SPLIT: A Secure and Scalable RPL routing protocol for Internet of Things

Mauro Conti*, Pallavi Kaliyar§,*, Md Masoom Rabbani§,*, Silvio Ranise†
*University of Padova, Padova, Italy
{conti, pallavi, rabbani}@math.unipd.it
†Fondazione Bruno Kessler, Povo, Trento, Italy
{ranise}@fbk.eu

***Abstract*—Due to recent notorious security threats, like Mirai-botnet, it is challenging to perform efficient data communication and routing in low power and lossy networks (LLNs) such as Internet of Things (IoT), in which huge data collection and processing are predictable. The Routing Protocol for low power and Lossy networks (RPL) is recently standardized as a routing protocol for LLNs. However, the lack of scalability and the vulnerabilities towards various security threats still pose a significant challenge in the broader adoption of RPL in LLNs.**

To address these challenges, we propose *SPLIT*, a secure and scalable RPL routing protocol for IoT networks. SPLIT effectively uses a lightweight remote attestation technique to ensure software integrity of network nodes. To avoid additional overhead caused by attestation messages, SPLIT piggybacks attestation process on the RPL's control messages. Thus, SPLIT enjoys the low energy consumption and scalability features of RPL protocol, which are essential in resource-constrained large scale networks such as IoT. The simulation results for different IoT scenarios show the effectiveness of SPLIT compared to the state-of-the-art in presence of different types of attacks, concerning metrics such as packet delivery ratio and energy consumption.

***Index Terms*—RPL, Internet of Things, Attestation, Security, Routing.**

I. Introduction

In today's world, we are moving towards an era, that is continuously permeating with the so-called "smart" devices. The network of these devices (i.e. IoT) are often resource constrained and work for specific tasks and mostly employed as a group. In particular, the group of IoT devices employed in smart facilities (e.g., smart city, smart home, smart factories, gas and oil exploration) is termed as "Swarm"[1].

Although IoT devices bring drastic improvements in our day to day life, they also give rise to security concerns as these *tiny*, low-end embedded devices are deployed in a wide range of applications and become an integral part in, e.g., industrial control systems, smart environments, wearable devices, military applications, and agriculture. As these devices deal with mission-critical, sensitive data, any security breach on these devices or communications among IoT devices can lead to catastrophic consequences for our privacy and security [2]. Hence, to ensure the correct operation in various IoT applications, it is crucial to maintain their software integrity and protect them against attacks. For instance, authors in [12] [18] show that large-scale industrial control systems or robot swarms are vulnerable to the large array of attacks. Nevertheless, the resource constraints and low-cost features of these devices hinder the adoption of specific hardware protection or complex cryptographic solutions, which make them an easy prey to malware attacks. Routing Protocol for Low power and Lossy Networks (RPL) is an open routing protocol standardized by the IETF (Internet Engineering Task Force) Routing Over Low power and Lossy networks (ROLL) working group in 2008, is used for data transportation and routing for IoT networks. However, due to RPL protocol, the network becomes vulnerable and exposed to various security risks. For instance, while routing, a malicious device can manipulate the network operations, depletes nodes energy and can disrupt the complete network functions. In order to prevent such attacks, to detect unintended software modifications, and to ensure the safe and secure operation of a device, it is essential to guarantee its software integrity and confidentiality.

A key technique to check the software integrity of smart devices is known as *remote attestation*. It is a process that allows a verifier to validate the integrity of software residing on a remote smart device. While efficient single hop and individual device attestation techniques exist, but data integrity verification in a large dynamic networks (such as IoT) remains an open problem [11]. It is due to high attestation time, communication overhead, and scalability challenges. The naive applications of remote attestation do not scale for systems that consists of device swarms with dynamic topologies, such as intelligent transportation systems and robots used for oil and gas search. Hence, it requires novel, reliable, and scalable solutions to safeguard network operations consist of IoT devices.

A. Contribution

In this paper, we propose a new secure and scalable RPL based routing protocol called as (SPLIT) for IoT networks. SPLIT uses the unique advantages of RPL protocol [29] to provide an efficient periodic device attestation report aggregation (concerning attestation time, energy consumption, and network overhead) in large-scale IoT network. The use of device attestation improves the security in data communication

§corresponding author

[1]https://www.techrepublic.com/article/iot-device-swarm-intelligence-think-about-security-before-its-too-late/

process of RPL by making it robust against an array of routing threats such as *rank* [14] and *sybil* [21] attacks. The primary aim of SPLIT is to ensure the integrity of the IoT devices as well as the data packets they exchange as these are considered the significant challenges in deployment of large-scale secure IoT networks. In particular, the paper has the following contributions.

- We propose a secure and scalable RPL based routing protocol called SPLIT for IoT networks. Our proposed approach make optimized use of RPL protocol's route discovery process and periodic topology maintenance messages to send and receive attestation related information. Thus, SPLIT achieves the attestation scalability while keeping the attestation caused overhead and the device attestation time to the minimum.
- We fully implemented SPLIT in *Cooja*, the Contiki network simulator, which is widely used for deploying energy-constrained and memory-efficient low power and lossy networks (LLNs) such as IoT. The security and energy efficiency evaluation show substantial improved simulation results with respect to the state-of-the-art. We show the correctness and effectiveness of SPLIT. Additionally, the results indicate that SPLIT is able to effectively perform the device attestation in moderate mobility scenarios, which is a major drawback for the state-of-the-art attestation schemes. We make available[2] an open-source implementation of SPLIT along with all the source code to the research community.

