International Journal on
"Technical and Physical Problems of Engineering"
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

December 2021 Issue 49 Volume 13 Number 4 Pages 152-161

STUDY AND ANALYSIS OF RPL PERFORMANCE ROUTING PROTOCOL UNDER VARIOUS ATTACKS

A. Krari [1] A. Hajami [1] E. Jarmouni [2]

1. Laboratory of Research Watch for EmergingTechnologies (VETE), Faculty of Sciences and Technology, Hassan I University of Settat, Settat, Morocco, ayoub.krari@uhp.ac.ma, abdelmajid.hajami@uhp.ac.ma
2. Laboratory of Radiation-Matter and Instrumentation (RMI), Faculty of Sciences and Technology, Hassan I University of Settat, Settat, Morocco, e.jarmouni@uhp.ac.ma

Abstract- RPL is a proactive protocol based on a distance vector algorithm with robust routing capability but has baseline security features. These essential security properties can potentially make RPL susceptible to a wide variety of attacks. An attacker may exploit the RPL routing scheme to perform harmful and damaging effects over an IoT network. Therefore, routing security has turned into an essential concern for the safety of the IoT environment. Our paper concentrates on the analysis of safety risks in the RPL and potential attacks that might impact the IoT systems. Many routing attacks against RPL protocol have been investigated and simulated by performing A different attacks scenarios. To better understand how attacks operate in RPL, we first surveyed the RPL protocol functioning. In addition, we also explored a set of routing attacks against this kind of wireless sensors networks. Attacks will be simulated by using the Contiki/Cooja simulator. The obtained results after the simulations are thoroughly discussed, analyzed, and compared with other references.

Keywords: Attacks, Contiki/Cooja, LLNs, Internet of Things (IoT), Routing Security, RPL.

1. INTRODUCTION

Today, millions of intelligent devices are used across a wide range of applications to enhance our work andliving quality by conserving time and resources and providing new opportunities for growth and innovation. Addressing possible attacks against RPLs is a critical priority for enhancing the security of the upcoming Internet of Things systems [1, 2].

With large-scale data production and exchange between IoT devices and restricted IoT security to safeguard data flow, it is getting easy for attackers to breach the data channels. The IoT is evolving in many fields and continues to grow. Intelligent devices have advanced into almost all domains of life for humans [3].

Manufacturing factories, businesses and the governments are embracing self-sustaining systems to improve the effectiveness, productivity and overall economic benefits. IoT involvement is spreading into many other areas, such as healthcare, energy, public health, education and security. Management, military, agriculture, logistics supply chain and smartcities, with the purpose of one intelligent world. Routing is now one of the most researched topic fieldsin the Internet of Things (IoT), as a result of the constraining characteristic of these smart devices [4].

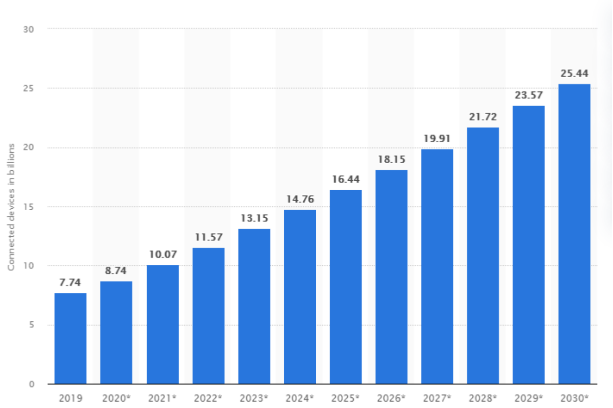

Figure 1. IoT growing connected devices by the time [3]

As compared to traditional Wireless sensor network (WSNs), Internet-connected IoT devices are reachable from anywhere, but this has the inconvenience of increasing the attack surface, both are vulnerable to external and internal attack threats to the network. The most common threats in LLNs, for example, arerouting-level attacks [5].

Our work aims to address and activate variousrouting attacks targeting the IoT networks. The goal is to test the performance of network parametersunder attack scenarios and to highlight the impacted parameters with the development of appropriate prevention and detection countermeasures.

2. RELATED WORKS

Before discussing our work, we would like to demonstrate what has been done in such studies on IoT routing attacks. In the following paragraphs, we have selected and reviewed many works that have strong relationships with our work, where authors have studied IoT routing attacks and how they work and how these attacks compromise our IoT networks.

Kumar, et al. in [6] investigated the possible impact of the Black hole attack on the communication of RPL nodes based on simulations. As expected, the attack affected many parameters, causing an increase in packet drop rate and latency as well as an escalation of control messages. The authors focused only on these parameters and did not evaluate network energyor radio capabilities.

In [7], the authors implemented a Rank attack by placing a malicious node in the network, affecting the creation of DODAG. They assumed that the attackingnode was already in the network and affected the nodes' security mechanism. They demonstrated that internal attacks are the most difficult to prevent and detect.

In [8], Anthea, et al., surveyed and reviewed the attacks in the RPL IoT Protocol, where they classifiedthe possible routing attacks against this protocol. They classified three main categories of attacks, against the resources, topology and data traffic, the risk management of these attacks has been addressed.In this work, the authors did not take us to a natural environment to test and simulate these attacks to get a clear picture of the harmful impact of these attacks against the IoT network.

In [9], A. Stephen and L. Arickiam listed out various attacks against RPL protocol. They gave an overviewof multiple attacks by providing a Literature review. They shared a summary of the attacks and the architecture design in the IoT routing protocols such as 6LoWPAN and RPL. they explained the challenges and the security issues. Still, they did not simulate the attacks, which motivated us to carry on and simulate various attacks in real-time.

As a result of all these studies and surveys on RPL attacks, some authors did not simulate any routing attacks, and others simulated only one or two attacks.Thus, based on these previous works, we propose a new study to examine and analyze the performance ofRPL under various attacks. This new study will implement five different attacks against the RPL protocol, both direct and indirect attacks, focusing on indicators of compromise, such as packet loss, powerconsumption, radio listen/transmit and other parameters.

