

# Analysis of RPL Objective Functions with Security Perspective

Cansu Dogan<sup>1</sup><sup>a</sup>, Selim Yilmaz<sup>1,2</sup><sup>b</sup> and Sevil Sen<sup>1</sup><sup>c</sup>

<sup>1</sup>WISE Lab., Department of Computer Engineering, Hacettepe University, Ankara, Turkey

<sup>2</sup>Department of Software Engineering, Muğla Sıtkı Koçman University, Muğla, Turkey

**Keywords:** Internet of Things, Routing Protocol, RPL, Objective Functions, RPL Security, RPL Attacks.

**Abstract:** The IPv6 Routing Protocol for Low Power Lossy Networks (RPL) is one of the standardized routing protocols for lossy networks consisting of resource-constrained Internet of Things (IoT) devices. RPL allows to use different objective functions based on different routing metrics such as expected transmission count (ETX), hop count, and energy to determine effective routes. In the literature, the performance of two objective functions namely Objective Function Zero (OF0), Minimum Rank with Hysteresis Objective Function (MRHOF) are evaluated thoroughly, since they are accepted as standard objective functions in RPL. However their performance under attack has not been evaluated comprehensively yet. Although RPL has defined some specifications for its security, it is still vulnerable to insider attacks, which could dramatically affect the network performance. Therefore, this study investigates how the performance of objective functions are affected by RPL specific attacks. Version number, DIS flooding, and worst parent attacks are analyzed by using the following performance metrics: packet delivery ratio, overhead, latency, and power consumption. Moreover, how they are affected by the number of attackers in the network are analyzed. To the best of the authors' knowledge, this is the first study that comprehensively explores RPL objective functions on networks under attacks.

## 1 INTRODUCTION

The recent progress in embedded system technology has led to the emergence of numerous sensor devices having different architectures today. These resource-constrained devices having small on-board memory, low power, and low computational capability can communicate with each other and connect to the Internet in order to complete specific tasks. IoT networks consisting of such sensors have grown so rapidly in a very short time (Statistica, 2016). They are used in various IoT applications in every aspect of our daily life such as healthcare, agriculture, transportation, security.

The Low Power and Lossy Networks (LLN) are a special type of IoT, in which resource constrained devices are connected over lossy links that have high packet loss and so low throughput. In order to meet the special requirements of such lossy and resource-constrained networks, a new routing protocol called RPL (Routing Protocol for Low Power and Lossy

Networks) is developed by IETF-ROLL (Winter et al., 2012). Due to its efficient routing capability, RPL has now become a standard routing protocol. The optimal route between two end-points is found by selecting the most appropriate communication links between every node. To ensure that, RPL employs different objective functions that are based on different routing metrics such as ETX, hop count, and energy. Although, a number of objective functions have been proposed till now; OF0 (Thubert, 2012) and MRHOF (Gnawali and Levis, 2012) are regarded as standard objective functions in RPL by the Internet Engineering Task Force Routing over Low power and Lossy networks (IETF-ROLL) working group and are widely implemented in the most popular IoT applications today (Onwuegbuzie et al., 2020; Pradittasnee, 2017). OF0 considers the hop count, and hence it targets the minimum hop count between sender nodes and the root node in the network. MRHOF, however, uses link- or node-based routing metrics. Therefore, it provides an optimal path based on the metric used. The selection of objective functions could change routing performance, so the selection of the appropriate objective function is usually based on the requirements of the application at hand.

<sup>a</sup> <https://orcid.org/0000-0002-3806-657X>

<sup>b</sup> <https://orcid.org/0000-0002-9516-6892>

<sup>c</sup> <https://orcid.org/0000-0001-5814-9973>

Although RPL ensures an efficient routing performance for such constrained networks, it is vulnerable to insider attacks. The insecure nature of this protocol is given one of the main obstacles for the further development IoT applications (Verma and Ranga, 2019; Abhishek and Virender, 2020). RPL attacks can easily harm the network they are incorporated by exploiting and exhausting the resources of constrained nodes. The degree to which the network is affected changes according to the objective functions because they rely on different routing metrics. In this study, we investigate how objective functions are sensitive to different attack types and explore if any correlation exists between number of attackers and performance degradation when different objective functions are used. In this regard, to the best of our knowledge, this is the first study in the literature that comprehensively analyzes objective functions from security point of view. Three RPL specific attacks, namely; version number, DIS flooding, and worst parent attacks are implemented on a large number of simulated networks with varying topologies in order to ensure a better evaluation. The simulation results are evaluated by using the following performance metrics: packet delivery ratio (PDR), overhead, latency, and power consumption. A large number of experimental environments are set in order to ensure a better evaluation. The experimental results show that RPL attacks, especially the ones aiming to consume network resources (i.e., version number and DIS flooding attacks) affect the performance of networks considerably even in the presence of a single attacker. Moreover, they affect networks that use different objective functions differently. While OF0 is more robust to attacks, MRHOF-ENERGY shows the worst performance in almost all performance metrics due to the overhead caused by attackers.

