Firstly, some solutions suffer from a single point of failure, while others are vulnerable to frequent attacks such as SH and BH Mayzaud et al. (2016a) and (Iuchi et al. 2015). EC is one of the most pivotal considerations when designing an RPL security algorithm. Unfortunately, several existing approaches necessitate nodes to operate in promiscuous mode, leading to substantial energy drain Sahay et al. (2020a), Sahay et al. (2022), and (Pishdar et al. 2022). researchers must address these

Table 8 Secure protocol-based (trust-mechanisms)

References	Attacks	Mechanism	Pros	Cons	Summary and Result
Maikol et al. (2021)	Rank, Sybil and BH	With a mobile sink, the proposed solution focuses on authentication and trust–based IoT security	The suggested Sec RPL –Ms outperforms existing systems, with a 23% identification	Frequent loss of IoT nodes, the other registration process for authentication of nodes, is alleviated	PDR = 97.1%, ACC =96.9%
Avila et al. (2020)	DIS attack	A lightweight / thresholds	identifying and isolating DIS attack perpetrators can reduce its effects and improve network security	ignores WSN–inherited attacks; Only defends against DIS–based attacks	PDR = 75%, E2E Delay= 45% PC = 150 pkt/s
Mayzaud et al. (2017)	DIS & FA	The proposed solution aims to distribute the load among multiple nodes	The proposed work finds and stops DIS FAs so that control packets take up less space and use less energy	Targeting load balancing to avoid FAs; It ignored network –related attacks	PDR = 96%
Prakash and Swaroop (2016)	Increasing rank	Threshold	compared to the conventional RPL scheme, reducing the total number of child nodes attached to attacking nodes	– Numerous attacks, including the Sybil and BH attacks, pose a threat	NA
Landsmann et al. (2013)	BH and SF	Lightweight/ Sec Trust	The proposed solution ensures that it does not cause excessive overhead on network traffic	–The proposed solution suffers from increased EC, primarily due to the circular path–based movement of the sink	Acc =76.25%, PDR =77.8%

Table 8 (continued)

References	Attacks	Mechanism	Pros	Cons	Summary and Result
Mayzaud et al. (2016a)	Worst Parent	Enhanced RPL (ERPL)	ERPL uses less power and works better than RPL, which is well–suited for IoT applications	Non–optimized topology & routes	PDR = 63%

challenges comprehensively before implementing the proposed solutions in real-world networks (Mayzaud et al. 2017). A robust security algorithm should address the vulnerabilities, optimise energy usage, and adapt to dynamic network conditions to ensure long-term efficacy and resilience.

3.2 IDS-based mechanism

This section covers a range of defense solutions that use IDSs to identify routing attacks against the RPL protocol. These IDSs are distinguishable by their properties, such as being Artificially Intelligent, Lightweight, and Distributed. The subsequent sections provide more details about each IDS type (Garcia Ribera et al. 2022).

3.2.1 Artificial intelligence (AI)-based mechanisms

AI and IDS can work together in IoT networks to detect and stop security threats. With AI algorithms, IDS can analyze network traffic in real-time to identify potential threats while correctly monitoring it for any unusual activity. Moreover, AI can help to increase intrusion detection ACC and decrease false alerts.

3.2.2 A. Deep learning (DL)-based mechanisms

DL techniques perform superior to traditional data processing methods when dealing with large-scale data (Anitha and Arockiam 2021). Numerous studies have proposed using DL in various domains, including routing attack detection in IoT networks.

Yavuz et al. Yavuz et al. (2018) developed a scalable routing attack detection system based on DL for IoT using Cooja emulation and the Contiki operating system. They created a dataset that included three categories of RPL attacks: HF, DR, and VNA. They attained impressive ACC rates of 94.9% for the decreased rank attack, 99.5% for the Hello deluge attack, and 95.5% for the VNA by utilizing a deep neural network (DNN) model.

As shown in another study Diro and Chilamkurti (2018), the NSL-KDD traffic distribution dataset was used to create a distributed IoT network attack detection system based on DL. Their model outperformed traditional ML methods such as support vector machines (SVM), decision trees (DT), and other neural networks (NN) in terms of ACC, TPR, false alarm rate, F1 measure, recall, and precision. The proposed DL model significantly improved the ACC from approximately 96% to above 99%, enabling precise identification of IoT attacks in the distributed architecture of IoT applications. These findings highlight the efficacy of DL in detecting and mitigating IoT attacks, particularly in scenarios involving large-scale and distributed IoT networks.

Nayak et al. NAY (2021) introduced a DL-based model to detect routing attacks in RPL networks utilized in the Industrial IoT. The proposed model exhibits remarkable capabilities in accurately distinguishing between genuine and misleading data, detecting attack events, and classifying the attack types into their respective categories. The authors employed adversarial training techniques to enhance the model's detection capabilities against intended routing protocol attacks in RPL. They developed a GAN-C model by combining GAN with SVM. This fusion of GAN and SVM displayed superior performance in detecting planned assaults in RPL, surpassing the effectiveness of traditional methods.

Kamel SOM et al. Kamel and Elhamayed (2020) introduced a novel approach that leverages CNN to predict suspicious traffic in IoT networks and detect routing attacks. The

researchers utilized a dataset of five attack groups for training their model. The authors employed three pre-processing methods on the dataset to enhance the model's performance: feature selection, Chi-squared, and weight by tree importance. These techniques were crucial in reducing overfitting and noise in the input data, improving the model's overall effectiveness. Table9. provides a summary of essential parameters, benefits, and drawbacks of DL-based techniques (Anitha and Arockiam 2021).

In summary, specific proposed models face notable limitations, including extended training times and susceptibility to attacks targeting specific layers (Yavuz et al. 2018). Additionally, some models have low detection rates, a problem that the integration of DL models with higher receiver operating characteristic (ROC) scores could solve. A compelling finding emerges from research showcasing the stability of the Very Narrow AI (VNA) classification, illustrating its insensitivity to specific class distinctions, be they majority (12 VOLUME 4, 2016) or minority (Diro and Chilamkurti 2018). However, there are still problems with openness. Some authors do not give important information about the datasets and features they chose, and basic parameters like PDR, Precision-Recall Curve PRC, and E2E latency are missing from their published results: Kamel and Elhamayed (2020), Sahay et al. (2020b), and (Rouissat et al. 2022). Another issue is that some solutions only work on Very Narrow AI (VNA), which makes people wonder how well they can protect against a wide range of attacks Sahay et al. (2020b) and (Rouissat et al. 2022).

3.3 B. Machine learning (ML)-based mechanisms

This section summarizes advancements in ML-based attack detection models. It focuses on RPL routing and attacks commonly used in IoT environments with limited resources and LLN (Seyfollahi and Ghaffari 2021). Table 10 IDS to ML

Osman et al. Osman et al. (2021) described ML-LGBM as a way to find VNA (Virtual Node Attack) in RPL-based IoT networks. The method utilized a Gradient Boosting Machine for VNA detection as its central component. In their research, the authors completed multiple phases, including the design of the RPL network, data acquisition and preprocessing, feature selection, and the development of the ML model. Creating a substantial dataset, extracting pertinent features, implementing an LGBM-based classification algorithm, and optimizing model parameters were required. The evaluation results demonstrated the effectiveness of the ML-LGBM model, achieving remarkable performance metrics such as 99.6% Acc, 99% precision, 99.6% F-Score, 99.3% TNR, and a low FNR of 0.0093. We got better ACC, precision, and F-Score results than other methods. This shows that the proposed ML-LGBM model is better for finding VNA in RPL-based IoT networks.

Sahay et al. Sahay et al. (2020b) proposed a framework for detecting VNAs in IoT systems, which can be deployed in the cloud or at the edge of IoT-LLN networks. Regardless of its deployment location, the framework aims to accurately detect VNAs without misidentification. The edge detection process is divided between cloud services and fog computing. Different steps are needed to build the framework, such as filtering the input features, preprocessing the features, and using machine learning classification algorithms like DT, SVM, RBM, and LR. Various parameters, such as VNA variations and the number of VNA changes, are used to identify VNAs in the network. Once an attack is detected, the root node is alerted to blacklist the malicious nodes involved. Simulation results demonstrate the framework's effectiveness, achieving an Acc of 98%, precision of 100%, and specificity of 100%. The recall results show that DT, Bernoulli RBM, and LR achieved a recall rate of 95%, while SVM achieved a recall rate of 94%. Overall, Sahay et al.'s

Table 9 IDS-based deep learning

Ref	Attacks	Mechanism	Pros	Cons	Summary and Result
Iuchi et al. (2015)	VNA, HF and DR	MLP Based ANN	Creates a new dataset and makes it available to other researchers	– Long Training Time. – Major Disadvantage: Attack datasets generated via simulation, not real Data traces	F1–Scores: DRA (94.7 %), HF (99%), and VNA (95%), AUC: DRA (94.2%), HF (98.1%), and VN (94.7%)
Perrey et al. (2013)	VNA, HF, and DR	GAN–C and SVM (Hybrid)	In terms of detection and response cycles, the distributed GAN–C model performs better than its centralized counterpart	The proposed approach requires a lot of computational resources, which resource–constrained IoT devices cannot provide	F1–Scores: VNA (70%), HF (83%), and DRA (92 %), Precision: VN (73%), HF (84%), and DRA (93%) Recall: VNA (68%), HF (82%), and DRA (92%)
Muzammal et al. (2022)	VNA	Threshold / neural network	The proposed approach demands a lot of computational resources, which resource–constrained IoT devices cannot Provide	It is specific to VNA, and unknown whether it can defend against other attacks	The classification ACC of the neural network is greater than 97%
Rakesh (2023)	VNA	Lightweight/mitigate	Minimizes EC and network overhead	The evaluation results may not correctly reflect real–world applications because they are simulation–based using the Cooja simulator under Contiki OS	Energy saving (58%), and control overhead (81%.)