3. RPL OVERVIEW

RPL is the routing protocol of IoT devices. It is the standard network routing protocol offered for LLNs QoS [10, 11, 12], It is applied to smart devices and objects with limited computing specifications. It can handle three kinds of behavior: point-to-multipoint, point-to-point, and multipoint-to-point topology. and it is listed in RFC because of its ability to provide efficient routing scalability and QoS.

3.1. RPL DODAG

The RPL relies on the formation of DODAG to arrange the object inside the network. It forms a directed acyclic graph [13].

It is called DAGs, the DAG composed of many interconnected nodes in which there is a node called the root. Inside the DAG resides one or more destination-oriented DAGs (DODAGs) [14, 15].

Toallow multiple applications to operate together but separately within the network, multiple RPL instances can coincide within a DAG. In an RPL instance, we can find one or more DODAGs, and the DODAGS in the same instance share the same ID [14]. Figure 2 illustrates a DAG consisting of two RPL instances and three DODAGs.

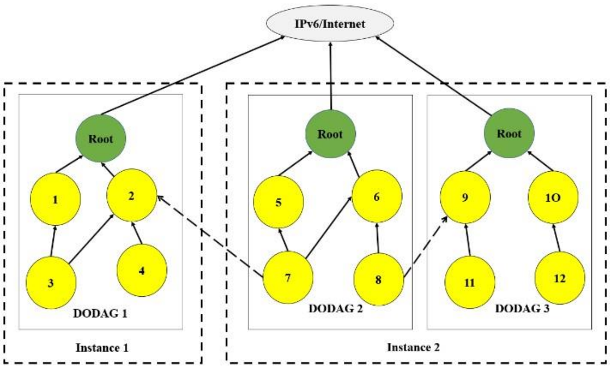

Figure 2. RPL DODAG instances [8]

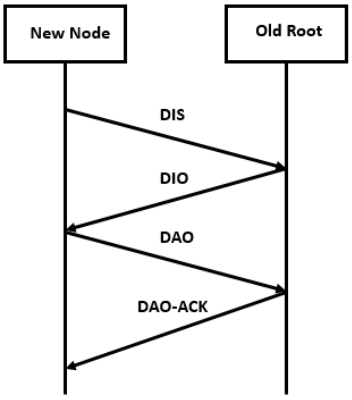

Figure 3. RPL ICMPv6 control messages [9]

The RPL protocol is composed of three separate kinds of messages (ICMPv6 type) which are described as:

- (DIO) DODAG Information Object: The root of the DODAG is the first node in the DODAG, and the node with rank set to one, it transmits a DIO messageall nodes to build a new DODAG tree. The structure of the DIO message holds all the network related details that enable any node to identify an RPL instance, select a parent DODAG set, obtain its setup settings, and eventually construct the DODAG [16].
- (DAO) Destination Announcement Object: As the DODAG is built, every node in the DODAG forwardsthis message information to spread and provide a node rank and routing table information to its preceding nodes that carry the downstream traffic (traffic to the egress nodes) [16].
- (DIS) DODAG Information Request: Any node triggers such messages to send DIO messages to thatnode, and then only if that node has not received a proper DIO message for a long time [16].

Most routing protocols typically broadcast control messages at a constant rate, resulting in wastingenergy for the network, Hence, the RPL protocol applies the Trickle algorithm to control sending rate of DIO messages of [16].

Control messages will be outstanding in a network with stable links, but control messages will be sent more often in situationswhere the topology changes repetitively.

4. ATTACKS STUDY: RESULTSAND ANALYSIS

4.1. Contiki OS (Network Reference)

Cooja is the acronym for Contiki OS Java Simulator. This simulator allows the emulation of different nodes on which the Contiki operating system and applications are loaded.

This tool enables applications to be tested at a low cost before being loaded into the flash memory or the flash memory of absolute sensors.

Contiki is a flexible, lightweight OS for networked miniature sensors. In recent years, the scientific world has paid significant attention to wireless sensor networks. The miniaturization of sensors and their relatively low cost makes it possible to imagine a wide range of applications in the scientific, military, industrial, and home automation fields. To facilitate the development of these applications

Cooja is a multi-tasking, fully open-source, extremely wearable OS for embedded networked systems and wireless sensor networks with low memory consumption [17].

4.2. Methodology Used

This subsection outlines the proposed methodology to investigate the impact of energy consumption, packets lost, and radio consumption incurred by attacks against WSNs employing RPL as a routing protocol. Furthermore, it can be used in turn to analyze possible solutions and countermeasures against the examined attacks. The following approach will be explained through various phases to achieve the goals and objectives described. The framework isalready chosen and explained before (Cooja simulator), all phases are described in above graph.

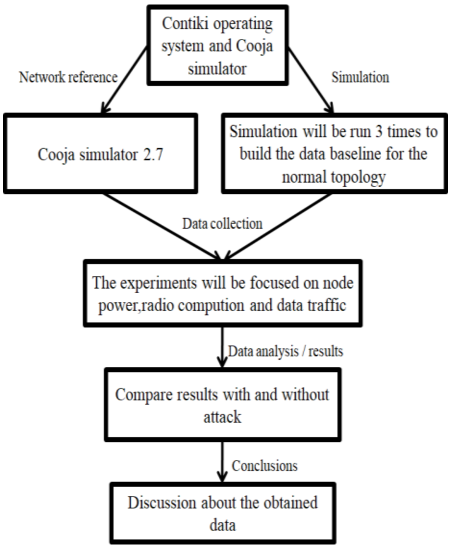
Contiki operating system and Cooja simulator
Network reference
Simulation
Cooja simulator 2.7
Simulation will be run 3 times to build the data baseline for the normal topology
Data collection
The experiments will be focused on node power,radio compution and data traffic
Data analysis / results
Compare results with and without attack
Conclusions
Discussion about the obtained data

Figure 4. Our Methodology used for our work

4.3. Simulation of Normal Topology without Attack

4.3.1. Description

This simulation is going to be our reference that we will compare to other simulations with attacks. All the simulations that we will work on are designed to be as realistic as possible. We have used the Contiki/Cooja simulator in an area of 100×100 meters with a random distribution of nodes, the configuration of the Normal simulation without attacks and the location of the nodes is described in the following graph in the Figure 5 and the Table 1. The Table 1 describes the details of our baseline simulation.

