Selective Sub-DODAGs Hiding "SSDH" a new Attack in IoT RPL-Based Networks

Sid Ahmed Hichame Belkhira[a], Mehdi Rouissat[b] Mohammed Belkheir[c],Merahi Bouziani[d]

[a] Assistance professor on computer science university Center Nour Bachir, El-Bayadh Algeria MIPS Laboratory, University of Haute Alsace, France

[b] Assistance professor on Telecommunication university Center Nour Bachir, El-Bayadh Algeria STIC Laboratory, University Aboubek Belkaid, Tlemcen, Algeria

[c] Assistance professor on Telecommunication Center Nour Bachir, El-Bayadh Algeria, LIMA Laboratory, Univeristy Center Nour Bachir, El-Bayadh, Algeria

[d] full professor on Telecommunication Djillali Liabes University, Sidi Bel Abbes, Algeria, LTTNS Labortory Djillali Liabes University, Sidi Bel Abbes, Algeria

Abstract: The security concern in RPL-based IoT networks has gained a close attention by the researchers in the recent past years. This is due to the inherent constraints of nodes and the frequent change in the network topology. This makes the network vulnerable to various attacks that intend to disrupt the network availability and nodes resources. Heavy and decentralized algorithms seeking to enable the security in RPL networks as cryptographic schemes or expensive solutions are not convenient due to intrinsic characteristics of IoT nodes. In this paper, we propose and analyse a new internal hybrid routing attack against RPL, named SSDH for Selective Sub-DODAGs Hiding attack. The intruder node performing the present attack intends to isolate and exhaust the resources of a targeted subset of nodes by a selective hiding, based on its routing table. Compared to other known isolation attacks, the proposed one shows a silent malicious behavior, in which the root never knows about the isolated nodes. After the selective hiding process by dropping all packets coming from its direct or indirect children nodes, the intruder node follows its malicious behavior by provoking the victim nodes to conduct a DIO flooding based on falsified DIO messages. Simulation results obviously depict the harmful disruption of the present attack in different scenarios of RPL-based networks, by measuring the main QoS metrics: Control overhead, energy consumed, packet delivery ration and average delay. It should be noticed that the present paper describes the process of the new proposed at- tack and its effect, where the preventive and mitigation solutions will be the subject of a future work

.**Keywords:** IOT, RPL, security, Attack, Cooja

1. Introduction

Since the last decade, the world is overwhelmed by a new trend of wireless technologies that allow connecting small smart devices called sensors, which are born from the micro- electronic and Nano electronic technologies. These emerging networks, mainly known as IoTs (Internet of Things), are in- tended to connect devices, machines and end users to gather data from various environments and forward it through inter- net. This data is then, collected and treated via smart applications for further analysis and decision-making. The omnipresence of sensors in various domains leads to the exponential growth of IoT devices, where it is expected to be about 50 billion devices in use worldwide at the end of 2030 . They are deployed almost everywhere, in military, clothes, oil and gas plants, human bodies, healthcare environments, smart ecosystems, and so on (Hassija, n.d.).

Although IoT devices do not require a high through- put expectation, the evolving scalability concern remains the first challenge when deploying IoT networks (Overmars & Venkatraman, 2020). The important number of connected devices makes the existing net- works leveraged by questions on the addressing and data forwarding processes. IPV4 routing protocols are unable to support this huge number of IoT devices, which makes the IPV6 implementation with its extended addressing scheme a suitable solution to connect IoT devices (Kassab & Darabkh, 2020). In addition, sensor devices are expected to operate under different conditions, compared to the existing wired networks, and are very constrained in terms of resources and energy efficiency, which presents an additional challenge when deploying such networks. Other challenges related to IOT specifications such as latency, real-time and secure data transfer should be resolved to ensure an acceptable efficiency in terms of QoS criterion (Avila et al., 2020). Many research articles and studies classify the 5th generation architecture as the potential candidate for IoT networks, since they are expected to offer a high scalability level by connecting various kinds of mobile users and IoT devices (*System architecture for the 5G system (5GS)*, 2020). This generation of mobile networks implements a flexible architecture allowing an efficient data transfer that fits the requirements of IoTs (Rong et al., 2020). IoTs networks are considered as Low Power and Lossy Networks (LLN), where classical routing mechanisms for wired networks that are implementing complex overheads are not suitable for such kind of networks, due to the limited re- sources of the IoT devices. Other concern is the network security level, since IoT devices cannot support heavy se- cure algorithms and cryptographic solutions, which make the IoT networks vulnerable for external attacks (Varga et al., 2020). In this paper, we are focusing on the security challenging concern of IoT networks implementing RPL (Routing Protocol for Low-Power and Lossy Networks). Our work is focusing on proposing a new internal hybrid attack scheme called SSDH, for Sub-DODAGs Hiding attack, where the intruder node seeks the network availability and resources exhausting. The intruder node starts its malicious behavior by pretending to have a good rank value through falsified DIO messages (DODAG Information Object), followed by performing a selective isolation attack in order to dissimulate its counterfeit action, and ends its harmful behavior by a flooding attack to exhaust the resources of the targeted nodes. In this proposed attack, the sink node will not be aware of the existing isolated nodes, which make the attack low profile and hard to detect. Simulations performed using Cooja depict the effect of the proposed attack in terms of QoS and security concern for different scenarios of IoT networks facing such kind of attack. The rest of the paper is organized as follows. In section 2 we briefly define the RPL routing protocol and its basic scheme for connecting nodes and routing data. In section 3 we detail some related works according to DAO attacks and black-hole attacks an IoT networks. In Section 4, we focus on the security challenging issues for IoT networks using RPL as routing protocol, and the well-known attacks against RPL. In section 5, we describe how the SSDH attack is conducted by a malicious node in an IoT network using RPL. In section 5, we analyze and discuss the obtained results from the different behavior of an RPL-based network through the three steps of the SSDH attack. Finally, we conclude the paper by providing some future proposals to prevent and avoid such attacks.

