Journal of Electronic Testing (2024) 40:259–273
https://doi.org/10.1007/s10836-024-06106-w

Simulation-based Analysis of RPL Routing Attacks and Their Impact on IoT Network Performance

Raveendranadh Bokka[1] · **Tamilselvan Sadasivam**[2]

Received: 14 September 2023 / Accepted: 7 February 2024 / Published online: 2 March 2024

Abstract
The recent expansion of the Internet of Things (IoT) owes a lot to the significant contribution of the 6LoWPAN protocol, which has been extensively employed in low-power and lossy networks. To facilitate communication in 6LoWPAN networks, the Internet Engineering Task Force (IETF) has suggested the usage of the Routing Protocol for Low-Power and Lossy Networks (RPL). Despite its usefulness, the open and restricted nature of the RPL protocol renders it susceptible to both internal and external attacks. Since IoT devices connected through the RPL protocol have limited resources like processing power, battery life, memory, and bandwidth, ensuring their security is of the utmost importance. One of the primary obstacles to IoT networks is RPL routing attacks, which disrupt the network's normal routing activities and structure. This study investigates the impact of five RPL routing attacks, namely Blackhole, Sybil, Selective Forwarding (SF), Sinkhole, DIO suppression, and DIS flooding, on the IoT networks' performance. The study evaluated the network's performance for normal and five routing attack scenarios using numerous performance metrics including Link throughput, No. of packets generated (control and data), Sensor data throughput, Packet Delivery Ratio (PDR), and Delay in packet delivery. This work conducted simulations using the Tetcos NetSim v12.1 IoT network simulator tool and is the first to analyze IoT network performance under multiple routing assault scenarios with various performance measures. The analysis showed that the performance metrics of PDR, Sensor data throughput, and No. of data packets transmitted decreased significantly in attack scenarios compared to the normal scenario, with an average decreased percentage of 70%, 70%, and 39.4%, respectively. In contrast, the metrics Link throughput, Delay, and No. of control packets transmitted increased in attack scenarios compared to the normal scenario, with average values supplemented by a factor of 35, 255, and 36, respectively. Additionally, the Destination-Oriented Directed Acyclic Graph (DODAG) real-time formation under different scenarios was provided.

Keywords Internet of Things (IoT) · Low power and lossy networks · 6LoWPAN · RPL · DODAG · Routing attacks · Black hole · Sybil attack · Selective forwarding · Sinkhole · DIS suppression attack · DIS flooding attack · Simulation · NetSim · Performance analysis

1 Introduction

A new paradigm has emerged with the IoT that involves internet-enabled digital devices connected through a network to share information. Sensors, actuators, and transceivers are included in these devices that facilitate interaction with the physical environment. However, to derive meaningful insights from the sensor data collected, it is crucial to store and analyze it intelligently [20].

Since most IoT devices have resource limits. It is simpler to route over IPv6 in Low Power Wireless Personal Area Networks due to the RPL, which was created by the IETF to address this issue (6LoWPAN) [8]. With IPv6 auto-configuration, new smart devices can be quickly

Responsible Editor: C. A. Papachristou

✉ Raveendranadh Bokka
bravindra64@pec.edu

Tamilselvan Sadasivam
tamilselvan@pec.edu

[1] Research Scholar, Department of ECE, Puducherry Technological University, Puducherry, India

[2] Department of ECE, Puducherry Technological University, Puducherry, India

connected to existing IoT networks. However, by inviting numerous insider and outsider threats, this functionality interferes with the IoT network's normal routing operation [25]. Because, during communication between the devices, the unauthorized device may enter into the communication and hack the useful data, which is the main vulnerability of IoT device-based communication. It will affect the further process of any monitoring areas, such as medical healthcare, smart city, military applications, etc.

In recent years, the RPL protocol has gained popularity as a Routing Protocol (RP) option in the network layer of IoT and Wireless Sensor Networks (WSN). Nevertheless, this protocol is vulnerable to numerous WSN and IoT routing attacks [13]. Routing attacks are potent, and they degrade the IoT network's performance by affecting some network parameters like throughput, PDR, and delay in packet delivery. Therefore, before developing a new lightweight intrusion detection system for RPL-centered IoT networks, it is worthwhile to do thorough research and simulation of such attacks against RPL and analyze the performance of networks under different attacks [9]. So, this paper focused on studying the impact of routing attacks like a blackhole, sinkhole, Sybil, SF, DIS flooding, and DIO suppression on the performance of IoT networks using the metrics Throughput, PDR, No of packers generated, and Delay. For every simulation, the traces of simulated attack traffic data were collected to develop a novel dataset that can be used in further research to create Deep Learning (DL), and Machine Learning (ML) centered attack detection systems.

The paper is divided into multiple sections. In Section 2, the relevant literature and background information in the research area are reviewed. The implementation of various RPL routing attacks on the IoT network is explained in Section 3. Section 4 covers the simulation of routing attacks using different network and DODAG topologies, whereas Section 5 signifies the simulation outcomes. The paper concludes with Section 6, which outlines suggestions for future research.

2 Background and Literature Review

The RPL protocol and its operation are briefly explained in this section, which is followed by a portion that concentrates effectively on examining the RPL routing attacks' effects on the functionality of IoT networks.

3 Routing Protocol for Low-Power Lossy Networks (RPL)

The RPL protocol's creation, which employs a DODAG approach, was executed by the IETF network working group. This RP operates on an IP-based, hop-by-hop model. As

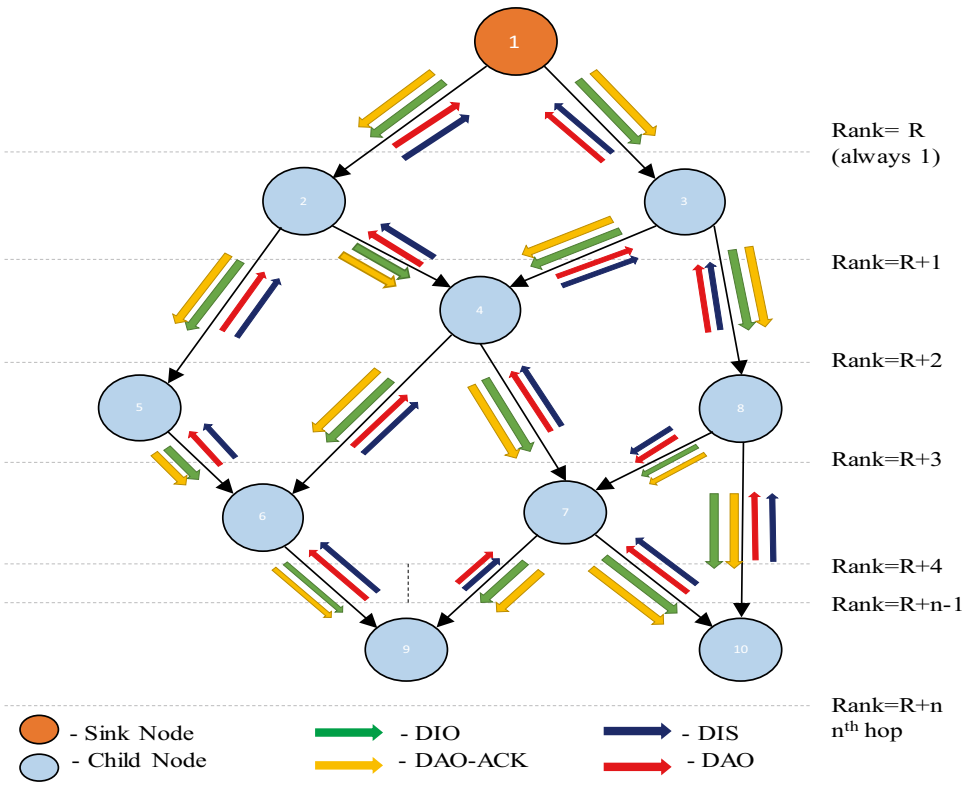


Fig. 1 RPL DODAG formation

depicted in Fig. 1, the DODAG comprises a root node, also known as a sink node, and a source node, or leaf node, which is associated with it.

The construction of the DODAG includes the exchange of several control messages, such as "*DODAG information object (DIO), DODAG acknowledgment object (DAO), and DODAG information solicitation message (DIS)*". Both unidirectional and bidirectional traffic can be handled by the DODAG protocol[7]. The root node transmits the DIO control message that includes vital details like the version and ID. A node in the network decides its position by employing the objective function after receiving the DIO [4]. The root node has a rank value of 1, indicating that it is at the top of the DODAG network. As a result, a node's rank decreases the closer it is to the root. A node's rank value is confirmed through a DAO and the node requests to join the network by sending a DIS control message to the root node[7].

