Microwave Review
July 2026, Vol. 32, No. 1, pp. 15-19
DOI: 10.18485/mtts_mr.2026.32.1.3

Infinite Rank Attack "IRA" against RPL based IoT Networks

Salah-Eddine Djeldjli [1], Mehdi Rouissat[2,3], Mohammed Belkheir[1], Allel Mokaddem[1], Djamila Ziani[1]

Abstract – **In this present paper, we study a modified rank attack in IoT networks. This attack is based on flooding and advertising an infinite rank value by a malicious node. By advertising such value, the malicious node pushes the nodes in its transmission range to reset their trickle timers continuously, which increases the control overhead and the consumed energy of the nodes, which leads to exhaust their resources and disrupting the network availability and life time. The attack has been studied using the default DIO interval, using a modified DIO interval and the position of the malicious node in the topology. The obtained results show a very damaging impact by the attack, where an increase of up to 440% in the sent control messages can take place, and an increase of up to 120 % in energy consumption is reached.**

Keywords –**Trickle timer, IoT, rank, energy, Infinite Rank**

I. INTRODUCTION

Among the technologies involved in various and numerous areas of our daily lives that has experienced a beyond compare degree of evolution in the last years lies in IoT (Internet of Things) networks [1]. The IoT interconnect billions of tiny smart devices, called "Things", to furnish access to many services and information anytime, anywhere and for anyone in the world, these objects can be sensors, actuators implemented in smartphones, wearables devices, computers or any interconnected "things" to perform a given task and provide specific services [2,3] The IoT is used in various domains such as monitoring, home automation [4], smart farming [5], industry [6,7], smart grids [8] and smart transportation in smart cities [9,10]. Deployed on a large scale, these sensors provide real-time, regular and systematic measurement and readings on a large number of objects of their environment, allowing more reactive decision-making on a complex system, with greater flexibility and ease of deployment compared to what wired traditional systems can usually offer.

Smart things that are used in IoT networks have inherent constraints. They are limited in terms of memory, processing and energy [11], where they are based on batteries which requires suitable mechanisms to wisely use their battery. Taking into consideration these limits, the RPL (Routing Protocol for Low-Power and Lossy Networks) is a dedicated routing protocol to LLNs [12,13], effort the IETF Routing Over Low power Lossy networks (ROLL) working group [14].

Since RPL protocol operates on top of the 6LoWPAN [15] layer it is quickly becoming the most widely used routing protocol in IoT environments. Nevertheless, this protocol is characterized by several limitations that can hinder the performance and lifetime of IoT networks. Due to the aforementioned constraints of IoT devices, there are several limitations and challenges to overcome. The RPL protocol is subject to several attacks category [16,17], one that targets the resource (direct attacks, indirect attacks), others the traffic, and others target the topology, where most of the security Routing mechanisms in RPL are optional. [18.19.20].

In this paper, we focus on an attack that target the topology, called Local repair Attack [21,22], more specifically Infinite rank Attack. The main goal of the attack is to provoke the nodes to reset their timer, based on which they send control messages. Based on the traditional attack, we and study the effect of flooding the network by falsified control messages, in order to make to attack more damaging.

II. THE RPL PROTOCOL

RPL is the IETF proposed standard protocol for IPv6 LLN networks. This protocol is part of the network layer and it is capable of operating on top of MAC and IEEE 802.15.4 PHY layers.[23]. Routes in RPL are created in the form of an acyclic mesh-tree topology, based on Destination-Oriented Directed Acyclic Graphs (DODAGs) controlled by an objective function (OF) [24], and rooted to an edge a resourceful node router called root or sink node.[25], this graph is created using control messages, in a step-by-step manner.

In RPL-Contiki, we find three types of ICMPv6 (Internet v6 Control Message Protocol) messages to build as well as to maintain the topology [26]:

- DODAG Information Object (DIO): used to create ascending routes (from nodes to root) in the topology [27]. It contains all the necessary information that allows the nodes to keep tracking the various configuration parameters, such as: RPL's instance ID, DODAG's ID, version number, RPL's mode of operation, the rank of sender node, and other necessary maintenance parameters.
- Destination Advertisement Object (DAO): used to create descending routes, where each node advertises itself and its direct and indirect children nodes to its chosen preferred parent.

