Chapter 3
Analysis of Blackhole Attack in RPL-Based 6LoWPAN Network Using Contiki-NG

Qais Al-Na'amneh
Applied Science Private University, Jordan

Asalla Al-Sheyab
Al-al-Bayt University, Jordan

Walid Dhifallah
https://orcid.org/0000-0003-1368-9612
University of Gabes, Tunisia

Rahaf Hazaymih
Jordan University of Science and Technology, Jordan

Mohammed Almaiah
https://orcid.org/0009-0008-9785-485X
University of Jordan, Jordan

Braa Qadoumi
https://orcid.org/0000-0002-4753-7820
Applied Science Private University, Jordan

ABSTRACT

The Internet of Things (IoT) has become one of the most significant topics in computer science study in the modern world. A standardized, ideal protocol for routing on the Internet of Things is the routing protocol for low-power and lossy networks (RPL). Connectivity, ubiquity, and low processing capability are the characteristics of devices that make up an Internet of Things network. An increase in IoT-based cyberattack occurrences has resulted from these features and their explosive growth in recent years. This chapter is to establish a reference application for conducting Blackhole attacks on the RPL protocol and improve network security, as well as to demonstrate how to create and test these attacks using COOJA and Contiki-NG.

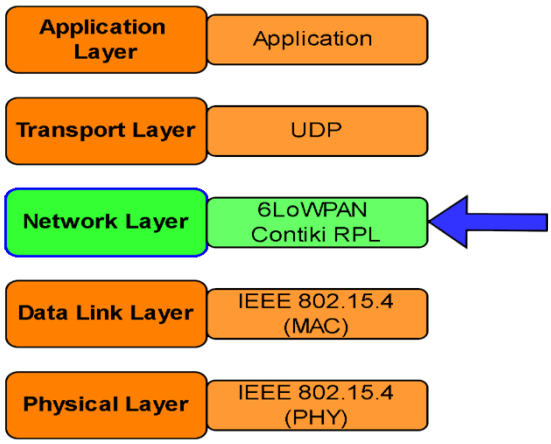
i. INTRODUCTION

The (RPL), a protocol used in wireless sensor networks and the Internet of Things, is the target of malicious operations known as RPL assaults. They may cause denial-of-service assaults, impede communication, and jeopardize data integrity. Blackhole, Sybil, wormhole, and selective forwarding attacks are examples of common RPL attacks (Algahtani, 2021). Network administrators should use secure

DOI: 10.4018/979-8-3693-7540-2.ch003

routing protocols, authenticate nodes, encrypt data transmission, monitor traffic, and carry out frequent security audits to prevent and minimize RPL attacks (Sharma, 2022).

Figure 1. The Contiki network architecture, emphasizing the attacked layer



The purpose of this chapter is to provide the results of specific attacks and to develop a framework for evaluating malicious nodes in Cooja environments. RPL Attacks, the framework, and experiments comprise the three sections that make up the document's structure. Using standards, the document shows the attacker as a red node labeled “A,” the root of DODAG as a green node, and normal nodes as yellow nodes labeled with a number.

Because of its effective routing capabilities, RPL, a routing protocol for low-power and lossy networks, is frequently utilized in Internet of Things applications (Wallgren, 2013). Nevertheless, network security may be jeopardized by assaults like version numbers, rank manipulation, and blackhole attacks. To investigate these assaults, researchers analyze network behavior, assess security measures, and create novel countermeasures using simulation tools like COOJA (W. Dhifallah,, 2021).

With an emphasis on wireless network attacks, the article describes how to implement RPL attacks using the Contiki-NG platform and COOJA software. It gives a summary of the COOJA and Contiki-NG platforms and emphasizes how crucial it is to comprehend the RPL protocol. The goal of the chapter is to increase wireless network security efficiency and provide a useful model for future research (W. Dhifallah, 2020).

With recent developments, embedded devices can now be connected to the internet for improved operation and data reporting. Sensor devices are actively utilized to monitor environmental and physical (Algahtani F. T., 2021).

A (WSN) is made up of inexpensive, tiny sensors. With the ability to perceive, process, and communicate data with other devices, sensor nodes have a distinct identity. WSN extend beyond the parts of simple sensors, such temperature sensors, to include the most intricate and crucial components of jet engines. Air conditioners and other smart home gadgets sense your body temperature to alter the temperature in the space. Devices that detect motion notify you of any questionable activities. WSN nodes use wireless media for communication, making them easier to install and less expensive. The processing,

computing, and battery life of sensor nodes are constrained. It is not possible to secure these devices with traditional cryptographic algorithms. Due of their limited resources and use of wireless technology, they are open to several attacks. Attacks from black holes are one of them. These nodes are easily compromised by hackers who can enter the network. Although a great deal of research has been conducted thus far, more effective work will be needed to shield sensor networks from these kinds of attacks. WSN is a less priced, self-organizing device network. By using actuators and sensors, these gadgets reduce the need for human involvement. WSN devices can be used for several different applications, such as in the military, in residences, or in the healthcare sector.

Sensors are actively used to track environmental and physical conditions, and new developments have made it possible to connect embedded sensors to the Internet for improved data reporting and operation (Azzedin, 2023). The IETF routing over (ROLL) group created the IPv6 RPL routing protocol. RPL has emerged as the main routing protocol for IoT because of the overlap between LPNs and IoT. Its single-destination, tree-like architecture is based on the Directed Acyclic Graph (DAG) design principle (Kumar, 2024).

A human, a health monitoring gadget, a smartphone, smart grid stations, driverless vehicles, smart watches, body detecting gadgets, and smart home appliances are all examples of things on the Internet of Things. To share information, these gadgets link wirelessly. WSN is made up of tiny devices that are placed in various locations that may be inaccessible to humans. We refer to these nodes as sensor nodes. Data can be gathered, processed, and transmitted to base stations by sensor nodes. These nodes translate environmental data into electrical signals, such as temperature, humidity, and air quality. While there are many uses for WSN, the military, control, tracking, housing industry, space, pollution observation, environmental / earth sensing, forest fire detection, and landslide detection, are among the most significant ones.

