AN EXPERIMENTAL STUDY OF IOT NETWORKS UNDER INTERNAL ROUTING ATTACK

Mohammad Alreshoodi

Applied Science Department, Unizah Community College,
Qassim University, Qassim, Saudi Arabia

ABSTRACT

Internet of Things (IoT) deployments mostly relies on the establishment of Low-Power and Lossy Networks (LLNs) among a large number of constraint devices. The Internet Engineering Task Force (IETF) provides an effective IPv6-based LLN routing protocol, namely the IPv6 Routing Protocol for Low Power and Lossy Network (RPL). RPL provides adequate protection against external security attacks but stays vulnerable to internal routing attacks such as a rank attack. Malicious RPL nodes can carry out a rank attack in different forms and cause serious network performance degradation. An experimental study of the impact of the decreased rank attack on the overall network performance is presented in this paper. In also besides, it is important to understand the main influencing factors in this context. In this study, several some many network scenarios were considered with varying network sizes, attacker properties, and topological setups. The experimental results indicate a noticeable adverse effect of the rank attack on the average PDR, delay, ETX, and beacon interval. However, such impact was varied according to network size, attacker position, attacker neighbor count, number of attack-affected nodes, and overall hops increase. The results give a practical reference to the overall performance of RPL networks under rank attacks.

KEYWORDS

Security; Routing Attack; RPL; Routing Protocols; Internet of Things.

1. INTRODUCTION

There has been a growing interest in the Internet of Things (IoT) technology and expanding deployments in varying IoT domains including industry, healthcare, transportation, and education. The main network requirements in most of these deployments rely on the establishment of underlying networking infrastructures of energy-efficient and low-power communications. Thus, Low-Power and Lossy Networks (LLNs) provide such a need with low-cost and less-complex deployments. LLNs enable effective connectivity among many small-sized and resource-limited IoT devices that are wirelessly interconnected.

The Internet Engineering Task Force (IETF) provides a customized and effective LLN routing protocol.That is the IPv6 Routing Protocol for Low Power and Lossy Network (RPL), which enables IoT networks with IPv6 routing. RPL has been designed to provide simple and structured network topologies with loop-free routing. It also facilitates flexible routing customization to fulfil certain network requirements for the different IoT applications. To this end, RPL provides a routing solution that relies on a customizable objective function considering the different requirements of the different IoT applications. Such an RPL property dictates two main routing parameters, node rank, and routing version.

DOI: 10.5121/ijcnc.2020.12406

However, such properties make RPL vulnerable to different internal routing attacks. These primarily include the RPL rank attack and version attack. That is, the original RPL protocol specification has no security support against such types of routing attacks. It only provides limited support to protect the RPL network from external security attacks [1].

Malicious nodes joining an RPL network can easily perform the rank attack in any form. These include increasing or decreasing its rank in order to affect the stability of the RPL topology and cause network convergence to suboptimal routing paths. For carrying out a rank attack, a malicious RPL node would increase its rank value and then advertise it in the network. As a result, routing inconsistency would be incurred, and the network topology would be reformed partially or completely. Such attacks can incur additional network and processing overhead and would lead to a degradation in the network performance. Therefore, it is important to understand how much such kinds of attacks would affect the overall performance of the network.

This research work contributes to an experimental study of a critical internal routing attack in IPv6-based IoT networks. The main objective is to help in understanding how much the network performance would be affected in the case of the decreased rank attack. Many network scenarios were considered with varying network size, attacker position, attacker's neighbour count, number of attack-affected nodes, and overall hop increase. The experimental results indicate a noticeable an impact of the rank attack on the network performance in terms of average PDR, end-to-end delay, ETX, and beacon interval. However, there was variation in such impact among the different considered scenarios. The results can be taken as an effective reference to provide additional security support for RPL against internal routing attacks.

The following section of this paper provides a protocol overview of the standard RPL and describes the main internal routing attacks of RPL. Section III presents an overview of the related work. In Section IV, the experimental setup for evaluating the considered security attacks is described. Section V presents and discussed the obtained evaluation results. The conclusion of this work is provided in Section VI.

2. THE RPL PROTOCOL

2.1. Protocol Overview

RPL facilitates an effective solution for network layer routing based on the distance vector approach. It runs on top of IPv6 over Low Power Wireless Personal Area Networks (6LowPAN) which provides the integration layer with IPv6 networks (RFC 4944 [2] and RFC 6282 [3]). The design of RPL enables a routing framework that allows different routing objectives to be implemented according to certain application requirements. Thus, RPL provides flexible support to meet the requirements of a wide range of IoT applications.

A typical RPL network consists of a set of RPL instances while each one is structured with one or multiple Destinations-Oriented Directed Acyclic Graph (DODAGs). Figure 1 presents an example of an RPL network with one instance having two DODAGs. The network topology of each DODAG has a single sink node interconnecting a number of some RPL nodes with amultihop connectivity.

