Investigating Routing Protocol Attack for Low Power and Lossy IoT Networks

Usha Kiran[1], Poonam Maurya[2], and Himanshu Sharma[3]

[1]Indian Institute of Technology Bhilai
[2]Aalborg Universitet Kobenhavn
[3]Krishna Institute of Engineering & Technology

May 29, 2023

Abstract

Internet-of-Things (IoT) networks are characterized by low-powered nodes with limited computational power and storage capacity. Consequently, protocols dedicated to Low Power and Lossy networks (LLNs) are designed to support communication in such resource-constrained nodes. One such protocol is Routing Protocol for Low-Power and lossy networks (RPL) which builds and maintains routes in RPL-based networks, leading to optimized routing and lower network overhead. However, the RPL-based protocol has several internal and external vulnerabilities that must be explored and addressed. Therefore, the present study illustrates the impact of several RPL-based attacks, including DIS attack, version number attack, decreased rank attack, and WPS attack, by employing the Contiki Cooja network simulator with specific simulation scenarios. In addition, we conduct a comparative analysis of the RPL-based attacks and find that the WPS attack results in the highest packet loss rate of 26%, whereas the DIS attack, version number attack, and rank attack result in packet loss rates of 17%, 15%, and 13%, respectively.

Investigating Routing Protocol Attack for Low Power and Lossy IoT Networks

Usha Kiran[1*], Poonam Maurya[2] and Himanshu Sharma[3]

[1]Department of Computer Science, Indian Institute of Technology Bhilai, India.
[2]Department of Electronics Systems, Aalborg University, Denmark.
[3]Department of Electronics & Communications, KIET Group of Institutions, Ghaziabad, India.

*Corresponding author(s). E-mail(s): ushak@iitbhilai.ac.in;
Contributing authors: poonamm@es.aau.dk; himanshu.researcher1@gmail.com ;

Abstract

Internet-of-Things (IoT) networks are characterized by low-powered nodes with limited computational power and storage capacity. Consequently, protocols dedicated to Low Power and Lossy networks (LLNs) are designed to support communication in such resource-constrained nodes. One such protocol is Routing Protocol for Low-Power and lossy networks (RPL) which builds and maintains routes in RPL-based networks, leading to optimized routing and lower network overhead. However, the RPL-based protocol has several internal and external vulnerabilities that must be explored and addressed. Therefore, the present study illustrates the impact of several RPL-based attacks, including DIS attack, version number attack, decreased rank attack, and WPS attack, by employing the Contiki Cooja network simulator with specific simulation scenarios. In addition, we conduct a comparative analysis of the RPL-based attacks and find that the WPS attack results in the highest packet loss rate of 26%, whereas the DIS attack, version number attack, and rank attack result in packet loss rates of 17%, 15%, and 13%, respectively.

Keywords: RPL attacks, DIS attack, Version number attack, Decreased rank attack, Worst parent selection attack, Intrusion detection system

1 Introduction

Routing Protocol for Low power and lossy network (RPL) has been specifically designed for IoT networks where nodes consume low power for computing and have less memory for information storage [1, 2]. RPL protocol builds and maintains efficient routes for packets in Low Power and Lossy networks (LLNs) to enable effective communication between nodes while minimizing energy consumption and reducing network overhead. RPL uses Destination Oriented Directed Acyclic Graph (DODAG) for routing purposes. DODAG connects all the nodes and does not form or allow any cycle (loop) in the network. Further, to form and manage a DODAG tree, RPL uses three control messages, namely, DODAG Information Object (DIO), DODAG Information Solicitation (DIS), and DODAG Destination Advertising Object (DAO) [3, 4], as illustrated in Fig. 1.

As shown in the Fig. 1, firstly, the root (sink) node disseminates the DIO control message throughout the network. DIO packets contain

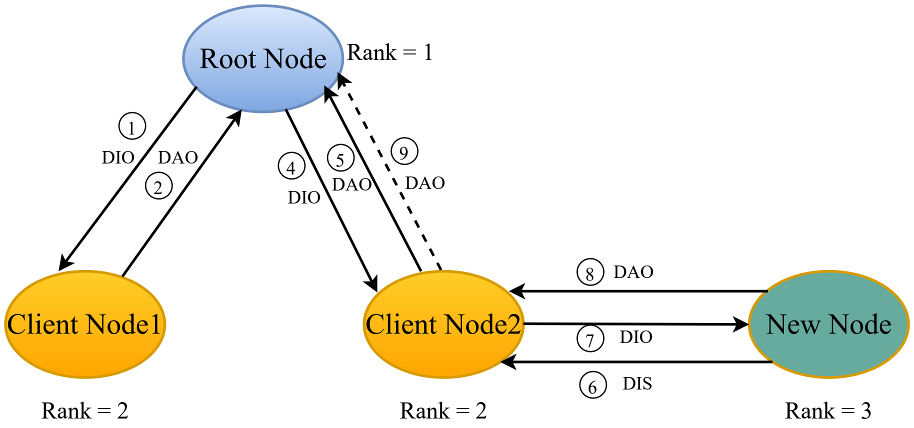


Fig. 1: DODAG tree construction process.

information regarding the sender node that helps a receiver node to select a preferred parent and keep the DODAG tree up to date. After selecting a preferred parent, the node advertises a DAO packet back to the root node in unicast mode across nearby nodes. It establishes and maintains the upward routing path through the DODAG tree [5, 6].

The DIS message seeks information regarding DODAG from neighboring nodes. As shown in the Fig. 1 when a new node wishes to join an existing or developing DODAG, it transmits a DIS message requesting information about the DODAG. The node receives a DIO message in response. DIO message contains all the relevant information regarding the node, like node id, node rank, path cost, and other matrices using which node determines whether to join the graph. After entering the tree and selecting the parent node, the node sends a DAO message to the root node through parent nodes [7].

A 16-bit rank value of a node in the DODAG tree determines the node's position relative to the root node. By default, the root node (server node/sink node) has a minimum rank value compared to all nodes in the tree [8, 9]. For instance, if the rank of the root node in RPL is one, the rank of the child nodes will be two, and the rank value will increase by one for each subsequent layer in the DODAG tree as shown in the Fig. 1. After network formation, every node possesses information regarding the node ID, rank, parent node ID, parent node rank, neighboring nodes' ID and rank, and the link matrix. Further to select the parent node, RPL uses two objective functions, i.e., Objective Function Zero (of0) and Hysteresis Objective Function (MRHOF). For example, when deciding which parent a node prefers, MRHOF utilizes the Expected Transmission Count (ETX), while of0 uses the hop count [10, 11]. However, the RPL protocol has several vulnerabilities, especially internal security issues, as shown in Fig. 2. RPL attacks can be categorized as topology-based, resource-based, or traffic-analysis-based attacks [12–14]. Attacks against resources force legitimate nodes to perform extra processing to deplete their resources like energy, memory, or processing capabilities [15]. Resource-based attacks may affect the network's availability by congesting available links and, thus, the network's lifespan, which may be considerably reduced. We categorize attacks against resources into two types. The first consists of direct attacks, in which a malicious node directly launches this attack, for example, flooding attack [16], where a malicious node generates many unnecessary packets to congest the network. In the indirect attack, the malicious node forces other nodes to perform malicious activities. For example, a version number attack, where a malicious node advertises a false version number, causes other nodes to send a control message to verify and update the version number [17, 18].