4 Related Works

In a recent study, [18] compared the RPL's performance with and without its security mechanisms against 4 types of routing attacks, namely Blackhole, Selective-Forward, Neighbor, and Wormhole attacks. To estimate the impact of these attacks, they assessed RPL's performance using a variety of parameters, including average data packet delivery rate, average data packet latency, and average power usage. In a related study, [25] examined the effects on network throughput performance of a number of renowned routing attacks, namely "*Blackhole, HELLO flooding, SF, Sinkhole, Sybil, Clone ID, and Local Repair*". By analyzing these attacks, the authors aimed to shed light on the vulnerabilities of the RPs and the potential threats they pose to the network's performance. Another relevant study by [2] centered on examining the characteristics and effects of RPL attacks. By utilizing the IoT-specific Contiki operating model, the authors constructed elevated rank RPL attacks and diminished rank RPL attacks and assessed their impacts on RPL's performance. They used the PDR as a performance metric to assess the effectiveness of RPL under these attacks. Furthermore [11] performed a study to assess RPL's performance under 4 RPL-centered attacks, including the diminished rank, local repair, neighbor, and DIS attacks. The Decreased Rank as well as Local Repair attacks had the biggest effects on PDR, while the DIS attack caused the most end-to-end latency, according to their research. The Neighbor attack, on the other hand, had the least influence on the network's performance. This study offers additional insights into the behavior of RPL under specific types of attacks and can be used to inform the design of more effective security mechanisms for RPL in IoT networks.

Additionally, [21] examined a version number attack's effects on an RPL-centered network, with a focus on the effects on confined networks when nodes are mobile. The influence of mobility in a limited environment, which was a vital concern in many IoT applications, was the focus of the study. When a version attack was implemented in an RPL-based IoT, the authors examined the network's performance regarding packet delivery, delay, along with power consumption. This study's outcomes provide valuable insights into the effects of a version number attack on the RPL's performance in IoT networks, particularly in the context of mobility, and can inform the development of more robust security mechanisms for RPL in such scenarios. Moreover, [3] conducted a study to examine the effects of many attackers on an RPL-based network's performance, considering numerous parameters like average delay, average power consumption attacker position, and PDR. According to their research, the PDR is mostly affected by numerous attackers, and the attack's impact on the network is greater the closer the malicious node is to the root node. This study's findings provide a better understanding of the multiple attackers' impact on the RPL-centered IoT networks' performance and highlight the importance of considering the position of attackers in developing effective security mechanisms. In another work, [6] the Cooja simulator was used to determine the factors that may influence how well the RPL performs in IoT networks. They evaluated the network's PDR, energy use, along with overhead control message for RPL performance while taking different scenarios' traffic patterns, transmission ranges, node mobility, along with network size into account. Their simulation results showed the impact of transmission distance and radio interference on PDR and overhead ratio and the importance of addressing node mobility to ensure reliable network solutions.

In the relevant study by [15], authors employ the RPL routing protocol to evaluate the impact of internal attacks like sinkholes as well as SF attacks, on a low-power and lossy network architecture. The study demonstrates that attacking motes consume substantially more power than non-attacking motes, and that attacks might have a detrimental impact on the network's performance. Tonapa et al. [24] carried out research on several cyberattacks against RPL, namely Hello Flood, Version Number Modification (VNM) Attack, together with Blackhole. Utilizing parameters like PDR, End-to-End Delay, Routing Overhead, and Network Lifetime, they conducted their attacks on a Cooja Simulator. The Flood Attack had the biggest effect, resulting in a 20-fold decrease in network lifetime, a slight decline in PDR, a massive rise in average E2E delay, and an increase in routing overhead. The VNM Attack caused a four-fold reduction in network lifetime, a 70% decrease in PDR, and had the most significant impact on Routing Overhead [10]. assess the effects of attacks on topology and resources on RPL's effectiveness, Hello Flooding, Increase Number, and Decrease Rank attacks were chosen as examples of

attacks on resources and topology. They investigated how these attacks affected RPL performance parameters, such as E2ED, throughput, PDR, and average power consumption using simulations. The results exhibited that all 3 attacks had detrimental effects, boosting E2ED, lowering PDR as well as network throughput, deteriorating the network, and elevating network node power consumption.

Collectively, all these studies highlight the significance of evaluating the performance of RPs under various sorts of attacks and in different network conditions to ensure their effectiveness in practical IoT applications. As a result, this paper's main goal was to investigate the effects of routing attacks like a Blackhole, Sinkhole, Sybil, SF, DIS flooding, along with DIO suppression, on the performance of IoT networks using the metrics Throughput, PDR, E2E Delay, and No of packers generated, including control and data packets.

5 Description and Implementation of the Routing Attacks

There exist many networking attacks against the RPL protocol. Some of the attacks considered in this paper are discussed in the following sections.

5.1 Black Hole Attack

The attacker node performs a DoS attack by dropping all sorts of traffic that passes via it, encompassing RPL control messages as well as data packets [17]. The black hole attack is a sort of attack that could be very damaging when joined with a sinkhole attack. A malicious node uses an advertised false rank value to entice other nodes for choosing it as a parent node and subsequently drops the whole incoming data packets to interfere with the Low Power Lossy Network's (LLN) functionality. The attacker node in a black hole attack discards every data packet it gets from other nodes, regardless of where it came from. The combination of both attacks can lead to a situation where nodes are forced to route their traffic through the malicious node, which then drops all packets, resulting in a complete network breakdown [12]. In this evaluation, the adversary node attack is combined with sinkhole and Sybil and SF attacks for dropping the data packets coming through the malicious node.

5.2 Sink Hole Attack

This attack involves an attacker or a malicious node advertising a false or advantageous routing path, leading multiple nodes for routing their traffic via it. Specifically, in the RPL protocol, a sinkhole attack can be initiated by the attacker promoting a better rank, causing nodes in the DODAG to choose it as their parent node. As a result, the malicious node can attract and intercept a significant portion of network traffic, effectively disrupting the network's routing service [19].

Algorithm 1 Implementation of Sinkhole and Blackhole Attack

```
if event == Network in Event, then
    if packet == control packet then
        if node == Malicious Node then
            assign the rank of the current node with Malicious Rank;
        else
            process the control packet;
        end
    else if a node is malicious and the packet is not empty, then
        drop the packet;
end
```

5.3 Sybil Attack

An attack of this kind, known as a Sybil attack, involves the attacker creating several identities (or "fake" identities) to deceive other nodes in a network. The attacker could utilize these fake identities to manipulate the network. In some cases, the attacker may utilize fake identities for gaining access to sensitive information or disrupting the network's normal operation [7].

Algorithm 2 Implementation of Sybil and Blackhole Attack

```
if event == Network in Event, then
    if packet == control packet then
        if node == Malicious Node then
            assign the rank of the current node with a random value as
            (except 1) Malicious Rank;
        else
            process the control packet;
        end
    else if a node is malicious and the packet is not empty, then
        drop the packet;
end
```

5.4 Selective Forwarding Attack

Similar to a sinkhole attack, this one is called an SF attack because the attacking node selectively sends some packets while discarding others. For instance, an attacker may choose to forward only routing messages while ignoring all other packets, thus causing disruption to a portion of the network [19].

Algorithm 3 Implementation of Selective Forwarding and Blackhole Attack

```
if event == Network in Event, then
    if packet == control packet then
        if node == Malicious Node then
            assign the rank of the current node with Malicious Rank;
        else
            process the control packet;
        end
    else if a node is malicious and the packet is not empty, and the random
    value is  divisible by 2, then
        drop the packet;
    else
        forward the packer;
end
```

5.5 DIS Flooding Attack

Receiving nodes purposefully decide not to join the already-existing DODAG, instead dropping the message and sending DIS messages repeatedly to carry out the DIS flooding attack. This behavior results in an excess of DIS messages being transmitted, and many malicious nodes remaining inactive and not joining the DODAG [5].

Algorithm 4 Implementation of DIS Flooding Attack

```
if event == Network in Event, then
    if packet == control packet then
        if node == Malicious Node then
            drop the DIO message;
            keep sending the DIS messages;
        else
            process the DIO message;
        end
end
```

5.6 DIO Suppression Attack

The functionality of the routing service in RPL can be significantly impacted by the DIO suppression attack. This is due to the attack's ability to prompt victim nodes to withhold the transmission of crucial RPL messages called DIO messages that are essential in establishing the routing topology. As a result, the quality of routes is generally degraded, eventually resulting in network partitions [16].

Algorithm 5 Implementation of DIS Flooding Attack

```
if event == Network in Event then
    if packet == control packet then
        if node == Malicious Node then
            drop the DIO message;
            resend the DIO message;
        else
            process the DIO message;
        end
end
```

6 Simulation of the Routing Attacks

The simulation was done in the Dell Inspiron Intel(R) Core(TM) i7-8550U CPU (clock speeds 1.80 GHz &1.99 GHz) with 16 GB of main memory. The simulation of the IoT Network topology was done using the NetSim standard v12.1 [14] software for three different setups: Normal, Single attacks node, and Two attack node scenarios. Five types of attacks discussed in the previous section are considered and simulated for each attack type separately in single and two attacker node scenarios. In all the simulation scenarios, DODAG formations were generated for understanding the attacks' impact on the Network topology. Additionally, the server node (Wire node 15) is connected to the wireless sensors with node IDs 1, 9, and 12 in order to track and assess the nodes' performance under the various network simulation situations depicted in the DODAG formation figures.