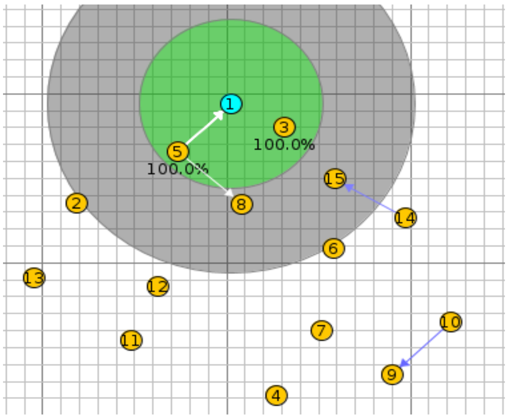

Figure 5. Topology of normal simulation under Cooja simulator

Table 1. configurations parameters for the normal simulation

Parameters	Values
Node type	SKY Mote
Os Version	Contiki 2.7
Protocol	RPL
Radio Medium	Unit Disk Graph Medium: distance loss
Objective Function	MRHOF
Tx Range	50 m/100 m
Interface Range	50 m/100 m
Simulation Area	100 m × 100 m
MTU Size	1280 Byte
Simulation Duration	30 minutes
Sender Nodes	15
Sink Node	1
Repetitions	3

4.3.1.1. Objective

The objective is to provide the baseline data without attack in order to compare the results of other attack simulations in terms of power, traffic data and lost packets, and other parameters. After the basic reference network is in place, it will be possible to collect the necessary data to serve as the basis for thestudy. The following sections describe the impact of performing several routing attacks using a malicious node in normal topology and launching attacks. As we will see later, the malicious node will maintainthe exact same position in the experiment area.

4.3.1.2. Results and Analysis

As previously stated, all the results we have got during the standard simulation without attacks are correct and our reference for the expected behavior ofthe nodes. Therefore, it can be used as a reference to compare the results of other simulations.

As observed in the following graphs in the Figures 6, 7 and 8, there are no affected parameters, the average power consumption for all the nodes is around the mean 1.074 mw, the radio listen/transmit is also in the norms and the lost packets for our baseline simulations after five repetitions for 30 minutes are zero, with zero reboots. These results willbe used as our baseline data:

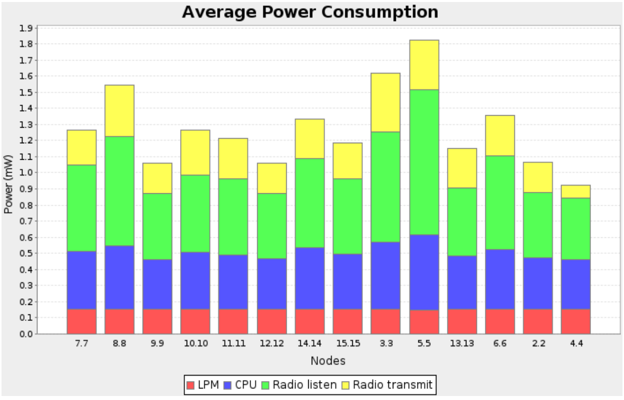

Figure 6. Graphical view of nodes power consumption

Also, the consumption of radio-listening and radio-transmitting is stable, the rates are regular, the average radio cycle duty is between 1.1% and 1.4%, radio-listening is logically higher than radio- transmitting because the nodes during the formationof the DODAG receive various control messages aswe can notice in the following graph in the Figure 7 and for the packet loss parameter, the result is positive. We did not drop any packets, during the simulation.

4.4. Attacks Implementations

In our work, we tested five different attacks:

In the following sections, a description, objective, and the impact of the attacks will be detailed.

For this research, the malicious node will always be situated at the same position, except when we want toprove the damage inflicted by the attacker's location.The map of the network with the malicious node (Node ID: 16) is shown below (Figure 9).

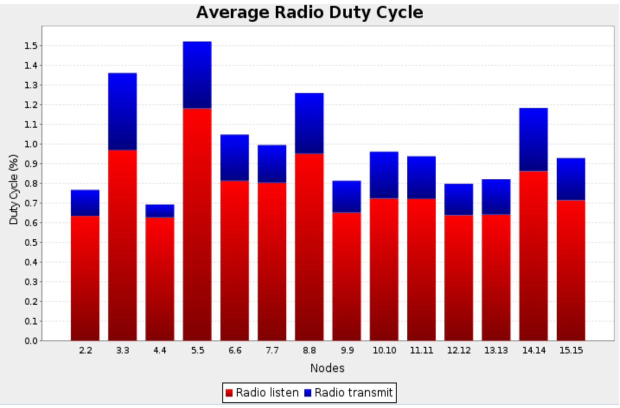

Figure 7. Graphical view of nodes radio consumption

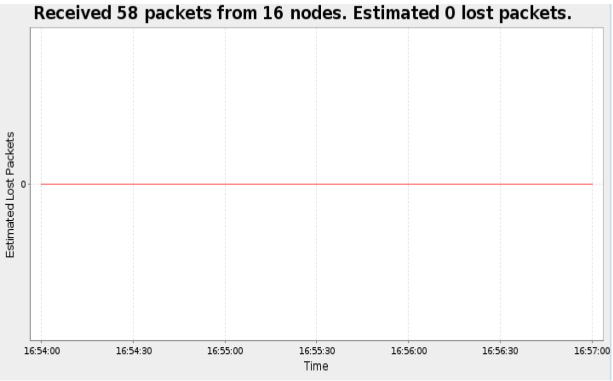

Figure 8. Graphical view of nodes lost packets

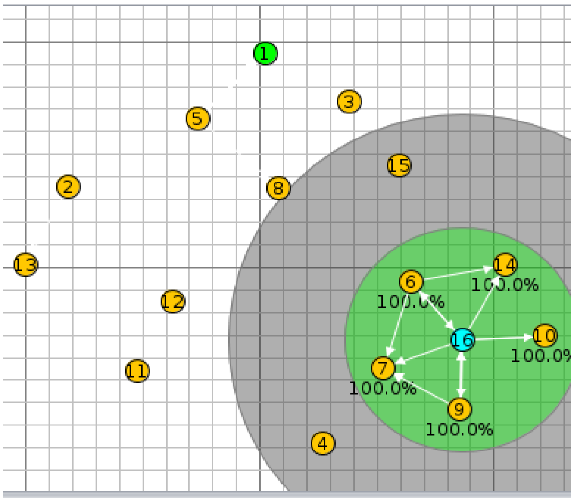

Figure 9. Position of the malicious node

4.4.1. DIS Attack

4.4.1.1. Description

In this attack, the flooding attack will be launched against the IoT nodes. The flooding attack is a denial-of-service attack as it attempts to make the nodes andlinks unavailable by generating massive traffic. The attacking node will cause other nodes to lose energy, have latency and lose packets, thus this type of attackis perilous as long as the objective of is to disrupt theservice and disable neighboring nodes and the servicein general [18].

