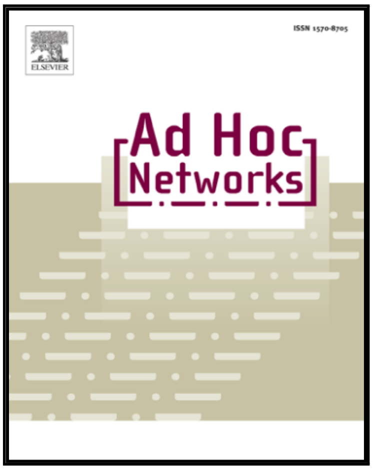


Attestation-enabled Secure and Scalable Routing protocol for IoT Networks

Mauro Conti, Pallavi Kaliyar, Md Masoom Rabbani, Silvio Ranise

PII:	S1570-8705(19)30447-0
DOI:	https://doi.org/10.1016/j.adhoc.2019.102054
Reference:	ADHOC 102054
To appear in:	*Ad Hoc Networks*
Received date:	7 May 2019
Revised date:	13 November 2019
Accepted date:	30 November 2019

Attestation-enabled Secure and Scalable Routing protocol for IoT Networks

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

***Abstract*—Cybercrime in the past decade has experienced an all-time high due to the inclusion of so-called smart devices in our daily lives. These tiny devices with brittle security features are often dubbed as the Internet of Things (IoT). Their inclusion is not only limited to our daily lives but also in different fields, for example, healthcare, smart-industries, aviation, and smart-cities. Although IoT devices make our lives easy and perform our jobs in a smart way, their fragile security mechanisms pose a severe challenge regarding safety and privacy of its users. Attacks like Stuxnet, and Mirai-botnet are the key examples of the damages that can be caused by maliciously controlling these devices. One effective tool to identify a malicious entity at a network device is to perform Remote Attestation (RA). However, performing RA over a large, heterogeneous IoT network is difficult tasks due to resource constrain nature of these networks. To this end, we propose a novel scheme called *SARP*, which is an attestation-assisted secure and scalable routing protocol for IoT networks. SARP performs attestation in large scale IoT networks by using Routing Protocol for Low Power and Lossy Networks (RPL) framework and exploiting the inbuilt features of RPL. In particular, SARP uses attestation technique that not only secures the network from internal attacks, but it also provides security to RPLs data communication process, which helps to improve the overall network performance. Moreover, SARP supports network mobility, device heterogeneity, and network scalability, while it does not sacrifice the key requirements of IoT networks such as low energy and memory consumption, and low network overhead. The simulation results obtained in different IoT scenarios in presence of various types of attacks show the effectiveness of SARP, concerning energy consumption, packet delivery ratio, network overhead, data integrity, and communication security.**

***Index Terms*—Routing Protocol for Low Power and Lossy Networks, Internet of Things, Attestation, Security, Routing.**

I. Introduction

In recent years, there has been an exponential increase in the growth of the Internet of Things (IoT). Millions of heterogeneous IoT devices are connected with each other in various application scenarios, such as health monitoring, automated buildings, military-applications, and smart city. Adoption of these “wonder-pills” in our day-to-day live makes daily-tasks easy, smarter, and automated. However, along with benefits, it introduces new type of threats as it opens a new cyber-space for hackers to exploit [34]. Attacks like Mirai-botnet [23] and smart-tv hack [3], [13], [2] fuel the concern of security and safety in the general publics’ mind.

Due to the high demand and less time to market approach, these tiny devices often lack in proper testing and security features [32]. These vulnerabilities are prone to exploit. Thus, it expose the users to a wide category of attacks [35], [33], [7]. As often these attacks lead to financial loss [1] or even worse. A low-cost solution to identify malicious devices is to perform attestation. However, the naive device-to-device remote attestation comes with a price concerning high attestation time and communication overhead, and scalability challenges. The naive applications of remote attestation do not scale for systems that consist 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 attestation solutions to safeguard network operations consist of IoT devices.

Internet Engineering Task Force (IETF) group called Routing Over Low Power and Lossy networks (ROLL) has made a number of efforts for designing an efficient routing protocol for low power and lossy networks (LLNs). In March 2012, IETF as RFC6550 [46] has adopted Routing Protocol for Low Power and Lossy Networks (RPL) as an Internet Protocol version 6.0 (IPv6), which is intended to be applicable in all sorts of applications and deployments of LLNs (e.g., IoT). Due to its lightweight functionality, RPL fits well with the resource constrain nature of IoT devices and networks. RPL is considered as a simple, flexible, scalable, and interoperable networking protocol that can be used for different IoT applications [24].

A. Motivation

The ever-increasing attacks on devices that are connected to an IoT infrastructure [27], where attackers exploit the low-computation and brittle protection of these devices; lead researchers to propose different schemes [39], [48], [25], [8] to safeguard these devices which leads to the safety of the whole network. Apart from security, the IoT networks also pose other challenges. For instance, the exponential growth of the IoT network requires security solutions to scale, however, scalable security features incur costs concerning complexity and computational overheads. Thus, we need a lightweight and secure protocol that can scale and is also compatible with dynamic network demands [28]. Therefore, to create a scalable and flexible secure scheme for IoT, we present a attestation-enabled Secure and Scalable Routing protocol for IoT Networks (SARP) for IoT networks. In SARP, we provide a realistic setting for IoT networks that will guarantee the safe and secure multi-layered low-cost operations along with scalable and modular design options for the network owner that could be customized as per the demands of IoT application.

This paper is an extension of our previous work called SPLIT. The basic idea behind SPLIT along with the initial simulation results were first presented in [17]. Apart from minor extensions in all the sections, we have extended SPLIT mainly in two ways:

- the functionality of SPLITs attestation mechanism is extended to improve its security against internal as well as external attacks. We have performed a detailed security analysis w.r.t different attackers and adversarial assumptions, which we present in section V-B to show the improvements that SARP provides over other RPL based attestation schemes, and
- the evaluation section is significantly enhanced by including additional results obtained on large number of target scenarios with varying network size, simulation time, and number of attacker nodes. Also, the result analysis is extended to evaluate the proposed protocol for various new network metrics which are important and were absent in SPLIT (e.g., energy and memory consumption).

B. Contribution

Our proposal (*SARP*) uses the unique advantages of de-facto IoT routing protocol called RPL [46] to perform an efficient (concerning attestation time, energy consumption, and network overhead) device self-attestation in large-scale IoT network. The use of device self-attestation technique improves the security in data communication process of RPL by making it more robust against an array of routing threats, such as *rank* [21], [25], and *sybil* [45], [48], [8] attacks. The primary aim of SARP is to ensure the integrity of the IoT devices and the data packets that they exchange. It is because these are considered as significant challenges in deployment of large-scale secure IoT networks. To this end, the paper has the following key contributions.

- We propose an attestation-enabled Secure and Scalable Routing protocol called (*SARP*) for IoT networks. SARP makes optimized use of the RPL's route maintenance process, where periodic topology maintenance takes place by sending control messages to the Root node (i.e., Verifier). We show that SARP achieves the attestation scalability while keeping the attestation overhead and the device attestation time to the minimum. In particular, SARP uses a modified version of RPL's periodic DAO[1] control message called $\text{DAO}_{\text{crypt}}$ (Crypted Destination Advertisement Object). $\text{DAO}_{\text{crypt}}$ carries not only the usual route maintenance information but also the attestation report for the Verifier. In this way, SARP utilizes the DAO control messages effectively and efficiently to make RPL more secure over a large heterogeneous IoT network.
- Unlike other attestation schemes [12], [9], [15] which has overlooked the mobility scenarios, we consider adversarial device mobility in our experiments. The evaluation results witness the effectiveness of SARP to counter roaming adversary along with a static adversary. SARP is the first that substantially improves the reliability and availability of the IoT network against internal threats.
- We fully implement SARP in *Contiki-Cooja* environment, which is a network emulator widely used for deploying resource constrained LLNs such as IoT. We perform the security and energy efficiency evaluations. With simulation results, we have shown the correctness and effectiveness of SARP. The results indicate that SARP is able to effectively perform the device attestation in moderate mobility scenarios, which is a major improvement with respect to the traditional state-of-the-art RPL schemes. We make available[2] an open-source implementation of SARP to the research community.
- Finally, we also prove that our proposal effectively performs a lightweight attestation which is essential requirement due to inadequate computational power of the IoT devices. Our results show that energy consumption for our protocol is affordable by low-end embedded devices (please refer to Section V).

C. Organization

The rest of the paper is organized as follows. In Section II, we briefly explain background, state-of-the-art, and working of device attestation process and RPL protocol. In Section III, we present system requirement and adversary model. Section IV provides detailed description of our proposed approach (i.e., SARP) along with its working methodology and design considerations. In Section V, we present the simulation setup details and performance evaluation of SARP. Section VI provides the limitations of our approach. Finally, in Section VII, we conclude our work along with the possible directions for future work.

