# A Trust-based Intrusion Detection System for Mobile RPL Based Networks

Faiza Medjek*, Djamel Tandjaoui†, Imed Romdhani‡, Nabil Djedjig§
*†§Research Center on Scientific and Technical Information - CERIST - Algiers, Algeria
*§University Abderrahamane MIRA - Bejaia, Algeria
‡Edinburgh Napier University, School of Computing, 10 Colinton Road, EH10 5DT, Edinburgh, UK

***Abstract*—Successful deployment of Low power and Lossy Networks (LLNs) requires self-organising, self-configuring, security, and mobility support. However, these characteristics can be exploited to perform security attacks against the Routing Protocol for Low-Power and Lossy Networks (RPL). In this paper, we address the lack of strong identity and security mechanisms in RPL. We first demonstrate by simulation the impact of Sybil-Mobile attack, namely SybM, on RPL with respect to control overhead, packet delivery and energy consumption. Then, we introduce a new Intrusion Detection System (IDS) scheme for RPL, named Trust-based IDS (T-IDS). T-IDS is a distributed, cooperative and hierarchical trust-based IDS, which can detect novel intrusions by comparing network behaviour deviations. In T-IDS, each node is considered as monitoring node and collaborates with his peers to detect intrusions and report them to a 6LoWPAN Border Router (6BR). In our solution, we introduced a new timer and minor extensions to RPL messages format to deal with mobility, identity and multicast issues. In addition, each node is equipped with a Trusted Platform Module co-processor to handle identification and off-load security related computation and storage.**

***Index Terms*—RPL security, Sybil attack, Routing security, Intrusion Detection System, IoT.**

## I. Introduction

Low power and Lossy Networks (LLNs) are emerging networks that will change human life with a range of real-life applications, such as smart-health, smart-home, smart-grid, and smart-transport. LLNs are composed of large number of smart, loosely, resource constrained and IP-enabled interconnected objects [1]. To cope with the specific requirements of LLNs, the Internet Engineering Task Force (IETF) Routing Over Low power and Lossy networks (ROLL) Working Group introduced and standardized the Routing Protocol for Low power and Lossy Networks (RPL) [2]. RPL deals with the constrained nature of such networks by considering the limited capabilities of LLNs with respect to energy power and computational. It defines some security and fault tolerance mechanisms, such as control messages encryption, local and global repairs, and loops detection and avoidance. The cryptographic security mechanisms can counter external attackers. However, an internal attacker can have valid security keys and credentials, and then bypass these mechanisms and trigger attacks against its own network.

In RPL, objects are connected wirelessly. From identity point of view, each object in RPL has an IPv6 address as identifier through stateless or stateful configuration. In addition, an internal attacker can exploit self-healing, self-maintenance and self-organizing capabilities of RPL to trigger several attacks such as selective forwarding, rank, sinkhole and blackhole, local repair, and DIS attacks [3]. One of the most serious threats against RPL is Sybil attack [4] [5]. In this attack, the same physical node illegitimately claims multiple logical identities in order to disrupt a routing protocol, overload the network with fake control messages, and thus, interrupt the network stability. Sybil attacks are widely treated in the literature. Nevertheless, to the best of our knowledge, there are few works that address Sybil attack on RPL without providing in-depth evaluation which is worth to be investigated.

As reported in the literature [3] [6] [7] [8], once an intruder gains access to the network, it can bring several damages. In this context, Intrusion Detection Systems (IDSs) are needed. Sherasiya et al. surveyed existing IDSs for IoT [9]. According to the detection methods, an IDS can be signature-based, anomaly-based or specification-based. An IDS system can be classified either as host-based, network-based or hybrid. Some IDSs have been proposed to deal with some RPL attacks. For instance, Anhtuan et al [10] proposed a specification-based IDS idea for securing RPL against topology attacks. In this approach, nodes monitor routing information conveyed in control messages to detect attackers. In [11] and [12], authors proposed an IDS to detect DoS attacks in 6LoWPAN networks. The proposed IDS has been integrated into the network framework ebbits developed within an EU FP7 project, where probe nodes located in the network send periodically the 6LoWPANs traffic through wired connection to the IDS. The IDS collaborates with a DoS protection manager to confirm the attack using jamming information. Nevertheless, this solution targets only DoS attack and is not compatible to general network architecture. Raza et al. [13] proposed SVELTE, a hybrid IDS for IP-based IoT where IDS modules were placed both in the 6BR and in constrained nodes. SVELTE targets spoofed or altered information, sinkhole, and selective-forwarding attacks. Furthermore, authors proposed a distributed mini-firewall to protect the network against external attackers. In [14], authors introduced a novel attack against RPL, namely, Routing Choice Intrusion. In this attack, an intruder learns RPLs routing rules, captures control messages and broadcasts fake ones. To counter this attack, authors proposed a stand-alone specification-based IDS with distributed Monitoring Nodes (MNs). In this IDS the detection data is network-based where in each MN is implemented a Finite-State-Machine (FSM) to detect RPL's abnormal behaviors. However, they relied their analysis on unrealistic assumptions specifically the stable state of LLN environment. In [15], Thanigaivelan et al. presented a cross-layer anomaly detection system for IoT. The proposed IDS is composed of a monitoring and grading subsystem (MGSS) and a reporting subsystem (RSS) that operate in network layer, and an isolation subsystem (ISS) that operates in link layer. ISS is used to avoid packets from abnormal detected nodes. Anomalies and network changes are communicated from the node to the edge-router through subsequent parents. The edge-router analyses reports and makes a decision. However, parents themselves can be compromised. From the other side, anomaly-based IDSs are very costly for resource-constrained objects [9]. In [16], a distributed IDS to identify wormhole attacks is proposed. The IDS uses nodes location. Each node uses the rank information from RPL control messages to estimate the relative distance to the Border Router (BR) and identify suspicious rank values. Thus, the rank value is compared with that of the neighbors; if the discrepancy exceeds a threshold value, it signals that a wormhole might exist. Nevertheless, the authors used the hop-count to calculate the rank and detect the attack. They should prove that their approach is effective if the rank is calculated differently (e.g. using ETX (Expected Transmission Count) objective function).

