Journal of Electrical Engineering, Vol. 75, No. 3, 2024, pp. 204-213

sciendo

PAPERS

Exploring and mitigating hybrid rank attack in RPL-based IoT networks

Mehdi Rouissat [1,2], Mohammed Belkehir [3], Allel Mokaddem [3],
Merahi Bouziani [4], Ibrahim Sulaiman Alsukayti [5]

Despite the widespread adoption of the Routing Protocol for Low-power and Lossy Networks (RPL) in IoT environments, its inherent limitations in addressing security vulnerabilities have left IoT networks vulnerable to ongoing attacks. This paper introduces a novel intrusion detection system tailored specifically for IoT networks, with a focus on mitigating attacks at the network's edge. The study presents the Hybrid Rank Attack (HRA), a sophisticated threat exploiting RPL vulnerabilities by alternately advertising decreased and increased rank values in control messages. Extensive experimentation evaluates the detrimental effects of HRA on critical network metrics including exchanged messages, energy consumption, PDR, latency, and memory footprint. Additionally, a lightweight and distributed countermeasure algorithm is proposed to effectively mitigate the impact of HRA. Simulation-based evaluations demonstrate significant reductions in control overhead (68.7%) and energy consumption (61.83%), with minimal additional RAM utilization (1.05%). This lightweight solution enhances the resilience of RPL-based IoT networks against HRA threats.

Keywords: RPL, IoT, rank attack, security, Contiki, cooja

1 Introduction

In recent years, our world has undergone a transformative technological revolution propelled by the pervasive integration of IoT networks into every facet of our daily lives [1-3]. The advent of IoT networks has ushered in a profound shift, creating self-automated environments geared towards facilitating seamless data exchange between processes. This has been instrumental in leveraging internet capabilities [4]. Despite the remarkable evolution exhibited by IoT technology, they remain vulnerable to various attacks, posing a significant challenge for researchers and network administrators [5-7]. This work specifically addresses the rank attack, where malicious actors attempt to manipulate the hierarchical structure, potentially disrupting the communication and collaboration between IoT devices. In response to this challenge, our paper introduces a novel attack termed the Hybrid Rank Attack (HRA). This attack method involves a malicious node alternately advertising both decreased and increased rank attack values in its DIOs. The aim is to simultaneously impact networks through both the Decrease Rank Attack (DRA) and the Withheld Parent Attack (WPA), while also inducing victim nodes to continually switch their preferred parents. This tactic results in destabilizing the network's edge, causing significant disruption. We compare the detrimental effects of our proposed attack with the well-known decrease rank attack [8], where illegitimate nodes advertise lower rank values to gain favorable network positions and capture a maximum number of nodes as hostages. Additionally, we present a lightweight, distributed algorithm wherein each node monitors the activity of its preferred parents as a countermeasure. Our proposed solution demonstrates efficiency in terms of generated and received control overhead, energy consumption, and node resource utilization.

2 RPL overview and HRA attack description

2.1 RPL overview and rank calculation

Routing Protocol for Low-Power and Lossy Networks (RPL) is a protocol designed for Low-Power and Lossy Networks (LLNs), which typically consist of limited and resource-constrained devices in terms of processing, storage, and energy [9]. RPL facilitates efficient and reliable communication among such

[1] Univeristy Center Nour Bachir, El-Bayadh, Algeria
[2] STIC Laboratory, University Aboubekr Belkaid, Tlemcen, Algeria
[3] LIMA Laboratory, Univeristy Center Nour Bachir, El-Bayadh, Algeria
[4] LTTNS Labortory, Djillali Liabes University, Sidi Bel Abbes, Algeria
[5] Department of Computer Science, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia
m.rouissat@cu-elbayadh.dz, m.belkheir@cu-elbayadh.dz,
a.mokaddem@cu-elbayadh.dz, bouzi_mera@hotmail.com, skiety@qu.edu.sa

https://doi.org/10.2478/jee-2024-0025, Print (till 2015) ISSN 1335-3632, On-line ISSN 1339-309X

devices by establishing and maintaining routes in the network. In RPL, the devices within a network are organized into a loop-free topology of nodes, directing traffic upwards towards a root node (see Fig. 1), creating a tree-like topology, known as a DODAG (Destination Oriented Directed Acyclic Graph) [10]. The assignment of rank values to network nodes follows a specific algorithm. The rank value of a node is determined by adding the rank value advertised by the parent node, to the Link Metric to that parent. The calculation of the rank value is governed by the objective function, which employs the following formula:

$$Rank_{node} = L_m \times \left(1 + floor(R_p/MHRI)\right) \quad (1)$$

where

- L_m is the link metric,
- R_p is the rank of the parent,
- $MHRI$ is the Minimum Hope Rank Increase.

