INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

**ISSN: 2454-132X**
**Impact factor: 4.295**
***(Volume3, Issue1)***
Available online at: www.ijariit.com

# A Detailed Classification of Routing Attacks against RPL in Internet of Things

Divya Sharma
Sr. Assistant Professor,
Department of ECE,
New Horizon College of Engg,
Bangalore

Ishani Mishra
Sr. Assistant Professor,
Department of ECE,
New Horizon College of Engg,
Bangalore

Dr. Sanjay Jain
HOD- Department of ECE,
New Horizon College of Engg,
Bangalore

***Abstract-With the advancement in mobile computing and wireless communications, a new paradigm called Internet of Things, is generating a lot of research interest and industrial revolution. The increasing interest for this paradigm has resulted in the large-scale deployment of Low power and Lossy Networks (LLN), such as wireless sensor networks and home automation systems. These networks are typically composed of many embedded devices with limited power, memory, and processing resources interconnected by a variety of links, such as IEEE 802.15.4 or low-power Wi-Fi. These networks have a wide scope of applications such as industrial monitoring, connected home, health care, environmental monitoring, urban sensor networks, energy management, and assets tracking etc.RFC 7228. In order to address the specific properties and constraints of these networks RPL (Routing Protocol for low power Lossy network) has been developed by the IETF working group [ROLL WG]. RPL is a lightweight, rank based routing protocol. However, this routing protocol is exposed to various attacks which can significantly impact the network resources and its performance. This paper presents an elaborate classification of the possible attacks against RPL in IoT network. Further, we have analysed and compared the severity of these attacks.***

***Keywords: Internet of things, LLN, RPL, security attacks.***

## I. INTRODUCTION

According to International Telecommunication Union (ITU) and the *IoT* European Research Cluster (IERC) the Internet of Things (IoT) is defined as a vivacious worldwide network infrastructure with self configuring capabilities centered on standard and communication protocols in which physical and virtual "things" have identities, physical features and virtual characteristics, communicate via intelligent interfaces and integrate into the information network in a seamless fashion (Fig. 1). IoT can be viewed as a fusion of heterogeneous networks that brings not only the same security challenges present in sensor networks, mobile telecommunications and the internet but also some peculiar and accentuated issues, like, network privacy problems, authentication on a heterogeneous network, access control challenges and secure routing among these heterogeneous devices.

These networks have strong resource constraints (energy, memory, processing) and their communication links are by nature characterized by a high loss rate and a low throughput. Moreover, the traffic patterns are not simply defined according to a point-to point schema. In many cases, the devices also communicate according to point-to-multipoint and multipoint-to point patterns. Existing routing protocols are not suitable to deal with these requirements [3]. Therefore a complete stack of standardized protocols has been developed including the IEEE 802.15.4 standard protocol for the communication layers in wireless personal area networks (WPAN) and the 6LowPAN protocol which defines encapsulation and header compression mechanisms between IPv6 and 802.15.4. At the routing layer, the ROLL1 working group has proposed a protocol called RPL (Routing Protocol for Low power and Lossy Networks) based on IPv6 [4]. Due to their constrained nature RPL-based networks may be exposed to a large variety of security attacks. Even if cryptographic mechanisms are used in first defense, they only prevent external attacks. When nodes are compromised and become as a result internal attackers, cryptographic techniques become unavailing and can no longer protect the network. In [5], authors performed a study of security in 6LowPAN networks including the routing protocol

 

RPL but only mentioned three attacks regarding the routing protocol. The authors of [10] performed a survey of some existing attacks targeting the RPL protocol and the 6LoWPAN protocol with no classification; they also provided a discussion on different types of IDS. Further in [2], the authors have discussed and implemented various routing attacks against RPL and also proposed an IDS for the same. Also, other studies [11, 12] present some attacks targeting the RPL protocol, but their main contribution consists in an intrusion detection system (IDS) whose goal is to detect these attacks.

In this paper, our objectives are the identification and classification of the different attacks against the routing protocol in an IoT network while providing details on how those attacks can take place. In [14], the authors have presented the taxonomy of been routing attacks against RPL. However there are several routing attacks that are not included. In this paper we have extended the taxonomy proposed in [14] by considering few other routing attacks that are possible against RPL. The contribution of this paper is three fold. First, we introduce the Internet of Things and its relevance as well as growing trends in today's global IT scenario. Second, we explore the IoT routing protocols in general and discuss few of the key secure IoT routing protocols. Third, the paper gives an overview of the threats associated with IoT routing (RPL). Lastly, the paper briefly summarizes the attacks and its possible countermeasures.

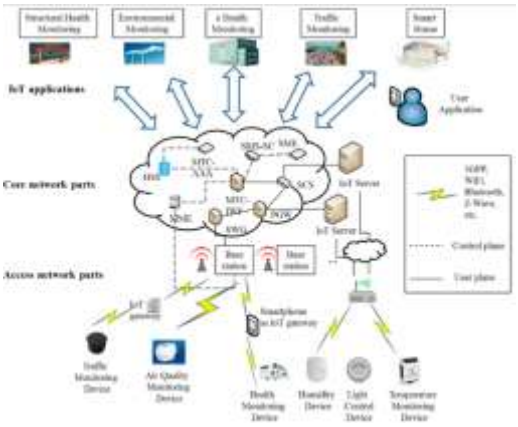


Fig.1. IoT Network and its Components

## II. ROUTING PROTOCOLS IN IOT

The Internet Engineering Task Force (IETF) created working groups (WGs) which developed various IoT protocols for IoT devices. We discuss below the routing protocols which have been developed by IETF for the Internet of Things (IoT).