Each of the aforementioned IDS has some advantages and disadvantages. The main weakness of the majority of proposed IDSs is the lack of mobility and secure identity that can be exploited by SybM attack [6]. In this paper, we introduce a new cross-layer trust-based IDS scheme that copes with mobility and identity issues to detect attacks against RPL networks.

The rest of this paper is organized as follows. Section II presents an overview of RPL . Section III presents SybM attack and simulation results. Section IV depicts our proposed IDS: T-IDS. Section V describes how T-IDS can be used to counter SybM attack. Finally, Section VI concludes the paper and gives future works.

## II. RPL OVERVIEW

RPL [2] organizes a logical representation of the network topology as a Directed Acyclic Graph (DAG). The DAG is composed of one or more Destination Oriented DAGs (DODAGs) through which data packets are routed. Each DODAG is a tree, which connects the nodes and the 6LoWPAN DODAG-root known as 6LoWPAN Border Router (6BR). The 6BR is connected to the Internet, to other 6BRs, and to a Backbone Router (BR) or Repository via a backbone link. For the construction and the maintenance of the network topology, RPL introduces specific ICMPv6 (Internet Control Message Protocol for IPv6) messages (DIO, DIS, and DAO) and a Trickle mechanism. The DODAG Information Object (DIO) message conveys the information that allow nodes to get DODAG configuration parameters. The DODAG Information Solicitation (DIS) message is sent by a new node wishing to join a DODAG. It allows nodes to request DIO messages from their neighbors. The DODAG Destination Advertisement Object (DAO) message is used to maintain downward routes. When a node joins a DODAG, it advertises a DAO message for its neighbors to update their routing tables. To support routing optimization and calculate best paths, an Objective Function (OF) and node and/or link related metrics and constraints are used [17] [18].

## III. SYBIL-MOBILE ATTACK (SYBM) SIMULATION

In this section we model SybM attacks model and evaluate RPL performances by using Cooja Contiki-2.7 simulator [19].

In SybM attack, a malicious node exploits RPL operations and the weakness of RPL to handle mobility and identity to trigger the attack. Nodes do not have significant defence resistance. Hence, some mobile nodes can be compromised by an attacker, which will reprogram and redeploy them into the network. Therefore, even in the case of a secure RPL (i.e. secure ICMPv6 messages), the compromised nodes can use the pre-configured group key [2], and can normally participate in the network operations. Each mobile-compromised-node can automatically generate new IPv6 addresses [20] [21]. The new IPv6 addresses are known as Sybil identities or Sybil nodes. In SybM attack, the Sybil nodes operate independently and do not cooperate during the attack. Each node is initially placed at a random location and sends periodically data packets to the border router (6BR). Malicious nodes pause for a period of time behaving the same way as honest nodes (sending data packets to the 6BR). Indeed, each adversary involves a set of its Sybil nodes alternately and periodically, while moving across the network. Thus, after the pause time, malicious nodes choose a new location across neighboring nodes and towards the 6BR, and move within the same 6BR prefix scope boundary. When malicious nodes reach their new locations, they repeat the same process before moving again. Upon moving, malicious nodes broadcast DIS messages within the network. In a micro-mobility scenario, IPv6 address of the node is more likely to remain unchanged. Nevertheless, as in SybM mobile nodes are malicious, they broadcast DIS messages using new IPv6 addresses corresponding to new Sybil identities. The number of Sybil identities corresponds to the number of time an attacker moves. As a result, neighborhood connectivity will change, and consequently more DIO messages will be exchanged to update the network topology.

We conducted a set of simulations using Cooja Contiki-2.7. We placed randomly 50 TelosB nodes in a $300x300m^2$ area with a transmission range of 50m. We placed one 6BR in the centre and 49 nodes around the 6BR. We increased the number of dynamic nodes from 0 (i.e. case of static network), 2, 4, 6, 8, to 10, while the number of Sybil identities per attacker is increased from 1, 3, to 5. Every node sends packets to the 6BR at the rate of 1 packet every 10 seconds. Simulations were executed for a duration of 330 seconds. We set node mobility using the Cooja-Mobility-Plugin. In order to manage Sybil identities, we relied on Preiss et al. work [21]. We set two scenarios:

1) First scenario: a network with no attacker and no mobility.
2) Second scenario: SybM attack scenario. We varied the number of Sybil mobile attacker from 2, 4, 6, 8, to 10 attackers. Likewise, the number of Sybil identities per attacker increases from 1, 3, to 5 (1SybM, 3SybM and 5SybM, respectively).