4.4.1.2. Results and Analysis

Based on the below graphs in the Figures 10, 11 and 12, it can be concluded that there is an overall increase in total energy consumption as occurred during the DIS attack. After launching the DIS attack,we can observe that the neighbor's nodes to the malicious node are affected, the energy of some nodesexceeded 45 mw, radio listening, and transmission cycle and also increased, and 51 packets lost during 30 minutes by all nodes. The effects of the DIS attackare relative as long as the neighboring nodes to the malicious nodes are the most affected, specifically thenodes in the radio range of the attacker node. With this scenario, we proved that if the nodes are close tothe attacker node, their consumption rates of energy, radio, and packet loss will increase.

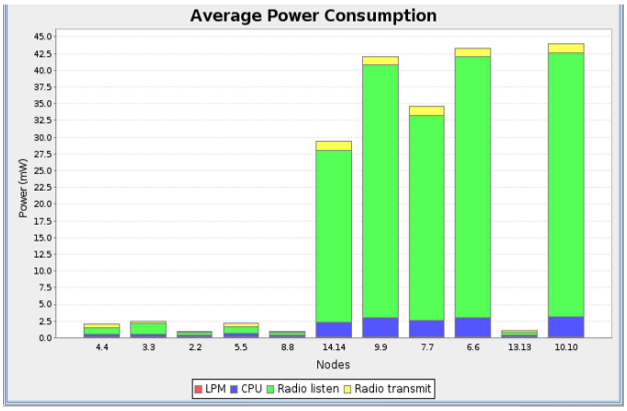

Figure 10. Power consumption during DIS attack

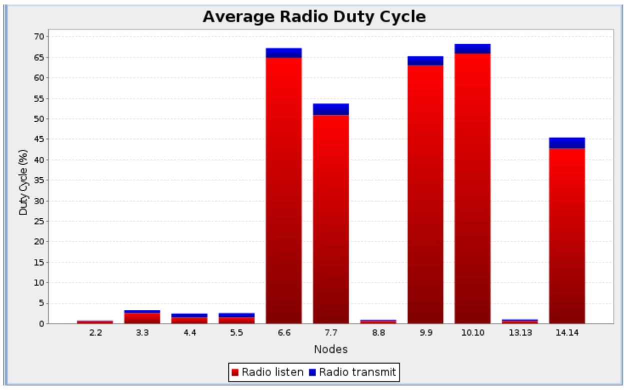

Figure 11. Radio consumption during DIS attack

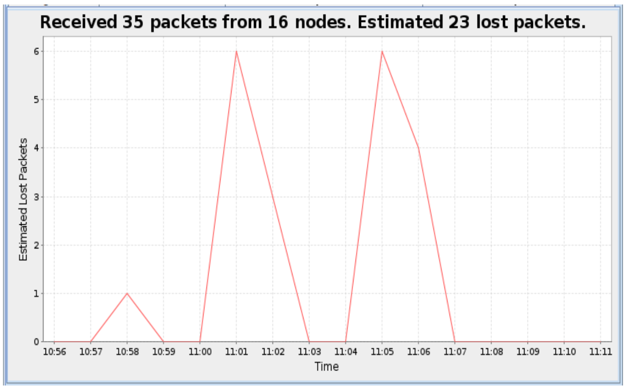

Figure 12. Lost packets during DIS attack

4.4.2. Version Number Attack

4.4.2.1. Description

This type of attack continues to send a higher version of DODAG every time, and this behavior will cause the IoT network topology to be restarted, the DODAG tree will trickle another topology formation, and it can cause instability in the nodes' topology and further wasting energy as long as the IoT devices are energy constrained devices [19]. The purpose of this simulation is to analyse the impact caused by this attack when the child nodes periodically receive DIOmessages with a higher version and to further demonstrate the effects on energy consumption, radioand data traffic. In addition, a solution can be proposed to shut down or mitigate this attack [20].

It can cause instability in the nodes' topology and further wasting energy as long as the IoT devices are energy constrained devices [19]. The purpose of this simulation is to analyse the impact caused by this attack when the child nodes periodically receive DIOmessages with a higher version and to further demonstrate the effects on energy consumption, radioand data traffic. In addition, a solution can be proposed to shut down or mitigate this attack.

4.4.2.2. Results and Analysis

Same as the previous attack, the power is increased during this attack. If we keep launching this attack for a long time, the energy will drain until we lose the devices. The radio consumption also increased among thenodes as we can observe in Figure 14. There are a lost packet, we lost 4 packets duringversion number attack.

