ONLINE FIRST July 19, 2024

Computer Assisted Methods in Engineering and Science
***, doi: 10.24423/cames.2024.764

This article belongs to the *Special Issue on AI-Based Future Intelligent Networks and Communications Security* edited by Dr. S. Kumar, Dr. G. Mapp, Dr. A. Bansal and Dr. K. Cengiz

A Review of Isolation Attack Mitigation Mechanisms in RPL-Based 6LoWPAN of Internet of Things

V.R. RAJASEKAR*, S. RAJKUMAR

School of Computer Science and Engineering, Vellore Institute of Technology, India, e-mail: rajkumars@vit.ac.in

* *Corresponding Author e-mail: rajasekarv.r2017@vitstudent.ac.in*

The Routing Protocol for Low-Power and Lossy Networks (RPL) is an open standard routing protocol defined by the Internet Engineering Task Force (IETF) to address the constraints of IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN). RPL is susceptible to various attacks, including isolation attacks, in which a node or a set of RPL nodes can be isolated from the rest of the network. Three significant isolation attacks are the black hole attack (BHA), selective forwarding attack (SFA), and destination advertisement object (DAO) inconsistency attack (DAO-IA). In a BHA, a malicious node drops all packets intended for transmission silently. In an SFA, a malicious node forwards only selected packets and drops the other received packets. In a DAO-IA, a malicious node drops the received data packet and replies with a forwarding error packet, causing the parent node to discard valid downward routes from the routing table. We review the literature on proposed mechanisms, propose a taxonomy, and analyze the features, limitations, and performance metrics of existing mechanisms. Researchers primarily focus on power consumption as the key performance metric when mitigating BHA (47%), SFA (51%), and DAO-IA (100%), with downward latency being the least addressed metric for BHA (4%) and SFA (3%), and control packet overhead being the least addressed for DAO-IA (37%). Finally, we discuss the unresolved issues and research challenges in mitigating RPL isolation attacks.

Keywords: IoT, LLN, 6LoWPAN, isolation attacks, black hole, selective forwarding, DAO inconsistency.

1. Introduction

The convergence of physical and digital realms has given rise to the Internet of Things (IoT) [1], where Low Power and Lossy Networks (LLNs) play a crucial role by connecting resource-constrained devices such as sensor nodes [2]. LLN faces challenges such as power constraints and communication issues such as packet loss and limited data rates. IP-connected IoT systems utilize 6LowPAN

to integrate with the traditional Internet [3]. The Routing Over Low Power and Lossy Networks (ROLL) [4] group of the IETF standardized the RPL to address LLN routing needs, RPL operates at the network layer, enabling efficient route formation and dissemination [5]. However, RPL is vulnerable to various attacks. This study focuses specifically on RPL isolation attacks (RPL-IA) and their mitigation in 6LoWPAN [6].

1.1. RPL overview

RPL, a lightweight routing protocol based on IPv6, is designed explicitly for 6LoWPAN [5]. RPL efficiently connects resource-constrained IoT nodes, adapting to diverse network setups to maintain quality of service (QoS) [7]. Figure 1 illustrates an overview of an RPL network, in which RPL defines a Destination-Oriented Directed Acyclic Graph (DODAG) utilizing an objective function (OF), a collection of metrics, and constraints [5].

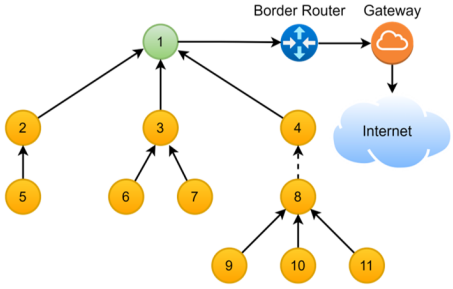

Fig. 1. RPL network overview.

1.2. RPL isolation attack

An isolation attack isolates a node or a subset of the RPL network and prevents communication with the parents and the root node. Isolated nodes become detached from the network topology and no longer participate in the DODAG. As shown in Fig. 2, the three major RPL isolation attacks are BHA, SFA, and DAO-IA; all three attacks are summarized below.

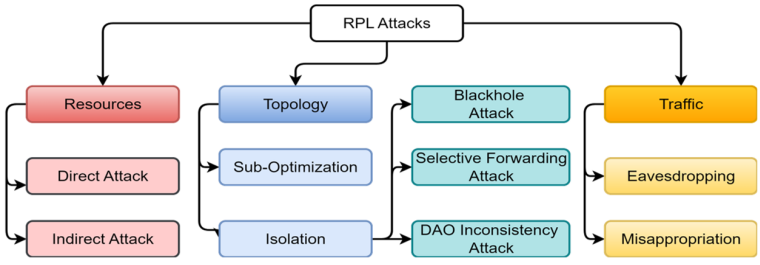

Fig. 2. RPL attacks.

1.3. Black hole attack

Once the DODAG is formed, each node in the RPL network has a predefined upward path to the border router (BR). Regardless of the packet's destination, a packet must be forwarded to the node's preferred parent, which comprises the route to the BR. During DODAG formation, a malicious node falsely claims to have an efficient route to the BR and becomes the preferred parent for most of the active nodes. When the malicious node receives packets from other network nodes, it silently drops them and forms a black hole in the network [8]. Figure 3a shows the RPL network with a single active BHA (N7); the packets from nodes 8, 9, and 10 are silently dropped by node 7; victim nodes (8, 9, 10) have no alternate paths to the BR, resulting in isolation from the network as depicted in Fig. 3b. Figure 3c illustrates the colluding BHA in which nodes 2 and 3 are colluding together and forming BHA. All packets received from nodes 5 and 6 are dropped by node 3, and packets from nodes 7–10 are dropped by node 3, forming a BH zone. The primary adverse effects of BHA are summarized in Table 1.

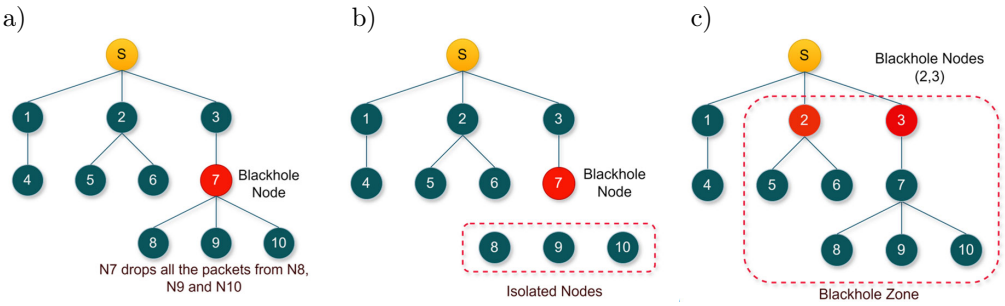

FIG. 3. a) Black hole node-N7, b) isolated nodes, c) colluding BHA.

1.4. Selective forwarding attack

In SFA, malicious nodes selectively transmit certain packets and drop the rest, as illustrated in Fig. 4. For example, node 8 may forward only RPL control

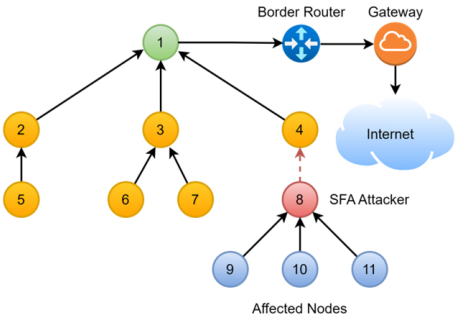

FIG. 4. Selective forwarding attack.

Table 1. Isolation attacks summary.

Attack	Attack type	Description	Type	Active/ Passive	CIA	Impact
BHA	BHA	Drops all packets, isolates a portion of the network	IN	AC	A, I	Increased CPOH, E2ED, EC, decreased PDR, un-stabilized topology, downward and upward packet loss
	FBHA	Modifies data packets by setting 'O' and 'R' flags, sends modified packets to neighbors	IN	AC	A, I	
	CBHA	Multiple malicious node join together and form a BH	IN	AC	A, I	
SFA	SFA	Attacker node drops selected packets passing through and isolates portion of network	IN	AC	A, I	Adverse effects on topology construction, disrupted routing, and decreased PDR
	SFA (DoS)	Attacker nodes drop all packets passing through and isolate network portion	IN	AC	A, I	
	SFA (N&G)	Attacker node purposefully omits to send specific packet types	IN	AC	A, I	
DAO-IA	DAO-IA	Uses "F" flag to make RPL routers remove legitimate downward routes	IN	AC	A, I	High E2ED, un-optimized topology, node isolation

Abbreviations: BHA – black hole attack, BH – black hole, FBHA – forced black hole attack, CBHA – colluding black hole attack, SFA – selective forwarding attack, DoS – denial of service attack, N&G – neglect and greed, IN – internal, AC – active, A – availability, I – integrity, CPOH – control packet overhead, E2ED – end to end delay, EC – energy consumption, PDR – packet delivery ratio, DAO-IA – destination advertisement object inconsistency attack.

messages and discard all other packets from the sender nodes, and vice versa [9]. Table 1 summarizes the three variants SFA along with their primary adverse effects and prerequisites.

1.5. DAO inconsistency attack

As depicted in Fig. 5a, in a DAO-IA, node 5 drops the received data packet and sets the forwarding-error flag in the packet option header to create a forwarding error packet, and then sends this packet as reply to cause the parent node to discard valid downward routes in its routing table. Subsequently, when the routing table no longer contains a valid downward route to the destination node, the parent node of node 5 responds to the forwarding error packet [10], as shown in Fig. 5b. Table 1 summarizes the impact of DAO-IA in 6LoWPAN.

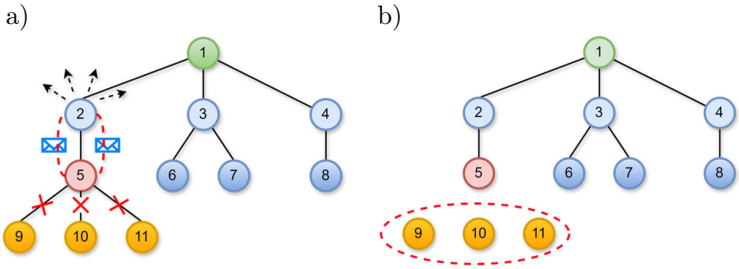

Fig. 5. DAO-IA a) initial stage, b) final stage.

