Performance Evaluation of RPL Protocol under Mobile Sybil Attacks

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*—In Sybil attacks, a physical adversary takes multiple fabricated or stolen identities to maliciously manipulate the network. These attacks are very harmful for Internet of Things (IoT) applications. In this paper we implemented and evaluated the performance of RPL routing protocol under mobile sybil attacks, namely SybM, with respect to control overhead, packet delivery and energy consumption. In SybM attacks, Sybil nodes take the advantage of their mobility and the weakness of RPL to handle identity and mobility, to flood the network with fake control messages from different locations. To counter these type of attacks there is a clear need for a trust-based intrusion detection system that we propose.**

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

I. Introduction

The Internet of Things (IoT) paradigm has become an important topic in our daily life. In an IoT application a set of objects are equipped with sensors/actuators and IP-connectivity to operate autonomously and to achieve a sensing requirement. These devices have reduced computational and storage resources [1]. While traditional networks are mainly composed of static objects (nodes), new IoT applications require mobile objects. When mobile nodes interact with their neighbors, they will trigger both topology and data traffic pattern changes. Therefore the network is more exposed to new security vulnerabilities.

The Routing Protocol for Low-Power and Lossy Networks (RPL) is the first standardized routing protocol specially designed to 6LoWPAN networks -IPv6 over Low-Power Wireless Personal Area Networks [2]. RPL deals with the constrained nature of such networks by considering limitations both in energy power and computational capabilities. As depicted in Fig. 1, RPL constructs a logical representation of the network topology as a set of Destination Oriented Directed Acyclic Graphs (DODAGs) through which data packets are routed. In each DODAG, nodes are connected to the 6LoWPAN Border Router (BR). The BR is connected to the Internet and to other BRs via a backbone link. The building process of RPL topology uses DIO (DODAG Information Object), DIS (DODAG Information Solicitation) and DAO (DODAG Destination Advertisement Object) control messages and a Trickle timer. In addition, RPL uses an Objective Function (OF) and node and/or link metrics and constraints to support routing optimization and calculate best paths [3] [4]. In RPL, each object has an IPv6 address as identifier and a Rank defining its position in respect to its parent. If inconsistencies happen involving changes in the topology, the Trickle timer will be reset to a lower value and control messages transmission rate will be fastened.

The fact that RPL uses IPv6 addresses as nodes' identifiers, makes the routing protocol vulnerable to Sybil attacks, in which an adversary creates easily fake identities called Sybil identities or Sybil nodes to participate in network operations as legitimate node [5] [6]. In Sybil attacks, 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. Once the adversary gains access to the network using a Sybil identity, it can exploit RPL other vulnerabilities to trigger different attacks. From one side, the malicious node can exploit the fact that RPL does not support mobility when routing to trigger a mobility-based attack. From the other side, the adversary can exploit the functioning rules of RPL to trigger specification-based attacks (i.e. Version number attack [7] [8], Rank attacks [9] [8], DIS attack [9], DAO attacks [10] [11], Local repair attack [12] [13], etc.). Both gaps can be combined and exploited by a Sybil node to disturb RPL.

Sybil attacks are widely treated for different networks such as P2P, Ad-hoc and WSNs. Nevertheless, to the best of our knowledge, there are only few works that address Sybil attack on RPL-based network without providing in-depth evaluation which is worth to be investigated. In [14], authors presented an analytical evaluation of Sybil attack on RPL under a dynamic and mobile topology. In [15], authors presented three types of Sybil attacks and their respective countermeasures. However, their analysis focus on Social Internet of Things. In this paper we present a simulation-based study of RPL performances in presence of a new Sybil attack, named SybM attack. In this attack, each malicious mobile node takes several Sybil identities and pollute the network with fake control messages from different locations.

The remainder of this paper is organized as follows. Section II presents the new Sybil attack model: SybM attack model. Section III presents simulation results and discussion, evaluating RPL performances in presence of SybM attack. Section IV introduces our new Trust-based intrusion detection system. Finally, Section V concludes the paper.

