Computer Standards & Interfaces 44 (2016) 85–93

Contents lists available at ScienceDirect

Computer Standards & Interfaces

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

A security gateway application for End-to-End M2M communications

Hsing-Chung Chen [a,b,*], Ilsun You [c], Chien-Erh Weng [d], Chia-Hsin Cheng [e], Yung-Fa Huang [f,*]

[a] Dept. of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan
[b] Research Consultant with Dept. of Medical Research, China Medical University Hospital, China Medical University Taichung, 40402, Taiwan
[c] Soon Chun Hyang University, South Korea
[d] National Kaohsiung Marine University, Taiwan
[e] National Formosa University, Taiwan
[f] Chaoyang University of Technology, Taiwan

ARTICLE INFO

Article history:
Received 1 February 2015
Received in revised form 28 July 2015
Accepted 2 September 2015
Available online 12 September 2015

Keywords:
Security gateway application
IoTs
M2M
End-to-End
Mutual authentication

ABSTRACT

M2M (Machine-to-Machine) communication for the Internet of Things (IoTs) system is considered to be one of the major issues in future networks. Considering the characteristics of M2M networks in IoTs systems, traditional security solutions are not able to be applied to E2E (End-to-End) M2M networks because the M2M network itself is vulnerable to various attacks. We consider security aspects for M2M communications and then propose a security gateway application (SGA) including the lightweight symmetric key cryptographic negotiation function, secure E2E M2M key exchange generation function and secure E2E M2M messages delivery function. The proposal of the SGA is newly suggested to improve the gateway application (GA) of the ITU-T M2M service layer in the IoTs reference model. We prove that it could prevent various attacks via the theoretical security analyses. Therefore, it could meet the basic security requirements of the M2M service layer.

1. Introduction

In recent years, with the development of computer science, communication technology and perception recognition technology, the network of things has made a great breakthrough. The Internet of Things (IoTs) [1,2] has immense potential to change many of our daily activities, routines and behaviors. The IoTs could find applications in many fields, from the earliest wireless sensor networks such as the military reconnaissance to the present intelligent transportation, smart grid, smart healthcare, smart agriculture, smart logistics and so on [3]. IoTs [4–7] are also defined as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies. Through the exploitation of identification, data capture, processing and communication capabilities, the IoTs make full use of things to offer services to all kinds of applications, while ensuring that security and privacy requirements are fulfilled [4–7]. The pervasive nature of the information sources means that a great amount of data pertaining to possibly every aspect of human activity, both public and private, will be produced, transmitted, collected, stored and processed. Consequently, integrity and confidentiality of transmitted data as well as the authentication of (and trust in) the services offering that data is crucial. Hence, security is a critical functionality for the IoTs [2]. Data networks, especially wireless, are prone to a large number of attacks such as eavesdropping, spoofing, denial of service and so on. Legacy Internet systems mitigate these attacks by relying on link layer, network layer, transport layer or application layer encryption and authentication of the underlying data. Though some of these solutions are applicable to the IoTs domain, the inherently limited processing and communication capabilities of IoTs devices prevent the use of full-fledged security suites [2].

In an ubiquitous environment, more and more devices are deployed in our daily life, and they need to communicate with one another. M2M (Machine-to-Machine) communication is considered to be one of the major issues in future networks. M2M is expected to bring various benefits in wireless communications when it is interconnected with the Internet [8]. Considering the characteristics of M2M networks, traditional security solutions are not suitable when being applied to M2M service networks because the M2M server network itself is vulnerable to various attacks [8]. A machine could communicate with another machine directly in wireless manners. The M2M communication has attracted a lot of people and industries for its ability to increase efficiency and improve productivity while reducing operating costs. It has great application areas and it could be connected with other infrastructure and brings much more powerful and efficient results. M2M devices or smart devices will ultimately connect to core services networks through a variety of means, from direct broadband or capillary wireless networks, to wired networks [8]. From the ITU-T perspective, the M2M technologies are a key enabler of the

* Corresponding authors.
E-mail addresses: shin8409@ms6.hinet.net, cdma2000@asia.edu.tw (H.-C. Chen), ilsunu@gmail.com (I. You), ceweng@mail.nkmu.edu.tw (C.-E. Weng), chcheng@nfu.edu.tw (C.-H. Cheng), yfahuang@cyut.edu.tw (Y.-F. Huang).

http://dx.doi.org/10.1016/j.csi.2015.09.001
0920-5489/

IoTs [4–7]. The M2M service layer in the ITU-T scope of the ITU-T M2M service layer includes a set of generic and specific functions for the support of a variety of applications enabled by the M2M technologies [4–7]. These functions include management functions and security functions as well as service support and application support functions. The capabilities of the ITU-T M2M service layer are a subset of the whole set of capabilities of the IoTs [4–7].

Moreover, in 2014, the number of mobile subscribers who use smart mobile devices has now surpassed more than 1.2 billion people in the world [9]. Smart devices especially in the third and fourth generations of cellular systems are able to connect fast to the Internet, and the subscribers are easily capable of sending and receiving M2M messages via the smart devices. Therefore, the M2M plays a very important role in the IoTs communications. Despite the critical role of IoTs in the typical Internet users' life, M2M is not so secure. The processing capabilities of smart devices are increasingly enhanced but it cannot compete with the processing capabilities of personal computers. With the increasingly growing reliance on E2E and M2M for the IoTs system in one hand, and the growing number of vulnerabilities and attacks on the other hand, there is an increasingly demand for security solutions [10–12]. There are also some additional security problems in the M2M communication that are not the case in the IoTs system. Therefore, special secure protocols are required for variety E2E (End-to-End) and M2M for the IoTs platforms.

