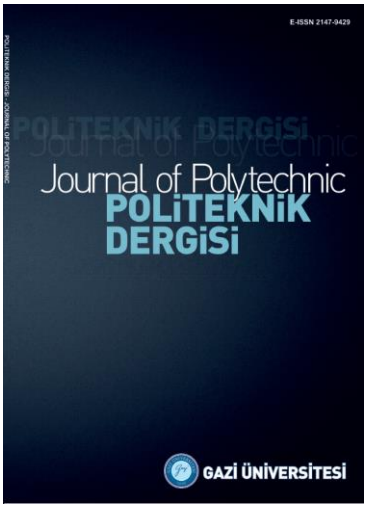

POLİTEKNİK DERGİSİ

JOURNAL of POLYTECHNIC

ISSN: 1302-0900 (PRINT), ISSN: 2147-9429 (ONLINE)

URL: http://dergipark.org.tr/politeknik

Assessing the impact of RPL attacks in challenging environments: An evolution-assisted study

Zorlu ortamlarda RPL saldırılarının etkisinin değerlendirilmesi: Evrim destekli bir çalışma

Yazar(lar) (Author(s)): *Özlem CEVİZ[1], Selim YILMAZ[2]*

ORCID[1]: 0000-0002-8610-4008

ORCID[2]: 0000-0002-9516-6892

To cite to this article: Ceviz Ö. and Yilmaz S., "Assessing the impact of RPL attacks in challenging environments: An evolution-assisted study", ***Journal of Polytechnic***, *(*): *, (*).

Bu makaleye şu şekilde atıfta bulunabilirsiniz: Ceviz Ö. ve Yilmaz S., "Zorlu ortamlarda RPL saldırılarının etkisinin değerlendirilmesi: Evrim destekli bir çalışma", ***Politeknik Dergisi***, *(*): *, (*).

Erişim linki (To link to this article): http://dergipark.org.tr/politeknik/archive

DOI: 10.2339/politeknik.1382088

Assessing the Impact of RPL Attacks in Challenging Environments: An Evolution-assisted Study

Highlights

- *The use of genetic algorithm to enhance the attack environment.*
- *The impact of enhanced RPL attacks on the performance of IoT networks.*
- *Thorough evaluation using packet delivery ratio, overhead, power consumption, and end-to-end delay.*

Graphical Abstract

In this study, we aim to assess the performance change of RPL-based networks when they are under attack. We considered the most effective attack scenarios that are evolved by the genetic algorithm.

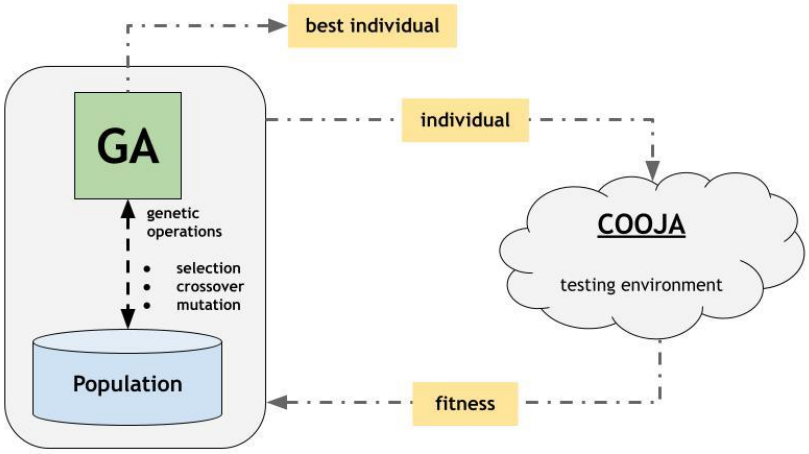

Figure. Flowchart for the evolution of the most effective attack environment.

Aim

To analyze the impact of RPL attacks at their highest effectiveness in the IoT network.

Design & Methodology

We first use the genetic algorithm to evolve malicious environments separately for seven RPL attacks. The malicious environment is achieved by finding the position as well as the density of attackers in the topology. Then, we evaluate the impact of attack on such learned environment using different evaluation metrics.

Originality

The use of genetic algorithm is first explored to achieve the most effective malicious environment.

Findings

Depending on the position and density of attackers, the operating performance of IoT network notably deteriorates as compared to baseline performance for all evaluation metrics.

Conclusion

Rather than a human-crafted environment, the use of the most effective attack environment learned by the genetic algorithm is very essential for performance analysis as it helps the security practitioner secure IoT networks considering such environment.

Declaration of Ethical Standards

The author(s) of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

Assessing the Impact of RPL Attacks in Challenging Environments: An Evolution-assisted Study

Research Article

Özlem CEVİZ[1], Selim YILMAZ[1,2*]

[1]WISE Lab., Department of Computer Engineering, Hacettepe University, Ankara, Turkey
[2]Engineering Faculty, Department of Software Engineering, Muğla Sıtkı Koçman University, Muğla, Turkey

(Geliş/Received :27.10.2023 ; Kabul/Accepted : 08.01.2024; Erken Görünüm/Early View :03.06.2024)

ABSTRACT

The integration of IoT-enabled smart technologies into our daily lives offers numerous benefits in many ways. This, however, requires well-founded security concerns because the protocols designed for IoT networks exhibit numerous vulnerabilities today. One such protocol is the IPv6 Routing Protocol for Low Power Lossy Networks (RPL) which is frequently used in IoT networks to enable routing between the heterogeneous devices. RPL has exhibited significant shortcomings and has become a target for various attacks up to now. Evaluating the performance of RPL attacks is a non-trivial task for securing IoT network effectively. Although performance analysis studies are numerous in literature, all of them rely on 'human-crafted' attack environments. In contrast, this study considers the most challenging malicious environments for performance evaluation. To achieve such environments, the use of genetic algorithm is explored in this study. The findings reveal that the impact of the attack is greatly influenced by the position as well as the density of the attackers in the network.

Keywords: IoT, RPL attacks, genetic algorithm, performance assessment.

Zorlu Ortamlarda RPL Saldırılarının Etkisinin Değerlendirilmesi: Evrim Destekli Bir Çalışma

ÖZ

IoT destekli akıllı teknolojilerin günlük yaşamımıza entegrasyonu birçok açıdan sayısız fayda sağlamaktadır. Fakat, protokollerin günümüzde çok sayıda güvenlik açığı sergilemesi, beraberinde güvenlik endişelerini de getirmiştir. Bu protokollerden biri, heterojen cihazlar arasında yönlendirmeyi sağlamak için IoT ağlarda sıklıkla kullanılan RPL (IPv6 Routing Protocol for Low Power Lossy Networks) protokolüdür. RPL bugüne kadar önemli eksiklikler sergilemiş ve çeşitli saldırıların hedefi haline gelmiştir. RPL saldırılarının performansını değerlendirmek, IoT ağının etkili bir şekilde güvenliğini sağlamak önemli bir görevdir. Performans analizi literatürde çok sayıda çalışılmasına rağmen tamamı 'insan yapımı' saldırı ortamlarına dayanmaktadır. Buna karşılık, bu çalışma performans değerlendirmesi için en güçlü saldırı ortamlarını dikkate almaktadır. Bu tür ortamları elde etmek için genetik algoritmanın kullanımı bu çalışmada araştırılmıştır. Bulgular, saldırının etkisinin, saldırganların ağdaki konumundan ve yoğunluğundan büyük ölçüde etkilendiğini ortaya koymaktadır.

Anahtar Kelimeler: IoT, RPL saldırıları, genetik algoritma, performans değerlendirme.