Fig. 1, Fig. 2, and Fig. 3 demonstrate the impact of SybM attack on RPL performances with respect to control overhead, energy cost and Packet Delivery Ratio (PDR). From Fig. 1, we notice that the extra control overhead of SybM attack with one Sybil node per attacker (1SybM) is approximately about 6% in the case of 2 moving attackers, and increases until reaching 32 % in the case of 10 moving attackers. Similarly, for SybM attack with 3 Sybil nodes per attacker (3SybM), the extra overhead is approximately about 24% in the case of 2 moving attackers, and increases until reaching 66% in the case of 10 moving attackers. For SybM attack with 5 Sybil nodes per attacker (5SybM), the extra overhead is approximately about 45% in the case of 2 moving attackers, and increases until reaching 133% in the case of 10 moving attackers. Hence, by increasing the number of mobile attackers, the overhead increases steadily in the case of 1SybM and 3SybM attacks, while it increases considerably in the case of 5SybM attack until being doubled. In addition, it is seen clearly that by increasing the number of Sybil mobile nodes within the network, the overhead increases significantly. In fact, the extra overhead form 3SybM is 2 times the one from 1SybM (in the case of 4 and 6 moving attackers the overhead almost doubles). Also, the extra overhead form 5SybM is almost 2,5 times the one from 3SybM (in the case of 8 and 10 attackers the overhead exceeds the double). These results are due to the fact that attackers stimulate honest nodes to send control messages more frequently. As attackers move towards the 6BR, more nodes are affected.

It is clear from Fig. 2 and Fig. 3 that the energy cost increases while Packet Delivery Ratio (PDR) is reduced remarkably in presence of SybM attack, as the number of attackers and Sybil nodes increase. This could be attributed to the growth of affected nodes within the network. The increase of the number of exchanged control messages and the probability of collisions, will in turn increases the power consumption. In addition, PDR is more important in SybM attack because of the weakness of RPL's performance to handle mobility.

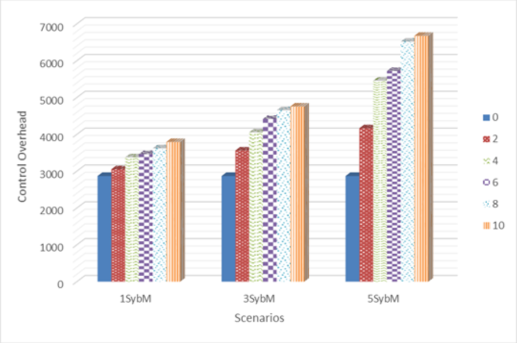

Fig. 1: Control Overhead

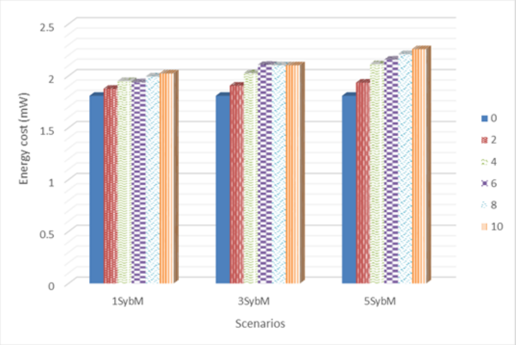

Fig. 2: Energy Cost

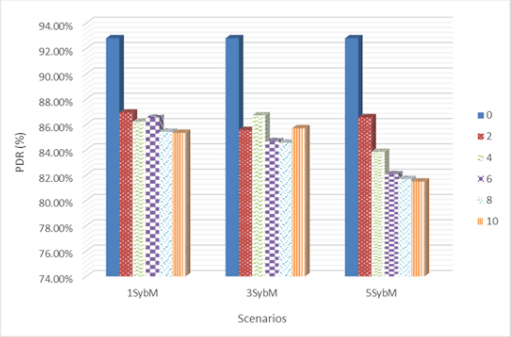

Fig. 3: Packet Delivery Ratio

## IV. Trust-based IDS Solution: T-IDS

The impacts caused by RPL attacks and especially the SybM ones require developing new mitigating mechanisms. Different approaches have been proposed to address Sybil attacks issue [22]. However, these solutions are not desirable for several reasons. Some of the proposed solutions are energy costly, or limited to some types of networks (Sensor Networks or Ad hoc Networks), or primarily designed for non-mobile nodes. In the context of IoT, other approaches have been proposed in [23]. What makes SybM attack more difficult to detect by existing approaches is the fact that malicious nodes intend to use one of their identities (IP addresses) at a time in one location. Hence, one Sybil identity is seen as one legitimate physical node. To overcome this type of attack, we propose a distributed, cooperative and hierarchical trust-based IDS architecture that integrates three cooperative modules: IdentityMod, MobilityMod and IDSMod as illustrated in Fig.5.

Our T-IDS system is a hybrid-IDS because both the 6BR and in-network nodes collaborate in defending against internal attackers. Furthermore, T-IDS is trust-based for two reasons. First, a Trusted Platform Module is integrated to each in-network node. Second, nodes rely on a new collaborative trust metric evaluation when routing [24]. In the following sections we introduce the hybrid trust-based IDS actors and components and demonstrate how they can be used.