### *2.1. Routing in IPv6 over low power wireless personal area networks (6LoWPAN)*

6LoWPAN is an IETF-standardized IPv6 adaptation layer (data link and cross-layer protocol) that enables IP connectivity over low power and lossy networks. This is observed as the basis for the network build up for the Internet of Things such as smart homes, smart cities and industrial control systems. A large number of applications utilize 6LoWPAN for IP-based communication through an upper layer protocol such as the RPL routing protocol. 6LoWPAN essentially adjusts IPv6 packets into frames of 127 bytes a frame size requirement that low power sensor devices can utilize among themselves. 6LoWPAN supports the transmission of large-sized IPv6 packets on the data link layer of the IEEE 802.15.4. It further provides fragmentation support at the adaptation layer involving processes such as buffering, forwarding and processing of fragmented packets which are expensive on these already resource constrained devices. Rogue nodes can send stale, overlapping or duplicate fragments to disrupt the network. At this layer there is no authentication, so the receiving nodes are debilitated in differentiating between legitimate and spurious packets during fragment reassembly. Usually the receiving nodes store up the fragments received in order to re-assemble them. If the entire set of frames making up the packet are not received after a certain timeout they are discarded. This system could also be exploited by malicious nodes which could send false fragments to fill up the nodes store so, it does not receive the legitimate fragments for re-assembly. This is indeed a challenging security issue in IoT networks. However, some protocols which have adopted 6LoWPAN (Winter et al., 2012; Hui and Thubert, 2011; Shelby et al., 2012) hinge on the security sub layer of the802.15.4 to prevent 802.15.4 frames introduced by malicious nodes. Indeed the 802.15.4 security sublayer actively achieves this aim by adding to every frame a Message Integrity Code (MIC) and a frame counter. Once a node has been compromised the attacker could easily inject spurious frames into the network and thus, add other non-authorized nodes into the victim's network. This error and security loophole could be propagated even to the upper layer of protocols since, the upper layer protocols rely on the 802.15.4 security sublayer for the security of frames (Winter et al., 2012; Shelby et al., 2012).

### *2.2. Routing protocol for low-power and lossy networks (RPL)*

RPL was developed by the IETF working group [ROLL WG] as routing functionalities in 6LoWPAN were very challenging due to the resource constrained nature of the nodes. RPL operates at the network layer making it capable to quickly build up routes and distribute route information among other nodes in an efficient manner. RPL is a Distance Vector IPv6routing protocol for LLNs, thus network path information is organized as a set of Directed Acyclic Graphs (DAGs) and this is further classified as a

 

set of Destination Oriented Directed Acyclic Graphs (DODAG). A DODAG typically consist of sensor nodes and a sink node which collects data from these nodes as shown in Fig.1.Every DODAG is distinguished by four factors which include: DODAG ID, DODAG version number, RPL instance ID and Rank while every DODAG sink is linked with each other (Winter et al.,2012). Route selection in RPL depends on the DODAG link, cost of information to a node such as workload, throughput, node power, latency or reliability. To produce a route topology, every node selects a set of parents that comprises nodes with equal or better paths towards the sink. The node with the best route link is chosen as the parent. RPL employs three types of control messages in order to form and manage routing of information in the network and these are: i. DODAG Information Object (DIO), used for setting and updating the network topology. ii. DODAG Advertisement Object (DAO) used for broadcasting and advertising destination information upwards during network route updates.iii. DODAG Information Solicitation (DIS) used when a new node seeks topology information while waiting to join the network.DAO and DIS are involved during a topology change process while the DIO message is broadcast and mainly used for the purpose of starting a topology change process. DIO is commonly used to distribute its routing state to other nodes using its rank (rank specifies the link quality to a sink node) and objective function (Winter et al., 2012; Anhtuan et al., 2013). Every node computes its rank according to the rank of its selected parent and the objective function. A DIO message is sent to all nodes every time a node updates its rank or preferred parent. To prevent the formation of loops, RPL utilizes the rank rule whereby a node in a parent should always have lower rank than its children. Also, to limit the amount of broadcast, RPL uses the trickle algorithm for scheduling DIO messages to be sent. It does this by setting a counter which observes the network topology and thereby decides when a node has to send a DIO message. For every DIO message received without comparing it with the previous DIO message this will cause the DIO counter to increase and if the DIO counter reaches a threshold value (redundancy value) the node will reset its DIO counter and double the trickle time. This is done to stabilize the network topology over a period of time and avoid the unnecessary frequent route updates which could consume the limited power and bandwidth available. This further helps to limit the number of DIOs produced so as to preserve scarce network resources. For incoming traffic, the node resets its DIO to zero and reduces its trigger time. This gives the opportunity for quick network route update through a rapid DIO generation (Winter et al., 2012).The RPL routing protocol has capacity to incorporate different types of traffic and signaling information swapped among nodes although this depends on the requirements of the considered data flows. RPL supports the Multipoint-to-Point (MP2P), Point-to-Multipoint (P2MP) and Point-to-Point (P2P) traffics (Fig 1b.).

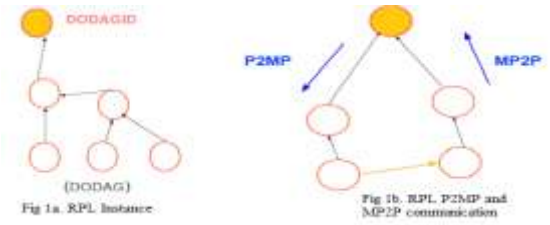


Fig 1a. RPL Instance

Fig 1b. RPL P2MP and MP2P communication

The RPL protocol integrates mechanisms to avoid loops, detect inconsistencies and repair DODAGs. Count-to infinity problem arises when a parent increases its rank value and selects its child as a new parent and the child do the same because it cannot re-attach to another node and so on. Then, the rank value of both parent and child does not stop to increase. To prevent this, the RPL protocol limits the maximum rank value allowed within the graph. DODAG loops appear when a node does not respect the rank property which means that the DODAG is no longer acyclic. To prevent this, a leaving node must poison its sub-DODAG by advertising an infinite rank. The leaving node has also the possibility to use a detaching mechanism, which consists in forming an intermediary DODAG and rejoining the main DODAG later. The RPL protocol can also detect inconsistencies using data path validation mechanism. When inconsistencies are detected, the RPL nodes should trigger repair mechanisms. These mechanisms contribute also to the topology maintenance when node and link failures happen. The local repair mechanism consists in finding an alternative path to route the packets when the preferred parent is not available. The node chooses another parent in its parent list. It is also possible to route packets via a sibling node e.g. node with the same rank. This alternative path may not be the most optimized one. According to [12], this local repair mechanism is effective and enables the network to converge again within a reasonable time. When the local repair mechanisms fail due to multiple inconsistencies, the DODAG root can initiate a global repair by incrementing the version number of the DODAG graph. The RPL network is then completely rebuilt.

