Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.040756

ARTICLE

Collaborative Detection and Prevention of Sybil Attacks against RPL-Based Internet of Things

Muhammad Ali Khan[1], Rao Naveed Bin Rais[2,*] and Osman Khalid[1]

[1]Department of Computer Science, COMSATS University Islamabad, Abbottabad Campus, Abbottabad, Pakistan

[2]Artificial Intelligence Research Center (AIRC), Ajman University, Ajman, United Arab Emirates

*Corresponding Author: Rao Naveed Bin Rais. Email: r.rais@ajman.ac.ae

Received: 29 March 2023 Accepted: 01 August 2023 Published: 31 October 2023

ABSTRACT

The Internet of Things (IoT) comprises numerous resource-constrained devices that generate large volumes of data. The inherent vulnerabilities in IoT infrastructure, such as easily spoofed IP and MAC addresses, pose significant security challenges. Traditional routing protocols designed for wired or wireless networks may not be suitable for IoT networks due to their limitations. Therefore, the Routing Protocol for Low-Power and Lossy Networks (RPL) is widely used in IoT systems. However, the built-in security mechanism of RPL is inadequate in defending against sophisticated routing attacks, including Sybil attacks. To address these issues, this paper proposes a centralized and collaborative approach for securing RPL-based IoT against Sybil attacks. The proposed approach consists of detection and prevention algorithms based on the Random Password Generation and comparison methodology (RPG). The detection algorithm verifies the passwords of communicating nodes before comparing their keys and constant IDs, while the prevention algorithm utilizes a delivery delay ratio to restrict the participation of sensor nodes in communication. Through simulations, it is demonstrated that the proposed approach achieves better results compared to distributed defense mechanisms in terms of throughput, average delivery delay and detection rate. Moreover, the proposed countermeasure effectively mitigates brute-force and side-channel attacks in addition to Sybil attacks. The findings suggest that implementing the RPG-based detection and prevention algorithms can provide robust security for RPL-based IoT networks.

KEYWORDS

RPL; Internet of Things; RPG; Sybil attack

1 Introduction

Internet of Things (IoT) consists of static and mobile nodes equipped with sensing, storage, processing and actuation modules connected via Internet communication protocols enabling pervasive communication [1]. IoT services, such as smart transportation, smart grid, smart homes, smart cities, etc., play a significant role in improving quality of life with easy access to information for intelligent decision making [2]. It is reported in [3] that by the end of 2025, 75.44 billion devices will be deployed and used across the world. The economic impact of the IoT market is expected to reach as high as $11 trillion by 2025 with a major portion from business and industrial applications [4]. Despite

several advantages, IoT networks face numerous challenges due to having limited resources in terms of processing power, memory and energy. IoT networks often operate on Low-power and Lossy wireless Networks (LLN) [5,6]. Traditional protocols optimized for wired or high-bandwidth networks may not be suitable for the intermittent connectivity, high packet loss and constrained energy of IoT environments. Moreover, due to limited resources, implementing complex and computationally intensive security mechanisms is a challenging task, which can leave routing protocols vulnerable to attacks.

To address the routing challenges in IoT environments, the Routing Protocol for Low-Power and Lossy Networks (RPL) [7] was standardized by Internet Engineering Task Force (IETF) in 2008 [8] and is one of the primary routing protocols for communication in IoT. RPL fulfills IoT network routing requirements and reduces resource consumption along the routing paths by prioritizing energy efficiency, scalability and adaptability to lossy networks. It supports point-to-point, point-to-multipoint and multipoint-to-point communication. RPL is a proactive distance-vector routing protocol based on IPv6 for LLNs and supports routing over a 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks) environment. It builds a Destination Oriented Directed Acyclic Graph (DODAG) with a single root and uses the objective function to rank nodes in the graph, which is based on their distance from the root node. The rank is increased by the Low-power and the lossy network Border Router (LBR) at which Directed Acyclic Graph (DAG) is grounded. In the DODAG structure, the constrained nodes use RPL control messages for neighbor discovery and to discover an RPL instance and join it. A node forwarding a packet to LBR selects a node with the lowest rank [9]. One or more LBRs, and the connected nodes, create an RPL instance that is uniquely identified. An RPL topology contains multiple RPL instances and hence, multiple DODAGs, each uniquely identified with DODAG ID (IPv6 address of the root). The nodes in the topology store the routing information in their routing table and forward the data to the root node.

1.1 Problem Statement

RPL efficiently maintains routes and can operate in harsh environments under lossy links with less overhead. Although RPL offers security options to protect its control messages and network privacy, it lacks inherent security mechanisms because it was not designed to operate under the security requirements for cyber-attacks. Moreover, the security options it provides are optional to implement since it greatly affects the performance of IoT devices constrained on resources [10]. Because RPL mostly operates under wireless media and is based on IPv6 open stack, it is exposed to a large number of cyber-attacks [11]. The sensor nodes are not immune to manipulations, making it possible for intruders to launch different routing attacks such as Sybil attacks [12], selective forwarding attacks and blackhole attacks, to name a few. In addition to RPL issues, the nature of IoT infrastructure, Internet Protocol (IP) and Media Access Control (MAC) addresses are vulnerable and can easily be spoofed [13], resulting in various attacks including Sybil attacks. A Sybil attack is an attack against identity in which an individual entity deceives other nodes by carrying multiple simultaneous identities. Sybil attack decreases the packet delivery ratio, increases network overhead and consumes more energy. Hence, it is considered a big threat to RPL mainly due to its DODAG structure [14]. As a Sybil node joins a network, it gets a rank value that describes its position in the DODAG. To join the network, the Sybil node sends a control message to its neighbor, which is further relayed to the LBR. The LBR returns the information of all the nodes in the network and their positions to optimize routing, recognize rank level and become synchronized with its neighbor nodes. However, the Sybil node collects all the information and intentionally misreports (decreases or increases) its rank in the network [15]. When the Sybil node decreases its rank, it could manipulate a large amount of traffic

flowing through it and could pretend to be falsely situated close to the root node. When it increases its rank, it eventually disrupts the network topology and depletes the neighbor nodes' resources [16].