2 RPL ROUTING PROTOCOL

RPL is one of the widely known routing protocols for LLNs, developed by IETF (Jurcut et al., 2020). RPL is an IPv6 based distance vector routing protocol, where devices are interconnected as DODAG. In LLNs using RPL, nodes exchange control messages to conclude the network topology and select their routers among their neighborhood nodes. RPL implements mainly four control messages to establish and maintain the DODAG:

DIS, DAO, DAO-Ack and DIO. Each message is defined by a type in ICMP stack and contains a header describing its functions. DIS (DAG Information Solicitation) are sent by a node to ask parameters allowing it to join a DODAG. DIO messages (DODAG Information Object) are exchanged between nodes in order to perform the upward routes. DAO messages (Destination Advertisement Object) are exchanged between nodes in order to perform the downward routes. A DAO message can be either generated by the node itself containing its own address, or it can be a message of one of its children being forwarded and containing the address of the child in the option target field (the node that generated the DAO message). This DAO messages are transmit- ted in end-to-end fashion, from a child node and forwarded several times equivalent to the number of parents up to the DODAG root. In addition, Upwards paths toward the sink are performed by using objective function called MRHOF (Minimum Rank Hysteresis Objective Function) defined by the RFC6719. The latter implements metrics allowing each node to calculate its proper Rank and advertises it via DIO messages. Based on this value, each node selects its parents among its neighbors. The rank value is calculated by converting the path cost through the parent or by adding the rank value advertised by a parent with the MinimumHopRank Increase parameter defined by RPL. If the DIO metrics container is empty, MRHOF uses by default the ETX metric (Expected Transmission Count) to compute the rank value. The objective function calculates the Rank value using, the following equation:

$$\mathrm{Rank}_{mode} = \mathrm{MHRI} * (1 + \mathit{floor}\,(\mathrm{Rank}_{parent}\,/\mathrm{MHRI})) \qquad (1)$$

Where:

– MHRI: is the MinHopRankIncrease value. By default MHRI value is 256 and represents the root rank value.

– Floor (x): calculates the greatest integer less than or equal to x.

This means that lower Rank value has a node, closer it is located to the root. Following the previous process, each node maintains a parent list with a preferred parent and thus, the network convergence is achieved. In case of inconsistency, RPL implements a preparation process called local repair that can be triggered by each node facing a problem. This allows nodes to detach from their preferred parents and restart the parent selection process. In addition, the root node may cording to a specific hybrid mesh/tree topology called DODAGs trigger a global repair in order to mitigate the occurred in (Destination Oriented Directed Acyclic Graphs). This latter is built from a root node acting as the data sink of the consistency. This process increments the DODAGVersion Number parameter.

3 RELATED WORK

Various recent works and surveys have studied the security challenging issues in IoT networks. In this section, we high- light some works related of rank attacks, black hole attacks and DAO attacks, as our present work involves these kinds of attacks. Other researches have focused on the mitigation solutions to counter attacks against RPL.

Rank attacks intend to fake the rank value by the malicious node in order to gain a good position in the DODAG, this behaviour is named the Decreased Rank Attack (Sanmartin et al., 2018). The malicious node can also increase its rank value to perform a greedy behaviour allowing it to move deeper in the DODAG and increase the list of its parent set (Djedjig et al., 2020).

Black hole attacks aim to drop packets from the neigh- boring nodes and don't forward them. Thus, we can consider two main possibilities; the malicious node takes into consideration control rules imposing by the routing protocol and fakes itself, or the node doesn't respect the routing rules and leverages the security weaknesses of the routing protocol in order to establish its malicious behaviour (A. Almusaylim et al., 2020). Depending on the number of malicious nodes performing the attack, we can distinguish between simple and cooperative black hole attacks (Seyedi & Fotohi, 2020).

Authors in (Hammamouche et al., 2018), exploited the DTSN (DAO trigger Sequence Number) field contained in DIO messages. In RPL, the value of DTSN is maintained by each node and it is communicated via DIO messages. A node that increments DTSN obliges nodes belonging to its Sub-DODAG to send DAO messages. Thus, a malicious node may constantly increments its DTSN to submerge the network by DAO messages and exhausts the resources of its children.

In (Baghani et al., 2020), authors have analysed the case when a malicious node having a good rank in the network, may send fake in- formation via DAO messages to its parents. Fake gathered information by the root may lead to establish non-optimized downward routes and affect the network efficiency.

Another attack known as "DAO inconsistency attack" is studied in (Ghaleb et al., 2019). This attack utilizes the packet option header containing the error-forwarding flag, which indicates whether a down-route is stale. In the storing mode, a malicious node may set the error forwarding bit and replies to a parent with a forwarding error packet in order to declare the old and the nonexistence of the selected route. This act leads to iso- late potential nodes belonging to the malicious node Sub- DODAG and subsequently an suboptimal topology of the network.

In (Wadhaj et al., 2020), authors highlighted the case when a malicious node exploits the feature of sending periodic DAO messages from a child node to its parents. The generation of a DAO message by a child node, leads to multiple forwarded mes- sages, depending on the number of hops up to the root. This overflowing of DAO messages exhaust the resources of the nodes and subsequently the possibly lifetime of the entire network.

The combination of the rank attack with blackhole attack and after a flooding attack leads to more dangerous hybrid attack in the stability of the network, since the malicious node well positioned in the DODAG, illegitimately hides an amount of selected nodes, drops their packets and exhausts their batteries. This has a significant disruption in increasing the control overhead, reducing the data packet delivery and increasing the latency. Many approaches have been pro- posed by researchers in order to prevent and mitigate some of the previous cited attacks (Min et al., 2020). The results show that these methods can be efficient for IoT networks, but the security challenge is still a relevant issue due to the various vulnerabilities that IoT networks are suffering from, and the large number of attacks that may arise. In addition, security solutions based on machine learning or complex algorithms remain heavy to be supported by constrained IoT devices due to their limited intrinsic characteristics in terms of calculation, power and memory capacity, which makes a tradeoff between the network security level and the QoS.

4 SECURITY ATTACKS AGAINST RPL

RPL protocol is threaded by a number of attacks that can be divided into three main categories (Raoof et al., 2019).

