Secure and Scalable routing protocol for Internet of Things

Pallavi Kaliyar
pallavi@math.unipd.it
University of Padua
Padua, Italy

Mauro Conti
conti@math.unipd.it
University of Padua
Padua, Italy

ABSTRACT

In this paper, we propose a secure and scalable routing protocol for IoT networks. Our proposed protocol effectively uses a lightweight remote attestation technique to ensure software integrity of network devices. To avoid additional overhead caused by attestation messages, our protocol piggybacks the attestation process using existing control messages. Thus, it causes low energy consumption and provides scalability features to the traditional routing protocol, which are essential in resource-constrained large scale networks such as IoT.

CCS CONCEPTS

• **Internet of Things** → **Security**; *Reliability*; Routing; • **Networks** → Network reliability.

KEYWORDS

Routing protocol for Low Power and Lossy networks (RPL), Internet of Things, Attestation, Security, Routing.

1 INTRODUCTION

In today's world, the Internet of Things (IoT) is an emerging technology, where many smart devices are connected. These devices are resource constrained and low-end, lacking in both computation and power. Although IoT devices bring drastic improvements in our day to day life, any security breach on these devices or communications among these IoT devices can lead to catastrophic consequences for our privacy and security. Hence, to ensure the correct operation of these devices in various IoT applications, it is crucial to maintain their software integrity and protect them against attacks.

In remote attestation technique [2], a verifier engages in an interactive protocol with a prover to obtain a cryptographically secure proof of the correctness of its configuration (e.g., software and data). This is typically enabled by trusted hardware support inside prover devices. Using this concept, we propose a new secure routing scheme based on traditional RPL [4, 5] protocol for the large-scale IoT Networks.

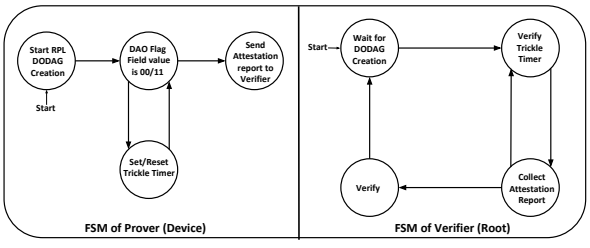

Figure 1: FSM-s for Prover (Device) and Verifier (Root)

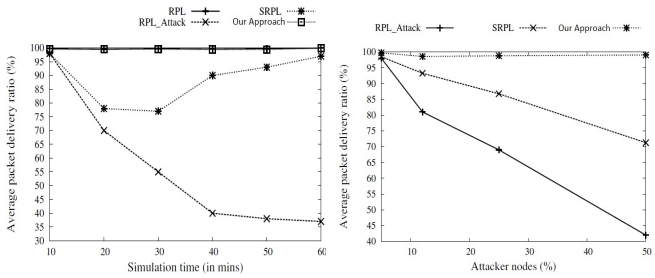

Figure 2: Results

2 PROPOSED APPROACH

Figure 1 [3] shows the step-by-step working mechanism of our proposal. The prover has four main functions, which are as follows. 1) It takes part in DODAG formation and become part of the network. 2) Based on the trickle time, the prover(s) perform attestation and send the attestation report to the verifier/Root node through DAO-attest message. 3) It will perform self-attestation. We have assumed that every prover in the network is capable of performing attestation as described in [4] and it corroborates the report along with DODAG-tree. 4) This operation is meant for attestation report corroboration to the Verifier through intermediary nodes using DAO-attest message. From the Verifier perspective, whenever the Verifier receives corroborate DAO-attest message, it verifies the received message and takes action as per the verification result.

3 RESULTS

As shown in Figure 2, our preliminary experiments show better performance of our proposed method w.r.t the traditional approaches.

4 CONCLUSION

We implement our technique over Contiki-Cooja emulator [1], and the simulation results show its effectiveness. As future work, we will perform extensive experiments over a robust network with intermittent connectivity. We will also implement our proposed approach in a real environment to validate its performance and energy consumption.

REFERENCES

[1] A. Dunkels. 2012. Contiki OS. http://www.contiki-os.org/download.html.
[2] Asokan et al. 2015. SEDA: Scalable embedded device attestation. In *Proceedings of the 22nd ACM SIGSAC CCS*.
[3] Conti et al. [n. d.]. SPLIT: A Secure and Scalable RPL routing protocol for Internet of Things. In *2018 IEEE WiMob*.
[4] H. S. Kim et al. 2017. Challenging the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL): A Survey. *IEEE Communications Surveys Tutorials* (2017).
[5] Winter et al. 2012. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks (RFC 6550). (2012). https://tools.ietf.org/html/rfc6550