Vulnerability Assessment of Objective Function of RPL Protocol for Internet of Things

Felisberto Semedo
School of Computing (SoC)
Edinburgh Napier University
Edinburgh, United Kingdom
40270613@live.napier.ac.uk

*Naghmeh Moradpoor
School of Computing (SoC)
Edinburgh Napier University
Edinburgh, United Kingdom
*n.moradpoor@napier.ac.uk

Majid Rafiq
School of Computing (SoC)
Edinburgh Napier University
Edinburgh, United Kingdom
40184826@napier.ac.uk

ABSTRACT

The Internet of Things (IoT) can be described as the ever-growing global network of objects with built-in sensing and communication interfaces such as sensors, Global Positioning devices (GPS) and Local Area Network (LAN) interfaces. Security is by far one of the biggest challenges in IoT networks. This includes secure routing which involves the secure creation of traffic routes and secure transmission of routed packets from a source to a destination. The Routing Protocol for Low-power and Lossy network (RPL) is one of the popular IoT's routing protocol that supports IPv6 communication. However, it suffers from having a basic system for supporting secure routing procedure which makes the RPL vulnerable to many attacks. This includes rank attack manipulation. Objective Function (OF) is one of the extreme importance features of RPL which influences an IoT network in terms of routing strategies as well as network topology. However, current literature lacks study of vulnerability analysis of OFs. Therefore, this paper aims to investigate the vulnerability assessment of OF of RPL protocol. For this, we focus on the rank attack manipulation and two popular OFs: Objective Function Zero (OF0) and the Minimum Rank with Hysteresis Objective Function (MRHOF).

CCS CONCEPTS

• Security and privacy → Intrusion/anomaly detection and malware mitigation → Intrusion detection systems

KEYWORDS

IoT, LLN, RPL, OF, Internal Threat, Rank Attack Manipulation

SIN '18, September 10–12, 2018, Cardiff, United Kingdom
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-6608-3/18/09…$15.00
https://doi.org/10.1145/3264437.3264438

1. INTRODUCTION

The Routing Protocol for Low-power and Lossy network (RPL), is a lightweight distance vector routing protocol proposed by Internet Engineering Task Force (IETF) to support IPv6 communication across wireless sensor or IoT networks. It is a rank-based protocol designed to support point-to-multipoint (P2MP; from the root to the nodes), multipoint-to-point (MP2P; from the nodes to the root), and point-to-point (P2P; from the child to the parent or vice versa) communications. An IoT network can have one or more RPL instances which forms multiple Destination Oriented Directed Acyclic Graph (DODAG). A node can join more than one instance but only be in one DODAG [3]. Each instance has its own Objective Function (OF). OF is one the most important parameters used by RPL to determine how the IoT nodes select and optimize routes towards the root based on a set of network metrics e.g. Expected Transmission Count (ETX), rank, power, or latency. It also defines how nodes translate metrics into rank to select their parents [2]. Although the literature has many flavors of the newly proposed OFs, the IETF work group has defined only two as the main OFs for RPL: Objective Function Zero (OF0) and the Minimum Rank with Hysteresis Objective Function (MRHOF). Contrary to the traditional routing protocol such as Open Shortest Path First (OSPF), RPL does not incorporate the security mechanisms needed to avoid intruders from unauthorized access to the data over an IoT network [3]. Due to this fact, RPL is exposed to several types of attacks such as rank attack which puts Confidentiality, Integrity, and Availability (CIA) of the data in constant danger. For RPL protocol, a rank is a network parameter that increases downward from the root to the child nodes and decreases upwards from the child nodes to the root. Rank attack is one of the most popular attacks on RPL protocol in which a malicious or a compromised node advertises a false rank in place of the one it should have, and thus affects the other nodes rank and consequently changes the routing path in the network [3]. The attack was introduced in [4-6] but only targeted the RPL protocol without considering the OF vulnerabilities which ended up having a very limited impact on the network performance.

To the best of our knowledge, only [1] exploited the rank attack on RPL using OF for the Low power and Lossy Networks (LLN). Although, their proposed rank attack is a more powerful attack as compared to the original one introduced in [4] & [6], they have only employed their attack on MRHOF without considering OF0. Therefore, in this paper, we mainly focus on OF0's security weaknesses to prove that OF0 of RPL protocol is also vulnerable to a rank attack. In this paper, we aimed to answer four research questions as follows.