The smallest rank increase between a node and its DODAG parents is represented by the Min Hop Rank Increase value. This value is provided by the root and is used by all nodes to determine their rank. The DAG may be altered by a rogue node pretending to have a higher rank than its neighbors. Although it doesn't harm the network, this attack can be useful when paired with other building pieces. Only unaffected nodes send packets at first, while the attacker node and its neighbors use a lot of power (Shabani Baghani, 2022).

Every IoT smart device needs to be uniformly provided with resources like memory, connectivity, and energy to connect to other devices over the cloud-MANET network. Cloud-based IoT devices connected to nodes and IoT nodes within MANETs. Cloud-based data servers can operate very effectively to guarantee that current information is available for making decisions in real-time [6].

Because of their extremely limited memory, processing, and energy capabilities, IoT nodes participating in cloud-based MANET for agricultural field monitoring are much more vulnerable to availability attacks like Denial of Service (DoS) attacks. This makes the implementation of a cloud MANET field monitoring extremely important.

An image representing the taxonomy of network assaults shows which attacks are indicated by blue frames. When malicious nodes force legitimate nodes to do needless actions, they drain network resources. This is the first type. This may influence node incapacitation, network availability, and link congestion, which may shorten the lifespan of the network.

Figure 2. RPL network attack taxonomy

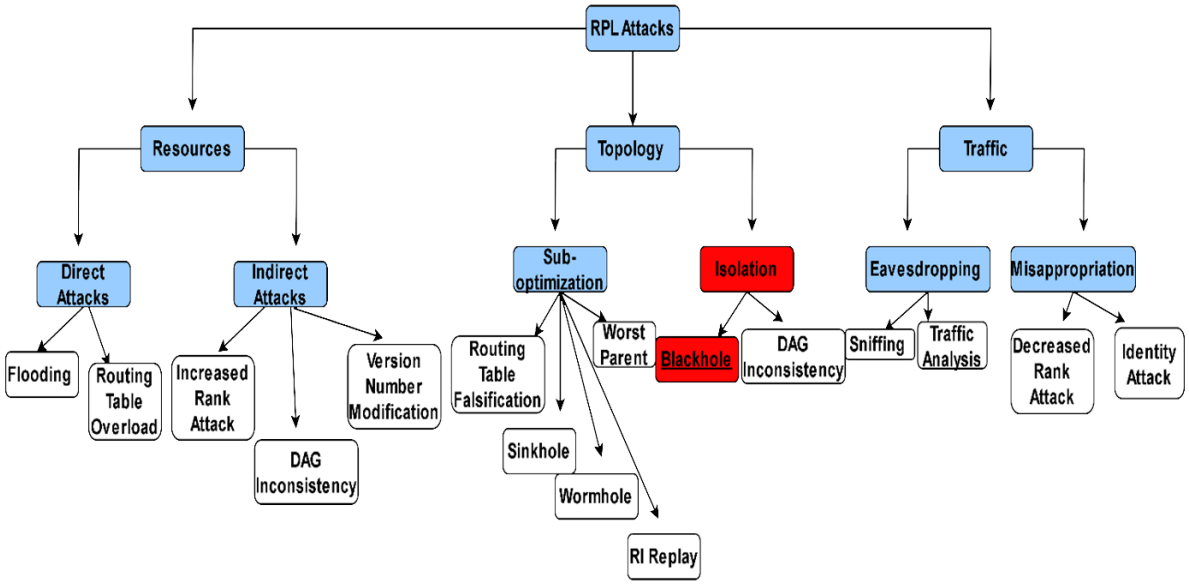
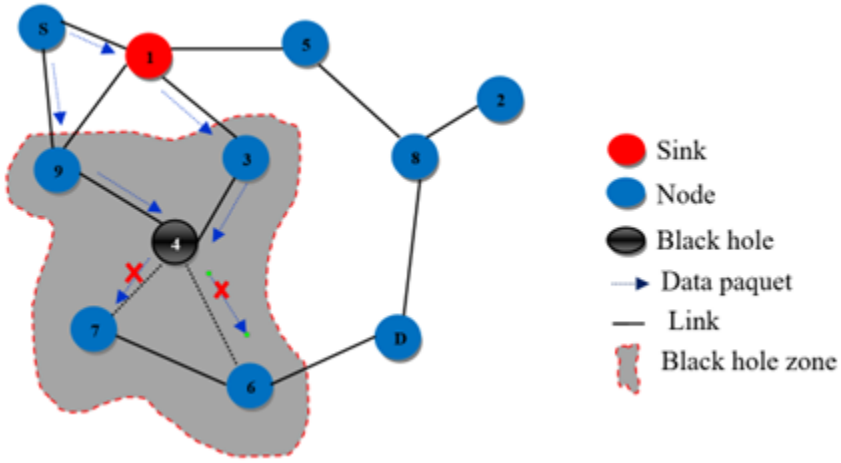


Figure 2 Attacks on the RPL network architecture fall into two categories: direct and indirect. Their goal is to cause node isolation and interfere with regular operations. Sub-optimization, which leads the network to converge to an unoptimal shape, and node isolation falls under this category. The third class consists of network traffic attacks, which try to insert rogue nodes into the network without interfering with its operation. Eavesdropping on traffic or pretending to be authentic nodes can result in information spillage. Both passive eavesdropping and the misuse of a node or group of nodes to alter properly sent data fall under this category.

Figure 3 shows Blackhole: attacks result in massive damage and denial-of-service (DoS) assaults when packets meant for malicious nodes are dropped. In the right place, they can isolate nodes. A version known as selective forwarding, or “gray hole,” makes it possible for malicious nodes to disrupt filtering protocols and routing paths by choosing packets to assault.