1.2 Research Motivation

For the mitigation of Sybil attacks, several approaches have been proposed in the existing literature. A few of the techniques utilized trust-based mechanisms to counter Sybil attacks [12,16–19]. However, a collaboration among neighbors required to detect intrusion in trust-based approaches, takes time, hence increasing latencies in large-scale networks. Moreover, the complex trust establishment requires significant computation resources, resulting in additional overhead and affecting the network performance and scalability. Such complex calculations may not be feasible for resource constrained IoT devices. Some mechanisms, such as [18], use trusted platform module but their reliance on cryptographic protocols make them unsuitable for implementations on IoT devices.

Besides, there are several statistical estimation-based schemes, e.g., [14,20], also presented in the existing literature. However, one of the problems with statistical-based techniques is that they often require initial parameters and perform complex calculations that cannot be run directly on resource-constrained nodes. In addition to trust-based and statistical estimation-based security mechanisms, some recent approaches use monitoring techniques to monitor the network traffic for anomaly detection. However, this introduces additional overhead because of continuous monitoring of the network, which can potentially generate false positive alarms leading to additional overhead and network downtime. Moreover, monitoring a large number of message exchanges between nodes results in significant energy consumption.

To fill the gap in the existing literature, a lightweight mechanism is required to secure RPL without imposing overheads on the network, which is proposed in this paper. The proposed countermeasure approach saves significant energy compared to the distributed defense mechanism and improves the network throughput. Moreover, the proposed countermeasure is effective against brute-force and side-channel attacks in addition to Sybil attacks.

1.3 Contributions

To overcome the issues discussed in the previous subsection, this paper proposes and evaluates a centralized and collaborative detection and prevention mechanism named Random Password Generation and Comparison (RPG) against Sybil attacks in RPL-based IoT. In RPG, a Random Key and Password Generator (RKPG) module is installed at the root node and sensor nodes. At the root node, the RKPG module creates and assigns a constant ID, referred to as node ID for each node in the network. Moreover, a random key is also generated for every node. When nodes start communicating with each other, a random password for the nodes based on their keys is generated by the RKPG module. During communication, the nodes' IDs and passwords are compared for detecting Sybil nodes in the network. A sensor node maintains a k_table that holds its node ID, key and password. In addition, the sensor node also maintains a s_table for updating the list of Sybil nodes in the network. A source node communicating with the destination node first sends its node ID and key for verification to the cluster head. The cluster head allows communication between nodes upon successful verification. Otherwise, a node is considered to be a compromised node. The detection algorithm checks the password of the compromised nodes. Failing the password check confirms the detection of a node as a Sybil node. Moreover, the prevention algorithm uses the time delay metric to prevent Sybil nodes' participation in communication.

The proposed system prevents node ID spoofing by assigning nodes the IDs that remain constant throughout the lifetime of the network. A whitelist of genuine nodes and a blacklist of Sybil nodes are maintained by the nodes that help in recreating routes from the source node to the destination node. The proposed work aims to enhance the overall security and reliability of IoT devices. Moreover, the benefits of research in this area extend to various stakeholders, e.g., IoT device manufacturers, network operators, application developers, end users, researchers and society at large with significant economic impact.

The main contributions of this paper are as follows:

- A centralized and collaborative countermeasure is proposed against Sybil attacks to improve the network throughput in the RPL-based (IoT).
- The first line of defense is deployed on a central root node to avoid node ID spoofing as is with the case of MAC and Internet Protocol (IP) addresses. This significantly saves energy consumption compared to the distributed defense mechanisms.
- A collaborative approach between the sensor nodes and the cluster heads is presented for speedy and efficient detection and prevention of Sybil nodes' participation in the communication. This also helps in preventing selective forwarding attacks and blackhole attacks.
- The proposed countermeasure demonstrates improvement in results when compared with the state-of-the-art in terms of throughput, packet delivery delay ratio and detection rate. The experimental results show that the proposed technique delivers nearly 100% more packets than the baseline with a low delivery delay ratio. Moreover, the detection rate improves as the number of nodes increases in the network.
- A security analysis of the proposed approach is presented to test its effectiveness in combatting side-channel attacks and brute-force attacks in addition to Sybil attacks.

The rest of the paper is organized as follows: In Section 2, the related work is presented. In Section 3, the details of the detection and prevention mechanism of Sybil's attack in RPL are described. In Section 4, the performance evaluation of the proposed methodology is presented. In Section 5, the security analysis of our system is presented. Finally, the conclusion and future work is presented in Section 6.

2 Literature Review

This section discusses a few state-of-the-art schemes for defense against Sybil attacks in IoT environments. In [21], the authors have used the Bloom filter, a probabilistic data structure and a Physical Unclonable Function (PUF) to detect Sybil attacks with low computational overhead and high accuracy. The Bloom filter detects unauthorized nodes in the network and stores their identities. The PUF generates unique and unclonable identifiers for each node in the network to distinguish between legitimate and Sybil nodes. Results show that the approach detects the Sybil attacks with a low false positive rate and high accuracy. However, the high cost and implementation challenges of PUF make it difficult to implement at scale in large IoT networks. Moreover, it is not compared with other state-of-the-art detection approaches and does not consider the prevention technique.

The authors in [22] proposed a trust-based routing scheme to address Sybil attacks in RPL-based IoT networks. The approach uses physical identification (PID) technology that involves the unique physical characteristics of the device, such as the device's MAC address or Radio Frequency Identifier (RFID). The PID technology authenticates the device and establishes trust between nodes in the network. Simulation results show that the proposed approach effectively detects and prevents

Sybil attacks in IoT networks with low communication overhead and energy consumption, making it suitable for use in low-power IoT devices. However, it heavily relies on PID technology that may not be commonly available. Moreover, the complex trust establishment requires significant computation resources resulting in additional overhead affecting the network performance and scalability.

In [23], the authors proposed a lightweight trust-enabled routing scheme to detect and prevent Sybil attacks in RPL-based IoT. Each node calculates the trustworthiness of other nodes based on the packet forwarding history and reliability of nodes. All the nodes in the network maintain a trust table to store the trustworthiness values. Moreover, it uses a cluster-based approach to prevent Sybil attacks. The nodes with the same trust level reside in the same cluster. The cluster head manages the communication. Simulation results show efficient Sybil attack detection and prevention with low overhead and energy consumption. However, the proposed method uses a complex calculation mechanism to calculate the trust level of each node, which may not be feasible for resource constrained IoT devices.