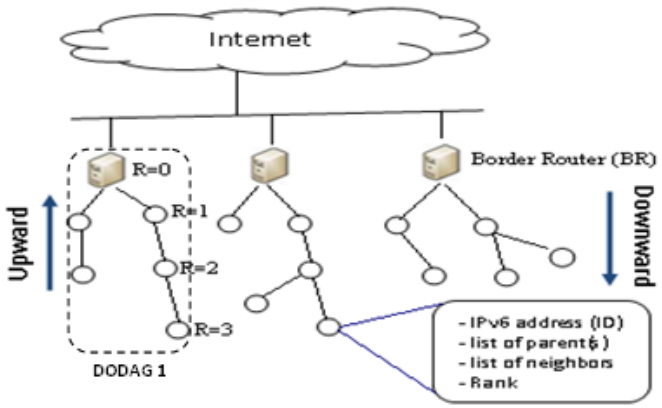


Fig. 1: RPL Topology

II. Sybil-Mobile Attack (SybM)

SybM attack is a combination of both Sybil and specification-based attacks where attackers are mobile. SybM attack is triggered against an RPL-based network where both mobile and static nodes coexist to achieve particular application requirements. In SybM attack, a malicious node exploits three gaps of RPL routing protocol to trigger the attack: identity, mobility, and DIS multicast function.

A. Mobility

Two kind of mobility exist: micro-mobility and macro-mobility. In micro-mobility, nodes move within the same network domain, whereas in macro-mobility, nodes move from one domain to another (i.e. between networks). In SybM, nodes move according to micro-mobility. In other words, they move physically within the same 6LoWPAN network (i.e. same DODAG IPv6 prefix).

B. Identity

As previously mentioned, RPL uses control messages dissemination. Thus, enabling minimal configurations in the nodes, allowing them to operate mostly autonomously. Consequently, nodes can calculate their ranks and set their IPv6 addresses based on the conveyed configurations (e.g. prefix, DODAG ID, IPv6 auto-configuration, etc.). Nodes use Stateless Address Auto-configuration (SLAAC) to auto-configure their addresses [16]. SLAAC is the most commonly used address assignment method, especially for networks where strict control of addresses is not a concern as long as host addresses are valid and routable. In SybM, each mobile-compromised-node can automatically fabricate new IPv6 addresses [16]. The new IPv6 addresses are known as Sybil identities or Sybil nodes, and are used by the attackers to participate within the network as new members. As the network prefix is always the same, the malicious node changes each time the MAC part of its address as explained in [17].

C. DIS Messages Multicast

A node can join an RPL topology either by waiting for DIO messages, or by using the DODAG solicitation mechanism (sending a DIS message). DIS messages allow a node to discover the DODAG information by soliciting DIO messages from its neighbors. Thus, DIS messages are similar to Router Solicitation in neighbor discovery mechanism. Once this node receives DIO messages, it selects its preferred parent. Then builds a DAO message, which contains its address (identifier) and parent set. This DAO message is advertised to other nodes in order to update their routing table or their parents list. In fact, the DODAG solicitation mechanism is designed to allow nodes within the network that want to join the DODAG to send a DIS message if no DIO message is received during an RPL DIS Interval. However, in the case of SybM attack, malicious nodes don't wait for the expiration of DIS Interval and multicast DIS messages using one of their Sybil identities (fabricated IP addresses).

D. Attack Model

In SybM attack, the Sybil nodes communicate directly with legitimate nodes. They operate independently and do not cooperate during the attack. In other words, each attacker sees other attackers as ordinary nodes. As depicted in Fig. 2, in SybM attack, each node is initially placed at a random location and sends periodically data packets to the BR. Malicious nodes pause for a period of time behaving the same way of honest nodes (sending data packets to the BR). Indeed, each adversary involves a set of its Sybil identities alternately and periodically, while moving through the network. Thus, after the pause time, malicious nodes choose a new location across neighboring nodes towards the BR, and move physically there. When malicious nodes arrive, they repeat the process of pausing and then selecting a new destination to which they intend to move. Upon moving, malicious nodes multicast DIS messages within the network. In macro-mobility, normally, the IPv6 address of the node remains unchanged. Nevertheless, as in SybM mobile nodes are malicious, they multicast 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 result, neighborhood connectivity will change, and obviously more DIO messages will be exchanged.