Table 9 (continued)

Ref	Attacks	Mechanism	Pros	Cons	Summary and Result
Mayzaud et al. (2017)	HF, SF, SA, WA, and VNA	Mitigation/CNN	The study succeeded by detecting attacks with minimal error and loss rates and lowering PRC while preserving IoT network stability	–NA	ACC(96.87%), Precision,(94.85%), Error Rate (3.13%), Recall (99.65%), Correlation,(93.8%), and F–(0.32%)
Ambarkar and Shekokar (2021)	Distributed network attack detection	Distributed	DL models are more accurate than conventional ML techniques in identifying IoT attacks	The NSL–KDD traffic distribution dataset employed in the study might not accurately represent all IoT traffic patterns, which could reduce the applicability of the findings	AC (96–99+ %)

Table 10 IDS-based machine learning

Ref	Attacks	Mechanism	Pros	Cons	Summary and Result
Muzammal et al. (2022)	VNA	DT, SVM Bernoulli and LR	The framework introduced in the study showed significant accuracy, precision, recall, and specificity results	– There was no evaluation of other critical metrics, such as PDR, PRC, and E2E delay – This work is restricted to detecting only one type of attack	Recall (95%), SVM (94%), AC (98%), Precision (100%), and Specificity(100%
Rakesh (2023)	DR,BH, SH,and SF	Genetic Recursive Feature Selection and Fuzzy K–Nearest Neighbor	The suggested system demonstrates superior accuracy in detecting attacks while utilizing minimal RPL attack–based IDS	– Evaluation of other critical metrics, such as PDR, PRC, and E2E delay, not provided – No mobility considered	Accuracy (98%)
Guo (2021)	HF,SH and VNA	Self–Organizing Maps/(SOM)	Due to the SOM's ability to classify attack types into four unique classes, it is possible to have a more thorough grasp of the type and severity of an attack	– No clear indications on the placement of the IDS and its power consumption in this study. – There is a significant implementation overhead. – No mobility considered	And the performance results show a high ACC F1 score (98%). It Clusters the Attacks and Normal traffic
Sahay et al. (2022)	VNA	Gradient Boosting & LGBM	The work presented in the study outperformed other methods in several metrics, such as training time, testing time, modelsize, and others	–No details are available on the generated dataset's availability. – Using small network nodes during the dataset'sgeneration process	AC (99.6%), precision (99%), F–Score (99.6%), TNR (99.3%), and FNR (0.0093)

Table 10 (continued)

Ref	Attacks	Mechanism	Pros	Cons	Summary and Result
Seeber et al. (2013)	HF,SH, and WH attacks	BFS–CFS, GS–CFS, MLP, SVM, J48, Naïve Bayes, Logistic, and RF	CHA–IDS outperforms SVELTE	– It cannot locate the attacker. – Technique requires a high–end machine. – No mobility considered	TPR (99 %)
Dvir et al. (2011)	VNA, HF, and DR	Six Types of ML Classifiers: DT, RF, KNN, NB,MLP, LR	generated a new dataset and publicly published It for other researchers	– It requires a long training time. – The attack datasets were simulated and not from actual data traces	–F1–Scores: DRA (94.7%), HF(99%), and VNA (95%), –AUC: DR Attack (94.2%),HF (98.1%), and VNA (94.7%)
Simha et al. (2020)	HF,DR,and VNA	ANN	The proposed approach achieved the highest accuracy results using the hold–out validation technique	–No information is available regarding the collected features. –The author used a small network size for the dataset collection	AC (100%)

framework provides a robust approach for detecting VNAs in IoT systems, offering deployment flexibility and delivering high Acc and precision in attack detection.

Rouissat et al. Rouissat et al. (2022) developed a new IDS based on ML algorithms to detect attacks in IoT-based LLN. It consists of two phases: feature selection and classification. In the feature selection phase, attributes are ranked based on their weighted function. In the classification phase, a fuzzy k-NN classifier efficiently detects RPL attacks. In summary, the IDS collects data from a simulator, selects optimal features using a genetic and recursive feature selection algorithm, and performs classification using the fuzzy k-NN classifier implemented in Python.

Sharma et al. Sharma and Verma (2021) created a machine learning (ML) method for finding routing attacks in RPL. They did this by simulating three types of routing attacks (HF, DRA, and VNA) and using an artificial neural network (ANN) to find them. One part of the proposed ANN-based IDS workflow was to set up network scenarios, watch how networks react to attacks, collect and process data, use ANN to sort and analyze network traffic, tune ANN's performance, and test the ANN using hold-out and k-fold cross-validation methods. The authors evaluated four simulation scenarios, each representing a distinct form of attack, except the concluding scenario, which incorporated them all.

In contrast to HF attacks, where the malicious node is the one that generates the most packets, in VNA, the attacker stimulates nearby nodes to do so. On the other hand, DRA initiated fewer packets than the other two attacks. The authors compared the performance of hold-out and k-fold cross-validation methods and found that the former required less time to attain 100% Acc. Moreover, they employed ten-fold cross-validation to avoid overfitting issues. Eventually, the ANN model achieved an Acc of 100% after optimizing its hyperparameters (Abhinaya and Sudhakar 2021).

Napiah et al. Napiah et al. (2018) developed a centralized IDS called CHA-IDS to detect High HF, SH, and WH Attacks in IoT networks. CHA-IDS leverages compression header data to identify single and multi-attacks, utilizing a best-first and greedy sequential technique for feature selection based on correlation to identify the most crucial components. These features are evaluated using six ML algorithms: DT, LR, Multi-layer Perceptron (MLP), Naive Bayes (NB), RF, and SVM to distinguish between legitimate and malicious communications. Compared to SVELTE and the IDS proposed in [44], CHA-IDS demonstrates superior performance. However, it has some drawbacks, such as a high memory and energy footprint. Additionally, it is incapable of identifying the perpetrator. CHA-IDS by Napiah et al. provides an effective centralized IDS solution for detecting specific attacks in IoT networks. It utilizes compression header data and ML algorithms for accurate classification. It yields promising outcomes but must address resource consumption and offender identification.

Kfoury et al. (2019) presented a system for detecting SH Attacks, Virtual Node Attacks, and High HF attacks using Self-Organizing Maps (SOM) to cluster normal and attack traffic. They made use of data from a Cooja simulator's PCAP (packet capture) file. The system comprises three components: an aggregator module, which collects data from the PCAP file; a normalizer, which standardizes the aggregated data; and a trainer module, which trains the SOM. The output is a matrix that can be visualized as a 2D image to display the clusters. Table10 summarizes studies that employed ML for ID in RPL networks.

In summary, the reviewed studies' AC levels differ due to their varied methodologies. While some accomplished commendable AC, they were not devoid of obstacles, such as increased memory and energy utilization, long training time Anitha and Arockiam (2021), Kfoury et al. (2019), Sharma and Verma (2021), Osman et al. (2021), and no mobility considered Rouissat et al. (2022), (Napiah et al. 2018). Therefore, additional research is

urgently needed to improve the accuracy and effectiveness of these models. Several studies concentrated narrowly on particular attack categories and lacked transparency regarding the availability of data sets (Sahay et al. 2020b). In addition, the reliance on sparse network nodes affected the dataset's quality, revealing potential biases. One study obtained remarkable AC Sharma and Verma (2021) and positive results for metrics such as PRC using the hold-out validation technique. Unfortunately, the absence of transparency regarding the features acquired in these experiments poses a significant hurdle for comprehensively evaluating their methodology. In the future, addressing these limitations is crucial. To make ML-based IDSs work better in RPL networks, we need to improve model accuracy and efficiency, ensure they cover all kinds of attacks, and ensure everyone knows how the datasets are being used. By concentrating on these areas and developing robust defenses against various security threats in RPL networks, future research can uncover the full potential of machine learning.

