TAKE-IoT: Tiny Authenticated Key Exchange Protocol for the Internet of Things

Article *in* International Journal of Embedded and Real-Time Communication Systems · July 2020

DOI: 10.4018/IJERTCS.2020070101

3 authors, including:

Roumaissa Khelf
Badji Mokhtar - Annaba University
4 PUBLICATIONS **14** CITATIONS

SEE PROFILE

Nassira Ghoualmi-Zine
Badji Mokhtar - Annaba University
78 PUBLICATIONS **230** CITATIONS

SEE PROFILE

International Journal of Embedded and Real-Time Communication Systems
Volume 11 • Issue 3 • July-September 2020

TAKE-IoT:
Tiny Authenticated Key Exchange Protocol for the Internet of Things

Roumaissa Khelf, Networks and Systems Laboratory, Badji Mokhtar - Annaba University, Algeria
Nacira Ghoualmi-Zine, Networks and Systems Laboratory, Badji Mokhtar - Annaba University, Algeria
Marwa Ahmim, Networks and Systems Laboratory, Badji Mokhtar - Annaba University, Algeria

ABSTRACT

The goal of this work is to develop a key exchange solution for IPsec protocol, adapted to the restricted nature of the Internet of Things (IoT) components. With the emergence of IP-enabled wireless sensor networks (WSNs), the landscape of IoT is rapidly changing. Nevertheless, this technology has exacerbated the conventional security issues in WSNs, such as the key exchange problem. Therefore, Tiny Authenticated Key Exchange Protocol for IoT (TAKE-IoT) is proposed to solve this problem. The proposed TAKE-IoT is a secure, yet efficient, protocol that responds to several security requirements and withstands various types of known attacks. Moreover, TAKE-IoT aims to reduce computation costs using lightweight operations for the key generation. The proposed protocol is validated using the automated validation of internet security protocols and applications (AVISPA) tool. Hence, results show that TAKE-IoT can reach a proper level of security without sacrificing its efficiency in the context of IoT.

KEYWORDS

6LoWPAN, Authentication, End-To-End Security, IKEv2, IoT, IP-Enabled WSN, IPsec, Key Exchange, Lightweight Cryptography

