Security and energy-efficiency in the Internet of Things: Challenges and solutions

Michaël Mahamat, Ghada Jaber, Abdelmadjid Bouabdallah

universités de technologie
Belfort-Montbéliard Compiègne Troyes

Security and energy-efficiency in the Internet of Things: Challenges and solutions

Michaël Mahamat[1], Ghada Jaber[1], Abdelmadjid Bouabdallah[1]
[1]Université de technologie de Compiègne, CNRS, Heudiasyc (Heuristics and Diagnosis of Complex Systems), CS 60 319 - 60203 Compiègne Cedex
{michael.mahamat, ghada.jaber , madjid.bouabdallah}[chez]hds.utc.fr

Abstract - The Internet of Things (IoT) is a breakthrough that empowers our everyday life. It allows real-time data analytics, improves industrial production, or provides tailored services. IoT networks deploy many small devices that are energy-constrained. Furthermore, IoT networks and applications lack efficient security. Several attacks occurred against IoT networks due to insufficient security in the past years. However, when security solutions are integrated into IoT networks, they drastically increase the energy consumption of those networks, thus, reducing their lifetime. A major question arises: is it possible to find trade-offs between ensuring security and the energy consumption of security? In this paper, we present a summary of the work done during the thesis, which is the guideline for the corresponding presentation.

Keywords: Internet of Things, security, energy consumption, energy harvesting, wireless charging.

I. INTRODUCTION AND CONTEXT

The Internet of Things (IoT) is a recent networking paradigm that reshapes the way we interact with our surroundings. IoT networks deploy a lot of tiny and energy-constrained devices to reduce the monetary cost of such networks. However, IoT networks face a plethora of threats, whether they target the devices themselves (side-channel attacks) or the data they produce (eavesdropping, false data injection, etc.). There exist security solutions, but they either are inefficient or consume too much energy. For instance, a device using an encryption algorithm such as the Advanced Encryption Standard (AES) [1] has a reduced lifetime compared to an approach without encryption, as shown in Fig. 1. Thus, if other security solutions are used on an IoT device (authentication, anomaly detection, etc.), the lifetime will be greatly reduced.

Thus, this thesis aims to answer the following question: *Is it possible to address energy and security challenges in IoT networks at the same time?* In this summary, we present firstly categories of IoT security solutions that are energy-efficient, then we detail the usefulness of energy provisioning for IoT security solutions.

II. POSSIBLE APPROACHES TO BALANCE SECURITY AND ENERGY CHALLENGES

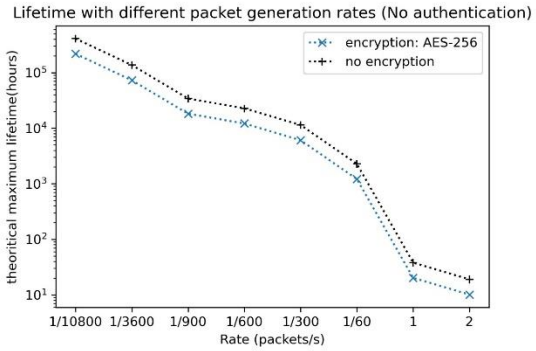

Figure 1. The simulated lifetime of an IoT device with (using AES-256) and without encryption.

There are two possible ways to tackle the challenges of energy and security at the same time:

- Designing security solutions that are energy-efficient by design;
- Designing strategies that consider energy provisioning (energy harvesting or wireless charging) to enable strong IoT security solutions.

In the former case, the security solutions are designed to consider the limited energy of IoT devices. In the latter case, it is the architecture of IoT networks and devices that is modified to enable energy harvesting and wireless charging.