Network topology is potentially a target of attackers and can be categorized as 1) sub-optimization and 2) isolation [19]. A sinkhole attack comes under the category of a sub-optimization attack, where a malicious node

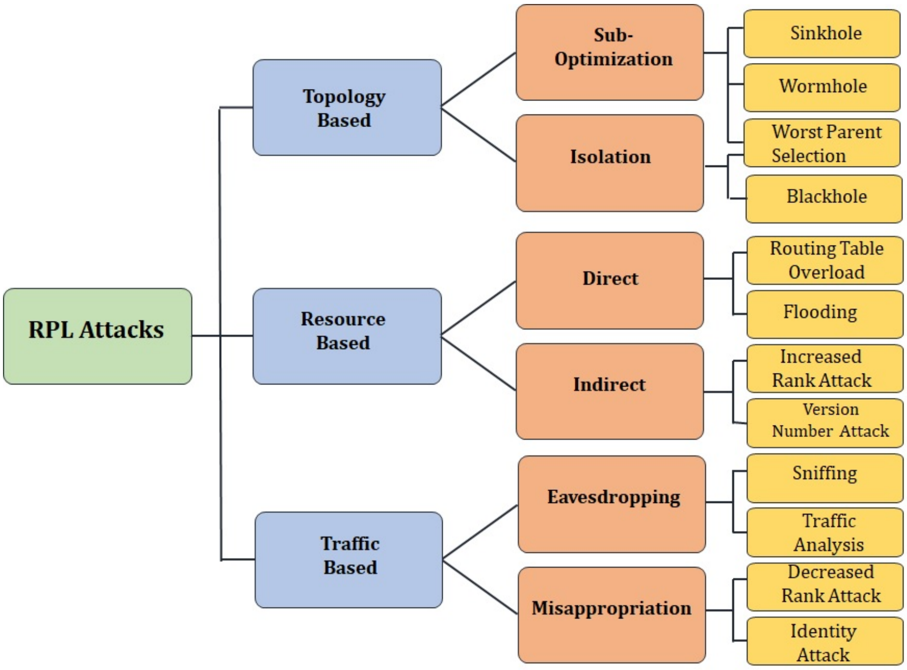


Fig. 2: Classification of vulnerabilities in RPL-based network.

attracts network traffic by advertising itself as having the shortest path to the root node, thus intercepting and redirecting network traffic to an unintended/unauthorized destination. Whereas an isolation attack makes several nodes isolated from the entire network, hence, preventing those nodes from communicating with the root or their parents. The worst parent selection attack is a type of isolation attack where the victim node selects the worst node from the surrounding [20–22].

The third category of RPL attack, known as traffic analysis, involves eavesdropping and misappropriation [23]. Traffic analysis tries to find out how to route traffic by looking at the characteristics and patterns of the traffic in a network. Furthermore, this attack is possible even if the packets are encrypted. For example, sniffing attacks aim to obtain relevant information related to the RPL network [24]. The location of the attacker node is very important since the node closer to the root node may gather maximum traffic and information [11].

Attacks that break intellectual property rights take over the identities of legitimate nodes (masquerading attacks) or exaggerate the functionalities of legitimate nodes. Furthermore, these attacks do not significantly harm the RPL network. However, such attacks are often used as a starting point for other attacks. For example, masquerading the root node may get maximum traffic from all the neighboring nodes. The decreased rank attack comes under this category, we will discuss this attack in a later section [25, 26].

While taking into consideration the demand for RPL-based IoT networks in various applications, it becomes very important to explore all its vulnerabilities and their corresponding mitigation and detection mechanisms. Therefore, in this paper, we discuss some of the prominent attacks of RPL-based networks, such as the DIS attack, version number attack, decreased rank attack, and WPS attack. Further, we investigate and analyze the effect of the above-mentioned attack on the network. Going forward, we perform a comparative analysis of the mentioned attacks. For the simulation purpose, we utilize the Contiki Cooja Simulator where nodes are referred to as motes, but we call them nodes in the paper for simplicity.

1.1 Novel Contribution

This study examines the security of RPL in IoT networks and the impact of RPL-based attacks on network performance. With the growing prevalence of IoT devices in different applications, ensuring network security and reliability has become increasingly crucial. Here are the novel contributions of our study:

1. Investigation and evaluation of RPL-based attacks including DIS attack, version number attack, rank attack, and WPS attack on the RPL protocol using Contiki Cooja network simulator.
2. Comparative analysis of the investigated RPL-based attack based on various performance metrics like power consumption, packet loss ratio, and others.
3. Comparison among attacks completely relies on results obtained after simulation of all the mentioned attacks in this paper.

1.2 Organization

The subsequent sections of this paper are structured as follows. Section 2 presents a thorough literature review encompassing current state-of-the-art work against RPL-based attacks. Theoretical foundations of the several RPL-based attacks are discussed in Section 3. Section 4 presents the experimental results and a detailed analysis of the outcomes. In Section 5, a comparative study of all the attacks is conducted. Finally, Section 6 concludes the work, offering insights into future directions for research.

2 Literature Review

The RPL protocol is widely used in IoT networks to enhance security to a high degree and has gained global acceptance. Significant progress has been made to explore and address the RPL vulnerabilities [27–30]. Some authors like Rajasekar and Rajkumar have implemented and analyzed the effect of DIS attack against RPL-based network [31]. In a DIS flooding attack, the increase in the number of attacker nodes causes a noticeable negative impact on packet delivery rate and power consumption. Active research has been done to mitigate and address the DIS flooding effect [32, 33]. In addition, some authors like Medjek et al. have proposed a mechanism to mitigate DIS attacks by making some changes in the RPL protocol itself [3]. For example, the authors have modified the response time of the RPL nodes to DIS messages and adjusted the RPL protocol's timer function to address the DIS attack. However, modification in the RPL protocol is burdensome. Further, the authors Verma and Ranga [16] proposed a mitigation mechanism to prevent the network from DIS flood attacks. The authors proposed a Secure-RPL to stop malicious nodes from sending DIO messages and resetting trickle timers. However, Secure-RPL required minimal extra work during installation on low-capacity nodes. Another prominent RPl-based attack is a version number attack; this attack drastically drops the packet delivery rate (PDR) in the network by creating congestion in the network. Some authors like Sharma, Girish et al. have illustrated that when there is a version number attack in the network, the average end-to-end delay increases as the number of nodes increases, and power consumption decreases because the network becomes dense. The nodes are near each other [17]. [34] has developed a distributed monitoring strategy for detecting version number attacks in RPL-Based Networks.

In Intrusion Detection System (IDS), whenever any node (except the root node) advertises the version number, receiving nodes verify the received version number by asking neighboring nodes and the root node [20, 35]. In case of conflicting information, a malicious node is blocklisted. Authors Wallgren et al. proposed a new IDS detecting routing attacks in an RPL-based network [36]. The name of the proposed IDS is Heartbeat which can detect selective forwarding attacks effectively. In the proposed IDS mechanism, an ICMPv6 echo request from the 6BR is sent to each node and expects a response. The authors utilized the concept that, in the case of a selective forwarding attack, 6BR will not receive a response from every node, hence detecting a selective forwarding attack. Furthermore, ICMPv6 echo/reply mechanisms are widely available in IPv6 networks [37]; reprogramming nodes are not required to make this IDS workable.

Further, a category where malicious node target the topology of an RPL-based network is a Rank attack. In a rank attack, a malicious node can affect the routing decision of victim nodes, may increase transmission delay, and increase traffic overhead in the network [38, 39]. Rehman et al.

proposed and analyzed rank attacks using objective functions [40]. However, the authors have modified the objective function in the proposed technique to launch the rank attack. Since the objective function has shifted, malicious nodes now appear to be the best nodes, attracting their neighbors' attention, who may then decide to make them their preferred parents. To prevent version number and rank attacks in RPL-based networks, Dvir et al. have proposed a protocol called VeRa [41]. The VeRa authenticates the version and rank numbers so that the integrity check can prevent the attack if any node forwards the wrong version number and ranks. The authors, however, did not include performance analysis of memory, CPU, time, and power. Instead, the authors employed computationally costly processes such as the hash function, the MAC function, and the digital signature.

Some attacks have gained less attention from researchers, like the worst parent selection (WPS) attack. Some authors like Kiran have discussed the WPS attack and IDS to detect WPS attack in [20]. In the WPS attack, a malicious node selects a node with a high-rank value from the surrounding as a parent node. Hence, it increases transmission delay. Sometimes, if the malicious node is the connecting node, then because of choosing the worst parent from the surroundings, a large number of nodes become isolated from the entire network. Further, the author has proposed IDS to detect WPS attacks. According to the IDS mechanism, the rank value of every node is compared with the surrounding node; if the parent of any node has a higher rank value from the surrounding, then immediately, IDS raises an attack alarm.

3 RPL-Based Attacks

In our study, we investigate DIS, rank, version number, and WPS attacks that can hinder the network from optimal convergence, may consume the network resources excessively, and may degrade the overall performance drastically.