6.1 Simulation Setup

Table 1 exhibits a comprehensive description of the simulation setup for diverse network scenarios. For all the scenarios, the maximum number of nodes considered is 20, in that one node is considered an attacker node for attack scenario one and two as attacker nodes for attack scenario 2. For each case, the RPL protocol was selected as the network layer protocol.

6.2 Normal Scenario

The IoT network topology for the normal scenario without malicious nodes considered for data collection is shown in Fig. 2. This sample topology comprises 1 sink node, 0 attacker nodes, and 20 benign nodes. The DODAG topology development in Fig. 3 shows that the entire nodes are linked to the root node (13 with Rank:1) for data transmission because there are no harmful nodes in the network environment.

Table 1 Simulation Setup for different Scenarios

Parameters	Normal Scenario	Attack	
		Scenario 1	Scenario 2
Simulation time	1000 s	1000 s	1000 s
Total number of nodes	20	20	20
Number of normal nodes	20	19	18
Number of Malicious Nodes (Mal. Nodes)	0	1	2
Path Loss	Yes	Yes	Yes
Network Layer Protocol	RPL	RPL	RPL

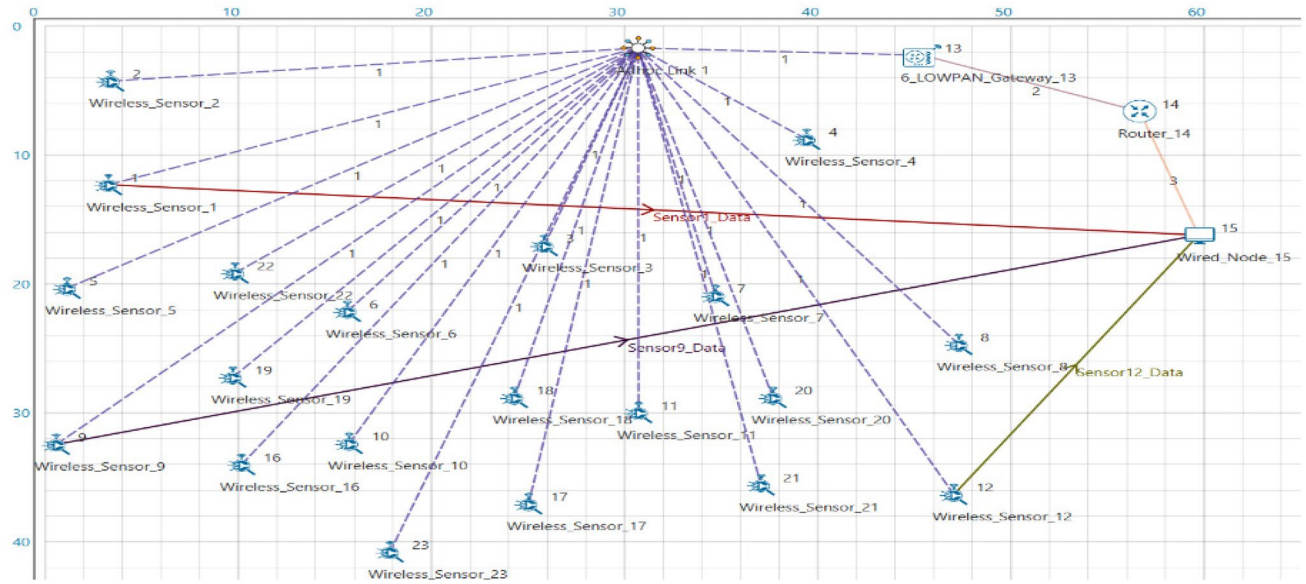


Fig. 2 IoT Network Setup for without attack nodes

6.3 Routing Attacks Scenario

The IoT network topology for attack scenarios 1 and 2 with malicious nodes one and two attack nodes are shown in Figs. 4 and 5. In attack scenario 1, the wireless sensor nodes 5 and in scenario 2, wireless sensor nodes 5 and 7 are considered malicious nodes. The malicious nodes are highlighted in red color in all the scenarios. The