The rest of the paper is organized as follows. The background information that covers an overview of RPL, the standard/default objective functions used in RPL, and attacks targeting RPL is given in Section 2. Section 3 discusses analysis studies in the literature that focus on objective functions and attacks in RPL separately. Experimental settings are introduced and the experimental results are discussed in Section 4. Finally, Section 5 concludes the study.

## 2 BACKGROUND

### 2.1 Overview of RPL

RPL is a distance vector routing protocol. Nodes in a RPL-based IoT network are connected to each other

through a special topology that is the combination of tree and mesh topologies called Destination Oriented Directed Acyclic Graphs (DODAG). A DODAG comprises of a root (or sink) node, which is responsible for the initiation of DODAG building, and a number of sensor nodes. RPL enables multipoint-to-point communication (MP2P) from sensor nodes to root node, point-to-multipoint communication (P2MP) from the root node to sensor nodes, and point-to-point communication (P2P) between sensor nodes.

A network can operate on one or more RPL instances where multiple DODAGs can take part. The role of each instance is to define an objective function to calculate the optimum path within the DODAG. A DODAG is built by using the following RPL control packets:

- *DODAG Information Object (DIO)*: It is initiated and broadcast by only the root node. DIO packets carry network information (e.g., instance ID, version number). Each of the receiving node adds the sender to its parent list, calculates its own rank value, which states its position in the graph with respect to the root node, and finally it forwards DIO to its neighbors. DIO packets are relayed throughout the graph and play a major role in constructing the default upward routes.
- *DODAG Information Solicitation (DIS)*: It is used as a solicitation for having DIO information when a new node is to join the DODAG. DIS packets are broadcast by the new node to its neighbors.
- *Destination Advertisement Object (DAO)*: It is used for the construction of the downward routes from the root to sensor nodes. Based on the mode of operation, the child nodes unicast DAO packets either to root node (in non-storing mode) or to its selected parent (in storing mode) so that it records downward routes in its routing table for the sub-DODAG.
- *Destination Advertisement Object Acknowledgement (DAO-ACK)*: Upon receiving DAO packets from a parent node, DAO-ACK packets are sent to the the sender node as an acknowledgement.

### 2.2 Objective Functions in RPL

Objective function (OF) is used to select optimal routes within a DODAG by affecting the calculation of the rank values of each participating node. As stated earlier, it differs with respect to the RPL instances, hence different objective functions could be simultaneously used within an RPL network by different instances. For example, one can take hop count into consideration to build routes of a DODAG graph,

the residual energy of the nodes could be used for finding the routes of another DODAG in the same network. Therefore, the selection of appropriate objective functions is crucially important, and it changes in accordance with the requirements of the application.

Even though there have been a number of objective functions proposed in the literature so far as discussed in Section 3, OF0 (Thubert, 2012) and MRHOF (Gnawali and Levis, 2012) are proposed as the default objective functions for RPL-based IoT networks:

### 2.2.1 OF0

OF0 takes the hop count between the root node and a sensor node into account for the calculation of rank value of that node. Therefore, it aims to minimize the number of hops to reach to the root node by choosing the node that has the lowest rank from its reachable neighbors as its parent. When OF0 is used as the objective function in the network, for a given node  $n$ , the rank of this node can be calculated by using (1).

$$R(n) = R(p) + RI \quad (1)$$

$R(n)$  is the new rank of node  $n$ ,  $R(p)$  is the rank of the preferred parent node, and  $RI$  stands for the rank increase metric that is calculated by using (2).

$$RI = (Rf \times Sp + Sr) \times MHRI \quad (2)$$

$Rf$  is a configurable rank factor and it uses 1 as the default value.  $Sp$  is the step of the rank, and  $Sr$  is the maximum value assigned to the rank level.  $MHRI$  stands for *MinHopRankIncrease* which is a constant value that is defined as 256 in RFC6550 (Winter et al., 2012).

### 2.2.2 MRHOF

Unlike to OF0, a number of link- and node-based additive routing metrics can easily be integrated into MRHOF. The rank value ( $R(n)$  in Eq. 1), and hence the routing path, is determined according to the employed routing metric which is stored in Metric Container suboption in the DIO packet.

While ETX, latency, packet loss rate, received signal strength indication are example to the link-based routing metrics; the remaining energy, maximum life time, and trustworthiness are examples to the node-based routing metrics for LLNs. By using one of these routing metrics, MRHOF ensures the lowest cost path in the LLN. Two metrics are integrated into MRHOF in this study: MRHOF with ETX (MRHOF-ETX), which is a link-based metric, and MRHOF

with energy (MRHOF-ENERGY), which is a node-based metric.