1.6. Contributions and structure of the study

RPL-IA poses a severe threat to RPL-based 6LoWPAN networks, allowing a single node or a group of nodes to be isolated from the topology, affecting various critical applications, including healthcare and smart grid, and potentially resulting in life-threatening incidents. The above fact drove us to thoroughly investigate the RPL-IA and the mitigation mechanisms proposed in the literature. The contributions of this study are five-fold:

1. Provide a comprehensive review of the state-of-the-art approaches to mitigate isolation attacks in RPL-based 6LoWPAN.
2. Develop a taxonomy of contemporary research directions in mitigating isolation attacks in RPL-based 6LoWPAN.
3. Analyzing the features and the limitations of the proposed mitigation mechanisms.
4. Explore the performance metrics addressed by the research community while mitigating isolation attacks in RPL-based 6LoWPAN.
5. Identify open research issues and state-of-the-art challenges related to isolation attacks in RPL-based 6LowPAN.

This study is structured as follows: Sec. 2 describes related surveys on RPL attacks; Sec. 3 presents the research questions formulated for this study; Sec. 4 presents the results and discussion for all research questions formulated in Sec. 3, and Sec. 5 concludes the paper.

2. Related surveys

This section provides an overview of recent surveys, studies, and reviews on RPL attacks and their mitigation mechanisms. Mayzaud *et al.* [11] analyzed RPL-based attacks and proposed a comprehensive taxonomy of attacks. However, they did not cover recently proposed attacks and defense solutions nor did they construct a taxonomy for defense solutions. Verma and Ranga [12] surveyed attacks and defense solutions in RPL, presenting a taxonomy of RPL attacks and discussing cross-layered and RPL-specific network layer-based defense solutions. Muzammal *et al.* [13] investigated security issues in IoT networks, including RPL attacks such as BHA, Spoofing, and Rank attacks, and discussed trust-based mitigation mechanisms and associated research challenges. Granja *et al.* [14] analyzed protocols for secure IoT communications but did not address RPL-specific attacks and defense mechanisms. Pongle *et al.* [15] provided a brief study on RPL and 6LoWPAN attacks, discussed defense solutions briefly, however, they omitted taxonomy development for RPL-specific attacks and defenses. Chauhan and Kumar [16] focused on IoT-secured communications protocols, reviewing trust-based defense solutions for RPL-specific attacks, primarily applicable to WSNs rather than directly to IoT networks.

To address the gaps mentioned above, this paper focuses solely on RPL-IA and its mitigation mechanisms. We introduce a taxonomy for RPL isolation defense mechanisms, analyzing the features, limitations, performance metrics, unresolved issues, and research challenges in mitigating RPL-IA.

3. Research questions

We followed the PRISMA [17] recommendations as our research methodology for this study, and investigated state-of-the-art studies, compiled the findings, and summarized observed evidence in mitigating isolation attacks in RPL-based 6LoWPAN. The following research questions are framed to achieve the five-fold contributions listed in Subsec. 1.6.

RQ 1: What mechanisms are available to mitigate isolation attacks in RPL-based 6LoWPAN?

RQ 2: How are the identified mechanisms sub-categorized as "taxonomy of isolation attacks defense mechanisms"?

RQ 3: How are RPL-embedded solutions further classified?

RQ 4: What state-of-the-art lightweight Intrusion Detection System (IDS) approaches have been used to detect isolation attacks in RPL-based 6LoWPAN?

RQ 5: What AI-based solutions are proposed for detecting isolation attacks in RPL-based 6LoWPAN?

RQ 6: What performance metrics are considered by the research community while mitigating RPL-IA?

RQ 7: What are the open issues and research challenges in mitigating RPL-IA?

4. Results and discussion

This section provides the study results and answers to the research questions presented in Sec. 3.

4.1. RQ 1: What mechanisms are available to mitigate isolation attacks in RPL-based 6LoWPAN?

This question is addressed by listing and categorizing the identified RPL isolation attack mitigation mechanisms proposed in the literature. We categorize the identified mechanisms based on the three major isolation attacks (BHA, SFA, DAO-IA) and each mechanism is associated with studies considering it, as shown in Fig. 6.

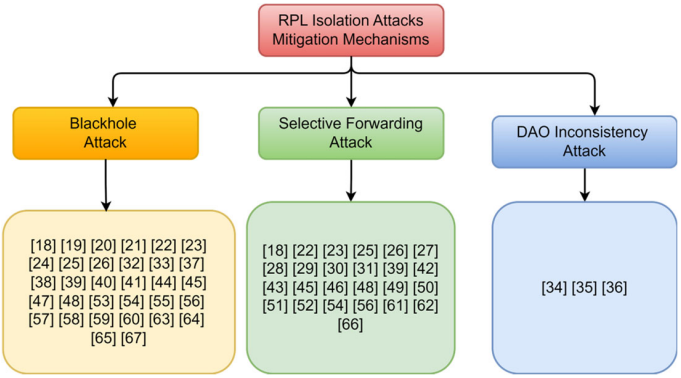

Fig. 6. RPL isolation attacks mitigation mechanisms.

4.2. RQ 2: How are the identified mechanisms sub-categorized as a "taxonomy of isolation attacks defense mechanisms"?

We answer this question by classifying the identified RPL-IA mitigation mechanisms and proposing a taxonomy. Figure 7 illustrates the proposed taxonomy, classifies the proposed solutions into three broad categories: RPL-embedded solutions, lightweight IDS, and AI-based solutions.

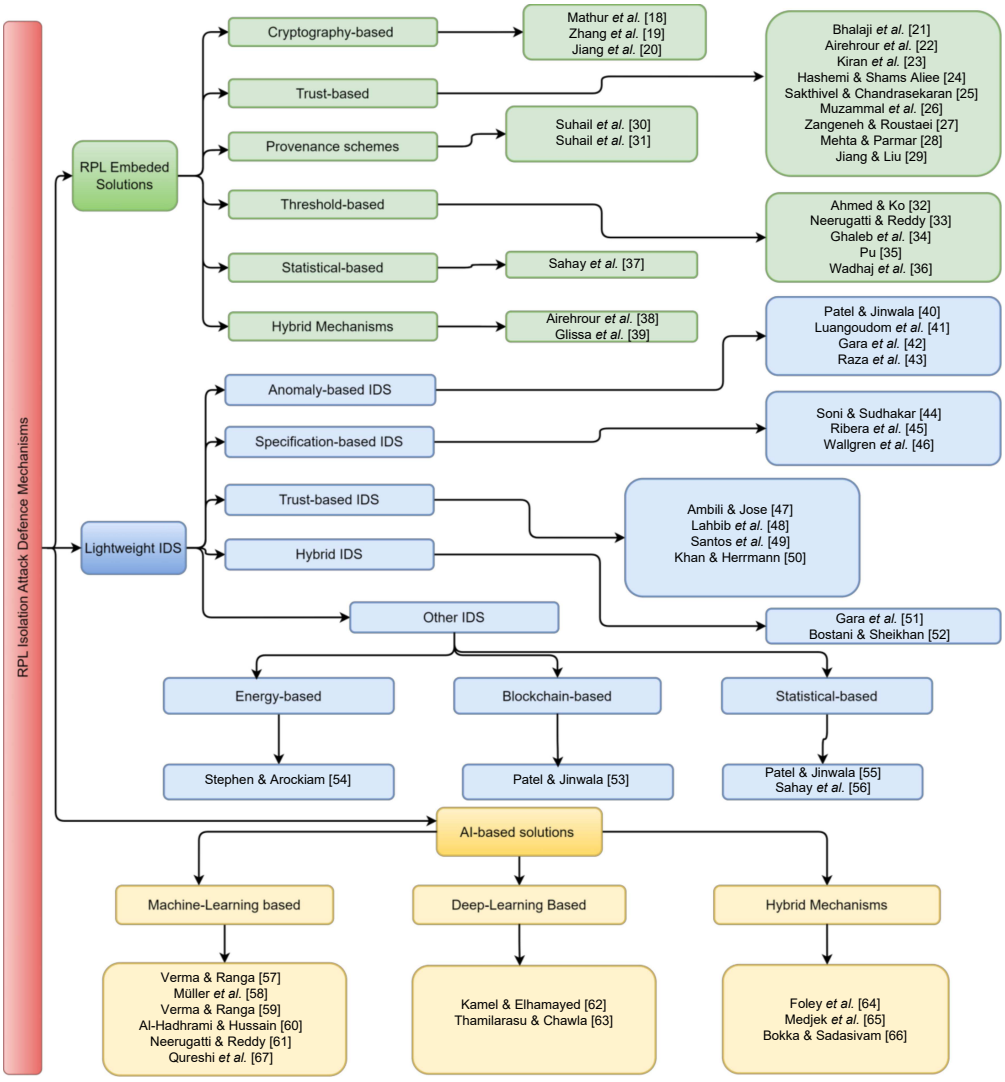

FIG. 7. Taxonomy of RPL isolation attacks defense mechanisms.

4.3. RQ 3: How are RPL embedded solutions further classified?

RPL-embedded solutions incorporate defense mechanisms into the RPL protocol, making it resistant to various attacks. In addressing this question, we categorize the identified RPL-embedded solutions into several types. Cryptography-based solutions rely on classical techniques to fortify security against diverse threats. Trust-based mechanisms evaluate node trustworthiness to aid routing decisions, while provenance schemes ensure reliable data transit and routing, integrating QoS considerations and data tracking. Threshold-based defense so-

lutions utilize RPL's inherent features by resetting the trickle timer. Statistical-based defense solutions leverage well-known statistical approaches for enhanced security. Hybrid mechanisms combine two or more schemes to offer comprehensive RPL-embedded solutions. This section thoroughly discusses the strengths and weaknesses of these solutions, with Table 2 providing a brief overview of the methodology, considered attacks, features, and limitations.

4.3.1. Cryptography-based. Cryptography-based mechanisms employ well-known cryptographic techniques like symmetric, asymmetric, and hash functions to provide security and protect RPL-based 6LoWPAN.

