Detection and Mitigation of RPL Rank and Version Number Attacks in Smart Internet of Things

Zahrah A. Almusaylim[1], Abdulaziz Alhumam[2], Wathiq Mansoor[3], Pushpita Chatterjee[4], NZ Jhanjhi[5]
[1,2] King Faisal University, Department of Computer Science, Al-Ahsa, Saudi Arabia
Taylor's University, School of Computer Science and Engineering SCE, Lakeside Campus, Malaysia
zahra.almusaylim@hotmail.com[1] , aahumam@kfu.edu.sa[2] , wmansoor@ud.ac.ae[3],
pushpita.C@gmail.com[4], noorzaman.jhanjhi@taylors.edu.my[5]
*Corresponding author: pushpita.c@gmail.com, noorzaman.jhanjhi@taylors.edu.my

Abstract

The rapid growth of the smart Internet of Things (IoT) and massive propagation of wireless technologies revealed the recent opportunities for development in various domains of real life such as smart cities and E-Health applications. A slight defense against different forms of attacks is offered for the current secure and lightweight Routing Protocol for Low Power and Lossy Networks (RPL) of IoT resource-constrained devices. Data packets are highly likely to be exposed while transmitting them during data packets routing. The RPL rank & version number attacks, which are two forms of RPL attacks, can have critical consequences for RPL networks. The studies conducted on these attacks have several security defects and performance shortcomings. The research proposes a Secure RPL Routing Protocol (SRPL-RP) for rank and version number attacks. It mainly detects, mitigates and isolates attacks in the RPL networks. The detection is based on a comparison of ranks strategy. The mitigation uses threshold and attacks status tables, and the isolation adds them to a blacklist table and alerts relevant nodes to skip them. SRPL-RP supports diverse types of network topologies and is comprehensively analyzed with multiple studies such as Standard RPL with Attacks, SBIDS and RPL+ Shield. The analysis results showed that the SRPL-RP achieves great improvements with Packet Delivery Ratio (PDR) of 98.48%, control message value of 991 packets/second, and average energy consumption of 1231.75 joules. It provides a better accuracy rate with 98.17% under the attacks.

Keywords: IoT, Security, RPL, Rank Attack, Version Number Attack, Smart IoT

1 INTRODUCTION

Smart Internet of Things (IoT) is the consequence of the seamless integration of devices between wireless communications and diverse technologies. The devices can perceive their surrounding environment and gather data from it for processing and decision making [1]. The smart city is one of the substantial domains of IoT. It is composed of innumerable services and applications that aim to increase the quality of life and services to residents [2-4]. However, the devices need to communicate in the smart city networks via the network layer in the IoT architecture. This layer utilizes various standards, protocols, and techniques to smoothen the secure transfer of data packets among devices. The RPL is a distance-vector routing protocol for low power and lossy networks, in which its topology is constructed dependent on a Destination Oriented Directed Acyclic Graph (DODAG). Which is intended to facilitate the functionalities of numerous link-layer protocols. These layers may be possibly lossy or consumed with strongly constrained devices. The RPL has the ability to have alternative routes and adapt with the network conditions when there is not an access to default routes. Depending on Objective Functions (OF), the RPL can nominate the optimal route to define the parent and neighbors nodes selection [5].

1.1 RPL Security

Data packets addressing and routing among resource-constrained devices are considered to be an issue because of the necessity of developing integrated protocols for data packets routing across different RPL networks [6]. Data packets routing in IoT constrained devices suffers from potential security threats, and it has a considerable impact since it is related to the user's life [7]. Several RPL attacks occur through the activities of the malicious nodes during the data packets routing among devices [8]. This impacts the data security of users since devices are vulnerable to different attacks [7, 8]. The RPL security The security of the RPL protocol has been reviewed vastly in [9-11]. Various kinds of RPL attacks have been analyzed, yet most of studies did not concentrate of the mechanisms of secure RPL.

doi:10.20944/preprints202007.0476.v1

1.2 Research Contribution

RPL protocol security has been studied vastly because of the innumerable security threats to resource-constrained devices. The RPL rank and version number attacks, which are two types of RPL attacks, can have critical consequences for RPL networks. The rank attack affects the network performance, low Packet Delivery Ratio (PDR), delay and generation of non-optimal path and loop. The version number attack affects the network performance because of increased overhead control, low delivery of packet ratio and high end-to-end delay. The studies conducted on these attacks have flaws such as:

- Several security defects and shortcomings regarding network performance and accuracy.
- Multiple attacks in RPL networks are not supported.
- They do not detect and mitigate the effects of both attacks in the RPL networks.

Therefore, there is a requirement for further research to handle the declared security problems for RPL routing protocols in IoT. Accordingly, this research work will extend our published previous work [12] that investigated in details the existing research gaps of RPL attacks, concentrating on the rank attack and the version number attack. This work will propose and implement a mechanism for secure RPL routing protocols. It will be based on and continue two pieces of research presented in [13, 14] by addressing and improving their security issues, with the help of a proposed protocol called Secure Detection and Mitigation RPL Routing Protocol (SRPL-RP). The main contribution of this research is as follows:

- Addition of a timestamp threshold to verify the legitimacy of the sender nodes.
- Formulation of a monitoring table during the construction of DODAG that contains information about all the nodes like node ID.
- Detection of rank and version number attack based on a comparison of ranks strategy.
- Mitigation of the effects of both rank attack and version number attack based on threshold and attacks status tables.
- Isolation of both rank attack and version number attack by adding them to a blacklist table and alerting relevant nodes to skip them. In addition, provision of multiple types of attacks (rank and version number attacks) in RPL networks, and support for different types of RPL networks topologies.

1.3 Research Paper Organization

The research paper is organized in a pattern as follows: Section II presents the Literature Review mainly on security area RPL attacks, which are rank and version number attack. It illuminates the recent studies related to them. The proposed protocol is introduced in Section III, in which the proposal and design of SRPL-RP is explained with its description, flow chart model and implementation. Section IV gives an overview of the simulation setups and performance parameters with the assumptions to simulate the proposed protocol and extract the results. The results analysis is provided in Section V, in which an analysis is presented focusing on the proposed protocol with the presence of a comparison of existing countermeasures. Section VI presents the discussion, which demonstrates the security analysis of the proposed SRPL-RP and justifies that SRPL-RP can significantly provide better results than the existing countermeasures in terms of network performance and accuracy. Finally, the conclusion is provided in Section VII that wraps up the research, achieve objectives, and future works.

2 LITERATURE REVIEW

This section will introduce the RPL attacks and their obstacles. It introduces the latest researches concerning the RPL security.

2.1 RPL Rank Attack

The rank attack in the RPL networks topology exposes the child nodes that are deeper rank in the network. Then, the malicious nodes have the ability to change the method, in which the neighbor nodes can process their DODAG Information Object (DIO) messages. In addition, for the preferred parent node, a malicious node can select a worse rank during its operations. The rank attack has several effects such as: 1) Un-optimized route formulation. 2) Un-recognized of formulated loop. 3) The RPL network topology never utilized the optimized routing. 4) When the malicious nodes increase, there will be a decrease in the PDR and small modification of end-to-end delay. 5) There will be an increase in the DIO messages due to the rapid changes in the network topology. Consequently, the network constrained merits are influenced such as energy consumption, delay, packets delivery ratio and control overhead [15]. Unauthorized access by attackers or third parties to data routing in the RPL networks can make the RPL security a serious problem that shall be considered [16].

The sub-sections will give details and classify the RPL rank attack countermeasures.

RPL Rank Attack Countermeasures Classification

The rank attacks countermeasures are classified into two categories, which are: 1) Modification techniques that can adjust or add the RPL standards and it can detect limited number of attacks. 2) Intrusion Detection Systems (IDS) that requires nodes collaboration and it can detect multiple types of attacks [17].

1) Classification Based RPL Rank Attack Modification Techniques

The authors in [18] proposed and developed the Secure-RPL (SRPL) protocol. The malicious node in the proposed protocol are blocked from better self-repositioning in the DODAG tree of the RPL network. The proposed protocol scans the number of times that the nodes' rank values increase by enabling a threshold function to reduce the impact of the attack in the network. The evaluation results of network performance indicate that the proposed protocol is efficient in protecting the RPL network. To overcome the overhead that existed in [18], Airehrour et al. [19] developed and proposed a Time-Based Trust-Aware RPL (SecTrust-RPL) to provide secure protection against rank attack and Sybil attack. It provides detection and isolation of the attacks with network performance optimization. A trustworthiness is computed by each node in the RPL network, in which its neighbor nodes have direct trust value and recommend trust value. Based on the evaluation results, the proposed protocol has better protection against rank attack.

2) Classification Based IDS

Authors in [20] designed a Specification-Based IDS. To detect the attacks, the system uses a Finite State Machine (FSM) transitions, and Monitoring Nodes (MN) are formed in the monitoring architecture. To detect the rank attack, the malicious nodes with lower ranks are scanned by the MN. However, the MN will suspect action changes of the valid rank and the fake rank of the malicious nodes. The information cross-checking of the MN will be started to detect the valid ranks. The study in [21] proposed secure parent node selection scheme, where based on a threshold value, a legitimate node will be selected by the child nodes as their parent node. Every node in the RPL network decides the rank value that is advertised by the neighbor nodes based on the threshold between the maximum and average rank. If the rank value is too low, then it will be selected as a parent node. The evaluation results of the scheme show that it is effective in decreasing linking the child nodes with the malicious nodes.

Althubaity et al. [22], designed an Authentication Rank and Routing Metric (ARM), which is a hybrid specification based ID. The sink node in ARM is defined as a centralized module, while other nodes are defines as a distributed module. The centralized module works in DIO messages analysis and decision making participation. On the other hand, the distributed module works in alerting the sink nodes regarding any changes happened in the destination nodes. The evaluation results indicate that ARM safeguards the RPL network with high accuracy rate. The researchers in [13] presented a Sink-Based Intrusion Detection System (SBIDS) to detect the rank attack in the RPL network. It works by the rule of comparing Node Current Rank (NCR) with Node Parent Rank (NPR), and checking the minimum rank between their siblings. The evaluation results of SBIDS show that it is effective in detecting the rank attack.

2.2 RPL Version Number Attack

The version number attack in the RPL networks topology can illegitimately increment the root node's DODAG version number by the malicious node when the DIO message is forwarded to its neighbors nodes to damage the network performance. When the neighbor nodes receive the DIO message that contains the incremented version number, the DODAG tree starts a new formulation and the trickle timer is reset [23]. After that, the neighbor nodes will transmit frequent updated version of the DIO messages to all nodes [24]. The version number attack has significant impacts such as: 1) The operation of the network are damaged. 2) The network control overhead is increased 18 times, which is unnecessary. 3) There will be routing loops in data routing. 4) The network energy consumption is increased. 5) The communication channels of the nodes have availability issues. In addition, packets delivery is lost, and the network delay is doubled [25].

The sub-sections will give details and classify the RPL version number attack countermeasures.

RPL Version Number Attack Countermeasures Classification

The rank attacks countermeasures are classified into two categories, which are: 1) Modification techniques that can adjust or add the RPL standards and it can detect limited number of attacks. 2) Intrusion Detection Systems (IDS) that requires nodes collaboration and it can detect multiple types of attacks [17].

1. Classification Based RPL Version Number Attack Modification Techniques

The study in [26] proposed and implemented a rank, and version number authentication security measure scheme based on one-way hash chains called VeRA. It provides security against internal attacks that broadcast incremented version number or higher rank in the DIO messages. The version number is checked if it is updated by the root node or not, and if the rank value of the parent node is illegitimately increasing or not. The evaluation results show that the overhead time of the scheme. Perrey et al. [27] proposed and designed a Trust Anchor Interconnection Loop (TRAIL) scheme to overcome the obstacles in the former study [26] by analyzing incompleteness of rank authentication message. The sink node works as a trust anchor, and every node in the RPL network validates each rank value and drops invalid rank value.

The studies above that are used to discover the version number attack can suffer from increased overhead. Therefore, to safeguard against version number attack, authors in [28] proposed and developed a cooperative, distributed verification mechanism. The mechanism depends on checking step phase and verification phase. The cooperative verification procedure works by allowing the receiving nodes to verify the neighbor node’s identity to determine if the neighbor noes has a malicious behavior or not. The evaluation results show that the control overhead is decreased and the mechanism is reliable.