A. Energy-efficient security solutions

This first approach considers that the energy consumption of IoT security solutions must be reduced to increase device (thus, network lifetime). More and more research works tackle this problem, but the majority of existing works do not consider the energy problem. Existing solutions can be categorized into 4 classes and a fifth support class which are namely:

- Lightweight cryptography solutions,
- Energy-efficient mechanisms for security solutions,
- Adaptive security solutions,
- Context-aware security solutions,

- Energy harvesting for security solutions (the support class).

This classification led to a survey of recent solutions [2]. Furthermore, we discussed the usefulness of Artificial Intelligence (AI) techniques for the design of energy-efficient security solutions in IoT networks.

B. Energy provisioning for IoT security solutions

The second approach to this problem is to design energy provisioning methods for IoT security solutions. These solutions focus on providing energy to the IoT devices when they will have to use strong security solutions.

The approach chosen within this category is the wireless charging approach, where a Wireless Mobile Charger (WMC) travels within an IoT network to charge the devices. Enabling wireless charging for IoT devices will increase network and device lifetimes. Furthermore, having a device with a rechargeable battery instead of a non-rechargeable battery reduces the impact on the environment [3]. Research in this field has been very active for wireless sensor networks and is being extended for IoT networks. However, existing works do not consider the context or varying threats to provide a suitable charging path.

To tackle these problems, we first tackled the question of context-aware charging IoT networks. We proposed a model [4] in which the context is defined as a variable *importance level* with regard to the ongoing event in the environment. Then, we expressed the problem as a Markov Decision Process (MDP) and proposed the use of Deep Reinforcement Learning (DRL) to solve it.

Then, based on the work done in [4], we secondly tackled the problem of threat-aware charging in IoT networks. Devices have a fixed importance level, but a new variable, called *threat level* is introduced. It represents the threat level in the IoT network at the current time t, which can be the true threat or an estimation. If this value is low, then, devices would use the bare minimum to secure themselves. However, a high value of the variable *threat level* would incur a high-security level, and thus, an increase in the energy consumption of the IoT devices. The goal of the WMC is to charge the devices according to the current threat level in the network. We proposed the underlying strategy based on DRL and submitted the work for IEEE ICC 2023 [5].

III. Conclusion

Reducing the impacts of security on IoT energy consumption is vital. Indeed, if more and more secured solutions are proposed for IoT communications without looking for reduced energy consumption, network and device lifetimes will be greatly impacted. Thus, designing security solutions that are energy-efficient by design or finding energy for security solutions is primordial. By taking advantage of the future rechargeable nature of IoT networks, it will be possible to fulfill the energy needs of IoT devices for their security needs.

Acknowledgment

This thesis and work are co-funded by the multidisciplinary initiative “Mastery of Safe and Sustainable Technological Systems” of the Sorbonne University Alliance.

References

[1] N. I. of S. and Technology, “Advanced Encryption Standard (AES),” U.S. Department of Commerce, Federal Information Processing Standard (FIPS) 197, Nov. 2001. doi: 10.6028/NIST.FIPS.197.

[2] M. Mahamat, G. Jaber, and A. Bouabdallah, “Achieving efficient energy-aware security in IoT networks: a survey of recent solutions and research challenges,” *Wireless Networks*, Nov. 2022, doi: 10.1007/s11276-022-03170-y.

[3] X. Liu and N. Ansari, “Toward Green IoT: Energy Solutions and Key Challenges,” *IEEE Communications Magazine*, vol. 57, no. 3, Art. no. 3, Mar. 2019, doi: 10.1109/MCOM.2019.1800175.

[4] M. Mahamat, G. Jaber, and A. Bouabdallah, “A Deep Reinforcement Learning-Based Context-Aware Wireless Mobile Charging Scheme for the Internet of Things,” in *2022 IEEE Symposium on Computers and Communications (ISCC)*, Jun. 2022, pp. 1–6. doi: 10.1109/ISCC55528.2022.9912767.

[5] M. Mahamat, G. Jaber, and A. Bouabdallah, “A Threat-Aware and Efficient Wireless Charging Scheme for IoT Networks.”, submitted.