### A. Contributions

1) RPL is based on IPv6 Neighbor Discovery mechanism. Hence, it relies on multicast operations to setup the network topology. In this context, a simple multicast DIS message can affect the whole network (DIS attack). The problem associated with multicast NS (Neighbor Solicitation) and NA (Neighbor Advertisement) messages are more frequent in large-scale radio environments with mobile devices which exhibit intermittent access patterns and short-lived IPv6 addresses [25]. The works proposed in [25] enables to lower the rate of RA (Router Advertisement) messages by extending the Address Registration Option (ARO), but does not solve the multicast associated problems. In our solution (T-IDS), RPL itself will be adapted to reduce the response to multicast messages in the case of mobile nodes. This is done by using two reserved bytes in the DIO message as Maximum Response Delay such as in RFC 3810 [26]. Fig. 4 depicts the new DIO message format. Details on how a node uses Maximum Response Delay field are presented in Section C-3).

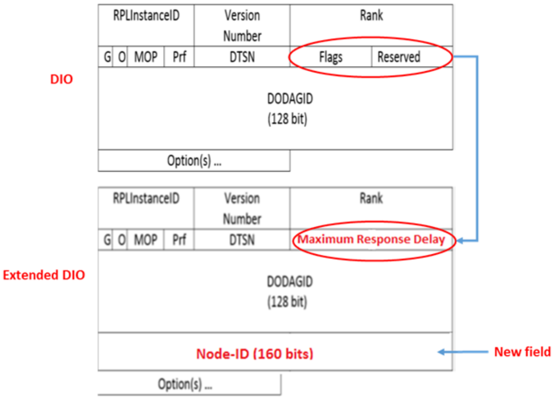

Fig. 4: New DIO message format

2) RPL relies on IPv6 addresses to identify nodes within the network. Hence, the same node can change its IPv6 address (Sybil attack) and try to join the network using the new address as a new identity. In T-IDS we propose a centralized beforehand registration of nodes. Each node has an associated unique identifier which will be conveyed within control messages with its IPv6 address (See Fig. 4). The identifier will be used by the IDS modules to detect and report intruders. This is inline with IETF approach to introduce registrars.
3) In trust-based RPL scheme [24], the in-network nodes collaborate to detect intruders using a trust-based routing scheme. In T-IDS, a mitigation method is induced as a third line of defence. The IDS reacts in a corrective action. This is done by executing trust-based RPL where nodes avoid malicious (suspicious) nodes when selecting their routing path. In T-IDS, trust calculation in trust-based RPL is enhanced by adding a new trust component: Mobility.

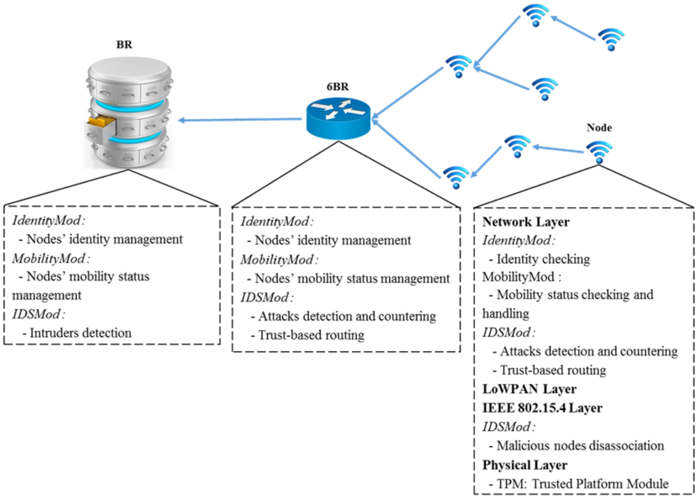
BR
6BR
Node
IdentityMod:
- Nodes' identity management
MobilityMod:
- Nodes' mobility status management
IDSMod:
- Intruders detection
IdentityMod:
- Nodes' identity management
MobilityMod:
- Nodes' mobility status management
IDSMod:
- Attacks detection and countering
- Trust-based routing
Network Layer
IdentityMod:
- Identity checking
MobilityMod :
- Mobility status checking and handling
IDSMod:
- Attacks detection and countering
- Trust-based routing
LoWPAN Layer
IEEE 802.15.4 Layer
IDSMod:
- Malicious nodes disassociation
Physical Layer
- TPM: Trusted Platform Module

Fig. 5: T-IDS Architecture

### B. T-IDS Actors

T-IDS is composed of a centralized Backbone Router (BR) or Repository that federates multiple 6LoWPAN sub-networks. The BR may be part of anycast group for redundancy issue. Each 6LoWPAN sub-network is attached to the BR via a 6LoWPAN Border Router (6BR). 6BRs are responsible of monitoring the in-network nodes and make the global intrusion detection decisions by associating and aggregating intrusion alerts from in-network nodes. Each in-network node monitors in a trusted-collaborative way its neighbors to detect intrusions. The BR and the 6BR are both supposed to be trusted entities. Fig. 6, Fig. 7, and Fig. 8 depict BR, 6BR and in-network nodes operations, respectively.

*1) Backbone Router (BR):* maintains the list of all Network Nodes (NNs) and their respective states. The BR handles the list of nodes authorized to access the network. In NNs, to each node is associated a TPM-ID, a Node-ID associated to the TPM-ID, the Node-Status flag (Mobile, Static), and the 6BR prefix associated to the node after deployment. When a node wants to join the network, it must be first registered at the NNs list. In addition, the BR maintains a list of potential MAlicious Nodes (MAN) for all 6BR sub-networks.