The routing process among the nodes in a DODAG is based on a customizable routing Objective Function (OF). RPL enables defining an OF with a set of routing metrics to meet certain network routing requirements as defined in RFC 6551 [4]. The default is for RPL are OF0 (Objective Function Zero) [5] and MRHOF (Minimum Rank with Hysteresis Objective Function) [6]. The former is based on the hop count metric whereas the latter uses the Estimated Transmission Count (ETX) metric that relies on the number of transmissions necessary for successful packet delivery. The OF enables the selection of a parent for data packet routing over an optimal path across the network.

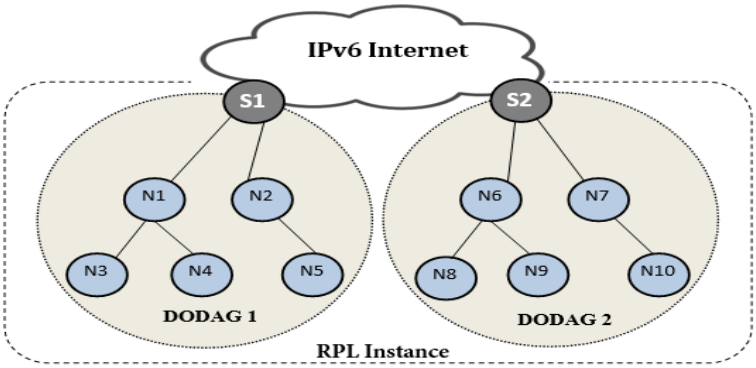

Figure 1. An RPL network of one instance having two DODAGs

2.2. RPL Operations

DODAG establishment is initiated by the sink node broadcasting a control message denoted as DODAG Information Object (DIO). This message contains certain parameters required for the discovery and maintenance of the DODAG. A node receiving such a message can join the advertised DODAG, after calculating its rank and nominating a preferred parent using the propagated OF. The DIO recipient further rebroadcasts the message, and the process continues until having upward routes completely established.

Upon the reception of the DIO messages, the nodes reply with Destination Advertisement Object (DAO) messages over the established upward route up to the sink node. Certain routing information including the node's IPv6 address is contained in the DAO message. As a result, the downward routes across the network are established for internal RPL routing. Besides, a node can request DIO transmission by sending a DODAG Information Solicitation (DIS) message. On the other hand, RPL relies on the Trickle algorithm [7] to reduce control traffic. The algorithm is based on controlling the time between DIO transmissions according to network stability. The time is exponentially increased as long as there is no changes in the network topology.

Moreover, RPL incorporates two procedures for addressing node or link failure. One is the local repair that enables a node to change its current preferred parent or switch to an alternative neighbor node. Global repair requires the sink node to rebuild its DODAG. These procedures are based on exchanging many DIS and DIO messages after resetting the trickle timer. This approach would allow for effective failure recovery but at the cost of additional network overhead.

2.3. RPL Rank Attack

In each DODAG, a single OF can be advertised to be then used by a receiving node for calculating its rank in the network and selecting its preferred parent. The rank specifies node-to-sink distance and indicates the position of a node in the network.

RPL relies on the rank property for performing loop-free routing in RPL networks. It requires the rank to increase in the downward direction from the sink node to the leaf nodes. Thus, a node can only select those of lower rank among its neighbour nodes as its preferred parent. However, the rank property can be used by a malicious node to initiate an internal routing attack. Without strict adherence to such rules, the node can select a node of a higher rank as its preferred parent. As a result, sub-optimal topology would be formed. Data packets routed through the node would traverse a network path of lower performance.

It is also possible to have a malicious node increases its ranks at some point after joining an RPL network. This would incur unwanted routing loops affecting in particular those in the sub-DODAG of the node. Such an attack can also drain node resources in the case of large network deployments. In other cases, a malicious node can initiate a rank attack by decreasing its rank. This would make it a better parent candidate for most of its neighbour nodes. They would then move their current preferred parent selection to the node. As a result, the node can further initiate other security attacks such as blackhole attack and make the situation worse. In all these different forms of rank attack, network stability would be adversely affected, and overall network performance would be degraded.

3. RELATED WORK

The IETF has specified the RPL in RFC 1111 [8] with consideration of specific security aspects. These only provide essential security mechanisms against external attack. Three basic security modes were specified for RPL. The first is the insecure mode in which RPL communications are performed with no security mechanisms. In the preinstalled mode, RPL nodes have preinstalled keys that are used to secure RPL Communications. The third one, the authentication mode, requires nodes to have a key from an RPL authentication authority before joining an RPL network.

