IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 28 July 2023, accepted 23 August 2023, date of publication 30 August 2023, date of current version 7 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3310242

RESEARCH ARTICLE

Passive Rule-Based Approach to Detect Sinkhole Attack in RPL-Based Internet of Things Networks

SHADI AL-SARAWI[1], MOHAMMED ANBAR[1], (Member, IEEE), BASIM AHMAD ALABSI[2], MOHAMMAD ADNAN ALADAILEH[3], AND SHAZA DAWOOD AHMED RIHAN[2]

[1]National Advanced IPv6 Centre (NAv6), University Sains Malaysia, Gelugor, Penang 11800, Malaysia
[2]Applied College, Najran University, Najran 1988, Saudi Arabia
[3]Cybersecurity Department, School of Information Technology, American University of Madaba (AUM), Amman 11821, Jordan

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

This work was supported by the Deanship of Scientific Research, Najran University, under the Research Groups Funding Program under Grant NU/RG/SERC/12/50.

ABSTRACT An Internet of Things (IoT) refers to a network of smart devices that enable data collection and exchange. RPL is a protocol specifically designed for IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) to bring the concept of IoT into reality. As a result, RPL has become a standard routing protocol for connecting IPv6 to IoT networks. However, like any other network protocol, RPL is vulnerable to various attacks, including sinkhole attacks, which can disrupt network operations. Sinkhole attacks exploit vulnerabilities in RPL by manipulating routing preferences by disseminating falsified data, leading to an abnormal increase in traffic directed toward the attacker's node. This paper introduces the Passive Rule-based Approach (PRBA) to detect sinkhole nodes in RPL-based IoT networks. The PRBA approach relies on three proposed behavioral indicators: (I) Bi-Directional behavior, (II) Bi-Directional Frequently behavior, and (III) Power Consumption behavior. The proposed PRBA approach was implemented and evaluated using the COOJA simulator and compared with state-of-the-art approaches. Simulation results demonstrate that the PRBA approach achieves a detection accuracy rate ranging from 90% to 100%, with a false-positive rate ranging from 0% to 0.2%. Additionally, due to its carefully designed deployment strategy, the proposed approach satisfies the power consumption requirements of constrained nodes without causing an increase in power consumption.

INDEX TERMS Internet of Things (IoT), routing protocol for low-power and lossy networks (RPL), IPv6 over low power wireless personal area networks (6LoWPAN), internet protocol version 6 (IPv6), international data corporation (IDC), distributed denial of service (DDoS).

I. INTRODUCTION

One of the most severe and damaging routing attacks in WSN is the sinkhole attack, which misleads nodes with fake routing information, drops packets, overrides data, or transfers selective and partial data. Additionally, it can deplete the surrounding nodes' energy, creating energy gaps in the network [1], [2], [3]. Therefore, many researchers proposed several sinkhole attack detection approaches in RPL-based networks.

The associate editor coordinating the review of this manuscript and approving it for publication was Byung-Seo Kim.

The IETF standardized the RPL protocol in RFC4919 and RFC6550 documents [4], [5] that focus on IP for LLNs by employing IPv6 over 6LoWPAN, leading to standardizing IPv6 in IEEE 802.15.4 networks. Subsequently, the IETF formed the Routing over Low Power and Lossy Links (ROLL) group to specify RPL. RPL is now a standard routing protocol for IPv6 connected to IoT, and the RPL's objective function selects an optimal route. Each node is assigned an ID centered on the rank and IPv6 address. Nodes exchange graph-related information with other nodes using three RPL-specific Internet Control Message Protocol version 6 (ICMPv6) messages: DIS, DAO, and DIO, as shown in Figure 1 [6]. Routing protocols allow routers to establish

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

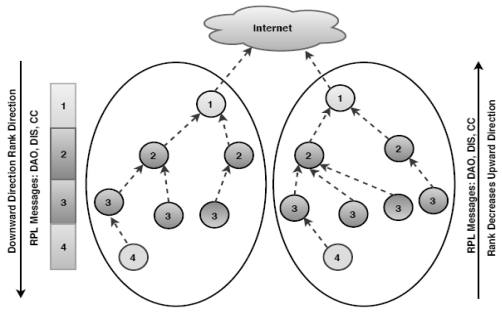

FIGURE 1. RPL topology.

routes between nodes by exchanging route details. However, networks could be vulnerable to attacks if these route details are leaked [7].

IDS has long been an active research topic in network security. Recently, researchers have started to include the detection of sinkhole attacks in IoT networks, which can be classified into two categories (Signature Based Approach and Anomaly-based approaches).

Anomaly-based approaches are more efficient in detecting attacks compared to signature-based approaches. In an anomaly-based approach, the network's normal behavior is defined and used as a baseline. Anomalies are detected when deviations from this baseline occur, and alerts are generated when traffic behavior exceeds a threshold. Anything that does not match normal behavior is considered an intrusion.

The existing approaches for detecting sinkhole attacks neglect the significant behavioral characteristics contributing to accurate detection. Furthermore, most current approaches suffer from increased energy consumption due to their deployment design. Therefore, there is a need for a better solution that can detect sinkhole attacks with low power consumption and high accuracy.

This research paper makes two contributions to the body of knowledge. First, we propose a set of behaviors that can indicate a sinkhole attack in an RPL-based network. These indicators include (i) Bi-Directional, (ii) Bi-Directional Frequency, and (iii) Power Consumption. Second, we propose a rule-based mechanism with predefined threshold values for detecting sinkhole attacks based on these behavioral indicators. The aim is to maximize detection accuracy and minimize the risk of sinkhole attacks.

The remainder of this research paper is organized as follows: Section II discusses IoT, IPv6, RPL, and Sinkhole attacks. Section III explores related works. Section IV describes the proposed approach. Section V presents the experimental findings. Finally, Section VI concludes the paper and suggests potential future works.

II. BACKGROUND

This section introduces the IoT, the IPv6 protocol, and RPL. This section also emphasizes the Sinkhole attack.

A. IoT OVERVIEW

IoT encompasses various constraints, including limited processing capability, low storage capacity, short power life, and restricted transmission range. Therefore, the successful implementation of IoT relies on leveraging the existing Internet Protocol (IP) infrastructure to optimize resource utilization and take advantage of the vast address space offered by Internet Protocol Version 6 (IPv6) [8], [9].

According to the International Data Corporation (IDC), it is estimated that by 2025, there will be 55.7 billion connected IoT devices. Furthermore, IDC predicts that the data collected by IoT devices will triple by 2025 compared to 2019, reaching 18.3 zettabytes [3]. Kaspersky Lab's IoT report highlights a significant increase of over 100% in cyberattacks targeting IoT in the first half of 2021. Attackers aim to steal data, mine cryptocurrency, or create botnets. The report indicates that the number of IoT attacks during the first half of 2021 exceeded 1.5 billion, more than twice the number in the previous six months. These attacks primarily focus on data theft and botnet creation [10].

Additionally, despite increased spending on IT security, IDC reports that 70% of breaches originate from endpoints. Moreover, there is a projected growth in the global security market from $167.1 billion in 2019 to $248.26 billion by 2023, with a Compound Annual Growth Rate (CAGR) of 10.4% [11], [12]. The COVID-19 pandemic has further emphasized the need for enhanced security measures, as remote work has become prevalent across numerous companies. Furthermore, Statista forecasts steady global growth in end-user spending on IoT solutions from 2023 to 2025 [13]. Additionally, IDC estimates that by 2025, there will be 55.7 billion connected IoT devices [3].

Among routing attacks, the sinkhole attack stands out as a particularly damaging Denial of Service (DoS) attack within the IoT environment. Combined with other attacks, it can result in even greater devastation and potential loss of information. If undetected, a sinkhole attack can disconnect nodes from the Internet leading to packet loss and failure to deliver data to the base station. Furthermore, this attack increases network overhead and reduces the network's lifespan due to increased energy consumption, ultimately causing network degradation [14], [15].