In [24], the authors proposed a DETONAR module that continuously monitors the network and alerts the network administrator when Sybil attacks are detected. The proposed solution analyzes the behavior of neighbor nodes to detect anomalies and Sybil nodes in addition to the node's cryptographic identity and MAC address. The administrator takes the necessary actions to prevent the Sybil attack. However, it introduces additional overhead because of continuous monitoring of the network. It can also potentially generate false positive alarms leading to additional overhead and network downtime.

A time-based trust-aware RPL routing protocol (SecTrust-RPL) was proposed in [16] to detect Sybil and Rank attacks in IoT. SecTrust-RPL includes the Trust calculation, Trust monitoring update and Trust rating processes embedded into the RPL protocol. Each node is evaluated by other nodes based on dependability, reliability, recommendations and competence resulting from the interactions among the nodes. The proposed protocol is practically deployed on a small-scale smart home testbed and the performance is compared with simulation results.

In [25], Sybil attacks against IoT were characterized into three types according to the capabilities of Sybil attackers. The authors presented a comprehensive comparison between mobile Sybil detection, behavior classification-based Sybil detection and social graph-based Sybil detection schemes. Although very informative, the paper does not discuss the Sybil attacks in the context of RPL-based IoT.

Topology-based attacks on RPL for IoT were detected in [18]. The authors obtained an RPL specification by semi-auto profiling technique that traces operations through the network and uses it as a reference for verifying node behaviors. The obtained RPL specification and the protocol states are implemented as a set of rules in cluster heads that serve as Intrusion Detection System (IDS) agents. Their mechanism is only used to detect RPL attacks and further reliance on cryptographic protocols is recommended for the prevention of such attacks.

An IDS for IoT called SVELETE was proposed in [26] to detect sinkholes and selective-forwarding routing attacks. The IDS include 6LoWPAN Mapper (6Mapper) capable of reconstructing RPL DODAG in 6LoWPAN Border Router (6BR) and is used in three detection techniques to counter the routing attacks. The 6Mapper only considers the information that is latest from all the hosts in the network. Although the proposed work claims to have protection against clone ID attacks and Sybil attacks, the claim is not supported by any evidence or simulations.

In [19], the authors proposed a Trust-based IDS (T-IDS) that detects intrusions by comparing network behavior deviations. T-IDS is distributed and cooperative system and each node in the network not only monitors the network but works in collaboration with neighbor nodes to report deviations to 6BR. RPL message format is extended to handle mobility, identity and multicast issues. The trusted Platform Module works on each node to handle offloaded security-related computation, storage and identification.

A novel attack, named Sybil-Mobile attack exploits the lack of a strong identity mechanism in the RPL [27]. This Sybil attack floods the network with fake control messages from different locations, hence indicating the lack of strong security and identity mechanisms in RPL. The impact of the Sybil-Mobile attack on RPL is evaluated using energy consumption, packet delivery and control overhead metrics.

A secure routing protocol based on RPL, referred to as Secure-RPL (SRPL), was proposed in [28]. The protocol prevents misbehaving nodes from maliciously modifying control messages, so that they may not disturb the network by creating a fake topology. The concept of rank threshold is introduced along with the hash chain authentication technique to deal with internal attacks like fake identity, sinkhole, etc. Their approach consists of three phases namely the initiation phase, verification phase and rank update phase. The proposed approach is simulated to show the effectiveness of SRPL in case of attacks based on malicious manipulation of RPL metrics. However, the proposed approach is not verified explicitly against the Sybil attack and hence lacks its contribution toward any significant improvement in the case of fake and multiple identities.

The authors in [29] provided a comprehensive analysis of the Sybil attack on IoT. The model classifies the entire process of a Sybil attack into three phases namely, compromise, deployment and launching phase, based on the attack operations. Although the proposed model helps understand the Sybil attack phases and the possible actions for each state, it is challenging to adapt it in the RPL-based LLNs where all the nodes are energy-constrained [14]. A distributed approach using the traffic flow theory to detect Sybil attacks in VANETs was proposed in [30]. The proposed scheme requires monitoring of a large number of message exchanges between the vehicles resulting in significant energy consumption.

3 Proposed Methodology

In this section, the working of RPG in RPL-based IoT is presented. The following types of nodes are considered in the paper: (a) root node (b) cluster head node and (c) sensor node. The methodology includes the following modules: (3.1) Detection algorithm and (3.2) Prevention algorithm. The description of these modules is presented as follows:

3.1 Detection Algorithm

The primary objective of the detection algorithm is to detect the Sybil nodes. The algorithm consists of the operations running on the root node and sensor nodes.

3.1.1 Operations at the Root Node

The root node deploys the first line of defense for detecting Sybil nodes. The Authenticated Mode of RPL is considered, where a root node provides keys to newly joining nodes entering DODAG. All the nodes in the network use the RKPG module. At the root node, the RKPG module generates

an alphanumeric random key and node ID for every node in the network. The node ID assignment is in addition to the IPV6 address and never changes throughout the lifetime of the node and the network. A new node without a key and a node_ID cannot join DODAG. The root node maintains the network topology and the database of participating peers in RPL IoT. A node communicates with the root node for a couple of reasons, such as for its key and node_ID allocation, for calculating its rank according to the root node if it is the adjacent node to the root node and for the validation of its key and node_ID if it is disconnected and rejoining. A rejoining node uses Destination Advertisement Object (DAO) control message to send its assigned key for verification and advertise its position in the topology. The root node protects its database by using an access control mechanism that authenticates the key and node_ID of a node in a communication request from the node. In addition to this access control mechanism at the root node, the security associations (SAs) feature of RPL security is utilized to ensure a secure communication channel between participating nodes so that only the authenticated nodes are authorized to communicate. Hence, it becomes difficult for the nodes to gain control of the database at the root node and disrupt the network operations.

3.1.2 Operations at the Sensor Nodes

The sensor node saves the node ID and key in its k_table. The RKPG module at the sensor nodes uses this key and generates a random password for the sensor node at run time during communication in the network. The password is regenerated periodically by each node in the network.