In [18], authors proposed a mitigation technique utilizing a cryptographic hash function to combat BHA and SFA. This method partitions the network into clusters with designated cluster heads, which amalgamate encrypted data and forward it to the nearest AP via mesh routing. Moreover, base stations assign random numbers to APs during routing phases, achieved through request and reply packet exchanges. Malicious nodes are identified using hash values. While effective against single and multiple attacks, this approach demonstrates high FPR and FNR and consumes more energy. In [19], a Cuckoo filter-based RPL was introduced for safeguarding AMI networks. Here, the root generates a list of legitimate nodes unalterable by the DODAG, authenticated solely by sender nodes. Unlike conventional methods, new nodes can only join as children without direct addition to the root node's hash table. Authentication with the root node is obligatory for new nodes to become formal members, triggering adjustments to the cuckoo hashing table by the root and broadcast of updated DODAG Information Object DIO messages, affecting network speed and bandwidth. The proposed model [20] incorporates a detection, reporting, and isolation module for managing BHA. In the detection module, non-root nodes are hash-protected to prevent data tampering by malicious nodes. The report module notifies other nodes of the BH node's presence, and the isolation module separates the identified BH node from its child node. However, this approach solely addresses direct BHAs, omitting considerations of colluding BHAs, attacker node mobility, performance, or detection accuracy.

4.3.2. Trust-based. Trust-based mechanisms determine a node's trustworthiness, facilitate routing decisions, provide network security, and defend RPL networks against isolation attacks. This section presents various trust-based (TB) defense solutions proposed in the literature to mitigate RPL-IA. In [21], an intra- and inter-DODAG TB mechanism is proposed to counteract BHA. It utilizes Packet Delivery Ratio (PDR) for preferred parent determination and routing decisions, along with rank metric and ETX for assessing trustworthiness. Intra-DODAG computes trust values via PDR analysis, while

Table 2. Summary of RPL-embedded solutions.

Author	Method	Attack	Features	Limitations
Mathur *et al.* [18]	CB	BHA SFA	Cryptographic hash, neighborhood watch, THB analysis	No data transmission security, high FPR and FNR, consumes high energy
Zhang *et al.* [19]	CB	BHA	A cuckoo filter-based hash table, defending AMI network	Lengthy authentication and updating the hash table affect performance
Jiang *et al.* [20]	CB	BHA	Detection, reporting, and isolation, hash-protected, non-storing mode	CBHA, node mobility, performance, and accuracy are not addressed
Bhalaji *et al.* [21]	TB	BHA	Two levels at intra and inter DODAG levels, PDR-based trust computation	Recalculating the ranks locally reduces the network's efficiency
Airehrour *et al.* [22]	TB	BHA SFA	PDR-based trustworthiness, rerouting using link quality	Promiscuous mode, not considering legitimate nodes dropping packets
Kiran *et al.* [23]	TB	BHA SFA	Integrates rank variance and DODAG contextual TM	Consider routing misbehavior and packet-dropping attacks
Hashemi & Shams Aliee [24]	TB	BHA	A multidimensional trust, PDR-based, ETX, energy, and mobility	Storing historical data is overhead
Sakthivel & Chandrasekaran [25]	TB	BHA SFA	Dummy packet-based, subjective, and fuzzy TM establishes node credibility	Packet loss and dummy packets result in high overhead and energy
Muzammal *et al.* [26]	TB	BHA SFA	Defining, calculating, indexes, updating, and recalculating trust	It has not been implemented, tested, or compared to demonstrate its efficiency
Zangeneh & Roustaei [27]	TB	BHA SFA	Three different security modes (un-secure, pre-installed, authenticated)	Error and imprecision in computation throughput influence attack detection
Mehta & Parmar [28]	TB	SFA	A lightweight TC using forwarding rate, rank, recommend and ETX	Does not consider other RPL attacks and node mobility

[Table 2. Cont.].

Author	Method	Attack	Features	Limitations
Jiang & Liu [29]	TB	SFA	It combines self-trust with tree-based descendent trust value on the root	Single point of failure since the model is deployed on the root node
Suhail *et al.* [30]	PS	SFA	PDR-based attack detection is appended to the packet's payload	Simple PDR calculation and does not consider the node's mobility
Suhail *et al.* [31]	PS	SFA	Provenance-enabled, PDR-based, data, and provenance	PDR, provenance size, and creation time influence the accuracy
Ahmed & Ko [32]	TH	BHA	Global verification and local decision, overhearing packets to monitor	Rank-related issues and node mobility are left uninvestigated
Neerugatti & Reddy [33]	TH	BHA	RPL-DODAG node's threshold value is derived using each node's PDR	Simplified PDR calculation
Ghaleb *et al.* [34]	TH	DAO-IA	THB limits parents to forward DAOs	Does not consider the node's mobility
Pu [35]	TH	DAO-IA	Restricts to 20 error packets, maintains mischief TH counter	Inefficient in terms of energy consumption
Wadhaj *et al.* [36]	TH	DAO-IA	Sub-DODAG, threshold-based, time slot limit, DAO counter	It must be activated prior to the network operating
Sahay *et al.* [37]	SB	BHA	Exponential smoothing forecasting, smoothing time series & prediction	The forecast lags the trend and needs to be updated frequently
Airehrour *et al.* [38]	HM	BHA	Distributed, PDR-based trust, positive feedback, and trust analysis	Local decision-making monitoring neighbors imposes high computation
Glissa *et al.* [39]	HM	BHA SFA	THB identification, verification, and authentication	Not effective for insider attacks, cryptography imposes overhead

inter-DODAG trust computations involve multiple servers and clients, employing a similar trust computation method but distinguishing between authentic and malicious servers. However, the proposed rank modification process requires local rank recalculations before complete repair initiation by the root, adversely affecting network efficiency. [22] presents a Trust-Aware RPL routing protocol that, compared to MRHOF-RPL, excels in attack detection, node rank adjustment, performance, and packet loss mitigation. However, it operates each node in promiscuous mode, making it incompatible with resource-constrained IoT nodes, and overlooks the possibility of legitimate nodes dropping packets due to unintentional errors. An adaptable IoT routing security solution is introduced in [23], integrating RPL rank variance and DODAG contextual trust models. It employs a non-zero-sum game to construct the trust model, selecting a trustworthy router via evolutionary game theory. Performance evaluation indicates that this solution outperforms other context-aware designs in detection accuracy and throughput. DCTM-IoT proposed in [24] incorporates a multidimensional trust view, calculating trust values based on various factors. However, it requires an excessive amount of data and needs further discussion on its integration with RPL. In [25], a framework is proposed, implementing a dummy packet-based acknowledgement method and subjective/fuzzy trust models. However, it suffers from high packet loss, overhead, and energy consumption, which could significantly impact the performance and energy efficiency of IoT networks. The SMTrust architecture, studied in [26], protects against RPL attacks using trust metrics but lacks implementation and testing. In [27], a TB protocol with three security modes is proposed to safeguard against BHA, utilizing the Ant Lion Optimizer (ALO) algorithm and Stochastic Learning Automata to enhance the RPL routing protocol. In [28], a lightweight trust computation technique to combat wormholes and Selective Forwarding Attacks (SFA) is presented, though it neglects other potential RPL attacks and relies solely on direct neighbor recommendations for trust computation. In [29], a centralized and lightweight approach to defend against SFA is introduced, demonstrating high detection accuracy and minimal power consumption.

4.3.3. Provenance schemes. Provenance can be utilized to maintain a record of data sources and actions performed by other entities during data propagation and processing. Widespread use of robust provenance has been observed in numerous application domains, yet provenance management in IoT necessitates considering constraints like storage, energy, and processor limits. The concept of provenance in the IoT has not yet been effectively studied due to the complex requirements. In [30], authors introduced a provenance-based approach for combating SFA. Packet Deliver Ratio (PDR) is computed and appended to the payload, tracking the packet's path through each forwarding node

to detect malicious nodes. The total packet count received by a forwarding node is added to the routing table, associating this information with the respective child node entry. PDR is then determined based on the received packet count to flag malicious nodes; nodes falling below baseline PDR criteria are identified as attackers. In [31], authors presented a provenance-enabled approach to mitigate SFA, assessing network performance by monitoring PDR at each forwarding node along the packet's path. The method comprises three core components: network, data, and provenance models. PDR computation occurs at each forwarding node, with results integrated as provenance data in the payload to detect network anomalies. Evaluation criteria include provenance size, creation time, and memory consumption.

4.3.4. Threshold-based. Threshold-based protection methods leverage RPL's inherent features, extending control over the trickle timer. Fixed threshold methods maintain a constant and predetermined threshold value throughout the detection process. Conversely, adaptive threshold methods dynamically adjust the threshold value during detection. This section explores both fixed and adaptive threshold-based defense solutions proposed in the literature to mitigate RPL-IA.

In [32], authors propose a method to counter both single and colluding BHA through a combination of global verification and local decision-making. Suspicious nodes failing to meet predefined threshold trigger are flagged, while colluding BHA nodes are identified if their parent or upstream neighbor fails to respond. Upon detecting suspicious nodes, legitimate nodes reroute data to the root node via alternate paths. The root node verifies and responds with query results regarding the reverse path, enabling the identification and isolation of suspicious nodes to prevent future communication. While enhancing data delivery and reducing end-to-end delay, this method overlooks investigating rank-related issues. [33] introduces an algorithm to detect BHA by setting a threshold value for RPL-DODAG nodes derived from each node's PDR. The evaluation of this algorithm is mainly focused on three key metrics: attack detection rate, end-to-end delay, and PDR, which are essential for assessing its effectiveness. SecRPL, as presented in [34], plays a pivotal role as a robust solution against DAO falsification attacks. It achieves this by restricting the number of DAO packets sent to each destination. Performance metrics, including CPO, APC, and latency, further affirm its effectiveness in forwarding DAOs. In [35] the impact of DAO insider attacks is studied and a dynamic threshold mechanism (DTM) is introduced to address them. However, concerns arise about inefficient energy consumption in RPL environments. In [36], SecRPL1 and SecRPL2 are introduced to counter DAO insider attacks in RPL. Both systems require activation before network functionality, which is a drawback.