## III. CLASSIFICATION OF ROUTING ATTACKS

Routing in an IoT network is subjected to a large variety of security attacks. The characteristics of LLN networks such as resource constraints, lack of infrastructure, limited physical security, dynamic topology and unreliable links make them susceptible and difficult to protect against attacks. These ones can be specific to the RPL protocol, but can also be applied to wireless sensor networks or even to wired networks. The RPL protocol defines several mechanisms that contribute to its security. As mentioned before, RPL integrates local and global repair mechanisms as well as loop avoidance and detection techniques. It also defines two security modes to encrypt data packets. However, typical deployments of such networks base their security on link layer and transport/application layer. In the following of the paper we assume that an attacker is able to bypass security at the link layer by either exploiting a vulnerability or gaining access to a shared key. The attacker can also be a malicious or faulty node whose behavior can disturb network functioning. In this paper, we present a classification of routing attacks against the RPL protocol.

 

This one takes into account the goals of the attack and what element of the RPL network is impacted. The taxonomy is depicted in Figure 2 and considers three categories of security attacks. In this paper we have broadly classified the routing attacks in IoT network in three categories. These are i). Attacks on Network Resources: These include attacks targeting the exhaustion of network resources (energy, memory and power). These attacks are particularly damaging for such constrained networks because they greatly shorten the lifetime of the devices and thus the lifetime of the RPL network. ii). Attacks on Network Topology: These cover attacks aiming at disrupting the RPL network topology. The attackers herein either aim at sub-optimization of the network topology or isolating a set of RPL nodes from the network. iii). Attacks on Network Traffic: This category corresponds to attacks against the network traffic, such as spoofing attacks or deception attacks.

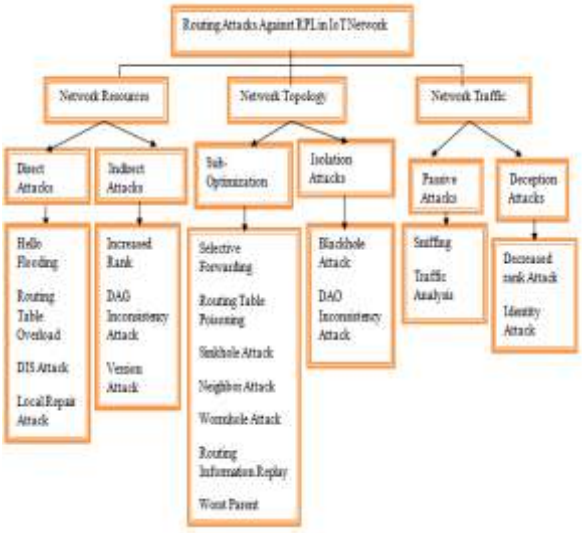


Fig 2. Classification of Routing Attacks against RPL in IOT

*3.1 Attacks on Network Resources:*

Attacks against resources aims at making legitimate nodes perform unnecessary processing in order to exhaust their resources. This eventually intends at consuming node energy, memory or processing. This may impact on the availability of the network by congesting available links and therefore on the lifetime of the network which can be significantly shortened. We further classify it into two subcategories of attacks against resources. The first one is direct attacks where a malicious node will directly generate the overload in order to degrade the network. The second one is indirect attacks where the attackers will make other nodes generate a large amount of traffic. Indirect attacks could be an attack that may create loops in the RPL network which in turn make other nodes produce traffic overhead.

*3.1.1 Direct Attacks*

In case of direct attacks, the attacker is directly responsible for resource exhaustion. This can typically be done by performing flooding attacks or by executing overloading attacks with respect to routing tables, when the storing mode is active.

*Hello Flooding Attacks:* For joining the network node broadcast initial message as HELLO message. Attacker can introduce himself as neighbor node to many node by broadcasting Hello message with strong routing metrics and enter in network. In RPL, DIO messages refereed as Hello message, which is used to advertise information about DODAG. This attack can be mitigated by using the link-layer metric as a parameter in the selection of the default route [2]. If it fails to receive link-layer acknowledgements then different route is chosen. Another solution can be by using the geographical distance, node should not select the nodes which are beyond their transmission range. This attack cannot exist for long time in RPL network, as RPL's Global and Local repair mechanism removes this attack. If this attack combines with the other attacks then RPL's Global and Local repair mechanism does not remove it.

*Routing Table Overload Attacks in Storing Mode:* It is also possible to perform direct attacks against resources by overloading the RPL routing tables. The RPL protocol is a proactive protocol. This means that the RPL router nodes build and maintain routing tables when the storing mode is enabled for those nodes. The principle of routing table overload is to announce fake routes using the DAO messages which saturate the routing table of the targeted node. This saturation prevents the build of new legitimate routes and impacts network functioning. It may also result in a memory overflow. Let us consider the example of the DODAG 2 graph described in Figure 3 and assume that node 12 plays the role of the attacker. Nodes 12 and 13 send a DAO message in order to add the corresponding entries in the routing table of node 11. The attacker, node 12 sends multiple forged DAO messages to node 11 with false destinations. As a consequence, node 11 builds all the corresponding entries in its routing table. Afterwards, when the other nodes including node 13 are sending legitimate DAO messages with respect to new routes, the node 11 is no longer able to record them because its routing table is overloaded. This attack is not specifically mentioned in the literature but it is part of overload attacks more generally [12].