3.1 DIS Attack

Initially, when a new node tries to join the DODAG tree, the node waits for a DIO message or multicast a DIS message to solicit DIOs from neighboring nodes [3]. However, sending Multicast DIS messages resets the timer that regulates the DIO transmission rate to its minimum value, causing the network to become congested with control messages. Moreover, due to the resource-constrained nature of RPL-LLNs, the lack of tamper resistance, and the security gaps in RPL, malicious nodes can use the Multicast DIS solicitation mechanism to launch an RPL-specification-based attack known as the DIS attack. The DIS attack can significantly impact RPL networks, particularly overhead control messages, and power consumption [42].

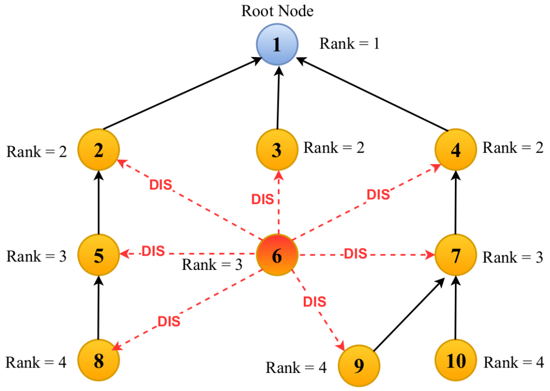


Fig. 3: DIS attack by generating a number of DIS packets by malicious node

DIS attack comes under the category of resource-based direct attack. This attack targets network resources by flooding them with a large amount of DIS control messages from multiple nodes. hence, making network resources unavailable for legitimate nodes [43]. As depicted in Fig. 3, node 6 is a malicious node that can send DIS control messages to neighboring nodes through broadcast or unicast, leading to increased network traffic. Hence increases the power consumption by nodes. DIS attack may cause disruption and make the network inaccessible for legitimate nodes, hence referred to as a *denial of service* attack.

We modify RPL files located in /Contiki/-core/net/rpl/ within the Contiki OS to investigate the DIS attack. We make changes to the following files: rpl_private.h and rpl_timers.h. Contiki RPL's rpl_private.h file contains the default values for ICMP control messages, related timers, operating mode, DAG routing tables, and other constant RPL values. Changing the value of the interval in the rpl_timers.c file causes malicious nodes to broadcast DIS messages continuously to neighboring nodes.

3.2 Version Number Attack

The RPL network provides global and local repair mechanisms for the following reasons: link failure, node failure, detects loops, or reception of any other inconsistent information. To initiate the global repair DODAG Version Number field within the DIO message is incremented. Only the root node can trigger the global repair mechanism. However, any non-root node that discovers an inconsistency (for example, a loop or connection failure) can initiate a local repair. The node should poison its routes by proclaiming a rank of INFINITE RANK. As a result, it breaks away from the DODAG and subsequently reconnects to it as a new joining node through a DIS message. Unfortunately, malicious nodes exploit this feature of local/global repair by spreading false version numbers and launching version number attacks in the RPL network [44].

As shown in the Fig. 4, node 7 is a malicious node that starts a local repair in a DODAG tree by sending a DIO message containing a higher version number [45]. Upon receiving the DIO message containing the revised version number, the nodes will subsequently start a local repair in a DODAG tree. The work proposed by the authors Dvir et al. [41] is vulnerable to this attack because it introduces inconsistency and topological inefficiency into their work. The attack simulation aims to learn how the constant receipt of DIO messages of higher version numbers affects the energy consumption by nodes. To implement the version number attack, we modify rpl_icmp6.c file. This file handles the input and output of control messages. Whenever a malicious node increases its version number due to the version number attack, it triggers a local repair in the DODAG tree.

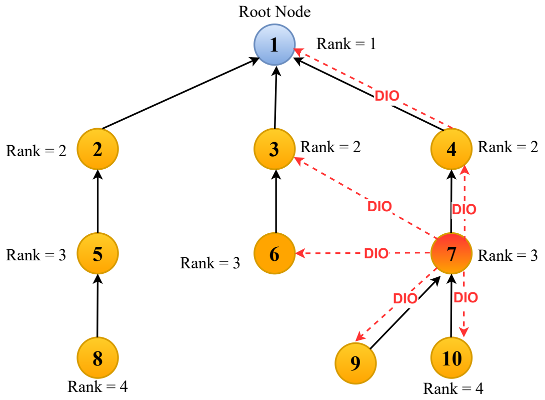


Fig. 4: VN attack by propagating higher version number through the DIO packet

3.3 Decreased Rank Attack

Rank is an attribute of a node in the RPL network that represents its position concerning the root node. However, malicious nodes can also exploit this attribute to harm the RPL network. For example, in a decreased rank attack, a malicious node introduced the false low rank through DIO to neighboring nodes, Resulting in neighboring nodes converging towards the malicious node and got select the malicious node as a preferred parent. Once a malicious node becomes the preferred parent node in the attacking region, it may help to launch several other attacks, like the blackhole attack, in which the malicious node deletes all the received messages it is supposed to forward toward the root node [46].

As shown in Fig.5, a malicious node 6 advertises its false rank (rank = 2) to neighboring nodes, resulting in nodes 8, 9, 10 selecting node 6 as a preferred parent. We modify the rpl_private.h

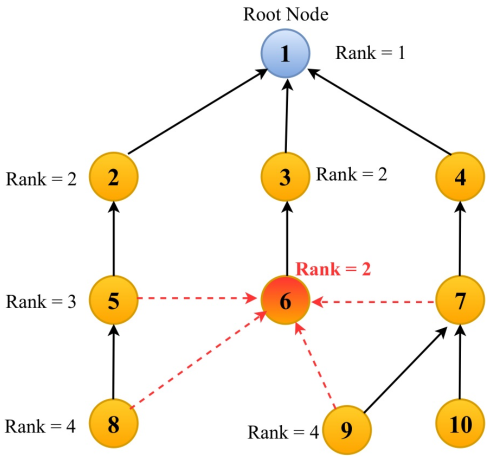


Fig. 5: Decreased rank attack by advertising lower rank

file. The rpl_private.h file contains the default values for ICMP control messages, relevant timings, operating mode, DAG routing tables, and other constant RPL values to execute the decreased rank attack.

3.4 Worst Parent Selection (WPS) Attack

RPL node uses objective functions to select a preferred parent. The Objective Function (OF) in RPL determines how RPL nodes choose the optimal path toward the root node in a network. For example, RPL nodes can use ETX as a routing metric for selecting parent or may use rank value to select parent node. However, modifying the parent selection procedure may lead to several attacks, including the worst parent selection (WPS) [20]. As we know, the root node has the minimum rank value among all nodes, so the RPL node selects a lower rank value node to have a route towards the root node. But, due to the effect of the WPS attack, the malicious node selects the worst (higher rank value) node from the neighboring node. The WPS attack may have the following effects on the network; it may increase transmission delay, create a loop in the RPL, prevent the network from optimal convergence, and isolate many nodes from the entire network. For example, as shown in Fig. 6, node 4 is malicious; due to the effect of the WPS attack, node 4 chooses node 8 as its parent, which is not the best possible choice of a preferred parent in the given scenario.

To implement the WPS attack, we change the algorithm in *rpl_mrhof.c* file that is used by nodes to select a preferred parent. Because of changes made in *rpl_mrhof.c* file, a malicious node chooses the worst parent from the surrounding nodes as the preferred parent.