B. IPv6 OVERVIEW

IoT has many constraints, including limited processing capability and storage volume, short power life, and limited radio range. Therefore, the IoT implementation uses the existing IP infrastructure to maximize the utilization of available resources while benefiting from the vast address space of IPv6. Additionally, 6LoWPAN is a promising solution that adds an adaptation layer in the network protocol stack to integrate low-power networks, which is suitable for wireless communication of constrained devices, as shown in Table 1 [16], [17], [18].

IPv6 is the next generation of IP to replace Internet Protocol Address Version 4 (IPv4), designed as an upgrade

TABLE 1. 6LoWPAN protocol stack.

Application Layer	CoAP
Transport Layer	UDP
Network Layer	IPv6 | ICMP | RPL
Adaptation Layer	6LoWPAN Adaption
MAC Layer	IEEE 802.15.4
PHY Layer	IEEE 802.15.4

to IPv4 to support the whole world network devices. IPv4 was introduced in 1981, and the number of interconnected computers has grown dramatically, leading to the exhaustion of IPv4 addresses. Accordingly, a new version of the addressing system called IPv6 was developed in 1995 with the main difference in their formats. IPv4 uses 32-bit (4-bytes) addresses to uniquely identify nodes within the global Internet, whereas IPv6 uses 128-bit (16-bytes) addresses. The ample IPv6 address space can resolve the IP address exhaustion issue in IPv4 [19], [20].

C. RPL OVERVIEW

RPL, designed for 6LoWPAN, enables IoT and utilizes various routing messages such as DIS, DIO, and DAO. It outperforms other protocols in terms of overhead, delay, and memory. However, RPL has limitations in physical node protection and cryptographic capabilities [21].

IETF standardized RPL in RFC4919 and RFC6550 [4], [5] to establish IPv6 over 6LoWPAN for IEEE 802.15.4 networks. RPL is now the standard routing protocol for IoT, with nodes identified by IPv6 address and rank. RPL uses ICMPv6 messages (DIS, DIO, and DAO) for exchanging graph-related information [6].

D. SINKHOLE ATTACK

A sinkhole attack is a network layer attack in which the attacker draws a vast amount of traffic and diverts or drops it, aiming to prevent a base station (root) from receiving complete data from nodes. The sinkhole node transmits fabricated routing information to neighboring nodes, who incorporate it into their routing metrics to determine the best data transmission route. As a result, all traffic is directed through the sinkhole node before reaching its intended destination [14], [22]. This continuous consumption and draining of node energy by the sinkhole node lead to decreased network lifetime.

Sinkhole attacks are considered one of the most destructive routing attacks. They flood surrounding nodes with false routing path information and engage in data falsification or selective forwarding of passing data. This attack can potentially drain the energy of neighboring nodes, creating energy holes in wireless sensor networks (WSNs). Furthermore, it can provoke inappropriate and possibly dangerous responses by enabling other attacks, such as selective forwarding attacks, acknowledge spoofing attacks, and drops or alters routing information [14], [23].

III. RELATED WORKS

Intrusion detection has long been an active research topic in network security. Recently, researchers have started to include the detection of sinkhole attacks in IoT networks. Many of the existing approaches for detecting sinkhole attacks suffer from increased energy consumption and a high false-positive rate, and inadequately studied behavioral characteristics, resulting in low detection accuracy [24], [25], [26], [27].

Alzubaidi et al. proposed the Neighbor Passive Monitoring Technique (NPMT) as a lightweight technique for detecting sinkhole attacks in RPL-based IoT networks. The proposed IDS employs a Passive Intermediate Node (PN) to analyze nodes' broadcasts. Neighboring nodes with similar ranks are not flagged as suspicious, while those with different ranks are identified as suspicious nodes. The NPMT outperforms the existing SVELTE method, achieving a 99.5% Accuracy Rate and a 0.53% false-positive rate based on COOJA simulation results. However, using passive intermediate and edge nodes introduces overhead [28], [29].

Ioulianou et al. developed a detection module called IDS Router and a lightweight monitoring module called IDS Detector. IDS Detector monitors and logs network traffic, forwarding it to the IDS Router for detecting malicious nodes. The IDS Router matches attacks against known signatures. IDS Detector only monitors operations within its area and forwards useful information to IDS monitors. A wired connection is recommended for IDS Detector nodes to prevent signal jamming. The evaluation demonstrates high accuracy and low false positives even in large networks, with the main challenge being balancing performance and overhead [30], [31].

Pandu et al. proposed a cognitive security approach for IoT networks to improve user services. The proposed components interact with the IDS, including a data acquisition module that collects data from IoT devices and delivers it to the central monitoring system. The central monitoring system consists of detection and cognitive modules that process the Access Control and Associated Accounting Schemes. The detection module is capable of detecting wormhole and sinkhole attacks. However, the evaluation results regarding performance efficiency are not available [32].

Kaur presented a hybrid IDS called the Ultimate Approach IDS for Mitigating Attacks in RPL-based Low Power Lossy Networks, which follows a universal approach. The IDS can detect known signatures and anomalies using blockchain and calculates trust values to identify attacks and isolate adversaries. It can detect up to eight attacks, including Sinkhole, flooding, wormhole, decreased rank, neighbors, DODAG version number, clone-ID, and sniffing attacks. The author provides a conceptual framework, highlighting its effectiveness, low resource requirements, and extensibility. The system partially supports mobile nodes, focusing on the root and sub-DODAG parents as fixed positions [33].

Verma and Ranga proposed Ensemble Learning Intrusion Detection System (ELNIDS), a signature-based detection

system utilizing machine learning mechanisms. They implemented four ensemble-based ML classifiers: Bagged Trees, RUSBoosted Trees, Boosted Trees, and Subspace Discriminant, to detect sinkhole attacks. ELNIDS consists of six modules: sniffer model, sensor events and traffic repository, feature extraction module, analysis engine, rule base database, and attack notification manager. The evaluation using the RPL-NIDDS17 dataset, containing traffic signatures of various attacks, shows the effectiveness of ELNIDS. The ensemble of Boosted Trees achieved the highest Detection Accuracy (94.5%), while the Subspace Discriminant method achieved the lowest Detection Accuracy (77.8%) [34], [35].

Bhale et al. proposed a lightweight IDS with a roving nature in their work. They placed a lightweight IDS in a 6BR router and a roving IDS in constrained nodes. The defense method was implemented using the Cooja network simulator on the Contiki operating system. Through experimental results, they demonstrated that the solution is lightweight, performs remarkably well, and can accurately identify sinkhole attacks. It achieved a True Positive Rate of 95.86% and a True Negative Rate of 94.31%. However, it should be noted that the Roving IDS, when placed in a constrained environment, exhibits high memory utilization [36].

In summary, the existing mechanisms for detecting sinkhole attacks face several challenges. First, they consume a large amount of network bandwidth and memory. Additionally, they have a notable false positive rate leading to incorrectly flagging normal network activity as sinkhole attacks. Thirdly, insufficient research into sinkhole attacks' behavioral characteristics results in low detection accuracy. Furthermore, many mechanisms have overlapping features and struggle to select the most crucial features for detecting sinkhole attacks. The problem contributes to a high false-positive rate and undermines detection accuracy. Finally, deployment design leads to challenges such as high overhead and energy consumption, as shown in Table 2, which presents the key findings of existing mechanisms.

TABLE 2. Summary of related works.