To mitigate the effect of the version number attack, the researchers in [29] proposed and designed a lightweight approach. Every node in the RPL network executes independent algorithms, in which the state of the nodes are not stored. The evaluation results indicate the proposed scheme is lightweight and compatible with constrained devices. The research in [14] proposed and implemented lightweight techniques for version number attacks to consider the version number legitimate update. The malicious update influences of the version number is eliminated by the elimination technique. A trust mechanism is used by the shield technique, in which a change to the version number is required if majority of the neighbor nodes that are close to the root node have a better rank. The evaluation results indicate that it is possible to mitigate the version number attack using these techniques.

2. Classification Based IDS

Mayzaud et al. [30] proposed and developed a mechanism to detect and identify the malicious nodes that have illegitimately incremented version number based on distributed monitoring architecture. It detects and monitors the nodes operations in the RPL network based on monitored nodes (regular nodes) and monitoring nodes, in which detection operations are performed. The evaluation results show that the mechanism has a satisfying performance.

The literature review demonstrated that the RPL security has been generally considered in view of the tremendous threats in the IoT. Studies [31]–[33] developed many solutions for RPL rank attack and version number attack. The challenges of these attacks need to be handled because of the trade-off between providing safeguard against these attacks and maintaining the efficient performance of the RPL in the IoT environment. The developed studies are effective in detecting these attacks, but they still suffer from many flaws that have to be treated. Further, from the analysis in [12], we can observe: 1) the RPL network topology type, 2) the number of nodes, 3) malicious nodes location, can have considerable consequences on network performance and accuracy. Therefore, a proposal to secure the RPL protocol should be conducted to support different kinds of attacks with multiple types of RPL network topologies. In addition, to detect and mitigate the effects of rank and version number attack, and to isolate the malicious nodes as well as alerting the normal nodes in the RPL network.

3 PROPOSED PROTOCOL

The proposed protocol is introduced in this section, in which the proposal and design of SRPL-RP is explained with its description, flow chart model and implementation.

3.1 SRPL-RP Proposal

We present the proposed SRPL-RP to detect, mitigate and isolate the attacks discussed in the previous section. The declared security issues for the RPL protocol can be handled by having the following features in the proposed protocol:

1. A timestamp threshold to verify the legitimacy of the sender nodes.
2. A monitoring table during the construction of DODAG that contains information about the nodes.
3. Detection of both rank and version number attack.
4. Mitigation of the effects of both rank and version number attack.

5. Isolation of both rank and version number attack.

The two below sections describe the protocol model flowchart and implementation, which are presented for consideration for this proposed protocol.

3.2 Attacker Model

In this section, the attacker model of the proposed protocol is introduced. The RPL network topology composes of one root node, multiple normal nodes and some malicious nodes that are rank attack and version number attack. We are assuming that the root node cannot be exposed, and its ID is encrypted and cannot be violated [13]. The proposed protocol is safe from insider attacks using Elliptic Curve Cryptography (ECC) [34]. In RPL, the version number and rank are carried DIO message, and the version number is used as an indicator for the global repair operation. The DODAG root node is the only node that can change the version number. All the nodes in the RPL network topology begins exchanging control messages to rebuild the network topology, after the root nodes changed the version number. While sending the DIO packet, malicious nodes attach their rank and version in the DIO packet. Subsequently, the attacker is able to exhaust the restricted drain the limited resources of all the nodes in the RPL network and lead to detrimental impacts on the network performance. The malicious nodes start their attacks by broadcasting fake rank and version number during the cycle RPL trickle time. The version attacker is the one that changes the version number of nodes by incrementing their nodes, and a rank attacker is the one that falsely proposes the rank value to be chosen as a parent node. The nodes can spread their version and rank in the DODAG. While receiving the DIO packets from the malicious nodes (include rank and version), then current node changes their rank and version. Hence, they cannot determine the path to reach the root node.

3.3 SRPL-RP Description

This section depicts the details of the proposed protocol that detects, mitigates and isolates malicious nodes of both rank and version number attacks. When a node receives a DIO control message, the protocol starts, and it consists of five phases:

Phase One: a timestamp is used to monitor and track the time that the DIO control messages are exchanged using the RPL trickle timer for synchronization. The difference of time between each DIO messages have to be not exceed a threshold value (that is calculated based on some equations [31, 35]. The time difference is registered as a timestamp and transmitted with the DIO message, thus, it helps in preventing malicious nodes. It is also used to determine the freshness of the DIO message throughout the process. If the time of the DIO message is above the threshold value, the DIO message will be discarded because it is indicated as malicious activity. In addition, if the time of the DIO message is less than the threshold value, then phase two is started.

Phase Two: if the DIO message has a lower value than the threshold value, the legitimacy of the sender node is verified by the receiver node by checking its ID. If it is invalid, the sender node will be discarded. Moreover, if it is valid, the sender node will be added to a monitoring table (that is formulated during the DODAG construction) that captures information about the node like node ID, node rank, DIO message information, version number, etc. Hence, by using the monitoring table, the legitimacy of the nodes is verified, during which every valid node will be added to the monitoring table. Thus, when the receiver node checks the sender's node ID, it will refer to this table to check if the sender's ID exists in the monitoring table or not.

Phase Three: we extend the detection functionality of the rank attack described in research work [13] and mitigation functionality of version number attack as described in the other work [14]. If the DIO message of the sender node does not have a greater version number than the version number of the root node (assuming that the root node cannot be compromised), then it will be a case of rank attack detection and mitigation. Moreover, if the DIO message of the sender node has a greater version number than the version number of the root node, then it will be the case of version number attacks detection and mitigation.

Phase Four: Fig. 1 shows the condition for rank attack detection, mitigation, and isolation is started, which is based and continued from research [13]. If Node Current Rank (NCR) is greater than Node Parent Rank (NPR), then it is considered a malicious node. If the DIO control message of the malicious node is not discarded and it is falsely verified as a legitimate node in the monitoring table for any reason, then the monitoring table will be updated to remove all information of the malicious node. The malicious node will be added to the blacklist table (that is formulated during the DODAG construction), which captures all information of the malicious nodes to mitigate the effect and isolate the malicious node from the network. The blacklist table contains IDs of all malicious nodes that should not join the RPL network topology again because they were detected as malicious nodes before. Then, an alert message will be sent to all the nodes in the network to notify them not to join this node in the future, so it is isolated from the network.

On the other hand, if the NCR is lower than the NPR, then the rank rule of the current node is compared with the rank rule of the previous rank. If NCR is greater than the Node Previous Rank (NPVR), then it is considered a mobile node in the RPL network. When a node reaches its final destination, it does not change its rank, but it is stabilized concerning its neighboring nodes. However, if the NCR is lower than NPVR, then it is checked whether the nodes are siblings. If the node does not have siblings, then it is checked whether they are child nodes. If the node is not a child, then it is a leaf node. In addition, if the nodes are children, then the minimum rank and Parent Switching Threshold (PST) is compared with the NPVR. If (minimum rank + SPT) is equal to the NPVR, then the node is legitimate and valid.

Nevertheless, if (minimum rank + SPT) is not equal to the NPVR, then it is considered a malicious node. The monitoring table will be updated to add the malicious node to the blacklist table. On the other hand, if the node has siblings, then the NCR is compared with the minimum rank and PST. If the NCR is lower than (minimum rank – PST), then it is considered and detected as a malicious node. The monitoring table will be updated to add the malicious node to the blacklist table. However, if the NCR is greater than (minimum rank – PST), then it is considered a mobile node in the RPL network.

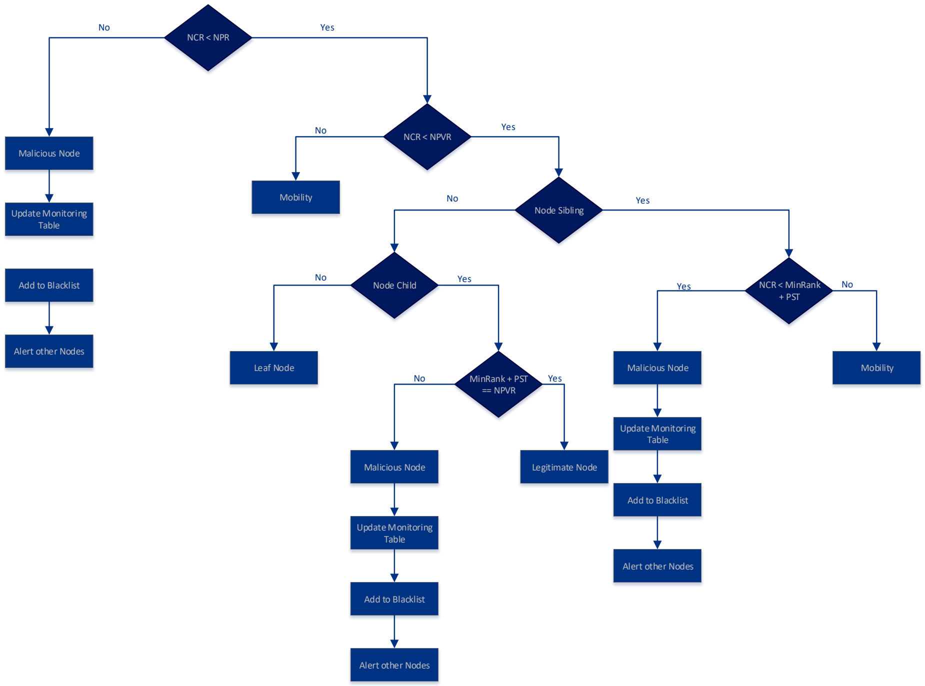


Figure 1. Protocol Model Flowchart, Phase Four.

Phase Five: Fig. 2 shows the condition for version number attack detection, mitigation, and isolation is started, which is based and continued from research [14]. If the DIO message of the sender node has a greater version number than the version number in the root node, then the rank rule of the parent node is compared with the rank rule of the current node. If the NPR is greater than the NCR, then it is considered a mobile node in the RPL network. However, if the NPR is lower than the NCR, then the rank rule of the previous node is compared with the rank rule of the current node. If the NPVR is greater than the NCR, then it is considered a mobile node in the RPL network. However, if the NPVR is lower than the NCR, then the version field of the sender node is updated in the neighbor table list (that is formulated during DODAG construction), which stores the information of the neighbor nodes and their version field. Then, it is checked whether half of the nodes have the same information of the version number in the neighbor table list. And if half of the neighbor nodes in neighbor table list have the same version number, then the version number in the DIO message of the sender node is updated and changed to the same majority version number in the table and clears the previous version number field. If half of the nodes do not share the same information of the version number field in the table, then it is considered a malicious node. The monitoring table will be updated to add the malicious node to the blacklist table.

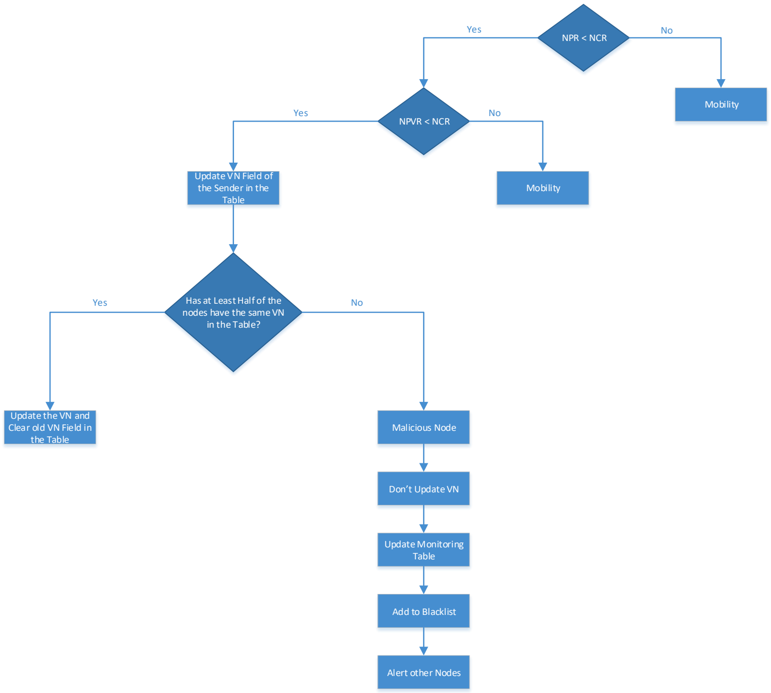

NPR < NCR
Yes
No
Mobility
NPVR < NCR
Yes
No
Update VN Field of the Sender in the Table
Mobility
Has at Least Half of the nodes have the same VN in the Table?
Yes
No
Update the VN and Clear old VN Field in the Table
Malicious Node
Don't Update VN
Update Monitoring Table
Add to Blacklist
Alert other Nodes

Figure 2. Protocol Model Flowchart, Phase Five.