III. Simulation

A. Simulation settings

We simulated a network of 50 TelosB nodes (Sky motes) with one BR placed in the centre and 49 senders placed randomly around the BR . Each Sky mote is powered by an 8MHz, 16-bit Texas Instruments MSP430 microcontroller with 10kB of RAM and 48kB of flash memory. Table I shows the simulation parameters.

We simulated four scenarios as summarised in Table II. The first and second scenarios are used as benchmarks. The third scenario represents the implementation of DIS attack (Sybil attack in a static network), and is also used as benchmark [9].

TABLE II: Scenarios

Scenario	Description
Fist	A network with no attacker and no mobility
Second	A network with no attacker and some mobile nodes. We varied the number of mobile nodes from 2, 4, 6, 8, to 10. Each mobile node moves towards the BR 1, 3 then 5 times (noted 1Move, 3Move and 5Move, respectively). The special case of 0 mobile node and 0 move corresponds to the first scenario
Third	A network with attackers (Sybil nodes) and no mobile nodes. In this scenario the attackers multicast periodically DIS messages from the same locations. We varied the number of attacker nodes from 2, 4, 6, 8, to 10. For each attacker the number of Sybil identities increases from 1, 3, to 5 (noted 1DIS, 3DIS and 5DIS, respectively)
Fourth	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 (noted 1SybM, 3SybM and 5SybM, respectively)

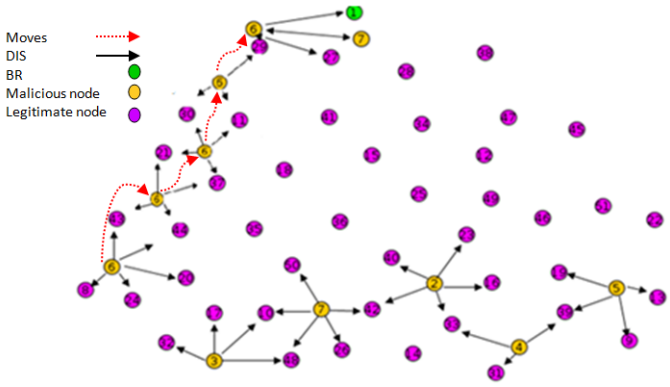


Fig. 2: SybM model, where 6 attackers move periodically across their neighbors towards the BR while multicasting DIS messages

TABLE I: Simulation Parameters

Parameter	Value
Simulator	Cooja-Contiki 2.7
Simulation time (s)	330
Number of nodes	50
Network area	$300x300m^2$
Transmission range	50m
Radio medium	UDGM : Distance Loss
Traffic rate	1 packet sent every 10 seconds
Number of mobile/attacker nodes	0, 2, 4, 6, 8, 10
Number of Sybil nodes per attacker	1, 3, 5

