Research on Anti Attack of Routing Protocol in Internet of Things

Zehao Zheng, Chuansheng Wu

University of Science and Technology Liaoning, Anshan, P. R. China

Abstract

The growing interest for the Internet of Things is contributing to the large-scale deployment of Low power and Lossy Networks (LLN). These networks support communications amongst objects from the real world, such as home automation devices and embedded sensors, and their interconnection to the Internet. An open standard routing protocol, called RPL, has been specified by the IETF in order to address the specific properties and constraints of these networks. However, this protocol is exposed to a large variety of attacks. Their consequences can be quite significant in terms of network performance and resources. In this paper, we propose to establish a taxonomy of the attacks against this protocol, considering three main categories including attacks targeting network resources, attacks modifying the network topology and attacks related to network traffic. We describe these attacks, analyze and compare their properties, discuss existing counter-measures and their usage from a risk management perspective.

Keywords

Internet of things, LLN, RPL, Security.

1. Introduction

The Internet of Things defines a new paradigm that is increasingly growing in the context of pervasive networks and services. It consists in the extension of the Inter net to objects from the real world which are interact ing with each other in order to reach common goals. The high 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 au tomation systems. These networks have strong resource constraints (energy, memory, processing) and their com munication 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 communi cate according to point-to-multipoint and multipoint-to point patterns. Existing routing protocols are not suitable to deal with these requirements . Therefore a com plete 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 en capsulation and header compression mechanisms between IPv6 and 802.15.4. At the routing layer, the ROLL 1 work ing group has proposed a protocol called RPL (Routing Protocol for Low power and Lossy Networks) based on IPv6 . 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 at tackers, cryptographic techniques become unavailing and can no longer protect the network.

Many studies have been conducted on security issues regarding mobile ad-hoc networks [1, 5] and wireless sen sor networks . Current published surveys regarding the RPL protocol have been focused on performance eval uation [8] and a few on some specific security aspects. The security threat analysis provided by the ROLL working group is probably the most complete study on possible RPL security issues. The attacks are classified according to a regular CIAA model (confidentiality, in tegrity,

authentication and availability). Guidelines and recommendations are provided to counteract these at tacks. However, this analysis is a general framework on generic threats. It does not detail how the attacks are instantiated using the RPL protocol. In [14], authors performed a study of security in 6LowPAN networks in cluding the routing protocol RPL but only mentioned three attacks regarding the routing protocol. The au thors of 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 such as and [14]. Also, other studies [16, 28, 24, 25] present some attacks targeting the

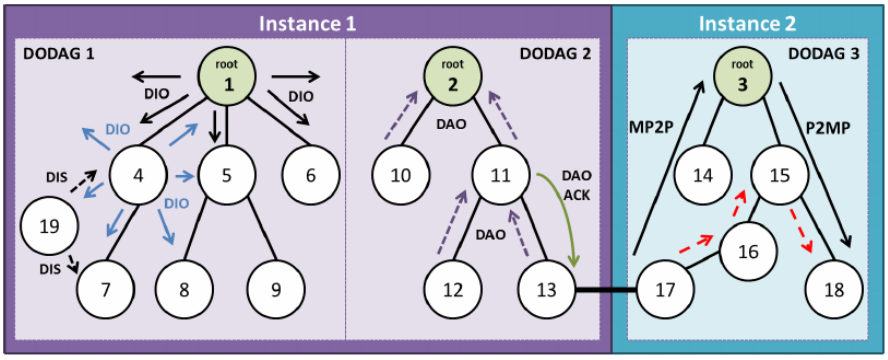


Figure 1. Example of a RPL network composed of two instances and three DODAGs

RPL protocol, but their main contribution consists in an intrusion detection system (IDS) whose goal is to detect these attacks. In , the authors presented an evaluation in the emulation environment Cooja using the contiki OS 2 of four attacks targeting the RPL protocol mostly men tioned in [14].

