RPL Attack Analysis: Evaluation of a Cryptography-Based Sybil Defence in IEEE 802.15.4

Ruben Stenhuis , Mauro Conti , Chhagan Lal
TU Delft

***Abstract*—While the Routing Protocol for Low Power and Lossy Networks (RPL) is built to support the constraints of low-powered devices, it struggles to meet the standards in security. Generally, low-powered devices are challenged with limited cryptography, tough key management, and interoperability issues. Despite these concerns, security is not only deficient for RPL, but proposed mitigations appear untouched as well. This paper therefore contributes a lightweight cryptosystem. It questions and justifies its virtue in a twofold. First, we illustrate the importance of this mitigation with an impactful Sybil attack that enables malicious routing on root level. Second, we construct an attack pattern model and life-cycle to demonstrate the operational capabilities and objectives of the adversary for Internet of Things (IoT) generic attack patterns. The cryptosystem divides IEEE 802.15.4 networks into isolated clusters with key derivation functions. Because the key derivation function adopts spectrum resource measurements, the proposal includes a cooperative defence to validate these measurements of joining nodes. To avoid overhead, the mitigation operates on symmetric-key cryptography, piggybacked cluster identifiers, and Maximum Transmission Unit (MTU) requests to the trusted party that stores encrypted identity keys of member nodes. This mitigation, when combined with the efficient routing of RPL, enables a broad application for smart low-power constrained devices in a scalable IoT network while it protects against Sybil attacks and eavesdropping.**

***Index Terms*—RPL, IoT, RPL Attacks, IoT Security, Routing Attacks, Security Analysis**

1 Introduction

The fast-paced development of electronic devices has led to a new prospect called Internet of Things (IoT). Typically, IoT describes a Low-powered and Lossy Networks (LLN) [1, p. 2350] that has a broad application in analytics, cloud services, and 'smart' household products. Already, IoT offers an enormous market potential for these applications, primarily in healthcare [1]. Another advantage of LLNs, is the efficiency and low cost of Reduced Function (RF) devices, as this facilitates a deployment at remote places. These characteristics of IoT form a broad and revolutionizing technology that has a great impact on our future residence.

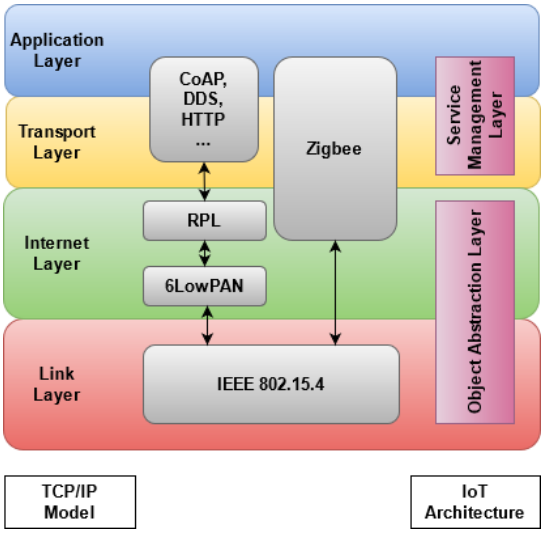

Figure 1: 6LoWPAN protocol stack put into perspective.

1.1 IoT Architecture

In order to compete with this demand, the Internet Engineering Task Force (IETF) suggested an assembly of standards for LLN routing in 2008 [2]. The main issue with existing protocols is the fact that LLNs were not capable to implement nor communicate with TCP-IP reference layers, as it violates the IoT requirement of being resource constraint [2]. The new protocol is introduced in RFC6550 and called Routing Protocol for Low Power and Lossy Networks (RPL) [3]. This is an infrastructure protocol and is build upon IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) and IEEE 802.15.4 that were standardized earlier. These protocols together form one of the layers of state-of-the-art IoT architecture.

The architecture that is currently purposed for IoT is described in [1] and is a layered 5-tier architecture. This paper focuses on the object abstraction layer that is described in [1]. This layer consists of protocols that manage the transfer of data. Examples of these protocols are Bluetooth, IEEE 802.11, and IEEE 802.15.4.

In Fig. 1, a modified version of the IP stack is demonstrated that inherits the three protocols RPL, 6LoWPAN, and IEEE 802.15.4. These protocols have the following functions:

1. **IEEE 802.15.4:** Capsulates the physical and link layer. It is able to handle a large and low-powered network due to its slotted multi-channel access control, that allow for low duty cycles [4]. It supports RF nodes and is controlled by Personal Area Network (PAN) coordinators.
2. **6LoWPAN:** Envelops IPv6-addressing with header compression to meet the Maximum Transmission Unit (MTU) requirement of IPv6 in IEEE 802.15.4.
3. **RPL:** Routes IPv6 packets in a Destination Oriented Directed Acyclic Graph (DODAG). The routing protocol maintains its structure by RPL control messages. This will be assessed in further detail within section 2.1.

Security research in IoT is crucial, as the RF devices cannot implement all preventative measures like a Fully Function (FF) device would. Two examples of this are public-key ciphers [5] and key distribution [1]. Besides, RPL has serious interoperability [2], security and privacy problems [6][7]. Analyzation of vulnerabilities in RPL is thus of high value, since such analysis can offer effective policy recommendations to researchers and developers.

1.2 Related Work

Currently, RPL has gained major attention under researchers [2]. Most of the published papers are about efficient routing, but there is a deficiency in physical tests, security research, and uniform implementations [2]; Despite the fact that security is the most important challenge in IoT [1, p. 2372][2]. Four of the most influential papers are presented in the following paragraphs.

Raoof et al. in [8], analyzed the performance hits of RPL secure modes when the protocol is attacked. The paper concludes that the modes are efficient without replay protection, but nodes should have more distinct paths to the root and a lower timeout duration to counter attacks.

Raoof et al. in [7], issued a comprehensive classification of RPL attacks and mitigation techniques. However, it is more focused on layer-specific attacks with a strong emphasis on mitigation techniques.