B. Organization

The rest of the paper is organized as follows. In Section II, we briefly explains background and state-of-the-art concerning device attestation process and RPL protocol. Section III-C provides description of our proposed approach SPLIT along with its working methodology and design considerations. In Section IV, we present the simulation and performance evaluation of SPLIT regarding its security and energy analysis. Finally, Section V concludes our work with possible directions of future work.

II. Preliminaries

In this section, we discuss typical attestation technique and the related state-of-the-art for the RPL protocol along with threats and its limitations, which lead us towards the motivation of our research work. Recently, attacks on smart devices are on the rise as they are gaining wider adoption. These attacks have caught the attention of the common public as the adoption of smart devices in all aspects of life make the attack surface broaden than ever. When these devices control personal data, any security breach in these devices or over communication channel can have a disastrous effect. SmartTV hacking [3] is a recent example of how a security breach in these devices can have a dramatic impact on users' privacy. In this era, where everything connects to everything, it is indeed crucial to look after the security concern. As there is no panacea to resolve all the IoT related security concerns, we are exploring RPL enabled security measures, which will guarantee reliable and low-cost solutions for the IoT networks.

[2]https://github.com/pallavikaliyar/SPLIT

[3]http://metro.co.uk/2016/05/23/smart-tv-hackers-are-filming-people-having-sex-on-their-sofas-and-putting-it-on-porn-sites-5899248/

A. Overview of Attestation

Remote Attestation (RA) is a well established technique to identify adversarial presence in a device. Since past decade researchers have proposed many RA schemes [3], [22], [27], [28] having different working procedure. However, typically RA is a technique where a trusted entity (Vrf) check the integrity of an "untrusted" device (Prv) by validating whether the device is indeed running the latest updated version of the software or data without any adversarial presence. As depicts in Figure 1 a Vrf sends a challenge to an untrusted Prv. Upon receiving the challenge, the Prv will perform the intended operation and sends back the response to Vrf. Based on the received response Vrf validate the "health" of the device.

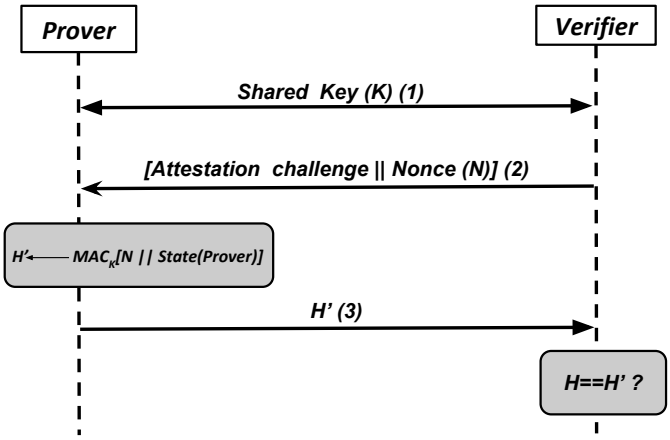

Fig. 1. Typical example of Remote Device-Attestation

Although RA is an efficient method to validate device's health, it is hard to implement on large networks due to its one-to-one verification model. In order to achieve low-cost and secure networks, RPL along with RA can be a suitable solution due to their unique interoperability.

B. Routing Protocol for Low Power and Lossy Networks (RPL)

The IETF ROLL work-group developed RPL for routing in LLN such as IoT, where devices are highly resource constraint. RPL is a proactive distance vector routing protocol, and it organises network devices into Directed Acyclic Graphs (DAGs), which is a spanning tree topology. In a DAG, all nodes are connected in a way to ensure that there are no loops, and the data is routed to reach one or more root nodes. Additionally, a DAG could consist of one or more Destination-Oriented DAG (DODAG), where each DODAG work towards to satisfy the requirements of a particular application running on top of it, thus it enables multiple applications to work

simultaneously, but independently, inside the same network. To create and maintain the DODAG, RPL uses a set of control messages which includes DODAG Information Object (DIO), DODAG Information Solicitation (DIS), and Destination Advertisement Object (DAO) and its Acknowledgment (DAO-ACK) messages. The detailed working of RPL and its features are out of the scope of this paper, hence we direct the interested users to more comprehensive literature given in [19] and [29].

C. Threats and Previously proposed security solutions for RPL

As we previously mentioned, due to new standardization of RPL routing protocol and in quest of providing best Quality of Service (QoS) while routing, RPL is exposed to many security threats. RPL is very strong against the external intruders given the cryptographic and authenticating techniques. But when it comes to a malicious node present internally in the system, important parameters such as Rank, Node ID, DODAG and version number can be compromised.