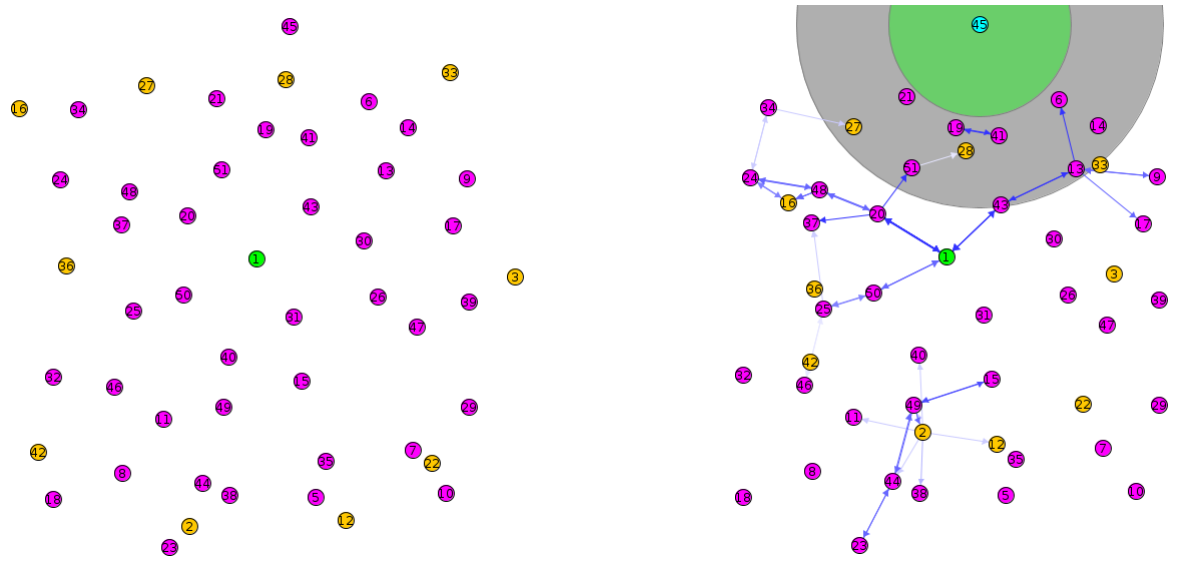
In fact, DIS attack represents a special case of SybM attack where attackers are static nodes. The fourth scenario represents SybM attack.

We conducted the simulations on Cooja Contiki-2.7 [18]. To handle nodes mobility, we used the Cooja-Mobility-Plugin. Furthermore, to handle Sybil identities we rely on Preiss et al. work [17]. For more accurate evaluation, each simulation was executed 5 times and simulations outputs were averaged. To study the impacts of SybM attack on RPL performances, we focus on control messages overhead, packets delivery and energy consumption parameters. For the control messages overhead and the energy consumption analysis, we used the radio messages and collect-view tools of Cooja. For packets loss analysis, we used the simulation script editor of Cooja. In Fig. 3, Figure 3a represents the experimental network topology for SybM attack in the case of 10 malicious nodes before triggering the attack. Whereas Figure 3b represents the topology evolution of the same network after triggering the attack. The mobility issue is seen clearly even without attacker. Once the node 28 moves, the node 45 becomes isolated from the network (Black hole in the network topology).

B. Simulations results and discussion

1) Control overhead: Fig. 4 depicts control overhead in SybM attack and the first scenario (No attack). When we compare SybM attack with one Sybil node per attacker (noted 1SybM) with No-attack scenario, we notice that the extra control overhead after triggering 1SybM is about 6% for 2 moving attackers, and increases until reaching 32 % for 10 moving attackers. Likewise, for SybM attack with 3 Sybil nodes per attacker (noted 3SybM), the extra control overhead is about 24% for 2 moving attackers, and increases until reaching 66% for 10 moving attackers. In the case of SybM attack with 5 Sybil nodes per attacker (noted 5SybM), the extra control overhead is about 45% for 2 moving attackers, and increases until reaching 133% for 10 moving attackers. In the case of 1SybM and 3SybM attacks, when the number of mobile attackers increases, the control overhead increases steadily, while it increases considerably in the case of 5SybM attack until being doubled. Furthermore, by increasing the number of Sybil mobile nodes within the network, the control overhead increases significantly. In fact, the extra control overhead from 3SybM is 2 times the one from 1SybM (in the case of 4 and 6 moving attackers the overhead almost doubles). In addition, the extra control 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).