Mayzaud et al. in [9], released a comprehensive security assessment of RPL attacks. The paper dives deep into their impact and other properties. It also offers a risk management technique that adheres to the National Institute of Standards and Technology (NIST) cybersecurity framework. However, it abstracts IEEE 802.15.4 and limits the threat assessment to the CIA model, which is criticized for an incomplete set of security goals [10, p. 5].

Tomić et al. in [11], noticed the deficient attention of cross-layer security and published a survey on this for IoT. It also includes an experiment on the impact of RPL attacks. However again, neither the life-cycle of the adversary nor a coherent threat assessment is considered.

1.3 Contribution

It is of high value to secure IoT as the industrial demand preserves growing. As a result, it is crucial to implement the proposed mitigation methods in the 8-year-old RPL. However, since there is an incoherent view of RPL's threats and a deficiency of uniformity, this is currently unfeasible. This paper will therefore contribute an analysis of IoT generic threats to clarify the origin of RPL vulnerabilities. Additionally, the paper will design and mitigate an attack that exploits these vulnerabilities to answer the research question below.

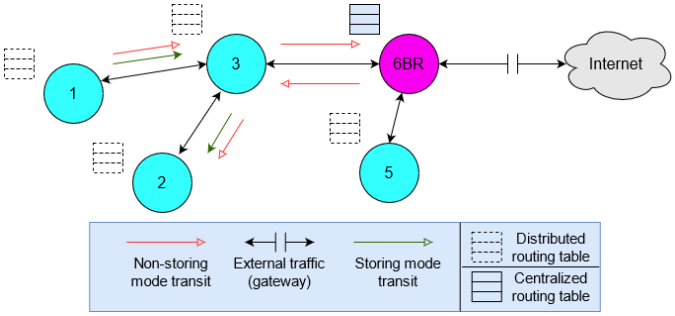

Figure 2: The cluster tree topology of RPL in both storing modes.

> *RQ: "What generic attacks to the Internet of Things remain an imminent security threat in RPL-based networks and what mitigation can be employed against this threat on IEEE 802.15.4?"*

The structure of the paper is as follows. Section 2 presents an overview of RPL's topology, control messages, vulnerabilities and attacks. Section 3 describes the method for the security assessment and the approach for the proposed mitigation. Section 4 sketches and mitigates a newly proposed threat. Section 5 relates to this mitigation and depicts an overview of generic RPL security threats. Section 6 forms the discussion of the research. Section 7 concludes the research.

2 Overview of RPL

RPL refers to a routing standard designed for devices that are resource constrained. RPL relies on the IPv6 protocol and ICMPv6 format for addressing and topology maintenance respectively. Further in this section, the topology and RPL's behavior are assessed, as well as its risks and security measures that were proposed in previous work. For each RPL vulnerability, it is assumed that the DODAG height is more than one and any hazard originates from internal nodes.

2.1 RPL

RPL has four identifiers: RPLInstanceID, DODAGID, DODAGVersionNumber and rank. The first two uniquely define any RPL instance. Here, DODAG refers to the graph that models RPL's topology, which can be thought of as a cluster tree network (Fig. 2). The rank or tree depth of a member node depends on the Objective Function (OF). The OF defines the metrics and the optimization objective that purpose parent selection [7].

The transit route is maintained by RPL control messages. However, the root can also force a repair operation by increasing the DODAGVersionNumber. When the DODAG is consistent, all member nodes can be reached via the root.

The transit route of a downward packet is defined by a source routing table. Source routing tables are central (non-storing mode) or distributed (storing mode). This table is

made based on Destination Advertisement Object (DAO) messages, as will be discussed in section 2.1.1.

Upward messages are sent to the preferred parent of the sender. The parent propagates the message in the same way until one knows the source route of the receiver. Thus, it is sometimes trivial for a message to reach the root. For example, with external addressed messages, or non-storing mode.

Upward and downward packets may be authenticated with HMAC or RSA in one of the two security methods: preinstalled mode or authenticated mode; but no system design is given by RFC6550 [3].

2.1.1: RPL Control Messages

RPL's communication is maintained by ICMPv6 RPL control messages. These messages are the following:

- **DODAG Information Solicitation (DIS):** Transmission of this message is meant for nodes that desire to explore the network. Depending on the flags set and existence of a Solicited Information option, the receiver uni- or multicasts a DIO.
- **DIO messages:** DIOs contain identifiers of member nodes and possibly also the configuration options of the DODAG. The message is meant to inform the network of a node's presence. It is multicasted as response to a Trickle timer [12] reset, or major changes in the network such as a global repair. DIO and DIS messages together maintain the network for upward traffic.
- **DAO messages:** DAOs propagate the preferred path to nodes that can store this routing information. The DAO message contains four Equal Cost Multiple Paths (ECMP) in the path control field that are preferred by the node. This information can then service the receiver to update the source routing table.
- **Consistency Check (CC):** CC synchronizes the counter value of two member nodes. This is part of a security feature against replay attacks.

2.1.2: Preventative Measures of RPL

All RPL control messages have a secure variant in which members sign the message with AES-128 in CBC-MAC. In addition, RPL has support for RSA signatures. However, both options are obsolete, as IEEE 802.15.4 already supports data authenticity [4, pp. 54-55] and RSA is too computationally heavy for some IoT devices [5]. RFC6550 [3] also proposes RPL authenticated mode. This mode appends the cryptography with a central authority and session keys. Unfortunately, its specification is not sufficient for implementation.

2.2 Vulnerabilities of RPL

With the background of the RPL protocol, one can reason about vulnerabilities in RPL's design. The following vulnerabilities are extracted from the topology (V1-4), control messages (V5-6), and preventative measures (V7-8).

$V1$) The tree topology restricts the path diversity of the network. Nodes that are close to the root may be congested quickly when it routes large sub-DODAGs [8]. Predictability can also be an issue, because it improves the effectiveness of scoping prior to an attack.

Table 1: Mitigation methods for IoT Generic Attacks.