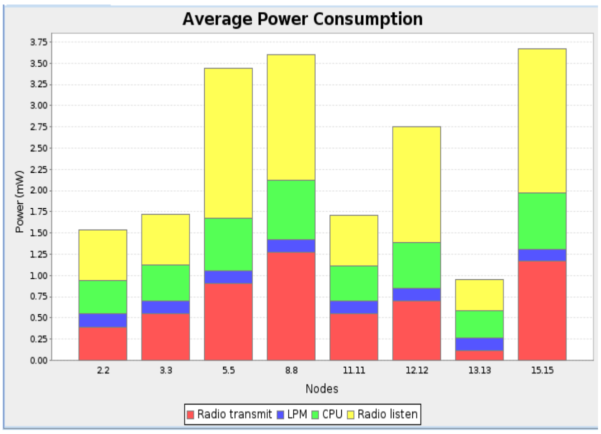

Figure 13. Graphical view of the power consumption duringVersion number attack

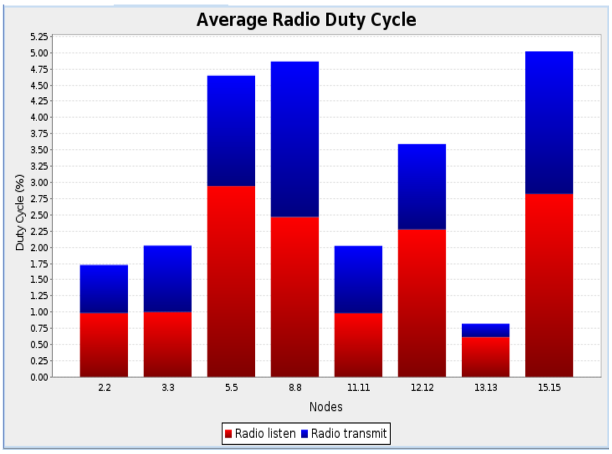

Figure 14. Graphical view of the radio consumption duringVersion number attack

The version attack attempts to release a higher version number of the DODAG to cause inconsistencies in the network. Due to the version number differences, RPL triggers a global repair to create a new DODAG. As we can see in the below graphs in the Figure3 13, 14 and 15, we have a traffic overload and increased energy consumption of the nodes, Radio listens, and transmit and packets lost.

We can see that all power metrics have been rising. Because of version attacks triggering full scale repairs, the amount of time nodes stays active increases from the original performance.

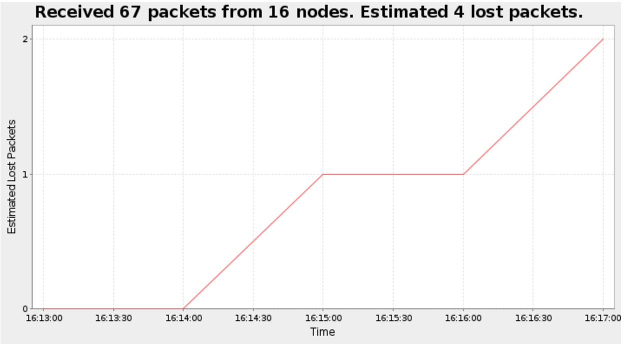

Figure 15. Lost packets during version number attack

4.4.3. Black Hole Attack

4.4.3.1. Description

The primary objective of a black hole attack is to launch a denial of service to the leaf nodes. The malicious node in this situation absorbs all the control messages received from the other nodes in the network. This can cause a perturbation to the network. The nodes should communicate adequatelyto form a legal DODAG without issues [21]. In addition, when launching a black hole attack, the malicious node does not generate any control messages. This can isolate some nodes from thenetwork. We explained the impact of this attack on the high packet loss rate, control, route traffic overhead, also energy consumption of the nodes.

4.4.3.2. Results

As we can notice in the results we got, that there is a high packet drop rate and high control and route traffic overhead, the power, and radio consumption isincreased for all nodes, this can cause a drain energy from surrounding nodes as same for the radio listen and transmit, we also lost four packets during the presented simulation, due to the malicious nodes are spreading black hole attacks, which drains the limited resources of IoT nodes. Network latency increases and node ranks are changed, disrupting the network topology and stability, in addition, the rank alteration forces nodes to recalculate their ranks. As we can seein the following graphs in the Figures 16, 17 and 18.

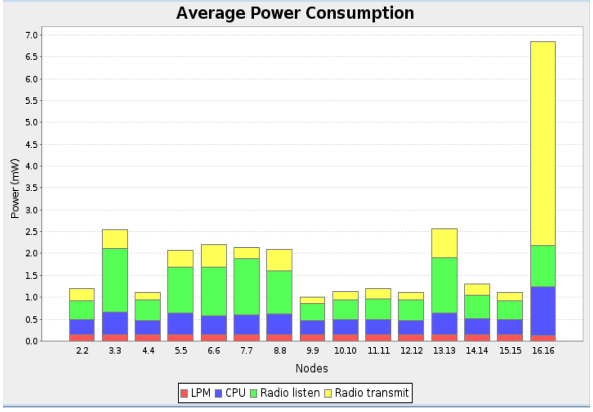

Figure 16. Graphical view of power consumption during black hole attack

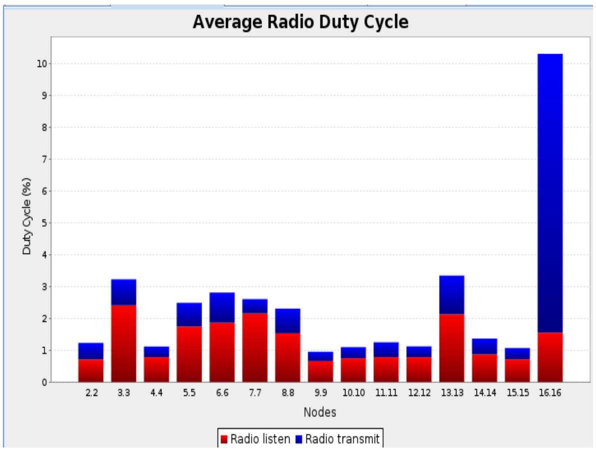

Figure 17. Radio consumption during black hole attack

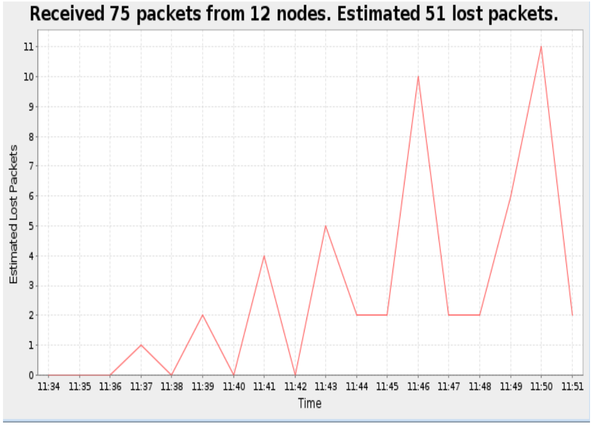

Figure 18. Lost packets during black hole attack

4.4.4. DIO Flood Attack

4.4.4.1. Description

The goal of DIO Flood attack is to send a vast amountof DIO messages to the malicious node's neighbors todrain all of its internal resources by attempting to serve the fake traffic so that it cannot handle any legitimate incoming service requests, this simulationaims to show the impact of the flood attacks, not only with DIS messages but also with DIO messages.