Figure 3. Data received from legal nodes is lost due to a blackhole attack



Mitigation: Make sure that the pathways between the source and destination nodes are distinct or use dynamic path selection to thwart deliberate forwarding attacks. Indicators for detection consist of DIO messages, delay, packet delivery ratio, and loss percentage. Analysis of traffic at the application level and encryption are beneficial. Make attackers cease all or none of their traffic. To guarantee the fundamental security of RPL, the IETF established several security measures throughout the protocol's creation.

For instance, loop detection and avoidance are among the local and global mending techniques that are natively integrated by the RPL protocol. Furthermore, two security functions are defined to offer extra choices for RPL message confidentiality, integrity, delay protection, and replay protection. These fundamental security and repair methods are far from sufficient. Numerous cryptography-based security measures are put forth without taking energy efficiency into account. Public key infrastructure (PKI), for instance, can safeguard communication between two endpoints. However, this technique will become extremely inefficient and energy-consuming when the number of devices in the network reaches a very high level. To protect data transmission, the writers in [encrypt messages using a hash function. On the other hand, using cryptographic technologies causes network packet sizes to grow and node resource consumption to accelerate. In addition, the encryption data, including the key, must be updated whenever a node switches networks.

We have used the widely known open-source Cooja and Contiki-NG to simulate the results. After the testing was completed, we used measures such as throughput, and average jitter sum delay about the total number of nodes in the network to assess the performance of the network. Additionally, we have assessed each node's goodput and throughput in the network both with and without wormhole and blackhole assaults. With a focus on the blackhole attack, we go over research on various approaches and existing defenses. Prospects in RPL security, as well as challenges and open research concerns, are also discussed. Additionally, studies on blackhole attacks and particular detection methods

Through this effort, we will gain a better understanding of the different species. The observed parameters and the study environment are explained in Section II. The results are tabulated in Section III. By linking the observations, Section Four explains the findings and assists in the conclusion-making

process. The results of the case study are concluded in Section V. Finally, Section VI attempts to guide how to further develop work to examine attacks more comprehensively.

ii. RELATED WORK

One of the key technologies behind the growing popularity of the (IoT) is the routing protocol for (RPL) networks. However, RPL is vulnerable to potential attacks that can compromise network security. Testing and experimentation on the reference implementation are necessary to understand these threats. Here are some studies about that.

In addition to its ability to offer efficient routing among IoT nodes with little resources and its flexibility in reacting to different (QoS) support and network architecture, RPL has gained favor in both business and academia. It was intended for RPL to be a straightforward—yet practical—organization that demonstrated control over Internet of Things networks, which include devices with limited resources. These tiny, interoperable devices are currently employed to do a wide range of tasks in a massive array of IoT application companies. On the other hand, because of their limited nature, RPL-based networks are susceptible to severe security flaws. The blackhole assault, which is thought to be among the deadliest and a point of entry for all other attacks, is the most dangerous attack in the deployment of IoT. RPL attacks, start when a rogue node surreptitiously drops every packet meant for transmission, resulting in enormous energy waste, congestion, and problems with network overhead. Additionally, RPL is helpless against blackhole attacks, which have the potential to cause a subnetwork in an LLN to become topologically separated. A malicious blackhole attack that is meant to be provocative drops packets from nodes in its subtree that it should be processing.

Distributed denial of service (DDoS) occurs when a blackhole attack is implemented by dispersing numerous nodes throughout a network. Attacks that are successfully hidden can make an attacked network behave remarkably similarly. to a functioning network and could obstruct data transfer and communication between connected devices. Enhanced delays in the bulk of packets being delivered to the sink, a decline in the packet delivery percentage overall, and (DODAG) information object (DIO) frequency increase

This study investigates four higher-level vulnerabilities to the (RPL): the Sinkhole, Blackhole, Version Number, and DIS Flooding Attack. It gives a taxonomy of RPL attacks based on traffic, topology, and resource availability and uses a Contiki/Cooja simulator to analyze their effects on RPL routing performance (Hussien, 2020).

Malicious activities like high packet loss rates, packet overhead, and resource depletion are carried out by blackhole attacks on IoT nodes. The rogue node's blackhole assault will cause changes in node ranks and an increase in network latency, which will impact the stability of the RPL network.

Moreover, the rank change results in a recalculation of the nodes' rankings. RPL's self-healing mechanism for breaking local routing loops is triggered by the rank change. The local repair becomes ineffective when blackhole attacks increase in frequency, necessitating the DODAG root to start the global repair. The RPL network became unstable because of the repair message's frequent changes. because of the dynamic nature of the protocol by keeping an eye out for attackers who might manipulate request packets. To do this, forged traffic is sent back together with information about the shortest path to the destination. Thus, a connection is established between the blackhole node and the source node. All packets on that path are typically under the control of the blackhole node. A DoS attack is caused by a child node's increased retransmission rate because of a blackhole assault.

The proliferation of the Internet of Things has spurred interest in multi-sink methods, especially in IPv6 RPL. Three techniques are compared in this study: multiple-DODAG, virtual root, and multiple-instance. It is found that the virtual root performs better with a higher loss (Goel, 2023).

The 6LoWPAN is an RPL-based network made up of embedded devices and sensors that gather data and send it to an IPv6 root via (6LoWPAN) border routers (6LBR) for processing and aggregation. Like other RPL-based networks, 6LoWPAN networks that employ the RPL protocol are susceptible to blackhole attacks, which can involve one or a small number of cooperating nodes and increase the difficulty of detecting the attack.