However, the standard RPL specification includes no consideration of internal routing attacks such as rank attack. Malicious nodes can easily join an RPL network and initiate a routing attack to adversely affect network performance. Therefore, varying research efforts have been made to review the potential security attacks for RPL. In [9, 10], RPL attacks were classified into those targeting network resources, network topology, and network traffic. For example, version, rank, and DAG inconsistency attacks were classified as network resource attacks whereas worse parent attack was categorized as network topology attack. Moreover, different studies were conducted to examine the performance of RPL under various internal attacks.

RPL is exposed to a number of internal routing attacks. Some of these were common security attacks such as selective forwarding, sinkhole, blackhole, Sybil, flooding, and clone ID attacks. The impact of these attacks on network performance was analzsed in [11]. The simulation results showed that low network throughput was achieved when the network under the attacks. The evaluation results in [12, 13] demonstrated that blackhole-attacked RPL networks experienced low

PDR in addition to the high delay, power consumption, packet loss, and network overhead. In [14], a performance study over a real-testbed RPL network setup illustrated how packet loss increased in the case of a wormhole attack.

Others specified other attacks more specific to RPL such as rank, version, worst parent, OF, DAG inconsistency, and local repair attacks [15-17]. The version attack was considered in [18] for analyzing its impact on RPL networks. As indicated by simulation results, the attack resulted in decreased PDR and increased delay and network overhead. The version attack also caused an increase in power consumption as demonstrated by the evaluation results in [19]. In the performance study presented by [20], it was observed that the worst parent attack in RPL networks led to low PDR and high delay and overhead. The evaluation results in [21] showed that local repair attacks in RPL networks caused an increase in end-to-end delay and a decrease in PDR.

A rank attacks can be initiated with increasing or decreasing rank. According to the simulation results showed in [22], the increased rank attack caused RPL networks to experience high power consumption and network overhead in addition to low beacon interval. The results also showed that decreased rank attack led to high ETX and power consumption in addition to low beacon interval. The study also illustrated how the rank attack would open the doors for further attacks in RPL networks. This was presented in an RPL attack graph that indicates the vulnerabilities of the RPL rank property. For example, a decreased rank attack can be initially conducted in order to then carry out different traffic attacks. such as selective forwarding attack. Such a combination was considered in a simulated RPL setup and the results showed that the attack increased ETX and packet loss in the network.

4. EXPERIMENTAL SETUP

Contiki OS is an open-source operating system for resource-constrained IoT devices. It implements an IPv6-based network protocol stack providing effective IP connectivity to the Internet. Such a stack incorporates both the 6LowPAN adaptation mechanism and the RPL routing protocol. Its latest version, Contiki 3.0, was adopted for the implementation of this work. The Contiki OS implementation [23] can be effectively used to emulate different IoT setups. This was facilitated by the Cooja Simulator, one of the tools provided by Contiki OS. It enables creating and running emulations of various IoT scenarios using different types of nodes that run the Contiki OS implementation.

In this work, the Cooja Simulator was used to differently emulate an RPL instance in varying RPL rank attack scenarios. The instance consists of one DODAG containing a single sink node and a collection of 35 sensor nodes, as presented in Figure 2. Each RPL node was emulated in Cooja as a Sky Mote device. The sink node also operates as a UDP server, in addition to running the Cooja Collect View that collects information of all the sensor nodes in the network. Each sensor node also operates as a UDP sender, regularly sending IoT data at an interval of ±10 seconds. The nodes were placed randomly in an area of more than 200×200m. Multihop network topology was formed among all the nodes. The communication and interference ranges were set to 25m and 50m, respectively, for all the nodes.

The current Contiki OS implementation supports both Objective Functions of RPL. In this experiment, MRHOF with the Expected Transmission Count (ETX) as a routing metric was adopted. The RPL implementation was also modified for the attacking nodes to trigger a decreased rank attack after 5 minutes of the simulation start time.

Multiple simulation setups were created to run the legitimate RPL implementation and varying rank attack scenarios. Each simulation setup was run 10 times and the average of the results was then taken. Each run lasted for a simulation time of 15 minutes. In each rank attack scenario, the same number of RPL nodes was implemented but the attack position was randomly varied. In addition, different nodes of the varying neighbour count were considered to carry out the decreased rank attack. Accordingly, the number of potential nodes to be affected by the attack was varied. Figure 3 shows one of the scenarios in which Node 35 was set to be the attacking node. The node had a hop count of 3 and a total of 5 neighbour nodes. It can also be seen that there were about 8 attack-affected nodes. Figure 4 indicates the considered nodes to carry out the attacks and presents the hop count and the number of neighbour nodes for each attacker.