3.1.3 Operations at the Cluster Head Nodes

A node operates under the control of cluster head nodes (referred to as CH in the rest of the paper). In the upward route, from the nodes to the CH and further, towards the root node, the CH stores the node ID and key of the nodes in its k_table in the storing mode. The maintenance of k_table at the CH is possible with the help of DAO control messages. If a node needs to communicate with another node in the network, it sends a request to the CH. The CH compares the node ID and key of the node with entries in its k_table. This operation finds the compromised nodes in the network. The CH labels a node as compromised before confirming it as a Sybil node because of a possibility that the root node has not yet verified its node ID due to intermittent disconnection. In such a case, a CH matches the key and associated password of a compromised node in the k_table. A node is detected as a Sybil node if it fails the verification process. The CH updates the s_table and shares the blacklist using the RPL Destination Information Object (DIO) control message that is shared periodically with the nodes. The flow diagram in Fig. 1 shows the working of the detection algorithm for detecting Sybil attacks in RPL-based IoT and Algorithm 1 presents the detection algorithm.

The detection of the Sybil node is depicted in Fig. 2. In Fig. 3, the sender is represented by ‘S’ and the destination is represented by ‘D’. There exist two routes, i.e., one created by the Sybil node and is shown in a dashed line and the other route represented by a solid line is safe. The proposed algorithm successfully detects the Sybil nodes and avoids the route created by the Sybil node and follows the safe route in conjunction with the RPL feature that enables the sensor nodes to discover each other and build paths in the network.

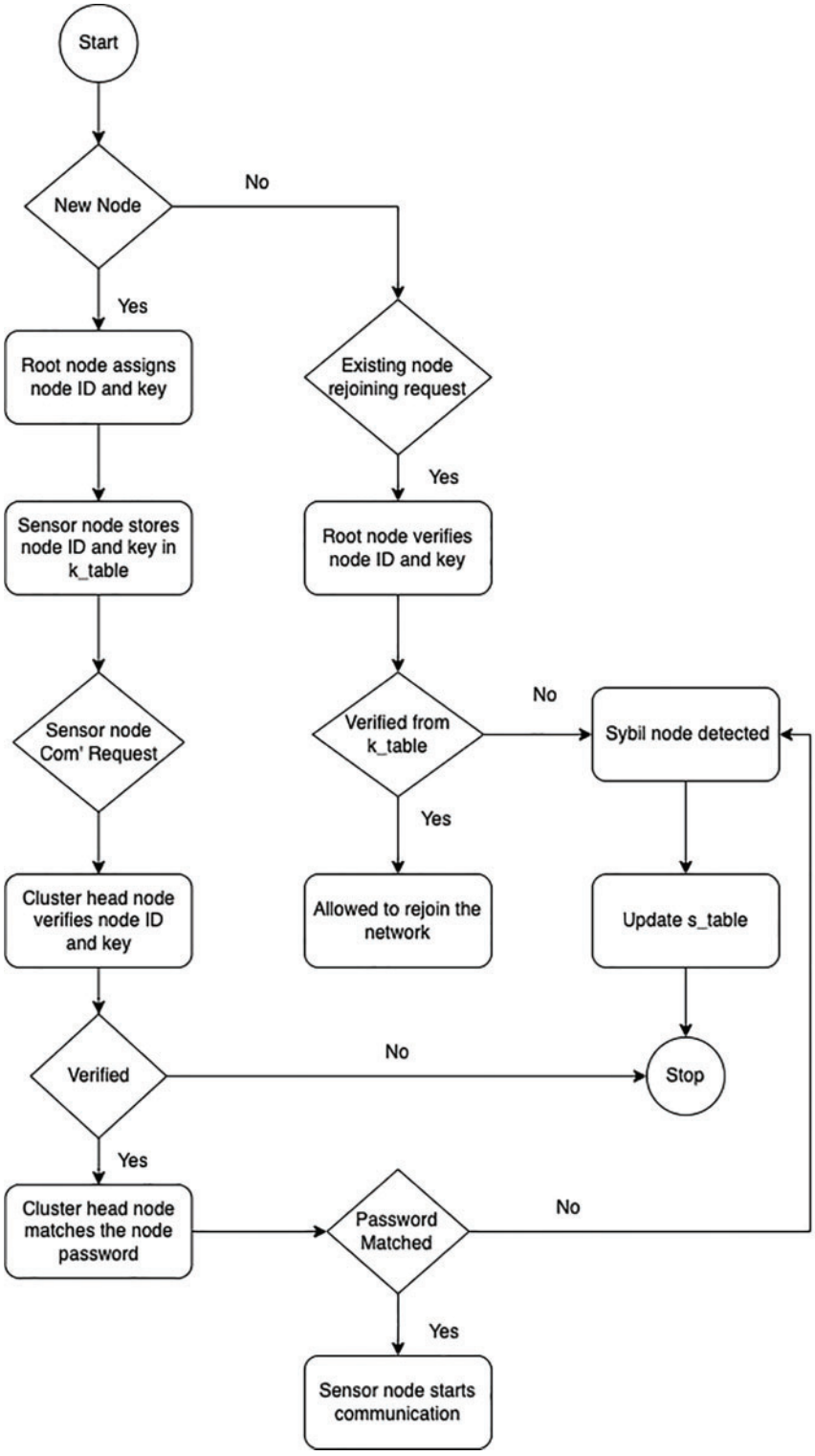

Figure 1: Flow chart of the detection algorithm

Algorithm 1: The Detection Algorithm

1: The root node creates and assigns node ID and key for each node in the network
2: The sensor node stores the assigned key and node ID in its k_table
3: A password is created at the sensor node using its key
4: The sensor node sends the node ID and key to the cluster head to request for communication
5: The cluster head node compares the node ID in the k_table
5.1: If the sender node ID matches, then the cluster head sends a message to the destination.
5.2: Otherwise stop and label the node as compromised
5.3: The sensor node password is checked for confirming it as Sybil node
5.4: If confirmed as Sybil node, then update s_table