Few of the researcher proposed solution to solve these attacks, for example, in [14] a security service against internal attacks is named "VeRA" is presented, which stops the malicious nodes from illegitimately increasing their DODAG Version Number and manipulating the Rank. An increase in DODAG Version Number causes a load on energy and energy consumption due to Global Repair. To address this attack authors proposed an approach [14], in which a version hash chain is created and for each member of this chain, a rank chain is created. So, whenever there is an illegal increase, each node can check it by comparing original values and a chained hash of current value using the MAC *mrh* function. Each node is able to counter the illegitimate increase in the parent rank. However, in [23] the authors show that despite of all the hashing, VeRA is still vulnerable to rank attack, and proposed a new approach TRAIL (Trust Anchor Interconnection Loop). TRAIL is based on the topological authentication. Unlike VeRA it utilizes very less cryptographic efforts and provides protection against the internal attacks such as Rank Spoofing and Rank Replay. Validation of upward path through round-trip messages is the key idea. On receiving a message from the parent, child sends an authentication message with its rank and a nonce. Each upward node check for two things that are 1) rank of the node sending that test messages is higher than its own, and 2) difference of rank between the sending node and his own.

In [26], the author describe the vulnerabilities and attacks adhered due to rank property in RPL. To analyze the rank attack and its vulnerabilities in RPL, authors proposed an approach named *attack graph*, which helps to analyze the attacks by providing all the possible action sequences taken to do the attack. Mostly using the form of a state diagram. The authors mainly focused on three categories of rank manipulation, which are first "Decrease Rank Attack" that gives rise to sniffing, identity attacks; second "Worst Parent Attack" that creates sinkhole and blackhole attacks; third "Increase Rank Attack" that can cause Dag Inconsistency attack.

In [24] an internal attack to RPL is presented. Authors discuss the effects of DAO inconsistency attack, and proposed a solution to mitigate it using a Dynamic Threshold Mechanism (DTM). In DAO inconsistency attack, a malicious node intentionally drops the received packets and forwards a new packet with setting the Forward Error Bit. It makes ancestors nodes to drop the route in their routing table and again look for new root, which increases overhead and energy consumption. To provide a solution, every node has a limited threshold of 20 forwarding error messages. Each node also has a mischief threshold counter, if a node is found not adhering to the error function, its mischief counter is increased by one. Once the counter value crosses the threshold, it is declared mischievous. The main drawback of this approach is that it is not energy efficient, and as RPL is used for energy constraint devices it is a serious issue to consider. Recently, in [5], a trust-based mechanism is presented to detect and isolate sybil and rank attacks. A sybil attack is basically defined as when a malicious node replicates its *id* in a DODAG in large quantity. The proposed trust mechanism has five phases, which are Trust Calculation, Trust Monitoring, Detection and Isolation, Trust Rating, and Backup to detect and mitigate the rank and sybil attack in the system.

A new Secure RPL (SRPL) is proposed in [16], which stops mischief caused by the internal attacks in RPL to make it more secure. The authors uses the concept of threshold rank and hash chains for authentication. Rank boundaries are determined by two factors "Decreased Rank Threshold" and "Increased Rank Threshold" and their function is related to the set of parents and descendants respectively (in an inverse manner), which causes stabilizing of the structure. The approach uses three phases to make the protocol more secure: 1) Initialization- DODAG formation with hashed rank distribution; 2) Verification- Parent of a child node is actor in this process and verifies the child and its descendants by multi-step hashing; and 3) Rank Update- Checking of old rank, new rank and verify the threshold using mentioned rank change algorithm. The main drawback of proposed threshold mechanism is that it acts against all the nodes including the non-malicious nodes with a large set of descendants, which causes additional overhead in the start due to the use of hashing technique.

Previous research on the RPL protocol has focused on making communication among IoT devices more secure and reliable for routing, but none has considered the problem of device authenticity. Due to the lack of any device authenticity mechanism, the RPL is vulnerable to security threats such as rank attack and sybil attack, which decreases the communication efficiency and disrupt the correct working of the network. It could lead to severe consequences if critical IoT applications use the network. However, RPL provides energy efficiency, adaptivity to work in various environments, and scalability, which makes it best suited routing protocol for resource-constrained large IoT networks [10]. Due to all these positive features of RPL, in our proposed approach, we consider device integrity and confidentiality to make the whole communication

system more secure and reliable.

III. Our Proposal: SPLIT

In this section, first, we present the details of the system and adversary models on which SPLIT is implemented and evaluated. Then we discuss SPLIT's design considerations, functioning, and working methodology.

A. System Model

- The network consists of a set $N = \{N_1, N_2, ...N_n\}$ of size n resource constraint IoT nodes (i.e., sensors and actuators). These nodes are static/mobile (for the different set of experiments) within the network area and are homogeneous concerning resources. However, the nodes could be heterogeneous regarding their functionalities (different underlying software or hardware) depending upon the type of the device.
- RPL creates a virtual DODAG on top of the physical network topology. For our experimental purpose, we have also assumed the presence of malicious nodes (Adv) in our network. The root node plays a critical role in creating and maintaining the DODAG in the existing network, in our system it also plays the role of the verifier Vrf.
- As it is common in most of the attestation literature, we are assuming that the root node (Vrf) is trusted and cannot be compromised. All the other devices in the network have trusted execution environment [8], [15], which is not accessible by any unauthorized entities and it stores the required keys along with the attestation-related details (e.g., attestation algorithm) for device attestation process as it is shown in Figure 2.