Authors	Approach	Key Findings
Alzubaidi et al. (2018)	Neighbor Passive Monitoring	- Proposed a lightweight technique (NPMT) for detecting sinkhole attacks in RPL-based IoT networks. -- Achieved a 99.5% Accuracy Rate and a 0.53% false-positive rate based on simulation results - Overhead introduced by passive intermediate and edge nodes.
Ioulianou et al. (2018)	IDS Router and IDS Detector	- Developed a detection module (IDS Router) and monitoring module (IDS Detector). - Demonstrated high accuracy and low false positives in large networks. - Wired connection recommended for IDS Detector nodes to prevent signal jamming.
Pandu et al. (2019)	Cognitive Security Approach	- Proposed a cognitive security approach for IoT networks. - Components interact with IDS for data collection and processing. - Detection module capable of identifying wormhole and sinkhole attacks. - Lack of performance efficiency evaluation.
Kaur (2019)	Ultimate Approach IDS	- Presented a hybrid IDS approach for mitigating attacks in RPL-based networks. - Able to detect known signatures and anomalies using blockchain. - Supported detection of multiple attacks with low resource requirements. - Partial support for mobile nodes.
Verma and Ranga (2019)	Ensemble Learning IDS	- Proposed a signature-based detection system (ELNIDS) using ensemble-based ML classifiers. <- Achieved high detection accuracy for sinkhole attacks. - Different classifier methods showed varied performance.
Bhale et al. (2020)	Lightweight IDS with Roving	- Proposed a lightweight IDS with a roving nature for sinkhole attack detection. - Achieved high True Positive Rate and True Negative Rate. - High memory utilization observed in a constrained environment.

IV. THE PROPOSED APPROACH

This section explains the proposed approach PRBA, which aims to detect sinkhole attacks with low power consumption and high detection accuracy. Figure 2 shows the general stages of PRBA.

A. DATA COLLECTION AND PRE-PROCESSING (STAGE1)

Data collection and pre-processing are essential stages that involve collecting and transforming power consumption values and capturing ICMPv6 network traffic into a meaningful format. This process prepares the data as an input dataset for the subsequent stage, which is feature selection. Often, datasets contain significant irrelevant information, which can increase processing time. Moreover, overlapping features and including insignificant features for sinkhole attack detection can negatively impact detection accuracy and result in a high false-positive rate [26], [37].

In this stage, power consumption data and ICMPv6 packets are passively collected from each node to identify relevant information contributing to sinkhole attack detection. This stage elaborates on data collection, capture, and filtering to construct a dataset. The data collection and preprocessing stage can be divided into two steps, as depicted in Figure 3.

1) DATA FILTRATION

In the IoT network, various types of network traffic, including different packet protocols, traverse through the system. However, not all protocols are relevant to detecting sinkhole attacks. The primary purpose of this step is to filter ICMPv6 packet-specific attributes, such as source, destination, and rank. Additionally, the power consumption features of each

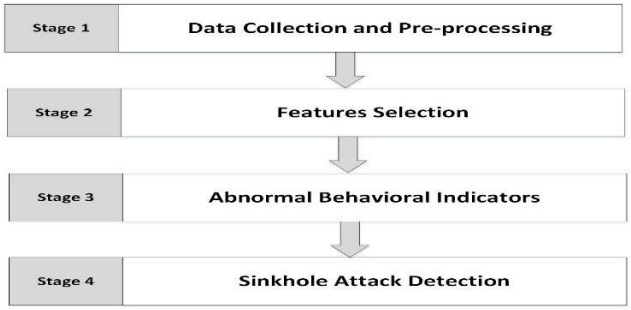

FIGURE 2. General stages of PRBA.

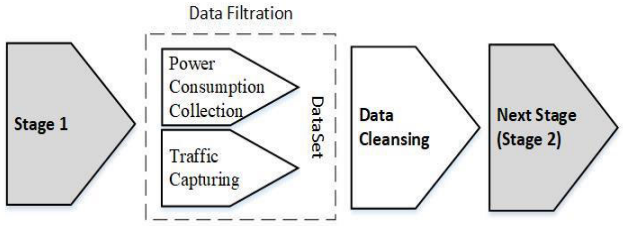

FIGURE 3. Data collection and preprocessing steps.

node are collected. The ICMPv6 packets and the power consumption feature are significant in detecting sinkhole attacks.

The COOJA simulator's 'collect view' feature provides the energy consumption details of each node, while the Wireshark tool offers information about the network traffic of ICMPv6 transmissions. The resulting data, which includes the features from both the ICMPv6 packet and power consumption values, are passed to the next stage (Feature Selection) to identify the most significant features that contribute to the detection of sinkhole attacks. Furthermore, these features will be categorized based on their contributions to sinkhole attack detection.

The Data Filtration step filters out the ICMPv6 packet and power consumption data as follows:

•ICMPv6 Packet: ICMPv6 helps to detect sinkhole attacks by filtering and keeping an eye on specific network traffic attributes like RPLInstanceID, DODAGID, DODAG Version Number, Rank, Sequence, and IPv6 Address. By looking at these attributes, ICMPv6 can find changes or inconsistencies in the network's topology and routing protocols that are not normal, leading to detecting possible sinkhole attacks early and taking quick steps to stop them. The reason for filtering these particular ICMPv6 attributes is their common usage in existing studies, as demonstrated in [29] and [35]. The Wireshark sniffing tool filters the ICMPv6 attributes through the "protocol==icmpv6" command. A total of 33 ICMPv6 attributes are filtered. However, not all these features significantly contribute to the detection of sinkhole attacks; hence, these attributes are passed to the next stage, "feature selection," to select the subset of features representative of all features and essential to the detection of sinkhole attacks.

•Power Consumption Values: Energy consumption monitoring can detect sinkhole attacks in IoT networks. Increased power consumption by devices in the network may indicate a sinkhole attack, where a malicious node serves as a central hub for all network activity. In a normal network operation, nodes maintain relatively balanced energy consumption by performing regular functions and communicating. However, a sinkhole node may exhibit higher-than-normal power usage as it diverts and reroutes traffic intended for other legitimate nodes. Abnormalities that suggest a sinkhole attack can be identified by continuously monitoring the power consumption of devices. In this research, the power consumption features/values such as all_cpu, all_lpm, and all_transmit are obtained using the Powertracer tool [29], which saves them as a "text" file. The features of power consumption are used as input for the next stage.

2) DATA CLEANSING

The Data Cleansing step aims to reduce the traffic volume in the dataset by addressing various issues such as fixing or removing corrupted, incorrectly formatted, duplicate, or incomplete data. By performing data cleansing, the detection accuracy is improved, and the search time for the dataset is reduced.

The resulting cleansed dataset, including the features derived from the ICMPv6 packet and power consumption values, will proceed to the next stage (Features Selection). In this stage, the most significant features that contribute to detecting sinkhole attacks will be selected. Additionally, these features will be categorized based on their respective contributions to detecting sinkhole attacks.

B. FEATURE SELECTION (STAGE 2)

In detecting sinkhole attacks, feature selection poses two significant challenges. Firstly, it selects practical features that efficiently identify and detect sinkhole attacks. Secondly, determining the importance of features, assigning higher weight values to those essential for sinkhole attack detection while excluding those with low weight values. The primary objective of feature selection techniques is to reduce the size of selected features and identify the most significant ones using appropriate algorithms. In the Feature Selection stage, the focus is on retaining the features with the most significant impact on detecting sinkhole attacks while discarding redundant or unnecessary features. This process typically employs ranking techniques that assign weight values to each feature as parameters, optimizing the sinkhole attack detection model.

Various algorithms are suitable for feature ranking, including ReliefF, Principal Component Analysis (PCA), and Information Gain Ratio (IGR). ReliefF is widely used among them due to its simplicity, high operational efficiency, and satisfactory results. It demonstrates good convergence and efficiency, making it practical for feature selection in most scenarios [38].

The ReliefF algorithm utilized in the proposed method is adapted using the Waikato Environment for Knowledge

Analysis (Weka) software [38], [39]. The ReliefF algorithm selects 15 of the 33 features as the most important for sinkhole detection. These 15 features are chosen based on equations that reflect their significance and importance in identifying and detecting sinkhole attacks. These essential features play a crucial role in contributing to the accuracy and effectiveness of sinkhole detection.