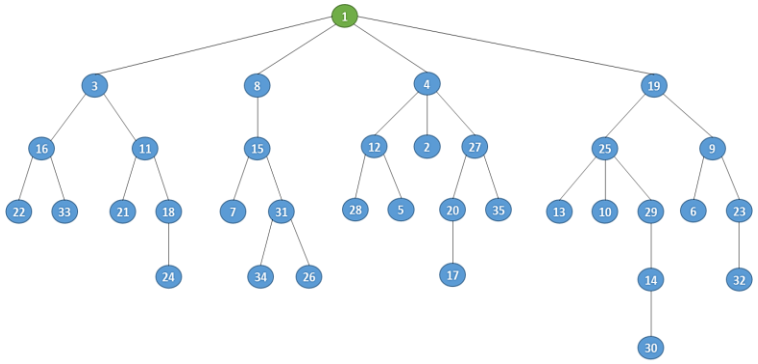

Figure 2. The considered RPL Network Topology in this Study

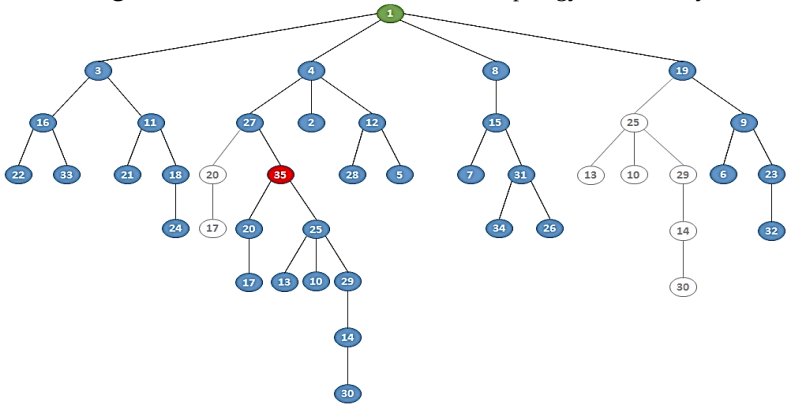

Figure 3. The resulted Network Topology after Node 35 attack

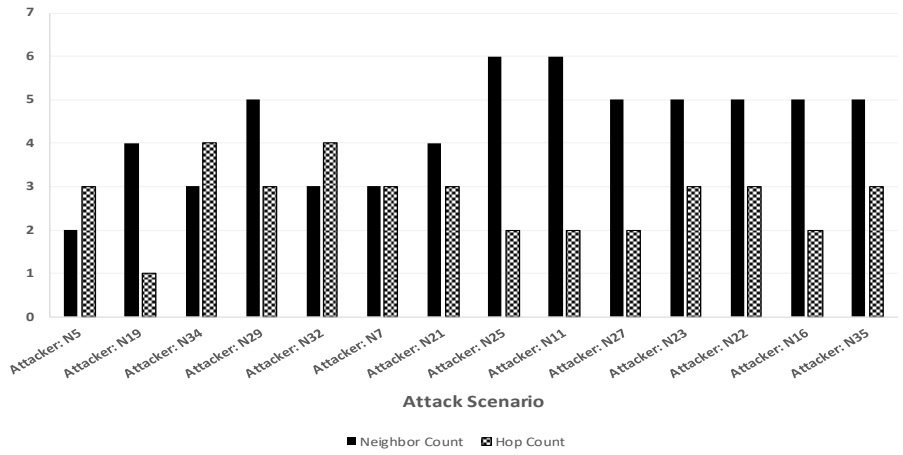

Figure 4. Neighbor Count and Hop Count of the Attacking Nodes

After completing these scenarios, the simulation setup was modified to increase the size of the RPL network. Additional 15 nodes were added in different topological positions across the network. This has resulted in a new network topology with higher node intensity and a larger simulation area. Accordingly, the count of the neighbor nodes and the number of attack-affected nodes increased for most of the attacking nodes. New simulation scenarios were then carried out considering some of the attacking nodes considered in the previous scenarios. These were namely the nodes: N5, N16, N21, N25, and N35.

The evaluation was based on measuring the RPL network performance during different decreased rank attack setups, to be then compared with the RPL network performance in a normal setup with no attacking node. The performance measurement parameters considered in this study were an average end-to-end delay, Packet Delivery Ratio (PDR), the ETX routing metric, and beacon interval. The average end-to-end delay is calculated as the average time taken by the transmitted packets to reach the UDP server running at the sink node. The average PDR is the ratio of all the transmitted packets that are received by the UDP server. The ETX is the number of transmissions and retransmissions required by the nodes for the successful delivery of data packets. Beacon interval indicates topology stability and lower beacon interval means that higher updates overhead in the network.