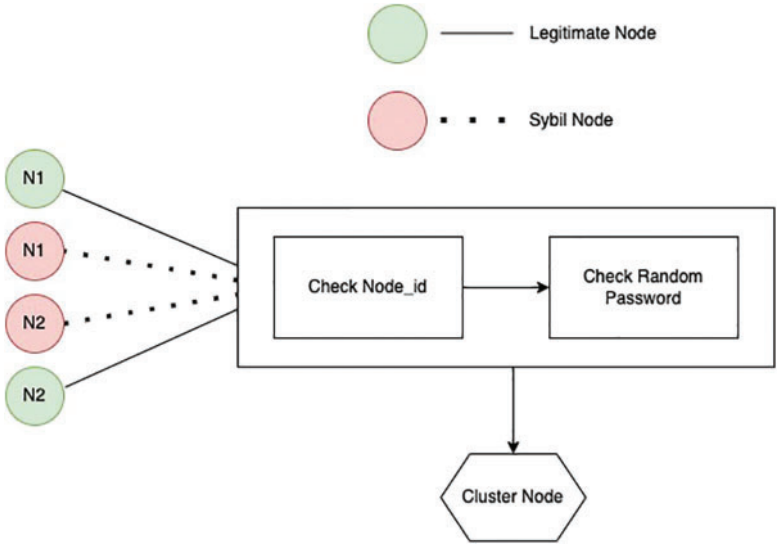

Figure 2: Detecting Sybil nodes

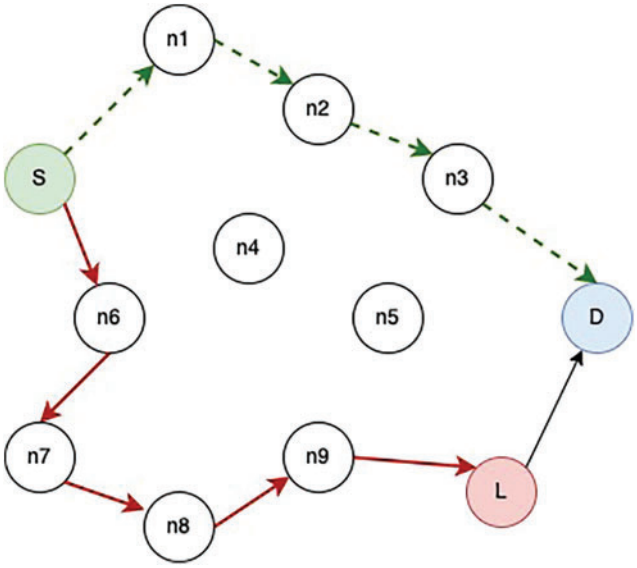

Figure 3: Avoiding routing path containing Sybil nodes

3.2 Prevention Algorithm

The prevention algorithm (Algorithm 2) works with the detection algorithm to avoid extra computation. It uses node ID, password and time delay metrics to prevent Sybil node participation in the network. Upon suspecting a node as a Sybil node, the prevention algorithm checks the time delay of a node in sending messages. It calculates the time delay for a node relative to the root node and their neighbor nodes. Abnormal time delay further confirms the detection of a Sybil node. The prevention algorithm updates the s_table at the CH and shares the blacklist using the RPL DIO control message that is shared periodically in the range of nodes. Table 1 provides sample data containing the node IDs assigned to the nodes, the passwords generated for sensor nodes against their keys and the time delay in sending messages. The sensor nodes with constant IDs, labeled as D, E and F in Table 1 are Sybil nodes since their time delay in sending messages is abnormal compared to the average time delay in communication.

Algorithm 2: The Prevention Algorithm

1: If the detection algorithm suspects a node as a Sybil node, then the time delay of nodes is checked
2: The destination node D sends a request message to sender node S
3: The time delay of a sender and receiver node is checked
4: S and D nodes will find the route between the nodes through the sub-function DISROUT(S, D)
5: If the path is verified then S will send data otherwise the node will be placed in Sybil table s_table

Table 1: Parameters considered in prevention algorithm

node ID	Time delay	Password
A	1.00	aDsY
B	1.04	FFsa
C	1.08	Jj12
D	2.00	sDTG
E	2.01	IKU2
F	2.00	Se45
G	1.05	KUI3

4 Performance Evaluation

The Sybil attack is implemented in the RPL protocol using the Contiki operating system [31], a well-known operating system for IoT. These attacks are demonstrated in the Cooja simulator [32]. RPL protocol is inspected in the 6LoWPAN IoT environment by exploring the Sybil attack and applying the proposed detection and prevention algorithms to detect Sybil attacks in RPL-based IoT. Table 2 shows the notations and their meanings used in this section.

Table 2: Notations and meanings

Notation	Meaning
RPL	Routing Protocol for Low-Power and Lossy Networks
IoT	Internet of Things

(Continued)

Table 2 (continued)

Notation	Meaning
6LoWPAN	IPv6 over Low Power Wireless Personal Area Networks
QoS	Quality of Service
CAM-PVM	Compare and Match-Position Verification Method
MAP	Message Authentication and Passing
AODV	Ad hoc on Demand Distance Vector
RPG	Random Password Generator

4.1 Performance Metrics

The performance of the proposed methodology is assessed in terms of three Quality of Service (QoS) parameters, i.e., the detection rate of Sybil nodes, throughput and packet latency. These QoS parameters are defined as follows.

4.1.1 Throughput

It is the amount of data that can be transmitted successfully over the network in a period. The following formula calculates the throughput.

$$T = \frac{P_t}{t_s} \times P_s, \tag{1}$$

where t is the throughput, P_t is the number of packets successfully transmitted over the network, t_s is the total time taken for the transmission and P_s is the packet size.

4.1.2 Average Delay

The average delay for a sensor node is the average of all delays the sensor node encounters when sending packets. The difference between the time at which the packet was received and the sending time defines a packet delay.

$$D_{avg} = \frac{\sum_{d=1}^{n} P_d}{d}, \tag{2}$$

where D_{avg} is the average delay and d is the number of packets.

4.1.3 Detection Rate

The network topology is implemented with the legitimate nodes and the Sybil nodes. Simulations are performed to obtain the accurate performance of the detection algorithm. The following formula calculates the detection rate at which the Sybil nodes are detected.

$$S_r = \frac{S_d}{S_n} \times 100\%, \tag{3}$$

where S_r is the Sybil node detection rate, S_d is the number of Sybil nodes detected, S_n is the total number of Sybil nodes.