C. BEHAVIOURAL INDICATORS (STAGE 3)

The Behavioral Indicators stage plays a crucial role in this approach as it aims to identify suspicious nodes in RPL networks by analyzing selected features. The features obtained from the previous stage (Feature Selection), including ICMPv6 and power consumption data, are utilized to detect abnormal behavior associated with sinkhole attacks in RPL-based networks. Abnormal behavior indicators are identified through repeated experiments and continuous monitoring of sinkhole attack behavior.

1) BI-DIRECTIONAL BEHAVIOUR

The Bi-Directional behavior has been identified through experiments and observations of normal packet transmission and abnormal behavior associated with a sinkhole attack. This behavior occurs when the victim node selects the sinkhole node as its parent node while the sinkhole node reciprocally selects the victim node as its parent. The purpose of this behavior is for the sinkhole node to attract a significant amount of traffic, aiming to disrupt the flow of complete data from the sensor nodes to the base station.

2) BI-DIRECTIONAL FREQUENTLY BEHAVIOUR

After conducting numerous experiments and closely monitoring the Bi-Directional behavior, it has been observed that the Bi-Directional Frequently Behavior occurs multiple times between the sinkhole node and its neighboring nodes. This behavior arises when the sinkhole node attempts to attract multiple victims from its neighboring nodes. Consequently, the number of member nodes transmitting data to the base station decreases. Furthermore, with an increased number of infected neighbors, the network's overall efficiency diminishes as the base station receives fewer data packets.

3) POWER CONSUMPTION BEHAVIOUR

The sensors near the sinkhole attack experience a severe battery power exhaustion issue, reducing the overall network lifetime and increasing control overhead. Additionally, the energy outflow surrounding the sinkholes is altered, negatively impacting the network's performance. The severity of energy drainage on neighboring nodes depends on the number of nodes affected by the sinkhole attack. Meanwhile, the remaining nodes in the network maintain energy levels similar to those in a network without sinkhole attacks.

The monitoring node performs the task of passively listening to all messages that traverse through the network topology. Whenever bi-directional behavior, bi-directional behavior, or power consumption behavior is detected, an alarm is triggered, indicating the transition to the next stage, the Sinkhole Attack Detection.

D. SINKHOLE ATTACK DETECTION (STAGE 4)

This stage aims to decide whether there is a sinkhole attack according to information from the previous stage (behavioural indicators). This stage consists of the following subsequent steps.

1) RULE-BASED

This step identifies the suspicious nodes by analyzing the ICMPv6 and power consumption features by applying specific rules with thresholds. Determining the threshold values involves conducting experiments, observations, and analyses under normal and abnormal conditions.

As a result, the Threshold values are applied to behavioural indicators. The rules are as follows:

Rule No.1: Bi-Directional Behaviour detection

The first proposed rule aims to detect Bi-Directional Behaviour using the following rule:

> Based on the following rule, Bi-Directional Behaviour is identified for each DODAG:
>
> If Child (Node) Refer Parent (Node) AND Parent (Node), Refer Child (Node) At the exact moment, then consider it as suspicious behaviour.

The Bi-Directional behaviour will be calculated for each DODAG every minute, and the above rule will be applied. Whenever a Bi-Directional behaviour occurs, an alert is triggered.

Rule No.2: Bi-Directional Frequently Behaviour detection

The second proposed rule aims to detect Bi-Directional Frequently Behaviour using the following rule:

> Based on the following rule, Bi-Directional Behaviour is identified for each DODAG:
>
> If Count (Bi-Directional behaviour) $>$ *th*, consider it suspicious behaviour.

An alert will be triggered if the Bi-Directional Behaviour count exceeds the threshold (*th*).

Rule No.3: Power Consumption Behaviour Detection

The third proposed rule aims to detect Power Consumption Behaviour. The power consumption for each node is calculated using the following rule:

> Based on the following rule, Power Consumption behaviour is identified for each node:
>
> If Power Consumption (Node) $>$ *th*1, then consider it as a suspicious behaviour

The thresholds *th* and *th*1 are preconfigured, and their values are determined through experiments, observations, and analyses conducted under various network conditions, including normal and abnormal scenarios. While using predefined thresholds allows for simplicity and ease of implementation, it is essential to acknowledge their limitations in adapting to dynamic and evolving attack patterns in real-world IoT environments. As a result, careful consideration should be given to regularly updating and fine-tuning these thresholds to optimize detection accuracy and minimize attack risks. The output of the rules is passed as input for the next stage in the detection process.

2) UNWEIGHTED VOTING METHOD FOR DETECTING THE SINKHOLE ATTACK

The proposed approach employs the unweighted voting method, wherein each voter or rule carries equal weight, to identify sinkhole anomalies accurately. This method does not allow voters to express their preference for one candidate over another, making it less complex as it does not involve intricate measures [37], [40]. To detect a sinkhole attack, a majority voting rule is applied to the outcomes of the behavioral rules. In particular, the unweighted voting method requires a majority of over 51% to determine the presence of a sinkhole attack based on the voting result [41], [42].

The unweighted voting method stands out due to its characteristic of assigning equal weight to each voter in the decision-making process. Unlike other selection methods like Preference Ballots or Plurality, the unweighted voting method avoids complexity and allows voters to express their preferences for candidates equally.

The selection of Bi-Directional behavioral, Bi-Directional Frequently behavioral, and Power Consumption behavior indicators for the unweighted voting method is based on their relevance and contribution to identifying sinkhole nodes within the proposed research context. These indicators have been carefully chosen from other options based on their ability to capture key characteristics of sinkhole attacks and distinguish them from normal network behavior [43], [44].

Although the specific indicators may be tailored to the IoT context of the sinkhole attack detection, the unweighted voting method can be generalized and applied to other related applications, as demonstrated in [45]. The technique can be adapted by selecting appropriate indicators relevant to the problem. For example, in a different application domain, such as anomaly detection in network traffic, the unweighted voting method can be utilized by selecting indicators that capture the desired abnormal behavior patterns.

The unweighted voting method offers simplicity and fairness by assigning equal weight to each voter or rule in the decision-making process. It enables straightforward implementation and interpretation while ensuring that all indicators are considered equally. This generalizability and flexibility make the unweighted voting method valuable in various applications where multiple indicators contribute to the decision-making process.

3) THE DETECTION OF SINKHOLE ATTACKS IS BASED ON EQUATION (1)

$$R = (\sum(\text{Abnormal Behaviours})/3) \quad (1)$$

If R > 51% Then Alert =True
Else
    Alert=False
End
R: is the result

Equation (1) shows sinkhole attacks will be detected if R exceeds 51%. Otherwise, it is treated as a normal packet.

By utilizing a threshold of 51% in the unweighted voting method, we aim to capture the majority of voters' preferences. This threshold represents a significant portion of the voting population, precisely two-thirds. Setting the threshold at this level ensures a clear majority consensus is reached before determining the presence of a sinkhole attack based on the voting results.

The selection of 51% as the detection threshold was motivated by a desire to maximize accuracy. It is rigorous enough to prevent false positives and broad sufficient to identify actual sinkhole assaults. The threshold facilitates an assured decision-making procedure by requiring a large margin of agreement among the indicators.

V. EXPERIMENTAL RESULTS

This section evaluates the proposed approach and provides insights and discussions regarding the experimental results. For the experiment of creating the RPL-NIDDS17 and NPMT datasets, a detailed list of specific parameters used is presented in Table 3.

TABLE 3. Parameter settings of the experiments.

Item	Description
Routing protocol	RPL
Running time	5 minutes
Number of nodes, including Sink Node	20 Nodes
Sinkhole Node	1Node
Passive Node (Sniffer Node)	1 Node
Total Number of Nodes	22 Nodes

A. DATASET

The PRBA is evaluated using the RPL-NIDDS17 [35] and NPMT [29] datasets to measure detection accuracy, false-positive rate, and power consumption. These datasets were chosen based on their common usage in existing research, such as [46], [47], and [48].