5. RESULT AND DISCUSSION

Table 1 shows the overall network performance in terms of the average PDR, end-to-end delay, and ETX for each of the considered scenarios. It can be seen that the network without any attack performed well with a relatively high PDR and low delay and ETX. In this scenario, the network achieved an average PDR of 98.89% and experienced an average delay of 104 ms. The overall ETX calculated by the RPL nodes was less than the value of 205.

Table 1. Overall Performance of the Different Scenarios

Attack Scenario	PDR (%)	Delay (ms)	ETX
No-Attack	98.881	104.063	204.66
Attacking Node: N5	97.590	108.039	209.177
Attacking Node: N7	92.016	126.427	231.884
Attacking Node: N11	89.767	118.072	240.702
Attacking Node: N16	82.642	145.328	260.764
Attacking Node: N19	97.001	106.318	211.349
Attacking Node: N21	91.694	127.461	233.046
Attacking Node: N22	83.263	157.940	253.787
Attacking Node: N23	85.253	142.231	249.076
Attacking Node: N25	90.975	129.744	237.335
Attacking Node: N27	86.627	138.954	246.491
Attacking Node: N29	94.952	111.676	225.399
Attacking Node: N32	94.616	125.356	226.240
Attacking Node: N34	95.610	117.127	223.536
Attacking Node: N35	81.053	164.586	268.038

5.1. Impact of Node Position and Neighbour Count

When it was under the different attacks, the network became affected and overall performance started to degrade. When the attack started after 5 sec of the simulation time, the PDR decreased and the delay increased as shown in Figures 5 and 6, respectively. This happened gradually with initial changes to the performance during the initial 40 seconds of the attack time. This was the required time for the attack to have its effect on the network.

However, there was a noticeable variation in performance degradation considering the different attack scenarios. In one example scenario (Attacking Node: N5), the PDR, delay, and ETX were degraded by 1.3, 3.9, 4.5%, respectively. In another scenario (Attacking Node: N21), a PDR reduction of 7.2% was observed in addition to increases in the delay and ETX of 23.4% and 28.4%, respectively. In general, it can be observed that the reduction in PDR reached 17.8% whereas an increase of more than 60% was experienced in the measured delay and ETX.