II. Background and Related Work

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 [43], [42], [4], [36], [10] having different working procedure. In particular, 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 without any adversarial presence. Figure 1 depicts a Vrf sending a challenge to an untrusted Prv. Upon receiving the challenge, 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. Although RA is an efficient method to validate device's health, but it is hard to implement on large networks due to its one-to-one

[1] an ICMPv6 control message used in RPL protocol for topology maintenance.

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

verification model. RA incurs cost in terms of computation, storage, communication overhead, and battery power. Often the computational burden introduced by RA schemes are intolerable for low-end embedded devices, thus, most of the IoT framework do not implement computationally heavy security mechanisms as a trade-off to better performance and energy savings. However, recently researchers addressed the issues by distributing and offloading the attestation process to the verifier(s) itself or making the operation lightweight [38]. To achieve low-cost and secure networks, RPL along with RA can be a suitable solution due to their unique interoperability [17]. As an ongoing effort, we propose to make the attestation process efficient and lightweight by utilising existing RPL framework. In SARP, we utilize DAO packet structure to communicate attestation results to the prover, instead of introducing another set of network communication messages. Also, unlike other attestation schemes where a *Vrf* sends attestation request to the network, we use trickle-time to automatically initiate attestation process. Thus, it saves the communication burden and help networks to tackle several attacks like man-in-the-middle attacks or replay attacks.

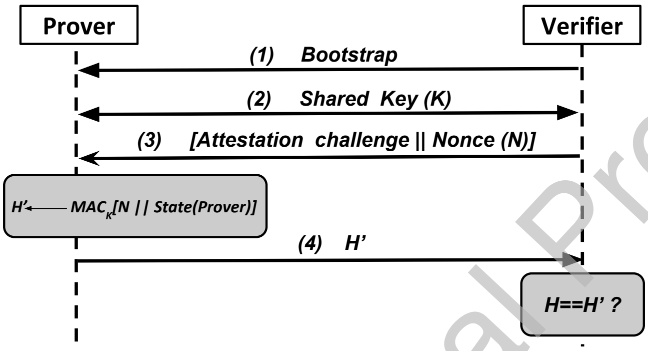

Prover
Verifier
(1) Bootstrap
(2) Shared Key (K)
(3) [Attestation challenge || Nonce (N)]
H'← MAC_K[N || State(Prover)]
(4) H'
H==H' ?

Fig. 1: Typical example of Remote Device-Attestation

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

RPL [46] is based on a virtual routing topology called Destination-Oriented Directed Acyclic Graph (DODAG) on top of an underlying physical topology. The DODAG is a directed graph oriented towards a root node without loops. In DODAG, each node have multiple parents towards the root, however, a node selects only a preferred parent based on routing metric and objective functions. The parent node will be used for forwarding data packets. The structure of DODAG supports multipoint-to-point communication in RPL, which provides communication from the nodes to the root. Each node receives a rank ID that depends on its distance from the root. The creation and the maintenance of the DODAG is done through ICMPv6 control packets known as DODAG Information Objects (DIO). Each node in RPL disseminates DIO packets, containing the link, node metrics, and an objective function that is used by each node to select the preferred parent among its neighbors. The node metrics contain values such as the expected transmission count (ETX) and the residual energy. To maintain the DODAG, DIO packets are rebroadcast by each node based on the Trickle algorithm [31]. Another control packet known as DODAG information solicitation (DIS) packet is triggered when a new node wants to join an existing DODAG. The DODAG node receiving the DIS will send a DIO packet.

RPL supports different types of communication such as point-to-multipoint, point-to-point, and multipoint-to-point, and it provides two modes known as storing and non-storing. In storing mode which is based on table-driven routing, the non-root nodes create and maintain a routing table for all their descendant nodes. While in non-storing mode which is based on source routing, only the root node create and maintain the routing information about all the network nodes. The creation and maintenance of routing tables in both the RPL modes is done with the help of RPL's control packets called Destination Advertisement Object (DAO). Each non-root node sent these packets towards the root to announce itself as a possible destination to the root. During their way towards root, these packets pass through their ancestors, thus establishing "downwards" routes along the way. The full implementation details of RPL and its design goals are out of the scope of this paper. Hence, we direct the interested readers to more comprehensive literature on RPL protocol given in [46], [29].

C. Related Work

As we have previously mentioned that due to the standardization of RPL routing protocol and in quest of providing the best Quality of Service (QoS) while routing, RPL is exposed to many security threats. RPL is strong against the external intruders given the cryptographic and authenticating techniques it uses. However, when it comes to an internal malicious node, the important parameters such as rank, node ID, and DODAG version number can be compromised.

In [21], a security service against internal attacks called *VeRA* is presented, which stop the malicious nodes from illegitimately increasing their DODAG version number and manipulating the rank. In VeRA, a one-way hash chain is used to assign and manage the correct values of rank, and each node is able to counter the illegitimate increase in the parent rank. In [30], the authors show that VeRA is still vulnerable to rank attack, and they proposed a new approach namely TRAIL (Trust Anchor Interconnection Loop). TRAIL is based on the topological authentication. Unlike VeRA, it utilizes 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 in TRAIL. On receiving a message from the parent, the child sends an authentication message with its rank and a nonce. Each upward node check for two things: (i) rank of the node sending the test messages is higher than its own, and (ii) difference of rank between the sending node and his own. Any non-corrupt node can easily check the integrity of the message and on not receiving the reply, it can put its parent in fault list. Recently, authors in [41] describe the vulnerabilities and attacks adhered due to rank property in RPL. Authors propose an approach namely Attack Graph, which helps to analyze the attacks better as it provides all the possible action sequences taken to launch an attack.

In [37] authors discuss the effects of DAO inconsistency attack and propose a solution to mitigate it by using a Dynamic Threshold Mechanism (DTM). In DAO inconsistency attack, a malicious node intentionally drop the received packet and forward a new packet with Forward Error Bit. This makes the ancestor nodes to drop the route in their routing tables and again look for new root which causes additional overhead and energy consumption. A solution for the attack is provided in which every node has a limited threshold of 20 forwarding error messages. The main drawback 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 [8], a trust-based mechanism is presented to detect and isolate sybil and rank attacks in IoT. The proposed trust mechanism has five phases which includes Trust Calculation, Trust Monitoring, Detection and Isolation, Trust Rating, and Backup, to detect and mitigate the rank and sybil attack in the system.

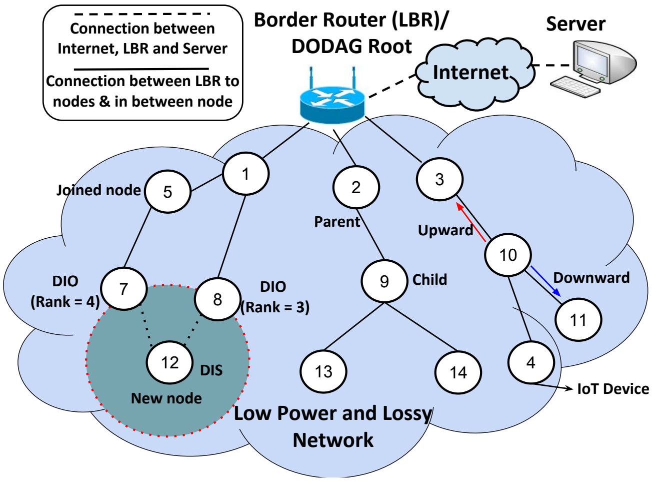
A new Secure RPL (SRPL) is proposed in [25], which stops mischief caused by the internal attacks in RPL. SRPL uses the concept of threshold rank and hash-chains for authentication. The main drawback of the threshold mechanism is that it acts against all the nodes including the non-malicious node with a large set of descendants, and it causes additional overhead in the start due to the use of hashing technique. Previous research on RPL has mainly focused on making communication among IoT devices more secure and reliable for routing, but none has considered the problem of device authenticity. For instance, a genuine device running a corrupt or compromised software. The lack of device authenticity mechanism makes RPL vulnerable to various security threats such as rank attack and sybil attack, which decreases the communication efficiency and disrupt the correct working of the network. Although, RPL still provides energy efficiency, adaptivity to work in various environments, and scalability which makes it best suited for resource-constrain large IoT networks [16], [17]. Due to all these positive features of RPL, in our proposed approach we consider device integrity and confidentiality to make the overall communication system more secure and reliable.

III. System Assumptions and Adversary Model

In this section, we present the details of the system and adversary models on which SARP is implemented and evaluated, and we also discuss SARP's security requirements.

A. System Model

- The network consists of a set $Z = \{Z_1, Z_2, ...Z_n\}$ of size n resource constraint IoT nodes (i.e., sensors and actuators). These nodes are static/mobile (for different set of experiments) within the network area and are homogeneous concerning resources. However, depending on the device type, the nodes could be heterogeneous with regard to their functionalities (different underlying software or hardware). Figure 2 shows an overview of the system model on which SARP is implemented and evaluated.