1. INTRODUCTION

The Internet of Things (IoT) paradigm, which enables heterogeneous devices to communicate with each other wirelessly and instantly transmit data over the Internet, has greatly influenced our daily lives over the last few decades. This has provided numerous beneficial applications, such as domotics, e-health services, smart agricultural applications, military and defense operations, smart city designs, and intelligent transportation systems, to facilitate people's lives [1], [2]. The rapid diversification of IoT applications has resulted in an increase in the number of IoT devices. It is expected that 75 billion IoT devices will be in use worldwide by 2025 [3]. Such a widespread adoption evidently brings security risks that threaten all humanity. This security risk mostly arises from communicating devices or protocols that are specifically developed for IoT networks. One of these protocols is RPL [4] that manages the routing process on IoT networks. RPL, selected as the default routing protocol for Low Power Lossy Networks (LLNs) enabling IoT, is effective for establishing routes between nodes having the high packet loss and low throughput characteristic. Despite its effectiveness in routing within LLNs, it is vulnerable against different types of routing attacks.

The weakness in RPL has motivated adversaries to continually enhance malicious attempts, resulting in the emergence of various routing attacks within LLN networks. These attacks exploit vulnerabilities in RPL, targeting its routing functioning to disrupt communication and compromise the integrity of data transmissions. This underscores the requirement for security analysts to rigorously evaluate the impacts of

*Sorumlu Yazar (Corresponding Author)
e-posta : selimyilmaz@mu.edu.tr

these attacks, highlighting the significance of comprehensive assessment to understand their implications on network integrity and functionality. There are several attempts in existing literature to address this issue, primarily focused on static scenarios where the attacker is located in a fixed position in the network. Furthermore, the majority of these simulations have only considered a single attacker, reflecting a limited scope in their analyses since the attack's impact is closely dependent on both the position and density of attackers in the topology. In addition, due to limitations in their selection strategies that mostly rely on 'random' or 'sequential' selection of the attackers, the existing analysis efforts can provide only partial assistance to the security community, resulting in a lack of depth and efficiency. Because the extent of the attack's impact is significantly influenced by the attackers' placement, random selection of attackers potentially misleads security practitioners, especially if they are positioned in an area where their effects are not readily apparent or noteworthy. The sequential selection strategy, however, is neither realistic nor feasible for the large-scale IoT networks. This is due to its impracticality, particularly when considering the exponential increase in costs associated with attacker placement. These approaches become even impractical especially when the number of attackers also becomes an additional parameter that needs to be investigated. To aid the security practitioners in anticipating vulnerabilities in IoT networks before implementing crucial measures, it is essential to evaluate the impact of the attackers effectively and efficiently in an environment that has not been artificially manipulated through human-crafted scenarios. This study refers to such an environment as the 'most challenging environment'. The main motivation behind this study is to address this gap in the literature and provide an evaluation of attacker impact in a more realistic setting.

We have conducted a comprehensive analysis in this study to assess how large RPL attacks could affect the performance of the network when the attack reaches its maximum potential, demonstrating the full impact of RPL attacks. To the best of our knowledge, there is no study in literature that analyses the impact of the attack in such environments. In order to achieve this goal, the most challenging environment is first learned through the Genetic Algorithm (GA), which is a learning algorithm under the umbrella of evolutionary computation [5]. The learned environment is then simulated and evaluated according to four different evaluation metrics that are very important for IoT networks: *i*) packet delivery ratio (PDR), *ii*) overhead (OVR), *iii*) average power consumption (APC), and *iv*) end-to-end delay (E2E). The results reveal that the network performance is seriously affected when the attackers are cooperatively located in the critical positions in the topology. The contributions of this study are outlined below:

- The simulation environments in the experiments are learned by the GA: Rather than the human-crafted, we considered 'evolved' scenarios for each attack type that dramatically reduces the performance of the network, ensuring a more realistic network setting. This is the first study that uses GA for exploring such challenging environments.
- A thorough attack analysis is carried out: The analysis is carried out based on an environment learned by GA, and unlike most of the current studies, we consider seven routing attacks targeting different aspects of the RPL-based networks.

The organization of this paper is as follows: Section 2 briefly explains the background information on RPL, RPL attacks, and the GA. The related studies that assess the impact of RPL attacks are discussed in Section 3. The proposed evolutionary-based method, experimental scenarios, simulation settings, and the results are given in Section 4. Finally, Section 5 concludes the findings of this paper.

2. BACKGROUND

2.1. RPL

Satisfying the needs of resource constrained IoT devices, RPL is a distance vector protocol that offers efficient and adaptable routing for LLNs specifically. It aims to support the integration of thousands of interconnected devices through a multi-hop network architecture, aligning with the vision of the IoT [6].

RPL has different characteristics from the other routing protocols in LLNs. The system incorporates an on-demand loop detection mechanism that employs data packets. This method effectively preserves energy and extends battery life by avoiding frequent updates to the routing topology due to transient and infrequent changes in connectivity that are commonly encountered in LLNs [4]. Moreover, it focuses on scalability and stability, which are the key issues in LLNs with potentially unstable connections and nodes. These factors led to the widespread adoption of RPL in LLNs.

2.1.1 Protocol overview

RPL has a special topology called Destination Oriented Directed Acyclic Graph (DODAG) to communicate among nodes. Four essential control messages are responsible for creating and maintaining the route required for communication between the nodes: Destination Information Object (DIO), DODAG Information Solicitation (DIS), Destination Advertisement Object (DAO), and Destination Advertisement Object Acknowledgment (DAO-ACK). The formation of DODAG, which includes a root node generally called the sink node and the other leaf nodes, is

initiated by the root node. The root node initially broadcast DIO control packets, which contain information for nodes to join the DODAG, such as version number, ID, and other necessary information. When a node receives a DIO packet, it includes the sender's address in its parent list. Furthermore, it computes the rank value and adds the DIO packet with its address and rank value prior to transmission. This propagation of DIO packets in the network results in an upward route. The downward route, however, is established by using DAO packets. A receiver responds to a unicast DAO message by sending a unicast DAO-ACK packet. DIS packets, used to request DODAG information, enable new nodes to join the DODAG. The neighbor node receiving the DIS packet responds by sending a DIO packet, sharing the current DODAG information.

There are two categories of repair mechanisms within RPL: global repair and local repair. Global repair is a process for repairing links and nodes, detecting loops, and other inconsistencies [4]. When the global repair mechanism is activated within RPL, it triggers a full reconstruction of the DODAG by incrementing the DODAG's version number [7]. Nodes then compare this version number in the DIO with the existing version number. If the current version number is greater, the node should disregard its existing rank information, reset trickle timers, and begin a new procedure to become part of the DODAG [8]. This process affects the entire network, as each node changes the version number to announce the new version and force the DODAG to rebuild itself. That's why global repair is a very costly process in terms of network performance and resource consumption. In some cases, local repair mechanisms can be more suitable, addressing issues without triggering a complete DODAG rebuild. There are two alternatives for local repair. The first is that if a parent node is not active, nodes can temporarily create a route through neighbors with the same rank, allowing efficient routing and ensuring continued connectivity within the network. The other is that by selecting a new parent from their parent list, nodes can maintain their position in the DODAG and continue functioning without the need for a global repair. These local repair mechanisms can be used individually or in combination to avoid any loss of connectivity in the network.