Then, the metric value is then multiplied by the 'floor' function which computes the greatest integer less than or equal to the given value. Nodes closer to the root node will have lower rank values, while nodes further away will have higher rank values. The objective function defines the criteria for calculating these rank values, considering factors such as energy consumption, link quality, and path length [11].

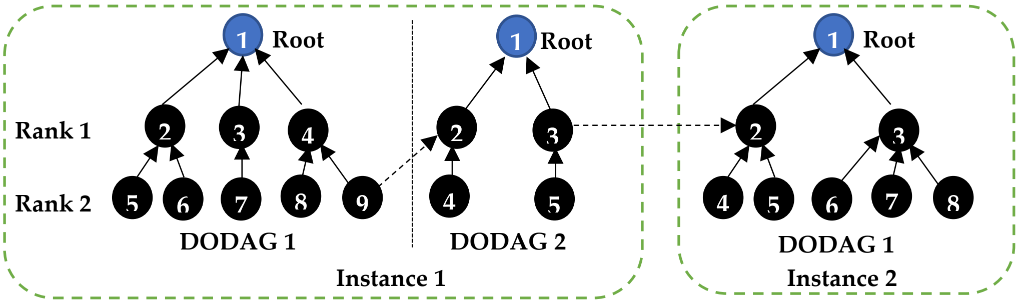

Fig. 1. RPL topology and DODAG construction

In addition, RPL employs the Trickle algorithm [12] during the creation and upkeep of topology to minimize control traffic and network overhead. This algorithm regulates the transmission frequency of DIO messages based on network stability.

2.2 Attack description

In its fundamental design, RPL lacks mechanisms to prevent the advertisement of falsified rank values. This absence leaves a vulnerability that can be exploited by malicious nodes, allowing them to broadcast counterfeit rank values with the intention of becoming parents to a significant portion of the network's nodes. As a result, the Decreased Rank Attack (DRA) is a well-known attack in RPL-based IoT networks, by which the malicious node advertises a lower rank value than the reel value it should advertise. Consequently, this malicious node can be frequently selected by the other nodes as the preferred parent, and gain a strategic position in the network by having numerous indirect and direct children nodes. On the other hand, an increased rank attack, known as Worst Parent Attack (WPA) is also a well-known attack, in which the node announces a higher rank value than its own, targeting the network topology, where usually it is not chosen as preferred parent despite its good position, which leads to create suboptimal paths.

Both attacks; DRA and WPA are based on advertising a falsified rank value. In this article, we propose a Hybrid Rank Attack (HRA), where the malicious node advertises, alternatively, a decreased Rank attack value and an increased rank attack in its DIOs. The main purpose of the attack is to affect the networks by both attacks at once; DRA and WPA, besides pushing the victim nodes to continually switch their preferred parents. The hybrid attack may create instability in the topology, where it is selected as the preferred parent in the decreased rank attack, and it is replaced when advertising a decreased rank value, where the topology experiences the two attack effects besides the permanent parent switching behavior. According to RPL-Contiki, replacing a preferred parent requires a node to:

- Send a No-Path DAO message to its current preferred parent,
- Send a regular DAO to the newly selected preferred parent,
- Resent the trickle timer.

This additional activity engenders useless exchanges of DAO messages, and instability in the network, which pushes the nodes to continually reset their DIO trickle timers and send more frequent DIO messages.

Considering DODAG 1 in the example network presented in Fig. 1, let’s assume that node 6 initiates an HRA attack by advertising a decreased rank value at first. This would cause changes to the topology as neighbor nodes such as nodes 5 and 7 would reattach to node 6. As a result, node 5 and 7 would unnecessarily switch their preferred parents and perform the three actions mentioned above. Upon completing the DRA, node 6 then starts advertising an increased rank value causing nodes 5 and 7 to switch their preferred parent back again. Node 6 can keep alternating between the two variants of the rank attack to keep the topology unstable. As long as the attack stays undetected, DODAG 1 would experience frequent unnecessary parent switching leading to degraded overall network performance.

3 Related works

Recent research has seen a surge in efforts to explore and address ranks. For example, in [13], the susceptibility of RPL to diverse attacks, particularly rank-based ones like the decreased rank attack, has been thoroughly examined. These studies shed light on the potential consequences of such attacks on the network's routing hierarchy and overall performance metrics. Additionally, in [14], two silent rank attacks, LPRA (Like Parent's Rank Attack) and BPRA (Better than Parent's Rank Attack), are delineated. LPRA involves a malicious node mimicking its preferred parent's rank value, while BPRA exploits Contiki RPL inconsistencies to advertise a superior rank without causing topology loops. Moreover, findings from experiments conducted on randomly constructed topologies reveal significant impacts on network behavior, including increased control overhead and energy consumption, as well as latency surges.