In the second scenario (see Fig. 5), we notice that even when the number of moving nodes increases, the overhead generated by 1 or 3 moves per moving node remains almost the same. However, when the number of moves exceeds 3 (is equal to 5), the overhead is more significant. It is almost the same overhead for 1SybM. Moreover, in the second and fourth scenarios, when the number of moves/Sybil-nodes exceeds 3 (case of 5Move and 5SybM) the control overhead increases because mobile and Sybil nodes are more close to the BR, and thus can be detected by it. Which means the whole DODAG needs to be reconstructed from scratch. Furthermore, even if the mobile nodes in the two scenarios move in the same way (same positions), we notice that the overhead generated by SybM is almost twice the second scenario. This is due to the nature of SybM and the RPL trickle timer mechanism. In



(a) Before triggering SybM (b) After triggering SybM

Fig. 3: The experimental network topology for SybM attack in the case of 10 malicious nodes

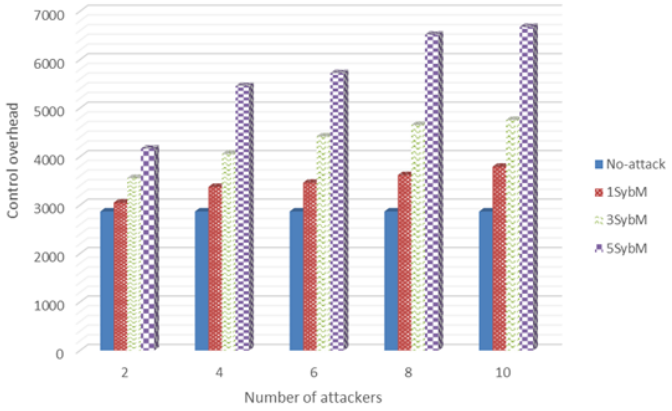


Fig. 4: SybM attacks control overhead

the second scenario there is no mechanism to detect mobile nodes and thus, the trickle timer interval is not updated accordingly. Nevertheless, in SybM scenario, in addition to mobility, submission of DIS messages from different locations resets the trickle timer and fasten the exchange of more control messages.

In Fig. 5 we see that in both third and fourth scenarios, when the number of Sybil nodes increases, the extra overhead increases too. Likewise, when the number of malicious nodes increases, the extra overhead increases too. Indeed, when the number of Sybil nodes increases, in the case of 2 attackers, the extra overhead of SybM attack almost doubles compared with DIS attack. Further, in the case of 10 attackers, the extra overhead of SybM attack almost triple compared with DIS attack. This is due to the fact that DIS attack (i.e. 0 move) represents a static environment while varying the number of attackers. Whilst SybM attack represents a dynamic environment where the mobility of malicious nodes causes the number of nodes affected by the attack to increase, and hence, the control overhead as well. For SybM attack, we notice that the overhead is almost the same in the case of 8 and 10 attackers. Also, it is almost the same in the case of 4 and 6 attackers. This can be explained by the fact that attackers are moving almost in the same area, and thus affect the same neighboring nodes. In addition, the attackers can be close to BR which involve reconstructing the whole topology. As seen in Fig. 3 (Figure 3b), from 6 attackers (even 6 mobile nodes), the node 45 is completely isolated and do not participate any more in the network. This also partly explains why the overhead do not increase as expected when increasing the number of attackers.

2) Packets Delivery and Energy Consumption: In Fig. 6 and Fig. 7 we see that in presence of SybM attackers, the energy cost increases whilst PDR reduces remarkably, as the number of attackers and Sybil nodes increase. This could be due to the growth of affected nodes within the network. Consequently the number of exchanged control messages is increased, which rises the probability of collisions and packets retransmission, and in turn increases the power consumption and lowers the PDR. In addition, we notice that damaging effects from SybM attack in terms of energy cost and PDR outpace the one from DIS attack by up to 33%. In fact, the effect of DIS attack on PDR is smaller even when compared with the second scenario. This is explained by the fact in DIS attack nodes are not mobile, and thus only few packets will be lost due to probable collisions. However, In the case of SybM attack and even in second scenario, packets sent to mobile nodes will systematically be lost if nodes are moving, which reduces PDR. On the other hand, the energy cost occasioned by DIS attack is more important than the one by second scenario. This

