IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 1 February 2024, accepted 19 February 2024, date of publication 21 February 2024, date of current version 1 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3368633

RESEARCH ARTICLE

Detecting Version Number Attacks in Low Power and Lossy Networks for Internet of Things Routing: Review and Taxonomy

NADIA A. ALFRIEHAT[1], MOHAMMED ANBAR[1], (Member, IEEE), SHANKAR KARUPPAYAH[1], (Member, IEEE), SHAZA DAWOOD AHMED RIHAN[2], BASIM AHMAD ALABSI[2], AND ALAA M. MOMANI[3]

[1]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), Penang 11800, Malaysia
[2]Applied College, Najran University, Najran 61441, Saudi Arabia
[3]School of Computing, Skyline University College, University City of Sharjah, Sharjah, United Arab Emirates

Corresponding author: Mohammed Anbar (anbar@usm.my)

This work was supported by the Deanship of Scientific Research at Najran University through the General Research Funding Program under Grant NU//RG/SERC/12/3.

ABSTRACT The internet of things (IoT) is an emerging technological advancement with significant implications. It connects a wireless sensor or node network via low-power and lossy networks (LLN). The routing protocol over a low-power and lossy network (RPL) is the fundamental component of LLN. Its lightweight design effectively addresses the limitations imposed by bandwidth, energy, and memory on both LLNs and IoT devices. Notwithstanding its efficacy, RPL introduces susceptibilities, including the version number attack (VNA), which underscores the need for IoT systems to implement effective security protocols. This work reviews and categorizes the security mechanisms proposed in the literature to detect VNA against RPL-based IoT networks. The existing mechanisms are thoroughly discussed and analyzed regarding their performance, datasets, implementation details, and limitations. Furthermore, a qualitative comparison is presented to benchmark this work against existing studies, showcasing its uniqueness. Finally, this work analyzes research gaps and proposes future research avenues.

INDEX TERMS IoT, RPL protocol, VNA, intrusion detection system, security, LLN.

I. INTRODUCTION

The internet of things (IoT) comprises an extensive network of low-power modules that are interconnected, serving as a critical component in various sectors, including healthcare, transportation, industrial systems, and residential automation [1], [2]. These programs heavily rely on wireless sensor networks (WSNs), integral to the IoT. Wide-area WSNs comprise compact, energy-efficient modules with sensing, processing, and communication functionalities, delivering accessible and innovative services. However, concerns arise about power consumption due to the utilization of battery-operated devices [3]

They have emerged in the IoT landscape to mitigate resource limitations in WSNs and LLNs. The IPv6 over low-power wireless personal area networks (6LoWPAN) protocol [4], widely adopted by WSNs, addresses resource limitations and lossy communication channels. Despite improvements, securing LLNs remains challenging, leaving vulnerabilities for attacks like VNAs and threatening data security, privacy, and availability.

The RPL, designed for resource-limited devices, is commonly used in LLNs. However, RPL is vulnerable to VNAs, compromising network security and efficacy. Scholars have proposed various security strategies, including secure transit protocols, lightweight encryption algorithms, and intrusion detection mechanisms [5]. This survey thoroughly evaluates and compares current security measures designed for LLNs, focusing on protecting against VNAs. After examining RPL's vulnerabilities to VNAs, we evaluate the proposed security measures within LLN limitations. A comprehensive literature review reveals numerous papers discussing using

The associate editor coordinating the review of this manuscript and approving it for publication was Young Jin Chu.

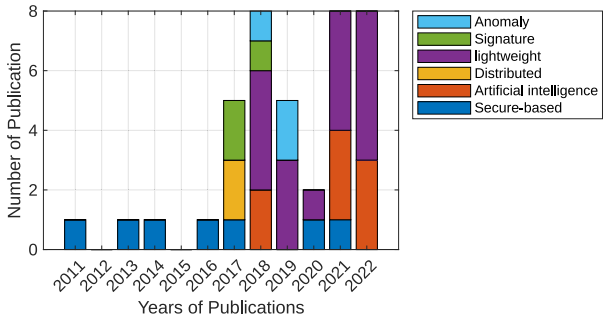

FIGURE 1. Distribution of published works related to VNAs on the RPL protocol.

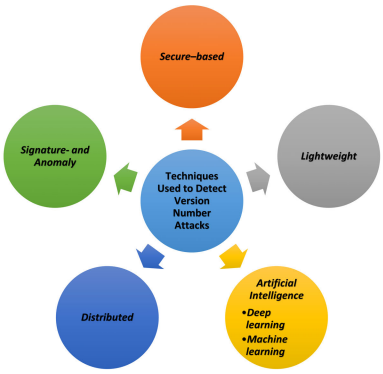

FIGURE 2. Existing approaches Used to detect VNAs.

intrusion detection systems for VNAs in RPL, as illustrated in Figure 1.

Figure 1 depicts the number of publications between 2011 and 2022 related to VNAs on RPL. We scrutinized these papers, comparing their effectiveness in securing the network against VNAs. Studying state-of-the-art security techniques for LLNs helps identify strengths and weaknesses in protecting against VNAs [1].

The term "IoT" denotes a network of tangible entities equipped with sensors, software, and connectivity functionalities, facilitating data exchange via the Internet. WSNs are crucial components of the IoT, with recent security improvements and energy-saving protocols like Low-energy adaptive clustering hierarchy (LEACH) and stable election protocol (SEP) [6], [7], [8], [9] efficient routing algorithms like RPL, and connectivity to both cloud and edge computing.

Recent contributions in the IoT and WSNs domains encompass energy-efficient protocols, routing and data aggregation algorithms, security mechanisms, integration with cloud and edge computing, and standardization efforts by organizations like the institute of electrical and electronics engineers (IEEE) and internet engineering task force (IETF). These contributions address challenges such as limited resources, scalability, network topology management, data aggregation, and security [10], [11].

1) energy-efficient protocols: LEACH and SEP minimize energy consumption at sensor nodes to prolong the network lifetime [12].
2) Routing and data aggregation algorithms: RPL and sensor protocols for information via negotiation (SPIN) reduce data transmission overhead [13], improve scalability, and minimize energy consumption.
3) Security mechanisms: encryption algorithms, authentication protocols, IDS, and secure key management techniques ensure data security in IoT and WSNs [14].
4) Integration with cloud and edge computing: Facilitates efficient data processing, storage, and analysis for real-time decision-making and resource management [15].
5) Standardization efforts: IEEE 802.15.4, 6LoWPAN, and CoAP ensure interoperability and compatibility among different devices and networks [16].

Comparison of IoT, WSN, and 6LoWPAN networks before going into specifics about IDS and how it can be used in IoT, WSN, and 6LoWPAN networks, it is helpful to know what makes these networks unique and how they differ from each other [17], [18].

Table 1 shows how IoT, WSN, and 6LoWPAN networks compare in terms of things like data collection, energy use, network performance, event detection, security, scalability, and communication protocols [19]. This comparison will help in comprehending the unique considerations and challenges associated with implementing IDS in these network environments. A summary of critical attributes among 6LoWPAN, IoT, and WSN networks is displayed in Table 1. Regarding data collection, each of the three networks is capable of amassing environmental information, including temperature and humidity. Energy consumption data pertains to a device or node's power and energy levels. Included in the metrics for network performance are latency, throughput, and dependability [3].

Detection of events requires both triggers and sensor data. Utilizing localization techniques, the location of nodes is ascertained. Aspects of security consist of encryption, authentication, and ID. Varying in scalability, the IoT supports large-scale deployments. IoT utilises MQTT, CoAP, and HTTP for communication, whereas WSN employs Zigbee, Z-Wave, and Bluetooth. 6LoWPAN utilises IPv6, 6LoWPAN, and RPL for communication [20].

After an examination of numerous innovations and developments in WSNs and the IoT, we shall now browse into a particular facet of network security known as VNAs. In contrast to the preceding discussion, which emphasised security mechanisms, routing algorithms, and energy-efficient protocols, it is imperative to focus on the obstacles associated with VNAs within the framework of LLNs and the RPL. The classification of proposed approaches against VNAs is illustrated in Figure 2, which serves as a visual aid for our systematic investigation of techniques and areas where further research is required in this specialised field.

Figure 2 illustrates the classification of proposed approaches based on intrusion detection techniques against VNAs.

As shown in Figure 2, a systematic examination of techniques for discovering research gaps and weaknesses is

TABLE 1. Comparison of IoT, WSN, and 6LoWPAN Networks.

Data Type	IoT	WSN	6LoWPAN Network
Environmental Data	Temperature, Humidity, Light Levels	Temperature, Humidity, Light Levels	Temperature, Humidity, Light Levels
Energy Consumption Data	Device Power, Battery Levels	Node Power, Energy Levels (Solar-powered nodes)	Node Power, Energy Levels (Battery-operated nodes)
Network Performance Data	Latency, Throughput, Reliability	Latency, Throughput, Reliability	Latency, Throughput, Reliability with emphasis on low power
Event Detection Data	Event Triggers, Sensor Data	Event Triggers, Sensor Data	Event Triggers, Sensor Data with context awareness
Localization Data	Geolocation, GPS Coordinates	Node Position, Localization (using triangulation)	Node Position, Localization (GPS-based)
Security and Intrusion Data	Authentication, Encryption	Security Protocols, Intrusion Detection	Security Protocols, and Intrusion Detection with AI-based anomaly detection
Scalability	Large-scale deployments (Smart Cities)	Moderate-scale deployments (Industrial IoT)	Scalable for IoT deployments of various scales
Communication Protocols	MQTT, CoAP, HTTP, LoRaWAN	Zigbee, Z-Wave, Bluetooth, Industrial Wireless HART	IPv6, 6LoWPAN, RPL, Thread

essential. This review addresses issues related to detecting VNAs in RPL by investigating specific research inquiries:

1) **What suggested approaches are currently available for detecting VNAs in RPL?**
2) **How are the datasets for the suggested detection methods produced by researchers?**
3) **What methodology is used to assess the proposed methods?**
4) **which metrics are used to assess the efficacy of the proposed methods During an evaluation?**
5) **Which areas of research have shortcomings that can be addressed and improved upon?**

Thus, we can outline the following as the principal contributions of this review paper:

1) **Recognizing the advanced techniques and IDS researchers use to find VNAs in RPL.**
2) **Determining the metrics for evaluating the proposed detection methods and the datasets, researchers utilize to assess their effectiveness.**
3) **It identifies research areas needing improvement and recommends further study on detection approaches and IDS for VNA under RPL.**

In the subsequent sections of this review, we delve into various aspects related to our study. Section II provides an in-depth exploration of background information, encompassing the RPL protocol, the VNA, performance metrics prevalent in current approaches, widely used simulators, and datasets commonly employed in related studies.

Following this background exposition, Section III conducts a thorough analysis of the existing security mechanisms, with a specific focus on detection techniques. This survey critically compares these techniques to prior studies within the same domain, establishing a contextual understanding of the advancements in security protocols.

Section IV serves as the platform for presenting the findings derived from our study. This section not only encapsulates the outcomes but also highlights potential research needs identified during the investigative process.

Concluding our discourse, Sections V and VI individually feature concluding notes and the conclusion. The concluding notes encapsulate lingering problems and unresolved issues in the field, while the conclusion outlines avenues for future studies. This structured progression through background exploration, analysis, findings presentation, and conclusion aims to provide a comprehensive and cohesive narrative in our review.

II. BACKGROUND

This section aims to provide essential background information and definitions to ensure a clear understanding of the concepts discussed in the subsequent sections, especially those related to IDS or detection methods described in the literature.

A. INTRUSION DETECTION SYSTEMS (IDS)

IDS plays a crucial role in enhancing the security posture of IoT, WSN, and 6LoWPAN networks. These systems monitor and analyze network and device activities to detect and respond to malicious behavior or security incidents. In this context, an IDS is pivotal in safeguarding network security [3].

An IDS, whether implemented as hardware or software, utilizes diverse detection methods to identify potential attacks on a system. Upon detecting an attack, the IDS promptly notifies the system administrator through notifications or reports. The IDS may be a standalone device overseeing an individual system or a network-based system conducting local analyses for attack detection. Furthermore, IDSs contribute significantly to the three fundamental security services, which are (i) data confidentiality, ensuring secure data storage within the system; (ii) data availability, confirming data availability for authorized users; and (iii) data integrity, verifying the correctness and consistency of data within the system [21], [22].