In this paper, our objectives are the identification and classification of the different attacks against the RPL net work protocol while providing details on how those at tacks can take place. This novel approach classifies the attacks according to the attacker's goal and means con sidering the specific properties of RPL networks. This classification allows us to prioritize attacks depending on the damages they cause to the network and can be used in a risk management perspective. We also describe in this taxonomy existing security solutions we have found in the literature.

The rest of the paper is consequently organized as fol lows. Section 2 overviews the RPL protocol and identifies its security issues. We then introduce our taxonomy of attacks related to the RPL protocol. In the following sections, we analyse each category of the proposed tax onomy. Section 3 focuses on security attacks targeting the network resources of RPL devices. Section 4 details security attacks targeting the topology and Section 5 ad dresses security attacks on network traffic. In Section 6, we show the utilization of the classification as a support for risk management and highlight benefits from a risk management perspective through an illustrative example. Finally, Section 7 concludes the paper and points out fu ture research perspectives.

2. RPL Concepts and Security Concerns

The RPL protocol is a distance-vector routing protocol based on IPv6. The RPL devices are interconnected according to a specific topology which combines mesh and tree topologies called Destination Oriented Directed Acyclic Graphs (DODAG). A DODAG graph is built from a root node which is the data sink of the graph. A network can operate one or more RPL instances which consist of multiple DODAG graphs as shown in Figure 1. Each RPL instance is associated to an objective function which is responsible for calculating the best path depending on a set of metrics or constraints. For instance, this function can minimize energy consumption or simply compute the shortest path. A RPL node can join several instances at the same time, but it can only join one DODAG graph per instance such as nodes 13 and 17 in Figure 1. These mul tiple instances enable the RPL protocol to perform dif ferent optimizations, such as quality-of-service ones. The RPL packets can be forwarded according to three traffic patterns as shown in the third DODAG of Figure 1: (i) multipoint-to-point traffic (MP2P) from leaves to the root via upward routes; (ii) point-to-multipoint traffic (P2MP) from the root to leaves

using downward routes; and (iii) point-to-point traffic (P2P) illustrated by red doted ar rows using both up and downward routes.

2.1 DODAG Building and Maintenance

The DODAG graph is built in a step by step manner. The root initially broadcasts a DIO message (DODAG Information Object) as depicted in Figure 1. This mes sage contains the information required by RPL nodes to discover a RPL instance, get its configuration parame ters, select a parent set, and maintain the DODAG graph. Upon receiving a DIO message, a node adds the sender of the message to its parents list and determines its own rank value by taking into account the objective function referred in the DIO message. The rank value of a node corresponds to its position in the graph with respect to the root and must always be greater than its parents' rank in order to guarantee the acyclic nature of the graph. It then forwards updated DIO messages to its neighbors. Based on its parents list, the node selects a preferred par ent which becomes the default gateway to be used when data has to be sent toward the DODAG root. At the end of this process, all the nodes participating in the DODAG graph have an upward default route to the DODAG root. This route is composed of all the preferred parents. The DIO messages are periodically sent according to a timer set with the trickle algorithm which optimizes the transmission frequency of control messages depending on the network state. A new node may join an existing net work by broadcasting a DIS message (DODAG Informa tion Solicitation) in order to solicit DIO messages from its neighbors. The DAO messages (Destination Adver tisement Object) are used to build downward routes. De pending on the mode of operation specified by the root in the DIO messages, routing tables can be maintained by router nodes. In the storing mode, the child unicasts a DAO message to the selected parent which records it. The parent aggregates the routes received from other DAO messages and sends the information to its parent recur sively through a DAO message. In the non-storing mode, DAO messages are unicasted to the DODAG root. In termediate nodes do not store routing information but simply insert their own address to the message in order to complete the reverse path. The DAO messages can be acknowledged with DAO-ACK messages (Destination Advertisement Object Acknowledgement).