B. Adversary Model

Based on the taxonomy in [4], we are considering remote and local adversaries (Adv) which are capable of mounting software-only attacks. We are keeping physical Adv out of the scope of our work. However, we will address possible detection mechanisms for physical tampering in SPLIT by employing a mechanism that could identify device absence in the network for a non-negligible amount of time, thus signals the possible presence of physical adversaries. In our target IoT network scenarios, the Adv are assumed to have the following characteristics:

- Software$_{Adv}$: the Adv is capable of launching various attacks that includes cloning, sybil, rank, blackhole, eavesdropping, and wormhole attacks. To perform all the mentioned attacks, either it can compromise an existing node, or it can be part of an existing network as a new node. However, we assume that the Adv cannot compromise the DODAG Root (i.e., LBR).
- Roaming$_{Adv}$: the adversary is mobile and, it can join the network for a short time-period and try to perform malicious activities to disrupt network integrity.
- Physical$_{Adv}$: Although this type of adversary is out of the scope of our work. In Section IV-A, we discuss the possible way to detect the presence of the physical adversary.

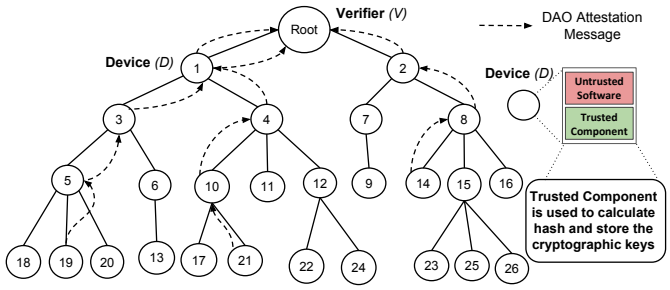

Fig. 2. SPLIT device attestation technique

C. SPLIT Design Considerations and Functioning

For SPLIT, we optimize and combine the best features of the RPL protocol on the one hand and of device attestation on the other. The primary purpose of the development of SPLIT is to improve the security by considering scalability factor in large-scale IoT networks. SPLIT functioning is to use device remote attestation method without introducing additional overheads on network. In SPLIT, we effectively exploit the built in features (e.g., energy efficiency, scalability, and adaptability) of traditional RPL to collect attestation reports without creating any additional network overhead and energy consumption. SPLIT exploits the Destination Advertisement Object (DAO) ICMPv6 control messages [19] of RPL to send attestation report. Additionally, the use of hybrid attestation[4] scheme ensures the authenticity of nodes that take part in the routing process, hence it will make the routing process more robust against various routing attacks.

SPLIT inherits the features from traditional RPL and exploits these features for improving the data communication system via device attestation. We show through our evaluations that SPLIT has significant advantages over the traditional routing protocols concerning network overhead, energy consumption, and communication security. Moreover, SPLIT can be adopted in existing IoT infrastructures because its implementation is using the RPL protocol, which is already a standard routing protocol for IoT networks.

- In our proposal, we use RPL's DAO ICMPv6 control messages for attestation purpose. We modify the required header fields in DAO (please refer to Figure 3). The modified and newly added data structures are as follows: (i) a 4 bit *"flag"* field to send the node ID, (ii) 8 bit *"reserved"* field for sending the "attested report with time-stamp where 6 bit is used for timestamp and 2 bit (00 in case of *BAD* node and 11 in case of *GOOD* node) is for outcome of the self-attestation" to the root, and (iii) a 32 bit *"option"* field to send attestation report of the device. The attestation report will contain the hash

[4]hardware-software co-design to safeguard attestation related details from attackers

value of the underlying software of the device and a timestamp to prove its time-bound freshness. The attestation message for any device (say D_i) is as follow.

$$Att_{D_i} = [hash_{D_i}||Timestamp]Root_{pk}$$

where Att_{D_i}, hash, Timestamp and $Root_{pk}$ denotes device specific attestation report, hash value of the underlying device specific software, attestation timestamp, and root node's (Vrf) public key. The attestation report will be encrypted using root node's public key, which allows only the root node to decrypt.

- Our approach makes use of the RPL's non storing mode (i.e., MOP2) because it is best suited for resource constrained devices due to its support for minimal memory and computational requirements. Furthermore, in this mode every device in the network sends the aforementioned DAO control messages directly to the root node, hence no intermediate device is allowed to alter these control messages.
- In RPL, the DAO message, apart from its various responsibilities (e.g., providing route support from downwards to upwards towards root in the DODAG) also works as a beacon message, which will provide the device attestation report to the root node after a specific time interval. The "Trickle-Timer" controls the generation of beacon messages [20]. Based on the application scenario, the timer can be tuned to ensure the time-based device attestation report generation. Additionally, the root node can get the network *health* status using "Trickle-timer" after a defined period interval, this will help to mitigate the threats deriving from Roaming$_{Adv}$.
- The DAO control message acts as regular DAO messages in the network, the updated/modified DAO message is only used for the attestation process. Whenever the attestation process starts, the fields of DAO message takes the altered values to the root and perform the device attestation process by sending a report to the root node (i.e., verifier). Then, on the basis of the attestation report, the verifier decides the next step (please refer to Figure 4).

