

Performance evaluation of rank attack impact on routing protocol in low-power and lossy networks

Laila Al-Qaisi, Suhaidi Hassan, Nur Haryani Zakaria

InterNetWorks Research Laboratory, School of Computing, Universiti Utara Malaysia, Kedah Darul Aman, Malaysia

Article Info

Article history:

Received Feb 4, 2024

Revised May 21, 2024

Accepted Jun 5, 2024

Keywords:

Impact analysis

IoT

Routing security

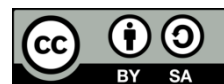
RPL attack

WSN

ABSTRACT

The internet of things (IoT) is a network of connected devices, enabling the exchange and collection of data from various environments. The routing protocol for low power and lossy networks (RPL) is a protocol for routing IPv6 over low-power wireless personal area networks, commonly used in IoT applications. However, RPL has several security and privacy issues that make it vulnerable to various attacks, including rank attacks (RA), which can lead to denial-of-service (DoS) scenarios. This research aims to address the impact of RA on RPL networks by conducting simulations using the Contiki/Cooja simulator with two topology types, random and grid, along with three RA scenarios and a normal network scenario. The study compares the performance of RPL network OF0 and MRHOF in terms of throughput, packet delivery ratio (PDR), hop count (HC) and delay. The results demonstrate that RA significantly degrades network performance and reduces network lifetime, thus draining its limited resources. Some possible solutions are also suggested to mitigate these attacks by focusing on core components of the network like objective function (OF) and node behavior. Future work will focus on studying security mechanisms for RPL against RA.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Laila Al-Qaisi

InterNetWorks Research Laboratory, School of Computing, Universiti Utara Malaysia

Sintok Kedah Darul Aman 06010, Malaysia

Email: layla_mohammad@ahsgs.uum.edu.my

1. INTRODUCTION

The fast-growing internet of things (IoT) field, which had 50 billion devices by 2020, affects daily life [1]. IoT is expected to have a 3.9 trillion to 11.1 trillion annual economic impact by 2025 [2]. Due to the rapid expansion of communications and information technologies, neighboring environment sensing systems have changed.

In most IoT deployment scenarios, including smart cities, homes, industry, agriculture, medical applications, and more, wireless communication and the Internet connect widespread devices. Wireless sensor networks (WSN) drive IoT growth. According to [3], WSN sensor nodes have restricted power, computation, and transmission. For sensor nodes to be IoT-compatible and enable WSN communication, the internet engineering task force (IETF) ratified IPv6.

According to Aljarrah *et al.* [4], the IETF ratified a low-power routing protocol (RPL) for IPv6 WSN connections. Traditional routing techniques in WSNs with modest sensors cannot efficiently route messages. Thus, IPv6 networks use RPL to solve difficult configuration, routing table extension, and security issues [5]. Despite its suitability for many IoT applications, Kharrufa *et al.* [6] found that RPL is vulnerable to many attacks.

The RPL is primarily vulnerable to attacks such as rank, blackhole, sybil, and wormhole due to topology construction design issues [7]. The main obstacle of using RPL practically in real-world IoT applications with all of these attacks. Even with the protection provided by the MAC layer, internal attacks remain a major issue with RPL.

According to Airehrour *et al.* [8], the rank attribute is crucial for all RPL operations. Its main benefits are optimal topology, loop prevention, and control overhead management. The biggest issue is that attacks violating rank attribute can potentially damage RPL performance. Security attacks like rank attack (RA) can affect low power and lossy networks (LLN) routing system efficiency.

A disruptive attack that can quickly create a fake topology and cause adjacent nodes to reroute traffic toward the attacker node is the RA. While earlier studies have explored it in great detail [6], they have not explicitly addressed RA different scenarios influence on variant RPL network topologies. Furthermore, no study addresses how the RPL networks enable this attack. Research studies focused on mitigation techniques rather than investigating the impact RA encounter on RPL performance [9].

This gave us the motivation to carry out this study and close the noted research gap. The major contributions of our work include: thorough discussion of the three scenarios of RA that may occur, an in-depth comparative analysis will be presented to target the impact of each RA scenarios on the network topology and some possible proposed solutions to work on to prevent this kind of attack from occurring in the network.

The remainder of this paper is organized as follows: Section 2 reviews the background of RPL, OF, RA, and related works. Section 3 explains the research method. In section 4 explains the experiment setup and evaluation criteria along with the simulation scenarios, which are deployed to build experiments and results analysis. Finally, section 5 draws the concluding remarks and future work.

2. BACKGROUND

2.1. RPL protocol

RPL is an IPv6 distance vector protocol for low-power and lossy networks (LLN) devices like IoT. These devices have memory, processor, and power limits. RPL was designed to adapt to changing network conditions and provide alternative routes when the default ones are unavailable for any reason. RPL is a proactive routing protocol that creates a topology depending on the distance between source and sink nodes, as described in [10].