Article history: Received April 26,2026; Accepted May 12,2026

[1] Djeldjli Salah-eddine, Mohammed Belkheir, Allel Mokaddem and Djamila Ziani are with LIMA Laboratory, Nour Bachir University Center El-Bayadh, Algeria, E-Mails: s.djeldjli@cu-elbayadh.dz, m.belkheir@cu-elbayadh.dz, a.mokaddem@cu-elbayadh.dz, ziani.djamilla@gmail.com

[2]Mehdi Rouissat is with the institute of Technology, Nour Bachir University Center, El-Bayadh, and affiliated to [3] STIC Laboratory, University Aboubekr Belkaid, Tlemcen, Algeria, E-Mail: m.rouissat@cu-elbayadh.dz

- DODAG Information Solicitation (DIS): Used by each to solicit a DIO message from neighbors in a given existing network. All receiving nodes respond by a DIO message.

When a given node intend to join a topology for its first time, it waits for a DIO for 5 seconds, in the case where it does not receive any DIO then it sends a DIS to silicate a DIO message. Once the willing node receives a DIO, it chooses DIO the sender as preferred parent and send a DAO message to its chosen parent, the DAO message contains its own address and the parent's address as a prefix.

III. Results and Discussion

To detail the possible impact of the possible attack, we consider the topology shown in Fig.1. Based on Fig.1, we consider three zones in the network:

- Zone A: it is a two hops zone, includes: Node 8, 9 and node 10,
- Zone B: it is an intermediate zone to zone A, and its one hop zone, includes: Node 5, 6 and node 10,
- Zone C: presents an isolated one hop zone, includes: nodes 2, 3 and node 4,

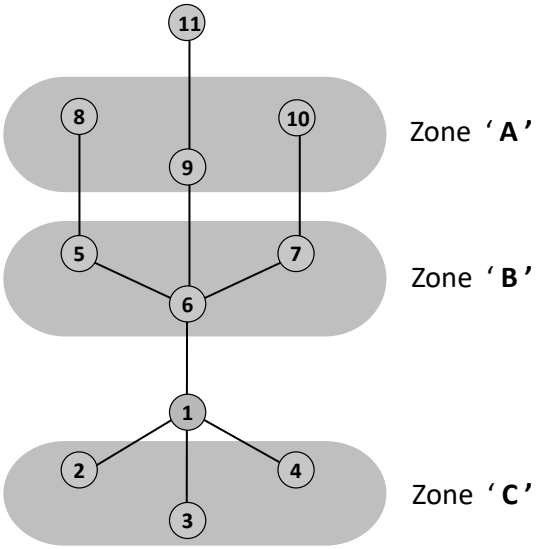

Fig. 1. Network topolgy in the normal case

We utilized Contiki's network simulator, also known as Cooja,. The simulations are based on Z1 nodes, which are ultralow-power MSP430 boards with a radio transceiver that operates at 2.4 GHz and is compatible with IEEE 802.15.4 for link layer protocol. In the first simulation, all the nodes run a legitimate code. The processed control messages during 10 minutes of simulation by the three zones are shown in table 1.

Table 1 shows the transmission ratio of control messages for the three zones. The zone B shows the most important ratio in terms of DAO forwarded messages, this is explained by the fact that zone B, is an intermediate zone, and all its nodes assure a forwarding task. These obtained results are used as reference to study and compare the network behaviours under attack.

TABLE 1
PROCESSED DIO AND DAO MESSAGES IN THE NORMAL CASE

	Generated		Forwarded		
Mote	DIO	DAO	DAO	Total	
All	130	74	61	265	100 %
Zone A	39	28	11	78	29 %
Zone B	39	20	50	109	41 %
Zone C	34	19	0	54	20 %

IV. First Scenario of the Attack

In the first scenario, the node 11 runs a tempered code in order to conduct an attack against the network. The malicious node is sending an infinite rank value in its regular sent DIO messages. A node receiving such a DIO message resets its DIO timers, i.e nodes 8, 9 and node 10. Table 2 shows the sent control messages after 10 minutes in the three zones.

