PERFORMANCE TESTING OF ROUTING PROTOCOL FOR LOW POWER AND LOSSY NETWORKS (RPL) AGAINST ATTACK USING COOJA SIMULATOR

Yusuf Trihartono Tonapa[1], Ida Wahidah[2], Nyoman Bogi Aditya Karna[3]

[1,2,3] Telecommunication Engineering Department, School of Electrical Engineering, Telkom University
[1]yusuftrihartono@student.telkomuniversity.ac.id, [2]wahidah@telkomuniveristy.co.id,
[3]aditya@telkomuniversity.ac.id

Abstract

The Wireless Sensor Network (WSN) consists of various devices with limited resources and is capable of detecting and tracking a certain space to gather data and transmit it to the root node by utilizing a routing protocol. To acquire and transfer data, these budget-friendly wireless devices are often deployed in a hostile, empty, and wide-open area, rendering them especially vulnerable to attack. Routing protocol for low power and lossy networks (RPL)-based low power and lossy networks (LLNs) largely determine the lifetime and quality of the network and the devices itself.

This research attempts to examine the RPL and exploring various types of cyberattacks against RPL, including Hello Flood, Version Number Modification Attack, and Blackhole. Based on this premise, the ultimate objective of this study is to implement these attacks against RPL and to holistically simulate them using the Cooja Simulator. Eventually, as data was collected through a simulation, the data was therefore processed and analyzed using relevant parameters such as Network's Lifetime, Packet Delivery Ratio, End-to-End Delay, and Routing Overhead.

The performance test results obtained for a normal WSN with RPL are E2E Delay around 150-300 ms, PDR = 100%, Routing Overhead = 60%, and an Estimated Network's Lifetime around 1.5 years. The following are the impact of each attack scenario caused. First, Network's Lifetime reduced by 20 times (Hello Flood Attack), and 4 times (VNM Attack). For PDR, there is a decrease of 20% (Hello Flood Attack), 70% decrease (VNM Attack), and 60% decrease (Blackhole). E2E Delay increased by 15 times (Hello Flood Attack), and 10 times (VNM Attack). Lastly, Routing Overhead had an increase of 30% (Hello Flood Attack), and 35% (VNM Attack).

Keywords: Wireless Sensor Network (WSN), Routing protocol for low power and lossy networks (RPL), Cooja Simulator.

1. Background

The extensive presence of various things and objects connected to the Internet embodies the idea of IoT. IoT enables multiple sensors and devices (nodes) to be combined and communicate seamlessly with each other to share decisions and information. As the main component of the fast-emerging IoT, low power and lossy networks (LLN) play a critical role in reaching ever-present and widespread computation. However, due to wireless media, resource limitations, and a lack of physical safety, LLN is susceptible to all kinds of attacks. When sensitive data being sent, developing countermeasures against potential attacks is extremely important and challenging for reliable and secure communication.

Nodes have limited resources, and routing is a solution that is often needed to send packets between nodes along the most efficient path from source to destination and vice versa [1]. Also, the algorithm is known to use up most of the resources in CPU and memory, and it significantly affects the performance of limited resource devices used in LLN applications, where RPL is used [2]. RPL is well known as an effective Routing protocol for LLN due to its low power consumption for routing in networks with a significant amount of nodes.

This thesis is intended to simulate the RPL facing several kinds of attack scenario, which is Blackhole attack, Hello Flood attack, and Version Number Modification (VNM) attack in Cooja Simulator. By using these scenarios, the author intended to measure the impact they caused. In this thesis, one node is selected as an attacker in each different attack scenarios for this simulation and compared to a similar network running normally without a malicious node. An understanding of impact and behavior is required when measuring network performance. In addition, the Cooja simulator is a network simulator that is widely known because of its high accuracy compared to the real implementation, so it is used by the author. By extending Cooja's features, Cooja could measure and measure these disturbances more accurately and efficiently.

2. Literature Review

2.1 Wireless Sensor Network

A WSN is a network without infrastructure consisting of up to thousands of sensor nodes. These nodes collaboratively perceive and manage the specified environment to allow their interaction with the user or device.