On the other hand, there are various detection techniques utilized in IDSs, which are categorized as follows:

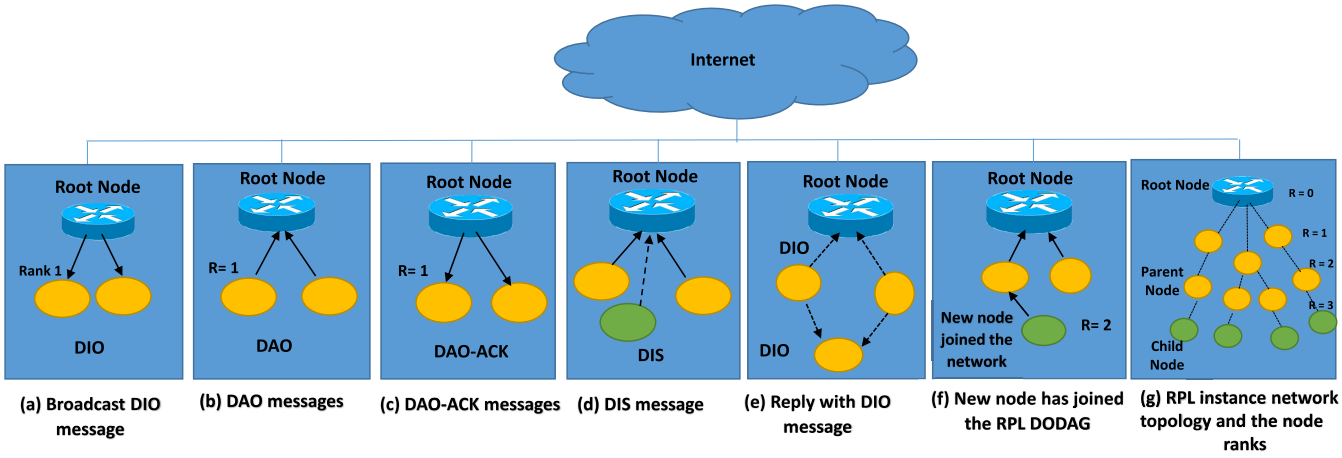

FIGURE 3. DODAG control message structure.

1) Misuse or Signature Detection: This method relies on a database or patterns derived from previously identified attacks. The IDS requires regular updates to its information to identify new attacks effectively.
2) Anomaly Detection: This approach observes the behavior of a system over a specific period, constructing a profile that encompasses all system activities. Various models, including time series and threshold models, can create this profile.
3) Hybrid Detection: This method combines signature and anomaly detection techniques."

B. OVERVIEW OF RPL

In 2012, the IETF established the RPL. In IoT and WSN systems, RPL acts as a distance vector routing mechanism. Its primary objective is to establish a Destination-Oriented Directed Acyclic Graph (DODAG), which comprises a root node, parent nodes, and child nodes [1].

The child nodes communicate with the root node by sending data packets through their parent nodes, with only the root node being directly connected to the internet.

RPL automatically improves the route topology and avoids network loops. In the hop-by-hop and IP-based distance vector routing techniques, each node determines its rank based on the number of hops from the root node. The path with the lowest rank is discovered to be the most direct way to the root node. Using an objective function and specific constraints, nodes in an RPL network choose the best parent node for each child node to connect with, as shown in Figure3.

RPL has two main objective functions (OF), which just account for hop count, and the minimum rank with hysteresis objective function (MRHOF), which also considers the expected transmission count metric.

The RPL protocol utilizes four types of messages to construct a DODAG. The four types of messages used by the RPL protocol are as follows: [5]

1) DODAG Information Object **(DIO)**: The root node transfers the DIO to a node that wants to join an existing DODAG and to its nearby nodes to construct the DODAG. Additionally, it updates the network topology information by broadcasting a message throughout the entire network.
2) A new node that wishes to join the neighboring DODAG will send a message of control known as a DODAG Information Solicitation **(DIS).** To locate an existing network, DIS is utilized.
3) A DODAG Advertisement Object **(DAO)** is a control message sent from child and parent nodes to the root node to update parent node information across the network.
4) A DAG Advertisement Object Acknowledgment **(DAO-ACK)** is a control message sent from the parent node to the child node during the formation of the DODAG or after the acknowledgement of a new node joining request.

The root node broadcasts a DIO message to its neighbors at the initial stage of joining the RPL instance to create a new DODAG (Figure 3, part a). The child nodes return DAO messages (Figure (Figure 3, part b). The root node then provides a DAO-ACK response, completing the DODAG (Figure 3, part c). A node will send a DIS message to the DODAG root node to establish a connection to an active RPL instance (Figure 3, part d). The closest nodes then respond with a DIS message, allowing the new node to join the network (Figure 3, part f). This procedure guarantees that the network has a single root node [23]. With the leaf nodes having the greatest rank values and the internet-connected root node having the lowest rank,(Figure 3, part g) presents the network architecture of an RPL network [24].

Once the nodes establish the network topology, they can begin the routing process and data transmission. However, various security issues may threaten the network, resulting from a malicious node infiltrating the network. Routing attacks are specific security attacks that target the routing process and network topology, resulting in message misdirection and disruption. Modifying the version number in the message

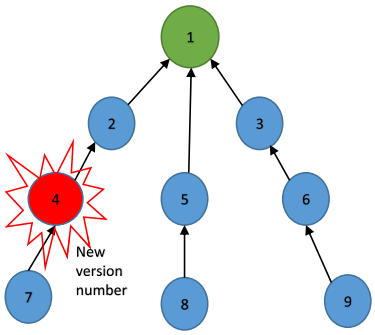

FIGURE 4. Version Number Attack.

header to cause message misdirection is a prime example of this type of attack. Such an attack can significantly affect the network's performance and safety, leading to data loss or security holes [23]. This attack could be a harbinger of more damaging attacks like WH, BH, and selective forwarding (SF) attacks. Additionally, the network architecture may vary due to the VNA, making finding efficient paths for message delivery challenging. Understanding the specifics of the VNA and how it affects RPL is key.

C. THE VERSION NUMBER ATTACK (VNA)

The network is susceptible to a VNA, wherein a malicious node deceitfully elevates the root node's DODAG version number before relaying the DIO message to neighboring nodes [23] Fig.4. Upon receiving the DIO message with the altered version number, the neighbor nodes initiate a new formulation, and the trickle timer is reset [25]. Subsequently, these neighboring nodes broadcast the updated DIO messages continuously [26]. The VNA has serious effects, such as (1) making the network less functional; (2) increasing the amount of work that needs to be done to keep the network running; (3) creating routing loops in data routing; (4) using more energy than it should; and (5) stopping communication channels between nodes from working.

This results in a twofold increase in network latency and an upswing in dropped packets [26]. This attack takes advantage of the global repair mechanism, which is set off when the network has a lot of problems and the root starts a global repair [23]. This mechanism involves rebuilding the entire DODAG by incrementing the version number of the DODAG, carried in a control message called DIO [27]. Each receiving node compares its existing version number with the one received from its parent, initiating a new procedure to join the DODAG if the received version is higher. While this guarantees a loop-free topology, it is a resource-intensive process.

Nodes with an older version in DIO messages should not be chosen as preferred parents. During a global repair, two versions of a DODAG can coexist, but to prevent loops, data packets from the old version can transit to the new version but not vice versa. However, in this transitional state, loop-free topologies cannot be guaranteed.

The version number should be propagated unchanged through the DODAG to maintain consistency. However, RPL lacks a mechanism to ensure the integrity of the version number in received DIO messages, allowing a malicious node to manipulate this value. The resulting propagation of illegitimate version numbers in the network causes unnecessary DODAG rebuilds and generates loops in the topology.

Detection of this attack is challenging for individual nodes due to the deceptive nature of malicious DIO packets, making it difficult to discern whether they originate from a parent or a child. Moreover, localization of the source of malicious DIOs is challenging from a purely local perspective, necessitating communication between nodes to trace the attack's origin [1].

D. SIMULATORS

In general, researchers evaluate the effectiveness of their methods by utilising simulation software and RPL communication datasets to simulate the behaviour of IoT and WSN networks [4]. In our review, we explored 15 studies to obtain the presented result. The details of these studies can be found in Table 2, which provides a comprehensive overview of the diverse evaluation mechanisms employed in the research community. Each of these studies contributes valuable insights into the performance and applicability of various approaches, shedding light on the advancements made in the field of IoT and WSN network evaluations.

The reviewed studies in this field have employed various network simulators, such as the COOJA simulator [28], the Network Simulator NS-2, OMNETT++, MATLAB [23], and Contiki OS. These simulators allow researchers to analyze and test their techniques under various scenarios and network topologies. The choice of a simulator depends on the research requirements and the available resources, as each simulator has limitations and strengths regarding features, scalability, and ease of use. For instance, the COOJA simulator the research community commonly uses the COOJA simulator due to its integration with the Contiki OS and its ability to simulate large-scale networks, as demonstrated in Table 2.

COOJA is considered the best choice for dealing with resource-constrained devices. Using COOJA, researchers can obtain a simulated view of proposed scientific contributions [24]. Table 2provides a comprehensive overview of simulators used in existing approaches to model the RPL protocol [29].

As shown in Table2, the NS-2 simulator is often used for networking research because it works with many different network protocols and has an extensive library of networking components. Also, OMNETT++ is a general-purpose network simulator that gives researchers a flexible environment for simulating a wide range of network scenarios.

Lastly, MATLAB is a popular simulation platform that lets researchers build and study network models through a graphical user interface (GUI). This feature helps investigators interact effortlessly with their models and evaluate

TABLE 2. RPL simulators used in the existing approaches.

Simulation	Developed Year	Programming Languages	Features	Limitations	ref
COOJA simulator	2002	Standard C	-Under its integration with Contiki OS, COOJA is a multifunctional IoT simulation tool that empowers scientists to simulate expansive networks. -evaluate bespoke protocols and applications -supports RPL entirely. -Prominent for its capability to simulate extensive IoT networks, it is capable of accommodating a substantial quantity of nodes and devices	Resource-Intensive: Considerable computing resources may be necessary to simulate large-scale networks.	[24] [36] [30] - [40]
Network simulators NS-2	1989	C++ and OTcl	NS-2 are widely used network simulators, offering flexibility for researchers to implement custom protocols and algorithms and a large user community with extensive documentation.	The interpreted nature of the Tool Command Language (TCL) scripting utilised by NS-2 for configuration and simulation may present difficulties for non-technical users and cause scalability issues in large-scale simulations.	-
OMNETT++	1997	C++ and NED language	-The system presents a range of frameworks for disseminating the network using RPL and can simulate various WSNs. Simulation models for energy consumption are being developed using OMNETT++, a modular architecture that allows researchers to create and integrate models for various network types.	The discrete-event simulation is a resource-intensive and intricate procedure that may demand substantial computational resources from its participants.	-
Contiki OS	2012	Python	Contiki OS are lightweight and energy-efficient, making them ideal for Internet of Things devices with limited resources as they optimize low-power devices and extend battery life.	Contiki OS, although well-suited for Internet of Things (IoT) applications, might be compromised regarding available resources and support due to its limited community size and absence of extensive application support compared to larger ecosystems.	-
MATLAB	1951	-	MATLAB is widely recognized for its potent numerical computing capabilities, which render it well-suited for simulating mathematical models. Additionally, its sophisticated tools facilitate data visualization and result analysis.	Licencing MATLAB, a commercial software, can be expensive; although it offers a wide range of functionalities, it may not be as specialized in network simulations as specialized simulators cost.	[41] [42]

the network's performance, making it a valuable instrument for network simulation research [28], [29]. Since each simulator has its assets and weaknesses regarding scalability, usability, and number of features, selecting a simulator depends on the research requirements and the available resources.

E. DATASETS

Datasets play a very crucial role in artificial intelligence (AI) and machine learning (ML) research, as they provide a means to train and evaluate models. The availability of high-quality datasets is particularly essential for network security and protection. These datasets can be generated synthetically, collected from existing sources, or created by researchers. Datasets may contain benign and malicious network traffic for IoT networks, enabling researchers to develop and evaluate models for identifying VNAs. To conduct effective research in this discipline, comprehending the characteristics and limitations of the available dataset is essential. Table 3 depicts the various categories of VNA-relevant datasets discussed in this section [4], [51]. In our review, we explored more than 15 studies to obtain the presented result. The details of these studies can be found in Table 3 and figure 5

1) **Synthetic datasets:** are generated via a mathematical or computational model instead of being gathered directly from actual observations or experiments. They are frequently used in machine learning and data analysis to create a controlled environment for testing algorithms, models, or methodologies. Synthetic datasets use a variety of algorithms or models to generate data that accurately simulate the statistical characteristics of real-world data. These datasets can be generated based on specified assumptions or distributions to construct scenarios challenging or impossible to observe or to create or generate data types for a specific population or occurrence [23].

TABLE 3. Various categories of VNA-relevant Datasets.