As discussed in [11], RPL builds a structure tree, or destination oriented directed acyclic graph (DODAG) that manages connections between accessible nodes using the DAG principle and distance vector approach. Using geographically closest nodes allows multi-hop communication. RPL methods for connecting are P2P, P2MP, and MP2P. In a topology, source nodes collect data, leaf nodes do nothing, and sink nodes are the largest and have the energy and processing power to compile network information. Two key concepts are control messages (CM), which begin and sustain connections and develop topology, and objective functions (OF), which determine routing decisions while traversing the network.

As explained in [12], the RPL network topology is maintained using the following five types of control messages (CM).

- DODAG information object (DIO) is sent in two scenarios: first, every node discloses its routing metrics, such as rank and DODAGID, to adjacent nodes so they can decide to join it. The second situation is the safe DODAG information solicitation (DIS) receipt.
- DODAG information solicitation (DIS): a message with destination information and routing information for DODAG-joining nodes.
- Destination advertisement object (DAO): the message that builds the descending path and finds neighbouring nodes.
- DAO acknowledgment (DAO-ACK): the sink node acknowledges the DAO message with a unicast message.
- Consistency check (CC): a CM that counts secure messages and challenges responses. These messages establish new node-DAG connections while retaining DODAG.

Figure 1 shows a network with several DODAG graph-based RPL instances. The OF function calculates the optimal path for each RPL instance. The RPL node connects multiple instances at once, but it can only connect to one DODAG graph node (such 13 or 17).

2.2. The objective function (OF)

According to [12], DODAG development relies on the objective function (OF). Nodes calculate rank when DIO messages come. To avoid DODAG cycles, the rank value must be greater than the parent

rank value. If DIO messages are received frequently, the best parent ranks lowest. For an acyclic network, the best parent must rank lower than child nodes.

After creating the topology, each node sends DAO messages to the DODAG sink. Lamaazi and Benamar [13] highlighted OF as an important component for managing key definitions, including link cost, parent node selection, rank cost, and advertising path cost. Minimum rank with hysteresis objective function (MRHOF) and objective function zero (OF0) are RPL default OFs. Their definitions are:

OF0: It increases the preceding rank by a value. The best parent is calculated using hops as a routing measure. Information regarding destinations and DODAG node routing is stored there. Nodes choose the best DODAG path to the ground root based on hop count. The rank value increases from root to nodes. Due to its node metric dependence, this OF has low link quality.

On unstable paths, choosing the shortest path with the fewest hops increases retransmissions and packet loss. Additionally, extra nodes would not shorten network longevity. OF0 calculates a node's rank based on the number of hops from the root node to the sensor nodes. The node with the lowest rank among its potentially reachable adjacent nodes is chosen as its parent to reduce the number of hops to the root node.

MRHOF: it was intended to address OF0's shortcomings in ranking and choosing a tree parent node using a single node metric. The expected transmission count (ETX) or energy consumption dynamic link parameter determines rank stability. It uses two mechanisms: the first selects the route with the lowest rank, and the second adjusts the rank if a lower-ranking option is available. Choosing the lowest price is guaranteed [14]. Unlike OF0, MRHOF allows easy insertion of link and node-based routing metrics. DIO packets specify routing metrics via the metric container suboption. This method determines rank and routing paths. ETX, delay, packet loss rate, and received signal strength indicator (RSSI) are link-based routing measures. LLN node routing metrics include energy, maximum life, and dependability. MRHOF ensures the LLN takes the lowest-cost path by implementing one of these routing criteria. The default MRHOF-ETX uses link ETX values to find pathways with the fewest transmission values [15].

2.3. Rank attack

Loop-free and optimal topologies depend on node rank. This attack routes network traffic to a node. According to [16], RA involves a malicious node providing lower-range information to position itself closer to the root than other nodes. Malicious nodes can capture as much traffic as possible and change many packets. Hashemi and Aliee [17] described RA as the most damaging attack as it intentionally manipulates rank to hinder network performance.

Malicious nodes send the root node an RPL control message with a bogus rank or path to initiate the RA process. RA shows RPL network nearest neighbor ranks, which govern how neighboring nodes handle DIO signals. In a worst-case situation, a malicious node with a fake rank becomes the best parent, resulting in more data packets due to incorrect routing and an unrealized network structure [18]. RA is defined as an attacker node faking a routing metric improvement to neighboring nodes, causing traffic to skip it may also impair network latency and speed [19].

According to [20], RA might cause inefficient pathways and hidden loops in the network. Also, a lower packet delivery ratio and a higher delay were observed. Rapid network topology changes will increase DIO messages. This affects network-restricted resource parameters like throughput, energy usage, latency, and data rate. Nandhini and Mehtre [21], RA seeks to monitor and attract network traffic. This node will not self-modify since RA violates rank-related information. According to [22], tracking node behavior in RPL is now impossible, bolstering RA. The ideal parent of a node in RPL routing is determined by its DIO message rank and OF. By adjusting DODAG rank values from lowest to highest, attackers can initiate RA. Finally, changing rank by a value and adjusting the OF to confuse genuine nodes are two techniques to change rank. The second obscure attackers.

2.4. Related works

RPL networks are used by many authorized and illegitimate users in many applications; thus, security is a serious challenge. IoT applications require different security levels depending on the application type, deployment environment, and data sensitivity [6]. Sensors are vulnerable to various attacks and may lose data and services due to their physical simplicity [23].