MRHOF-ETX chooses the paths with the lowest number of transmission value by considering ETX values of the links. The ETX value of the links is calculated using (3).

$$ETX = \frac{1}{Df \times Dr} \quad (3)$$

$Df$  is the probability of the packet being reached by the neighbor, and  $Dr$  is the probability of the acknowledgment packet being received.

MRHOF-ENERGY chooses the path that provides maximum remaining energy for the RPL nodes. Energy metric of the nodes is calculated using (4).

$$ENERGY = \frac{P_{max}}{P_{now}} \quad (4)$$

where  $P_{max}$  is defined as the targeted maximum power, and it is calculated from the initial energy of node divided by the targeted lifetime;  $P_{now}$ , however, is the actual power of node.

## 2.3 RPL Specific Attacks

One of the main drawbacks of the RPL protocol is that it is vulnerable to a variety of attacks due to its nature. Moreover, resource-constraint characteristic of LLNs makes them vulnerable to Denial-of-Service (DoS) attacks. RPL specific attacks can vary according to what they primarily target, and these attacks are divided into three categories: attacks targeting network resources, network topology, and network traffic (Mayzaud et al., 2016). In this study, we have studied version number, DIS flooding, and worst parent attacks:

- *Version Number*: Version number in DIO packets is used by the DODAG root in order to perform global repair, and it is increased by only the root node. In the attack scenario, the malicious node illegitimately increases the incoming version number, causing unnecessary rebuilding of DODAG.
- *DIS Flooding*: It is a typical RPL specific DoS attack that targets consuming network resources. In order to make nodes or links unavailable in LLNs, attacker continuously sends large amount of control packets. This attack is often performed by sending broadcast or unicast DIS packets after receiving a DIO packet from a node. By doing so, the DIS flooding attack brings about network congestion or overloading of RPL nodes.
- *Worst Parent*: As stated earlier, an RPL node chooses its own parent node according to the rank

value that is determined by the objective function, which ensures the ‘best parent’ for that RPL node. However, in this attack scenario, attacker node contrarily chooses the worst parent, resulting in non-optimized routing path and hence leading LLN to show very poor performance.

### 3 RELATED WORKS

By building efficient routes among sensor nodes, the objective functions defined on LLNs have a great impact on the Quality of Service (QoS) in an IoT network. That’s why, the attention towards RPL objective functions has been growing; and until now, there is a good deal of studies proposed on this research area in the literature. In this section, we mainly discuss the studies that analyze the existing standard OFs and that propose new OFs by integrating different routing metrics. Lastly, the studies analysing routing attacks against RPL are summarized and the contribution of the current study is emphasized.

As stressed earlier, OF0 and MRHOF objective functions are the basic functions defined in the RPL protocol. That’s why they have been investigated by far in the literature. In (Kechiche et al., 2017), how efficient routing built by OF0, MRHOF-ETX, and MRHOF-ENERGY as a response to different network densities is investigated. The analysis in this study shows that MRHOF-ENERGY performs poorly in high and low traffic, while OF0 and MRHOF-ETX perform better on low traffic. A very similar analysis that shows the impact of network density on different OFs is given in (Qasem et al., 2015). Unlike to (Kechiche et al., 2017), the authors here took the topology (grid and random) and the packet reception ratio (RX) into consideration as key parameters since they might play a major role on the performance of OFs. For both topologies, a higher PDR performance and lower battery level are obtained as RX increases and as the network becomes more dense. The routing performances of OF0 and MRHOF (with ETX and expected lifetime [ELT] metrics) are analyzed in (Jamil et al., 2019) according to the distance of sensor nodes to the root node. The findings reveal that, for all OFs, the network performance (PDR, overhead, latency) gradually decreases with the increase in the average distance of nodes to the root. The parameters like node density, transmission range, and time interval for sending control packets are considered in (Mardini et al., 2018) for the performance analysis of OF0 and MRHOF-ETX. As expected, the authors found that a positive correlation between the sending interval and PDR; whereas, a negative correlation between

the sending interval and power consumption. The node density, however, has no major impact on the performance metrics.

The fact that network requirements could vary according to IoT applications or services, the development of new objective functions for these applications by integrating new RPL metrics or combining existing metrics has become one of the most studied research areas in RPL (Pancaroglu and Sen, 2021). In (Al-Kashoash et al., 2016), the authors showed that a great number of data packets are lost when the data traffic is high. To ensure a reliable and efficient routing when the network is under congestion, they took the buffer occupancy into consideration as a routing metric; and hence, Congestion-Aware Objective Function (CA-OF) is proposed. Even though the performance of CA-OF degrades when the traffic is higher, it still performs superior than OF0, MRHOF-ETX, and MRHOF-ENERGY in terms of PDR, energy consumption, and packet loss.

