A Taxonomy of Attacks in RPL-based Internet of Things

Anthéa Mayzaud[1,2], Rémi Badonnel[2], and Isabelle Chrisment[2]
(Corresponding author: Anthéa Mayzaud)

Inria Grand Est - Nancy, France[1]
TELECOM Nancy, Université de Lorraine, LORIA, UMR 7503, France[2]
(Email: anthea.mayzaud@inria.fr)

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 Internet to objects from the real world which are interacting 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 automation systems. 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 [19]. 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 ROLL[1] working group has proposed a protocol called RPL (Routing Protocol for Low power and Lossy Networks) based on IPv6 [31]. Due to their constrained nature RPL-based networks may be exposed to a large variety of security attacks [27]. 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.

Many studies have been conducted on security issues regarding mobile ad-hoc networks [1, 5] and wireless sensor networks [29]. Current published surveys regarding the RPL protocol have been focused on performance evaluation [8] and a few on some specific security aspects. The security threat analysis [27] 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, integrity, authentication and availability). Guidelines and recommendations are provided to counteract these attacks. 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 including the routing protocol RPL but only mentioned three attacks regarding the routing protocol. The authors of [23] 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 [24] and [14]. Also, other studies [16, 28, 24, 25] present some attacks targeting the

---

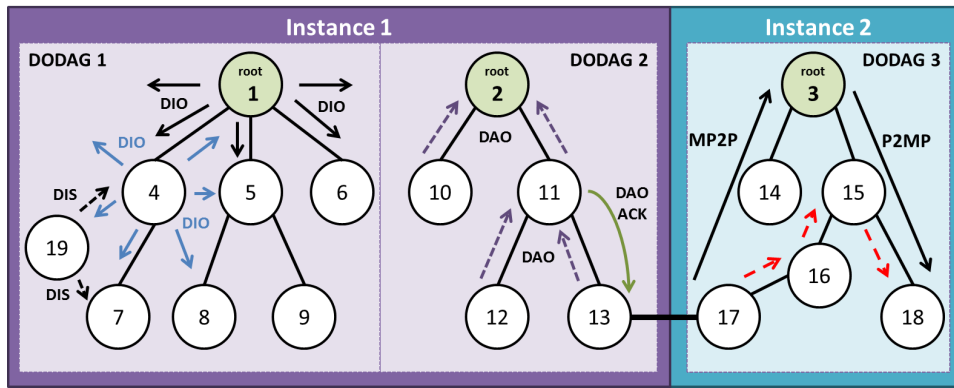[1]Routing Over Low power and Lossy networks

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 [17], the authors presented an evaluation in the emulation environment Cooja using the contiki OS[2] of four attacks targeting the RPL protocol mostly mentioned in [14].

In this paper, our objectives are the identification and classification of the different attacks against the RPL network protocol while providing details on how those attacks can take place. This novel approach classifies the attacks according to the attacker's goal and means considering 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 follows. 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 taxonomy. Section 3 focuses on security attacks targeting the network resources of RPL devices. Section 4 details security attacks targeting the topology and Section 5 addresses 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 future 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 multiple instances enable the RPL protocol to perform different 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 arrows 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 message contains the information required by RPL nodes to discover a RPL instance, get its configuration parameters, 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 parent 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 [18] which optimizes the transmission frequency of control messages depending on the network state. A new node may join an existing network by broadcasting a DIS message (*DODAG Information Solicitation*) in order to solicit DIO messages from its neighbors. The DAO messages (*Destination Advertisement Object*) are used to build downward routes. Depending 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 recursively through a DAO message. In the non-storing mode, DAO messages are unicasted to the DODAG root. Intermediate 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 mechanism, which consists in forming an intermediary DODAG and rejoining the main DODAG later. The RPL protocol can also detect inconsistencies using datapath validation 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 forwarded 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 [31].

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.

