Analyses of Integrated Security Framework with Embedded RFID System for Wireless Network Architecture

Jung Tae Kim

Mokwon University, E-mail: jtkim3050@mokwon.ac.kr

Abstract

An integrated security mechanism is one of the key challenges in the open wireless network architecture because of the diversity of the wireless network in open wireless network and the unique security mechanism used in each one of these networks. Optimized security protocols and mechanisms are necessary for the high performance and security concerns. Finally, a challenge and requirement of advanced security mechanism will meet the integration of open ubiquitous sensor network with security protocols for applying their applications in the near future. We analyzed and surveyed features of infrastructure and security mechanism of various heterogeneous wireless networks.

Keywords: *Security protocol, Wireless network architecture, Security requirement*

1. Introduction

Recently, communication environment has been changed very much due to advances in information and communication. The current existing information networks consist of the wired and wireless network with a split network and the individual networks which can be developed. However, in recent years, wired and wireless network are integrated with two-step fusion of traditional wired and wireless networks. The network tends to integrate and fuse to set up total topology. With the characteristics of various types of wireless networks are advancing due to the needs of users' demand for their network. Therefore, each network is developing with each their characteristics. From the user's perspective, the current existing network with integrated wireless communications based on the user-centric network architecture is developing new features and fusing with different networks. Depending on needs, the characteristics of wireless and mobile communication can be opened in order to realize the structure-based wireless networks that have been developed using the form and needs [1].

The recent surge in cyber-attacks as a measure for the "fusion of security and privacy' has emerged as the hot-issue in these days. In particular, process of promoting the standards of ITU, such as the international organization for standardization in the NGN (Next Generation Network) technology and the next Internet, web technology by the international organization for standardization fourth-generation mobile communication technology, combined with the standardization of RFID (Radio Frequency identification) and US. Things and people can communicate with each other while supporting remote communication between people, and it can be serviced and supplemented the services of the IoT (Internet on Things) and M2M (Machine to Machine), WoT (Web-of-Things) that share them with services to be linked. In addition, mutual information networks have been composited due to network convergence, the sense of privacy and cyber-attacks on RFID and sensor network security is expected to surge in importance. There are different kinds of sensors, which we require for living. Temperature, humidity, acceleration, touch, pressure, vibration, earthquake, time, location, coordinates, etc. are the physical sensors. Dust, chemical drugs, toxic gases such as chemical sensors blood, bacteria, fungi, yeast, DNA, RNA are bio-sensors. Cameras and microphones are video and sound sensors to detect the photocathode, and electric power and electromagnetic sensors to detect magnetic antenna and so on. In the future, long-term domestic and international markets, leading to global warming, green industries to support purification, as well as the resolution of food depletion, energy depletion, natural disasters, disaster and peaceful collaboration of the international community on these kinds of issues that require business followed the war, terrorism, drugs, crime, unethical accidents, incidents to resolve RFID, USN, bar code, QR code and combined RTLS, GPS, LBS location services, as well as health, nutrition, hygiene, environmental, health, In this paper, several types of wireless network are configured and consist of an open wireless network which has a lot of issues that need to be addressed. Especially, the most important factors in wireless sensor network are

the mobility management techniques to manage the quality of service, a unique problem in wireless network vulnerabilities, and interaction between the different systems, such as security and connectivity issues. In this paper, based on the integration of these open wireless environments, we analyzed requirement of network, problems, and for security needs [2, 3].

2. Related Work

In the 21st century, advanced technologies have developed with fusion technology related to information technology and another fields of technology. The inherent and open fundamental differences among the various open network related to wireless networks, integration of the security schemes of those networks is not easy job to be solved. To integrate several open networks related to wireless networks into a single architecture, there are a number of challenges that must be addressed. The main topic are supporting of mobility management, providing of quality of services and security interoperability. Security requirement of wireless communication are more important because of its inherent vulnerability. The security and privacy issues and solutions for WSNs (Wireless Sensor Networks) are imperative. The lack of physical security combined with conventional operation make sensor node prone to a high risk of being captured and compromised. Jeong, et al, comparatively analyzed the unique network-centric features and security mechanisms of various heterogeneous wireless networks that are expected to be part of OWA (Open Wireless Network Architecture) and proposed an integrated security platform based on the security profile concept [4]. Bo sun, et al, introduced WSNs and RFID system and presented their security concerns and related solution. They focused on linear configuration generator based on lightweight block cipher that can meet security co-existence requirements of WSNs and RFID system for pervasive computing [5].