1. Is the OF0 of RPL protocol vulnerable to a rank attack as is MRHOF?
2. What happens when a malicious node executes a rank attack on MRHOF? How does this impact other nodes?
3. What happens when a malicious node executes a rank attack on OF0? How does this impact other nodes?
4. Which objective function is more disruptive when a rank attack is executed, OF0 or MRHOF?

The remainder of this paper is organised as follows. In Sections 2, we review the related work on the RPL attacks and countermeasures followed by our network model and simulation results in Sections 3. This is trailed by the simulation results and analysis in Section 4 and 5 followed by conclusions & future work in Section 6 and references.

2. Related Work

RPL is a novel and highly vulnerable protocol for the emerging IoT technology. This protocol is under constant study and improvements with the aim to improve its security mechanism. There are various attacks exploiting the RPL protocol in the literature along with the proposed countermeasures [3] and [7]. This includes: direct attacks (e.g. hello flooding attack), indirect attacks (e.g. increased rank attack and version number attack), attacks on the network topology (e.g. sinkhole, wormhole and worse parent attacks), isolation attacks (e.g. blackhole attack), attacks on the traffic (e.g. traffic sniffing and selective-forwarding attacks), misappropriation attacks (e.g. decreased rank attack and identity attack), and attacks targeting objective functions (e.g. rank attack using MRHOF in RPL). It also includes other known attacks such as: clone id/sybil attack, Denial of Service (DoS) attack, local repair attack, and neighbor attacks.

For example, the direct attacks are the ones responsible for exhausting network resources by using RPL flood mechanisms or executing overloading attacks on the routing table when the storing mode is enabled. In flooding attacks, the malicious node introduce itself as neighbor to the network nodes, by broadcasting DODAG messages with strong routing metrics to facilitate its entrance in the network [7] and [11]. If the hello flooding attack isn't combined with other attacks, the RPL Global and Local repair mechanism is able to defeat it by trying to stabilize the network flood or inconsistency. The authors in [8] proposed the use of link-layer metric as a parameter when selecting default route to mitigate hello flooding attacks. Likewise, to defeat other attacks on RPL the following techniques have been proposed in the literature. The use of version number and rank authentication (VeRA) proposed by [7] and [9] to mitigate increased rank attack, attacks on the network topology, and misappropriation attacks, use of local decision and a global verification process proposed by [10] to defeat isolation attack such as blackhole attack, use of heartbeat proposed by [8] to mitigate attacks on traffic such as select-forwarding attack, use of the instances tracking numbers to minimize clone id/sybil attack and detect the cloned identities proposed by [8]. The only rank manipulation attacks exploiting the OF capabilities with a focus on MRHOF was presented by the authors in [1] but they do not recommend any solution to counter this attack.

The attacks are used as means to steal valuable data travelling over the network, but also to affect the networks by consuming resources such as memory, energy, processing power or permanently isolating reliable nodes from the network, disabling them from communicating. Although RPL protocol comprises some attacks defence mechanism such as: local repair and topology inconsistence detection which can help mitigate certain attacks, but its lightweight characteristics and the energy limitation does not permit the inclusion of all defence mechanisms that the traditional routing protocols have. This leaves the RPL protocol highly vulnerable. There are several different attacks on RPL performed in many ways, however, attacks such as: Hello Flooding [7], Selective-Forwarding [3], Sybil/Clone ID [8] or Neighbor attacks, cause minor damage to the network. They are only severe when coupled with other attacks. The attacks that force the network to rebuild the DODAG structure, exhausting nodes power, eavesdropping a large amount of traffic or isolating big parts of the network have a major impact on the network performance. The effort researching and studying RPL vulnerabilities and attacks is on ongoing, as a lot more needs to be done to discover new trends of attacks and countermeasures that will help improve this novel and highly vulnerable protocol. There are many studies on attacks exploiting RPL features such as rank, DODAG Information Object (DIO) messages, and nodes identity, but the literature lacks comprehensive studies on attacks targeting RPL OFs (e.g. OF0 and MRHOF).