The data would be collected by the sensor node, compressed, and then sent to the gateway. In a gateway connection, the data is afterwards forwarded by the base station to the server.

These are some features that cause a WSN considered as less secure to attacks compared to the wired one:

a. Self-organization

The sensor network has no fixed structure, and the sensor node positions are placed randomly. All kinds of failures in the network must be neutralized via a self-regulatory mechanism to allow the node to find other nearby nodes and re-establish communications.

b. Self-adaptive flow control

In accordance with the amount of transmission failures and the quality of the link, the transmission flow is modified to compensate for the deterioration of network performance in unreliable transmission states.

c. Resource restrictions

The limitation processing, storage and communication capacities could enable the use of light security mechanisms, which could fend off the majority of external attacks. However, it cannot protect itself from internal attacks.

d. Centralized control

The routing algorithm is applied per the protocol of sensor nodes to control them centrally and control the data flow between nodes.

e. Open environment

WSN is deployed in an easily reachable environment, which makes the likelihood of enemy seizing control of nodes higher. In addition, many internal attacks can be triggered by malicious nodes, and the enemy can take complete control of the network.

2.2 RPL

RPL or Routing Protocol for Low power and lossy network is an infrastructure protocol. It is an IPv6 routing protocol based on distance vectors. It targets data aggregation networks consisting of up to thousands of nodes, most of which have minimal and constrained resources.

RPL uses Destination Oriented Directed Acyclic Graphs (DODAG) topology to maintain the state and information in the network. DODAG is composed of DODAG ID, DODAG Version Number, and RPLInstanceID. Every instance of DODAG has its own Root or Sink node. To build and maintain the topology of its network RPL depend on four different routing control messages: DODAG Information Object, DODAG Information Solicitation, Destination Advertisement Object, and Destination Advertisement Object Acknowledgement.

a. Auto-configuration

RPL is a routing protocol based on IPv6; it means the network could be configured automatically without the user's intervention.

b. Self-healing

RPL could automatically detect and repair failures that occur in the network to a normal working state.

c. Loop avoidance and detection

There is a rule in RPL that dictates a child node could not choose a parent node with a Rank value higher than itself.

d. Multiple Edge Routers

It is possible to build more than one DODAGs in a single RPL network that has its own Sink node. A particular node may be included in multiple RPL instances and act in different roles in each. For that reason, excellent availability in the RPL network is guaranteed.

2.3 Type of Attack on RPL

2.3.1 Resources Category Attack

This type of attack is intended to cause legitimate nodes to waste their energy, processing, or memory resources to interfere with network availability. There are two main categories of attacks on resources. First, the attacker uses nodes to generate traffic overhead to disrupt the network directly, and it will be referred to as a direct attack. Secondly, the attacker uses other nodes to cause excess burden to the network; this is an indirect attack. The most significant ones are determined as follows:

a. Hello Flood

By generating excess discovery packet (DIS in this case) in a network to make the nodes unavailable and unstable. It could be executed internally or externally. It is also could be considered as an attack against topology [10].

b. Rooting Table Overload

The attacker makes use of a node operating in storage mode by issuing a fake route in the DIO message to the target node. It will disrupt normal network operations, populate the routing table, and prevent the attempt to create new routes.

c. Increased Rank Attack

By intentionally change the Rank of the tampered node with the same value as its child node, it causes routing loops to occur.

d. Version Number Modification

The attacks aim to increase the version number value contained in the DIO message and then send it to its neighbors. Because of that, the DODAG had to be rebuilt from scratch, and the consequences are network congestion, massive loss of data packets, and resource wastage due to the high amount of routing control messages being sent [8].

