Journal of Electrical Engineering, Vol. 74, No. 6, 2023, pp. 454-462

sciendo

PAPERS

Implementing and evaluating a new Silent Rank Attack in RPL-Contiki based IoT networks

Mehdi Rouissat[1,2,*], Mohammed Belkheir[3], Hichem S. A. Belkhira[1], Allel Mokaddem[3], Djamila Ziani[3]

IoT networks are witnessing a rapid growth in various domains of our daily life, offering more attractive features in terms of measurement accuracy, easy implementation and affordable deployment costs. This outstanding boom is not undoubtedly far away from different challenging issues that impede the network efficiency and quality. The security concern remains one among the prominent issues that affect both the edge and the core IoT network where risks increase in conjunction with the network expansion. RPL is the well-known routing protocol for the edge part of the IoT network, intended to meet the requirements of the constrained IoT devices. Despite its various advantages, RPL remains suffering from various security attacks targeting the topology, the traffic, and the nodes resources. Our work presents a new silent decreased rank attack against RPL-Contiki, as well as a lightweight countermeasure. The obtained results on a random studied topology show that almost half the existing nodes in the topology were attracted by the planted malicious node, through its falsified low rank. Moreover, an increase of 12.5% in the control overhead and an increase of 15% in the total consumed energy are recorded compared to the attack-free topology. On the other hand, the attack did not heavily affect the PDR, but the latency showed an increase of 45% compared to the attack free case. This damaging effect makes this modified rank attack a serious threat to IoT RPL based networks.

Keywords: IoT, RPL, Contiki, security, rank

1 Introduction

The world is witnessing a huge transformation in recent times with the advent of new technologies based on smart devices called sensors. These devices build together to form a new kind of self-organized smart networks named IoTs, very suitable to thoroughly collect real-time data from a monitored environment for further processing and decision. This revolutionized technology that transforms our daily life digital, offers numerous features such as: easy deployment, scalability, measurement accuracy, affordable installation cost, high salability, and many other advantages that allowed it to grow rapidly from the research stage to the industry field. For that purpose, IoTs networks have been widely involved in many sensitive domains such as smart cities, smart industry 4.0, smart healthcare, smart education, smart agriculture, smart oil/gas fields, smart transportation, and other various monitored environments. In addition, and for more benefits, IoT networks are often connected through internet to cloud platforms that intend to store the huge amount of the gathered data for more efficiency in terms of analysis and decision making. Furthermore, IoT networks are more and more federated by artificial intelligence (AI) techniques that aim to resolve the inefficiency of the manual traditional systems and bring an added value for more reliable and predictable processes with fast and accurate real-time decisions. The purpose is to reduce downtimes and to provide more trustworthy solutions. This is witnessed by the better insights brought by AI-IOT enabled solutions, especially for detecting infections of COVID-19 pandemic and helping to stop the massive spread of the pandemic in many countries. The pairing of the two aforesaid technologies has given rise to a new trend of an inspiring digitization model called “digital twin” which is considered as one among the current interesting research topics.

Despite the enormous growth of IoT networks and their wide range of applications, they remain suffering from various weaknesses that should be addressed, such as QoS, energy efficiency, wireless networking issues and security challenges [1-4]. This is mainly due to the limited characteristics of the IoT devices in terms of energy saving, processing, and storage memory, knowing that sensors are considered as constrained devices and run a lightweight unsecured operating

[1] University Center Nour Bachir El-Bayadh, 32000, El-Bayadh, Algeria
[2] STIC Laboratory, University Aboubekr Belkaid, Tlemcen, Algeria
[3] LIMA Laboratory , Univeristy Center Nour Bachir, El-Bayadh, Algeria
* m.rouissat@cu-elbayadh.dz

https://doi.org/10.2478/jee-2023-0053, Print (till 2015) ISSN 1335-3632, On-line ISSN 1339-309X

system [5, 6]. Moreover, the upsurge number of the connected devices abroad a large spectrum of areas leads IoT networks to face various challenges in different scales of the network (edge, cloud, fog, *etc*) [7, 8]. Statistics in [9] reveal a gigantic evolution in the IoT market where 7 billion of IoT devices are interconnected over the world with 400 platforms. This number is expected to reach 25 billion by 2030. According to [10], cyberattacks in IoT reached 1 billion in 2021, since the third of the connected devices are infected, where phishing attacks and DDoS are the most dominant. Given this statistics, the security concern is still a challenging research topic.

Our present work focuses on securing the edge part of the IoT network, especially the routing stack. As known, IoT constrained devices are considered as LLNs (Low power and Lossy Networks) and run a networking protocol named RPL (Routing Protocol for LLNs) described in the IETF RFC 6550 [11]. Despite, the latter seems very suitable for saving the intrinsic properties of the IoT devices; it suffers from a wide range of vulnerabilities widely discussed and categorized by researchers. These attacks target both the topology and network resources [12, 13].