Dataset Name	Developed year	Type of data	Description	Number of instances	Attack families	Ref
synthetic datasets	-	Network traffic	Generated using mathematical or computational models	10,000	VNA, Rank, and HF attacks	[31] [35] [29] [24] [36] [37] [39] [40] [32]
IDC and EDC	2021	Environmental data, body sensor data	depicts a smart hospital structure containing body sensors and environmental data.	1000 (training), 200 (testing)	VNA, rank, and HF attacks	[47] [48]
IRAD	2018	Network traffic	RPL simulation software for VNAs	1,050,861	VNA, DR, and HF attacks	[49] - [51] [30]
Real-time Simulation Dataset	-	Network traffic	RPL specifically tailored for monitoring network behavior and gathering datasets related to IoT networks.	-	VNA, DR,BH,SF, HF and Rank Attack	[33] - [35] [52]

2) **EDC and IDC Dataset:** are two datasets created by researchers [46]at the SERCOM Lab of the University of Carthage that reflect a smart hospital infrastructure. The IDC dataset includes both normal and malicious network traffic, as well as traces of three categories of attacks: rank, deluge, and VN modification. The dataset is split into training and testing sets, with 1000 instances used for training and 200 for testing. The EDC dataset includes environmental and body sensor data, with the former providing temperature, light, and humidity information. The training and testing set for environmental data consists of 100 and 200 instances, respectively [44], while the body sensor data includes information on body temperature and heart rate. A training set of 1000 instances and a testing set of 200 instances were used for the body sensor data.
3) **IRAD dataset:** There are three routing attacks within the dataset: DR attack, greeting HF attack, and VNA attack., developed by Yavuz et al. [40]. The dataset comprises 1,050,861 records, with 884,861 assigned as benign and the remainder as malicious traffic. The authors created a Python model to extract dataset features, with 113 parts extracted. The authors also developed a lightweight mechanism to detect the attack. This dataset is unique in focusing on DR, HF, and VN attacks and using a Python model to extract features [29].
4) **A real-time dataset** is a collection of data that is continuously created, updated, and available for processing or analysis in real-time. It accurately records and depicts dynamic events or phenomena, often from sensors, streaming platforms, or live event data. Due to their size, effective data processing, storage, and analysis methods are needed [42].

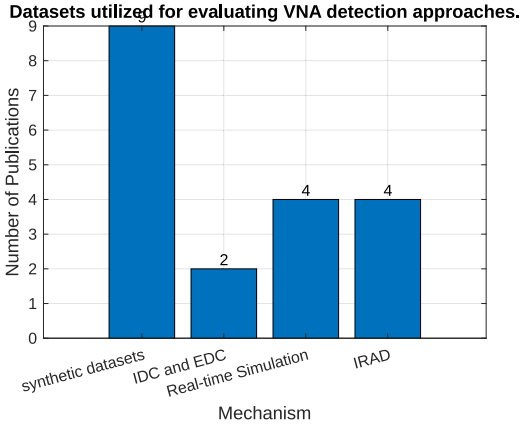

FIGURE 5. Datasets utilized for evaluating VNA detection approaches.

Figure 5 shows the datasets Utilized for evaluating VNA detection approaches.

As indicated in Figure 5 and Table 3, the researchers have widely used synthetic datasets to evaluate their methods in the context of VNAs because they offer greater control over the data characteristics and enable the creation of many instances with specific features. Different approaches, such as simulation software and mathematical models, can produce customized synthetic datasets that mimic network topologies, traffic patterns, and attack scenarios. This flexibility allows researchers to systematically vary the dataset's features and evaluate the impact of various factors on the performance of

their methods. Additionally, synthetic datasets can generate instances with known ground-truth labels, facilitating the training and testing of machine-learning models. Overall, using synthetic datasets provides researchers with a controlled environment to evaluate the effectiveness of their methods and gain insights into the behaviour of VNAs.

F. PERFORMANCE EVALUATION METRICS

When evaluating proposed systems, researchers use different metrics. The following metrics are commonly employed in the literature to assess the effectiveness of approaches proposed for detecting VNAs [43], as shown in Table 4.

The primary objective of detecting attacks is to achieve optimal effectiveness, measured through the performance metrics presented in Table 4, which highlights the different metrics employed by researchers to evaluate the effectiveness of their proposed techniques. The commonly used metrics include packet delivery ratio (PDR), energy consumption, the true positive rate (TPR), and the false positive rate (FPR) are all crucial indicators of malicious attacks.

1) **PDR refers to the proportion of data packets the Gateway has received concerning the overall quantity of packets the sensor nodes have transmitted, calculated as follows.**

$$PDR = \frac{\text{Number of Packets Received at Sink}}{\sum_{i=1}^{N} \text{Packets Sent By Node } i} \quad (1)$$

2) **Average End-to-End Delay (AE2ED)** shows the relationship between the time it takes for each packet to be successfully transmitted to the Gateway and the number of packets that have been sent, without considering any packets that were not successfully delivered [49].

$$\text{AE2ED} = \frac{\sum_{i=1}^{N} \text{Packet Delay}_i}{\text{Total Packets (Received Successfully)}} \quad (2)$$

3) **Energy consumption (EC) or energy usage** is evaluated for various conditions of the node, such as whether the radio is active or not, whether the microcontroller is sending or receiving signals, or if the microcontroller is in a state of low power.

$$Energy_c = (C_{\text{CPU}} + C_{\text{LMP}} + C_{\text{TX}} + C_{\text{RX}})\,\text{mj} \quad (3)$$

$$\text{Power} = \frac{\text{Energy}_c}{\text{Total\_Time}}\,\text{mW} \quad (4)$$

4) **Control Overhead (CO)** is a dimensionless metric that quantifies the ratio of received to control packets. This measure needs to be evaluated carefully because a specific IDS system could increase network overheads. The success of the system's prediction depends on its accuracy, either positive or negative, depending on whether it relates to an attack.
Therefore, there are four possible outcomes: accurate and safe prediction, correct attack prediction, safe attack false negative, and false positive. These outcomes are classified as true positive (TP), true negative (TN), false positive (FP), and false negative (FN), respectively. The classification error is determined by the ratio of incorrect predictions to the total number of forecasts, as follows [29], [46]:

5) **Accuracy:** The metric of accurately identifying whether the network activity is regular or under attack is calculated using Equation (5).

$$\text{Accuracy} = \frac{(TP + TN)}{(TP + TN + FP + FN)} \quad (5)$$

6) **Precision** indicates the number of accurate attacks identified among the detected attacks.

$$rCl\text{Precision} = \frac{TP}{TP + FP} \quad (6)$$

7) **Recall metric** indicates the proportion of true positives with the combined number of TP and FNs.

$$\text{Recall} = \frac{TP}{TP + FN} \quad (7)$$

8) **F1-score** is a weighted harmonic average that considers both precision and recall, providing a measure of the balance between the two.

$$\text{F1} = 2 \times \left(\frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}\right) \quad (8)$$

9) This research employed two distinct metrics to address the issue of imbalanced datasets. The first metric, called True positive rate (TPR), positive class accuracy, or recall, is sensitivity. The second metric, negative class accuracy or true negative rate (TNR), is specificity [29].

$$\text{Sensitivity (TPR)} = \frac{TP}{TP + FN} \quad (9)$$

$$\text{Specificity (TNR)} = \frac{TN}{TN + FP} \quad (10)$$

10) **Throughput** Measured by dividing the period by the total number of active packet arrivals detected at the destination. Its equation is as follows: [64]:

$$\text{Throughput} = \frac{Number\ of\ packetsent}{Time} \quad (11)$$

III. LITERATURE REVIEW

This section focuses on the research papers published on IDS and detection techniques for RPL networks susceptible to VNAs. The review also includes a performance review and how the suggested methods have been implemented. This review has also summarized other literature reviews, highlighting the unique contribution of this review.

Researchers have proposed various methods to identify VNAs in RPL networks, which fall into the following categories: secure-based, lightweight, AI, signature, anomaly, and distributed. In this review, we have explored each of these classifications in detail.

TABLE 4. Distribution of the metrics in the existing studies.

REF	PDR	TPR	FPR	CO	AE2ED	EC	ATTACKER POSITION	CONTROL PACKETS	TIME	LA-TENCY	F-SCORE	PRECI-SION	ACCU-RACY	RE-CALL
[54]	✓	✓	✓	✓	×	×	×	×	×	×	×	×	×	×
[44]	✓	×	×	×	✓	✓	×	×	×	×	×	×	×	×
[55]	✓	×	×	×	✓	✓	✓	×	×	×	×	×	×	×
[55]	✓	×	×	×	×	×	×	✓	×	×	×	×	×	×
[37]	✓	×	×	×	✓	✓	×	×	×	×	×	×	×	×
[57]	×	×	×	×	×	✓	×	×	×	×	×	×	×	×
[25]	✓	×	×	✓	×	×	×	×	×	✓	×	×	×	×
[26]	×	✓	✓	×	×	×	×	×	×	×	×	×	×	×
[58]	✓	✓	✓	✓	×	×	×	×	×	×	×	×	×	×
[59]	×	✓	✓	×	×	×	×	×	×	×	✓	×	×	×
[55]	✓	✓	✓	✓	×	✓	×	×	×	×	×	✓	×	×
[60]	×	×	×	✓	×	✓	×	×	×	×	×	×	×	×
[23]	×	×	×	×	×	✓	×	×	×	×	×	×	×	×
[62]	×	×	×	×	×	✓	×	×	×	×	×	×	×	×
[63]	✓	✓	✓	✓	×	×	×	×	×	×	×	×	×	×
[64]	✓	×	×	✓	×	×	×	×	×	×	×	×	×	×
[65]	×	✓	✓	×	×	×	×	×	×	×	✓	✓	✓	✓
[50]	×	×	×	×	×	×	×	×	×	×	✓	✓	✓	✓

A. SECURE PROTOCOL-BASED MECHANISMS

This section provides an overview of multiple defense mechanisms that employ secure protocols to protect the RPL protocol from VNAs. Table 5 summarizes these secure protocol solutions.

The authors of [56] suggest a security system called VeRA that is designed to ward off attacks employing fake VNs and rank modifications. The fundamental idea behind this strategy is to employ hash chains to verify nodes whose rank, or VN, changes. VeRA incorporates a hash-based, minimally time-consuming authentication method. VeRA's resistance to circumvention is a noteworthy trait except for rank fabrication and replay attacks [59].

In another study by Landsman et al. [57], a novel security technique is introduced to counter the reduced rank attack. This solution uses a multilayer encryption chain to stop attackers from broadcasting updated hash chains and maintain rank integrity. VN and rank hash chains are connected by the encryption chain. It should nevertheless be emphasized that this security feature does not offer a defense against rank-replay attacks.

To detect and prevent topological differences, Perrey et al. [57] presented an addition to the security technique suggested in [65]. RPL offers topology-based authentication with the trust anchor interconnection loop (TRAIL) general security technique. Without depending on encryption chains, TRAIL enables every node to verify its upward routing path to the root and spot TRAIL can locate and eliminate unwanted nodes from a network's topology. VeRA and TRAIL, on the other hand, demand that nodes prohibit their states for nodes with low memory resources.

Mayzaud et al. expanded their previously described technique [58] for detecting VNAs in their investigations [43]. They admitted that a higher VN spreads throughout the entire graph and that a monitoring node cannot tell on its own whether this is an attack. To improve the effectiveness of global detection, they updated the distributed monitoring architecture to allow monitoring nodes to cooperate using a multi-instance network. However, this defense design assumes a solitary attacker and disregards mobility, limiting its usefulness in more complicated circumstances.

In [43], the authors built on their prior work by incorporating detection and localization methods. They put the "LOCAL ASSESSMENT" algorithm on monitoring nodes separate from the root to give them the ability to inform the sender's root of an increased version number in their neighborhood. They discovered an attack on the sink node using the "DISTRIBUTED DETECTION" approach, and they collected all the information from the monitoring nodes into tables. Finally, they used the information acquired to find the perpetrator by applying the "LOCALIZATION" algorithm to the drain node [66], Table5 provides a summary of essential parameters, benefits, and drawbacks of a secure-based mechanism.

Summary and Analysis: The analysis of a secure-based mechanism is presented in Table 5. This section focuses on several secure protocol-based defense approaches to safeguard the RPL protocol. However, these approaches possess

TABLE 5. A review of secure-protocol- based detection techniques.

Ref	Attacks	Specific Mechanism	Pros	Cons/Limitations	Summary of Result
[58]	VNA and DR	VeRA	-Low-time overhead -Implementable in real scenarios	Vulnerable to Rank-reply attacks, adds memory computation overhead	VeRA can strictly detect attacking nodes using a one-way hash chain
[67]	VNA and DR	Enhanced VeRA	-Solves some issues discovered in VeRA	Issue with TRAIL: a child node can choose an attacking node as its parent, leading to extra overhead when using the Trail method in RPL	No TRAIL evaluation concerning energy or resource consumption was present
[59]	VNA, DR, and Rank replay	Hash chain / TRALL	Less complicated computations compared to VeRA	If a vulnerable child node has extra memory overhead, it may incorrectly identify the offender as a parent	-NA
[44]	VNA	Distributed monitoring architecture	-	Only One Attacker Case Considered. To find anomalies, monitoring nodes must operate in promiscuous modes	-NA

limitations in offering sufficient security for IoT networks owing to several challenges that necessitate resolution.

For instance, vulnerability to rank forgery and replay attacks [56], increased resource overheads (i.e., memory and processing) [43], [57], and significant increase in communication overhead [65] restrict their usage in existing 6LoWPAN networks. To effectively use secure-based solutions, further exploration into IoT constraints is necessary. It can also investigate lightweight cryptographic keys for developing security solutions for the IoT.

B. LIGHTWEIGHT MECHANISMS

Resource-constrained nodes may experience scalability and resource limitations due to RPL's complex structure and high control message overhead. Lightweight mechanisms that streamline RPL and lower its overhead while preserving its routing performance have been offered to solve these problems. These mechanisms include streamlined default parameter sets, simplified control message formats, and fewer control messages.