Not only a single RPL metric, but also multiple metrics can be integrated to OFs so that it considers more than one objective simultaneously. In (Sousa et al., 2017), Energy Efficient and Path Reliability Aware Objective Function (ERAOF) is proposed. By considering two RPL metrics, energy consumed and ETX, ERAOF disregards the routes with low energy level and high probability of packet loss. In comparison to OF0 and MRHOF-ETX, ERAOF yields higher PDR, lower number of hops, and comparable energy consumption. In (Xiao et al., 2014), the authors combined hop count and ETX metrics in order to improve MRHOF-ETX. However, that the cumulative ETX value can only be calculated along the path (as in MRHOF-ETX) might be misleading in the selection of appropriate route. Regardless of the quality of each link, a node using MRHOF-ETX is likely to choose the path with fewer hops where the cumulative ETX value is relatively smaller. In order to avoid this situation, authors calculated the ETX value per hop by dividing ETX by the number of hops. This yield a higher PDR, shorter latency, and lower energy consumption in comparison to OF0 and MRHOF-ETX. The results suggest that network shows better performance when multiple RPL metrics are used together to choose paths. These metrics could be combined in various ways according to requirements of different applications. In (Karkazis et al., 2012) two different strategies for combining four different RPL metrics that are hop count, ETX, packet forwarding indication, and remaining energy are proposed. These are additive and lexical combinations. While these metrics values are averaged with relative weights in the additive combination, it is the prioritization of the

metrics that plays a key role in the lexical combination. For example, in the lexical combination of hop count and packet forwarding indication, the hop count is checked first and only if two paths have an equal hop count metric, then the packet forwarding indication metric value is taken into consideration.

The performance of an RPL-based IoT network is not only affected by the OFs, but also by malicious attempts; since attackers could dramatically harm the resource, traffic, and topology of a network. Therefore, there are also studies in the literature that analyze the effects of RPL attacks. The version number attack is studied in (Aris et al., 2016). The effect of this attack on network performance is analyzed by two parameters: the attacker location (with respect to the root node) and attacking probability. They found that the attacker location has a clear effect on PDR and overhead, but not the key factor for power consumption and latency. As expected, all performance metrics dramatically decrease as the attacking probability increases. This study is extended in (Arıř and Oktuđ, 2020) by integrating multiple attackers into the network.

The rank value plays an important role in RPL operations such as including creation of optimal topology, prevention of loop formation in DODAG. However, it could be exploited by malicious nodes in order to dramatically affect the network's resources, topology, and traffic. This illegitimate attempt is known as rank attack. The rank attack is analyzed with different attacker locations in (Le et al., 2013). The analysis here shows that the bigger the forwarding load area, which is the sum of the forwarding load of all nodes in the area, is, the more impact attack leads to on the network performance. In addition, the cooperation of multiple attackers gives severe damage to the network performance. The DIO packets are very crucial in constructing the DODAG, and finding upward routing paths where the majority of application traffic follows. In order to harm a network, the malicious nodes could either interrupt or at least slow down the propagation of DIO packets, which is known as DIO suppression attack. This attack is analyzed in (Perazzo et al., 2017) with five cooperative malicious nodes. It is shown that DIO suppression attack considerably affects the packet delivery ratio and network path stretch which is a metric used in order to show the difference between the cost of a current route cost and the cost of the shortest path.

As shown in the literature, the performance of an RPL-based IoT network is very sensitive to routing attacks. In addition, how a network is affected might vary according to the OFs as RPL attacks target network- or node-related properties. That's why, it is

worth analyzing OFs against various RPL specific attacks. This is the main motivation of this study. To the best of our knowledge, there is only a study (Semedo et al., 2018) in the literature that addresses this problem. However, in that study the authors assess only OF0 and MRHOF-ETX objective functions against rank attack. In their experiments, only one network with a single attacker node is simulated. That's why, the impact of the number of attackers on different OFs is not studied. Moreover, the simulation is run on a very small network consisting of only 19 nodes, leading a very low traffic. Hence, how OFs perform in dense networks is disregarded in that study. More importantly, it is suggested in (Kim et al., 2017) to use at least 25 nodes in network simulations in order to see multi-hop characteristics of RPL. In short, a lot of research questions are left unresolved in (Semedo et al., 2018). In this current study, we include multiple RPL specific attacks with varying number of attackers. Instead of a single network, we consider ten networks with 50 nodes for each attack scenario. The main contribution of this current study is to analyze OF0, MRHOF-ETX and MRHOF-ENERGY objective functions with security perspective thoroughly and discuss the effects of attacks on these OFs with comprehensive simulations.

## 4 ANALYSIS OF RPL OBJECTIVE FUNCTIONS

This study analyzes the impact of routing attacks on RPL-based IoT networks based on different objective functions. In order to that, different attack scenarios are implemented on simulated networks. The subsequent chapters introduces the details of these simulated networks and the performance metrics that are used to compare different objective functions. Finally, the experimental results are discussed thoroughly.