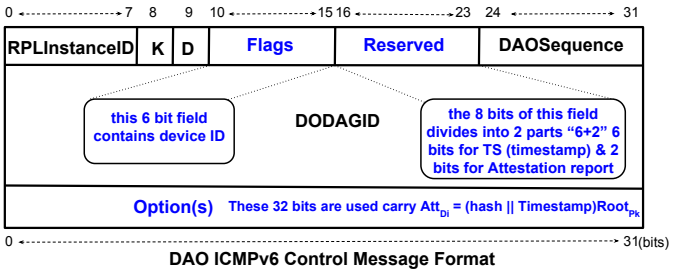

Fig. 3. Modified DAO ICMPv6 Control Message Format

D. SPLIT Working Methodology

SPLIT's pseudo code for both prover and verifier are provided in algorithms 1 and 2, and the finite state machine (FSM) model is shown in Figure 4. The primary stakeholders in SPLIT are (1) Verifier (Vrf), and (2) Prover (Prv).

1) SPLIT-Prover: The prover has four main functions, which are as follows:

- *Initial Joining*: Prover(s) take part in DODAG formation and become part of the network.
- *Verify Trickle time*: Based on the trickle time, prover(s) perform attestation and send the attestation report to the verifier.
- *Attestation*: Prover(s) in SPLIT will perform self-attestation. We have assumed that every prover in the network is capable of performing attestation as described in [17].
- *Send Report*: This operation is meant for attestation report corroboration to the verifier through intermediary nodes using DAO-attest message.

Algorithm 1: SPLIT execution for provers (i.e., non-root devices)

Step1: Initial setup of the network(s), devices are bootstrapped (with attestation details and device-ID).
Step2: RPL DODAG formation.
Step3: SPLIT initialization.
Step4: if (trickle-timer = true) then perform self attestation, send DAO-attest message to root, else send DAO-normal (RPL-default) to root
Step5: End and go to Algorithm 2 (SPLIT execution for verifier/root)

2) SPLIT-verifier: From verifier perspective, SPLIT also consist of four main functions to follow:

- *DODAG creation*: Verifier/Root node of the network will initialise the DODAG formation.
- *Verify Trickle time*: Based on trickle time verifier receives aggregated attestation report of the whole network through DAO-attest message.
- *Attestation report gathering*: Prover(s) in SPLIT will perform self-attestation and corroborate the report along with DODAG-tree.
- *Verify*: This operation is meant for attestation report verification by the verifier.

Algorithm 2: SPLIT execution for verifier/root

Step1: Receive DAO-attest.
Step2: If (Flag == 00) then block/remove the device from DODAG (as it is adversary)
else if (Flag == 11) then keep the device in DODAG (as it is in healthy state)
Step3: End of Algorithm 2.

IV. Simulation and Performance Evaluation

In this section, we present the performance evaluation of SPLIT using the simulation results. We have fully implemented SPLIT on top of the available open source code

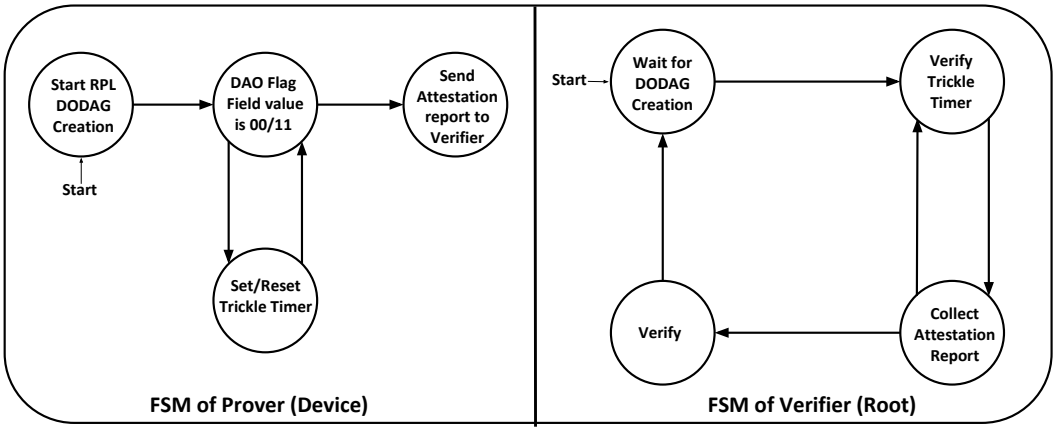

Fig. 4. SPLIT FSM-s for Prover (Device) and Verifier (Root)

of RPL protocol for IoT networks. The implementation is performed in *Cooja*, the Contiki network simulator [1], [25], which is widely used for deploying energy-constrained and memory-efficient devices. We make available[5] an open-source implementation of SPLIT. We have compared the performance of SPLIT with SRPL [16], and the traditional RPL protocol in different scenarios. The existing results of SRPL approach that are presented in [16] have been taken on very small network (i.e., 22 notes only including one Root node and two attackers node), which is not feasible for a scalable approach, so we took our results by increasing the same ratio of attacker nodes with respect to node density in the network used in SRPL [16]. Table I provides the details of various parameters along with their values that we have used to configure the target IoT network scenarios in *Cooja* simulator [13].