TABLE 2
PROCESSED DIO AND DAO MESSAGES IN THE FIRST SCENARIO OF THE ATTACK

	Generated		forwarded		
Mote	DIO	DAO	DAO	Total	
All	188	93	104	385	100 %
Zone A	98	32	34	164	42 %
Zone B	35	21	70	126	32 %
Zone C	35	18	0	53	13 %

The sent messages by a given node could be generated by itself like DIO, DIS or generated DAO, or it can be received from another node and forwarded to the preferred parent.

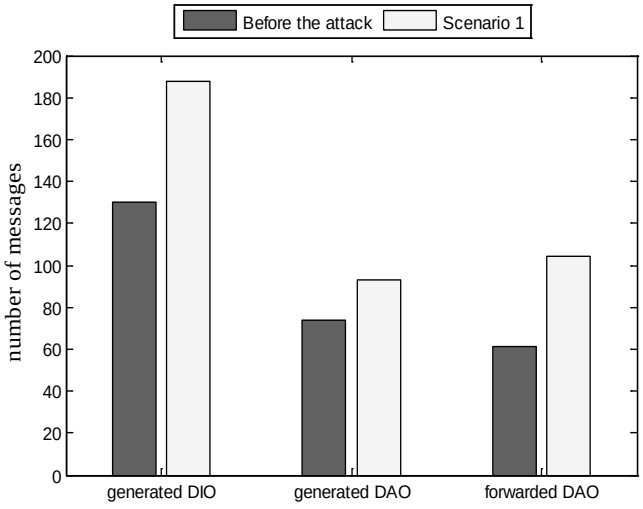

Fig. 2. Total processed messages before and after the attack

Figure 2 shows the number of sent messages in the normal case and in the first scenario of the attack. The figure shows an increase in the sent DIO messages from 130 to 188, an

increase of 44 %. And an increase of forwarded DAO messages from 61 to 104, an increase of 70 %.

The 3 zones contributed differently in this increase. The zone A, is the major contributor by 42%. This is due to the fact that the affected nodes by the inconsistency, and trickled their timers are those of zone A. which lead to a fact that 27 % of the nodes are generating 46 % of the control messages.

Fig.3 shows the consumed energy in LPM, CPU TX and RX modes before the attack and after the first scenario of the attack. The figure illustrates that the mode that shows a significant increase is the TX mode. It shows an increase from 1213 mj to 1573 mj, which presents an increase of 30%.

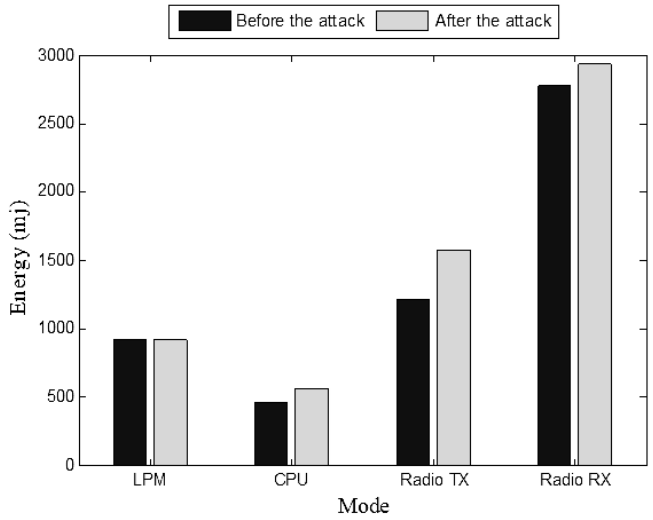

Fig. 3. Concummed energy before and after the first scenario of the attack

The most consuming nodes in the transmission mode are those of zone A, with 52 % of the total consumed energy in TX mode. The forwarding task presents 20 % of the 52 %, (34 forwarded messages out of 164 sent).

V. Second Scenario of the Attack

In this second scenario, the malicious node is sending an infinite rank value in its sent DIO messages, like the first scenario, but using modified parameters that define the trickle timer. In other words, the malicious nodes is not using a regular intervals, but it is flooding the network by falsified DIO messages. The RPL DIO INTERVAL DOUBLINGS is changed from 8 (default value in Contiki) to 2. This modification leads to:

$$I_{max} = 4096 \cdot 21 = 1048576\text{ms} \approx 8\text{seconds} \quad (1)$$

Thus, the transmission interval is 4 s (minimal interval) and 8 s (maximal interval). This modification leads to a significant increase in the transmission ratio of DIO messages, consequently a continuous influence on the victim nodes.

