IBIMA Publishing
Communications of the IBIMA
https://ibimapublishing.com/articles/CIBIMA/2025/335263/
Vol. 2025 (2025), Article ID 335263, 17 pages, ISSN: 1943-7765
https://doi.org/10.5171/2025.335263

Research Article

Performance of RPL-based Wireless Sensor Networks Subjected to Selected Attacks

Przemyslaw MACIEJKO and Jaroslaw KRYGIER

Military University of Technology, Faculty of Electronics, Warsaw, Poland

Correspondence should be addressed to: Jaroslaw KRYGIER; jaroslaw.krygier@wat.edu.pl

Received date: 4 September 2024; Accepted date:10 December 2024; Published date: 3 February 2025

Academic Editor: Pascal Muam Mah

Abstract

The paper focuses on evaluating the performance of wireless sensor networks (WSNs) equipped with the Routing Protocol for Low-Power and Lossy Networks (RPL) that have been subjected to Blackhole, Sinkhole, Version Number and DIS Flooding attacks. In a WSN consisting of dozens of sensors, which are also nodes forwarding IPv6 traffic to a border node, the IPv6/6LoWPAN/IEEE 802.15.4 protocol stack was used. The indicated attacks were carried out in two scenarios. In the first, selected sensors were replaced with sensors with modified software, which enabled an attack on the RPL protocol. In the next scenario, intruder nodes were added to the network, which attached themselves to the existing network structure and thus carried out attacks on the RPL protocol. The article is oriented not to evaluate the effectiveness of the attacks in both scenarios, but to evaluate the performance of the sensor network during the success of each attack. Thus, it was possible to draw conclusions about such an organization of sensor network structures that will enable minimizing the effects of selected attacks in the context of maximizing network performance. Due to the fact that all of the aforementioned attacks were carried out simultaneously at different locations on the network, the degradation of the network resulted in a significant decrease in its performance. Nevertheless, thanks to the research performed, a number of recommendations were prepared to prepare a network that performs its tasks despite the success of individual attacks.

Keywords: WSN, RPL, routing protocols, sensor network security

____

Cite this Article as: Przemyslaw MACIEJKO and Jaroslaw KRYGIER (2025)," Performance of RPL-based Wireless Sensor Networks Subjected to Selected Attacks", Communications of the IBIMA, Vol. 2025 (2025), Article ID 335263, https://doi.org/10.5171/2025.335263

Introduction

The growth of the Internet of Things (IoT) observed in recent years has contributed to the rise of Wireless Sensor Networks (WSN). In particular, networks in which sensors use popular wireless communication techniques such as Bluetooth, Wi-Fi, or techniques based on the IEEE 802.15.4 recommendation are of great interest. Given the large number of sensors that can be used in IoT implementations, the use of IPv6 (Internet Protocol version 6) is of particular importance. Therefore, IPv6 is becoming a natural fit for sensor networks. It should also be noted that battery-powered sensors force a reduced radio range, resulting in the need to use sensors not only as end nodes but also as intermediate nodes for data retransmission. The transmission of data in such networks therefore requires the use of routing protocols as well to find routes. Given the limitations associated with the Maximum Transmission Units (MTU) offered by the radio communication techniques used in WSNs, a set of mechanisms has been developed to allow IPv6 packets to be transmitted over such networks. Perhaps the most mature mechanism is 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) (Montenegro, 2007). 6LoWPAN is basically used to transmit IPv6 packets in a WSN based on the IEEE 802.15.4 standard, which offers an MTU size of 127 bytes. Such a small MTU is a limitation to the transmission of native IPv6 packets, which cannot be smaller than 1280 bytes. The 6LoWPAN therefore offers mechanisms to segment IPv6 packets so that they can be transmitted over a network with small MTU sizes (where inbuilt IPv6 fragmentation is not possible). In addition, it offers mechanisms for neighborhood discovery, headers compression, and segments forwarding. To implement routing in a WSN based on the 6LoWPAN, the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) (Winter, 2012) was developed. The RPL is a proactive routing protocol that, through the periodic exchange of signaling messages, allows the creation of a directed acyclic graph (DAG) – a tree with a root node that corresponds to the WSN gateway. Each node in the network is assigned a rank, which increases as that node moves away from the root node. Thus, the nodes (sensors) send data (e.g., measurement data) to the gateway (root) via intermediate nodes using the shortest paths according to the principle, minimizing the rank of subsequent nodes. Graphically, the data flow graph of the network is illustrated by the Destination Oriented Directed Acyclic Graph (DODAG) rooted at the gateway. To create a routing tree, the RPL protocol uses three types of signaling messages: DIS (DODAG Information Solicitation), DIO (DODAG Information Object), and DAO (Destination Advertisement Object).

Unfortunately, the exchange of these messages in WSNs can be a potential target for attacks to destabilize network operations. A number of attacks on the RPL protocol have been well described in the literature (for example, by Albinali and Azzedin, 2024), which, quite simply, either disable part or all of the network or allow traffic to be routed through malicious nodes. The purpose of our paper is not to show the possibility of attacking a 6LoWPAN-based sensor network with the RPL protocol, thus duplicating literature solutions, but to show how the deployment of malicious nodes performing selected attacks affects the performance of the WSN and its resistance to these attacks.

Thus, the main contribution of this paper is to evaluate the impact of a sensor network topology, as well as the location of attacker nodes, on the effectiveness of selected attacks on network topology and attacks on network resources.

The paper is organized as follows. The next section describes the main related works on attacks on sensor networks with the RPL protocol. The basic features of the attacks on the 6LoWPAN/RPL-based network are then described, which were analyzed in the context of the purpose of this paper. After that, assumptions about the topology of the sensor network under test were made. Test results and discussion section includes a discussion of the results obtained during the set of tests. A summary of the paper is included in the last section.

Related Works

In 6LoWPAN/RPL-based WSNs, the impact of malicious nodes on security and performance has been widely studied. In addition, different types of attacks have been analyzed and solutions have been proposed to mitigate them to ensure network reliability and performance. Only the main references are indicated in this section to show the comprehensiveness and importance of the issue of sensor network security.

As an example, Rajasekar V. R. and Rajkumar S. (2021) focus on the analysis of Blackhole attacks in RPL-based networks. They investigate how blackhole attacks disrupt network operations by maliciously dropping packets intended for specific destinations, leading to significant data loss and network instability. They used simulation-based experiments to analyze the impact of these attacks on packet delivery ratio, end-to-end delay, and control message overhead. The results highlight the severe degradation in network performance due to blackhole nodes and emphasize the need for effective detection and mitigation strategies to maintain network reliability.