1. Attacks Against resources: are accomplished by making legitimate nodes perform unnecessary processing in order to exhaust their resources i.e. power, processing or memory resources, this leads to disrupting the network availability. The most known attacks in this category are Flooding, Increased Rank attack, DAG inconsistency, Routing table Overload and Version number modification (Mayzaud et al., 2016).

2. Attacks Against topology: aim to produce topological distortion in RPL based IoT networks. Consequently, the network will not converge to the optimal form in terms of routing (e.g. optimal paths). Attacks against the topology include also isolating nodes or isolating Sub-DODAGS, which means that those nodes are no longer able to communicate with their parents or with the RPL root (Hashemi & Shams Aliee, 2019) The most serious attacks in this category are Routing table tampering, Sink hole, Blackhole, Worst parent, Worm- hole, and DAO inconsistency.

3. Attacks against traffic: these attacks usually aim to capture network traffic or information transmitted by nodes. The most serious attacks in this category are Sniffing, Traffic Analysis, Eavesdropping, Decreased Rank attack, and Sybil attack (Mirshahjafari & Ghahfarokhi, 2019).

Our present work deals with another trend of attacks called hybrid attacks. The disruption level of this kind of attacks depends on the affected area and nodes in the DODAG:

- Upward nodes (parents)
- Downwards nodes (children)
- Neighbors
- All the nodes in the DODAG

The hybrid attacks possibly affect more than one area comparing to a simple attack. This explains their severity on disrupting the network availability and resources.

5 SSDH ATTACK PROCESS

The attack scheme we are proposing is a hybrid attack that simultaneously affects traffic, resources and topology. Fig. 1., illustrates the process performed by the malicious node, starting by a rank attack through which the traffic is targeted, followed by nodes isolation where the topology is affected and then flooding attack that disrupts the isolated nodes re- sources as well as their neighbors. By the following, we will detail the different operations carried out by the malicious node to perform the SDH attack.

5.1 Rank attack

The rank is a value that determines the position of a given node with respect to the root node (Preeth et al., 2020). In RPL, nodes select the preferred parent from a set of nodes based on the best rank value, this parent becomes the default used gateway to send data toward the DODAG root. The lower the rank value is, the closer the node is to the sink node, and consequently the more traffic has to be managed by this node, because of its strategic position in the DODAG. In Rank at- tack, a malicious intruder node advertises a lower rank value in instead of the real value it should has, and illegitimately attracts neighboring nodes with a misused counterfeit rank value, through which it overclaims its performances and announces that it is well positioned and close to the root. This allows it to be more frequently chosen as preferred parent, which leads to a suboptimal topology. To implement the rank attack, the objective function is modified as shown by the following equation:

$$\text{Rank}_{\text{Malicious}} = \text{Rank}_{\text{Best parent}} + 1 \qquad (2)$$

As shown by Fig. 1., the malicious node modifies its rank value at the beginning of its attack process.

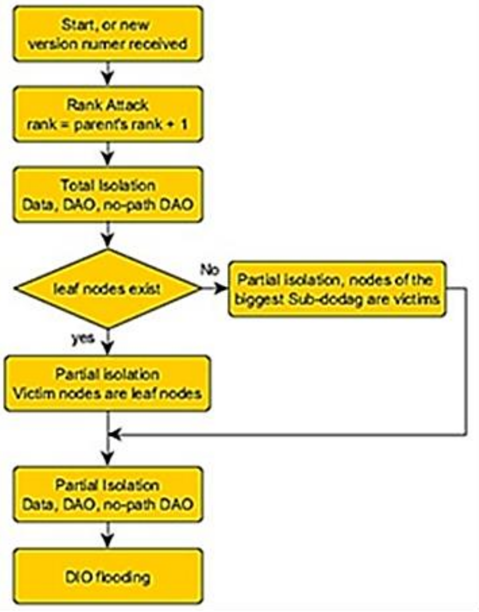
Start, or new version numer received
Rank Attack rank = parent's rank + 1
Total Isolation Data, DAO, no-path DAO
leaf nodes exist
No
Partial isolation, nodes of the biggest Sub-dodag are victims
yes
Partial isolation Victim nodes are leaf nodes
Partial Isolation Data, DAO, no-path DAO
DIO flooding

Fig. 1 SSDH Attack process

When nodes select the malicious node in the context of a false rank value, the traffic will be routed through this malicious node and non optimized paths are created. We should notice that RPL has no mechanism of protection against the illegally alteration of a node's rank. The rank attack is generally followed by dropping packets attacks.

5.2 Isolation Attack

After well positioning in the network, an important amount of traffic will pass through the attacker node. The next step carried out by the intruder is to isolate all the nodes connected directly or indirectly to it. This is done by dropping DAO messages, No-path DAO messages and data messages. DAO messages are sent upwards between nodes in order to create the downward routes. By dropping DAO messages, the downward routes toward the children nodes could not be created. This sub-DODAGs hole, will isolate an entire part of the network, and the root will never hear of the isolated nodes. The ingenuity of the present attack is that the intruder performs a selective hiding rather than isolating all the children belonging to it, in order to dissimulate it malicious behavior. To do so, this operation is based on the routing table of the malicious node that allows it to select children among its connected sub-Dodags, to hide their traffic. As depicted by figure 1, if the intruder has leaf nodes connected to it, it will forward that traffic and drop the remaining. On the other hand, if no leaf is connected, but only composed sub- Dodags, it will isolate the biggest sub-Dodag. Let's M is the malicious node performing the selective isolation, the formula (2) illustrates the selective isolation of the node M :

$$S(M) = Max_{N \in C(M)}(\sum^{i} C(i)) \qquad (3)$$

Where :

– S(M) is the selective set to hide by the node M

– N is a child connected to the node M

– C(i) is the children set of a node N

This adaptive isolation based on the routing table of the malicious node makes the attack dynamic, silent and hard to detect by the network.

5.3 Flooding Attack

Legitimates. The obtained results from the simulation of the reference network (where all available nodes in the graph ran legitimate RPL source code) are used as a benchmark to compare and evaluate the different behaviors of the network in the case of attacks.

To evaluate the impact of the proposed attack on the net- work, we performed the simulations using the Contiki operating system (Lamaazi & Benamar, 2020), an open-source and lightweight operating system designed for IoT.