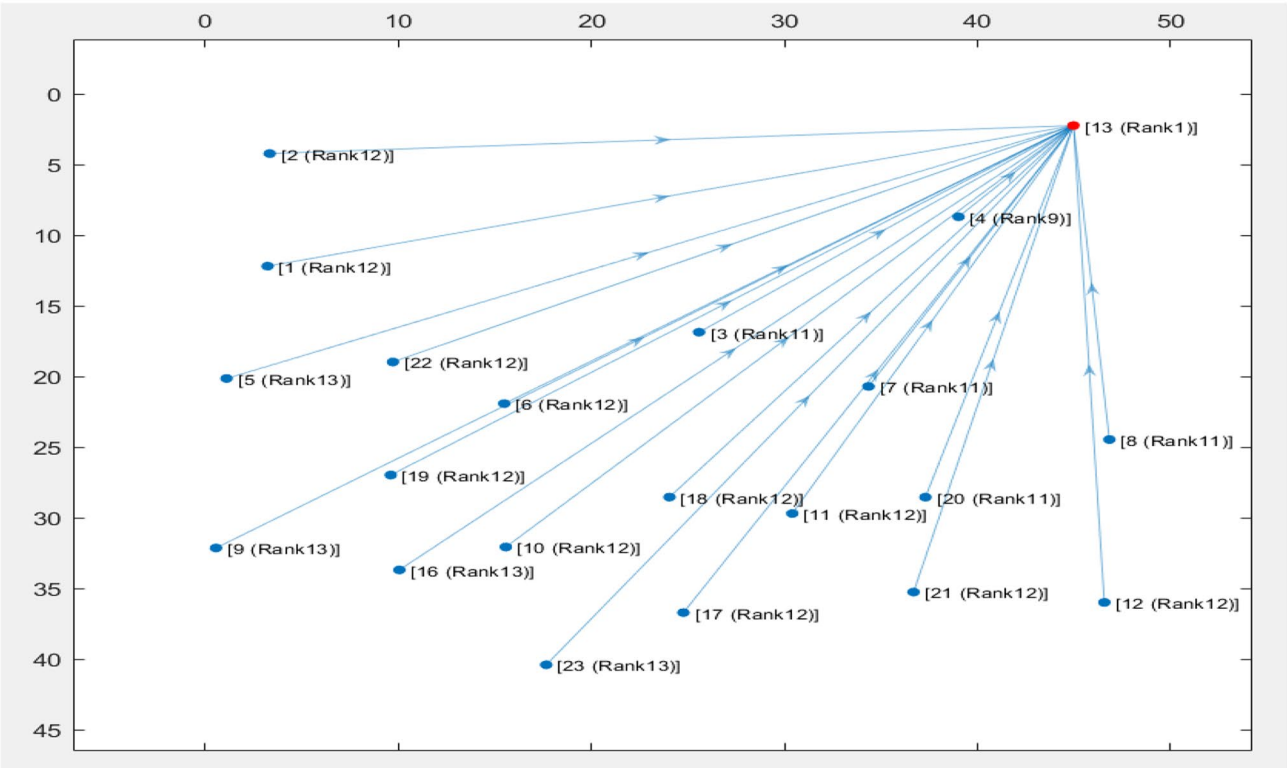


Fig. 3 DODAG Formation for Normal Scenario

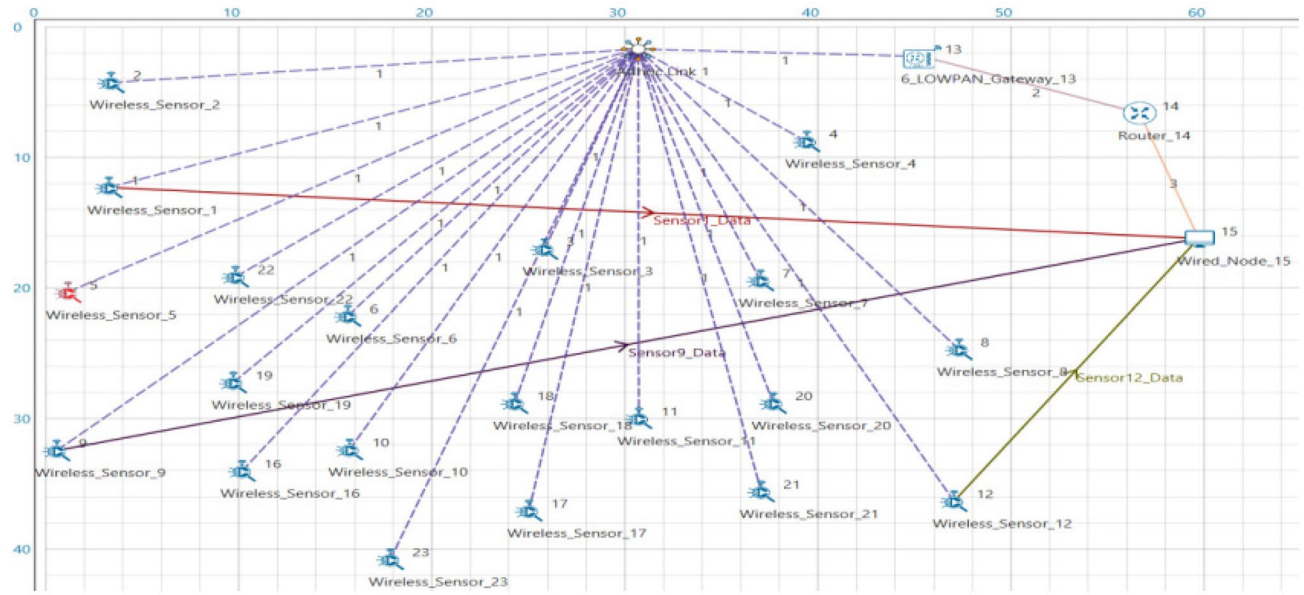


Fig. 4 IoT Network Setup with Single attack Node Scenario 1

topology comprises 1 sink node, one attacker node,19 benign nodes, and one sink node, two attacker nodes, and 18 benign nodes for attack scenarios 1 and 2, respectively. The malicious nodes are activated with different types of RPL attacks, and the formation of the DODAG topology for each attack type is discussed in the following sections.

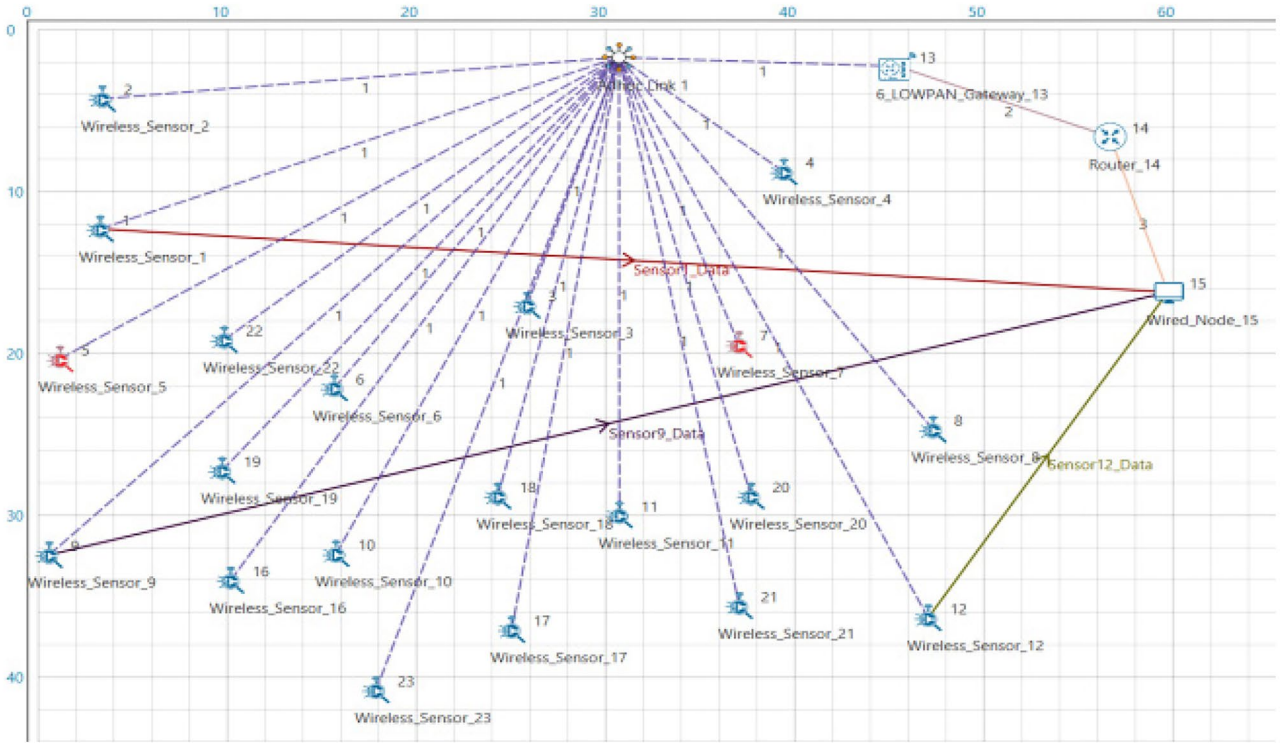


Fig. 5 IoT Network Setup with Two attack nodes Scenario 2

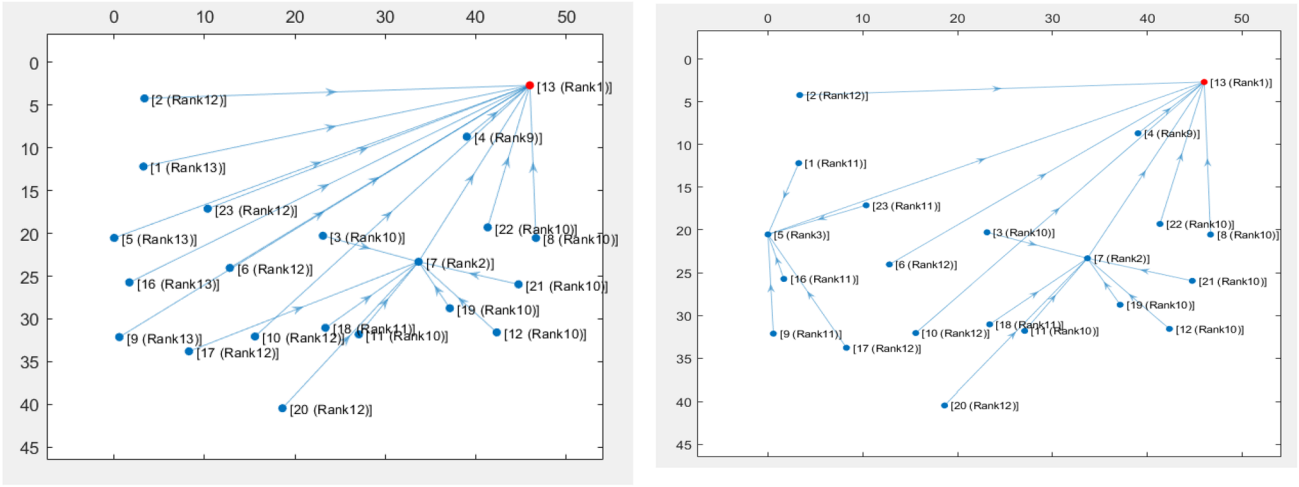


Fig. 6 DODAG Formation for sinkhole attack scenario with **a** One node and **b** Two nodes

Using network topologies and DODAG formations, this study is the first to analyze the RPL attack's impact on the IoT network under normal and attack scenarios.

6.3.1 Sinkhole and Black Hole Attack

The figure details the DODAG formation for the sinkhole attack scenario. Since node 7 in Fig. 6(a) is a malicious node that advertises with the rank of 2, all nearby nodes are connected to it for data transmission. Nodes 6 and 7 in Fig. 6(b) are shown as malicious nodes and are advertising with ranks 3 and 2, respectively. Therefore, the neighboring nodes are connected to the malicious nodes because of fewer ranks for data transmission. Traffic diverted through the malicious nodes is dropped as the nodes are connected to the malicious nodes.