2.2 Loops, Inconsistencies and Repairs

The RPL protocol integrates mechanisms to avoid loops, detect inconsistencies and repair DODAGs. Count-to infinity phenomena occur 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 mecha nism, which consists in forming an intermediary DODAG and rejoining the main DODAG later. The RPL proto col can also detect inconsistencies using datapath valida tion mechanism. Routing information is included in data packets within a RPL Option carried in the IPv6 Hop by-Hop header. Several flags are defined: (i) the Down 'O' flag indicates the expected direction up or down of a packet. If a router sets this flag, the packet should be for warded to a child node using downward routes, otherwise it should be sent to a parent with a lower rank toward the DODAG root; (ii) the Rank-Error 'R' flag indicates that a rank error is detected. It occurs when a mismatch is observed between the rank values and the direction of a packet indicated by the Down flag, (iii) the Forwarding Error 'F' flag indicates the inability of a node to forward the packet toward the destination in case of downward packets .

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 pack ets when the preferred parent is not available. The node chooses another parent in its parent list. It is also pos sible 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 con verge again within a reasonable time. When the local re pair mechanisms fail due to multiple inconsistencies, the DODAG root can initiate a global repair by increment ing the version number of the DODAG graph. The RPL network is then completely rebuilt.

2.3 Security Concerns

The RPL protocol is exposed to a large variety of secu rity attacks. The characteristics of LLN networks such as resource constraints, lack of infrastructure, limited physical security, dynamic topology and unreliable links make them particularly vulnerable and difficult to pro tect 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 proto col defines several mechanisms that contribute to its se curity. As previously mentioned, it 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 trans port/application layer [3]. 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 gain ing access to a shared key. The attacker can also be a misconfigured or faulty node whose behavior can disturb network functioning.

In this paper, we propose to establish a taxonomy 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 de picted in Figure 2 and considers three categories of se curity attacks. The first category covers attacks target ing 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. The second category includes attacks tar geting the RPL network topology. They disturb the nor mal operation of the network: the topology may be sub optimized in comparison with a normal convergence of the network or a set of RPL nodes may be isolated from the network. The third category corresponds to attacks against the network traffic, such as eavesdropping attacks or misappropriation attacks.

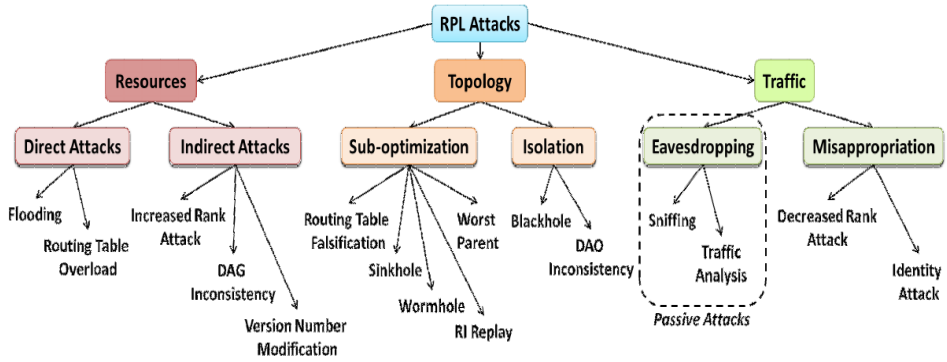


Figure 2. Taxonomy of attacks against RPL networks

3. Attacks Against Resources

Attacks against resources typically consists in making le gitimate nodes perform unnecessary processing in order to exhaust their resources. This category of attacks aims at consuming node energy, memory or processing. This may impact on the availability of the network by con gesting available links and therefore on the lifetime of the network which can be significantly shortened. We distinguish two subcategories of attacks against re sources. The first one gathers direct attacks where a ma licious node will directly generates the overload in order to degrade the network. The second one contains indirect attacks where the attackers will make other nodes gener ate a large amount of traffic. For instance, such an attack can be performed by building loops in the RPL network so that make other nodes produce traffic overhead.

3.1 Direct Attacks

In case of direct attacks, the attacker is directly responsi ble 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.