 

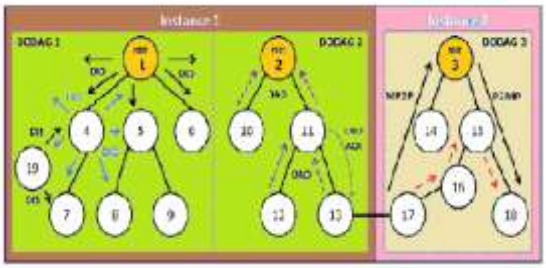

Fig 3. RPL Instance consisting of 2 Instances and 3 DAGs

*DIS Attack:* DIS (DODAG Information Solicitation) message used by new node to get the topology information before joining the RPL network. In this attack, malicious nodes periodically send the DIS messages to its neighbours. When the DIS messages broadcast by attacker, the receiver nodes upon receiving DIS message reset the DIO timer assuming something went wrong with the topology around it. When attacker unicast the DIS message the receiver node in return send the DIO message indicating that sender is willing to join the network. Both way of sending DIS message adds the consequences in network as no impact on delivery ratio [1] but DIS multicast attack showed most increase in end to end delay. This attack helps to generate more control overhead and eventually results in energy exhausting.

*Local Repair Attacks:* In local repair attack, attacker without any problem with link quality periodically sends the local repair message. This causes the local repair around the nodes which hears the local repair message. Local repair attack creates more impact on delivery ratio than any other kind of attack [1], generates more control packets and increases the end to end delay. Also exhaust the energy of nodes unnecessarily.

*3.1.2 Indirect Attacks*

Indirect attacks correspond to attacks where the malicious node makes other nodes generate an overload for the network. It includes: increased rank attacks, DAG inconsistency attacks and version number attacks.

*Increased Rank Attacks:* In RPL rank value increases from root to child node. By changing Rank value, an attacker can attract child node for selecting as parents or improve some other metric, and can attract large traffic going toward the root. The variation of rank attack [8] based on the attack existing duration (continuous or discontinuous) and update or no update of DIO information into four types and evaluated in RPL environment against network QOS parameters. The increased rank attack consists in voluntarily increasing the rank value of a RPL node in order to generate loops in the network. This attack has been studied in [9] through ns-2 simulations. The authors showed that their loop avoidance mechanisms costed more than the attack itself. Concretely, in a RPL network, a rank value is associated to each node and corresponds to its position in the graph structure according to the root node. As previously mentioned, the node rank is always increasing in the downward direction in order to preserve the acyclic structure of the DODAG. When a node determines its rank value, this one must be greater than the rank values of its parents. If a node wants to change its rank value, it has to first update its parents list by removing the nodes having a higher rank than its new rank value. Once a node has established the set of parents in a DODAG, it selects its preferred parent from this list in order to optimize the routing cost when transmitting a packet to the root node. A malicious node advertises a higher rank value than the one it is supposed to have. Loops are formed when its new preferred parent was in its prior sub-DODAG and only if the attacker does not use loop avoidance mechanisms. In that case, two attack scenarios are possible as illustrated in Figure 4. In the first scenario, the attacker is node 13 and the new preferred parent (node 24) has already a substitute parent (node 12) to re-attach to. The node 13 increases its rank value to 3 and chooses node 24 as the new preferred parent. This operation generates a routing loop in the DODAG graph, because the node 24 was in the prior sub-DODAG of node 13. The formed loop is composed of nodes 13 and 24 and is easily repaired because the node 24 can re-attach to node 12 after sending few control messages. However, this attack becomes more problematic when the node does not have a substitute parent such as node 31 in the second scenario. As depicted in Figure 1, the attacker increases its rank value which requires node 31 to also increase its own in order to find a new parent. Meanwhile nodes 32 and 33 have to connect to a substitute parent (node 22) so node 31 selects node 32 as new preferred parent. At the end, node 21 increases its rank value to 5 in order to add node 31 as its preferred parent. The count-to-infinity problem is avoided because of the limitation of the maximum rank value advertised for a DODAG. The increased rank attack is more damaging in this second scenario, because more routing loops are built at the neighbourhood. In that case, the loop repair mechanism requires sending many DIO messages (resets of the trickle timer) and requires a longer convergence time. The more the number of affected nodes increases, the longer the convergence time is. We consider this attack as part of the resource consumption attacks because the churn is exhausting node batteries and is congesting the RPL network. To mitigate this attack, the number of times a RPL node is increasing its rank value in the DODAG graph should be monitored to determine if a node can be considered as malicious or misconfigured. It is important to notice that a node can legitimately increase its rank value if it no longer matches the objective function and/or cannot manage the amount of received traffic. However, it must use the loop prevention techniques or it can wait for a new version of the DODAG graph.

 

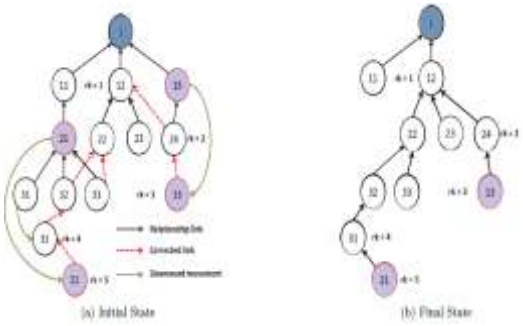

Fig 4. Rank increased attack in a RPL network

*DAG Inconsistency Attacks:* A RPL node detects a DAG inconsistency when it receives a packet with a Down 'O' bit set from a node with a higher rank and vice-versa [15] e.g. when the direction of the packet does not match the rank relationship. This can be the result of a loop in the graph. The Rank-Error 'R' bit tag is used to control this problem. When an inconsistency is detected by a node, two scenarios are possible: (i) if the Rank-Error tag is not set, the node sets it and the packet is forwarded. Only one inconsistency along the path is not considered as a critical situation for the RPL network, (ii) if the 'R' bit is already set, the node discards the packet and the timer is reset [18]. As a consequence, control messages are sent more frequently. A malicious node has just to modify the tags or add new tags to the header. The immediate outcome of this attack is to force the reset of the DIO trickle timer of the targeted node. In that case, this node starts to transmit DIO messages more frequently producing local instability in the RPL network. This also consumes the battery of the nodes and impacts the availability of links. All the neighbourhood of the attacker is concerned by the attack, since it has to process unnecessary traffic. Moreover, by modifying legitimate traffic, all the packets are discarded by the targeted node. This causes a blackhole and isolates segments of the network. To mitigate the flooding induced by this attack, [6] proposes to limit the rate of trickle timer resets due to an RPL Option to no greater than 20 resets per hour. In [16] , authors have proposed two solutions that takes into account network characteristics by using adaptive threshold and node's specific parameters respectively.