Lightweight techniques can increase the scalability and effectiveness of LLN routing by lowering the complexity and overhead of RPL. As shown in Table 6, several studies have proposed lightweight mitigation techniques for VNAs.

In the study [51], researchers proposed two methods to mitigate VNA, each with different resource requirements and performance outcomes. The first technique eliminates VN updates from leaf node directions, effectively mitigating the most critical attack positions but not addressing the rest of the attacking positions. The second technique allows nodes to change their VN neighbors with better ranks and claim a VN update, mitigating the attack's effects regardless of the attacking positions.

The effectiveness of these techniques is tested on four different topologies, showing a reduction in adverse effects caused by the attack while allowing legitimate VN updates. Results indicate a significant decrease in delay caused by the attacker, up to 87%, a reduction in average power consumption of up to 63%, a lowering of control message overhead by up to 71%, and an increase in data packet delivery ratio of up to 86%. Therefore, researchers proposed a lightweight solution to address the negative impact of VNAs [67].

The approach involves each node in the RPL network running unique algorithms that do not require storing node states. The evaluation results demonstrate that the proposed scheme is lightweight and compatible with resource-constrained devices.

In addition, Belkheir et al. [55] proposed a novel, lightweight, decentralized approach to minimizing VNAs in RPL-based IoT networks [66]. Their solution entails modifying the fundamental DIO processing conducted by a node to maintain the same VN as the root and only accept VN from its preferred parent. The researchers conducted simulations to evaluate the effectiveness of their proposed solution. They found that it exhibited superior performance compared to existing techniques, with energy savings of up to 58% and a reduction in control overhead of up to 81% depending on the attacker's position in the network. Hence, CDRPL, a security scheme proposed in [62], is a collaborative and distributed approach that aims to improve the resilience of RPL against VNAs. The method offers fast and accurate detection of attacks, quick convergence of the network topology, and efficient network stability with reduced energy consumption.

Rosewelt et al. [53] used a two-phase approach based on machine and deep learning (DL) techniques in their study. In the first phase, they employed a qualitative feature extraction method based on filter techniques independent of any classifiers, allowing for selected features independent of machine learning or DL algorithms. In the second phase, the authors addressed the issue of imbalanced datasets by

TABLE 6. Intrusion Detection System based on Lightweight.

Ref	Attacks	Specific Mechanism	Pros	Cons/Limitations	Summary of Result
[53]	VNA	Lightweight / Mitigate	Compared to other options, SRPL-RP demonstrated higher levels of effectiveness in detecting and addressing the issue [57].	-The proposed mechanism didn't support multiple attacks. - It doesn't incorporate mobility	- Average delay (87%), PDR (86%), Control overhead (71%), AR (92.93%), and Energy Consumption (63%)
[55]	VNA	Lightweight	Simulations for various scenarios verified the efficacy of the suggested approach for increasing the network lifetime.	The approach did not consider mobility traits and energy consumption	Control overhead (81%), and energy saving reaches (58%)
[70]	VNA	Lightweight / Mitigate	Improve virtual networks by evaluating CDRPL's robustness and performance.	This work only detects a single type of attack	PDR (97.98%), Control overhead (950), Energy Consumption (1247.90), and ACC (99.0%)
[26]	VNA	Lightweight	Can effectively implement the proposed approach as a unified framework for detecting VNAs in a real-world, complex IoT network.	- Other significant parameters, such as PRC, E2E delay, and PDR, were not assessed. - Only one form of attack can be detected in this investigation.	Accuracy of the NN classifier is above 97%.

using the SMOTE oversampling technique. Table6 shows a summary of lightweight-based mechanisms.

Summary and Analysis: the analysis of lightweight-based mechanisms is presented in Table 6. One method proposed for detecting RPL attacks involves a monitoring architecture where nodes collaborate and share information [67]. However, this approach assumes only one attacker and does not account for node mobility, which can negatively affect system performance [51], [53]. Another proposed method involves cooperative verification between neighboring nodes, which can increase false detections as the number of attackers grows [26]. These methods are limited in accurately detecting VNAs in RPL networks, mainly when multiple attackers and mobility are present. Improvements are needed to address these challenges effectively.

C. ARTIFICIAL INTELLIGENCE (AI) BASED MECHANISMS

Integrating AI, IoT, and 5G is a pivotal strategy in developing the next-generation smart network. As explored in the research paper [68], the paper delves into the imperative need for automated decision-making, security fortification, scalability, real-time monitoring, and seamless interoperability across network layers.

Within IoT networks, the synergy of AI techniques with IDS is transformative. Leveraging ML and DL algorithms, IDS can intricately scrutinize real-time network traffic, swiftly identifying potential threats and monitoring deviations from normal behaviour [4]. This innovative integration not only bolsters the accuracy of intrusion detection but also minimizes false alarms, culminating in a more secure and resilient IoT network [69]. The comprehensive exploration of this integration is reflected in Tables 7 and 8 below.

1) DEEP LEARNING

Several studies have proposed using DL for detecting routing attacks in IoT networks. Yavuz et al. [29] presented a scalable DL-based system that caught three types of RPL attacks using a dataset created with Cooja emulation and the Contiki operating system. The authors used a deep neural network(DNN).

Model to detect these attacks and obtained an accuracy rate of 99.5 % for the greeting deluge attack, 94.9% for the

DR attack, and 95.5% for the VNA attack. Additionally, they developed a distributed IoT network attack detection system based on DL.

They compared its performance with traditional ML methods like support vector machines (SVM), decision trees (DT), and other neural networks (NN). The results showed that the DL-based system outperformed traditional ML methods regarding accuracy, detection rate, false alarm rate, F1 measure, recall, and precision. DL increased the proposed model's accuracy from around 96% to above 99%Ȯverall, this work demonstrates the potential of DL for accurately identifying IoT attacks in the distributed architecture of IoT applications.

Kamel SOM et al. [37] developed a new model that uses a convolutional neural network (CNN) to find routing attacks and guess suspicious traffic in IoT networks. The dataset used to train the algorithm had five attack groups. The authors utilized three preprocessing techniques, including feature selection, Chi-squared, and weighting by tree importance, to improve the model's performance. These techniques reduced overfitting and noise in the input data, which enhanced the model's predictability. In their study, Rosewelt et al. [53] introduced an ML and DL technique that consists of two phases.

In the first phase, the authors employed a qualitative feature extraction approach based on filter techniques independent of any classifiers. They ensured that the selected features were not reliant on any specific ML or DL algorithm.

In the second phase, they utilized the synthetic minority oversampling technique (SMOTE) to address imbalanced datasets. This approach helped improve the model's accuracy by generating synthetic samples for the minority class, thereby achieving a better balance between the classes in the dataset.

On the other hand, Nayak et al. [60] developed a DL-based routing attack detection model for industrial internet of things (IIoT) networks. This model can detect planned attacks in RPL using adversarial training. The authors combined the generative adversarial network (GAN) and SVM to create the GAN-C model, demonstrating superior performance in detecting attack events. Table7. provides a summary of essential parameters, benefits, and drawbacks of DL-based techniques.

Summary and Analysis: the analysis of DL-based mechanisms presented in Table7 reveals several significant limitations. The proposed model for detecting routing attacks in IoT networks has limitations, such as its long training time and vulnerability to other attacks. Incorporating DL models, however, can increase detection rates, as shown in previous studies [29].

In another work, VNA classification was stable and not sensitive to specific classes [58]. However, important metrics like PDR, PRC, and E2E delay data were missing, and the authors of [37] and [53] did not share the datasets and features they used. Furthermore, the suggested solutions in [60] are targeted at VNAs, and it is uncertain if they would be effective against other kinds of attacks.

Additionally, as shown in Table 7, DL techniques are more effective than traditional data processing methods for analyzing large datasets [40]

2) MACHINE LEARNING

ML techniques have emerged as a promising solution for enhancing the detection performance of IDSs in the IoT domain. Specifically, RPL-based networks can utilize ML algorithms to learn from large-scale datasets and adapt to changing attack patterns, improving the accuracy and efficiency of IDSs. The utilization of ML in RPL-based IDSs is a growing research area that can lead to more reliable and secure IoT applications.

Sahay et al. developed a method for identifying VNAs in IoT systems [24]. It is applicable at the edge of the IoT-LLN network or in the cloud, with accurate detection and no misidentification. The framework is divided into many stages, including filtering input features, feature preprocessing, and application of ML classification algorithms (DT, SVM, Bernoulli RBM, and LR). VN fluctuations and the quantity of VN changes when malicious nodes issue a warning are two criteria used in detecting VNAs. The root node for blacklisting. The findings indicated that the Light Gradient Boosting Machine (ML-LGBM) model outperformed existing approaches with high accuracy, precision, and f-score. The ML-LGBM model achieved an ACC of 99.6% a precision of 99% an F-Score of 99.6% a true negative rate of 99.3% and a false negative rate of 0.0093.

In their study, Kfoury et al. [30] introduced the Self Organizing Map Intrusion Detection (SOMID) tool to identify Sinkhole, VRA, and HF attacks. SOMID utilizes Self Organizing Maps (SOM) to group regular and malicious network traffic based on data extracted from a packet capture (PCAP) file generated by a Cooja simulator. The system consists of three main components: an aggregator that compiles data from the PCAP file, a normalizer that standardizes the collected data, and a trainer that educates SOM.

The result is a matrix that can be displayed as a 2D image, demonstrating the clustering patterns. Also, Sharma et al. [45] proposed the ML approach to detect routing attacks in RPL. They simulated three types of attacks, such as HF, DR, and VNA, and utilized an artificial neural network (ANN) for attack detection. Setting up network scenarios, watching how networks behave during attacks, gathering and processing data, using ANN to sort and analyze network traffic, and fine-tuning ANN's performance were all parts of the proposed ANN-based IDS workflow.

They evaluated the system's performance using hold-out and k-fold cross-validation techniques across four simulation scenarios, each representing one type of attack, and a final scenario combining all attacks.

During HF attacks, the malicious node generated the most packets, while during VNAs, it encouraged neighboring

TABLE 7. Intrusion Detection System based DL.

Ref	Attacks	Specific Mechanism	Pros	Cons/Limitations	Summary of Result
[30]	VNA, HF, and DR	MLP-Based ANN	Making new datasets accessible to other researchers.	- Long training time. - The major disadvantage of this approach was that the attack datasets were generated through simulation, and the authors did not use real data traces.	- F1-Scores: DR (94.7%), HF (99%), and VNA (95%) - AUC: DRA (94.2%), HF (98.1%), and VN (94.7%)
[38]	VNA, HF, and DR	GAN-C and SVM (Hybrid)	The comparison results indicate that the distributed GAN-C model outperforms the centralized GAN-C model regarding detection and response times.	- Need a lot of computational resources, which might be restrictive for IoT devices with limited resources.	- F1-Scores: VNA (70%), HF (83%), and DR (92%) - Precision: VNA (73%), HF (84%), and DR (93%). - Recall: VNA (68%), HF (82%), and DR (92%).
[55]	VNA	Threshold / NN	The proposed approach could need a lot of computational resources and might be restrictive for IoT devices with limited resources.	The approach is specific to VNA, and whether it can be used to defend against other attacks is unknown.	The accuracy of the NN classifier is above 97%
[60]	VNA	Lightweight/ Mitigate	Minimize energy consumption and network overhead.	- The evaluation results may not correctly reflect real-world applications because they are based on simulations with the Cooja simulator running under Contiki OS.	Energy saving (58%) and reduced control overhead (81%)
[62]	HF, SF, SH, WH, 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	HF attacks AC (96.87%), precision (94.85%), Error Rate (3.13%), recall (99.65%), Correlation (93.8%), measure (97.19%), and F- (0.325)

nodes to create more packets. During DR attack scenarios, it initiated the fewest packets. The hold-out approach was shown to be more effective when compared to the k-fold cross-validation method since it required less time to reach 100% accuracy.

Tenfold cross-validation was used to prevent overfitting problems. The accuracy of the ANN model was eventually ideal after hyperparameter optimization.ANN for attack detection. Setting up network scenarios, watching how networks behave during attacks, gathering and processing data, using ANN to sort and analyze network traffic, and fine-tuning ANN's performance were all parts of the proposed ANN-based IDS workflow.

They evaluated the system's performance using hold-out and k-fold cross-validation techniques across four simulation scenarios, each representing one type of attack and a final scenario combining all attacks.

During HF attacks, the malicious node generated the most packets, while during VN attacks, it encouraged neighboring nodes to create more packets. During DR attack scenarios,

TABLE 8. Intrusion detection system based ML.