*2) 6LoWPAN Border Router (6BR):* maintains three dynamic lists: the first list contains 6BR Area Nodes (6BRAN) within the 6BR's IPv6 prefix. 6BRAN is elaborated and updated by the BR and transferred to 6BR in a secure channel. The second one contains MObile Nodes (MON) and the third list contains the MAlicious Nodes (MAN). The 6BR is responsible of setting the Maximum Response Delay field in the DIO message.

*3) Monitoring Nodes (MNs):* each in-network node is a MN by default. MNs maintain a list of SUspicious Nodes (SUN) and a list of malicious nodes (MAN). They also keep a copy of MON list elaborated by 6BR. The lists are stored in the TPM. It is assumed that a node is already registered with one 6BR in the 6BRAN list.

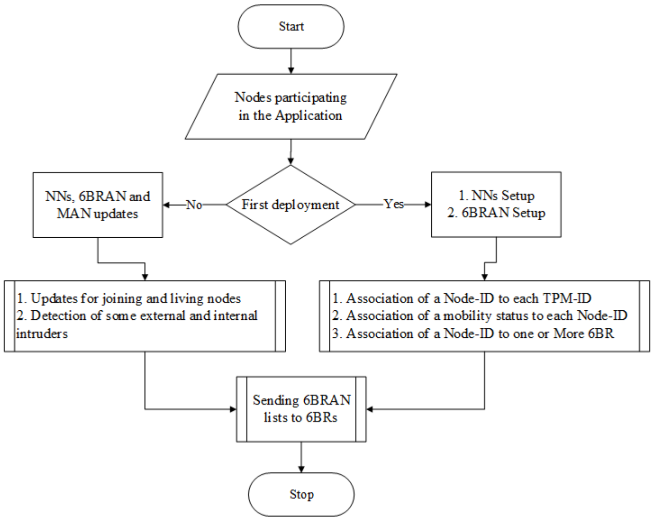
Start
Nodes participating in the Application
First deployment
No
Yes
NNs, 6BRAN and MAN updates
1. NNs Setup
2. 6BRAN Setup
1. Updates for joining and living nodes
2. Detection of some external and internal intruders
1. Association of a Node-ID to each TPM-ID
2. Association of a mobility status to each Node-ID
3. Association of a Node-ID to one or More 6BR
Sending 6BRAN lists to 6BRs
Stop

Fig. 6: BR Operations

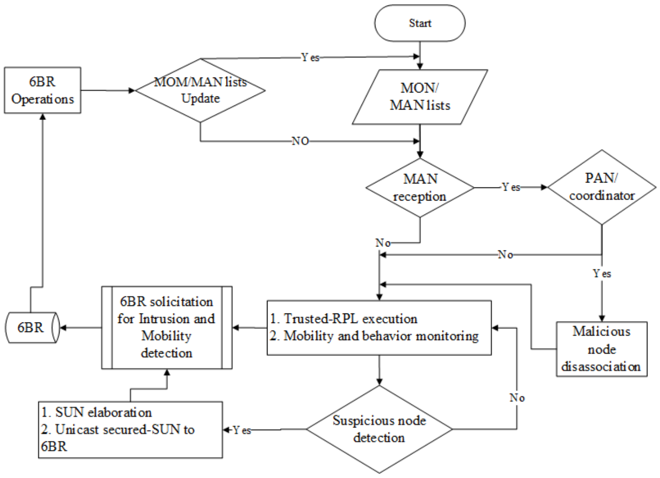
Start
6BR Operations
MOM/MAN lists Update
Yes
NO
MON/ MAN lists
MAN reception
Yes
PAN/ coordinator
No
No
Yes
Malicious node disassociation
6BR
6BR solicitation for Intrusion and Mobility detection
1. Trusted-RPL execution
2. Mobility and behavior monitoring
No
1. SUN elaboration
2. Unicast secured-SUN to 6BR
Yes
Suspicious node detection

Fig. 8: In-network nodes Operations

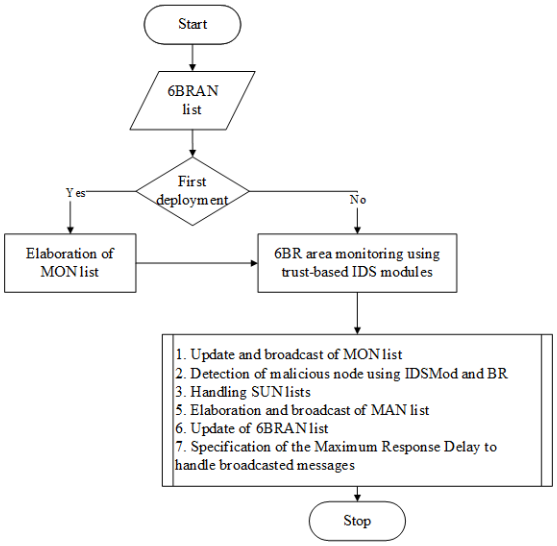
Start
6BRAN list
First deployment
Yes
No
Elaboration of MON list
6BR area monitoring using trust-based IDS modules
1. Update and broadcast of MON list
2. Detection of malicious node using IDSMod and BR
3. Handling SUN lists
5. Elaboration and broadcast of MAN list
6. Update of 6BRAN list
7. Specification of the Maximum Response Delay to handle broadcasted messages
Stop