### 4.1 Simulation Settings

RPL attacks, objective functions, and the number of attackers are used as parameters that are to be investigated in the experiments. The combination of these input parameters defines a network scenario. In order to simulate each scenario, Cooja simulator (Osterlind et al., 2006), a Java-based network simulator of sensor nodes running the Contiki (version 2.7) operating system (Contiki-Ng, 2004), is used. Each scenario is simulated with a parameter set given in Table 1.

OF0, MRHOF-ETX, and MRHOF-ENERGY are taken into consideration as objective functions in the simulation environment; where version number, DIS

Table 1: Simulation Parameters.

Simulation Parameters	Values
Radio Environment	UDGM: Distance Loss
Objective Functions	OF0, MRHOF-ETX, MRHOF-ENERGY
TX Range	50m
INT Range	100m
Simulation Time	1 hour
Area of Deployment	200x200
Number of Sink Node	1 node
Number of Sensor Node	50 nodes
Platform	Sky mote
Traffic Pattern	UDP packets, every 60 sec. by sensor nodes

flooding, and worst parent attacks are considered to perform malicious activities in the network. The effects of these attacks on the objective functions are also investigated with respect to the number of attackers. To do that, the simulations are first run without any attacker node to create the baseline performance of the objective functions. Then, the same simulation scenarios are run with one (2%), three (6%), and five (10%) attacker nodes.

For each scenario, the simulation is run with 10 different network topologies where the nodes are randomly localized. The simulation is run for one hour for every scenario considered. Unit Disk Graph Medium (UDGM) is used to simulate the real lossy environment in LLN.

## 4.2 Performance Evaluation Metrics

In order to reveal how the network is affected by the objective function employed, four performance metrics are used in this study: packet delivery ratio, traffic overhead, average latency, and average power. In the following, these metrics are explained:

- *Overhead (OVR)*: It represents the total number of control packets propagated in DODAG to build network. Therefore, it is expected for a network to have less OVR value when it is operated under ideal conditions. The calculation of OVR is given in (5).

$$OVR = \sum CP \quad (5)$$

where  $CP \in \{DIO, DIS, DAO\}$  stands for control packets propagated in the network.

- *Packet delivery ratio (PDR)*: It is defined as the ratio of the total number of packets received by the root node to the the total number of packets sent to the root node. PDR shows how reliable the network is, and the greater the PDR value is, the more reliable the network is. The calculation of

PDR is given in (6).

$$PDR = \left( \frac{RTP}{STP} \right) \times 100 \quad (6)$$

where  $RTP$  and  $STP$  represent the total number of packets that are, respectively, received and sent by the root node.

- *Average Latency (ALT)*: Packet latency is the time between sending a packet and reaching its destination. ALT is calculated by the total latency ( $TL$ ) of each packet divided by the total received packets ( $TRP$ ), which is given in (7).

$$ALT = \frac{TL}{TRP} \quad (7)$$

- *Power Consumption (PC)*: One of the most important performance metrics in LLNs is power consumption, since power is one of the main constraints in sensor devices. PC stands for the power measured from nodes during the lifetime of the network. The average power consumption of the network is calculated by the ratio of the total PC of the network to the total number of nodes. Powertace (Dunkels et al., 2011) is integrated into the Contiki OS in order to calculate PC of nodes by using the (8).

$$Energy(mJ) = (Transmit \times 19.5mA + Listen \times 21.5mA + CPU \times 1.8mA + LPM \times 0.0545mA) \times 3V/32768 \quad (8)$$

$$PC(mW) = Energy(mj)/Time(sec) \quad (9)$$

## 4.3 Simulation Results

Ten random networks are simulated for each attack type with different percentage of attackers (2%, 6%, 10%), and the average results of these ten runs are shown in the results. Please note that while each topology is randomly created, the same ten network topologies in which attackers are located in the same

positions are run for each attack type/attacker percentage for a fair comparison.

Firstly, the average overhead introduced by attacks is shown in Figure 1. As expected, version number attack results in a big increase in the number of control packets, since it triggers the reconstruction of DODAG. DIS flooding attack by its nature also increases the number of DIS packets and the number of DIO packets as a response to these DIS requests considerably. The maximum number of control packets is produced by MRHOF-ENERGY in all attack types. Moreover, MRHOF-ENERGY shows dramatic increase in the number of control packets, particularly at DIS flooding attacks. As more attackers take part in the network; MRHOF-ETX results in lower overhead than OF0; while OF0 still shows an incline to increase in the number of control packets, MRHOF-ETX is less affected by the number of attackers.

The average PDR of simulated networks with different objective functions under version number, DIS flooding, and worst parent attacks is shown in Figure 2. As shown in the figure, OF0 and MRHOF-ETX reach to nearly the optimal PDR when there is no attack in the network. MRHOF-ENERGY not only shows the lowest PDR, but also shows the fastest decrease in PDR when the network is under attack. However, all objective functions are considerably affected by the version number attack even when there is only one attacker in the network. As shown in the results, while OF0 and MRHOF-ETX show comparable performance against attacks, OF0 is slightly better than MRHOF-ETX in each scenario.