2.3 Security Concerns

The RPL protocol is exposed 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 particularly vulnerable 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 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 transport/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 gaining 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 depicted in Figure 2 and considers three categories of security attacks. The first category covers 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. The second category includes attacks targeting the RPL network topology. They disturb the normal 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.
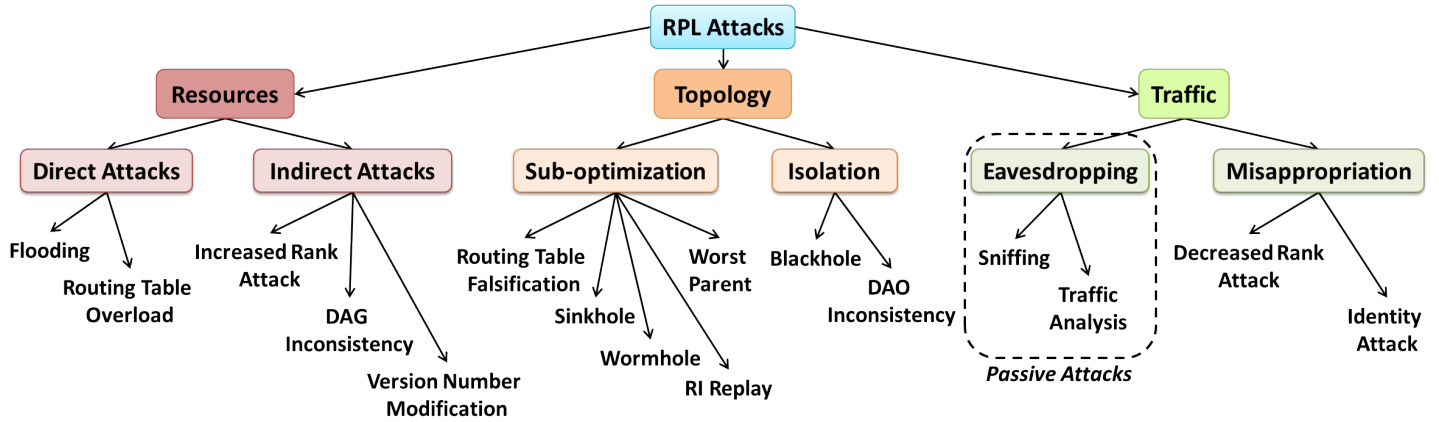
Figure 2: Taxonomy of attacks against RPL networks

3 Attacks Against Resources

Attacks against resources typically consists in making legitimate 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 congesting available links and therefore on the lifetime of the network which can be significantly shortened.

We distinguish two subcategories of attacks against resources. The first one gathers direct attacks where a malicious 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 generate 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 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.

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 solicitation 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 [17], 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 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 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 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 [25].

3.2 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.

3.2.1 Increased Rank Attacks

The increased rank attack consists in voluntarily increasing the rank value of a RPL node in order to generate
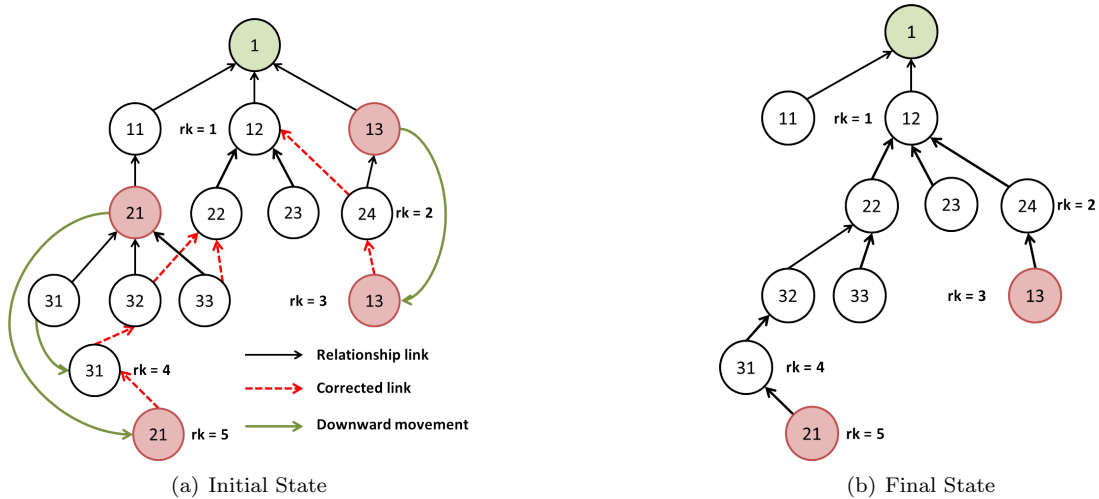
Figure 3: Rank increased attack in a RPL network

loops in the network. This attack has been studied in [32] 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 first to 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 3. 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 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 maximum 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 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. 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 [31].