Table 3 shows the exchanged ICMPV6 messages during the simulation. The table shows that the total number of sent messages increased from 385 to 882, a percentage of 130 %, which presents a huge increase that may affect the node's residual energy, consequently the life time of the network. It is worth highlighting that the zone A presents 53 % of the sent messages, where zone C presents 6 %.

TABLE 3
PROCESSED DIO AND DAO MESSAGES IN THE SECOND SCENARIO

	Generated		forwarded		
Mote	DIO	DAO	DAO	Total	
All	389	189	304	882	100 %
Zone A	242	88	138	468	53 %
Zone B	35	20	166	221	25 %
Zone C	36	17	0	53	06 %

The different types of messages contributed differently to this increase, Fig.4 shows the total processed messages before, after the first scenario of the attack, and after the second scenario of the attack. The figure shows that the number of sent DIO messages increased from 130 messages in the normal case to 389, a percentage of 200 %, and the DAO sent messages from 61 to 304 message, an increase of 398%. These results show the very damaging impact of the attack after implementing the second scenario's parameters. This very important increase in the control overhead affects considerably the resources and lifetime of the nodes as well as the network, and affect also the availably of the nodes.

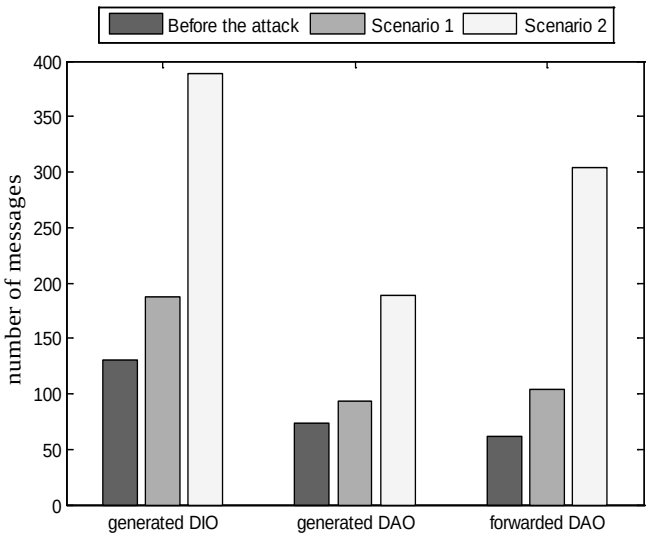

Fig. 4. Total processed messages before, after the first scenario, and after the second scenario of the attack

The important increase in the control overhead leads to an increase in the total consumed energy. Fig.5 shows the consumed energy in the three cases and for the four modes LMP, CPU, TX, and RX. The total consumed energy increased from 5370 mj to 8290 mj, an increase of 54 %, compared to the normal case. this increase in the percentage is dominated by an increase in the transmission mode, from 1213 to 2941 mj, an increase of 142 %. This is due to the continues reset of the trickle timer of the victim nodes.

Fig.6 depicts how the different modes and the different zone differently increase the total consumed energy. It can be noticed that the RX mode is dominating in the zone B. The zone B is under the transmission range of the direct victims of

the attack, this increases the listening mode rather than the transmitting mode. On the other hand, the most consuming mode in the zone A is the transmission mode, as the nodes of the zone are resetting their trickle timer and sending DIO messages in intervals of 4 seconds (minimal possible interval) or 8 seconds.