Connection between Internet, LBR and Server
Connection between LBR to nodes & in between node
Border Router (LBR)/ DODAG Root
Server
Internet
Joined node
1
2
3
5
Parent
Upward
10
Downward
DIO (Rank = 4)
7
8
DIO (Rank = 3)
9
Child
11
12
DIS
New node
13
14
4
IoT Device
Low Power and Lossy Network

Fig. 2: RPL Functioning

- RPL creates a virtual DODAG on top of the physical network topology. For our experimental purpose, we assumed the presence of malicious nodes (Adv) in target network. The root node plays a critical role in creating and maintaining the DODAG in the network. Additionally, in our system the root node also plays the role of the Verifier Vrf.
- In line with other RA schemes, devices on the network have trusted execution environment [22], [14] that is not accessible to any unauthorized entity, 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 3.

In this work, we assume that the root node is trusted entity. However, in a realistic setting, the root might be accessible to potential adversaries. In that case, traditional security measures can be introduced to check the sanity of the root node. Note that SARP's goal is to make sure that the root node can successfully monitor and attest the other nodes in the network. Furthermore, securing communication channels among different entities fall out of our current scope. However, we encourage proper authentication and encryption should be done.

B. Adversary Model

Based on the taxonomy in [5], we consider software adversaries which are capable of mounting software-only attacks either remotely or being present locally near to the device. We keep physical Adv out of the scope of our work. However, we will address possible detection mechanisms for physical tampering in SARP by employing a scheme that could identify device absence (for a non-negligible amount of time) in the network, thus, it signals the possible presence of physical adversaries. In our target IoT network scenarios, the Adv are assumed to have the following characteristics.

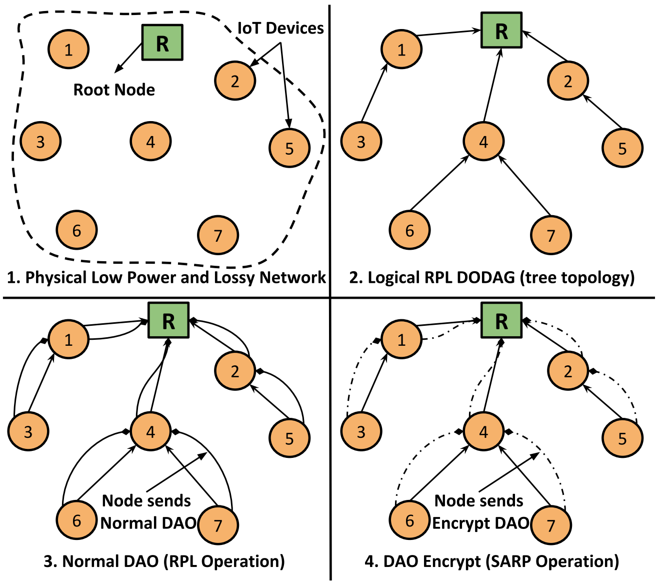

IoT Devices
R
Root Node
1
2
3
4
5
6
7
1. Physical Low Power and Lossy Network
2. Logical RPL DODAG (tree topology)
Node sends
Normal DAO
3. Normal DAO (RPL Operation)
Node sends
Encrypt DAO
4. DAO Encrypt (SARP Operation)

Fig. 3: SARP device attestation technique

- $\text{Remote}_{\text{adv}}$: the *Adv* is capable of launching various attacks like cloning, sybil, rank, blackhole, eavesdropping, and wormhole, to name a few. It can compromise an existing node or it can be part of an existing network as a new node to perform all of the aforementioned attacks. However, we assume that the *Adv* cannot compromise the DODAG root (i.e., LBR).
- Moving_{Adv}: the adversary is mobile and can join the network for a short period of time and attempt to perform malicious activities to disrupt the integrity of the network.
- Physical_{Adv}: although this type of adversary is out of the scope of our work. In Section V-B, we discuss the possible way to detect the presence of a physical adversary.

Apart from above adversarial assumptions, we also consider an adversary who has full control over communication channels (Dolev-Yao model [19]), and it can manipulate messages that are exchanged between devices and root node.

a) Assumptions.: We assume that Software_{Adv} and Roaming_{Adv} can manipulate the software at nodes. Nonetheless, those aforesaid adversaries can not tamper the protected hardware. In addition, attacks like code-reuse or runtime, distributed denial of services (DDoS) attacks are out of our current scope.

C. Security Requirements

In order to be considered successful, SARP has to fulfill below four design goals while addressing the adversarial threats in the network.

Preserving the integrity of the network: The protocol, through attestation, should identify and remove compromised nodes which in turn provides reliability in preserving the sanity of the whole network.

Unforgeable communication: The protocol should guarantee the authenticity of the message-communication among different nodes in the network. It must ensure that the messages are not modified by unauthorized entities in their way.

Freshness: The protocol should be able to detect where a compromised node is trying to evade detection by sending precomputed attestation result or launching replay or man-in-the middle attacks.

Lightweight operation: Operations performed by the proposed protocol should be lightweight due to the resource-constrain nature of network devices. Computationally heavy operations will degrade the performance of overall network operations.

IV. Our Proposal: SARP

In this section we provide detailed design principles of SARP and how SARP works over an RPL based IoT network.

A. SARP Design Rationale

For SARP, we optimize and combine the best features of RPL protocol with traditional device attestation scheme. The primary purpose of SARP's development is to improve network security by considering the scalability factor in large-scale IoT networks. SARP's functioning uses device remote attestation scheme without introducing additional overheads on the network. In particular, SARP effectively exploits 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. It extends the functionality of DAO ICMPv6 control messages [29] of RPL to piggyback the attestation reports to the verifier. Moreover, the integration of hybrid attestation[3] scheme with RPL ensures the authenticity of the nodes that take part in the routing process, which leads the whole process of routing more robust against various routing attacks.

SARP aims to inherit the features of traditional RPL and use them to improve the data communication system through device attestation. Through our evaluations, we show that SARP has significant advantages over traditional routing protocols in IoT regarding network overhead, energy consumption, and communication security. Moreover, SARP can be easily adopted in existing IoT infrastructures because its implementation uses the RPL protocol, which is already considered as a de-facto routing protocol for these networks. Below, we present the SARP design rationale that enables its desired functionalities that are needed to perform secure communication in efficient way.

- For attestation purpose, SARP uses RPL DAO ICMPv6 control messages whose header fields are enhanced accordingly as it is shown in Figure 4. The modified and newly added data structures are as follow: (i) a 4 bit *"flag"* field to send the node ID, (ii) 8 bit *"reserved"* field for sending the "attestation result 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) represent

[3] Hardware-Software co-design to safeguard attestation related details from attackers.

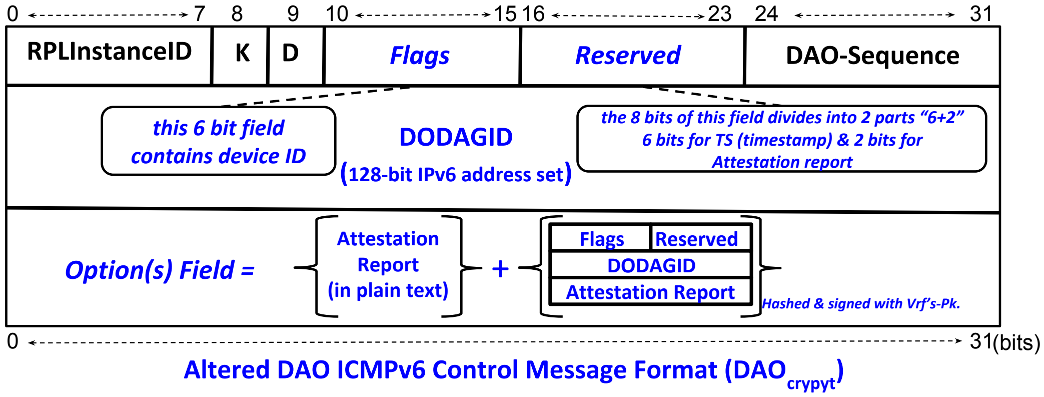

0
7
8
9
10
15
16
23
24
31
RPLInstanceID
K
D
Flags
Reserved
DAO-Sequence
this 6 bit field contains device ID
DODAGID
(128-bit IPv6 address set)
the 8 bits of this field divides into 2 parts "6+2" 6 bits for TS (timestamp) & 2 bits for Attestation report
Option(s) Field =
Attestation Report (in plain text)
+
Flags
Reserved
DODAGID
Attestation Report
Hashed & signed with Vrf's-Pk.
0
31(bits)
Altered DAO ICMPv6 Control Message Format (DAO_crypyt)

Fig. 4: Modified DAO ICMPv6 Control Message Format

the outcome of self-attestation" to the root, and (iii) a 32 bit *"option"* field to send *encrypted hash of the DAO message* (DAO_{crypt}) of the device along with the attestation result in plain text. The attestation result contains the hash value of the underlying software of the device and a time-stamp to prove its time-bound freshness. The attestation message (say D_k) for any device is as follow.

$$D_k{}^{\text{Att}} = (Hash_{D_k}||Timestamp)Root_{pk}$$

.