2.1.2 Attacks

Exploiting the weaknesses in the protocol, adversaries have been consistently developing routing attacks that are categorized based on what they primarily target [9]: *i*) targeting resource, *ii*) targeting topology, and *iii*) targeting traffic. In this study, the following seven attacks are considered:

- *Blackhole (targeting topology):* In this attack, the intruder drops all the packets that are passed through it. Therefore, a dramatic degradation in packet delivery performance is observed.
- *Selective Forwarding (targeting topology):* In this attack, rather than the entire network, a portion of the traffic is discarded by the attackers. As compared to the blackhole, this attack is known to be more challenging as the malicious pattern may change over time, and even attackers can behave almost identically to benign nodes to avoid being detected. Similar to a blackhole attack, it directly affects the PDR of the network.
- *DAG Inconsistency (targeting resources):* The protocol uses the 'O' and 'R' flags to cause an inconsistency in DODAG. The 'O' flag indicates the direction in which the packet should be forwarded, while the 'R' flag indicates whether a sequence error has been detected by a node. If the direction of a packet is inconsistent with the direction represented by the 'O' flag, the relevant node forwards the packet but also sets the 'R' flag. If the 'R' flag has been previously marked by other nodes, the corresponding device drops the incoming packet, sends DIO packets, and resets the trickle timer, resulting in a local repair. The attacker performs this attack in two ways: *i*) it transmits the incoming packet after setting the 'O' and 'R' flags, *ii*) it sends a new packet in which these flags are already set. This attack leads to unnecessary local repairs, consumes resources and increases the overhead.
- *Decreased Rank (targeting traffic):* Here, the intruder intentionally broadcast a lower rank value to the neighboring nodes, feigning proximity to the root node because a high amount of traffic passes through the root node, attracting most of the existing traffic in the network. This consequence of this attack can become even more severe when it is coupled with other attacks.
- *DIS Flooding (targeting resources):* It creates a huge amount of network traffic, making nodes and connections on the network inaccessible. Here, the intruder continuously broadcast DIS packets, leading neighboring nodes to continuously respond with DIO packets. This results in congestion in the network as well as additional resource consumption by victim nodes.
- *Increased Version (targeting resources):* As stated earlier, the version number in the DIO package is regularly checked by the root node to find out if the current DODAG is up to date. Contrary to the specification of RPL, the intruder intentionally increases the version number to result in continuous renewal of DODAG, thus consuming the resources of the network.
- *Worst Parent (targeting topology):* According to the RPL protocol, each packet travels through the

parent node before reaching the root node. The parent of a node can be one of the nodes in its neighborhood. The node chooses the best parent node by inspecting the rank value of neighboring nodes. In case of an attack, the malicious node makes the 'worst' neighbor node the parent node instead of the 'best' one to forward incoming packets. This mainly results in suboptimal routing performance.

2.2. Evolutionary Computation and Genetic Algorithm

Evolutionary computing is a general name given to a set of learning algorithms based on the evolution of a population to develop solutions to a problem. Evolutionary calculation algorithms, or evolutionary algorithms, rely on the theory of 'survival of the fittest' and aim to develop good individuals in the population by replacing them with the non-promising ones, thus ensuring the production of good-quality solutions at the end of the evolution.

Several evolutionary algorithms have been developed to date, and GA is the most popular evolutionary algorithm today. Evolutionary algorithms, including GA, follow similar processes to evolve better individuals for subsequent generations through genetic operators, such as selection, crossover, and mutation. Individuals in a GA are often randomly generated and represented through a vector-like structure in which a few genes take part. According to the fitness function, individuals are evaluated just after they are generated or bred. The fitness functions illustrate an individual's quality or proximity to the optimal state. The individuals are selected to form pairs concerning the selection strategy, like a roulette wheel. The selection strategies take into account the fitness scores of individuals, making it more probable for individuals with higher fitness to produce offspring. Upon selection, the pairs are subject to, in order, crossover and mutation. There are several crossover strategies in GA, such as one-point, two-point, uniform, and the like. The common behavior behind these strategies is to swap sub-vectors that the individuals represent. As for the mutation, which is applied as the final operator in a step, some genes in the vector of selected individuals are mutated by flipping (for binary values) or disturbing (for real values) them. For a more comprehensive discussion on GA, including an in-depth analysis of its working principles, applications, and a thorough examination of both advantages and limitations, refer to [10].

3. RELATED WORK

Over the past few decades, researchers have been studying on enhancing and analyzing the security measures IoT-based networks [11], [12], [13]. However, since this paper primarily concentrates on the RPL protocol, we here discuss only the important researches that analyze attacks on RPL-based IoT networks and their impact on network performance.

According to this protocol, each node has a parent list, in which the rank of the parent is always smaller than the child's rank, and the parent has the best rank. The earlier study [14] presented a type of attack called rank attack to aim at selecting the worst parent with a greater rank. The attack was applied to four different types of scenarios. In the first scenario, the rank attack was implemented during the simulation period, enabling DIO packages to be updated, while in the second scenario, DIO package updating was disabled. In the other scenario, the simulation time is divided by a certain period, and the attack terminates after the first half of the period. Similarly, to the first two scenarios, the DIO package was updated in one scenario but not in the other. Proposed attack scenarios have the potential to drastically increase E2E and decrease PDR. The authors emphasized that the impact of attacker collaboration can severely damage network performance, especially if it is deliberately located in areas with high network traffic. In another study [15], a decreased rank attack is presented. Grid and random topologies were used to create four different topologies with 36 nodes and 1 root. Grid topology is used to implement two distinct situations: The first is where the root node is in the center, and the second is where the root node is in the upper left corner. In random topology, static nodes are located first, while mobile nodes are utilized in the second scenario. The four topologies were evaluated without attack, and then the attack was implemented so that all nodes, except the root node, were selected as attacker nodes sequentially, called 'sequential' selection in this study, to reveal the impact of attacker positions. After each single attacker implementation, packet delivery time, OVR and APC increased for all four topologies and the PDR decreased. When the grid topology was used and the root was in the corner, the attack had the greatest impact on this network, reducing PDR by 13.44%. In addition, it has been observed that nodes selected near the root node reduce network performance more. The authors expanded the network area and experimented with 69 nodes and 1 root, using a random static node topology. Experiments were conducted by gradually increasing the attacker ratio (up to 20%). As the attacker ratio increases, the PDR decreases, and the packet delivery time, OVR, and APC increase. Similarly, the decreased rank attack was presented in [16], in three different ways, with the attacker located one, two, and three hops away from the root, respectively. However, the attack was only effective in terms of PDR and APC when the attacker was located three hops away from the root.

In [17], a rank attack is initiated by an attacker node capturing DIO packets and changing the rank value. The attacker node replicates the IPv6 address of the victim

node within the intercepted DIO packets, a form of attack referred to as a rank attack with a spoofed IP. It is observed that the PDR is greatly reduced because of this attack. In [18], the authors propose a novel rank attack in which the attacker changes both the rank value and an ETX, a routing metric used to measure the quality of a path between two nodes. Parameters like APC and radio duty cycle were examined in [19] for network performance analysis under decreased and increased rank attacks. For both attacks, higher APC and loops were observed according to the reference network. The increased rank consumes more energy than the decreased rank because of more loops.

A different type of attack against RPL routing protocols, a version attack, was conducted in [8], [20], [21], which increased the number of versions in the DIO package and triggered the routing discovery process. In [8], the attack was analyzed by using sequential selection to assess the position impact of the attacker on OVR, PDR, and E2E. As a result of the analysis, the distance between the attacker and the root is a crucial factor that affects two things: the OVR and the amount of packet loss. Additionally, OVR and packet loss increased when the attackers were in positions with a greater number of neighbors. The PDR has declined by almost 30%, and the OVR, E2E, and APC have increased. These factors collectively demonstrate the negative impact of the attacker's position on the system or network's performance and efficiency. Similarly, [20] investigated the impact of a single attacker, which was randomly selected and located with respect to the root node on the network, in terms of PDR, OVR, E2E, and APC. The authors used both static and mobile nodes in the simulation to observe the impact of the attacker's location on performance. In their extended study [21], multiple attackers were implemented in an extensive simulation to evaluate the cooperation of attackers' effect on the network's performance. Sharma et. al. [22] discussed how mobile nodes affect network performance under version attacks. The attacker nodes were selected from static nodes located at different distances from the root, up to a maximum increase of 30%. It was observed that a hybrid network consisting of 50% mobile and 50% static nodes decreased the PDR more than a network with only static nodes.