3. Basic Security Concepts

To integrate several open wireless sensor network into single networks, a lot of consideration should be taken into account to solve challenges that must be addresses. These matters include support for mobility management, quality of service provision, and security interoperability. An integrated security mechanism is one of the key challenges in open wireless network architecture because of the diversity of the networks in open wireless network architecture and the unique security mechanism used in each of the networks. Configuration of infrastructure of unification of wireless and wired system is shown in figure 1. Therefore, it is required to integrate individual communication topology and each security requirement. Recently, we are faced with a lot of change of communication because new technologies have advanced. Communication topology of former days divided into wireless and wire communication. It consists of individual communication topology. But, recently the topology of communication is merged and united with wired and wireless part [6].

Security of wireless networks can be more easily compromised and may be vulnerable to a more diverse range of threats than wired networks. The generic security requirements are as follows.

- Confidentiality
- Authentication
- Integrity
- Availability
- Non-repudiation

Security technology can be implemented with cryptographic mechanism. Cryptographic is composed of two processes, encryption and decryption. The popular techniques are private key cryptosystem and public key cryptosystem. The representative factors are as follows.

A. Fundamental security approaches

- Multiple security mechanisms for source to destination security
- Evolution from the notion of security mechanisms to the notion of security management
- Upper layer security approach
- Multiple independent security processes

For example, to realize u-healthcare system, we take into consideration components such as confidentiality by authentication and encryption, data privacy, confidentiality, and availability by authorization, encrypted database and backup of database. The measures can be categorized into four security layers [7]. They are authentication based on network, authentication based on application, database protection and user's privacy. The example is shown in figure 2 and 3.

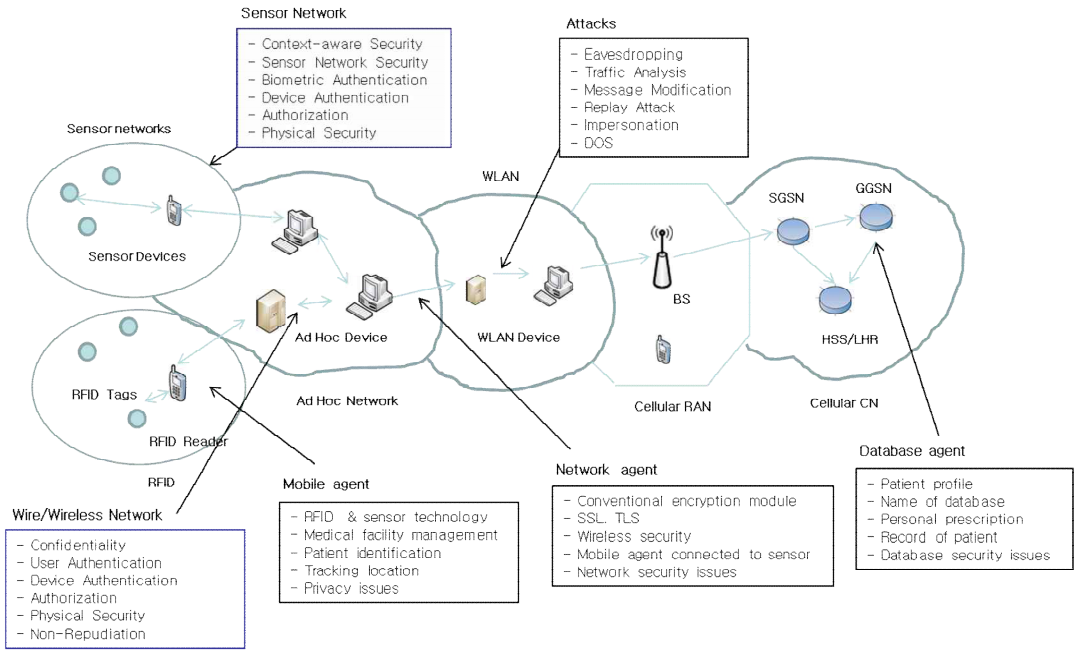

Figure 1. Configuration of Infrastructure of Unification of Wireless and Wired System