In RPL nodes are organized in a tree topology, where the root node (gateway) gains the governing position, and it is responsible for applying and spreading RPL routing rules over the network. The other IoT nodes are positioned in the network according to their capabilities expressed by a value called “rank”, which is clearly explained in the following sections. A malicious node can take part of the network and advertises a fake rank value to its neighborhood aiming to attract other nodes to relay their data through it. This attack has been widely discussed by several recent researches, since RPL does not have any countermeasure to deny this harmful action triggered by an intruder. In the literature various researches have addresses the rank attack, where in [14] authors presented a study using Friedman test to compare recent researches related to the proposed mitigation solutions against the rank attack. In [15], authors proposed a new objective function named EMBOF for Echelon Metric Based Objective Function which involves an echelon value triggered and exchanged between the root and the corresponding parent node, by which a faked rank value is detected. Authors in [16] proposed an updated version of the basic RPL protocol named MFO-RPL for Moth-Flame, they implement a petal algorithm for the parent selection process and the rank attack is detected using Moth-Flame algorithm to prevent any falsified rank value. Another work in [17] consists on a security system called SRF-IoT based on an external intrusion detection system to prevent any illegitimate nodes to intrude the network. In [18], authors proposed an IDS system called DETONAR for DETection of rOuting Attacks in RPL, it includes signature rules to detect any malicious behavior in the network. In another work, [19] proposes a secured version of the basic RPL protocol named SRPL-RP, where a timestamp and a threshold are included to detect the legitimacy of a DIO sender. Each node is identified by an ID and the root node ID is encrypted to avoid its imitation, in addition, a monitoring table is established in conjunction with the DODAG building process, contains nodes parameters (ID, Rank) that help the receiving node to detect further changing of nodes behaviors, each node sets a blacklist table to avoid any new rooting rules coming from an intruder.

All the proposed solutions in the literature to thwart the rank attack have demonstrated improvements in different studied metrics compared to the basic RPL. However, it is strongly recommended to develop lightweight solutions which meet the constrained properties of the IoT network in terms of power saving, computational and storage limitations of the constrained devices. Heavy cryptographic solutions are not suitable for the edge network components and rapidly exhaust the network resources leading to reduce its lifetime.

The effects of rank attacks are: (i) routing loops, (ii) unoptimized route formation, (iii) decreased packet delivery ratio, (iv) increased delay and (v) increased transmission of DIO messages, lead to more consumption of resources [20-23]. In this paper we present and analyze a new special silent decreased rank attack, where an intruder advertises a better fake rank value than its parent, without prompting any loops, making the attack silent and hard to detect. At first, we clearly describe the harmful defeat caused by this attack by simulations using Cooja under Contiki 3.0. Thereafter, we explain our countermeasure approach and its better insight allowing detecting this potential attack.

2 RPL protocol and rank value

The core functioning of RPL is defined in the RFC 6550 [11], it consists of a tree-based topology named DODAG (Direct Oriented Destination Acyclic Graph) as illustrated in Fig. 1.

The root node is responsible for building the topology and disseminating the routing rules over the entire network via control messages. The other nodes are positioned according to their rank value defined by an objective function. The root node has the lower rank value which increases downward the DODAG.

RPL defines four control messages, where DIS (DODAG Information Solicitation**)** message is sent by a node to request joining the DODAG, it is sent by a node when no DIO message is received within a time interval (5 s is the default value in RPL Contiki) [24].

DIO (DODAG Information Object) message is responsible to broadcast DODAG parameters, this includes the Instance ID, DODAG ID, and Version Number (VN), which are used for DODAG identification and topological update tracking [25]. DAO (Destination Advertisement Object) message is used for building downward routes from the root node. Finally, DAO-Ack, an optional message used to acknowledge a DAO message.

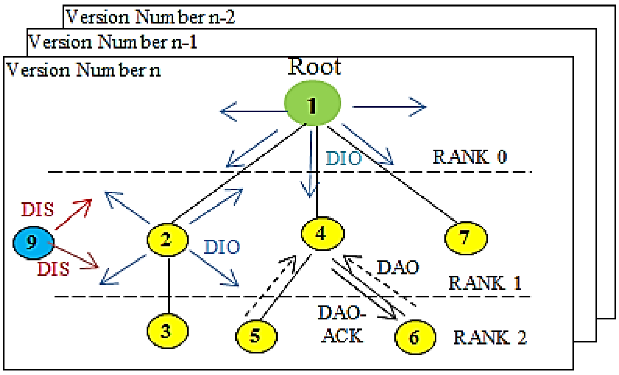

Fig. 1. RPL topology and control messages

In order to select the optimum path to the root, a node uses the objective function to calculate and translate one or more metrics into rank value, based on its parent's, and it advertises it in its DIO messages. Based on the different received rank values, a node chooses the node advertising the lower rank value as its preferred parent, a gate toward the root. Two objective functions are defined in RPL standards:

- Objective Function Zero (OF0) [26], based on which the rank is based mainly on the number of hops toward the root. The goal is to minimize the number of hops from nodes to the sink
- Minimum Rank with Hysteresis Objective Function (MRHOF): is the default O.F in the used Contiki O.S, the rank is also based the link's quality; ETX (Expected Transmission Count) [27]. Thus, the rank is calculated as follows:

$$new\_rank = base\_rank + rank\_increase \tag{1}$$

where

- new_rank is the node's Rank,
- base_rank: is the DIO sender's Rank,
- rank_increase is a value that shows the property of the link (path cost) between the node and the DIO sender.

RPL in its basic scheme does not implement any mechanism to deny advertising a faked rank value. Thus, a malicious node can take advantage of this gap to broadcast a better falsified rank value aiming to be a parent of a large part of the network's nodes. Upon having a good position, an intruder can establish any other harmful behavior such as Blackhole, targeting thereby the network traffic, topology or the nodes resources.

3 Results and discussion

In this section, simulated results and overall analysis of the obtained results are discussed. At the beginning, we simulated a basic scenario (attack free case), used as a reference to judge the effect of the attack on the performance of the network. The studied topology is shown in Fig. 2, it consists of 1 sink node, 23 fair nodes and a single malicious node (node "25") placed two hops from the sink node.

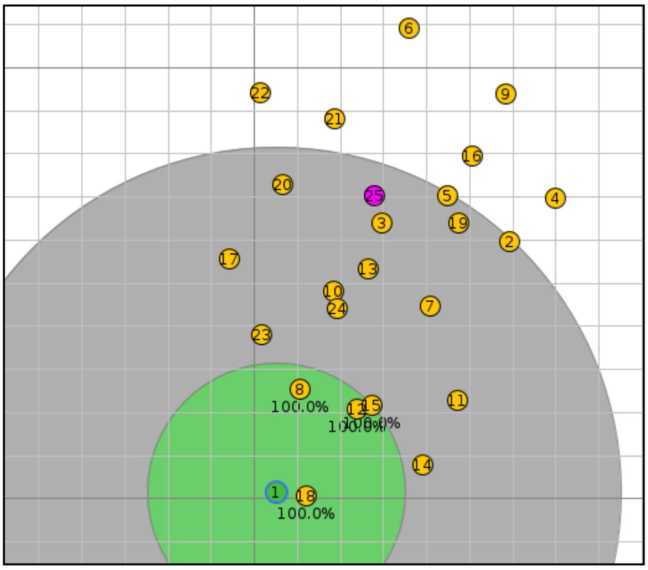

Fig. 2. Studied network topology

The UDP client-server model is used with Zolertia Z1 motes. The reason behind choosing Z1 motes is that Contiki RPL mote Sky engenders bugs during the compilation, because of the total code would not fit into the program memory of the Tmote Sky (48 kB). The different simulation parameters are summarized in Tab. 1.

As discussed in the previous section, the rank value in RPL-Contiki is not related only to the number of hops toward the sink, but it also depends on the link's quality, for this reason, the rank value changes continuously in a static topology. The evolution of the node's “25” rank during an attack free simulation is shown in Fig. 3. According to the figure, the rank's value kept continuously changing during the simulation, reaching a maximum value of 1384 and a minimum value of 1161.

Table 1. Simulation parameters

Parameter	**Values**
Network layer Protocol	RPL
Operating System	Contiki 3.0.
Simulator	Contiki Cooja
Emulated nodes	Z1
MAC layer Protocol	IEEE 802.15.4
Radio model	UDGM
Simulation area	200 m × 200 m
Simulation time	20 minutes
Data transmission	1 Packet / 60s
Objective function	MRHOF

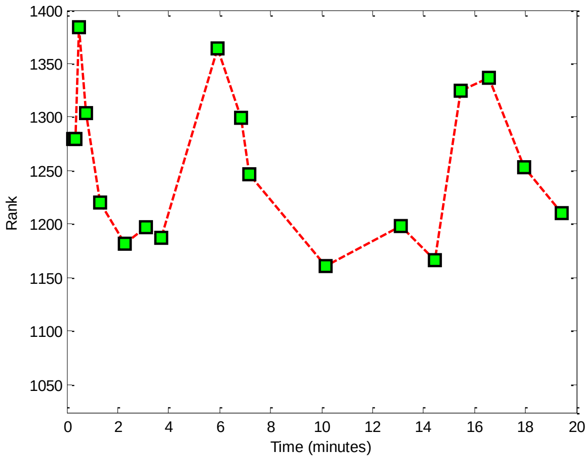

Fig. 3. Rank value of node "25" during simulation

In the following, we present two special and silent rank attacks against RPL-Contiki. In RPL-Contiki, loops, sign of rank attack, are detected based on comparing the number of hops toward the sink, not the rank value itself. Consquently, the only case where a loop is detected is when a child node with strict lower number of hops sends a DAO message to its parent that has a higher number of hops. In the first proposed attack, we take advantage of the above montionned feature, where the intruder node advertises a rank value equal to its own preferred paret.