3.4 Lightweight-based mechanisms

Nikravan et al. Nikravan et al. (2018) introduced a signature-based technique for RPL networks, where distinct nodes run different algorithms, demonstrating its safety and energy efficiency.

Aris et al. Arış and Oktuğ (2020) proposed two mitigation techniques with varying resource requirements Nikravan et al. (2018) and performance. The first technique blocks virtual node updates from leaf nodes, while the second allows a node to change its VN only if most of its higher-ranked neighbors also claim a VN update. These techniques reduced delay, controlled message overhead, improved data packet delivery, and increased the delivery ratio by up to 87%, 63%, 71%, and 86%, respectively. CDRPL is a collaborative and distributed security scheme that was created to make RPL more resistant to virtual node attacks (VNA) (Mayzaud et al. 2017). It provides fast and accurate attack detection, quick topology convergence, and effective network stability and EC. Meanwhile, Anitha Anitha and Arockiam (2021) proposed another method to mitigate VNAs by comparing the VN to the root node's version and triggering a validation phase if there is a mismatch.

Belkheir et al. Belkheir et al. (2022) developed a novel, lightweight, decentralized approach to mitigating VNAs in RPL-based IoT networks. The proposed solution modifies a node's fundamental DIO processing to maintain the same root VN and only takes VN updates from the preferable parent. Simulations demonstrated that the proposed solution provided superior performance, including energy savings of 58% and a reduction in control overhead of 81%, depending on the perpetrator's position within the network.

Additionally, researchers have proposed numerous collaborative and distributed security strategies to address RPL's security issues. You can use a mitigation technique that stops updates or only lets changes happen with majority approval Raoof et al. (2018), compare VNs to the root and start a validation phase if there is a mismatch (Mayzaud et al. 2017), or set up a trust-based method that uses Contikimac Sleep Mode (CSM) (Ahmed and Ko 2016). Adjusting a node's processing to maintain the same VN as the root and only accepting updates from the selected parent Belkheir et al. (2022) is another straightforward and decentralized method. Depending on the attacker's position, the solution enhances performance by conserving energy and decreasing control overhead. These techniques can aid in preventing source-based attacks and improve the security and efficacy of RPL-based IoT networks.

The study Azzaoui et al. (2024) presents an RPL-based lightweight cooperative IDS for Internet of Things networks. It attempts to solve the difficulties associated with implementing IDS in IoT devices with little resources by creating a productive plan that works with the RPL protocol. To identify malicious traffic, the IDS method uses a lightweight artificial neural network (ANN) model-equipped parent nodes that have been chosen as distributed agents. Working at several layers-application, presentation, network, and MAC-the technique enables packet collection and analysis in conjunction with RPL. Using the Contiki OS and Cooja simulator, the RPL-IDS system was implemented and assessed, showcasing its low weight and high detection rates with little energy use. The study also examines related research in IDS for IoT networks, classifying IDS systems according to their deployment tactics and reviewing different methods and algorithms suggested for IoT networks. Overall, the paper offers a fresh take on IDS in IoT networks, combining resource efficiency, cross-layer collaboration, and lightweight design to improve IoT system security.

3.4.1 Distributed-based mechanisms

A distributed IDS necessitates that each network node be configured with a complete IDS implementation, allowing it to detect intrusions at any stage effectively. Several investigations have suggested the following distributed techniques:

Mayzaud et al. Mayzaud et al. (2017) proposed a way for monitoring nodes in RPL networks to work together and share information to find VNAs (Mayzaud et al. 2016a). However, the defense architecture only assumes one attacker and does not consider mobility. Ahmed and Ko Ahmed and Ko (2016) proposed a cooperative approach to improve the detection of malicious nodes, but the false detection rate increases with the number of attackers.

Table 11 summarizes lightweight and distributed IDS techniques' essential parameters, benefits, and drawbacks. It is crucial to note that these proposals have varying resource requirements and performance Almusaylim et al. (2020), and their efficacy may depend on the specific use case and network environment(Azzaoui et al. 2024). Additional investigation and experimentation may be necessary to identify the most effective solution for a given scenario. Table 11 summarizes lightweight and distributed mechanisms.

In summary, various proposed techniques utilize distributed monitoring buildings, where monitoring nodes share information collaboratively. However, this method often results in a higher rate of FPR, especially when dealing with multiple wrongdoers. Hence, there is a crucial necessity for improvements to ensure the ACC detection of multiple malicious nodes. Future research endeavours should devise strategies accommodating multiple adversaries and dynamic node mobility patterns. Additionally, refining the cooperative verification methods to minimize false positives is pivotal. There is also an urgent need to advance techniques to identify narrow AI threats within RPL networks. By overcoming these limitations, the proposed method can transform into a robust and dependable defense mechanism capable of countering a broader spectrum of sophisticated attacks.

4 Critical review

RPL is an IoT routing protocol designed to facilitate communication among resource-constrained devices. However, RPL networks are vulnerable to attacks that target network resources, topology, and traffic. These security vulnerabilities raise significant concerns for

Table 11 IDS based-Lightweight & Distributed

References	Attacks	Mechanism	Pros	Cons	Summary and Result
Azzaoui et al. (2024)	Dos,Routing attacks	lightweight /cooperative	–Suitable for IoT devices with limited resources It boasts high detection rates compared to existing schemes and incurs minimal energy overhead	–The need to balance detection accuracy with resource consumption, may apply	–The experimental results indicate that RPL–IDS is lightweight and can be deployed on devices with limited resources
Anitha and Arockiam (2021)	VNA	Lightweight / Mitigate	Compared to other options, SRPL–RP demonstrated higher levels of effectiveness in detecting and addressing the issue [6]	–The proposed mechanism did not Support Multiple Attacks. – It does not incorporate mobility [61]	–Average delay: decreased to (87%), PDR(92.68 %), Control overhead (decreased by 71 %), AR (92.93%), and EC (1314.884)
Simha et al. (2020)	VNA, RS, and RRAs	Lightweight / Mitigate	The scheme works well for environments with limited device resources due to its minimal EC and processing time	–It is probable that the strategy will not work with all types of devices with limited resources. – It is probable that the strategy will be unsuccessful against other types of attacks	Reduction in delay (87 %), control message overhead (71%), PDR (86 %), Computation time (5.23), and EC (132.426)
Nikravan et al. (2018)	VNA	Lightweight /decentralized. solution	The simulations run for various scenarios verified the efficacy of the suggested approach for increasing the network lifetime	The approach did not consider mobility traits and EC	Reduced control overhead (81%), and increased energy saving (up to 58%)

Table 11 (continued)

References	Attacks	Mechanism	Pros	Cons	Summary and Result
Raza et al. (2013)	VNA	Distributed	Potentially locates the attacker	–The inclusion of high–order devices for monitoring purposes introduces additional expenses in terms of overhead costs. –However, a limitation of this work is its restricted capability to detect only a single type of attack	–NA
Kamel and Elhamayed (2020)	VNA	Distributed	The proposed technique can more accurately detect malicious nodes, which is crucial for identifying and mitigating network security problems	–No evaluation exists for the extra communication overhead. – misuse the neighbors' resources	TPR (95%), PDR (95%), and Control overhead (1500vs)

the overall security and operational longevity of RPL networks, as discussed in Sects. 3. Numerous researchers have proposed defense solutions categorized as Secure Protocols or IDS to address these concerns, as tabulated in Tables 6, 7, and 8.

It's worth noting that most of these research studies have primarily focused on single-attack detection and addressed only specific types of attacks, such as DODAG inconsistency and FH attacks. Furthermore, a common limitation observed in many of these studies is their inability to achieve high detection ACC, which often results in increased EC and vulnerability to attacks like BH attacks.

Tables 9, 10, and 11 highlight that IDS solutions have been widely employed to enhance the security and extend the lifetime of IoT networks. The existing research shown in Tables 9 and 10 also suggests that AI techniques, especially DL models, could help make IoT networks last longer and easily find IoT attacks. The studies have predominantly focused on the VNA as a primary threat in RPL-based networks, as indicated in Tables7, 8, and 9.

However, these studies have identified several notable challenges in detecting attacks in RPL networks. These challenges include long computation times and complexity, which limit the number of attacks that can be effectively detected. Based on a comprehensive literature analysis, it is evident that there is a critical need for a robust and efficient solution that can extend the lifetime of RPL networks. Such a solution should incorporate additional features that enable a single model to effectively detect multiple types of attacks.