Type	[15]	[16]	[17]	[18]	[20]	Proposed (section 4.2)
HELLO-Flooding	✓	✓	✓	-	-	-
Isolation Attack	-	-	-	✓	-	-
Sybil Attack	-	-	-	-	✓	✓
Wormhole Attack	-	✓	-	-	-	-
Sinkhole Attack	✓	✓	-	✓	-	✓
Replay Attack	-	-	-	-	-	-
Traffic Analysis	-	-	-	-	-	Eavesdropping
Cross-Layer	-	-	-	-	-	-

$V2$) The tree topology requires all the parents to propagate messages of their children. Thereby, disobeying parents form a risk to the network.

$V3$) Centralized routing tables rely on Source Resource Measurements (SRM), such as the Received Signal Strength Indicator (RSSI) in IEEE 802.15.4 [4, Sec. 6.16][7]. Thus, forgery of these metrics can cause the root to depart out of memory or take alternate routing paths.

$V4$) Distributed routing tables have the same issues as centralized routing tables. Only now, malicious nodes can have easier access to the tables.

$V5$) DIO messages have a significant amount of information. This information can form a basis for attacks such as impersonation attacks.

$V6$) RPL control messages can trigger repair operations. A node that advertises fictitious paths, can thus initiate a local repair [13].

$V7$) RPL is an internet layer protocol. Thus, RPL is also vulnerable for link layered and IPv6 addressing exploits. An example of cross-layer attacks is the 6LoWPAN fragment duplication attack that spoofs IPv6 addressing in RPL [6][14].

$V8$) RPL is still vulnerable to internal attacks when the member key is shared because all members of an RPL instance have access to this key.

2.3 Exploits and Previous Proposed Mitigations

IoT generic attacks exploit the vulnerabilities of section 2.2. This paper gives a brief analysis of the existing attacks In the following paragraphs. This analysis mentions the goal, resources, and mitigation (Tab. 1) of the attack. Notice that the adversary requires to possess any shared key for all attacks except traffic analysis and cross-layer attacks.

- **HELLO-Flooding:** In a HELLO-flooding attack, a large number of control messages are sent by or due to the adversary, with an aim to congest the network. To achieve significant congestion, the adversary can either broadcast a DIO message with substantial routing metrics [7] or DIS messages [9]. Only DIS-flooding can be performed without joining the network. *Mitigation:* SRPL and CHA-IDS for DIO-flooding [15][16]. But these have a significant overhead for joining nodes [15]

or security system [16]. Secure-RPL [17] is an efficient mitigation method for DIS-flooding.

- **Isolation Attacks:** In an isolation attack, packets are dropped on purpose to isolate a sub-DODAG. This might not be complete isolation as the adversary might be selective. The adversary is then called a greyhole. Both attacks can only be done as a parent. *Mitigation:* SVELTE [18] and trust functions [7]. However, greyhole attacks remain unpleasant to detect with these methods, because of their low profile.
- **Sybil and Cloning Attacks:** To clone the victim, a malicious node spoofs the identifiers of that node. For example, a nearby adversary may capture DIO messages of a legitimate member node, which grants the adversary the information to spoof the target node. In the more sophisticated Sybil attack, one or more of these pseudonyms then treat other operations. Zhang et al. [19] documented Sybil attacks in three models that aim to either eavesdrop (SA-2 and SA-3) or manipulate data (SA-1). Therefore, Sybil attacks might be the most severe exploit, as it can directly be used to isolate, spy, and achieve privileges of the victim. Because the identifiers are captured for the RPL instance, the adversary can execute these attacks when it is within range of the network. *Mitigation:* trust functions such as SecTrust [20] and signatures [19].
- **Wormhole Attacks:** Wormhole Attacks maintain a path to another malicious node. This way the nodes look like a child and parent for the root. The aim of this construction is to disturb the network by taking a longer and congested path. By definition, the adversary requires at least one member and an external node that have a shared medium. *Mitigation:* Round Trip Time (RTT) based IDS, trust functions, and Specification-based IDSes on RSSI [7].
- **Sinkhole Attacks:** In a sinkhole Attack, the adversary lures member nodes with tweaked metrics. This grants an influential position (similar to DIO-flooding). When the adversary abuses this position it becomes problematic. The aim is a high dependency on member nodes. Any sinkhole must be an internal node [9] with insight into the OF. *Mitigation:* see the mitigation of HELLO-flooding.
- **Replay attack:** The adversary retransmits captured frames. Considering RPL control messages, the purpose of the adversary is to bring inconsistency in RPL's topology. For instance, routing information replay attacks facilitate DIO-flooding [7][9]. This attack can be executed when the adversary is in range of the network with recorded packets. *Mitigation:* signed sequence counters. This is already defined in RFC6550 of RPL [3]. Unfortunately, this protection has an enormous performance hit in mobile networks [21].
- **Traffic Analysis & Eavesdropping:** Eavesdropping is an issue for the privacy of member nodes when the network is not protected with encryption. Additionally, this attack can be purposed as the main scope method before a more sophisticated attack. This attack is passive, thus the only requirement for the adversary is a shared medium. *Mitigation:* impossible, the impact can only be minimized with encryption and increased path diversity.
- **Cross-Layer Attacks:** In a cross-layer attack, the adversary performs an exploit on a lower layer to impact a higher layer. For RPL these include: CSMA-CA unfairness, network address spoofing, and node tampering [6]. There is no general aim for this attack, as lower-layered attacks are diverse. *Mitigation:* individual mitigations are documented in [6] and [11].

3 Methodology

This section includes the models for the contribution that purpose the following approach. The contribution opens with an example of a new exploit to underline the importance of Sybil attack mitigation. It explains the setup, prerequisites, and impact according to the design in RFC6550 [3]. The mitigation is aimed to be a scalable and energy efficient handshake on IEEE 802.15.4 [4]. This is theoretically validated with the metrics: energy consumption, control message overhead, transmission time, and End-to-End (E2E) delay; since these have been introduced to consider the requirements of LLN [22]. Lastly, the threat assessment and adversarial capabilities will demonstrate the effectiveness of the mitigation. This is accomplished with the attack pattern model of T. Li et al. [23] and the Office of the Director of National Intelligence (ODNI) cyber threat framework [24]. The attack pattern model defines the operationalization of the attack strategies of the adversary, while the cyber threat framework defines the adversarial life cycle for the threat events. Attack patterns are conducive to the determination and illustration of attack vectors and in the mitigation of threats, as these are clearly depicted as directed paths. A threat framework enables a consistent assessment [24].