The comparative average latency values (in sec) of simulated networks under version number, DIS flooding, and worst parent attacks are given in Figure 3. There is no considerable performance difference of OFs in terms of latency when they operate completely in a benign network. However, they behave differently on networks under attacks. Version number and DIS flooding attacks result in much more latency on networks than worst parent attack, because of the extra overhead introduced by these attacks. Furthermore, in these attack scenarios, packet arrival times are often delayed as the number of attackers increases. Again here, OF0 shows much better performance than the MRHOF objective functions. An interesting result here is that, MRHOF-ENERGY shows a slight decrease in overhead and a decrease in latency in the version attack scenarios, when the number of attackers gets bigger than 6% of all nodes in the network. Since it shows a big reaction to even a single attacker (2%), this attack is less affected by the further increase in the number of attackers. MRHOF-ENERGY also performs a smaller rate of increase in

latency for DIS flooding attack, when the number of attackers are increased up to 10% of all nodes. In the future, this can be further explored by simulating networks with more attackers.

Average power consumption of simulated networks is demonstrated in Figure 4. Even when there is no attacker in the network, MRHOF-ENERGY results in more power consumption than other objective functions. Again, MRHOF-ENERGY shows a big jump in power consumption even when a single attacker is introduced into the network. While the MRHOF objective functions behave similarly under attacks, MRHOF-ENERGY always consumes more energy than MRHOF-ETX. Again, version number and DIS flooding attacks consume much more energy than worst parent attack due to the higher number of control packets they introduced. Please note that MRHOF-ENERGY prefer routes that consist of nodes with higher remaining energy among alternative routes between the same end-points, it does not aim to decrease energy consumption but to guarantee the delivery of packets. Hence, it might compute a longer path for some traffic in order to increase the network life duration (Barthel et al., 2012).

To sum up, the presence of attackers adversely affects the performance of networks as expected, especially, the effects of version number and DIS flooding attacks on simulated networks are more obvious as they inherently bring more control packets to the network. On one hand, the worst parent attack which aims to change the network topology does not cause a dramatic effect on networks using different objective functions. On the other hand, version and DIS flooding attacks that target consuming of network resources clearly affect networks in all performance metrics. However, networks using different OFs are affected differently from such attacks. Networks using OF0 are more robust to attacks. Since attacks often negatively affect the quality of the links and the energy of the nodes, thus affect the ETX and ENERGY metrics used in the MRHOF objective functions, attacks can cause more changes such as frequent parent changes in networks using such objective functions.

## 5 CONCLUSION

This is the first study that comprehensively analyzes the standardized RPL objective functions from the security point of view. Since objective functions play a key role in determining optimal routes between end-points, they might be affected differently from different type of attackers. The comprehensive simulation

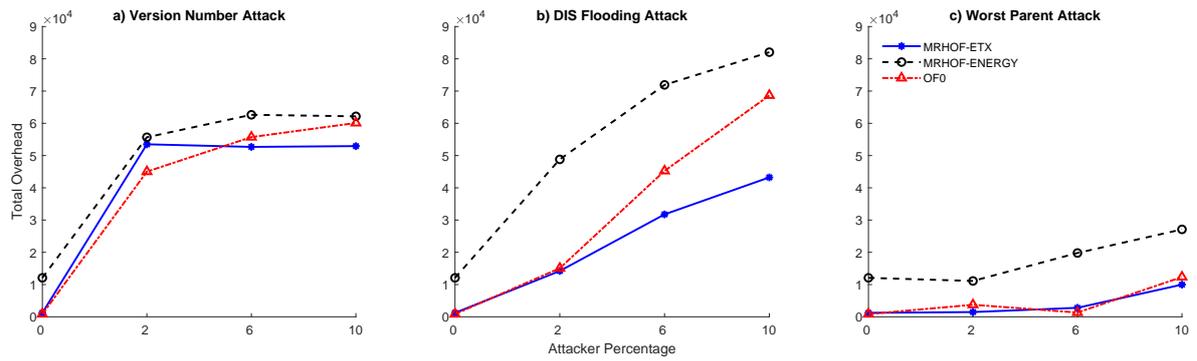


Figure 1: Average overhead of simulated networks.