1. Characterization of the Results: Following an extensive evaluation of 41 articles, we have exhaustively examined the application of diverse security attacks in the context of the IoT and compared it with the findings of existing reviews. The investigation outcomes presented in this section of the compiled articles are methodically structured based on the analyzed subject matter and scrutinized under three major groupings: surveys, reviews, and taxonomy. Figure 8 shows the attack distribution in the reviewed research. Notably, the most frequently researched attack on RPL protocol in the literature is the VNA, as depicted in Fig. 8. Some papers supported the idea of multiple topologies, and some discussed the issue of various attacks, as shown in Fig. 9. However, there is a

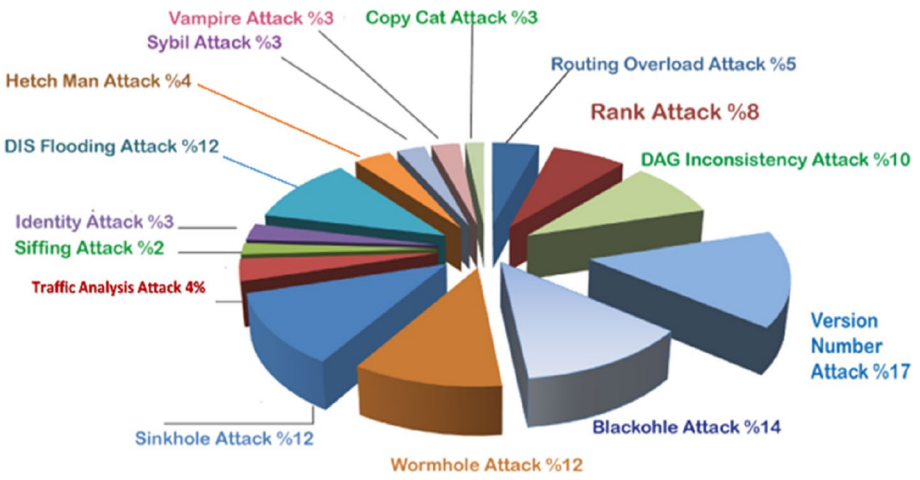

Fig. 8 Attack distribution in the reviewed research

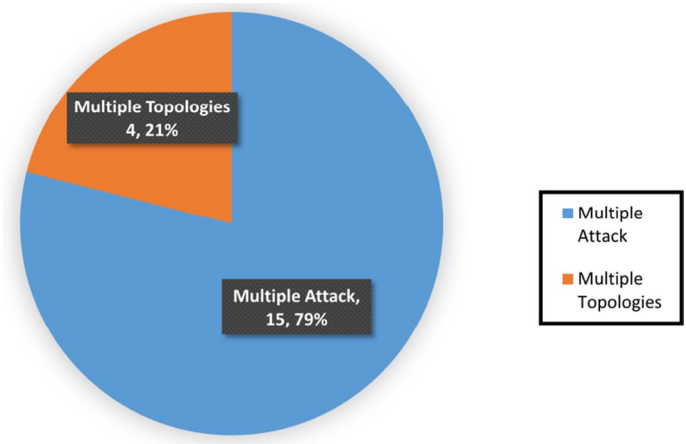

Fig. 9 Multiple attacks & multiple topologies

need for more support for more than one topology and for discovering and solving the problem of different attacks, which could be potential future research.

2. Techniques to Detect Attacks Against RPL protocol: Numerous essential IoT applications operate within networks that have limited resources. These applications require lightweight, secure, scalable, and well-supported solutions to ensure user security and privacy. As depicted in Fig. 10, researchers have proposed various approaches to detect and mitigate attacks targeting RPL networks. Trust-based methods have gained significant attention in addressing these challenges. Additionally, some researchers have explored cryptography-based or rule-based solutions, although their popularity is rela-

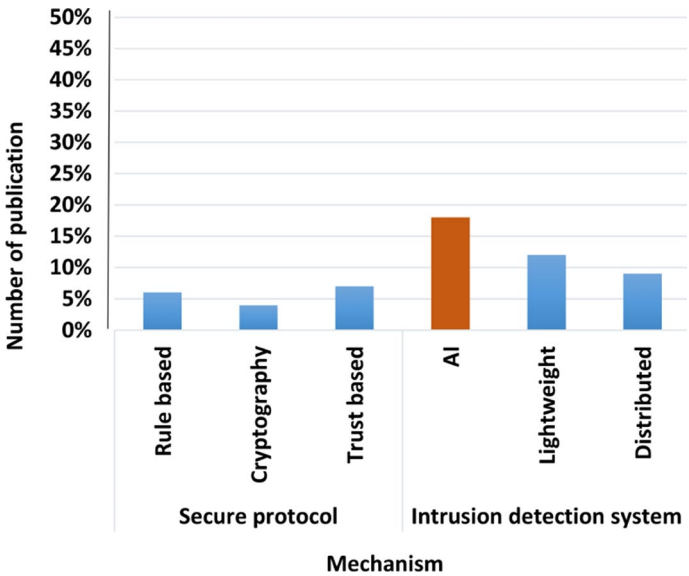

Fig. 10 Summary of techniques to detect attacks against RPL protocol

tively lower in resource-constrained networks. Figure 10 shows a summary of techniques to detect attacks against the RPL protocol. Based on Figure 10, researchers have increasingly turned to AI-based IDS to detect RPL protocol attacks in IoT networks. There are several reasons for this trend. First, the RPL protocol is prevalent in IoT networks, and traditional IDSs may struggle to detect attacks that exploit the protocol's vulnerabilities. On the other hand, AI-based algorithms are trainable to identify these attacks based on patterns in network traffic. Additionally, IoT networks create a large amount of data, which can be challenging to control with conventional IDS equipment. Nevertheless, AI-based algorithms can rapidly analyze and interpret this data, enabling threats to be identified and dealt with in real-time. Lastly, algorithms founded on AI can adapt and learn from new data, which improves their ability to detect previously undetectable attacks and enhances the overall security of IoT networks. Nonetheless, one of the potential limitations of AI-based IDS algorithms is the elevated risk of encountering false positives and negatives. False positives arise when the algorithm mistakenly identifies an attack that did not transpire, leading to the allocation of time and resources for investigating non-existent threats, resulting in a false alarm. Conversely, an FN arises when the algorithm fails to recognize a genuine attack, permitting it to inflict undetected damage on the system. These errors can be attributed to various factors, including inaccurate training data, inadequately constructed algorithms, or changes in the network environment that the algorithm cannot adapt to.

3. Algorithms and results: Algorithms are critical in any security solution to detect and prevent attacks, including VNA, RA, and BH attacks. Additionally, the algorithm's ability to operate efficiently in resource-constrained environments while maintaining network performance and minimizing EC makes it an essential component of any secure RPL-based network. Overall, the algorithm's capacity to enhance the security of the RPL protocol and improve the reliability of IoT applications underscores its significance in safeguarding the network against potential security breaches. This section highlights

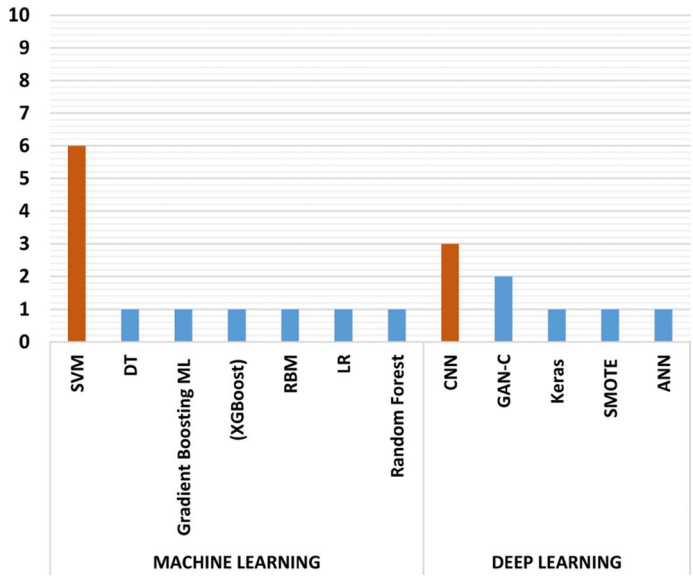

Fig. 11 Summary of AI algorithms

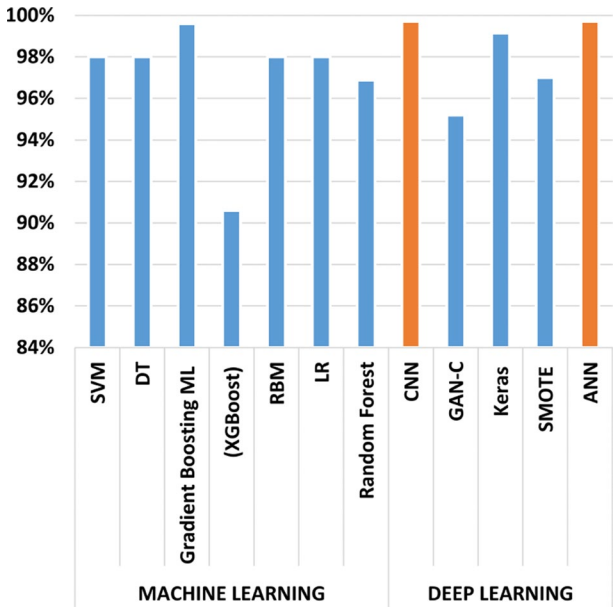

Fig. 12 Accuracy of AI algorithms

the algorithms referenced in the literature cited in this study, which emphasizes the importance of AI algorithms in addressing attacks on the IoT, as shown in Figs. 11 and 12. As shown in Fig. 11, existing literature suggests SVM is the most popular ML algorithm among researchers. Its popularity is because it is trainable on fragmented data containing normal and abnormal network traffic to detect patterns that differentiate them. Following the training, the algorithms can detect new instances of anomalous network behaviour that may imply a potential intrusion attempt. Nevertheless, DL algorithms, specifically CNNs, yielded more precise outcomes than others, as shown in Fig. 12.