Zaminkar M. and Fotohi R. (2020) present a comprehensive security framework named SoS-RPL, aimed at securing IoT networks against Sinkhole attacks. Sinkhole attacks involve a malicious node attracting all traffic by falsely advertising an optimal route, leading to severe data interception and potential network collapse. The SoS-RPL framework integrates anomaly detection techniques and cryptographic methods to identify and isolate malicious nodes effectively. Zaminkar and Fotohi (2020) describe the implementation of their approach and validate its effectiveness through extensive simulations, demonstrating improved resilience and stability of IoT networks against Sinkhole attacks.

Almusaylim Z. A. et al. (2020) address the problem of rank and version number attacks in RPL networks. The authors propose an attack detection and mitigation scheme that includes monitoring tables and blacklisting strategies to identify and counter malicious activity. Their experimental results show a significant reduction in the adverse effects of these attacks on network performance, highlighting the effectiveness of their proposed solution.

Of course, there are many more publications that describe various attacks on sensor networks that use the RPL protocol. Most of the authors, similarly to the ones cited above, show the method of attack and often methods to counter it, assuming special cases of sensor network topology. However, the authors of this publication focused on evaluating the location of nodes attacking with selected attacks on the effectiveness of the attacks and on the performance of the attacked sensor network. To the best of our knowledge, there is no similar assessment in available publications, which can provide valuable insight into how to minimize the effects of attacks on sensor networks by using an appropriate network topology.

Features of selected attacks on 6LoWPAN/RPL-based WSNs

Sensor systems using low-power and high-packet-loss wireless networks, due to limited resources, lack of infrastructure, variable topology and unstable links, are extremely vulnerable to attacks. This section briefly characterizes the categories and subcategories of attacks on the RPL routing protocol used in such networks. This description is based on the analysis available in Mayzaud et al. (2016) and was prepared to give the reader an idea of the features of the attacks analyzed in this publication.

Attacks on network topology

Attacks on network topology can be divided into suboptimization and isolation attacks. In the case of the former, the network under attack will not achieve an optimal topological structure (i.e. packets will not be sent along optimal routes), resulting in poor network performance. The second aims to isolate a node or group of nodes in the network, meaning that these sensors will not be able to communicate with the root sensor (gateway). This paper focuses on Blackhole and Sinkhole attacks, which are examples of attacks on network topology. They are briefly characterized in the following subsections.

Blackhole attacks

A Blackhole attack belongs to a subcategory of isolation attacks. It is similar to a black hole that sucks in all packets. This attack involves the attacker silently discarding all data packets that should be forwarded. The intruder being the intermediate node between the communicating nodes, therefore, prevents communication between them. The RPL protocol is vulnerable to this type of attack because it does not reconfigure the network to look for alternative routes, due to the lack of information about incoming packets and the lack of changes in routing tables (Mayzaud et al., 2016; Pongle and Chavan, 2015). Fig. 1 shows the principle of the Blackhole attack, where node 4 is the Blackhole attacker and node 1 is the root node (the gateway). Packets sent by nodes 7 and 8 to the gateway are lost in node 4.

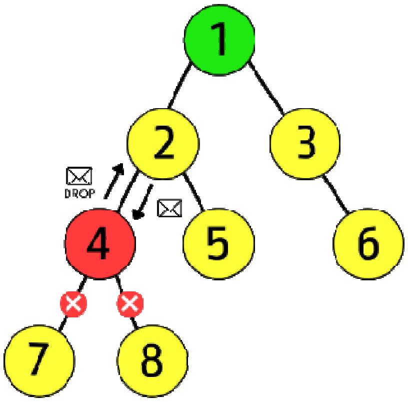

Fig. 1. Blackhole attack principle (Source (Own))

Sinkhole attacks

A Sinkhole attack belongs to the subcategory of suboptimization attacks. It takes place in two stages. First, the attacking node announces a more favorable communication path in order to attract many nearby sensors to route their traffic through it. Then the intruder, after receiving the packets, discards them. This attack in an RPL-based sensor network can be carried out by manipulating the rank value of the sensors. It is a combination of two attacks, Blackhole and Rank Decrease. The RPL protocol is susceptible to the Sinkhole attack because it does not have the ability to self-repair after the attack, which modifies the topology and degrades network performance (Pongle and Chavan, 2015). Fig. 2 shows the principle of the Sinkhole attack, where node 4 is the attacker and node 1 is the root node. Before the attack, node 5 communicated with the gateway through node 3. During the attack, the attacking node forced a route for node 5 through itself, while blocking transmission to the gateway.

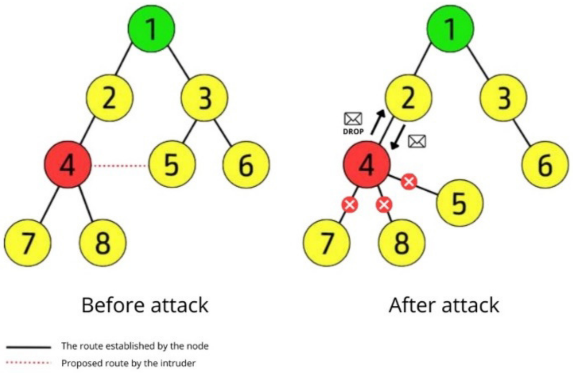
1
2
3
4
5
6
7
8
Before attack
1
2
3
DROP
4
5
6
7
8
After attack
The route established by the node
Proposed route by the intruder

Fig 2. Sinkhole attack principle (Source (Own))

Attacks against resources

Attacks targeting network resources of RPL-based sensor devices typically involve forcing nodes to generate unnecessary network traffic to drain their resources. Among the goals of these attacks is increasing the energy or memory consumption of sensors, which can affect the performance of complex functions by overloading available links. Two subcategories of these attacks can be distinguished. The first focuses on direct attacks, during which the intruder generates unnecessary traffic to overload and degrade the network. The second includes indirect attacks, in which the attacking nodes cause other sensors in the network to start generating unnecessary traffic. This paper analyzes the impact of the deployment of nodes attacking with the DIS Flooding and Version Number methods, which represent attacks on network resources. The following subsections briefly characterize these attacks.