2.3.2 Against Topology

This attack is intended to produce topology distortion in the targeted network. This attack could also be categorized into two types based on the consequences. Hence, a sub-optimization attack refers to an attack that prevents optimal network convergence, and an isolation attack refers to an attack that tries to isolate a node or a group of nodes from DODAG. The most significant ones are determined as follows:

a. Routing Table Falsification

The malicious node will modify the DAO control message with a fake route to create confusion in the network. As a result, the affected nodes would get the wrong routing information from the routing table, lead to increasing delays and congested network.

b. Sinkhole

This attack attracts traffic as many as it could through false informational advertisements to direct traffic through it. Thus, network performance will be affected. Furthermore, this attack would become more destructive if it is combined with other attacks (Blackhole or Selective Forwarding) [6].

c. Blackhole

In this attack, the attacker attracting traffic as much as it can get but to isolate nodes from the topology and drop the packets through its node. A blackhole attack could be considered a DoS attack.

d. Routing Information Reply

This attack comprises sending packets but intentionally repeating and delaying the packets.

e. Wormhole

This attack intentionally creates a connection between 2 nodes that has significant distances that normally would not happen. It causes a disturbance in the creation of the optimum paths and routes.

2.3.3 Against Traffic

This attack aims to seize control of all the ongoing information transmission. This attack could also be categorized into two types based on its final objectives. First, for collecting all the traffic in the network, and the second one is intended to acquire valuable details regarding the topology and the targeted network.

a. Sniffing

This attack consists of eavesdropping the packets sent by nodes over the network that compromise the secrecy that happens during transmission.

b. Traffic Analysis

Traffic Analysis Attack could be used in conjunction with a sniffing attack. Valuable information such as the relationship between node can be extracted by analyzing the routing information even if it is already encrypted. This particular attack objective is to gather sufficient information to carry out another type of attack.

c. Decreased Rank Attack

Nearer nodes tend to appear more desirable compared to those located at greater distances. Malicious nodes could falsely be issued a lower Rank value via fake DIO packets to draw more traffic to carry out attacks such as Blackhole, sinkholes, and eavesdropping.

d. Identity Attack

The malicious node would disguise itself to be a normal node on the network. If it is used simultaneously with Sniffing attack, the attacker would be able to identify nodes of interest in order to fake their addresses and impersonate legitimate nodes. An identity attack carried out on a DODAG root would lead to the attacker taking over the entire network.

3. System Design and Experimental Setup

This subsection discusses the setup for the experiment conducted to analyze the performance of RPL against attack.

As Figure 3.2 has shown, it begins with designing each attack scenario used in this performance test by using a Network simulation tool, Cooja Simulator. After each scenario is successfully compiled, each one of them is going to execute one by one until the data on the desired parameters are obtained. By gathering each of the acquired data from the simulation, then the result, which consists of a comparison between each scenario, could be obtained. Lastly, analysis and discussion of these results would be conducted by different approaches.

Figure 3.1 The procedure of simulation implementation and data collection in this study

The construction process of RPL DODAG is shown in Figure 3.2:

a. To create a DODAG and build a route redirected from another node to the Sink node. The sink node needs to send DIO packets that consist of the DODAG root ID, Rank, and Objective Functions describing routing metrics.
b. Each node that receives a DIO and wishes to join DODAG must add DIO sender to its parent list. The node's Rank would be calculated corresponding to the obtained OF. Rank is a numeric value that provides a scale of the node locations in comparison to its Sink node.
c. DIO could also be used by the node that already joined the DODAG to probe the surrounding area of any new nodes and invite them to DODAG. In case of a node wish to become a part of the network and never received an invitation through DIO, it could send a DIS broadcast to request a DIO.
d. Nodes need to send DAO packet to spread reverse-route information and register nodes the DAO travelled along the upward route. Afterwards, the DAO packet succeeded to reach the Sink node, a complete path between the data collection node and the Sink node is created.

.

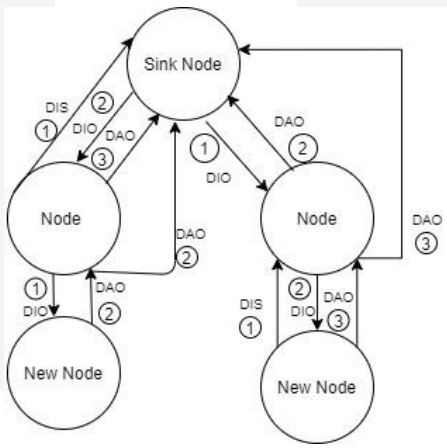

Figure 3.2 Construction process of RPL DODAG between child and parent nodes

3.2 Evaluation Parameters

a. Packet Delivery Ratio

Packet Delivery Ratio or PDR is the ratio of data packets amount that has reached the Sink node and the total amount of data packets that data collection nodes generated. Also, as the PDR value increases, the network performance will increases.