*Version Attack:* This attack takes place by publishing the higher version number of DODAG tree. When nodes receive the new higher version number DIO message they start the formation of new DODAG tree. This can cause the generation of new un-optimized topology and brings inconsistencies in topology. The loops and rank inconsistencies created by the attack are generally located around the neighbourhood of the attacker. VeRA schema prevents this attack by providing verification to version number using digital signature and MAC. The attack increases control overhead 18 times [13], impacts energy consumption and channel availability. It also reduce the delivery ratio of packets by up to 30% and nearly double the end-to-end delay in a network. An attacker located at large distance from the root causes the highest increase in overhead, and the higher packet loss.

*Denial of Service Attack:* Denial of service or Distributed denial of service attack is attempt to make resources unavailable to its intended user. In RPL this attack can be bring using the IPv6 UDP packet flooding. Many malicious nodes by coordinating can bring the Distributed denial of service attack, wherein it is difficult to identify the malicious nodes. However IDS system in [7] proposed the framework for detection of DOS attack in 6LoWPAN. The architecture integrates the IDS into the network framework developed within the EU FP7 project ebbits. At the security layer of ebbits Dos protection module is added. IDS probe nodes located in the network which sends periodically the traffic in 6LoWPAN through wired connection to IDS system. Dos protection manager receives the alerts from IDS system. It takes the network related information from other modules of network manager layer to confirm the attack. IDS send the jamming information of attack to Dos protection manager. The presence of jamming information at the modules of network manager of ebbits indicated the presence of attack.

*3.2. Attacks on Network Topology*

Attacks against the RPL protocol can also target network topology. We distinguish two main categories amongst these attacks: sub-optimization and isolation.

*3.2.1. Sub-optimization Attacks*

In case of sub-optimization attacks, the attackers aim at inducing poor performance of the network by not generating the optimal paths.

*Selective Forwarding Attack:* This attack takes place by selectively forwarding packets. With this attacks DoS (Denial of Service) attack can be launched. The purpose of attack is to disrupt routing paths and filter any protocol. In RPL attacker could forward all RPL control messages and drop the rest of the traffic. Solution on this attack can be creating the disjoint path or dynamic path between parent and children. Other solution is by using encryption technique in which attacker will not be able to identify the traffic flow. Heartbeat protocol [2] basically used for detection of the disruption in network topology but also can be used as defend against selective forwarding attack. IDS solution [11] given the End to End packet loss adaptation algorithm for detection of selective forwarding attack. Such attacks need to be detected and removed, RPL self-healing [2] does not correct the topology.

*Routing Table Poisoning Attacks in Storing Mode:* In a routing protocol, it is possible to forge or modify routing information to advertise falsified routes to other nodes. This attack can be performed in the RPL network by modifying or forging DAO control

 

messages in order to build fake downward routes. This can only be done when the storing mode is enabled. For instance, a malicious node advertises routes toward nodes that are not in its sub-DODAG. Targeted nodes have then wrong routes in their routing table causing network sub- optimization. As a result, the path can be longer inducing delay, packet drops or network congestion.

*Sinkhole Attack:* In sinkhole attacks attacker node advertises beneficial path to attract many nearby nodes to route traffic through it. This attack does not disrupt the network operation but it can become very powerful when combined with another attacks. The IDS system [11] gives the solution to detect this attack. To defend against sinkhole attack [17] evaluated parent fail-over and a rank authentication technique. The rank authentication technique relies on one way hash technique. The root begins to generate hash value by picking random value, and broadcast it in DIO message. All nodes calculate the hash value using previous received one and again broadcast it using DIO message. Assumed that malicious node doesn't calculate the hash value, it simply broadcast received DIO message. Each node stores the hash value received by its parent along with number of hops in the path. When root node broadcast random number securely, then node can verify its parent rank using that intermediates hops number. Parent fail-over technique uses UNS (unheard nodes set) field in DIO message indicating that the nodes are in sinkhole compromised path. If the node receives the DIO message containing its ID in UNS then it adds its parent in black list. RPL does not have the self-healing capacity against the sinkhole.

*Neighbor Attack:* In this attack the malicious node broadcast DIO messages that it received without adding information of himself. The node who receives this type of messages may think that new neighbor node send this DIO message. The victim nodes try to select the node which is not in range as parent node and change the route to the out range neighbors. This attack is similar to the wormhole attack with special case of selective forwarding of DIO message only. This attack affects network QOS parameters as no change in packet delivery ratio, slightly increases the end to end delay, slight change in network topology, negligible control overhead. When combined with other attack can be dangerous.

*Wormhole Attack:* RPL can undergo the wormhole attack [2]. The main purpose of this attack is Disrupt the network topology and traffic flow. This attack can takes place by creating tunnel between the two attackers and transmitting the selective of all traffic through it. Wormhole attack can be prevented using the construction of Markle tree authentication [18]. In RPL the tree construction starts from root to leaf nodes and Markle tree construction starts from leaf node to root. It uses ID of node and public key for calculation of hash. Each parent is identified by its children. Authentication of any node begins with the root node up to the node itself. If any node failed to authenticate, then children nodes avoids the wrong parent selection.

*Routing Information Replay Attacks:* A RPL node can also perform routing information replay attacks. It records valid control messages from other nodes and forwards them later in the network. In case of dynamic networks, this attack is quite damaging because the topology and the routing paths are often changed. Replay attacks cause nodes to update their routing tables with outdated data resulting in a false topology. The RPL protocol uses some sequence counters to ensure the freshness of the routing information such as the Version Number for DIO messages or the Path Sequence present in the Transit Information option of DAO messages [15]. This attack is mentioned in [12] however the authors neither study the consequences of such attack nor explained how it can takes place in RPL networks.