3.2.2 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 [31] 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 flag is used to control this problem. When an inconsistency is detected by a node, two scenarios are possible: (i) if the Rank-Error flag 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

Table 1: Summary of attacks on resources

Attacks	I/E	A/P	Prerequisites	Impact	CIA	Mitigation/ Protection	Overhead
Flooding	I/E	A	-	Link/Battery	A	None	None
Routing Table Overload	I	A	Storing Mode	Memory/Battery	A/I	None	None
Increased Rank Attack	I	A	-	Battery/Link	A	RPL loop detection and avoidance mechanisms [31]	None (by default in RPL)
DAG Inconsistency Attack	I	A	Option Header	Battery/Link	A/I	Limitation of timer resets [10, 26, 22]	Low (for both solutions)
Version Number Attack	I	A	-	Battery/Link	A/I	VersionNumber and Rank Authentication [7], TRAIL [13]	Low (for both solutions)

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 flags or add new flags 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, [10] proposes to limit the rate of trickle timer resets due to an RPL Option to no greater than 20 resets per hour. In our previous works [26] and [22], we proposed instead of a fixed threshold two solutions that takes into account network characteristics. The first solution presented in [26] is an adaptive threshold with fixed parameters that we improved in a dynamic approach [22] where node's specific parameters are used instead. We showed that these approaches are more effective than the fixed threshold while preserving energy consumption of the nodes. Also another variant of a similar attack is described by the authors of [16] and [14]. Their attack termed as rank attack consists in not checking the rank relationship for a malicious node. The attacker does not set the 'R' flag if an inconsistency is detected. The difference with the DAG inconsistency is that the attacker does not manipulate flags to build "fake loops" but chooses to not solve "real loops" if they occur but the consequences are still similar.

3.2.3 Version Number Attacks

The version number is an important field of each DIO message. It is propagated unchanged down the DODAG graph and is incremented by the root only, each time a rebuilding of the DODAG is necessary which is also called global repair. An older value indicates that the node has not migrated to the new DODAG graph and cannot be used as a parent node. An attacker can change the version number by illegitimately increasing this field of DIO messages when it forwards them to its neighbors. Such an attack causes an unnecessary rebuilding of the whole DODAG graph. We showed in [21] that this attack can create many loops and as a consequences loss of data packets. Also the successive unnecessary rebuildings of the graph increase significantly controle message overhead exhausting nodes resources and congesting the network. Dvir et al. [7] proposed a security mechanism called VeRa (standing for Version Number and Rank Authentication) that prevents compromised nodes from impersonating the root and from sending an illegitimate increased VersionNumber. The solution uses authentication mechanisms based on hash operations. In that case, a node can easily check if the VersionNumber has been modified by the root node or by another malicious node, which can no longer usurp the identity of the DODAG root. Also, authors of [13] proposed an improvement of the previous solution solving some issues they discovered in VeRA.

3.3 Analysis

We discuss in this section the properties of the identified 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 belong 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 passive (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 observable by other nodes in the network. They are usually more critical than passive attacks which mainly target data confidentiality or topology information. Attacks targeting 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 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.

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 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.

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 modification, and availability requires that forwarding services and routing information exchanges are accessible for the nodes. Regarding the identified attacks targeting resources, 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 resource or legitimate traffic is corrupted e.g. routing table of legitimate nodes is altered during routing table overload 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 mechanisms prevent increased rank attacks. The protocol also proposes an optional mitigation mechanism that limits inconsistency attacks impact [10]. Specific approaches have been designed for the RPL protocol. The VeRa [7] and the TRAIL [13] 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. Moreover, we cannot really consider that the mechanisms which are inherent to

the RPL protocol operation introduce an overhead. Also in [24] and [16], authors proposed an IDS to detect different security threats.