3.1 Like parent's rank attack (LPRA)

The selection of a preferred parent by a given node is simply choosing the node with the best rank (minimum rank). If a malicious node modifies its advertised rank value, then it causes an adverse effect on topology [28]. Usually, rank attack is combined and followed by other types of attack such as isolation attacks, IP spoofing, Selective forwarding attack, *etc*.

In this LPRA, we propose and implement a special case of the well-known decreased rank attack, where the malicious node advertises the same rank value as its preferred parent. For this purpose, we modified the RPL's objective function of the malicious node, file “rpl-mrhof.c”, where the value of the calculated rank is modified to

$$new\_rank = base\_rank \qquad (2)$$

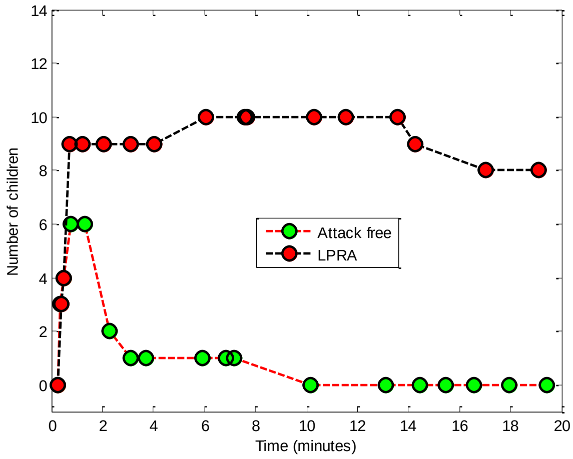

Fig. 4. Number of children of node 25 through time

Figure 4 shows that the number of direct or indirect children the malicious node owns in its sub-DODAGs for the attack free case and for the proposed attack Like parent's rank attack (LPRA). Regarding the attack free case, the number of children shows a change in the first 10 minutes and it drops to be zero in the second 10 minutes of the simulation. When it comes to LPRA attack, the malicious node has most of the time 8 to 10 children, which reflect the success of the conducted attack. This behavior in the network leads to the creation of non-optimal paths, since all the upward traffic sent by the children passes through the malicious node.

3.1.1 Impact of LPRA on the control overhead

Exchanging control messages in the proactive RPL protocol is vital to keep the nodes noticed about any changes in the network, and keep their routing tables up to date. However, an extra overhead makes the nodes process more control packets and exhaust their energy and processing resources. The obtained results related to the control message overhead, basically DIO and DAO messages, are summarized in Tab. 2. The results show that the attack did not engender an increase in the total control overhead.

Table 2. Control overhead in the attack free case and in LPRA

	Sent messages			
	Generated		Forwarded	
	DIO	DAO	DAO	Total
Attack-free	548	284	430	1262
LPRA	564	275	423	1262

3.1.2 Impact of LPRA on the energy consumption

The energy of a node is an important resource in LLN networks, where network efficiency and lifetime is usually affected by the nodes energy consumption, which is a major concern. In our comparison, we did not take into consideration the root node, as naturally it is the most loaded node with the greater energy resources and processing capabilities. Thereby, energy consumption is more critical for the rest of the operating nodes, usually on their batteries.

Figure 5 depicts the total consumed energy by the nodes, in four modes: CPU, LPM, TX and energy consumed in the RX mode. In this regard, it can be observed in Fig. 5 that a slight increase of 3.4% in the total consumed energy is recorded, from 48.9 J to 50.5 J, result of the attack.

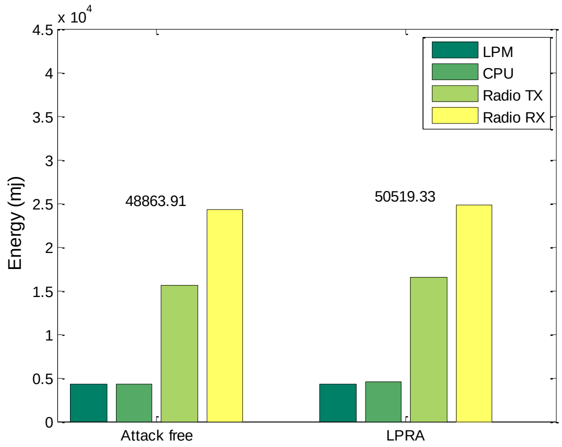

Fig. 5. Energy consumption in the attack free case and in LPRA

The increase in the consumed energy is mainly due to the increase in the TX mode, where it jumped from 15.57 J in the attack free case to 16.53 J in the case of LPRA, as table 3 details.

