Ad Hoc Networks 32 (2015) 17–31

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Survey on secure communication protocols for the Internet of Things

Kim Thuat Nguyen [a,*], Maryline Laurent [b,1], Nouha Oualha [a,2]

[a] CEA, LIST, Communicating Systems Laboratory, 91191 Gif-sur-Yvette CEDEX, France
[b] Institut Mines-Telecom, Telecom SudParis, UMR CNRS 5157 SAMOVAR, 9 rue Charles Fourier, 91011 Evry, France

ARTICLE INFO

Article history:
Received 5 June 2014
Received in revised form 20 November 2014
Accepted 11 January 2015
Available online 9 February 2015

Keywords:
Security
Key management
Internet of Things
Wireless sensor network
Cryptographic primitives

ABSTRACT

The Internet of Things or "IoT" defines a highly interconnected network of heterogeneous devices where all kinds of communications seem to be possible, even unauthorized ones. As a result, the security requirement for such network becomes critical whilst common standard Internet security protocols are recognized as unusable in this type of networks, particularly due to some classes of IoT devices with constrained resources. The document discusses the applicability and limitations of existing IP-based Internet security protocols and other security protocols used in wireless sensor networks, which are potentially suitable in the context of IoT. The analysis of these protocols is discussed based on a taxonomy focusing on the key distribution mechanism.

1. Introduction

The Internet of Things (IoT) is designed as a network of highly connected devices (things). In today perspective, the IoT includes various kinds of devices, e.g., sensors, actuators, RFID tags, smartphones or backend servers, which are very different in terms of size, capability and functionality. The main challenge is how to adapt such network so to operate in the conventional Internet. Inspired by that motivation, recent research efforts focus on the design, application and adaptation of standard Internet protocols in the IoT.

The initiative of 6LoWPAN [9] working group allowed the smallest devices with limited processing capabilities to become part of the Internet by enabling the use of IP over these devices. Such great feature enables the connection of literally billions of devices to the Internet, in which very different *things* such as a humidity sensor or an RFID tag can communicate with each other, with a human carrying a smartphone, or with a remote backend server.

While the concept of IoT is easy to grasp, major research efforts still need to be made. Various aspects of IoT are currently being discussed, such as IoT applications and architectures. In addition, more and more research efforts are initiated in resolving challenges associated with security, privacy, and trust as IoT devices are increasingly deployed. According to Gartner's forecast [21], the IoT, which excludes PCs, smartphones and tablets, will grow to more than 26 billion units installed in 2020. Allowing each single physical object to connect to the Internet and to share information, may create more threats than ever for our personal data and business secret information. Concerned objects cover our everyday friendly devices, such as, thermostats, fridges, ovens, washing machines, and TV sets. It is easy to imagine how bad it would be, if these devices were spying on us and revealing our personal information. As an example, a major cyber-attack campaign observed by

[*] Corresponding author. Tel.: +33 1 69 08 00 98.
E-mail addresses: kimthuat.nguyen@cea.fr (K.T. Nguyen), maryline.laurent@telecom-sudparis.eu (M. Laurent), nouha.oualha@cea.fr (N. Oualha).
[1] Tel.: +33 1 60 76 44 42.
[2] Tel.: +33 1 69 08 46 25.

http://dx.doi.org/10.1016/j.adhoc.2015.01.006
1570-8705/© 2015 Elsevier B.V. All rights reserved.

Proofpoint's researchers [28] in January 2014, proved that even a harmless fridge can be employed to launch security attacks. Their analysis shows that 25 percent of malicious emails from the cyber-attack between December 23, 2013 and January 2014 (over 750,000 messages), came from "*smart*" things, including home appliances (TVs, refrigerators…). It would be even worse if critical IoT applications, for instance, the control system in nuclear reactors, the vehicle safety system or the remote monitoring in healthcare, were compromised.