The OF in RPL is one of the major features, influencing many others important parameters such as rank calculation, parent's selection, the construction of the entire network topology or DODAG structure. Additionally, literature comprises only two works on rank manipulation attacks as follows. The authors in [5], evaluated the performance of the rank attack on RPL network topology, and noticed that parameters such as number of DIO messages, end-to-end delay and delivery ratio significantly change when rank attacks take place. The authors suggested monitoring the alteration of those parameters as a solution to detect rank attack on RPL network. However, they did not consider exploiting OF in their rank manipulation attack. The only rank manipulation attacks exploiting the OF capabilities was presented by the authors in [1] but they did not recommend any solution to counter this attack. Additionally, they have only considered MRHOF and not OF0. Therefore, due to the high number of attacks targeting RPL and the importance of the OF in RPL, in this paper, we focus only on the vulnerability assessment of OF0 and MRHOF by considering the rank attack manipulation. To the best of our knowledge OF0's vulnerability assessments against the rank attack have not been considered in the existing work.

3. NETWORK MODEL

In this paper, we use Contiki Operating System (OS) and Cooja network simulator [12] for our experiments. Contiki [12] is a reliable and widely used open source OS for IoT devices which is fully capable of enabling the connections of tiny low-cost and low-power devices to the Internet. It also supports the RPL protocol for low-power IPv6 networking as well as the 6LowPAN adaptation layer protocol. On the other hand, Cooja [12] is a reliable and widely used network simulator capable of emulating the behavior of real IoT devices. It is the default network emulator for the Contiki OS and enables the simulation of large or small networks using Contiki sensors.

Our experiments intend to evaluate and understand the performance of an RPL protocol under rank manipulation attack using OF0 and MRHOF, in which MRHOF uses ETX. As previously stated, the construction of the RPL network topology starts with root node sending DIO messages to leaf nodes. When the nodes receive the root's message they run an algorithm to select the best parent based on the constraints and used metric defined by the OF (e.g. ETX). Once the nodes have computed their own rank, they state it on DIO message and send it to the neighboring peers. The RPL DIO message structure is depicted in Figure 1 [13]. In the rank manipulation attack, the malicious node forges its rank and propagates a lower rank to draw network traffic towards itself.

In this paper, to perform the rank manipulation attack, the RPL control message file in Cooja (rpl-icmp6) is altered to enable the malicious node advertising a fake rank (i.e. 257) in DIO message and thus deceiving the trusted nodes to send data through it.

To better understand the impact of this attack, we also study the energy consumption and the packet delivery ratio under non-malicious and malicious circumstances, using OF0 and MRHOF. In our experiments, the energy consumption is tracked using PowerTracker which is an embedded tool in Cooja to track the power consumption for each node as well as the average power consumed for the whole network. Likewise, for the Packets Delivery Ratio (PDR), we use CollectView which is also an embedded tool in Cooja to track the number of received or lost packets. The packets received are counted from the sink perspective, so the sink will always show: 0 (zero) packets received as it is not supposed to send/receive packets to/from.

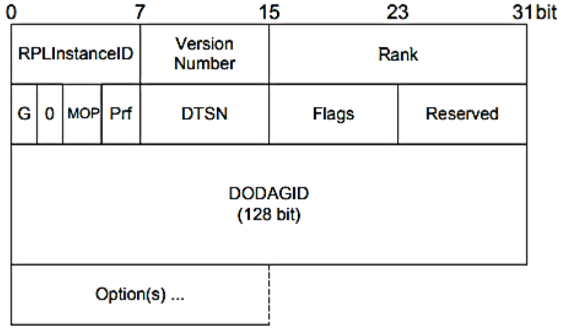

Figure 1. RPL DIO message structure [13]

Table 1. Simulation parameters

Parameters	Values
Sink node	1
Non-malicious nodes (leaves)	19
Malicious nodes	1
Sensor type	Sky mote
Objective function	OF0, MRHOF (ETX)
Simulation duration	10 minutes
Event reporting	Every 60 seconds

Our simulation environment includes 20 nodes, Table1, which consist of: a sink node (nodes: 1), 18 leaves (nodes: 2 to 20), and one malicious (node: 21)). The nodes are strategically located and once they are they will remain at the same location for all our simulations. This has been considered to make the simulation environments as close as possible to each other and avoid the effect that the different distance between nodes may have on the results obtained.