$$PDR = \frac{\sum Packet\ Received}{\sum Packet\ Sent} . 100\% \quad (3.1)$$

b. Routing Overhead

Routing packet overhead is the ratio of routing control-related data total size, and the overall size of the

transmitted packet in the whole network. According to [11], RPL has higher Routing Overhead than other routing protocols.

$$Routing\ Overhead\ = \frac{\sum Routing\ Packets\ Size}{\sum Routing\ Packets\ Size + \sum Data\ Packets\ Size} \times 100\% \quad (3.2)$$

c. End to End Delay

End to End Delay is the amount of time needed for a packet to travel from the data collection node to Sink node. Naturally, E2E Delay comprises of Processing, Propagation, Queuing, and Transmission Delay.

d. Estimated Network's Lifetime

In Cooja Simulator, the average power consumption of each node is calculated automatically by its feature called collect view. The users did not need to manually calculate the node's power consumption through the radio energy dissipation formula, and the average power consumption could be converted to Energy consumption with ratio 1 Watt = 1 Joule/second. This study is taking advantage of it and directly calculates each node lifetime using the formula below.

$$Node\ Lifetime\ = \frac{Sensor\ Battery\ Capacity \times 3600 \times Voltages}{Average\ Energy\ Consumption} \quad (3.3)$$

4. Result and Analysis

This section consists of discussions about the measurement the performance of each simulation scenario and analyzing the impact of the attack in different scenarios with four metrics: Network's Lifetime, Packet Delivery Ratio (PDR), End-to-end Delay (E2E Delay), and Routing Overhead.

4.1 Estimated Network's Lifetime measurement

There are four different types of power consumption in nodes, namely Low Power Mode (LPM) power, CPU power, Listen power, and Transmission power. The Microcontroller Unit (MCU) model used in Cooja Simulator has an average voltage of 3 Volt but has no specification of its Battery Supply slot. It is safe to assume it has two slots of AA battery, just like other similar models. Then we should be able to assume its Battery Capacity safely.

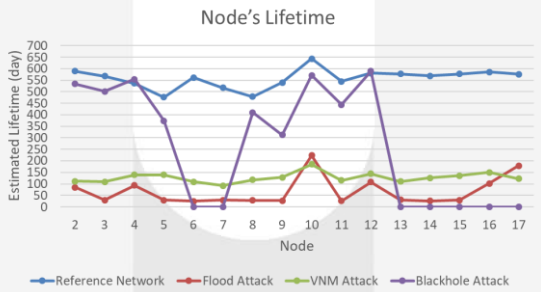

Figure 4.1 All the simulation resulted Estimated Node's Lifetime

From the Figure above, Reference Network simulation that uses 16 sensor nodes for gathering information such as relative humidity, illumination, and the temperature has an average power consumption of 1.12 mW. Also, by using the formula above to calculate the lifetime of each node, the obtained value is 1.5 years worth of lifetime on average.

By observing the nodes position and table above, nodes 3, 5, 6, 7, 8, 9, 11, 13, 14, and 15 have higher values in total power consumption. The Listen Power consumption made up around 85-90% of total power consumption. It should be noted that the power consumption on average differs by more than 20 times compared to the Reference Network. Consequently, the nodes' lifetime also reduced from around 1.5 years to less than a month. Even the other nodes that are not directly attacked by the DIS flooding, had their lifetime reduced by 6-7 times. Therefore, it can be concluded that this attack has a direct impact on the nodes within the attacker's transmission radius.

From the table above, there is an overall increase in power consumption through all nodes in VNM Attack scenario. On average, all of them experience an increase of around 400 to 500%. However, this increase in power consumption appears to be consistent as there are no significant differences between nodes. There is no particular relationship between the distance of the malicious node and other nodes with power consumption values.