Fig. 2. shows the convergence of the reference network after 15 minutes of simulation, where the node 18, is acting like a legitimate node. In this normal case, two nodes are connected to the node 18, which are node 15 and node 11.

Usually, the flooding attack is directly conducted by the malicious node itself, by sending multicast DIS messages to its neighboring nodes frequently (Stephen & Arockiam, 2018). In our case, the flooding is both, directly and indirectly conducted, by provoking the victim nodes to send DIO messages more frequently. The two parameters 'RPL_DIO_INTERVAL_MIN' the 'RPL_DIO_INTER define the DIO trickle timer, and are used to calculate respectively, the minimum (Imin) and the maximum interval (Imax) between DIO messages, [35](Abhinaya & Sudhakar, 2021). According to RPL (Imax) is a number of doublings of (Imin), where :

$$K = log_2 \frac{I_{max}}{I_{min}} \quad (4)$$

For example if k=16, and Imin = 100ms, so we can define Imax ≈ 109 minutes. In addition to these parameters a trickle instance maintains three other parameters as follows:

– I: the current Interval Value

– t: a time within the current value

– c: a counter

These values are defined by the sink and shared to all nodes through DIO messages. The malicious node sends falsified DIO messages, with modified and lower values of minimum and maximum interval DIO sending interval. This tampering will force the victim children to send DIO messages more frequently. This behavior intends to exhaust victim nodes resources (i.e. energy and processing). It also affects all the neighborhood of those nodes, where unnecessary DIO traffic must be processed, which leads to disrupting the network availability.

In order to study and compare the different behaviors of the network facing the proposed attack, we established a free It can be noticed from Fig. 2 that the sink node has two neighbors, node 17 with two connected children, and node 9 with 13 children.

Table 1 shows the total number of control messages processed during the 15 minutes of simulation, by the node 18 on the one hand, and by all the other nodes on the other hand.

Table 1 PROCESSED DIO AND DAO MESSAGES

	Sent / Generated		Transferred	Received	
Mote	DIO	DAO	DAO	DIO	DAO
All	281	166	255	731	411
18	14	10	31	68	39

According to the table 1, the generated DAO messages by node 18 is 10 messages, while forwarded DAO messages is 31, this is due the number of nodes attached to it, which is 2 and it presents 12.5Powertrace tool is used to extract the Energy consumption from the Cooja simulator, the collected raw data are given in terms of ticks. To calculate the consumed energy we use the formula (1).

$$Energy(mJ) = \frac{EnergestValue * Current * Voltage}{RT\ IMER} \quad (3)$$

The energy consumption is presented by four indicators, which are :

- Processor power (CPU) - it refers to the consumed en- ergy to process the different tasks of the nodes.
- LPM Power - refers to the energy consumed by the node in standby mode (idle mode).
- Listening Power - it refers to the energy consumed by the node to listen to messages.
- Transmit Power - - it refers to the energy consumed in transmitting packets.

In our simulations, we used Z1 motes, a MSP430-based board with an IEEE 802.15.4 compatible CC2420 radio chip. All nodes, including the intruder node have the same characteristics. Needed characteristics of Z1 mote are summarized in Table 2 [37] (*Zolertia Platforms - Zolertia*, n.d.)

Parameters	Value
Contiki OS version	Contiki 3.0
Mote device model	Z1 Zolertia
Z1 mote voltage	3?V
Z1 mote TX current	17.4 mA
Z1 mote RX current	18.8 mA Z1 mote CPU idle current
RTimer	32768 ticks per second Measurement interval
Parameters	Value
Contiki OS version	Contiki 3.0

Table 2 ZOLERTIA MOTE AND SIMULATION PARAMETERS

The energy consumption in 'mj' by the different nodes during 15 minutes of simulation is shown in figure 3. The figure illustrates that the node 16 has the most important consumed energy, 1917 mj, due to the number of nodes con- nected to it, which is 7, presents 47% of the available nodes. This is adding an additional task of forwarding which affect the energy consumption.

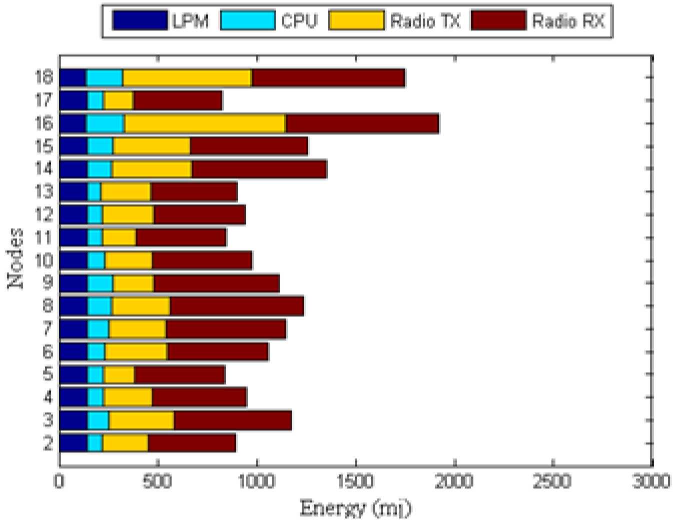

Fig. 3 Consumed energy in the reference network by the different nodes during 10 minutes

Leaf nodes, like the node 5, show the lowest consumption, due to its positions, that does not require any forwarding task.

7 RESULTS AND ANALYSIS

As described by the section IV, the proposed attack starts with rank decreasing attack, where the fake rank value that the malicious node is pretending to has will allow it to at- tract the nodes, and consequently chosen as preferred parent. In our simulations of the attack behavior, we consider four steps:

- Rank Attack only
- Rank attack followed by total isolation attack,
- Rank attack followed by total isolation, and then partial isolation,
- Rank attack followed by total isolation, then partial isolation and flooding attack

7.1 Rank attack

At the beginning of the convergence of a given network, every mote chooses over its list of parents, the one that has the best rank value. In order to have a strategic position within the network, the intruder node will pretend to has a good de- creased fake value of rank. Thus, through falsified DIO messages, the malicious node will be chosen more frequently as best parent by the other nodes in its neighborhood. This first step in the SSDH attack will allow an important amount of traffic to pass through the malicious node. Compared to the reference network in Fig. 2., the new topology when achieving a rank attack by the node 18 is illustrated by Fig. 4..