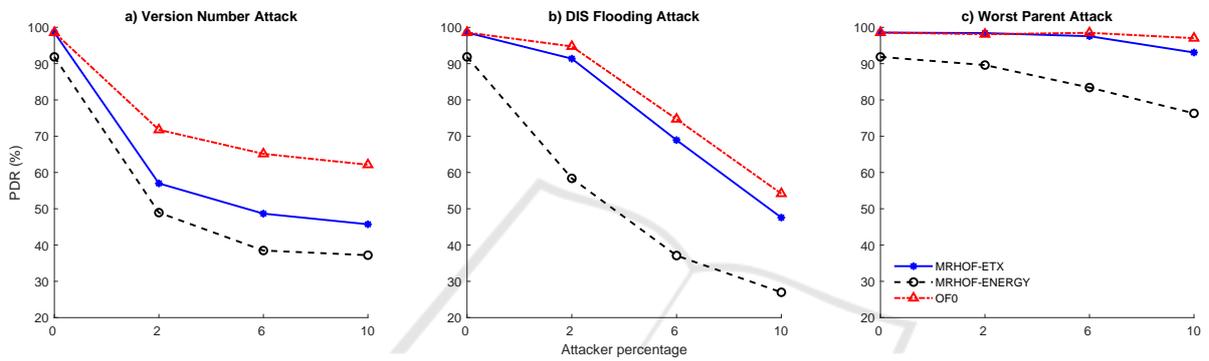


Figure 2: Average PDR of simulated networks.

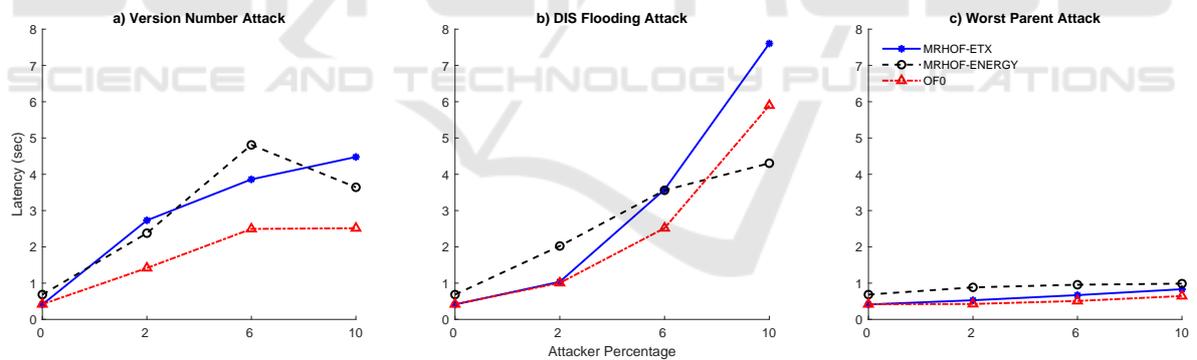


Figure 3: Average latency of simulated networks.

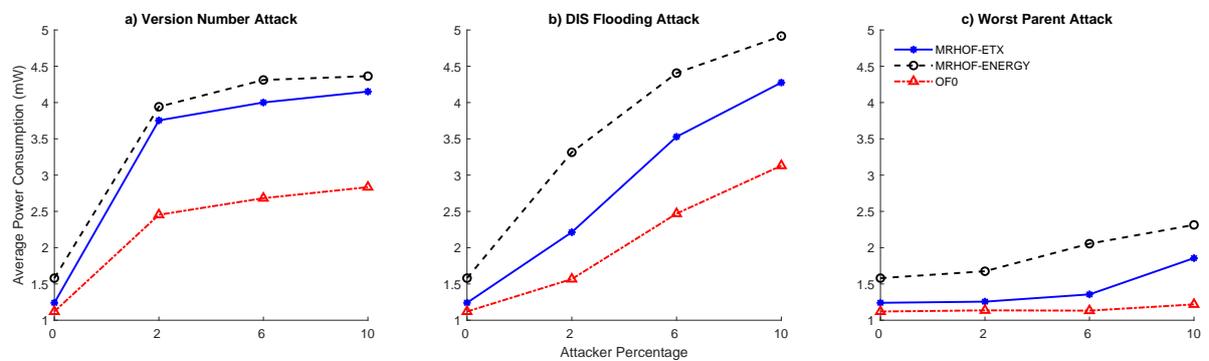


Figure 4: Average power consumption of simulated networks.

results confirm this hypotheses and show that OF0 is more robust to attacks than MRHOF and, MRHOF-ENERGY obtains the worst packet delivery ratio. The results also show that attacks targeting network resources (version number and DIS flooding attacks) have a more clear effect on all network performance metrics. We believe researchers developing security solutions for RPL will benefit from the results presented in this current study. The study could be extended with more attack types and more parameters such as mobility in the future.