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 falsified 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 parent 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 [28] and [24], 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 consequence the possiblity to detect incoherences in the network such as sinkholes. In [30], 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 legitimate 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 (according 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.
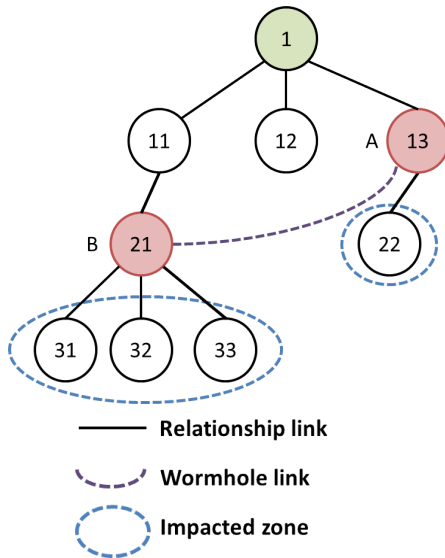

Figure 4: A wormhole attack in a RPL network

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 network connection. An example is depicted in Figure 4. In this scenario, every packet received by node 13 is forwarded 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 attack 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 problematic 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 [28] which showed that the RPL protocol cannot solve this attack by itself. The authors 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] proposed to prevent this attack by using Merkel trees to authenticate nodes and paths.

4.1.4 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 [31]. This attack is mentioned in [25] however the authors neither 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 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 [24].

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 network 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 subpart 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
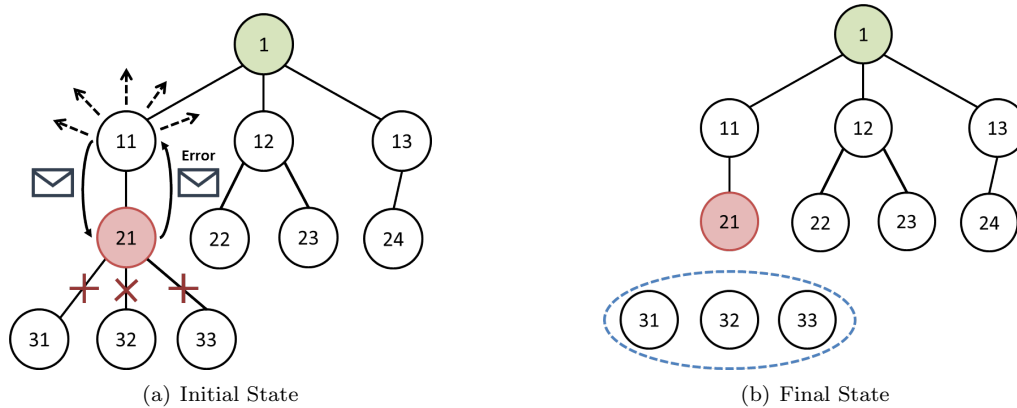
(a) Initial State

(b) Final State

Figure 5: Illustration of a DAO inconsistency attack

percentage and delay. The IDS SVELTE proposed in [24] 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 [31]. 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 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 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 [2]. 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 [10].

4.3 Analysis

Table 2 synthesizes attacks targeting the topology. We notice 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 falsifications 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.

In this table, the impact characterizes how the network is affected (modified or isolated) and what type of traffic is concerned (e.g. downward (D) or upward traffic (U)). We consider two main areas that may be impacted: (1) the neighbourhood of a RPL node corresponding to nodes in the direct vicinity such as parents, children, and siblings nodes, and (2) the subnet of a node. We can observe in that table that the routing table falsification attack and the DAO inconsistency attacks are characterized by a similar impact. Indeed, these two attacks corrupt the routing tables of the target. Only downward traffic is concerned because routing tables are only used for downward routing. Therefore, the subnet of the target is modified but the upward traffic is not disturbed. All the other attacks can have consequences on both upward and downward traffic since they concern all types of packets. In that case, both the subnet and/or the neighbourhood can be damaged. These attacks do not target a specific node but try to impact on the overall network traffic in general, even if some filtering is also be performed.