The RPL-NIDDS17 dataset consists of seven types of modern routing attacks: Sinkhole, Blackhole, Selective Forwarding, Clone ID, Sybil, Hello Flooding, and Local Repair.

The evaluation of the RPL-NIDDS17 dataset involves assessing four machine-learning classifiers: RUSBoosted trees, bagged trees, boosted trees, and subspace discriminant boosted trees. Performance measures such as accuracy, area under the curve, and the ROC curve are evaluated as part of the performance assessment process. The RPL-NIDDS17 dataset is used to train the classifiers, although the classifier tuning and feature selection techniques were not employed.

NetSim is a tool employed to generate the RPL-NIDDS17 dataset. The IoT network comprises a gateway, sensor nodes, wired nodes, and a router, as depicted in Figure 4.

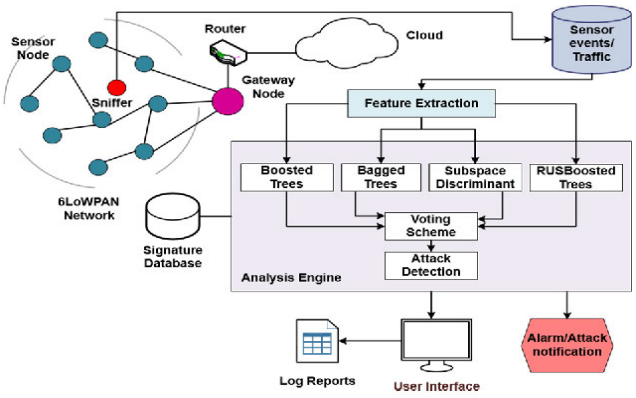

FIGURE 4. ELNIDS architecture.

The RPL-NIDDS17 dataset consists of twenty-two attributes, such as Time, Source Destination ID, Packet Type (TCP, ICMPv6, and UDP), Attack Category, and Label (Normal or Attack) [49], [50].

To generate the NPMT dataset, the COOJA simulator is run for basic DODAG topology without any attack for a specific time, then runs the attack after a while, and two datasets are collected. The COOJA simulator tool created these datasets with a simulated IoT network topology that includes a Base station (Router/Sink), Passive nodes, and Sensor nodes, as shown in Figure 5 [51], [52].

The first dataset comprises data from the packet analyzer collected using the COOJA simulator and saved as a ''PCAP'' file. The second dataset includes each skymote's power consumption data obtained using the Powertracer tool, which saves the data in a ''text'' file. All the information is kept in a separate CSV and text file for sinkhole attacks. The packet analyzer dataset consists of ten features, such as Time, Source IP, Destination IP, Rank, Info, Protocol Type (TCP, ICMPv6, and UDP), and Label (Normal or Attack) [29].

B. RESULTS OF THE FEATURE SELECTION STAGE

Sixteen features with the highest ReliefF algorithm value weights are selected and nominated as contributors to detecting sinkhole attacks. The result of the field ranking using the ReliefF algorithm in WEKA tools shows the selected features.

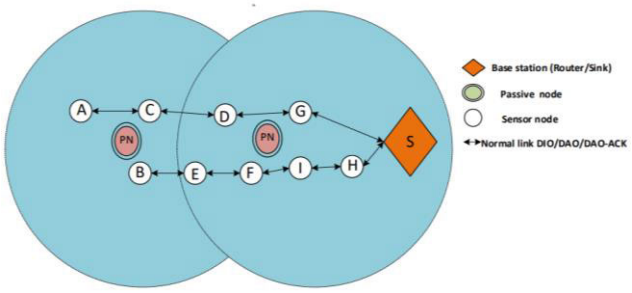

FIGURE 5. NPMT architecture.

C. RESULTS OF BEHAVIOURAL INDICATORS STAGE

The stage aims to identify suspicious nodes in RPL-based networks by analyzing the features listed in Table 4, which are associated with abnormal behavior. These features were introduced in the previous step specifically to detect abnormal behavior.

1) DETECTION OF BI-DIRECTIONAL BEHAVIOURAL INDICATOR

Bi-Directional behavior occurs when the attacked node selects the sinkhole node as its parent node, and simultaneously the sinkhole node selects the attacked node as its parent. This means that the parent node considers its child as a parent, and the child node simultaneously considers its parent as a parent. The sinkhole node attempts to attract a significant amount of traffic, making the base station unable to receive sensor data from the nodes exhibiting this behavior. Table 5 presents the records of Bi-Directional behavior in the RPL-NIDDS17 and NPMT datasets, explicitly indicating the occurrences between the parent and destination nodes.

In the RPL-NIDDS17 dataset, it is evident that there is Bi-Directional behavior between the parent node and the destination node. The records show that the source IP address of the parent node, fe80::212:7407:7:707, corresponds to the destination IP address of the parent node, fe80::212:7411:11:1111. Similarly, the records indicate that the source IP address of the parent node, fe80::212:7411:11:1111, corresponds to the destination IP address of fe80::212:7407:7:707. This reciprocal relationship confirms the presence of Bi-Directional behavior in the RPL-NIDDS17 dataset.

In the NPMT dataset, it is evident that Bi-Directional behavior is observed between the parent node and the destination node. The records show that the source IP address of the parent node, fe80::212:7405:5:505, corresponds to the destination IP address of the parent node, fe80::212:7404:4:404. Similarly, the records indicate that the source IP address of the parent node, fe80::212:7404:4:404, corresponds to the destination IP address of fe80::212:7405:5:505. This reciprocal relationship confirms the presence of Bi-Directional behavior in the NPMT dataset.

The detected Bi-Directional behavior is an essential input for the unweighted voting method in the Sinkhole Attack

TABLE 4. List of selected features.

Features	Description
IPv6.IP Source Address	IPv6 source address
IPv6.Time	The timestamp of the packet
PowerConsumption.ALL_LPM	Accumulated low power mode energy consumption
IPv6.IP Destination Address	The IPv6 address where this packet is going to
IPv6.Info	– Additional information about the packet content Options: – DAO – DIO – DIS – Ack
ICMPv6.RplOptType	RPL Option Types Options: – RPL Target Transit Information DODAG configuration
ICMPv6.RplOpt.Length	Length of Option Types Options: • 18 bit • 14 bit • 0 bit
IPv6.Protocol Type	The protocol type like TCP, UDP, and ICMPv6
PowerConsumption.ALL_CPU	Accumulated CPU energy consumption
ICMPv6.CheckSum	The checksum field detects data corruption in the ICMPv6 message and parts of the IPv6 header.
ICMPv6.CheckSumStatus	If the ICMP header is changed or corrupted between Source and Destination, then ICMPv6.CheckSumStatus will be Bad; if not, then ICMPv6.CheckSumStatus =Good Options: – Good – Bad
PowerConsumption.ALL_TRANSMIT	Accumulated transmission energy consumption
IPv6.ProtocolType	The Protocol name like TCP, UDP, and ICMPv6
IPv6.Rank	Defines the individual node's position relative to other nodes concerning the DODAG root
PowerConsumption.ALL_LISTEN	Accumulated energy consumption

Detection stage. Since the Bi-Directional behavior is considered suspicious, it contributes to the decision-making process in identifying potential sinkhole attacks. Including this behavioral indicator in the unweighted voting, method helps enhance the accuracy and effectiveness of detecting sinkhole attacks in the network.

2) DETECTION OF BI-DIRECTIONAL FREQUENTLY BEHAVIOURAL INDICATORS

The primary objective of this behavior is to track the frequency of Bi-Directional occurrences within a specific DODAG ID. By monitoring the event of Bi-Directional behavior, the IDS (Intrusion Detection System) can identify potential sinkhole attacks. An alert is triggered when

TABLE 5. Bi-directional records.