4.3.5. Statistically/mathematically-based. This strategy employs well-established statistical or mathematical models for mitigation. In [37], authors propose a BHA detection method using exponential smoothing, a common technique for smoothing time series data with an exponential window function. It enables short-, medium-, and long-term predictions, aiding in forecasting packet arrival times at the sink node from all other nodes in LLNs. However, a drawback is that the forecast may lag behind as trends fluctuate, potentially failing to adapt to LLNs' dynamic nature and requiring constant updates for maintaining accuracy.

4.3.6. Hybrid mechanisms. Hybrid mechanisms employs two or more techniques mentioned above; this section examines hybrid approaches used to combat isolation attacks. In [38], authors presented a distributed Trust-Based approach to mitigate BHA, where nodes assess neighboring nodes' trustworthiness based on PDR. Only trusted neighbors serve as preferred parents for data transmission, determined through positive feedback awareness and trust analysis. However, this approach may introduce overhead and increased computational demands. Despite demonstrating superior performance in detection rate, node rank stability, throughput, and packet loss, its efficiency has only been evaluated under static topology conditions without considering mobile nodes. In [39], SPRL is introduced as a secure routing system aimed at preventing rank value manipulation by constraining rank value fluctuations. It restricts malicious nodes from altering ranks, safeguarding against internal attacks and conserving network resources. Malicious nodes are identified through a threshold function monitoring rank changes, while verification and authentication provide added security layers. However, an evident drawback is the absence of immediate protection, resulting in all nodes, regardless of legitimacy, bearing extra overhead due to threshold implementation. Additionally, employing cryptography with a hash chain imposes a substantial computational burden on constrained devices, rendering nodes susceptible to insider attacks.

4.4. RQ 4: What state-of-the-art Lightweight IDS approaches have been used to detect isolation attacks in RPL-based 6LoWPAN?

In the realm of RPL-based IoT, IDS serves as a secondary defense line against irregular operations. However, applying IDS solutions directly to resource-constrained nodes poses challenges due to computational, communication, memory, and energy constraints. Lightweight IDS solutions tailored for resource-constrained devices aim to minimize these overheads. Various types of IDS, including anomaly detection, specification-based detection, trust-based detection, hybrid models, adaptive threshold methods, blockchain-based IDS, energy-efficient IDS, and statistically/mathematically based models, have been explored

by the research community to mitigate isolation attacks. Table 3 provides a summary of the methodology, attacks considered, features, and limitations of proposed Lightweight IDS solutions in the literature aimed at addressing RPL-IA.

4.4.1. Anomaly-based IDS. Anomaly-based IDSs (A-IDS) analyze network traffic to create an expected behavior profile and compare network events to the actual profile, flagging any anomaly as a possible attack. A-IDSs detect both known and potential new attacks through anomalous behavior but frequently exhibit erroneous positive/negative detections and are more resource-intensive.

In [40], Strainer based Intrusion Detection of Black Hole in 6LoWPAN for the Internet of Things (SIEWE) IDS detects BHA in RPL-based 6LoWPAN using node-level (local module) and branch-level (BR/global module) components. Each node monitors neighboring communication, compiles a list of suspect nodes, transmits it to the BR for malicious node identification, and broadcasts it to all nodes for blacklisting. Though improving PDR, its limitation lies in focusing on nearby nodes rather than covering all resource-constrained nodes. In [41], svBLOCK targets BHA by incorporating SVELTE, a real-time IDS for IoT, to reconstruct the DODAG, verify node availability, authenticate control messages, and isolate BHA nodes. A distinguishing feature is svBLOCK's provision of CIA assurances regarding DODAG-rooted control messages. In [42], an IDS for IPv6-based Mobile WSNs detects SFA and isolates compromised nodes during global repair. Combining SPRT with an adaptive threshold based on ETX addresses path quality and network topology changes due to sensor mobility, albeit incurring notable network overhead. In [43], SVELTE serves as a real-time IDS for 6LoWPAN, employing anomaly-based detection to identify various threats, though exhibiting drawbacks such as low PDR and Correct Positive Output (CPO), inconsistent rank measurement, and vulnerability to coordinated attacks. Authors of [35] introduce a Dynamic Threshold Mechanism (DTM) to counter DAO inconsistency attacks, enabling parent nodes to dynamically adjust thresholds over time based on received packets and estimated error rates, thereby enhancing network security.

4.4.2. Specification-based IDS. A specification-based IDS (S-IDS) profiles the network's usual behavior and generates the network profile based on network (or protocol) parameters defined manually, leading to significantly lower FPR and FNR. However, the manual definition of specifications makes it challenging to respond to environmental changes.. This section discusses the S-IDS solutions proposed in the literature to defend against RPL-IA. In [44], the L-IDS technique is introduced to mitigate BHA by integrating data transmission at each hop and identifying the attacker's presence through the LHV value, effectively neutralizing the attacker's network presence. However, it overlooks

TABLE 3. Summary of lightweight IDS solutions.

Author	Method	Attack	Features	Limitations
Patel & Jinwala [40]	A-IDS	BHA	Local and global architecture modules, local overhears, and global decisions	Validates only nodes near suspicious nodes
Luangoudom *et al.* [41]	A-IDS	BHA	A real-time IDS ensures the authenticity of control messages	Authenticating control messages consumes time and resources
Gara *et al.* [42]	A-IDS	SFA	Incorporating SPRT with an ETX-based ATH and sensor mobility	Significant network overhead due to the exchange of hello packets
Raza *et al.* [43]	A-IDS	SFA	Three centralized modules: Mapper, Analyzer, and Detector	Incorrect topology building due to inconsistent rank results in a high FPR
Soni & Sudhakar [44]	S-IDS	BHA	Nodes cooperate on routing and packet delivery; LHV value detects malicious nodes	Does not consider the sender and sink nodes' mobility
Ribera *et al.* [45]	S-IDS	BHA, SFA	UDP packets, ICMPv6 echo request, and no echo reply indicate suspicion	Increases CPU use and TX/RX rates
Wallgren *et al.* [46]	S-IDS	SFA	A 3-phase heartbeat protocol uses Echo request and malicious node detection	The inclusion of additional packets increases the communication overhead
Ambilik & Jose [47]	TB-IDS	BHA	Trust is based on node activity; the score is maintained on the blockchain	Require higher bandwidth due to computation nature
Lahbib *et al.* [48]	TB-IDS	BHA, SFA	A multidimensional approach to compute trust. Ensures trust and provides QoS	Susceptible to failure at a single point

[Table 3. Cont.].

Author	Method	Attack	Features	Limitations
Santos *et al.* [49]	TB-IDS	SFA	Watchdog, reputation, and trust metrics, clustering and reliability modules	Personification attacks on the IoT routing service are not considered
Khan & Herrmann [50]	TB-IDS	SFA	A distributed mechanism, root nodes aggregate trust values/reputation values	Calculation-intensive with a high FPR and FNR
Gara *et al.* [51]	H-IDS	SFA	Distributed module and centralized module, several sink nodes	Adds network OH and imposes additional network implementation
Bostani & Sheikhan [52]	H-IDS	SFA	Unsupervised OPFC algorithm, sink node equipped with an A-IDS	Disregards the nodes' energy limits, considers one-way communication
Patel & Jinwala [53]	BC-IDS	BHA	Utilizing a 6MID Micro-chain connected to an external blockchain	Managing and storing blockchain systems is a crucial challenge
Stephen & Arockiam [54]	EB-IDS	BHA, SFA,	Rank calculation, substantiation, and mitigation based on energy consumption	Single point of failure, prolonged detection process
Patel & Jinwala [55]	SAT-IDS	BHA	Reduces promiscuous nodes by using statistical filtering criteria	It consumes more resources with a higher PDR and runs in promiscuous mode
Sahay *et al.* [56]	SAT-IDS	BHA, SFA	Packet dropping, statistical learning, and in-depth analysis of the traffic patterns	More resources and app. computation are needed due to lossiness

the mobility of sender and sink nodes. In [45], an IDS enhances the LHP-based method with UDP heartbeat signals to detect BHA and SFA. Leveraging UDP increases the likelihood of detecting malicious nodes, but it incurs CPU overhead and TX/RX rates. In [46], a three-phase IDS utilizing the heartbeat protocol periodically sends ICMPv6 Echo messages, cross-references replies and takes appropriate action, such as removing the source of non-responses or issuing alerts. While ensuring node vitality, it increases communication overhead due to additional packet transmissions.

4.4.3. Trust-based IDS. In trust-based IDS (TB-IDS), trust is computed directly or via other nodes' recommendations. The trust value is calculated using various characteristics, such as reputation, recommendation credibility, and honesty. This section describes different TB-IDS proposed in the literature to defend against RPL-IA. In [47], TN-IDS is presented as a system monitoring nodes and their activities, relying on blockchain-stored trust scores determined by node behavior during routing requests and interactions with nearby nodes. Neighborhood tables track node details for trust-based neighbor notifications, with misbehaving nodes indicating potential attackers. In [48], LT-RPL introduces a trust manager evaluating node trustworthiness based on broadcasted metrics. Despite its efficacy against SFA and BHA, LT-RPL lacks justification for recommendations and overlooks other attack vectors. In [49], THATACHI utilizes watchdog, reputation, and trust mechanisms to manage clustering and isolate attacker devices targeting data routing, demonstrating low FPR and FNR. However, it does not address personification attacks. In [50], a distributed method counters SFA, sinkhole, and identity alteration attacks by regulating neighboring node reputations through a TMS. Yet, its multiple checks impact trust levels and performance.

4.4.4. Hybrid IDS. Hybrid-IDS (H-IDS) combines multiple well-known ID approaches, such as anomaly-based, specification-based, and TB IDS, to mitigate isolation attacks in RPL-based 6LoWPAN. This section discusses the literature that proposed hybrid IDS to mitigate RPL-IAs. In [51], an IDS is proposed to address SFA and clone attacks. It employs distributed modules in each node with a centralized module in the sink node. Multiple sink nodes are deployed to mitigate single points of failure in large-scale networks. One sink node establishes the DODAG, while another identifies attackers. In large networks, a sink node detects hello packets from node clusters. However, this system adds network overhead and implementation costs, potentially challenging for resource-constrained networks. In [52], a real-time hybrid IDS architecture is introduced, using optimum path forests to detect sinkholes, SFA, and wormhole threats. IDS modules on router nodes analyze child nodes and transmit local results via data packets

to the gateway node. The gateway node hosts an A-IDS module employing the unsupervised Optimal Path Finding and Clustering (OPFC) algorithm to form clusters from incoming data packets.