To protect the Routing Protocol for Low-Power Wireless Personal Area Networks (6LoWPAN) against Dropped Destination Advertisement Object (DDAO) attacks, a lightweight Challenge-Response Authentication-based approach is introduced in this study. The technique is critical to the expansion of the IoT industry because it effectively detects and counteracts DDAO assaults without adversely affecting resource-constrained nodes. It has been implemented on Contiki-NG and proven on the Cooja Simulator (Przybocki, 2023).

Cybercrime is on the rise worldwide, mostly targeting vital infrastructure such as power plants. Denial-of-service (DoS) attacks that leverage embedded devices put infrastructures and systems at serious risk. By simulating attacks on embedded systems, this chapter explores the effects of heavy loads. The Contiki OS and Power Tracker plugins were used in experiments with real and virtual wireless sensor networks. According to the results, there is a drop in power consumption with a bigger sensor network and peak power draining at a ratio of 13 to 1 for malicious nodes to sensor devices (KRARI, 2023).

The study offers a novel technique that makes use of deep learning models, particularly (LSTM) and (DNN), to identify RPL version number attacks in IoT. The study trains LSTM and DNN models to understand complex attack patterns by simulating the attack using the Cooja simulator. The goal of the research is to strengthen IoT network security since weak security might result in interruptions and data breaches (Mizher, 2021).

The Internet of Things (IoT) is vulnerable to security breaches because of resource constraints and lossy communications. For RPL-based IoT, researchers are creating intrusion detection systems, however, most of them overuse resources and disregard network constraints. To protect against RPL threats, this research attempts to develop an effective and efficient IDS using evolutionary computation techniques (Ahmad, 2024).

differentiated aspects of wireless sensor networks present distinct security concerns to the RPL network. Three primary components can be identified in common security assaults. The first kind of assault is called a resource attack, where the attacker usually tricks nodes into completing a lot of pointless tasks quickly. These procedures have the potential to drastically deplete nodes' scarce resources and reduce their operational lifespan. The purpose of a traffic attack, which is the second kind, is to alter network traffic. Attackers may, for instance, disseminate misleading information throughout the network, add to its overall burden, and listen in on node-to-node communications.

Network topology attacks are the third form of assault, where attackers primarily compromise the security and stability of the network by altering the

To detect numerous attacks (Jaradat, 2023), the article suggests DETONAR-Light, a DETONAR framework adaptation that uses data gathered at a border router. Because DETONAR is made to identify types of attacks, this method lowers the cost of hardware and maintenance without appreciably affecting the detection and classification rate of most attacks (Al-Na'amneh, 2024).

Wireless networks sharing readily available medium is without a doubt their biggest advantage, but it is also one of their biggest disadvantages. This strategy makes it easier for an attacker to launch an attack. Conventional denial-of-service attacks attempt to flood user core zone buffers. Nonetheless, an adversary could occasionally find it simpler to initiate an attack on wireless networks. Even with the extensive study attempts that have been recently published, identifying DoS attacks on the Internet of Things is still a major challenge. Machine learning has significantly improved information security and can identify a wide range of security threats, such as denial-of-service assaults. (Algahtani F. T.)

(Azzedin, 2023)presented a technique to identify DoS attacks in WSNs. Their goal is to use an RF classifier to identify four different types of assaults that are present in the WSN-DS dataset. Regarding classification accuracy, the suggested approach works better than the ANN detection model. Because of the features of IoT data, building a protocol that is effective in networks of IoT devices is one of the difficult jobs. Any modifications to the topology or the bandwidth restriction must be handled by the effective routing protocol. Many of the suggested protocols are merely mediocre.

(Sharma, 2022)suggested a pricing utility technique for data buying as well as online heuristics for public data supply in smart city settings. Their pricing process considers the limitations of the data provider's resources in terms of lifetime, capacity, and latency as well as the user's needs for quality and trust. The authors were unable to demonstrate network stability and convergence using this strategy.

iii. ADOPTED METHODOLOGY

With its scalability and energy efficiency, the RPL protocol is a popular routing protocol in Internet of Things networks. The goal of this chapter is to develop a reference application for carrying out attacks on this protocol. The chapter will give a general introduction to the RPL protocol, go over popular attacks, and show how to use COOJA and Contiki-NG (Al-Na'amneh Q. A., 2024). to create and test these assaults. Increasing the resistance of RPL-based networks to hostile actors is the aim.

The simulations for all scenarios were conducted using the Cooja network simulator, a flexible Java-based tool specifically designed for simulating networks of sensors operating on the Contiki operating system (Laila, 2024).

A blackhole attack is initiated when a deceitful node within the network deliberately discards all packets intended for the sink node. This nefarious act unfolds in two main phases. Initially, the malicious node lures neighboring nodes into designating it as the parent by falsely advertising a low rank, thus manipulating the network's topology, and disrupting the selection of optimal paths, resulting in a suboptimal network configuration. The second phase involves the malicious node dropping all packets originating from other nodes. There are two variants of the blackhole attack: the sinkhole attack and the selective forwarding attack. Both variants involve spoofing rank to entice neighboring nodes but differ in their approach to packet dropping. In the sinkhole attack, the malicious node reroutes traffic through itself without discarding any packets, potentially facilitating additional network traffic interception through a sniffing attack. Conversely, the selective forwarding attack permits some packets to reach the sink node according to predefined rules.

Figure 4 illustrates a scenario where 20 nodes have formed a DODAG (Destination-Oriented Directed Acyclic Graph) and are functioning normally. In contrast, Figure 5 depicts the same scenario under a blackhole attack initiated by node 9, disrupting the RPL routing path and coercing neighboring nodes to designate it as their parent.