DIS flooding is another attack that exploits a process in the RPL protocol in which nodes send DIS packets to their neighbors to join a topology. In [23], this attack was performed by dropping the DIO packets and frequently sending illegitimate DIS packets to neighbors. The impact of the attack was evaluated for both different data generation rates and changes in DIS packet interval time. DIS flooding attack causes an increase in control packets and consumes network resources. Unlike other studies, the positions of attacker nodes are fixed in the experiments and are not considered. In contrast to prior studies, the positions of attacker nodes were fixed in the experiments, and their effects were not considered. Similarly, in [24], the authors proposed the DIS flooding attack. Multiple experiments were conducted by placing potential attackers both within and beyond the transmission area of the root. It showed that increasing the number of attacker nodes within the range of the root node and locating them in important positions negatively affects PDR, E2E, and APC. To the best of our knowledge, the study [25] is the first to focus on the DAO inconsistency attack. The PDR decreases rapidly as the ratio of attackers increases in the network. This occurs because intruders often intentionally discard received data packets and respond with error-forwarding packets to their parents, leading them to discard valid downward routes. Furthermore, this attack increases both APC and OVR.

The previous studies generally focused on a scenario based on a single attacker. However, the coexistence of multiple attacks targeting the RPL protocol together provides detailed analysis, thus improving future studies in attack detection. In [26], three different attacks that affect the resource and topology are proposed: DIS flooding, increased number, and decreased rank. For multiple attacker ratios, the impact of the analyzed attacks is summarized based on the most critical parameters (i.e., E2E, throughput, PDR, and APC). E2E and APC increase as the number of attackers increases, while PDR and throughput decrease. It is the increased version attack that has the greatest impact on network performance. Decreased rank, however, does not have a significant impact on PDR. In a recent study [27], version number, DIS flooding, and worst parent attacks were implemented, with the attacker ratio increasing by up to 10%. Increased version and DIS flooding attacks have a negative impact on all metrics (OVR, PDR, E2E, and APC). The worst parent attack could not have a similar effect on the network. Similarly, in [28], the authors presented decreased rank, increased version, worst parent, and replay attack to evaluate network performance under single-, multi-, and hybrid-attackers. In addition, it also shows the impact of attacks on networks of different densities by using different numbers of nodes. The result revealed that the coexistence of increased version and decreased rank attacks causes great damage to the network.

All studies are summarized in

Table 1. In general, all prior research has focused on analyzing a single attack and implementing a single attacker. Some studies [15], [19] have analyzed the attacker's position, but in these cases, the evaluation of

the attacker's location was limited to a superficial analysis due to the lack of the attacker's cooperation and the manual selection of attackers. Additionally, there are no clear and detailed explanations as to why parameters like PDR, OVR, E2E, and APC change depending on attacker positions. Other studies [26], [27] that analyze multiple attacks did not mention the importance of the positions of attackers.

In this study, we implemented seven different attack types in detail and evaluated the impact of cooperating attackers on network performance using a multi-attacker scenario. We analyzed the impact of the attacks according to the position and density of the attackers. Moreover, attacker positions were selected using a GA because examining the individual locations of attackers in a network with many nodes is a difficult and time-consuming process.

Table 1. Outline of the studies on RPL attack analysis.

Reference	Year	Attack Type	Selection strategy of attackers	Description
[14]	2013	Worst Parent	Random	Attacker positions can significantly decrease the performance of the network.
[8]	2014	Version attack	Sequential	The attack was performed with the choice of a single attacker, and its position was evaluated. However, the cooperation of the attackers is not mentioned.
[18]	2016	Decreased Rank	Random	In terms of network performance, five different simulations are presented, each with randomly chosen attackers in various locations. Depending on the position of the attackers, the PDR could decrease between 30% and 57%.
[20]	2016	Increased Version	Random	Only a single attacker was adopted. Using static and mobile nodes to investigate the effect of the attacker's location on performance.
[17]	2017	Decreased Rank	Sequential	The importance of location is emphasized, but the results are limited to the attacker node that affected the network performance the most, and there were single attacker scenarios.
[25]	2018	DAO Inconsistency	Random	Attacks were evaluated based on the attacker ratio.
[21]	2020	Increased Version	Random	Using multi-attackers to describe the cooperation of attackers and the effect of their location on network performance
[19]	2021	Increased and Decreased Rank	Random	A single attacker was selected for the attack, and its position was not rigorously assessed.
[23]	2021	DIS Flooding	Random	Evaluating the attack's impact for various data rates as well as variations in DIS packet interval time. The impact of attackers' positions on performance was not well discussed.
[22]	2022	Increased Version	Random1	Using static and mobile nodes, analyze the impact of the attacker's location relative to their hop away from the root.
[26]	2022	DIS Flooding Increased Version Decreased Rank	Random	Based on the attacker density, attacks were assessed.
[27]	2022	Increased Version DIS Flooding Worst Parent	Random	Based on the attacker density, attacks were assessed.
[24]	2022	DIS Flooding	Random	Discussing attacks in terms of the transmission range of the attacker to the root.
[15]	2023	Decreased Rank	Sequential	Discussing the importance of the attacker's position, but each attacker was manually selected as a single attacker.
[16]	2023	Decreased Rank	Random1	The impact of the attacker's position is evaluated in only three scenarios in terms of the hop distance of the attacker to the root. However, there was only a single attacker in the scenarios.
[28]	2023	Decreased Rank Increased Version Worst Parent	Random	Network performance with 3 different densities was evaluated by creating single-, multi-, and hybrid-attack scenarios.

	Replay Attack

[1]based on the hop count

4. ANALYSIS OF EVOLVED ATTACK ENVIRONMENT

As stressed earlier, prior to the attack analysis, we aim to learn about an attack environment by finding the challenging configuration with respect to the attacker location and density, which makes this study significantly different from the existing studies. This is because not every attack has the same impact on the RPL-driven networks, even if the environments are nearly identical. The proposed approach that yields a learned 'attack environment' at the end of evolution is explained below.

4.1. Evolution of Attack Environment

Although traditional approaches, like brute-force, can be regarded as an alternative to find a typical challenging attack environment, they are hardly applicable, particularly when the scale of the network greatly increases. That's why the use of a computationally effective learning algorithm is worth exploring. This fact provides a clear explanation for the adoption of GA, which plays a key role in the proposed framework of this study. The main objective of GA is to find a subset among all configurations that define the challenging attack environment for each of the attack types outlined in Section 2.1.2.

The evolutionary-based architecture adopted here is illustrated in **Figure 1**. It is clear from the figure that this architecture is mainly based on a continuous interaction between the algorithm and the network environment throughout the evolution. Speaking concretely, the population's members are evaluated within the testing environment during each generation, ultimately yielding 'fitness' scores for each individual. In this context, the fitness score denotes the extent to which an individual affects the network environment adversely, thereby impacting their performance. Therefore, depending on the fitness scores of the individuals, they undergo genetic operations to breed new, hopefully better, offspring individuals. PDR, explained and formulated in Section 4.3, is considered a fitness function in this study. So, the individuals here mainly target this metric for evolving a challenging malicious network environment. Note that the PDR is particularly chosen as a fitness function since it is inevitably affected by a degradation in other network performance metrics such as OVR, APC, etc.

