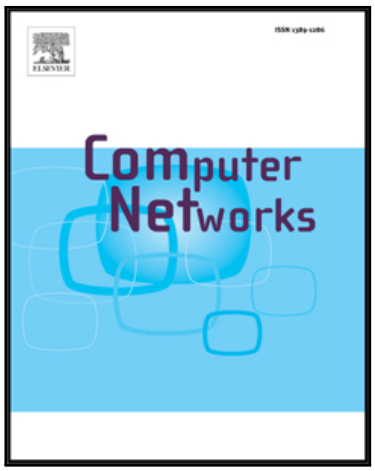

Energy-efficient Mechanisms in Security of the Internet of Things: A survey

Hamed Hellaoui, Mouloud Koudil, Abdelmadjid Bouabdallah

PII: S1389-1286(17)30314-6
DOI: 10.1016/j.comnet.2017.08.006
Reference: COMPNW 6279

To appear in: *Computer Networks*

Received date: 24 February 2017
Revised date: 8 July 2017
Accepted date: 14 August 2017

Please cite this article as: Hamed Hellaoui, Mouloud Koudil, Abdelmadjid Bouabdallah, Energy-efficient Mechanisms in Security of the Internet of Things: A survey, *Computer Networks* (2017), doi: 10.1016/j.comnet.2017.08.006

Energy-efficient Mechanisms in Security of the Internet of Things: A survey

Hamed Hellaoui[a,*], Mouloud Koudil[a], Abdelmadjid Bouabdallah[b]

[a]*Ecole nationale Supérieure d'Informatique ESI, LMCS Laboratory, BP 68 M 16309 Oued Smar, El Harrach, Algiers, Algeria.*
[b]*Sorbonne Universités, Université de Technologie de Compiègne UTC, CNRS, Heudiasyc UMR 7253 CS 60 319, 60 203 Compiègne cedex, France.*

Abstract

Security primitives in the IoT (Internet of Things) are energy consuming. Finding the best solutions that reduce energy consumption while ensuring the required security services is not an easy task. Many works proposed in the literature address security overhead issues by tackling some aspects such as cryptographic primitives, deployment environments, target applications, etc.

This paper is a survey on energy-efficient mechanisms used in IoT security services. By studying the techniques that allow developing energy-efficient security solutions, it goes further than the previous surveys which focus more on the energy-efficient solutions themselves. To the best of our knowledge, this is the first work that tackles IoT security from this perspective. Not only security issues are addressed in this survey, but the energy impact of the solutions are also discussed. Energy consumption related to security services is first introduced. A taxonomy is then proposed for energy-efficient mechanisms in IoT security. The main factors affecting the application of an energy-saving technique for security solutions are finally analyzed.

Keywords: Internet of Things (IoT), Security, Energy efficiency.

1. Introduction

The Internet of Things (IoT) is a relatively new paradigm that is attracting increasing attention from both scientific and industrial communities. It consists in extending the network to the real world, allowing the connection of physical objects. Thanks to communication technologies, objects (such as sensors, actuators, RFID tags) are able to communicate with each other and with users in order to achieve common objectives. Although the potential offered by the IoT allows many applications in different areas (e.g. smart cities, smart grids, healthcare monitoring, etc.), a large-scale deployment of this technology depends on its robustness and its security [1, 2].

Many IoT applications are very sensitive. As an example, parameters measured by sensor nodes in a healthcare application are related to human physiological signs, such as heart rate or body temperature. These sensitive data must not be available for unauthorized parties for capture or modification.In the other hand, the IoT is vulnerable to many types of attacks. The ability to listen, alter or disrupt information is easier to do in such networks, which typically use wireless communications without infrastructure. Objects can also be compromised and malicious nodes can be injected in the network, which may result in unauthorized actions on data and network resources. Moreover, as connected objects tend to invest our daily lives, the IoT could become a huge breach in users' privacy. It is therefore important to consider the required security services to ensure IoT protection from attacks.

Security services are typically instantiated on the basis of heavy schemes (e.g. encryption/decryption and signature/verification). They are generally designed to maintain a high security level without taking resource consumption into account. However, the IoT includes devices that are constrained in terms of resources (e.g. energy, storage, communication). The application of heavy security primitives on some nodes, as sensors and RFID tags, would consume resources and may divert these nodes from executing their main tasks. As the nodes can be battery-powered and expected to operate for a long time, energy consumption is therefore critical in this network. Replacing the battery may even be impossible in many situations, where objects must operate autonomously without human intervention. Security solutions must therefore be adapted to the energy constraints of the nodes in order to prolong their lifetime.

With the emergence of Low-power and Lossy Networks (LLNs), several research works have been led to propose energy-saving solutions for security services. These proposals are varied and cover diverse aspects, such as security primitives, deployment environments, target applications, etc. Therefore, finding the efficient method that reduces the energy consumption while ensuring the required security service is not a trivial task, and it requires careful study so as not to sacrifice security. The objective of this work is to survey energy-efficient mechanisms that can be applied in IoT security solutions. It is intended to assist security protocol designers to select appropriate mechanisms for energy saving, before proceeding with implementation. It is with this aim in mind that this paper proposes a taxonomy of energy-efficient mechanisms in IoT security, studies each one, and analyzes their applicability. The added value of this survey is to contribute to the application of

*Corresponding author.
Email addresses: h_hellaoui@esi.dz (Hamed Hellaoui), m_koudil@esi.dz (Mouloud Koudil), abdelmadjid.bouabdallah@hds.utc.fr (Abdelmadjid Bouabdallah)