In [15], a solution named LEACE (Level-based Energy-Aware Rank-based Attack Countermeasure) is introduced to detect and thwart rank attacks by aligning the ranks and levels of nodes. Additionally, in [16], a lightweight solution called DSRPL (DIOF-Secure RPL) is discussed to combat flooding attacks in RPL-based networks. This solution is based on a collaborative and distributed security scheme that verifies updates received by nodes before trust is established. In [17], a streamlined and effective technique for managing and containing rank attacks was introduced. A newly developed Echelon Metric Based Objective Function (EMBOF) was implemented instead of the default RPL to verify the validity of the advertised rank. The Echelon value is determined through additive collaboration between the root node and its associated parent node(s) within the RPL network structure. The focus was not only to identify the attacker node(s) but also to promptly isolate them. In [18], the proposed E-RAD (Enhanced-Rank Attack Detection) algorithm incorporates a rate-limiting mechanism to regulate the production of DIO (DODAG Information Object) packets. Additionally, it employs DIS (DODAG Information Solicitation) messages to identify and isolate rank attackers. Should an attacker elude detection through these means, their presence can be revealed by verifying the consistency of hash values in DAO (Destination Advertisement Object) messages. Upon detection, an alarm is triggered against the rank attackers immediately.

Other proposals introduced advanced solutions based on machine-learning approaches. In [19], a novel lightweight multiclass classification-based attack detection model tailored for RPL-based sensor networks, termed MC-MLGBM, is proposed. This model addresses the lack of suitable datasets by generating a new dataset through diverse network models. Employing optimal feature selection techniques and a light gradient boosting machine-based algorithm, MC-MLGBM enhances performance in detecting multiclass attacks. In [20], an artificial neural network (ANN) framework was proposed for identifying decreased rank attacks. It comprised three main phases: data pre-processing, feature extraction utilizing a random forest classifier, and an artificial neural network model implemented for detection purposes. Another ANN-based solution was also proposed in [21] which introduced an IDS based on the Multi-Layer Perceptron (MLP) neural network to help in verifying and classifying normal and abnormal network traffic. In [22], the proposed approach was based on employing anomaly detection with Support Vector Machines. The focus was on the healthcare sector, particularly smart hospitals, which present multifaceted challenges.

The study in [23] focused on a trust-based model to enhance security in RPL networks against attacks, specifically Rank and Blackhole attacks. The research delves into the vulnerabilities posed by these attacks in the context of both static and mobile nodes within the Internet of Things (IoT) environment. A similar approach was also proposed in [24] which was based on a mitigation scheme using a trust threshold strategy.

Moreover, recent works continue to explore solutions for various well-known attacks against RPL-based IoT networks [25]. These efforts collectively contribute to enhancing the security posture of RPL-based IoT networks and mitigating the risks posed by different types of attacks. In this paper, the proposed solution is based on a lightweight approach with limited, where the distributed mitigation solution is the major novelty of this work as shown in Tab. 1.

Table 1. Related work comparison

Reference	Approach	Solution	Attack
[15] LEACE	In-protocol Modification	aligning the rank and level of nodes	Increase Rank
[16] DSRPL		a collaborative and distributed security scheme	Rank Calculation
[17] EMBOF-RPL		Echelon Metric Based Objective Function (EMBOF)	Increase Rank
[18] E-RAD		A DIO exchange rate limiting mechanism	Increase Rank
[19] MC-MLGBM	Machine Learning	Multiclass classification-based attack detection model	Increase Rank
[20]		An artificial neural network (ANN) framework	Decrease Rank
[21]		an ANN-IDS based on the Multi-Layer Perceptron (MLP)	Increase Rank
[22]		Anomaly detection with Support Vector Machines	Increase Rank
[23]	Trust-based Model	Addressing static and mobile environments	Increase Rank
[24]		A trust threshold strategy	Increase Rank
This study	In-protocol Modification	A distributed algorithm based on Monitoring parent activities	Hybrid Rank

4 Studied topology

We have chosen a random topology composed of 20 nodes, including the sink (node 1) and the malicious node (node 20), as Fig. 2 shows. Note that the malicious node was configured to be three hops away from the sink, and to have 7 neighbors. This was set up to represent a practical scenario that is approximate between the best and worst-case scenarios.

Z1 motes were utilized in our simulations. Every node has the same properties, including the intruding node. Equation (1) is used as the basis for obtaining data about energy consumption using the powertrace tool, which is natively implemented in Contiki. The following formula, implemented in a Perl script, is used to calculate the energy consumed by a specific node for a certain mode in millijoules:

$$Consumed_{energy} = \frac{Energest \times I \times V}{Rtimer}, \qquad (2)$$

where

Energest presents the number of recorded ticks for each energy mode,
I is the current,
V is the voltage,
Rtimer is the number of ticks per second.