3.1.1 Flooding Attacks

Flooding attacks consist in generating a large amount of traffic in a network and make nodes and links unavailable. These attacks can be performed by an external or internal attacker. They exhaust the resources of all the network nodes in the worst case. More specifically, using solicita tion messages to perform the flooding is called an HELLO flood attack. In RPL networks, an attacker can either broadcast DIS messages to its neighboring nodes which have to reset their trickle timer, or, unicast DIS message to a node which has to reply with a DIO message. In both cases, this attack leads to network congestion and also to the saturation of the RPL nodes. The consequences of such attacks has been studied in , the authors show that the control message overhead significantly increased but the delivery ratio is not affected. However no solution especially designed for RPL has been proposed.

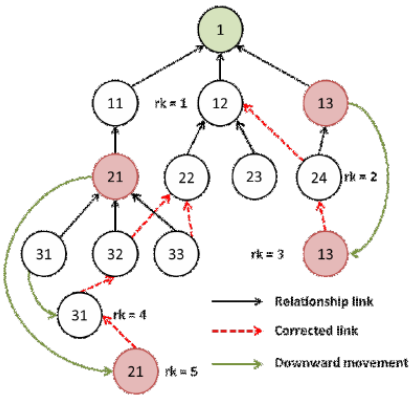
3.1.2 Routing Table Overload Attacks in Storing Mode

It is also possible to perform direct attacks against re sources 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 1 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 ta ble. 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 be cause its routing table is overloaded. This attack is not specifically mentioned in the literature but it is part of overload attacks more generally .

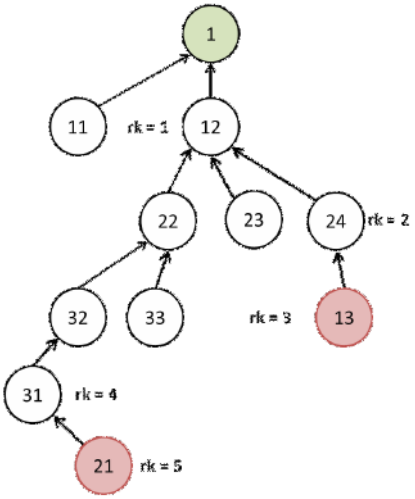
3.2 Indirect Attacks

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

The increased rank attack consists in voluntarily increasing the rank value of a RPL node in order to generate



(a) Initial State



(b) Final State

Figure 3. Rank increased attack in a RPL network

Loops in the network. This attack has been studied in 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 as sociated to each node and corresponds to its position in the graph structure according to the root node. As previ ously mentioned, the node rank is always increasing in the downward direction in order to preserve the acyclic struc ture 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 first to update its parents list by removing the nodes hav ing 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 mecha nisms. In that case, two attack scenarios are possible as illustrated in Figure 3. In the first scenario, the attacker is node 13 and the new preferred parent (node 24) has al ready 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 gener ates 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 eas ily repaired because the node 24 can re-attach to node 12 after sending few control messages. However, this at tack becomes more problematic when the node does not have a substitute parent such as node 31 in the second scenario. As depicted in Figure 3, 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 max imum rank value advertised for a DODAG, as seen in Section 2.2. The increased rank attack is more damaging in this second scenario, because more routing loops are built at the neighborhood. In that case, the loop repair mechanism requires to send 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 at tack 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 con sidered 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 can not 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. Also, thanks to the data

path validation mechanism, the RPL protocol is able to deal with these loops even if resources are consumed to repair them .

3.3 Analysis

We discuss in this section the properties of the identi fied attacks as well as methods and techniques to address them. Table 1 summarizes attacks against resources. A first property to be analysed 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 be long to the RPL network or are not allowed to access it. We can observe that only the flooding 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.

A second property is to determine if the attack is pas sive (P) or active (A). Passive attacks do not modify the behavior of the network. On the contrary, active attacks require the node to perform operations that are observ able by other nodes in the network. They are usually more critical than passive attacks which mainly target data confidentiality or topology information. Attacks tar geting the resources are all active since the attacker has to send packets.

A third property is the prerequisites property. The prerequisites are the required conditions to initiate the attack besides the internal/external nature of the attack, such as particular configuration of the network. The stor ing 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 incon sistency attacks.

The next property corresponds to the impact of the attacks. The objective is to quantify the consequences of a successful attack on the network.