Table 3. Energy consumption by the four modes in (mJ)

	LPM	CPU	TX	RX	Total
Attack free	4340.2	4338.5	15572.3	24288.7	48863.9
LPRA	4336	4478.4	16537.3	24843.5	50519.3

3.2 Better than parent's rank attack (BPRA)

In RPL-Contiki, inconsistencies in rank values are detected based on comparing the number of hops toward the sink. If a child node with lower number of hops sends a DAO message to its parent that has higher number of hops then a loop is detected.

On the other hand, the rank value is not necessarily an exact multiple of 256, since it is not based only on the number of hops, but also on to the link's quality (ETX). Based on these features, a malicious node can take advantage of this conception and advertises a better rank than its own preferred parent, by considering only the last multiple of 256 of its parent's rank.

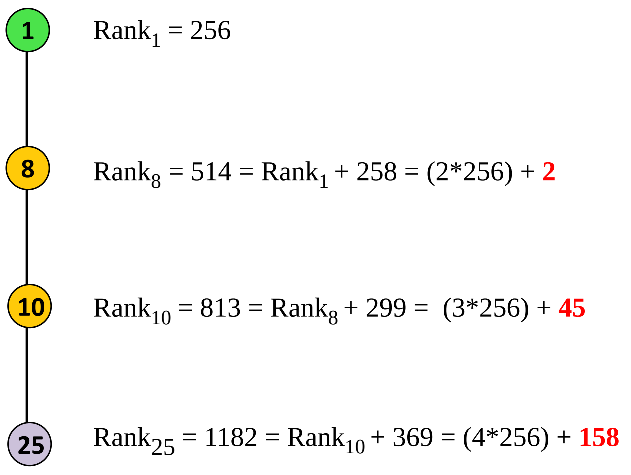
1
8
10
25
$Rank_1 = 256$
$Rank_8 = 514 = Rank_1 + 258 = (2*256) + 2$
$Rank_{10} = 813 = Rank_8 + 299 = (3*256) + 45$
$Rank_{25} = 1182 = Rank_{10} + 369 = (4*256) + 158$

Fig. 6. Rank values of the malicious node and its parents

To give a better understanding of the discussed concept, Fig.6 shows the rank values of the malicious node "node 25" and its parents after 135 seconds of simulation. The malicious node's parent, node 10, is advertising a rank of 813 = 768 + 45. If the malicious node advertises a rank value of 768, it will advertise a rank value better than its preferred parent, without engendering any loops, since, as discussed earlier it is not violating the hop counts.

To implement this special attack, we modified the RPL "rpl-mrhof.c" file of the malicious node, where the value of the calculated rank is modified to

$$Rank_{Node} = abs(base\_rank \ / \ 256\ ) * 256 \qquad (3)$$

By doing so, a modified rank attack is conducted without triggering any loops in the topology, which make it silent and hard to detect.

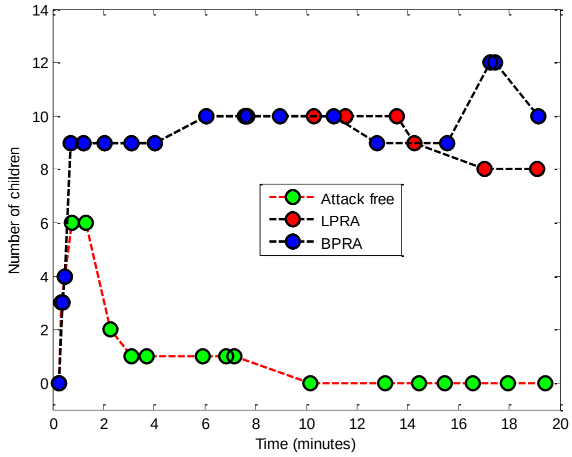

Fig. 7. Number of children of node 25 through time for the three cases

Figure 7 illustrates the effect of BPRA, where it shows an identical behavior compared to LPRA in the first 10 minutes. This behavior did not remain during the second 10 minutes, where the number of children the malicious node has is higher in BPRA, it successfully could have up to 12 children nodes. Based on these results, this second modified rank attack is considered as more successful compared to LPRA.

3.2.1 Impact of BPRA on the control overhead

Table 4 summarizes the exchanged control messages for the three cases. It can be seen that the BPRA engenders an increase in the overhead, from 1262 to 1420 messages, an increase of 12.5%.

Table 4. Control overhead for the three cases

	Sent messages			
	Generated		Forwarded	
	DIO	DAO	DAO	Total
Attack free	548	284	430	1262
LPRA	564	*275*	*423*	1262
BPRA	603	326	491	1420

The main factor that leads to this increase is the forwarded DAO messages. This increase reflects a non-optimal topology, due to the non-optimally created paths by the attack, where around half the existing nodes are direct or indirect children attached to the malicious node. This successful attack has reflected on the number of the forwarded DAO messages by the malicious node. In the attack free case, it forwarded 10 DAO messages, in LPRA it has forwarded 59 DAO messages, while in BPRA 71 DAO messages have been forwarded by the malicious node, which again explain the strategic position it gained in the network. The recorded increase in the control messages would impose higher amounts of resource consumption, particularly in terms of energy and links availability.