Where $D_k{}^{\text{Att}}$, 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 it.

- In SARP, during the self-attestation process, the nodes first perform the hashing of the above mentioned modified DAO ICMPv6 message, and then encrypt the resultant hash string with the public key of the root [4]. The result of the encryption along with the self-attestation report (in plain-text format) is stored in the DAO 32-bit option field. The hashing and encryption is essential to maintain the integrity of the DAO messages and also of the self attestation report, which resides in the DAO message. For example, an adversary could alter the attestation report during its way towards root (or Vrf). In SARP, such alterations will be identified at root when the matching of the decrypted [5] hash string is performed with the hash of the plain-text attestation report. It is because changing the plain-text self-attestation report or the encrypted hash value will create a mismatch during hash comparison at the root.
- Performing encryption over self-attested value incurs cost in terms of computational overhead and memory consumption. However, in SARP, we exploited the DAO message packet to relay the attestation result to the root. The clever design rationale does not consume any extra memory for communicating the attestation result in the network. Thus, the modified DAO message packet (i.e., DAO_{crypt}) provide the network owner with minimal overhead in terms of memory consumption. In addition, computational overhead for encryption operation is a trade-off for security of the network.
- Our approach uses the non-storing mode of the RPL (i.e., MOP2) because it is best suited for resource-constrained devices due to its support for minimal memory and computational requirements. In addition, during the MOP2, each device in the network sends the above-mentioned DAO control messages directly to the root node. In SARP, the DAO message apart from its various responsibilities (e.g., providing route support from downwards to upwards towards root in the DODAG) also work as a beacon message, which provides the device attestation report to the root after a specific time interval called "Trickle-Timer". The Trickle-Timer controls the generation rate of beacon (or DAO) messages [31]. In SARP, the timer is tuned to send the DAO_{crypt} message to the Vrf. 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$_{Adv}$.
- Network owners can decide the frequency of the network-wide attestation process through trickle-time algorithm. Trickle-time provide the root with the evidence of attestation freshness as every node in the network has to include the current timestamp with the calculated attestation result. Upon receiving the trickle-time a node will perform self-attestation with the help of hybrid root of trust (i.e., TEE). An optimised value for the trickle-time depending upon the target application's requirements can effectively improve the network security while providing a trade-off between network overhead and security. In particular, a lower value of "Trickle-timer" will increase the frequency by which the attestation process is performed in the network, a higher frequency will allow early detection of an attack but it will also increase the network overhead caused by the DAO_{crypt} messages.
- The DAO control message acts as regular DAO mes-

[4] The public key of root node resides in the TEE along with the attestation software.

[5] Only root node can perform the decryption because the encryption is done using its public key.

sages in the network, the modified DAO message (i.e., DAO_{crypt}) 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 root node (i.e., verifier). Then, on the basis of the attestation report, the verifier decides the next step (please refer to Figure 5).

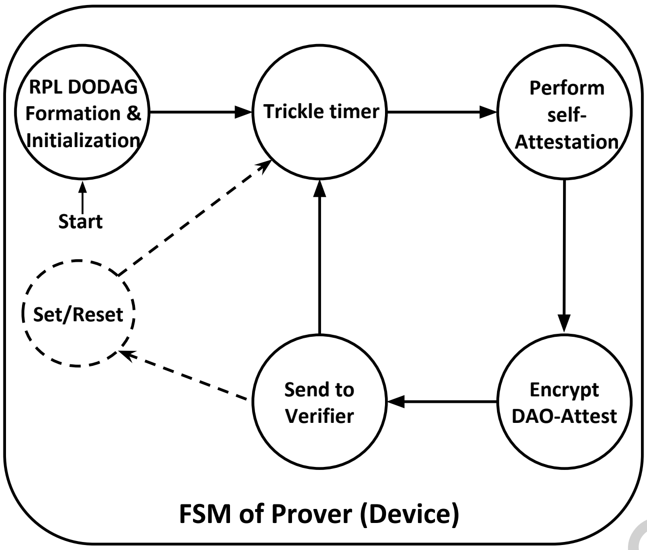


Fig. 5: SARP FSM-s for Prover (IoT Device)

- Our previous proposal “SPLIT” make use the inbuilt features of DAO messages. However, the updated DAO message was not immune to the internal network attacks, where an Adv can manipulate the message by altering the Flags and Reserved fields, i.e., the message integrity was not supported in SPLIT. Additionally, to overcome the shortcomings and to make the attestation result immune to the aforesaid attacks, we employ the SHA-256 [18], which encrypt the whole DAO message and send it in option field of DAO_{crypt}. Furthermore, the network Adv cannot manipulate with the DAO_{crypt} packet in polynomial time.
- The DAO_{crypt} message is encrypted with the Vrf's public-key [6]. Using the key cryptography, SARP provides another layer of security because an Adv may try to forge the DAO_{crypt}, however, the Vrf can identify the same from the received attestation results.

B. SARP Working Methodology and Functioning

The primary stakeholders in SARP are (1) Verifier (Vrf), and (2) Prover (Prv). The notations used for describing the SARP working is shown in Table I. Algorithms 1 and 2 summarizes SARP's pseudocode for prover and verifier. Also, the finite state machine (FSM) model for both Prover (device) and Verifier (Root/LBR) is shown in figures 5 and 6.

TABLE I: Notation Table

Symbol	Definition
D_{id}	Device Id
D_{sec}	Encryption details
D_{att}	Device specific attestation result
TT_{attest}	Trickle timer for attestation timing
DAO_{crypt}	Encrypted DAO message
Vrf_{rcv}	Verifier's receiving function
R_{node}	Remove node function for VRF
Prv	Prover or Device
Vrf	Verifier node in RPL DODAG (root node)

1) SARP-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 timer*: Based on the trickle-timer, prover(s) perform attestation and send the attestation report to the verifier.
- *Attestation*: Prover(s) in SARP will perform self-attestation. We have assumed that every prover in the network is capable of performing attestation as described in [26].
- *Encryption*: Prover(s) will encrypt the attestation message using SHA-256. We call the encrypted attestation message DAO_{crypt}. However, usual network related operations will carry on using the general DAO messages.
- *Send Report*: This operation is meant for attestation report corroboration to the Vrf through intermediary nodes using DAO_{crypt} message.

Algorithm 1 SARP execution for Provers

```
$D_{id} \leftarrow Device_{id}$;
$D_{sec} \leftarrow attestation\ related\ cryptographic\ details$;
$D_{att} \leftarrow Device\ specific\ self\text{-}attestation\ details$;
$TT_{attest} \leftarrow Trickle\ timer$;
$DAO_{crypt} \leftarrow\ 0$;
while True do
    DODAG Formation();
    if == "True" then
        Perform $D_{att}$;
        $M_{att} \leftarrow encrypt\ attestation\ message$;
        $DAO_{crypt} \leftarrow M_{att}$;
        Send DAO$_{crypt}$;
    else
        perform normal operation;
        send (DAO)
    end
end
```

2) SARP-verifier: From a verifier's perspective, SARP also consist of four main functions which are as follow:

- *DODAG creation*: Verifier/Root node of the network will initialise the DODAG formation.
- *Verify Trickle timer*: Based on trickle timer Vrf receives attestation reports from Prv (s) of the whole network through DAO_{crypt} message.

[6] For the simplicity of our proposed mechanism we exploit public-private key cryptography. However, based on requirements and usage options, different key mechanisms can be employed.

- *Attestation report gathering*: Prv (s) in SARP will perform self-attestation and corroborate the report along with DODAG-tree.
- *Verify*: This operation is meant for attestation report verification by the Vrf.

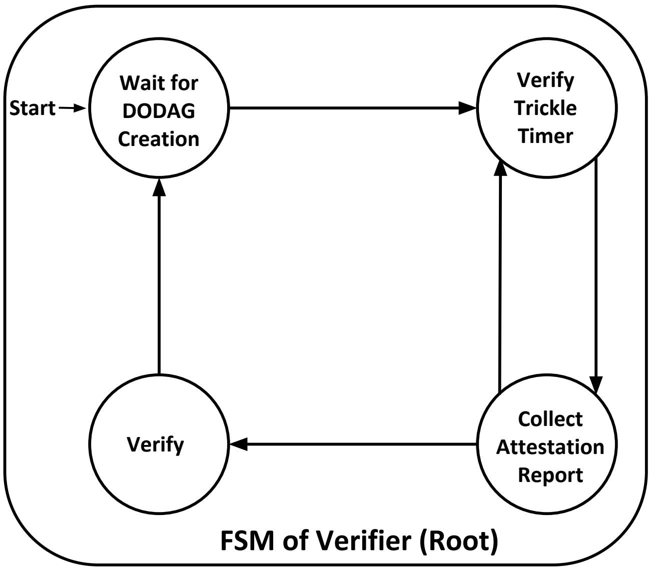


Fig. 6: SARP FSM-s for Verifier (Root)

Algorithm 2 SARP execution for Verifier

```
Bootstrap the network;
$Vrf_{rcv} \leftarrow receive\ attestation\ results$;
$R_{node} \leftarrow remove``faulty''nodes$;
while True do
    check() ← $Flag$;
    if check() == 0 then
        Verify $DAO_{crypt}$;
        perform $R_{node}$;
    else
        Keep the node in DODAG;
        Perform normal-Operation ();
    end
end
```

V. Simulation and Performance Evaluation

In this section, we present the performance evaluation of SARP using the simulation results. We have fully implemented SARP on top of the available open source code of RPL protocol for IoT networks. The implementation is performed in *Cooja*, the Contiki network emulator [40], [47], which is widely used for deploying networks that consists of energy-constrained and memory-efficient devices. We make available[7] an open-source implementation of SARP. We have compared the performance of SARP with SRPL [25], and the traditional RPL protocol [46] in different scenarios. The existing results of SRPL approach that are presented in [25] have been taken on small size network (i.e., 22 nodes, out of which one is Root node and two are attacker nodes), which is not feasible for a scalable approach. Therefore, we took our results by increasing the same ratio of attacker nodes with respect to node density in the network as used in SRPL [25]. Table II provide the details of various parameters along with their values that we have used to configure the target IoT network scenarios in *Cooja* emulator [20].