The impact in this category is evaluated as the type of over-consumed resources (e.g. memory, battery, link availability). 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 im pacted since the attack requires sending a large number of control messages. The memory is also over-consumed in case of routing table overload attacks.

The fifth property corresponds to the CIA acronym standing for confidentiality, integrity and availability, and refers to a security reference model. In the context of the RPL protocol, confidentiality means the protection of routing information and exchanges. Integrity involves the protection of routing information from unauthorized mod ification, and availability requires that forwarding ser vices and routing information exchanges are accessible for the nodes. Regarding the identified attacks targeting re sources, they systematically impact network availability. Indeed, these attacks involve that the attacker jeopardizes resources of the network (battery, memory, processing, link availability). The integrity is also impacted when the result of the attack supposes that a legitimate re source or legitimate traffic is corrupted e.g. routing table of legitimate nodes is altered during routing table over load attacks. Version number modifications and DAG inconsistency attacks induce that the integrity of packets is jeopardized.

The two last columns of tables indicate respectively the possible security mechanisms to address the attacks, and their overhead (according to their authors). We saw that RPL provides internal mechanisms which contribute to counter attacks. For instance, the loop avoidance mecha nisms prevent increased rank attacks. The protocol also proposes an optional mitigation mechanism that limits in consistency attacks impact [10]. Specific approaches have been designed for the RPL protocol. The VeRa [7] and the TRAIL [13] approaches address version number modifica tions. In many cases, it is difficult to evaluate the over head induced by the security mechanisms because they are still at a conceptual level. Moreover, we cannot re ally consider that the mechanisms which are inherent to the RPL protocol operation introduce an overhead. Also in and , authors proposed an IDS to detect differ ent security threats.

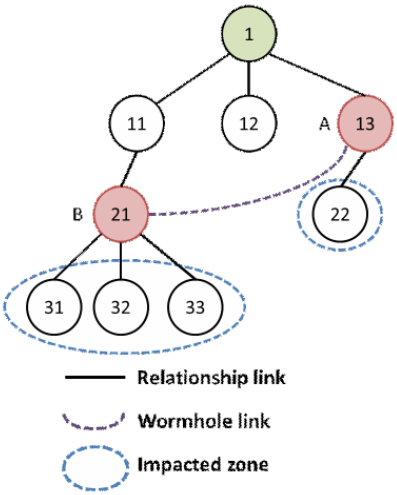


Figure 4. A wormhole attack in a RPL network

4. Attacks on Topology

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

4.1 Sub-optimization Attacks

In case of sub-optimization attacks, the network will not converge to the optimal form (i.e optimal paths) inducing poor performance.

4.1.1 Routing Table Falsification 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. This has not been studied yet in the context of the RPL protocol.

4.1.2 Sinkhole Attacks

An alternative attack consists in building a sinkhole. Such an attack takes place in two steps. First, the malicious node manages to attract a lot of traffic by advertising fal sified information data (for instance, up and downward links of superior quality). Then, after having received the traffic in an illegitimate manner, it modifies or drops it. In RPL networks, the attack can be easily performed through the manipulation of the rank value as shown in Section 5.2.1. Because of this falsified advertisement, the malicious node is more frequently chosen as preferred par ent by the other nodes, while it does not provide better performance. Thus, the routes are not optimized for the network. The attack modifies the topology and degrades network performance. Moreover, if the attacker decides to drop all the traffic, it also performs a blackhole attack as described in 4.2.1.

This attack was studied in and , the authors proposed an IDS to counter it. A functionality of this IDS is to build a global view of the network and as a con sequence the possiblity to detect incoherences in the net work such as sinkholes. In , the authors investigated defence techniques against sinkholes. The first technique is called Rank verification and restricts the possibility for the attacker to decrease its rank value. It allows legiti mate nodes to check if another node along the path has a fake rank. The second technique is called parent fail-over and operates as an end-to-end acknowledgement. When a root node does not receive enough traffic from a node (ac cording to a certain threshold value), it adds this node's address

in a DIO message field. When the node receives the DIO message with its own identity, it blacklists its parent and selects another one. The authors show that a combination of these two techniques provides efficient results in a RPL network.