In order to evaluate the individuals in the testing environment, we have used the COOJA emulator [29], a software developed in Java to emulate IoT nodes running the Contiki O.S. (version 3.0 used in this study) [30]. The COOJA emulator relies on a configuration file, a typical 'xml' file, to load the network environment. This mainly involves *i*) the number of nodes, *ii*) their positions as well as identities (i.e., root, malicious, benign, etc.), *iii*) additional plugins, and *iv*) the path to the OS that the running nodes load. That's why this is the only file that one can modify to configure a network environment by specifying the number of attackers as well as their positions.

The GA is run separately for each attack type to generate the malicious network environment. So, depending on the state of the individuals in the algorithm, the configuration is organized from scratch every time the individuals are evaluated in the testing environment. Because the individuals are represented through binary values (i.e., 0s and 1s) in the algorithm, called '*genotype*', these values should be transformed into another representation so that they could be interpretable in the problem domain, called '*phenotype*'. To do that, a decoding process is applied to the individuals before proceeding. This procedure is shown in **Figure 2**. Note that 0s and 1s in genotype represent the benign and malicious nodes, respectively. Their positions in the chromosome are considered for decoding from 'genotype' to 'phenotype'. Note also that the algorithm tends to make all nodes as malicious nodes to achieve the worst PDR score, which is not a realistic scenario. That's why we allow the algorithm to make only 20% of all the nodes as attackers.

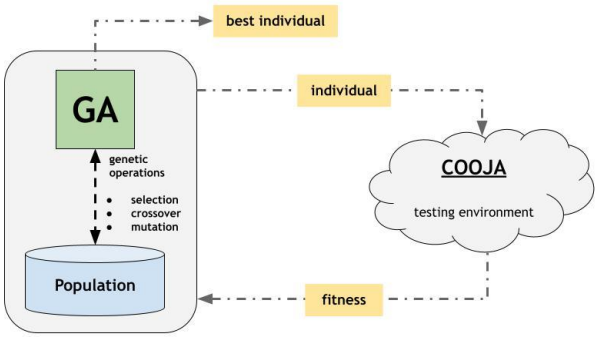

Figure 1. The architecture of the evolutionary-based attack improvement.

After the decoding process, the individuals are now represented by different network configuration files in the testing environment that are separately imported as network environments in COOJA. As for the implementation of genetic algorithm, we have used the Evolutionary Computation in Java (ECJ) toolkit in our study. The parameter settings of the GA are listed in **Table 2**, and the other settings not listed in the table are the default parameters of ECJ.

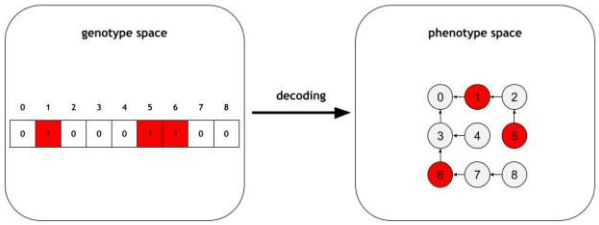

Figure 2. Decoding procedure from genotype to phenotype.

Table 2. Parameters and their values used for evolution.

Parameter	Value
Individual Representation	Bit Vector (with 29 Genes)
Selection Strategy	Best Selection (Size: 2)
Mutation Type and Rate	Flip and 20%
Crossover Type and Rate	One-point and 90%
Generation	100
Individual and Elite Individual Size	20 and 2

4.2. Simulation Settings

An exemplar application in the Contiki project, called 'rpl_udp', is used in the experiments. This application simply provides packet exchange between the client and the server nodes at certain periods, which takes 15 seconds in this study. Zolertia 1 (Z1) is selected as the device architecture in the experiments due to its ability to provide larger memory than the alternative architectures. Each network environment is simulated in COOJA for 15 minutes. A grid topology with 30 nodes, including 29 client nodes and 1 root node, is adopted in the experiments as it is suggested to use at least 25 nodes to see the multi-hop characteristic of LLNs [6]. The preference for grid topology over random topology stems from the fact that, unlike the random arrangement of nodes in the latter, nodes in grid topology are deliberately and relatively positioned, resulting in reduced stochasticity. **Figure 3** shows the network topology used in the experiments. The nodes shown in the figure are located at different DODAG levels, represented by different colors based on their rank values. The nodes are in a 100 x 80 m area, and they are 20 m away from each other. The transmission range (TX) of the nodes was selected as 25 m so that any node can communicate with one hop away neighboring nodes only.

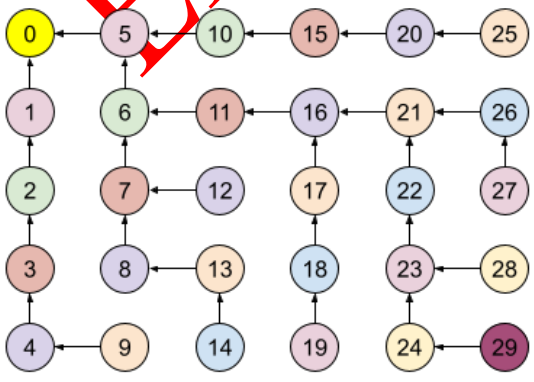

Figure 3. Grid-based network topology used in simulations.

4.3. Evaluation Metrics

The following important evaluation metrics that are commonly studied in the literature to assess network performance are used in this study:

- *PDR* represents the ratio of packets sent by the nodes (P_{sent}) to the packets received by the root node ($P_{received}$):

$$PDR = \frac{P_{received}}{P_{sent}} \quad (1)$$

- *OVR* refers to the total number of DIO (P_{DIO}), DAO (P_{DAO}), and DIS (P_{DIS}) packets propagated in the network:

$$OVR = P_{DIO} + P_{DAO} + P_{DIS} \quad (2)$$

- *APC* is the overall power consumption of all nodes including the root node, and it evaluated by dividing the energy units ($Energy$) within the time over which it has been consumed:

$$Energy(mJ) = \left(\begin{matrix} Transmit \times 19.5 + Listen \times 21.5 + \\ CPU \times 1.8 + LPM \times 0.0545 \end{matrix}\right) \times 3V/32768 \quad (3)$$

$$APC(mW) = \frac{Energy(mJ)}{Time} \quad (4)$$

where; $Transmit$ is total transmission time, CPU is time for which mote is active, LPM is total time for which the node is in low power mode, and finally $Listen$ is total listening time. The constants in eq. (3), however, represent the typical operating voltage and current values (in mA) of the Z1 motes [31].

- *E2E* represents the time taken by a data packet to reach the root node ($T_{received}$) after it is sent by the sender node (T_{sent}). Results are obtained in microseconds and converted into milliseconds (ms):

$$E2E(ms) = \frac{T_{received} - T_{sent}}{10^3} \quad (5)$$

4.4. Simulation Results

We have comparatively assessed performances with and without the attackers. To do that, we have initially simulated a scenario where all nodes function legitimately (i.e., no attacker is present in the network) to reveal baseline performance, which is given in **Table 3**.

Table 3. The baseline performances.

PDR	OVR	APC	E2E
0.995	1781	946.216	483.822

The baseline performance obtained in an environment free from potential attackers (henceforth called a benign environment) reveals a remarkable achievement in PDR, reaching a score of 99.5%. At this level, the E2E reaches approximately 0.5 s. Further examination demonstrates that within this same environment, approximately 1800 control packets are transmitted for the construction and

maintenance of the DODAG, resulting in an estimated energy consumption of around 950 mW.

After obtaining the baseline performance, we have used the GA to evolve a malicious environment by learning the positions and density of the attackers that represent the most challenging network environment. The algorithm has been run five times, and each run spanned 100 generations. The PDR convergence obtained throughout the generations is shown in **Figure 4** in comparison with the one obtained completely in the benign environment.