3.2.2 Impact of BPRA on the energy consumption

Regarding the energy, which is a significant and decisive metric on increasing the network lifetime, Fig. 8, depicts the total consumed energy, in four modes: CPU, LPM, TX and energy consumed in the RX mode. The figure depicts an increase of 15% on the energy recorded by BPRA compared to the attack free case, where LPRA shows an increase of only 3.4%.

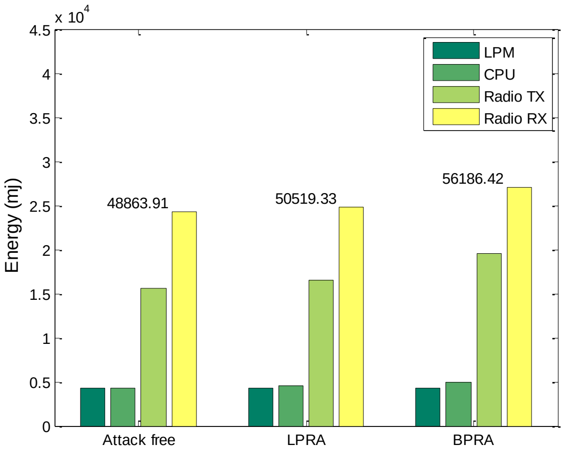

Fig. 8. Energy consumption for the three scenarios

The contribution of the different modes in the total consumed energy is detailed in table 5. The TX mode is the main contributor, it showed an increase of 25.7% compared to the attack free case.

Table 5. Energy consumption in the three cases in mJ

	LPM	CPU	TX	RX	Total
Attack free	4340.2	4338.5	15572.3	24288.7	48863.9
LPRA	4336	4478.4	16537.3	24843.5	50519.3
BPRA	4321.8	4945.3	19566.7	27028.5	56186.4

Based on its strategic position in the topology and its new forwarding tasks, the malicious node is the main contributor in the total consumed energy. According to Fig. 9, the total consumed energy of node 25 has increased compared to the attack free case, by 98% and 118% in the LPRA, and BPRA respectively.

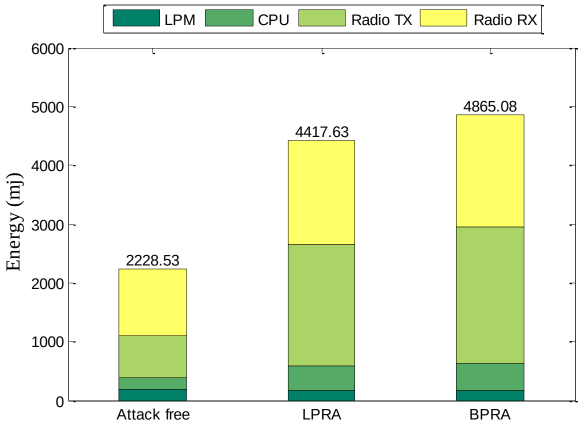

Fig. 9. Energy consumption of node 25 for the three cases

The most affected mode by the attack is the TX, where it shows an increase of 227% in the case of BPRA compared to the attack free case, as Tab. 6 details.

Table 6. Energy consumption of node 25 in the three cases in mJ

	LPM	CPU	TX	RX	Total
Attack free	180.09	205.71	707.71	1135.02	2228.53
LPRA	173.78	414.58	2072.14	1757.12	4417.63
BPRA	172.54	454.94	2316.73	1920.87	4865.08

3.2.3 Impact on the PDR and on the latency

The PDR (Packet Delivery Ratio) presents the ratio of the total number of received data packets by the root node to the total number of sent data packets by the rest of the network's nodes [29], while the latency is the average time taken for a given number of successful data packets transmitted by the network's nodes to be received by the root node [30]. Table 7 shows the PDR for the three studied cases. The figure shows that the PDR has been slightly affected under the attack, where a ratio of 95% is recorded in LPRA and a ratio of 94% is recorded in the case of BPRA. This is mainly due to the congestion incurred due to non-optimal paths created by the attack, in particular at the level of the forwarder nodes.

Table 7. PDR and latency for the three cases

	Latency (s)	PDR (%)
Attack free	0.42	97
LPRA	0.50	95
BPRA	0.61	94

Table 7 also shows the recorded latency in the three cases. The latency has been adversely affected by the attack, where it raised from 0.42 s in the attack free case to 0.61 s in the case of BPRA, which presents a significant increase of 45 %. This deterioration can be attributed to the non-optimal topology and the non-optimal paths created by advertising a falsified rank value by the malicious node to gain a strategic false position within the targeted topology.