3.4 SRPL-RP Implementation

Their creation can detect the rank attack and version number attack. A timestamp is attached to DIO control messages. The timestamp is used to monitor and track the time of exchange of the DIO control messages. The time difference between DIO messages should be within a threshold value that is registered as a timestamp, and it is transmitted with the DIO message. If the time of the DIO message is above the threshold value, the DIO message will be discarded because it is indicated as malicious activity. In addition, if the time of the DIO message is less than the threshold value, the legitimacy of the sender node will be verified by the receiver node for more security by checking the ID of the sender nodes against the values in the monitoring table that is created during the establishment of the RPL DODAG by the root node. If it is valid, it will be added to the monitoring table. After that, if the node version number in the DIO message is greater than the default version number in the root node, the rank attack will be checked. The rank value of the rank needs to be checked according to the comparison strategy.

3.4.1 Rank and Version Number Attacks Detection

The rank attack is detected with the comparison strategy. The NCR is compared with its parent, child and its neighbors. A node table is used to access the rank of parent, child and neighbor nodes. The node needs first to satisfy the parent and child rank relationship. The parent should have a lower rank value compared to than the child. Then, the NCR is compared with its NPR and NPVR. The node's rank is comparatively evaluated against child and sibling rank, by following algorithms 1 and 2, and their output shown in the charts in Section V. In algorithm 1, if the minimum rank among sibling nodes that are deduced from minimum PST is greater than the NCR, then the node is considered a malicious one, otherwise, it is considered a legitimate node. Similarly, in algorithm 2, if the minimum rank among child nodes that are summed together with PST is greater than or equal to the NCR, then the node is considered a malicious one, otherwise, it is considered as a legitimate node.

Algorithm 1. Evaluation of Node Current's Rank and Node Sibling's Rank.

```
Begin
input: node_id
input: min_sibling_rank
input: node_current_rank
input: parent_threshold_divisor
input: min_pst
input: threshold
```

```
set min_pst = (min_sibling_rank – parent_threshold_divisor)

if node_current_rank < min_pst then
    set threshold[node_id] = 5

else
    set threshold[node_id] = 4
End if

End
```

Algorithm 2. Evaluation of Node Current's Rank and Node Child's Rank.

```
Begin
input: node_id
input: min_child_rank
input: node_current_rank
input: parent_threshold_divisor
input: minch_pst
input: threshold

set minch_pst = (min_child_rank + parent_threshold_divisor)

if node_current_rank <= minch_pst then
    set threshold[node_id] = 7

else
    set threshold[node_id] = 6
End if

End
```

On the other hand, the version number attack is detected if the version number node is greater than the default root node's version number (240). The NCR is compared with its NPR (parent rank must be lower than current rank). Similarly, node rank is compared with its NPVR. If the NPVR is lower than the NPR, then the network is stabilized and the version field of each node in a table needs to be checked (after receiving DIO). Otherwise, it needs to update its version number. If half of the neighbor nodes in the neighbor table list have the same version number, then the version number in the DIO message of the current node is updated and changed to the same majority version number in the list by checking the condition (version != 240) in algorithm 3. Its output is shown in the charts in Section V.

Algorithm 3. Checking the Condition of the Initial Default Version Number.

```
Begin
input: version
input: neighbor_1_current_rank
input: neighbor_1_previous_rank
input: neighbor_1_version
input: number
input: neighbor_1
input: neighbor_1_id
input: neighbor
input: neighbor_table_head
input: neighbor_table_next
input: n
input: m
input: p

if version != 240                //DEFAULT VERSION(DODAG)= 240
```

```
    for neighbor_1 = neighbor_table_head; neighbor_1 != null; neighbor_1 = neighbor_table_next then
        set number ++
        set neighbor_1_id = address
        set neighbor[number] = neighbor_1_id
        set n[neighbor[number] = neighbor_1_current_rank
        set m[neighbor[number] = neighbor_1_previous_rank
        set p[neighbor[number] = neighbor_1_version

End for
End if

End
```

3.4.2 Rank and Version Number Attacks Mitigation

For mitigation purposes, in the version number attack, if a node has malicious behavior, then the malicious version number will behave as a legitimate node by updating its version number to the same one as in the neighbor list table. With this technique, nodes are prevented from being the attacker. At every DIO reception, the table will be updated as in algorithm 4. Its output shown in the charts in Section V. Moreover, in the rank attack, we set the attack status in the neighbor table to restrict the malicious node from being a parent node in algorithm 5, and its output is shown in the charts in Section V. Hence, the mitigation mechanism occurs.

Algorithm 4. Version Number Attack Mitigation.

```
Begin
input: version_count
input: divisor
input: version
input: ver
input: j
input: threshold_table
input: node_id

if version_count >= divisor then
    set version = ver[j]                    //updating version number
    set threshold_table[node_id] =  2

Else
    set threshod_table[node_id] = 3
End if

End
```

Algorithm 5. Rank Attack Mitigation.

```
input: preferred_parent1
input: preferred_parent2
input: preferred_parent1_status
input: preferred_parent2_status
input: parent1_metric
input: parent2_metric
input: p1
input: p2

if preferred_parent1 == 1 || preferred_parent2 == 1 then
    if parent1_metric < parent2_metric then
        set p1
    else
        set p2
    End if

Else
    if preferred_parent1_status != 1 && preferred_parent2_status != 1 then
        if parent1_metric < parent2_metric then
```

```
            set p1

          else
              set p2
          End if
      End if
End if

End
```

3.4.3 Rank and Version Number Attacks Isolation

To add extra security and isolate the malicious nodes from the network and add them to the blacklist, alerting all other relevant nodes to skip nodes in that list, we attached a threshold alert to the DIO messages because every node sends DIO messages to other nodes to prevent the malicious nodes from sending DIO messages. Hence, through this, it conveys the attacker's status of itself. Thus, the node is alerted to the malicious node in the network in Algorithm 6, and its output is shown in the charts in Section V.

Algorithm 6. Attacks Isolation.

```
input: node_id
input: attack_status
input: alert

if  attack_status[node_id] == 0 then
   set alert: (legitimate node, node_id)

else
if attack_status[node_id] == 1 then
   set alert: (malicious node, node_id)
End if
End if

End
```

4 SIMULATION OF SRPL-RP

This section will present the simulation setup and performance parameters to simulate and measure the effectiveness of our proposed protocol.

4.1 Simulation Setup

To implement and measure the effectiveness of the proposed secure protocol, the Cooja simulator based on Contiki OS 3.00 was used [36]. It is a networking system and a multitasking operating system for IoT devices. Hence, it is used for creating different simulations in this research paper. We conducted three types of topologies to analyze the security effectiveness of the proposed protocol and the network performance: Grid-Center topology, Grid-Random topology and Random topology. The nodes are placed in 100m x 100m area, and each node is distributed in a transmission range of 50 m that maintains the linkage between nodes and interference range of 100 m based on the UDGM-Distance Loss model (link failure model). These parameters are the default settings of Cooja simulator [14]. The network topology can be deployed in E-applications as mentioned in the research [37]. Table 2 shows a summary of the simulation model.

Table II. The Simulation Model Parameters.

Parameter	**Value**
Simulator	Cooja 3.0
Node Type	Wismote
Number of Nodes	20 with 1 root node, 14 normal nodes
Number of Malicious Nodes	5: 4 rank attacker nodes, 1 version number attacker node
Routing Protocol	RPL Protocol
Area	100 m * 100 m
Simulation Time	60 minutes

Transmission Range	50 meters
Interference Range	100 meters
Packet Send Interval	60 Second
Data Packet Size	127 Bytes
Confidence Interval (CI)	95%
Topology	Grid-Center, Grid Random, Random

4.2 Performance Parameters

A measurement of the performance parameters was presented to examine how the proposed protocol can perform efficiently in detecting, mitigating and isolating the attacks comparing to the existing secure routing protocols by classifying the parameters into two categories:

Network Performance Parameters: PDR, control message, and average energy consumption.

Accuracy Metrics: Accuracy Rate (AR), which is the rate of the total of True Positive (TP) and True Negative (TN) divided by the total of True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN).

5 RESULTS ANALYSIS

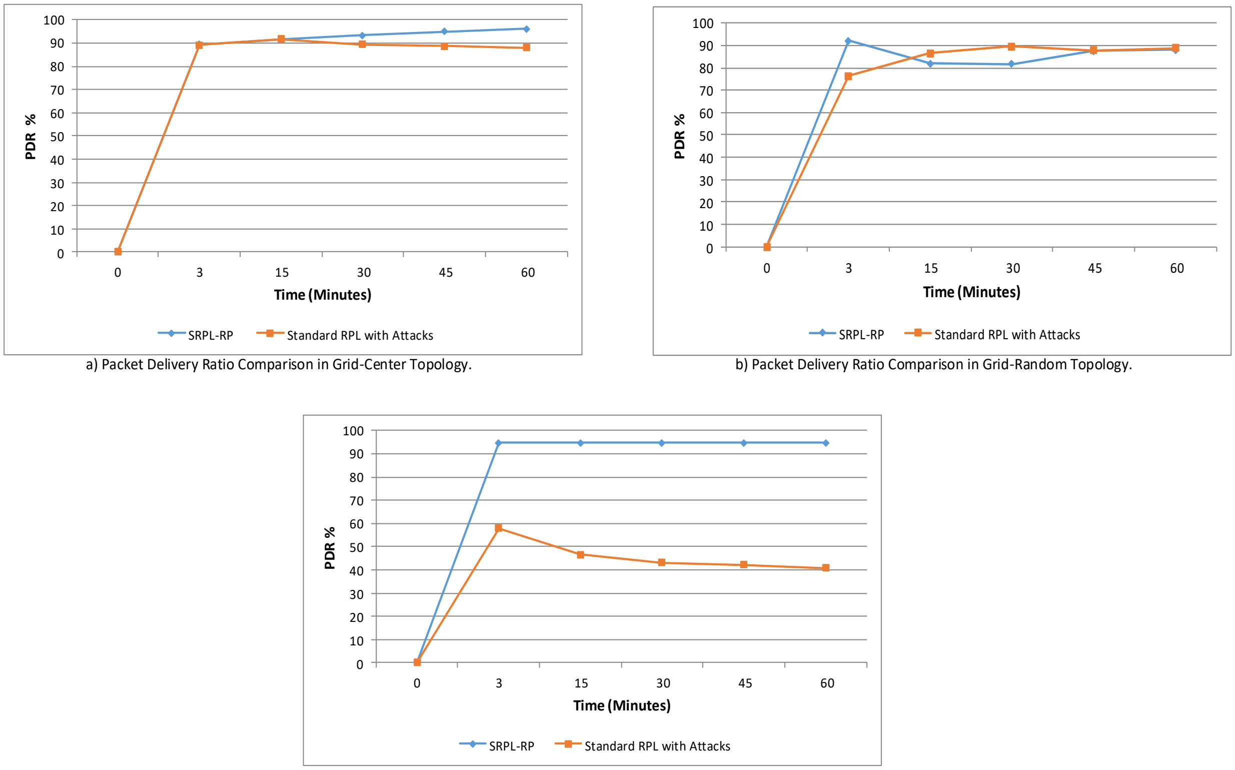
This section will present an analysis of the proposed SRPL-RP. We tested the proposed SRPL-RP in grid-center network topology, grid-random network topology, and random network topology. We ran and repeated the simulations 60 times for the three types of topologies at different time stages: the network convergence, the network stability and the network at the end of the simulation. This measures the changes in security accuracy and network performance levels of the proposed protocol concerning time in 3 minutes, 15 minutes, 30 minutes, 45 minute and 60 minutes. The extracted results of the proposed SRPL-RP are used for comparison with the existing countermeasures of RPL security, which are the Standard RPL with Attacks, SBIDS [13] and RPL+ Shield [14] to measure its effectiveness and performance.

5.1 (SRPL-RP) and Standard RPL with Attacks Results and Comparison

In this sub-section, we presented the performance of our proposed SRPL-RP concerning rank attack and version number attack. We compared it with the standard RPL under rank attack and version number attack.