Cooja offer different mode types such as: Z1 or Sky. In this paper, we chose the Sky mote type which is ideal in terms of initial configuration as well as OS and resource capabilities.

4. RESULTS

For our experiments, we consider four scenarios as follows.

- Scenario1: Non-malicious simulation using OF0
- Scenario2: Malicious simulation using OF0
- Scenario3: Non-malicious simulation using MRHOF (ETX)
- Scenario4: Malicious simulation using MRHOF (ETX)

4.1 SIMULATION SCENARIO 1 & 2

This section includes the results obtained from scenario 1 (non-malicious scenario) and scenario 2 (malicious scenario) employing OF0 to understand the performance of OF0 on an RPL-based network.

Figure 2 represents the network layout for scenario 1 which is a non-malicious setting using OF0. The grids are distance indicators. It shows that nodes 6,7, and 8 have selected node 15 as the best parent to reach the sink (i.e. node 1) through node 16. The green lines show the path used by nodes 6, 7, 8, 15 and 16 to reach the sink. We have also captured the Average Power Consumption (APC) for scenario 1, which is 6.39%, where the sink node (i.e. node 1) has the highest APC. This is due to the fact that this node is responsible for processing all the incoming/outgoing messages for the entire IoT network.

Then the nodes: 2 (1.55%), 14 (1.46%) and 15 (1.42%) are then the ones with higher APC, all respectively. This is due to the fact that these nodes are closer to the sink node compared to the other nodes and used as the best parent for other nodes trying to reach the sink (i.e. node 1). We also captured the PDR for this scenario which is 100% due to the fact that there is no malicious node in the network to disturb the packet delivery ratio and nor the network being congested.

Figure 3 represents the network layout for scenario 2 which is a malicious setting using OF0. The malicious node is shown in pink and numbered as 21. The orange circle in Figure 3 contains the nodes effected by the rank manipulation attack. The green lines show how node 21 makes the data generated by the attracted nodes reach the sink. After introducing the malicious node to the network and due to the rank attack, node 21 attracts nodes 6, 7 and 8. Recall that, these nodes were using the trusted node 15 in scenario 1, Figure 2. Furthermore, node 21 attracts nodes 3, 4 and 5, which were using the trusted node 2 in scenario 1 to reach the sink node. Additionally, node 9 is left isolated and unable to communicate due to the rank attack. As a whole, from the 18 leaf nodes in scenario2, 7 of them chose the malicious node as the parent. This shows that the inclusion of the malicious node has an impact on 38.88% of the total nodes. The APC for scenario 2 is 6.34% and 4.74% excluding the malicious node. The sink node (i.e. node1) is the node with the highest APC which is followed by node 9 with 3.05%. We then have nodes: 2 (1.45%), 4 (1.44%), 5 (1.46%), 6 (1.43%) and 16 (1.48%) with almost identical APC. We also captured 100% PDR for scenario 2. The PDR in scenario 2 is similar to scenario 1 and it is because the inclusion of the malicious node did not affect this metric as the rank attack itself does not force the malicious node to drop any packet.

In conclusion, when we are comparing the non-malicious and malicious simulations using OF0, a decrease of 25.8% in the total APC was noticed. This is due to the malicious node deceiving several trusted nodes to select it as the parent, and thus alleviating the power consumption of some trusted nodes that were being used by those deceived nodes. The introduction of the malicious node in scenario 2, using OF0, left the node 9 isolated and unable to communicate with the other nodes and thus affecting even more the average of the packets delivered to the sink. The sink is the node with the highest APC in both scenarios as