*Worst Parent Attacks:* This attack described in [19] and termed as "Rank attack" consists in choosing systematically the worst preferred parent according to the objective function. The outcome is that the resulting path is not optimized inducing poor performance. This attack cannot be easily tackled because children node rely on their parent to route packets and this attack cannot be monitored by neighbors. However, using a security solution which rebuilds a global view of the graph based on nodes information should detect this attack such as the proposed solution in [11].

*3.2.2. Isolation Attacks*

The attacks against the topology also serve as a support for isolating a node or a subset of nodes in the RPL network which means that those nodes are no longer able to communicate with their parents or with the root.

*Blackhole Attacks:* In a blackhole attack, a malicious intruder drops all the packets that it is supposed to forward. This attack can be very damaging when combined with a sinkhole attack causing the loss of a large part of the traffic. It can be seen as a type of denial-of-service attack. If the attacker is located at a strategic position in the graph it can isolate several nodes from the network. There is also a variant of this attack called gray hole (or also selective forwarding attack) where the attacker only discards a specific subpart of the network traffic. Chugh et al.[20] investigated the consequences of blackhole attacks in RPL networks through a set of Cooja simulations. They highlighted different indicators to detect these attacks such as rate and frequency of DIO messages, packet delivery ratio, loss percentage and delay. The IDS SVELTE proposed in [11] was designed to detect selective forwarding attacks in such networks.

*DAO Inconsistency Attacks in Storing Mode:* DAO inconsistencies occur when a node has a downward route that was previously learnt from a DAO message, but this route is no longer valid in the routing table of the child node [4]. RPL provides a mechanism to repair this inconsistency, called DAO inconsistency loop recovery. This optional mechanism allows the RPL router nodes to remove the outdated downward routes using the Forwarding-Error 'F' flag in data packets which indicates that a packet cannot be

 

delivered by a child node. The packet with the 'F' flag is sent back to the parent in order to use another neighbour node, as depicted in Figure 5. Once a packet is transmitted downward, it should normally never go up again. When it happens the router sends the packet to the parent that passed it with the Forwarding-Error 'F' bit set and the Down 'O' bit left. When the parent receives the packet with 'F' set it removes the corresponding routing state, clear the 'F' bit, and try to send the packet to another neighbor. If the alternate neighbor still has an inconsistent state the process reiterates. In this scenario, the malicious node is represented by node 21. It uses the 'F' flag to make RPL routers remove legitimate downward routes and thus isolate nodes from the DODAG graph. Each time node 21 receives a packet from node 11, it only changes the RPL 'F' flag and sends it back to node 11. As a consequence, the other nodes of the network (nodes 31 to 33) are isolated from the graph. The objective of this attack is to make router nodes discard available downward routes. This makes the topology of the DODAG graph sub-optimal. One possible consequence of this attack is to isolate the sub-DODAG bound to the attacker which can no longer receive packets, as in our example. This also leads to additional congestion (if the packets are forwarded through sub-optimal paths), partitions and instabilities in the network. The consequences for the children nodes include starvation and delay. To reduce the effects of this attack on the network, RFC 6553 proposes to limit the rate of the downward routing entries discarded due to an 'F' flag to 20 per hour [6].

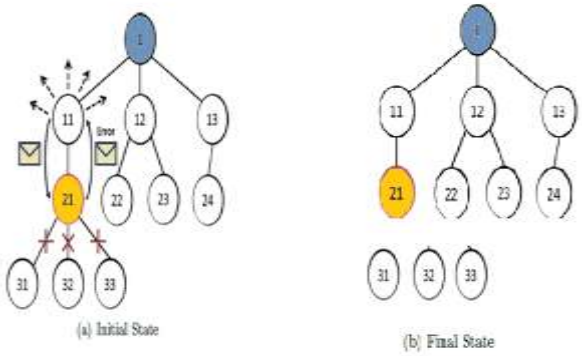


Figure 5: DAO Inconsistency Attack

*3.3 Attacks on Network Traffic*

This third category concerns the attacks targeting the RPL network traffic. It mainly includes eavesdropping attacks on the one hand, and misappropriation attacks on the other hand.

*3.3.1 Passive Attacks*

The pervasive nature of RPL networks may facilitate the deployment of malicious nodes performing passive attacks wherein the attacker focus on eavesdropping activities such as sniffing and analysing the traffic of the network.

*Sniffing Attacks:* A sniffing attack consists in listening the packets transmitted over the network. This attack is very common in wired and wireless networks and compromises the confidentiality of communications. An attacker can perform this attack using a compromised device or directly capture the packets from the shared medium in case of wireless networks. The information obtained from the sniffed packets may include partial topology, routing information and data content. In RPL networks, if an attacker sniffs control messages, it can access information regarding the DODAG configuration such as DODAG ID, Version Number, ranks of the nodes located in the neighborhood. By sniffng data packets, the attacks can not only discover packet content but also have a local view of the topology in the eavesdropped area by looking at source/destination addresses. This attack is difficult to be detected due to its passive nature. The only way to prevent sniffing is encryption of messages when the attacker is external. Even if RFC 6550 mentions encryption of control messages as an option, the technical details are left out from the specification making implementation difficult.

*Traffic Analysis Attacks:* Traffic analysis aims at getting routing information by using the characteristics and patterns of the traffic on a link. This attack can be performed even if the packets are encrypted. The objective is, like sniffing attacks, to gather information about the RPL network such as a partial view of the topology by identifying parent/children relationships. Thanks to this attack, a malicious node can possibly perform other attacks with the gathered information. The consequences depend on the rank of the attacker. If this one is close to the root node, it can process a large amount of traffic and therefore can get more information than when the node is located on the edge of a sub-DODAG.

*3.3.2. Deception Attacks*

In deception attacks, the identity of a legitimate node is usurped or performances are over claimed. These attacks are not so damaging for the RPL network. However, they are often used as a first step for other attacks such as those seen in the previous two main categories. They allow the attacker to gain a better understanding of the network and its topology, to gain better access or to intercept a large part of the traffic.