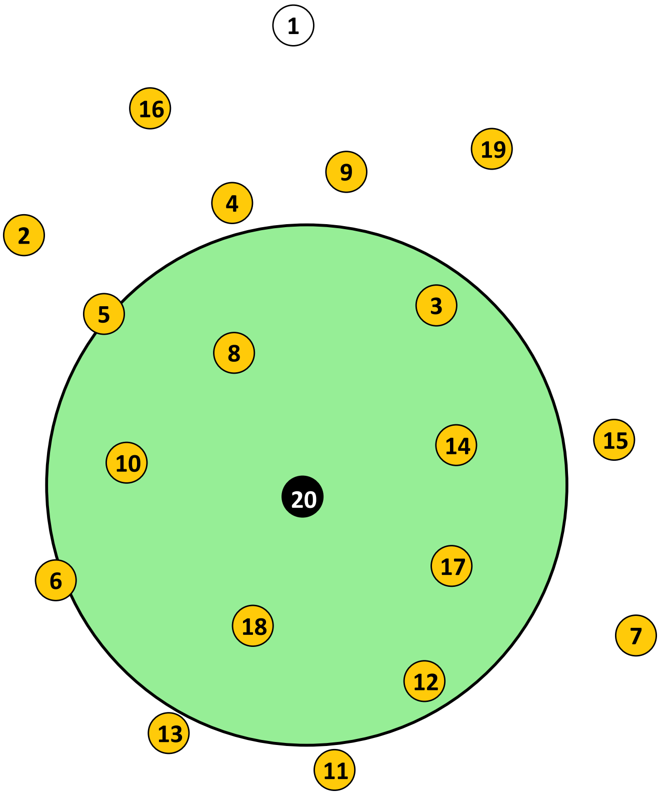

Fig. 2. Studied topology

5 Results and discussion

In this section, we present and elucidate the detrimental impact of the traditional DRA, as well as the proposed HRA. We then go on to show how our suggested approach might mitigate the impact of the HRA. The following metrics and indicators are used to evaluate the impact of the attacks and performance of the proposed approach:

- Control packet overhead,
- Consumed energy,
- PDR,
- Latency
- Memory footprint.

5.1 Impact of DRA and HRA

The foundation of both the DRA and HRA attacks is the dissemination of a falsified rank value. In this subsection, we show the impact of both attacks on the different network metrics.

5.1.1 Control overhead

Table 2 shows the exchanged overhead during 20 minutes of simulation for the studied scenarios. Note that Table 2 is split into two sections: one for the number of generated control messages and another for the number of forwarded control messages. Table 2 shows that DRA causes a remarkable increase in the total overhead from 931 to 3933 messages, where all the types of generated and forwarded messages witnessed that increase, especially no-path DAO messages.

Table 2. Network overhead results: sent messages

	Sent Messages						
	Generated				Forwarded		Total
Scenario	DIS	DIO	DAO	No-Path DAO	DAO	No-Path DAO	
Attack free	19	363	178	20	339	12	931
DRA	19	1148	641	571	1221	333	3933
HRA	19	1758	902	905	1603	500	5687

Conversely, the hybrid attack demonstrates a dramatic increase compared to the attack-free case, where it shows an increase of 5678 messages. All types of messages show that increase, where the most touched type is no-path DAO messages.

The parameters that affected the increase of exchanged overhead are summarized in Table 3. The obtained results show that the number of received DIOs with infinite rank value jumped to 62 messages in DRA and to 326 in the case of HRA, where the most significant increase is shown in the preferred parent changing, where 721 changes in the HRA had been recorded compared to only 12 changing in the attack free topology.

On the other hand, 463 loops are detected in HRA compared to 242 in DRA and zero loops in the attack-free topology. The highest number of loops is recorded by the malicious node itself, with 44 loops. When the malicious node announces a lower value of rank its victim children nodes use that value as base rank value, and when the malicious node advertises the higher rank value (alternative advertisement) it sees the advertised rank value from its children victim node lower, which create loops in the topology.

Table 3. Statistics of factors leading to trickle timer reset

	Attack free	DRA	HRA
Infinite rank received	0	62	326
Changed preferred parent	12	431	721
Local repair	0	0	0
Loops	0	242	463

Table 4. Network overhead results: received messages

	Received messages			
Scenario	DIS	DIO	DAO	Total
Attack free	21	962	544	1527
DRA	21	2886	2540	5447
HRA	21	4275	3539	7835

Another important parameter is taken into account in our analysis, which is the number of received messages, see Tab. 4. It can be considered as a decisive parameter to analyzing the impact of the attacks in the listening mode. The DRA shows an increase to 5447 received messages compared to 1527 received messages in the attack free case, where the HRA shows the highest record with 7835 received messages, presenting an increase of 413%. These obtained results allow to understand the variation in the consumed energy, in the listening mode in particular.