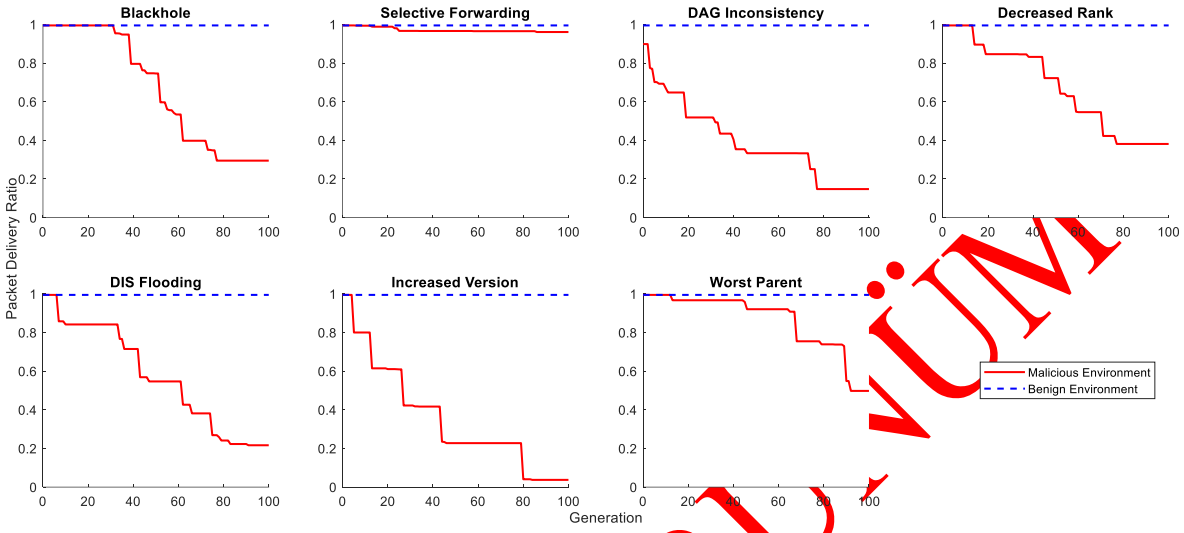

Figure 4. Convergence of the best individuals found by genetic algorithm.

Considering the constraint that up to 20% of network nodes can serve as attacker nodes within the network, the GA encounters initial challenges in identifying the individuals that meet this constraint, except for the DAG inconsistency attack. Consequently, as illustrated in the figure above, the performance in the malicious environment remains consistent with the performance in the benign environment during the early generations.

In addition, by examining the convergence behavior above, one can easily derive the following conclusions: *i*) the GA has a strong capability to acquire knowledge about malicious environments resulting in a PDR decrease, sometimes dropping below 5% (as evident in the case of the increased version attack), *ii*) the decrease in PDR observed for the selective forwarding attack, which is approximately 5‰, is not notably significant, and also *iii*) the blackhole attack exhibits the highest variance, with individual run performances displaying substantial variations, ranging from as low as 0% to as high as 78%.

Figure 5 provides the locations of the top-performing individuals within the network topology, representing an influential decrease in PDR across five runs. Further, we also performed a detailed analysis of the performance achieved for each attack type, considering the evaluation metrics explained in Section 4.3. A comprehensive overview of network performances is outlined in **Table 4**, and the subsequent sections give an elaborate discussion of the results. Please observe the table where the shading is used to highlight the poorest performances in comparison to the baseline performance that is given in **Table 3**, and the changes in the poorest performance are denoted by (▲, ▼) along with respective percentages.

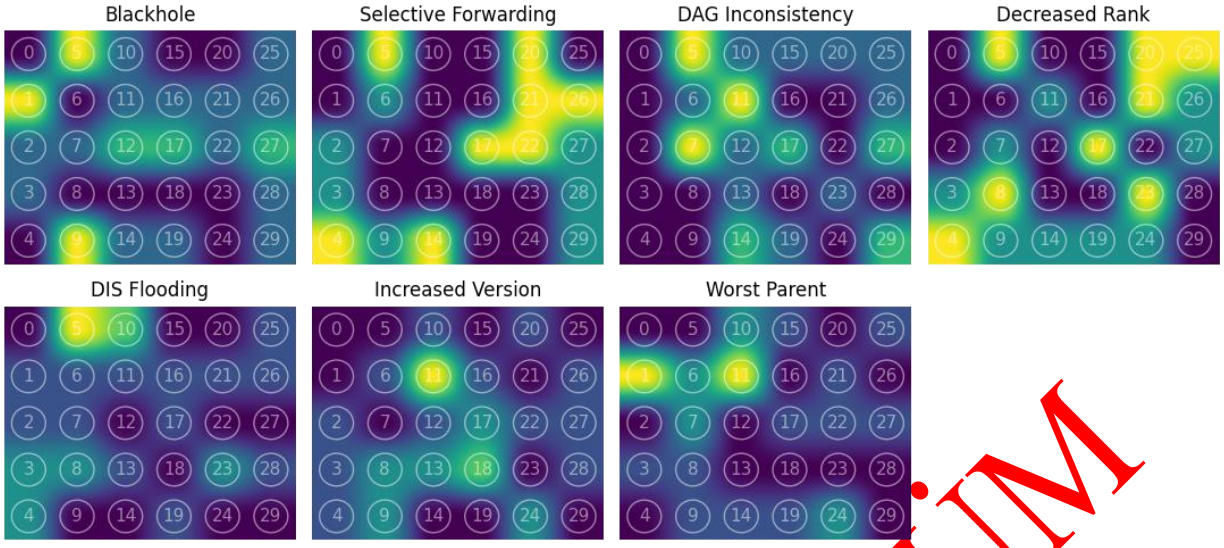

Figure 5. The positions of attackers resulting in the most challenging environment (Note: Light and dark colors represent, respectively, the 'most' and 'least' preferred positions).

Table 4. Network performances obtained in malicious environments.

Attack	#	Attacker IDs	PDR	OVR	APC	E2E
Blackhole	1	1,5,9,12,17,22	0.000(▼100.0%)	493	395.2	0.0
	2	1,5,9,16,29	0.000(▼100.0%)	493	395.2	0.0
	3	7,10,12,14,25,27	0.700	6428(▲260.92%)	1694.4(▲79.1%)	580.9(▲20.1%)
	4	2,9,11,17,27,28	0.784	3977	1170.5	455.7
	5	1,3,5,19,21,26	0.000(▼100.0%)	493	395.2	0.0
Selective Forwarding	1	9,22,26,28	0.992	1904	988.0	507.6
	2	2,4,5,6,21	0.990	1827	910.8	478.3
	3	14,17,20,21,29	0.995	1823	913.4	447.3
	4	3,5,14,26,27	0.997	1974	949.8	462.4
	5	4,17,20,22	0.972(▼2.3%)	2090(▲17.3%)	993.0(▲4.9%)	566.6(▲17.1%)
DAG Inconsistency	1	5,11,13,19,25,29	0.068	3406	1091.6	21.1
	2	5,12,14,17,27	0.068	3647	1130.9	21.5
	3	7,11,14,23,26,27	0.241	3479	1125.5	141.7
	4	5,7,10,20,29	0.066(▼93.3%)	3605	1194.2(▲26.2%)	30.7
	5	6,7,11,15,17	0.184	3840(▲115.6%)	1193.3	164.5
Decreased Rank	1	8,20,23	0.172(▼82.7%)	1315	760.4	84.9
	2	3,4,5,7,21,27	0.379	1469	762.9	224.5
	3	4,5,17,23,25,26	0.590	1570	827.3	293.8
	4	17,19,21,24,25	0.995	1795	944.0	457.5
	5	8,9,11,14,20	0.172(▼82.7%)	2976(▲67.1%)	1209.8(▲27.9%)	84.0
DIS Flooding	1	3,4,5,8,23,28	0.359	113654(▲6281.5%)	9431.6	1596.8
	2	3,5,7,8,10,19	0.168	113610	9444.1	1523.2
	3	5,10,13,16,25	0.170	95529	9942.6	1348.3
	4	1,4,6,10,17,21	0.155(▼84.4%)	113361	11289.3	2161.1
	5	2,5,11,23,26	0.229	96211	11741.7(▲1140.9%)	2469.0(▲410.3%)
Increased Version	1	2,4,9,11,13,27	0.044	5429	1493.8	204.5
	2	8,11,12,13,18,28	0.036	5317	1469.5	76.1
	3	3,9,11,17,18	0.047	5967	1765.1(▲86.5%)	118.1
	4	10,11,20,22,24,26	0.086	6252(▲251.0%)	1681.8	168.1