## REFERENCES

- Abhishek, V. and Virender, R. (2020). Security of rpl based 6lowpan networks in the internet of things: A review. *IEEE Sensors Journal*, 20(11):5666–5690.
- Al-Kashoash, H. A., Al-Nidawi, Y., and Kemp, A. H. (2016). Congestion-aware rpl for 6lowpan networks. In *2016 Wireless Telecommunications Symposium (WTS)*, pages 1–6. IEEE.
- Ariş, A. and Oktuğ, S. F. (2020). Analysis of the rpl version number attack with multiple attackers. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pages 1–8. IEEE.
- Aris, A., Oktug, S. F., and Yalcin, S. B. O. (2016). Rpl version number attacks: In-depth study. In *NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium*, pages 776–779. IEEE.
- Barthel, D., Vasseur, J., Pister, K., Kim, M., and Dejean, N. (2012). Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks. RFC 6551.
- Contiki-Ng (2004). contiki-ng/contiki-ng. [accessed 13-July-2021].
- Dunkels, A., Eriksson, J., Finne, N., and Tsiftes, N. (2011). Powertrace: Network-level power profiling for low-power wireless networks.
- Gnawali, O. and Levis, P. (2012). The minimum rank with hysteresis objective function. *RFC 6719*.
- Jamil, M. Z., Khan, D., Saleem, A., Mehmood, K., and Iqbal, A. (2019). Comparative performance analysis of rpl for low power and lossy networks based on different objective functions. *International Journal of Advanced Computer Science and Applications*, 10(5).
- Karkazis, P., Leligou, H. C., Sarakis, L., Zahariadis, T., Trakadas, P., Velivassaki, T. H., and Capsalis, C. (2012). Design of primary and composite routing metrics for rpl-compliant wireless sensor networks. In *2012 international conference on telecommunications and multimedia (TEMU)*, pages 13–18. IEEE.
- Kechiche, I., Bousnina, I., and Samet, A. (2017). A comparative study of rpl objective functions. In *2017 Sixth International Conference on Communications and Networking (ComNet)*, pages 1–6. IEEE.
- Kim, H.-S., Ko, J., Culler, D. E., and Paek, J. (2017). Challenging the ipv6 routing protocol for low-power and lossy networks (rpl): A survey. *IEEE Communications Surveys & Tutorials*, 19(4):2502–2525.
- Le, A., Loo, J., Lasebae, A., Vinel, A., Chen, Y., and 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.
- Mardini, W., Aljawarneh, S., Al-Abdi, A., and Taamneh, H. (2018). Performance evaluation of rpl objective functions for different sending intervals. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, pages 1–6.
- Mayzaud, A., Badonnel, R., and Chrisment, I. (2016). A taxonomy of attacks in rpl-based internet of things. *I. J. Network Security*, 18:459–473.
- Onwuegbuzie, I. U., Razak, S. A., and Isnin, I. F. (2020). Control messages overhead impact on destination oriented directed acyclic grapha wireless sensor networks objective functions performance comparison. *Journal of Computational and Theoretical Nanoscience*, 17(2-3):1227–1235.
- Osterlind, F., Dunkels, A., Eriksson, J., Finne, N., and Voigt, T. (2006). Cross-level sensor network simulation with cooja. In *Proceedings. 2006 31st IEEE Conference on Local Computer Networks*, pages 641–648.
- Pancaroglu, D. and Sen, S. (2021). Load balancing for rpl-based internet of things: A review. *Ad Hoc Networks*, page 102491.
- Perazzo, P., Vallati, C., Anastasi, G., and Dini, G. (2017). Dio suppression attack against routing in the internet of things. *IEEE Communications Letters*, 21(11):2524–2527.
- Pradittasnee, L. (2017). Improving performance of route maintenance processes in rpl protocol. In *2017 9th International Conference on Information Technology and Electrical Engineering (ICITEE)*, pages 1–6.
- Qasem, M., Altawssi, H., Yassien, M. B., and Al-Dubai, A. (2015). Performance evaluation of rpl objective functions. In *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomous and Secure Computing; Pervasive Intelligence and Computing*, pages 1606–1613.
- Semedo, F., Moradpoor, N., and Rafiq, M. (2018). Vulnerability assessment of objective function of rpl protocol for internet of things. In *Proceedings of the 11th International Conference on Security of Information and Networks*, pages 1–6.
- Sousa, N., Sobral, J. V., Rodrigues, J. J., Rabêlo, R. A., and Solic, P. (2017). Eraof: A new rpl protocol objective function for internet of things applications. In *2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*, pages 1–5. IEEE.
- Statistica (2016). Internet of things (iot) connected devices installed base worldwide from 2015 to 2025 (in billions). <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>. Accessed: 2020-04-01.

- Thubert, P. (2012). Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL). RFC 6552.
- Verma, A. and Ranga, V. (2019). Addressing flooding attacks in ipv6-based low power and lossy networks. In *TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON)*, pages 552–557.
- Winter, T., Thubert, P., Brandt, A., Hui, J. W., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, J.-P., Alexander, R. K., et al. (2012). Rpl: Ipv6 routing protocol for low-power and lossy networks. *rfc*, 6550:1–157.
- Xiao, W., Liu, J., Jiang, N., and Shi, H. (2014). An optimization of the object function for routing protocol of low-power and lossy networks. In *The 2014 2nd International Conference on Systems and Informatics (ICSAI 2014)*, pages 515–519. IEEE.