DIS flooding attack

The DIS Flooding attack belongs to a subcategory of direct attacks. It involves generating a lot of traffic on the network, causing nodes and links to become unavailable. In RPL-based networks, the attacker can continuously send DIS control messages, causing network overflow. Furthermore, an excess of these messages causes an inconsistency to be detected in the network, and nodes begin to reset their DIO sending clock, causing them to send more of these messages. Among other things, this attack can cause the nodes to consume more power and make network communication more difficult (Verma and Ranga, 2020). Fig. 3 shows the principle of the DIS Flooding attack, where node 10 is the attacking sensor, and node 1 is the root. Node 10 floods neighboring nodes with DIS messages, causing those nodes to consume significantly more resources, mainly energy.

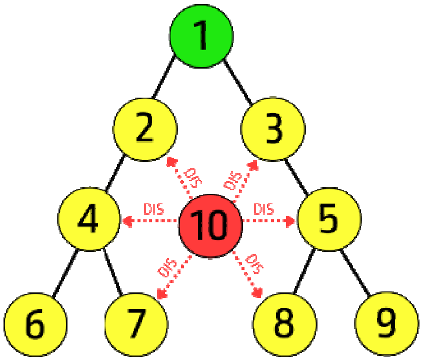

Fig. 3. DIS flooding attack principle (Source (Own))

Version Number attack

The Version Number attack belongs to a subcategory of indirect attacks. In RPL-based sensor networks, it is implemented by incrementing the version number of the DODAG tree in a DIO control message sent by the attacking node. When sensors receive such a message with a new and higher version number, they start creating a new DODAG tree. This causes an excessive generation of control traffic in the network. This parameter is modified only by the root node, however, the RPL protocol does not have proper safeguards against its modification by an intruder. This attack can result in increased energy consumption and control overhead from sensors, as well as higher packet loss (Pongle and Chavan, 2015).

Assumptions for studying the impact of malicious node deployment on the performance of a 6LoWPAN/RPL-based WSNs

For the purpose of our study, the structure of the sensor network was adopted in an example scheme
of a shopping mall, where sensors perform the function of air quality monitoring. We assumed the use of Zolerta Z1 sensors based on a 16-bit MSP430F2617 microcontroller (Tracey, 2020). The sensor nodes are equipped with a transceiver (CC2520) compliant with the IEEE 802.15.4 standard. The sensors allow radio communication within a range of 30 to 125 m (Al-Suhail et al., 2017). During our tests, it was assumed that the sensors operate at minimum power and that radio wave propagation through walls results in a 20-30% reduction in range. We assumed the use of the 6LoWPAN/RPL protocol stack implemented in the Contiki OS (Oikonomou et al., 2022). In order to increase the efficiency of the research, the Cooja emulator (Solapue, et al., 2020; Algahtani, et al., 2021) was used for the tests, allowing the emulation of a sensor network with the real Contiki OS and with simulated IEEE 802.15.4-based radio links. The Collect View available in the Cooja emulator enabled the collection of node data, and the Mote Output tool captured and analyzed messages sent by individual nodes. The RPL routing protocol control messages were analyzed, as well as information related to parent selection and sensor routing tables. The data collected by the Collect View tool were also verified in the context of the number of packets received by the root sensor from the remaining nodes. Additionally, average energy consumption of each sensor was checked. To observe the effectiveness of the attacks and the behavior of the network, 10 minutes of network operation were analyzed.

Reference network topology

In order to evaluate the impact of the location of attackers on the effectiveness of the attack and the efficiency of the network, a reference network was assumed, in which there were no malicious nodes in the first stage, and then some nodes were swapped with nodes that performed selected attacks.

Fig. 4 shows the reference topology of a sensor network on a map of a hall consisting of 17 rooms (Pom 1 through 17). The other numbers specify the size of the rooms (in meters). The network consists of one root node (N1: green) and twenty-two transmitting sensors (N2 - N23: yellow). Some of the transmitting sensors (N2 - N4) are within the direct radio range of the root, while the rest must provide data via other intermediate nodes. Arrows represent the radio links.

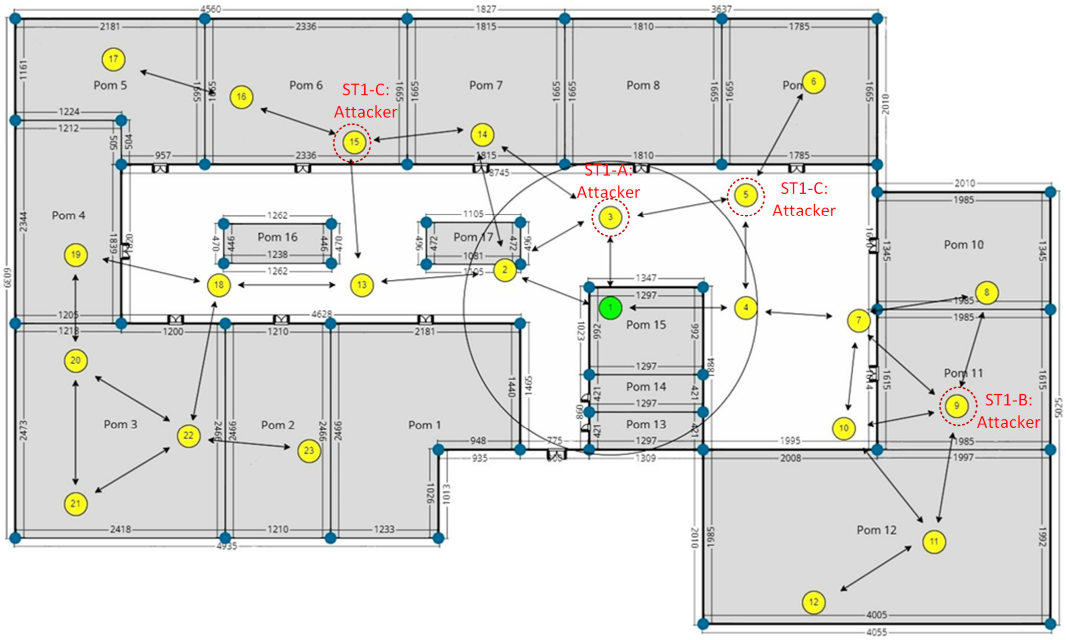

Fig. 4. Reference sensor network topology (Source (Own))

Assumptions for attacks on the network topology

To study the vulnerability of the RPL protocol to topology attacks, intruders are added to network structure presented in Fig. 4. The tests were conducted for two main scenarios. In the first scenario (ST1), the selected sensors were replaced with the attacker sensors, while, in the second scenario (ST2), attacks were carried out by adding a new malicious node to the network topology, as shown in Fig. 5 (nodes 24 and 25 are added to the reference topology).