6.3.2 Sybil and Black Hole Attack

As discussed in the previous section, when there is a Sybil attack in the network, the affected malicious node advertises multiple ranks or replicates other neighboring nodes' ranks. The same is shown in the DODAG formation given in Fig. 7 for the Sybil attack simulation in the network. For instance,

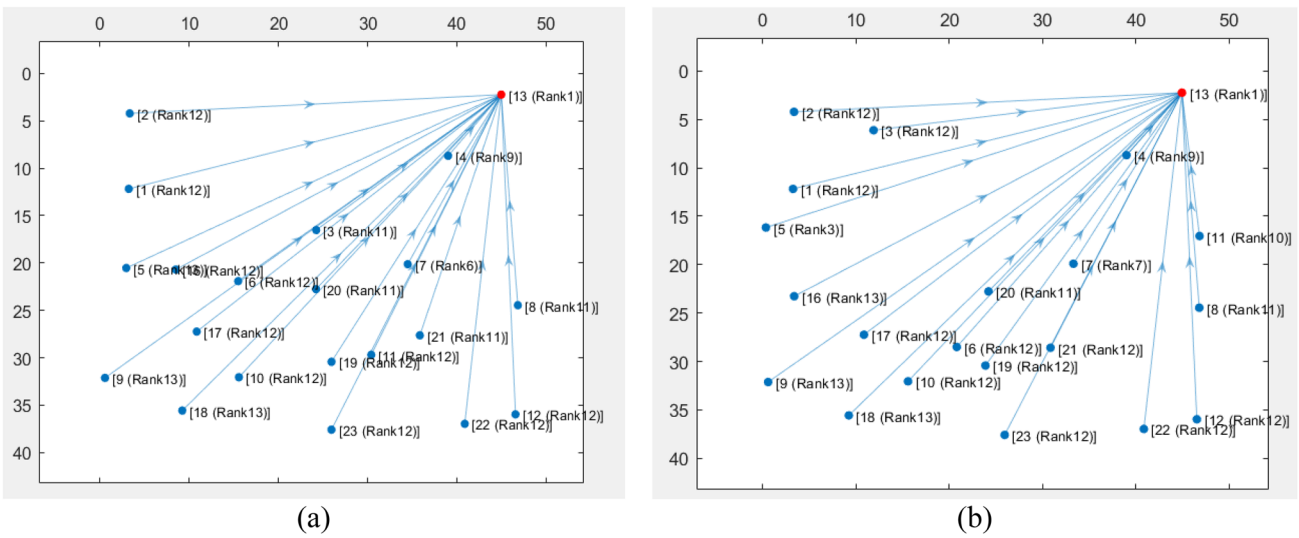


Fig. 7 DODAG Formation for Sybil attack scenario with **a** One node and **b** Two nodes

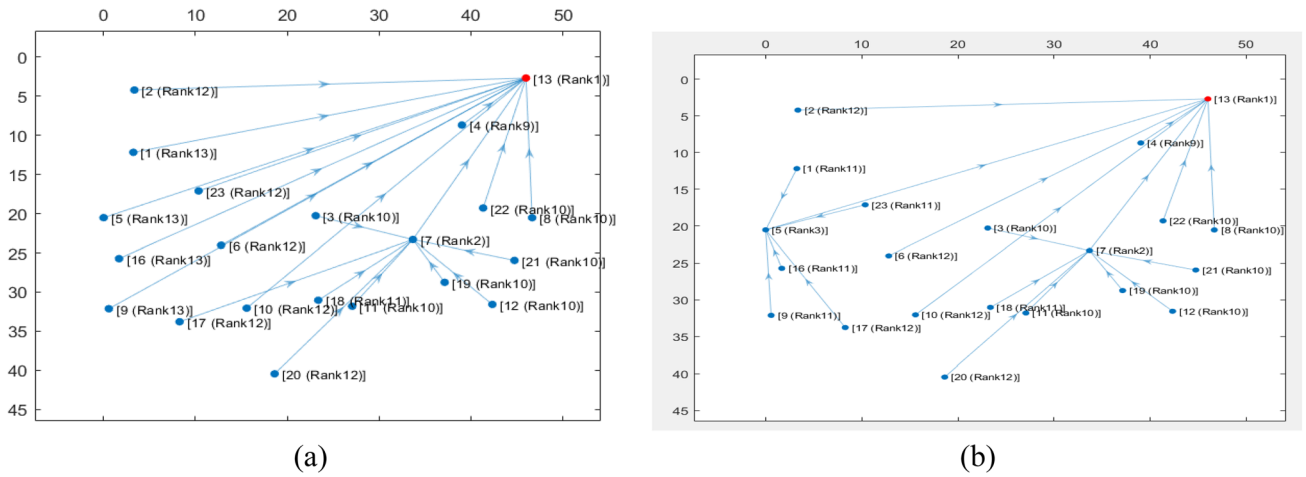


Fig. 8 DODAG Formation for selective forwarding attack scenario with **a** One node and **b** Two nodes

the sensor node with ID seven is changed with ranks 6 and 7. The rank of the malicious node changes with random values.

6.3.3 Selective Forwarding and Black Hole Attack

The SF attack is like the sinkhole attack in the network. The DODAG formation in Fig. 8 shows that malicious nodes 6 and 7 attract traffic by advertising the small ranks. Here, the malicious nodes will drop only the selected packets and forward the rest of the packets to the destination.

6.3.4 DIS Flooding Attack

The malicious node forges and sends numerous control packets (DIO or DIS). Forged messages keep the neighbors busy, trying to process them. This attack creates a massive amount of network traffic with huge control packets. This paper creates network topology, and wireless sensor nodes 5 and 7 are modified as malicious nodes. In order to avoid joining an existing DODAG topology, the malicious nodes drop the DIO messages and retransmit the DIS messages to the nearby nodes. This causes them to become idle. The DIS flooding attack's effect on the DODAG formation is shown in Fig. 9.

6.3.5 DIO Suppression Attack

Figure 10 exhibits how the DIO suppression attack affected the creation of the DODAG topology for single and dual attack nodes. It affected total topology formation in both scenarios. Node seven is considered malicious for a single attack scenario, and two nodes attack scenario nodes 5 and 7 are considered malicious nodes. Because of the DIO suppression attack, some of the normal nodes become idle, not joined in any existing topology, and the topology is portioned into multiple networks.

7 Results and Discussion

For the normal and attack scenarios, three wireless sensor nodes with ID 1, 9, and 12 data are taken for analyzing the network performance using metrics like PDR, Link throughput, No. of packets generated, Sensor data throughput, and Delay in packet delivery.

7.1 Sensor's Data Throughput

To calculate a network's throughput, various tools can be utilized on various platforms. Throughput is a measure of the amount of useful data that can be transmitted per unit of time and is expressed in Mbps. The higher the throughput, the better it is for the network. Among the performance metrics of RPs, throughput is the most critical one to evaluate [22].

The data throughput of each sensor is calculated using Eq. (1), and it is the ratio of the total payload received at the destination in bytes per the total simulation time. The payload is the product of 'Packets delivered' and 'Packet Size' Fig. 11.

$$\begin{aligned} &\textit{Sensor Data Throughput}(\textit{in Mbps}) \\ &= \frac{\textit{Total payload delivered to destination}(\textit{bytes}) * 8}{\textit{Simulation Time}\,(\mu\,\textit{sec})} \end{aligned} \tag{1}$$

With the help of Eq. (1), the sensors' data throughput was calculated for nodes 1, 9, and 12 to evaluate the IoT

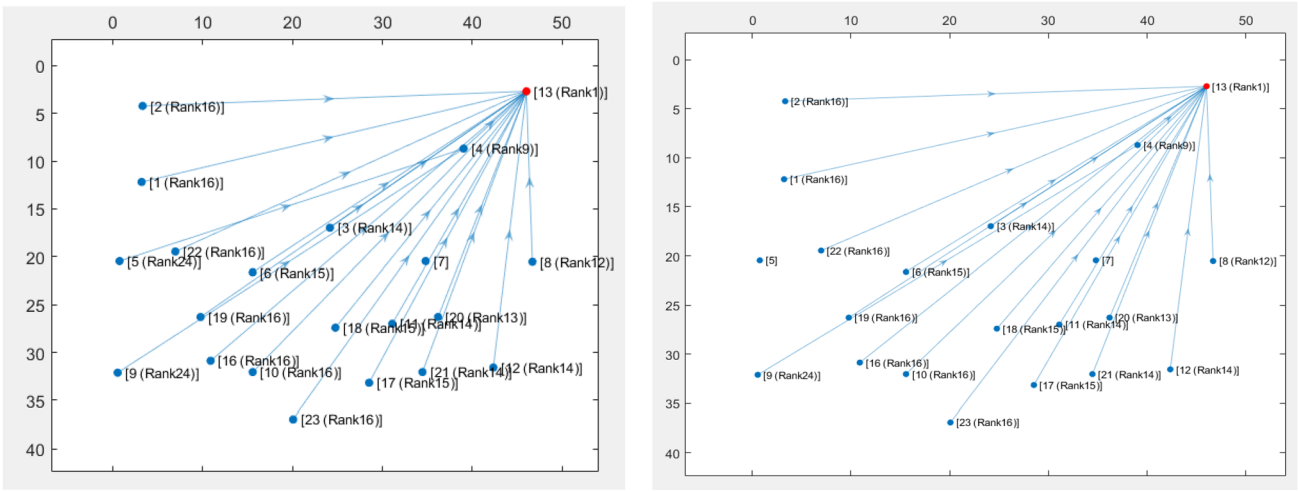


Fig. 9 DODAG Formation for DIS flooding attack scenario with **a** One node and **b** Two nodes

network's performance in normal as well as attack scenarios. The throughput was measured in bps, which is shown in the figure. From this, it was observed that in a normal scenario, the average throughput for all three nodes is *243 bps,* and in the case of attack scenarios, the overall average throughput of one and two malicious node conditions is *78, 172,133,143,* and *40 bps* for *sinkhole, SF, DIS flooding, Sybil, and DIO suppression attacks*, respectively. Furthermore, it was observed that the throughput for attack scenarios is significantly less compared with a normal scenario. For example, the throughput in the sinkhole attack scenario was less because the malicious nodes dropped most of the data packets by attracting traffic. Additionally, the network topology partitions in the DIO suppression attack scenario prevent most of the data from reaching the target, lowering throughput. And the throughput is relatively modest in the remaining attack scenarios.