	5	6,8,16,17,18,24	0.034(▼96.6%)	5258	1477.5	91.9
Worst Parent	**1**	1,3,6,11,21,25	0.762	9750	2781.5	1696.0
	2	1,7,8,9,11,15	0.165	11934	3857.7(▲307.7%)	799.7
	3	1,7,10,11,19,24	0.157(▼84.2%)	12025(▲575.2%)	3729.9	1728.3(▲257.2%)
	4	6,10,11,17,22,27	0.617	9676	2944.2	872.3
	5	1,14,24	0.995	2138	1036.4	558.2

4.4.1 Performance evaluation

***Blackhole*:** As stated earlier, the attacker discards all incoming packets in this attack. Therefore, positioning the attacker on the active routes where the majority of the data traffic is passed can significantly prevent packet transmission to other nodes. Given that a majority of data traffic in LLNs traverses through the root node, attacker nodes near the root node deliberately discard packets, significantly reducing the PDR. The attackers are found to be in 'active' routes in this attack (nodes 1 and 5, see **Figure 5**), and they drop all packets before being transmitted to the root node. Additionally, it has been observed that DIO and therefore DAO packages decreased, preventing DODAG from being established, and intermediate nodes constantly sent requests to join DODAG with DIS packets, thus causing an increase in DIS packets in the network (run 1, 2, and 5; see **Table 4**). The decrease in the number of DIO packets is because they are sent by the root node but dropped by malicious nodes before reaching the sensor nodes. The decrease in the number of DAO packets is closely related to that in DIO packets, as DIO packets announce DODAG information exploited by other nodes to establish the upward routing path. For these runs, a notably decreased APC is observed as DODAG cannot be established. As for the other runs, the attacker nodes are far away from the 'traffic-heavy' regions and the root. They are unable to completely deteriorate the data and control packet transmission performance because they cannot drop all the packets. In this case, new routes could be established, causing an increase in OVR, APC, and E2E.

***Selective Forwarding*:** It is found that the change in network performance, particularly the PDR performance, is not notable here as compared to other attacks. The main reason for that the locations of attackers found by the GA are often far away from the root node where only few data traffic passes on. However, it is inevitable that the impact of this attack increases with an increase in the attacker density, especially when they are in critical positions. To sum up, it has been observed that the effect of this attack is generally limited compared to the blackhole attack, and threshold value for attacker to drop packets (adopted as 50% in this study) should be increased to significantly increase the impact of this attack. In the most challenging environment (run 5, see **Table 4**), in comparison with the benign environment (**Table 4**), the change in PDR and APC is less than 5%, whereas it is about 17% for OVR and E2E.

***DAG Inconsistency*:** It is observed that the overall performance significantly decreases in this attack. As explained earlier, attackers lead to inconsistency by illegitimately manipulating the 'O' and 'R' flags in this attack. This results in continuous local repair in the network and, hence, the dropping of packets by the nodes. It is observed that the PDR performance dramatically downs up to 6% (runs 1, 2, and 4; see **Table 4**), especially when the attackers are one hop away from the root node. As a result of the attack, DIO packets are propagated to restart route discovery. This causes an excessive OVR in the network for all runs, resulting in a part of the network becoming isolated, and even packets may be dropped by the benign nodes. Dropping the packets without being transmitted also reduces E2E because only successfully transmitted packets are considered for evaluation. Finally, the unnecessary initiation of the local repair process by the nodes increases the APC in the network.

***Decreased Rank*:** This attack is carried out as a preliminary step and used to increase the impact of other attacks when they are simultaneously applied in the network. Pretending to have a lower rank value, the attacker aims to attract most of the network traffic and thus exploits the incoming traffic by activating different attacks (usually blackhole, selective forwarding, etc.). From the results, it is seen that the PDR performance of the network drops up to 17%, especially when nodes 8 and 20 are selected as attacker nodes (runs 1 and 5; see **Table 4**). Moreover, OVR and APC performances significantly reduce in such challenging environment, while the change in E2E performance is not notable.

***DIS Flooding*:** The attacker nodes constantly send DIS packets in this attack, causing an unnecessary propagation of DIO packets and hence traffic congestion. The analysis results show that the attack is effective when it is far away from each other and has more neighbor nodes. In other words, degradation in performance is not notable if the attackers are located one hop away from each other and have fewer victim neighbor nodes. The PDR performance downs up to 15.5% in this attack (run 4; see **Table 4**). Because the attackers send DIS packets to their neighbors and wait for a DIO, many control messages are generated in the network. This causes a dramatic increase in OVR, APC, and E2E.

***Increased Version*:** Increasing illegitimately the version number in DIO packets, the attackers continuously trigger the repair process, ultimately dropping data packet transmission. It is observed in PDR performance that a large number of the packets do not reach the root node, and especially critically positioned attackers can cause significant damage to the network. Based on a small number of transmitted packets, the E2E performance declines. Since global and local repair maintenance is triggered repeatedly, there are too many control packets propagating in the network, resulting in an increase in OVR (almost a 10-fold increase in DIO packets is observed) as well as in APC.

***Worst Parent*:** The data packets that are supposed to be sent to the root are prevented from being transmitted on the optimal route according to the objective function. However, the attacker selects the worst parent node from the parent list and forwards the incoming packets through it. In line with the findings, it has been observed that the PDR performance decreases more, especially when the nodes close to the root node are selected as attackers. This is because the traffic flow becomes denser as it approaches the root node. For this reason, the attackers disrupt the flow of traffic at a higher rate and perform suboptimal routing. In such circumstances, the PDR reaches approximately 15% (runs 2 and 3; see **Table 4**). Additionally, in comparison to the baseline performance (**Table 4**), a dramatic increase in OVR, APC, and E2E is observed in all runs. Note that a lower impact on network performance is often achieved when attackers are away from the root (run 5; see **Table 4**).

In summary, the findings from the experiments reveal that the appropriate identification of the position as well as the density of attackers through GA significantly deteriorates the network performance. Although this impact varies depending on the types of attacks, it is shown that the adverse effect of the 'best' selection by GA may reach a catastrophic level where the network is nearly not operable. Analysis of the outcomes revealed distinct impacts of each attack on the network. Speaking concretely, blackhole, DAG inconsistency, and increased version attacks emerged as the most detrimental, significantly impairing network performance due to dropping large number of packets. In some instances, strategically positioned attackers drop all of packets (in blackhole attack), resulting in the network becoming entirely unusable. In contrast to these attacks, the selective forwarding attack, which may easily deceive intrusion detection system by selectively dropping packets, caused a lowest impact on network performance, even when attackers are strategically positioned using GA. This clearly proves that the performance evaluation of RPL attacks based on a scenario where the attackers are positioned in a random manner becomes unhelpful for security practitioners seeking to take effective measures against these attacks.