RA, which goes under RPL-specific attacks, is the focus of our study. Additionally, this section lists all relevant research articles on the rank attack's impact on the RPL protocol. Xie *et al.* [24] found that rank value changes can affect network performance. A power line communication WSN node moved up or down in the hierarchy, which they examined. They solely evaluate static network topologies and don't distinguish between types. The impact of four attack types was analyzed on key network metrics related to the attacker's topology position [25] and research was limited to static networks and did not propose RA defenses. A new RA was introduced by adjusting the (OF) and rank value [26]. RPL nodes used the OF to select forwarding

nodes using application-defined routing metrics like estimated transmission count, and residual energy. The proposed RA is more devastating since the attacker can simply force surrounding nodes to route data via it. This increased attacker data flow control. The extensive simulation showed that the RA may be used to create a fake routing path to degrade network throughput and increase communication latency. The type of RA shown is not specified. In addition, the impact of RA was examined using a fake IP address [27]. However, this study does not examine the rank attack's impact on the RPL protocol. Furthermore, the concept of enhanced RA was pioneered and suggested an ego-based defense as a countermeasure [28]. However, this study used a topology with 12 nodes instead of a realistic one. At no point were mobile nodes considered for this research.

Table 1 summarizes all the studies mentioned about impact analysis and shows this paper's contribution among them. Three types of RA were considered, along with two types of topologies. Also, both RPL conventional OF were examined. Afterward, some proposed solutions were suggested.

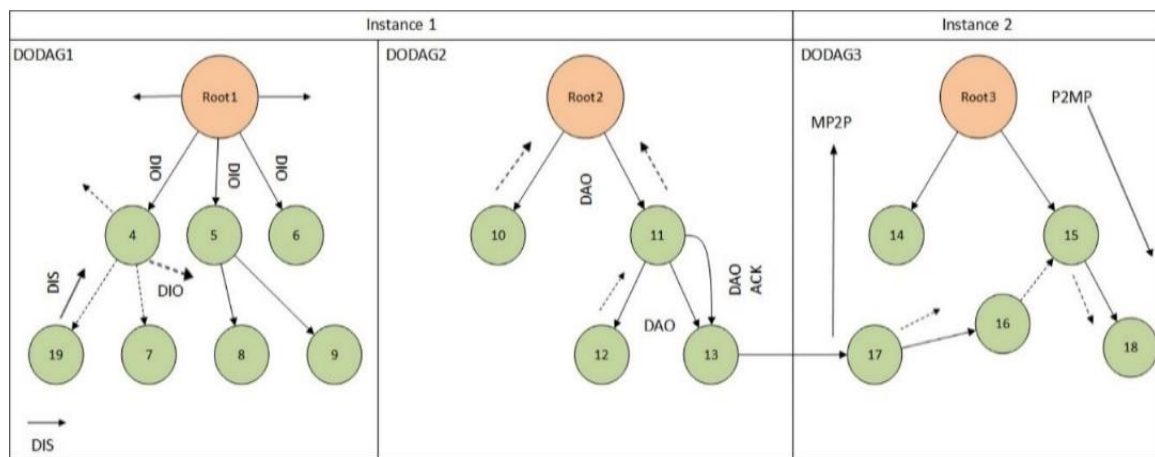


Figure 1. RPL DODAG construction [26]

Table 1. Previous studies on RA impact analysis

Ref	Year	DRA	IRA	WPS-RA	Different topologies	OF explained	Proposed solutions
[24]	2010	√	×	×	×	×	×
[25]	2013	√	×	×	×	×	×
[26]	2016	√	×	×	×	×	×
[27]	2017	√	×	×	×	×	×
[28]	2018	×	√	×	×	×	×
This study	2024	√	√	√	√	√	√

√: topic covered, ×: topic not covered

3. METHOD

First, experiments designed to assess the efficiency of a standard RPL implementation without any form of attack across the two network topologies under consideration. Second, to illustrate the effects of RA on RPL, a solitary attacker node is positioned within the chosen topologies. RA can be launched in three main scenarios, as discussed in [23], all of which are explained as follows.

3.1. Decreased rank attacks (DRA)

Malicious nodes, employing tactics like a sinkhole attack, will attempt to influence the choice of preferred parents by advertising a lower rank. The DRA severely disrupts the RPL DODAG and network traffic, which leads to a rise in power consumption. Algorithm 1 shows the DRA implemented in the RPL core.

Algorithm 1. Decreased rank attack (DRA) pseudo code

1. In function: calculate-rank (Node V)
2. DIO with an illegitimately decreased rank
 RPL_Conf_Min_HopRankInc = 0; RPL_Max_RankInc = 0;
 Infinite_Rank limited to 256; Rpl_recalculate_ranks = null;
3. if (V== attacker Node)

```

    v.rank← v.rank
4. Else
5. v.rank← v.rank + min-hop-rank-inc
6. return path metric

```

3.2. Increased rank attacks (IRA)

This attack aims to exhaust the computational and energy reserves of LLN nodes by disrupting affected nodes in a roundabout way. Furthermore, it disrupts LLN-internal communication. The attacker begins by increasing its rank and then sending DIO messages to other nodes using this new, higher rank (which is worthless). As a result, the children will have to figure out how to cross the border by looking for another parent. The intruder node either goes back to its previous rank or broadcasts a lower (better) rank to win back the support of the surrounding nodes as a parent once the children have found a new parent. Algorithm 2 shows the IRA implemented in the RPL core.

