Sustainable Security for Internet of Things

De Donno, Michele; Malarski, Krzysztof Mateusz; Fafoutis, Xenofon; Dragoni, Nicola; Petersen, Martin Nordal; Berger, Michael Stübert; Ruepp, Sarah Renée

Published in:
Proceedings of the IEEE International Conference on Smart Applications, Communications and Networking

Publication date:
2020

Document Version
Peer reviewed version

Sustainable Security for Internet of Things

Michele De Donno*, Krzysztof Mateusz Malarski*, Xenofon Fafoutis*, Nicola Dragoni*+,
Martin Nordal Petersen*, Michael Stübert Berger*, and Sarah Ruepp*
*Technical University of Denmark, Denmark
+ Örebro University, Sweden
mido@dtu.dk, krmal@fonotik.dtu.dk, xefa,ndra@dtu.dk, mnpe,msbe,srru@fotonik.dtu.dk

***Abstract*—Internet of Things (IoT) has been one of the leading innovations of the 21^{st} century. However, the future of the IoT heavily depends on the ability of current technologies to incorporate it. On one side, end-devices and network communication need to be energy efficient, affordable, and environmentally friendly. On the other side, no IoT deployment should be placed without ensuring seamless system and network security. In this paper, we define *Sustainable Security for Internet of Things (SSIoT)*, a new research angle that aims at addressing the challenges posed by the IoT, placing sustainability and security as its key pillars.**

***Index Terms*—Internet of Things, IoT, Security, Sustainability**

I. Introduction

Internet of Things has been one of the key technologies over the last few years, mainly because of its core principle of interconnecting "things" with the aim of optimising and automating the industry and evolving existing services. Today, common IoT applications include: smart cities, smart homes, remote health care, asset tracking, smart grid, smart agriculture, etc. [1]. According to Nokia, there will be 30 billion connected IoT devices by 2025 [2].

Nowadays, IoT is mainly composed of resource-constrained, low-power, small, and affordable wireless devices relying on lightweight communication protocols to communicate over the Internet. The exact requirements of IoT systems vary significantly with different use-cases, however, *security* and *sustainability* are always core aspects [3].

On one side, security constitutes one of the main challenges for IoT [4]. Indeed, most IoT devices are often poorly secured, which makes them easy prey for different types of malware. As a result, cybersecurity threats, such as Distributed Denial-of-Service (DDoS) attacks, have recently become more dangerous and easy to achieve than ever [5] [6]. Moreover, in the near future, health care industry and (to a great extent) everyday life will mainly be sensor-based, thus compromising, damaging or destroying the devices will impose direct harm to peoples' lives, for instance, making pacemakers malfunction [7] or causing car accidents [8]. Also eavesdropping on IoT data may have severe consequences, such as blackmailing people based on their private data (such as health condition) or leakage of secret information of a company.

There are many reasons behind the intrinsic vulnerability of IoT systems. First of all, it needs to be remembered that core features of most IoT devices are small size, low cost, and low power consumption and that IoT applications are tailored for optimising energy consumption (i.e., long battery life) and minimise data transfer. Thus, since security, in its nature, introduces computational overhead, both hardware and applications in IoT have to be engineered to find a trade-off between power consumption and security guarantees [3]. Furthermore, IoT devices are easily available on the market, and inexpensive easy-to-use open-source platforms such as OpenHAB [9] can easily be adopted to enable IoT services such as smart homes. As a result, some of the deployments are conducted by customers that lack basic knowledge about security and are not aware of the high risk that cyber attacks pose.

On the other side, sustainability is becoming extremely relevant for IoT, from different perspectives. Firstly, low energy consumption is a must for IoT devices, because of the need for permanent connectivity and long life span operation. Secondly, the environmental impact has to be considered, thus, the systems should aim at using eco-friendly hardware and reducing the CO_2 footprint of the network. In 2013 the Information and Communication Technology (ICT)-related CO_2 emissions reached the level of 2% of the global CO_2 pollution, comparable with the emissions of aviation industry [10]. Last, but not least, the economic aspect is crucial, since IoT users often choose low-cost IoT devices, regardless their security level [11].

In this paper, we aim at motivating and defining the concept of Sustainable Security for Internet of Things (SSIoT). The goal is to raise the awareness about security and sustainability issues of IoT and to push the research towards practices, procedures, and technologies that would enable the use of affordable, energy-efficient, and eco-friendly IoT systems, in a secure way.