TABLE II: Simulation setup: Parameters for SARP Evaluation

Parameters	Values
Simulator	Cooja on Contiki v3.0
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 SARP
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 25%
Traffic rate	0.50 pkt/sec - 500 packets
Average Mobility Speed	3 m/s

We show that SARP has been improved w.r.t the aforesaid schemes in terms of heterogeneity. We simulated SARP over different types of motes (i.e., skymote, MicaZ, ESB and Z1 mote which are available on Cooja platform). As depicted in Figure 7, SARP can accommodate heterogeneous nodes over a network and the performance of SARP is quite promising.

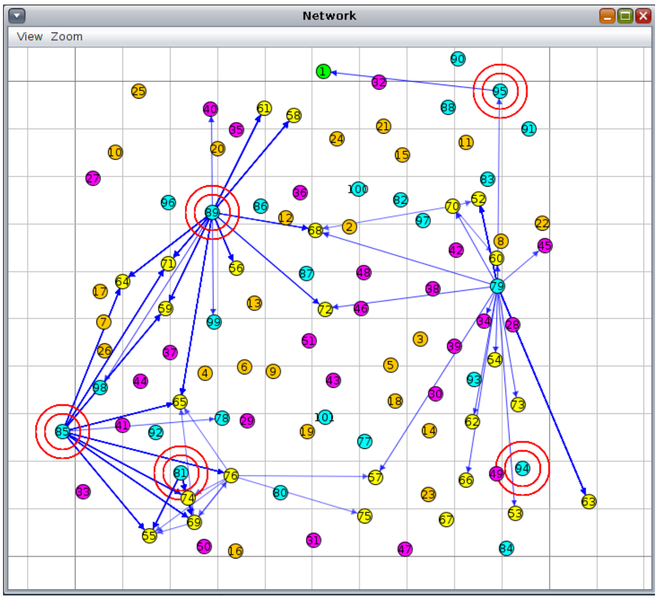


Fig. 7: Simulation of Heterogeneous nodes with SARP (RPL based topology) in the Contiki Cooja environment

We now present a comparative analysis of SARP and traditional RPL using the metrics namely Average Packet Delivery Ratio (APDR) and Energy Consumption. The evaluation of these metrics is required because: (i) the presence of different types of attacker (e.g., topological and data communication) nodes can adversely effect the APDR by altering various network parameters that disrupt the networking process, and

[7] https://github.com/pallavikaliyar/SARP

(ii) the self attestation process effects the energy consumed by the nodes.

To calculate the simulation results, we consider three different network scenarios which are as follow: (1) In first scenario, the number of nodes are increased from 25 nodes to 100 nodes, while the simulation time (60 minutes) and number of attackers (five nodes) are kept constant; (2) In second scenario, the simulation time is increased from 10 minutes to 60 minutes, while the number of nodes (51 nodes, including root node) and attackers (5 nodes) are kept constant; and (3) finally, in third scenario, the percentage of the attacker nodes are increased from 5 to 25, while the simulation time (30 minutes) and number of nodes (51, including root node) are kept constant.

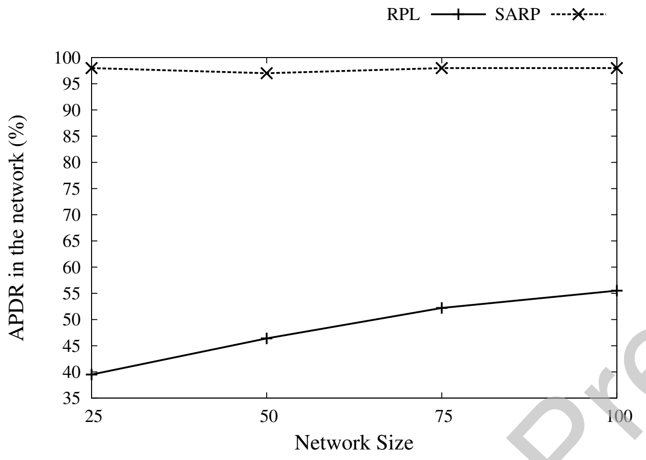


Fig. 8: APDR with respect to increasing number of nodes in the network

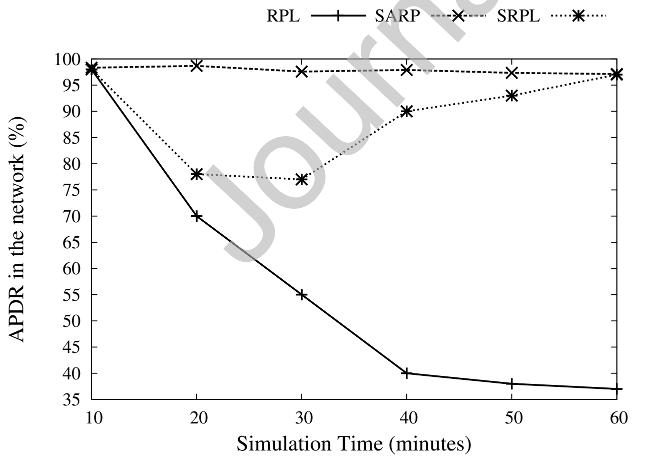


Fig. 9: APDR with respect to increasing simulation time in the network

As shown in Figure 8, the APDR of SARP with respect to increasing number of nodes is substantially higher than RPL. At the same time, SARP is providing better security by identifying attacker nodes. Thus, it provides better resiliency against attacker nodes residing in a network. Traditional RPL has no mechanism to identify malicious nodes in the network.

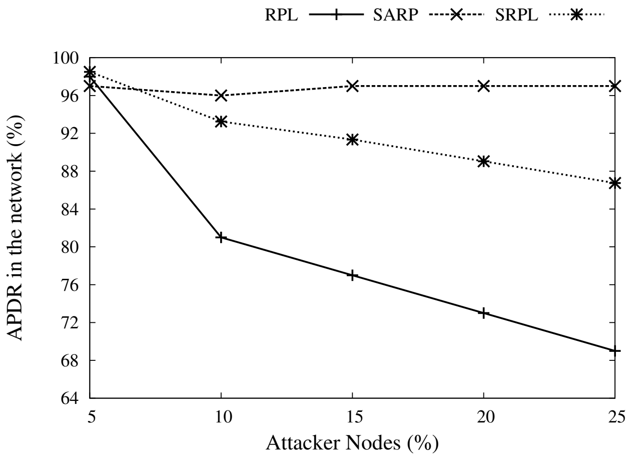


Fig. 10: APDR with increasing number of attacker nodes in the network

Figure 9 shows that SARP has the significantly higher performance of APDR with increasing time of operations over a network. The comparison was drawn among SARP, RPL, and SRPL protocols.

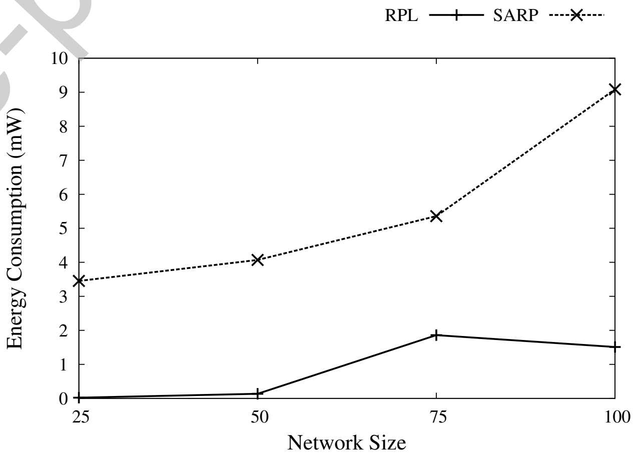


Fig. 11: Energy Consumption with increasing number of nodes in the network

Figure 10 show that SARP demonstrates higher APDR comparing to RPL and SRPL. It is due to the capabilities of SARP in identifying malicious nodes during attestation process, which is followed by the prevention scheme that isolates them from the DODAG. Thus, the generic network operations remain unhindered.