 

*Decreased Rank Attacks:* In a DODAG graph, the lower the rank is, the closer the node is to the root and the more traffic this node has to manage. When a malicious node illegitimately advertises a lower rank value, it overclaims its performance. As a result, many legitimate nodes connect to the DODAG graph via the attacker. This results in the attraction of a large part of the traffic, as shown in Figure 6. Thanks to this operation, the malicious node is capable of performing other attacks such as sinkhole and eavesdropping attacks. In the RPL protocol, an attacker can change its rank value through the falsification of DIO messages. The VeRa [21] solution as well as the Rank verification method [17] is able to address this issue. However authors in [22] have shown that VeRa is not sure regarding rank authentication and they proposed improvements to address this issue called TRAIL. They also showed another way to perform this attack by replaying the rank of the attacker's parent which allows it to decrease its rank by one. Since SVELTE [11] can detect sinkhole attacks it can also detect the decreased rank attack.

*Identity Attacks:* Identity attacks gather both spoofing and sybil attacks. In a clone ID attack, an attacker copies the identities of a valid node onto another physical node. This can, for example, be used in order to gain access to a larger part of the network or in order to overcome voting schemes. In a sybil attack, which is similar to a clone ID attack, an attacker uses several logical entities on the same physical node. Sybil attacks can be used to take control over large parts of a network without deploying physical nodes. By keeping track of the number of instances of each identity it is possible to detect cloned identities. It would also be possible to detect cloned identities by knowing the geographical location of the nodes, as no identity should be able to be at several places at the same time. The location of nodes or similar information could be stored either centralized in the 6BR or distributed throughout the network in a distributed hash table (DHT). In an IP/RPL network cloned identities will cause trouble when packets are heading to one of the cloned identities. Packets will be forwarded to *one* of the cloned identities based on the routing metrics in the network, and the rest of the cloned identities will be unreachable from certain nodes in the network. This however does not affect the network otherwise, and therefore cloned identities on their own, do not cause harm on a 6LoWPAN network.

## IV. ANALYSIS

In this section, we have summarized the properties of the identified attacks as well as methods and techniques to address them. Table 1 summarizes attacks against RPL in IoT. First property considered is the internal (I) or external (E) nature of the attacks. Internal attacks are initiated by a malicious or compromised node of the RPL network. External attacks are performed by nodes that do not belong to the RPL network or are not allowed to access it. Second property is the precondition or criterion to launch these attacks. The next property corresponds to the impact of the attacks. The impact in this category is assessed as the type of over-consumed resources (e.g. memory, battery, link availability). The last column of table indicates the possible security mechanisms to address the attacks. Considering the attacks targeting the network resources, we can observe that only the DIS attack can be performed externally because the attacker does not need to join the graph to perform the DIS flooding since DIS message are used to discover the DODAG. For the rest of the attacks, the malicious node needs to be part of the DODAG to have enough knowledge in order to launch its attacks. The storing mode which means maintaining routing table has to be enabled to launch routing table overload and the RPL option header has to be implemented to run DAG inconsistency attacks. We observe that all the attacks consume node battery as they imply additional processing for the nodes. Most of the time, the link availability is also impacted since the attack requires sending a large number of control messages. The memory is also over-consumed in case of routing table overload attacks. We studied that RPL provides internal mechanisms which contribute to counter attacks. For instance, the loop avoidance mechanisms prevent increased rank attacks. The protocol also proposes an optional mitigation mechanism that limits inconsistency attacks impact [6]. Specific approaches have been designed for the RPL protocol. The VeRa [23] and the TRAIL [22] approaches address version number modifications. In many cases, it is difficult to evaluate the overhead induced by the security mechanisms because they are still at a conceptual level. In network topology attacks we observe that the attacker has to be both internal and active for these attacks. Indeed, the malicious node has to join the graph to manipulate the topology. The attacks related to routing tables such as routing table poisoning and DAO inconsistency attacks need the storing mode to be enabled to be performed. Also the RPL option header has to be implemented for the second attack since the malicious node misuses the data path validation which relies on this header. At least two malicious intruders are required to perform the wormhole attack.

Eavesdropping attacks can be performed externally. They are usually exploited to gain access to the internal network. As for the other categories, the attacker has to be an insider to perform misappropriation attacks. Only the eavesdropping attacks have been classified as passive attacks. All the other identified attacks induce that the attacker generates or modifies packets. Passive attacks are quite difficult to detect, in particular in RPL networks which are often supported by wireless links. There is no particular prerequisite for attacks on traffic.

 

| **Routing Attacks in IoT Network** | **I/E** | **Pre-Condition** | **Impact on Network Parameter** | **Counter- measure** |
|---|---|---|---|---|
| Hello Flooding Attacks | I | - | Route formation through attacker node | RPL's Global and Local repair mechanism removes attack |
| Routing Table Overload | I | Storing Mode | Memory/ Battery making resources unavailable | None |
| Local Repair Attack | I | | Control overhead, Disrupt routing and traffic flow | IDS based solution [5] |
| Neighbor and DIS | I/E | | Packet delay | No technique evaluated yet |
| Rank Attack | I | - | Packet delay, delivery ratio and generation of Un-optimised path and loop | IDS based solutions [2],[16], VeRA [23], TRAIL[22] |
| DAG Inconsistency | I | Option Header | Battery/ Power consumption, unavailability of resources | Limitation of Timer Resets |
| Version Number Attack | I | - | control overhead, delivery ratio, end to end delay | VeRA [23] |
| Denial Of Service | I | | Make resources unavailable to Intended user | IDS based solution [11] |
| Selective forwarding | I | | Disrupt routing path | Heartbeat protocol [2], End to end packet loss |
| Routing Table Poisoning | I | Storing Mode | Target's Subnet | |
| Sinkhole | I | | Large traffic flows through attacker node | IDS solution [11], parent fail-over, rank authentication technique[17] |
| Wormhole | I | Min. 2 Intruders | Disrupt the network topology and traffic flow | Markle tree authentication [18] |
| Routing Information Replay | I | | Attacker's Neighborhood | Using Sequence Number |
| Worst Parent | I | | Attacker's Subnet | None |
| Blackhole | I | | Packet delay and control overhead | No technique evaluated yet |
| DAO Inconsistency | I | Storing Mode, Option Header | Attacker's subnet, corrupt routing tables affecting downward packets | Limitation of discarding routing state |
| Sniffing and Traffic Analysis | I/E | | Critical Data disclosure | Lightweight Encryption |
| Sybil and Clone ID | I | | Routing traffic unreachable to victim node | No technique evaluated yet |