INTRODUCTION

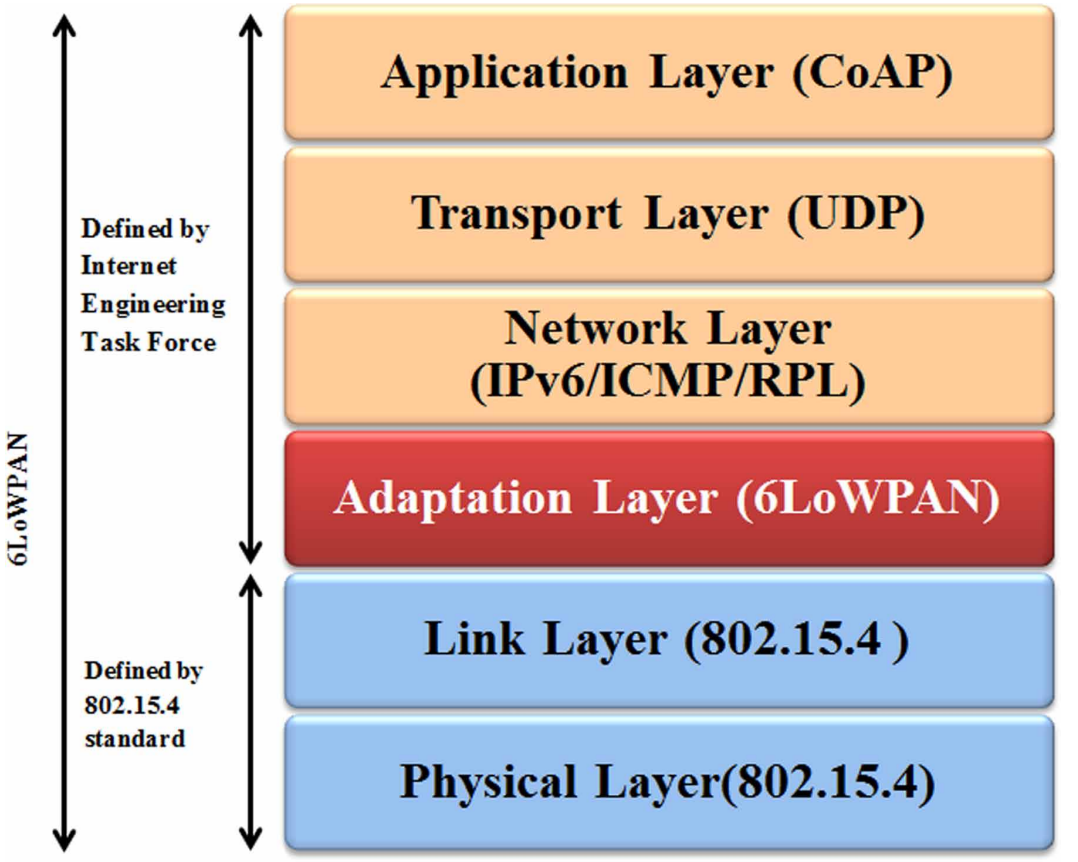
The Internet of Things (IoT) defines the ability to integrate heterogeneous objects from the real world to the Internet. This paradigm aims to exploit intelligent objects (things) to perform human's daily tasks. It is worth noting that, these objects are generally limited in terms of power and computing capabilities. As a part of IoT technology, wireless sensor networks (WSNs) are proliferating into human daily life in the form of different applications, such as eHealth (Korzun, Borodin, Paramonov, Vasilyev, & Balandin, 2015), home automation (Langhammer & Kays, 2012), and traffic control (Hussian, Sharma, Sharma, & Sharma, 2013). In today's Internet, things are mostly servers and switches, firewalls and routers, laptops, phones and tablets, etc. Hence, these things need an IP address for IP connectivity. Actually, IP-enabled wireless sensor networks (IP-enabled WSNs) are considered the new underlying technology for IoT. IP-enabled WSNs are based on the IEEE 802.15.4 standard, which defines the Physical and the Medium Access Control (MAC) layer features for low-power wireless applications (Molisch, Balakrishnan, Chong, Emami, Fort, Karedal, & Siwiak, 2004). Internet protocol version 6 (IPv6) offers optimal addressing to accommodate the large number of devices with individual IP addresses. However, this protocol was designed for resource-rich networking scenarios.

DOI: 10.4018/IJERTCS.2020070101

Therefore, the Internet Engineering Task Force (IETF) created the IPv6 over low-power wireless personal area networks (6LoWPAN) working group (Kushalnagar &Montenegro, 2007). 6LoWPAN designs a new adaptation layer added to the OSI model, placed between the Data Link and Network layer (illustrated in Figure 1). This layer fulfills the operations of IPv6 header compression. These operations achieve a low overhead and allow making available about 81 bytes to transmit data on the Internet into an IEEE 802.15.4 frame. Thus, IP-enabled WSNs can be tightly integrated with existing IP-based infrastructures using 6LoWPAN.

The security issue in IP-enabled WSNs is a controversial subject within the field of IoT because of several challenges: resource constrained devices, wireless medium, unreliable Internet, etc. In fact, there is a growing body of literature that confirms the efficiency of IPsec for IP-enabled WSNs in the context of IoT. In the survey conducted by Nguyen et al. (Nguyen, Laurent, & Oualha, 2015), authors stressed that lightweight internet security protocols are more recommended reducing the communication complexity. A more recent review is presented in (Benslimane, Benahmed, & Benslimane, 2018), where authors discussed the IPsec applicability in IoT environment. They proposed a classification of different mechanisms used to ensure End-to-End security. Indeed, IPsec is mature and proven technology, but a heavyweight security protocol. IPsec needs some adaptations to suit the 6LoWPAN environment. An academic proposal is presented in (Raza, Duquennoy, Chung, Yazar, Voigt, & Roedig, 2011; Raza, Duquennoy, & Selander, 2013) to extend 6LoWPAN with IPsec using header compression techniques. It is worth noting that, these techniques were later enhanced in (Wang & Sun, 2018; Garg & Sharma, 2018). Regarding security solutions of the other layers, a

Figure 1. The 6LoWPAN stack of layers



Related Content