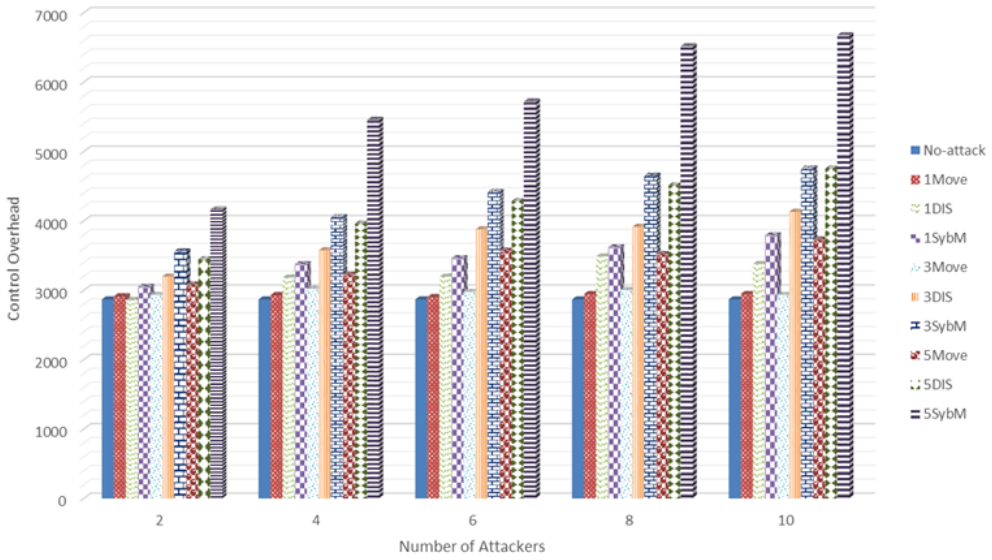


Fig. 5: Control Overhead

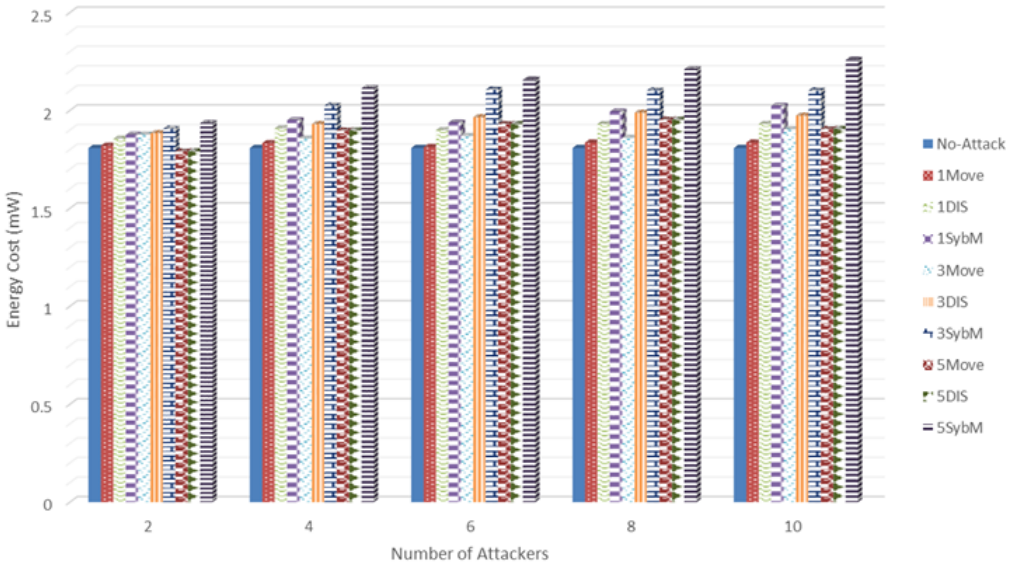


Fig. 6: Energy Cost

is due to the fact in DIS attack there is more control overhead and thus more energy consumption. PDR is more important in SybM attack and in second scenario because of the weakness of RPLs performance in mobility case.