It is worth noting here that certain GA parameters are initially set to default values of ECJ, and optimizing these parameters can improve the effectiveness of GA, and hence the attacks. Although the majority of attacks contribute to heightened APC and generate a negative impact by increasing OVR, this adversarial performance may become even more evident, particularly when the positions of attackers are determined with the optimal parameter values of GA, which may be regarded as a limitation of the current study.

5. CONCLUSION

This study explores the vulnerabilities of RPL-based networks when they are targeted by malicious nodes. Because of the extent to which the intruder effect is heavily related to position and density, we mainly focus on a most challenging network environment where the attack diminishes performance at its highest level, which is possible by GA in this study. It is found that RPL-based networks are vulnerable to attacks and that the use of GA plays a critical role in finding how large the selection of attacker's position and density affect the performance. This study considers a static environment where the nodes are immobile, which is the main limitation when contemplating IoT applications, where IoT nodes are occasionally mobile during operation. So, analysis of the attack on 'most challenging mobile environment' can be a potential future direction of this study. Additionally, investigation of RPL networks under hybrid attacks, specifically examining their maximum impact by concurrently worsening multiple metrics of the network, is worth studying in the future. We plan to broaden the scope of this study to explore these issues in the future.

ACKNOWLEDGEMENT

This study is funded by the Scientific and Technological Research Council of Turkey (TUBITAK-122E331). We would like to thank TUBITAK for its support.

DECLARATION OF ETHICAL STANDARDS

The author(s) of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

AUTHOR'S CONTRIBUTION

Özlem CEVİZ: Conducted the experiments, analyzed the outcomes, and composed manuscript.

Selim YILMAZ: Conducted the experiments, analyzed the outcomes, and composed manuscript.

CONFLICT OF INTEREST

There is no conflict of interest in this study.

REFERENCES

[1] Shah S. H. and Yaqoob I., "A survey: Internet of Things (IOT) technologies, applications and challenges", ***4th IEEE International Conference on Smart Energy Grid Engineering***, 381-385, (2016).

[2] Balaji S., Nathani K., and Santhakumar R., "IoT Technology, Applications and Challenges: A Contemporary Survey", ***Wireless Personal Communications***, 108(1): 363-388, (2019).

[3] Columbus L., "Roundup of the Internet of Things Forecasts and Market Estimates", ***Forbes Tech***, (2016).

[4] Winter T. and Thubert P., "RPL: IPv6 Routing Protocol for Low power and Lossy Networks", ***IETF Internet-Draft***, (2010).

[5] Holland J.H., "***Adaptation in natural and artificial systems : an introductory analysis with applications to biology, control, and artificial intelligence***", MIT Press, (1992).

[6] Kim H.S., Ko J., Culler D.E., and Paek J., "Challenging the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL): A Survey", ***IEEE Communications Surveys and Tutorials***, 19(4): 2502-2525, (2017).

[7] Almusaylim Z.A., Jhanjhi N.Z., and Alhumam A., "Detection and mitigation of RPL rank and version number attacks in the internet of things: SRPL-RP", ***Sensors***, 20(21), (2020).

[8] Mayzaud A., Sehgal A., Badonnel R., Chrisment I., and Schönwälder J., "A study of RPL DODAG version attacks", ***Lecture Notes in Computer Science***, 92-104, (2014).

[9] Mayzaud A., Badonnel R., and Chrisment I., "A taxonomy of attacks in RPL-based internet of things", ***International Journal of Network Security***, 18(3): 459-473, (2016).

[10] Katoch S., Chauhan S.S., and Kumar V., "A review on genetic algorithm: past, present, and future", ***Multimed Tools Appl***, 80(5): 8091–8126, (2021).

[11] Bütün İ., "Security Implications of Underlying Network Technologies on Industrial Internet of Things", ***Politeknik Dergisi***, 25(1): 223–229, (2022).

[12] Taş O. and Kiani F., "Nesnelerin İnterneti (IoT) ve Kablosuz Algılayıcı Ağların Güvenliğine Yapılan Saldırıların Tespit Edilmesi ve Önlenmesi", ***Politeknik Dergisi***, 24(1): 219–235, (2021).

[13] Calp M.H. and Bütüner R., "Makine Öğrenimi Algoritmaları Kullanılarak IoT Tabanlı Ağ Cihazlarına Yönelik Siber Saldırıların Tespiti", ***Journal of Polytechnic***, (2023).

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

[15] Bang A. and Rao U.P., "Impact Analysis of Rank Attack on RPL-Based 6LoWPAN Networks in Internet of Things and Aftermaths", ***Arab J Sci Eng***, 48(2): 2489–2505, (2023).

[16] Ghaleb B., Al-Dubai A., Hussain A., Ahmad J., Romdhani I., and Jaroucheh Z., "Resolving the Decreased Rank Attack in RPL's IoT Networks", (2023).

[17] Rai K.K. and Asawa K., "Impact analysis of rank attack with spoofed IP on routing in 6LoWPAN network", ***2017 10th International Conference on Contemporary Computing***, (2018).

[18] Rehman A., Khan M.M., Lodhi M.A., and Hussain F.B., "Rank attack using objective function in RPL for low power and lossy networks", ***2016 International Conference on Industrial Informatics and Computer Systems***, (2016).

[19] Ambarkar S.S. and Shekokar N., "Impact Analysis of RPL Attacks on 6Lo WPAN based Internet of Things network", ***7th IEEE International Conference on Electronics, Computing and Communication Technologies***, (2021).

[20] Aris A., Oktug S.F., and Berna S., "RPL version number attacks: In-depth study", ***2016 IEEE/IFIP Network Operations and Management Symposium***, 776-779, (2016).

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

[22] Sharma G., Grover J., and Verma A., "Performance evaluation of mobile RPL-based IoT networks under version number attack", ***Comput Commun***, 197: 12-22, (2023).

[23] Bokka R. and Sadasivam T., "DIS flooding attack Impact on the Performance of RPL Based Internet of Things Networks: Analysis", 1017-1022, ***Proceedings of the 2nd International Conference on Electronics and Sustainable Communication Systems***, (2021).

[24] Rajasekar V.R. and Rajkumar S., "A Study on Impact of DIS flooding Attack on RPL-based 6LowPAN Network", ***Microprocess Microsyst***, 94, (2022).

[25] Pu C., "Mitigating DAO inconsistency attack in RPL-based low power and lossy networks", ***8th***

Annual Computing and Communication Workshop and Conference, 570-574, (2018).

[26] Hkiri A., Karmani M., and MacHhout M., "The Routing Protocol for low power and lossy networks (RPL) under Attack: Simulation and Analysis", ***5th International Conference on Advanced Systems and Emergent Technologies***, 143-148, (2022).

[27] Dogan C., Yilmaz S., and Sen S., "Analysis of RPL Objective Functions with Security Perspective", ***Proceedings of the 11th International Conference on Sensor Networks***, 71-80, (2022).

[28] Alsukayti I.S. and Alreshoodi M., "RPL-Based IoT Networks under Simple and Complex Routing Security Attacks: An Experimental Study", ***Applied Sciences***, 13(8), (2023).

[29] Österlind F., Dunkels A., Eriksson J., Finne N., and Voigt T., "Cross-level sensor network simulation with COOJA," ***Conference on Local Computer Networks***, 641-648, (2006).

[30] **www.contiki-os.org**, "Contiki-OS", (2024).

[31] Bandekar A., Kotian A., and Javaid A.Y., "Comparative analysis of simulation and real-world energy consumption for battery-life estimation of low-power IoT (Internet of Things) deployment in varying environmental conditions using Zolertia Z1 motes", ***Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering***, 137–148, (2017).