A. Related Work

In the literature, few works truly address joint security and sustainability aspects for IoT.

Karlof et. al [12] present TinySec, a lightweight link-layer protocol for sensor networking, developed more than 10 years ago. The authors designed a complete security architecture for wireless sensor networks, providing robustness in detriment of a small increase in energy-consumption.

Trappe et. al [13] highlight that network security tools currently available need to be tailored for low-energy communication. The study points out IoT resource limitations, emphasises a need for energy harvesting, and recommends

that the best way to achieve lightweight security is to use physically unclonable functions (PUF) and intrinsic communication properties as authentication, along with the tuning of the security scope to a specific application profile. For instance, it is unnecessary to encrypt an alarm message that cannot have a payload.

We consider both works very relevant inputs in the direction of SSIoT, however, we believe that a more complete and comprehensive approach towards a fully sustainable (not only energy-efficient) IoT security is still missing.

B. Outline of the Paper

The remainder of this paper is organised as follows. Section II describes ongoing efforts in research fields related to SSIoT. Section III includes a clarification on our meaning of sustainability and presents the definition of SSIoT and its rationale, in comparison to related concepts. Section IV concludes the work.

II. Related Concepts

In this section, we present an overview of some concepts related to SSIoT and that have inspired our work: Green/Sustainable Computing, Green/Sustainable IoT, and Green/Sustainable Security.

A. Green and Sustainable Computing

Green computing has been defined as the collection of practices and procedures for designing, manufacturing, using, and disposing of computing resources in an environmental-friendly way, while maintaining the overall computing performance [14]. The need for green computing was recognised more than a decade ago with the idea of having more recyclable computers and energy-saving data centres [15] and it is still an open research area [14] [16].

The notion of sustainable computing refers to the research area addressing findings related to energy-aware and thermal-aware management of computing resources as well as applications of computing that can have ecological and societal impacts [17]. Recently, Stergiou et al. [18] studied the effects of IoT and Cloud Computing (CC) integration. The authors claim that combining both concepts is two-way beneficial. CC provides IoT with computational resources and core infrastructure while its scope of applications and services becomes enriched by what IoT enables. All in all, the combination constitutes a base of what they called Sustainable Computing. In addition, the work presented in [19] implies that it is possible to make mobile applications greener by offloading the computing tasks to edge/cloud computing nodes in a smart way. As a result, both power consumption and delays can be optimised. Related to security, Li et al. [20] developed a novel architecture based on analogue spiking reservoir computing, which can be applied to anomaly detection in smart grids. The solution exhibits performance that is comparable to other state-of-the-art proposals, however, it is more energy-efficient, which makes the work a contribution to sustainable computing.

In this work, we consider green/sustainable computing as a single research area that results from the union of the two.

B. Green and Sustainable Internet of Things

Green IoT has been defined as the approach adopted in IoT either to reduce the greenhouse effect of existing services and application or to minimise the greenhouse effect generated by IoT [21] [22]. According to this definition, green IoT can be seen from two different perspectives: (i) an umbrella of IoT solutions enabling more environmentally-friendly approaches in industry and consumer applications (e.g., sensor-based energy-efficient waste management in the town); (ii) a family of hardware, software, network- and architecture-based improvements on IoT making the whole system less energy-hungry and diminishing its negative impact on the nature.

Arshad et al. [23] formulated a taxonomy of green IoT approaches and provided a detailed survey on the state-of-the-art solutions. It has to be mentioned that many of the considered proposals improve the energy consumption of the network, but privacy and security levels are degraded.

In [24], an energy-efficient IoT system model is presented. The authors define and test an algorithm for centralised scheduling that employs three power-consumption-related stages (On, Pre-Off, Off) and is intended to increase the sleep time of less active end-devices.

One of the goals of efficient IoT protocols is to prolong the battery life of end-devices. However, in the case of massive deployments, a more radical approach needs to be considered: gathering energy from the surroundings (Energy Harvesting (EH)) instead of using external batteries. That is because replacing batteries in all the devices would be extremely costly and time-consuming, and eliminating the battery from the sensors minimises the exposure of nature to the toxic substances in the batteries that are difficult to recycle [21].

An overview of the EH concept is presented in [25]. The authors underline that the most crucial point is to ensure proper power management, so that the device may communicate according to the schedule even though it harvests the energy in an opportunistic and rather unpredictable manner. An algorithm for resource management, considering both device activities and harvested energy, is described in [26]. Efficient operation is achieved by handling data collection control and channel scheduling over a small time scale, whilst the power management over the large time scale.