The simulation runs for 25,000 seconds in each scenario, A clear network scenario serves as a reference, aiding in understanding the deviation of specific parameter values from other scenarios. The impact of malicious activity on the arrival delay of data packets at the receiving node was analyzed, as an increase in packet delay can indicate the presence of attacking nodes. Additionally, the delay of data packets originating from node 9 (the malicious node) is compared with those originating from its peer node in the explicit network scenario, helping to identify the impact of malicious behavior on the delay experienced by data packets from the malicious node itself, thus identifying the attacked node within the network. Scenario 2 (with attack) is compared to scenario 1 (without attack) in terms of the frequency of DIO messages to determine if malicious activity is affecting the exchange of these messages, which are crucial for path stability.

Figure 4. Sensor nodes w.r.t. sink node

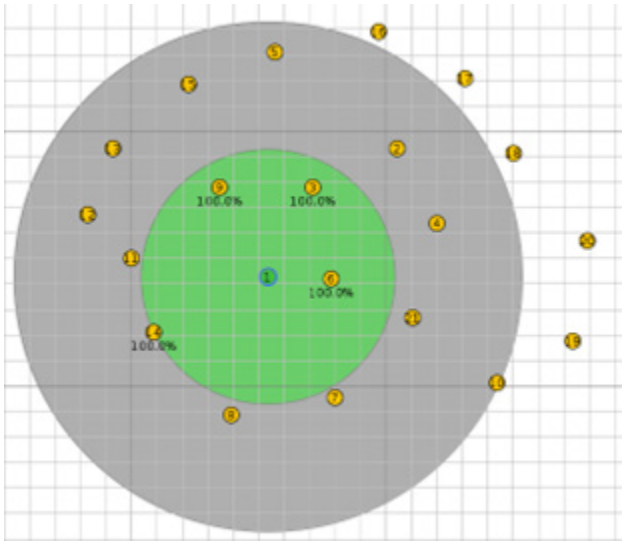
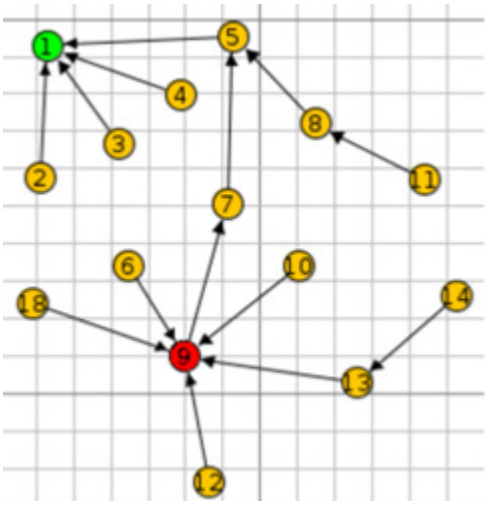
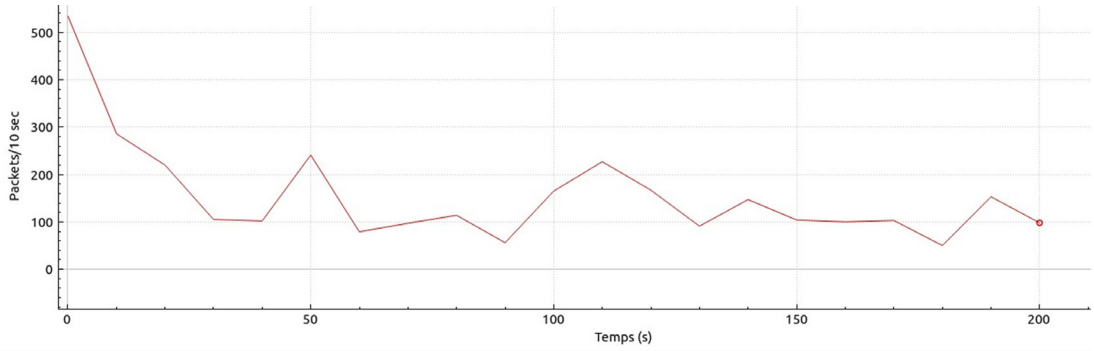


Figure 5. Blackhole attack



The data flow graph and packet transmission frequency in a typical network environment are displayed in Figure 6(a). The network flow is shown in Figure 6(b) for a traffic behavior scenario with assaults.

Figure 6. Flux normal (a) and attacks traffic (b)



(a)

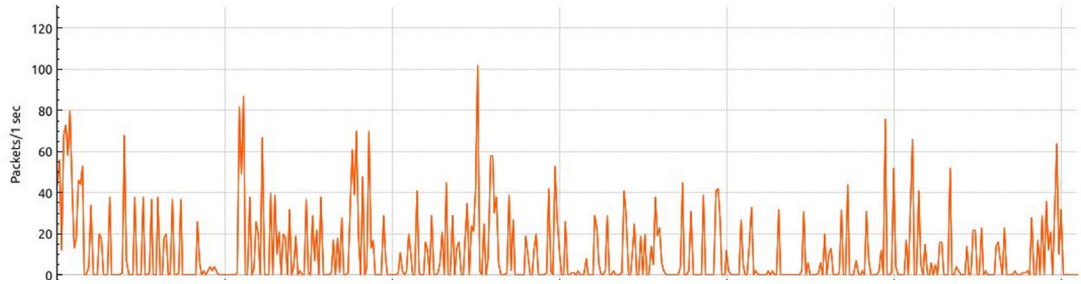
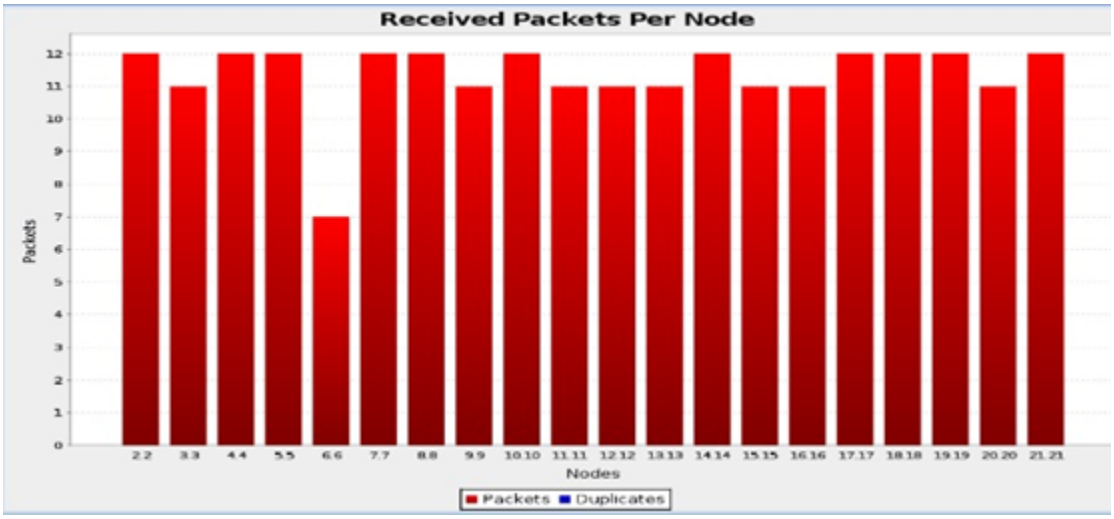