3.3 Countermeasure

The two discussed rank attacks have been described as silent, because no trace is left behind. Since the detection of the rank attack in many works is based on the detection of loops [31], it is sufficient to engender loops in the topology in order to make the detection of the attack possible. For this purpose, we modified the "rpl-icmp6.c" file of the nodes, where the code of loops detection has been changed to

DAG _RANK(p->rank, instance) =
< DAG_RANK(dag->rank, instance)

instead of

(DAG _RANK(p->rank, instance) < DAG_RANK(dag->rank, instance).

This modification triggers loops if a child node pretends to have the same number of hops toward the sink like its parents, regardless the rank value it is advertising. The obtained results regarding the number of loops recorder in the network after implementing the proposed change are summarized in Tab. 8.

Table 8. Recorded loops for the three cases

	Number of loops
Attack free	0
LPRA	1
BPRA	603

Thereby, the network is more usually advertised by the inconsistency engendered by the harmful behavior of the malicious node. Thus, further isolation or elimination process will be easily triggered.

4 Conclusion

In this paper, we presented and studied two special silent rank attacks against RPL-Contiki protocol. The demonstrated results in a random topology show how the intruder node could attract half the existing nodes in the topology to join its sub-DODAGs, without leaving any traces behind. Usually, rank attack is combined and followed by other types of attack such as isolation attacks, IP spoofing, selective forwarding attack, *etc.* The obtained results show that the default RPL-Contiki requires many improvements in terms of security to face the potential threads in IoT networks.

In order to make the detection of the new variant of rank attack possible, a slight modification in RPL functioning code is proposed to allow triggering loops in the case where a malicious node advertises a similar rank value as its preferred parent. Combined to existing RPL rank attack countermeasure based on the detection of loops, it becomes easy to detect the attack and neutralize the intruder node. This implementation presents a viable addition to enhance the security aspect in default RPL Contiki.

References

[1] M. Majid *et al.*, "Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review," *Sensors*, vol. 22, no. 6, p. 2087, 2022. doi:10.3390/s22062087.

[2] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *Journal of Network and Computer Applications*, vol. 161, p. 102630, Jul. 2020, doi: https://doi.org/10.1016/j.jnca.2020.102630.

[3] M. Saleh *et al.*, "Deep reinforcement learning based transmission policy enforcement and multi-hop routing in QoS aware LoRa IoT networks," *Computer Communications*, vol. 183, pp. 33-50, Feb. 2022, doi: https://doi.org/10.1016/j.comcom.2021.11.010.

[4] A. Raghuvanshi, U. Kumar Singh, M. Shuaib, and S. Alam, "An investigation of various applications and related security challenges of Internet of things," *Materials Today: Proceedings*, Mar. 2021, doi: https://doi.org/10.1016/j.matpr.2021.01.821.

[5] M. N. Khan, A. Rao, and S. Camtepe, "Lightweight Cryptographic Protocols for IoT Constrained Devices: A Survey," *IEEE Internet of Things Journal*, pp. 4132-4156, 2020, doi: https://doi.org/10.1109/jiot.2020.3026493.

[6] V. Adat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture," *Telecommunication Systems*, vol. 67, no. 3, pp. 423-441, Jun. 2017, doi: https://doi.org/10.1007/s11235-017-0345-9.

[7] J. Neeli and S. Patil, "Insight to Security Paradigm , Research Trend & Statistics in Internet of Things(IoT)," *Global Transitions Proceedings*, Jan. 2021, doi: https://doi.org/10.1016/j.gltp.2021.01.012.

[8] N. Miloslavskaya and A. Tolstoy, "Internet of Things: information security challenges and solutions," *Cluster Computing*, vol. 22, no. 1, pp. 103-119, Jul. 2018, doi: https://doi.org/10.1007/s10586-018-2823-6.

[9] J. Howarth, "80+ Amazing IoT Statistics (2022-2030)," *Exploding Topics*, Dec. 22, 2021. https://explodingtopics.com/blog/iot-stats

[10] Liebermann. N, "2021 IoT Security Landscape - SAM Seamless Network," Apr. 07, 2022. https://securingsam.com/2021-iot-security-landscape

[11] T. Winter , "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," *tools.ietf.org*. https://tools.ietf.org/html/rfc6550

[12] Gupta, M., Jain, S., & Patel, R. B, "Security issues in internet of things: principles, challenges, taxonomy. In: Singh, P.K., Singh, Y., Kolekar, M.H., Kar, A.K., Chhabra, J.K., Sen, A. (eds) Recent Innovations in Computing. ICRIC 2020. Lecture Notes in Electrical Engineering, Springer, Singapore 701. https://doi.org/10.1007/978-981-15-8297-4_52, 2021

[13] R. R. Krishna, A. Priyadarshini, A. V. Jha, B. Appasani, A. Srinivasulu, and N. Bizon, "State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and Solutions," *Sustainability*, vol. 13, no. 16, p. 9463, Jan. 2021, doi: https://doi.org/10.3390/su13169463.