4.1.3 Wormhole Attacks

Wormhole attacks are defined as the use of a pair of RPL attacker nodes, nodes A and B, linked via a private net work connection. An example is depicted in Figure 4. In this scenario, every packet received by node 13 is for warded through the wormhole to node 21 in order to be replayed later. Since the roles are interchangeable, node 21 may perform the same operations than node 13. In the case of wireless networks, it is easier to perform this at tack because the attacker can send through the wormhole the traffic addressed to himself as well as all the traffic intercepted in the wireless transmissions. The wormhole attack distorts the routing path and is particularly prob lematic for RPL networks. If an attacker tunnels routing information to another part of the network, nodes which are actually distant, see each other as if they are in the same neighbourhood. As a result, they can create non optimized routes according to the objective function. This attack was studied in which showed that the RPL protocol cannot solve this attack by itself. The au thors explained that countering this type of attack is a research challenge if one node of the wormhole is in the Internet. If both attackers are in the RPL networks, the authors suggested to use geographical data and different cryptographic keys at the mac layer for different segments to solve this threat issue. Also the authors of [11] pro posed to prevent this attack by using Merkel trees to au thenticate nodes and paths.

4.1.4 Routing Information Replay Attacks

A RPL node can also perform routing information re play 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 ta bles 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 . This attack is mentioned in however the authors nei ther study the consequences of such attack nor explained how it can takes place in RPL networks.

4.1.5 Worst Parent Attacks

This attack described in [15] and termed as ”Rank at tack” consists in choosing systematically the worst pre ferred parent according to the objective function. The outcome is that the resulting path is not optimized induc ing poor performance. This attack cannot be easily tack led because children node rely on their parent to route packets and this attack cannot be monitored by neigh bors. 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 .

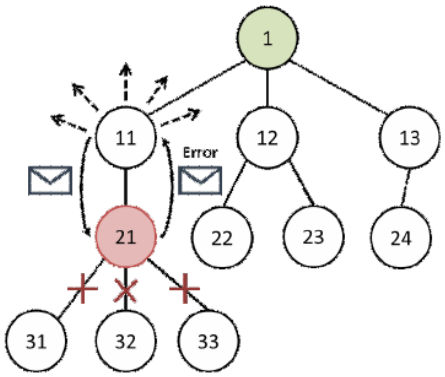
4.2 Isolation Attacks

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

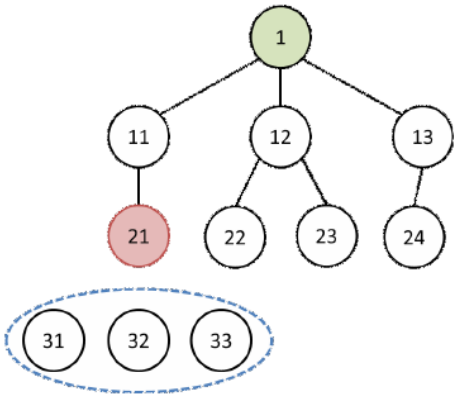
4.2.1 Blackhole Attacks

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 sub part of the network traffic. Chugh et al.[4] 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



(a) Initial State



(b) Final State

Figure 5. Illustration of a DAO inconsistency attack

percentage and delay. The IDS SVELTE proposed in [was designed to detect selective forwarding attacks in such networks.

4.2.2 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 . RPL provides a mechanism to re pair this inconsistency, called DAO inconsistency loop re covery. This optional mechanism allows the RPL router nodes to remove the outdated downward routes using the Forwarding-Error 'F' flag in data packets which in dicates that a packet can not 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 de picted in Figure 5. Once a packet is transmitted down ward, 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 incon sistent 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 down ward routes. This makes the topology of the DODAG graph sub-optimal. One possible consequence of this at tack 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 [2]. To re duce 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 [10].