Attack distribution in the reviewed research

5 Qualitative comparisons with existing reviews

We conducted a qualitative comparison to highlight the uniqueness of our work compared to other routing protocol-based attack reviews as tabulated in Table 12. The comparison relies on two metrics: the RPL architecture and the classification of attacks in RPL-based IoT, based on an intensive study of existing attacks. It is essential to perform such a comparison to understand the critical issues related to routing protocol-based attacks in IoT networks and identify the most active attacks on routing protocols. Additionally, this comparison could guide future researchers in a similar field.

Table 12 shows that the VNA and HF attacks are the most reviewed among researchers, followed by WH, SH, and BH attacks. A few researchers also investigated DAG, DR, and identity attacks. However, the lesser attention given to the remaining attacks suggests that they are either straightforward to detect or pose implementation challenges within RPL networks.

Table 12 Qualitative comparisons with existing reviews

References	Recourse					Toplolgy		Traffic				
	RPL Architecture	DIS–HF	Routing tables overload	Rank	DAG	VNA	SH	WH	BH	Traffic Analysis	SA	Identity Attacks
Dhingra et al. (2022)	–	✓	–	–	–	–	–	–	–	–	–	–
Jahangeer et al. (2023)	✓	–	–	–	–	✓	–	–	–	–	–	–
Simha et al. (2020)	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Azzaoui et al. (2024)	✓	✓	–	–	–	–	–	–	–	–	–	–
Thubert et al. (2018)	–	–	–	–	✓	–	–	–	–	–	–	–
Omar et al. (2023)	✓	–	–	–	–	–	✓	–	–	–	–	–
Al–Amiedy et al. (2022)	✓		–	✓	✓	✓	–	–	–	✓	–	–
Seyfollahi and Ghaffari (2021)	✓	✓	×	✓	✓	✓	✓	✓	✓	–	–	–
Heidari and Jabraeil Jamali (2023)	–	✓	–	–	–	–	–	–	–	–	–	–
Alfriehat et al. (2024)	✓	–	–	✓	✓	✓	✓	✓	–	✓	✓	–
Kamble et al. (2017)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
Mayzaud et al. (2016b)	✓	✓	–	–	–	–	–	✓	✓	–	–	–
Kharrufa et al. (2019)	✓	–	–	✓	✓	✓	✓	✓	✓	–	–	–
Nandhini et al. (2021)	✓	–	–	✓	✓	✓	✓	✓	✓	–	–	–
Darabkh et al. (2022)	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	✓	–
Seyfollahi and Ghaffari (2021)	✓	✓	–	✓	✓	✓	✓	✓	✓	–	–	✓
Radovici et al. (2018)	✓	✓	–	–	–	✓	–	–	–	–	–	–
Mehta and Parmar (2018)	✓	–	–	–	–	✓	–	–	–	–	–	–
Wang et al. (2021)	✓	–	–	–		✓	–	–	–	–	–	–
Kharrufa et al. (2019)	✓	✓	–	–	–	–	✓	✓	✓	–	–	–
Albinali and Azzedin (2024)	✓	–	–	–	–	–	–	–	–	–	–	✓
Raghavendra et al. (2022)	✓	✓	–	–	✓	–	–	–	–	–	–	–
Rouissat et al. (2022)	✓	–	–	✓	✓	✓	–	✓	✓	–	–	–

Table 12 (continued)

References	Recourse					Toplolgy		Traffic				
	RPL Architecture	DIS–HF	Routing tables overload	Rank	DAG	VNA	SH	WH	BH	Traffic Analysis	SA	Identity Attacks
HDIDOU and EL ALAMI (2024)	✓	–	–	–	–	–		–	–	–	–	–
Pasikhani et al. (2021)	✓	–	–	–	–	–	–	–	–	–	–	–
Satilmiş et al. (2024)	✓	–	–	–	–	–	–	–	–	–	–	–
Omar et al. (2023)	✓	–	–	–	–	–	✓	–	–	–	–	–
S et al. (2024)	✓	–	–	–	–	–	–	–	–	–	–	–
Kuroda (2024)	✓	✓	–	–	–	✓		✓	✓	–	–	–
This work	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

We conducted a qualitative comparison to highlight the uniqueness of our work in comparison to other reviews of routing protocol-based attacks. This comparison is based on two key metrics: the RPL architecture and the classification of attacks in RPL-based IoT. We defined these metrics ourselves after thoroughly examining the existing attacks. Such a comparison is crucial for understanding the critical issues related to various attacks against the RPL protocol and identifying more effective detection techniques. Additionally, it can serve as a guideline for future researchers working in a similar field. Our review was benchmarked with approximately 30 other articles, In our qualitative comparison analysis, we made the following observations:

6 Future directions

This review highlights the critical need to address network attacks in IoT networks. Here are key areas for future research to bolster RPL-based attack detection:

1. Advanced DL Techniques: Applying advanced DL methods can potentially improve the performance of existing attack detection models.
2. Broader Attack Detection Scope: Expanding these models' ability to identify a wider variety of routing attacks is essential.
3. Unified Attack Detection Model: Exploring the development of a single model capable of detecting multiple attack types through novel features holds promise.
4. Hybrid Mitigation Strategies: Analyzing the effectiveness of combining different mitigation approaches to better counterattacks is crucial.
5. Mobility Considerations: Future research should account for node mobility in IoT networks, as it can significantly impact attack detection mechanisms.

Focusing on these areas can significantly improve the effectiveness of RPL-based attack detection methods. These advancements will ultimately enhance the security and reliability of IoT networks, making them more resilient against malicious attacks.

6.1 Specific techniques for different attacks

The review also proposed specific techniques to address various attack types:

1. VNA: Anomaly detection algorithms can identify unusual behavior like inconsistent VN transmission, helping to thwart this attack.
2. SH: Trust-based mechanisms can be employed. Nodes can maintain trust scores for neighbors based on behavior. Suspicious activity, such as attracting excessive traffic, can be flagged and isolated.
3. RA: Reputation systems where nodes share information to assess neighbor trustworthiness can be utilized. Nodes with low reputation scores can be avoided when routing decisions are made to mitigate this attack.
4. BA: AI techniques, particularly ML, can analyze network traffic patterns and identify attack signatures. Real-time traffic pattern analysis by DL algorithms such as CNNs and recurrent Neural Networks (RNNs) can improve detection even more.

These techniques aim to strengthen the security of RPL-based IoT networks by effectively detecting and mitigating various attacks. Additionally, future research should focus on these directions to improve the effectiveness of RPL-based attack detection approaches in IoT networks. By addressing these research areas, we can enhance the security and reliability of IoT networks and better protect against malicious attacks.

7 Conclusion

This survey explores a key type of attack that captures the interest of researchers, highlighting its significant and influential nature, which warrants further investigation. It presents an exhaustive and comprehensive review of the number and types of attacks, providing insight into researchers' interests and the types of attacks they focus on.

Our paper offers researchers comprehensive references regarding attacks on RPL-based IoT networks and their classifications. We did not pre-determine the types of attacks to be considered; instead, we extracted the most significant ones from our research. Our search process involved manually checking relevant articles to ensure a deep understanding of the subject matter. For example, we reviewed approximately 30 articles on the RPL attacks. Furthermore, we extensively investigated the various limitations of DL algorithms and future directions in attack detection.

Our analysis revealed that the proposed solutions were generally effective, achieving satisfactory performance while supporting security modes and protection techniques that require context-specific considerations. The VNA emerged as the most devastating attack. We also observed that many studies on detecting routing attacks on resource-constrained devices overlooked task distribution and parallel processing during the learning phase. Additionally, most of these studies did not address the simultaneous detection of multiple attacks.

Therefore, it is crucial to develop algorithms. Our analysis underscores the need for future research to focus on developing more sophisticated algorithms that can mitigate the most severe attacks and handle the simultaneous detection of multiple attacks.