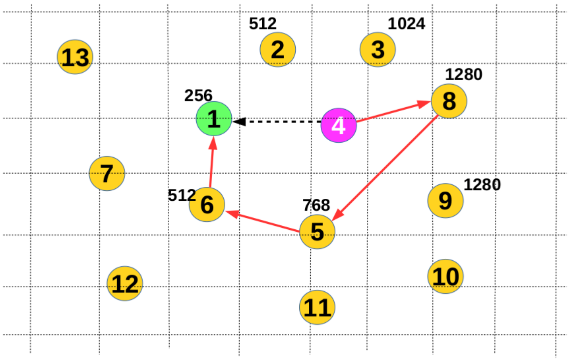


Fig. 6: WPS attack by selecting worst parent from the surrounding

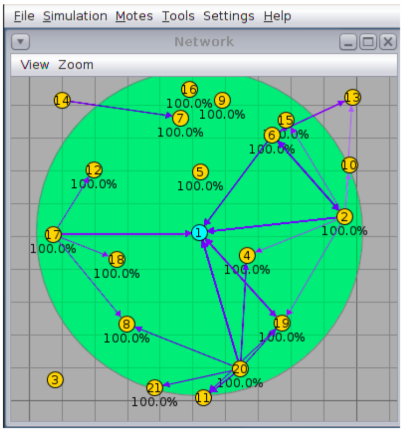
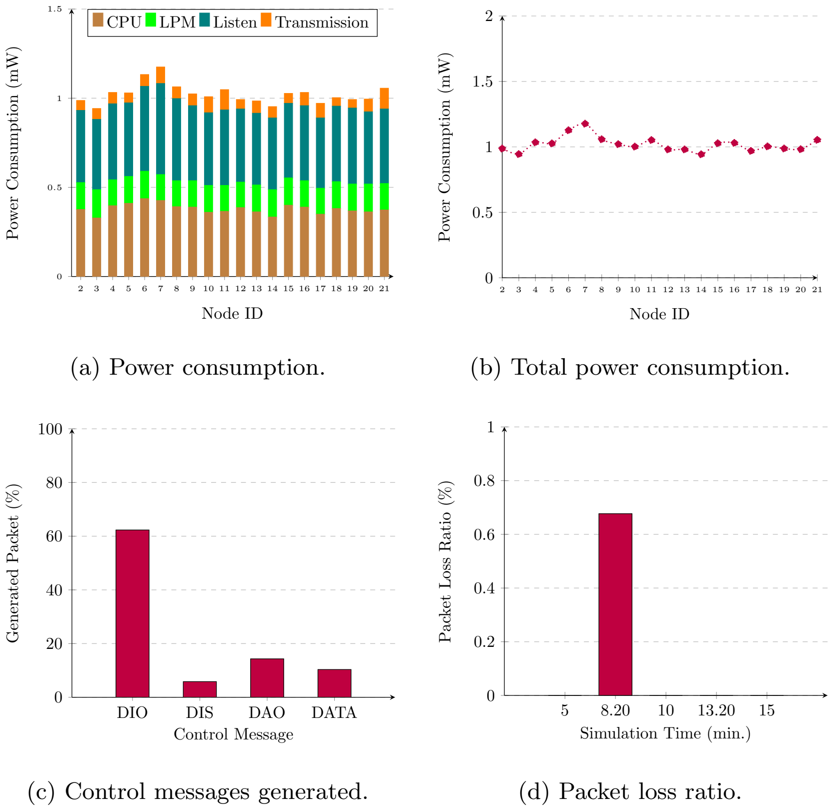


Fig. 7: Reference network with no malicious node

4 Experimental Results and Discussions

The network scenario shown in the Fig.7 is the reference network, the baseline scenario for further experiments. Further, we illustrate the outcomes obtained after simulation in normal and attack scenarios. The information collected from the reference network, as shown in the Fig.7, becomes the benchmark for comparing and assessing the results obtained in simulating RPL-based attacks covered in this paper: DIS and Version number attacks. We use the Contiki Cooja simulator for the simulation and analysis of the discussed attacks. The Cooja simulator offers a log file; the information gathered from the collect view editor is the basis for simulation result analysis.

Fig. 8 illustrates the simulation output obtained in normal scenario where we do not have any malicious nodes. Fig. 8a depicts the impact of power usage on the following parameter: CPU power is the amount of energy required to perform computation by nodes. LPM power refers to the energy a node consumes while in standby (idle) mode. Listen power is the energy a node consumes to listen for messages. Transmission power is the energy to transmit a message from the source to the destination node. Fig. 8b depicts the total energy consumed by nodes in a normal scenario.



(a) Power consumption.

(b) Total power consumption.

(c) Control messages generated.

(d) Packet loss ratio.

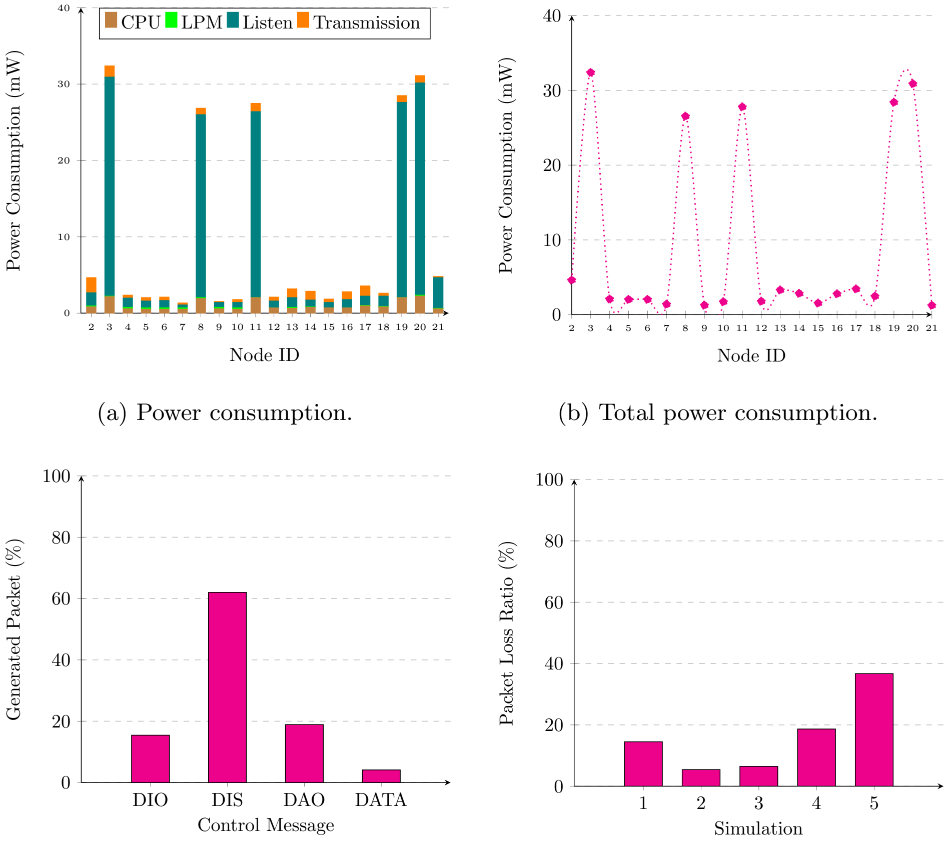
Fig. 8: Simulation results in the normal scenario (reference network).

The ratio of control packets to data packets generated by nodes is shown in Fig. 8c. Fig. 8d depicts the packet loss ratio (PLR) i.e., the proportion of lost packets to the total number of packets sent under normal circumstances.

Discussion: The reference network provides the baseline for other simulations. From the Fig. 8a, we can see the amount of power consumption nodes required during simulation. Fig. 8b shows the amount of total power required by the nodes; due to their resource-constrained nature, nodes do not consume much power on average or in totality. Therefore, any significant violation of the power consumption shown in Fig. 8a, 8b may indicate malicious activity in the network. Further, Fig. 8c shows that a number of DIO packets is generated more than other control messages as DIO is sent regularly. Again the reference network indicates how much control message needs to be generated. Any violation of this may require further investigation. From Fig. 8d, we can observe that, in a normal scenario, because of the lossy and resource-constrained nature of RPL nodes, we may have packet loss up to 1%. However, any scenario raising the packet loss more than mentioned in the reference network may indicate malicious activity or fault.

4.1 DIS Attack Results

In a DIS attack, a malicious node aims to flood the network by sending a huge number of DIS control messages. As a result, we may see unnecessary power consumption, network congestion, and high packet loss ratio; in the worst-case scenario, we may witness depletion of node resources in the network as shown in the Fig. 9. The Fig. 9a presents the power consumption results concerning: CPU power, LPM power, Listening power, and Transmitting power. Further, the total power consumption by the nodes in the network is shown in Fig. 9b. Finally, the percentage of control messages generated and packet loss ratio for each



(a) Power consumption.

(b) Total power consumption.

(c) Control message generated.