4.4.4.2. Results

Figures 20, 21, 22 and 23 are extracted from the Cooja simulator show that the most impacted parameters during this attack are the power conception, radio listens, and transmit. Because it's a flood attack, we also noticed a packet delay and latency in the network, the malicious node keeps sending a massiveamount of DIO messages to the child nodes causing them a drain in the term of energy and radio.

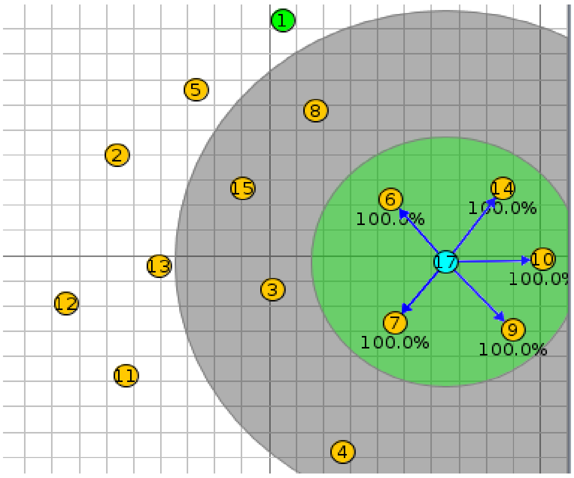

Figure 19. The malicious node flooding the neighboring nodes with DIO messages

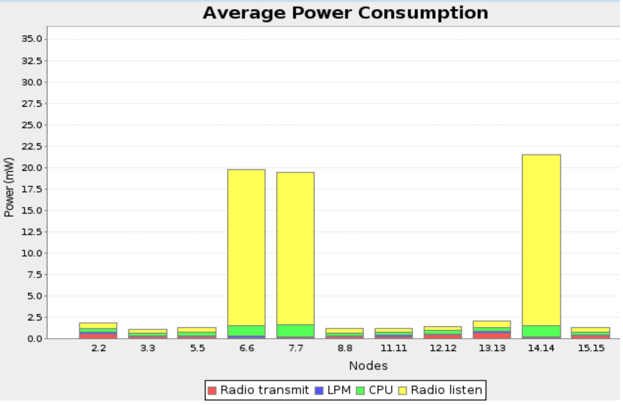

Figure 20. Graphical view of power consumption during DIO flood attack

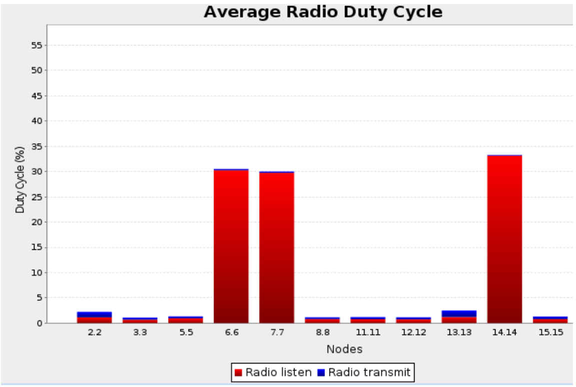

Figure 21. Graphical view of radio consumption during DIO flood attack

And as we can observe in the DODAG map above, some nodes (ID: 4,10 and 9) were unable to join the network due to the massive number of DIO messages transmitted by the malicious node, resulting in latency and response issues for the simulator and the collect view function, even though we repeated the simulation many times and even for an hour, we can say that the DIO flooding attack causes many problems to the network, such as the enormous number of packets, energy consumption, and latency.

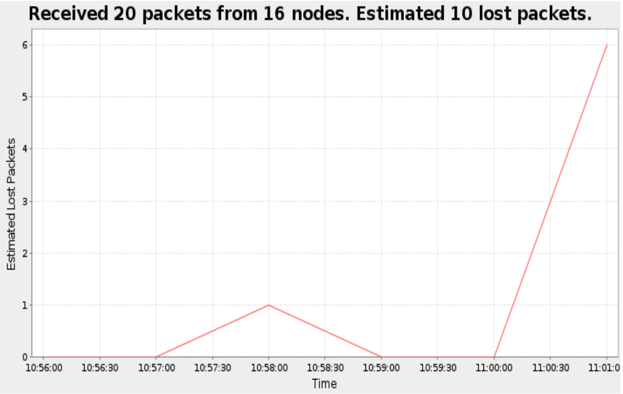

Figure 22. Graphical view of lost packets during DIO flood attack

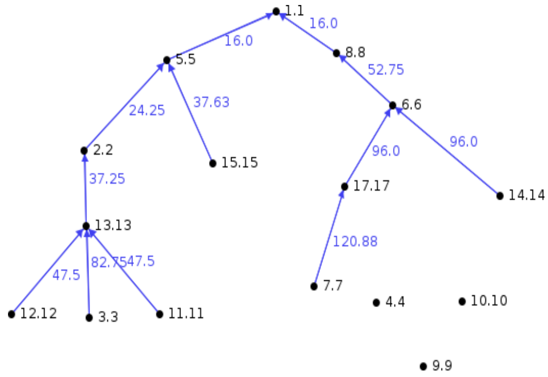

Figure 23. DODAG map formation during DIO flood attack

4.4.5. DAO Attack

4.4.5.1 Description

Relies on DAO messages to establish downlink routes for bidirectional communication. The RPL requirement does not specify when and how often DAOs are forwarded. Thus, this routing mechanism can be abused by a malicious node that regularly forwards a large number of DAO messages to its parent and so on until they reach the root of the DODAG (Direction-Oriented Directed Acyclic Graph) [22]. This eventually has a detrimental impacton the efficiency of the network in terms of energy consumption, latency, and availability, the goal of oursimulation is to shows how this behavior can negatively affect network performance, increase energy consumption, latency, and reduce reliability.