5.1.2 Energy consumption

Figure 3 illustrates the consumed energy in the studied scenarios, in terms of Low Power Mode (LPM), CPU TX, and RX. According to the results, the total consumed energy has shown an increase from 26.32 Joules recorded in the normal topology to 73.8 Joules in the DRA, presenting an increase of 280%, that is the direct result of the higher exchanged overhead due to the instability of the topology. When it comes to the HRA it presents an immense increase of 373 % compared to the first scenario, which is the result of the highest exchanged overhead due to the attack. These results how the HRA negatively effects on the node’s energy, which has a significant influence on node autonomy and, in turn, network longevity.

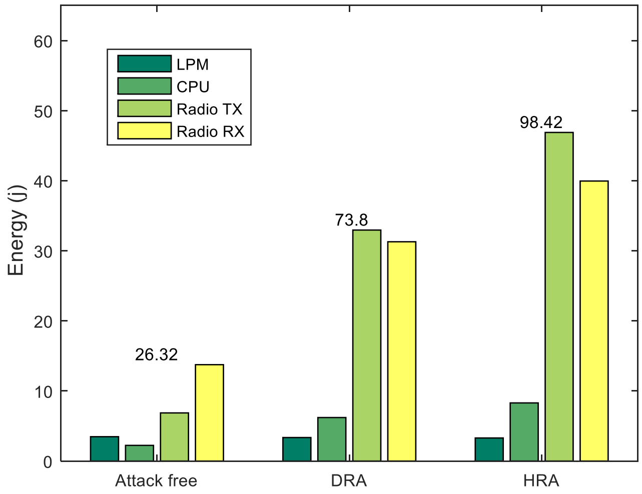

Fig. 3. Energy consumption results

5.1.3 PDR and latency

PDR (Packet Delivery Ratio) shows the ratio of the total number of packets sent by network's nodes and successively received by the sink node. Thus, it is a metric used to assess the network's end-to-end dependability, and evaluate the paths availability toward the sink node. The results regarding the PDR are presented in Table 6. The results illustrate that PDR degrades under the HRA, with a ratio of 60%, while a ratio of 79.4% is obtained in the case of DRA. This immense deterioration is mostly the result of high traffic and collisions of packets as a result of the high exchanged overhead, particularly in the neighborhood of the malicious node, where the effect of a high ratio of parent switching can be observed. The PDR (Packet Delivery Ratio) shows the ratio of the total number of packets sent by network's nodes and successively received by the sink node. Thus, it is a metric used to assess the network's end-to-end dependability, and evaluate the paths availability toward the sink node. The results regarding the PDR are presented in Tab. 5. The results illustrate that PDR degrades under the HRA, with a ratio of 60%, while a ratio of 79.4% is obtained in the case of DRA. This immense deterioration is mostly the result of high traffic and collisions of packets as a result of the high exchanged overhead, particularly in the neighborhood of the malicious node, where the effect of a high ratio of parent switching can be observed.

Table 5. PDR and latency results

Scenario	PDR (%)	Latency (s)
Attack free 2	99.7	0.243
DRA	79.4	0.746
HRA	60	0.889

The recorded delay for the three scenarios is displayed in Table 5. The results show that the HRA had a large effect on latency, which increased to 0.746 seconds in the case of DRA, and up to 0.889 seconds in HRA. These results show how damaging is the HRA, where all the networks’ parameters have shown noticeable degradation.

5.2 Countermeasure

To address the HRA, a lightweight mitigation solution is developed, based on a distributed approach, in which every node supervises the activity of its own preferred parents, where, as presented in Algorithm 1, where “sus_behvr” presents the number of times a suspicious behavior is detected. The algorithm works as follows:

- DIOs from blacklisted parents are not treated,
- If a node receives a higher rank value from its preferred parent more than three times (sus-behvr superior or equal to 3), then this parent will be removed and blacklisted. Note that making it three times is a design parameter, choosing a higher value may lead to a delay in detecting the attack whereas a lower value may lead to a false positive detection,

- In order to avoid blacklisting a parent node that is a victim of the malicious node, this victim parent node will send an infinite rank value in its next DIO message right after detecting the malicious behavior, discarding the rank value of the suspect parent.

Algorithm 1 HRA Mitigation Solution

```
Begin
if (sender is not blacklisted)
    if (sender is the preferred parent)
        if (advertised rank = infinite)
            sus_behvr = 0
        else if (advertised rank > node's rank)
            if (sus_behvr $\geq$ 3)
                preferred parent removed
                preferred parent blacklisted
                sending DIO (rank = infinite)
            else
                sus_behvr = sus_behvr + 1
            end if
        end if
    end if
else
    ignore the received DIO message
end if
end
```

This distributed treatment is considered lightweight and allows to avoid extra exchange of control messages among the nodes or, dedicating additional fields in the control messages. The proposed approach has proved its efficiency in detecting the malicious behavior as shown in Tab. 6. The table shows that the attack is detected by the victim nodes after three receiving three times higher rank value from the preferred parent, where node 17 was the first node that detected the malicious behavior after 296 seconds, and node 8 was the last one where it detected the attack after 361 seconds.