[14] M. A. Boudouaia, A. Ali-Pacha, A. Abouaissa, and P. Lorenz, "Security Against Rank Attack in RPL Protocol," *IEEE Network*, vol. 34, no. 4, pp. 133-139, Jul. 2020, doi: https://doi.org/10.1109/mnet.011.1900651.

[15] 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: https://doi.org/10.1007/s12083-021-01275-3.

[16] A. Seyfollahi, M. Moodi, and A. Ghaffari, "MFO-RPL: A secure RPL-based routing protocol utilizing moth-flame optimizer for the IoT applications," *Computer Standards & Interfaces*, vol. 82, p. 103622, Aug. 2022, doi: https://doi.org/10.1016/j.csi.2022.103622.

[17] P. P. Ioulianou, V. G. Vassilakis, and S. F. Shahandashti, “A Trust-Based Intrusion Detection System for RPL Networks: Detecting a Combination of Rank and Blackhole Attacks,” *Journal of Cybersecurity and Privacy*, vol. 2, no. 1, pp. 124-152, Mar. 2022,
doi: https://doi.org/10.3390/jcp2010009.

[18] A. Agiollo, M. Conti, P. Kaliyar, T.-N. Lin, and L. Pajola, “DETONAR: Detection of Routing Attacks in RPL-Based IoT,” *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1178-1190, Jun. 2021,
doi: https://doi.org/10.1109/tnsm.2021.3075496.

[19] Z. A. Almusaylim, N. Jhanjhi, and A. Alhumam, “Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP,” *Sensors*, vol. 20, no. 21, p. 5997, Oct. 2020, doi: https://doi.org/10.3390/s20215997.

[20] P. S. Nandhini, S. Kuppuswami, and S. Malliga, “Energy efficient thwarting rank attack from RPL based IoT networks: A review,” *Materials Today: Proceedings*, May 2021,
doi: https://doi.org/10.1016/j.matpr.2021.04.167.

[21] A. Mayzaud, R. Badonnel, I, Chrisment, “A taxonomy of attacks in RPL-based internet of things”, *International journal of network security*, 18 (3), 459-473, 2016, DOI : 10.6633/IJNS.201605

[22] H. Kumar Saini and M. Poriye, “Threats, Detection and Mitigation of Rank Attack: A Survey,” *SSRN Electronic Journal*, 2021,
doi: https://doi.org/10.2139/ssrn.3884409.

[23] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, “The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks,” *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3685-3692, Oct. 2013,
doi: https://doi.org/10.1109/jsen.2013.2266399.

[24] M. Rouissat, M. Belkheir, and H. S. A. Belkhira, “A potential flooding version number attack against RPL based IOT networks,” *Journal of Electrical Engineering*, vol. 73, no. 4, pp. 267-275, Aug. 2022, doi: https://doi.org/10.2478/jee-2022-0035.

[25] 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.

[26] P. Thubert, (2012, March). Objective function zero for the routing protocol for low-power and lossy networks (RPL). Internet Engineering Task Force. Retrieved July 20, 2022.
http://www. ietf.org/rfc/rfc6552.txt

[27] O. Gnawali, P. Levis, (2012 September), The minimum rank with hysteresis objective function. Internet Engineering Task Force. Retrieved July 20, 2022. URL http://www.ietf.org/rfc/rfc6719.txt

[28] D. Airehrour, J. Gutierrez, and S. K. Ray, “Secure routing for internet of things: A survey,” *Journal of Network and Computer Applications*, vol. 66, pp. 198-213, May 2016,
doi: https://doi.org/10.1016/j.jnca.2016.03.006.

[29] M. Amirinasab Nasab, S. Shamshirband, A. Chronopoulos, A. Mosavi, and N. Nabipour, “Energy-Efficient Method for Wireless Sensor Networks Low-Power Radio Operation in Internet of Things,” *Electronics*, vol. 9, no. 2, p. 320, Feb. 2020,
doi: https://doi.org/10.3390/electronics9020320.

[30] S. S. Solapure and H. H. Kenchannavar, “Design and analysis of RPL objective functions using variant routing metrics for IoT applications,” *Wireless Networks*, vol. 26, no. 6, pp. 4637-4656, May 2020, doi: https://doi.org/10.1007/s11276-020-02348-6.

[31] R. Stephen, L. Arockiam, (2018) “RIAIDRPL: Rank Increased Attacks (RIA) Identification algorithm for avoiding loop in the RPL DODAg”, *International Journal of Pure and Applied Mathematics*, 119 (16), 1203-1210, 2018.

Received 23 October 2023