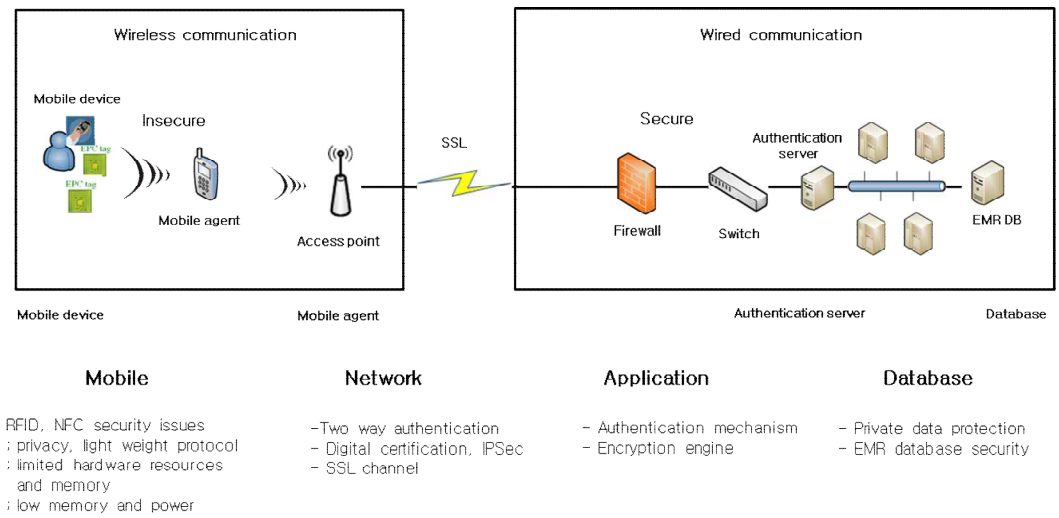

Figure 2. Example of Ubiquitous Sensor Network Infrastructure

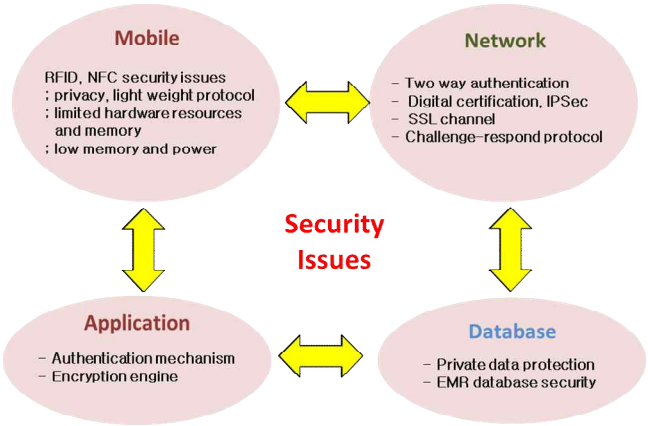

Figure 3. Element of Security Issues in Layer

4. Security Features and Mechanisms of Wireless Sensor Network

For security applications in wireless sensor networks (WSNs), choosing best algorithms in terms of energy-efficiency and of small-storage requirements is a real challenge because the sensor networks must be design with limited resources and capabilities. Sensor networks are made by the tremendous advances and convergence of micro-electro-mechanical systems (MEMS), wireless communication technologies and digital electronics. Sensor networks are composed of a large number of tiny devices or sensors which monitor their surrounding area to measure environmental information, to detect movements, vibrations [8]. We analyzed requirements to implement an architecture based on wireless part related to wireless networks with specialized features.

A. Requirement of security mechanism between heterogeneous device level

We need to analyze integrated infrastructure with heterogeneous wireless network and to optimize security issues under ubiquitous surroundings. We deduced requirement of security issues as follows.

- Analyses of problem for security mechanism under multiple surroundings from transmitter to receive
- Optimization of individual security mechanism under different security level under heterogeneous network level and possibility of mathematical calculation with standard algorithm
- Design of optimization of upper level to implement individual security level in transport layer
- Design of independent mutual security authentication in heterogeneous device
- Analyses of group key management and protocol to utilize different security mechanism in upper layer

B. Adaptation of procedure of security requirement

It is necessary to analyze optimized protocol and procedure between transmitter and receiver and approach networks to be accessed individually as shown in figure 1 [9].