Fig. 7: 6BR Operations

### C. T-IDS Modules

*1) Module for identity management (IdentityMod):* The Identity Module (IdentityMod) is used to control access to the network. Each node which is part of the network or try to join the network must have a unique identity, to limit exposure of the network to attacks from unauthorized nodes. To handle identity issue and off-load security feature, each node uses a Trusted Platform Module (TPM), which provides uniquely unforgeable identity for the node (TPM-ID). TPM is a cryptographic co-processor chip known to be used in building hardware support identification, storing security parameters, and handling cryptography calculation. In our solution, manufacturers are required to equip each device with a TPM chip before factory. One component of a TPM is the Endorsement Key (EK); a public-private RSA key pair created during manufacture. The public EK value will not change during the TPM's lifetime and it represents the TPM-ID (Node-ID). Besides EK, each node within the network uses two different symmetric keys: a Long Term Key (LSK) shared with the 6BR, and a Group-Key (GK) shared between all nodes. All symmetric keys are stored in the TPM chip. GK will be used to secure RPL's control messages. If an insider attacker compromises one node it gains access to the GK, and the security of the whole network is compromised. Hence, LSK will be used to send securely data packets and security related messages to the 6BR. The authenticity and integrity of exchanged messages between the 6BR and a particular node can be secured using lightweight IPsec with LSK [27] .

After nodes' deployment, and before starting the construction of the RPL topology, the BR uses IdentityMod to set-up 6BRAN list of each 6BR within the network. This list will be used to control access and authenticate nodes. To authenticate a node at any stage of the network execution, RPL control messages should convey besides the IPv6 address of the node, its unique identifier. In other word, the identifier of each node has to be embedded in 6LoWPAN packets. In addition, each node records the identifier associated to the IPv6 address in its routing table. In this way, even if nodes autonomously calculate their IP addresses, while moving, they could be authenticated using their identifier Node-ID. Once an attack is detected, the responsible nodes will be known. If a node detects that another node is malicious, it updates SUN list with the identity of the suspicious node and sends it securely to the 6BR using LSK.

The BR uses IdentityMod to associate to each TPM-ID 20 bytes long Node-ID. Thus, the Node-ID is a cryptography-based unique representation of a node derived from the a TPM-ID. For RPL networks, the MAC Maximum Transmission Unit (MTU) size is about 127 bytes. And the size of the TPM-ID varies from 64 to 254 bytes depending on manufacturing. To handle control overhead issue caused by a large number of fragments for the same message, we propose to shorten the size of the node identifier from 64-254 bytes to 20 bytes long using the SHA1 hash function. In our solution, we propose to extend DIO, DIS and DAO control messages with 20 Bytes before Options Object to carry Node-ID [2]. Fig. 4 depicts how DIO is extended. DIS and DAO are extended in the same way.

*2) Module for mobility management (MobilityMod):* Mobility is also handled through a hierarchical manner with the collaboration of BR, 6BR and in-network nodes. MobilityMod is used by the different actors to maintain the state of the network regarding mobile nodes. In fact, 6BRAN contains the mobility status of each node. Upon receiving 6BRAN from the BR, the 6BR defines a new list by keeping only the mobile nodes; MON: MObile Nodes. After the construction of RPL, the BR broadcasts MON to all nodes. Hence, mobile nodes are known by all in-network nodes, and thus using its identity (Node-ID) the presence of the mobile node is determined by neighboring nodes. In other words, when a node constructs its routing table, it uses the MON list to check and monitor the mobility status of each neighboring node. From this point, if any moving node sends DIS message using a new IPv6 address, its neighbors can detect it as suspicious node (i.e. same Node-ID with different IPv6 address) and add it to SUN lists. Furthermore, if any moving node sends DIS message using a new Node-ID and a new IPv6 address, its neighbors can check MON list. If the node does not exist on MON list, it will be detected as suspicious (i.e. node not registered within 6BRAN) and add it to SUN lists. In addition to MON list, and to handle mobility, each node verifies the RSSI (Received Signal Strength Indication) of its respective neighbors. If the RSSI value of a monitored node has degraded or has been null, this could be due to the fact that it is a malicious mobile node that has not been added in the MON list. In all cases, the monitoring node considers that node as suspicious, updates SUN list and unicast it to the 6BR using LSK.

If a mobile node sends packets with identifier not known by the 6BR (not present in 6BRAN list); the 6BR sends a request to the BR to ask if the new mobile node belongs to the network. If the mobile node is a legitimate node, the BR replies by sending an updated 6BRAN list containing the identity of this node. However, if the node is not previously registered in the NNs list, the BR informs the 6BR that the node is an intruder. If there is any node that joins or leaves the 6BR's 6loWPAN, the 6BR will update MON list, and triggers a global repair with the new MON list. In the same way, if there are any intruders, the 6BR will update MAN list and broadcasts it to its 6LoWPAN's nodes.

MobilityMod can be used to obtain the localization of the mobile malicious node in the network. This can be done by gathering mobility information from the neighbor list (routing table) of different static nodes.