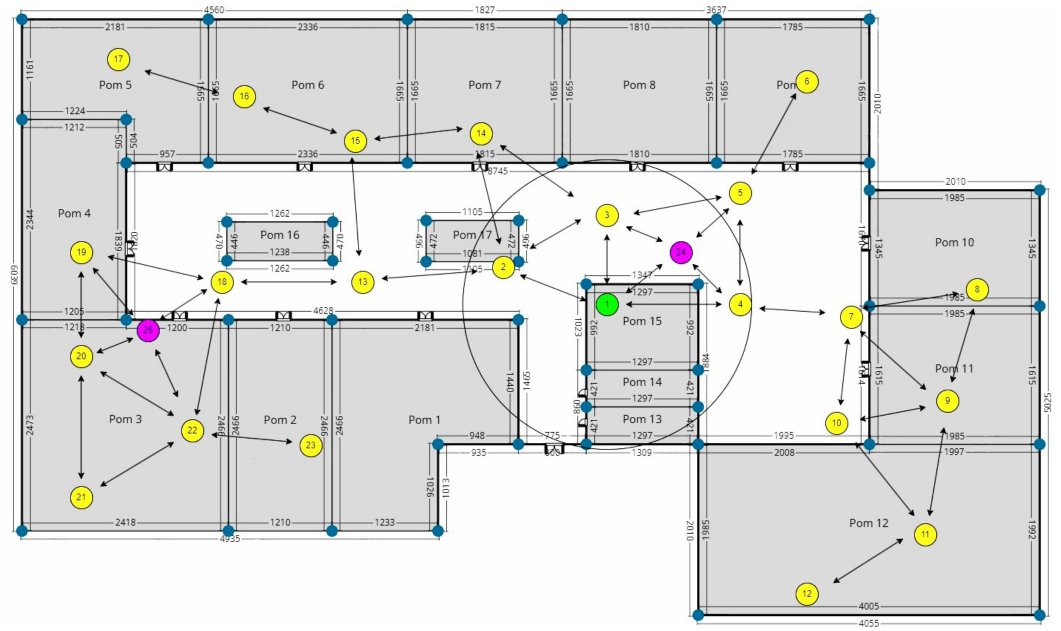

Fig. 5. Network topology for scenario ST2 (Source (Own))

Table 1 briefly describes the deployment of the attackers.

Table 1: Description of the scenarios to study the vulnerability of the network to topology attacks (Source (Own))

Scenario acronym	Scenario description
ST1-A	Node N3 was transformed into an intruder. Now we named it as an attacker with an acronym A3. This setup allowed us to study the impact of an attack on the network when the intruder was located in direct radio range of root node N1. Thus, sensor A3 had a communication range to sensors N2, N4, N5 and N14, making it an intermediate node in the potential delivery of packets sent by these sensors to the root.
ST1-B	Node N9 has been transformed into an intruder. Now we named it as an attacker with an acronym A9. This sensor represents a potential route for nodes N10 - N12. This configuration will make it possible, among other things, to analyze the vulnerability of the network with the RPL protocol to attacks involving rank modification and influence on the selection of the master node.
ST1-C	Sensors N5 and N15 have been replaced by attackers. Now, we named them as attackers with an acronym A5 and A15. In this configuration, A15 is the only communication path to root N1 for N16 and N17, and A5 is the only available route for node N6. Such changes force the transmitting sensors to direct their traffic exclusively through the attack nodes.
ST2-A	A malicious node A24 has been added to the network structure (Fig. 5), which is located in the direct radio range of the sink node. Furthermore, A24 is a potential intermediary in communication with N1 for nodes N7 - N12.
ST2-B	A malicious node A25 has been added to the network structure (Fig. 5), whose radio range includes sensors N19, N20, N21 and N22. In addition, it is part of a potential route for the sensors N21 and N23.
ST2-C	Two additional sensors, A24 and A25, were introduced into the network structure as intruders (Fig. 5). Sensor A24 provides an additional potential route for N6 to the main sensor. Sensor A25 connects sensors N17 and N19, which previously had no direct connection to each other.

Assumptions for attacks against resources

In order to study the vulnerability of the sensor network with the RPL protocol to attacks against resources, similarly to the assumptions for the attacks on the network topology, two scenarios were assumed. In the first scenario (SZ1), in the topology from Fig. 4, selected sensors were swapped to attackers. In scenario 2 (SZ2), several attackers were added to the existing network, as shown in Fig. 5. Table 2 shortly describes the deployment of the attackers.

Table 2: Description of the scenarios to study the vulnerability of the network to attacks against resources (Source (Own))

Scenario acronym	Scenario description		
SZ1-A	Node N9 has been transformed into an attacker. It is now named A9. This intruder has direct communication with sensors N7, N8, N10, and N11. The intruder is located within the radio range of four other sensors, which will allow analysis of the impact of attacks, especially those related to overloading the network by spreading DIS signaling packets.		
SZ1-B	Nodes N2 and S9 have been transformed into malicious nodes. Now they are named A2 and A9. N2 is in the direct radio range of the main sensor N1. This configuration will allow the effectiveness of the attack to be tested in the presence of two active intruders in the network.		
SZ2-A	A malicious sensor A24 has been introduced into the network structure (Fig. 5). It can communicate directly with sensors N3 - N5. Adding the sensor here allows to study the impact of selected attacks on network resources when the intruder is in direct radio range of the main sensor.		
SZ2-B	Another A25 attacker has been added to the SZ2-A network structure (Fig. 5), which has a radio range covering four other transmitting nodes, N18 – N20, and N22.		

Test results and discussion

Impact of the Blackhole attack on the RPL-based WSN

In order for a Blackhole attack to be effective, sensors must choose a default route through the intruder. Analyzing the obtained testing results of various attack scenarios, it can be seen that the Blackhole attack does not adversely affect the transmission of control messages as well as the power consumption of individual sensors. Depending on the location and number of intruders in the network, a different number of transmitting sensors are isolated. The attack is more effective when the attacking nodes are in the direct radio range of the primary sensor, as there is a greater chance that the default route will be routed through them. It is also worth noting that the full effectiveness of the attack is achieved when the intruder is the only possible route to forward packets. Fig. 6 shows the average power consumption of the sensors, depending on the scenario.