4.4.5.2. Results

The restructuring operations performed by DAO Attack potentially cause significant overhead in termsof energy and radio consumption for all the nodes in the network like we can notice in the following graphical views in the Figures 24 and 25.

4.5. Comparison of Attacks Based on Affected Parameters

In this section, we compared the impact of the different attacks to identify which ones significantly affect the network resources, we present the following graphical views in the Figures 26, 27 and 28, that clearly show the effect of each attack on the most impacted metrics during the simulations.

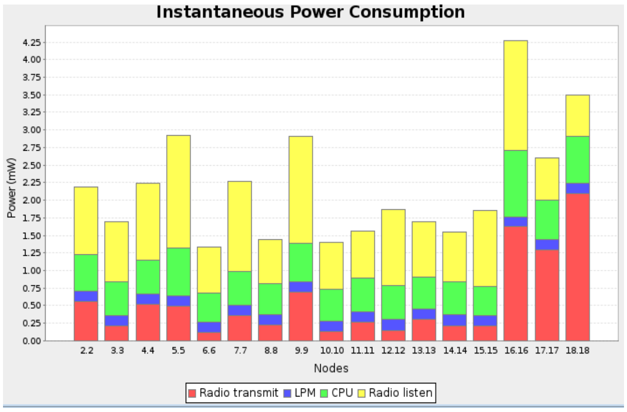

Figure 24. Graphical view of power consumption during DAO attack

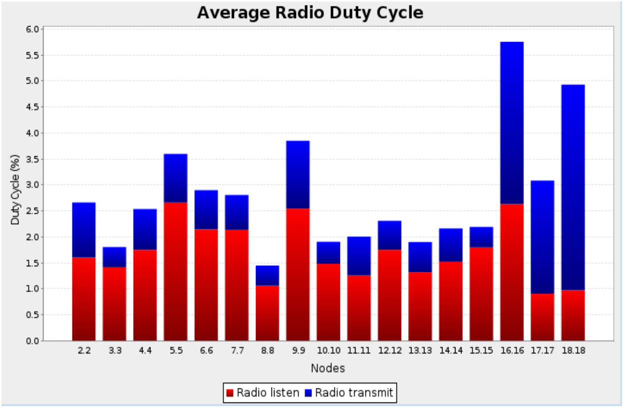

Figure 25. Graphical view of radio consumption during DAO attack

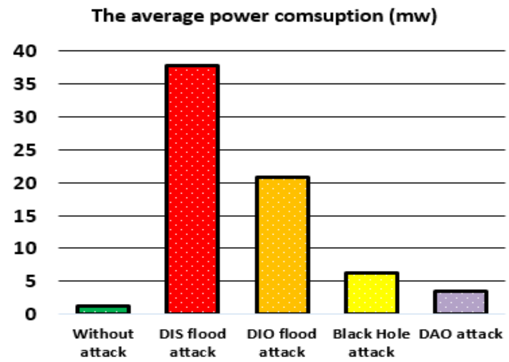

Figure 26. Average power consumption of the five attacks

The Figure 27 is a comparison of the packet loss. Packet loss is a highly critical factor. Whenever welose a packet during a simulation, it can affect the whole network. The more packets we lose, the greater our network resources will be exhausted. We can useit as an indicator of compromise. For the five studied attacks. We also compared the average duty cycle ofradio listening and transmission of the nodes affectedby the different routing attacks implemented. The following graph (Figure 28) facilitates and clearly demonstrates how much the nodes are being affected by these attacks, in some attacks, the radio listening is boosted dueto the nodes receiving a large amount of control messages and other attacks, we can see that the radiotransmitter is higher because the nodes are transmitting and flooding other nodes, thus consuming a lot of energy.

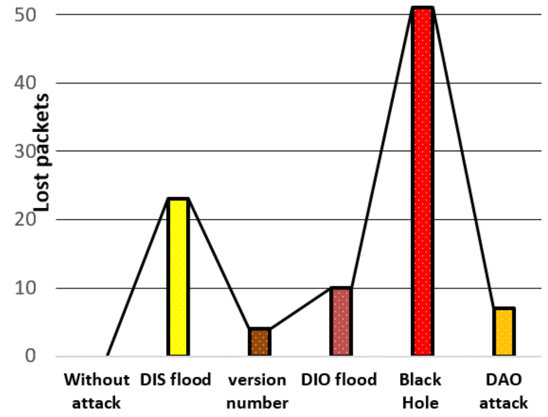

Figure 27. Comparison of the total lost packets

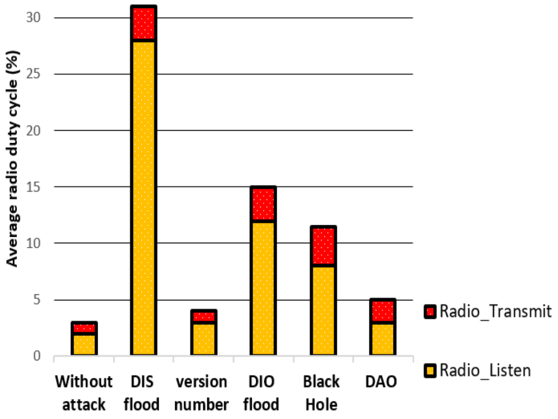

Figure 28. Average radio consumption of the five attacks

Finally, we can conclude that our work focused on the most impacted parameters. After all these analyses, the most impacted parameters when we launch an attack against an IoT network are the power drain, radio listens and transmits, and the impacted data traffic like latency and packet loss. It will be helpful and easy to monitor IoT devices when theseparameters are touched. These results can be used to build a detection mechanism in future work.

5. CONCLUSION

In our work, we implemented multiple direct and indirect attacks in RPL/6LoWPAN routing protocol. RPL is the standards routing protocol for the internet of things. With the enormous connected numbers today, the need for security is in high demand. The IoT network is connecting billions of devices and generating massive heterogeneous data. In our work, we showed how these attacks operate and proved their impact on performance metrics. We compared the effect to the standard simulation. Therefore, it is our baseline reference, thus performing a full range of analyses of attacked components of network (resources, topology, and related data streams) in various situations.

We reviewed the results obtained to help define which parameters should be tracked or referenced for the applied attacks. We will use both sets of results and identified indicators of compromise detailed in this paper regarding our future work. We work on a system architecture where we will be based on artificial intelligence in order to detect, prevent and determine suitable countermeasures for these attacks.