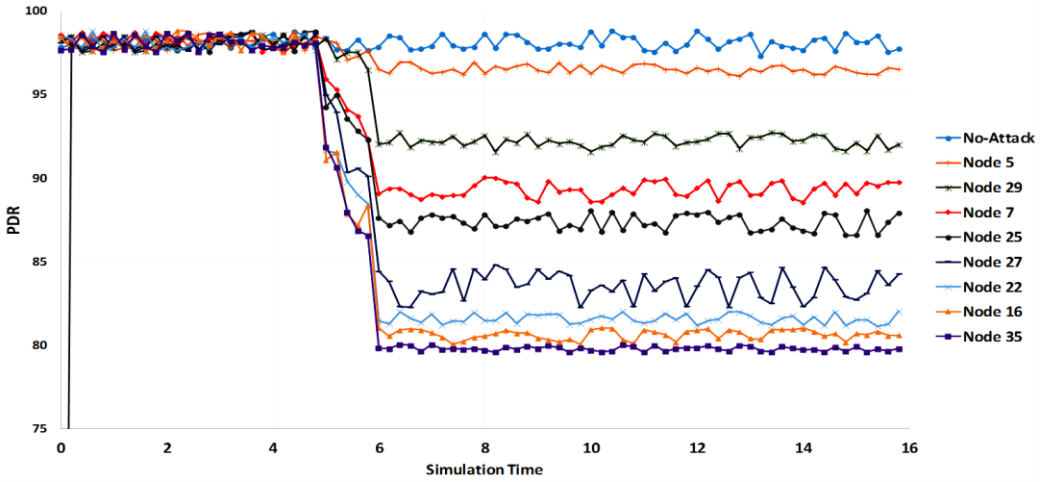

Figure 5. Average PDR Results of Selected Scenarios

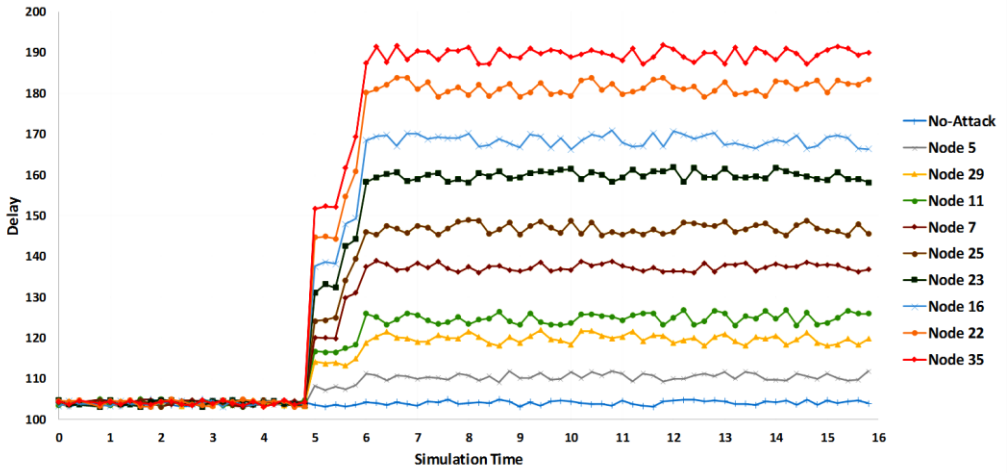

Figure 6. Average Delay Results of Selected Scenarios

That was highly dependent on different aspects of the attacking nodes such as their position (hop count) and neighbour count. Another important consideration is the topological effect of the attack, in regards to the number of affected nodes and the resulted overall hop increase. For example, all these properties were similar in the scenarios where the attacking nodes were N23 and N27. Therefore, it can be seen that very close network performance degradation was experienced. Comparing the situations in the scenarios where the attacking nodes were N7, N21, and N25, all the attacking nodes shared the same number of affected nodes and overall hop increase, thus the network experienced similar performance degradation. However, the network was relatively more affected when the attacking node was N25 as it relatively has a higher neighbour count and located in a higher position. On the other hand, we can observe that the results are extremely varied when the attacking nodes were N11 and N16. Both attackers shared the same position but N11 had more neighbour count whereas N16 affected more nodes and caused higher hop increase. It is evident that the network performed better in the former case.

5.2. Impact of Topological Changes after the Attack

The variation in the delay results was mainly dependent on the resulted overall hop increase after the attack. Table 2 shows the overall hop increase for each scenario, in addition to the number of attack-affected nodes and those with hop increase of one and two hops. In the scenarios where the attacking nodes were N22 and N35, the attack resulted in high overall hop increases of 12 and 14 hops, respectively. This led to relative increases of more than 50% in the overall delay. In the scenarios where the resulted overall hope increase was 4 hops (Attacking Node: N7, N21, N25, N32), the increases in the experienced delay were within a very close range. Comparing these four scenarios, the network experienced a relatively higher delay when the attacking node was N25 as it also had a higher neighbour count and topological position. On the other hand, a delay increase of less than 8% was experienced in the scenarios where the increase in the hops was two or less (Attacking Node: N19, N5, N29). Although there was no hop increase at all in the scenario where the attacking node was N19, a very little increase in the delay was experienced since the attacker node has a high neighbour count and a number of affected nodes.

Table 2. Calculations of the Number of Affected Nodes and Hop Increase in Different Scenarios

Attack Scenario	# of Affected Nodes	# of Nodes Hop Inc. (+1)	# of Nodes Hop Inc. (+2)	Overall Hop Inc.
No-Attack	0	0	0	0
Attacking Node: N5	1	1	0	1
Attacking Node: N19	5	0	0	0
Attacking Node: N34	2	1	1	3
Attacking Node: N29	3	2	0	2
Attacking Node: N32	2	0	2	4
Attacking Node: N7	4	4	0	4
Attacking Node: N21	4	4	0	4
Attacking Node: N25	4	4	0	4
Attacking Node: N11	5	3	0	3
Attacking Node: N27	7	7	0	7
Attacking Node: N23	5	1	4	9
Attacking Node: N22	7	2	5	12
Attacking Node: N16	9	9	0	9
Attacking Node: N35	8	2	6	14

Another important measure that can be considered in this context is the duration of the beacon interval. It is given that frequent network updates would decrease beacon intervals whereas fewer

updates across the network lead to long beacon intervals. Since the attack would incur routing updates and topological changes, the beacon interval would then decrease as shown in Figure 7. The more the nodes that is affected and involved in the situation the more beacons would be broadcasted in the network. An illustrative example is the cases when N16 and N27 were the attackers and the resulted overall beacon intervals were the lowest. This was due to the higher position of the attackers in the network in addition to having high u count and more nodes in their sub-DODAGs. It can also be seen that the beacon interval was reduced by almost 20% in the scenario where N19 was attacking, although less performance degradation was experienced during that scenario. This was due to the very high network position of the attacker and the large size of its sub-DODAG, but a very limited number of nodes affected by the attack and very low overall hop increase. On the other hand, the overall beacon interval decreased by than 5% when the attacker had a sub-DODAG of two or fewer nodes and positioned in a low level of the network.