Network Performance Results

The simulation results for the network performance parameters of both SRPL-RP and Standard RPL with attacks comparison, concerning the three topologies and time stages, are shown in Fig. 3, Fig. 4 and Fig. 5. where Fig. 3 shows the PDR results of SRPL-RP and Standard RPL with Attacks comparison in Grid-Center Topology (a), Grid-Random Topology (b) and Random Topology (c) respectively. It shows that PDR at the convergence time is 89.47% for SRPL-RP and 89.19% for Standard RPL with Attacks in grid-center topology, 92.11% for SRPL-RP and 76.32% for Standard RPL with Attacks in grid-random topology and 94.74% for SRPL-RP and 57.89% for Standard RPL with Attacks in random topology. The PDR at the stability time is 93.43% for SRPL-RP and 89.47% for Standard RPL with Attacks in grid-center topology, 81.67% for SRPL-RP and 89.47% for Standard RPL with Attacks in grid-random topology and 94.74% for SRPL-RP, in which it is decreasing because the attacks become active at this time, and 43.01% for Standard RPL with Attacks in random topology. The PDR at the end of the simulation is 95.99% for SRPL-RP and 88.04% for Standard RPL with Attacks in grid-center topology, 88.12% for SRPL-RP and 89.93% for Standard RPL with Attacks in grid-random topology and 94.74% for SRPL-RP and 40.82% for Standard RPL with Attacks in random topology. We notice that SRPL-RP has a higher PDR in gird-center topology than in other topologies compared with Standard RPL with Attacks.



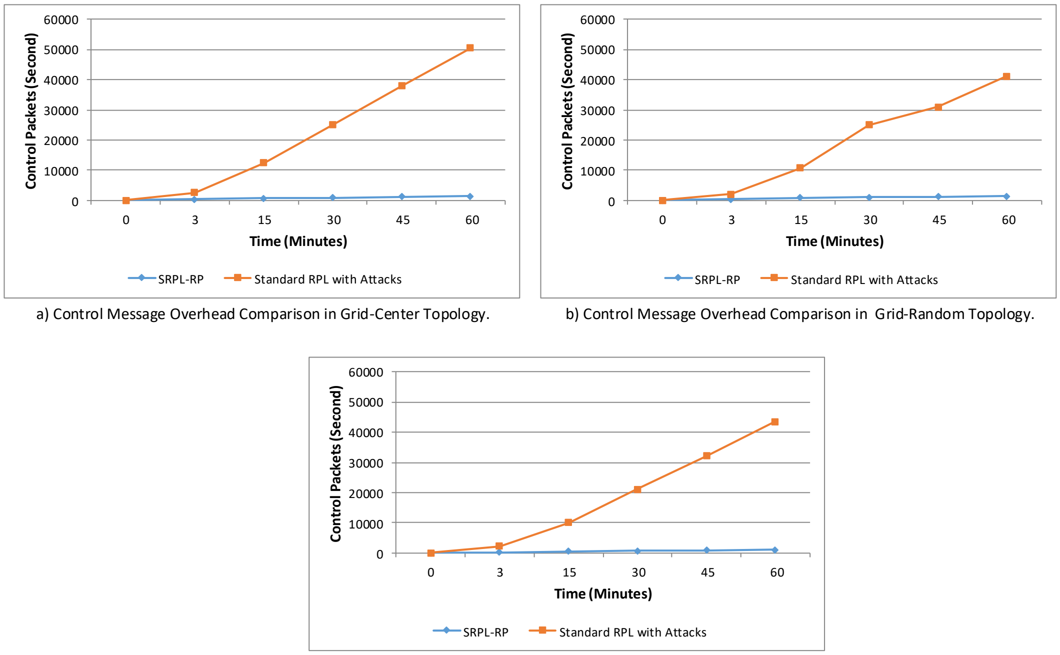
a) Packet Delivery Ratio Comparison in Grid-Center Topology.

b) Packet Delivery Ratio Comparison in Grid-Random Topology.

c) Packet Delivery Ratio Comparison in Random Topology.

Figure 3. Packet Delivery Ratio Comparison between SRPL-RP and RPL Standard RPL with Attack in Three Topologies.

Fig. 4 shows the Control Message results of SRPL-RP and Standard RPL with Attacks comparison in Grid-Center Topology (a), Grid-Random Topology (b) and Random Topology (c) respectively. It shows that the control message value at the convergence time is 259 packets/second for SRPL-RP and 2525 packets/second for Standard RPL with Attacks in grid-center topology, 414 packets/second for SRPL-RP and 2146 packets/second for Standard RPL with Attacks in grid-random topology, and 255 packets/second for SRPL-RP and 2247 packets/second for Standard RPL with Attacks in random topology. The control message value at the stability time is 867 packets/second for SRPL-RP and 25008 packets/second for Standard RPL with Attacks in grid-center topology, 1107 packets/second for SRPL-RP and 25008 packets/second for Standard RPL with Attacks in grid-random topology and 658 packets/second for SRPL-RP and 21167 packets/second for Standard RPL with Attacks in random topology. The Control Message at the end of the simulation is 1332 packets/second for SRPL-RP and 50462 packets/second for Standard RPL with Attacks in grid-center topology, 1468 packets/second for SRPL-RP and 41160 packets/second for Standard RPL with Attacks in grid-random topology and 991 packets/second for SRPL-RP and 43481 packets/second for Standard RPL with Attacks in random topology. We notice that the random topology has the highest performance in reducing the redundant amount of produced control messages than other topologies compared with Standard RPL with Attacks that have more generated control messages.



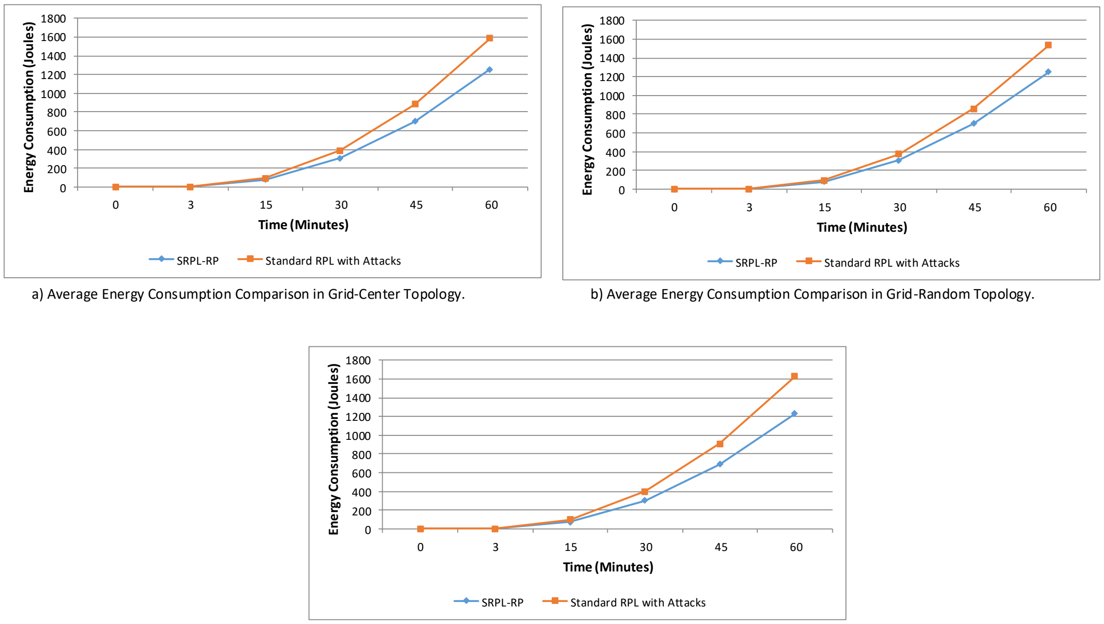
a) Control Message Overhead Comparison in Grid-Center Topology.

b) Control Message Overhead Comparison in Grid-Random Topology.

c) Control Message Overhead Comparison in Random Topology.

Figure 4. Control Message Comparison between SRPL-RP and RPL Standard RPL with Attacks in Three Topologies.

Fig. 5 shows the Average Energy Consumption results of SRPL-RP and Standard RPL with Attacks in Grid-Center Topology (a), Grid-Random Topology (b) and Random Topology (c) respectively. It shows that average energy consumption at the convergence time is 2.875 joules for SRPL-RP and 3.499 joules for Standard RPL with Attacks in grid-center topology, 2.864 joules for SRPL-RP and 3.354 joules for Standard RPL with Attacks in grid-random topology and 2.939 joules for SRPL-RP and 3.535 joules for Standard RPL with Attacks in random topology. The average energy consumption at the stability time is 308.576 joules for SRPL-RP and 387.081 joules for Standard RPL with Attacks in grid-center topology, and 307.403 joules for SRPL-RP and 375.805 joules for Standard RPL with Attacks in grid-random topology 304.300 joules for SRPL-RP and 398.095 joules for Standard RPL with Attacks in random topology. It shows that average energy consumption at the end of the simulation is 1255.538 joules for SRPL-RP and 1585.021 joules for Standard RPL with Attacks in grid-center topology, 1249.873 joules for SRPL-RP and 1535.808 joules for Standard RPL with Attacks in grid-random topology and 1231.778 joules for SRPL-RP and 1626.198 joules for Standard RPL with Attacks in random topology. We notice that our SRPL-RP can reduce the average energy consumption by up to 60% and even much lower in the random topology than in other topologies.



a) Average Energy Consumption Comparison in Grid-Center Topology.

b) Average Energy Consumption Comparison in Grid-Random Topology.

c) Average Energy Consumption Comparison in Random Topology.

Figure 5. Average Energy Consumption between SRPL-RP and RPL Standard RPL with Attacks in Three Topologies.

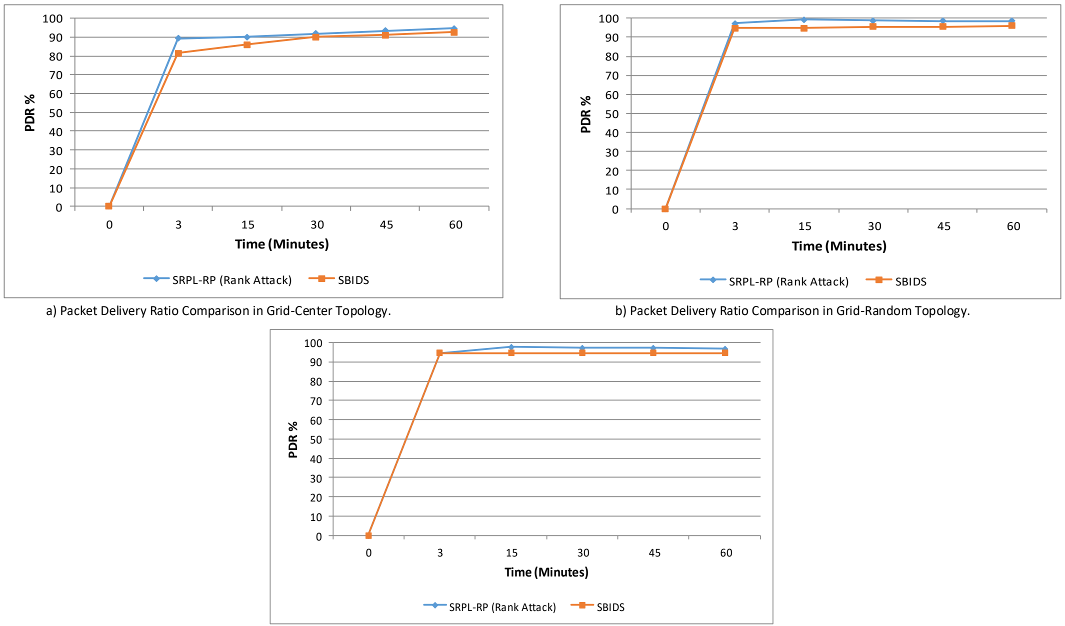
In the sub-section below, we divided the proposed SRPL-RP into two groups based on the rank attack and version number attack to compare and evaluate them with SBIDS [13], which offers detection of the rank attack and RPL+ Shield [14], which offers mitigation against version number attack. We ran 60 simulations for the rank attack group and in the three types of topologies at different time stages: the network convergence time, the network stability and the network at the end of the simulation.

5.2 SRPL-RP (Rank Attack) and SBIDS Results and Comparison

In this sub-section, we compared the performance of the proposed SRPL-RP (Rank Attack) and SBIDS [13] to evaluate their results in terms of network performance and detection accuracy.