In summary, this review offers valuable resources to researchers working on PL-based attack detection techniques in IoT networks. Our findings highlight the need for future research to focus on developing more sophisticated algorithms that can mitigate the most severe attacks and handle the detection of multiple attacks simultaneously. Our study is important because it fully reviews and classifies RPL-based attack detection methods in IoT networks.

Author contributions A.B. and C.G. conceived and designed the research study, conducted data collection and analysis, and drafted the main manuscript text. A. E.F. prepared figures 1-11, contributed to data analysis, and provided valuable insights. D. critically reviewed and edited the manuscript for intellectual content. A.B. offered critical feedback and revised the manuscript for important intellectual content. B.C. supervised the overall study, provided administrative support, and ensured the coherence of the research. Lokman Bin Mohd Fadzil funding acquisition. All authors carefully reviewed and approved the final manuscript before submission.

Funding This work is supported by Renesas-Universiti Sains Malaysia (USM) industry matching grant as per MoA#A2021098 agreement with grant account no [7304.PNAV.6501256.R128].

Data availability Our manuscript has no associated data

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose.

Ethical approval Not Applicable.

Consent to participate Not Applicable.

Consent for publication Not Applicable.

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by-nc-nd/4.0/.

References

Abhinaya E, Sudhakar B (2021) A secure routing protocol for low power and lossy networks based 6lowpan networks to mitigate DIS flooding attacks. J Ambient Intell Humaniz Comput. https://doi.org/10.1007/s12652-020-02804-3

Agarwal R, Dhoot A, Kant S et al (2024) A novel approach for spam detection using natural language processing with AMALS models. IEEE Access. https://doi.org/10.1109/ACCESS.2024.3391023

Agiollo A, Conti M, Kaliyar P et al (2021) Detonar: detection of routing attacks in RPL-based IoT. IEEE Trans Netw Serv Manage 18(2):1178–1190

Ahmed F, Ko YB (2016) A distributed and cooperative verification mechanism to defend against dodag version number attack in RPL. In: International conference on pervasive and embedded computing, SciTePress, pp 55–62

Al-Amiedy TA et al (2023) A systematic literature review on attacks defense mechanisms in RPL-based 6lowpan of internet of things. Internet Things (Netherlands). https://doi.org/10.1016/j.iot.2023.100741

Al-Amiedy TA, Anbar M, Belaton B et al (2022) A systematic literature review on machine and deep learning approaches for detecting attacks in RPL-based 6lowpan of internet of things. Sensors 22(9):3400

Al-Amiedy TA, Anbar M, Belaton B et al (2023) A systematic literature review on attacks defense mechanisms in RPL-based 6lowpan of internet of things. Internet Things 22:100741

Albinali H, Azzedin F (2024) Towards RPL attacks and mitigation taxonomy: systematic literature review approach. IEEE Trans Netw Serv Manag. https://doi.org/10.1109/TNSM.2024.3386468

Alfriehat N, Anbar M, Karuppayah S et al (2024) Detecting version number attacks in low power and lossy networks for internet of things routing: review and taxonomy. IEEE Access. https://doi.org/10.1109/ACCESS.2024.3368633

Al-Mubarak MJ, Conejo AJ (2023) Storing freshwater versus storing electricity in power systems with high freshwater electric demand. J Modern Power Syst Clean Energy. https://doi.org/10.35833/MPCE.2023.000306

Almusaylim ZA, Jhanjhi N, Alhumam A (2020) Detection and mitigation of RPL rank and version number attacks in the internet of things: SRPL-RP. Sensors 20(21):5997

Almusaylim ZA, Alhumam A, Mansoor W et al (2020) Detection and mitigation of RPL rank and version number attacks in smart internet of things. Solid State Technol. https://doi.org/10.20944/preprints202007.0476.v1

Alsukayti IS, Alreshoodi M (2023) Rpl-based IoT networks under simple and complex routing security attacks: an experimental study. Appl Sci 13(8):4878

Ambarkar SS, Shekokar N (2021) Critical and comparative analysis of dos and version number attack in healthcare IoT system. In: Proceeding of first doctoral symposium on natural computing research: DSNCR 2020, Springer, pp 301–312

Anitha AA, Arockiam L (2021) Venadet: version number attack detection for RPL based internet of things. Solid State Technol 64(2):2225–2237
Arış A, Yalçın SBÖ, Oktuğ SF (2019) New lightweight mitigation techniques for RPL version number attacks. Ad Hoc Netw 85:81–91
Arış A, Oktuğ SF (2020) Analysis of the RPL version number attack with multiple attackers. 2020 International conference on cyber situational awareness. IEEE, Data analytics and assessment (CyberSA), pp 1–8
Ashrif FF, Sundararajan EA, Ahmad R et al (2023) Survey on the authentication and key agreement of 6lowpan: open issues and future direction. J Netw Comput Appl. https://doi.org/10.1016/j.jnca.2023.103759
Avila K, Jabba D, Gomez J (2020) Security aspects for RPL-based protocols: a systematic review in IoT. Appl Sci 10(18):6472
Azzaoui H, Boukhamla AZE, Perazzo P et al (2024) A lightweight cooperative intrusion detection system for RPL-based IoT. Wirel Pers Commun 134:2235
Banerjee M, Samantaray S (2019) Network traffic analysis based iot botnet detection using honeynet data applying classification techniques. Int J Comput Sci Inf Secur. 17(8)
Belkheir M, Rouissat M, Boukhobza MA, et al (2022) A new lightweight solution against the version number attack in RPL-based iot networks. In: 2022 7th International conference on image and signal processing and their applications (ISPA), IEEE, pp 1–6
Bokka R, Sadasivam T (2024) Simulation-based analysis of RPL routing attacks and their impact on IoT network performance. J Electron Test. https://doi.org/10.1007/s10836-024-06106-w
Cao W, Mirjalili V, Raschka S (2020) Rank consistent ordinal regression for neural networks with application to age estimation. Pattern Recogn Lett 140:325–331
Chen T, Liu Z, Su H (2024) Tampering attack detection for remote interval observer. J Franklin Inst 361(1):71–84
Darabkh KA, Al-Akhras M, Zomot JN et al (2022) RPL routing protocol over IoT: a comprehensive survey, recent advances, insights, bibliometric analysis, recommendations, and future directions. J Netw Comput Appl 207:103476
Deng H, Sun X, Wang B, et al (2009) Selective forwarding attack detection using watermark in WSNS. In: 2009 ISECS International colloquium on computing, communication, control, and management, IEEE, pp 109–113
Dhingra A, Sindhu V, et al (2022) A review of dis-flooding attacks in RPL based IoT network. In: 2022 International conference on communication, computing and internet of things (IC3IoT), IEEE, pp 1–6
Diro AA, Chilamkurti N (2018) Distributed attack detection scheme using deep learning approach for internet of things. Futur Gener Comput Syst 82:761–768
Dvir A (2017) Vera—version number and rank authentication in RPL. Australian J Telecommun Digit Econ 5:50
Dvir A, Buttyan L, et al (2011) Vera-version number and rank authentication in RPL. In: 2011 IEEE Eighth international conference on mobile Ad-Hoc and sensor systems, IEEE, 709–714
Faraj O, Megías D, Ahmad AM, et al (2020) Taxonomy and challenges in machine learning-based approaches to detect attacks in the internet of things. In: Proceedings of the 15th international conference on availability, reliability and security, pp 1–10
Ferraz Junior N, Silva AA, Guelfi AE et al (2022) Performance evaluation of publish-subscribe systems in IoT using energy-efficient and context-aware secure messages. J Cloud Comput 11(1):6
Garcia Ribera E, Martinez Alvarez B, Samuel C et al (2022) An intrusion detection system for RPL-based IoT networks. Electronics 11(23):4041
Gowtham M, Vigenesh M, Ramkumar M (2024) An artificial immune system-based algorithm for selfish node detection in mobile Ad Hoc networks (MANETs). Trans Emerg Telecommun Technol 35(2):e4938
Guo G (2021) A lightweight countermeasure to dis attack in RPL routing protocol. In: 2021 IEEE 11th Annual computing and communication workshop and conference (CCWC), IEEE, pp 0753–0758
Hannachi A, Jaafar W, Bitam S, et al (2024) A novel energy-efficient cross-layer design for scheduling and routing in 6tisch networks. arXiv preprint arXiv:2403.12949
Hasan MK, Habib AA, Islam S et al (2023) Ddos: distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments. Energy Rep 9:1318–1326
Hassan M, Tariq N, Alsirhani A et al (2023) Gitm: a gini index-based trust mechanism to mitigate and isolate Sybil attack in RPL-enabled smart grid advanced metering infrastructures. IEEE Access. 111:62697