- User to device
- Sensor device to sink or RFID tag to reader
- Sensor networks to Ad hoc network
- Ad Hoc networks to WLAN
- WLAN to cellular network
- Secure routing protocols
- Security of cellular networks
- WLAN security
- Security of Ad hoc networks
- Key distribution
- Security of sensor networks

- RFID security
- Non-cryptographic schemes
- Lightweight cryptographic schemes
- Conventional cryptographic schemes

C. Analyses of lightweight protocol in RFID application

Security problem due to limited resources and computing power under unified protocol between wireless sensor network and RFID device

- Analyses of privacy requirement and security of wireless sensor network
- Key management technique and process of call procedure
- Mutual authentication process between RFID and tags
- Performance analyzes with different algorithm such as non-cryptographic schemes, lightweight cryptographic schemes and conventional cryptographic schemes

Table 1 is shown the summary of threats and risk mitigation in RFID system [10]. Some well-known attacks includes such as physical attacks, Denial of Service (DoS), counterfeiting, spoofing, eavesdropping, traffic analysis, relay (man in the middle) attacks and replay attacks [11].

Table 1. Threat analyses matrix of RFID system [10]

Threats	***Affected RFID component***	***Risk mitigation***
Rogue reader	Tag, Air-interface, reader	Reader authentication
Eavesdropping	Tag, Air-interface	Encryption the data, shielding the tag or limit the tag-reader distance
Reply attack	Air-interface	Using short range tags, shielding the tag or implementing the distance bounding protocol
Replay attack	Tag, Air-interface	Encryption the data, shielding the tag or limit the tag-reader distance, tag authentication
Tag cloning	Tag, Air-interface	Tag authentication
Tracking object	Tag, Air-interface	Low range tags or shielding tags, authenticating the readers or disabling the tags
Blocking and jamming	Air-interface	Detect early and localize, take appropriate action
Physical tag damage	Tag	Use protective material

Table 2 shows structure of secure layer and its characteristics.

Table 2. Structure of secure layer and its characteristics

Mobile Device	***Network***	***Database***
RFID, NFC security issues	Two way authentication	Private data protection
Privacy, light weight protocol	Digital certification, IPSec., Encryption engine	EMR data security
Limited hardware resources and memory	SSL channel	Authentication Mechanism
Low memory and power consumption	Challenge response protocol	Encryption engine

RFID (Radio Frequency Identification) is an automatic identification technology to remotely store and retrieve data. A typical RFID system is composed of RFID tags, RFID readers and a back-end server. Recently, the wide deployment of RFID systems in a variety of applications has raised many concerns about the privacy and the security. An RFID tag can be attached to a product, an animal, or a person for the purpose of identification using radio waves. The RFID and NFC (Near Far Communication) technologies bring required functions for developing and building a modern identification system for decreasing mistakes in healthcare. Deploying RFID technology in the healthcare industry for promoting patient's data and records in hospital is a complex issue since it involves technological, economic, social, and managerial factors. Hailong Feng and Wenxiu Fu proposed recent development about privacy and security of the IoT (Internet of things) and challenges and future trends of the IoT [12].

For any possible reasons, an adversary may perform various attacks such as eavesdropping, traffic analysis, spoofing, disabling the service, or disclosing sensitive information of tags, and hence infringes people's privacy and security. Although there have been many works devoted to design security mechanisms for low-cost RFIDs, most of these works require the tags to be equipped with costly operations such as one-way hashing functions, which are still unavailable on low-cost tags because limited resources. Contrary to these works, schemes which are developed in recently do not require the support of hashing functions on tags. However, the schemes have been reported to show some security weaknesses. Recently, Lars Kulseng et al. [13], proposed a lightweight RFID authentication protocol for low-cost RFIDs based on only bitwise XOR. Different from most of existing solutions which used conventional cryptographic primitives such as encryptions and hashing, theses protocols only used simple operations like XOR and substring [14]. Therefore, many attacks are occurred and the representative attacks are described in table 3.

Table 3 summarizes the major barriers, benefits and attacks from collected literature as shown in 2 [12].