5.2.1 Network Performance Results

The simulation results for the network performance parameters with respect to the three topologies and time stages are shown in Fig. 6, Fig. 7, and Fig. 8. where Fig. 6 shows the PDR results of SRPL-RP (Rank Attack) and SBIDS [13] in Grid-Center Topology (a), Grid-Random Topology (b) and Random Topology (c) respectively. It shows that PDR at the convergence time is 89.47% for SRPL-RP (Rank Attack) and 81.58% for SBIDS [13] in grid-center topology, 97.37% for SRPL-RP (Rank Attack) and 94.74% for SBIDS [13] in grid-random topology and 94.74% for SRPL-RP (Rank Attack) and 94.74% for SBIDS [13] in random topology. The PDR at the stability time is 91.83% for SRPL-RP (Rank Attack) and 90.02% for SBIDS [13] in grid-center topology, 98.73% for SRPL-RP (Rank Attack) and 95.46 for SBIDS [13] in grid-random topology and 97.46 % for SRPL-RP (Rank Attack) and 94.74% for SBIDS [13] in random topology. The PDR at the end of the simulation is 94.82% for SRPL-RP (rank Attack) and 92.69% for SBIDS [13] in grid-center topology, 98.48% for SRPL-RP and 95.99% for SBIDS [13] in grid-random topology and 96.88% for SRPL-RP and 94.74% for SBIDS [13] in random topology. We notice that SRPL-RP (Rank Attack) in gird-random topology has the highest PDR and can perform better than other topologies compared with SBIDS [13].



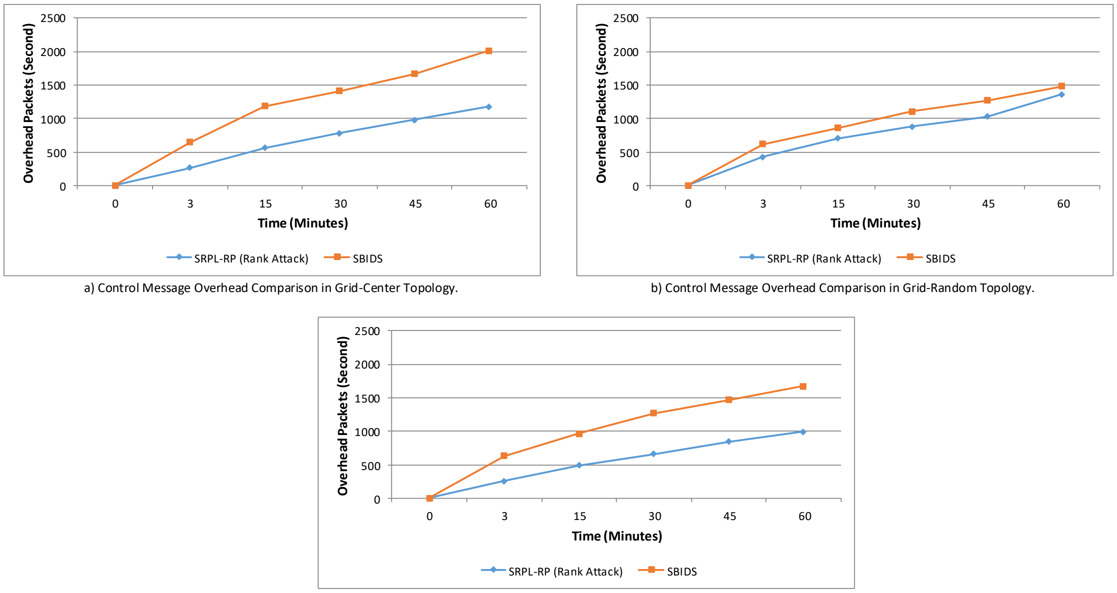
a) Packet Delivery Ratio Comparison in Grid-Center Topology.

b) Packet Delivery Ratio Comparison in Grid-Random Topology.

c) Packet Delivery Ratio Comparison in Random Topology.

Figure 6. Packet Delivery Ratio Comparison between SRPL-RP (Rank Attack) and SBIDS [13] in Three Topologies.

Fig. 7 shows the Control Message results of SRPL-RP (Rank Attack) and SBIDS [13] comparison in Grid-Center Topology (a), Grid-Random Topology (b) and Random Topology (c), respectively. It shows that the control message value at the convergence time is 267 packets/second for SRPL-RP (Rank Attack) and 245 packets/second for SBIDS [13] in grid-center topology, 430 packets/second for SRPL-RP (Rank Attack) and 619 packets/second for SBIDS [13] in grid-random topology and 255 packets/second for SRPL-RP (Rank Attack) and 630 packets/second for SBIDS [13] in random topology. The control message value at the stability time is 782 packets/second for SRPL-RP (Rank Attack) and 1414 packets/second for SBIDS [13] in grid-center topology, 877 packets/second for SRPL-RP (Rank Attack) and 1104 packets/second for SBIDS [13] in grid-random topology and 658 packets/second for SRPL-RP (Rank Attack) and 1272 packets/second for SBIDS [13] in random topology. The control message value at the end of the simulation is 1180 packets/second for SRPL-RP (Rank Attack) and 2015 packets/second for SBIDS [13] in grid-center topology, 1363 packets/second for SRPL-RP (Rank Attack) and 1479 packets/second for SBIDS [13] in grid-random topology, and 991 packets/second for SRPL-RP (Rank Attack) and 1676 packets/second for SBIDS [13] in random topology. We notice that the random topology has the highest performance in reducing the redundant amount of produced control messages than in other topologies compared with SBIDS [13].



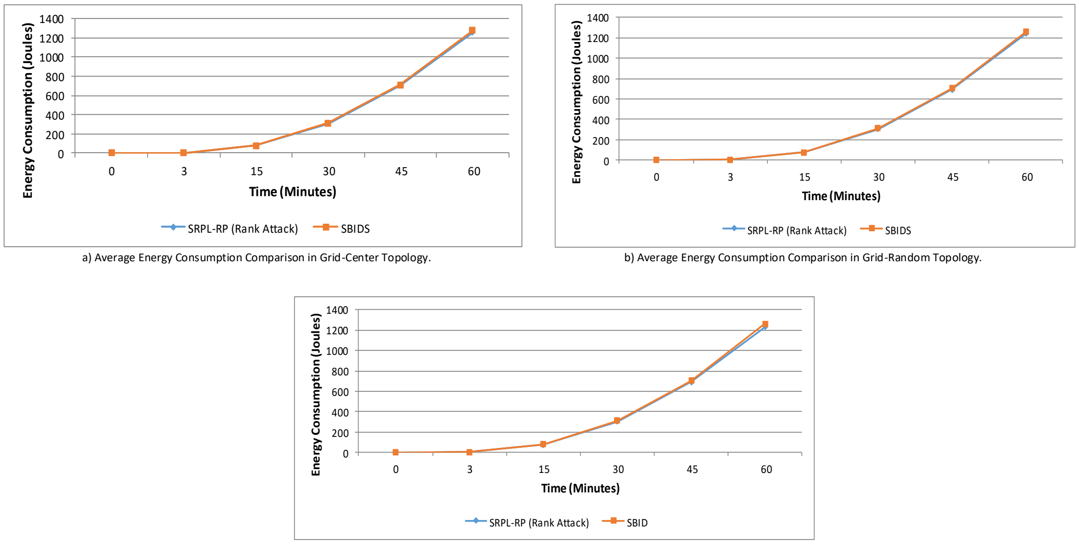
a) Control Message Overhead Comparison in Grid-Center Topology.

b) Control Message Overhead Comparison in Grid-Random Topology.

c) Control Message Overhead Comparison in Random Topology.

Figure 7. Control Message Comparison between SRPL-RP (Rank Attack) and SBIDS [13] in Three Topologies.

Fig. 8 shows the Average Energy Consumption results of SRPL-RP (Rank Attack) and SBIDS [13] in Grid-Center Topology (a), Grid-Random Topology (b) and Random Topology (c), respectively. It shows that average energy consumption at the convergence time is 2.927 joules for SRPL-RP (Rank Attack) and 3.084 joules for SBIDS [13] in grid-center topology, 2.827 joules for SRPL-RP (Rank Attack) and 2.973 joules for SBIDS [13] in grid-random topology and 2.939 joules for SRPL-RP (Rank Attack) and 3.005 joules for SBIDS [13] in random topology. The average energy consumption at the stability time is 309.474 joules for SRPL-RP (Rank Attack) and 314.903 joules for SBIDS [13] in grid-center topology, 303.417 joules for SRPL-RP (Rank Attack) and 309.661 joules for SBIDS [13] in grid-random topology, and 304.300 joules for SRPL-RP (Rank Attack) and 311.054 joules for SBIDS [13] in random topology. It shows that average energy consumption at the end of the simulation is 1258.783 joules for SRPL-RP (Rank Attack) and 1276.162 joules for SBIDS [13] in grid-center topology, 1237.753 joules for SRPL-RP (Rank Attack) and 1255.469 joules for SBIDS [13] in grid-random topology, and 1231.778 joules for SRPL-RP (Rank Attack) and 1259.908 joules for SBIDS [13] in random topology. We notice that the average energy consumption is lower and better in random topology than in other topologies.



a) Average Energy Consumption Comparison in Grid-Center Topology.

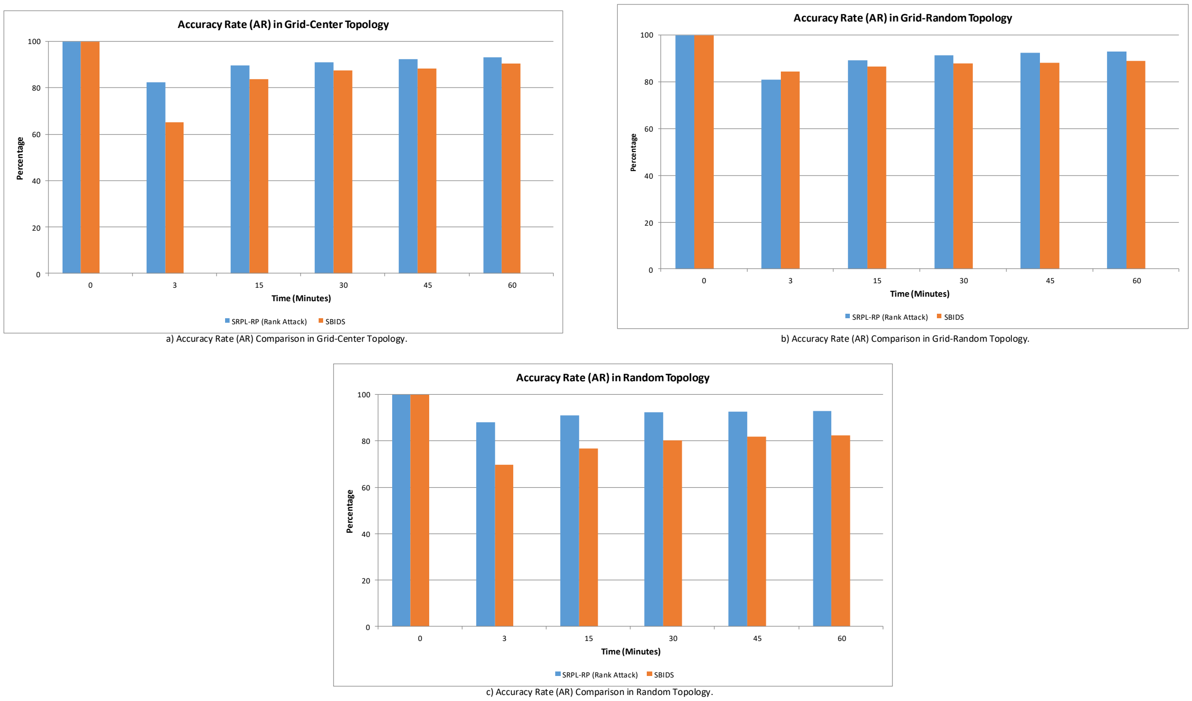
b) Average Energy Consumption Comparison in Grid-Random Topology.

c) Average Energy Consumption Comparison in Random Topology.

Figure 8. Average Energy Consumption Comparison between SRPL-RP (Rank Attack) and SBIDS [13] in Three Topologies.