TABLE I
SIMULATION SETUP: PARAMETERS FOR SPLIT EVALUATION

Parameters	Values
Simulator	Cooja on Contiki v2.7
Simulation time	10 to 60 Minutes
Scenario Dimension	200 x 200 to 800 x 800 sq.meter
Number of nodes	101 sky motes (including root for fixed scenario)
Number of nodes	25 to 100 sky Motes (for node varying scenario)
Transport layer protocol	UDP
Routing Protocols	RPL and SRPL and SPLIT
Root waiting timer t	Depends on the value of α
Radio Medium	Unit Disk Graph Medium (UDGM)
PHY and MAC Layer	IEEE 802.15.4 with CSMA and ContikiMAC
Application protocol	CBR
Transmission Range	25m
Number of attacker nodes	5% to 50%
Traffic rate	0.50 pkt/sec - 500 packets
Average Mobility Speed	3 m/s

A. Security Analysis

In Section III-B, we have introduced the adversarial model. We now will analyse SPLIT's performance against those adversarial settings.

1) We consider a remote or local Adv who can launch software attacks on any Prv in the network by introducing malicious software. Although this attack is feasible, it will be recognized when the self-attestation is performed by the "Trusted" part of the Prv. Thus, Adv cannot compromise the attestation process.
2) The Adv mentioned in SecIII-B can launch attacks like eavesdropping and packet discarding. Firstly, eavesdropping, the Adv can eavesdrop the ongoing messages among nodes in the network but will not be able to compromise them. Use of *asymmetric key crypto* makes this attack unfeasible. Secondly, in case of packet discarding or blackhole attacks, the Vrf can quickly identify which of the nodes are missing after receiving the attestation results of the nodes during every trickle period.
3) Predominantly, we have considered software only attackers. But, use of trickle timer can help us identify the presence of physical adversaries. In fact, adversaries need a non-negligible amount of time to capture and perform malicious activities. It is safe to assume that the time required for mounting physical attacks is greater than two consecutive trickle time gap. During each trickle time interval, every device has to perform self-attestation and send the report to the Vrf. Thus, the Vrf will identify missing attestation report.
4) As shown in Table II, SPLIT requires negligible amount of extra power with respect to traditional RPL protocol, while introducing superior security feature in it. Thus, it leads to minimal overhead in the network.
5) Mobility is another crucial feature to be taken care of for IoT networks. However, most of the attestation literature has overlooked the mobility scenario. Unlike other attestation schemes [6], [7], [9], we consider adversarial device mobility in our experiments, and the results witness that the effectiveness of SPLIT to counter roaming adversary is similar in case of static adversary. SPLIT substantially improves the reliability and availability of the IoT network against the threats mentioned above.

We now present an comparative analysis of SPLIT with

[5]https://github.com/pallavikaliyar/SPLIT

respect to other protocols (e.g., RPL, RPLAttack, SRPL) using the metric called Average packet Delivery Ratio (APDR). As the different types of attacker (e.g., topological and data communication) nodes present in a network can adversely effect the APDR by altering different network parameters in order to disrupt the network. Therefore, it is indeed critical to show the performance of a network using APDR metric. The simulation results clearly depict the considerably better performance of SPLIT with respect to aforementioned protocols.

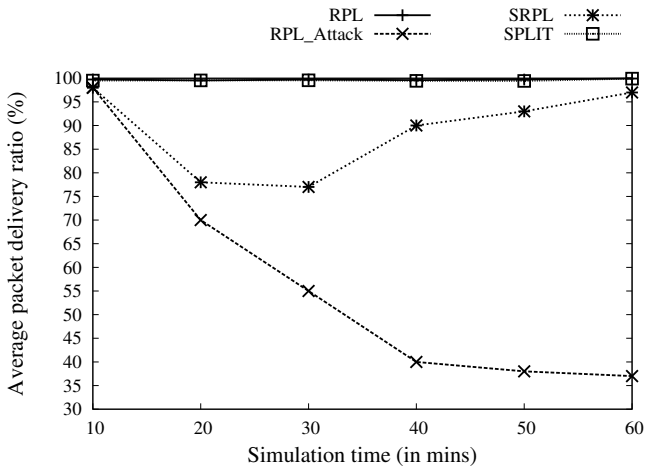

Fig. 5. APDR with respect to increasing simulation time

As shown in Figure 5, the APDR of SPLIT with respect to increasing time frame is substantially higher than RPLAttack (i.e.,with attacker node), and SRPL. At the same time SPLIT is providing better security by identifying attacker nodes. Thus, it provides better resiliency against attacker nodes in a network. Figure 6 shows SPLIT's significantly higher performance of APDR with respect to increasing number of nodes in a network. The comparison was drawn among SPLIT and RPL, RPLAttack protocols.