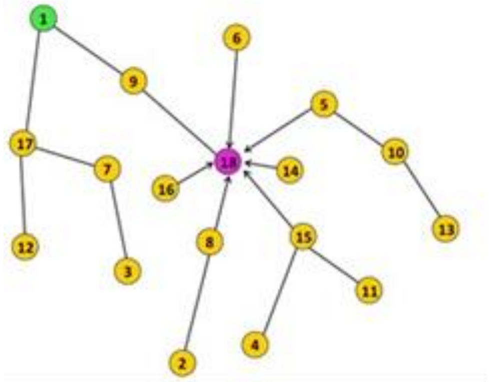

Fig. 4 Network topology, and the affected part after the rank attack

Fig.4 shows that 11 nodes are directly or indirectly connected to the malicious node, which presents 78.5% of the available nodes in the DAG that can be connected to the malicious node; excluding itself, the root, its parent (node 9), and the root's neighbors; (11/ (18-1-1-1-1)). The attractive rank value disseminated by the node 18 results in a successful rank attack.

Table 3 shows the total number of DIO and DAO control messages processed during 10 minutes period of simulation, by the malicious node 'node 18', and the total of all the nodes of the DAG.

	Sent/Generated		Transferred	Received DIO	
		DAO		DIO	DAO
	All the nodes				
Normal	281	116	255	731	411
Rank	263	157	246	697	412
	Node 18				
Normal	14	10	31	68	39
Rank	14	9	73	70	78

Table 3 Processed control messages before and after the rank attack

Table 3 shows that the number of forwarded DAO messages by the attacker node has increased from 31 messages in the normal case to 73 in the case of the rank attack. This increase is due to the strategic position the node 18 is claiming to has, which allowed it to be chosen as best parent by multiple nodes. Subsequently more unicasted DAO messages are sent to it. The intruder node can take advantage of the important traffic passing through it to make a dropping packets attack.

The energy consumed over 15 minutes of simulation is shown in figure 5. It depicts that the most energy consuming node is the malicious one, in terms of CPU, listening and transmitting radio, due to the amount of nodes connected to it. The total consumed energy increased by 67 %, where it jumped from 1751 m.J in the normal case to 2939 m.J after the rank attack. This is an expected result, due to the new role of the intruder node that presents a gateway to the sink.

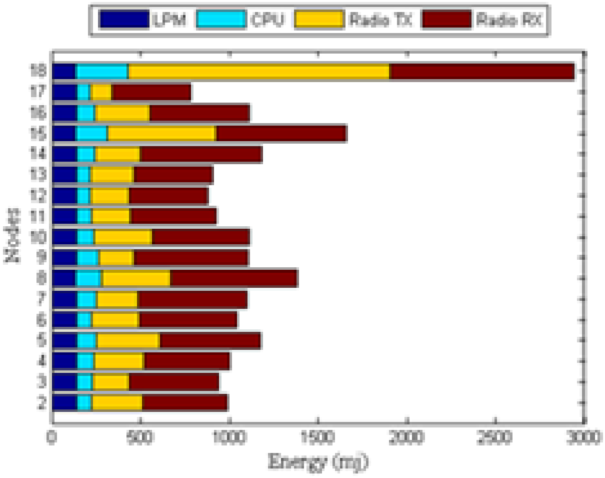

Fig. 5 Energy consumed by the different nodes after the rank attack

7.1 Total Isolation attack

As mentioned earlier, the aim of our work is not to implement a black-hole attack, where an attacker drops all the traffic passing through which, but the aim the present attack is to implement a smart hybrid action, by performing a partial isolating followed by a flooding. The partial isolation is adaptive, and it depends on the routing table of the intruder. This means that the latter must wait the network convergence achievement to make a decision about which amount of connected children will be isolated, while its dropping all the traffic passing through it. In order to simulate the present malicious activity, modifications are made in conby the malicious node, as well as DAO and no-path DAO control messages. This aims to totally isolate traffic coming from the selected intruder children.

Table 4 Processed control messages in the reference network, after the rank attack and after the isolation attack

	Sent/Generated		Transfered	Received DIO	
		DAO		DIO	DAO
	All the nodes				
Normal	281	116	255	731	411
Rank	263	157	246	697	412
Total isolation	265	141	115	693	272
	Node 18				
Normal	14	10	31	68	39
Rank	14	9	73	70	78
Total isolation	14	8	0	63	63

In this stage of the present attack, we compared the processed control messages in the reference network, after the rank attack and after the total isolation attack, where results are illustrated by table 4. It can be noticed a drop in the transferred DAO messages by the malicious node, from 58 in the rank attack to zero message in the isolating attack, which depicts the main malicious activity of the attack in this stage. This obtained result confirms the total isolation of every single node connected directly or indirectly to the intruder. By dropping all packets passing through it, the intruder is saving its listening and transmitting energy. This is well shown in Fig. 6. , where the energy consumption is decreased by 145%.

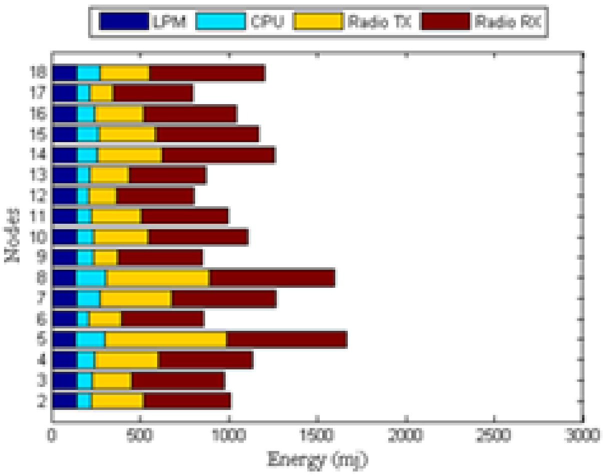

Fig. 6 Energy consumed by the different nodes after the total isolation attack

7.3 Partial Isolation attack

In order to show a normal behavior, the intruder will not drop all the traffic passing through it at the end, but just some of it, creating a partial isolation, as shown in figure

1. Based on the algorithms of figure1, and the topology after the rank attack shown in figure 4, the nodes which will not be isolated anymore are 14, 16 and 6 (figure 7) whereas the traffic coming from the remaining nodes will be dropped. In other words the traffic of 8 nodes will be dropped, which presents 72% of the traffic passing through it. This partial isolation is implemented in order to camouflage the malicious behavior of the attacker, therefore no abnormal signs will be noticed from the parents of the attacker node. More- over, having an attractive value of rank with low forwarding rate can be considered as a suspicious behavior, in order to make the isolation silent and low profiled, the intruder will not drop all the packet, but only a specific traffic. The attack can be considered as a special case of selective forwarding attack, where not a type of traffic is discarded, but the traffic of selected nodes is dropped in an adaptive way.