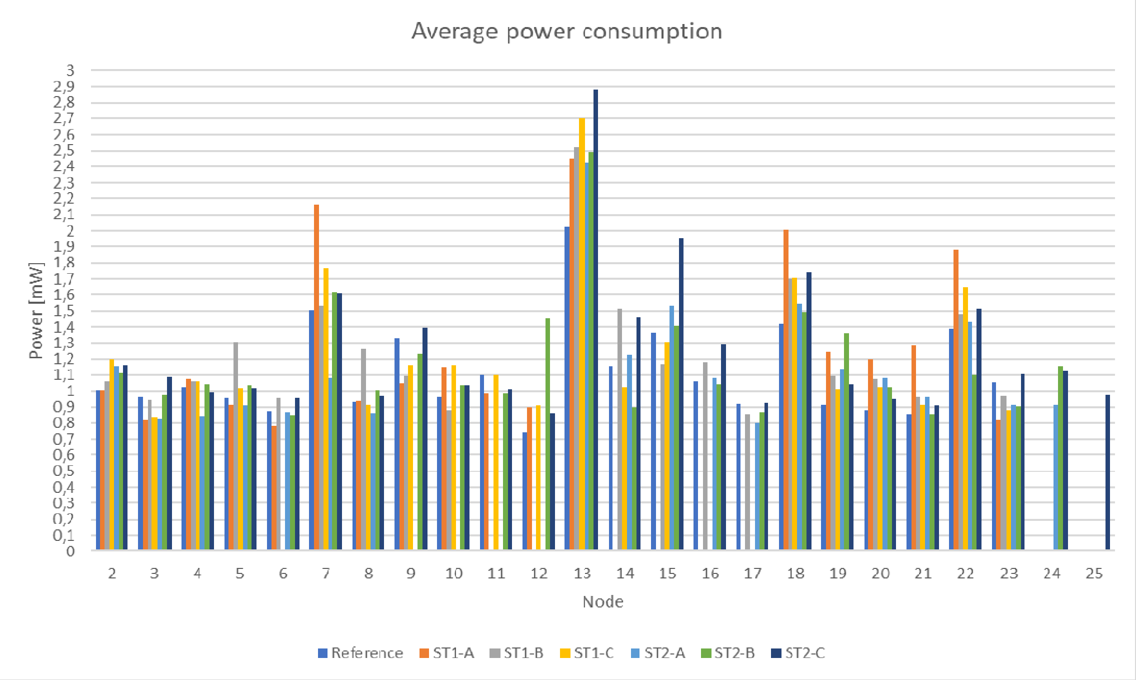

Fig. 6. Graph of average power consumption of sensors during the Blackhole attack (Source (Own))

Table 3 summarizes the data obtained when testing different scenarios for a Blackhole attack. The noticeable differences are due to the different number of nodes available in the network.

Table 3: Number of packets and control messages sent by nodes during Blackhole attack (Source (Own))

Scenario	Number of received packets	Number of DIS messages	Number of DIO messages	Number of DAO messages	Average time between packets [s]
Reference	197	24	264	176	52
ST1-A	163	22	294	212	54
ST1-B	174	23	264	178	55
ST1-C	170	22	267	177	48
ST2-A	171	24	275	168	55
ST2-B	206	25	278	185	55
ST2-C	214	24	299	207	54

As shown in Fig. 6, in each of the scenarios analyzed, the average power consumption of each node was very similar. Differences occur only due to the different number of sensors available in the network. If a node was isolated from the network structure, then information on its power consumption is not collected. The fewest packets (163) were received for the ST1-A scenario, in which the malicious node was within direct radio range of the root. A similar situation occurred for the ST2-A scenario. Despite the higher number of sensors, a comparable number of packets were lost. For the ST2-B and ST2-C scenarios, the number of packets did not decrease but actually increased, which means that the attack was not fully successful. To prevent a Blackhole attack in the assumed network topology, additional sensors would need to be added so that nodes (e.g., 5 and 17) have more routes to forward packets. In addition, as many sensors as possible should be within the root range.

An intruder performing a Blackhole attack focuses on blocking IPv6 packets by discarding those not addressed to it, thereby isolating selected nodes in the network. Due to the existence of routes in the routing table to all sensors in the network and the lack of information on the incoming packets, the RPL protocol does not reconfigure the network in search of alternative routes. To reduce the risk of this type of attack, it would be necessary to design the network structure so that nodes have more than one default gateway to choose from. Furthermore, increasing sensor saturation so that attacking nodes are not the only critical parts of the paths leading to the gateway minimizes the impact of such attacks. Another way to deal with Blackhole attacks in networks with the RPL protocol is to implement mechanisms in the network nodes to detect and mitigate intruders carrying out this attack. Examples of such mechanisms have been described by Sharma, D. K et al. (2022).

Impact of the Sinkhole attack

The Sinkhole attack focuses on blocking IPv6 packets and reducing the intruder's rank, and consequently changing the default routes of subordinate sensors. The attack is effective when the malicious node is within the radio range of other nodes. The location of the intruder affects the number of nodes affected by the attack. Comparing the ST2-B and ST2-C scenarios during the Blackhole and Sinkhole attack, it can be seen that the first attack in these network structures did not adversely affect the implementation of the complex functions of the RPL routing protocol-based network, since the intruders were not selected as master sensors by any of the slave sensors. However, in the case of the Sinkhole attack, by reducing the rank of the intruder, the slave sensors were forced to change their parent and were isolated from the network. Fig. 7 shows a graph of the average power consumption of individual nodes depending on the scenario.