4.2 Baselines

Although, there exist methodologies in the recent literature that detect and prevent Sybil attacks in RPL-based IoT, however, they deal with mobile Sybil attacks. Therefore, our methodology is compared with the two baselines, namely [33]: (a) Compare and Match-Position Verification Method (CAM-PVM) and (b) Message Authentication and Passing (MAP) algorithm. These methods detect and prevent Sybil attacks in wireless sensor networks. Moreover, the selected baselines considered directed acyclic graphs in wireless sensor networks which is an exact match to the graph dealt with in RPL instances. A brief explanation of the baselines is as follows.

4.2.1 CAM-PVM

In [33], the authors assumed that all the nodes in the network are energy efficient. All the nodes in the network receive a HELLO message from the root node. The nodes respond by sending their ID, timestamp and location. An Ad hoc On-Demand Distance Vector (AODV) routing protocol is implemented for route discovery through an N-hop intermediate nodes. A routing table stores the information of nodes during route discovery. The authors used CAM-PVM for Sybil node detection during route discovery. During route discovery, the algorithm compares the ID, timestamp and location with the information in the routing table. A node is detected as a Sybil node if it fails the verification process.

4.2.2 MAP

A MAP algorithm is used for Sybil node prevention in the network for the mitigation of Sybil attacks. On network creation, a sender node sends its key issued by the root node to the destination node. The destination node also sends its key issued by the root node. The communication starts if the base station verifies these keys.

4.3 Results

In this subsection, the simulation results of the proposed scheme compared to the baselines are presented. As the IoT-systems are usually deployed in a wide variety of real-world environments, this can introduce variability in terms of device capabilities, network connectivity and data traffic patterns. Therefore, it can be challenging to simulate this variability in a controlled and repeatable way. Moreover, simulating large-scale deployments of such devices in dynamic network environments can be computationally expensive, requiring significant computational resources.

The proposed methodology and the baselines considered in this paper are all implemented with RPL in the Contiki operating system, and the results are demonstrated in the Cooja simulator. The topology comprises 22 nodes of which ten are legitimate, ten are compromised and two are Sybil nodes.

4.3.1 Throughput

The throughput comparison is presented in Fig. 4 which shows the effectiveness of our methodology in delivering a maximum number of packets during communication. Compared to the baselines, the proposed scheme exhibits stable throughput values despite the network variabilities. This is because the proposed methodology is efficiently maintaining the blacklist, i.e., Sybil nodes' information and avoids delivering packets on the routes created by Sybil nodes, where packet loss occurs resulting in degradation in the network performance. The simulation results for throughput show that our methodology delivers nearly 100% more packets than the baselines.

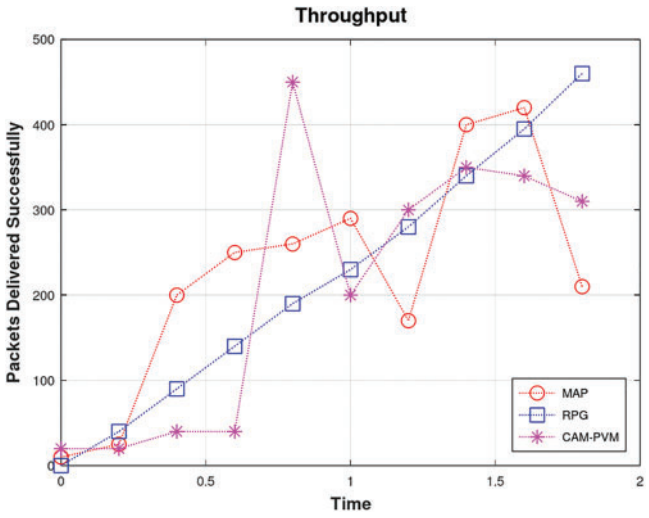

Figure 4: Throughput comparison of RPG with CAM_PVM and MAP

4.3.2 Latency

The throughput results can be verified by the fact that the latency of our proposed methodology (shown in Fig. 5) is much less as compared to the baselines. This is because the maintained whitelist and malicious list help in faster communication between the source node and destination node as it avoids the routing paths involving Sybil nodes.

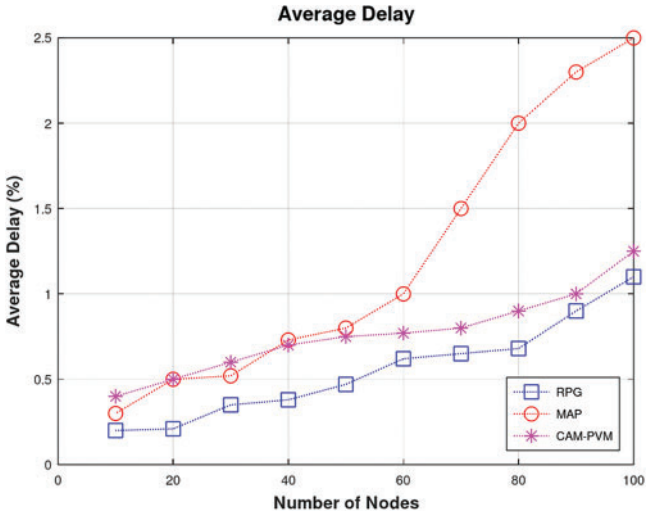

Figure 5: Average latency in delivering packets RPG *vs.* CAM_PVM and MAP

4.3.3 Detection Rate

Fig. 6 indicates the performance comparison of our proposed methodology in terms of detection rate of the Sybil nodes. Fig. 6 also shows the scalability performance of the proposed method. It can be observed that almost up to the middle of the graph, the detection rate of Sybil nodes is comparable to the baselines. However, the detection rate improves as the number of nodes increases in the network,

which shows that the proposed scheme is scalable. This is because the nodes initially require a specific period to maintain the blacklist (also known as warmup time). Once the list is updated, the information is shared with the network's new nodes. Overall, this improves the detection rate at later rounds in the simulation run.