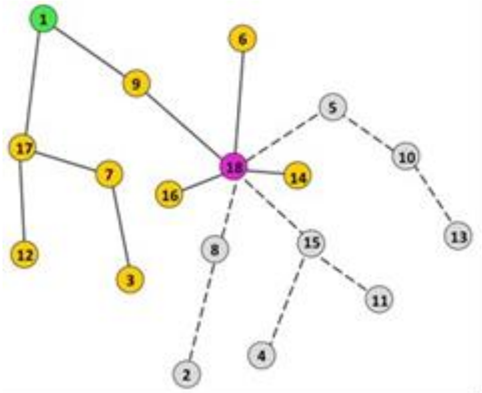

Fig. 7 Network topology, and the affected parts after the rank and partial isolation attacks

Through the partial isolation attack, the intruder is ensuring a forwarding task, this is shown in the increase in the power consumption, where it shown a slight increase from 1202 mj to 1259 mj, as shown in figure 8.

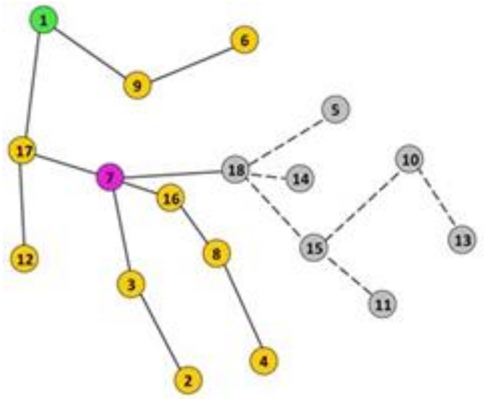

Fig. 8 Partial isolation in the case the node 7 is the intruder

We simulated the case where the node 7 is playing the intruder node, the result of rank attack is shown in figure

8. Based on the algorithm of figure 1, the nodes that will be isolated are the node 18 and its children, presenting the biggest Sub-Dodag.

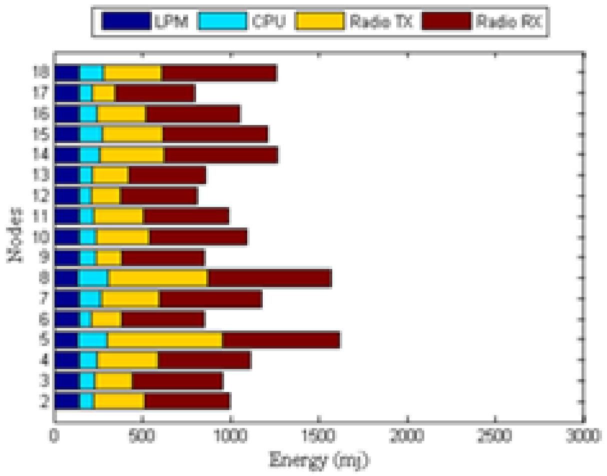

Fig. 9 Energy consumed by the different nodes after the rank and partial isolation attacks

The processed control messages during 15 minutes of simulation is shown in table 5, it shows an increase from zero to 16 DAO messages forwarded by the intruder.

	Sent/Generated		Transfered	Received DIO	
		DAO		DIO	DAO
	All the nodes				
Normal	281	116	255	731	411
Rank	263	157	246	697	412
Total isolation					
Partial Isolation	278	168	138	708	318
	Node 18				
Normal	14	10	31	68	39
Rank	14	9	73	70	78
Total isolation	14	8	0	63	63
Partial Isolation	15	6	16	59	86

Table 5 Processed control messages in the reference network, after the rank attack and after the partial isolation attack

The consumed energy by the malicious node, in case of the reference network, after the rank attack, after the total isolation attack and after the partial isolation attack are shown in figure 10. It can be seen from the figure that the consumed energy in the isolation step is much lower com- pared to the rank attack, which can be explained by the fact that the malicious node is not forwarding packets to its par- ents. And it shows a slight increase due to the partial for- warding task.

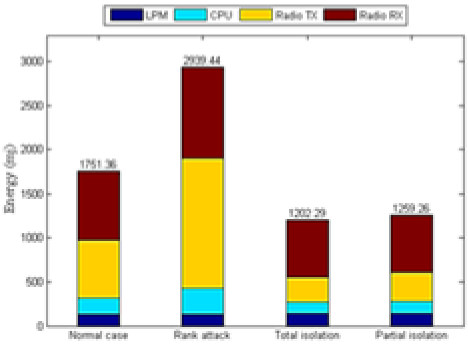

Fig. 10 Energy consumed by node 18 in the normal case, after rank attack, after the isolating attack, and after the partial isolation attack, respectively

The obtained results obviously demonstrate the impact of proposed hybrid, that shows a silent profile and it can be implemented without showing any suspicious behavior from the malicious node, which make it very damaging and difficult to be detected.

7.4 Flooding attack

In order to make the proposed SDH attack more damaging, a DIO flooding attack is conducted after the selective isolation attack. The goal of the flooding is to exhaust the resources of all the neighbors of the malicious node (direct flooding attack), and the isolated nodes plus their neighbors (indirectflooding attack). In order to conduct the DIO flooding attack, the malicious node set the value of the 'RPL_DIO_INTERVA to be five for itself, which is also the value shared in its sent DIO messages. The 'RPL_DIO_INTERVAL_DOUBLINGS' is set to be 8 for itself, and also it is the value shared in its sent DIO messages.