4.4.5. Other IDS. This section describes other types of IDS proposed in the literature to defend against RPL-IAs, including adaptive threshold-based, blockchain-based, energy-based, and statistical IDS.

4.4.5.1. Adaptive threshold. An adaptive threshold is a dynamic technique for establishing thresholds used to detect anomalies or potential intrusions by adjusting to evolving patterns of network or system behavior. In contrast, fixed threshold methods can be inflexible and may fail to accommodate shifts in network traffic or system usage patterns, potentially resulting in false positives or false negatives. Few IDS solutions [34, 36, 42], as discussed in Subsec. 4.4, utilize adaptive threshold mechanisms in conjunction with other detection strategies.

The proposed SecRPL framework [34] addresses DAO falsification attacks through two distinct approaches. The first approach involves a fixed threshold to limit both the total number of forwarded DAOs and the number of DAOs forwarded to each destination. The second approach employs an adaptive threshold to prevent the blocking of DAOs from non-attacker nodes, thereby ensuring fairness among nodes. In [36], two mitigation mechanisms, SecRPL1 and SecRPL2, are proposed to address DAO Inconsistency attacks. SecRPL1 manages DAO forwarding by parent nodes, stopping the forwarding process when fixed thresholds are surpassed until the synchronization time slots conclude. DAO counters are reset at each DIO interval. SecRPL2, on the other hand, restricts DAO forwarding during specific time slots to ensure accuracy and prevent DAO discards due to timing issues, with timings being dynamic values. An anomaly-based IDS [42] integrates the SPRT with an adaptive threshold based on ETX to detect SFA in RPL networks. This system comprises a centralized module located on the sink node and a distributed module deployed on the routing nodes. While it performs exceptionally well in mobile networks due to the use of hello packet exchanges, it results in significant network overhead.

4.4.5.2. Blockchain-based. In [53], the 6MID blockchain architecture is introduced, leveraging Micro-chains to bolster RPL for distributed ledger functionality on resource-constrained 6LoWPAN devices and detect BHA. It enables short-term blockchain-like trust management between BR and sensing devices. It integrates with an external blockchain to preserve temporal Micro-chains for subsequent joint data analysis for attack detection. The authors propose a computationally efficient Micro-block data structure for 6LoWPAN networks, using

a 32-bit hash value to reduce the block header to 16 bytes, requiring only 6.4 kb of RAM to store a chain of 400 nodes in minimum mode. However, a key challenge remains in efficiently managing blockchain processing and storage on mobile-like smart devices.

4.4.5.3. Energy-based. In [54], the E2V architecture is introduced to combat RInA attacks such as sinkholes, SFA, or BHA in RPL-based IoT networks. It consists of rank calculation, substantiation, and malicious node elimination modules. By identifying rank inconsistencies based on energy consumption, the method enhances routing security. Nodes compute their rank and select preferred parent nodes, but attackers can manipulate rankings to disrupt communication. E2V employs an energy-based IDS to detect attacks and pinpoint malicious nodes, reducing energy consumption and time for attack detection and network convergence. However, a drawback is the single-point failure vulnerability, as the system is deployed at the root node.

4.4.5.4. Statistically based. In [55], T-SIEWE is introduced as a trust and strainer-based method for detecting BH nodes. It statistically limits monitored nodes and excludes questionable ones to enhance efficiency. Utilizing filtering criteria and restricting nodes in promiscuous mode, T-SIEWE reduces energy consumption and memory costs associated with BH node detection. Conversely, in [56], an IDS is proposed for mitigating BHA and SFA at the 6LoWPAN network edge. It imposes no computing burden on constrained nodes and includes a network controller, packet information agent, and detection agent. This approach evaluates packet-dropping attack characteristics to aid detection and mitigation but prolongs network operating time and complicates packet management.

4.5. RQ 5: What AI-based solutions are proposed for detecting isolation attacks in RPL-based 6LoWPAN?

We respond to the above question by categorizing the identified AI-based solutions as machine learning (ML)-based, deep learning (DL)-based, and hybrid-based. ML ensemble classifiers (boosted tree, bagged trees, subspace discriminant, and RUSBoosted trees), along with AI-based PDR, kernel density estimation, threshold statements, naïve Bayes (NB), decision trees (DT), logistic regression (LR), artificial neural networks (ANNs), expectation–maximization (EM) clustering, and support vector machine (SVM) classifier are frequently used. Researcher use DL classification or detection mechanisms, including deep neural networks (DNN), deep belief networks (DBN), one-R, chi-square, and

TABLE 4. Summary of AI-based solutions.

Author	Method	Attack	Detection mechanisms	Advantages	Limitations
Verma & Ranga [57]	ML	BHA	Ensemble classifiers	Generates less noise and a higher prediction AC	No evaluation findings, comparison, or deployment
Müller *et al.* [58]	ML	BHA	KDM	Detects all attacks with a significant TPR	AC, PC, PDR, and E2ED are not evaluated
Verma & Ranga [59]	ML	BHA	NB, DT, LR, ANNs, EM	The probability distribution correlation – using five approaches	The results of the EM and LR classifiers for FAR are disappointing
Al-Hadhrami & Hussain [60]	ML	BHA	SVM classifier	A real-time behavior monitoring of network and network statistics	The application layer includes humidity, temperature, and power
Neerugatti & Reddy [61]	ML	SFA	AI-based PDR	Obtains significant results in terms of TPR and FPR, improved E2ED	Changing network factors influence PDR and system performance
Kamel & Elhamayed [62]	DL	SFA	one-R, chi-square, weighted RF	CNN-based attacks, comprises medical data collecting layer	Decreased PRC and longer processing time. PDR, PRC, and E2E delay details are not provided
Tamilarasu & Chawla [63]	DL	BHA	DNN, DBN	Better attack detection and precision results	Does not addresses PDR, E2ED, PRC. Dataset information is not available
Foley *et al.* [64]	ML, DL	BHA	NB, SVM, MLP, RF, ZeroR	Data preprocessing, feature selection reduction, sampling technique, and normalization for attack detection	AC, PC, recall, PDR, E2ED, and PRC were not examined
Medjek *et al.* [65]	ML, DL	BHA	RF, PC	Data collection, feature engineering, selection, and classification modules	Dataset not provided, no analysis of PDR, PRC, or E2ED
Bokka & Sadasivam [66]	ML, DL	SFA	MLP, KNN, AdaBoost, RF, GNB, LR, DT	Using seven types of ML algorithms and performance indicators (ACC, precision, recall, F1-score)	Does not addresses PDR, E2ED, or PRC, and no information regarding the dataset
Qureshi *et al.* [67]	ML	BHA	Threshold statements	Two-phased approach, in-order traversal-based features	PDR decreased with node increase, inaccurate attack detection

weighted random forest (RF), which are also used by the research community for mitigating isolation attacks in RPL-based 6LoWPAN.

4.5.1. Machine-learning-based. In [57], ELNIDS is introduced as a novel ensemble learning-based Network IDS, a unique integration of components like a sniffer, repository, feature extraction, analysis, signature database, user interface, and notification management. It stands out by combining multiple ML classifiers, showcasing enhanced classification outcomes compared to single ML approaches. In [58], an efficient distributed anomaly detection approach for RPL networks is presented, leveraging pre-trained models in network nodes to eliminate data collection and model training overhead. It utilizes a distributed architecture to reduce communication costs significantly and evaluates using kernel density estimation, successfully detecting attack types with a high TPR. RPL-NIDDS17, introduced in [59], employs five unique ML techniques, achieving a maximum accuracy of 93% and the lowest FAR of 3.57%, albeit with some classifier variation due to dataset distribution. [60] proposes an SVM-based ML technique for attack identification, featuring a real-time monitoring tool for IoT network behavior and statistics collection. It considers physical, network, and application-layer data for attack detection, including jamming, BH, and DRA attacks, along with application-layer features. AIPDR, proposed in [61], mitigates SFA using neighborhood information and PDR. It involves decentralized nodes adapting to environmental conditions, but adaptability may impact PDR calculation and system operation.

4.5.2. Deep-learning-based. The mechanism proposed in [62] tackles routing attacks in medical contexts using CNN. It comprises three layers: a medical data collection layer, a routing network layer, and a medical application layer. Preprocessing involves three feature selection strategies (one-R, chi-square, and weighted RF). CNN effectively detects abnormal network traffic patterns, achieving low error and loss rates in attack identification while maintaining network stability by reducing the PRC. However, it requires longer processing time, and distribution methods need clarification. Details such as dataset specifics, selected attributes, and essential metrics such as PDR, PRC, and E2ED are missing. In [63], an anomaly-based IDS model using DL is introduced to detect malicious data. This model categorizes network traffic into sessions and identifies various attacks, including BHA, DDoS, sinkhole, and wormhole. It consists of three phases: network connection, anomaly detection, and mitigation. The network connection phase establishes the necessary network channel for traffic sniffing. In the anomaly detection phase, features are extracted and transformed before being input into a ML module, which utilizes perceptual learning and supervised

ML techniques for training. The mitigation phase involves actuator and handler modules to counteract detected attacks.

4.5.3. Hybrid mechanisms (ML&DL). In [64], a hybrid approach is proposed for detecting threats in RPL-based IoTs, targeting multiple RPL attacks, including rank, version number, Sybil and BHA. The approach involves data preprocessing, feature selection and reduction, sampling strategy, and normalization to enhance attack detection accuracy. Various classification techniques, such as NB, SVMs, MLP, RF, and ZeroR classifiers, are employed. The technique successfully identifies threats to both objective functions, with voting (MLP and RF) yielding superior results. However, analysis of accuracy, precision, recall, PDR, E2ED, and PRC is not provided. Furthermore, details regarding deployment techniques and the dataset used are kept a secret. In [65], a fault-tolerant AI-based IDS is introduced for detecting various routing attacks in Industry 4.0 networks, including DODAG rank attack (DRA), BH, sinkhole (SH), hello flooding (HF), Sybil attack (SF), and version number (VN). The architecture includes modules for data collection, feature engineering, selection, and classification. It incorporates RF and Pearson correlation filter techniques for feature selection. Six ML classifiers – DR, RF, k-nearest neighbors (KNN), NB, multi-layer perceptron (MLP), and logistic regression (LR) – are utilized for classification, with assessment using the Sequential DL model. The model successfully detects attacks across all metrics for both two-class and multi-class classifications, with the RF classifier exhibiting the fastest fitting time. Additionally, the study introduces the RF-IDSR approach, providing fault and intrusion tolerance for Industry 4.0 networks. However, dataset availability and deployment methods are unspecified, and crucial indicators like PDR, PRC, and E2ED are not examined. In [66], an ML-based approach is proposed for identifying risks in RPL-based IoT networks, employing seven ML algorithms: KNN, LR, RF, GNB, DT, AdB, and MLP. Performance evaluation includes accuracy, precision, recall, F1-score, and AUC. Decision Trees achieved the highest scores in accuracy, precision, and F1-score. LR, GNB, and MLP models had the highest recall, while RF had the highest AUC. However, PDR, E2ED, and PRC studies were not discussed, and dataset availability and deployment strategy were unspecified. Additionally, the complexity of ML algorithms may render them unsuitable for constrained devices.