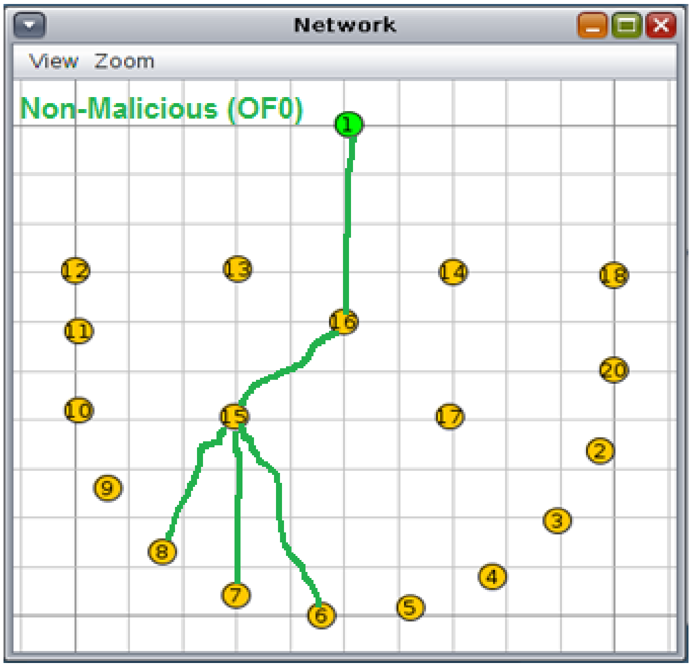

Figure 2. Network layout for scenario 1; non-malicious scenario using OF0

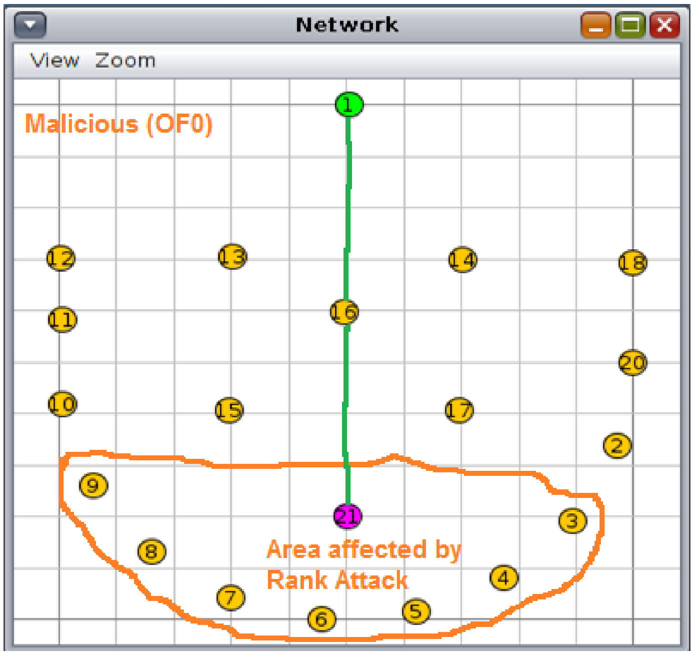

Figure 3. Network layout for scenario 2; malicious scenario using OF0

it controls and manages the entire network and has to deal with the transmission of every single packet that reaches it. The inclusion of the malicious node also decreased packets delivery success to 14.29%, affecting the overall nodes or network performance. The rank attack did not affect the PDR in both of simulations (non-malicious and malicious) using the OF0. In order for the malicious node to drop packets, the rank attack has to be coupled with other attacks such as blackhole attack.

4.2 SIMULATION SCENARIO 3 & 4

In this section, we discuss the results obtained from scenario 3 (i.e. non-malicious scenario) and scenario 4 (i.e. malicious scenario) using MRHOF to understand the performance of MRHOF on an RPL-based network.

Figure 4 represents the network layout for scenario 3 which is a non-malicious setting using MRHOF in which nodes: 6, 7, 8 and 9 have chosen node 15 as the best parent to reach the sink. Then node 15 selected node 16 as the best path to the sink (i.e. node 1). The APC for scenario 3 is 6.42%. As per scenario 1 & 2, the sink node has the highest power consumption given that all the network traffic passes via this node. Nodes: 2 (1.42%), 4 (1.41%), 14 (1.44%) and 15 (1.41%) are then the ones with the higher PCA, all respectively due to the fact that those nodes being used as the path to reach the sink. For scenario 3, the PDR remains the same (i.e. 100%) given that no lost packet has been registered.

Figure 5 represents the network layout for scenario 4 which is a malicious setting using MRHOF where a malicious node (i.e. node 21) is introduced to the network. After adding this node, all the nodes that were using node 15 to reach the sink, selected node 21 as the best path due the rank manipulation attack. As it is shown in Figure 5, the nodes: 3, 4, 5, 6, 7, 8, 9, 15 and 17 have now selected the malicious node 21 as best route to the sink. The APC for this scenario is 6.35% and 4.59%, excluding the malicious node. As seen in the non-malicious scenario, this scenario has no packet losses. Therefore, the PDR remains as 100%.