Algorithm 2. Increased rank attack (IRA) pseudo code

```

1. In function: calculate-rank (Node V)
2. if (V== attacker Node)
    v.rank← v.rank + min-hop-rank-inc
3. Else
4. v.rank← (v.parentNode).rank + link-metric
5. return path metric

```

3.3. Worst parent selection (WPS)

This scenario begins when an attacker chooses the worst parent to represent it while using the actual rank. Then, mock the nearby nodes into picking it as a parent by utilizing the decreased rank approach. Hence, packets are transmitted along the path through it. Therefore, the network will not be fully optimized, resulting in E2E delays, and possible formation of routing loops. Furthermore, as per [24], it is difficult to detect WPS, and no mitigation approach has been presented. Algorithm 3 shows the WPS implemented in the RPL core.

Algorithm 3. Worst parent selection (WPS) Pseudo code

```

1. In function: best-parent (p1, p2)
2. return p1_rank > p2_rank? p1: p2
3. End function

```

4. RESULTS AND DISCUSSION

4.1. Simulation settings

The attacks scenarios were assessed through simulation conducted on the Cooja simulator utilizing embedded systems running the Contiki 3.0 operating system. After simulating the network normally, each type of RA explained in terms of OF for each topology to evaluate how it affects network performance. Thus, normal RPL network, DRA, IRA, and WPS were tested for OF0 and MRHOF. Normal random and grid networks had 1 root and 25 nodes and are used as a baseline to compare the attacks scenario with. RA networks had 1 root, 25 normal, and 1 malicious node. Multiple modifications were applied to the contiki source files, “contiki3.0/core/net/rpl/rpl-mhrof.c” and “contiki3.0/core/net/rpl/rpl-of0.c”, allowing compromised nodes to launch attacks and act as RA in each case. Using the collect view interface in Cooja, findings were saved as files for analysis. The simulation scenario deployed for this research is based on previous research that used 25 sensors covering 50 m each on a 100 m×100 m area to simulate [27], [29]. Table 2 describes the simulation scenario.

Table 2. Simulation scenario

Parameters	Value
Simulator	Cooja
OS	Contiki3.0
Node type	Tmote Sky
Number of nodes	27 (including 1 sink, 1 malicious)
Radio medium	Unit disk graph medium (UGDM)
OF	OF0, MRHOF
Duration	60 minutes
Simulation area	100 x 100 m

4.2. Performance evaluation

4.2.1. Received packets

Figure 2 shows each experiment’s average packets. Normal conditions demonstrated random topology with 58.96 packets for OF and grid topology with 58.8, 58.9 for OF0 and MRHOF without packet loss. In attack situations, DRA values were around normal with OF0 and MRHOF packet loss. OF0 has 0.53% packet loss and MRHOF 0.07% in random topology. Grid topologies lost 0.65% OF0 and 0.57% MRHOF packets. IRA degraded random topology by 9% in OF0 and 6.5% in MRHOF. In grid topology, OF0 and MRHOF reduced values by 13% and 27%, respectively. Finally, OF0 and MRHOF dropped 12% and 15% in WPS random topology. Grid topology reduced OF0 and MRHOF by 10% and 12%. Table 3 summerizes all values. It was found that weak attack detection and routing decisions cause substantial packet loss on OF0 and MRHOF. Other causes include ordinary nodes choosing a malicious node as a parent to block traffic, disrupting the network.

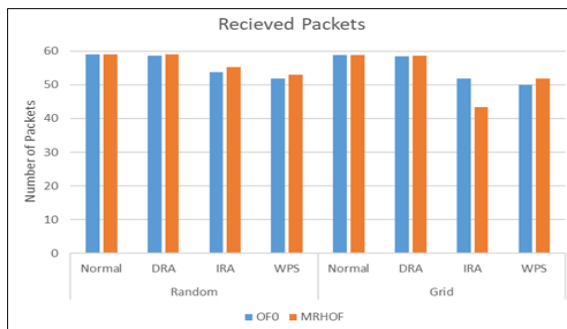


Table 3. Received packets

Topology	Scenario	OF0	MRHOF
Random	Normal	58.96	58.96
	DRA	-0.53%	-0.07%
	IRA	-9%	-6.5%
	WPS	-12%	-15%
Grid	Normal	58.8	58.9
	DRA	-0.65%	-0.57%
	IRA	-13%	-27%
	WPS	-10%	-12%

Figure 2. Received packets

4.2.2. Packet delivery ratio (PDR)

OF0 and MRHOF often yielded 0.99 for random and grid topologies in RPL operation (Figure 3). OF0 and MRHOF topologies have 0.99 in DRA. DRA had fewer impact on PDR as it is an introductory step for other serious attacks like blackhole and sinkholes as mentioned in [29]. The graph shows that the IRA scenario had the lowest PDR. Random topology reduction was 10% for OF0 and 7% for MRHOF. Grid topology cuts OF0 PDR 11% and MRHOF 24%. Because the network couldn’t handle the attack, a routing loop formed, dramatically reducing OF0 and MRHOF’s performance. Also, more control messages congest RPL which depletes node resources faster and shortens life. OF0 degraded most in WPS, 11% random and 14% grid. Both topologies lost 10% MRHOF. Table 4 summerizes all recorded values for both OF0 and MRHOF. DRA recorded no impact as the percentage of received packets had the lowest degraded amounts.