*3) Module for intrusion detection (IDSMod):* To detect attacks, each time the IDSMod will query the IdentityMod and the MobilityMod to verify if the node belongs to the network and if it is a mobile node. From one side, in RPL, there is no mechanism for nodes to monitor the behavior of their neighbors. From the other side, attackers generally focus on specific behaviors and repeat them in high or low rate. Consequently, with minimal knowledge, and by observing and collaborating, nodes can detect misbehaving nodes. In this context, we propose to consider some appending for RPL to be used in IDSMod:

1) The first one consists on the integration of the new trust-based RPL scheme proposed in our previous work for attacks countering [24]. In T-IDS, an enhancement of trust-based RPL is used in collaboration with IdentityMod, MobilityMod and IDSMod to detect misbehaving nodes. In trust-based RPL scheme [24], nodes within the network collaborate to detect malicious nodes according to specification-based behaviors. Periodically, each node calculates trust values of its one hop neighbors; $\mathrm{ERNT_{ij}}(t)$. Moreover, the node receives trust values evaluations of other nodes from its neighbors and aggregates all received and calculated trust values. The final trust values represent the result of collaboration of different participating nodes. In IDSMod, if a trust value of a node is less than a threshold, the node identity will be added to SUN list, the list will be encrypted (using LSK), and sent in unicast to the 6BR. Upon receiving SUN lists, the 6BR processes them and creates a new list containing MAlicious nodes; MAN. MAN list will be then broadcasted to all nodes. In our IDSMod solution, we propose to add a new trust component namely mobility when calculating trust values as follow:

$$\begin{cases} ERNT_{ij}(t) = w_1 ERNT_{ij}^{honesty}(t) \\ \qquad\qquad\quad +w_2 ERNT_{ij}^{energy}(t) \\ \qquad\qquad\quad +w_3 ERNT_{ij}^{mobility}(t) \\ \mathrm{w}_1 + \mathrm{w}_2 + \mathrm{w}_3 = 1 \end{cases} \tag{1}$$

Where *ERNT* is the acronym for Extended RPL Node Trustworthiness, represents the trust value evaluation of node *i* for its neighbor *j* at time *t*, and takes values between 0 and 1. $\mathrm{w}_1$, $\mathrm{w}_2$ and $\mathrm{w}_3$ are weights associated respectively to the three trust components: honesty, energy and mobility. $\mathrm{ERNT_{ij}}^{honesty}(t)$ is calculated by IDSMod, whilst $\mathrm{ERNT_{ij}}^{mobility}(t)$ is calculated by MobilityMod using MON list and RSSI. In a very dynamic environment, the weight of mobility component ($\mathrm{w}_3$) can have the biggest value.

2) The second appending consists of dealing with security related multicast messages. For instance, to handle DIS-based attacks (DIS and SybM attacks), we introduce a new mechanism in RPL. This mechanism is based on the RFC 3810 [26]. More specifically, we use the Maximum Response Code (MRC) field to reduce response to multicast messages. In fact, in the DIO Base Object, there exist two unused bytes: Flags and Reserved fields. In our approach, we use these two bytes as one MRC field set by the 6BR (See Fig. 4). Hence, upon receiving a multicast DIS message, instead of responding immediately by a DIO message, the node delays its response by a random amount of time in

the range [0, Maximum Response Delay], where the Maximum Response Delay (MRD) value is derived from MRC [26]. This solution can be extended to be used for different kinds of multicast messages within the RPL network. Each of which may require its own delayed response. Thereby, control overhead can be reduced especially in the presence of an attacker.

3) The third appending consists on introducing a cross layer scheme, where information collected from the network layer is used to discard malicious nodes from the link layer. Because IDSMod is a cross layer based IDS, if a suspicious node is set as malicious by the BR or the 6BR, the 6BR will broadcast MAN list to the whole network. Upon receiving MAN by PAN/Coordinator associating the malicious node, the coordinator sends a disassociation notification to remove the malicious node from the PAN. Hence, the malicious node will be totally isolated from participating in the network operations.

### *D. T-IDS Advantages and Limitations*

## V. Using T-IDS to counter SybM attack

One specific misbehavior is SybM attack [6]. In fact, our proposed scheme can deal with this attack as depicted in Algorithm 1:

## VI. Conclusion

In this paper we addressed security issues of RPL. In particular, RPL's gaps related to mobility, identity, and self-organising characteristics. We demonstrated by simulation that the so-called SybM attack can exploit easily those gaps to disrupt the network performances in term of control overhead, energy cost and packet delivery ratio. We next introduced a new Trust-based IDS, namely T-IDS to deal with the presented gaps. The IDS is hierarchical where three layer cooperate to handle attacks: the Backbone Router, the 6LoWPAN Border Router, and the in-network nodes. Furthermore, T-IDS uses three modules: IdentityMod, MobilityMod, and IDSMod to detect and avoid malicious nodes. We presented a demonstrative algorithm to show how T-IDS can deal with SybM attack. Even if T-IDS seems to be resources costly, we believe that off-loading security computations and data-storage using TPM reduces the cost. In our future work, we will present performance evaluation of T-IDS using a simulation framework.

## References

[1] A. Andrushevich, B. Copigneaux, R. Kistler, A. Kurbatski, F. Le Gall, and A. Klapproth, "Leveraging multi-domain links via the internet of things," in *Internet of Things, Smart Spaces, and Next Generation Networking*. Springer, 2013, pp. 13–24.

[2] 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, Internet Engineering Task Force*, 2012.

