FADIA: FAirness-Driven collaboratIve remote Attestation

Mohamad Mansouri*† THERESIS R&D LAB Thales SIX GTS

Wafa Ben Jaballah* THERESIS R&D LAB Thales SIX GTS

Melek Önen† Digital Security Department EURECOM

Md Masoom Rabbani‡ RESEARCH GROUP COSIC KU LEUVEN

Mauro Conti§ SPRITZ Security and Privacy Research Group University of Padua

Email: *{mohamad.mansouri,wafa.benjaballah}@thalesgroup.com, †{mohamad.mansouri,melek.onen}@eurecom.fr, ‡mdmasoom.rabbani@esat.kuleuven.be, §conti@math.unipd.it

***Abstract*—Internet of Things (IoT) technology promises to bring new value creation opportunities across all major industrial sectors. This will yield industries to deploy more devices into their networks. A key pillar to ensure the safety and security of the running services on these devices is remote attestation. Unfortunately, existing solutions fail to cope with the recent challenges raised by large IoT networks. In particular, the heterogeneity of the devices used in the network affects the performance of a remote attestation protocol. Another challenge in these networks is their dynamic nature: More IoT devices may be added gradually over time. This poses a problem in terms of key management in remote attestation.**

We propose `FADIA`, the first lightweight collaborative remote attestation protocol that is designed with fairness in mind. `FADIA` enables fair distribution of load/tasks on the attesting devices to achieve better performance. We also leverage the Eschenauer-Gligor scheme to enable efficient addition of devices to the network. We implement our solution on heterogeneous embedded devices and evaluate it in real scenarios. The evaluation shows that `FADIA` can increase the lifetime of a network by an order of magnitude.

***Index Terms*—remote attestation, collaborative attestation, heterogeneous IoT networks, fairness, embedded systems**

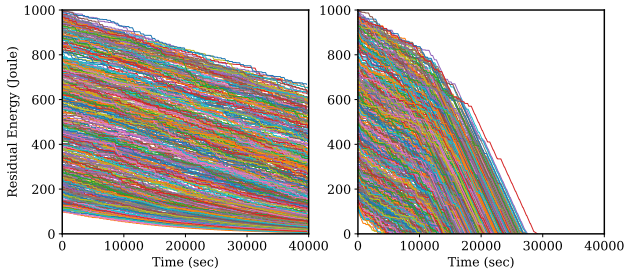
I. Introduction

The evolution of the Internet of Things (IoT) technology leads to a tremendous increase in the deployment and use of IoT devices in the industries and factories. An IoT device could be an entry point or attack vector for malicious hackers to explore. One should therefore continuously verify the software integrity of IoT devices. Remote attestation (RA) helps achieve this goal by enabling a device acting as a prover to prove the integrity of its software configuration to a remote verifier. There exist many RA solutions in the literature [1]–[3].

While existing solutions have improved a lot in terms of scalability, security and robustness, they unfortunately fall short in addressing the heterogeneous aspects of the network. Indeed, IoT devices deployed in the same network may feature different configurations. Furthermore, based on their role and/or position in the network/system they may also differ in terms of battery and computation level. Another problem that is untackled in the existing literature is the increasing size of the network (i.e., devices are added to the network gradually over time). Such problem raises challenges in terms of key management since new keys need to be distributed to existing devices in the network to enable the device-to-device communication. This often turns to be impractical and does not scale well.

To address these challenges, we propose a fairness-driven approach whereby remote attestation tasks/operations are not equally distributed to all devices in the network. Instead, their capabilities in terms of computation and energy are taken into account and devices with more power perform more operations related to the remote attestation compared to more lightweight devices. With this goal, we introduce `FADIA`, a lightweight collaborative remote attestation protocol whereby all devices participate to the protocol by computing their own attestation and also forwarding others' ones. The protocol uses a tree-based architecture where each node in the tree aggregates its attestation with the ones received by its children nodes and forwards the result to its parent node. The number of children of a given node and its role in the tree is determined based on its capabilities (ex. hardware specifications) and current capacity (ex. battery level). With `FADIA`, we show that by tuning these two parameters, we can achieve a more optimized runtime of the remote attestation protocol and a longer lifetime in sensor networks (i.e., time to the first sensor node failure). `FADIA` is also lightweight since it uses symmetric message authentication codes and integrates the efficient key management scheme proposed by Eschenauer and Gligor [4]. Thanks to this scheme each node probabilistically shares a symmetric key with other nodes in the network and can therefore authenticate each other without the need for a key redistribution on each device addition.