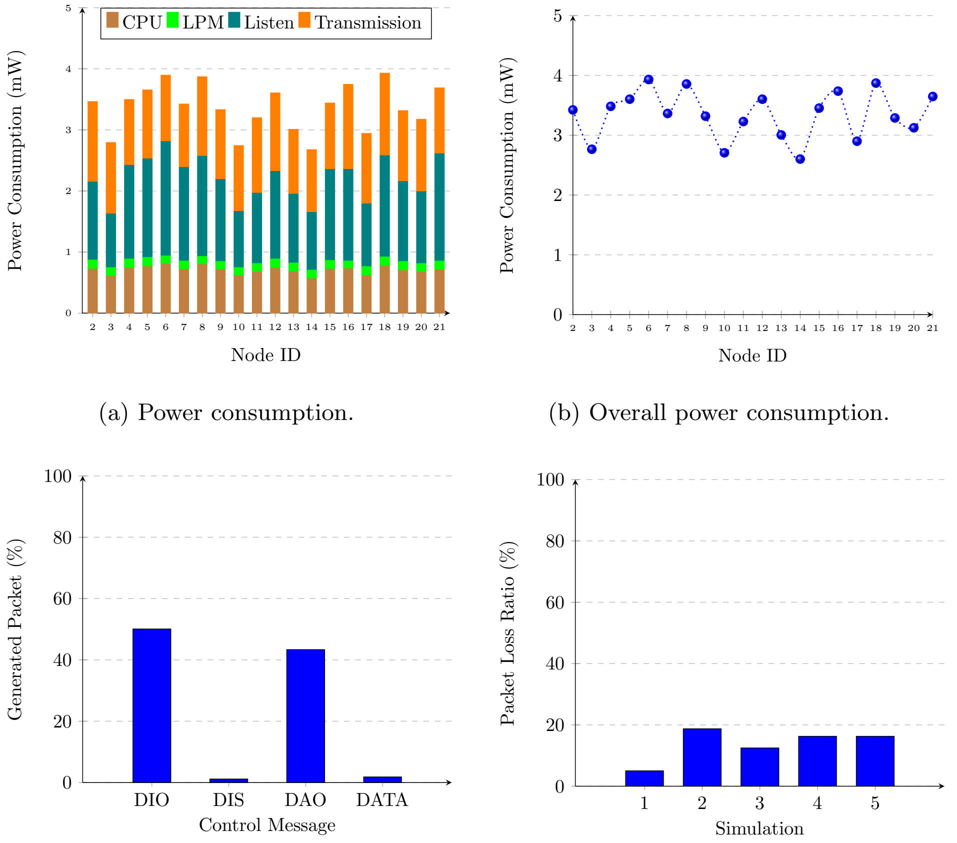
(d) Packet loss ratio.

Fig. 9: Simulation results for DIS attack scenario.

simulation are shown in Fig. 9c and Fig. 9d respectively.

Discussion - Comparing the outcome to the baseline network performance shown in Fig. 8a and Fig. 8b, we observe that the CPU, LPM, listen, transmission, and overall power consumption by the nodes have increased significantly in case of the DIS attack, as shown in Fig. 9a and Fig. 9b respectively. Nodes within the transmission range of a malicious node consume a substantial amount of resources. We may also conclude that the DIS attack directly affects nodes inside the malicious nodes' transmission range.

Additionally, there is a correlation between the malicious node's distance and energy expenditure against all other nodes. Except for the LPM numbers, all power indicators have risen substantially. The LPM value is the total energy required to keep the node on standby. Therefore, we deduce that DIS message-triggered requirements keep nodes alive longer. Also, nodes with lower LPM consumption values are closer to the malicious node. We can observe that neither the loop avoidance (the DIS attack does not affect the DIO messages) nor the DODAG local/global repair methods have been activated. However, there is a significant increase in the DIS (62%) control message generated during the DIS attack (see Fig. 9c) as compared to the DIS control message (5%) generated in a normal scenario (see Fig. 8c). Further, we can observe that in a normal scenario, due to the lossy nature of the RPL network, we have a packet loss ratio of about 1% (see Fig. 8d), whereas in the DIS attack scenario, we have packet loss upto 38% (see Fig. 9d). The increase in packet loss ratio may degrade the overall performance of the



(a) Power consumption.

(b) Overall power consumption.

(c) Control messages generated.

(d) Packet loss ratio in various simulations.

Fig. 10: Simulation results for version number attack scenario.

RPL network and make the network unreliable for communication purposes.

4.2 Version Number Attack

In a DODAG version number attack, a malicious node publishes a higher DODAG version number to neighboring nodes. In response, receiving nodes call unnecessary local/global repair processes in the network. Therefore, RPL activates a global repair process to build a new DODAG tree due to variations in the version number. As a consequence, traffic will overwhelm, and nodes will consume more [43] as shown in the Fig. 10. Fig. 10a and Fig. 10b illustrate the amount of power consumption for CPU, LPM, Listen, Transmit, and total power consumption, respectively. The other simulation results shown in Fig. 10c and Fig. 10d indicate the control packets generated and the packet loss ratio during the simulation, respectively. **Discussion** - The Fig. 10a and Fig. 10b show an increase in total power consumption across all nodes during the version number attack as compared to the normal scenario (see Fig. 8a, 8b). However, we do not find any correlation between the distance to the malicious node and the amount of energy consumed; however, nodes located close to the malicious node slightly increase power consumption (see Fig. 10a, 10b).

Further, as shown in the Fig. 10c, we can observe the increase in the number of DAO messages (42%) compared to normal scenario DAO messages (17%) as nodes are sending their parent information through DAO message through upward nodes to the root node to complete network repair process again and again. Further, there is a relation between the position of a malicious node and packet loss ratio, as we can see in the Fig. 10d, nodes close to the malicious node are busy sending control message instead of transmission of the data packet. In some cases, the network may experience packet loss up to 18% (see Fig. 10d) as well in this attack scenario.

4.3 Decreased Rank Attack

Fig. 11 is the reference network for the decreased rank attack. Further, we demonstrate the effect of decreased rank attack and show the scenario obtained before and after the decreased rank attack in the Fig. 12. In the Cooja simulator, for every network simulation, the Cooja displays a network map showing the nodes' connectivity, especially how nodes are connected to reach the root node. So, Fig. 12a, 12b are the network maps obtained after simulation in normal and the decreased rank attack, respectively. For clarity, we illustrate the same network map in the Fig. 12c, 12d.

Discussion - In the normal scenario, as shown in the Fig. 12c, node 21 is the parent node for nodes 5 and 7, and node 21 is directly connected to node 1. Nodes 9, 15, 17, and 19 are also directly connected to node 1. Now consider an attack scenario where node 21 is the malicious node that advertises its lower rank and tries to attract neighboring nodes. Therefore, due to the effect of the decreased rank attack as shown in the Fig. 12d, node 21 becomes the parent node of 5, 7, 9, 15, 17, and 19. From the results obtained from Fig. 12, it is evident that a malicious node attracts many nodes by propagating a false value of its rank. However, there is no significant effect on other factors except transmission delay since malicious nodes usually deliver packets.

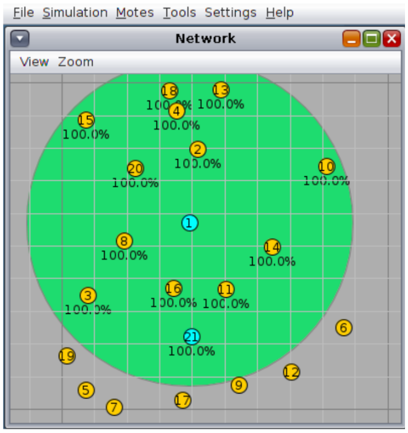


Fig. 11: Reference scenario for the decreased rank attack.