IV. Trust-based IDS Approach

As seen previously, SybM attacks degrade RPL performances. Hence, counter solutions are necessary. In this context, we propose a new distributed, cooperative and hierarchical Trust-based Intrusion Detection System (T-IDS). T-IDS deals with mobility, identity and multicast security issues which can be exploited by SybM attacks. In T-IDS, each node is equipped with a Trusted Platform Module co-processor to handle identification and off-load security related computation and storage. Each node is a monitoring node and collaborates with his neighbors to detect intrusions and report them to the BR. T-IDS introduces a new timer and minor extensions to RPL messages format to deal with mobility, identity and multicast issues. Hence, T-IDS architecture integrates three cooperative modules: IdentityMod, MobilityMod and IDSMod.

A. *IdentityMod*

In T-IDS a centralized beforehand registration of nodes to a backbone router is required to control access to the network. The backbone router associates to each node a unique 20 bytes long identifier (Node-ID) which is a cryptography-based unique representation of a node derived from its TPM-ID. To authenticate a node at any stage of the network execution, we

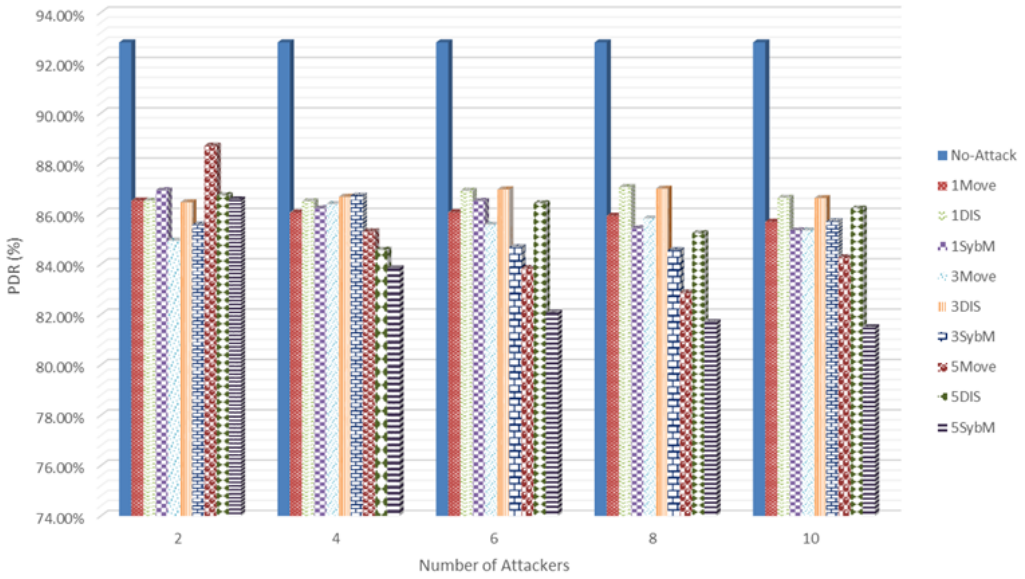


Fig. 7: Packet Delivery Ratio

propose Node-ID to be conveyed within RPL control messages with its associate IPv6 address as depicted in Fig. 8. Node-ID field will be used by participating nodes to detect and report intruders.