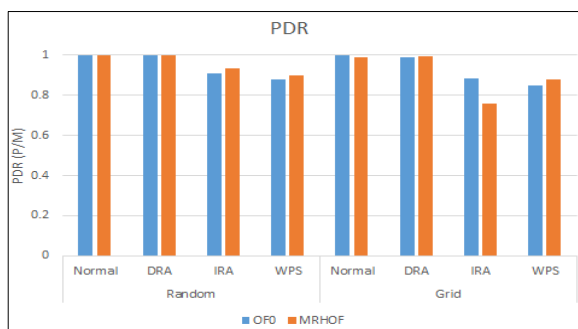


Table 4. Packet delivery ratio (PDR) (P/M)

Topology	Scenario	OF0	MRHOF
Random	Normal	0.99	0.99
	DRA	0	0
	IRA	-10%	-7%
	WPS	-11%	-10%
Grid	Normal	0.99	0.99
	DRA	0	0
	IRA	-11%	-24%
	WPS	-14%	-10%

Figure 3. Packet delivery ratio (PDR)

4.2.3. Throughput

Standard RPL procedure yielded 0.98 for all OF. Figure 4 demonstrates that DRA had the maximum throughput because OF0 dropped 1% in both topologies. Random MRHOF throughput was same, but grid topology lost 1%. Random topology declined 10% and 7% for OF0 and MRHOF in IRA. Grid topology cut

OF0 12% and MRHOF 26%. IRA results predominantly affected overall performance. As nodes deliberately pick bad parents. Damaged normal nodes have 0 (P/M) throughput because their packets never reach the sink. Unsent packets from network segment. IRAs cause topological loops and rank discrepancies. Network topology may be divided and isolated. WPS lowered OF0 random topology throughput by 12% and grid topology by 15%. Random and grid topology MRHOF degradation rates were 10% and 12%, respectively. As Table 5 shows, DRA had the lowest degraded throughput as this relies on degraded amount of recieved packets and PDR values.

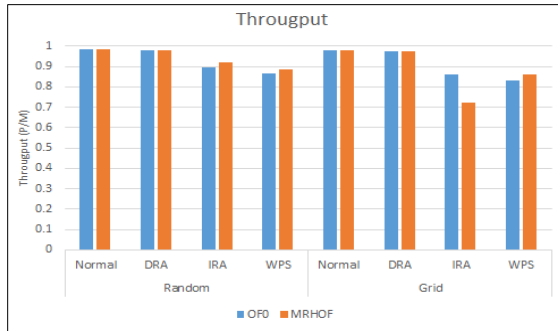


Table 5. Throughput (P/M)

Topology	Scenario	OF0	MRHOF
Random	Normal	0.98	0.98
	DRA	-1%	-0%
	IRA	-10%	-7%
	WPS	-12%	-10%
Grid	Normal	0.98	0.98
	DRA	-1%	-1%
	IRA	-12%	-26%
	WPS	-15%	-12%

Figure 4. Throughput

4.2.4. Hop count (HC)

Simulation experiments average HC values are shown in Figure 5. In normal conditions, OF0 and MRHOF had random topology values of 1.4 and 1.5. Grid topology was 1.3 for MRHOF and 1.2 for OF0. OF0 reached 3.7 in random and 2.5 in grid topology under DRA. Additionally, random and grid MRHOF values rose to 1.74 and 2.7. MRHOF increased most in IRA, hitting 2.3 for random and 3 for grid. Next was OF0, 2.5 and 2.8 for random and grid. OF0 has the highest HC values in WPS, which explains its poor performance since routing decisions depend on HC. MRHOF rises to 2.6 random and 2.9 grid.

Table 6 shows increasing HC values for each attack scenario and OF. For OF0, WPS in grid topology increased the most, followed by DRA in random topology. MRHOF under DRA in random topology increased least. However, the network maintained its performance and kept packets and PDR close to normal.