4.4 WPS Attack

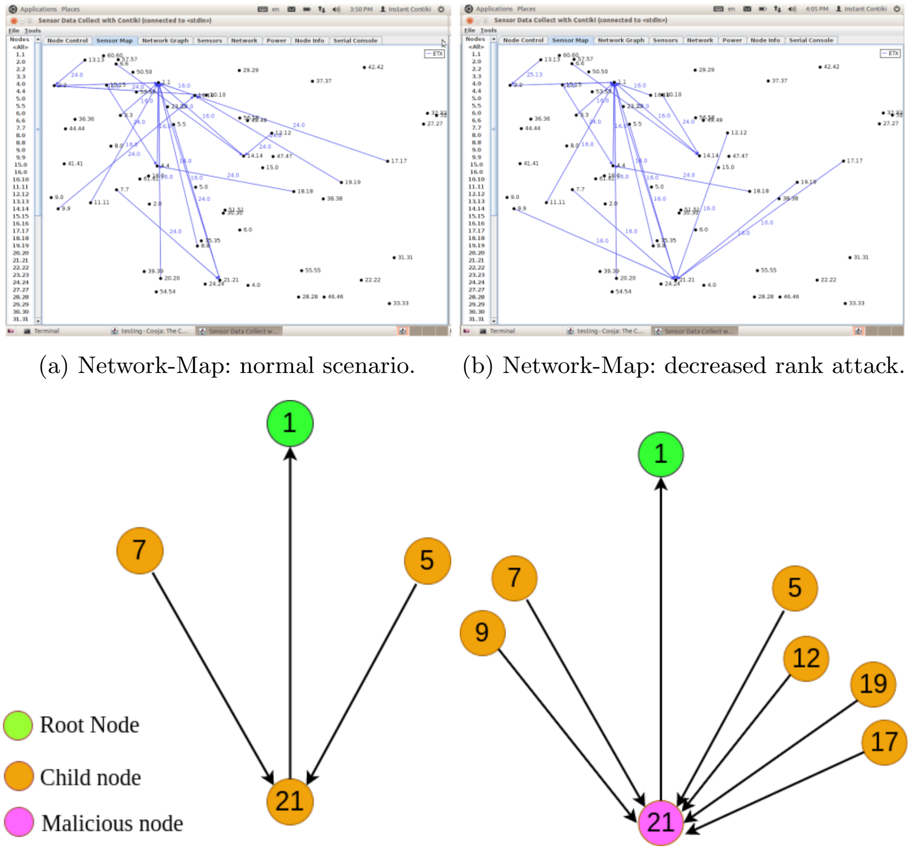
Fig. 13 is the reference network for the worst parent selection (WPS) attack. In a normal scenario (when no attack exists), node 1 is the root node, and all other nodes are client nodes. However, node 21 is malicious in the attack scenario, and the rest of the nodes behave as in the normal scenario. Further, in this scenario, the malicious node is the connecting node that connects nodes 2, 3, 4, 5, 8, 9, 10, 13, and 20 and the root node.

The Fig. 14 illustrate the result of simulations in normal and in the WPS attack scenarios. The Fig. 14a represents the network map obtained in a normal scenario, whereas Fig. 14b illustrates the network map obtained in the WPS attack scenario. Furthermore, we compare control messages generated in normal and attack scenarios as shown in the Fig. 15a. Further, in the Fig. 15b, we illustrate average and total transmission delay in the case of normal and attack scenarios. In addition, the Fig. 15c demonstrate the effect of the WPS attack in terms of the packet loss ratio and packet transmission delay compared to the normal scenario.

Discussion - We can observe from the Fig. 14 due to the effect of the WPS attack; the malicious node chooses the worst node from the surroundings, i.e., node 9. However, a malicious node is the only node reaching the root node and can transmit the packets from its surrounding nodes to the root node. Therefore, neighboring nodes of the malicious node form a loop due to unreachability toward the root node. Hence form a loop in the network, which violates one of the properties of the RPL network. Hence, in this scenario, a significant number of nodes become isolated from the entire network.

Further, as shown in the Fig. 15, we compare some of the network performance parameters to compare the effect of the WPS attack against normal scenarios. The Fig. 15a shows the number of control packets (DIO, DIS, DAO) generated during normal and WPS attack simulations. In the normal scenario, DIO packets account for the highest percentage (65.14%), followed by DAO packets (19.24%) and DIS packets (9.22%). During a WPS attack, the percentage of DIO and DIS packets generated remains relatively low (9.02% and 0.80%, respectively), while the percentage of DAO packets increases significantly (84.19%). DAO packets are transmitted at the time node selects its parent and send DAO packet back to the root node through the intermediate nodes to notify about its parent and to form an upward route. So, we can observe that, because of unreachability towards the root node, nodes send DAO packets repeatedly to set the upward route towards the root node.

The Fig. 15b shows average transmission delay and total transmission delay in normal and WPS attack scenarios. In the case of a WPS attack, the average delay is lower compared to the normal scenario, but the total delay is higher. The results imply that the WPS attack may have some scenarios for which transmission delay may increase significantly. The simulation result in Fig. 15c illustrates packet received ratio (PRR) and packet loss ratio (PLR) in the normal and WPS attack scenario. In the normal scenario, approximately 95% of the packets were received. Only 5% of the packets were lost due to the lossy nature of the RPL network. While in the WPS attack scenario, approximately 78% of the packets were received, and approximately 25% of the packets were lost (in case a significant number of nodes become isolated). Overall, the WPS attack caused a significant decrease in the PRR and an increase in the PLR. So, the effect of the WPS attack may be drastic in some cases and may make the network unreliable for communication purposes. So, finally, we can conclude that due to the effect of the WPS attack, transmission delay increases, create a loop



(a) Network-Map: normal scenario.

(b) Network-Map: decreased rank attack.

(c) Parent selection: normal scenario.

(d) Parent selection: attack scenario.

Fig. 12: Decreased rank attack effect in the parent selection process.

in the RPL-based network, prevent the network from optimal convergence, and isolate many nodes from the entire network.

5 Comparative analysis of RPL attacks

This section provides a comparative analysis of the discussed RPL-based attacks. Fig. 16 shows the packet loss ratio in the following RPL-based attacks scenarios: DIS attack, version number attack, rank attack, and WPS attack. From the Fig. 16, it can be deduced that the WPS attack has the maximum packet loss ratio as it isolates a significant number of nodes from the network. As compared to WPS, the packet loss ratio in DIS, VNA, and WPS are less, approximately 50%, 74%, and 88%. Furthermore, Table 1 compares the control packets generated in different attack scenarios. The decreased rank attack generates the highest number of DIO packets, potentially leading to network congestion and increased latency. The version number attack generates the highest number of DAO packets, focusing on node discovery and route creation rather than data transmission. On the other hand, the DIS attack generates the highest number of DIS packets, indicating its aim to prevent nodes from discovering each other.

6 Conclusion

This paper has discussed and evaluated the following RPL-based attacks: DIS attack, version number attack, decreased rank attack, and WPS attack. DIS attack floods the network by forcing nodes to send DIS control messages to cause network congestion. Moreover, in the DIS attack, the overall power consumption of all nodes increases significantly. Whereas version number attack forces RPL to activate a local/global repair to build a new DODAG tree due to the malicious node's propagation of the wrong version number. We have also experienced an increase in total power consumption across all nodes during the version number attack. Further, during the decreased rank attack, it is evident that a malicious node attracts many nodes by propagating a false rank value. However, we did not experience increased power consumption, but the transmission delay rose significantly, and especially, this attack may open the door for other attacks like blackhole attacks. Finally, in the WPS attack, the malicious node selects the worst node from the surroundings. Consequently, transmission delay increases, creating a loop in the RPL-based network, preventing the network from optimal convergence, and isolating many nodes from the entire network.

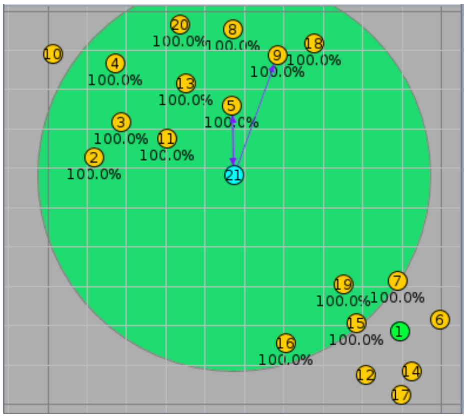


Fig. 13: Reference network for WPS attack.

Table 1: Comparison of control packets generated in various scenario.

Attacks	DIO	DIS	DAO	Data
RN	62.18	5.57	14.2	9.85
VNA	49.99	3.88	43.08	1.69
DIS	15.07	61.9	18.78	3.89
DRA	60.23	6.02	13.79	8.77
WPS	59.99	7.02	15.23	10.12

Finally, we present a comparative study of different RPL-based attacks, indicating that the WPS attack is more harmful than other attacks in affecting network performance and forcing many nodes to become isolated. Moreover, transmission delay increases in the WPS attack, creating a loop in the RPL-based network, preventing the network from optimal convergence, and isolating many nodes from the entire network. In the future, more RPL-based attacks can be analyzed to see the effect of attacks on the network and to design a detection system for the attacks.