3.1 Attack Pattern Model

T. Li et al. [23] simplifies attack strategies with a systematic approach both for analyzing and modelling context-specific attack patterns. This is done in three steps.

3.1.1: Attack Pattern Problem

The problem of an attack pattern is the anti-goal of the adversary. Anti-goals are goals from the perspective of the adversary. T. Li et al. [23] define anti-goals as a quadruple of an asset, threat, target, and interval of an attack. The model in [23] focuses on the threat and target of an anti-goal. Targets are the domain of an attack. Attacks in this paper are all in the communication domain because the research is limited to RPL. Threats are simplified in STRIDE. STRIDE is an acronym for six security threat types defined in [25].

3.1.2: Attack Pattern Context

The context defines the conditions of the attack. These predicates include protected_by, communicate, use_technique, use_data_from, and accept_user_input. Notice that the predicates are distinct from the domain. This allows for a simpler domain model within the model as explained in [23].

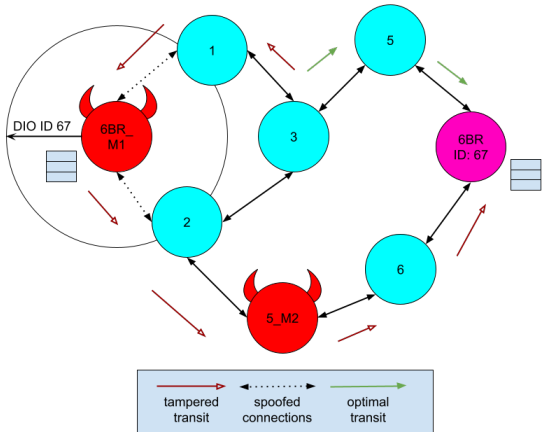

Figure 3: RPL Rogue Root Attack, with the adversary (left) spoofing DIO packets of the root (right).

3.1.3: Attack Pattern Solution

The solution forms an attack execution flow. Thus, it hierarchically demonstrates the tasks that the adversary requires to accomplish before the attack can be executed. An anti-goal is said to be operationalizable when a path meets the prerequisites of an anti-goal in a valid context.

This paper adopts this method for the operationalization of attack strategies in RPL. However, T. Li et al. [23] adopt Mitre's database for the attack patterns. This paper does not consider these and only considers the attack patterns of section 2.3 from: [7], [9], and [19].

One major limitation of this method is that the categorization can be disputed due to its simplification [25, p. 64]. However, this is not the aim of section 5, as this study focuses on determination and illustration of threats.

3.2 ODNI Threat Framework

ODNI Threat Framework characterizes any threat in 4 stages: preparation, engagement, presence, and consequence. With these stages, the framework pictures the life cycle of adversaries in the system. Each stage distinguishes three aspects. The objective of the attacker, for instance hiding at the presence stage. Then, the adversary applies a strategy to achieve this purpose (called the action), for hiding this could be the adoption of fictitious routing metrics. Lastly, these actions can have indicators, such as failed transmissions.

4 Rogue Root Attack

This section describes a new exploit that elevates the privilege of Sybil nodes. This attack is then mitigated with a cooperative Sybil defence, based upon a symmetric-key cryptosystem. The threat assessment of section 5 demonstrates the changed perspective of the adversary, as explained in section 3.

4.1 Overview of Rogue Root Attacks

The rogue root attack is demonstrated in Fig. 3. It can be thought of as a rogue access point of an IEEE 802.11 network. This characterizes the rogue root attack as a man-in-the-middle (MITM) attack between the victim and the root. The adversary maintains the spoofed network with almost full control in non-storing mode. The next subsections will visualize this in more detail with Fig. 3.

4.1.1: Setup

To attain the depicted state, adversary $6BR_{M1}$ will first perform an impersonation attack on the DIO message of the legitimate root $6BR$. The adversary then transmits the message out of range of the legitimate root. FF nodes 1 and 2 are unable to distinguish the messages without authentication. Thus, the nodes attach to the closer adversarial node and propagate the inconsistency to their children until the paths to $6BR_{M1}$ and $6BR$ have a similar rank (node 3 and 5_{M2}).

4.1.2: Prerequisites

The rogue root attack exploits rudimentary RPL instances. Assuming that the adversary has all preinstalled keys, each instance of this protocol can be attacked when the adversary has the ability to either do a Sybil attack or replay attack. The latter has the limitation that the attack might be identified earlier because it is not able to maintain the data flow through a collaborating adversary. Consequently, the node becomes a blackhole at root level.

Maintainance of the state is possible when $6BR_{M1}$ tampers Source Routing Headers (SRH) [26] to route to the colluding Sybil node 5_{M2}. When the Sybil node receives the traffic, it is redirected to $6BR$ in the original RPL instance. Finally, one or more Sybil nodes send and receive traffic as a bridge on behalf of the victims.

4.1.3: Impact

The attack has the highest impact when the RPL instance is in non-storing mode and dispersed. Non-storing mode ensures more traffic to the malicious root. Dispersed members make the possibilities of one-hops smaller, therefore this also increases the dependency to the root.

Adversary $6BR_{M1}$ might abuse the privileges of being root with amplified Sybil attacks. For example, the privileges can be misused to choose sub-optimal routes as depicted in Fig. 3, eavesdrop, or perform routing loops.

4.2 Mitigation

As mitigation for the rogue root attack, this paper proposes a solution to Sybil attacks. Sybil attacks originate from nodes that can have multiple identities in a network. Cryptography-Based Mobile Sybil Detection (CMSD) cause pseudonym maintenance to be more difficult [7].