Figure 7. Received packets per node



iv. OBSERVATION

The recorded data includes the count and timestamp of DIO messages dispatched by each sender node. This information aids in calculating and evaluating the frequency of DIO messages. The summary of DIO message counts across scenarios is presented in Table 1. A rise in the number of exchanged DIO messages directly signals instability within the routing topology. Examining the number of DIO messages released per node allows us to determine whether individual nodes were aware of network instability and whether they endeavored to stabilize the network by transmitting their own DIO packets. The clear network scenario acts as a benchmark for comparison with the other scenarios, as depicted in Table 2. Node 9 is the malicious node in scenario 2. Nodes 12/13/18/6/10 are the affected nodes.

Table 1. Scenes with DIO packets released

Node	Scenario1	Scenario2
2	51	55
3	59	62
4	59	56
5	52	53
7	56	55
8	64	72
9/12/13/18/6/10	72	41
14	59	49
15	64	60

Table 2. Overview of the overall number of control messages sent in a scenario

Scenario No.	Scenario1	Scenario2
Total DIO Messages	536	503
% increase	Benchmark	-6,16%

Table 3 presents the packet delay experienced by Node 9 in Scenario 2, juxtaposed with the delay of data from a healthy node, specifically Node 5 in Scenario 1. It's important to note that the malicious node in Scenario 3 is excluded from the packet delay calculations, consistent with its status as a malicious entity.

Table 3. Average packet delay for nodes 5 and 9 in scenarios 1 and 2

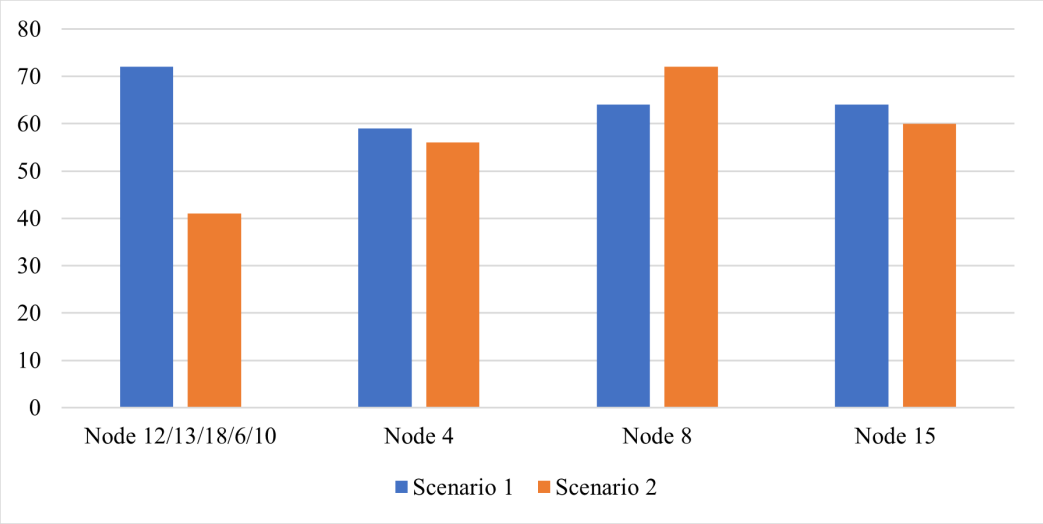
Scenario No.	Packets Sent.	Packets Rec.	Delay(ms)
Node 5 in Scenario 1	380	380	3042.21
Node 9 in Scenario 2	375	225	19542.75

v. RESULTS DISCUSSION

The Contiki RPL routing protocol exchanges a variety of control messages between sender and sink nodes to create a topology. Nodes exchange control information with one another to produce DIO. The hop count of these control packets from the sink is useful in identifying the node's own relative location to the sink node, and the (RTT) of these packets aids in estimating the distance from neighbors. DIO frequency drops after the topology are considered stable.

Upon analyzing the rate and frequency of DIO released by nodes across different scenarios, it becomes apparent that the introduction of malicious activity by node 9 in Scenario 2 led to an unstable network topology experienced by all nodes. Scenario 2 exhibited an overall escalation in the number of DIO messages. As depicted in Figure 4, data from Scenario 2 illustrated that all nodes released a higher number of DIO compared to the clear network scenario. However, the total count of DIO messages in Scenario 2 was lower than in Scenario 1. This suggests that despite node 9 in Scenario 2 dropping all data packets from its neighbors, there was no perceivable effect on the other nodes, leading them to believe the network was stable. Consequently, the rate of DIO closely resembled that of the clear network scenario. This observation is reinforced by Figure 5, indicating that Node 5 in Scenario 1 took significantly longer to release the same number of DIO as its counterpart malicious node in Scenario 2. Examining the DIO from Node 9 in Scenario 2, it selected the malicious node as its parent, releasing the first 50 DIO messages in a notably shorter timeframe compared to Scenario 1, as illustrated in Figure 8.