4.6. RQ6: What performance metrics are considered by the research community while mitigating RPL-IA?

The mitigation mechanisms discussed in the preceding section tend to improve the RPL protocol's performance while mitigating isolation attacks. On the other hand, the metrics addressed vary according to the attack and methodology

adopted. This section discusses various performance metrics in the literature concerning the mitigation of RPL-IA. Table 5 summarizes the various performance metrics addressed in each reference.

Table 5. Isolation attack performance metrics considered.

Ref.	Method	Attack	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17
[18]	CB	B,S	✓	✓	✓														
[19]	CB	B		✓															
[20]	CB	B				✓	✓												
[21]	TB	B				✓	✓	✓											
[22]	TB	B,S				✓		✓	✓										
[23]	TB	B,S	✓	✓				✓				✓							
[24]	TB	B	✓		✓	✓			✓										
[25]	TB	B,S	✓	✓			✓	✓				✓		✓		✓			
[26]	TB	B,S	✓		✓	✓			✓										
[27]	TB	B,S		✓	✓		✓							✓					
[28]	TB	S		✓		✓		✓											
[29]	TB	S	✓		✓						✓								
[32]	TH	B			✓		✓			✓	✓								
[33]	TH	B		✓	✓		✓												
[35]	TH	D	✓				✓										✓		
[36]	TH	D	✓				✓										✓	✓	✓
[37]	SB	B		✓															
[38]	HM	B				✓		✓	✓										
[39]	HM	B,S	✓									✓	✓						
[40]	A-IDS	B	✓				✓										✓		
[42]	A-IDS	S												✓		✓			
[43]	A-IDS	S	✓							✓						✓			
[44]	S-IDS	B				✓	✓	✓				✓							
[45]	S-IDS	B,S		✓										✓					
[47]	T-IDS	B	✓				✓										✓	✓	✓
[48]	T-IDS	B,S	✓			✓													
[49]	T-IDS	S	✓	✓			✓	✓			✓	✓		✓	✓	✓	✓	✓	✓
[50]	T-IDS	S									✓				✓	✓			
[51]	H-IDS	S	✓	✓												✓			
[52]	H-IDS	S		✓						✓	✓								
[54]	E-IDS	B,S	✓	✓	✓									✓					
[55]	S-IDS	B	✓				✓			✓		✓							
[56]	S-IDS	B,S					✓												

Abbreviations: M1 – average power consumption (APC), M2 – accuracy (ACC), M3 – end-to-end delay (E2ED), M4 – packet loss (PL), M5 – packet delivery ratio (PDR), M6 – throughput (TP), M7 – frequency of node rank change (FNRC), M8 – true positive rate (TPR), M9 – false positive rate (FPR), M10 – CPU/memory overhead (CP/MO), M11 – packet reception rate (PRR), M12 – detection rate (DR), M13 – false negative rate (FNR), M14 – overhead (OH), M15 – DAO-FO, M16 – upward latency (UL), M17 – download latency (DL), B – black hole attack, S – selective forwarding attack; D – DAO-inconsistency attack; CB – cryptography-based, TB – trust-based, PS – provenance scheme, TH – threshold-based, SB – statistical-based, HM – hybrid mechanism, A-IDS – anomaly-IDS, S-IDS – specification-IDS, T-IDS – trust-based IDS, H-IDS – hybrid IDS, B-IDS – blockchain-based IDS, E-IDS – energy-based IDS, S-IDS – statistical-based IDS.

4.6.1. Black hole attack. The research community addresses several performance parameters in mitigating the BHA within the resource-constrained environment of 6LoWPAN. Among these, the most prioritized performance metric is the average packet consumption, owing to its resource-constrained nature. Following APC, the PDR is predominantly addressed due to the susceptibility of isolation attacks, resulting in significant packet drop rates. Accuracy is the third most considered performance metric, indicating the precision of attack identification. Figure 8 illustrates the array of performance metrics focused on by the research community exclusively in mitigating the BHA. The first five performance metrics are APC, PDR, ACC, PL, and E2ED, whereas the least significant performance metrics are TPR, FPR, OH, UL, and DL.

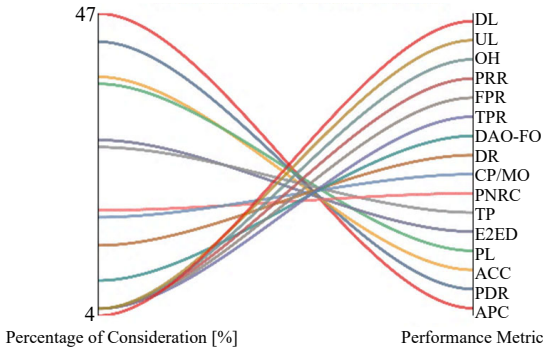

FIG. 8. Black hole attack vs. performance metrics.

4.6.2. Selective forwarding attack. The research community assesses various performance metrics in addressing the SFA, as depicted in Fig. 9. Given its resource-constrained context, the APC emerges as a highly esteemed performance metric, followed closely by ACC. The OH introduced by the proposed

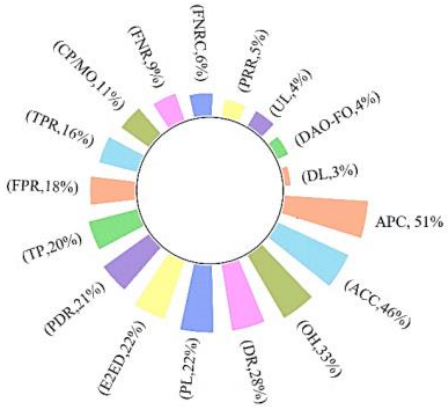

FIG. 9. Selective forwarding attack vs. performance metrics.

mechanism ranks as the third most critical performance metric, followed by DE and E2ED. Conversely, FNRC, PRR, DAO-FO, UL, and DL are among the least prioritized performance metrics.

4.6.3. DAO-IA attack. Figure 10 showcases the performance metrics analyzed by researchers in combatting the DAO-IA. The foremost metric of significance is APC, which PDR succeeded due to the attack's characteristics. Since a DAO-IA typically amplifies DAO packets within the network topology, the research community also extensively evaluates the DAO Forwarding Overhead metric. Upstream and downstream latencies are given nearly equal consideration, while CPO stands as the least prioritized performance metric in addressing DAO inconsistency attacks.

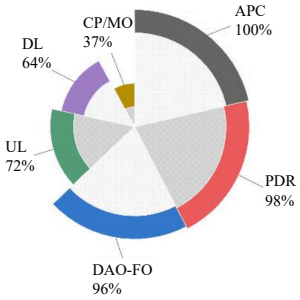

FIG. 10. DAO inconsistency attack vs. performance metrics.

4.7. RQ7: What are the open issues and research challenges in mitigating RPL-IA?

This question is crucial as it drives our inquiry into unresolved aspects of RPL-IAs, encouraging further investigation. LLNs consist of resource-constrained devices linked by largely unreliable wireless connections. LLNs find applications in various fields, including industrial monitoring, building automation, healthcare, and environmental sensing. They operate under strict constraints to conserve energy and typically utilize link layers with limited frame sizes and short packet transmission times. The Routing Protocol for LLNs (RPL) is susceptible to isolation attacks, where malicious nodes disrupt data transmission, leading to network instability and reduced performance.

4.7.1. RPL embedded solutions. IoT sensing devices often lack the computational capacity for complex security tasks, with proposed cryptographic techniques demanding significant resources. Hash chain authentication, Merkle tree authentication, and dynamic keying, though popular, impose heavy computational, memory, and energy burdens on resource-constrained systems. Key

management is incredibly challenging in such networks, necessitating resource optimization for both operation and security. Centralized trust models delegate trust calculation to a single entity, introducing single points of failure and requiring all nodes to submit trust evaluations centrally. However, this approach is impractical for resource-constrained nodes and fails to address dynamicity, mobility, and high packet loss rates. Additionally, privacy concerns remain unaddressed in many trust-based solutions, hindering public confidence and innovation in IoT systems.

4.7.2. Lightweight IDS solutions. Only lightweight IDS systems are recommended for resource-constrained devices because of computational, communication, memory, and energy OH. IDS are the second line of defense responsible for detecting RPL operation anomalies. Designing lightweight IDS in terms of computation and resource utilization is challenging. Modern IDS leverages ML and DL to improve attack detection accuracy. Attaining appropriate TPR and FPR in real-time using available resources in IoT devices is challenging. Due to the lack of appropriate attack datasets to train the models, ML-based techniques still need refinement to be a successful defense mechanism against RPL-IA.

4.7.3. AI-based solutions. Existing mitigating mechanisms for RPL-IA are often static and may not adapt well to mobile and heterogeneous environments. The dynamic nature of RPL networks means devices can join, leave, or change availability unpredictably. Unfortunately, many proposed solutions fail to address this dynamic aspect. Additionally, most existing defense solutions are tested on more minor scales than large IoT networks, so their effectiveness may vary when applied broadly. There is a lack of focus on emerging threats like DIO suppression, routing choice intrusion, and ETX manipulation, necessitating the development of new defense mechanisms. However, utilizing machine learning for RPL-specific security is challenging due to resource constraints despite its success in other networks. While a few ML-based strategies have been proposed, they often require heavy computational tasks that are difficult to integrate into RPL-based 6LoWPAN. Few solutions are fully integrated with RPL, and most only address single attacks rather than multiple threats. Furthermore, existing security solutions are mainly evaluated in constrained network scenarios, and their performance may degrade in physical RPL-based 6LoWPAN deployments.