Table 6. The suspect behavior's detection chronology

Node	First suspect behavior	Second suspect behavior	Third suspect behavior
17	44 s	74 s	296 s
18	44 s	80 s	296 s
14	44 s	80 s	296 s
12	80 s	174 s	350 s
8	296 s	350 s	361 s

5.2.1 Control overhead

Table 7, summarizes the obtained exchanged overhead before and after implementing the proposed mitigation. The results show that the mitigation solution has succeeded in bringing down the total overhead to a total of 1777 messages, which presents a significant decrease.

Note that the total recorded overhead is affected by the quantity of messages before the detection of the attack. As depicted by Fig. 4, 83.25% of the total overhead had been exchanged before the eighth minute. For instance, 265 messages are generated in the last 12 minutes in the case of the attack-free topology, whereas 280 messages are generated for the same period after implementing the proposed mitigation approach. These results prove that the extra messages are generated before detecting the malicious behavior.

Table 7. Network overhead results: sent messages

	Sent Messages						
	Generated				Forwarded		Total
Scenario	DIS	DIO	DAO	No-Path DAO	DAO	No-Path DAO	
Attack free	19	363	178	20	339	12	931
DRA	19	1148	641	571	1221	333	3933
HRA	19	1758	902	905	1603	500	5687
After Solution	19	633	295	144	607	79	1777

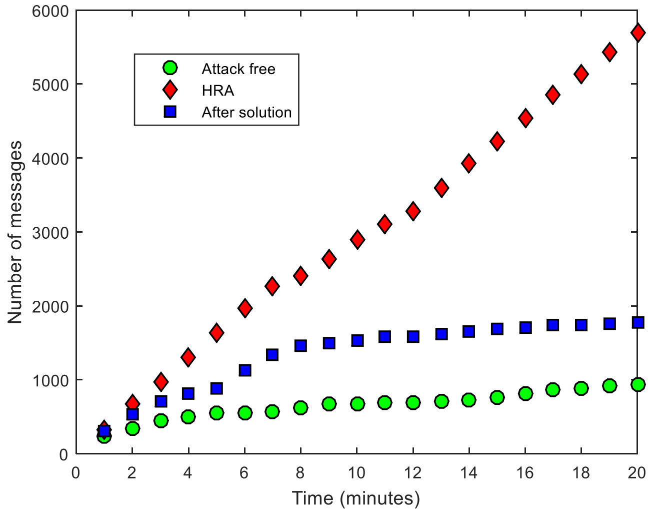

Fig. 4. Total of generated messages through time

5.2.2 Energy consumption

As shown in Fig. 5, the developed method effectively decreased the consumed energy from 98.42 Joules to 37.56 Joules, a drop of 61.83%. These obtained results validate the effectiveness of the proposed approach in reducing the attack's harmful impacts on the consumed energy, where the difference in the consumed energy is used prior to the attack detection.

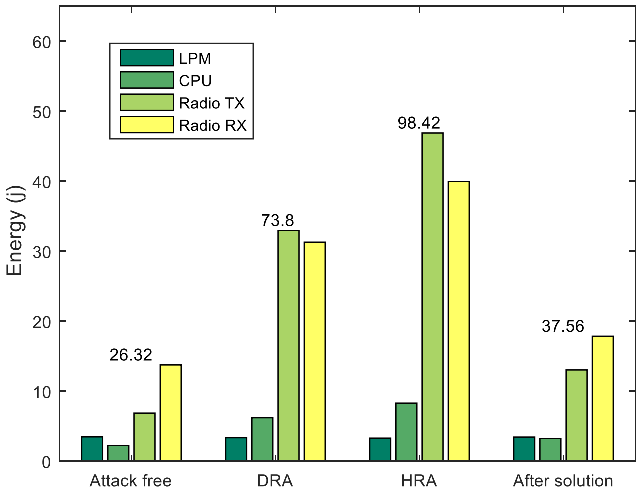

Fig. 5. Energy consumption before and after implementing the proposed approach

5.2.3 PDR and latency

The results presented in Table 8 illustrate the effectiveness of the proposed solution in mitigating the impact of HRA on PDR and Latency. Compared to HRA results, the proposed solution succeeded in maintaining high PDR and low latency with improvements of more than 60% in both. Only a little PDR reduction of less than 2% and a latency rise of less than 0.1 seconds were experienced by the proposed solution compared to the standard RPL.

Table 8. PDR and latency results

Scenario	PDR (%)	Latency (s)
Attack free 2	99.7	0.243
HRA	60	0.889
Modified RPL	98	0.311

5.2.4 Memory footprint

Nodes in RPL networks, and Z1 in particular are frequently installed with built-in restrictions. They often only have a small amount of Flash Memory and RAM, as Table 10 depicts, where the employed Z1 nodes are limited to 20 and 100 kilobytes of RAM and ROM, respectively. Based on these features, it is essential to develop solutions with a tiny memory footprint because of the limited processing capacity of the limited storage.