C. Green and Sustainable Security

Green security is a research direction "defining and investigating security solutions under an energy-aware perspective" [27]. In this light, an approach that makes the communication more secure cannot be considered convenient if the corresponding decreased power consumption effect on the network is not simultaneously visible. Nevertheless, it does not imply that the goal of making the communication more secure is necessarily divergent from the one of green data transfer. For instance, an energy-aware routing algorithm can allow for switching some devices off to simultaneously save energy and increase the level of system security by decreasing the number and/or size of possible attack vectors (inactive devices can no longer be compromised and used for malicious actions)

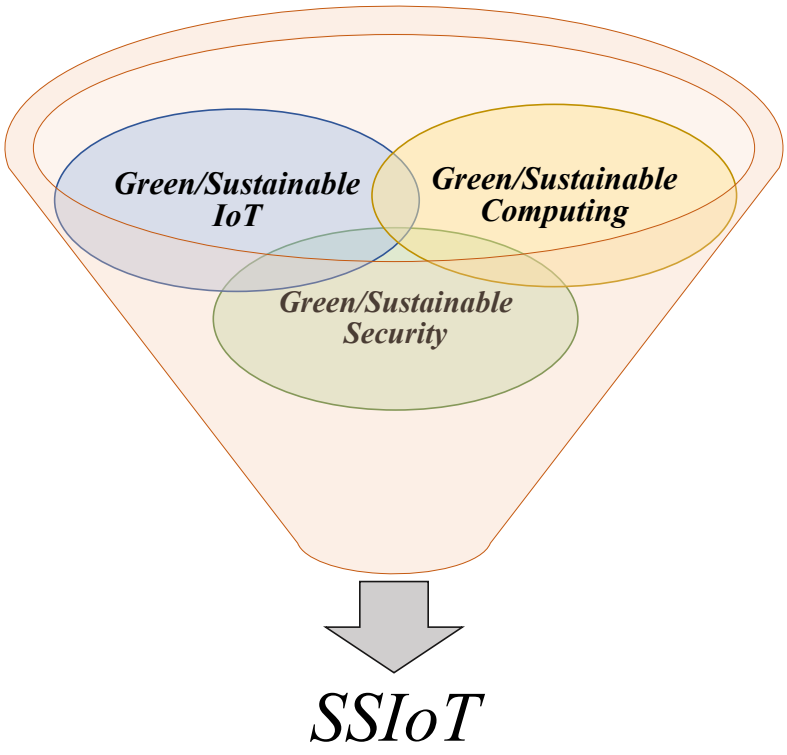

Fig. 1. The SSIoT concept

[28]. Nevertheless, preserving confidentiality, integrity, and availability of information requires additional computations (e.g., for (de)ciphering data, creation and exchange of secret keys, etc.), thus power. That is why achieving high-level security with minimal energy impact appears a challenge.

The green aspect of security has been an object of consideration both in academia and industry for several years, with one of the key enablers being virtualisation of security appliances [29], [30]. Albeit, the majority of network improvements either target security or energy consumption, but only rarely strive to address both [28].

III. Sustainable Security for Internet of Things

This section defines the notion of *Sustainable Security for Internet of Things* (SSIoT).

In our vision, SSIoT is a new research angle addressing all aspects that are relevant to improve the security level of the IoT, in a sustainable way. We consider a solution *sustainable* when it is affordable, eco-friendly (i.e., it has a low impact on the environment), and energy-efficient. Thus, an approach relevant for SSIoT has to meet the two following conditions: (i) it addresses the security of IoT by taking into account the environmental impact, the cost, and the energy efficiency of the solution itself; (ii) it provides an improvement in one of the aforementioned aspects (sustainability or security) without negatively affecting the other one.

As represented in Figure 1, the concept of SSIoT originates from the union of the notions discussed in the previous section: green/sustainable computing, green/sustainable security, green/sustainable IoT. Green/sustainable computing aims at improving IT infrastructures in a green and sustainable way. SSIoT pursues the same goal, but taking into account the requirements of IoT infrastructures. We also share the aim of green/sustainable IoT, but in our vision green/sustainable IoT solutions need to ensure efficient security, otherwise, they should not be in the scope of SSIoT. Finally, we believe that green/sustainable security alone cannot be the best option for IoT due to the multitude of differences between IoT and the traditional Internet infrastructure that green/sustainable security is originally intended for. Thus, we need to apply the green/sustainable security approaches carefully, yet only as far as the IoT requirements are met.