7.2 Packet Delivery Ratio

One way to calculate the average PDR is to divide the total number of packets that were received successfully by the

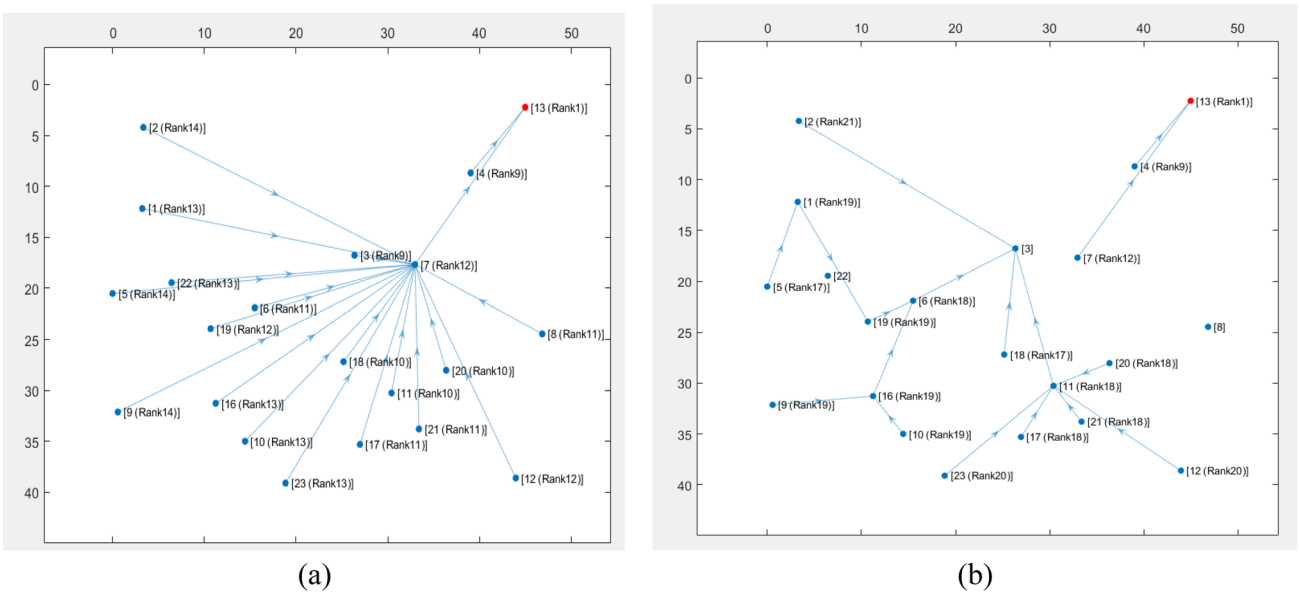


Fig. 10 DODAG Formation for DIO suppression attack scenario with **a** One node and **b** Two nodes

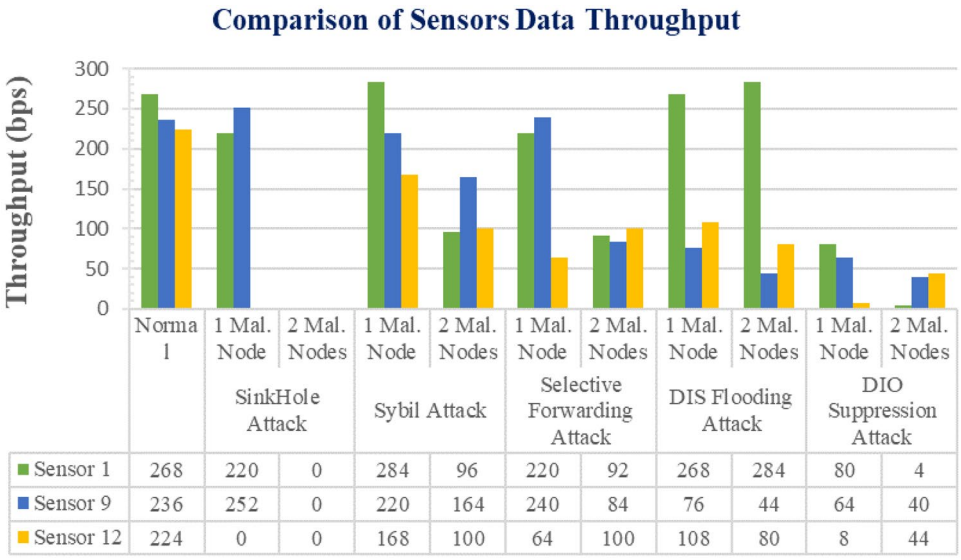


Fig. 11 Sensor's data throughput

total number of packets sent from all nodes to the sink. This calculation provides a gauge of the ratio of packets that were successfully delivered, on average, across all nodes in the network [1] Fig. 12.

$$Packet\ Delivery\ Ratio(in\%) = \frac{Total\ Number\ of\ packets\ delivered\ successfullly}{Total\ Number\ of\ packets\ generated} x100 \quad (2)$$

Equation (2) was used to calculate the PDR in the IoT network under both normal and attack scenarios. The same thing was shown in the above figure as a graphical representation. For evaluation, we considered only the three nodes 1, 9, and 12 data for all the scenarios instead of considering all the node's packets. From the figure, it was observed that the average PDR% of the three nodes is 60.67% in the case of the normal scenario. Similarly, in attack scenarios, the combined average PDR% of one and two malicious nodes is *19.67%, 43%, 33.33%, 35.83%,* and *10%* for *DIS flooding, Sybil, DIO suppression, SF, and sinkhole attack*, respectively. In attack scenarios, the PDR is lower than it is under normal circumstances. The effect on PDR is more in the case of a DIO suppression attack because of partition in the topology; most nodes cannot join.

7.3 Link Throughput

The total number of bytes transmitted is measured for both successful data packets and control packets. The calculation is based on the size of the packet in bytes, which includes the payload of the application layer and the overheads of all layers at the Physical (PHY) layer. This metric excludes error

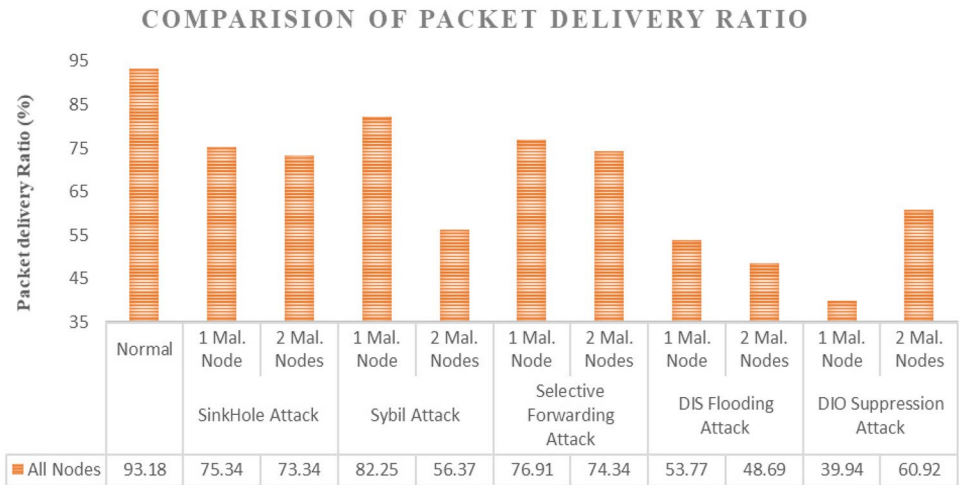
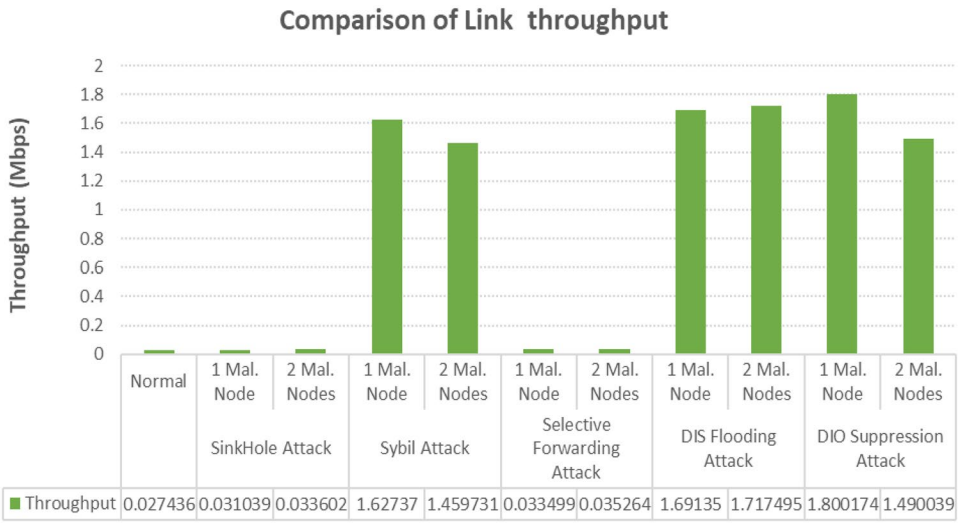


Fig. 12 Packet Delivery Ratio

Fig. 13 Link Throughput



and collision packets and only takes into account successful packets for the calculation.