Abbreviation

DODAG	Destination Oriented Directed Acyclic Graph
DIO	DODAG Information Object

DIS	DODAG Information Solicitation
DAO	DODAG Destination Advertising Object
ETX	Expected Transmission Count
IDS	Intrusion Detection System
IoT	Internet-of-Things
LLNs	Low Power and Lossy Networks
MRHOF	Hysteresis Objective Function
PDR	Packet Delivery Rate
RN	Reference Network
RPL	Routing Protocol for Low Power and Lossy Networks
VNA	Version Number Attack
WPS	Worst Parent Selection

Conflict of Interest

All authors declare that they have no conflict of interest.

Data availability

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

References

[1] Ali Seyfollahi and Ali Ghaffari. A review of intrusion detection systems in RPL routing protocol based on machine learning for internet of things applications. *Wireless Communications and Mobile Computing*, 2021:1–32, 2021.

[2] Temur ul Hassan, Muhammad Asim, Thar Baker, Jawad Hassan, and Noshina Tariq. CTrust-RPL: A control layer-based trust mechanism for supporting secure routing in routing protocol for low power and lossy networks-based Internet of Things applications. *Transactions on Emerging Telecommunications Technologies*, 32(3):1–20, 2021.

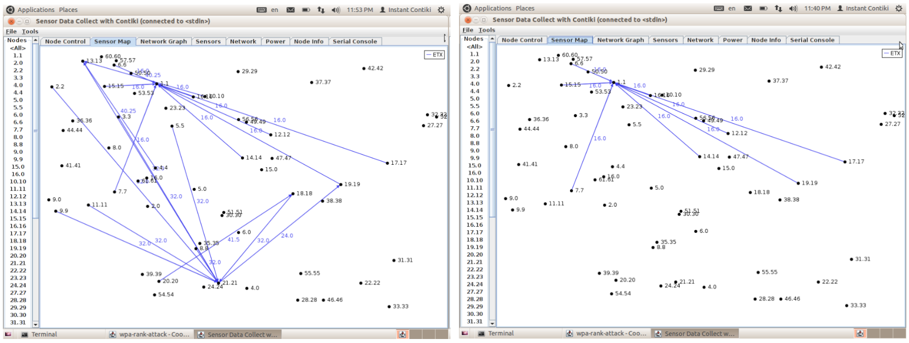
[3] Faiza Medjek, Djamel Tandjaoui, Nabil Djedjig, and Imed Romdhani. Multicast DIS attack mitigation in RPL-based IoT-LLNs. *Journal of Information Security and Applications*, 61:102939, 2021.

[4] Arvind Kamble, Virendra S Malemath, and Deepika Patil. Security attacks and secure routing protocols in RPL-based Internet of Things: Survey. In *2017 International Conference on Emerging Trends & Innovation in ICT (ICEI)*, pages 33–39. IEEE, 2017.

[5] Rashmi Sahay, G Geethakumari, and Barsha Mitra. A novel blockchain based framework to secure IoT-LLNs against routing attacks. *Computing*, 102:2445–2470, 2020.

[6] Fatma Mohamed Alatersh, Salem Sati, and Mohamed Sullabi. Impact of network topologies on RPL Performance. In *2021 22nd International Arab Conference on Information Technology (ACIT)*, pages 1–7. IEEE, 2021.

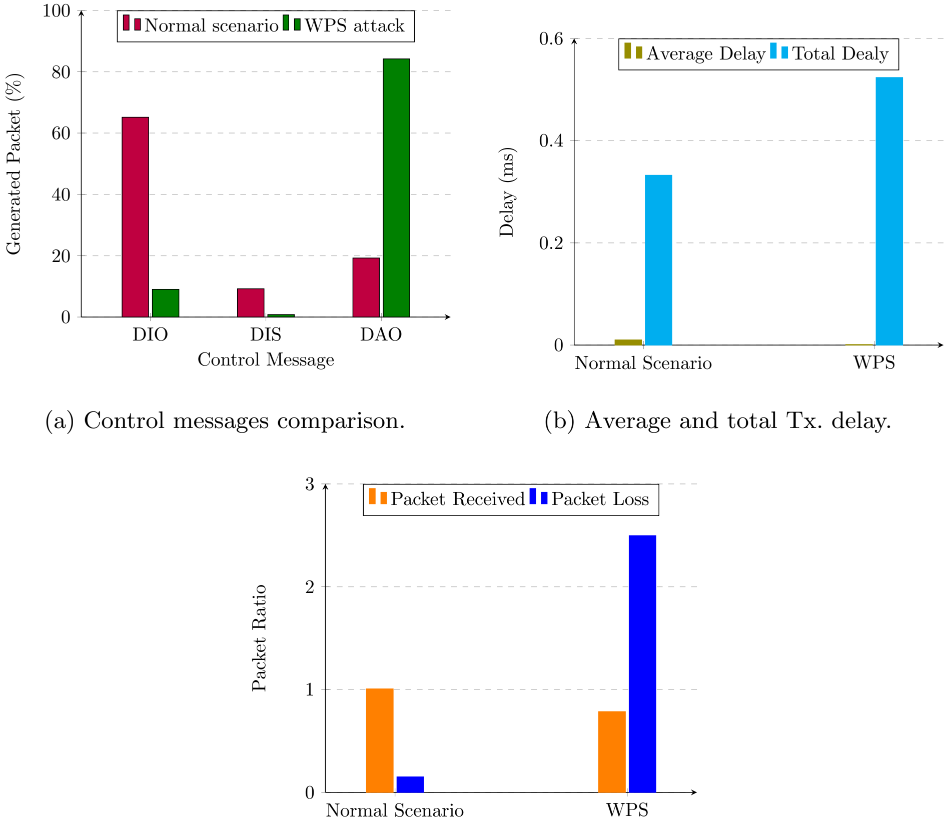
[7] Eden Hunde, Diana Deac, Steffen Thielemans, Matthias Carlier, Kris Steenhaut,



(a) Reference network.

(b) WPS-attack.

Fig. 14: Network map obtained in normal and in the WPS-attack scenario.



(a) Control messages comparison.

(b) Average and total Tx. delay.

(c) Packet received and packet loss ratio.

Fig. 15: WPS attack effect on: control packet generation and network parameters.

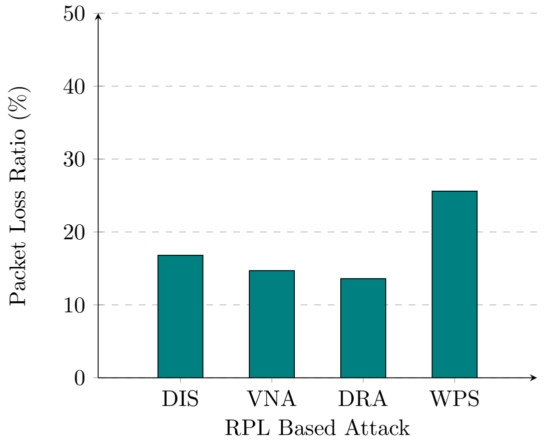


Fig. 16: Comparative analyses of RPL attacks.

An Braeken, and Virgil Dobrota. Time slotted channel hopping and contikimac for ipv6 multicast-enabled wireless sensor networks. *Sensors*, 21(5):1–26, 2021.

[8] Ghulam Shabbir, Adeel Akram, Muhammad Munwar Iqbal, Sohail Jabbar, Mai Alfawair, and Junaid Chaudhry. Network performance enhancement of multi-sink enabled low power lossy networks in SDN based Internet of Things. *International Journal of Parallel Programming*, 48(2):367–398, 2020.

[9] Anhtuan Le, Jonathan Loo, Aboubaker Lasebae, Mahdi Aiash, and Yuan Luo. 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach. *International Journal*

of Communication Systems, 25(9):1189–1212, 2012.

[10] Arslan Musaddiq, Yousaf Bin Zikria, Sung Won Kim, et al. Routing protocol for Low-Power and Lossy Networks for heterogeneous traffic network. *EURASIP Journal on Wireless Communications and Networking*, 2020(1):1–23, 2020.

[11] Arun Kumar, Sharad Sharma, Nitin Goyal, Sachin Kumar Gupta, Saru Kumari, and Sachin Kumar. Energy-efficient fog computing in Internet of Things based on Routing Protocol for Low-Power and Lossy Network with Contiki. *International Journal of Communication Systems*, 35(4):e5049, 2022.