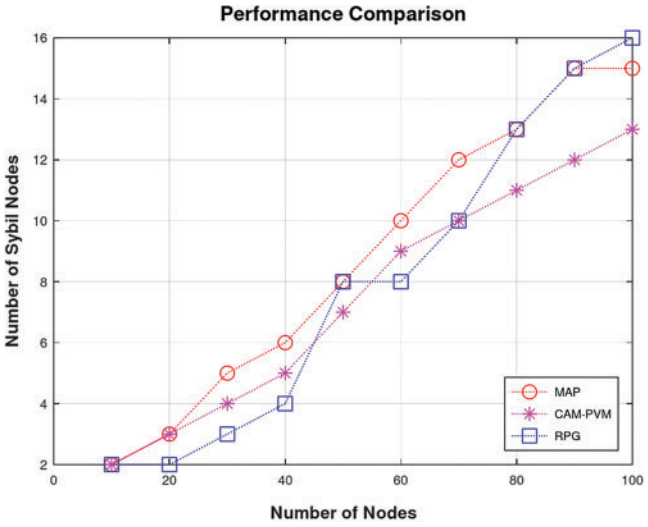

Figure 6: Performance comparison of RPG with CAM_PVM and MAP

5 Security Analysis

This section presents the security analysis of the proposed scheme. Due to the dynamic and heterogeneous environments of IoT, complexities of network topology, device types, complex interactions of devices, communication patterns and lack of standardization in performance parameters, it is challenging to perform a quantitative security analysis of the proposed work. Therefore, a qualitative analysis is presented in terms of how the proposed system is capable of defending against the following different types of attacks.

5.1 Sybil Attack

- **Attack scenario:** The attacker intentionally broadcasts excessive DODAG Information Solicitations (DIS) packets with fake node identifiers. When a genuine node receives DIS packets from the attacker, it has to reset its DIO Trickle timer repeatedly and broadcast DIO packets. This results in extensive consumption of battery energy.
- **Proposed solution:** The proposed system is resistant to Sybil attacks. If an attacker node impersonates a legitimate node, it will never be able to join the network because of the duplicate node ID with different ranks. The communication between participating peers in the network requires a password generated by the RKPG module. If an attacker node somehow impersonates the legitimate node in the network, it cannot communicate with peers because it cannot copy the RKPG module. Therefore, it becomes difficult for the attacker node to impersonate a legitimate node.

5.2 Side-Channel Attack

- **Attack scenario:** The attacker attempts to extract the node ID and key of the sensor node during communication to gain unauthorized access. It disrupts the network routing protocol and compromises the integrity of the data transmitted.
- **Proposed solution:** The SAs feature of RPL security mitigates such attempts by ensuring a secure communication channel between participating nodes so that only authenticated nodes are authorized to communicate. Despite SAs, if an attacker gets the node ID and key of a node by analyzing and intercepting network traffic, it will not be able to generate a password that is required for the sensor nodes during communication requests and authorization.

5.3 Brute-Force Attack

- **Attack scenario:** The attacker tries every possible combination of keys and passwords to gain unauthorized access to a network.
- **Proposed solution:** Our detection algorithm uses random passwords to increase the level of randomness in the network and reduces the risk of password-guessing and brute-force attacks. The purpose of using random passwords in the detection algorithm is to make it difficult for Sybil attackers to create and maintain multiple fake identities since the sensor nodes require passwords to join the network and participate in the communication.

6 Conclusion

This paper focuses on the security of RPL-based IoT systems. A centralized and collaborative approach is presented for the detection and prevention of Sybil attacks in RPL-based IoT networks. The first line of defense deployed on the root node tackles the problem of IP and MAC address spoofing by creating and assigning constant IDs and keys to sensor nodes using the RPKG module. The collaboration between cluster head nodes and sensor nodes detects the Sybil nodes and prevents their participation in communication. Simulations show that the successful detection of Sybil nodes results in high throughput and a low average delay in delivering packets. Moreover, the proposed countermeasure significantly saves energy consumption compared to the distributed defense mechanisms. In addition, the proposed approach works efficiently against selective forwarding attacks, brute-force attacks and side-channel attacks.

There are some limitations and tradeoffs of the proposed work, however. If there are frequent intermittent disconnections, users may face increased latency. This is because when a sensor node disconnects from the network and wants to rejoin, the root node first verifies the identity of the sensor node, thus causing some delay. Moreover, the cluster head node only allows communication between sensor nodes when it verifies their ID, key and password. This increased latency is not suitable for time sensitive IoT applications, such as monitoring a heart patient in a remote area. In addition to increased latency, the root node and cluster head nodes experience increased processing overhead.

In future, the authors plan to develop a testbed for deploying a small-scale real network composed of motes to see the accuracy and output of our proposed solution. Moreover, the solution will be tested considering mobility in the network, along with other routing protocols whose design is specialized for IoT networks.

Acknowledgement: The authors are thankful to colleagues for helping in the finalization of this paper.

Funding Statement: The work in the paper is funded by Ajman University, UAE under the Project Grant ID: 2022-IRG-ENIT-4, received by R.N.B.R., https://www.ajman.ac.ae/.