5. Conclusion

We evaluated RPL-IAs, including the BHA, SFA, and DAO-IA, along with their mitigation mechanisms proposed in the literature. To our knowledge, no comparable survey has exclusively focused on RPL-IA and their mitigating tech-

niques. By presenting a taxonomy for RPL-IA defense mechanisms, including RPL embedded solutions, Lightweight IDS, and AI-based solutions, and further subcategorizing them, we comprehensively addressed all the research questions framed. Each category of the proposed mitigation mechanism was exhaustively analyzed by identifying the adopted methodology, features, limitations, and performance metrics. While mitigating BHA, SFA, and DAO-IA, the APC emerges as the key performance measure addressed by approximately 47%, 51%, and 100% of the research community, respectively. The type of performance metric addressed varies, but the top five are APC, PDR, E2ED, ACC, and CPOH. Downward latency is the performance metric addressed the least in mitigating the BHA (4%) and SFA (3%). However, CPO is the performance metric addressed the least when it comes to DAO-IA (37%). We also discussed the unresolved issues and research challenges that need to be addressed while mitigating the RPL-IA, which will guide the research community in future studies.

References

1. K. Kumar, A.K. Singh, S. Kumar, P. Sharma, J. Sharna, The role of dynamic network slicing in 5G: IoT and 5G mobile networks, [in:] *Evolution of Software-Defined Networking Foundations for IoT and 5G Mobile Networks*, S. Kumar, M.C. Trivedi, P. Rajan [Eds.], pp. 159–171, IGI Global, 2021, doi: 10.4018/978-1-7998-4685-7.ch009.
2. A. Čolaković, M. Hadžialić , Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues, *Computer Networks*, **144**: 17–39, 2018, doi: 10.1016/j.comnet.2018.07.017.
3. N. Kushalnagar, G. Montenegro, C. Schumacher, *RFC 4919 – IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals*, Network Working Group, 2007, doi: 10.17487/RFC4919.
4. A. Musaddiq, Y. Bin Zikria, O. Hahm, H. Yu, A.K. Bashir, S.W. Kim, A survey on resource management in IoT operating systems, *IEEE Access*, **6**: 8459–8482, 2018, doi: 10.1109/ACCESS.2018.2808324.
5. D. Sourailidis, R.-A. Koutsiamanis, G.Z. Papadopoulos, D. Barthel, N. Montavont, RFC 6550: On minimizing the control plane traffic of RPL-based industrial networks, [in:] *IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks (WoWMoM)"*, Cork, Ireland, pp. 439–444, 2020, doi: 10.1109/WoWMoM49955.2020.00080.
6. A. Agiollo, M. Conti, P. Kaliyar, T.N. Lin, L. Pajola, DETONAR: Detection of routing attacks in RPL-based IoT, *IEEE Transactions on Network and Service Management*, **18**(2): 1178–1190, 2021, doi: 10.1109/TNSM.2021.3075496.
7. M.R. Palattella *et al.*, Standardized protocol stack for the Internet of (important) Things, *IEEE Communications Surveys & Tutorials*, **15**(3): 1389–1406, 2013, doi: 10.1109/SURV.2012.111412.00158.
8. P.P. Ioulianou, V.G. Vassilakis, S.F. Shahandashti, A trust-based intrusion detection system for RPL networks: detecting a combination of rank and blackhole attacks, *Journal of Cybersecurity and Privacy*, **2**(1): 124–153, 2022, doi: 10.3390/JCP2010009.

9. D.C. Mehetre, S.E. Roslin, S.J. Wagh, Detection and prevention of black hole and selective forwarding attack in clustered WSN with active trust, *Cluster Computing*, **22**(Suppl. 1): 1313–1328, 2019, doi: 10.1007/S10586-017-1622-9/METRICS.

10. A.S. Baghani, S. Rahimpour, M. Khabbazian, The DAO induction attack against the RPL-based Internet of Things, [in:] *2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Split, Croatia, 17–19 September, pp. 1–5, 2020, doi: 10.23919/SOFTCOM50211.2020.9238224.

11. A. Mayzaud, R. Badonnel, I. Chrisment, A taxonomy of attacks in RPL-based Internet of Things, *International Journal of Network Security*, **18**(3): 459–473, 2016, doi: 10.6633/IJNS.201605.18(3).07.

12. A. Verma, V. Ranga, Security of RPL based 6LoWPAN networks in the Internet of Things: A review, *IEEE Sensor Journal*, **20**(11): 5666–5690, 2020, doi: 10.1109/JSEN.2020.2973677.

13. S.M. Muzammal, R.K. Murugesan, N.Z. Jhanjhi, A comprehensive review on secure routing in Internet of Things: Mitigation methods and trust-based approaches, *IEEE Internet Things Journal*, **8**(6): 4186–4210, 2021, doi: 10.1109/JIOT.2020.3031162.

14. J. Granjal, E. Monteiro, J. Sa Silva, Security for the Internet of Things: A survey of existing protocols and open research issues, *IEEE Communications Surveys & Tutorials*, **17**(3): 1294–1312, 2015, doi: 10.1109/COMST.2015.2388550.

15. P. Pongle, G. Chavan, A survey: Attacks on RPL and 6LoWPAN in IoT, [in:] *2015 International Conference on Pervasive Computing (ICPC)*, Pune, India, pp. 1–6, 2015, doi: 10.1109/PERVASIVE.2015.7087034.

16. R. Chauhan, S. Kumar, Packet loss prediction using artificial intelligence unified with big data analytics, internet of things and cloud computing technologies, [in:] *2021 5th International Conference on Information Systems and Computer Networks (ISCON)*, Mathura, India, pp. 01–06, 2021, doi: 10.1109/ISCON52037.2021.9702517.

17. A. Liberati *et al.*, The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration, *Journal of Clinical Epidemiology*, **62**(10): e1–e34, 2009, doi: 10.1016/j.jclinepi.2009.06.006.

18. A. Mathur, T. Newe, M. Rao, Defence against black hole and selective forwarding attacks for medical WSNs in the IoT, *Sensors*, **16**(1): 118, 2016, doi: 10.3390/S16010118.

19. T. Zhang, T. Zhang, X. Ji, W. Xu, Cuckoo-RPL: Cuckoo filter based RPL for defending AMI network from blackhole attacks, [in:] *2019 Chinese Control Conference (CCC)*, Guangzhou, China, pp. 8920–8925, 2019, doi: 10.23919/ChiCC.2019.8866139.

20. J. Jiang, Y. Liu, B. Dezfouli, A root-based defense mechanism against RPL blackhole attacks in Internet of Things networks, [in:] *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, Honolulu, HI, USA, pp. 1194–1199, 2018, doi: 10.23919/APSIPA.2018.8659504.

21. N. Bhalaji, K.S. Hariharasudan, K. Aashika, A trust based mechanism to combat blackhole attack in RPL protocol, [in:] *ICICCT 2019 – System Reliability, Quality Control, Safety, Maintenance and Management*, V. Gunjan, V. Garcia Diaz, M. Cardona, V. Solanki, K. Sunitha [Eds.], pp. 457–464, Springer, Singapore, 2019, doi: 10.1007/978-981-13-8461-5_51.

22. D. Airehrour, J. Gutierrez, S.K. Ray, A trust-aware RPL routing protocol to detect blackhole and selective forwarding attacks, *Journal of Telecommunications and the Digital Economy*, **5**(1): 50–69, 2017, doi: 10.18080/ajtde.v5n1.88.

23. V. Kiran, S. Rani, P. Singh, Towards a light weight routing security in IoT using non-cooperative game models and Dempster–Shaffer theory, *Wireless Personal Communications*, **110**(4): 1729–1749, 2020, doi: 10.1007/S11277-019-06809-W.

24. S.Y. Hashemi, F. Shams Aliee, Dynamic and comprehensive trust model for IoT and its integration into RPL, *Journal of Supercomputing*, **75**(7): 3555–3584, 2019, doi: 10.1007/S11227-018-2700-3.

25. T. Sakthivel, R.M. Chandrasekaran, A dummy packet-based hybrid security framework for mitigating routing misbehavior in multi-hop wireless networks, *Wireless Personal Communications*, **101**(3): 1581–1618, 2018, doi: 10.1007/S11277-018-5778-2.

26. S.M. Muzammal, R.K. Murugesan, N.Z. Jhanjhi, L.T. Jung, SMTrust: Proposing trust-based secure routing protocol for RPL attacks for IoT applications, [in:] *2020 International Conference on Computational Intelligence (ICCI)*, Bandar Seri Iskandar, Malaysia, pp. 305–310, 2020, doi: 10.1109/ICCI51257.2020.9247818.

27. S. Zangeneh, R. Roustaei, A novel approach for protecting RPL routing protocol against blackhole attacks in IoT networks, PREPRINT (Ver. 1) available at Research Square, 2021, doi: 10.21203/rs.3.rs-174724/v1.

28. R. Mehta, M.M. Parmar, Trust based mechanism for Securing IoT Routing Protocol RPL against Wormhole and Grayhole Attacks, [in:] *2018 3rd International Conference for Convergence in Technology (I2CT)*, Pune, India, pp. 1–6, 2018, doi: 10.1109/I2CT.2018.8529426.

29. J. Jiang, Y. Liu, Secure IoT routing: Selective forwarding attacks and trust-based defenses in RPL network, *arXiv*, 2022, doi: 10.48550/arxiv.2201.06937.

30. S. Suhail, S.R. Pandey, C.S. Hong, Detection of selective forwarding attack in RPL-based Internet of Things through provenance, [in:] *Proceedings of the 2018 Korean Software Conference (KSC2018)*, Pyeongchang, South Korea, Dec. 19, 2018, pp. 965–967, Korean Society of Information Scientists and Engineers Academic, 2018.

31. S. Suhail, S.R. Pandey, C.S. Hong, Using provenance to detect selective forwarding attack in RPL-based Internet of Things, *Journal of Information Science and Computing Practices*, **26**(1): 20–25, 2020, doi: 10.5626/KTCP.2020.26.1.20.