5. Conclusion

The Internet of Things relies on the deployment of Low power and Lossy networks in order to support commu nications amongst objects and their interconnection to the Internet. These networks are characterized by scarce resources in terms of energy, processing and memory. Their development has led to the specification by the IETF ROLL working group of a dedicated routing proto col called RPL. Considering the nature of these networks composed of devices from the real life, it is a mandatory to identify and analyse the security attacks to which this protocol is exposed.

We have therefore proposed in this paper a taxonomy in order to classify the 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 sub optimal configuration or isolate nodes. Finally, attacks against network traffic let a malicious node capture and analyse large part of the traffic. Based on this taxon omy, we have compared the properties of these attacks and discuss methods and techniques to avoid or prevent them. While the RPL specification mentions two possible security modes, it does not define how they might be im plemented nor how the management of keys could be per formed. Most of the security solutions in the area are still at a proof-of-concept level. Moreover, while several solu tions from wired and wireless networks are available, they might significantly degrade network performance, which are limited in the Internet of Things. Risk management mechanisms provide new perspectives with respect to this issue. They could typically serve as a support for dy namically selecting the security modes and the protection techniques to be considered for a given context. The con text including the potentiality of attacks and the network properties (size, nature of devices). This adaptive config uration of RPL networks is a major challenge for address ing the trade-off between the level of security required by applications and the overhead induced by countermea sures.

Acknowledgments

Project number: University of Science and Technology Liaoning college students innovation and entrepreneurship training program in 2016 201610146026

References

[1] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," IEEE Communication Surveys & Tutorials, vol. 10, no. 4, pp. 78–93, Oct. 2008.

[2] A. Barbir, S. Murphy, and Y. Yang, Generic Threats to Routing Protocols, RFC 4593 (Informational), In ternet Engineering Task Force, Oct. 2006.

[3] A. Brandt, E. Bacceli, R. Cragie, and P. van der Stok, Applicability Statement: The Use of the RPL Protocol Set in Home Automation and Building Con trol, May 2014. (https://tools.ietf.org/html/ draft-brandt-roll-RPL-applicability-home -building-04)

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

[5] D. Djenouri, L. Khelladi, and A. N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," IEEE Communication Surveys & Tutori als, vol. 7, no. 4, pp. 2–28, 2005.

[6] J. R. Douceur, "The sybil attack," in First International Workshop on Peer-to-Peer Systems (IPTPS'01), pp. 251–260, London, UK, 2002.

[7] A. Dvir, T. Holczer, and L. Buttyán, "Vera version number and rank authentication in RPL," in Pro ceedings of Mobile Adhoc and Sensor Systems Con ference (MASS'11), pp. 709–714, 2011.

[8] O. Gaddour and A. Koubâa, "RPL in a nutshell: A survey," Computer Networks, vol. 56, no. 14, pp. 3163–3178, Sept. 2012.

[9] B. Guttman and E. A. Roback, An Introduction to Computer Security: The NIST Handbook, NIST Spe cial Publication 800-12, NIST, 1995.
[10] J. Hui and J. Vasseur, The Routing Protocol for Low Power and Lossy Networks (RPL) Option for Car rying RPL Information in Data-Plane Datagrams, RFC 6553 (Proposed Standard), Internet Engineer ing Task Force, Mar. 2012.
[11] F. I. Khan, T. Shon, T. Lee, and K. Kim, "Wormhole attack prevention mechanism for RPL based lln net work," in Fifth International Conference on Ubiqui tous and Future Networks (ICUFN'13), pp. 149–154, July 2013.
[12] K. D. Korte, A. Sehgal, and J. Schönwälder, "A study of the RPL repair process using contikirpl," in Proceedings of Dependable Networks and Services, LNCS 7279, pp. 50–61, Springer, 2012.
[13] M. Landsmann, H. Perrey, O. Ugus, M. W ählisch, and T. C. Schmidt, "Topology authentication in RPL," in IEEE Conference on Computer Commu nications Workshops (INFOCOM WKSHPS'13), pp. 73–74, 2013.
[14] A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, "6lowpan: A study on qos security threats and coun termeasures using intrusion detection system ap proach," International Journal of Communication Systems, vol. 25, no. 9, pp. 1189–1212, 2012.
[15] 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.