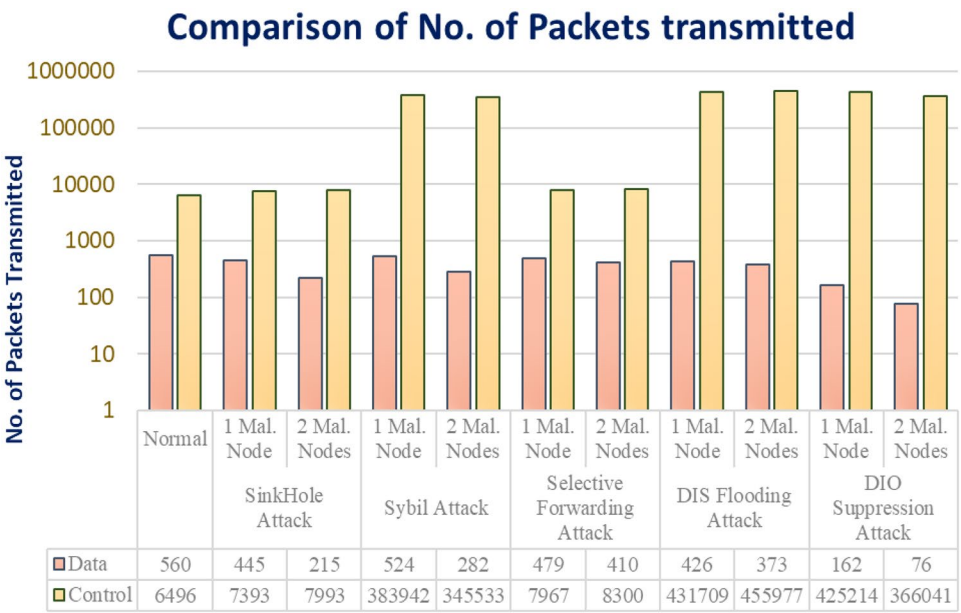
$$Link\ Throughput(in\ Mbps) = \frac{Total\ bytes\ transmitted\ over\ the\ link * 8}{Simulation\ Time\ (\mu\ sec)} \quad (3)$$

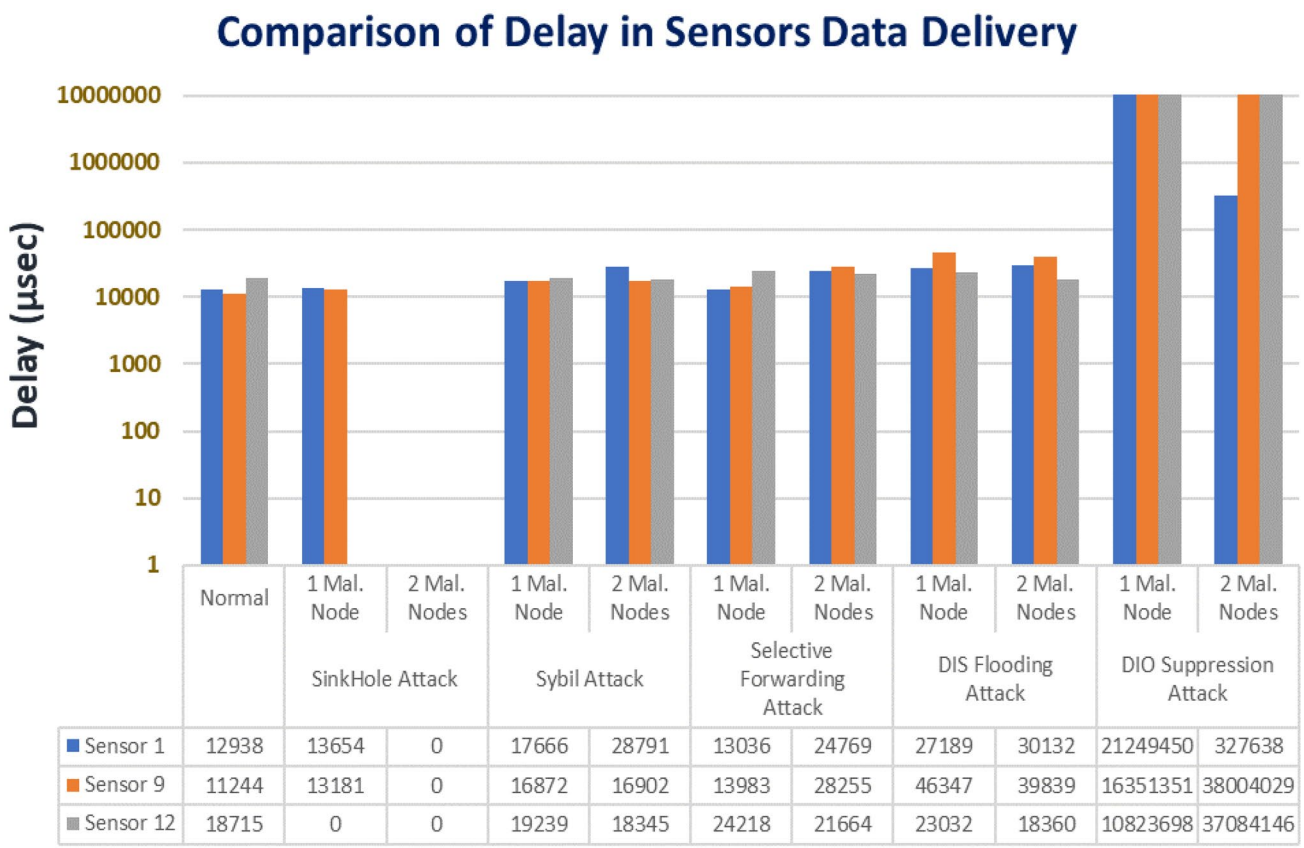
The link throughput of the whole network was calculated using Eq. (3). The comparison of those values for different scenarios is mentioned in the figure. The link throughput rose for the Sinkhole, Sybil, DIO suppression, SF, and DIS flooding attack scenarios by factors of 1.17, 56.26, 1.25, 62.12, and 59.96, respectively, in comparison to the normal scenario. From the values, it was understood that in three attack scenarios, i.e., Sybil, DIS flooding, and DIO suppression, the link throughput was increased by a factor greater than 50 compared to the normal scenario because of more control packet generation in the network. In the attack scenario, the average link throughput experiences a 36-fold increase when compared to the normal network topology.

7.4 No. of Packets Generated

The figure compares the total number of data and control packets generated in the normal and attack scenarios. Compared to the normal scenario, all attack scenarios' average data packets decreased % by *41.1,28,20.5,28.6,* and *78.8.* Similarly, the control packets are increased by a factor of 1.18, 56.14, 1.25, 68.32, and 60.90, respectively. The network performance degrades drastically because of the vast increment of control packets in attack scenarios Figs. 13 and 14.

Fig. 14 No. of Packets transmitted





	Normal	SinkHole Attack		Sybil Attack		Selective Forwarding Attack		DIS Flooding Attack		DIO Suppression Attack	
		1 Mal. Node	2 Mal. Nodes	1 Mal. Node	2 Mal. Nodes	1 Mal. Node	2 Mal. Nodes	1 Mal. Node	2 Mal. Nodes	1 Mal. Node	2 Mal. Nodes
Sensor 1	12938	13654	0	17666	28791	13036	24769	27189	30132	21249450	327638
Sensor 9	11244	13181	0	16872	16902	13983	28255	46347	39839	16351351	38004029
Sensor 12	18715	0	0	19239	18345	24218	21664	23032	18360	10823698	37084146

Fig. 15 Delay

7.5 Delay in Packet Delivery

The delay refers to the average duration, measured in microseconds, from the moment a packet is transmitted as of the application layer of the source node to the point at which it successfully arrives at the destination application layer. This is calculated by considering all successfully transmitted packets. The Delay for every packet is calculated as the period between the application layer arrival time to the physical layer end time. The Delay for all the scenarios for nodes 1, 9, and 12 are shown in the figure. The distraction or division in the network architecture is the main source of the delay in the DIO suppression attack scenario. The average Delay for all three nodes' attack scenarios was increased by a factor of 289 compared with the normal scenario Fig. 15.