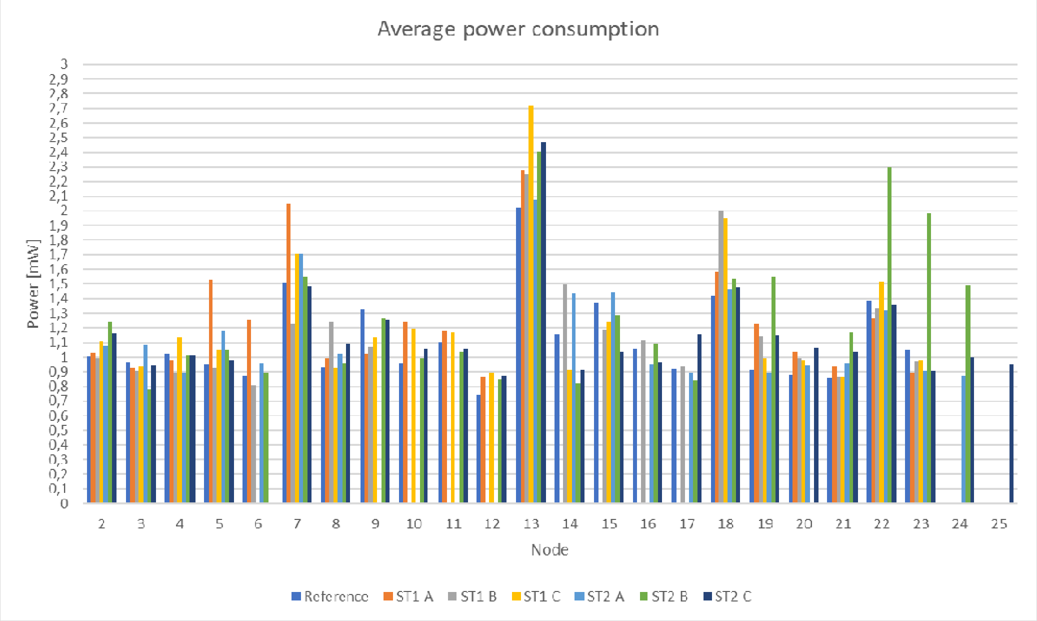

Fig. 7. Graph of average power consumption of sensors during the Sinkhole attack (Source (Own))

Table 4 summarizes the data obtained when testing different scenarios for a Sinkhole attack.

The noticeable differences are due to the different number of sensors available in the network.

Table 4: Number of packets and control messages sent by nodes during Sinkhole attack (Source (Own))

Scenario	Number of received packets	Number of DIS messages	Number of DIO messages	Number of DAO messages	Average time between packets [s]
Reference	197	24	264	176	52
ST1-A	148	22	267	174	52
ST1-B	164	22	269	169	53
ST1-C	171	22	274	172	54
ST2-A	147	24	275	185	53
ST2-B	166	25	275	190	53
ST2-C	197	24	295	191	54

This attack does not adversely affect the transmission of control messages, as well as the power consumption of individual sensors. The number of packets received for each scenario is less than during the tests of the reference network. The fewest packets were received in scenarios ST1-A and ST2-A, in which the malicious node was within direct radio range of the root. This means that most nodes were isolated. In other tests, fewer or more packets were lost. This shows that the Sinkhole attack was always successful. The only possible way to prevent this attack in the tested topology is to add a significant number of sensors to the network structure. Such a solution will reduce the risk that an intruder will announce a more attractive route to transmit data.

In the case of a Sinkhole attack, changing the position of the sensors will not affect protection against the attack. As mentioned above, the attack is effective whenever the malicious node is within the radio range of other sensors. Therefore, in order to reduce the risk of this type of attack, it would be necessary to block the ability of slave sensors to modify their rank. A comprehensive security framework based on detection and cryptographic methods to identify and isolate a malicious node was presented by M. Zaminkar and R. Fotohi (2020).

Impact of DIS Flooding attack

In RPL-based WSNs, each node that joins the network sends a DIS message first. Nodes, upon receiving this message, respond with a DIO message. The frequency of sending DIO messages is defined by the DIO timer. The high redundancy of DIS messages sent to a multicast address resets the timer of nodes within the direct radio range of the intruder, forcing more DIO messages to be sent.

The DIS Flooding attack causes the network to overflow with signaling messages. Analyzing the obtained simulation results of four different scenarios, we can see that this attack has an impact on power consumption, mainly by sensors that are in the direct radio range of the attacking node (e.g., nodes 7-11). In the case of attacking nodes, it can be seen that the dominant area in power consumption is transmission, while sensors in the direct radio range of the intruder manifested the highest consumption during listening. The values of average power consumption increased several times compared to the reference simulation, as shown in Fig. 8.

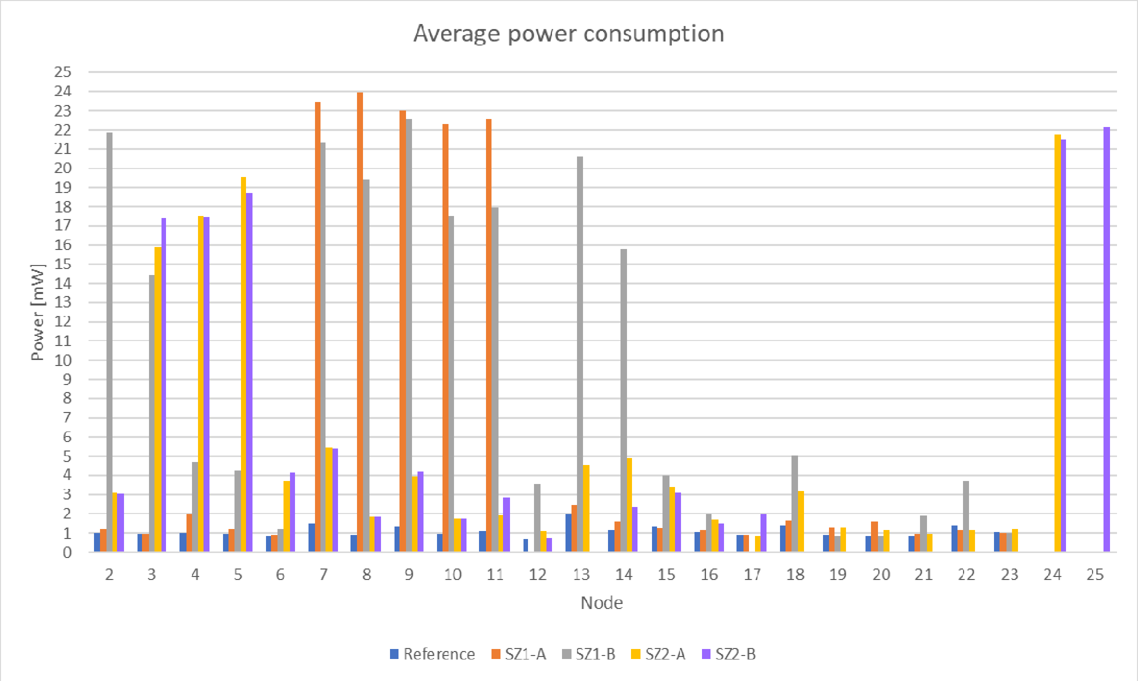

Fig. 8. Graph of average power consumption of sensors during the DIS Flooding attack (Source (Own))

The closer the intruder is to the root, the impact of the attack is noticeable over a larger area of the network. This can be observed by comparing the SZ1-A and SZ2-A scenarios. In the case of the second one, the attacking node was within range of the sink node, and the average power consumption also increased on sensors not within the intruder's radio range. For a DIS Flooding attack to be effective, the attacking sensor must be in the direct range of a node included in the network topology.