Table1. Summary of Attacks Against RPL in IOT

 

## CONCLUSION

6LoWPAN is novel technology designed for resource constrained devices to connect to internet using IPv6. These could go under attack due to vulnerabilities of 6LoWPAN, IPv6 and RPL protocol. 6LoWPAN can undergo attack from internal WSN and external internet environment. Resource constrained devices has limited computational capacity so the traditional security solution could be optimized to light weight design. RPL does not provide the security as the AODV, DSDV protocol. Attacker can take benefit of this to generate attacks. Network layer attack form IPv4 network can be takes place on IPv6 networks. Some of these attacks has been evaluated in RPL and 6LoWPAN environment, however there are several other attacks yet to be explored. We have extended the taxonomy proposed in [14] by including few more attacks against the RPL protocol in three main categories. The attacks against resources reduce network lifetime through the generation of fake control messages or the building of loops. The attacks against the topology make the network converge to a suboptimal configuration or isolate nodes. Finally, attacks against network traffic let a malicious node capture and analyse large part of the traffic. Based on this classification, we have compared the properties of these attacks and discuss methods and techniques to avoid or prevent them. Few more attacks such as Internet smurf attack and homing attack have not been covered in this classification and needs to be evaluated in future.

## REFERENCES

[1]. Le, Anhtuan, et al. "The impacts of internal threats towards Routing Protocol for Low power and lossy network performance." *Computers and Communications (ISCC), 2013 IEEE Symposium on*. IEEE, 2013.

[2]. LinusWallgren, Shahid Raza and Thiemo Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things", International Journal of Distributed Sensor Networks, Volume 2013, Article ID 794326, 11 pages, http://dx.doi.org/10.1155/2013/794326.

[3]. P. Levis, A. Tavakoli, and S. Dawson- Haggerty, Overview of Existing Routing Protocols for Low Power and Lossy Networks, Internet Engineering Task Force (IETF) Internet Draft: draft-ietf-roll-protocols-survey-07, April 2009. (http://tools.ietf.org/html/draft-levis-roll-overview-protocols-00).

[4]. T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, RPL: IPv6 routing protocol for low-power and lossy networks, RFC 6550,IETF,2012.

[5]. A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, "6lowpan: A study on QoS security threats and countermeasures using intrusion detection system approach," International Journal of Communication Systems, vol. 25, no. 9, pp. 1189-1212, 2012.

[6]. J. Hui and J. Vasseur, The Routing Protocol for Low- Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams, RFC 6553 (Proposed Standard), Internet Engineering Task Force, Mar. 2012.

[7]. Kasinathan, Prabhakaran, et al. "Denial-of-Service detection in 6LoWPAN based internet of things." *Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on*. IEEE, 2013.

[8]. Le, Anhtuan, et al. "The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks."(2013).

[9] W. Xie, M. Goyal, H. Hosseini, J. Martocci, Y. Bashir, E. Baccelli, and A. Durresi, "Routing loops in dag-based low power and lossy networks," in Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications, pp. 888-895, Washington, USA, 2010.

[10]. Pavan Pongle, Gurunath Chavan "A Survey : Attacks on RPL and 6LoWPAN in IoT", International Conference on PervasiveComputing(ICPC).

[11]. S. Raza, L. Wallgren, and T. Voigt, "Svelte: Real time intrusion detection in the internet of things," Ad Hoc Networks, vol.11,no.8,pp.2661-2674,2013.

[12]. A. Rghiout, A. Khannous, and M. Bouhorma, "Denial-of-service attacks on 6lowpan-RPL networks: Issues and practical solutions," Journal of Advanced Computer Science & Technology, vol. 3,no. 2, pp. 143-153, 2014.

[13].Mayzaud, Anthéa, et al. "A Study of RPL DODAG Version Attacks.", 2013.

[14]. Anthea Mayzaud, Remi Badonnel, and Isabelle Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things", International Journal of Network Security, Vol.18, No.3, PP.459-473,May2016.

[15]. T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "RPL: IPv6 routing protocol for low-power and lossy networks", RFC 6550,IETF,2012.

[16]. A. Sehgal, A. Mayzaud, R. Badonnel, I. Chrisment, and J. Sch□onw□alder, "Addressing DODDAG inconsistency attacks in RPL networks," in Proceedings of Global Information Infrastructure and Networking Symposium (GIIS'14), pp. 1-8, 2014.

[17]. Weekly, Kevin, and Kristofer Pister. "Evaluating sinkhole defense techniques in RPL networks." *Network Protocols (ICNP), 2012 20th IEEE International Conference on*. IEEE, 2012.

[18]. Khan, Faraz Idris, et al. "Wormhole attack prevention mechanism for RPL based LLN network." *Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference* IEEE,2013.

[19]. 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, vol. 13,no.10,pp.3685-3692,2013.

[20]. K. Chugh, L. Aboubaker, and J. Loo, "Case study of a black hole attack on 6lowpan-RPL," in Proceedings of the SECUREWARE Conference, pp. 157-162, Aug,2012.

[21]. A. Dvir, T. Holczer, and L. Butty_an, "Vera – version number and rank authentication in RPL," in Proceedings of Mobile Adhoc and Sensor Systems Conference (MASS'11), pp. 709-714,2011.

 

[22]. M. Landsmann, H. Perrey, O. Ugus, M. Wahlisch, and T. C. Schmidt, "Topology authentication in RPL," in IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS'13), pp.73-74, 2013.
[23]. Dvir, Amit, Támas Holczer, and Levente Buttyan. "VeRA-version number and rank authentication in rpl." *Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on*. IEEE, 2011.

 