Hdidou R, El alami M (2024) Intrusion detection systems in internet of things: A recent state of the art. J Theor Appl Inform Technol. 102(1)
Heidari A, Jabraeil Jamali MA (2023) Internet of things intrusion detection systems: a comprehensive review and future directions. Clust Comput 26(6):3753–3780
Hemalatha S, Pallathadka H, Chinchewadi RP (2024) Finding packet dropper and collecting missing packet due to packet dropping attackers in mobile Adhoc network using divide and conquer algorithm. Int J Media Netw 2(1):1–6
Islam MM, Karmakar G, Kamruzzaman J et al (2020) A robust forgery detection method for copy-move and splicing attacks in images. Electronics 9(9):1500
Iuchi K, Matsunaga T, Toyoda K, et al (2015) Secure parent node selection scheme in route construction to exclude attacking nodes from RPL network. In: 2015 21st Asia-Pacific conference on communications (APCC), IEEE, pp 299–303
Jahangeer A, Bazai SU, Aslam S et al (2023) A review on the security of IoT networks: from network layer's perspective. IEEE Access 11:71073–7108. https://doi.org/10.1109/ACCESS.2023.3246180
Javed M, Tariq N, Ashraf M et al (2023) Securing smart healthcare cyber-physical systems against black-hole and greyhole attacks using a blockchain-enabled gini index framework. Sensors 23(23):9372
Jiang X, Shi Q, Miao H et al (2024) Credible link flooding attack detection and mitigation: a blockchain-based approach. IEEE Trans Netw Serv Manag. https://doi.org/10.1109/TNSM.2024.3357660
Juneja V, Dinkar SK (2023) A predictive vampire attack detection by social spider optimized gaussian mixture model clustering. Concurr Comput Pract Exp 35(2):e7481
Kamble A, Malemath VS, Patil D (2017) Security attacks and secure routing protocols in RPL-based internet of things: survey. In: 2017 International conference on emerging trends & innovation in ICT (ICEI), IEEE, pp 33–39
Kamel SOM, Elhamayed SA (2020) Mitigating the impact of IoT routing attacks on power consumption in IoT healthcare environment using convolutional neural network. Int J Comput Netw Inf Secur 12(4):11–29
Kfoury E, Saab J, Younes P et al (2019) A self organizing map intrusion detection system for RPL protocol attacks. Int J Interdiscip Telecommun Netw 11(1):30–43
Kharrufa H, Al-Kashoash HA, Kemp AH (2019) RPL-based routing protocols in IoT applications: a review. IEEE Sens J 19(15):5952–5967
Kiran U, Maurya P, Sharma H (2024) Investigating routing protocol attacks on low power and lossy IoT networks. SN Comput Sci. https://doi.org/10.1007/s42979-024-02747-y
Krentz KF, Voigt T (2024) Secure opportunistic routing in 2-hop IEEE 802.15. 4 networks with SMOR. Comput Commun 217:57–69
Kuroda K (2024) A review of the optimization of thyroid function, thrombophilia, immunity and uterine milieu treatment strategy for recurrent implantation failure and recurrent pregnancy loss. Reprod Med Biol 23(1):e12561
Landsmann M, Wahlisch M, Schmidt TC (2013) Topology authentication in rpl. In: 2013 IEEE Conference on computer communications workshops (INFOCOM WKSHPS), IEEE, pp 73–74
Lewis C, Li N, Varadharajan V (2023) Targeted context based attacks on trust management systems in IoT. IEEE Internet Things J 10:12186
Li T, Wang Z, Zou L et al (2023) A dynamic encryption-decryption scheme for replay attack detection in cyber-physical systems. Automatica 151:110926
Li G, Ma Y, Wang W et al (2024) The self-detection method of the puppet attack in biometric fingerprinting. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2024.3365714
Lin J, Xu L, Liu Y, et al (2020) Composite backdoor attack for deep neural network by mixing existing benign features. In: Proceedings of the 2020 ACM SIGSAC conference on computer and communications security, pp 113–131
Maheswari S, VIJAYABHASKER R, Kandasamy K (2022) A novel firefly-based nodal gradient artificial neural network to mitigate black hole and grey hole attacks. NeuroQuantology 20(8):4489
Maikol SO, Khan AS, Javed Y et al (2021) A novel authentication and key agreement scheme for countering MITM and impersonation attack in medical facilities. Int J Integr Eng 13(2):127–135
Makina H, Letaifa AB, Rachedi A (2024) Survey on security and privacy in internet of things-based ehealth applications: challenges, architectures, and future directions. Secur Privacy 7(2):e346
Manjula HS, Chaitra M, Channaraju A et al (2024) Intrusion detection system to detect impersonation attacks in IoT networks. In: 2024 International conference on intelligent and innovative technologies in computing, electrical and electronics (IITCEE). https://doi.org/10.1109/IITCEE59897.2024.10467569
Mattern J, Mireshghallah F, Jin Z, et al (2023) Membership inference attacks against language models via neighbourhood comparison. arXiv preprint arXiv:2305.18462

Mayzaud A, Sehgal A, Badonnel R et al (2015) Mitigation of topological inconsistency attacks in RPL-based low-power lossy networks. Int J Network Manage 25(5):320–339
Mayzaud A, Badonnel R, Chrisment I (2016a) Detecting version number attacks in RPL-based networks using a distributed monitoring architecture. In: 2016 12th International conference on network and service management (CNSM), IEEE, pp 127–135
Mayzaud A, Badonnel R, Chrisment I (2016) A taxonomy of attacks in RPL-based internet of things. Int J Netw Secur 18(3):459–473
Mayzaud A, Badonnel R, Chrisment I (2017) A distributed monitoring strategy for detecting version number attacks in RPL-based networks. IEEE Trans Netw Serv Manage 14(2):472–486
Mehta R, Parmar M (2018) A survey on security attacks and countermeasures in RPL for internet of things. Int J Adv Res Sci Eng. 7
Moreira CM, Kaddoum G (2023) Sd6lowpan security: issues, solutions, research challenges, and trends. IEEE Internet Things Mag 6(3):132–137
Mottola L, Hameed A, Voigt T (2024) Energy attacks in the battery-less internet of things: Directions for the future. In: Proceedings of the 17th European workshop on systems security, pp 29–36
Muzammal SM, Murugesan RK, Jhanjhi NZ et al (2022) A trust-based model for secure routing against RPL attacks in internet of things. Sensors 22(18):7052
Nandhini P, Kuppuswami S, Malliga S (2021) Energy efficient thwarting rank attack from RPL based IoT networks: a review. Mater Today Proc 81:694
Nandhini P, Kuppuswami S, Malliga S (2023) Energy efficient thwarting rank attack from RPL based IoT networks: a review. Mater Today Proc 81:694–699
Nandhini P, Kuppuswami S, Malliga S et al (2023) Enhanced rank attack detection algorithm (e-rad) for securing RPL-based IoT networks by early detection and isolation of rank attackers. J Supercomput 79(6):6825–6848
Napiah MN, Idris MYIB, Ramli R et al (2018) Compression header analyzer intrusion detection system (cha-ids) for 6lowpan communication protocol. IEEE Access 6:16623–16638
Nayak S, Ahmed N, Misra S (2021) Deep learning-based reliable routing attack detection mechanism for industrial internet of things. Ad Hoc Netw 123:102661. https://doi.org/10.1016/j.adhoc.2021.102661
Nikravan M, Movaghar A, Hosseinzadeh M (2018) A lightweight defense approach to mitigate version number and rank attacks in low-power and lossy networks. Wirel Pers Commun 99:1035–1059
Oladipupo ET, Abikoye OC, Imoize AL et al (2023) An efficient authenticated elliptic curve cryptography scheme for multicore wireless sensor networks. IEEE Access 11:1306–1323
Omar AARA, Soudan B et al (2023) A comprehensive survey on detection of sinkhole attack in routing over low power and lossy network for internet of things. Internet Things 22:100750
Osman M, He J, Mokbal FMM et al (2021) Ml-lgbm: A machine learning model based on light gradient boosting machine for the detection of version number attacks in RPL-based networks. IEEE Access 9:83654–83665
Palani A, Loganathan A (2024) Semi-blind watermarking using convolutional attention-based turtle shell matrix for tamper detection and recovery of medical images. Expert Syst Appl 238:121903
Pasikhani AM, Clark JA, Gope P et al (2021) Intrusion detection systems in RPL-based 6lowpan: a systematic literature review. IEEE Sens J 21(11):12940–12968
Patil AS, et al (2022) Security and privacy issues in the internet of things. In: Information security practices for the internet of things, 5G, and next-generation wireless networks. IGI Global, pp 70–91
Perrey H, Landsmann M, Ugus O, et al (2013) Trail: topology authentication in RPL. arXiv preprint arXiv:1312.0984
Pishdar M, Seifi Y, Nasiri M et al (2022) PCC-RPL: an efficient trust-based security extension for RPL. Inf Secur Global Perspective 31:168–178
Platt M, McBurney P (2023) Sybil in the haystack: a comprehensive review of blockchain consensus mechanisms in search of strong sybil attack resistance. Algorithms 16(1):34
Pongle P, Chavan G (2015) A survey: Attacks on rpl and 6lowpan in iot. In: 2015 International conference on pervasive computing (ICPC), IEEE, pp 1–6
Prakash S, Swaroop A (2016) A brief survey of blackhole detection and avoidance for ZRP protocol in manets. 2016 International conference on computing. Communication and automation (ICCCA), IEEE, pp 651–654
Prathapchandran K, Janani T (2021) A trust-aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest-rftrust. Comput Netw 198:108413
Pu C, Song T (2018) Hatchetman attack: A denial of service attack against routing in low power and lossy networks. In: 2018 5th IEEE international conference on cyber security and cloud computing (CSCloud)/2018 4th IEEE International conference on edge computing and scalable cloud (EdgeCom), pp 12–17, https://doi.org/10.1109/CSCloud/EdgeCom.2018.00012