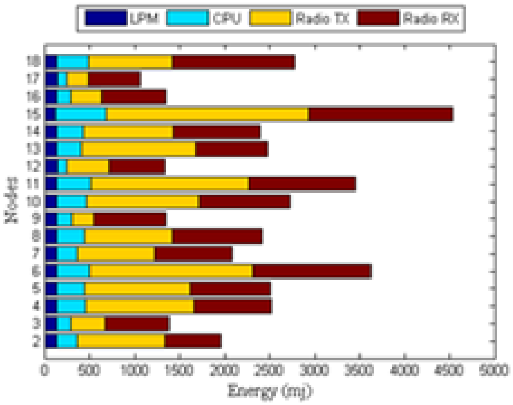

Fig. 11 Energy consumed by the different nodes after the flooding attack

Figure 11 shows the energy consumed by the different nodes after the flooding attack. The figure shows that all the isolated nodes and their neighbors are differently affected. The most affected nodes are the neighbors, such as nodes 5, 8, 7 and 14. Figure 12 shows the consumed energy by the affected nodes in the normal case and after the flooding attack. The figure illustrates the serious effect on the con- sumed energy, for instance the consumed energy by node 15 increases from 1260 m.J to 4532 m.J which presents an increase of 259%.

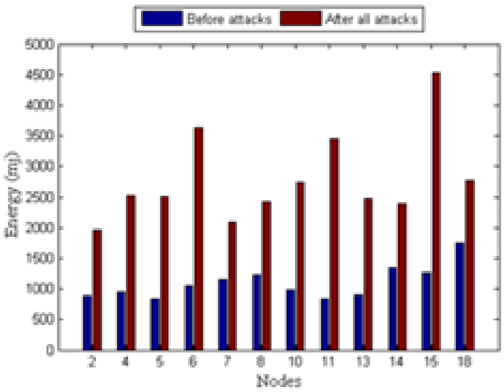

Fig. 12 Consumed energy by the affected nodes in the normal case and after the flooding attack

These obtained results show how seriously the nodes are affected, this huge increase in the consumed energy will affect directly the life time of the nodes, and consequently the network.

7.5 Packet delivery ratio and Latency measurements

In addition to the control overhead and the energy consumption that are analyzed earlier, the packet delivery ratio (PDR) and the latency are other important metrics that measure the QoS of a network. The PDR is defined as the ration between the number of received packets to the total number of the send ones. Higher is the PDR, better is the quality of a net- work. Figure 13 shows the PDR for different stages of the attack. It clearly shows that the total isolation attack has the worst delivery ratio; 37%. This ratio a little bit higher in the case of the partial isolation, due to the adaptive hiding selection.

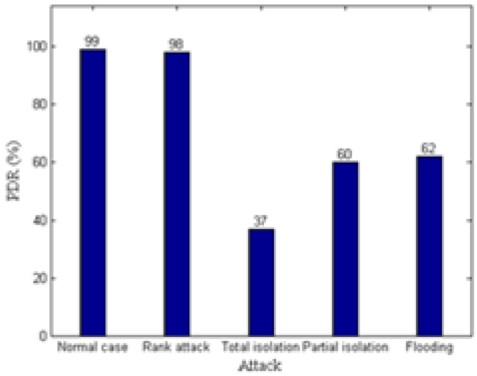

Fig. 13 Packet Delivery Ratio for the different stages of the global attack

The latency metric measures the average delay made by packets passing through the network, from the source to their destination. This parameter indicates the efficiency level of a network to hold some real time application sensi- tive to the time.

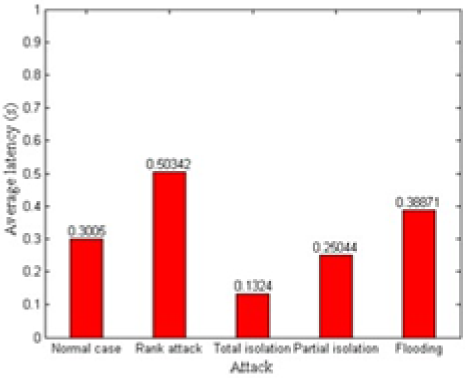

Fig. 14 Average Latency for the different stages of the global attack

The figure 14 shows the average latency for the different stages of the attack. The average delay shows an increase in the rank attack, this is the result of the non-optimal paths cre- ated because of the attack. The total isolation attack shows a lower latency, which is based on the lowest PDR recorded. In the case of the flooding, the latency is increased, this is due to the important amount of control messages exchanged within the network during the flooding.

8 CONCLUSION AND FUTURE WORK

In this paper, we have presented an hybrid attack, named SSDH for Selective Sub-DODAG Hiding attack, in which the intruder node starts its malicious behavior by pretending having a good position in the DODAG, through advertising a good decreased fake value of rank in falsified DIO messages. After that, the selective isolation is conducted, based on the state of the network and the routing table of the malicious node, in this adaptive isolation, DAO, no-path DAO and data packets are dropped, where the malicious node does not forward packets it supposed to forward to its parent. Thus, no downward routes will be created toward the isolated nodes, and neither the parent of the intruder node, nor the sink will be aware about the isolated nodes, here the PDR dropped to 60 %.

The obtained and discussed results show the effects of the attack on the topology, and on the intruder node itself, where the value of consumed energy has dropped from 1751

m.J to 1202 m.J in the isolating attack because the intruder does not assure any forwarding task.

The adaptive partial isolation attack is followed by a flooding mechanism aiming to exhaust the resources of targeted nodes. The obtained results show that 66% of the nodes were seriously affected, where its lifetime decreased by 75%. This may significantly degrade the network performances and then lead to reducing the network lifetime.

References

System architecture for the 5G system (5GS), 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 23.501 ___ (2020).

