사물 인터넷망을 위한 RFID 보안 프레임워크와 프로토콜 분석

김정태

목원대학교

Analyses of RFID Security Framework and Protocol Supporting Internet of Things

Jung Tae Kim

Mokwon University

E-mail : jtkim3050@mokwon.ac.kr

ABSTRACT

Radio frequency identification system (RFID) is an automatic technology and aids machines or computers to identify objects, record metadata or control individual target through radio waves. Connecting RFID reader to the terminal of Internet, the readers can identify, track and monitor the objects attached with tags globally, automatically, and in real time, if needed. This is the so-called Internet of Things (IoT). RFID is often seen as a prerequisite for the IoT. This paper introduces amd surveyed the technologies of RFID and IoT, discusses the applications and challenges of RFID technology used in IoT.

Keyword

lRFID, Internet of things, Authentication, Security protocol

Ⅰ. Introduction

With its capability to store and wirelessly communicate information as well as automatically identify and track objects in real time, radio frequency identification (RFID) is considered as one of the enabling technologies of the Internet of Things (IoT). IoT refers to uniquely identifiable smart objects (things) and their virtual representations in an Internet-like structure. The potential applications of IoT are limitless and will permeate economic, health, community and private lives [1]. The most important part in the network of things is theinterconnection and interoperability between the machines, which is often called M2M. It is a general term of all that can enhance the communication of machinery equipment and capability of network technology, which organically combined in communication between machines, machine control communications, interactive communication, mobile Internet communications and other types of communication technologies, to share information with machine, equipment, application process, background information system and the operator. M2M means "Machine to Machine", including "Machine to Mobile", "Man to Machine", etc., which mainly refers to real-time data exchange of "machine to machine", "machine to mobile" or "man to machine" via the transmission of information of the wireless network and back-end server networks, in addition to the interconnection and interoperability of machine [2] .

Ⅱ. Security of the IoT

IoT will pervade people everyday's life in future and could be used to improve quality of their users' lives. But it is vulnerable to attacks on security or privacy. In recent years, the world's major developed countries and regions have thrown out the information strategy

connected with IoT [3].

The security of information and network should be equipped with these properties such as identification, confidentiality, integrality and undeniability. Different from internet, the IoT will be applied to the crucial areas of national economy, e.g., medical service and health care, and intelligent transportation, thus security needs in the IoT will be higher in availability and dependability. In general, the IoT can be divided into four key levels [4]. Fig. 1 shows that the level architecture of the IoT.

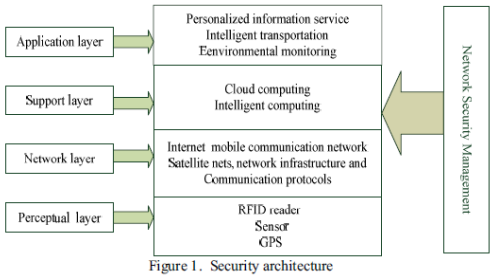

Fig 1. Security Architecture of IoT

According to the security requirement analysis, we can summarize the security requirements for each level in the following, as shown in Fig. 2.

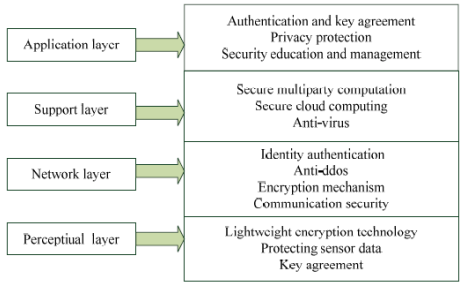

Fig 2. Security Requirement in Each Level

2.1 Trend of Study for Security of IoT

Nowadays, in literature, various methods are proposed to mitigate privacy and security problems in RFID systems. These RFID security mechanisms mainly are divided into three categories: physical methods, anti-collision algorithm mechanism and encryption authentication mechanism.

1) Physical security mechanism:
2) Anti-collision algorithm mechanism:
   - Tag Anti-collision Algorithm:
   - Reader Anti-collision Algorithm
3) Encryption& Authentication Protocol mechanism:

2.2 Security Strategy based on architecture for Privacy and Security of the IoT

1) HIP-Tags Architecture Implementation for IoT:

2) Self Managed Security Cell.a security model for the IoT and Services:

3) Mobile Proxy-a novel RFID privacy protection mechanism:

4) LKC-privacy and its anonymization algorithm –a protection method of RFID data privacy:

III. Conclusion

In this paper,we make a simple presentation about the Internet of Things ,then we discuss about security mechanisms which had been already proposed recently for the IoT. At the same time, we also point out that the challenges for IoT's development remain existing. In the future, research on the Internet of Things will remain a hot issue, and a lot of knotty problems are waiting for researchers to deal with[3,4].

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (grant number: 2010-0024133)

참고문헌

[1] Biplob R. Ray, Jememal Abawajy and Morshed Chowdhury, "Scalable RFID security framework and protocol supportiing internet of things, Computer Network, V.67, pp.89-103, 2014

[2] Du Jiang and Chao Shi Wei, "A Study of Information Security for M2M of IoT", 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), pp.576-579

[3] Hailong Feng and Wenxiu Fu, "Study of recent development about privacy and security of the Internet of Things", 2010 International Conference on Web Information Systems and Mining, pp.91-95

[4] Hui Suoa, Jiafu Wana, Caifeng Zoua and Jianqi Liua, "Security in the Internet of Things: A Review", 2012 International Conference on Computer Science and Electronics Engineering, pp.648-651