Quintero JCM, Cuesta EPE, Lopez LJR (2023) A new method for the detection and identification of the replay attack on cars using SDR technology and classification algorithms. Results Eng 19:101243
Rabet I, Fotouhi H, Alves M et al (2024) Actor: adaptive control of transmission power in RPL. Sensors 24(7):2330
Radovici A, Cristian R, ŞERBAN R (2018) A survey of iot security threats and solutions. In: 2018 17th RoEduNet conference: networking in education and research (RoEduNet), IEEE, pp 1–5
Raeini M (2024) The golden era of mathematics: from computer science to data science. Available at SSRN 4686564
Raghavendra T, Anand M, Selvi M et al (2022) An intelligent RPL attack detection using machine learning-based intrusion detection system for internet of things. Procedia Comput Sci 215:61–70
Rakesh B (2023) Novel authentication and secure trust based RPL routing in mobile sink supported internet of things. Cyber Phys Syst 9(1):43–76
Raoof A, Matrawy A, Lung CH (2018) Routing attacks and mitigation methods for RPL-based internet of things. IEEE Commun Surv Tutor 21(2):1582–1606
Raza S, Wallgren L, Voigt T (2013) Svelte: real-time intrusion detection in the internet of things. Ad Hoc Netw 11(8):2661–2674
Remya S, Pillai MJ, Arjun C et al (2024) Enhancing security in LLNs using a hybrid trust-based intrusion detection system for RPL. IEEE Access 12:58836–58850. https://doi.org/10.1109/ACCESS.2024.3391918
Roberts MK, Ramasamy P (2023) An improved high performance clustering based routing protocol for wireless sensor networks in IoT. Telecommun Syst 82(1):45–59
Rouissat M, Belkheir M, Belkhira HSA (2022) A potential flooding version number attack against RPL based IoT networks. J Electr Eng 73(4):267–275
Sahay R, Geethakumari G, Mitra B (2020) A novel blockchain based framework to secure IoT-LLNs against routing attacks. Computing 102:2445–2470
Sahay R, Geethakumari G, Mitra B, et al (2020b) Efficient framework for detection of version number attack in internet of things. In: Intelligent systems design and applications: 18th international conference on intelligent systems design and applications (ISDA 2018) held in Vellore, 2018, Volume 2, Springer, pp 480–492
Sahay R, Geethakumari G, Mitra B (2022) Mitigating the worst parent attack in RPL based internet of things. Clust Comput 25(2):1303–1320
Satilmiş H, Akleylek S, Tok ZY (2024) A systematic literature review on host-based intrusion detection systems. IEEE Access 12:27237–27266
Saurabh K, Upadhyay P, Rani N (2024) Towards blockchain decentralized autonomous organizations (DAO) design. Inf Syst Front. https://doi.org/10.1007/s10796-023-10455-w
Seeber S, Sehgal A, Stelte B, et al (2013) Towards a trust computing architecture for RPL in cyber physical systems. In: Proceedings of the 9th international conference on network and service management (CNSM 2013), IEEE, pp 134–137
Sehgal A, Mayzaud A, Badonnel R, et al (2014) Addressing dodag inconsistency attacks in rpl networks. In: 2014 Global information infrastructure and networking symposium (GIIS), IEEE, pp 1–8
Seyfollahi A, Ghaffari A (2021) A review of intrusion detection systems in RPL routing protocol based on machine learning for internet of things applications. Wirel Commun Mob Comput 2021:1–32
Shafi M, Lashkari AH, Rodriguez V et al (2024) Toward generating a new cloud-based distributed denial of service (DDoS) dataset and cloud intrusion traffic characterization. Information 15(4):195
Sharma S, Verma VK (2021) Security explorations for routing attacks in low power networks on internet of things. J Supercomput 77:4778–4812
Sharma G, Grover J, Verma A (2023) Performance evaluation of mobile RPL-based IoT networks under version number attack. Comput Commun 197:12–22
Sharma G, Grover J, Verma A, et al (2022) Analysis of hatchetman attack in rpl based iot networks. In: International conference on emerging technologies in computer engineering, Springer, pp 666–678
Simha SV, Mathew R, Sahoo S, et al (2020) A review of RPL protocol using contiki operating system. In: 2020 4th international conference on trends in electronics and informatics (ICOEI)(48184), IEEE, pp 259–264
Suzuki T, Altomare C, Willems M et al (2023) Non-hydrostatic modelling of coastal flooding in port environments. J Marine Sci Eng 11(3):575
Tasneem B, Wahid M (2021) A review of secure routing challenges in low power and lossy networks. In: 2021 International conference on communication technologies (ComTech), IEEE, pp 120–125
Thubert P, Nordmark E, Chakrabarti S, et al (2018) Registration extensions for IPv6 over low-power wireless personal area network (6LoWPAN) neighbor discovery. RFC 850https://doi.org/10.17487/RFC8505, https://www.rfc-editor.org/info/rfc8505

Thungon LC, Sahana SC, Hussain I (2024) A lightweight authentication scheme for 6lowpan-based internet-of-things. Global Perspect Inf Secur J. https://doi.org/10.1080/19393555.2024.2332962
Verma A, Ranga V (2020) Security of RPL based 6lowpan networks in the internet of things: a review. IEEE Sens J 20(11):5666–5690
Wang Z, Xie W, Wang B et al (2021) A survey on recent advanced research of CPS security. Appl Sci 11(9):3751
Wang L, Chen M, Lu L et al (2023) Voicelistener: a training-free and universal eavesdropping attack on built-in speakers of mobile devices. Proc ACM Interact Mobile Wearable Ubiquitous Technologies 7(1):1–22
Wisdom DD, Vincent OR, Igulu K et al (2024) Industrial IoT security infrastructures and threats. Commun Technol Secur Chall in IoT Present Future. https://doi.org/10.1007/978-981-97-0052-3_19
Xiang X, Cao J, Fan W et al (2024) Blockchain enabled dynamic trust management method for the internet of medical things. Decis Support Syst 180:114184
Yang H, Zhang X, Wu Z et al (2024) Co-sharding: a sharding scheme for large-scale internet of things application. Res Pract Distributed Ledger Technol 3:1–16
Yavuz FY, Ünal D, Gül E (2018) Deep learning for detection of routing attacks in the internet of things. Int J Comput Intell Syst 12(1):39–58
Zhang K, Bhandari KS, Cho G (2023) TB-RPL: A try-the-best fused mode of operation to enhance point-to-point communication performance in RPL. Electronics 12(7):1639
Zhou H (2024) Research on improvement and optimization design of mobile switching in RPL routing protocol. Adv Eng Technol Res 9(1):858–858

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Nadia Alfriehat[1] · Mohammed Anbar[1] · Mohammed Aladaileh[2] · Iznan Hasbullah[1] · Tamarah A. Shurbaji[1] · Shankar Karuppayah[1] · Ammar Almomani[3,4,5]

✉ Nadia Alfriehat
adnad1981@gmail.com

✉ Mohammed Anbar
anbar@usm.my

Mohammed Aladaileh
m.adaileh@aum.edu.jo

Iznan Hasbullah
iznan@usm.my

Tamarah A. Shurbaji
tamarashorabji@student.usm.my

Shankar Karuppayah
kshankar@usm.my

Ammar Almomani
ammarnav6@bau.edu.jo

[1] National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), 11800 Penang, Malaysia

[2] American University of Madaba, Amman 11821, Madaba, Jordan

[3] Higher Collages of Technology, Department of Information Science, Sharjah, UAE

[4] University City of Sharjah, P.O. Box 1797, Sharjah, United Arab Emirates

[5] I.T. department- Al-Huson University College, Al-Balqa Applied University, P.O. Box 50, Irbid, Jordan