Ad Hoc Networks 24 (2015) 264–287

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Survey Paper

Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey

Jorge Granjal *, Edmundo Monteiro, Jorge Sá Silva

Department of Informatics Engineering, University of Coimbra, 3030-290 Coimbra, Portugal

ARTICLE INFO

Article history:
Received 14 September 2013
Received in revised form 16 May 2014
Accepted 1 August 2014
Available online 11 August 2014

Keywords:
Internet-integrated WSN
6LoWPAN
RPL
DTLS
CoAP
Internet of Things

ABSTRACT

The integration of low-power wireless sensing and actuating devices with the Internet will provide an important contribution to the formation of a global communications architecture encompassing Wireless Sensor Networks (WSN), and to enable applications using such devices designed to bring unprecedented convenience and economical benefits to our life. Such applications also take place in the context of our current vision on an Internet of Things (IoT), which promises to encompass heterogeneous devices and communication technologies, including WSN. Due to the characteristics of the devices in WSN and to the requirements of applications, low-power wireless communications are employed and the functionalities supported must be carefully balanced against the limited resources at the disposal of applications. Low-power communication technologies are also currently being designed with the purpose of supporting the integration of WSN with the Internet and, as in isolated WSN environments, security will be a fundamental enabling factor of future applications using Internet-integrated WSN. Although various surveys currently exist addressing security mechanisms for WSN environments, our goal is to analyze how security may be addressed as an enabling factor of the integration of low-power WSN with the Internet, in the context of its contribution to the IoT. We analyze the current research and industry proposals supporting this integration, together with the security solutions and mechanisms designed in its context. Our discussion is supported by an analysis on the attack and threat model against Internet-integrated WSN, and on the security requirements to consider in this context. We believe that a survey with such goals may provide an important contribution to readers interested in embracing this important area of research and ours is, as far as our knowledge goes, the first article with such goals.

1. Introduction

The Internet of Things (IoT) is a widely used expression, currently referring to a vision of a future Internet where ubiquitous sensing applications in diverse areas will provide benefits to our daily lives. Security will be a fundamental requirement of most of such applications, and appropriate mechanisms will be required to cope with the users' expectations and requirements in terms of security. Various communication patterns will be supported by a future IoT communications infrastructure, among which Human-to-Machine (H2M) and Machine-to-Machine (M2M) communications, and this infrastructure is expected to encompass diverse communication technologies, as Near Field Communications (NFC), Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN), among others. The integration of WSN with the Internet may play an important role in the evolution of the architecture of the

* Corresponding author. Tel.: +351 239790035.
E-mail addresses: jgranjal@dei.uc.pt (J. Granjal), edmundo@dei.uc.pt (E. Monteiro), sasilva@dei.uc.pt (J.S. Silva).

http://dx.doi.org/10.1016/j.adhoc.2014.08.001
1570-8705/

Internet, since WSN deployments may be used to support the sensorial capabilities required by future applications. Such aspects also motivate our analysis throughout the article on how security may be addressed in the context of the integration of WSN with the Internet.

In an architectural context, technologies supporting IoT communications may be currently classified in three main categories, as considered later in this article: backbone, backhaul and capillary communication technologies, to which low-power WSN belong. Communication and security technologies adopted for Internet-integrated WSN are expected to share many characteristics with proposals for classic WSN environments, in which sensing devices are employed to enable applications that are proprietary and designed with very particular goals in mind. Numerous challenging aspects characterize the design of communication and security technologies for WSN environments, and such challenges will also be present from the minute we start integrating such networks with the Internet, particularly if this integration involves the exposure of constrained sensing devices and of low-power wireless communications to external or Internet-originated threats and attacks. The characteristics and constraints of WSN environments and devices typically determine the employment of technologies designed to support wireless communications with appropriate reliability and a moderate impact on the energy of sensing devices. As a consequence, such communications run at low speeds in order to reduce collision and retransmission probabilities. Such aspects will also pose difficulties to the design and adoption of appropriate security measures against security threats in Internet-integrated WSN. Despite such challenges, security will be one fundamental enabling factor of this integration, and as such is of paramount importance.

In this article we perform a detailed survey on the available mechanisms offering security in the context of Internet-integrated low-power WSN. Such mechanisms may be related with particular communication technologies developed to enable such environments, or on the other end be designed to protect them from security threats and attacks. With this goal in mind, we analyze the various approaches currently proposed to achieve this integration, which result both from research and industry efforts, and also the open issues and research challenges in this area. In particular, we consider the integration via cloud-based platforms, front-end proxies and specialized architecture frameworks. Our discussion on such approaches also lays the ground for our analysis on the integration of WSN with the Internet communications architecture via standard communication protocols currently being developed for low-power WSN environments, which we analyze in detail in respect to the technologies and recent research proposals at the various layers of the protocol stack. We must also note that the goal of this article is distinct from the numerous existing surveys on security for WSN environments [1,2], given that such works focus on proposals for WSN applications using sensing devices in isolated deployments, where such devices are unable to communicate with other entities or devices on different WSN or on the Internet. Our discussion also differs from existing surveys focusing on security on the IoT in a high-level perspective [131,133], or on the other end on its legal aspects [132]. It is also important to observe that, as mechanisms enabling the integration of WSN with the Internet result from both research and standardization efforts, our analysis along the survey reflects this duality.

The discussion on this article proceeds as follows. In Section 2 we discuss the importance of low-power WSN communications and of its integration with the Internet, while in Section 3 we discuss the attack and threat model applicable to this integration, its main security requirements and the current integration approaches. In Section 4 we perform an exhaustive analysis on the existing mechanisms to support communications and security in the various integration approaches, together with the open issues and research challenges in this area. Finally, in Section 5 we conclude the survey.

2. IoT and M2M technologies

Various communication technologies are already available or currently being designed that may be part of a future communications architecture supporting various types of devices. In this context, WSN devices serve the important purpose of providing applications with the required sensing and actuating capabilities using low-power devices and wireless communications. The technologies currently identifiable in this context are identified in Fig. 1 and, as illustrated, we consider them to be divided in three main categories: backbone, backhaul and capillary communications technologies. In this figure we also illustrate the possible interactions between technologies at different categories.

Interactions between different technologies may be in practice supported by devices implementing mechanisms for translation between different communication technologies, or on the other end supporting different communication technologies simultaneously. In the former situation we may encounter specialized devices or gateways interconnecting different communication domains and that may support different integration strategies, while on the later devices may be employed that support two or more wireless communication technology simultaneously, such as recent Wi-Fi/ZigBee single chip platforms [3]. As illustrated in Fig. 1, we also consider that low-power WSN communications based on IEEE 802.15.4 [16] and 6LoWPAN [17–19] support capillary communications for applications requiring sensing and actuating capabilities using low-power WSN devices.

2.1. Backbone communication technologies

As in the current Internet communications architecture, backbone communications can be supported by both wired and wireless communication technologies. Wired communication technologies may include IEEE 802.3 [4] Ethernet-based communications, as well as Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) [5] fiber optic-based communications. A particularly important role in this context will be played by broadband wireless communication technologies, given the increasing