[12] Ankur O Bang, Udai Pratap Rao, Pallavi Kaliyar, and Mauro Conti. Assessment of routing attacks and mitigation techniques with RPL control messages: A survey. *ACM Computing Surveys (CSUR)*, 55(2):1–36, 2022.

[13] Andrea Agiollo, Mauro Conti, Pallavi Kaliyar, Tsung-Nan Lin, and Luca Pajola. DETONAR: Detection of routing attacks in RPL-based IoT. *IEEE Transactions on Network and Service Management*, 18(2):1178–1190, 2021.

[14] Taief Alaa Al-Amiedy, Mohammed Anbar, Bahari Belaton, Abdullah Ahmed Bahashwan, Iznan Husainy Hasbullah, Mohammad Adnan Aladaileh, and Ghada AL Mukhaini. A systematic literature review on attacks defense mechanisms in RPL-based 6LoWPAN of Internet of Things. *Internet of Things*, page 100741, 2023.

[15] A Sofi, J Jane Regita, Bhagyesh Rane, and Hieng Ho Lau. Structural health monitoring using wireless smart sensor network–An overview. *Mechanical Systems and Signal Processing*, 163:108113, 2022.

[16] Abhishek Verma and Virender Ranga. Mitigation of DIS flooding attacks in RPL-based 6LoWPAN networks. *Transactions on emerging telecommunications technologies*, 31(2):e3802, 2020.

[17] Girish Sharma, Jyoti Grover, and Abhishek Verma. Performance evaluation of mobile RPL-based IoT networks under version number attack. *Computer Communications*, 197:12–22, 2023.

[18] Theodore Zahariadis, Helen C Leligou, Panagiotis Trakadas, and Stamatis Voliotis. Trust management in wireless sensor networks. *European Transactions on Telecommunications*, 21(4):386–395, 2010.

[19] Arash Heidari and Mohammad Ali Jabraeil Jamali. Internet of Things intrusion detection systems: A comprehensive review and future directions. *Cluster Computing*, pages 1–28, 2022.

[20] Usha Kiran. IDS To Detect Worst Parent Selection Attack In RPL-Based IoT Network. In *2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, pages 769–773. IEEE, 2022.

[21] Areej Althubaity, Reda Ammar, and Song Han. Detecting Rules-related Attacks in RPL-based Resource-Constrained Wireless Networks. In *2020 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, pages 1–8. IEEE, 2020.

[22] Aadil Sarwar Khan, Abdul Qayyum Khan, Naeem Iqbal, Muhammad Sarwar, Atif Mahmood, and M Asim Shoaib. Distributed fault detection and isolation in second order networked systems in a cyber–physical environment. *ISA transactions*, 103:131–142, 2020.

[23] Sambuddho Chakravarty, Georgios Portokalidis, Michalis Polychronakis, and Angelos D Keromytis. Detection and analysis of eavesdropping in anonymous communication networks. *International Journal of Information Security*, 14:205–220, 2015.

[24] George Simoglou, George Violettas, Sophia Petridou, and Lefteris Mamatas. Intrusion detection systems for RPL security: a comparative analysis. *Computers & Security*, 104:102219, 2021.

[25] Zahrah A Almusaylim, Abdulaziz Alhumam, and NZ Jhanjhi. Proposing a secure RPL based internet of things routing protocol: A review. *Ad Hoc Networks*, 101:102096, 2020.

[26] Yujing Liu, Wei Peng, and Jinshu Su. A study of IP prefix hijacking in cloud computing networks. *Security and Communication Networks*, 7(11):2201–2210, 2014.

[27] Fatima tuz Zahra, NZ Jhanjhi, Sarfraz Nawaz Brohi, Nazir A. Malik, and Mamoona Humayun. Proposing a Hybrid RPL Protocol for Rank and Wormhole Attack Mitigation using Machine Learning. In *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, pages 1–6, 2020.

[28] Abhishek Verma and Virender Ranga. Security of RPL Based 6LoWPAN Networks in the Internet of Things: A Review. *IEEE Sensors Journal*, 20(11):5666–5690, 2020.

[29] Mohammed Amine Boudouaia, Adda Ali-Pacha, Abdelhafid Abouaissa, and Pascal Lorenz. Security Against Rank Attack in RPL Protocol. *IEEE Network*, 34(4):133–139, 2020.

[30] Baraq Ghaleb, Ahmed Y. Al-Dubai, Elias Ekonomou, Ayoub Alsarhan, Youssef Nasser, Lewis M. Mackenzie, and Azzedine Boukerche. A Survey of Limitations and Enhancements of the IPv6 Routing Protocol for Low-Power and Lossy Networks: A Focus on Core Operations. *IEEE Communications Surveys & Tutorials*, 21(2):1607–1635, 2019.

[31] VR Rajasekar and S Rajkumar. A Study on Impact of DIS flooding Attack on RPL-based 6LowPAN Network. *Microprocessors and Microsystems*, 94:104675, 2022.

[32] Abhishek Verma and Virender Ranga. Addressing Flooding Attacks in IPv6-based Low Power and Lossy Networks. In *TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON)*, pages 552–557, 2019.

[33] R.K.C. Chang. Defending against flooding-based distributed denial-of-service attacks: a tutorial. *IEEE Communications Magazine*, 40(10):42–51, 2002.

[34] Anthéa Mayzaud, Rémi Badonnel, and Isabelle Chrisment. A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks. *IEEE Transactions on Network and Service Management*, 14(2):472–486, 2017.

[35] Abhay Deep Seth, Santosh Biswas, and Amit Kumar Dhar. Ldes: Detector design for version number attack detection using linear temporal logic based on discrete event system. *International Journal of Information Security*, pages 1–25, 2023.

[36] Linus Wallgren, Shahid Raza, and Thiemo Voigt. Routing attacks and countermeasures in the RPL-based internet of things. *International Journal of Distributed Sensor Networks*, 9(8):794326, 2013.

[37] Benamar Bouyeddou, Benamar Kadri, Fouzi Harrou, and Ying Sun. DDOS-attacks detection using an efficient measurement-based statistical mechanism. *Engineering Science and Technology, an International Journal*, 23(4):870–878, 2020.

[38] Anhtuan Le, Jonathan Loo, Aboubaker Lasebae, Alexey Vinel, Yue Chen, and Michael Chai. The impact of rank attack on network topology of Routing Protocol for Low-power and lossy networks. *IEEE Sensors Journal*, 13(10):3685–3692, 2013.

[39] Anhtuan Le, Jonathan Loo, Yuan Luo, and Aboubaker Lasebae. The impacts of internal threats towards Routing Protocol for Low power and lossy network performance. In *2013 IEEE Symposium on Computers and Communications (ISCC)*, pages 789–794, 2013.

[40] Abdul Rehman, Meer Muhammad Khan, M Ali Lodhi, and Faisal Bashir Hussain. Rank attack using objective function in RPL for low power and lossy networks. In *2016 International Conference on Industrial Informatics and Computer Systems (CIICS)*, pages 1–5. IEEE, 2016.

[41] Amit Dvir, Levente Buttyan, et al. VeRA-version number and rank authentication in rpl. In *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*, pages 709–714. IEEE, 2011.

[42] Ge Guo. A lightweight countermeasure to DIS attack in RPL routing protocol. In *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0753–0758. IEEE, 2021.

[43] Divya Sharma, Ishani Mishra, and Sanjay Jain. A detailed classification of routing attacks against RPL in Internet of Things. *International Journal of Advance Research, Ideas and Innovations in Technology*, 3(1):692–703, 2017.

[44] Rashmi Sahay, G Geethakumari, Barsha Mitra, and Ipsit Sahoo. Efficient framework for detection of version number attack in Internet of Things. In *Intelligent Systems Design and Applications: 18th International Conference on Intelligent Systems Design and Applications (ISDA 2018) held in Vellore, India, December 6-8, 2018, Volume 2*, pages 480–492. Springer, 2020.

[45] Zahrah A. Almusaylim, NZ Jhanjhi, and Abdulaziz Alhumam. Detection and mitigation of RPL rank and version number attacks in the internet of things: SRPL-RP. *Sensors*, 20(21):5997, 2020.

[46] Usman Shafique, Abid Khan, Abdur Rehman, Faisal Bashir, and Masoom Alam. Detection of rank attack in routing protocol for Low Power and Lossy Networks. *Annals of Telecommunications*, 73:429–438, 2018.