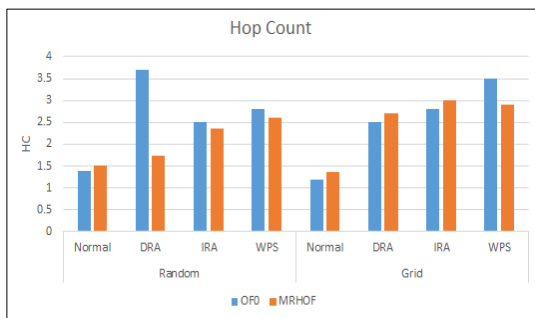


Table 6. Hop count (HC)

Topology	Scenario	OF0	MRHOF
Random	Normal	1.4	1.5
	DRA	+2.3	+0.24
	IRA	+1.1	+0.8
	WPS	+1.2	+1.1
Grid	Normal	1.2	1.3
	DRA	+1.3	+1.4
	IRA	+1.6	+1.7
	WPS	+2.5	+1.6

Figure 5. Hop count (HC)

4.2.5. Delay

This calculates each packet’s average node-to-DODAG root latency. High DAO packet destination acknowledgment latency degrades networks. Retransmissions occur due to delay. This reduces PDR and throughput, lowering network performance. Hop increase greatly affected delay results after the incident [30]. OF0’s average grid and random topology time is 101 ms under normal network conditions. Both topologies of MRHOF recorded 98 ms. Routing decisions utilizing one metric cause this. Figure 6 shows that DRA increased OF0 delay by 3% at random and 1% in grid. Random topology outcomes for MRHOF were

the same despite 2% increase in grid. OF0 latency increased 52% and MRHOF 45% with IRA random topology. Grid topology increased OF0 and MRHOF delays 59% and 135%. MRHOF had the largest HC rise; hence node rank information affected route selection. OF0 and MRHOF increased WPS random topology average delay by 10% and 8%. Grid topology growth reached 7% in MRHOF and 31% in OF0. Table 7 shows a summary of increased delay results, where IRA affected the network performance the most in both topologies random and grid. This is due to the decreased PDR, throughput and increased HC.

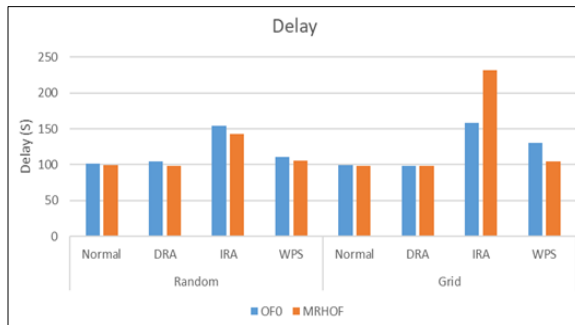


Figure 6. Delay

Table 7. Delay (Ms)

Topology	Scenario	OF0	MRHOF
Random	Normal	101 Ms	98 Ms
	DRA	+3%	+0%
	IRA	+52%	+45%
	WPS	+10%	+8%
Grid	Normal	101 Ms	98 Ms
	DRA	+1%	+2%
	IRA	+59%	+135%
	WPS	+31%	+7%

This study explored a comprehensive insights into the impact of RA on the RPL network and its subsequent degradation of performance. However, further and in-depth studies may be needed to confirm RA impact by considering mutple scenarios in terms of network size. Furthermore, future studies may explore subsequent remedies for future examination to alleviate and mitigate RA, as shown by the data. The OF is the central element that directly contributes to the building of DODAG, and making modifications to it would help mitigate the occurrence of attacks. Releying on combined metrics may be a suitable solution to the single metric basic challenge in conventional OF. Techniques like fuzzy logic need further investigation in this regard.

Our findings provide conclusive evidence that this phenomenon is associated with the presence of any abnormal event taking place within the network. Consequently, it is feasible to detect any unusual activity in a node by recognizing any adjacent node transmitting DIO packets with greater frequency than the surrounding nodes. The enhancement of network performance can be achieved by the advancement of anomaly detection algorithms, which effectively detect any node that deviates from the norm, such as malicious nodes. Subsequently, a process of isolation can be implemented on this node to mitigate its influence on the entire network and any resulting consequences.

5. CONCLUSION

RPL is a widely used routing protocol in IoT applications and is garnering many research studies due to its importance. Since it is ratified, security formed a major challenge and it is prone to various kinds of attacks. Rank attacks were found to be most disruptive attacks that is violating RPL security. This study investigated the impact of RA existance in three main scenarios, that are DRA, IRA, and WPS in two mainly used topologies; random and grid. The results indicate that RA has a negative impact on RPL performance. Furthermore, the attacker only needs to change the software code to execute the attack; no physical hardware is required. In addition, some alternative strategies were offered to protect against RA. Our future objective is to provide a resilient security solution to protect RPL against RA.

ACKNOWLEDGEMENTS




This research was supported by the Ministry of Higher Education (MoHE) of Malaysia through fundamental research grant scheme (Ref: FRGS/1/2020/ICT03/UUM/02/1). The content of this article is solely the responsibility of the authors and does not necessarily represent the official views of the MoHE, Malaysia.

REFERENCES




[1] L. Al-Qaisi, S. Hassan, and N. H. B. Zakaria, "Secure routing protocol for low power and lossy networks against rank attack: a systematic review," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 5, pp. 330–339, 2022, doi: 10.14569/IJACSA.2022.0130539.