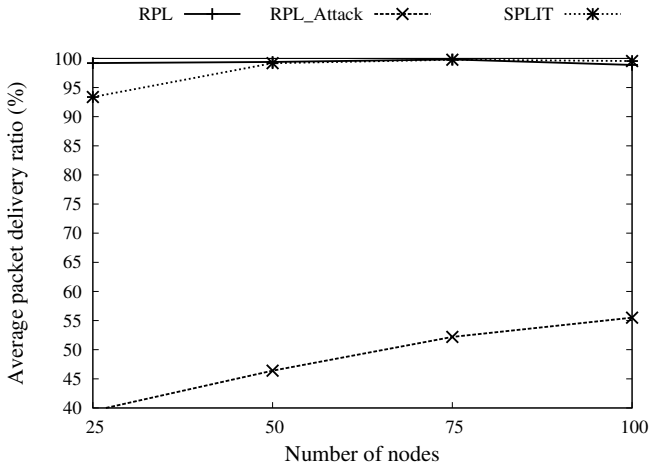

Fig. 6. APDR with increasing number of nodes in the network

Figure 7 exhibits SPLIT's superior performance compared to other aforementioned protocols with increasing number of attacker nodes in a network. These simulation results demonstrate SPLIT's better performance compared to other protocols. The main advantage apart from security and scalability is that SPLIT introduce minimal overhead, and the Figure 5 shows that SPLIT has high APDR like traditional RPL protocol. The main reason behind SPLIT's high APDR is, during initial attestation phase, SPLIT is able to identify and bar malicious nodes to adversely effect DODAG in the later phase. Thus making SPLIT an ideal candidate to replace general RPL over a legacy network.

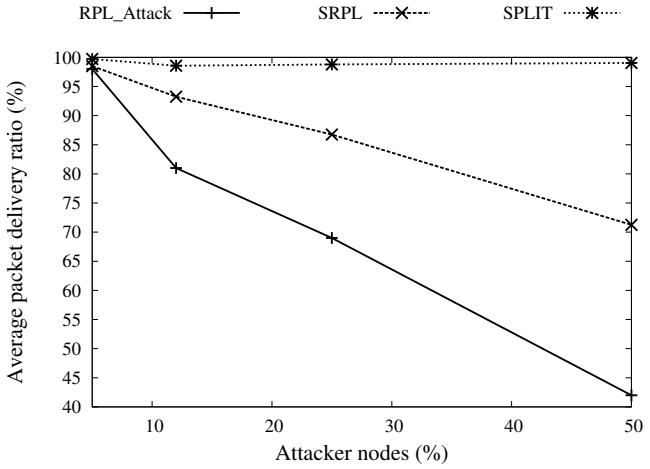

Fig. 7. APDR with increasing number of attacker nodes in the network

B. Energy Consumption Analysis

We compute the overall energy consumption based on energy required to send and receive SPLIT messages and to perform the main cryptographic operations. Let E_{send} be the energy required to send a byte, E_{recv} the energy required to receive a byte, E_{hash} the energy required to calculate a hash, and N the number of devices participating in attestation process. As mentioned in Section III-C based on trickle time at each round t all Prv sends the attestation time T_{att}, and a hash. Thus, we can estimate the energy consumption for sending a single SPLIT message for prover Prvi as follow:

$$E_{send}^{Prv_i} \leq E_{hash} + DAO_{Message}.$$

Similarly the energy consumption for receiving a message is calculated as follow:

$$E_{recv}^{Prv_i} \leq (E_{hash} + DAO_{Message}) * N.$$

Furthermore, we consider the power consumption and duty cycle based on standard contiki measurement[6]. The energy consumption and duty cycle are mention in Table II.

Based on our simulation results, the energy consumption of nodes in SPLIT is less, and most importantly it does not have a significant difference from general RPL energy consumption. The important achievement of SPLIT is that we are performing

[6]http://thingschat.blogspot.com/2015/04/contiki-os-using-powertrace-and.html

TABLE II
POWER CONSUMPTION WHILE SPLIT SIMULATION FOR SKY MOTES

Time (In sec)	CPU Power consumption (mW)	Duty Cycle (mW)
10	0.007528931	0.007228695
20	0.02099762	0.022265709
30	0.007731354	0.007289762
40	0.007423187	0.006024465
50	0.007767609	0.015067756
60	0.128571899	0.224695261
70	0.031744171	0.039779544
80	0.092942413	0.136530826

attestation of network devices without introducing additional high overheads from energy consumption perspective as mentioned in Table II. This minimal cpu power consumption and duty-cycle proves its efficiency for large-scale network implementation.

V. CONCLUSION

We presented *SPLIT*, the first RPL based energy efficient and scalable device attestation approach for IoT networks that consists of large swarms. On one hand, SPLIT helps to substantially improve the attestation speed with minimal additional overheads for large swarms over IoT networks, while on the other hand, it increases the security, and availability in data communication process of RPL. The performance analysis of SPLIT which is done on *Cooja* emulator on various IoT network scenarios regarding essential metrics such as communication security, network overheads, scalability, and energy efficiency clearly shows its effectiveness. Finally, we also noted that SPLIT performed better for security perspective concerning scalability and energy efficient with no network delays.