Author Contributions: The authors confirm contribution to the paper as follows: conceptualization: M.A. and O.K.; methodology: M.A. and R.N.B.R.; software: M.A.; validation: M.A., O.K. and R.N.B.R.; formal analysis: M.A.; investigation: O.K. and R.N.B.R.; resources: O.K. and R.N.B.R.; writing—original draft preparation: M.A.; writing—review and editing: O.K. and R.N.B.R.; supervision: O.K. and R.N.B.R; funding acquisition: R.N.B.R. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The authors did not use any external data for this work. The data is generated in real-time through the simulator.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] H. Kopetz and W. Steiner, "Internet of Things," in *Real-Time Systems*, 3rd ed., Cham, Switzerland AG: Springer Cham, pp. 325–341, 2022.
[2] A. G. Mirsaraei, A. Barati and H. Barati, "A secure three-factor authentication scheme for IoT environments," *Journal of Parallel and Distributed Computing*, vol. 169, no. 1, pp. 87–105, 2022.
[3] S. Ketu and P. K. Mishra, "Cloud, fog and mist computing in IoT: An indication of emerging opportunities," *IETE Technical Review*, vol. 39, no. 3, pp. 713–724, 2022.
[4] J. Pittman, "Forget the consumer IoT," [Online]. Available: https://www.ge.com/reports/forget-consumer-internet-things-iiot-really/
[5] M. E. Ekpenyong, D. E. Asuquo, I. J. Udo, S. A. Robinson and F. F. Ijebu, "IPv6 routing protocol enhancements over low-power and lossy networks for IoT applications: A systematic review," *New Review of Information Networking*, vol. 27, no. 1, pp. 30–68, 2022.
[6] A. M. Pasikhani, J. A. Clark, P. Gope and A. Alshahrani, "Intrusion detection systems in RPL-based 6LoWPAN: A systematic literature review," *IEEE Sensors Journal*, vol. 21, no. 11, pp. 12940–12968, 2021.
[7] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey *et al.,* "RPL: IPv6 routing protocol for low-power and lossy networks," [Online]. Available: https://www.ietf.org/archive/id/draft-ietf-roll-rpl-13.html
[8] J. Vasseur and D. Culler, "Routing over low power and lossy networks (roll)," [Online]. Available: https://datatracker.ietf.org/wg/roll/about/
[9] M. I. Younis, R. M. A. Latif, I. Haq, N. Z. Jhanjhi and A. Karim, "An evaluation of Sybil attack's detection approaches in Vehicular Ad-Hoc Networks (VANETs)," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 10, no. 2s, pp. 124–133, 2022.
[10] H. Kim, J. Ko, D. Culler and J. Paek, "Challenging the IPv6 routing protocol for low-power and lossy networks (RPL): A survey," *IEEE Communication Surveys and Tutorials*, vol. 19, no. 4, pp. 2502–2525, 2017.
[11] G. Simoglou, G. Violettas, S. Petridou and L. Mamatas, "Intrusion detection systems for RPL security: A comparative analysis," *Computers & Security*, vol. 104, no. 1, pp. 1–21, 2021.
[12] S. Murali and A. Jamalipour, "A lightweight intrusion detection for Sybil attack under mobile RPL in the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 379–388, 2020.
[13] Z. H. Toman, L. Hamel, S. H. Toman, M. Graiet, D. Cézane *et al.,* "Formal verification for security and attacks in IoT physical layer," *Journal of Reliable Intelligent Environments*, pp. 1–19, 2023. https://doi.org/10.1007/s40860-023-00202-y

[14] C. Pu, "Sybil attack in RPL-based internet of things: Analysis and defenses," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4937–4949, 2020.
[15] F. Zahra, N. Z. Jhanjhi, S. N. Brohi, N. A. Khan and M. Masud, "Rank and wormhole attack detection model for RPL-based internet of things using machine learning," *Sensors*, vol. 22, no. 18, pp. 1–17, 2023.
[16] D. Airehrour, J. A. Gutierrez and S. K. Ray, "SecTrust-RPL: A secure trust-aware RPL routing protocol for internet of things," *Future Generation Computer Systems*, vol. 93, no. 1, pp. 860–876, 2019.
[17] P. Thulasiraman and Y. Wang, "A lightweight trust-based security architecture for RPL in mobile IoT networks," in *IEEE Consumer Communications and Networking Conf.*, Las Vegas, NV, USA, pp. 1–6, 2019.
[18] A. Le, J. Loo, K. K. Chai and M. Aiash, "A specification-based IDS for detecting attacks on RPL-based network topology," *Information*, vol. 7, no. 2, pp. 1–19, 2016.
[19] F. Medjek, D. Tandjaoui, I. Romdhani and N. Djedjig, "A trust-based intrusion detection system for mobile RPL based networks," in *IEEE/ACM Int. Conf. on Cyber, Physical and Social Computing*, Exeter, UK, pp. 735–742, 2017.
[20] B. Groves and C. Pu, "A gini index-based countermeasure against Sybil attack in the Internet of Things," in *Military Communications Conf.*, Norfolk, VA, USA, pp. 1–6, 2019.
[21] C. Pu and K. R. Choo, "Lightweight Sybil attack detection in IoT based on bloom filter and physical unclonable function," *Computers & Security*, vol. 113, no. 102541, pp. 1–19, 2022.
[22] J. D. Kim, M. Ko and J. M. Chung, "Physical identification based trust path routing against Sybil attacks on RPL in IoT networks," *IEEE Wireless Communications Letters*, vol. 11, no. 5, pp. 1102–1106, 2022.
[23] D. Arshad, M. Asim, N. Tariq, T. Baker, H. Tawfik *et al.,* "THC-RPL: A lightweight trust-enabled routing in RPL-based IoT networks against Sybil attack," *PLoS One*, vol. 17, no. 7, pp. 1–13, 2022.
[24] A. Agiollo, M. Conti, P. Kaliyar, T. N. Lin and L. Pajola, "DETONAR: Detection of routing attacks in RPL-based IoT," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1178–1190, 2021.
[25] A. O. Bang and U. P. Rao, "A novel decentralized security architecture against Sybil attack in RPL-based IoT networks: A focus on smart home use case," *The Journal of Supercomputing*, vol. 77, no. 1, pp. 13703–13738, 2021.
[26] S. Raza, L. Wallgren and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, 2013.
[27] F. Medjek, D. Tandjaoui, I. Romdhani and N. Djedjig, "Performance evaluation of RPL protocol under mobile Sybil attacks," in *IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Sydney, Australia, pp. 1049–1055, 2017.
[28] G. Glissa, A. Rachedi and A. Meddeb, "A secure routing protocol based on RPL for Internet of Things," in *IEEE Conf. and Exhibition on Global Telecommunications (GLOBECOM)*, Washington DC, USA, pp. 1–7, 2016.
[29] A. K. Mishra, A. K. Tripathy, D. Puthal and L. T. Yang, "Analytical model for Sybil attack phases in internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 379–387, 2019.
[30] M. Ayaida, N. Messai, S. Najeh and K. B. Ndjore, "A macroscopic traffic model-based approach for Sybil attack detection in VANETs," *Ad Hoc Networks*, vol. 90, pp. 1–12, 2019.
[31] G. Oikonomou, S. Duquennoy, A. Elsts, J. Eriksson, Y. Tanaka *et al.,* "The contiki-NG open source operating system for next generation IoT devices," *SoftwareX*, vol. 18, no. 1, pp. 1–8, 2022.
[32] A. Velinov and A. Mileva, "Running and testing applications for contiki OS using Cooja simulator," in *Int. Conf. on Information Technology and Development of Education*, Zrenjanin, Republic of Serbia, pp. 279–285, 2016.
[33] U. S. R. K. Dhamodharan and R. Vayanaperumal, "Detecting and preventing Sybil attacks in wireless sensor networks using message authentication and passing method," *The Scientific World Journal*, vol. 33, no. 12, pp. 1–7, 2015.