# 사물 인터넷망에서의 RFID 응용 기술 및 보안 문제 분석

김정태
목원대학교

# Analyses of RFID Application and Its Security Problems Embedded in Internet of Things(IoT)

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 wireless 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 surveys the technologies of RFID and IOT, discusses the applications and challenges of RFID technology used in IoT.

Keyword
RFID, IoT, Security issues, Embedded system

## Ⅰ. Introduction

IoT is considered one of the major communication advances in recent years, since it offers the basis for the development of independent cooperative services and applications. Extensive research is underway using this concept in different areas, such as building automation, Intelligent transport systems, and, in particular, healthcare. For example, IoT potential for mobile health applications has been reported in [1]. A ubiquitous and mobile integrated clinical environment platform based on the IoT offers support for large scale connectivity with different physiological sensors, as well as integration with information systems. This improves accessibility to clinical services, compatibility and ubiquity, enhancing citizen mobility, and guarantees access to medical information, anywhere and anytime. Specifically, the capabilities of technologies for the identification of objects, such as Radio Frequency Identification (RFID), and for communication and ubiquitous access to information, such as wireless personal devices, embedded systems and smart objects are evaluated. IoT is actually cyber-physical systems or a network of networks. With the huge number of things/objects and sensors/actuators connected to the Internet, a massive and in some cases real-time data flow will be automatically produced by connected things and sensors. Most of papers cover topics including sensors and devices for IoT, efficient communications and networking for IoT, security and privacy in IoT, crowd sensing and crowd sourcing, localization and tracking, services and applications, and IoT data modeling and management. Despite these challenges, it's only a matter of time before these issues could be solved. RFID's potential benefits are large, and many novel applications will be see in the future, even some of which can not begin to imagine [2].

## Ⅱ. Related Works

The IOT system architecture is generally divided into three layers: the perception layer, the network layer, and the service layer (or application layer), as shown in Fig.1 [3,4].

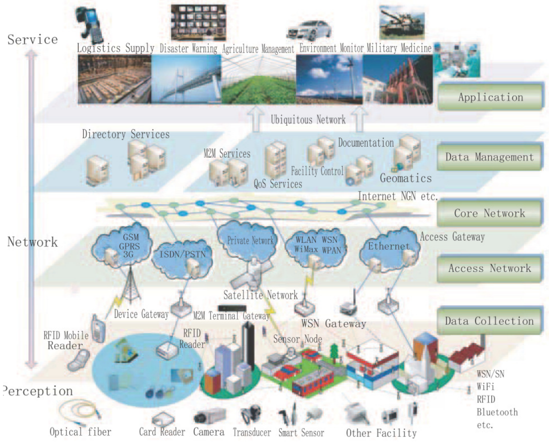

Fig. 1. General architecture of Internet of Things

1) Perception layer: It is the information origin and the core layer of IOT. All kinds of information of the physical world used in IOT are perceived and collected in this layer, by the technologies of sensors, wireless sensors network (WSN)

2) Network layer: This layer, also called transport layer, including access network and core network, provides transparent data transmission capability. By the existing mobile communication network, radio access network, wireless sensor network (WSN) and other communications equipment

3) Service layer: This layer, also called application layer, includes data management sub-layer and application service sub-layer. The data management sub-layer provides processing complex data and uncertain information, such as restructuring, cleaning and combining, and provides directory service, market to market (M2M) service, Quality of Service (QoS), facility management, geomatics, etc.

Security and privacy issues of RFID tags can effect both organizations and individuals. Unprotected tags may be vulnerable to eavesdropping, traffic analysis, spoofing or denial of service and many more. Even unauthorized readers can affect the privacy by accessing tags without enough access control. Even if the tag content is secure then also it can be tracked by the predictable tag responses; “location privacy” can be affected by a traffic analysis attack. Attacker can also threaten the security of systems, which depends on RFID technology through the denial of service attack.

## III. Conclusion

Many researcher and scientist work to implement low cost security and privacy protocol to increase the applicability. Lots of lightweight solutions have been proposed for RFID, but they are still expensive and vulnerable to the security and do not fully resolve the security issues.

## 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: 2013-052980

## References

[1] Antonio J. Jara, Miguel A. Zamora- Izquierdo, and Antonio F. Skarmeta, "Interconnection Framework for mHealth and Remote Monitoring Based on the Internet of Things," IEEE Journal on Selected Areas in Communication, Vol. 31, No. 9, 2013, pp.47-64

[2] R. S. H. Istepanian, A. J. Jara, A. Sungoor, and N. Philips, “Internet of Things for M-health applications (IoMT),”in Proc. AMA IEEE Medical Tech. Conf. Individualized Healthcare, 2010.

[3] D. Guinard, V. Trifa, S. Karnouskos, P. Spiess, and D. Savio, “Interacting with the SOA-based Internet of Things: Discovery, query, selection, and on-demand provisioning of web services,”IEEE Trans. Services Comput., vol. 3, no.3, pp. 223 – 235, 2010.

[4] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. D. Johnson, “M2M: From mobile to embedded Internet,” IEEE Commun. Mag., vol. 49, no. 4, pp. 36 – 43, Apr. 2011.