5.2.2 Accuracy Results

In this section, we analyzed how the proposed SRPL-RP (Rank Attack) is accurately effective in detecting the malicious nodes and mitigating their effects by measuring the distinguish between legitimate nodes and malicious nodes with respect to the three types of topologies characteristics and comparison of the results with SBIDS [13]. Fig. 9 shows a comparison of the AR of SRP-RP (Rank Attack) and SBIDS[13] in the three types of topologies. It shows that the grid-center topology has the highest AR among other topologies compared with SBIDS [13]. The grid-random topology has the highest TN accuracy and the lowest FP accuracy among other topologies compared with SBIDS [13]. The grid-center topology has the lowest FN accuracy and the highest TP accuracy among other topologies compared with SBIDS [13]. Therefore, we notice that SRPL-RP (Rank Attack) is very effective at detecting the rank attack and mitigating their effects at the same time, especially in grid-center topology and grid-random topology.



a) Accuracy Rate (AR) Comparison in Grid-Center Topology.

b) Accuracy Rate (AR) Comparison in Grid-Random Topology.

c) Accuracy Rate (AR) Comparison in Random Topology.

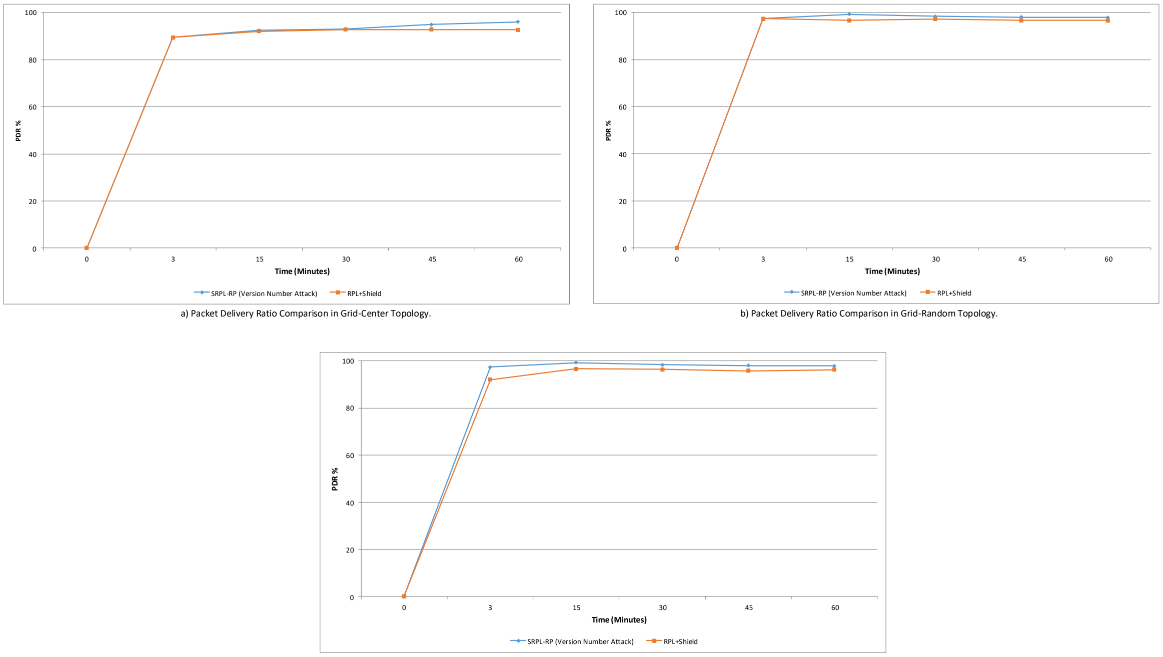
Figure 9. Accuracy Rate (AR) Comparison between SRPL-RP and SBIDS [13] in Three Topologies.

5.3 SRPL (Version Number Attack) and RPL+ Shield Results and Comparison

In this sub-section, we compared the performance of the proposed SRPL-RP (Rank Attack) and RPL+ Shield [14] to evaluate their results in terms of network performance and detection accuracy.

5.3.1 Network Performance Results

The simulation results for the network performance parameters with respect to the three topologies and time stages are shown in Fig. 10, Fig. 11, and Fig. 12. where Fig. 10 shows the PDR results of SRPL-RP (Version Number Attack) and RPL+ Shield [14] in Grid-Center Topology (a), Grid-Random Topology (b) and Random Topology (c) respectively. It shows that PDR at the convergence time is 89.47% for SRPL-RP (Version Number Attack) and 89.47% for RPL+ Shield [14] in grid-center topology, 97.37% for SRPL-RP (Version Number Attack) and 97.37% for RPL+ Shield [14] in grid-random topology and 97.37% for SRPL-RP (Version Number Attack) and 92.11% for RPL+ Shield [14] in random topology. The PDR at the stability time is 92.92% for SRPL-RP (Version Number Attack) and 92.74% for RPL+ Shield [14] in grid-center topology, 98.37% for SRPL-RP (Version Number Attack) and 97.28% for RPL+ Shield [14] in grid-random topology and 98.37 % for SRPL-RP (Version Number Attack) and 96.37% for RPL+ Shield [14] in random topology. The PDR at the end of the simulation is 96.07% for SRPL-RP (Version Number Attack) and 92.68% for RPL+ Shield [14] in grid-center topology, 97.95% for SRPL-RP (Version Number Attack) and 96.61% for RPL+ Shield [14] in grid-random topology and 97.95% for SRPL-RP (Version Number Attack) and 96.24% for RPL+ Shield [14] in random topology. We notice that the PDR is higher and better in random topology than in other types of topologies for SRPL-RP (Version Number Attack) compared with RPL+ Shield [14].



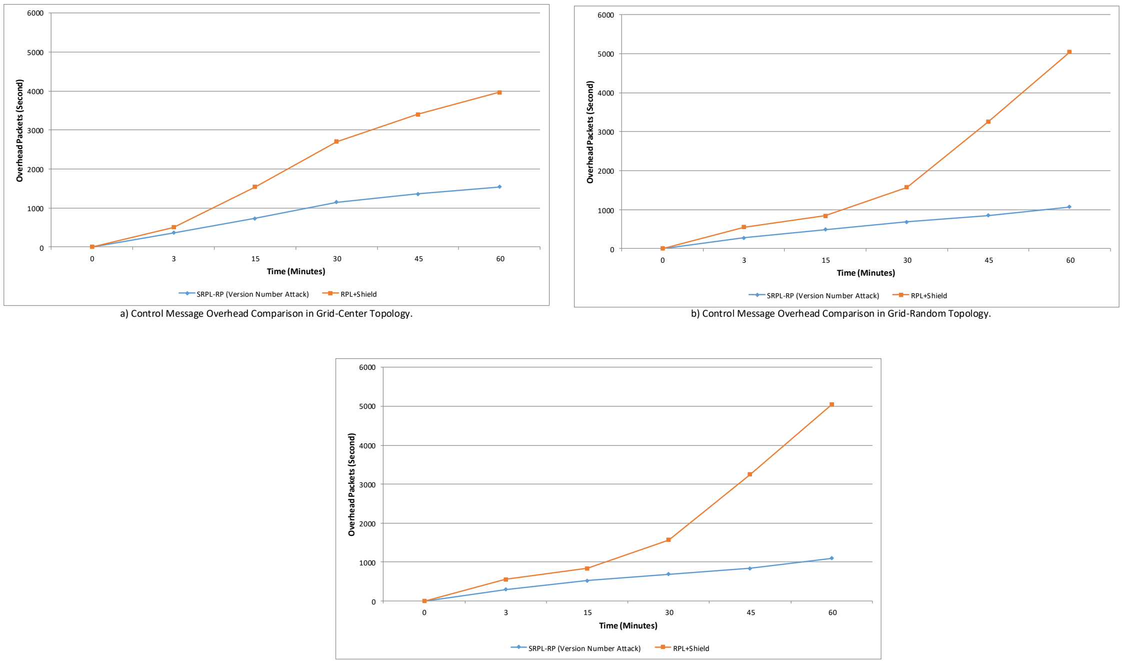
a) Packet Delivery Ratio Comparison in Grid-Center Topology.

b) Packet Delivery Ratio Comparison in Grid-Random Topology.

c) Packet Delivery Ratio Comparison in Random Topology.

Figure 10. Packet Delivery Ratio Comparison between SRPL-RP (Version Number Attack) and RPL + Shield [14] in Three Topologies.

Fig. 11 shows the Control Message results of SRPL-RP (Version Number Attack) and RPL+ Shield [14] comparison in Grid-Center Topology (a), Grid-Random Topology (b) and Random Topology (c) respectively. It shows that control message value at the convergence time is 364 packets/second for SRPL-RP (Version Number Attack) and 501 packets/second for RPL+ Shield [14] in grid-center topology, 275 packets/second for SRPL-RP (Version Number Attack) and 555 packets/second for RPL+ Shield [14] in grid-random topology and 297 packets/second for SRPL-RP (Version Number Attack) and 555 packets/second for RPL+ Shield [14] in random topology. The control message value at the stability time is 1150 packets/second for SRPL-RP (Version Number Attack) and 2700 packets/second for RPL+ Shield [14] in grid-center topology, 689 packets/second for SRPL-RP (Version Number Attack) and 1570 packets/second for RPL+ Shield [14] in grid-random topology and 690 packets/second for SRPL-RP (Version Number Attack) and 1570 packets/second for RPL+ Shield [14] in random topology. The control message value at the end of the simulation is 1543 packets/second for SRPL-RP (Version Number Attack) and 3964 packets/second for RPL+ Shield [14] in grid-center topology, 1072 packets/second for SRPL-RP (Version Number Attack) and 5045 packets/second for RPL+ Shield [14] in grid-random topology, and 1095 packets/second for SRPL-RP (Version Number Attack) and 5045 packets/second for RPL+ Shield [14] in random topology. We notice that the random topology has the highest performance in reducing the redundant amount of produced control messages than in other topologies compared with RPL+ Shield [14].



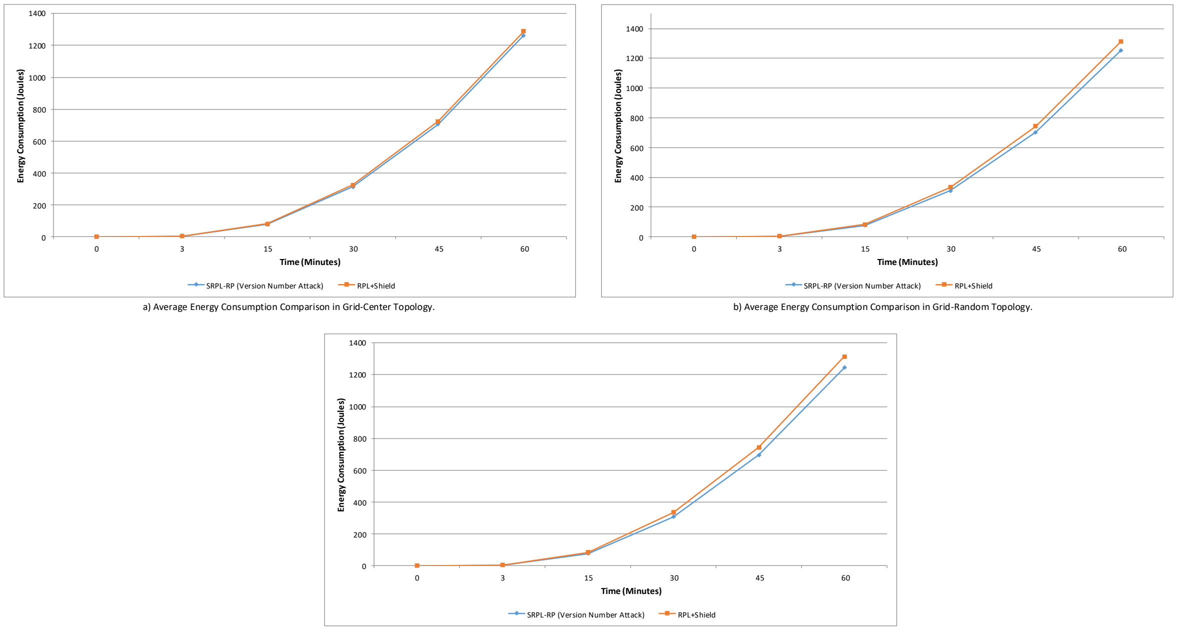
a) Control Message Overhead Comparison in Grid-Center Topology.

b) Control Message Overhead Comparison in Grid-Random Topology.

c) Control Message Overhead Comparison in Random Topology.

Figure 11. Control Message Comparison between SRPL-RP (Version Number Attack) and RPL+ Shield [14] in Three Topologies.