Direction	Parent > Child Direction		Child Direction > Parent	
Datasets	Parent Node	Destination Node	Parent Node	Destination Node
RPL-NIDDS17	fe80::212:7407:7:707	fe80::212:7411:11:1111	fe80::212:7411:11:1111	fe80::212:7407:7:707
NPMT	fe80::212:7405:5:505	fe80::212:7404:4:404	fe80::212:7404:4:404	fe80::212:7405:5:505

TABLE 6. Bi-directional frequency records.

Direction	Parent > Child Direction		Child Direction > Parent	
Datasets	Parent Node	Destination Node	Parent Node	Destination Node
RPL-NIDDS17	fe80::212:7407:7:707	fe80::212:7411:11:1111	fe80::212:7411:11:1111	fe80::212:7407:7:707
	fe80::212:7407:7:707	fe80::212:7412:12:1212	fe80::212:7412:12:1212	fe80::212:7407:7:707
NPMT	fe80::212:7405:5:505	fe80::212:7404:4:404	fe80::212:7404:4:404	fe80::212:7405:5:505
	fe80::212:7405:5:505	fe80::212:7409:9:909	fe80::212:7409:9:909	fe80::212:7405:5:505

the number of Bi-Directional behaviors surpasses a predefined threshold, indicating a higher likelihood of sinkhole attacks. Table 6 presents the records of Bi-Directional Frequently behavior observed between the parent node and destination node in both the RPL-NIDDS17 and NPMT datasets. The RPL-NIDDS17 dataset exhibits two instances of Bi-Directional behavior. In the first instance, the source IP VOLUME XX, 2017 address for the parent node, fe80::212:7407:7:707, refers to the destination IP address for the parent node, fe80::212:7411:11:1111. Simultaneously, the dataset records show that the source IP fe80::212:7411:11:1111 of the parent node refers to the destination IP fe80::212:7407:7:707. Similarly, in the second instance, the source IP address for the parent node, fe80::212:7407:7:707, refers to the destination IP address for the parent node, fe80::212:7412:12:1212, while the source IP fe80::212:7412:12:1212 of the parent node refers to the destination IP fe80::212:7407:7:707. Thus, Bi-Directional Frequent behavior is observed in the RPL-NIDDS17 dataset.

Similarly, the NPMT dataset displays Bi-Directional Frequently behavior in two instances. In the first instance, the source IP address for the parent node, fe80::212:7405:5:505, refers to the destination IP address for the parent node, fe80::212:7404:4:404, while the source IP fe80::212:7404:4:404 of the parent node refers to the destination IP fe80::212:7405:5:505. In the second instance, the source IP address for the parent node, fe80::212:7405:5:505, refers to the destination IP address for the parent node, fe80::212:7409:9:909, and the source IP fe80::212:7409:9:909

of the parent node refers to the destination IP fe80::212:7405:5:505. These occurrences of Bi-Directional Frequently behavior surpass the threshold value set to one, indicating suspicious behavior.

The results of the Bi-Directional Frequently behavior are subsequently used as input for the unweighted voting method in Sinkhole Attack Detection.

3) DETECTION OF POWER CONSUMPTION BEHAVIOURAL INDICATOR

The passive node collects power consumption values from the nodes, and changes in CPU, LPM, TX, and RX power consumption values indicate the stability or instability of the network routing topology. An increase in these power consumption values suggests an unstable network, while a decrease indicates a stable network. By analyzing the power consumption of each node, the impact of the sinkhole attack can be determined.

Table 7 provides information on the power consumption behavior of the sinkhole node in the RPL-NIDDS17 dataset. The table describes the CPU, LPM, TX, and RX power consumption values, indicating whether the values increase or decrease.

TABLE 7. Power consumption records for sinkhole node (NODE 7) - RPL-NIDDS17 dataset.

Time in Minute	CPU	LPM	TX	RX	Power Consumption (mW)
1	0.1266	0.1487	0.1161	0.4356	0.8270
2	0.0964	0.1606	0.0641	0.4145	0.7355
3	0.0935	0.1607	0.0564	0.4133	0.7239
4	0.2545	0.1558	0.3564	0.6051	1.3717
5	0.2556	0.1557	0.0844	0.4302	0.9259

Similarly, Table 8 presents the power consumption behavior for the sinkhole node in the NPMT dataset. It provides details on the CPU, LPM, TX, and RX power consumption values and indicates whether these values increase or decrease.

TABLE 8. Power consumption records for sinkhole node (NODE 5) – NPMT DATASET.

Time in Minute	CPU	LPM	TX	RX	Power Consumption (mW)
1	0.1034	0.1604	0.1056	0.4275	0.7969
2	0.1221	0.1598	0.0524	0.4215	0.7557
3	0.1211	0.1598	0.0460	0.4168	0.7437
4	0.1888	0.1615	0.1639	0.5873	1.1015
5	0.1389	0.1593	0.1255	0.4800	0.9038

The impact of the sinkhole attack on the network can be assessed by analyzing the power consumption behavior recorded in these tables.

The power consumption of the sinkhole node exhibits significant changes after the attack. In both the RPL-NIDDS17 and NPMT datasets, the power consumption of the CPU, LPM, TX, and RX experienced an increase, with values changing from 0.7239 mW to 1.3717 mW and 0.7437 mW to 1.1015 mW, respectively.

Rule No.3, which focuses on power consumption, has been applied, and it has been observed that the power consumption exceeds the threshold value of 1 mW. This behavior is considered suspicious.

The increase in power consumption results from the sinkhole node attracting and processing traffic from nearby nodes. The sinkhole node handles two types of illegitimate traffic: transmitted traffic (TX) and received traffic (RX).

The analysis of power consumption behavior serves as input to the unweighted voting method in the Sinkhole Attack Detection process.

D. COMPARISON WITH THE ELNIDS APPROACH

This section compares the detection accuracy of the PRBA, and ELNIDS approaches using the datasets provided in Table 9 and Table 10. The detection accuracy is evaluated to assess the performance of each approach in identifying sinkhole attacks.

TABLE 9. Comparison between PRBA and ELNIDS on false-positive rate and detection accuracy rate.

Approaches	False-Positive Rate	Detection Accuracy Rate
ELNIDS	-	77.8 - 94.5%
PRBA without an unweighted voting method	0.2%	90%
PRBA with an unweighted voting method	-	100%

TABLE 10. Comparison between PRBA and NPMT on false-positive rate and detection accuracy rate.

Approaches	False-Positive Rate	Detection Accuracy Rate
NPMT	0.53%	99.5%
PRBA without an unweighted voting method	0.2%	90%
PRBA with an unweighted voting method	-	100%

Comparing the PRBA approach and the ELNIDS approach for detecting sinkhole attacks indicates that the ELNIDS approach achieves the highest accuracy rate of 94.5%. However, it also has the worst accuracy rate, 77.8%, as shown in Table 9. On the other hand, the NPMT technique achieves a high accuracy rate of 99.5% with a low false-positive detection rate of 0.53%, as shown in Table 10.

The simulation results reveal that the PRBA approach with the unweighted voting method achieves a perfect accuracy rate of 100%. Without the unweighted voting method, the PRBA approach still achieves a high accuracy rate of 90% with a low false-positive rate of 0.2%. These results are summarized in Table 9 and Table 10.

The PRBA approach demonstrates better detection accuracy than the ELNIDS and NPMT approaches due to its reliance on three indicators supported by rules and an unweighted voting method.

This research proposes a passive rule-based approach for detecting sinkhole attacks in 6LoWPAN RPL-based IoT networks, prioritizing low power consumption and high detection accuracy. Sinkhole attacks are evaluated using three primary behavior indicators. The subsequent subsections provide a detailed discussion of the obtained results. The PRBA approach is implemented and evaluated using the COOJA simulator, and its performance is compared with the ELNIDS approach and NPMT technique.