In conclusion, when using MRHOF, the APC in the malicious scenario decreased by 28.5% in comparison with the non-malicious scenario. Although both scenarios did not record any packet loss, the inclusion of the malicious node attracted 50% of the nodes to send data through it, forcing a decrease of 59% on the packets delivered to the sink. The decrease on the network performance is due to the congestion suffered by malicious node, given that 50% of the network was using this node to send data to the sink and thus consuming most of its resources.

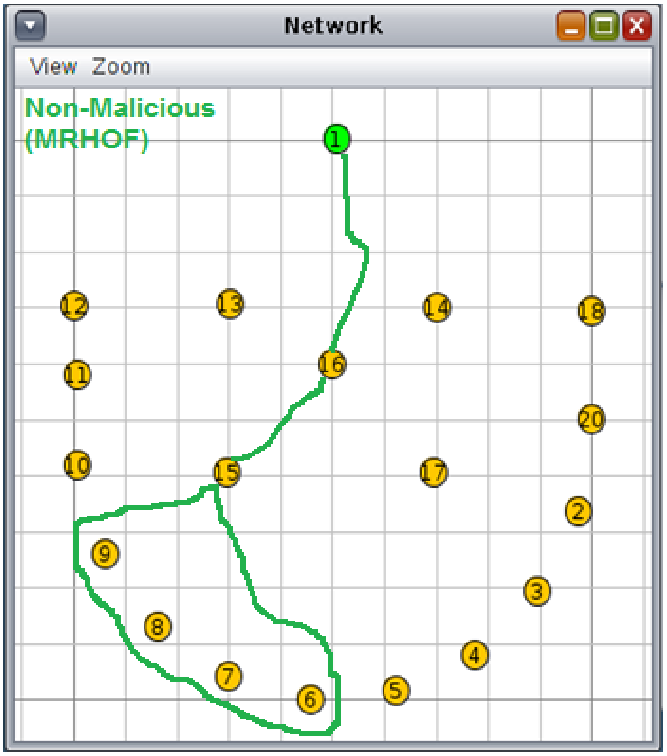

Figure 4. Network layout for scenario 3; non-malicious scenario using MRHOF

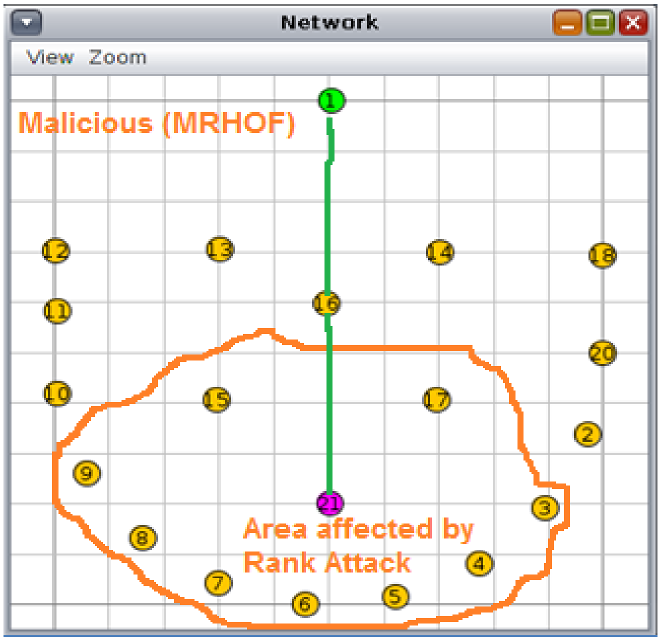

Figure 5. Network layout for scenario 3; malicious scenario using MRHOF

5. Simulation Analysis

Addressing the non-malicious scenarios, the MRHOF shows that it is more efficient in delivering packets to the sink in comparison with OF0. Overall, MRHOF delivers 45.7% more packets to the sink than OF0. This suggests that the MRHOF takes advantage of being able to use metrics (e.g. ETX) to select the best or fastest path to sink and thus greatly increasing the network performance. However, MRHOF suffered a total APC increase of 0.03%. The APC for the sink node is also increased by 0.05% when it is compared with OF0.