In Figure 11, we show the energy consumption of SARP. Undoubtedly, SARP requires higher energy-consumption than traditional RPL. Note that SARP executes a security protocol which is build upon the framework of traditional RPL protocol, and it satisfies its primary role in identifying malicious nodes in the network. Figure 12 provides the energy consumption of SARP w.r.t increasing simulation time. Due to the use of complex hashing algorithm to provide encryption of the attestation results, SARP requires more energy than the traditional RPL protocol. However, through our simulation we

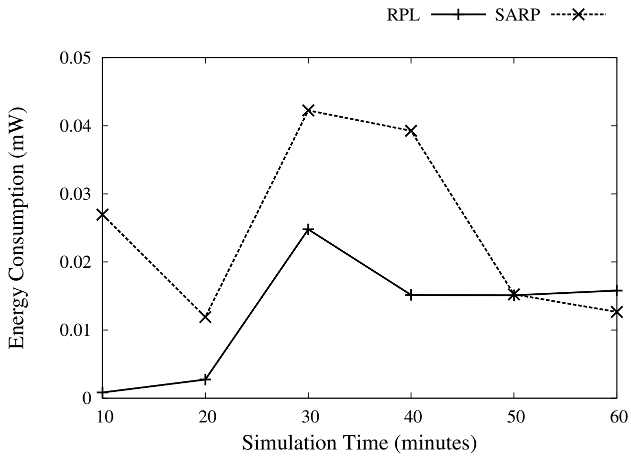


Fig. 12: Energy Consumption with increasing simulation time in the network

found out that with increasing simulation time the average energy requirements for SARP substantially decreases. As early detection of malicious nodes prevents healthy nodes from sending iterative messages for communication.

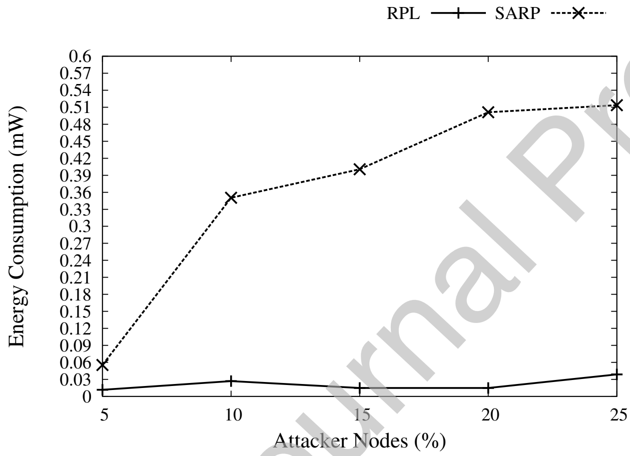


Fig. 13: Energy Consumption with increasing number of attacker nodes in the network

Energy consumption for SARP over a network with increasing number of attacker nodes reveal interesting results as shown in Figure13. In comparison with traditional RPL, SARP requires substantially higher energy consumption. Recall that SARP executes a security protocol, and it performs complex and energy consuming hashing operations to protect attestation related information and send this information securely to the Vrf. However, the energy required for these operations are not too high, and the resource constrained IoT devices can afford the same.

Figure 14 displays the duty cycle for the SARP w.r.t increasing number of attacker nodes in the network. Duty cycles in SARP is slightly higher than the traditional RPL protocol. The duty cycle of SARP in the presence of increasing number of nodes is not substantially higher than the traditional RPL even though SARP performs critical and complex cryptographic operations.

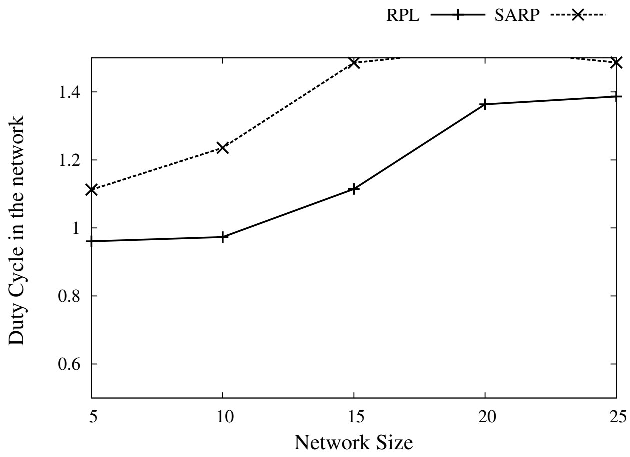


Fig. 14: Duty Cycle with the increasing number of attacker nodes in the network

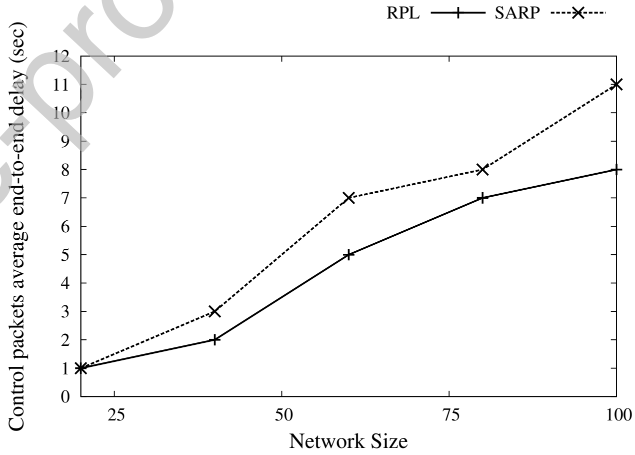


Fig. 15: End-to-end delay with increasing number of nodes in the network

Figure 15 shows the average end-to-end delay of entire DODAG w.r.t. increasing number of nodes in the network. Generally, the size of network and control packets contribute in the delay of message propagating to the root node due to the multiple hops distance. In RPL, DAO messages are used to maintain the downward network topology. Through DAO messages, the root node gets the global view of network topology which helps it to control the DODAG topology in network. In SARP, we exploited the DAO packet to embed and propagates the attestation result to the root node. Performing attestation and encrypting the result with SHA-256 incurs cost. However, the result shows that SARP does not introduce higher delays to propagate DAO messages to the network, which can be considerable as a minimal cost to pay for an added security feature. In particular, SARP achieves network security without introducing any significant delays to the network management operations, and the root node can be updated with network status without having any substantial delays in the network.

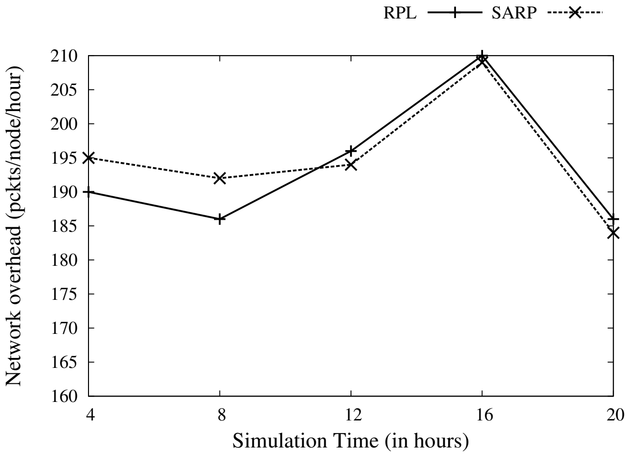


Fig. 16: Network Overhead with increasing simulation time in the network

In Figure 16 the network overhead w.r.t. increasing simulation time is depicted. Undoubtedly, SARP introduces higher overhead when comparing it with RPL. But, in SARP, we are not only performing device attestation but also propagating the attestation results by using the DAO packets (i.e., DAO_{crypt}). Upon receiving DAO_{crypt}, the root node will be notified about the network health. Despite performing cryptographic operation SARP does not introduce higher overhead on the network due to the exploitation of the existing DAO packets.

The simulation results illustrate SARP's superior performance compared to other protocols. The main advantage apart from security and scalability is that SARP introduce minimal overhead. The figures 8, 9 and 10 shows that SARP is more secure, and it has high APDR in different network scenarios over traditional RPL protocol. The main reason behind SARP's higher APDR is that during initial attestation phase SARP is able to identify malicious nodes, which adversely effect DODAG in the later phases. Thus, it makes SARP an ideal candidate to replace general RPL over a legacy network.

A. Energy Consumption Analysis

We compute the overall energy consumption based on energy required to send and receive SARP messages and to perform the main cryptographic operations. Let E_{send} be the energy required to send one byte, E_{recv} the energy required to receive one byte, E_{hash} the energy required to perform a hash operation, E_{crypt} is energy required to perform encryption of the DAO message, E_{att} is the energy required to perform attestation, and N the number of devices participating in attestation process. As mentioned in Section IV that based on trickle-time t, all Prv send the attestation time T_{att} and a hash. Thus, we can estimate the energy consumption for sending a single SARP message from prover Prvi as follow:

$$E_{send}^{Prv_i} \leq E_{att} + E_{hash} + (DAO_{Message}) * E_{crypt}.$$

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

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

Based on our simulation results, the energy consumption [8] of nodes in SARP is low, and most importantly, it does not have a significant difference from general RPL energy consumption. The important achievement of SARP is that we are performing attestation of network devices without introducing additional overheads from energy consumption perspective. It is because SARP uses the RPL's DAO messages. Moreover, this minimal cpu power consumption and duty-cycle proves its efficiency for large-scale network implementation as well.