- [2] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in internet of things: challenges, solutions and future directions," *Electronics (Switzerland)*, vol. 9, no. 7, p. 1177, Jul. 2020, doi: 10.3390/electronics9071177.
- [3] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal, and W. K. Mashwani, "A survey on intrusion detection and prevention in wireless ad-hoc networks," *Journal of Systems Architecture*, vol. 105, p. 101701, May 2020, doi: 10.1016/j.sysarc.2019.101701.
- [4] E. Aljarrah, M. B. Yassein, and S. Aljawarneh, "Routing protocol of low-power and lossy network: survey and open issues," in *Proceedings - 2016 International Conference on Engineering and MIS, ICEMIS 2016*, Sep. 2016, pp. 1–6, doi: 10.1109/ICEMIS.2016.7745304.
- [5] J. V. V. Sobral, J. J. P. C. Rodrigues, R. A. L. Rabêlo, J. Al-Muhtadi, and V. Korotaev, "Routing protocols for low power and lossy networks in internet of things applications," *Sensors (Switzerland)*, vol. 19, no. 9, p. 2144, May 2019, doi: 10.3390/s19092144.
- [6] H. Kharrufa, H. A. A. Al-Kashoash, and A. H. Kemp, "RPL-based routing protocols in IoT applications: a review," *IEEE Sensors Journal*, vol. 19, no. 15, pp. 5952–5967, Aug. 2019, doi: 10.1109/JSEN.2019.2910881.
- [7] B. H. Patel and P. Shah, "RPL routing protocol performance under sinkhole and selective forwarding attack: experimental and simulated evaluation," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 18, no. 4, pp. 1849–1856, Aug. 2020, doi: 10.12928/TELKOMNIKA.V18I4.15768.
- [8] D. Airehrour, J. A. Gutierrez, and S. K. Ray, "SecTrust-RPL: a secure trust-aware RPL routing protocol for internet of things," *Future Generation Computer Systems*, vol. 93, pp. 860–876, Apr. 2019, doi: 10.1016/j.future.2018.03.021.
- [9] A. Raouf, A. Matrawy, and C. H. Lung, "Routing attacks and mitigation methods for RPL-based internet of things," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1582–1606, 2019, doi: 10.1109/COMST.2018.2885894.
- [10] Z. A. Almusaylim, A. Alhumam, and N. Z. Jhanjhi, "Proposing a secure RPL based internet of things routing protocol: a review," *Ad Hoc Networks*, vol. 101, p. 102096, Apr. 2020, doi: 10.1016/j.adhoc.2020.102096.
- [11] A. Arena, P. Perazzo, C. Vallati, G. Dini, and G. Anastasi, "Evaluating and improving the scalability of RPL security in the Internet of Things," *Computer Communications*, vol. 151, pp. 119–132, Feb. 2020, doi: 10.1016/j.comcom.2019.12.062.
- [12] A. O. Bang, U. P. Rao, P. Kaliyar, and M. Conti, "Assessment of routing attacks and mitigation techniques with RPL control messages: a survey," *ACM Computing Surveys*, vol. 55, no. 2, pp. 1–36, Feb. 2023, doi: 10.1145/3494524.
- [13] H. Lamaazi and N. Benamar, "RPL enhancement using a new objective function based on combined metrics," in *2017 13th International Wireless Communications and Mobile Computing Conference, IWCMC 2017*, Jun. 2017, pp. 1459–1464, doi: 10.1109/IWCMC.2017.7986499.
- [14] S. Manvi, K. R. Shobha, and S. Vastrad, "Performance analysis of routing protocol for low power and lossy networks (RPL) for IoT environment," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13776 LNCS, 2023, pp. 341–348.
- [15] R. Cyriac and M. A. S. Durai, "RPL enhancement with mobility-aware two-stage objective function for improving network lifetime in IoT," *International Journal of Electronic Business*, vol. 17, no. 3, pp. 244–269, 2022, doi: 10.1504/IJEB.2022.124325.
- [16] T. ul Hassan, M. Asim, T. Baker, J. Hassan, and N. Tariq, "CTrust-RPL: a control layer-based trust mechanism for supporting secure routing in routing protocol for low power and lossy networks-based internet of things applications," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 3, Mar. 2021, doi: 10.1002/ett.4224.
- [17] S. Y. Hashemi and F. S. Aliee, "Dynamic and comprehensive trust model for IoT and its integration into RPL," *Journal of Supercomputing*, vol. 75, no. 7, pp. 3555–3584, Jul. 2019, doi: 10.1007/s11227-018-2700-3.
- [18] A. Verma and V. Ranga, "Security of RPL based 6LoWPAN networks in the internet of things: a review," *IEEE Sensors Journal*, vol. 20, no. 11, pp. 5666–5690, Jun. 2020, doi: 10.1109/JSEN.2020.2973677.
- [19] N. Mishra and S. Pandya, "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: a systematic review," *IEEE Access*, vol. 9, pp. 59353–59377, 2021, doi: 10.1109/ACCESS.2021.3073408.
- [20] P. S. Nandhini and B. M. Mehtre, "Intrusion detection system based RPL attack detection techniques and countermeasures in IoT: a comparison," in *Proceedings of the 4th International Conference on Communication and Electronics Systems, ICCES 2019*, Jul. 2019, pp. 666–672, doi: 10.1109/ICCES45898.2019.9002088.
- [21] P. S. Nandhini and B. M. Mehtre, "Directed acyclic graph inherited attacks and mitigation methods in RPL: a review," *Lecture Notes on Data Engineering and Communications Technologies*, vol. 39, pp. 242–252, 2020, doi: 10.1007/978-3-030-34515-0_25.
- [22] S. M. Muzammal, R. K. Murugesan, and N. Z. Jhanjhi, "A comprehensive review on secure routing in internet of things: mitigation methods and trust-based approaches," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4186–4210, Mar. 2021, doi: 10.1109/JIOT.2020.3031162.
- [23] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017, doi: 10.1109/JIOT.2017.2683200.
- [24] W. Xie *et al.*, "Routing loops in DAG-based low power and lossy networks," in *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, 2010, pp. 888–895, doi: 10.1109/AINA.2010.126.
- [25] 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, pp. 3685–3692, Oct. 2013, doi: 10.1109/JSEN.2013.2266399.
- [26] 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 *2016 International Conference on Industrial Informatics and Computer Systems (IIICS)*, Mar. 2016, pp. 1–5, doi: 10.1109/IIICSII.2016.7462418.
- [27] K. K. Rai and K. Asawa, "Impact analysis of rank attack with spoofed IP on routing in 6LoWPAN network," in *2017 Tenth International Conference on Contemporary Computing (IC3)*, Aug. 2017, vol. 2018-Janua, pp. 1–5, doi: 10.1109/IC3.2017.8284340.
- [28] S. Shukla, S. Singh, A. Kumar, and R. Matam, "Defending against increased rank attack on RPL in low-power wireless networks," in *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Dec. 2018, pp. 246–251, doi: 10.1109/PDGC.2018.8745752.
- [29] Z. A. Almusaylim, N. Z. Jhanjhi, and A. Alhumam, "Detection and mitigation of RPL rank and version number attacks in the internet of things: SRPL-RP," *Sensors (Switzerland)*, vol. 20, no. 21, pp. 1–25, Oct. 2020, doi: 10.3390/s20215997.
- [30] M. Alreshoodi, "An experimental study of IoT networks under internal routing attack," *SSRN Electronic Journal*, 2020, doi: 10.2139/ssrn.3690813.