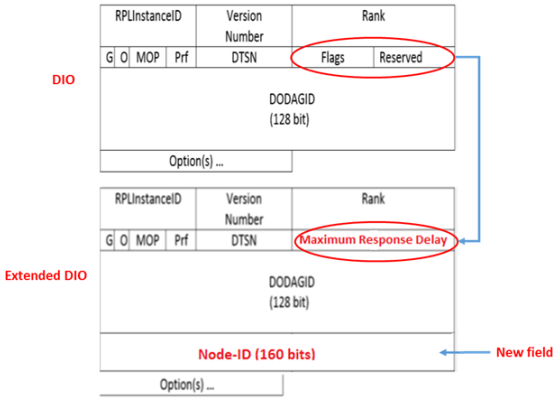


Fig. 8: New DIO message format

B. MobilityMod

MobilityMod aims to maintain the state of the network regarding mobile nodes. The backbone router, the border router and in-network nodes maintain a list with Node-IDs of all legitimate mobile nodes. Hence, if a joining request (DIS message) is received from a Node-ID not registered within the mobility list, this node will be reported as intruder.

C. IDSMod

IDSMod queries IdentityMod and MobilityMod to verify if the node belongs to the network and if it is a mobile node. IDSMod uses a new Trust-based RPL scheme to route traffic. In this scheme, in-network nodes with the BR observe and collaborate to detect misbehaving nodes. Indeed, periodically each node calculates trust values of its one hop neighbors and receives trust values evaluations of other nodes from its neighbors. It then aggregates all received and calculated trust values (i.e. collaborative calculation). To evaluate trust, the node uses three components: energy, honesty and mobility [19]. T-IDS reacts in a corrective action. In fact, if the final trust value is less than a threshold, this node will be avoided when selecting routing paths as a mitigation method, and reported as intruder.

Furthermore, to handle (reduce) the response to multicast messages, especially, in the case of malicious mobile nodes. We propose to adapt RPL itself by using two reserved bytes in the DIO message as Maximum Response Delay such as in RFC 3810, as depicted in Fig. 8. Indeed, 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] [20].

In addition, we propose T-IDS to be a cross layer based IDS where information collected from the network layer is used to discard malicious nodes from the link layer. When an attacker is detected, the BR broadcast the information to other nodes. Upon receiving the Node-ID of the intruder by the 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.

V. Conclusion

In this paper we presented a new attack against RPL named SybM attack. In this attack adversaries exploit some RPL functioning and gaps to trigger the attack. We evaluated the performances of RPL in terms of control overhead, packet delivery ratio (PDR) and energy consumption in the presence

of SybM attackers. The implementation results showed that the previously cited performances are sensitive to SybM attack. Indeed, the fact that RPL does not support mobility, by increasing the number of malicious nodes, and increasing the number of sybil moving nodes, SybM attack increases control overhead and energy cost, while decreasing PDR. Indeed, this attack is difficult to detect given that it is carried out solely through the use of seemingly innocent interactions (joining and constructing the DODAG). To counter this attack, we introduced a Trust-based IDS solution. The proposed T-IDS handles identity, mobility and control messages multicast issues.

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

[4] 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.

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

[6] 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.

[7] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "A study of rpl dodag version attacks," 2013.

[8] A. Dvir, T. Holczer, and L. Buttyan, "Vera-version number and rank authentication in rpl," in *Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on*. IEEE, 2011, pp. 709–714.

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

[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, Internet Engineering Task Force*, 2012.

[11] M. Richardson, A. Lozano, T. Tsao, V. Daza, R. Alexander, and M. Dohler, "A security threat analysis for routing protocol for low-power and lossy networks (rpl)," *draft-ietf-roll-security-threats-10*, 2013.

[12] A. Le, J. Loo, Y. Luo, and A. Lasebae, "Specification-based ids for securing rpl from topology attacks," in *Wireless Days (WD), 2011 IFIP*. IEEE, 2011, pp. 1–3.

[13] 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.

[14] 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.

[15] S. Pawar and P. Vanwari, "Sybil attack in internet of things," *International Journal of Engineering and Innovative Technology (IJESIT)*, 2016.

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

[17] 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.

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

[19] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, "New trust metric for the rpl routing protocol," in *2017 IEEE The 8th International Conference on Information and Communication Systems (ICICS)*. IEEE, 2017.

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