5.3. Impact of Network Size

Another critical consideration in this study is the impact of network size on the rank attack. After adding more RPL nodes to the topology, it was noticed that neighbour count and the number of attack-affected nodes increased for the considered attacking nodes. This was has also resulted in a higher overall hop increase in all the scenarios. Compared to the results of the overall performance with the original network size, the new setup caused additional network performance degradation. There was an overall decrease of approximately 3% on the average PDR results and an increase of approximately 2% on the average delay. It could also be observed that the overall ETX relatively increased and the beacon interval relatively decreased as a result of increasing network intensity. Therefore, the larger the size of the rank-attacked RPL network the higher the overall network performance degradation. In the case of having Node 35 as the attacker, for example, the neighbour count and the number of affected nodes increased to 7 and 10, respectively. In addition, there was an increase of 3 hops to the overall hop increase. As a result, the average PDR decreased by 2.6% as shown in Figure 8. There was also an increase of 1.9% and 1.7% on the average delay and ETX, respectively, and a decrease of 2.1% on the overall beacon interval.

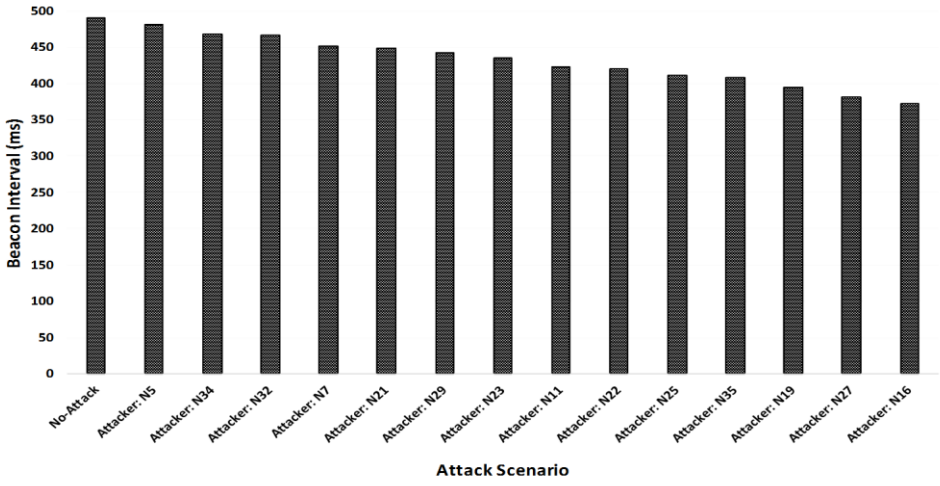

Figure 7. Average Beacon Interval Results

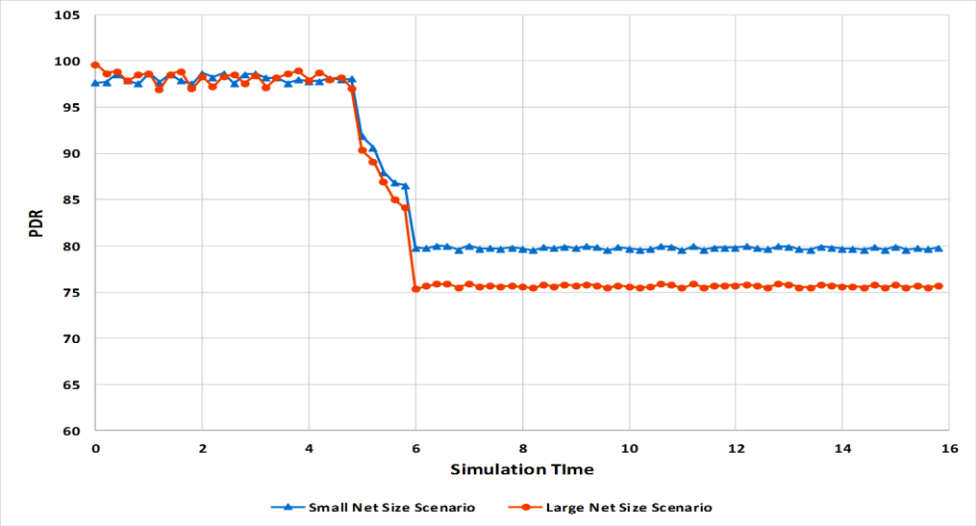

Figure 8. Average PDR Results for Node 35 Rank Attacking Scenarios

6. CONCLUSIONS

The vulnerability of the IPv6-based IoT network running the RPL routing protocol is evident. RPL provides no security support for network protection against different internal routing attacks. The experimental study presented in this paper provides a practical understanding of the performance of IPv6-based IoT networks under rank attacks. The results can serve as an effective reference to deeply comprehend rank-attacked RPL networks towards the development of effective Intrusion Detection Systems (IDSs). Different insights can be drawn in this regard.