Fig. 12 shows the Average Energy Consumption results of SRPL-RP (Version Number Attack) and RPL+ Shield [14] in Grid-Center Topology (a), Grid-Random Topology (b) and Random Topology (c). It shows that average energy consumption at the convergence time is 2.931 joules for SRPL-RP (Version Number Attack) and 3.236 joules for RPL+ Shield [14] in grid-Center topology, 2.975 joules for SRPL-RP (Version Number Attack) and 3.326 joules for RPL+ Shield [14] in grid-random topology and 2.876 joules for SRPL-RP (Version Number Attack) and 3.326 joules for RPL+ Shield [14] in random topology. The average energy consumption at the stability time is 311.687 joules for SRPL-RP (Rank Attack) and 325.414 joules for RPL+ Shield [14] in grid-center topology, 309.380 joules for SRPL-RP (Version Number Attack) and 333.502 joules for RPL+ Shield [14] in grid-random topology and 305.617 joules for SRPL-RP (Version Number Attack) and 333.502 joules for RPL+ Shield [14] in random topology. It shows that average energy consumption at the end of the simulation is 1263.291 joules for SRPL-RP (Version Number Attack) and 1287.982 joules for RPL+ Shield [14] in grid-center topology, 1254.235 joules for SRPL-RP (Version Number Attack) and 1314.884 joules for RPL+ Shield [14] in grid-random topology and, 1244.819 joules for SRPL-RP (Version Number Attack) and 1314.884 joules RPL+ Shield [14] in random topology. We notice that the average energy consumption is lower and better in random topology than in other topologies.



a) Average Energy Consumption Comparison in Grid-Center Topology.

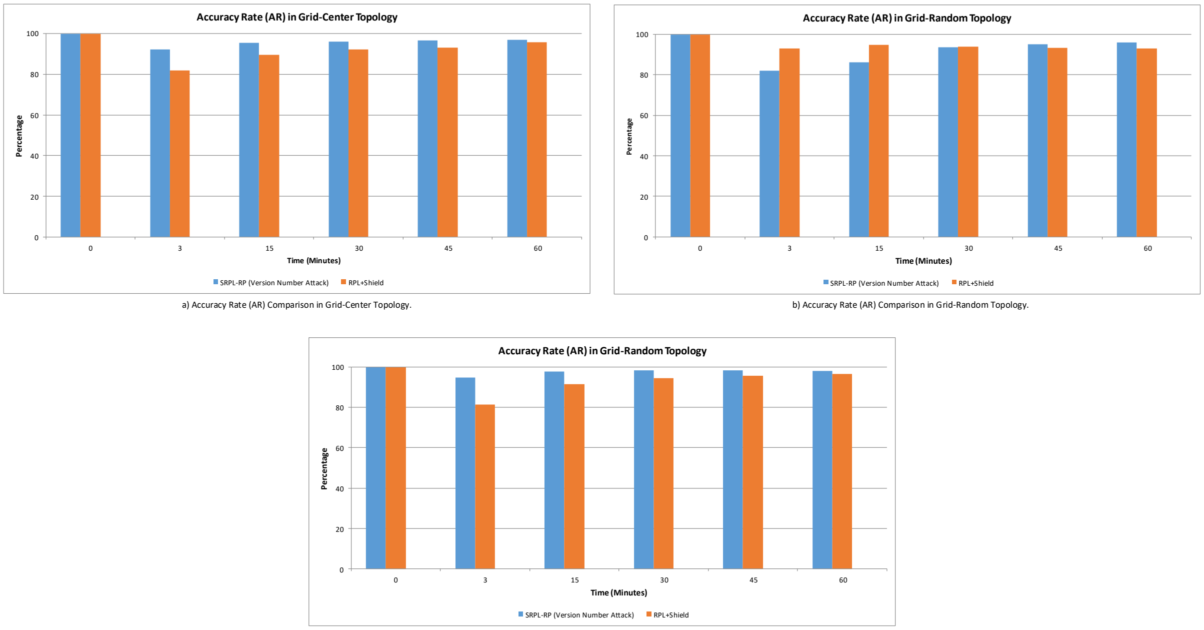
b) Average Energy Consumption Comparison in Grid-Random Topology.

c) Average Energy Consumption Comparison in Random Topology.

Figure 12. Average Energy Consumption Comparison between SRPL-RP (Version Number Attack) and RPL+ Shield [14] in Three Topologies.

5.3.2 Accuracy Results

In this section, we analyzed how the proposed SRPL-RP (Version Number Attack) is accurately effective in detecting the malicious nodes and mitigating their effects by measuring how the legitimate nodes are discriminated from malicious ones concerning the three types of topologies characteristics and comparison of the results with RPL+ Shield [14]. Fig. 13 shows a comparison of the AR of SRP-RP (Version Number Attack) and RPL+ Shield [14] in the three types of topologies. It shows that the random topology has the highest AR among other topologies compared with RPL+ Shield [14]. The grid-center topology has the highest TN accuracy and the lowest FP accuracy among other topologies compared with RPL+ Shield [14]. The random topology has the lowest FN accuracy and the highest TP accuracy among other topologies compared with RPL+ Shield [14].



a) Accuracy Rate (AR) Comparison in Grid-Center Topology.

b) Accuracy Rate (AR) Comparison in Grid-Random Topology.

c) Accuracy Rate (AR) Comparison in Random Topology.

Figure 13. Accuracy Rate (AR) Comparison between SRPL-RP (Version Number Attack) and RPL+ Shield [14] in Three Topologies.

6 DISCUSSION

In this section, we will demonstrate the security analysis of the proposed SRPL-RP and present the research findings and compare them with existing countermeasures to justify its effectiveness in terms of network performance and detection and mitigation accuracy.

6.1 Network Performance Discussion

From the analysis of the results in Section V, we find that SRPL-RP in the grid-center topology, SRPL-RP (Rank Attack) in the grid-random topology and SRPL-RP (Version Number Attack) in the random topology have the highest PDR and the best performance among other topologies compared with Standard RPL with Attacks, SBIDS [13] and RPL+ Shield [14]. On the other hand, the effects of attacks in Standard RPL with Attacks is almost doubled in random topology causing routing errors with majority of packets lost at the routing layer due to non-existing routes. Moreover, even though the SBIDS [13] provides detection against rank attack, but it still has a lower impact by providing better PDR compared with our SRPL-RP (Rank Attack), especially in grid-center topology, where the effect of rank attack is almost doubled. Furthermore, the effect of version number attack in RPL+ Shield [14] is almost tripled in grid-center topology, even though it provides mitigation of the attack compared with our SRPL-RP (Version Number Attack). It shows that the best average results for PDR can be extracted in the grid-center topology. The reason behind that is that the nodes are placed in uniform distribution and densities, and this ensures that each node can reach only its vertical and horizontal neighbor's during the simulation. Thus, this influences the RPL network and the quantity of parent nodes and child nodes that are created by the DODAG, in which a smaller number of parent nodes serving more child nodes. While in grid-random topology and random topology, each node may have more parent nodes. Hence, the parent nodes allow most of their child nodes to listen to the control messages. Thus, the DODAG of the RPL network can be constructed with more control messages. Therefore, PDR mainly depends on the node distribution and network topology, thus nodes that have more child nodes have a higher probability of having higher PDR. Furthermore, when the malicious nodes are closer to the root node, they can be easily detected by the proposed protocol, because when the malicious nodes are far from the root node, it may take longer for the root node to realize that there is a change in the network and it becomes harder to be detected, and by the time the changes are recognized in the network by the root node, the rest of legitimate nodes can be affected by the attack.

We find that SRPL-RP in the random topology, SRPL-RP (Rank Attack) in the random topology and SRPL-RP (Version Number Attack) in the random topology have the lowest and best performance in reducing the redundant amount of produced control messages than other topologies compared with Standard RPL with Attacks, SBIDS [13] and RPL+ Shield [14]. On the other hand, the effects of attacks in Standard RPL with Attacks are higher in grid-center topology. In addition, the number of generated control messages in SBIDS [13] is higher in grid-center topology. Additionally, RPL+ Shield [14] has more generated control messages even after applying the mitigation mechanism, especially in random topology. It shows that the best average results for a control message can be extracted in the random topology. This is due to the nature of topologies in which the malicious nodes spread in random topology faster than in the grid-center and grid-random topology that has a unified nature. This affects the number of parents and child nodes that create the DODAG that has more parent nodes in random placement, in which the parent nodes allow few of their child nodes to listen to the control messages. Thus, the DODAG of the RPL network can be constructed with more control messages. Hence, the proposed SRPL-RP can reduce the effect of excess generated control messages and successfully mitigate the effect of the attacks in which it prevents the malicious nodes from rebuilding the DODAG with higher parent nodes, thus less control messages will be generated.

We find that SRPL-RP in the random topology, SRPL-RP (Rank Attack) in the random topology and SRPL-RP (Version Number Attack) in the random topology have the lowest and the best performance for average energy consumption than other topologies compared with Standard RPL with Attacks, SBIDS [13] and RPL+ Shield [14]. On the other hand, the effects of attacks in Standard RPL with Attacks are higher in random topology for average energy consumption. Also, it is higher in SBIDS [13] in grid-center topology. At the same time, it is higher in both grid-random topology and random topology than the grid-center topology of RPL+ Shield [14] even after applying the mitigation mechanism. It shows that the best average results for average energy consumption can be extracted in the random topology. This is because there will be fewer paths among nodes owing to the impact of SRPL-RP, which results in fewer packets lost and generates few control messages. We notice that the average energy consumption is greater in random topology than the other topologies and this is because of both attacks and because there exist longer paths among nodes. Thus, majority of packets lost at the routing layer are due to routing errors caused by both attacks that makes most of the nodes dropping their packets, which consume much energy.

6.2 Accuracy Discussion

From the analysis of the result in Section V, we find that SRPL-RP in the grid-random topology, SRPL-RP (Rank Attack) in the grid-random topology and SRPL-RP (Version Number Attack) in the grid-center topology have the highest TN accuracy and the lowest FP accuracy among other topologies compared with SBIDS [13] and RPL+ Shield [14]. It means that in the case of TN, the percentage of the total number of malicious nodes that are correctly identified as attacking nodes is 97.65%, 98.04% and 98.04% for SRPL-RP, SRPL-RP (Rank Attack) and SRPL-RP (Version Number Attack). On the other hand, in case of FP, the percentage of the total number of malicious nodes that are falsely identified as legitimate nodes is 2.35%, 1.96% and 1.89% for SRPL-RP, SRPL-RP (Rank Attack) and SRPL-RP (Version Number Attack), which is a very small number compared with SBIDS [13], which has 7.04%, and RPL+ Shield [14], which has 7.61%. We find that SRPL-RP in the grid-center topology, SRPL-RP (Rank Attack) in the grid-center topology and SRPL-RP (Version Number Attack) in the random topology have the lowest FN accuracy and the highest TP accuracy among other topologies compared with SBIDS [13] and RPL+ Shield [14]. It means that in FN, the percentage of the total number of legitimate nodes that are falsely identified as the malicious node is only 5.33%, 11.22% and 1.35% for SRPL-RP, SRPL-RP (Rank Attack) and SRPL-RP (Version Number Attack), respectively, which is a very small number compared with SBIDS [13] and RPL+ Shield [14]. While in TP, the percentage of the total number of legitimate nodes that are not influenced by the proposed protocol is 94.67%, 88.78% and 98.65% for SRPL-RP, SRPL-RP (Rank Attack) and SRPL-RP (Version Number Attack), respectively. We find that SRPL-RP in the grid-center topology, SRPL-RP (Rank Attack) in the grid-center topology and SRPL-RP (Version Number Attack) in the random topology have the highest AR among other topologies compared with SBIDS [13] and RPL+ Shield [14]. It means that the percentage of the total accuracy metrics is 95.62%, 93.05% and 98.16% for SRPL-RP, SRPL-RP (Rank Attack) and SRPL-RP (Version Number Attack) compared with SBIDS [13] and RPL+ Shield [14].

The above analysis and discussion can clarify that the proposed SRPL-RP can be better in detecting, mitigating and isolating both rank and version number attacks in RPL networks in comparison with existing countermeasures in terms of network performance and detection and mitigation accuracy. Moreover, on basis of the comparison in Table 3 of studies in the literature review and the proposed SRPL-RP, it is shown that the proposed SRPL-RP can provide better functionalities, better network performance and better detection accuracy, as well as supporting against multiple attacks at the same time in the network. It is noticed that the effectiveness of the proposed SRPL-RP in terms of network performance is better in grid-center topology for PDR as the best result obtained is 98.48%, in random topology for control message value, as the best result obtained is 991 packets/second, and in random topology for average energy consumption as the best result obtained is 1231.778 joules. However, the effectiveness of the proposed SRPL-RP in terms of accuracy is better in grid-ceter topology of both SRPL-RP and SRPL-RP (Rank Attack) and random topology of SRPL-RP (Version Number Attack) for AR, as the best result obtained is 98.17% for the aforementioned reasons. The reason behind that is that the proposed SRPL-RP can provide verification of sender nodes by using the threshold, and after the detection happens, a mitigation technique can be applied to cope with the severe effects of both attacks.