This mitigation builds upon this concept. It consists of Trusted Third Parties (TTP) and internal devoted nodes. The idea is that devoted nodes create a domain of protection and access policy for an IEEE 802.15.4 network. This access policy relies on link attributes, consequently, any pseudonym could be detected, when it has an inconsistent metric (stolen identities [7]) or unverified keys (fabricated identities [7]).

The subsection will first define and relate the roles of this system. Then, it defines the stepping stones and adversarial model of the handshake; this will demonstrate why the link attributes form an access policy on member nodes. The subsection ends with a cooperative algorithm and performance analysis. For the mitigation, this paper assumes that one-way

Table 2: Notations of the proposed mitigation

ID_i	Categorized identifier of node i.
M_h	Hello message of the routing protocol.
m^{DN}, m^{NN}	Ciphertext of message m that is accessible by the devoted or new node.
K_{id}, K_{cl}	Identity key and cluster key (section 4.2.1).
MK_{inst}	Master key (section 4.2.1).
$Encr(k, m)$	Encryption with symmetric key k.
$Decr(k, m)$	Decryption with symmetric key k.
$Sign(k, m)$	Sign operation with symmetric key k.
$\|\|$, $h(\cdot)$	Concatenation and hash operation.
E_{Enc}, E_{Dec}	Overhead of encryption and decryption.
E_{Sig}, E_{Ver}	Overhead of sign operations.
E_{Hash}, E_{Ret}	Overhead of hash operations and TTP communication.

functions exist ($P \neq NP$) and a negligible downtime of TTP. The notation for the mitigation is presented in Tab. 2.

4.2.1: System Model

The system consists of three roles: devoted nodes, TTPs and member nodes. Devoted nodes operate an authentication key exchange with soliciting nodes. The exchange results in distinct cluster keys K_{cl} for a secure connection between the member and devoted nodes. Mutual communication of devoted nodes is realized with the master key (MK_{inst}).

The TTP provides private identity key K_{id} from member nodes, which is required for sharing the generated K_{cl} with the soliciting node. The TTP stores these keys encrypted with MK_{inst}, however only devoted nodes possess this key.

Member nodes publish their identifier (link attribute) to the network for key generation. Identifiers are then classified into clusters by a function, such as k-means clustering. The detection of anomalies on this identifier is realized by a cooperative algorithm, such as the one in section 4.2.4.

4.2.2: System Working Methodology

The handshake (Fig. 4) begins with a signed hello message M_h, this message should be routed through any devoted node. The devoted node saves the message and waits for a threshold to be reached, which should limit the messages to the TTP with Nagle's algorithm. Then, the TTP retrieves K_{id} and sends this to the devoted node. M_h is validated, and the devoted node generates K_{cl} with a hash function; also known as a key derivation function [27].

The hash function demands the cluster identifier of the new node, an identifier of the devoted node, and MK_{inst} as input. The aim of this function is that each identity depends on metrics such as RSSI and that only the soliciting node has to store K_{cl}, because the devoted node may generate K_{cl} out of piggybacked cluster identifiers. Intra-cluster Sybil attacks are then detected when the piggybacked cluster identifier does not match its value at solicitation or at inconsistencies in link attributes, as will be explained in section 4.2.3.

4.2.3: Adversarial Model

This paper assumes that the adversary has a Probabilistic Polynomial-time Turing Machine (PPT). The additional capabilities of the adversary are then modeled as follows:

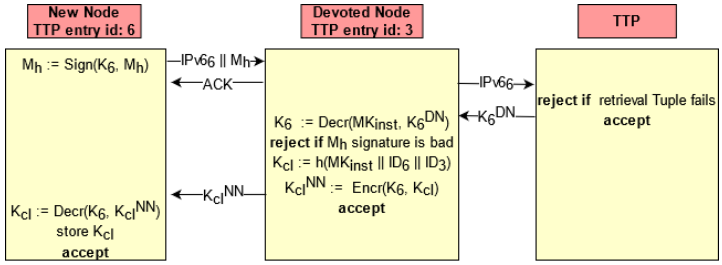

Figure 4: Handshake of devoted nodes.

1. Test the validity of K_{cl}, MK_{inst}, and K_{id}.
2. Offline brute force of K_{cl}, MK_{inst}, and K_{id}.
3. Execute handshakes and retrieve K_{cl}.
4. Execute collision attacks to capture K_{cl} or MK_{inst}.
5. Exploit ciphers-specific vulnerabilities to perform attacks among saturation, and related key attacks.

Remark 1: Capability one is not feasible to assess, as synchronization for Perfect Forward Secrecy (PFS) or any operation mode with nonce-based counters (CTR and CCM) will be computationally intensive, which is also the issue for signed sequence counters messages [21]. However, PFS might be applicable on global repairs via hash chained MK_{inst} when most nodes lost connection.

Remark 2: Capability four can be performed in two methods, either an adversary spoofs a cluster identifier or brute forces the hash function. To mitigate the first issue, one can combine the cryptosystem with a hybrid IDS and choose the identifiers accordingly. However, This paper proposes an extension to prevent this issue in section 4.2.4.

Second, the MK_{inst} can get compromised in $O(2^{hashlen})$ work, especially when the entropy of the hash function is low. Similarly, the adversary could find colliding identifiers with a birthday attack in $O(2^{\frac{hashlen}{2}})$ work, but this requires that the state of the hash function is known at the input of identifiers [27].

Example: Assume that $6BR_{M1}$ and 5_{M2} are in the same situation (Fig. 3) and that the network is divided into clusters. Now, 5_{M2} needs a consistent flow of DIOs and DAOs to claim the identity of node 3. But corruption of DAOs is only feasible when the adversary has all cluster keys of the victims, and because of the pigeon hole principle, the adversary has to perform capability four to capture more than two clusters. Similarly, replay attacks generate incorrect or inconsistent transit path fields and link-layer metrics of the sender.