All in all, **Sustainable Security for Internet of Things (SSIoT)** can be defined as *the collection of practises, procedures, and technologies aimed at improving the security level of IoT in an energy-efficient, affordable, and eco-friendly manner*.

As depicted in Fig. 2, the four main pillars of SSIoT can be extrapolated from its definition: *security*, *energy efficiency*, *affordability*, *eco-friendliness*. All solutions in the scope of SSIoT have to be secure by design while meeting the key requirements of IoT, in terms of low power consumption and low cost, and without having a negative impact on the environment.

IV. Conclusion

In this work, we paved the way for a new research perspective: Sustainable Security for IoT. Even though substantial

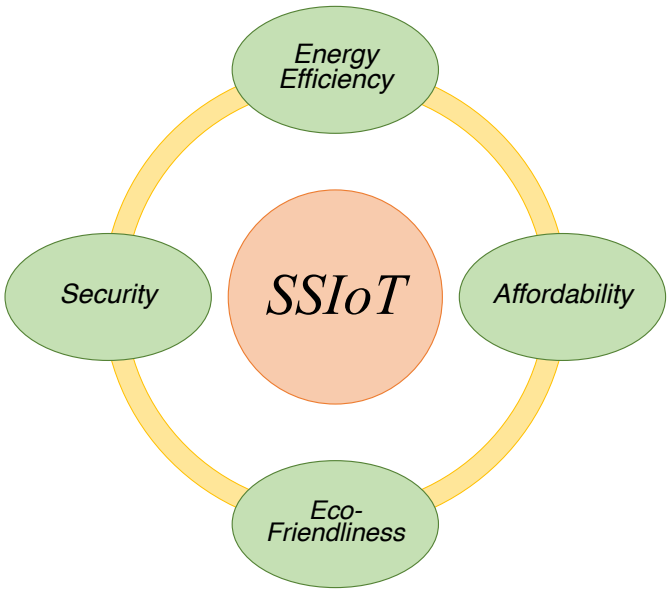

Fig. 2. SSIoT Pillars

efforts have already been done towards a more energy-efficient and secure IoT, we believe that insufficient emphasis has been put on developing lightweight security that would simultaneously ensure IoT sustainability. The latter term intended not only as energy efficiency, but also in terms of environmental impact and economic repercussions (e.g., installation, maintenance, disposal of devices).

The aim of this work is to increase the awareness about security and sustainability issues in IoT, inviting to a more intense research effort towards solutions that would enable a future where IoT can be seamlessly and securely integrated into our society, without undesirable consequences.

ACKNOWLEDGMENTS

This work was partially supported by Poul V. Andersen Fund and Innovation Fund Denmark through the Eureka Turbo project IoT Watch4Life.