Table 9. Memory footprint results (in Bytes)

	RAM	ROM	Total
Standard RPL	4958	47107	52393
Modified RPL	4994	47621	52943

Table 9 presents a comparison of the used memory of the modified protocol and the regular RPL following the use of our suggested mitigation approach. Note that the implementation of the modified RPL is comprised of only the proposed countermeasure incorporated into the standard RPL implementation. The results show that the updated RPL adds 514 more bytes of ROM memory. When it comes to RAM utilization, just 1.05% extra RAM footprint is added. These findings demonstrate that the suggested strategy is practical, and appropriate for LLN networks.

6 Conclusions

This paper has addressed the pressing need for enhanced security measures in IoT networks, particularly focusing on the vulnerability of the edge part of the network to sophisticated attacks. Through the introduction of the Hybrid Rank Attack (HRA), we have demonstrated the significant impact that such attacks can have on critical network metrics. Our findings underscore the importance of developing robust countermeasures to mitigate the effects of HRA and enhance the resilience of RPL-based IoT networks. The proposed lightweight and distributed countermeasure algorithm represents a significant step forward in addressing the challenges posed by HRA. Through extensive simulation-based evaluations, we have shown that our solution achieves substantial reductions in control overhead (68.7%) and energy consumption (61.83%), while incurring minimal additional RAM utilization. This underscores the effectiveness and efficiency of our approach in safeguarding RPL-based IoT networks against HRA threats.

Moreover, the proposed solution in this paper still provided effective protection against only the rank attack in its hybrid form whereas it remains vulnerable to other similar attacks. An example is the version number attack which is also based on advertising false DIO information. In our future work, the focus would be on addressing a more comprehensive solution to mitigate the different forms of attacks that rely on manipulating the header of the DIO messages. This would be combined with extensive exploration of the solution focusing on different considerations such as varying-scale and attack-positioning scenarios.

References

[1] X. Mu and M. F. Antwi-Afari, "The applications of Internet of Things (IoT) in industrial management: a science mapping review," *International Journal of Production Research*, vol. 62, no. 5, pp. 1928–1952, Dec. 2023, doi: 10.1080/00207543.2023.2290229.

[2] R. Chataut, A. Phoummalayvane, and R. Akl, "Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0," *Sensors*, vol. 23, no. 16, p. 7194, Aug. 2023, doi: 10.3390/s23167194.

[3] M. Albreem, A.M. Sheikh and A.E. Ayman, "Towards a Sustainable Environment with a Green IoT: An Overview,". *2022 International Conference on Computer Technologies (ICCTech)*, 2017, doi: 10.1109/ICCTech55650.2022.00017.

[4] P. Gkonis, A. Giannopoulos, P. Trakadas, X. Masip-Bruin, and F. D'Andria, "A Survey on IoT-Edge-Cloud Continuum Systems: Status, Challenges, Use Cases, and Open Issues," *Future Internet*, vol. 15, no. 12, p. 383, Nov. 2023, doi: 10.3390/fi15120383.

[5] S. Syaifuddin, S. S. Kusumawardani, and W. Widyawan, "Tackling DDOS Attacks in IoT: Asynthesis of Literature 2018 to 2022", *Int J Intell Syst Appl Eng*, vol. 12, no. 1, pp. 802–809, Dec. 2023

[6] A. Heidari and M. A. Jabraeil Jamali, "Internet of Things intrusion detection systems: a comprehensive review and future directions," *Cluster Computing*, vol. 26, no. 6, pp. 3753–3780, Oct. 2022, doi: 10.1007/s10586-022-03776-z.

[7] N. A. Alfriehat, M. Anbar, S. Karuppayah, S. D. A. Rihan, B. A. Alabsi, and A. M. Momani, "Detecting Version Number Attacks in Low Power and Lossy Networks for Internet of Things Routing: Review and Taxonomy," *IEEE Access*, vol. 12, pp. 31136–31158, 2024, doi: 10.1109/access.2024.3368633.

[8] H. Almutairi and N. Zhang, "A Survey on Routing Solutions for Low-Power and Lossy Networks: Toward a Reliable PathFinding Approach," *Network*, vol. 4, no. 1, pp. 1–32, Jan. 2024, doi: 10.3390/network4010001.

[9] A. El Hajjar, "Key-Pre Distribution for the Internet of Things Challenges, Threats and Recommendations," *Wireless Networks*, pp. 1–42, 2023, doi: 10.1007/978-3-031-33631-7_1.

[10] I. S. Alsukayti and M. Alreshoodi, "Toward an understanding of recent developments in RPL routing," *IET Networks*, vol. 8, no. 6, pp. 356–366, Nov. 2019, doi: 10.1049/iet-net.2018.5167.