Addressing the malicious scenarios, MRHOF proved to be more susceptible to the rank manipulation. With MRHOF in operation, 50% of the network nodes selected the malicious node as best parent, while with the OF0 operating only 38.88% of the network was affected. On the other hand, the MRHOF delivered 21% more packets to the sink than the OF0 under the same circumstances. This confirms once again that the use of metrics favour MRHOF in improving the network performance. The OF0 also fully isolated one of the nodes disabling it from connecting or communicating with the entire network affecting the average of the packet delivery success. In terms of power consumption for the malicious scenarios, the MRHOF increased the total APC by 0.01% in comparison with OF0.

6. Conclusion and Future Work

In general, rank plays a crucial role in almost all the RPL operations, varying from optimizing topology to preventing loop or nodes' parent selection. The manipulation of such important parameters affects a great number of nodes as well as the overall network performance.

In this paper, we show that the rank attack can leave a node completely isolated from the network. Disabling a particular node from reaching the network is a severe damage to overall network performance, as this node may have other nodes that depend on it to communicate with the sink, avoiding an entire section of network from losing sensitive data. We also reveal that the rank manipulation attack is directly influenced by the efficiency of the selected OF (e.g. OF0 and MRHOF). In terms of MRHOF, which can use different metrics to improve network performance, rank attack seems more damaging or affect more nodes on the network. We monitor APC and PDR metrics to evaluate the RPL network performance in which throughput or PDR was the most affected metric by the rank manipulation attack. However, the APC did not suffer a significant increase, as this attack by itself does not drop packets in order to force nodes to continuously retransmit them leading to high power and other resource wastage. Although RPL does not embed the capability of monitoring the nodes behaviours, we suggest monitoring certain network parameters such as PDR, APC, and overhead that may suffer a significant change when rank manipulation attack is coupled with other attacks (e.g. blackhole attack or version attack). In general, our future work is focused on employing techniques such as machine learning and data mining to detect rank attack using OF0 and MRHOF.

REFERENCES

[1] Rehman, A., Khan, M. M., Lodhi, M. A., & Hussain, F. B. (2016). Rank attack using the objective function in RPL for low power and lossy networks. 2016 International Conference on Industrial Informatics and Computer Systems, CIICS 2016. https://doi.org/10.1109/ICCSII.2016.7462418.

[2] Richardson, M., & Robles, I. (2012). RPL- Routing over Low Power and Lossy Networks. Retrieved 19 November 2017, from https://www.ietf.org/proceedings/94/slides/slides-94-rtgarea-2.pdf

[3] Kamble, A., Malemath, V. S., & Patil, D. (2017, February). Security attacks and secure routing protocols in RPL-based Internet of Things: Survey. In Emerging Trends & Innovation in ICT (ICEI), 2017 International Conference on (pp. 33-39). IEEE.

[4] L.Anhtuan, L. Jonathan, and L. Aboubaker,"The Impacts of Internal Threats towards Routing Protocol for Low power and lossy Network Performance".IEEE Symposium on Comupters and Communication, Split,July 2013.

[5] Le, A., Loo, J., Lasebae, A., Vinel, A., Chen, Y., & Chai, M. (2013). The impact of rank attack on network topology of routing protocol for low-power and lossy networks. IEEE Sensors Journal, 13(10), 3685-3692.

[6] L. Anhtuan, L. Jonathan, and L. Aboubaker, "The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and LossyNetworks".IEEE Sensor Journal, Vol. 13, PP. 3685-3692, 2013.

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

[8] 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.

[9] Dvir, A., & Buttyan, L. (2011, October). VeRA-version number and rank authentication in rpl. In Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on(pp. 709-714). IEEE.

[10] Ahmed, F., & Ko, Y. B. (2016). Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks. Security and Communication Networks, 9(18), 5143-5154.

[11] Pongle, P., & Chavan, G. (2015). Real time intrusion and wormhole attack detection in internet of things. International Journal of Computer Applications, 121(9).

[12] Contiki Operating Systems and Cooja Netwrok Simulator, availabe at: http://www.contiki-os.org/index.html, last accessed: 12 June 2019.

[13] Tsvetkov, T., & Klein, A. (2011). RPL: IPv6 routing protocol for low power and lossy networks. Network, 59.