REFERENCES

[1] J.A. Stankovic, "Research Directions for the Internet of Things", IEEE Internet of Things Journal, Issue 1, Vol. 1, pp. 3-9, March 2014.

[2] O. Ali, M.K. Ishak, "Bringing intelligence to IoT Edge: Machine Learning based Smart City ImageClassification using Microsoft Azure IoT and Custom Vision", International Conference on Emerging Computing Technology and Sports (JICETS), Issue 4, Vol. 1529, Bandung, Indonesia, April 2020.

[3] I.M.M. El Emary, "Improving the Performance of Integrated Service Networks Using Self Adaptive CSMA/CD and Various Control Algorithms", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 2, Vol. 2, No. 1, pp. 66-72, March 2010.

[4] B. Farzaneh, M. Koosha, E. Boochanpour, E. Alizadeh, "A New Method for Intrusion Detection on RPL Routing Protocol Using Fuzzy Logic", The 6th International Conference on Web Research (ICWR), pp. 245-250, Tehran, Iran, June 2020.

[5] T. Heer, O. Garcia Morchon, R. Hummen, S.L. Keoh, S.S. Kumar, K. Wehrle, "Security Considerations in the IP-based Internet of Things", Wireless Personal Communications, pp. 527-542, March 2012.

[6] A. Kumar, R. Matam, S. Shukla, "Impact of Packet Dropping Attacks on RPL", The Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), pp. 694-698, April 2017.

[7] R. Sahay, G. Geethakumari, K. Modugu, "Attack graph - Based vulnerability assessment ofrank property in RPL-6LOWPAN in IoT", IEEE 4th World Forum on Internet of Things (WF-IoT), pp. 308-313, Singapore, May 2018.

[8] A. Mayzaud, R. Badonnel, I. Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things", International Journal of Network Security, pp. 459-473, May 2016.

[9] A. Stephen, L. Arickiam, "Attacks against RPL in IoT: A Survey", Issue 4, Vol. 25, pp. 9767-9786, April 2021.

[10] M.R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L.A. Grieco, G. Boggia, M. Dohler, "Standardized protocol stack for the internet of (important) things", IEEE Communications Surveys and Tutorials, Issue 3, Vol. 15, pp. 1389-1406, December 2012.

[11] J. Granjal, E. Monteiro, J.S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", IEEE Communications Surveys & Tutorials, Issue 3, Vol. 17, pp. 1294-1312, January 2015.

[12] A. Oliveira, T. Vazao, "Low-power and lossy networks under mobility: A survey", Computer Networks, The International Journal of Computer and Telecommunications Networking, Issue 2, Vol. 107, P. 339-352, October 2016.

[13] M. Zhao, A. Kumar, P. Chong, R. Lu, "A comprehensive study of RPL and P2P-RPL routing protocols: Implementation, challenges and opportunities", Peer-to-Peer Networking and Applications, Issue 5, Vol. 10, pp. 1232-1256, July 2016.

[14] J. Granjal, E. Monteiro, J.S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", IEEE Communications Surveys and Tutorials, Issue 3, Vol. 17, pp. 1294 - 1312, City, Country, January 2015.

[15] J.C. Agustin, H. Jacinto, R. Limjoco, J. Rhodette, "IPv6 routing protocol for low-power and lossy networks implementation in network simulator", TENCON 2017, IEEE Region 10 Conference, Penang, Malaysia, December 2017.

[16] A.A. Hakeem, A.A. Hady, H. Kim, "RPL Routing Protocol Performance in Smart Grid Applications Based Wireless Sensors: Experimental and Simulated Analysis", Electronics, Issue 2, Vol. 8, No. 3, February 2019.

[17] A. Dunkels, B. Gronvall, T. Voigt, "Contiki - a lightweight and flexible operating system for tiny networked sensors", The 29th Annual IEEE International Conference on Local Computer Networks, p. 455-462 Tampa, FL, USA, December 2004.

[18] G. Guo, "A Lightweight Countermeasure to DIS Attack in RPL Routing Protocol", IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), NV, USA, March 2021.

[19] A.B. Balametov, A.K. Salimova, E.A. Balametov, "Energy Efficient Solutions for Electric Power Supplu Rural and Suburban Consumers", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 25, Vol. 7, No. 1, pp. 33-38, December 2010.

[20] A. Aris, S.F. Oktug, "Analysis of the RPL Version Number Attack with Multiple Attackers", 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pp. 1-8, Dublin, Ireland, June 2020.

[21] F. Ahmed, Y.B. Ko, "Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks", Security and Communication Networks, Issue 18, Vol. 9, pp. 5143-5154, December 2016.

[22] I. Wadhaj, B. Ghaleb, C. Thomson, A. Al Dubai, W.J. Buchanan, "Mitigation Mechanisms Against the DAO Attack on the Routing Protocol for Low Power and Lossy Networks (RPL)", IEEE Access, Vol. 8, pp. 43665-43675, March 2020.

BIOGRAPHIES

Ayoub Krari was born in Settat, Morocco, in 1996. He received his master's degree in telecommunications system and network engineering from University Sultan Moulay Slimane of Beni Mellal, Morocco in 2019. He is currently a systems and security engineer at the Ministry of National Education, Morocco. His research areas include the internet of things (IoT), networks security, and artificial intelligence.

Abdelmajid Hajami was born in Morocco, in 1975. He received the Ph.D. degree in informatics and telecommunications from Mohamed V Souissi University, Rabat, Morocco. He was ex-trainer in regional centre of teaching and training. He is currently a

Professor at Faculty of Science and Technology, Settat, Morocco. He is a member of LAVETE Lab at the same faculty. His research interests are security and QoS in wireless networks, radio access networks, next generation networks, ILE (informatics learning environments) eLearning, biotechnology communications.

Ezzitouni Jarmouni was born in Settat, Morocco, in 1994. He received his master's degree in electrical engineering from faculty of science and technology Settat, Morocco in 2019. He is currently a qualified secondary school mathematics teacher at Ministry of National Education, Morocco. His research areas include smart grid, renewable energy, and artificial intelligence.