In addition, data confidentiality, authentication, integrity, non-repudiation, access control, and availability are the most important security services in the security criteria that should be taken into account in secure applications and systems [13,10–12,14–17]. However, there is no provision for such security services in the E2E M2M for IoTs system. Both smart device and M2M gateway applications servers are vulnerable to both passive and active attacks. Passive threats include release of message contents, and traffic analysis while active threats include modification of message contents, masquerade, replay, and denial of Service (DoS) [10–12,18–20]. Actually, all the mentioned threats are applicable to the E2E M2M communications [21,22].

The requirement of secure E2E M2M communication enables smart devices to securely communicate in the relationship of M2M. Despite the many solutions [13,10–12,14] that are available now that provide the E2E secure communications, most of them are using the classical ciphers, traditional symmetric cryptosystems and public key cryptography which are dealing with processing the secure communications among a variety of personal computers and server platforms, the solutions designed for M2M could not be suitable for E2E and secure M2M communication. However, several implementations [13,10–12] provide these services, but none of them offers real simple utility security and preserve the privacy of the end-users. However, it will permit traditional security solutions to become more vulnerable, because it is easily suffers from key guessing attacks [16,17]. In the other words, the new SGA approach for E2E M2M service proposed in this paper will realize new applications that are more suitable for secure E2E M2M communications for use with IoTs systems.

Our contribution is that we have newly suggested the basic definitions of a security gateway application (SGA) to improve the gateway application (GA) of the ITU-T M2M service layer in the IoTs reference model [4–7]. The SGA is proposed and defined as a security gateway application for secure E2E M2M communication consisting of the Lightweight Symmetric Key Cryptographic Negotiation Function, Secure E2E M2M Key Exchange Generation Function and Secure E2E M2M Messages Delivery Function for the IoTs system. In addition to that, a lightweight cryptographic symmetric key algorithm will be negotiated by both smart devices for each E2E M2M communication session, which is an efficient choice in the energy and flexibility for the energy-limited smart device. However, the proposed lightweight cryptographic exchange key algorithm could provide the mutual authentication mechanism and prevent the key guessing attack, the undetectable on-line key guessing attack, the data privacy attack as well as the relay attack. The proposed SGA in this paper meets the basic security requirements of the M2M service layer [4–7]. Our proposal includes following:

- Secure Exchange Key establishment between a pair of smart devices and SGA server for E2E M2M communication in the IoTs;
- Lightweight Symmetric Key Cryptographic Negotiation Function;
- The basic definitions of the SGA is first proposed to improve the GA of the ITU-T M2M service layer in the IoTs reference model [4–7];
- The proposed SGA in this paper meets the basic security requirements of the M2M service layer.

The remainder of the paper is structured as follows: the next section addresses previous work on the topic. Section 3 describes the system's overall architecture and presence. Section 4 introduces the designed SGA approach for E2E M2M service. Section 5 evaluates the proposed schemes in terms of security and provides theoretical analyses. Section 5.3 describes why the proposed SGA in this paper is suitable to be a new standard interface. The last session concludes the paper and gives pointers to future work.

2. Related works

In this section, the introduction of the ITU-T Machine to Machine (M2M) service layer and requirements of the ITU-T M2M security service layer in secure E2E M2M communication are described briefly below.

The M2M service layer and their relationship with the IoTs reference model are described as follows: from the ITU-T perspective, the M2M technologies are a key enabler of the IoTs [4–7]. The M2M service layer in the ITU-T scope, the "ITU-T M2M service layer," includes a set of generic and specific functions for the support of a variety of applications enabled by the M2M technologies. These functions include management functions and security functions as well as service support and application support functions. The capabilities of the ITU-T M2M service layer are a subset of the entire set of capabilities of the IoTs. Fig. 1 shows the ITU-T M2M service layer and its position in the IoTs reference model [4–7]. The layered architectural approach, as illustrated in Fig. 1, reduces the implementation complexity while providing interoperability between different applications enabled by the M2M technologies. The specific support capabilities in the service support and application support layer include application specific support capabilities (e.g., the e-health support and telematics support capabilities as shown in Fig. 1). Three types of applications are identified on top of the ITU-T M2M service layer (Application layer): device applications (DAs), gateway applications (GAs) and network application servers (NAs). DA, GA and NA reside, respectively, in a device, gateway and network application server. All these applications can use capabilities provided by the ITU-T M2M service layer [4–7].

The ETSI M2M SCL, the ITU-T M2M service layer as shown in Fig. 1 [4–7] includes specific support capabilities in the service support and application support layer, specific management capabilities and specific security capabilities which are compared in Ref. [4–7]. The interfaces are anticipated and are required to extend including the support of the specific support capabilities in the service support and application support layer, the specific management capabilities and the specific security capabilities [4–7].

However, the ITU-T M2M service layer and ETSI M2M service layer in the IoTs reference model mentioned above did not address the mutual authentication mechanism for the smart device in secure E2E M2M communication. Thus, the mutual authentication mechanism is suggested into the basic requirements of the secure M2M service layer in this paper for smart devices. The basic requirements of the secure M2M service layer are listed below.