Ref	Attacks	Specific Mechanism	Pros	Cons/Limitations	Summary of Result
[24]	VNA	(DT, (SVM) Bernoulli and (LR)	The system presented in the research demonstrated exceptional accuracy, precision, recall, and specificity outcomes.	- Did not assess other crucial measures like PDR, PRC, and E2E. - This research is limited to detecting only a particular form of attack.	- DT and Bernoulli Recall (95%), RBM (95%), LR (95%), SVM (94%), Acc (0.98), Precision (1.00), and Specificity (1.00)
[31]	VNA	ML and DL / Logistic Regression SVM, G NB, and NN	As a comprehensive system for identifying attacks related to VNs, can the suggested approaches efficiently apply in a complex IoT network in the real world	The study didn't assess other vital parameters, including PDR, PRC, and E2E delay. The scope of this research is limited to detecting a single form of attack.	The Acc Of the NN Classifier Is Above (97%).
[51]	HF SH, and VNA	Self-Organizing Maps/ (SOMIDS)	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 research. - There is significant implementation overhead, and it did not consider mobility.	It Clusters the Attacks and Normal traffic
[48]	VNA	Gradient Boosting	The research introduced in the paper surpassed alternative techniques in various measurements, including training duration, testing duration, and model dimensions.	-Information regarding the accessibility of the dataset created is not provided. The authors utilized minor network nodes when generating the dataset.	Acc (99.6%), Precision (99%), F-Score (99.6%), and TNR (0.0093)
[73]	HF, DR, and VNA	ANN	The AIEMIA method attained the most exceptional accuracy results using the hold-out validation technique.	- No data is provided about the acquired characteristics. - Additionally, the author utilized a diminutive network size for assembling the datasets.	Accuracy (100%)
[47]	HF, DR, and VNA	SVM	In this investigation, attacks on e-health networks were detected with great accuracy. - the strategy used a trustworthy management program with industry-standard features to provide a cost-effective decision-making solution.	The feature selection methodology utilized by the authors was not disclosed, nor were the details of the dataset's accessibility made clear.	NA

it initiated the fewest packets. The authors compared the efficacy of the hold-out and k-fold cross-validation methods and determined that the hold-out method required percent accuracy to achieve 100 percent accuracy.

They utilized 10-fold cross-validation to prevent overfitting problems. Eventually, after optimizing its hyperparameters, the ANN model attained 100 percent accuracy. Osman et al. [49] presented a multi-layer (MLRPL) model

TABLE 9. Intrusion Detection System Based-Distributed.

Ref	Attacks	Specific Mechanism	Pros	Cons/Limitations	Summary of Result
[60] [44]	VNA	Distributed	Potentially locates the attacker	It requires significant monitoring equipment, which results in increased costs. This project is only capable of identifying one type of attack.	-NA
[75]	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%), Prediction Rate (95%), and Control overhead (1500vs)

that uses an ANN approach to recognize DR attacks in RPL.

Data preprocessing, feature extraction, and ANN-based attack detection comprise the three phases of the MLRPL model. The authors tested their model using the IRAD dataset, which included VNA, DR, and HFs. The authors combined the VNA and DR attack datasets into a single RPL attack dataset with 18 features during the data preprocessing step.

In the second phase, the scientists trained an RF classifier on the dataset and used an entropy approach called information gain to evaluate each quality. The ideal eight attack detection features were created during this phase. As a result, many detection situations, including binary and multi-class classification, were utilized to gauge the model's effectiveness [67].

The experimental findings also revealed that for binary class detection, the training and testing accuracies were 97.14% and 97.01% respectively, while for multi-class detection, the values were 96.59% and 96.39%The proposed methods produced a 97.14% overall accuracy, a 97.03% precision score, a 0.36% FPR, and a 98% AUC-ROC score. Regarding training time and ANN model complexity, the MLRPL approaches work better than earlier ones [67], [71].

Summary and Analysis: Table 8 provides an overview of studies that used ML for ID in RPL networks. The proposed models had varying accuracy and approaches, some having high accuracy but with drawbacks like increased memory and energy consumption or an inability to identify the attacker [24]. This section highlights the need for further research to improve the accuracy and efficiency of these models. Additionally, some studies only detect one type of attack [36], [53], [62], and no information is available about the generated dataset's availability [37], [45].

The authors of [46] also provided an architecture with a real-time data collection tool for tracking network activity and gathering IoT network information. The data collection model (DCM), detection model (DM), and classification model (CM) make up the suggested architecture. The DCM can gather IoT communication data from the physical, network, and application layers and is interoperable with all IoT protocols.Table8 summarizes studies that employed ML for ID in RPL networks.

D. DISTRIBUTED BASED MECHANISMS

IDS utilizes distributed methodologies to identify and mitigate threats and vulnerabilities in IoT networks. Distributed monitoring stands out among these methods because it entails cooperation between various IDS nodes to monitor and investigate network traffic for suspected intrusions. This cooperative strategy can help decrease FP and increase the precision of ID. Many studies have been performed on the efficiency of this strategy, and this section presented some of them.

Mayzaud et al. [58] developed a distributed monitoring system for DODAGs using RPL's multi-instance feature and dedicated monitoring nodes. The system combines regular and monitoring nodes, enhancing security. Monitoring nodes use local anomaly detection algorithms to analyze data and identify potential distributed attacks. However, the system faces limitations in detecting multi-attacker scenarios and high-end device use, requiring further improvement. Additionally, the authors [43], [72]of the study acknowledged that the propagation of an incremented version number across the entire graph could make it difficult for a monitoring node to determine if this results from an attack.

Therefore, they proposed an extension to the distributed monitoring architecture that enables monitoring nodes to

collaborate and share information to identify malicious nodes. The proposed multi-instance network facilitates global detection, enabling monitoring nodes to collaborate and share information to identify malicious nodes. However, it is essential to note that this defense architecture assumes only one attacker case and does not consider mobility. Table 9 shows a summary of distributed mechanisms.

Summary and Analysis: As presented in Table 9 above, the ideas in [43] and [72] come with extra costs for setting up networks, which are not ideal for networks with limited resources. Furthermore, tackling these crucial challenges to advance IDS for the IoT is imperative.

E. IDS-BASED, SIGNATURE- AND ANOMALY

Securing RPL networks against various attacks is a challenging task. One common approach for securing RPL networks is anomaly-based and signature-based IDS [65].

1) Signature-based detection is a method to detect and prevent malicious behaviors using preexisting attack signatures [54]. It is commonly used in IDS and can effectively identify known attacks. However, it may struggle to identify unknown or previously unseen attacks due to its reliance on existing signatures [30].
2) Anomaly-based detection assumes that the normal behavior of a network is known, and any deviation from this behavior can be considered an anomaly. This approach analyzes network traffic and system behavior to identify variations from normal patterns, indicating a potential intrusion [28]] , [73].

It was recognized by Mayzaud et al. [58] that an increased VN could spread throughout the graph, making it challenging for a monitoring node to verify whether it results from an attack. Therefore, they increased the distributed monitoring architecture, enabling monitoring nodes to cooperate and boosting detection effectiveness. However, the protection architecture only considered a single attacker and ignored mobility.

They developed this work in [67], where they introduced techniques for detection and localization. For monitor nodes [43], other than the root, to notify the root of the sender of an increased VN in their local area, the LOCAL ASSESSMENT algorithm was implemented on those nodes. The DISTRIBUTED DETECTION algorithm was used on the sink node to recognize the attack and gather information from all monitoring nodes. On the other side, the LOCALIZATION method was used on the sink node, and the information gathered was evaluated to determine who the attacker was. This framework carried over the drawbacks of the earlier strategy by Mayzaud et al. [58].

Philokypros et al. [74] proposed a framework for detecting DIS and VNA using a signature-based IDS. The approach requires the installation of detection and monitoring modules on nodes, like hybrid detection schemes, but with the addition of two types of nodes: sensors and IDS detectors, including routers. While sensors and IDS detectors watch and report on malicious traffic to the router nodes, IDS routers feature detection and firewall modules. All incoming traffic is analyzed by the IDS router to identify whether a packet's source is malicious.

The IDS detector simultaneously computes metrics like packet failure and transmission rates. Based on the information it receives from each node, the detection module running on 6BR analyzes whether each node is malicious. However, the authors have not validated the proposed framework, which is a significant flaw.

SOMIDS, proposed by Kfoury et al. [30], is a system that detects sinkhole, VNA, and HF attacks using SOM. The SOMIDS system is designed to cluster normal and attack traffic for detection using a PCAP file from a Cooja simulator. The aggregator module collects traffic data from the captured PCAP file, including ICMPv6 code, IPv6 destination, and timestamp, and then aggregates it into six variables.

The normalizer module normalizes the aggregated data, while the trainer module trains the SOM. The SOMIDS output is a matrix transformed into a 2D picture for improved cluster visibility. However, SOMIDS is imperfect because it ignores node mobility, and its implementation overhead has not been studied. However, SOMIDS is a novel approach to employing SOM to identify attack types, which may help defend RPL networks.

Summary and Analysis: As shown in Table 10, some proposed approaches rely on outdated signatures for classifiers. Training, making them less effective in securing RPL networks. On the other hand, the solutions in [30] utilized signatures obtained from simulated attacks and showed encouraging outcomes concerning key indicators. However, real-world physical network fingerprints should be more useful for developing classifiers [74]. Therefore, there is a need to develop a real traffic dataset for RPL-based networks that contain traces of common routing attacks, as suggested in [33], [73], and [75]. Lastly, the energy usage of the anomaly-based IDS is suggested in consideration [43], [67] and might be further reduced.

F. A QUALITATIVE COMPARISON BETWEEN THIS REVIEW AND OTHER EXISTING REVIEWS

This section focuses on comparing this review with other existing reviews, surveys, and systematic review studies on attack detection in RPL networks. Additionally, we emphasize the topics related to VNAs covered in these studies and their limitations and gaps, as shown in Table 11. The comparison aims to point out the uniqueness of this work.

Previous review on detecting network attacks using ML, DL, and combined ML-DL techniques was carefully reviewed and judged by those who conducted the study [23]. The review was based on thoroughly searching various information sources and screening many studies using pre-defined inclusion criteria. Ultimately, they identified 49 studies as relevant for inclusion in their review, which were then carefully analyzed and evaluated.

TABLE 10. Intrusion detection system based signature-and Anomaly.

Ref	Attacks	Specific Mechanism	Pros	Cons/Limitations	Summary of Result
[31]	HF, SH, and VNA	SOMIDS/ signature	- 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.	Energy consumption of 6BR is not studied; no important performance indicators are evaluated.	It clusters the attacks and normal traffic
[68]	HF and VNA	Framework signature-based IDS /Signature	-Signature-based detection can provide high accuracy in identifying known attacks. -The proposed IDS can detect intrusions from external networks and internal nodes.	-No validation is done to back up the framework. When dealing with unique or unidentified attacks, signature-based detection may not be as effective as it may be.	NA
[34]	VNA	Distributed Monitoring Architecture/ anomaly	Potentially locates the attacker	Monitoring nodes must run in promiscuous mode and take into account only one perpetrator case to discover anomalies. -Relies on sophisticated monitoring tools	NA
[77]	VNA	Distributed Monitoring Architecture /Anomaly	The proposed technique can accurately detect malicious nodes, which is crucial for identifying and mitigating network security problems.	Higher overhead - Ignores node mobility and depends on monitoring nodes' coverage of common nodes because it uses high-order devices for monitoring.	True positive rate (95%), Prediction rate (95%), and Control overhead (1500vs)

Meanwhile, Pasikhani et al. [76] reviewed IoT's 6LoWPAN security using RPL. They provided an overview of the IoT architecture and RPL protocol before discussing current threats to RPL and the necessary countermeasures. Additionally, the study elaborated on the evaluation metrics utilized in these measures. The authors concluded by identifying the limitations of previous review studies, discussing the problems encountered, and proposing possible future research directions.

In a separate study, Faraj et al. [77] focused on using ML techniques to identify attacks on IoT devices. Specifically, the authors designed an IDS that utilized ML and discussed the essential components of such systems, how they can be grouped, and how they can be used in IoT networks. They also examined various IDS methods to detect attacks on IoT devices and pointed out their shortcomings. Finally, the authors highlighted unresolved issues and research challenges in IoT security and suggested directions for future studies to overcome them.

In [78], researchers conducted an SLR of IDSs in RPL-based 6LoWPAN. The review analyzed 103 published works in this field, providing comprehensive explanations of the detrimental impacts of network attacks and the architecture of RPL. The authors evaluated the studies gathered and suggested potential modifications. They also provided a detailed classification and analysis of IDS-based RPL techniques, including methodologies for validating methods, monitoring data sources, detection strategies, and countermeasures.

The authors thoroughly collected and analyzed the evaluated studies, considering assessment metrics, network simulators, the harmful consequences of RPL attacks, and study outcomes. They also discussed frequently used IoT network datasets and briefly reviewed RPL datasets. Lastly, the author identified research gaps and suggested several future research directions to address the gaps. This review provides a comprehensive and in-depth analysis of IDSs in RPL-based 6LoWPAN and is a valuable resource for future research.

It is worth mentioning that the research studies in Table 11 do not comprehensively analyze VNAs. While some studies evaluate the impact of VNAs on IoT networks, they do so within the context of their respective research

TABLE 11. Various Categories of Security Attacks in IoT.