Other than the inability to observe nodes 6, 7, 13, 14, 15, 16, and 17 power consumption because Cooja simulator cannot detect the power consumption of nodes that have never successfully transmit their data to Sink node, nothing else changed. The rest of the nodes in the Blackhole Attack scenario has similar power consumption

value compared to Reference Network. Blackhole Attack only works to isolate and prevent nodes from transmitting data to the Sink node successfully.

Lastly, after observing and comparing the Estimated Network's Lifetime of each attack scenario simulations to the reference network, the conclusions could be drawn. The conclusions are Hello Flood Attack has the highest degree of impact in terms of Estimated Network's Lifetime, followed by VNM Attack and then Blackhole Attack, which did not cause any notable changes in power consumption.

4.2 Packet Delivery Ratio measurement

It is important to note that the Reception and Transmission ratio is set to 100%. In other words, there will be no dropped packets caused by the transmission of packets between 2 nodes. Therefore, in a typical working network like Reference Network, there is no packet loss. In WSN, each node has a periodic Listen time for accepting transmitted packet from other nodes, by occupying most of the Listen time, Hello flood attack indirectly causes an increase of packet loss in the network. The position and range of the malicious node also influence how big of an impact it is to network's PDR. Also, the higher number of nodes within its range, the greater the packet loss.

VNM Attack force a functioning DODAG topology to rebuild itself from the beginning again. It causes nodes to drop the Data packet that is still in the middle of delivery to the sink. Then, Network would experience a massive drop in packets that should be delivered to the sink. The position and range of the malicious node have no relation to how disruptive it is to network's PDR, and it only needs to join the DODAG. Regarding the impact Blackhole Attack to a WSN, it is influenced mainly by malicious node positioning and range. The more other node uses this malicious node as their next-hop destination, the more WSNs PDR suffers.

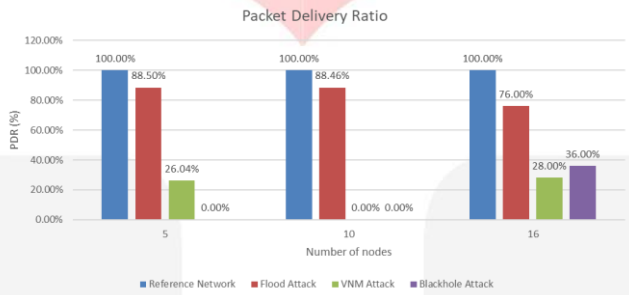

Figure 4.2 All the simulation resulted Packet Delivery Ratio

4.3 End-to-end Delay measurement

From the figure below, we can see the difference between the average E2E Delay of each scenario. Reference networks would act as a baseline, and then it can be compared to other scenarios. First, Flood Attack uses the exploit of repeatedly sending a large number of DIS as a means to waste resources, and then it would waste the resources of processing units of nodes, which resulting in an increasing Processing Delay. It also increases the Queuing Delay, through congestion it caused.