Regarding the next property, the availability is im-

Table 2: Summary of attacks on topology

Attacks	I/E	A/P	Prerequisites	Impact	CIA	Mitigation/ Protection	Overhead
Routing Table Fals.	I	A	Storing Mode	Target's Subnet, D	A/I	None	None
Sinkhole	I	A	-	Attacker's Subnet and Neighbourhood, D/U	A/I	SVELTE [24], Rank verification [7] and Parent fail-over [30]	Low, No evaluation
Wormhole	I	A	2 intruders min.	Attackers Subnet, D/U	A/I	Geographical data [28], Merkel trees [11]	No evaluation (for both)
Routing Information Replay	I	A	-	Attacker's Neighbourhood, D/U	A/I	Sequence Number [31]	None (by default in RPL)
Worst Parent	I	A	-	Attacker's Subnet, D/U	A/I	None	None
Blackhole	I	A	-	Attacker's Subnet, D/U	A/I	Monitoring of counters [4], Parent fail-over [30], SVELTE[24]	Depends on the solution, No evaluation
DAO Inconsistency	I	A	Storing Mode, Option Header	Target's Subnet, D	A/I	Limitation of discarding routing state [10]	Low

pacted in all attacks because the malicious node modifies the topology and then isolates nodes or degrades network performance through sub-optimization. The integrity is also impacted by attacks targeting topology. For instance, routing table falsification attacks and DAO inconsistency attacks alter routing table. Decreased rank attacks induce that the integrity of packets is jeopardized. Moreover, the routing information held by legitimate nodes such as parent identity, freshness or routing path are corrupted during routing information replay, sinkhole, wormhole, blackhole and worst parent attacks.

Replay attacks can be countered by sequence numbers implemented by default in the RPL protocol; also the optional mechanism proposed in RFC 6553 mitigates the effects of DAO inconsistency. The cost of this mitigation is low because it consists in implementing a fixed threshold. Different authors proposed several countermeasures to topology attacks such as the Rank verification [7], the Parent fail-over [30] or Merkel trees [11], however the costs of these solutions have not been evaluated yet. Chugh et al. [4] have defined methods for efficiently detecting blackholes in these networks. The SVELTE IDS [24] is also designed to detect the sinkhole and blackhole attacks. We notice that there is no solution for routing table falsification since this attack has not been studied in the context of the RPL protocol. The worst parent attack also does not have any counter-measures although this threat has been studied [15].

5 Attacks on 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.

5.1 Eavesdropping Attacks

The pervasive nature of RPL networks may facilitate the deployment of malicious nodes performing eavesdropping activities such as sniffing and analysing the traffic of the network.

5.1.1 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 sniffing 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.

5.1.2 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
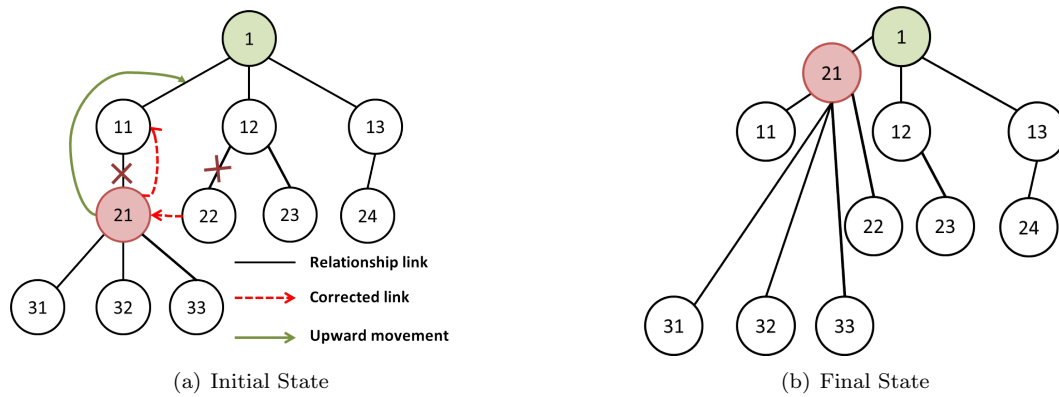
(a) Initial State   (b) Final State

Figure 6: Illustration of a decreased rank attack

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.

5.2 Misappropriation Attacks

In misappropriation attacks, the identity of a legitimate node is usurped or performance are overclaimed. These attacks are not so damaging for the RPL network per se. 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.