Ref	RPL Architecture	Recourses				Topology			Traffic			
		Direct attacks		Indicter attacks		Sub Optimization		Isolation	Passive attacks		Misappropriation	
		DIS-Flooding	Routing tables overload	Rank	DAG	VNA	SH	WH	BH	Traffic Analysis	Sniffing	Identity Attacks
[68]		✓	×	×	×	×	×	×	×	×	×	×
[65]	✓	×	×	×	×	✓	×	×	×	×	×	×
[83]	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	×	×
[23]	×	×	×	×	×	×	✓	×	×	×	×	×
[50]	✓	×	×	×	×	✓	×	✓	×	×	×	×
[84]	✓	×	×	×	×	✓	×	×	×	×	×	×
[85]	×	✓	×	✓	✓	✓	✓	✓	✓	×	×	×
[86]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	×
[87]	✓	×	×	✓	✓	✓	✓	✓	✓	×	×	×
[88]	✓	×	×	✓	✓	✓	✓	✓	✓	×	×	×
[89]	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	×
[90]	✓	✓	×	×	×	✓	×	×	×	×	×	×
[91]	✓	×	×	×	×	✓	×	×	×	×	×	×
[92]	✓	×	×	×	×	✓	×	×	×	×	×	×
[88]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
[87]	✓	✓	×	×	×	×	✓	✓	✓	×	×	×
[44]	✓	×	×	×	×	×	×	×	×	×	×	✓
[85]	✓	✓	×	×	×	✓	✓	✓	✓	×	×	×
[93]	✓	×	×	✓	✓	✓	×	✓	✓	×	×	×
[75]	✓	×	×	×	×	×	✓	×	×	×	×	×
[44]	✓	×	×	×	×	×	×	×	×	×	×	×
[44]	✓	×	×	×	×	×	×	×	×	×	×	×
[94]	✓	×	×	×	×	×	✓	×	×	×	×	×
This work	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

areas. This review, on the other hand, focuses exclusively on VNAs.

It contrasts the implementation, datasets, performance evaluation measures, and proposed detection algorithms. Furthermore, this review covers VNAs from 2011 to 2023 in the most thorough and current manner. Although fewer papers are in this review than other surveys, it is useful because it concentrates on efforts that directly address VNAs.

Additionally, Table 11 reveals that VNA and HF attacks are the most prevalent, followed by WH, SH, and BH attacks. Researchers have also explored DAG, decreased rank, and identity attacks. Nevertheless, the limited attention given to the remaining attacks implies that they may either be straightforward to detect or challenging to implement within RPL networks.

In conclusion, our goal was to distinguish our review from others and gain a deeper understanding of the crucial issues related to routing protocol-based attacks while identifying the most prevalent attacks on routing protocols. This comparison can be a useful reference for future researchers in this field. By examining the attacks analyzed in previous studies, researchers can recognize and concentrate on novel types of attacks.

IV. DISCUSSIONS WITH REGARDS TO RESEARCH QUESTIONS

This section discusses the findings of the publication review. It involves addressing research questions, identifying gaps and potential future research avenues, and discussing the review's findings. The review revealed that the VNA targets vulnerabilities in the RPL protocol and manipulates node rank values to significantly disrupt the network's operation, potentially leading to further damaging attacks. Consequently, many researchers proposed techniques to address the problem of VNA attacks by detecting and mitigating them early. The review revealed significant distinctions between the evaluation metrics, datasets, and simulators.

Most studies focused on various network routing attacks without investigating specific countermeasures for each.

To circumvent this ambiguity, this review focuses on the security techniques designed to detect and counteract VNAs.

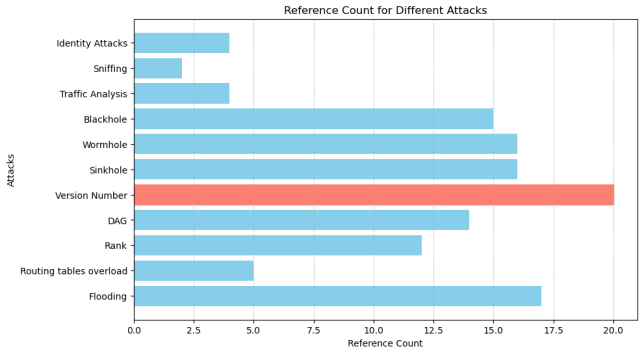

FIGURE 6. Distribution of the attacks in the existing research.

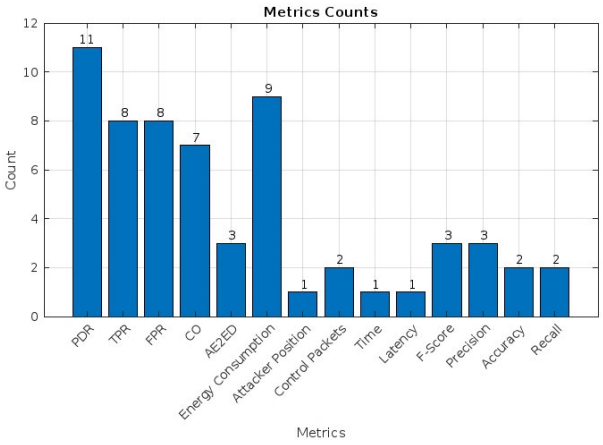

FIGURE 7. Distribution of metrics in previous studies.

A. IDENTIFYING THE RESEARCH GAPS

The review identified many potential future research areas on this topic, summarized as follows:

1) Most of the research covered in this review looked at how well-proposed methods worked with a single network topology. Only a few studies examined how their performance changed with different network topologies. The evaluation of suggested approaches in network topology comprising a single case of RPL as opposed to numerous cases has thus been identified as a research gap (Section II-D).
2) A requirement for solutions that are lightweight, secure, scalable, and serve critical IoT applications running on networks with limited resources (section III-B)
3) Several solutions have been proposed to detect and mitigate VNAs, including signature-based and anomaly-based approaches; trust-based solutions have also been proposed.
   Still, they are not widely used in resource-limited networks (section III-E).
4) The distribution of attacks in the research under consideration is shown in Section III-D above. Figure 6 shows that the most researched attacks are VNA and HF, followed by WH, SH, and BH attacks. DAG, DR, and identity attacks are also investigated in some detail. However, the remaining attacks received little attention from researchers. Therefore, it can be inferred that because these attacks are either easy to detect or challenging to implement in RPL networks, they have gotten less attention.
   In summary: examining the attacks implemented in previous studies would assist future researchers in detecting such attacks and concentrating on new types.
5) To progress the development of anomaly-based IDS for the IoT, significant hurdles must be overcome, highlighting the need for additional research to resolve these issues and enhance the overall effectiveness of IDS in the IoT.
6) The RPL protocol is intended for use in LLN networks, an essential aspect of IoT systems. Nevertheless, not all IoT systems operate similarly. As reported in one of the reviewed papers, a detection method was developed specifically for a healthcare IoT system [41], [76], [79]. Whether a suggested detection method can be applied in IoT systems or is designed for a specific IoT application must be determined.
7) All but one of the ML-based detection techniques under study did not include hyperparameter adjustment. To adjust the hyperparameters and choose features, the researchers, however, employed a genetic optimization technique [72]. Optimization approaches for hyperparameter tweaking ML-based detection algorithms are highlighted as a research gap that should be investigated.
8) The literature analysis finds that previous research has focused primarily on detecting attacks and isolating malicious nodes. Furthermore, there is a lack of initial acknowledgment of efforts to prevent the attack. This raises the question of identifying a research gap in the proposed security approach. Specifically, there is a need for mechanisms capable of detecting, isolating, and thwarting VNAs within RPL networks.
9) **Finally,** the reviewed works utilized a variety of performance metrics to evaluate their proposed methods. Figure 7 presents statistics on the frequency of these metrics and the references that employ them. However, these statistics reveal that specific critical metrics for IoT systems, such as accuracy, F1-score, recall, time, average delay, and precision, were not given sufficient attention. Therefore, future research on IoT systems should address these metrics.

B. ANSWERS TO RESEARCH QUESTIONS

Section I of this review presented several research inquiries to direct this investigation. This segment will respond to these inquiries by utilizing the insights obtained from the literature review.

1) **What proposed techniques currently exist for detecting VNAs in RPL?**
   Several approaches have been suggested to detect VNAs, which can be categorized based on their

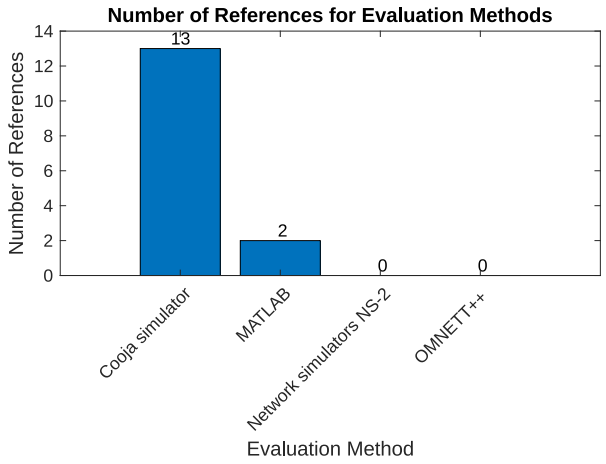

FIGURE 8. Instruments for Evaluating Proposed Detection Methods.

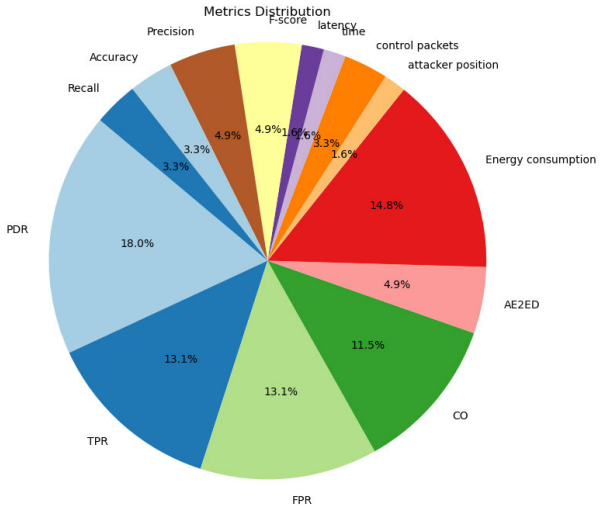

FIGURE 9. Commonly Metrics Based used in Existing Researches.

detection approach, as discussed in SectionIII. They include secure-based construction systems, signature and anomaly detection, distributed-based, lightweight-based systems, and systems that utilize AI data models. The literature review section thoroughly investigated each of these techniques.

2) **How are the datasets used in the suggested detection algorithms being created by researchers?**
This work's literature survey failed to find a dataset explicitly designed to address the RPL issue VNA, as discussed in Section II-E. While some researchers use datasets focusing on various attacks, such as synthetic, most prefer creating artificial datasets using web simulators like COOJA.
3) **What is the methodology used to assess the proposed methods?** On actual IoT platforms, evaluating attack detection techniques might be quite difficult. As a result, many researchers use network simulators like Cooja or matlab to simulate the operation of IDS. The instruments frequently used in literature for assessing suggested detection methods are listed in Table 2.See section II-D,
As shown in Figure 8 and Table 2, the Cooja simulator is the most widely used method in the scientific literature
4) **Which metrics are used to measure the performance of the proposed methods during an evaluation?** The researchers evaluated the efficacy of their proposed techniques using a variety of metrics. Figure 9 illustrates these metrics: TPR, FNR, FPR, detection rate, detection Acc, packet loss ratio, energy consumption, overhead, and average latency. Indicators for detecting malicious attacks, PDR, energy consumption, TPR, and FPR were the most frequently employed metrics. The reviewed studies did not utilise critical metrics such as overhead, throughput, and average latency as frequently.
5) **Which research areas have shortcomings that can be addressed and improved upon?**
Section IV-A and IV-B provides a detailed discussion of various research gaps that have been identified.

V. ISSUES AND RESEARCH CHALLENGES

This review has highlighted several critical areas in the research on VNAs in LLN and RPL networks that have not received sufficient attention. These areas can be summarized as follows:

1) Evaluating the impact of the VNA on RPL networks based on multiple variables, such as the location of the criminal within the network, the number of hops between the attacker and the root node, and the presence of multiple or a single malicious node.
2) Examining the interaction between VNAs and other routing attacks.
3) Comparing the applicability, adaptability, and network integration complexity of proposed detection approaches. Exploring the fundamental characteristics of a network's traffic flow that can be used to apply ML and DL models to detect an attack and identify the malicious node.

VI. CONCLUSION AND FUTURE DIRECTIONS

In conclusion, while numerous proposals for using machine learning techniques to detect and prevent VNAs have been put forward by researchers, less attention has been given to optimizing the model's hyperparameters. The majority of studies have evaluated the effectiveness of suggested solutions using detection metrics without taking into account important IoT system characteristics like complexity, overhead, delay, and ACC. Furthermore, researchers have made some suggestions for identifying and separating malicious nodes, but little attention has been given to preventing attacks from occurring in the first place.

Our research aims to address these gaps by achieving satisfactory performance and supporting security modes and protection techniques specific to contexts. We have discovered that VNAs are the most pernicious, yet many studies on routing attack detection have ignored task distributions and parallel processing during the learning phase. Effective security performance requires real-time prediction and detection of attacks; however, most studies have not addressed the issue of multiple attacks. Therefore, our study seeks to fill these gaps by optimizing hyperparameters, identifying and preventing attacks from occurring, considering critical IoT metrics, and addressing multiple attacks.