It is evident that performance degradation in terms of PDR, delay, and ETX would be experienced during the attack. Beacon broadcasting would also increase and cause higher resource consumption. Such effects were highly correlated with certain properties of the attacker node. As the attacking node has less hop count and more neighbours, the network performance would be more adversely affected by the attack. The higher the number of affected nodes and overall hop increases the higher the average delay in the network. Nodes attacking at higher positions in the network with large-sized subnet would incur more routing updates reducing beacon intervals and draining node resources. In addition, such an attack effect on the overall network performance would be amplified by increasing network size.

These implications resulted from the rank attack in RPL-based IoT networks make it critical to develop more secure routing mechanisms. This is evident as the integrity of the RPL control messages, which include the rank information, can be easily compromised. However, IoT devices are of limited capabilities and operate in low power and lossy networks, thus lightweight solution should be considered in this context. Addressing such considerations in an effective routing security solution is the main objective for future work. A machine learning-based IDS solution will be developed according to a centric deployment approach

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano andM. Richardson, "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)," IETF RFC 7416, Jan 2015. available: https://tools.ietf.org/html/rfc7416.

[2] N. Kushalnagar, G. Montenegro, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," IETF RFC 4944, September 2007.

[3] J. Hui and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," IETF RFC 6282, September 2011.

[4] J. Vasseur, M. Kim, K. Pister, N. Dejean, and D. Barthel, "Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks," IETF RFC 6551, March 2012.

[5] P. Thubert, "Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)," IETF RFC 6552, March 2012.

[6] O. Gnawali and P. Levis, "The Minimum Rank with Hysteresis Objective Function," IETF RFC 6719, September 2012.

[7] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko, "The Trickle Algorithm," IETF RFC 6206, March 2011.

[8] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik,J. P. Vasseurand, and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," IETF RFC 6550, March 2012

[9] A. Mayzaud, R. Badonnel, I. Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things," International Journal of Network Security (IJNS), Vol. 18, No. 3, 2016, pp. 459-473.

[10] B. Al Absi, "A Comprehensive Review on Security Attacks in Dynamic Wireless Sensor Networks based on RPL protocol," International Journal of Pure and Applied Mathematics, Vol. 118 No. 20, 2018, pp. 653-667.

[11] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures," IEEE Communications Surveys & Tutorials (in press).

[12] A. Verma and V. Ranga, "Analysis of routing attacks on RPL based 6LoWPAN networks," International Journal of Grid and Distributed Computing, Vol. 11, No. 8, 2018, pp. 43-56.

[13] A. Kumar, R. Matam and S. Shukla, "Impact of packet dropping attacks on RPL," In Proc. the *4th International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Waknaghat, India, Dec. 2016, pp. 694-698.

[14] P. Perazzo, C. Vallati, D. Varano, G. Anastasi and G. Dini, "Implementation of a wormhole attack against a rpl network: Challenges and effects," *In Proc. the 14th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, Isola, France, Feb 2018, pp. 95-102.

[15] P. O. Kamgueu, E Nataf, and T. D. Ndie, "Survey on RPL enhancements: A focus on topology, security and mobility," *Computer Communications,* Vol. 120, 2018, pp.10-21.

[16] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," *In Proc the International Conference on Pervasive Computing (ICPC)*, Pune, India, Jan 2015, pp. 1-6,

[17] A. Rehman, M. M. Khan, M. A. Lodhi and F. B. Hussain, "Rank attack using objective function in RPL for low power and lossy networks," In Proc. The International Conference on Industrial Informatics and Computer Systems (CIICS), Sharjah, UAE, March 2016, pp. 1-5.

[18] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, J. Schönwälder, "A Study of RPL DODAG Version Attacks," In: Sperotto A., Doyen G., Latré S., Charalambides M., Stiller B. (eds) Monitoring and Securing Virtualized Networks and Services. AIMS 2014. Lecture Notes in Computer Science, vol 8508. Springer, Berlin, Heidelberg, 2014, pp. 92–104.

[19] A. Aris, S. F. Oktug and S. Berna Ors Yalcin, "RPL version number attacks: In-depth study," *In Proc. The IEEE/IFIP Network Operations and Management Symposium*, Istanbul, Turkey, April 2016, pp. 776-779.

[20] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen and M. Chai, "The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks," *IEEE Sensors Journal*, vol. 13, no. 10, Oct. 2013, pp. 3685-3692.

[21] A. Le, J. Loo, Y. Luo and A. Lasebae, "The impacts of internal threats towards Routing Protocol for Low power and lossy network performance," *In Proc. The IEEE Symposium on Computers and Communications (ISCC)*, Split, Croatia, July 2013, pp. 789-794.

[22] R. Sahay, G. Geethakumari and K. Modugu, "Attack graph — Based vulnerability assessment of rank property in RPL-6LOWPAN in IoT," *In Proc. the IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, Singapore, Feb 2018, pp. 308-313.

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