5.2.1 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 [7] solution as well as the Rank verification method [30] described in Sections 4.1.2 and 3.2.3 are able to address this issue. However authors in [13] 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 [24] can detect sinkhole attacks it can also detect the decreased rank attack.

5.2.2 Identity Attacks

Identity attacks gather both spoofing and sybil attacks. A spoofing attack also called Clone ID attack occurs when a malicious node pretends to be a legitimate existing node. In RPL networks, the root node plays a key role in a DODAG graph. It builds and maintains the topology by sending routing information. An attacker may sniff the network traffic to identify the root node. Once this identification is performed, it can spoof the address of the DODAG root and take the control over the network. During sybil attacks [6], one malicious node uses several logical entities on the same physical node. Identity attacks are used as a premise to perform other operations. They were studied in [28], the authors showed that the RPL protocol cannot solve this issue by itself and proposed to consider geographical data to detect such attacks.

5.3 Analysis

As we can observe in Table 3, 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.

Regarding attacks on traffic, Table 3 describes the cases where the consequences can be considered as critical for the RPL network. The effect of eavesdropping attacks depends on the nature of the listened data. For instance, data content may be of high importance for patients in the area of healthcare sensor networks, while the criticality is lower when the objective of the RPL network is

Table 3: Summary of attacks on traffic

Attacks	I/E	A/P	Pre.	Impact	CIA	Detection/ Protection	Overhead
Sniffing	I/E	P	-	Critical data	C	Encryption [31]	Depends on the algorithms
Traffic Analysis	I/E	P	-	Critical data	C	None	None
Decreased Rank	I	A	-	Node's rank	I	VeRA [7], TRAIL [13], Rank verification [30], SVELTE [24]	Low, Low, Not evaluated, Low
Identity attack	I	A	-	Node's rank	I	None	None

simply to collect weather temperatures. In case of misappropriation attacks, the consequences are determined by the location of the malicious or spoofed node. Indeed, when the malicious node has a lower rank, it is closer to the root. It is therefore capable of intercepting a larger amount of data and the opportunities to attack the RPL network are bigger.

The next property to be discussed is the classification according to the CIA model. The confidentiality aspect concerns eavesdropping attacks, where the goal of the attacker is to obtain information about the network configuration. Due to the nature of misappropriation attacks, the integrity property is affected in these cases.

The only way to prevent sniffing is to use encryption however in our security model we assumed that the attacker is able to break the cryptography due to the physical constraints of RPL networks. As mentioned previously, even if cryptographic mechanisms are suggested in the standard, it is difficult to implement them because important feature like key-management are left out by the RFC. Moreover, cryptographic algorithms are known to occupy the most memory and take many CPU cycles, thereby greatly affecting the performance of constrained devices. Current RPL implementations, as such, do not enable secure operation modes. There is no current existing solution to prevent traffic analysis and identity attacks in RPL networks. However, the decreased rank attack has been widely studied because it is also used in sinkhole attacks 4.1.2 and several counter-measures has been proposed.

6 Exploitation for Risk Management

This taxonomy provides an overview of the main attacks that the RPL protocol therefore the Internet of Things is currently facing and details their properties. It shows that most of the studies within the area are proof of concepts and that mature security mechanisms are far from being fully deployed. The classification is conceived in a way it is easily expendable with possible future attacks in RPL networks. Our objective is to give a view of the different possibilities. We design this taxonomy so it can be exploited for risk management which consists in identifying, evaluating and treating the risks that a network

or an information system faces. The attacks, their consequences and their security mechanisms are considered separately but it is likely that a real attacker combines several of these attacks. Existing approaches from similar networks such as MANETs (Mobile Ad-hoc NETwork) and WSNs (Wireless Sensor Networks) could be investigated. However, they are often too expensive or too difficult to deploy in such highly constrained networks.

