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.