REFERENCES

[1] Ericsson AB, "Cellular networks for Massive IoT," Tech. Rep. January, 2016.
[2] Nokia, "LTE evolution for IoT connectivity," Tech. Rep., 2017.
[3] S. Ray, T. Hoque, A. Basak, and S. Bhunia, "The power play: Security-energy trade-offs in the IoT regime," in *In Proceedings of the 34th International Conference on Computer Design (ICCD)*. IEEE, oct 2016, pp. 690–693.
[4] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," *In Proceedings of the 10th International Conference on Frontiers of Information Technology, FIT*, pp. 257–260, 2012.
[5] M. De Donno, N. Dragoni, A. Giaretta, and A. Spognardi, "Analysis of DDoS-Capable IoT Malwares," in *Federated Conference on Computer Science and Information Systems (FedCSIS)*. IEEE, 2017, pp. 807–816.
[6] ——, "DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation," *Security and Communication Networks*, vol. 2018, 2018.
[7] CNN, "FDA confirms that St. Jude's cardiac devices can be hacked," accessed: 05-03-2019. [Online]. Available: https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/
[8] IBM, "Eight Crazy Hacks: The Worst and Weirdest Data Breaches of 2015," accessed: 05-03-2019. [Online]. Available: https://securityintelligence.com/eight-crazy-hacks-the-worst-and-weirdest-data-breaches-of-2015/
[9] openHAB, "openHAB: Empowering the smart home," accessed:05-03-2019. [Online]. Available: https://www.openhab.org
[10] Lawaspect.com, "Efficient Green ICT and Energy Management for Mobile Communication," accessed: 05-03-2019. [Online]. Available: https://lawaspect.com/efficient-green-ict-energy-management-mobile-communication/
[11] M. Favaretto, T. Tran Anh, J. Kavaja, M. De Donno, and N. Dragoni, "When the Price Is Your Privacy: A Security Analysis of Two Cheap IoT Devices," in *In Proceedings of the 6th International Conference in Software Engineering for Defence Applications (SEDA)*.
[12] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," *In Proceedings of the 2nd international conference on Embedded networked sensor systems*, pp. 162–175, 2004.
[13] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the internet of things," *IEEE Security and Privacy*, vol. 13, no. 1, pp. 14–21, 2015.
[14] B. Saha, "Green Computing: Current Research Trends," 2018.
[15] P. Kurp, "Green Computing," *Communications of the ACM*, vol. 51, no. 10, pp. 11–13, 2008.
[16] R. Sharma, "Approaches of Green Computing," *International Journal of Innovative Computer Science & Engineering*, vol. 2, no. 3, pp. 52–55, 2015.
[17] Journal of Sustainable Computing: Informatics and Systems, "About the journal," accessed: 05-03-2019. [Online]. Available: https://www.journals.elsevier.com/sustainable-computing-informatics-and-systems
[18] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Sustainable Computing: Informatics and Systems Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT."
[19] S. K. Mishra, D. Puthal, B. Sahoo, S. Sharma, Z. Xue, and A. Y. Zomaya, "Energy-Efficient Deployment of Edge Dataenters for Mobile Clouds in Sustainable IoT," *IEEE Access*, pp. 1–1, 2018.
[20] J. Li, L. Liu, C. Zhao, K. Hamedani, R. Atat, and Y. Yi, "Enabling Sustainable Cyber Physical Security Systems through Neuromorphic Computing," *IEEE Transactions on Sustainable Computing*, vol. 3, no. 2, pp. 112–125, apr 2018.
[21] F. K. Shaikh, S. Zeadally, and E. Exposito, "Enabling Technologies for Green Internet of Things," *IEEE Systems Journal*, vol. 11, no. 2, pp. 983–994, 2017.
[22] C. Zhu, V. C. Leung, L. Shu, and E. C.-H. Ngai, "Green internet of things for smart world," *IEEE Access*, vol. 3, pp. 2151–2162, 2015.
[23] R. Arshad, S. Zahoor, M. A. Shah, A. Wahid, and H. Yu, "Green IoT: An investigation on energy saving practices for 2020 and beyond," *IEEE Access*, vol. 5, pp. 15 667–15 681, 2017.
[24] S. F. Abedin, M. G. R. Alam, R. Haw, and C. S. Hong, "A System Model for Energy Efficient Green-IoT Network," *International Conference on Information Networking*, pp. 7 057 878, 177–182, 2015.
[25] A. S. Adila, A. Husam, and G. Husi, "Towards the self-powered Internet of Things (IoT) by energy harvesting: Trends and technologies for green IoT," *2018 2nd International Symposium on Small-Scale Intelligent Manufacturing Systems, SIMS 2018*, pp. 1–5.
[26] D. Zhang, Y. Qiao, L. She, R. Shen, J. Ren, and Y. Zhang, "Two Time-Scale Resource Management for Green Internet of Things Networks," *IEEE Internet of Things Journal*, vol. 4662, no. c, pp. 1–12, 2018.
[27] L. Caviglione, A. Merlo, and M. Migliardi, "What is Green Security?" in *In Proceedings of the 7th International Conference on Information Assurance and Security (IAS)*. IEEE, 2011, pp. 366–371.
[28] M. Migliardi, A. Merlo, and L. Caviglione, "A survey of green, energy-aware security and some of its recent developments in networking and mobile computing," *In Proceedings of the 8th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS*, pp. 241–246, 2014.
[29] D. Frangiskatos, M. Ghassemian, and D. Gan, "Technology Perspective: Is Green IT a Threat to IT Security?" *Lecture Notes of the Institute for Computer Sciences, Social-informatics and Telecommunications Engineering*, vol. 41, pp. 147–154, 2010.
[30] R. Arnfield, "Information Security Goes Green," *Infosecurity*, no. 3, pp. 32–34,36.