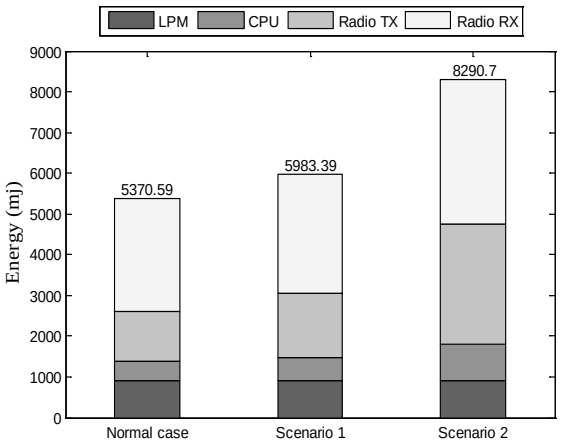

Fig. 5. Total consummed enegy for the three cases

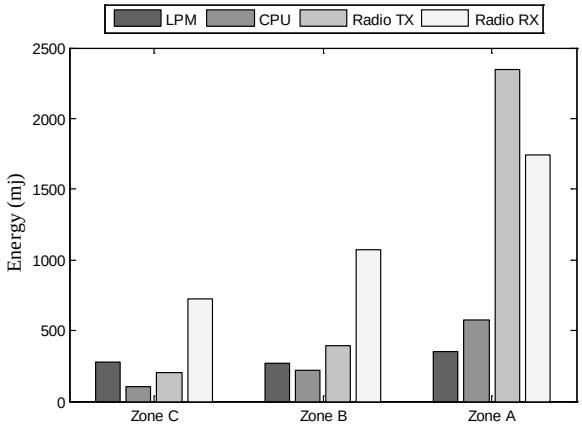

Fig. 6. Total consummed enegy by the the differents mode for the three zones

VI. THIRD SCENARIO OF THE ATTACK

In this third scenario, we place the malicious node in the middle of the network, unlike the previous scenarios, as Fig.7 shows, the node 9 is the one playing the malicious node. The first thing that should be noticed is that node 9 does not has children, this is explained by the fact that nodes do not chose a node advertising infinity rank value as preferred parent.

TABLE 4
PROCESSED DIO AND DAO MESSAGES FOR ALL THE CASES

	Generated		forwarded	
	DIO	DAO	DAO	Total
Normal	130	74	61	265
Scenario 1	188	93	104	385
Scenario 2	389	189	304	882
Scenario 3	584	329	520	1433

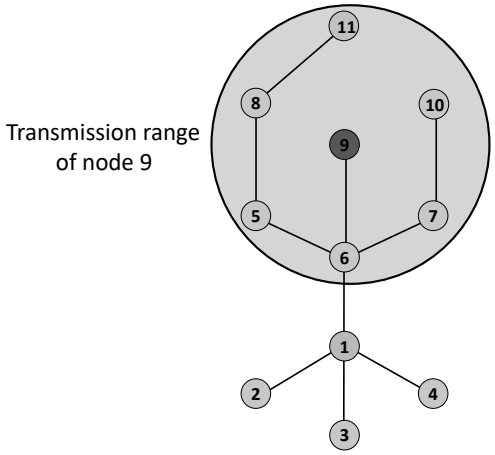

Fig. 7. Topology of the third scenario

In this scenario, the direct victims of the attack are the nodes in transmission range of node 9, which are : nodes 5, 6, 7, 8, 11 and 10. On the other hand, only one node is in transmission coverage of the direct victims, which is node 1, affected indirectly by the attack.

Table 4, shows the evolution of sent control messages for the four cases. The results show that the position of the malicious node incredibly increases the total overhead, it jumped to a total of 1433 messages, an increase of 440 % in the total control overhead compared to the normal case, where the DIO message presents an increase from 130 in the normal case to 584 in this third scenario, which presents an increase of 350 % . The obtained results show that, advertising infinite rank in DIO messages by a malicious node, combined to a low interval of transmission and combined to a good position in the network, affect incredibly the control overhead in a given network.

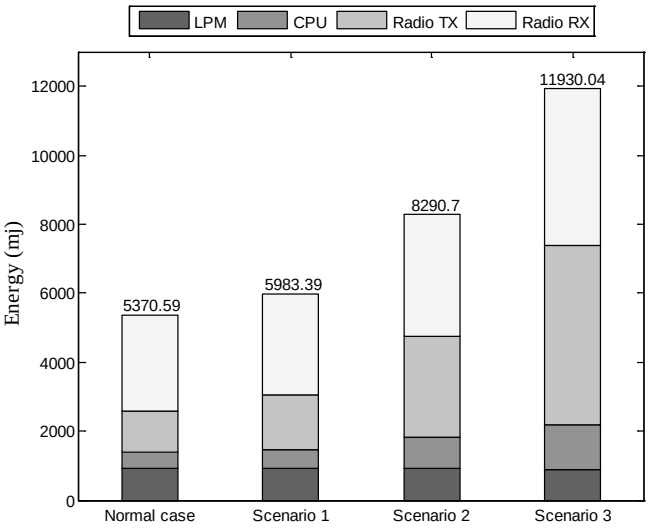

Fig. 8. Total consummed enegy for the four cases

The total consumed energy in the different scenario is shows in Fig.8, it shows that the total consumed energy by all the nodes jumped to 11930 mj, presents an increase of 120 %. The figure shows also that unlike the first scenarios, the transmission mode dominates the third scenario. This increase, is due mainly to the position taken by the malicious

node, which allowed it to affect most of the nodes of the network directly or indirectly.