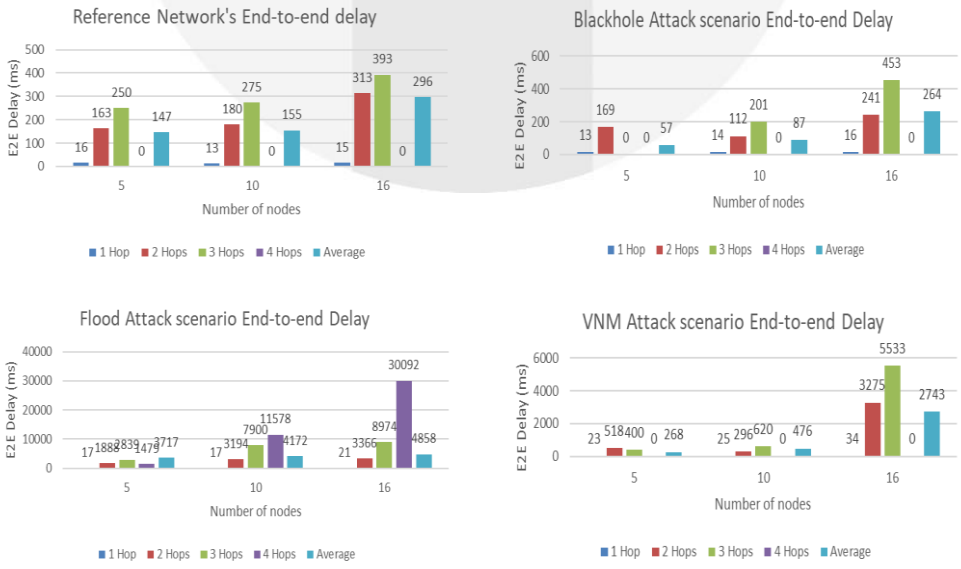

Figure 4.3 All the simulation resulted End-to-end Delay

From the previously said, VNM Attack is designed to repeatedly sending a request for DODAG reconstruction from scratch. While not as significant as flood attack, the processing delay did increase a lot. Lastly, Blackhole Attack is not a scenario where the network resources are influenced in any way, so the E2E Delay is not that much different from Reference Network. In Figure 4.3, the specific change of E2E Delay of each simulation could be observed. It contains E2E Delay categorized by the number of hops that data packets experience to complete the transmission and average E2E Delay of the network as a whole.

4.4 Routing Overhead measurement

Compared to Reference Network, the Flood Attack scenario has a notable increase in its Routing Overhead. From the gathered data, It can be concluded that the routing packet in the Flood Attack scenario is mostly comprised of DIS packets caused by flooding. The same Routing Overhead increment also can be observed from the VNM Attack scenario. Instead of DIS packets, it is mainly consisting of DAO and DIO packets that tried rebuilding the DODAG repeatedly. Comparatively, nothing changed for the Blackhole Attack scenario because it is only affected Data collection that wants to pass through the malicious node

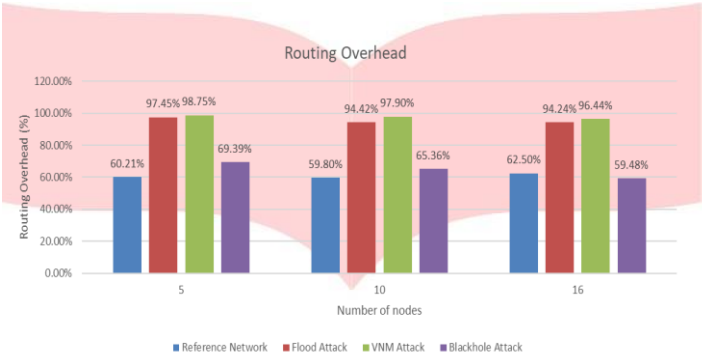

Table 4.4 All the simulation resulted Routing Overhead

4.2.5 Countermeasure for Mitigation

The first method, increase the interval which DIO sent on the affected network. This method could reduce Power Consumption, E2E Delay, and Routing Overhead of network attacked by VNM Attack. In Cooja, there is a variable called "RPL_CONF_DIO_INTERVAL_MIN" that can be modified in file Home/Contiki/core/net/rpl/rpl-conf.h. By default, each node will send DIO packets with a minimum interval of 4 seconds, increasing its interval will decrease the number of DIO and DAO packets by nodes. Figures below is the result of changing this variable to 60 seconds, but by doing this, the response time of DODAG to the change of route in topology will be slower.

Table 4.5 All the result of Mitigated Network

The second method reduces the interval of each collected data packet sent by the node. By doing this method, all scenario would yield lower Routing Overhead, but higher Power Consumption. The variable "PERIOD" value located at Home/Contiki/examples/ipv6/rpl-collect/collect-common.c can be changed to a lower value for higher sending rate of data packet.

Thirdly, reduces the increment value of Rank to advertise the affected nodes better. Nodes in RPL prefer to select a node with Rank with lower value as their next hop. Then, by lowering the variable related to it, the affected nodes would have a higher priority to become the next destination for the hop. `RPL_CONF_MIN_HOPRANKINC` variable is the minimum increase in Rank between a node and any of its DODAG parents. While `RPL_MAX_RANKINC` variable, is the maximum increase in Rank between a node and its parent. Thus, our node will now advertise the parent's Rank, incremented by any value between the min and max rank increase values. After modifying these 2 variables to a new low value compared to their initial values, the nodes in this network would have higher or same priority as a next-hop destination than a malicious node in Blackhole scenario. The 2 variable can be found at Home/Contiki/core/net/rpl/rpl-private.h.