Figure 8. DIO message comparison for malicious/affected nodes



Another significant observation pertained to the selection of the preferred parent by Node 4. The parent selection is based on metrics derived from DIO. In Scenario 2, the malicious node successfully advertised itself as the preferred parent. This is elaborated upon in Table 4, which indicates that while Node 4 initially taken into consideration the benign node with ID: 6 as its preferred parent, it eventually reverted to the malicious node 13. Additionally, Node 13 exhibited superior route metrics compared to Nodes 5 and 9 in Scenarios 1 and 2, respectively. Figure 9 depicts nodes within direct range of Node 4 available for selection as the preferred parent, further confirming the efficacy of the malicious node in Scenario 2 in doing out damaging actions that go unnoticed.

Figure 9. Comparing the frequency of DIO messages sent by malicious and counterparties nodes

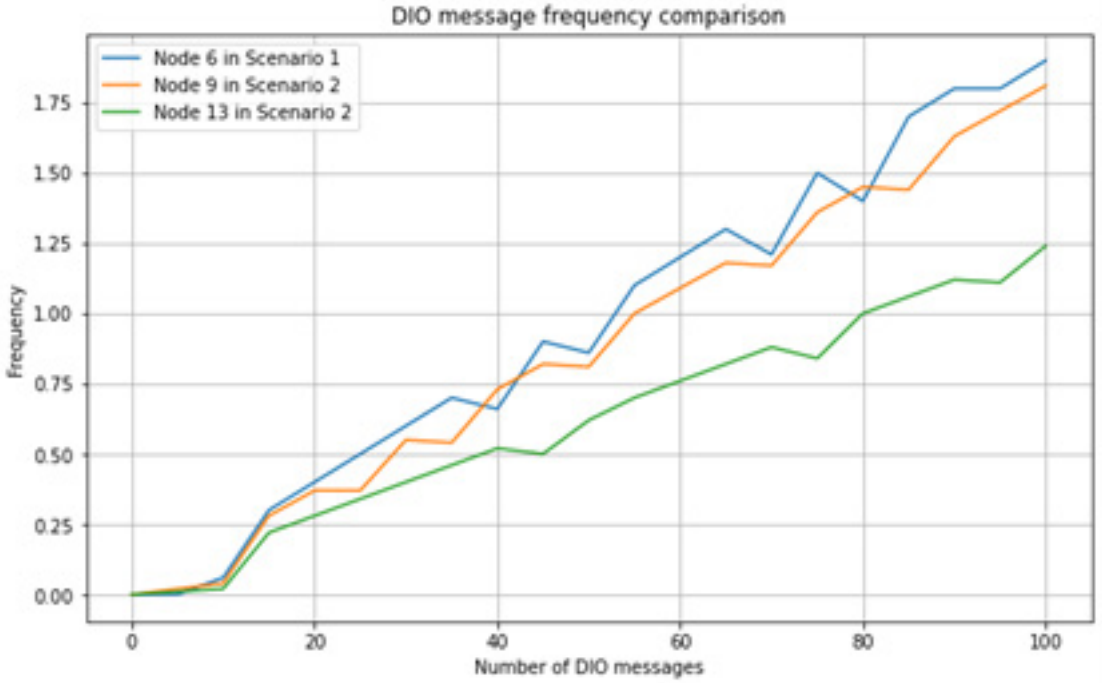


Figure 9: When it came to packet latency, the malicious node in Scenario 2 (Node 9)'s data packets suffered noticeably more delay than those from its counterpart node in Scenario 1. In Scenario 1, Node 9's packet latency was roughly 4.3 times greater than Node 5's. Data packets from rogue nodes alone were not the only source of increased packet latency. In Scenario 2, delays were greater for both benign packets that were close to and distant from the malicious node. In comparison to the previous cases, all nodes in Scenario 2 had significantly greater delays. Buffer-dense queues, in which packets are delayed processing while the sink node creates and processes DIO packets to stabilize the network topology, could be the fundamental cause of packet delay. Based on the (TTL), extended waiting periods may cause packet expiration. Additionally, the sink node did not release any data packets, and the malicious node in Scenario 2 suppressed the forwarding of any self-generated data packets. In every case, the total number of packets received at the sink node was counted. Long wait times in the buffer queue, packet loss from the malicious node dropping packets, or even success in the simulation if it had been permitted might all cause packet loss.

vi. CONCLUSIONS

When it comes to DoS attacks on IOT availability, blackhole and wormhole attacks are well-known and extremely destructive. When monitoring field-enabled Internet of Things networks, real-time data availability is essential. Data centers offer the best computing capacity in an emergency, and IoT nodes are outfitted with the (LLN) topology for routing protocol standard (RPL). The RPL's hardware resources

are inadequate and its current security measures are insufficient to fend off multiple security breaches. For the protection of both Internet and MANET routing protocols, gateway routers connected to Internet of Things devices in MANETs need to be reliable and consistent.

According to a chapter, network performance and reliability in RPL-based 6LoWPAN networks can be greatly impacted by a reduced rank attack. The attack can result in routing loops, more energy usage, and a lower packet delivery ratio since it maliciously lowers node rank. By simulating the attack with Contiki-NG and COOJA, researchers discovered that it causes network topology disruption, deteriorates latency and packet delivery ratio, and increases node energy consumption, which may result in premature battery depletion.

vii. LIMITATIONS AND FUTURE WORK

There are some drawbacks to the standard implementation of RPL attacks utilizing Contiki-NG and cooja, such as its narrow scope, inaccurate real-world applicability, inaccurate performance impact measurement, and inability to scale in big networks. Future research should concentrate on creating sophisticated attack methods, looking into fresh attack avenues, and examining RPL weaknesses. Additionally, to lessen RPL attacks and improve network security, researchers should create complex protection systems. Subsequent research must encompass practical trials and assessments of scalability.