There are several potential avenues for future work in this area. Firstly, there is a need to analyze multiple VNA situations that have not yet been addressed in the literature. Exploring a hybrid mitigation scenario that uses the elimination technique for nodes with limited resources and the shield technique for other nodes could be interesting. Another factor to consider is mobility, which could incorporate evaluating the impact of dynamic node ranking and topology changes on attack mitigation. These potential research directions could improve our understanding of VNAs in LLN and RPL networks.

Finally, there is still ample opportunity to contribute significantly to this field of study, and additional research should be encouraged.

REFERENCES

[1] A. Jamalipour and S. Murali, "A taxonomy of machine-learning-based intrusion detection systems for the Internet of Things: A survey," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9444–9466, Jun. 2022.

[2] A. Agiollo, M. Conti, P. Kaliyar, T.-N. Lin, and L. Pajola, "DETONAR: Detection of routing attacks in RPL-based IoT," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 2, pp. 1178–1190, Jun. 2021.

[3] J. Kipongo, T. G. Swart, and E. Esenogho, "Design and implementation of intrusion detection systems using RPL and AOVD protocols-based wireless sensor networks," *Int. J. Electron. Telecommun.*, vol. 69, no. 2, pp. 309–318, 2023.

[4] T. A. Al-Amiedy, M. Anbar, B. Belaton, A. H. H. Kabla, I. H. Hasbullah, and Z. R. Alashhab, "A systematic literature review on machine and deep learning approaches for detecting attacks in RPL-based 6LoWPAN of Internet of Things," *Sensors*, vol. 22, no. 9, p. 3400, Apr. 2022.

[5] J. Rani, A. Dhingra, and V. Sindhu, "A detailed review of the IoT with detection of sinkhole attacks in RPL based network," in *Proc. Int. Conf. Commun. Comput. Internet Things*, Mar. 2022, pp. 1–6.

[6] H. Ning, *Unit and Ubiquitous Internet of Things*. Boca Raton, FL, USA: CRC press, 2013.

[7] A. Malik and R. Kushwah, "A survey on next generation IoT networks from green IoT perspective," *Int. J. Wireless Inf. Netw.*, vol. 29, no. 1, pp. 36–57, Mar. 2022.

[8] Z. H. Ali and H. A. Ali, "Towards sustainable smart IoT applications architectural elements and design: Opportunities, challenges, and open directions," *J. Supercomput.*, vol. 77, no. 6, pp. 5668–5725, Jun. 2021.

[9] A. S. Martey and E. Esenogho, "Improved cluster to normal ratio protocol for increasing the lifetime of wireless sensor networks," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 26, no. 2, p. 1135, May 2022.

[10] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, "Complementing IoT services through software defined networking and edge computing: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1761–1804, 3rd Quart., 2020.

[11] B. Omoniwa, R. Hussain, M. A. Javed, S. H. Bouk, and S. A. Malik, "Fog/Edge computing-based IoT (FECIoT): Architecture, applications, and research issues," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4118–4149, Jun. 2019.

[12] S. B. KaebehYaeghoobi, M. K. Soni, and S. S. Tyagi, "Performance analysis of energy efficient clustering protocols to maximize wireless sensor networks lifetime," in *Proc. Int. Conf. Soft Comput. Techn. Implementations (ICSCTI)*, Oct. 2015, pp. 170–176.

[13] N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, "Energy-efficient routing protocols in wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 551–591, 2nd Quart., 2013.

[14] U. Tariq, I. Ahmed, M. A. Khan, and A. K. Bashir, "Fortifying IoT against crimpling cyber-attacks: A systematic review," *Karbala Int. J. Modern Sci.*, vol. 9, no. 4, p. 9, Oct. 2023.

[15] S. Nastic, T. Rausch, O. Scekic, S. Dustdar, M. Gusev, B. Koteska, M. Kostoska, B. Jakimovski, S. Ristov, and R. Prodan, "A serverless real-time data analytics platform for edge computing," *IEEE Internet Comput.*, vol. 21, no. 4, pp. 64–71, Jul. 2017.

[16] P. Narendra, S. Duquennoy, and T. Voigt, "BLE and IEEE 802.15.4 in the IoT: Evaluation and interoperability considerations," in *Internet of Things. IoT Infrastructures*. Cham, Switzerland: Springer, 2016, pp. 427–438. [Online]. Available: https://citation-needed.springer.com/v2/references/10.1007/978-3-319-47075-7_47?format=bibtex&flavour= citation

[17] H. A. A. Al-Kashoash, H. Kharrufa, Y. Al-Nidawi, and A. H. Kemp, "Congestion control in wireless sensor and 6LoWPAN networks: Toward the Internet of Things," *Wireless Netw.*, vol. 25, no. 8, pp. 4493–4522, Nov. 2019.

[18] A. Haka, D. Dinev, V. Aleksieva, and H. Valchanov, "Comparative analysis of ZigBee, 6LoWPAN and BLE technologies for the Internet of Things," in *Proc. 9TH Int. Conf. INDONESIAN Chem. Soc. ICICS : Toward Meaningful Soc.*, vol. 2570, no. 1, 2022, Paper 020007.

[19] L. F. Schrickte, C. Montez, R. D. Oliveira, and A. R. Pinto, "Integration of wireless sensor networks to the Internet of Things using a 6LoWPAN gateway," in *Proc. 3rd Brazilian Symp. Comput. Syst. Eng.*, Dec. 2013, pp. 119–124.

[20] M. Bouaziz and A. Rachedi, "A survey on mobility management protocols in wireless sensor networks based on 6LoWPAN technology," in *Computer Communications*, vol. 74. Amsterdam, Netherlands, Europe: Elsevier, 2016, pp. 3–15.

[21] M. Garuba, C. Liu, and D. Fraites, "Intrusion techniques: Comparative study of network intrusion detection systems," in *Proc. 5th Int. Conf. Inf. Technol. New Generat.*, Apr. 2008, pp. 592–598.

[22] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, and R. Atkinson, "Shallow and deep networks intrusion detection system: A taxonomy and survey," 2017, *arXiv:1701.02145*.

[23] P. S. Nandhini, P. Srinath, P. Veeramanikandan, and S. Malliga, "Version attack detection using claim algorithm in RPL based IoT networks: Effects and performance parameters evaluation," in *Proc. 2nd Int. Conf. Smart Electron. Commun. (ICOSEC)*, Oct. 2021, pp. 209–215.

[24] R. Sahay, G. Geethakumari, B. Mitra, and I. Sahoo, "Efficient framework for detection of version number attack in Internet of Things," in *Proc. Intell. Syst. Des. Appl. 18th Int. Conf. Intell. Syst. Des. Appl.*, vol. 2, Cham, Switzerland: Springer, Dec. 2018, pp. 480–492.

[25] S. S. Ambarkar and N. Shekokar, "Critical and comparative analysis of DoS and version number attack in healthcare IoT system," in *Proc. 1st Doctoral Symp. Natural Comput. Res.*, Springer, 2021, pp. 301–312.

[26] A. D. Seth, S. Biswas, and A. K. Dhar, "LDES: Detector design for version number attack detection using linear temporal logic based on discrete event system," *Int. J. Inf. Secur.*, vol. 22, no. 4, pp. 961–985, Aug. 2023.

[27] A. A. Anitha and L. Arockiam, "VeNADet: Version number attack detection for RPL based Internet of Things," *Solid State Technol.*, vol. 64, no. 2, pp. 2225–2237, 2021.

[28] K. N. Qureshi, S. S. Rana, A. Ahmed, and G. Jeon, "A novel and secure attacks detection framework for smart cities industrial Internet of Things," in *Sustainable Cities and Society*, vol. 61. Amsterdam, The Netherlands: Elsevier, 2020, p. 102343.

[29] F. Y. Yavuz, D. Ünal, and E. Gül, "Deep learning for detection of routing attacks in the Internet of Things," *Int. J. Comput. Intell. Syst.*, vol. 12, no. 1, p. 39, 2018.

[30] E. Kfoury, J. Saab, P. Younes, and R. Achkar, "A self organizing map intrusion detection system for RPL protocol attacks," *Int. J. Interdiscipl. Telecommun. Netw.*, vol. 11, no. 1, pp. 30–43, Jan. 2019.

[31] E. Aydogan, S. Yilmaz, S. Sen, I. Butun, S. Forsström, and M. Gidlund, "A central intrusion detection system for RPL-based industrial Internet of Things," in *Proc. 15th IEEE Int. Workshop Factory Commun. Syst. (WFCS)*, May 2019, pp. 1–5.

[32] A. A. Anitha and L. Arockiam, "ANNIDS: Artificial neural network-based intrusion detection system for the Internet of Things," *Int. J. Innov. Technol. Explor. Eng. Regul*, vol. 8, no. 11, pp. 2583–2588, 2019.

[33] N. M. Müller, P. Debus, D. Kowatsch, and K. Böttinger, "Distributed anomaly detection of single mote attacks in RPL networks," in *Proc. 16th Int. Joint Conf. e-Bus. Telecommun.*, vol. 2, 2019, pp. 378–385.

[34] E. Canbalaban and S. Sen, "A cross-layer intrusion detection system for RPL-based Internet of Things," in *Proc. Ad-Hoc, Mobile, Wireless Netw. 19th Int. Conf. Ad-Hoc Netw. Wireless*. Springer, 2020, pp. 214–227.

[35] V. Kumar, V. Kumar, D. Sinha, and A. K. Das, "Simulation analysis of DDoS attack in IoT environment," in *Proc. 4th Int. Conf. Internet Things Connected Technol. (ICIoTCT)*. Springer, 2019, pp. 77–87.

[36] M. Osman, J. He, F. M. M. Mokbal, N. Zhu, and S. Qureshi, "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*, vol. 9, pp. 83654–83665, 2021.

[37] S. O. M. Kamel and S. A. Elhamayed, "Mitigating the impact of IoT routing attacks on power consumption in IoT healthcare environment using convolutional neural network," *Int. J. Comput. Netw. Inf. Secur.*, vol. 12, no. 4, pp. 11–29, Aug. 2020.

[38] J. Foley, N. Moradpoor, and H. Ochenyi, "Employing a machine learning approach to detect combined Internet of Things attacks against two objective functions using a novel dataset," *Secur. Commun. Netw.*, vol. 2020, pp. 1–17, Feb. 2020.

[39] F. Medjek, D. Tandjaoui, N. Djedjig, and I. Romdhani, "Fault-tolerant AI-driven intrusion detection system for the Internet of Things," *Int. J. Crit. Infrastruct. Protection*, vol. 34, Sep. 2021, Art. no. 100436.

[40] A. Verma and V. Ranga, "ELNIDS: Ensemble learning based network intrusion detection system for RPL based Internet of Things," in *Proc. 4th Int. Conf. Internet Things, Smart Innov. Usages (IoT-SIU)*, Apr. 2019, pp. 1–6.

[41] A. Verma and V. Ranga, "Evaluation of network intrusion detection systems for RPL based 6LoWPAN networks in IoT," *Wireless Pers. Commun.*, vol. 108, no. 3, pp. 1571–1594, Oct. 2019.

[42] M. Karami, H. Lombaert, and D. Rivest-Hénault, "Real-time simulation of viscoelastic tissue behavior with physics-guided deep learning," in *Computerized Medical Imaging and Graphics*, vol. 104. Amsterdam, The Netherlands: Elsevier, 2023, p. 102165.

[43] A. Mayzaud, R. Badonnel, and I. Chrisment, "A distributed monitoring strategy for detecting version number attacks in RPL-based networks," *IEEE Trans. Netw. Service Manage.*, vol. 14, no. 2, pp. 472–486, Jun. 2017.

[44] M. Albishari, M. Li, R. Zhang, and E. Almosharea, "Deep learning-based early stage detection (DL-ESD) for routing attacks in Internet of Things networks," *J. Supercomput.*, vol. 79, no. 3, pp. 2626–2653, Feb. 2023.

[45] G. Sharma, J. Grover, and A. Verma, "Performance evaluation of mobile RPL-based IoT networks under version number attack," in *Computer Communications*, vol. 197. Amsterdam, The Netherlands: Elsevier, 2023, pp. 12–22.

[46] A. M. Said, A. Yahyaoui, and T. Abdellatif, "Efficient anomaly detection for smart hospital IoT systems," *Sensors*, vol. 21, no. 4, p. 1026, Feb. 2021.

[47] F. Ahmed and Y.-B. Ko, "A distributed and cooperative verification mechanism to defend against DODAG version number attack in RPL," in *Proc. 6th Int. Joint Conf. Pervasive Embedded Comput. Commun. Syst.*, 2016, pp. 55–62.

[48] A. Aris, S. F. Oktug, and S. Berna Ors Yalcin, "RPL version number attacks: In-depth study," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp.*, Apr. 2016, pp. 776–779.

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

[50] M. D. Momand and M. K. Mohsin, "Machine learning-based multiple attack detection in RPL over IoT," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2021, pp. 1–8.