From all the mitigated results shown previously, all the suggested methods had achieved a remarkable result in improving at least one parameter in a simulated scenario. Naturally, that includes the varying degree of trade-off.

5. Conclusion

Based on the results of simulation and analysis, the following conclusions can be drawn:

The performance test of RPL using Cooja simulator has been implemented by designing a simulation on how it usually works and simulation scenarios where a malicious node is attacking it. The metric parameters have also been acquired, such as Network's Lifetime, E2E Delay, Packet Delivery Ratio, and Routing Overhead

Flood Attack scenario had the highest increase in power consumption, the affected Network's Lifetime reduced by a staggering 20 times, a moderate decrease of 20% in PDR, overwhelming 15 times increase in average E2E Delay, and increased Routing Overhead by 30%. For VNM Attack scenario, the affected Network had 4 times less Lifetime than it should have, caused massive packets lost, which decreased PDR value by 70%, a significant 10 times increase in average E2E Delay, and had the highest impact on Routing Overhead compared to another simulated scenario. Blackhole scenario did not have any noticeable influence to affected Network's lifetime, E2E Delay and Routing Overhead. Nonetheless, Blackhole attack impact on the network showed a decrease of 60% to the PDR value. The mitigation method that has been implemented on the network in attack scenarios could reduce the impact of these attack scenarios, but it came with various trade-offs. Overall, three attack scenarios that had been tested in this thesis had various degrees of impact on the simulated WSN network, which had been mitigated to a certain degree by the method of countermeasure suggested by the author.

Reference:

[1] Emran Aljarrah, Muneer Bani Yassein. Routing protocol of low-power and lossy network: Survey and open issues. *2016 International Conference on Engineering & MIS (ICEMIS)*, 2016.

[2] Ivana Tomic, Julie A. McCann. A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols. *IEEE Internet of Things Journal*, Volume 4, Pages 1910 – 1923, 2017.

[3] Karel Heurtefeux, Nasreen Mohsin. Enhancing RPL Resilience Against Routing Layer Insider Attacks. *2015 IEEE 29th International Conference on Advanced Information Networking and Applications*, 2015.

[4] Manpreet Kaur, Amarvir Singh. Detection and Mitigation of Sinkhole Attack in Wireless Sensor Network. *2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE)*, 2016.

[5] Pravin Khandare, Yogesh Sharma. Countermeasures for selective forwarding and wormhole attack in WSN. *2017 International Conference on Inventive Systems and Control (ICISC)*, 2017.

[6] M.N. Napiah, M.Y. Idna. Detection and Mitigation of Sinkhole Attack in Wireless Sensor Network. *IEEE Access*, Volume 6, pages 16623 – 16638, 2018.

[7] Airehrour, D., Gutierrez, J., & Ray, S. K. *Secure routing for Internet of things: A survey. Journal of Network and Computer Applications*, 66, 198–213. 2016.

[8] Dvir, A., Holczer, T., & Buttyan, L. *VeRA - Version number and Rank authentication in RPL. Proceedings - 8th IEEE International Conference on Mobile Ad-Hoc and Sensor Systems*, MASS 2011, 709–714. 2011.

[9] Mayzaud, A., Badonnel, R., & Chrisment, I. *A Taxonomy of Attacks in RPLbased Internet of Things. International Journal of Network Security IJNS*, 18(3),459–473. 2016.

[10] Pongle, P., & Chavan, G. *A survey: Attacks on RPL and 6LoWPAN in IoT. In 2015 International Conference on Pervasive Computing (ICPC)* (pp. 1–6). IEEE. 2015.

[11] Haofei Xie, Guoqi Zhang. Performance evaluation of RPL routing protocol in 6lowpan. *2014 IEEE 5th International Conference on Software Engineering and Service Science*, 2014.