7.6 Vulnerability Trust and Assurance Level

The vulnerability level of the node communication is calculated by the number of malicious nodes divided by the total number of nodes and the value is multiplied by 100. Here, the vulnerability level is 10% according to the scenario 2. With respect to the vulnerability level, the trust value is presented. The trust level is calculated during node communication. The trust level and the assurance level are presented by the sensor's data throughput, packet delivery ratio, link throughput, number of packets generation, and delay in packet delivery analysis metrics.

8 Conclusion and Future Work

This research concentrates on the vulnerability of IoT devices connected through the RPL protocol to routing attacks and the significance of securing them to prevent insider as well as outsider attacks. The investigation of the impacts of five RPL routing attacks on the IoT networks' performance using a variety of performance indicators offers important new information about the routing attacks' effects on IoT networks. The simulation-based study using the Tetcos NetSim v12.1 IoT network simulator tool reveals that the metrics Link throughput, Delay, and Number of control packets transmitted rise while the metrics PDR, Sensor data throughput, and Number of data packets transmitted significantly decrease in attack scenarios when compared to the normal scenario. These results underline how crucial it is to put in place strong

security controls to shield IoT networks and devices from routing attacks. The research helps improve security protocols for IoT networks and evaluate the routing attacks' impact on IoT network performance using a set of performance indicators. The generated dataset can be utilized to perform additional research and create attack detection approaches centered on ML and DL in subsequent work.

Acknowledgements We thank the anonymous referees for their useful suggestions.

Author's Contributions All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by **[*1]Raveendranadh Bokka, [2]Tamilselvan Sadasivam**The first draft of the manuscript was written by **[*1]Raveendranadh Bokka**and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding This work has no funding resource.

Data Availability Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Ethical Approval This article does not contain any studies with human participants or animals performed by any of the authors.

Consent of Publication Not applicable.

Conflict of Interest The authors declare that they have no conflict of interest.

Competing interests The authors declare that they have no competing interests.

References

1. Ali H, Duquennoy S, Boldt M (2015) A Performance evaluation of RPL in Contiki. CLOSER 2015 - In: Proceedings of 5th International Conference on Cloud Computing and Services Science, Proceedings. pp 233–240
2. Ambarkar SS, Shekokar N (2021) Impact Analysis of RPL Attacks on 6Lo WPAN based Internet of Things network. In: Proceeding 2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT) 1–5. IEEE. https://doi.org/10.1109/CONECCT52877.2021.9622711
3. Arış A, Oktuğ SF (2020) Analysis of the RPL version number attack with multiple attackers. In: Proceeding 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). IEEE. https://doi.org/10.1109/CyberSA49311.2020.9139695
4. Barthel D, Vasseur JP, Pister K, Kim M, Dejean N (2012) Routing metrics used for path calculation in low-power and lossy networks. https://doi.org/10.17487/RFC6551
5. Bokka R, Sadasivam T (2021) DIS flooding attack Impact on the Performance of RPL Based Internet of Things Networks: Analysis. In: Proceeding 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC) 1017–1022 . IEEE. https://doi.org/10.1109/ICESC51422.2021.9532901
6. Ching TW, Aman AHM, Azamuddin WMH, Sallehuddin H, Attarbashi ZS (2020) Performance analysis of internet of things routing protocol for low power and lossy networks (RPL): energy, overhead and packet delivery. In: Proceeding 2021 3rd International Cyber Resilience Conference (CRC) 1–6. IEEE. https://doi.org/10.1109/CRC50527.2021.9392475
7. Dhamodharan USRK, Vayanaperumal R (2015) Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing method. Sci World J 2015:841267. https://doi.org/10.1155/2015/841267
8. Gaddour O, Koubaa A (2012) RPL in a nutshell: A survey. Comput Netw 56(14):3163–3178. https://doi.org/10.1016/j.comnet.2012.06.016
9. Helmer G, Wong JS, Honavar V, Miller L, Wang Y (2003) Lightweight agents for intrusion detection. J Syst Softw 67(2):109–122. https://doi.org/10.1016/S0164-1212(02)00092-4
10. Hkiri A, Karmani M, Machhout M (2022) The routing protocol for low power and lossy networks (RPL) under attack: simulation and analysis. In: 2022 5th International Conference on Advanced Systems and Emergent Technologies (IC_ASET) ,143–148. IEEE. https://doi.org/10.1109/IC_ASET53395.2022.9765901
11. Le A, Loo J, Luo Y, Lasebae A (2013) July The impacts of internal threats towards routing protocol for low power and lossy network performance. In: 2013 IEEE symposium on computers and communications (ISCC) ,000789-000794. IEEE. https://doi.org/10.1109/ISCC.2013.6755045
12. Luangoudom S, Tran D, Nguyen T, Tran HA, Nguyen G, Ha QT (2020) svBLOCK: Mitigating black hole attack in low-power and lossy networks. Int J Sens Netw 32(2):77–86. https://doi.org/10.1504/IJSNET.2020.104923
13. Mainetti L, Patrono L, Vilei A (2011) Evolution of wireless sensor networks towards the internet of things: A survey. In: SoftCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks , 1–6. IEEE
14. Network Simulator, NetSim, Emulator, 5G, Military Communication, Vehicular networks. Accessed 7 Jan 2022. https://www.tetcos.com/
15. Patel BH, Shah P (2020) RPL routing protocol performance under sinkhole and selective forwarding attack: experimental and simulated evaluation. TELKOMNIKA (Telecommunication Computing Electronics and Control) 18(4):1849–1856. https://doi.org/10.12928/telkomnika.v18i4.15768
16. Perazzo P, Vallati C, Anastasi G, Dini G (2017) DIO suppression attack against routing in the Internet of Things. IEEE Commun Lett 21(11):524–2527. https://doi.org/10.1109/LCOMM.2017.2738629
17. Raoof A, Matrawy A, Lung CH (2018) Routing attacks and mitigation methods for RPL-based Internet of Things. IEEE Commun Surv Tutor 21(2):1582–1606. https://doi.org/10.1109/COMST.2018.2885894
18. Raoof A, Matrawy A, Lung CH (2020) Enhancing routing security in IoT: Performance evaluation of RPL's secure mode under attacks. IEEE Internet Things J 7(12):11536–11546. https://doi.org/10.1109/JIOT.2020.3022276
19. Raza S, Wallgren L, Voigt T (2023) SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Netw 11(8):2661–2674. https://doi.org/10.1016/j.adhoc.2013.04.014
20. Sethi P, Sarangi SR (2017) Internet of things: architectures, protocols, and applications. J Electr Comput Eng. https://doi.org/10.1155/2017/9324035
21. Sharma G, Grover J, Verma A (2023) Performance evaluation of mobile RPL-based IoT networks under version number attack. Comput Commun 197:12–22. https://doi.org/10.1016/j.comcom.2022.10.014
22. Singh G, Cheema AK, Kapoor N (2017) Performance evaluation of routing protocol in Internet of Things using Netsim. Int

J Adv Comput Res 8(3). http://ijarcs.info/index.php/Ijarcs/article/view/3114
23. Stephen R, Arockiam L (2007) Intrusion detection system to detect sinkhole attack on RPL protocol in Internet of Things. International Journal of Electrical Electronics and Computer Science 4(4):16–20
24. Tonapa YT, Wahidah I, Karna NBA (2020) Performance Testing Of Routing Protocol For Low Power And Lossy Networks (rpl) Against Attack Using Cooja Simulator. eProceedings of Engineering 7(2):4093–4101
25. Verma A, Ranga V (2018) Analysis of routing attacks on RPL based 6LoWPAN networks. Int J Grid Distrib Comput 11(8):43–56. https://doi.org/10.14257/ijgdc.2018.11.8.05

Mr. Raveendranadh Bokka received his M. Tech. Degree from the Department of Electronics and Communication Engineering with specialization in VLSI and Embedded Systems at SNIST, JNTU Hyderabad, India, in 2010. Currently he is pursuing his Ph.D. degree in Electronics and Communication Engineering from Pondicherry University. His current research interest includes Wireless Sensor Networks, Internet of Things Security, Machine Learning, and Deep Learning.

Dr. S. Tamilselvan received his Ph.D. degree from the Department of Electronics and Communication Engineering at Pondicherry University, Pondicherry, India, in 2011. He is currently working as Associate professor in the Department of Electronics and Communication Engineering at Puducherry Technological University, Puducherry, India. His research area of interest includes in Wireless Communication and Networks, Internet of Things, VLSI Design and Nano Electronics, and Image processing.