Furthermore, to add extra security, a blacklist table with a threshold alert is implemented to isolate and alert all other relevant nodes to skip the malicious nodes from the network. Therefore, the proposed SRPL-RP can assist in the development and in reducing the risks of RPL networks security. Furthermore, an improved and higher safeguard can be provided against these two attacks, while providing efficient services and boosting user confidence.

Table III. Comparison among Studies in Literature Review and our Proposed Protocol.

Study/Parameters	**Support Multiple Attacks**	**Support Multiple Topologies**	**PDR**	**Control Message Overhead**	**Average Energy Consumption**	**AR**
SRPL [18]	Yes	No	83%	1550	4320 joules	-
SecTrust-RPL [19]	Yes	No	80%	-	-	-
Specification-Based IDS [20]	Yes	No	-	-	-	-

Secure Parent Node Selection Scheme [21]	No	No	-	-	-	-
ARM [22]	No	No	-	-	3560.796 joules	60%
SBIDS [13]	No	No	95.99	1479	1276.162 joules	90.40%
VeRA [26]	Yes	No	-	-	-	-
TRAIL [27]	No	No	-	-	-	-
Distributed and Cooperative Verification Mechanism [28]	No	No	97%	1500	-	-
Lightweight Defense Approach [29]	Yes	No	-	-	-	-
Lightweight Mitigation Techniques [14]	No	Yes	92.68%	5045	1314.884 joules	92.93%
Distributed Monitoring Strategy [30]	No	No	-	-	-	-
Our Proposed SRPL-RP	Yes	Yes	98.48%	991 packets/second	1231.778 joules	98.17%

7 CONCLUSION

Data packets addressing and routing among smart IoT constrained devices are an issue because of the necessity of developing integrated protocols for data packets routing across different RPL networks. Several RPL attacks occur through the activities of malicious nodes during the data packets routing among devices. This research has studied the latest research literature that focus on rank, and version number attack. Considering the research gap, we found that recent studies do not support multiple attacks in RPL networks for measuring the effectiveness of their proposals. They do not detect and mitigate the effects of both attacks in the RPL networks.

Furthermore, this research has provided a proposal and implementation of SRPL-RPL protocol that can address the current flaws in the existing studies by limiting the impacts of these attacks. According to the simulation results in the analysis, the proposed SRPL-RP is more secure and more efficient in terms of network performance and accuracy. It can provide a higher PDR, and lower control message value compared with existing countermeasures in all types of network topologies. In addition, it can provide more than a 95% accuracy rate in all types of network topologies.

8 FUTURE WORK

We aim to implement the feature of mobile nodes in the RPL network including mobility, and to safeguard these nodes against attacks. Hence, they have the ability to be scalable, communicating more efficiently and covering large networks such as smart city networks.

9 REFERENCES

[1] Z. A. Almusaylim and N. Zaman, “A review on smart home present state and challenges: linked to context-awareness internet of things (IoT),” Wirel. Networks, vol. 25, no. 6, pp. 3193–3204, 2019, doi: 10.1007/s11276-018-1712-5.

[2] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of Things for Smart Cities,” IEEE Internet Things J., vol. 1, no. 1, pp. 22–32, 2014, doi: 10.1109/jiot.2014.2306328.

[3] Z. A. Almusaylim, N. Zaman, and L. T. Jung, “Proposing A Data Privacy Aware Protocol for Roadside Accident Video Reporting Service Using 5G In Vehicular Cloud Networks Environment,” 2018 4th International Conference on Computer and Information Sciences (ICCOINS). IEEE, Kuala Lumpur, Malaysia, pp. 1–5, 2018, doi: 10.1109/iccoins.2018.8510588.

[4] Z. A. Almusaylim and N. Z. Jhanjhi, “Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing,” Wirel. Pers. Commun., pp. 1–24, 2019, doi: 10.1007/s11277-019-06872-3.

[5] G. Ma X. Li, Q. Pei, and Z. Li, "A Security Routing Protocol for Internet of Things Based on RPL," 2017 International Conference on Networking and Network Applications (NaNA). IEEE, Kathmandu, Nepal, pp. 209–213, 2017, doi: 10.1109/NaNA.2017.28.
[6] B. N. Silva, M. Khan, and K. Han, "Internet of Things: A Comprehensive Review of Enabling Technologies, Architecture, and Challenges," IETE Tech. Rev., vol. 35, no. 2, pp. 205–220, 2018, doi: 10.1080/02564602.2016.1276416.
[7] M. Humayun, M. Niazi, N. Z. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," Arab. J. Sci. Eng., 2020, doi: 10.1007/s13369-019-04319-2.
[8] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," J. Netw. Comput. Appl., vol. 66, pp. 198–213, 2016, doi: 10.1016/j.jnca.2016.03.006.
[9] H. Kharrufa, H. A. A. Al-Kashoash, and A. H. Kemp, "RPL-Based Routing Protocols in IoT Applications: A Review," IEEE Sens. J., vol. 19, no. 15, pp. 5952–5967, 2019, doi: 10.1109/Jsen.2019.2910881.
[10] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, "The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks," IEEE Sens. J., vol. 13, no. 10, pp. 3685–3692, 2013, doi: 10.1109/jsen.2013.2266399.
[11] V. Abhishek and R. Virender, "Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review," IEEE Sens. J., vol. 20, no. 11, pp. 5666–5690, 2020, doi: 10.1109/JSEN.2020.2973677.
[12] Z. A. Almusaylim, A. Alhumam, and N. Z. Jhanjhi, "Proposing a Secure RPL based Internet of Things Routing Protocol: A Review," Ad Hoc Networks, pp. 1–26, 2020.
[13] U. Shafique, A. Khan, A. Rehman, F. Bashir, and M. Alam, "Detection of rank attack in routing protocol for Low Power and Lossy Networks," Ann. Telecommun., vol. 73, no. 7–8, pp. 429–438, 2018, doi: 10.1007/s12243-018-0645-4.
[14] A. Arış, S. B. Örs Yalçın, and S. F. Oktuğ, "New lightweight mitigation techniques for RPL version number attacks," Ad Hoc Networks, vol. 85, pp. 81–91, 2019, doi: 10.1016/j.adhoc.2018.10.022.
[15] V.K.Karthik and M.Pushpalatha, "Addressing Attacks and Security Mechanism in the RPL based IOT," Int. J. Comput. Sci. Eng. Commun., vol. 5, no. 5, pp. 1715–1721, 2017.
[16] S. Mangelkar, S. N. Dhage, and A. V Nimkar, "A comparative study on RPL attacks and security solutions," 2017 International Conference on Intelligent Computing and Control (I2C2). IEEE, Coimbatore, India, pp. 1–6, 2017, doi: 10.1109/i2c2.2017.8321851.
[17] A. Raoof, A. Matrawy, and C.-H. Lung, "Routing Attacks and Mitigation Methods for RPL-Based Internet of Things," IEEE Commun. Surv. Tutorials, vol. 21, no. 2, pp. 1582–1606, 2019, doi: 10.1109/comst.2018.2885894.
[18] G. Glissa, A. Rachedi, and A. Meddeb, "A Secure Routing Protocol Based on RPL for Internet of Things," 2016 IEEE Global Communications Conference (GLOBECOM). IEEE, Washington, DC, USA, pp. 1–7, 2016, doi: 10.1109/glocom.2016.7841543.
[19] D. Airehrour, J. A. Gutierrez, and S. K. Ray, "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things," Futur. Gener. Comput. Syst., vol. 93, pp. 860–876, 2019, doi: 10.1016/j.future.2018.03.021.
[20] A. Le, J. Loo, Y. Luo, and A. Lasebae, "Specification-based IDS for securing RPL from topology attacks," 2011 IFIP Wireless Days (WD). IEEE, Niagara Falls, ON, Canada, pp. 1–3, 2011, doi: 10.1109/wd.2011.6098218.
[21] K. Iuchi, T. Matsunaga, K. Toyoda, and I. Sasase, "Secure parent node selection scheme in route construction to exclude attacking nodes from RPL network," 2015 21st Asia-Pacific Conference on Communications (APCC). IEEE, Kyoto, Japan, pp. 299–303, 2015, doi: 10.1109/apcc.2015.7412530.
[22] A. Althubaity, H. Ji, T. Gong, M. Nixon, R. Ammar, and S. Han, "ARM: A hybrid specification-based intrusion detection system for rank attacks in 6TiSCH networks," 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). IEEE, Limassol, Cyprus, pp. 1–8, 2017, doi: 10.1109/etfa.2017.8247593.
[23] H. Patel, H. Patel, and B. Shrimali, "A Survey on Trust-based Intrusion Detection for Version Number Attack on RPL," Int. J. Comput. Sci. Eng., vol. 6, no. 10, pp. 449–454, 2018.
[24] P. O. Kamgueu, E. Nataf, and T. D. Ndie, "Survey on RPL enhancements: A focus on topology, security and mobility," Comput. Commun., vol. 120, pp. 10–21, 2018, doi: 10.1016/j.comcom.2018.02.011.
[25] A. Aris, S. F. Oktug, and S. Berna Ors Yalcin, "RPL version number attacks: In-depth study," NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium. IEEE, Istanbul, Turkey, pp. 776–779, 2016, doi: 10.1109/noms.2016.7502897.
[26] Dvir, T. Holczer, and L. Buttyan, "VeRA - Version Number and Rank Authentication in RPL," 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems. IEEE, Valencia, Spain, pp. 709–714, 2011, doi: 10.1109/mass.2011.76.

[27] H. Perrey, M. Landsmann, O. Ugus, M. Wählisch, and T. C. Schmidt, "TRAIL: Topology Authentication in RPL," in EWSN '16 Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks, 2016, pp. 59–64.
[28] F. Ahmed and Y.-B. Ko, "A Distributed and Cooperative Verification Mechanism to Defend against DODAG Version Number Attack in RPL," in PECCS 2016 Proceedings of the 6th International Joint Conference on Pervasive and Embedded Computing and Communication Systems, 2016, pp. 55–62, doi: 10.5220/0005930000550062.
[29] M. Nikravan, A. Movaghar, and M. Hosseinzadeh, "A Lightweight Defense Approach to Mitigate Version Number and Rank Attacks in Low-Power and Lossy Networks," Wirel. Pers. Commun., vol. 99, no. 2, pp. 1035–1059, 2018, doi: 10.1007/s11277-017-5165-4.
[30] A. Mayzaud, R. Badonnel, and I. Chrisment, "A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks," IEEE Trans. Netw. Serv. Manag., vol. 14, no. 2, pp. 472–486, 2017, doi: 10.1109/tnsm.2017.2705290.
[31] P. Thulasiraman and Y. Wang, "A Lightweight Trust-Based Security Architecture for RPL in Mobile IoT Networks," 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), vol. IEEE. Las Vegas, NV, USA, pp. 1–6, 2019, doi: 10.1109/ccnc.2019.8651846.
[32] Tandon and P. Srivastava, "Trust-based Enhanced Secure Routing against Rank and Sybil Attacks in IoT," 2019 Twelfth International Conference on Contemporary Computing (IC3). IEEE, Noida, India, pp. 1–7, 2019, doi: 10.1109/ic3.2019.8844935.
[33] V. Neerugatti and A. R. M. Reddy, "Machine Learning Based Technique for Detection of Rank Attack in RPL based Internet of Things Networks," Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 9S3, p. 5, 2019.
[34] D. Hankerson, S. Vanstone, and A. Menezes, Guide to Elliptic Curve Cryptography. New York: Springer, 2004.
[35] M. Sarumathi and J. Abbas, "A Lightweight Intrusion Detection for Sybil Attack Under Mobile RPL in the Internet of Things," IEEE Internet Things J., vol. 7, no. 1, pp. 379–388, 2020, doi: 10.1109/JIOT.2019.2948149.
[36] Dunkels, "Contiki: The Open Source OS for the Internet of Things," 2003. http://www.contikios.org/index.html.
[37] Maria, I. Nazurl, and J. NZ, "A Lightweight and Secure Authentication Scheme for IoT Based E-Health Application," IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 19, no. 1, pp. 107–120, 2019.