A. Almusaylim, Z., Jhanjhi, N. Z., & Alhumam, A. (2020). Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP. *Sensors*, *20*(21), 5997. https://doi.org/10.3390/s20215997

Abhinaya, E. V., & Sudhakar, B. (2021). A secure routing protocol for low power and lossy networks based 6LoWPAN networks to mitigate DIS flooding attacks. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-020-02804-3

Avila, K., Jabba, D., & Gomez, J. (2020). Security Aspects for Rpl-Based Protocols: A Systematic Review in IoT. *Applied Sciences*, *10*(18), 6472. https://doi.org/10.3390/app10186472

Baghani, A. S., Rahimpour, S., & Khabbazian, M. (2020). The DAO Induction Attack Against the RPL-based Internet of Things. *2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 1–5. https://doi.org/10.23919/SoftCOM50211.2020.9238224

Djedjig, N., Tandjaoui, D., Medjek, F., & Romdhani, I. (2020). Trust-aware and cooperative routing protocol for IoT security. *Journal of Information Security and Applications*, *52*, 102467. https://doi.org/10.1016/j.jisa.2020.102467

Ghaleb, B., Al-Dubai, A., Ekonomou, E., Qasem, M., Romdhani, I., & Mackenzie, L. (2019). Addressing the DAO Insider Attack in RPL's Internet of Things Networks. *IEEE Communications Letters*, *23*(1), 68–71. https://doi.org/10.1109/LCOMM.2018.2878151

Hammamouche, A., Omar, M., Djebari, N., & Tari, A. (2018). Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET. *Journal of Information Security and Applications*, *43*, 12–20. https://doi.org/10.1016/j.jisa.2018.10.004

Hashemi, S. Y., & Shams Aliee, F. (2019). Dynamic and comprehensive trust model for IoT and its integration into RPL. *The Journal of Supercomputing*, *75*(7), 3555–3584.

Hassija, C. (n.d.). Goyal, and Sikdar. Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B (2019b) A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access*, *7*, 82721–82743.

Jurcut, A., Niculcea, T., Ranaweera, P., & Le-Khac, N.-A. (2020). Security Considerations for Internet of Things: A Survey. *SN Computer Science*, *1*(4), 193. https://doi.org/10.1007/s42979-020-00201-3

Kassab, W., & Darabkh, K. A. (2020). A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations. *Journal of Network and Computer Applications*, *163*, 102663. https://doi.org/10.1016/j.jnca.2020.102663

Lamaazi, H., & Benamar, N. (2020). RPL Enhancement Based FL-Trickle: A Novel Flexible Trickle Algorithm for Low Power and Lossy Networks. *Wireless Personal Communications*, *110*(3), 1403–1428. https://doi.org/10.1007/s11277-019-06792-2

Mayzaud, A., Badonnel, R., & Chrisment, I. (2016). A Taxonomy of Attacks in RPL-based Internet of Things. *International Journal of Network Security*, *18*(3), 459–473.

Min, S.-W., Chung, S.-H., Lee, H.-J., & Ha, Y.-V. (2020). Downward traffic retransmission mechanism for improving reliability in RPL environment supporting mobility. *International Journal of Distributed Sensor Networks*, *16*(1), 1550147720903605. https://doi.org/10.1177/1550147720903605

Mirshahjafari, S. M. H., & Ghahfarokhi, B. S. (2019). Sinkhole+CloneID: A hybrid attack on RPL performance and detection method. *Information Security Journal: A Global Perspective*, *28*(4–5), 107–119. https://doi.org/10.1080/19393555.2019.1658829

Overmars, A., & Venkatraman, S. (2020). Towards a Secure and Scalable IoT Infrastructure: A Pilot Deployment for a Smart Water Monitoring System. *Technologies*, *8*(4), 50. https://doi.org/10.3390/technologies8040050

Preeth, S. K. S. L., Dhanalakshmi, R., Kumar, R., & Si, S. (2020). Efficient parent selection for RPL using ACO and coverage based dynamic trickle techniques. *Journal of Ambient Intelligence and Humanized Computing*, *11*(11), 4377–4391. https://doi.org/10.1007/s12652-019-01181-w

Raoof, A., Matrawy, A., & Lung, C.-H. (2019). Routing Attacks and Mitigation Methods for RPL-Based Internet of Things. *IEEE Communications Surveys & Tutorials*, *21*(2), 1582–1606. https://doi.org/10.1109/COMST.2018.2885894

Rong, B., Han, S., Kadoch, M., Chen, X., & Jara, A. (2020). Integration of 5G Networks and Internet of Things for Future Smart City. *Wireless Communications and Mobile Computing*, *2020*, 2903525. https://doi.org/10.1155/2020/2903525

Sanmartin, P., Jabba, D., Sierra, R., & Martinez, E. (2018). Objective Function BF-ETX for RPL Routing Protocol. *IEEE Latin America Transactions*, *16*(8), 2275–2281. https://doi.org/10.1109/TLA.2018.8528246

Seyedi, B., & Fotohi, R. (2020). NIASHPT: A novel intelligent agent-based strategy using hello packet table (HPT) function for trust Internet of Things. *The Journal of Supercomputing*, *76*(9), 6917–6940. https://doi.org/10.1007/s11227-019-03143-7

Stephen, R., & Arockiam, L. (2018). E2V: Techniques for Detecting and Mitigating Rank Inconsistency Attack (RInA) in RPL based Internet of Things. *Journal of Physics: Conference Series*, *1142*, 012009. https://doi.org/10.1088/1742-6596/1142/1/012009

Varga, P., Peto, J., Franko, A., Balla, D., Haja, D., Janky, F., Soos, G., Ficzere, D., Maliosz, M., & Toka, L. (2020). 5G support for Industrial IoT Applications—Challenges, Solutions, and Research gaps. *Sensors*, *20*(3), 828. https://doi.org/10.3390/s20030828

Wadhaj, I., Ghaleb, B., Thomson, C., Al-Dubai, A., & Buchanan, W. J. (2020). Mitigation Mechanisms Against the DAO Attack on the Routing Protocol for Low Power and Lossy Networks (RPL). *IEEE Access*, *8*, 43665–43675. https://doi.org/10.1109/ACCESS.2020.2977476

Zolertia Platforms—Zolertia. (n.d.). Retrieved September 29, 2022, from https://zolertia.io/zolertia-platforms/