4.2.4: Link Quality Validation

The identifier in the handshake is based upon a measurement of the joining node, this allows for spoofing. Mitigation of this issue is an extension of the cryptosystem and will work as follows. the PAN coordinator will choose dispersed beacons for the measurement. RSSI data of the beacons and the PAN coordinator indicates the dispersion quality. After this, beacons get isolated in their own cluster.

When a node joins, it has to send any SRM Information Element (IE) on path scope, these messages are propagated

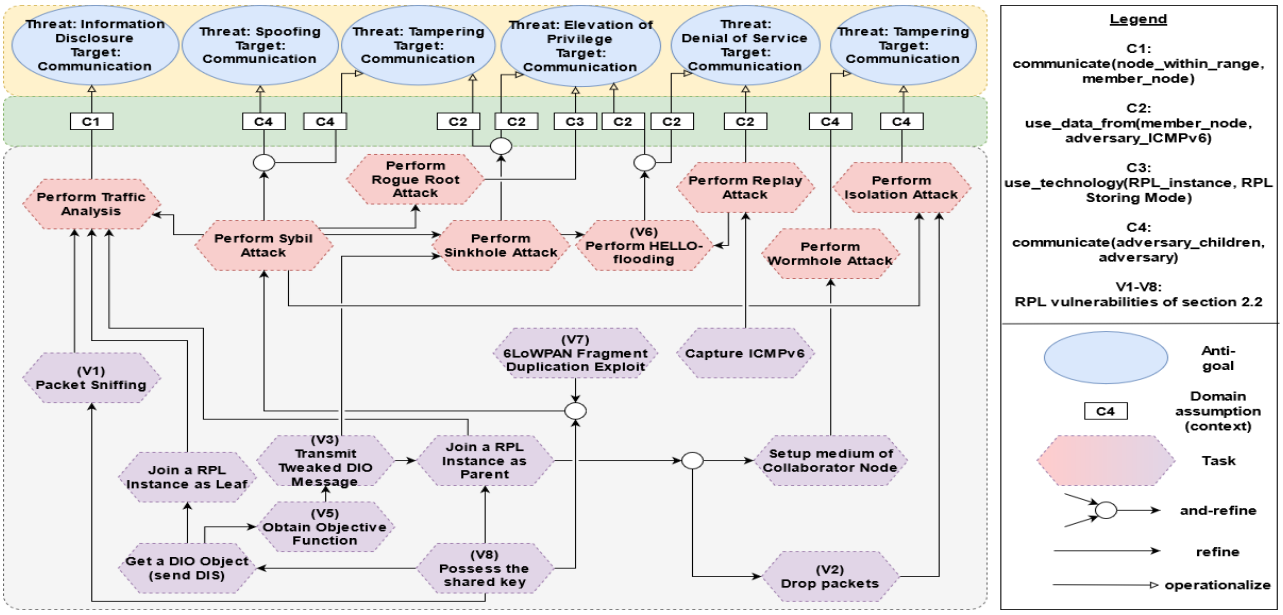

Figure 5: IoT Generic RPL Attack Pattern Model.

to the coordinator [4, p. 55]. Beacons append on this SRM IE with their RSSI on the joining node. Now, the coordinator either starts a new cluster or offers the new node an existing K_{cl} when the node is close to this cluster. Therefore, the coordinator is required to be a devoted node or broker.

4.2.5: Performance Analysis

In the worst case, messages transit to another cluster or through an unstable network. These circumstances affect the performance as follows.

$$3 \cdot E_{Sig} + 3 \cdot E_{Ver} + 2 \cdot E_{Hash} \quad (1)$$

- **Energy consumption:** The energy consumption of intra-cluster transits (Eq. 1) add an overhead of three sign operations at the two devoted nodes that control the clusters and sender. These are then validated at the receiver and two devoted nodes. Also, devoted nodes probably need to derive the two cluster keys before the sign operation. Whereas, the energy consumption of the handshake is defined by Eq. 2. It originates from the key derivation function TTP communication, and symmetric-key operations for K_{cl}, K_{id} and M_h.

$$E_{Sig} + E_{Ver} + E_{Hash} + 2 \cdot E_{Enc} + 2 \cdot E_{Dec} + E_{Ret} \quad (2)$$

- **Transmission time:** The transmission time is affected by the same elements (Eq. 1-2). However, large packet counts of key retrieval requests significantly decrease the Packet Delivery Rate (PDR). The solution is the threshold of section 4.2.2.
- **E2E delay:** The E2E delay increases when the devoted node is not on the most optimal routing path, as member nodes require this path for intra-cluster messages or handshakes. Fortunately, the delay is minimized with lightweight hash that generate the keys, without TTP communication. Also, caching and a better distribution of devoted nodes can minimize this metric.
- **Control message overhead:** the distributed calculation on the SRM IEs is the only operation that adds control message overhead, as each beacon propagates the SRM IE separately.

5 Threat Assessment and Gained Defence for RPL

The two proposals of this paper can best be displayed from the perspective of the adversary. In the attack pattern model (Fig. 5), the adversarial paths demonstrate the attack patterns that may or may not be defended by the cryptosystem of section 4.2. The upcoming subsections explain this with the ODNI cybersecurity framework and Fig. 5. It is assumed that the adversary operates a PPT.

5.1 Information Disclosure

Attack patterns for information disclosure include passive sniffing; SA-2 and SA-3 Sybil attacks; or the capture of messages that were routed through adversaries. One may impact others' privacy with these exploits or prepare a continuation attack with the gained information, as the topology of RPL may be retrieved easily due to the traffic flow (V1). The passive attacks do not have indicators [9], but distinct geographic location, packet loss, and overhead of network control are indicators for Sybil attacks [28].

5.2 Tampering

Corruption of the routing path is trivial with isolation, wormhole, sinkhole, and cloning attacks. However, SA-1 is modeled to tamper content [18]. These attacks achieve this with actions such as packet dropping, IPv6 fragment duplication, and forged link attributes. This forms the consequence or presence of the life-cycle, as corrupt routes can amplify attacks. Sinkholes signify this behaviour. As a result, the sub-

optimal paths embay a decreased quality of service for the targeted subnet during the attack.