1) DISCUSSION IN TERMS OF ACCURACY DETECTION

Table 9 demonstrates that the PRBA approach achieves a higher detection accuracy than ELNIDS and NPMT, as evidenced by the experimental results. This superiority can be attributed to PRBA's utilization of three indicators supported by rules and unweighted voting methods. The ELNIDS approach, although accurate and effective in detecting known attacks through signature-based intrusion detection, lacks the comprehensive coverage provided by PRBA. On the other hand, NPMT's reliance on only two indicators, namely power consumption, and ranking, renders it susceptible to failure if any of these indicators fail to trigger.

Incorporating the three major behavior indicators in PRBA significantly enhances its detection accuracy, especially with the unweighted voting methods. These indicators revolve around bi-directional behavior, bi-directional frequency behavior, and power consumption behavior. By leveraging these indicators, PRBA can effectively identify and detect sinkhole attacks in RPL networks, surpassing the capabilities of ELNIDS and NPMT.

2) DISCUSSION IN TERMS OF POWER CONSUMPTION

The PRBA approach aims to meet the requirements of constrained nodes by conserving energy, prolonging battery life, and minimizing power consumption. In contrast, ELNIDS consumes significant power due to the necessity of maintaining an extensive attack signature database. Similarly, NPMT exhibits higher energy consumption than PRBA due to an inappropriate deployment design where the IDS is installed on a passive intermediate node that analyzes all nodes' broadcast traffic.

In the case of PRBA, power consumption is measured with and without the passive node, ensuring that data collection by the passive node does not impact other constrained nodes in the network. The average power consumption without the passive node is approximately the same as the average power consumption with the passive node and without any attacks. Moreover, since the passive node is connected via a wired network, it does not interfere with the power supply of normal nodes. This aligns with the primary objective of the thesis, which is to propose a low-power consumption approach for detecting sinkhole attacks in RPL-based IoT networks.

VI. CONCLUSION

The current approaches for detecting sinkhole attacks lack consideration of significant behavioral characteristics crucial for accurate identification. Moreover, the deployment design of these approaches often leads to increased energy consumption. Therefore, there is a need for a more efficient and precise method of detecting sinkhole attacks. The PRBA approach aims to meet constrained node requirements by conserving energy, improving battery life, and reducing power consumption. Adopting this approach makes it possible to detect sinkhole attacks effectively while minimizing the impact on power consumption. In future research, exploring additional behavioral indicators that can enhance the detection accuracy of sinkhole attacks in RPL networks is recommended. For instance, investigating the effectiveness of DIO transactions as an indicator of abnormal behavior could provide valuable insights.

Furthermore, considering the influence of mobility and environmental factors on sinkhole attack detection may lead to developing more robust and reliable detection mechanisms in RPL networks. Moreover, a combination of rule-based systems with other advanced techniques such as machine learning, anomaly detection, and behavior analysis is often employed to ensure maximum detection accuracy and minimum attack risk. These approaches enable the detection of unknown and emerging attack patterns, providing better protection against evolving IoT attacks. Also, evaluating the proposed approach in a real-world environment is recommended to assess its effectiveness and performance in practical scenarios. Finally, we plan to explore more sophisticated techniques for threshold determination, such as machine learning algorithms or adaptive thresholding methods.

REFERENCES

[1] J. Arshad, M. A. Azad, R. Amad, K. Salah, M. Alazab, and R. Iqbal, "A review of performance, energy and privacy of intrusion detection systems for IoT," *Electronics*, vol. 9, no. 4, p. 629, Apr. 2020.

[2] G. H. An and T. H. Cho, "Improving sinkhole attack detection rate through knowledge-based specification rule for a sinkhole attack intrusion detection technique of IoT," *Int. J. Comput. Netw. Appl.*, vol. 9, no. 2, pp. 169–178, 2022.

[3] A. U. Rehman, S. U. Rehman, and H. Raheem, "Sinkhole attack in wireless sensor networks: A survey," *Wireless Pers. Commun.*, vol. 106, no. 4, pp. 2291–2313, 2019.

[4] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals," Netw. Work. Group, Internet Eng. Task Force, Tech. Rep. RFC 4919, 2007.

[5] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, and P. Levis, "RPL: IPv6 routing protocol for low-power and lossy networks," Internet Eng. Task Force, Tech. Rep. RFC 6550, 2012.

[6] M. Liscio, "Design development and assessment of a multi-interface IoT platform," M.S. thesis, School Ind. Inf. Eng., Politecnico di Milano, 2016. [Online]. Available: https://www.politesi.polimi.it/handle/10589/123244

[7] D. Airehrour, J. Gutierrez, and S. K. Ray, "A testbed implementation of a trust-aware RPL routing protocol," in *Proc. 27th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2017, pp. 1–6.

[8] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2661–2674, Nov. 2013.

[9] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) communication protocols: Review," in *Proc. 8th Int. Conf. Inf. Technol. (ICIT)*, May 2017, pp. 685–690.

[10] L. Deng, H. Wen, M. Xin, H. Li, Z. Pan, and L. Sun, "Enimanal: Augmented cross-architecture IoT malware analysis using graph neural networks," *Comput. Secur.*, vol. 132, Sep. 2023, Art. no. 103323.

[11] *Statista*. Accessed: Feb. 16, 2021. [Online]. Available: https://www.statista.com/statistics/693303/smart-home-consumer-spending-worldwide/

[12] L. Columbus. (2020). *Roundup of Cybersecurity Forecasts and Market Estimates*. Retrieved From Forbes. Accessed: Jun. 1, 2022. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates

[13] S. Al-Sarawi, M. Anbar, R. Abdullah, and A. B. Al Hawari, "Internet of Things market analysis forecasts, 2020–2030," in *Proc. 4th World Conf. Smart Trends Syst., Secur. Sustainability (WorldS)*, Jul. 2020, pp. 449–453.

[14] S. Padmanabhan, R. Maruthi, and R. Anitha, "An experimental study to recognize and mitigate the malevolent attack in wireless sensors networks," *Global Transitions Proc.*, vol. 3, no. 1, pp. 55–59, Jun. 2022.

[15] G.-X. Yang and F.-J. Li, "Investigation of security and defense system for home based on Internet of Things," in *Proc. Int. Conf. Web Inf. Syst. Mining*, vol. 2, Oct. 2010, pp. 8–12.

[16] X. Li, Z. Xuan, and L. Wen, "Research on the architecture of trusted security system based on the Internet of Things," in *Proc. 4th Int. Conf. Intell. Comput. Technol. Autom.*, vol. 2, Mar. 2011, pp. 1172–1175.

[17] 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.

[18] C.-A. La, M. Heusse, and A. D. Grenoble, "Link reversal and reactive routing in low power and lossy networks," in *Proc. IEEE 24th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2013, pp. 3386–3390.

[19] A. K. Al-Ani, M. Anbar, A. Al-Ani, and D. R. Ibrahim, "Match-prevention technique against denial-of-service attack on address resolution and duplicate address detection processes in IPv6 link-local network," *IEEE Access*, vol. 8, pp. 27122–27138, 2020.

[20] O. E. Elejla, M. Anbar, S. Hamouda, S. Faisal, A. A. Bahashwan, and I. H. Hasbullah, "Deep-learning-based approach to detect ICMPv6 flooding DDoS attacks on IPv6 networks," *Appl. Sci.*, vol. 12, no. 12, p. 6150, Jun. 2022.

[21] A. Le, J. Loo, K. Chai, and M. Aiash, "A specification-based IDS for detecting attacks on RPL-based network topology," *Information*, vol. 7, no. 2, p. 25, May 2016.

[22] G. W. Kibirige and C. Sanga, "A survey on detection of sinkhole attack in wireless sensor network," 2015, *arXiv:1505.01941*.

[23] O. E. Elejla, M. Anbar, B. Belaton, and S. Hamouda, "Labeled flow-based dataset of ICMPv6-based DDoS attacks," *Neural Comput. Appl.*, vol. 31, no. 8, pp. 3629–3646, Aug. 2019.

[24] T. Eswari and V. Vanitha, "A novel rule based intrusion detection framework for wireless sensor networks," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2013, pp. 1019–1022.