B. Security Analysis

In Section III-B, we have introduced the adversarial model. This section provides an analysis of SARP'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 Section III-B can launch attacks like eavesdropping and packet discarding. The Adv can eavesdrop the messages exchanged among different nodes in the network but it will not be able to compromise them. The use of hashing mechanism makes this type of attacks unfeasible. While, 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 considered software only attackers, but the use of trickle timer can help us identify the presence of physical adversaries as well. In fact, to avoid detection, the 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 timer gap. During each trickle timer interval, every device has to perform self-attestation and send the report to the Vrf. The Vrf will identify missing attestation reports, if any.
4) In SARP, the devices use DAO_{crypt} to send attestation result. The attestation result and the associated information are transmitted in encrypted way. An Adv can not forge the encrypted result in polynomial time due to the short-time between trickle-timer. In a scenario where the Adv manipulates the flag and reserved field of the DAO_{crypt} message, the same will be identified by the root node. However, this scenario is very unlikely as the Adv will try to invade the detection and forging those fields will make it visible to the Vrf.
Now we will discuss SARP's performance w.r.t the security requirements as described in Section III. In order to be successful, SARP has to satisfy those aforementioned properties.

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

- **Preserving the integrity of the network.** In SARP, the Vrf will receive the attestation result from all the nodes at every trickle-timer period. The nodes will perform self-attestation and send the result in an encrypted from as a payload. Upon receiving the attestation results, the Vrf can identify the presence of malicious nodes. Through attestation, the sanity of the network is preserved.
- **Unforgeable communication.** An Adv may try to eavesdrop or forge the attestation results. But, the Adv cannot forge the attestation result as it is encrypted using SHA-256 and the DAO_{crypt} message is signed using the public key of the root node. Thus, any manipulation with the attestation message will be noticed by the Vrf during the hash comparison process performed at its end.
- **Freshness.** Freshness is preserved in SARP by conducting self attestation during every trickle-timer. The value of the trickle-timer is unique, which is also included in the DAO_{crypt} message. This unique trickle-timer value prevents an adversary to launch replay attack or sending a pre-computed attestation result. Additionally, the timestamp value used along with the attestation result also provides the proofs of freshness of the attestation messages.
- **Lightweight operations.** As shown in Figure 14, SARP 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.

In past, researchers have addressed the impact of network attacks on traditional wireless networks such as wireless sensor networks [44], and mobile ad hoc networks [6]. However, in IoT networks, the data routing process is challenging and insecure due to the predictable gathering of a massive amount of data, and the resource-constrained and low-cost IoT devices. Authors in [11] provided a detailed survey on IoT networks w.r.t. different security issues and countermeasures. Besides, researchers have proposed VeRA [21] and TRAIL [30], [37] which provides security against version number and Rank attacks, and DAO inconsistency attacks. Moreover, [8] creates trust mechanism against rank and sybil attack, and SRPL [25] addresses the Blackhole attack. However, the aforesaid mechanisms can address only one type of adversary and overlook other attacks. Thus, leaving the RPL-IoT networks vulnerable against a broader category of attacks. Unlike, the aforesaid schemes, SARP improves on the state-of-the-art approaches by facilitating the network owners with the flexibility to counter a broader kind of adversarial activities in the network. Our proposed mechanism exploits the existing RPL architecture to counter the above adversarial capabilities. In particular, SARP achieves better performance and delivers better security against different attacks in RPL-IoT networks. The experimental evaluation in Section V clearly shows that SARP's overall performance is adequate, and it is lightweight, and it provides better security in comparison with the state-of-the-art techniques.

VI. Limitations

Our main objective is to develop a secure and robust routing mechanism for LLNs. In particular, the mechanism should ensure secure communication among IoT nodes and with the root node along with the fast identification of malicious nodes in the network. Despite SARP's many advantages, it has few disadvantages that we mentioned below.

- SARP does not consider a strong physical adversary (i.e., an Adv capable of tamper with the hardware of the device or can launch side-channel attacks) in its adversarial consideration. However, use of trickle-timer facilitates the Vrf with the indication of a possible missing device in case the device is absent for consecutive attestation processes.
- To send the attestation results to the Vrf, SARP uses encrypted DAO messages which also safeguard the attestation results from a broad category of attackers (as mentioned in Section III). Due to encryption of DAO messages using SHA-256, SARP is computationally expensive w.r.t traditional RPL. Nevertheless, the simulation results are promising and reveals the effectiveness of SARP over a heterogeneous network of resource-constrained IoT devices.
- SARP kept internal RPL attacks (e.g., DODAG version attack), distributed denial of service attacks out of its experimental setup. However, we would like to consider these attacks in our future experiments.

VII. Conclusion & Future work

In this paper, we presented *SARP*, an RPL based energy efficient and scalable device attestation approach for IoT networks that consists of large swarms. On one hand, SARP 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 SARP, 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 SARP performed better for security perspective concerning scalability and energy efficient with no significant network delays.

As a future work, we would like to implement SARP over IoT networks with intermittent connectivity to evaluate robustness in our proposed scheme. We will explore different approaches to minimize hardware assumptions by reducing secure code and cryptographic device specific attestation details. In addition to the aforementioned works, we would also like to implement SARP in a real testbed environment to validate its performance and energy consumption claims.

Acknowledgement

Pallavi Kaliyar is pursuing her Ph.D. with a fellowship for international students funded by Fondazione Cassa di Risparmio di Padova eRovigo (CARIPARO). Md Masoom Rabbani is supported by Fondazione Bruno Kessler fund for his PhD. This work is also supported in part by EU LOCARD Project under Grant H2020-SU-SEC-2018-832735. The work of M. Conti was supported by the Marie Curie Fellowship through European Commission under Agreement PCIG11-GA-2012-321980.

References

[1] FBI Identifies Biggest Cyber Threats as IoT, Ransomware, Compromised Email, 2018.

[2] Is YOUR smart TV at risk of being hacked? Consumer Reports warns MILLIONS of Samsung and Roku devices have 'easy-to-find security flaws', 2018.

[3] PewDiePie hackers take over Google smart TV systems, 2019.

[4] T. Abera, N. Asokan, L. Davi, J. E. Ekberg, T. Nyman, A. Paverd, A. R. Sadeghi, and G. Tsudik. C-FLAT: Control-flow attestation for embedded systems software. In *Proceedings of the ACM Conference on Computer and Communications Security*, volume 24-28-Octo of *CCS '16*, pages 743–754, 2016.

[5] 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 *Proceedings - Design Automation Conference*, volume 05-09-June, page 121. ACM, Institute of Electrical and Electronics Engineers Inc., jun 2016.

[6] L. Abusalah, A. Khokhar, and M. Guizani. A survey of secure mobile Ad hoc routing protocols. *IEEE Communications Surveys and Tutorials*, 10(4):78–93, 2008.

[7] T. Advisories. BrickerBot Results in PDoS Attack. \url{https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/}, 2017.

[8] 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*, 93:860–876, 2019.

[9] 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 ACM Conference on Computer and Communications Security*, volume 24-28-Octo of *CCS '16*, pages 731–742, 2016.

[10] M. Ambrosin, M. Conti, R. Lazzeretti, M. M. Rabbani, and S. Ranise. PADS: Practical Attestation for Highly Dynamic Swarm Topologies. *ArXiv e-prints*, 2018.

[11] M. Ammar, G. Russello, and B. Crispo. Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 38:8–27, 2018.

[12] 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 ACM Conference on Computer and Communications Security*, volume 2015-Octob of *CCS '15*, pages 964–975, 2015.

[13] R. Brandom. Here's how to use the CIA's weeping angel' smart TV hack - The Verge. \url{https://www.theverge.com/2017/4/25/15421326/smart-tv-hacking-cia-samsung-weeping-angel-vulnerability}, 2017.

[14] F. N. Brasser, B. El Mahjoub, A. R. Sadeghi, C. Wachsmann, and P. Koeberl. TyTAN: Tiny trust anchor for tiny devices. In *Proceedings - Design Automation Conference*, volume 2015-July, 2015.

[15] X. Carpent, K. El Defrawy, N. Rattanavipanon, and G. Tsudik. Lightweight swarm attestation: A tale of two LISA-s. In *ASIA CCS 2017 - Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security*, ASIACCS '17, pages 86–100, 2017.

[16] M. Conti, P. Kaliyar, and C. Lal. REMI: A reliable and secure multicast routing protocol for IoT networks. In *ACM International Conference Proceeding Series*, volume Part F1305, 2017.