6.1 Risk Management

In this context, risk management offers new perspectives to dynamically activate or deactivate security mechanisms in RPL-based networks, in order to prevent attacks while maintaining network performances [20]. We propose in this section to investigate risk management methods and techniques to address the trade-off between security and cost in the Internet of Things. The risk level is defined by Equation (1) [9].

$$\mathcal{R}(a) = P(a) \times E(a) \times C(a). \tag{1}$$

Let consider a security attack noted a. The risk level $R(a)$ depends on the potentiality $P(a)$ of the attack, the exposure $E(a)$ of the RPL network, and the consequences $C(a)$ on the network if the attack succeeds. Risk management is a process consisting in monitoring, prioritizing and controlling risks. For instance, when this process observes a high potentiality $P(a)$, it may activate security mechanisms (being aware of their costs) to reduce the exposure $E(a)$ and maintain the risk level $R(a)$ to a low value.

As depicted in Figure 7, risk management process is composed of two main activities: risk assessment and risk treatment. Risk assessment consists in quantifying the potentiality of attacks. For that, it is necessary to evaluate the performance of detection techniques (based on anomalies or known signatures) in these RPL environments, and to identify the network nodes able to perform this activity. Risk assessment aims also at quantifying the consequences of successful attacks. The objective is to assess the relative importance of nodes in the RPL network, and to analyze how the attack against a given node may impact on the functioning of the overall network.

The risk treatment activity consists then in selecting and applying the security mechanisms that are needed having the cost of the solution in mind.
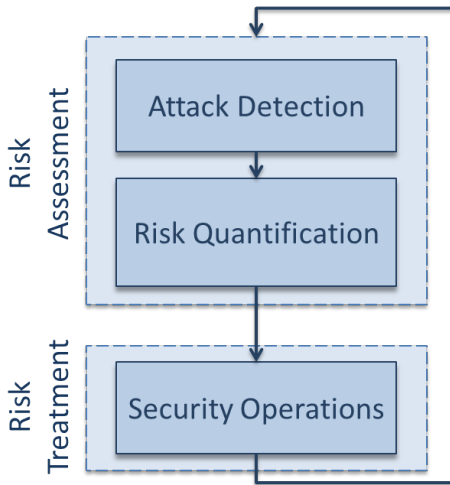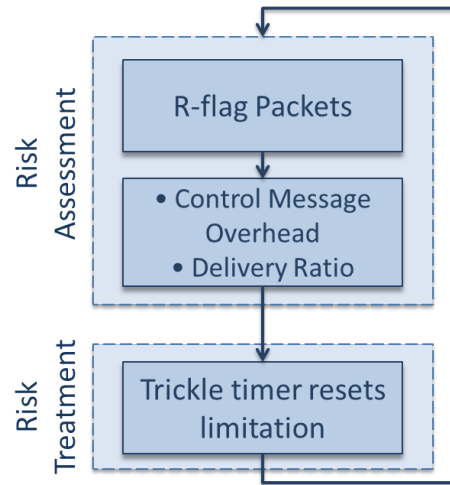
Figure 7: Risk management process

Figure 8: Risk management process applied to the DAG inconsistency attack

6.2 Instantiation

In this section, we propose to show how risk management can be applied to a particular attack. We choose the DAG Inconsistency attack from Section 3.2.2 that we studied in [26]. Risk assessment is composed of quantification of potentiality and consequences of an attack. To quantify the potentiality of an attack we need to define a metric allowing us to detect it. In the DAG inconsistency attack case, an efficient metric is the number of 'R'-flag packets. An attack is detected if this value reach a threshold defined in [26]. To quantify the consequences of this attack, we can use interesting metrics such as control message overhead and delivery ratio.

Regarding the risk treatment, in order to reduce the impact of such attack in the network, several countermeasures can be considered and applied. We already mentioned the solution proposed in the RFC 6553 [10] which is to limit at 20 per hour the number of trickle timer resets due to DAG inconsistency detection. The other countermeasures that we proposed are also to limit the number of trickle timer resets but using an adaptive or a dynamic threshold instead of fixed one. Our approaches are able to adapt according to the aggressiveness of the attacker. The adaptive threshold relies on set values and the dynamic is based on node's specific parameters. Figure 8 summarizes the risk management process applied to the DAG inconsistency attack.

This process can be applied to each attack we described in this taxonomy. For that purpose, each attack has to be accurately studied (with detection metrics and techniques highlighted) and security countermeasures developed or identified. The classification can help prioritizing the risks according to which main network resources are harmed.