[25] Y. EL Mourabit, A. Toumanari, A. Bouirden, H. Zougagh, and R. Latif, "Intrusion detection system in wireless sensor network based on mobile agent," in *Proc. 2nd World Conf. Complex Syst. (WCCS)*, Nov. 2014, pp. 248–251.

[26] A. Stephen and L. Arockiam, "Attacks against Rplin IoT: A survey," *Ann. Romanian Soc. Cell Biol.*, vol. 25, no. 4, pp. 9767–9786, 2021.

[27] V. Kaviani, "Efficient algorithm for feature intruder detection system," *Network*, vol. 3, no. 8, pp. 7–10, 2016.

[28] T. Parkavi and L. Arockiam, "A survey on sinkhole attack in RPL," *Ann. Romanian Soc. Biol.*, vol. 25, no. 5, p. 511–515, 2021.

[29] M. Alzubaidi, M. Anbar, Y.-W. Chong, and S. Al-Sarawi, "Hybrid monitoring technique for detecting abnormal behaviour in RPL-based network," *J. Commun.*, vol. 13, no. 5, pp. 198–208, 2018.

[30] G. Simoglou, G. Violettas, S. Petridou, and L. Mamatas, "Intrusion detection systems for RPL security: A comparative analysis," *Comput. Secur.*, vol. 104, May 2021, Art. no. 102219.

[31] P. Ioulianou, V. Vasilakis, I. Moscholios, and M. Logothetis, "A signature-based intrusion detection system for the Internet of Things," *Inf. Commun. Technol. Form*, 2018. [Online]. Available: https://eprints.whiterose.ac.uk/133312/1/ictf_2018_IoT.pdf

[32] V. Pandu, J. Mohan, and T. P. Kumar, "Network intrusion detection and prevention systems for attacks in IoT systems," in *Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems*. Hershey, PA, USA: IGI Global, 2019, pp. 128–141.

[33] J. Kaur, "An ultimate approach of mitigating attacks in RPL based low power lossy networks," 2019, *arXiv:1910.13435*.

[34] B. Mehtre, "RPL attacks and its mitigation methods," Dept. Comput. Sci., Semantic Scholar, 2019. [Online]. Available: https://www.semanticscholar.org/paper/RPL-ATTACKS-AND-ITS-MITIGATION-METHODS-Mehtre/edf7e3e263fc1b0579a3c86c3de2168b0154cad4

[35] 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.

[36] P. Bhale, S. Dey, S. Biswas, and S. Nandi, "Energy efficient approach to detect sinkhole attack using roving IDS in 6LoWPAN network," in *Proc. Int. Conf. Innov. Community Services*. Bhubaneswar, India: Springer, Jan. 2020, pp. 187–207.

[37] M. van Erp, L. Vuurpijl, and L. Schomaker, "An overview and comparison of voting methods for pattern recognition," in *Proc. 8th Int. Workshop Frontiers Handwriting Recognit.*, Aug. 2002, pp. 195–200.

[38] M. Zhao, A. Kumar, P. H. Joo Chong, and R. Lu, "A comprehensive study of RPL and P2P-RPL routing protocols: Implementation, challenges and opportunities," *Peer Peer Netw. Appl.*, vol. 10, no. 5, pp. 1232–1256, Sep. 2017.

[39] C. Zhang, M. Ye, L. Lei, and Y. Qian, "Feature selection for cross-scene hyperspectral image classification using cross-domain I-ReliefF," *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.*, vol. 14, pp. 5932–5949, 2021.

[40] Q. M. Alzubi, M. Anbar, Z. N. Alqattan, M. A. Al-Betar, and R. Abdullah, "Intrusion detection system based on a modified binary grey wolf optimization," *Neural Comput. Appl.*, vol. 32, pp. 6125–6137, May 2020.

[41] Z. S. Zubi, A. A. Elrowayati, and I. S. A. Fanas, "A movie recommendation system design using association rules mining and classification techniques," *WSEAS Trans. Comput.*, vol. 21, pp. 189–199, Jun. 2022.

[42] Q. M. Alzubi, M. Anbar, Y. Sanjalawe, M. A. Al-Betar, and R. Abdullah, "Intrusion detection system based on hybridizing a modified binary grey wolf optimization and particle swarm optimization," *Expert Syst. Appl.*, vol. 204, Oct. 2022, Art. no. 117597.

[43] T. A. Al-Amiedy, M. Anbar, B. Belaton, A. A. Bahashwan, I. H. Hasbullah, M. A. Aladaileh, and G. A. Mukhaini, "A systematic literature review on attacks defense mechanisms in RPL-based 6LoWPAN of Internet of Things," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100741.

[44] 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.

[45] A. Singh, S. C. Satapathy, A. Roy, and A. Gutub, "AI-based mobile edge computing for IoT: Applications, challenges, and future scope," *Arabian J. Sci. Eng.*, vol. 47, pp. 9801–9831, Jan. 2022.

[46] P. J. Prakash and B. Lalitha, "Optimized ensemble classifier based network intrusion detection system for RPL based Internet of Things," *Wireless Pers. Commun.*, vol. 125, no. 4, pp. 3603–3626, Aug. 2022.

[47] G. Rohini, C. G. Kousalya, and J. Bino, "Intrusion detection system with an ensemble learning and feature selection framework for IoT networks," *IETE J. Res.*, pp. 1–17, 2022, doi: 10.1080/03772063.2022.2098187.

[48] R. Alkanhel, E.-S. M. El-kenawy, A. A. Abdelhamid, A. Ibrahim, M. A. Alohali, M. Abotaleb, and D. S. Khafaga, "Network intrusion detection based on feature selection and hybrid metaheuristic optimization," *Comput., Mater. Continua*, vol. 74, no. 2, pp. 2677–2693, 2023.

[49] 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.

[50] J. Pokala and B. Lalitha, "A novel intrusion detection system for RPL based IoT networks with bio-inspired feature selection and ensemble classifier," Res. Square, Jawaharlal Nehru Technol. Univ. Anantapur, 2021. [Online]. Available: https://assets.researchsquare.com/files/rs-442429/v1_covered.pdf?c=1631865048

[51] A. Bahaa, A. Abdelaziz, A. Sayed, L. Elfangary, and H. Fahmy, "Monitoring real time security attacks for IoT systems using DevSecOps: A systematic literature review," *Information*, vol. 12, no. 4, p. 154, 2021.
[52] N. Singh and D. Virmani, "Computational method to prove efficacy of datasets," *J. Inf. Optim. Sci.*, vol. 42, no. 1, pp. 211–233, Jan. 2021.

SHADI AL-SARAWI received the M.Sc. degree from Arab Academy for Banking and Financial Sciences, Jordan, in 2004. He is currently pursuing the Ph.D. degree with the National Advanced IPv6 Center (NAv6), Universiti Sains Malaysia. His research interests include intrusion detection systems (IDS), 6LoPAN, the Internet of Things (IoT) attacks, and routing protocol for low-power and lossy networks (RPL) security.

MOHAMMED ANBAR (Member, IEEE) received the B.Sc. degree in software engineering from Al-Azhar University, Palestine, in 2008, the M.Sc. degree in information technology from Universiti Utara Malaysia, in 2009, and the Ph.D. degree in advanced internet security and monitoring from Universiti Sains Malaysia (USM), in 2013. He is currently a Senior Lecturer with the National Advanced IPv6 Centre (NAv6), USM. His current research interests include malware detection, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), network monitoring, the Internet of Things (IoT), software-defined networking (SDN) security, cloud computing security, and IPv6 security.

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.

MOHAMMAD ADNAN ALADAILEH received the Ph.D. degree in internet infrastructure security from University Sains Malaysia (USM). He is currently an Assistant Professor with the American University of Madaba. His current research interests include computer networks, network security, the Internet of Things (IoT), intrusion detection systems (IDS), intrusion prevention systems (IPS), and software defined networking (SDN).

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 systems from 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.