By means of IP protocols crafted for the IoT, an IoT device is able to directly interact with other Internet entities located far beyond its local network. In a typical WSN, devices should be properly authenticated in the network based on a set of credentials stored in a secure area. The security solutions generally deployed within the network are poorly defined to protect communications within the network premises and not between external entities. To provide end-to-end security, the potential adaptations of several standard security protocols have been studied in [1] such as IKE/IPsec, TLS, DTLS, and HIP-DEX, but certain issues continue to persist using these solutions. In particular, resource limitations and the large volume of IoT devices deployed in a network hamper the application of Internet standard solutions.

According to the authors in [33], several new issues brought by IoT need also to be addressed, such as secure booting, firewalling and secure updating and patching. For example, we need to ensure that only authorized and authenticated software are loaded into the embedded device, for example, by verifying a digital signature attached to the software image. As stated in a recently HP security report [9], almost 60 percent of smart devices are not using encryption when downloading software updates. In order to deploy security solutions to this problem, devices are required not only to use cryptographic algorithms to perform encryption, but also to share the necessary keys required by these algorithms, which is an even worse issue considering the foreseen large deployment and the general resource limitations of these devices.

The main motivation of this survey is to identify security issues associated with IoT, and to demonstrate the limitations of existing security solutions to fulfill these issues. The reviewed solutions are analyzed and compared.

1.1. Related surveys and positioning

There have been several conducted studies and surveys [e.g., 60–64] that are relevant to the security in the IoT. For instance, Wang et al. [64] gave a very detailed survey of security issues in wireless sensor networks, which can be considered as a reference for the IoT. The authors identified the constraints and the requirements based on the existing attacks against the IoT at different layers. They also presented the key management systems in WSN according to the employed cryptographic primitives. Atzori et al. [61] focused on authentication, data integrity and privacy issues in the IoT, particularly in RFID systems and sensor networks. Kumar et al. [62] gave a general overview of security and privacy issues in IoT. They provided a description of different security threats and privacy concerns while processing, storing, and transmitting data. The main line of the existing surveys in relation with the IoT security is that they generally focus on identifying the challenges and the security threats present in the IoT. However, several security solutions and techniques have been proposed since the advent of the IoT. For this reason, the present survey takes a different direction by looking in depth into these security protocols and techniques. Indeed, we will not focus on specific security properties needed for the IoT. We will look closer at the security protocol itself, how it is constructed, which security properties are provided, and which cryptographic primitives are used. Moreover, the survey proposes a new taxonomy of key establishment mechanisms in the context of IoT that allows to better understand the proposed security approaches. In this way, strong and weak features of existing approaches can be identified with the objective to build secure protocols for the IoT.

The contributions of the document are threefold:

- present an overview of the challenges and the requirements to build a secure IoT;
- provide a taxonomy of different security protocols proposed for WSN and IoT with respect to the employed key bootstrapping mechanism and also propose a comparative analysis of these protocols and techniques; and
- finally, provide a review of ongoing research initiatives in the field of security in the IoT.

1.2. Paper outline

The rest of this paper is organized as follows. Section 2 discusses the security requirements and challenges associated with the IoT. Section 3 gives a classification of recently proposed security protocols for IoT. Sections 4 and 5 give in-depth description of the protocols based on asymmetric key schemes and the protocols based on symmetric key pre-distribution schemes. Section 6 evaluates the solutions according to the considered categories in terms of the challenges identified in Section 3. In Section 7, we look into promising security research directions for the IoT. Finally, concluding remarks are provided in Section 8.

2. IoT security overview

The IoT offers connectivity for both human-to-machine and machine-to-machine communications. In the near future, *everything* is likely to be equipped with small embedded devices which are able to connect to the Internet. Such ability is useful for various domains in our daily life: i.e. from building automation, smart city, and surveillance system to all wearable smart devices. However, the more the IoT devices are deployed, the greater our information system is at risk. Indeed, a non-negligible number of devices in IoT are vulnerable to security attacks, for example, denial of service and replay attacks, due to their constrained resources and the lack of protection methods. This kind of attacks leads to sensor battery depletion and results in poor performances of sensing applications. In more serious cases, information leak from such tiny