BIOGRAPHIES OF AUTHORS

Laila Al-Qaisi    received a bachelor's degree from the King Abdulla II School for Information Technology, The University of Jordan, in 2008, a master's degree in information technology management from the University of Sunderland, in 2012, and a second master's degree in web intelligence from The University of Jordan, in 2017. She is currently a Ph.D. candidate at Internetworks Lab in the School of Computing, Universiti Utara Malaysia. Her research interests include the web and its enormous data, cybersecurity, IoT, routing security, artificial intelligence, machine learning, fuzzy logic, and big data analytics. She can be contacted at email: layla_mohammad@ahsgs.uum.edu.my.



Suhaidi Hassan    He earned a bachelor's degree in computer science from Binghamton University, a master's in information science (telecommunication/networks) from Pittsburgh University, and a Ph.D. in computing (computer networks) from Leeds University. He is a tenure-track computer networks professor and founding chair of the InterNetWorks Research Laboratory at UUM's School of computer. Academy of Professors Malaysia fellow, founding president of Internet Society Malaysia Chapter, and Internet Society Fellow alumni of the Internet Engineering Task Force. He has supervised 28 Ph.D. students in computer and communication networks and written over 250 refereed technical papers. He was on the Malaysian Research and Educational Network (MYREN) technical steering committee, the Cisco Network Academy (Malaysia) Council (2007–2008), and the Malaysian ICT Deans Council (2007–2011). In 2006, he led a task force to establish the International Telecommunication Union (ITU)-UUM Asia-Pacific Centre of Excellence for Rural ICT Development, a human resource development initiative of the ITU that coordinates rural ICT development initiatives in Asia-Pacific. He speaks at worldwide public forums like ICANN, Internet Governance Forums, and IETF meetings in addition to research conferences and technical meetings. He reviewed and refereed publications and conferences and examined over 100 doctoral and postgraduate researchers in his subject areas. He audited IPv6 adoption among Malaysia's top ISPs for the Malaysian Communication and Multimedia Commission, the ICT regulator. He can be contacted at email: suhaidi@uum.edu.my.



Nur Haryani Binti Zakaria    is currently an Associate Professor at the School of Computing, Universiti Utara Malaysia. She received her Ph.D. in Computing Science from Newcastle University, United Kingdom, and her Master of Science in Computer Science from Universiti Teknologi Malaysia. Her research interests include usable security and privacy, cybersecurity, information security, and network security. She has taught many courses in security-related fields both at postgraduate and undergraduate levels. Besides that, she has authored and co-authored many technical publications and is involved in research-funded grants both international and national grants. She has served as editor, associate editor, reviewer, and referee for international and local journals and conferences, as well as an examiner for many doctoral and postgraduate scholars in her research areas. She can be contacted at email: haryani@uum.edu.my.