Table 3. Benefits, barriers and attacks of RFID applications in healthcare system [15]

Benefits	***Barriers***	***Attacks***
Increased safety or reduced medical errors	Interference	Denial of service
Real-time data access	Ineffectiveness	Physical attack
Time saving	Standardization	Tag cloning attack
Cost saving	Cost	Replay attacks
Improved medical process	Privacy and legal issues	Spoofing attack
Other benefits : improve resource utilization	Other barriers : Lack of organizational support, security	Side channel attack Tag tracking

Wei-Bin proposed a cryptographic key management solution for HIPAA Privacy and security regulations [16]. The HIPPA privacy and security regulations are two crucial provisions in the protection of healthcare privacy. Privacy regulations create a principle to assure that patients have more control over their health information and limits on the usage and disclosure of health information. The security regulations give a guideline the provisions which are implemented to guard data integrity, confidentiality, and availability.

5. Conclusion

With the development of RFID technology, its data security and personal privacy issues become increasingly prominent becomes an obstacle to the further development of RFID security concern. Therefore, how to improve its security and protect personal privacy becomes a research focus. RFID technology has a number of advantages, but also opens a number of security problems that need to be addressed before its successful deployment. In this paper, we analyzed wireless sensor networks and RFID systems on real sensor hardware to apply optimized security issues. The security solution used in communication networks including wireless ad hoc and sensor networks are essential for privacy and security concerns related 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: 2012-0007896)

6. References

[1] Chun-Liang Lai, Show-Wei Chien, Li-Hui Chang, Shiu-Ching Chen and Kwoting Fang, "Enhancing medication safety and healthcare for inpatients using RFID", In Proceedings of PICMET 2007, pp.2783-2790, 2007.
[2] Mykletun, E., Girao, J., and Westhoff, D., "Public key based crypto-schemes for data concealment in wireless sensor networks," In Proceedings of IEEE International Conference on Communications, pp. 2288-2295, 2006.
[3] Ari Juels, "RFID security and privacy: A Research survey", IEEE Journal of selected areas in communications, v.24, v.2, pp.381-394, 2006.
[4] Jongmin Jeong and Zygmunt J. Haas, "An integrated security framework for open wireless networking architecture", IEEE Wireless Communication, April, pp.10-18, 2007.
[5] Bo sun, Yang Xiao, Chung Chih Li, Hsiao-Hwa Chen, and T. Andrew Yang, "Security co-existence of wireless sensor networks and RFID for pervasive computing,", Computer Communication, 31, pp.4294-4303, 2008.
[6] Pardeep Kumar, Sang-Gon Lee and Hoon-Jae Lee, "A user authentication for healthcare application using wireless medical sensor networks", 2011 IEEE International Conference on High Performance Computing and Communication, pp.647-652, 2011.
[7] Cheng-Chan Hung and Shiow-Yuan Huang, "On the study of a ubiquitous healthcare network with security and QoS", In Proceedings of IET2010, pp.139-144, 2010.
[8] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar. "SPINS: Security Protocols for Sensor Networks. Wireless Networks", v.8., n.5., pp.521–534, 2002.
[9] D. Djenouri and L. Khelladi., "A survey of security issues in mobile Ad Hoc and sensor networks", IEEE Communication Surveys and Tutorials, v.7, n.2., pp.2-28, 2005.
[10] Benjamin Khoo, "RFID as an enabler of the Internet of Things: Issues of security and privacy", In 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing, pp.709-712, 2011.
[11] Se-Hwan Kwon and Dea-Woo Park, "Hacking and security of encrypted access points in wireless network," Journal of Information and Communication Convergence Engineering (JICCE), vol.10, no.2, pp.156-161, 2012.
[12] 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, 2010.
[13] Lars Kulseng, Zhen Yu, Yawen Wei, and Yong Guan, "Lightweight secure search protocols for low-cost RFID system," 2009 29th IEEE International Conference on Distributed Computing Systems, pp.40-48, 2010.
[14] Hung-Min Shin and Wei-Chih Ting, "On the security of Chien's Ultra-lightweight RFID authentication protocol," IEEE Transaction on Dependable and Secure Computing, V.8, N.2, pp.315-317, 2011.
[15] Hung-Yu Chien,"Varying pseudonyms-based RFID authentication protocols with DOS attacks resistance", In 2008 IEEE Asia-Pacific Services Computing Conference, pp.507-615, 2008.
[16] Wei-Bin Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," IEEE Transaction on Information technology in Biomedicine, vol.12, no.1, pp.34-4, 2008.