VII. CONCLUSIONS

In this paper, we presented and analyzed a modified infinite rank attack, which aims to affect the network topology and exhaust the network resources. The basic idea of the attack is to force the direct victim nodes to initialize their trickle timers, over and over which lead to an unnecessary generated, forwarded and listen to traffic, as well as indirect victim through targeting their Listening mode. Our modified attack is based on a tempered sending interval.

According to the obtained results, the attack can be described as successful, where it reaches the goal behind it. The network under attack shows an important increase in the control overhead, by about 440 %, on the other hand the total consumed energy shows an increase of 120 %. This destructive impact limits the nodes lifetime and consequently the network's. It is worth mentioning that using smaller fixed intervals may be more harmful and damaging to the network, this will be the subject of our future work, beside the focus on how to detect and mitigate such attack.

REFERENCES

[1] M. M. Sithik and B. M. Kumar, "Intelligent Agent based Virtual Clustering and Multi-Context aware Routing for congestion Mitigation in Secure RPL-IoT Environment",*.Ad Hoc Networks*, vol. 137, 2022, DOI: 10.1016/j.adhoc.2022.102972.

[2] S. M. Muzammal, R. K. Murugesan and N. Z. Jhanjhi, "A Comprehensive Review on Secure Routing in Internet of Things: Mitigation Methods and Trust-Based Approaches," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4186-4210, 2021, DOI: 10.1109/JIOT.2020.3031162.

[3] K. S. Sudha and N. Jeyanthi,. "A Review on Privacy Requirements and Application Layer Security in Internet of Things (IoT)", *Cybernetics and Information Technologies*, vol. 21, pp. 50-72, 2021, DOI: 10.2478/cait-2021-0029.

[4] C. -H. Lu, "Context-Aware Service Provisioning via Agentized and Reconfigurable Multimodel Cooperation for Real-Life IoT-Enabled Smart Home Systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 8, pp. 2914-2925, 2020, DOI: 10.1109/TSMC.2018.2831711.

[5] N. Ahmed, D. De and I. Hussain, "Internet of Things (IoT) for Smart Precision Agriculture and Farming in Rural Areas," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4890-4899, 2018, DOI: 10.1109/JIOT.2018.2879579.

[6] M. W. Condry and C. B. Nelson, "Using Smart Edge IoT Devices for Safer, Rapid Response With Industry IoT Control Operations," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 938-946, 2016, DOI: 10.1109/JPROC.2015.2513672.

[7] Y. -C. P. Chang, S. Chen, T. -J. Wang and Y. Lee, "Fog Computing Node System Software Architecture and Potential Applications for NB-IoT Industry," 2016 *International Computer Symposium (ICS)*, pp. 727-730, 2016, DOI: 10.1109/ICS.2016.0150.

[8] E. Ancillotti, R. Bruno and M. Conti, "The Role of the RPL Routing Protocol for Smart Grid Communications," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 75-83, 2013, DOI: 10.1109/MCOM.2013.6400442.

[9] A. J. V. Neto, Z. Zhao, J. Rodrigues, H. B. Camboim, and T. Braun. "Fog-Based Crime-Assistance in Smart IoT Transportation System", *IEEE Access*, vol 6, 2018, DOI: 10.1109/ACCESS.2018.280343.

[10] P. S. Saarika, K. Sandhya and T. Sudha, "Smart Transportation System using IoT," 2017 *International Conference on Smart Technologies for Smart Nation (SmartTechCon)*, pp. 1104-1107, 2017, DOI: 10.1109/SmartTechCon.2017.8358540.