To evaluate `FADIA`, we implement it on heterogeneous embedded systems, namely Rasberry Pi 2 devices and Tmote Sky sensor nodes. We evaluate the performance of our solution. The results show that `FADIA` can increase the lifetime of the network by an order of magnitude.



(a) Energy trace

Fig. 1: The residual energy over time. w/ (left side) and w/o (right side) activating fairness.

II. The approach

We design a lightweight collaborative remote attestation protocol (FADIA) that addresses the heterogeneity and device addition problems. To solve the heterogeneity problem, FADIA is designed with fairness in mind. In a collaborative remote attestation protocol, we define fairness as the ability to distribute the load of the protocol according to the capabilities of the provers. The goal is to increase the performance of the protocol and to reach a better lifetime for the network. In a fair remote attestation protocol, provers in FADIA will be assigned a score depending on their capabilities. This score will be frequently updated. In FADIA, similar to PASTA [3], a group of provers collaborate and create a spanning tree in which parent nodes collect attestations from children nodes. However, in contrast to PASTA [3], the choice of the position and the number of children of a prover in the tree are adaptively regulated. These are determined by the scoring function which is computed based on the hardware capabilities (e.g., CPU) of the prover and its current residual battery. The *score* function outputs a score value between 0 and 1. When the score is closer to 1, the prover can assign more tasks with respect to the remote attestation protocol (for example, the node can have a higher number of children). To cope with the dynamic nature of the network, the protocol should support the addition of new devices at runtime. As mentioned previously, involving a central key server for key distribution at runtime results in a significant overhead. Instead, we propose to rely on Eschenauer-Gligor's (E-G) scheme [4] for the distribution of *communication keys*. Thanks to this scheme, FADIA easily addresses the trade-off between the connectivity of the provers and the security of the communication. Furthermore, thanks to [4], the addition of a new prover to the protocol does not require any modification at the other provers.

III. Evaluation

We evaluate FADIA on a heterogeneous network to measure the influence of fairness on the performance. We consider two variants of FADIA. Variant (1) with fairness activated and variant (2) without fairness. We simulate FADIA on 500 Tmote Sky sensors acting as provers. Additionally, we consider a simple energy consumption model: The model updates the current energy consumption based on the status of the transceiver and the microcontroller of the prover. The transceiver can either be transmitting, listening, or OFF. Similarly, the microcontroller can either be ON or idle. The provers move in a random waypoint model at a linear speed uniform between $1mps$ and $2mps$ in a $300m \times 300m$ area. Each of the provers is equipped with a battery of $1000J$ max capacity. The initial energy level a prover starts with is chosen randomly (uniformly $[100J, 1000J]$). We run FADIA for $60,000$ seconds. For variant (1) of FADIA we implement the $score()$ to return the current battery level of a device. Alternatively, for variant (2) $score()$ always retrurns 0.5.

We measure the consumption of energy of each prover with respect to time. Figure 1a shows the energy traces of the provers in both variants of FADIA. As expected, variant (2) of FADIA (i.e. fairness is not activated), shows a fast depletion of the energy of all the provers while for variant (1), most of the provers remain active after $40,000$ seconds. The reason for the fast depletion of energy in the "unfair" protocol (i.e. variant 2) is that provers with low energy are treated indifferently from high energy provers. This leads to putting a significant load on these devices due to the high (i.e. unfair) number of children they need to collect attestations from. Moreover, since the active time is not adapted to the energy level of the device, provers may spend more time waiting to be invited to a tree construction process. This keeps the transceivers of these devices in the listening state for a longer time instead of switching sooner to the OFF/idle state. Additionally, we measure the time taken until we detect 1st, 3rd and 5th crash of a prover (i.e., its energy is completely depleted). We observe that the lifetime of the provers in a fair protocol is an order of magnitude longer.

IV. Conclusion

We propose FADIA, a lightweight collaborative attestation protocol that can be deployed on heterogeneous networks of IoT devices. FADIA is the first RA protocol that integrates fairness in its design. We show that fairness is an important feature for remote attestation protocols. Fairness can increase the lifetime of the network by an order of magnitude. **We note that a complete version of this paper is under submission to an international conference.**

References

[1] 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, Association for Computing Machinery, 2016.

[2] F. Kohnhäuser, N. Büscher, and S. Katzenbeisser, "Salad: Secure and lightweight attestation of highly dynamic and disruptive networks," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ASIACCS '18, Association for Computing Machinery, 2018.

[3] F. Kohnhäuser, N. Büscher, and S. Katzenbeisser, "A practical attestation protocol for autonomous embedded systems," in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2019.

[4] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, CCS '02, Association for Computing Machinery, 2002.