[51] A. Arış, S. B. Yalçın, and S. F. Oktuğ, "New lightweight mitigation techniques for RPL version number attacks," in *Ad Hoc Networks*, vol. 85. Amsterdam, The Netherlands: Elsevier, 2019, pp. 81–91.

[52] G. Sharma, J. Grover, and A. Verma, "QSec-RPL: Detection of version number attacks in RPL based mobile IoT using Q-learning," in *Ad Hoc Networks*, vol. 142. Amsterdam, The Netherlands: Elsevier, 2023, p. 103118.

[53] L. A. Rosewelt, B. Sreedevi, and C. G. Shivani, "An effective detection of version number attacks in the IoT using neural networks," in *Proc. 2nd Int. Conf. Adv. Electr. Comput. Commun. Sustain. Technol. (ICAECT)*, Apr. 2022, pp. 1–7, doi: 10.1109/ICAECT54875.2022.9807966.

[54] H. Tyagi and R. Kumar, "Attack and anomaly detection in IoT networks using supervised machine learning approaches," *Revue d'Intell. Artificielle*, vol. 35, no. 1, pp. 11–21, Feb. 2021.

[55] M. Belkheir, M. Rouissat, M. Achraf Boukhobza, A. Mokaddem, and M. Bouziani, "A new lightweight solution against the version number attack in RPL-based IoT networks," in *Proc. 7th Int. Conf. Image Signal Process. Appl. (ISPA)*, May 2022, pp. 1–6.

[56] A. Dvir, T. Holczer, and L. Buttyan, "VeRA–Version number and rank authentication in RPL," in *Proc. IEEE 8th Int. Conf. Mobile Ad-Hoc Sensor Syst.*, Oct. 2011, pp. 709–714.

[57] H. Perrey, M. Landsmann, O. Ugus, T. C. Schmidt, and M. Wählisch, "TRAIL: Topology authentication in RPL," 2013, *arXiv:1312.0984*.

[58] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "Using the RPL protocol for supporting passive monitoring in the Internet of Things," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp.*, Apr. 2016, pp. 366–374.

[59] S. Sanjay Ambarkar and N. Shekokar, "A secure model to protect healthcare IoT system from version number and rank attack," *J. Univ. Shanghai Sci. Technol.*, vol. 23, no. 7, pp. 502–515, Jul. 2021.

[60] M. Nikravan, A. Movaghar, and M. Hosseinzadeh, "A lightweight defense approach to mitigate version number and rank attacks in low-power and lossy networks," *Wireless Pers. Commun.*, vol. 99, no. 2, pp. 1035–1059, Mar. 2018.

[61] I. S. Alsukayti and A. Singh, "A lightweight scheme for mitigating RPL version number attacks in IoT networks," *IEEE Access*, vol. 10, pp. 111115–111133, 2022.

[62] M. Rouissat, M. Belkheir, and A. Mokaddem, "Parent supervision lightweight solution against version number attacks for IoT networks," *Res. Article*, 2023. [Online]. Available: https://doi.org/10.21203/rs.3.rs-2605250/v1

[63] Z. A. Almusaylim, N. Jhanjhi, and A. Alhumam, "Detection and mitigation of RPL rank and version number attacks in the Internet of Things: SRPL-RP," *Sensors*, vol. 20, no. 21, p. 5997, Oct. 2020.

[64] X. Liu, B. Xu, K. Zheng, and H. Zheng, "Throughput maximization of wireless-powered communication network with mobile access points," *IEEE Trans. Wireless Commun.*, vol. 22, no. 7, pp. 4401–4402, Dec. 2022.

[65] S. Nayak, N. Ahmed, and S. Misra, "Deep learning-based reliable routing attack detection mechanism for industrial Internet of Things," in *Ad Hoc Networks*, vol. 123. Amsterdam, The Netherlands: Elsevier, 2021, p. 102661.

[66] A. Dhingra and V. Sindhu, "A review of DIS-flooding attacks in RPL based IoT network," in *Proc. Int. Conf. Commun. Comput. Internet Things*, Mar. 2022, pp. 1–6.

[67] A. Mayzaud, R. Badonnel, and I. Chrisment, "Detecting version number attacks in RPL-based networks using a distributed monitoring architecture," in *Proc. 12th Int. Conf. Netw. Service Manage. (CNSM)*, Oct. 2016, pp. 127–135.

[68] E. Esenogho, K. Djouani, and A. M. Kurien, "Integrating artificial intelligence Internet of Things and 5G for next-generation smartgrid: A survey of trends challenges and prospect," *IEEE Access*, vol. 10, pp. 4794–4831, 2022.

[69] S. Sharma and V. K. Verma, "AIEMLA: Artificial intelligence enabled machine learning approach for routing attacks on Internet of Things," *J. Supercomput.*, vol. 77, no. 12, pp. 13757–13787, Dec. 2021.

[70] F. Hu, D. Xie, and S. Shen, "On the application of the Internet of Things in the field of medical and health care," in *Proc. IEEE Int. Conf. Green Comput. Commun. IEEE Internet Things IEEE Cyber, Phys. Social Comput.*, Aug. 2013, pp. 2053–2058.

[71] J. A. Kaw, N. A. Loan, S. A. Parah, K. Muhammad, J. A. Sheikh, and G. M. Bhat, "A reversible and secure patient information hiding system for IoT driven e-health," *Int. J. Inf. Manage.*, vol. 45, pp. 262–275, Apr. 2019.

[72] S. Sharma and V. K. Verma, "Security explorations for routing attacks in low-power networks on the Internet of Things," in *The Journal Supercomputing*, vol. 77. Cham, Switzerland: Springer, Oct. 2021, pp. 4778–4812.

[73] V. K. Verma and S. Sharma, "Investigations on information solicitation and version number attacks in Internet of Things," *IEEE Sensors J.*, vol. 23, no. 3, pp. 3204–3211, Feb. 2023.

[74] M. A. Jabbar and R. Aluvalu, "Intrusion detection system for the Internet of Things: A review," in *Proc. Smart Cities Symp.*, 2018, p. 6.

[75] T. A. Alamiedy, M. Anbar, Z. N. M. Alqattan, and Q. M. Alzubi, "Anomaly-based intrusion detection system using multi-objective grey wolf optimization algorithm," in *Journal Ambient Intelligence Humanized Computing*, vol. 11. Cham, Switzerland: Springer, Nov. 2020, pp. 3735–3756.

[76] A. M. Pasikhani, J. A. Clark, P. Gope, and A. Alshahrani, "Intrusion detection systems in RPL-based 6LoWPAN: A systematic literature review," *IEEE Sensors J.*, vol. 21, no. 11, pp. 12940–12968, Jun. 2021.
[77] O. Faraj, D. Megías, A.-M. Ahmad, and J. Garcia-Alfaro, "Taxonomy and challenges in machine learning-based approaches to detect attacks in the Internet of Things," in *Proc. 15th Int. Conf. Availability, Rel. Secur.*, Aug. 2020, pp. 1–10.
[78] A. Verma and V. Ranga, "Security of RPL based 6LoWPAN networks in the Internet of Things: A review," *IEEE Sensors J.*, vol. 20, no. 11, pp. 5666–5690, Jun. 2020.
[79] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," in *Proc. Int. Conf. Pervasive Comput. (ICPC)*, Jan. 2015, pp. 1–6.
[80] S. N. V. Simha, R. Mathew, S. Sahoo, and R. C. Biradar, "A review of RPL protocol using contiki operating system," in *Proc. 4th Int. Conf. Trends Electron. Informat.*, Jun. 2020, pp. 259–264.
[81] A. S. Patil et al., "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, 2022, pp. 70–91.
[82] W. Yang, Y. Wang, Z. Lai, Y. Wan, and Z. Cheng, "Security vulnerabilities and countermeasures in the RPL-based Internet of Things," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery (CyberC)*, Oct. 2018, pp. 49–495.
[83] A. Kamble, V. S. Malemath, and D. Patil, "Security attacks and secure routing protocols in RPL-based Internet of Things: Survey," in *Proc. Int. Conf. Emerg. Trends Innov. ICT (ICEI)*, Feb. 2017, pp. 33–39.
[84] H. Kharrufa, H. A. A. Al-Kashoash, and A. H. Kemp, "RPL-based routing protocols in IoT applications: A review," *IEEE Sensors J.*, vol. 19, no. 15, pp. 5952–5967, Aug. 2019.
[85] P. S. Nandhini, S. Kuppuswami, and S. Malliga, "Energy efficient thwarting rank attack from RPL based IoT networks: A review," in *Materials Today: Proceedings*. Amsterdam, The Netherlands: Elsevier, 2021.
[86] K. A. Darabkh, M. Al-Akhras, J. N. Zomot, and M. Atiquzzaman, "RPL routing protocol over IoT: A comprehensive survey, recent advances, insights, bibliometric analysis, recommendations, and future directions," *J. Netw. Comput. Appl.*, vol. 207, Nov. 2022, Art. no. 103476.
[87] A. Radovici, C. Rusu, and R. Serban, "A survey of IoT security threats and solutions," in *Proc. 17th RoEduNet Conf. Netw. Educ. Res. (RoEduNet)*, Sep. 2018, pp. 1–5.
[88] R. Mehta and M. M. Parmar, "A survey on security attacks and countermeasures in RPL for Internet of Things," *Int. J. Adv. Res. Sci. Eng.*, vol. 7, no. 3, pp. 55–69, 2018.
[89] Z. Wang, W. Xie, B. Wang, J. Tao, and E. Wang, "A survey on recent advanced research of CPS security," *Appl. Sci.*, vol. 11, no. 9, p. 3751, Apr. 2021.
[90] M. Rouissat, M. Belkheir, and H. S. A. Belkhira, "A potential flooding version number attack against RPL based IoT networks," *J. Electr. Eng.*, vol. 73, no. 4, pp. 267–275, Aug. 2022.
[91] A. A. R. A. Omar and B. Soudan, "A comprehensive survey on detection of sinkhole attack in routing over low power and lossy network for Internet of Things," in *Internet of Things*. Amsterdam, The Netherlands: Elsevier, 2023, pp. 10075–0.

NADIA A. ALFRIEHAT received the B.S. degree in computer science from Jerash University and the M.Sc. degree in computer science from Amman Arabiya University, in 2018. She is currently pursuing the Ph.D. degree with the National Advanced IPv6 Centre (NAv6), University Sains Malaysia (USM). Her research interests include computer networks, network security, intrusion detection systems (IDS), artificial intelligence (AI), and the Internet of Things (IoT).

MOHAMMED ANBAR (Member, IEEE) received the Ph.D. degree in an advanced computer network from University Sains Malaysia (USM). He is currently a Senior Lecturer with the National Advanced IPv6 Centre (NAv6), USM. His current research interests include malware detection, web security, intrusion detection systems (IDS), intrusion prevention systems (IPS), network monitoring, the Internet of Things (IoT), and IPv6 security.

SHANKAR KARUPPAYAH (Member, IEEE) received the B.Sc. degree (Hons.) in computer science from University Sains Malaysia (USM), in 2009, the M.Sc. degree in software systems engineering from the King Mongkut's University of Technology North Bangkok (KMUTNB), in 2011, and the Ph.D. degree from TU Darmstadt with his dissertation titled Advanced Monitoring in P2P Botnets, in 2016. He has been a Senior Researcher/a Postdoctoral Researcher with the Tele Cooperation Group, TU Darmstadt, since July 2019. He has also been a Senior Lecturer with the National Advanced IPv6 Centre (NAv6), USM, since 2016. He is working actively on several cybersecurity projects and working groups, e.g., the National Research Center for Applied Cybersecurity (ATHENE), formerly the Center for Research in Security and Privacy (CRISP).

SHAZA DAWOOD AHMED RIHAN received the B.S. degree in computer engineering from the University of Gezira, Sudan, in 2002, the M.Sc. degree in information system from the Arab Academy for Science and Technology, Egypt, in 2007, and the Ph.D. degree in information systems from Omdurman Islamic, Sudan, in 2016. She is currently an Assistant Professor with Najran University. Her current research interests include computer networks, cybersecurity, and distributed databases.

BASIM AHMAD ALABSI received the B.Sc. degree in computer science from Al-Azhar University, Palestine, in 2000, the M.Sc. degree in computer science from Aman Arab University, Jordan, in 2005, and the Ph.D. degree in internet infrastructure security from Universiti Sains Malaysia (USM), in 2020. He is currently an Assistant Professor with Najran University. His current research interests include the Internet of Things (IoT), routing protocol for low-power and lossy networks (RPL) security, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), and IPv6 security.

ALAA M. MOMANI received the Ph.D. degree in software engineering. He is currently the Associate Dean of the School of Computing, Skyline University College, Sharjah, United Arab Emirates. He has experience teaching at several universities in Jordan, Saudi Arabia, Malaysia, and United Arab Emirates, where he has been in the academic field, since 2005. He has valuable research articles published in international journals and participated in conferences as the author or reviewer. His research interests include the area of software engineering, technology acceptance and usage behaviors, artificial intelligence, machine learning, e-commerce, e-tourism, e-learning, social applications, expert systems, and decision support systems.