[17] M. Conti, P. Kaliyar, M. Rabbani, and S. Ranise. SPLIT: A Secure and Scalable RPL routing protocol for Internet of Things. In *International Conference on Wireless and Mobile Computing, Networking and Communications*, volume 2018-Octob, 2018.

[18] Q. Dang. Changes in Federal Information Processing Standard (FIPS) 180-4, Secure Hash Standard. *Cryptologia*, 37(1):69–73, 2013.

[19] D. Dolev and A. C. Yao. On the Security of Public Key Protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, mar 1983.

[20] A. Dunkels. Contiki {O}{S}.

[21] A. Dvir, T. Holczer, and L. Buttyan. VeRA - Version number and rank authentication in RPL. In *Proceedings - 8th IEEE International Conference on Mobile Ad-hoc and Sensor Systems, MASS 2011*, pages 709–714, 2011.

[22] K. Eldefrawy, A. A. Francillon, D. Perito, G. Tsudik, K. E. Defrawy, A. A. Francillon, D. Perito, and G. Tsudik. SMART: Secure and Minimal Architecture for (Establishing a Dynamic Root of Trust. In *Ndss*, volume 12 of *NDSS '12*, pages 1–15, 2012.

[23] S. Evans. Mirai Botnet DDoS Attack Type. \url{https://www.corero.com/resources/ddos-attack-types/mirai-botnet-ddos-attack.html}, 2019.

[24] B. Ghaleb, A. Y. Al-Dubai, E. Ekonomou, A. Alsarhan, Y. Nasser, L. M. Mackenzie, and A. Boukerche. A Survey of Limitations and Enhancements of the IPv6 Routing Protocol for Low-Power and Lossy Networks: A Focus on Core Operations. *IEEE Communications Surveys Tutorials*, 21(2):1607–1635, 2019.

[25] G. Glissa, A. Rachedi, and A. Meddeb. A secure routing protocol based on RPL for internet of things. In *2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings*, pages 1–7, dec 2016.

[26] 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 2017*, WiSec '17, pages 64–74, 2017.

[27] IOT For All. The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History — IoT For All. \url{https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/}, 2017.

[28] P. O. Kamgueu, E. Nataf, and T. D. Ndie. Survey on RPL enhancements: A focus on topology, security and mobility. *Computer Communications*, 120:10–21, 2018.

[29] 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 and Tutorials*, 19(4):2502–2525, 2017.

[30] M. Landsmann, M. Wahlisch, and T. Schmidt. Topology Authentication in RPL. In *Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks*, EWSN '16, pages 73–74, 2014.

[31] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko. RFC 6206 - The Trickle Algorithm. *Internet Requests for Comments*, pages 1–13, 2011.

[32] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella. IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. *IEEE Internet of Things Journal*, 6(5):8182–8201, oct 2019.

[33] T. Micro, A. Trendlabs, S. Intelligence, and T. Micro. Persirai : New Internet of Things (IoT) Botnet Targets IP Cameras. \url{https://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/}, 2019.

[34] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Communications Surveys Tutorials*, 21(3):2702–2733, 2019.

[35] Y. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow. IoTPOT: analysing the rise of IoT compromises. In *Emu*, volume 9, page 1, Washington, D.C., 2015. {USENIX} Association.

[36] D. Perito and G. Tsudik. Secure code update for embedded devices via proofs of secure erasure. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 6345 LNCS of *ESORICS*, pages 643–662, 2010.

[37] 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 2018*, volume 2018-Janua, pages 570–574, 2018.

[38] M. M. Rabbani, J. Vliegen, J. Winderickx, M. Conti, and N. Mentens. SHeLA: Scalable Heterogeneous Layered Attestation. *IEEE Internet of Things Journal*, pages 1–1, 2019.

[39] S. Raza, L. Wallgren, and T. Voigt. SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Networks*, 11(8):2661–2674, 2013.

[40] I. Romdhani, A. Al-Dubai, M. Qasem, C. Thomson, B. Ghaleb, and I. Wadhaj. Cooja Simulator Manual. Technical report, Edinburgh, 2016.

[41] R. Sahay, G. Geethakumari, and K. Modugu. Attack graph-Based vulnerability assessment of rank property in RPL-6LOWPAN in IoT. *IEEE World Forum on Internet of Things, WF-IoT 2018 - Proceedings*, 2018-Janua:308–313, 2018.

[42] R. Sailer, X. Zhang, T. Jaeger, and L. V. Doorn. Design and Implementation of a TCG-based Integrity Measurement Architecture. In *USENIX Security Symposium*, page 17, 2004.

[43] 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, pages 272–282, 2004.

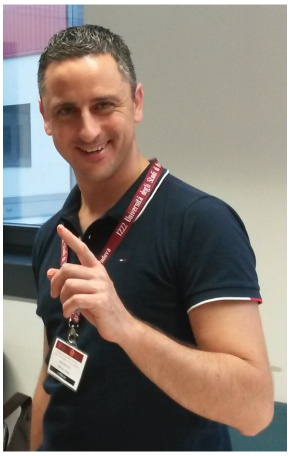
[44] I. Tomić and J. A. McCann. A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols. *IEEE Internet of Things Journal*, 4(6):1910–1923, dec 2017.

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

[46] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander. {R}{P}{L}: {I}{P}v{6} Routing Protocol for Low-Power and Lossy Networks (RFC 6550). 2012.

[47] G. E. T. S. With. Get Started With, 2015.

[48] K. Zhang, X. Liang, R. Lu, and X. Shen. Sybil attacks and their defenses in the internet of things. *IEEE Internet of Things Journal*, 1(5):372–383, 2014.



Mauro Conti is Full Professor at the University of Padua, Italy, and Affiliate Professor at the University of Washington, Seattle, USA. He obtained his Ph.D. from Sapienza University of Rome, Italy, in 2009. After his Ph.D., he was a Post-Doc Re- searcher at Vrije Universiteit Amsterdam, The Netherlands. In 2011 he joined as Assistant Professor the University of Padua, where he became Associate Pro- fessor in 2015, and Full Professor in 2018. He has been Visiting Researcher at GMU (2008, 2016), UCLA (2010), UCI (2012, 2013, 2014, 2017), TU Darm- stadt (2013), UF (2015), and FIU (2015, 2016, 2018). He has been awarded with a Marie Curie Fellowship (2012) by the European Commission, and with a Fellowship by the German DAAD (2013). His research is also funded by com- panies, including Cisco, Intel and Huawei. His main research interest is in the area of security and privacy. In this area, he published more than 250 papers in topmost international peer-reviewed journals and conferences. He is Area Editor-in-Chief for IEEE Communications Surveys Tutorials, and Associate Editor for several journals, including IEEE Communications Surveys Tutorials, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing, and IEEE Transactions on Network and Service Management. He was Program Chair for TRUST 2015, ICISS 2016, WiSec 2017, and General Chair for SecureComm 2012 and ACM SACMAT 2013. He is Senior Member of the IEEE.

Pallavi Kaliyar is currently a Ph.D. student in school of Brain Mind and Computer Science at the University of Padova, Italy with a fellowship for international students funded by Fondazione Cassa di Risparmio di Padova e Rovigo (CARIPARO). Here, she is part of the SPRITZ Security and Privacy Research Group research group under the supervision of Prof. Mauro Conti. She received her Master of Technology in Computer Science and Engineering in 2012 and Bachelor of Engineering in Computer Science and Engineering in 2008. She is conducting research on fields including security and communication reliability related to the Internet of Things.

Md Masoom Rabbani is a PhD student under the supervision of Prof. Mauro Conti in SPRITZ re- search group at University of Padova, Italy. He is affiliated in the Brain, Mind Computer Science (BMCS) school of University of Padova. After his master's degree, he worked in IBM India Pvt Ltd as an Application Developer from 2013 to 2016. In 2016 he joined the University of Padova as a PhD student. His research interests predominantly include security privacy and more precisely Remote attestations and its various techniques.

Silvio Ranise received his Ms. Eng. in 1997 at the University of Genova (Italy) and his PhD in Computer Engineering from the University of Genova (Italy) and the University H. Poincare (Nancy, France) in 2002 in the context of a joint PhD program between Italy and France. He works at FBK in the ST Research Unit as Senior Researcher since April 2010. His previous appointments are: assistant professor at the U. H. Poincare in 2001-2002, INRIA researcher at the LORIA computer science laboratory of Nancy in 2002-2008, research associate at the University of Verona (in the context of the EU Project AVANTSSAR) in 2008- 2010, visiting professor at the Department of Computer Science of the University of Milano. His research focuses on formal methods for the automatic analysis of security-sensitive applications and he has published more than 65 papers in international conferences and journals on automated analysis of security policies, infinite state model checking, and Satisfiability Modulo Theories (SMT) solving. He has been initiator and co-ordinator of the SMT-Lib initiative, and started the SMT workshop series on SMT techniques. He has also given tutorials on SMT and infinite state model checking techniques at international conferences. In 2010, he received the HVC award for his "pivotal and continuous role in building and promoting the SMT community."

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.