As a future work, we will investigate SPLIT's performance over the more robust network of intermittent connectivity; we will also look into different approaches to minimise hardware assumptions by reducing secure code and cryptographic device specific details for attestation. Apart from the aforementioned works, we would also like to implement SPLIT on a real environment to validate its performance and energy consumption.

ACKNOWLEDGEMENT

This work is partially supported by the EU TagItSmart! Project (agreement H2020-ICT30-2015-688061), the EU-India REACH Project (agreement ICI+/2014/342-896), and the grant n. 2017-166478 (3696) from Cisco University Research Program Fund and Silicon Valley Community Foundation.

REFERENCES

[1] Get Started with Contiki. http://www.contiki-os.org/start.html.
[2] Jeep hacking 101. https://goo.gl/ulBt4U, 2015.
[3] T. Abera, N. Asokan, L. Davi, J. Ekberg, T. Nyman, A. Paverd, A. Sadeghi, and G. Tsudik. C-FLAT: control-flow attestation for embedded systems software. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austri*.
[4] T. Abera, N. Asokan, L. Davi, F. Koushanfar, A. Paverd, A.-R. Sadeghi, and G. Tsudik. Invited: Things, trouble, trust: on building trust in IoT systems. In *DAC '16*.
[5] 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*, pages 1–18, 2018.
[6] M. Ambrosin, M. Conti, A. Ibrahim, G. Neven, A.-R. Sadeghi, and M. Schunter. SANA: Secure and Scalable Aggregate Network Attestation. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16.
[7] N. Asokan, F. Brasser, A. Ibrahim, A.-R. Sadeghi, M. Schunter, G. Tsudik, and C. Wachsmann. SEDA: Scalable embedded device attestation. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15.
[8] F. Brasser, B. El Mahjoub, A.-R. Sadeghi, C. Wachsmann, and P. Koeberl. Tytan: tiny trust anchor for tiny devices. In *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE*.
[9] X. Carpent, K. ElDefrawy, N. Rattanavipanon, and G. Tsudik. LIghtweight Swarm Attestation: a Tale of Two LISA-s. In *Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security*, ASIACCS '17.
[10] M. Conti, P. Kaliyar, and C. Lal. Remi: A reliable and secure multicast routing protocol for iot networks. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ARES '17, 2017.
[11] M. Conti, P. Kaliyar, and C. Lal. Censor - cloud enabled secure iot architecture over sdn paradigm. *In (Wiley) Concurrency and Computation: Practice and Experience*, 2018.
[12] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti. A large-scale analysis of the security of embedded firmwares. In *Proceedings of the 23rd USENIX Conference on Security Symposium*.
[13] A. Dunkels. Contiki OS. http://www.contiki-os.org/download.html.
[14] A. Dvir, T. Holczer, and L. Buttyan. Vera - version number and rank authentication in rpl. In *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*.
[15] K. Eldefrawy, G. Tsudik, A. Francillon, and D. Perito. SMART: Secure and Minimal Architecture for (Establishing Dynamic) Root of Trust. In *Proceedings of the 19th Annual Network & Distributed System Security Symposium*, NDSS '12.
[16] 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)*, pages 1–7, Dec 2016.
[17] A. Ibrahim, A.-R. Sadeghi, and S. Zeitouni. SeED: Secure Non-Interactive Attestation for Embedded Devices. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '17.
[18] A. G. Illera and J. V. Vidal. Lights off! The darkness of the smart meters. In *In BlackHat Europe*, 2014.
[19] 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 Communications Surveys Tutorials*, 19, 2017.
[20] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko. The trickle algorithm (rfc 6206). 2011.
[21] S. R. Linus Wallgren and T. Voigt. Routing attacks and countermeasures in the RPL-based internet of things. *International Journal of Distributed Sensor Networks*, 2013.
[22] D. Perito and G. Tsudik. Secure Code Update for Embedded Devices via Proofs of Secure Erasure. ESORICS, 2010.
[23] H. Perrey, M. Landsmann, O. Ugus, M. Wählisch, and T. C. Schmidt. TRAIL: Topology authentication in RPL. In *Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks*, EWSN '16.
[24] C. Pu. Mitigating dao inconsistency attack in rpl-based low power and lossy networks. In *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*.
[25] I. Romdhani, A. Al-Dubai, M. Qasem, C. Thomson, B. Ghaleb, and I. Wadhaj. Cooja simulator manual. Technical report, 2016.
[26] R. Sahay, G. Geethakumari, and K. Modugu. Attack graph based vulnerability assessment of rank property in rpl-6lowpan in iot. *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*.
[27] R. Sailer, X. Zhang, T. Jaeger, and L. van Doorn. Design and implementation of a tcg-based integrity measurement architecture. In *Proceedings of the 13th Conference on USENIX Security Symposium*.
[28] A. Seshadri, A. Perrig, L. Van Doorn, and P. Khosla. SWATT: Software-based attestation for embedded devices. In *Proceedings of the 2004 IEEE Symposium on Security & Privacy*, IEEE S&P '04.
[29] 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). 2012.