5.3 Spoofing

An adversary can spoof legitimate nodes with the information in the DIO messages as there is no validation for the 6LoWPAN addressing [6]. Typically, the adversary deploys this capability to engage the network and prepare for more sophisticated Sybil attacks. This leads to man-in-the-middle attacks or second-order attacks such as the disclosure of authenticators [25, p. 66]. See section 5.1 for Sybil indicators.

5.4 Elevation of Privilege

Elevation of privilege consists of attacks that delude the OF. This can be achieved with rank impersonalization or forged link attributes. The main issue with the OF is that it is calculated by members themself (V3), making it simple to impersonalize the rank. When the tampered rank is adopted by the network the adversary elevates in rank. This threat increases the influence of the adversary over the network and the severity of some threats. For example, sinkholes amplify the information disclosure threat, and rogue root attacks the Denial of Service (DoS) threat. Isolation and rogue root attacks may practice additional measures to hide and thereby maintain the privilege by feigned consistent traffic [7]. An indicator is the greediness of the member for increasing its rank that interferes with OF's objective.

5.5 Denial of Service

DoS attacks can be categorized into two types, temporal and persistent threats [25, p. 73]. In RPL, the adversary aims to waste resources with temporal attacks on consistency such as DIO-flooding, DIO replay attacks, DIS-flooding, and link-layer DoS attacks like CSMA-CA unfairness. Routing attacks are not mapped to this threat as these increase or maintain the performance of the RPL instance [11].

Persistent attacks exist on the routing table but these are specific RPL attacks and out of scope. Therefore, a successful attack can impact the network with an increased amount of control messages or complete network failure, due to table overloads for example.

5.6 Secured Paths of Proposed Mitigation

The mitigation of section 4.2 protects for IP spoofing on other clusters. As modelled, the adversary can still perform the attack when one steals the cluster key by spoofing their identifiers. Although this requires the adversary to know the cluster location, which is unlikely as an outlier, this does add one prerequisite for large-scale Sybil attacks and eavesdropping. The path in Fig. 5 is thus appended with '(V3) transmit tweaked DIO message'. For further mitigation against large-scale Sybil attacks, rogue root attacks (storing mode), and sinkhole attacks, the network requires IDSes on link attributes or the extension of section 4.2.4. The mitigation of the other attacks remains the same.

6 Discussion and Future Work

The Sybil defence of section 4.2 is an example of the RPL authenticated mode, which design was limited by RFC6550 [3]. It regulates an access policy on clusters. As an extension, collaborating beacon nodes make cluster infiltration unfeasible and detectable. The mitigation refrains from synchronization and asymmetric cryptography, which add attack vectors but more importantly performance benefits [5, Tab. 2-3]. Raoof et al. [8] reveal that CBC-MAC is efficient in RPL. Hence, this paper expects that the performance hit is negligible.

Despite its exploratory nature, this study offers limited insight into physical attacks or other environmental-dependent challenges. Moreover, internal devices are assumed to be safe and not colluding with joining nodes. But this is definitely a risk, as it is often deployed in public areas [11]. Therefore, the system may be extended with PFS at global repairs to remove captured cluster keys, however this can be subject to large performance hits. Subsequent research may investigate this hit, the achieved performance or mobility-persistent handoff for the mitigation. The provided formulas can help with this analysis, but this should not be generalized as the performance is dependent on hardware, message size, ciphers, and hash functions [5].

Similarly, the provided attack pattern model does describe the origin and objective of the threats in RPL and this can assist in the outline of new mitigation techniques; and this might be extended to RPL-specific attacks.

Additionally, this paper added an attack pattern on Sybil attacks. The mitigation of section 4.2 is not the only defence, as TRAIL's path validation [29] mitigates root impersonation; and SecTrust [20] the required Sybil node. The same applies for the other mitigations, as there are more mitigation techniques, for instance in [7][19].

6.1 Ethical Considerations

As mentioned in the introduction, IoT application is broad and cannot always provide the security it requires without expensive additional hardware. This paper provides an analysis of the origin and mitigation of these threats in RPL without any (control of) funded companies. This is based upon the attack patterns of [7], [9] and [19]. The discussed vulnerabilities may only be for research-related purposes and strictly remains to be used in this context. The proposed mitigation is well documented and reproducible, due to the description in section 4.2. This mitigation can thus be consumed for further performance investigation or implementation. These continuations should compare existent Sybil defences to this solution. This study did not include this, as one can only compare the behavioural differences with the design, which is already done in [7]. Any vulnerabilities of the system are originated and referred to existent mitigations in section 2.3. Whilst, the exploits are only briefly described and modelled, to refrain from malicious use cases. Additionally, section 5 provides a proper attack pattern model implementation of two systematic methods and with a proper argumentation of the paths. This model offers an excellent overview for future mitigation techniques in RPL on generic attacks. Therefore, the paper could only be adopted in further research with limited consequences.

7 Conclusion

This paper aimed to analyze and mitigate IoT generic security threats of RPL. The first contribution proposed a mitigation on the rogue root attack. This attack depends on Sybil attacks, allowing adversaries to perform amplified (routing) attacks. The proposed Sybil defence ensures that the identity is dependent on SRM IE, while it most likely preserves efficiency on transits. Subsequently, external source measurement can substantiate spoofed SRM IEs.

The second contribution demonstrated these threats on an adversarial perspective using the operational capabilities, objectives, and life-cycle of the adversary. This analysis has provided a deeper insight into the origin and use case of RPL attacks; and it may well determine the covered attack vectors of the proposed and future mitigations.

Acknowledgment

This research is supported by a research group of five peers including Ruben Stenhuis. The authors would like to thank Pieter Tolsma for cooperating with the excogitation on RPL exploits and Fimme Neeleman for introducing the performance metrics of the performance analysis.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015, doi: 10.1109/COMST.2015.2444095.

[2] H. S. Kim, J. Ko, D. E. Culler, and J. Paek, "Challenging the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL): A Survey," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 4, pp. 2502–2525, 2017, doi: 10.1109/COMST.2017.2751617.