[11] M. Rouissat; M. Belkheir; I. S. Alsukayti and A. Mokaddem, "A Lightweight Mitigation Approach against a New Inundation Attack in RPL-Based IoT Networks", *Appl. Sci.* 2023, vol. *13*, no. 18, 2023, DOI: 10.3390/app131810366.

[12] P. S. Nandhini, S. Kuppuswami and S. Malliga, "Energy Efficient Thwarting Rank Attack from RPL Based IoT Networks: A Review", *Materials Today: Proceedings*, vol. 81, no. 7, 2021, DOI:10.1016/j.matpr.2021.04.167.

[13] T. C. J. Jermin and V. Sarasvathi, "A Multi-Agent Reinforcement Learning-Based Optimized Routing for QoS in IoT", *Cybernetics and Information Technologies*, vol 21, no. 4, 2021, DOI: 10.2478/cait-2021-0042.

[14] T. Winter et al., "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," Request for Comments: 6550, IETF, 2012.

[15] M. Rouissat, M. Belkehir, A. Mokaddem, M. Bouziani and I. S. Alsukayti, "Exploring and Mitigating Hybrid Rank Attack in RPL-Based IoT Networks", *Journal of Electrical Engineering*, vol. 75, no. 3, pp. 204–213, 2024, DOI:10.2478/jee-2024-0025.

[16] A. Imteaj, U. Thakker, S. Wang, J. Li and M. H. Amini, "A Survey on Federated Learning for Resource-Constrained IoT Devices," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 1-24, 2022, DOI: 10.1109/JIOT.2021.3095077.

[17] I. S. Alsukayti, M. Alreshoodi and M. Rouissat, "A Lightweight Mitigation Technique Against a Modified Version Number Attack in IoT Networks," *IEEE Access*, vol. 13, pp. 20472-20490, 2025, DOI: 10.1109/ACCESS.2025.3535166

[18] T. Winter et al., "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC 6550, *Internet Engineering Task Force (IETF)*, 2012, DOI: 10.17487/RFC6550.

[19] A. Raoof, A. Matrawy and C. -H. Lung, "Secure Routing in IoT: Evaluation of RPL's Secure Mode under Attacks," 2019 *IEEE Global Communications Conference (GLOBECOM)*, Waikoloa, pp. 1-6, 2019, DOI: 10.1109/GLOBECOM38437.2019.9013120.

[20] H. H. Alazzam, O. Abualghanam, Q. M. Alzubi, A. Alsmady and E. Alhenawi, "A New Network Digital Forensics Approach for Internet of Things Environment Based on Binary Owl Optimizer" *Cybernetics and Information Technologies*, vol. 22, no. 3, pp.146-160, 2022, DOI: 10.2478/cait-2022-0033.

[21] A. Raoof, A. Matrawy and C. -H. Lung, "Enhancing Routing Security in IoT: Performance Evaluation of RPL's Secure Mode Under Attacks," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11536-11546, 2020, DOI: 10.1109/JIOT.2020.3022276.

[22] M. Alreshoodi, "An Experimental Study of IoT Networks Under Internal Routing Attack", *The International Journal of Computer Networks & Communications*, vol. 12, no. 4 , 2020, DOI: 10.2139/ssrn.3690813.

[23] T. Winter et al., "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC 6550, *Internet Engineering Task Force (IETF)*, 2012.

[24] M. A. Boukhobza, M. Rouissat, M. Belkheir, A. Mokaddem and P. Lorenz, "Optimized Route Selection in RPL: Static and Dynamic Parent Evaluation for Energy-Efficient IoT Networks", *Journal of Network and Systems Management*, vol. 34, no. 42, 2026, DOI: 10.1007/s10922-025-10023-4.

[25] R. Elisa, H. Hedayat, G. Carles, C. David and J. F . Cotrim, "Outperforming RPL with Scalable Routing Based on Meaningful MAC Addressing", *Ad Hoc Networks*, vol. 114, no. 1, 2021, DOI:10.1016/j.adhoc.2021.102433.

[26] 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.

[27] F. Medjek, D. Tandjaoui, N. Djedjig and I. Romdhani, "Multicast DIS Attack Mitigation in RPL-Based IoT-LLNs", *Journal of Information Security and Applications*, vol. 61, 2021, DOI: 10.1016/j.jisa.2021.102939.