

---

# 사물 인터넷 통신망의 적용에 따른 보안 위협과 보안 요구사항 분석

김정태

목원대학교

## Analyses of Requirement of Security and Threat of IoT Application

Jung Tae Kim

Mokwon University

E-mail : jtkim3050@mokwon.ac.kr

### Abstract

With the development of sensor, wireless mobile communication, embedded system and cloud computing, the technologies of Internet of Things have been widely used in real world. Connecting wireless sensor networks with traditional communication networks or Internet, IoT gateway plays an important role in IoT applications. It facilitates the integration of wireless sensor networks and mobile communication networks or Internet. The IoT gateway is a key component in IoT application systems. But It has lot of security issues. We analyzed the issues of security and privacy.

### Keyword

Security, IoT, Gateway, Privacy, WSN

## I . Introduction

The technologies of the Internet of Things can effectively facilitate the integration of material production and service management, the integration of the physical world and the digital world. With development of IoT technologies, the most important IoT application includes infrastructure construction, public security, environment protection, modern agriculture, intelligent industry, urban management, business service and other fields [1]. Usually, IoT has four major components including sensing, heterogeneous access, information processing, applications and services, and additional components such as security and privacy. Communication security mechanisms are also seldom applied to many applications nowadays. Because small devices in the IoT are less processing power, this makes communication security is often weak point. Meanwhile the core network consist of the current or next-generation Internet, most of the

information will be transmitted through the Internet. Information security, privacy and data protection should systematically be addressed at the design stage. The representative technique is IoT gateway solution. In this paper, we survey the concept of gateway and requirement.

## II . IoT Architecture

The typical IoT application architecture can be divided into three layers as follows [2]:

1) Perception Layer: In the perception layer, the system aims to acquire, collect and process the data from the physical world, which consists of two parts: the sensor device and wireless sensor networks.

2) Transmission Layer: In the transmission layer, the system aims to transfer data in a large area or long distance, which is constructed based on the traditional mobile broadband communication network, Wi-Fi and other communication technologies to realize the

integration of the perception and communication network.

3) Application Layer: Data processing and services providing are two major purposes of the application layer.

Applying these kinds of layers or variants of them in the IoT applications require substantial re-construction to address device constraints. Embedded devices are designed for low power consumption, with a small silicon form factor, and often have limited resources. They typically have only as much processing capacity and memory as needed for their tasks. Characteristics of IoT gateway includes a wide range of access capability, manageability and protocol internetworking. System requirements to design IoT gateway should be considered such as data forwarding, protocol conversion and management and control. IoT as a active and new research field, a variety of research need to be solved, at different layers of the architecture and from different aspects of information security, the following subsections analyze and summarize common challenges for security of IoT [3].

- A. Security Structure
- B. Key Management
- C. Security Law and Regulations
- D. Requirements for Burgeoning Applications

There are a number of technique to solve these kinds of security problems. The representative is that crypto algorithms could be used. To implement these cryptographic algorithm available resources are necessary such as processor speed and memory. So how to apply these cryptographic techniques to the IoT is not clear, we have to make more effort to further research to ensure that algorithms can be successfully implemented using of constrained memory and low-speed processor in the IoT. Cryptosystem is basis of information security. In the traditional network, there are two uppermost forms of cryptographic applications such as point to point encryption and end to end encryption. As far as we know, their system can be merged with the IoT framework. Generally, the node of sensor layer is low speed CPU such as single chip system. Encrypt and decrypt programs cannot use large storage and high-power. So Encryption mechanism in IoT should be lightweight [4].

### III. Systematic Approach to Security and Privacy

First, small steps towards systematic approach is as follows and should be solved.

1. Categorization of topics in the Internet of Things

- Take a step back from the technical perspective

- What are the generic topics taking part?

2. Assign technologies to topics

- What technologies fall into which topics?

- Do technologies appear in several topics?

3. Analyze sensitivity of topics to S&P

- See how sensitive topics are to S&P properties?

- Don't analyze technologies, analyze topics!

4. Analyze state of research in topics

- How much research has been done for the S&P properties?

- Has something been neglected?

### IV. Conclusion

The advances in the smart objects systems and Internet of Things approach are remarkable developed. To realize this application, we discussed the research status in this field from encryption mechanism, communication security, protecting sensor data, and encryption algorithm.

### Reference

- [1] Qian Zhu, Ruicong Wang, Qi Chen, Yan Liu and Weijun Qin, "IOT Gateway: Bridging Wireless Sensor Networks into Internet of Things", 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, pp.347-352
- [2] Romano Fantacci, Tommaso Pecorella, Roberto Viti and Camillo Carlini, "Short Paper: Overcoming IoT Fragmentation Through Standard Gateway Architecture", 2014 IEEE World Forum on Internet of Things (WF-IoT), pp.181-182
- [3] Hui Suo, Jiafu Wan Caifeng Zou and Jianqi Liu, "Security in the Internet of Things: A Review", 2012 International Conference on Computer Science and Electronics Engineering, pp.648-651
- [4] Chibiao Liu and Jinming Qui, "Study on a Secure Wireless Data Communication in Internet of Things Applications", International Journal of Computer Science and Network Security, Vol.15, No.2, 2015, pp.18-23