Table 5 summarizes the simulation results of various scenarios for a DIS Flooding attack. Due to the large number of control messages, a DIS Flooding attack can lead to the isolation of sensors from the network. It can be seen that fewer IPv6 packets were delivered to the root during the attack. In the SZ1-B and SZ2-B scenarios, where there were two malicious nodes, the number of packets delivered was the lowest. DIS control messages sent by the intruder cause the sensors to respond with DIO and DAO type messages. This causes even more network congestion. A comparison of the SZ1-A and SZ2-A scenarios shows that the farther the malicious node was from the root, the fewer DAO messages were sent. The attack was successful in each scenario.

Table 5: Number of packets and control messages sent by nodes during DIS Flooding attack (Source (Own))

Scenario	Number of received packets	Number of DIS messages	Number of DIO messages	Number of DAO messages	Average time between packets [s]
Reference	197	24	264	176	52
SZ1-A	177	12115	663	348	55
SZ1-B	89	22257	1185	650	72
SZ2-A	136	11206	658	648	67
SZ2-B	107	22227	964	529	71

topology would reduce the impact of the attack, as fewer nodes would be affected. With this solution, fewer DIO and DAO control messages would be transmitted.

No matter where the nodes are located in the network structure, a DIS Flooding attack will be effective. To reduce the effects of this attack, a conditional instruction could be added to the RPL protocol to prevent it from responding to DIS messages after receiving too many of them in a short period of time. Such a solution could reduce network congestion during the attack. An example of solutions built into the RPL protocol to minimize the knocks of a DIS Flooding attack is the Secure-RPL mechanism proposed by Verma, A. and Ranga, V. (2020). Their solution prevents legitimate nodes from performing unnecessary trickle timer resets and DIO transmissions. Another example is the solution presented by Abhinaya, E. V., and Sudhakar, B. (2021), which enables adaptive load balancing and route discovery mechanism to eliminate DIS flooding attacks.

Impact of Version Number attack

The Version Number attack causes a continuous incrementation of the DODAG version (DODAG Version Number), thus initiating a global repair operation. This parameter is sent in a control message of type DIO. The nodes, upon receiving a control message with a higher version number, start creating a new DODAG tree.

The consequence of this attack is an increase in the power consumption of all sensors in the network topology. The increase depends on the location of the node in the network; that is, if a given sensor is an intermediate point for a large number of slave sensors, its power consumption will be the highest due to the large number of messages being processed. In Fig. 9, comparing the SZ1-A scenario with the SZ1-B scenario, it can be observed that the more intruders in the network, the higher the power consumption.

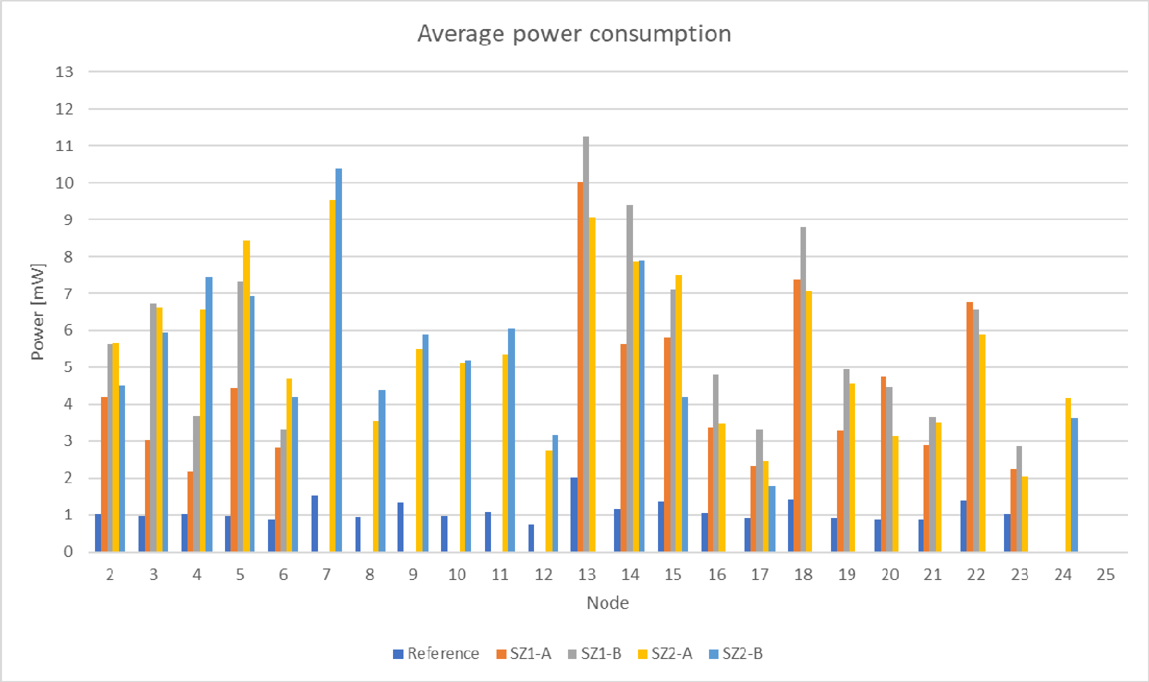

Fig. 9. Graph of average power consumption of sensors during the Version Number attack (Source (Own))

Table 6 summarizes the simulation results of various scenarios for the Version Number attack.

Table 6: Number of packets and control messages sent by nodes during Version Number attack (Source (Own))

Scenario	Number of received packets	Number of DIS messages	Number of DIO messages	Number of DAO messages	Average time between packets [s]
Reference	197	24	264	176	52
SZ1-A	105	22	1434	1047	55
SZ1-B	85	22	1544	1470	74
SZ2-A	98	23	1218	1400	62
SZ2-B	89	24	1890	1635	63

Analyzing the obtained data, it can be observed that this attack causes redundancy of DIO and DAO-type control messages due to the initiation of DODAG tree rebuilding. The number of these messages relative to the reference simulation increased several times. It is worth noting that the closer the intruder is to the root node, the higher the number of DAO messages is sent, while fewer DIO messages are generated, as can be observed by comparing the SZ1-A and SZ2-A scenarios. The existence of the attacker had no effect on the number of DIS packets sent. The large number of control messages in the network resulted in fewer IPv6 packets reaching the sink node. Comparing scenarios where there was a single intruder, it can be seen that the closer the attacking sensor is to the root node, the more packets are lost, and the time between packets increases. The number of control messages sent did not change significantly with the addition of a second intruder, as can be seen by comparing scenarios SZ1-A and SZ1-B, as well as SZ2-A and SZ2-B. This means that one malicious node is enough to carry out a successful attack.