32. F. Ahmed, Y.B. Ko, Mitigation of black hole attacks in routing protocol for low power and lossy networks, *Security and Communication Networks*, **9**(18): 5143–5154, 2016, doi: 10.1002/sec.1684.

33. V. Neerugatti, A.R.M. Reddy, Detection and prevention of black hole attack in RPL Protocol based on the threshold value of nodes in the Internet of Things networks, *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, **8**(9S3): 325–329, 2019, doi: 10.35940/ijitee.I3060.0789S319.

34. B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani, L. Mackenzie, Addressing the DAO insider attack in RPL's Internet of Things networks, *IEEE Communications Letters*, **23**(1): 68–71, 2019, doi: 10.1109/LCOMM.2018.2878151.

35. C. Pu, Mitigating DAO inconsistency attack in RPL-based low power and lossy networks, [in:] *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, pp. 570–574, 2018, doi: 10.1109/CCWC.2018.8301614.

36. I. Wadhaj, B. Ghaleb, C. Thomson, A. Al-Dubai, W.J. Buchanan, Mitigation mechanisms against the DAO attack on the routing protocol for low power and lossy networks (RPL), *IEEE Access*, **8**: 43665–43675, 2020, doi: 10.1109/ACCESS.2020.2977476.

37. R. Sahay, G. Geethakumari, B. Mitra, V. Thejas, Exponential smoothing based approach for detection of blackhole attacks in IoT, [in:] *2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Indore, India, Vol. 2018, 2018, doi: 10.1109/ANTS.2018.8710073.

38. D. Airehrour, J. Gutierrez, S.K. Ray, Securing RPL routing protocol from blackhole attacks using a trust-based mechanism, [in:] *2016 26th International Telecommunication Networks and Applications Conference (ITNAC)*, Dunedin, New Zealand, pp. 115–120, 2016, doi: 10.1109/ATNAC.2016.7878793.

39. G. Glissa, A. Rachedi, A. Meddeb, A secure routing protocol based on RPL for Internet of Things, [in:] *2016 IEEE Global Communications Conference (GLOBECOM)*, Washington, DC, USA, pp. 1–7, 2016, doi: 10.1109/GLOCOM.2016.7841543.

40. H.B. Patel, D.C. Jinwala, Blackhole detection in 6LoWPAN based Internet of Things: An anomaly based approach, [in:] *TENCON 2019 – 2019 IEEE Region 10 Conference (TENCON)*, Kochi, India, pp. 947–954, 2019, doi: 10.1109/TENCON.2019.8929491.

41. S. Luangoudom, D. Tran, T. Nguyen, H.A. Tran, G. Nguyen, Q.T. Ha, svBLOCK: Mitigating black hole attack in low-power and lossy networks, *International Journal of Sensor Networks*, **32**(2): 77–86, 2020, doi: 10.1504/IJSNET.2020.104923.

42. F. Gara, L. Ben Saad, R. Ben Ayed, An intrusion detection system for selective forwarding attack in IPv6-based mobile WSNs, [in:] *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Valencia, Spain, pp. 276–281, 2017, doi: 10.1109/IWCMC.2017.7986299.

43. S. Raza, L. Wallgren, T. Voigt, SVELTE: Real-time intrusion detection in the Internet of Things, *Ad Hoc Networks*, **11**(8): 2661–2674, 2013, doi: 10.1016/j.adhoc.2013.04.014.

44. G. Soni, R. Sudhakar, A L-IDS against dropping attack to secure and improve RPL performance in WSN aided IoT, [in:] *2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)*, Noida, India, pp. 377–383, 2020, doi: 10.1109/SPIN48934.2020.9071118.

45. E.G. Ribera, B. Martinez Alvarez, C. Samuel, P.P. Ioulianou, V.G. Vassilakis, Heartbeat-based detection of blackhole and greyhole attacks in RPL networks, [in:] *2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, Porto, Portugal, pp. 1–6, 2020, doi: 10.1109/CSNDSP49049.2020.9249519.

46. L. Wallgren, S. Raza, T. Voigt, Routing attacks and countermeasures in the RPL-based Internet of Things, *International Journal of Distributed Sensor Networks*, **9**(8): 794326, 2013, doi: 10.1155/2013/794326.

47. K.N. Ambili, J. Jose, TN-IDS for network layer attacks in RPL based IoT systems, *Cryptology ePrint Archive*, **2020**: 1094, 2020, https://ia.cr/2020/1094.

48. A. Lahbib, K. Toumi, S. Elleuch, A. Laouiti, S. Martin, Link reliable and trust aware RPL routing protocol for Internet of Things, [in:] *2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)*, Cambridge, MA, USA, pp. 1–5, 2017, doi: 10.1109/NCA.2017.8171360.

49. A.L. Santos, C.A.V. Cervantes, M. Nogueira, B. Kantarci, Clustering and reliability-driven mitigation of routing attacks in massive IoT systems, *Journal of Internet Services and Applications*, **10**(1): 18, 2019, doi: 10.1186/S13174-019-0117-8.

50. Z.A. Khan, P. Herrmann, A trust based distributed intrusion detection mechanism for Internet of Things, [in:] *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*, Taipei, Taiwan, pp. 1169–1176, 2017, doi: 10.1109/AINA.2017.161.

51. F. Gara, L. Ben Saad, R. Ben Ayed, An efficient intrusion detection system for selective forwarding and clone attackers in IPv6-based wireless sensor networks under mobility, *International Journal on Semantic Web and Information Systems*, **13**(3): 22–47, 2017, doi: 10.4018/IJSWIS.2017070102.

52. H. Bostani, M. Sheikhan, Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach, *Computer Communications*, **98**: 52–71, 2017, doi: 10.1016/j.comcom.2016.12.001.

53. H.B. Patel, D.C. Jinwala, 6MID: Mircochain based intrusion detection for 6LoWPAN based IoT networks, *Procedia Computer Science*, **184**: 929–934, 2021, doi: 10.1016/J.PROCS.2021.04.023.

54. R. Stephen, L. Arockiam, E2V: Techniques for detecting and mitigating rank inconsistency attack (RInA) in RPL based Internet of Things, *Journal of Physics: Conference Series*, **1142**(1): 012009, 2018, doi: 10.1088/1742-6596/1142/1/012009.

55. H.B. Patel, D.C. Jinwala, Trust and strainer based approach for mitigating blackhole attack in 6LowPAN: A hybrid approach, *International Journal of Computer Science*, **48**(4): 1062, 2021, https://www.iaeng.org/IJCS/issues_v48/issue_4/IJCS_48_4_25.pdf.

56. R. Sahay, G. Geethakumari, B. Mitra, N. Goyal, Investigating packet dropping attacks in RPL-DODAG in IoT, [in:] *2019 IEEE 5th International Conference for Convergence in Technology (I2CT)*, Bombay, India, pp. 1–5, 2019, doi: 10.1109/I2CT45611.2019.9033926.

57. A. Verma, V. Ranga, ELNIDS: Ensemble learning based network intrusion detection system for RPL based Internet of Things, [in:] *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Ghaziabad, India, pp. 1–6, 2019, doi: 10.1109/IoT-SIU.2019.8777504.

58. N.M. Müller, P. Debus, D. Kowatsch, K. Böttinger, Distributed anomaly detection of single mote attacks in RPL networks, [in:] *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications (ICETE)*, Prague, Czech Republic, Vol. 1, pp. 378–385, 2019, doi: 10.5220/0007836003780385.

59. A. Verma, V. Ranga, Evaluation of network intrusion detection systems for RPL based 6LoWPAN networks in IoT, *Wireless Personal Communications*, **108**(3): 1571–1594, 2019, doi: 10.1007/S11277-019-06485-W.

60. Y. Al-Hadhrami, F.K. Hussain, A machine learning architecture towards detecting denial of service attack in IoT, [in:] *Complex, Intelligent, and Software Intensive Systems (CISIS 2019)*, L. Barolli, F. Hussain, M. Ikeda [Eds.], Advances in Intelligent Systems and Computing, Vol. 993, pp. 417–429, Springer, Cham, 2019, doi: 10.1007/978-3-030-22354-0_37.

61. V. Neerugatti, A.R.M. Reddy, Artificial Intelligence-based technique for detection of selective forwarding attack in RPL-based Internet of Things networks, [in:] *Emerging Research in Data Engineering Systems and Computer Communications*, P. Venkata Krishna,

M. Obaidat [Eds.], Advances in Intelligent Systems and Computing, Vol. 1054, pp. 67–77, Springer, 2020, doi: 10.1007/978-981-15-0135-7_7.

62. S.O.M. Kamel, S.A. Elhamayed, Mitigating the impact of IoT routing attacks on power consumption in IoT healthcare environment using convolutional neural network, *International Journal of Computer Network and Information Security (IJCNIS)*, **12**(4): 11–29, 2020, doi: 10.5815/ijcnis.2020.04.02.

63. G. Thamilarasu, S. Chawla, Towards deep-learning-driven intrusion detection for the Internet of Things, *Sensors*, **19**(9): 1977, 2019, doi: 10.3390/s19091977.

64. J. Foley, N. Moradpoor, H. Ochenyi, Employing a machine learning approach to detect combined Internet of Things attacks against two objective functions using a novel dataset, *Security and Communication Networks*, **2020**(1): 2804291, 2020, doi: 10.1155/2020/2804291.

65. F. Medjek, D. Tandjaoui, N. Djedjig, I. Romdhani, Fault-tolerant AI-driven intrusion detection system for the Internet of Things, *International Journal of Critical Infrastructure Protection*, **34**: 100436, 2021, doi: 10.1016/J.IJCIP.2021.100436.

66. R. Bokka, T. Sadasivam, Machine learning techniques to detect routing attacks in RPL based Internet of Things networks, *International Journal of Electrical Engineering and Technology (IJEET)*, **12**(6): 346–356, 2021, doi: 10.34218/IJEET.12.6.2021.033.

67. K.N. Qureshi, S.S. Rana, A. Ahmed, G. Jeon, A novel and secure attacks detection framework for smart cities industrial Internet of Things, *Sustainable Cities and Society*, **61**: 102343, 2020, doi: 10.1016/J.SCS.2020.102343.

Received August 1, 2022; revised version September 13, 2022; accepted October 4, 2022; published online July 19, 2024.