7 Conclusions

The Internet of Things relies on the deployment of Low power and Lossy networks in order to support communications 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 protocol 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 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 taxonomy, 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 implemented nor how the management of keys could be performed. Most of the security solutions in the area are still at a proof-of-concept level. Moreover, while several solutions 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 dynamically selecting the security modes and the protection techniques to be considered for a given context. The context 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 countermeasures.

Acknowledgment

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), Internet 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 Control*, 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 & Tutorials*, 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 *Proceedings of Mobile Adhoc and Sensor Systems Conference (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 Special Publication 800-12, NIST, 1995.

[10] 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.

[11] F. I. Khan, T. Shon, T. Lee, and K. Kim, "Wormhole attack prevention mechanism for RPL based lln network," in *Fifth International Conference on Ubiquitous 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. Wählisch, and T. C. Schmidt, "Topology authentication in RPL," in *IEEE Conference on Computer Communications 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 countermeasures using intrusion detection system approach," *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.

[16] A. Le, J. Loo, Y. Luo, and A. Lasebae, "Specification-based ids for securing RPL from topology attacks," in *Wireless Days*, pp. 1–3, 2011.

[17] A. Le, J. Loo, Y. Luo, and A. Lasebae, "The impacts of internal threats towards routing protocol for low power and lossy network performance.," in *IEEE Symposium on Computers and Communications (ISCC'13)*, pp. 789–794, 2013.

[18] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko, *The Trickle Algorithm*, RFC 6206 (Proposed Standard), Internet Engineering Task Force, Mar. 2011.

[19] 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`)

[20] A. Mayzaud, R. Badonnel, and I. Chrisment, "Monitoring and security for the internet of things," in *Emerging Management Mechanisms for the Future Internet*, LNCS 7943, pp. 37–40, Springer, 2013.

[21] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "A study of RPL dodag version attacks," in *Monitoring and Securing Virtualized Networks and Services*, LNCS 8508, pp. 92–104, Springer, 2014.

[22] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "Mitigation of topological inconsistency attacks in RPL-based low-power lossy networks," *International Journal of Network Management*, 2015.

[23] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6lowpan in IOT," in *International Conference on Pervasive Computing (ICPC'15)*, pp. 1–6, Jan. 2015.

[24] 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.

[25] 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.

[26] A. Sehgal, A. Mayzaud, R. Badonnel, I. Chrisment, and J. Schönwälder, "Addressing DODDAG inconsistency attacks in RPL networks," in *Proceedings of Global Information Infrastructure and Networking Symposium (GIIS'14)*, pp. 1–8, 2014.

[27] T. Tsao, R. Alexander, M. Dohler, V. Daza, A Lozano, and M. Richardson, *A Security Threat Analysis for Routing Protocol for Low-power and Lossy Networks (RPLs)*, RFC 7416, Internet Engineering Task Force, 2015.

[28] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based internet of things," *International Journal of Distributed Sensor Networks*, vol. 2013, pp. 1-11, 2013.

[29] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, pp. 2–23, 2006.

[30] K. Weekly and K. S. J. Pister, "Evaluating sinkhole defense techniques in RPL networks," in *Proceedings of the 20th IEEE International Conference on Network Protocols (ICNP'12)*, pp. 1–6, 2012.

[31] 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.

[32] 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.

Anthéa Mayzaud is a researcher at the MADYNES Team at Inria, France and a third year PhD student at the University of Lorraine, France. She received her M. D. in Computer Science at TELECOM Nancy, France. Her main research interests are security issues in the Internet of Things mostly based on the RPL protocol and lightweight security solutions based on risk management.

Rémi Badonnel is an Associate Professor at TELECOM Nancy and a research staff member of the MADYNES Research Team at Inria. Previously he worked on change management methods and algorithms at IBM T.J. Watson in USA and on autonomous systems at the University College of Oslo in Norway. His research interests include network and service management, dynamic and autonomic environments, security and defence techniques.

Isabelle Chrisment is currently a Professor at TELE-COM Nancy, University of Lorraine. She received her PhD in Computer Science in 1996 from University of Nice-Sophia Antipolis and her Habilitation Degree in 2005 from University of Lorraine. Head of the MADYNES Reseach team at Inria, her research activities focus on network monitoring and security within dynamic networks.