[3] T. Winter et al., "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," 2012. [Online]. Available: https://tools.ietf.org/html/rfc6550. [Accessed: Jun. 14, 2020].

[4] IEEE P802.15 Working Group, "IEEE Standard for Low-Rate Wireless Networks," IEEE Std 802.15.4-2020, 2020, doi: 10.1109/IEEESTD.2020.914469.

[5] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," *J. Ambient Intell. Humaniz. Comput.*, vol. 1, no. 1, pp. 1–18, 2017, doi: 10.1007/s12652-017-0494-4.

[6] I. Butun, P. Osterberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 1, pp. 616-644, 2020, doi: 10.1109/COMST.2019.2953364.

[7] A. Raoof, A. Matrawy, and C. H. Lung, "Routing Attacks and Mitigation Methods for RPL-Based Internet of Things," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1582-1606, 2019, doi: 10.1109/COMST.2018.2885894.

[8] A. Raoof, A. Matrawy, and C. H. Lung, "Enhancing Routing Security in IoT: Performance Evaluation of RPL's Secure Mode under Attacks," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11536–11546, 2020, doi: 10.1109/JIOT.2020.3022276.

[9] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in RPL-based internet of things," *Int. J. Netw. Secur.*, vol. 18, no. 3, pp. 459–473, 2016.

[10] I. Alsmadi, R. Burdwell, A. Aleroud , A. Wahbeh, M. Al-Qudah, and A. Al-Omari, "Introduction to Information Security," in *Practical Information Security*, Springer International Publishing, pp.1-16, 2018.

[11] I. Tomić and J. A. McCann, "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols," *IEEE Internet Things Journal*, vol. 4, no. 6, pp. 1910–1923, 2017, doi: 10.1109/JIOT.2017.2749883.

[12] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko, "The Trickle Algorithm," 2011. [Online]. Available: https://tools.ietf.org/html/rfc6206. [Accessed: Jun. 14, 2020].

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

[14] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, "6LoWPAN fragmentation attacks and mitigation mechanisms," *WiSec 2013 - Proc. 6th ACM Conf. Secur. Priv. Wirel. Mob. Networks*, pp. 55–66, 2013, doi: 10.1145/2462096.2462107.

[15] G. Glissa, A. Rachedi, and A. Meddeb, "A Secure Routing Protocol Based on RPL for Internet of Things," in *2016 IEEE Global Communications Conference (GLOBECOM)*, 2016, pp. 1–7, doi: 10.1109/GLOCOM.2016.7841543.

[16] M. N. Napiah, M. Y. I. Bin Idris, R. Ramli, and I. Ahmedy, "Compression Header Analyzer Intrusion Detection System (CHA - IDS) for 6LoWPAN Communication Protocol," *IEEE Access*, vol. 6, pp. 16623–16638, 2018, doi: 10.1109/ACCESS.2018.2798626.

[17] A. Verma and V. Ranga, "Mitigation of DIS flooding attacks in RPL-based 6LoWPAN networks," *Trans. Emerg. Telecommun. Technol.*, vol. 31, no. 2, 2020, doi: 10.1002/ett.3802.

[18] 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, doi: 10.1016/j.adhoc.2013.04.014.

[19] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," *IEEE Internet Things Journal*, vol. 1, no. 5, pp. 372–383, 2014, doi: 10.1109/JIOT.2014.2344013.

[20] D. Airehrour, J. A. Gutierrez, and S. K. Ray, "SecTrust-RPL: A secure trust-aware RPL routing protocol

for Internet of Things," *Future Generation Computer Systems*, vol. 93, pp. 860–876, 2019, doi: 10.1016/j.future.2018.03.021.

[21] P. Perazzo, C. Vallati, A. Arena, G. Anastasi, and G. Dini, "An Implementation and Evaluation of the Security Features of RPL," In *International Conference on Ad-hoc, Mobile, and Wireless Networks*, 2017, pp. 63–76, doi: 10.1007/9783319679105.

[22] J. Tripathi, J. C. de Oliveira, and J. P. Vasseur, "Performance Evaluation of the Routing Protocol for Low-Power and Lossy Networks (RPL)," 2012. [Online]. Available: https://tools.ietf.org/html/rfc6687. [Accessed: Jun. 21, 2020].

[23] T. Li, E. Paja, J. Mylopoulos, J. Horkoff, and K. Beckers, "Security attack analysis using attack patterns," In *2016 IEEE Tenth International Conference on Research Challenges in Information Science*, 2016, pp.1-13, doi: 10.1109/RCIS.2016.7549303.

[24] Office of the Director of National Intelligence, "Cyber Threat Framework," *Office of the Director of National Intelligence*. [Online]. Available: https://www.odni.gov/index.php/cyber-threat-framework. [Accessed: Jun. 14, 2020].

[25] Shostack, A., "Threat Modeling, Designing for Security," *John Wiley & Sons*, 2014.

[26] J. Hui, JP. Vasseur, D. Culler, and V. Manral, "An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)," 2012. [Online]. Available: https://tools.ietf.org/html/rfc6554. [Accessed: Jun. 14, 2020].

[27] C. Adams, G. Kramer, S. Mister, and R. Zuccherato, "On the security of key derivation functions," In *International Conference on Information Security*, 2004, pp. 134-145, doi: 10.1007/978-3-540-30144-8_12.

[28] F. Medjek, D. Tandjaoui, M. R. Abdmeziem, and N. Djedjig, "Analytical evaluation of the impacts of Sybil attacks against RPL under mobility," *12th Int. Symp. Program*. Syst. ISPS 2015, pp. 13–21, 2015, doi: 10.1109/ISPS.2015.7244960.

[29] H. Perrey, M. Landsmann, O. Ugus, T. C. Schmidt, and M. Wählisch, "TRAIL: Topology Authentication in RPL," 2013 [Online]. Available: http://arxiv.org/abs/1312.0984. [Accessed: Jun. 14, 2020].