[11] M. Rouissat, M. Belkheir, H. S. A. Belkhira, S. Boukli Hacene, P. Lorenz, and M. Bouziani, "A new lightweight decentralized mitigation solution against Version Number Attacks for IoT Networks," *JUCS - Journal of Universal Computer Science*, vol. 29, no. 2, pp. 118–151, Feb. 2023, doi: 10.3897/jucs.85506.

[12] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko, "The Trickle Algorithm," Mar. 2011, doi: 10.17487/rfc6206.

[13] A. Hkiri, M. Karmani, O. B. Bahri, A. M. Murayr, F. H. Alasmari, and M. Machhout, "RPL-Based IoT Networks under Decreased Rank Attack: Performance Analysis in Static and Mobile Environments," *Computers, materials and continua (Print)*, Jan. 01, 2023. doi : 10.32604/cmc.2023.047087.

[14] M. Rouissat, M. Belkheir, H. S. A. Belkhira, A. Mokaddem, and D. Ziani, "Implementing and evaluating a new Silent Rank Attack in RPL-Contiki based IoT networks," *Journal of Electrical Engineering*, vol. 74, no. 6, pp. 454–462, Dec. 2023, doi: 10.2478/jee-2023-0053.

[15] F. Zahra, N. Jhanjhi, S. N. Brohi, N. A. Khan, M. Masud, and M. A. AlZain, "Rank and Wormhole Attack Detection Model for RPL-Based Internet of Things Using Machine Learning," *Sensors*, vol. 22, no. 18, p. 6765, Sep. 2022, doi: 10.3390/s22186765.

[16] M.M Savitha, and P.I Basarkod, "Securing AMI-IoT networks against multiple RPL attacks using ensemble learning IDS and lightchain based prediction detection and mitigation mechanisms," *Information Security Journal: A Global Perspective*, vol. 33, no. 1, pp. 73–95, Jun. 2023, doi: 10.1080/19393555.2023.2218852.

[17] A. O. Bang and U. P. Rao, "EMBOF-RPL: Improved RPL for early detection and isolation of rank attack in RPL-based internet of things," *Peer-to-Peer Networking and Applications*, vol. 15, no. 1, pp. 642–665, Jan. 2022, doi: 10.1007/s12083-021-01275-3.

[18] P. S. Nandhini, S. Kuppuswami, S. Malliga, and R. DeviPriya, "Enhanced Rank Attack Detection Algorithm (E-RAD) for securing RPL-based IoT networks by early detection and isolation of rank attackers," *The Journal of Supercomputing*, vol. 79, no. 6, pp. 6825–6848, Nov. 2022, doi: 10.1007/s11227-022-04921-6.

[19] M. Rouissat, M. Belkheir, I. S. Alsukayti, and A. Mokaddem, "A Lightweight Mitigation Approach against a New Inundation Attack in RPL-Based IoT Networks," *Applied Sciences*, vol. 13, no. 18, p. 10366, Sep. 2023, doi: 10.3390/app131810366.

[20] M. Osman, J. He, F. M. M. Mokbal, N. Zhu, and S. Qureshi, "ML-LGBM: A Machine Learning Model Based on Light Gradient Boosting Machine for the Detection of Version Number Attacks in RPL-Based Networks," *IEEE Access*, vol. 9, pp. 83654–83665, 2021, doi: 10.1109/access.2021.3087175.

[21] W. Choukri, H. Lamaazi, N. Benamar, "RPL rank attack detection using Deep Learning". *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies*, 2020

[22] A. M. Said, A. Yahyaoui, F. Yaakoubi, and T. Abdellatif, "Machine Learning Based Rank Attack Detection for Smart Hospital Infrastructure," *Lecture Notes in Computer Science*, pp. 28–40, 2020, doi: 10.1007/978-3-030-51517-1_3.

[23] S. M. Muzammal, R. K. Murugesan, N. Z. Jhanjhi, M. Humayun, A. O. Ibrahim, and A. Abdelmaboud, "A TrustBased Model for Secure Routing against RPL Attacks in Internet of Things," *Sensors*, vol. 22, no. 18, p. 7052, Sep. 2022, doi: 10.3390/s22187052.

[24] M. A. Boudouaia, A. Abouaissa, A. Ali-Pacha, A. Benayache, and P. Lorenz, "RPL rank based-attack mitigation scheme in IoT environment," *International Journal of Communication Systems*, vol. 34, no. 13, Jul. 2021, doi: 10.1002/dac.4917.

[25] M. Saied, S. Guirguis, and M. Madbouly, "Review of artificial intelligence for enhancing intrusion detection in the internet of things," *Engineering Applications of Artificial Intelligence*, vol. 127, p. 107231, Jan. 2024, doi: 10.1016/j.engappai.2023.107231.

Received 10 March 2024