References

Ahmad, S. S., Almasalha, F., Qutqut, M. H., & Hijjawi, M. (2024). Centralized smart energy monitoring system for legacy home appliances. *Energy Informatics*, 7(1), 29. DOI: 10.1186/s42162-024-00334-2

Al-Na'amneh, Q., Almomani, A., Nasayreh, A., Nahar, K. M., Gharaibeh, H., Al Mamlook, R. E., & Alauthman, M. (2024, February). Next Generation Image Watermarking via Combined DWT-SVD Technique. In 2024 2nd International Conference on Cyber Resilience (ICCR) (pp. 1-10). IEEE. DOI: 10.1109/ICCR61006.2024.10532782

Al-Na'amneh, Q., Nasayreh, A. N., Al Mamlook, R., Gharaibeh, H., Alsheyab, A. M., & Almaiah, M. (2024). Improving Memory Malware Detection in Machine Learning with Random Forest-Based Feature Selection. In Almaiah, M., Maleh, Y., & Alkhassawneh, A. (Eds.), *Risk Assessment and Countermeasures for Cybersecurity* (pp. 96–114). IGI Global., DOI: 10.4018/979-8-3693-2691-6.ch006

Algahtani, F., Tryfonas, T., & Oikonomou, G. (2021, July). A Reference Implemenation for RPL Attacks Using Contiki-NG and COOJA. In 2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS) (pp. 280-286). IEEE. DOI: 10.1109/DCOSS52077.2021.00053

Algahtani, F., Tryfonas, T., & Oikonomou, G. (2021, July). A Reference Implemenation for RPL Attacks Using Contiki-NG and COOJA. In 2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS) (pp. 280-286). IEEE. DOI: 10.1109/DCOSS52077.2021.00053

Azzedin, F. (2023). Mitigating Denial of Service Attacks in RPL-Based IoT Environments: Trust-Based Approach. *IEEE Access : Practical Innovations, Open Solutions*, 11, 129077–129089. DOI: 10.1109/ACCESS.2023.3331030

Dhifallah, W., Tarhouni, M., Moulahi, T., & Zidi, S. (2021, October). A novel realistic dataset for intrusion detection in IoT based on machine learning. In *2021 International Symposium on Networks, Computers and Communications (ISNCC)* (pp. 1-6). IEEE.

Goel, S., Verma, A., & Jain, V. K. (2023). CRA-RPL: A Novel Lightweight challenge-Response authentication-based technique for securing RPL against dropped DAO attacks. *Computers & Security*, 132, 103346. DOI: 10.1016/j.cose.2023.103346

Hussien, Z. W., Qawasmeh, D. S., & Shurman, M. (2020, December). MSCLP: Multi-sinks cluster-based location privacy protection scheme in WSNs for IoT. In 2020 32nd International Conference on Microelectronics (ICM) (pp. 1-4). IEEE.

Jaradat, A. S., Nasayreh, A., Al-Na'amneh, Q., Gharaibeh, H., & Al Mamlook, R. E. (2023, November). Genetic Optimization Techniques for Enhancing Web Attacks Classification in Machine Learning. In 2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) (pp. 0130-0136). IEEE.

KRARI, A., HAJAMI, A., & JARMOUNI, E. (2023). Detecting the RPL Version Number Attack in IoT Networks using Deep Learning Models. *International Journal of Advanced Computer Science and Applications*, 14(10).

Kumar, D., Sinha, N., Mishra, A. K., & Tripathy, A. K. (2024, January). An Experimental Comparison and Impact Analysis of Various RPL-Based IoT Security Threats Using Contiki Simulator. In 2024 16th International Conference on COMmunication Systems & NETworkS (COMSNETS) (pp. 111-116). IEEE.

Laila, D. A., Al-Na'amneh, Q., Aljaidi, M., Nasayreh, A. N., Gharaibeh, H., Al Mamlook, R., & Alshammari, M. (2024). Simulation of Routing Protocols for Jamming Attacks in Mobile Ad-Hoc Network. In *Risk Assessment and Countermeasures for Cybersecurity* (pp. 235–252). IGI Global. DOI: 10.4018/979-8-3693-2691-6.ch013

Mizher, M. A., Mazhar, A. A., & Mizher, M. A. A. (2021, October). A review of Mobile Cloud Computing in Education during the Covid-19 Pandemic in Jordan. In *Proceedings of the 2021 International Conference on Computer, Control, Informatics and Its Applications* (pp. 187-193). DOI: 10.1145/3489088.3489101

Przybocki, P., & Vassilakis, V. G. (2023). An analysis into physical and virtual power draw characteristics of embedded wireless sensor network devices under dos and rpl-based attacks. *Sensors (Basel)*, 23(5), 2605. DOI: 10.3390/s23052605 PMID: 36904809

Shabani Baghani, A. (2022). Improving Security and Performance of the RPL Routing Protocol for Low Power and Lossy Networks.

Sharma, D. K., Dhurandher, S. K., Kumaram, S., Gupta, K. D., & 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. DOI: 10.1016/j.comcom.2022.04.003

Verma, A., & Ranga, V. (2020). Mitigation of DIS flooding attacks in RPL-based 6LoWPAN networks. *Transactions on Emerging Telecommunications Technologies*, 31(2), e3802. DOI: 10.1002/ett.3802

Wallgren, L., Raza, S., & Voigt, T. (2013). Routing attacks and countermeasures in the RPL-based internet of things. *International Journal of Distributed Sensor Networks*, 9(8), 794326. DOI: 10.1155/2013/794326