[3] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in rpl-based internet of things," *International Journal of Network Security*, 2016.

[4] J. R. Douceur, "The sybil attack," in *International Workshop on Peer-to-Peer Systems*. Springer, 2002, pp. 251–260.

**Algorithm 1** SybM Detection and Countering

```
Input: MON, MAN, SUN
  Upon receiving a multicast DIS message
    1) Step 1: The receiving node delays responding by a
       DIO according to MRC previously conveyed in DIO
    2) Step 2: Meanwhile, receiving node uses the Node-
       ID field in the DIS message and queries IdentityMod
       and MobilityMod to verify if the node belongs to the
       network (using the routing table and/or querying the
       6BR), and if it is a mobile node (checking if the
       sender is in MON list)
       If (Node-ID$\in$MON) do
           Evaluate Node-ID trust value (ERNT) in col-
           laboration with neighboring nodes
           if (ERNT<Threshold) do
               1. Add Node-ID to SUN list
               2. Send encrypted SUN list to the 6BR
               3. Execute trust-based RPL routing by
               avoiding Node-ID
       Else do
           Querying 6BR and Waiting for a $\delta$ time
           If 6BRAN not yet updated, 6BR query the
           BR
           If (Newly deployed mobile node) do
               1. 6BR updates MON and Broadcasts
               it to its 6LoWPAN area
               2. Upon receiving MON, in-network
               nodes update RPL routing
           if (Newly deployed static node) do
               1. If not receiving MON or MAN by
               6BR after the $\delta$ time, update RPL
               routing
           if (Malicious node) do
               1. Add Node-ID to MAN list bu the
               6BR
               2. Broadcast MAN list by the 6BR
               3. Upon receiving MAN list:
                   If (malicious Node-ID asso-
                   ciated PAN/Coordinator) do :
                   Store MAN and Send a disas-
                   sociation request to discard the
                   malicious node
                   Else Store MAN list
```

[5] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson, "A security threat analysis for the routing protocol for low-power and lossy networks (rpls)," Tech. Rep., 2015.

[6] F. Medjek, D. Tandjaoui, M. R. Abdmeziem, and N. Djedjig, "Analytical evaluation of the impacts of sybil attacks against rpl under mobility," in *Programming and Systems (ISPS), 2015 12th International Symposium on*. IEEE, 2015, pp. 1–9.

[7] 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 *, 2013 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 2013, pp. 000 789–000 794.

[8] P. Pongle and G. Chavan, "A survey: Attacks on rpl and 6lowpan in iot," in *Pervasive Computing (ICPC), 2015 International Conference on*. IEEE, 2015, pp. 1–6.

[9] T. Sherasiya, H. Upadhyay, and H. B. Patel, "A survey: Intrusion detection system for internet of things," *International Journal of Computer Science and Engineering (IJCSE)*, vol. 1, no. 5, pp. 81–90, 2016.

[10] 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.

[11] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-service detection in 6lowpan based internet of things," in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on*. IEEE, 2013, pp. 600–607.

[12] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, and M. A. Spirito, "Demo: An ids framework for internet of things empowered by 6lowpan," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 1337–1340.

[13] 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.

[14] L. Zhang, G. Feng, and S. Qin, "Intrusion detection system for rpl from routing choice intrusion," in *2015 IEEE International Conference on Communication Workshop (ICCW)*. IEEE, 2015, pp. 2652–2658.

[15] N. K. Thanigaivelan, E. Nigussie, R. K. Kanth, S. Virtanen, and J. Isoaho, "Distributed internal anomaly detection system for internet-of-things," in *Consumer Communications & Networking Conference (CCNC), 2016 13th IEEE Annual*. IEEE, 2016, pp. 319–320.

[16] G.-H. Lai, "Detection of wormhole attacks on ipv6 mobility-based wireless sensor network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 1, p. 274, 2016.

[17] P. Thubert, "Objective function zero for the routing protocol for low-power and lossy networks (rpl)," *RFC 6552, Internet Engineering Task Force*, 2012.

[18] J. Vasseur, M. Kim, K. Pister, N. Dejean, and D. Barthel, "Routing metrics used for path calculation in low power and lossy networks," *RFC 6551, Internet Engineering Task Force*, 2012.

[19] F. Österlind, "A sensor network simulator for the contiki os," *SICS Research Report*, 2006.

[20] S. Thomson, "Ipv6 stateless address autoconfiguration," 1998.

[21] T. Preiss, M. Sherburne, R. Marchany, and J. Tront, "Implementing dynamic address changes in contikios," in *Information Society (i-Society), 2014 International Conference on*. IEEE, 2014, pp. 222–227.

[22] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Proceedings of the 3rd international symposium on Information processing in sensor networks*. ACM, 2004, pp. 259–268.

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

[24] N. Djedjig, D. Tandjaoui, and F. Medjek, "Trust-based rpl for the internet of things," in *2015 IEEE Symposium on Computers and Communication (ISCC)*. IEEE, 2015, pp. 962–967.

[25] P. Thubert, "Ipv6 backbone router draft-ietf-6lo-backbone-router-03," 2017.

[26] R. Vida and L. Costa, "Rfc 3810," *Multicast Listener Discovery Version*, vol. 2, 2004.

[27] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, and U. Roedig, "Securing communication in 6lowpan with compressed ipsec," in *Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on*. IEEE, 2011, pp. 1–8.