The Version Number attack is effective regardless of the location of the intruder in the network. It affects the execution of complex functions by the RPL protocol whenever the attacker's sensor is in the direct range of a node included in the network topology. To prevent this attack, some security policy can be added to block the response of the entire network to a change in the version number of a slave node. Reconstruction of the DODAG tree would only be possible through the root node. One example of detection and isolation of the Version Number attack is the solution proposed by Almusaylim, Z.A. et al. (2020), where the attack detection is based on a comparison of the rank strategy. Version Number attack mitigation uses threshold and attack status tables, and isolation adds them to a blacklist table and warns nodes to skip them.

Conclusions

Performed tests of the location of sensors that carry out selected attacks show that the network topology and the location of the attackers have a significant impact on the performance of the entire network. As can be seen in the results presented in the test results and discussion section, intruders attacking locally can affect the network. However, with a limited number of intruders, the network as a whole is still capable of performing a significant part of its functions. Thus, it can be seen that network topology and the deployment of intruders are important in both the success of attacks and the effectiveness of network operations. The Blackhole attack focuses on blocking IPv6 packets. The attack is more effective when the attacking nodes are within direct radio range of the primary sensor, as there is a greater chance that the packets will be routed through them. It is also worth noting that the full effectiveness of the attack is achieved when the intruder is the only possible route to transmit packets. The Sinkhole attack is a combination of Blackhole and Rank Decrease attacks. Regardless of the setting of the attacker's sensor in the network structure, the attack is effective because of the changes made to the default routes, only the number of nodes attacked may change. DIS Flooding attack leads to continuous spreading of DIS messages by intruders. The effectiveness of the attack does not depend on the location of the attacker node in the network structure, however, the closer the intruder is to the gateway, the impact of the attack is noticeable over a larger area of the network. The Version Number attack of the sensor network is implemented by increasing the version number of the DODAG tree. The effectiveness of the attack does not depend on the location of the attacker node in the network structure, however, the closer the intruder was to the root, the higher was the number of DAO messages sent, while the lower was the number of DIO messages.

The research conducted indicates that it is difficult to create a network topology that would be completely resistant simultaneously to all the attacks described in the paper. By changing the location and number of sensors, we can only minimize the effects of attacks. When designing a WSN, it should be taken into account that sensors should have more than one default route to the gateway, and that as many of them as possible should be in direct radio range of the root. This will reduce the risk of a successful Blackhole or Sinkhole attack on the network topology. The DIS Flooding and Version Number attacks are the global attacks, that is, no matter where the malicious node is located in the network, the attack will be successful. To minimize the impact of this attack, the intruder should be prevented from communicating directly with a large number of nodes. The spatial dispersion of sensors will reduce the overhead of control messages during the attack, as fewer sensors will be affected.

References

- Abhinaya, E. V. and Sudhakar, B. (2021), ‘A secure routing protocol for low power and lossy networks based 6LoWPAN networks to mitigate DIS flooding attacks.’ Journal of Ambient Intelligence and Humanized Computing, 1-12.
- Albinali, H. and Azzedin, F. (2024), 'Towards RPL Attacks and Mitigation Taxonomy: Systematic Literature Review Approach,' IEEE Transactions on Network and Service Management, doi: 10.1109/TNSM.2024.3386468.
- Algahtani, F., Tryfonas, T. and Oikonomou, G. (2021), 'A Reference Implemenation for RPL Attacks Using Contiki-NG and COOJA' 2021

17th International Conference on Distributed Computing in Sensor Systems (DCOSS), doi: 10.1109/DCOSS52077.2021.00053, 14-16 July 2021, Pafos, Cyprus, 280-286.

- Almusaylim, Z. A., Jhanjhi, N. Z. and Alhumam, A. (2020), 'Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP,' Sensors, 20(21), 1-25.
- Al-Suhail, Ghaida, A., Mehdi, J. and Nikolakopoulos, G. (2017), 'A practical survey on wireless sensor network platforms,' Journal of Communications Technology, Electronics and Computer Science, 13, 23-30.
- Mayzaud, A., Badonnel, R. and Chrisment, I. (2016), 'A Taxonomy of Attacks in RPL-based Internet of Things,' Internation Journal of Network Security, 18(3), 459-473.
- Montenegro, G. et al. (2007), 'Transmission of IPv6 Packets over IEEE 802.15.4 Networks,' RFC 4944, September.
- Oikonomou, O. et al. (2022), 'The Contiki-NG open source operating system for next generation IoT devices,' SoftwareX, 18(101089), 1-8.
- Pongle, P. and Chavan, G. (2015), 'A survey: Attacks on RPL and 6LoWPAN in IoT' 2015 International conference on pervasive computing (ICPC), doi: 10.1109/PERVASIVE.2015.7087034, 08-10 January 2015, Pune, India, 1-6.
- Rajasekar, V. R. and Rajkumar, S. (2021), 'Analysis of Blackhole Attack in RPL-based 6LoWPAN Network: A Case Study' 2021 28th IEEE International Conference on Electronics, Circuits, and Systems (ICECS), doi: 10.1109/ICECS53924.2021.9665623, Dubai, United Arab Emirates, 28 November 2021 - 01 December 2021, 1-6.
- Sharma, D. K., Dhurandher, S. K., Kumaram, S., Gupta, K. D., and Sharma, P. K. (2022), Mitigation of black hole attacks in 6LoWPAN RPL-based Wireless sensor network for cyber physical systems. Computer Communications, 189, 182-192.
- Solapue, S. S., Kenchannavar, H. H. and Sarode, K. P. (2020), 'Issues Faced During RPL Protocol Analysis in Contiki-2.7,' In: ICT Systems and Sustainability. Springer, Singapore, 477-485.
- Tracey, D. (2020) A holistic architecture using peer to peer (P2P) protocols for the internet of things and wireless sensor networks, University College Cork.
- Verma, A., and Ranga, V. (2020), ‘Mitigation of DIS flooding attacks in RPL-based 6LoWPAN networks.’ Transactions on emerging telecommunications technologies, 31(2), e3802.
- Winter, T., Ed, (2012), 'RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks' RFC 6550, March.
- Zaminkar, M. and Fotohi, R. (2020), 'SoS-RPL: securing internet of things against sinkhole attack using RPL protocol-based node rating and ranking mechanism,' Wireless Personal Communications, 114(2), 1287-1312.