A Study on RFID System with Secure Service Availability for Ubiquitous Computing

Dae-Hee Seo*, and Im-Yeong Lee*

Abstract: Spotlighted as an innovative information technology environment, ubiquitous computing has been actively researched on recently. Especially, domestic and global researches focus on the RFID system, which is being eyed to replace the existing bar-code system. As an essential technology for ubiquitous computing, the RFID system can be applied for various purposes. The security issues of the RFID system focus on how the low-priced tag type could have reasonable price competitiveness. The Auto-ID Center in the U.S. is spearheading the research on distribution service and omni-directional security. As for Japan, the researches on omni-directional security and EPC application are necessary in securing the technology for ubiquitous computing with support from the Ministry of Public Management Home Affairs, Posts, and Telecommunication. In this paper, a method of ensuring the availability of the RFID system service will be presented based on the ubiquitous computing environment with the existing omni-directional security and user-friendly interface. While the existing researches focus on the RF reader system and tag-based security, this paper's suggestion also considers the availability of a service to suggest ways of increasing the practical usage of a low-priced RF tag.

Keywords: RFID, Service Availability, Secure Communication, Network Management Ubiquitous Computing

1. Introduction

The ubiquitous network environment features a network that finds user-focused surrounding situations and environments intelligently, optimizes user network environments, and conveniently connects to the network. It also features a network that is free and safe to use contents. The ubiquitous network technologies include ubiquitous, flexible wide band, ubiquitous teleportation, ubiquitous agent, contents, appliances, ubiquitous platform, and ubiquitous sensor network. Among these technologies, the ubiquitous sensor network is the essential component that enables peripheral devices that is in close proximity to the user to communicate, and, thus, independently collect and manage necessary data.

RFID is the key technology of the ubiquitous network that enables exchange of data by remote detection, and recognition of the data through wireless communication. It can replace the existing bar code system, which is applied widely in off-line systems. Through this technology, many application services are available for individual and industrial users as well. Many R&D activities have been conducted recently.

Manuscript received October 5, 2005; accepted November 21, 2005.
This research was supported by MIC(Ministry of Information and communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment)

* Division of Information Technology Engineering, Soonchunhyang University, Asan, Korea ({ patima, imylee}@sch.ac.kr)

However, among existing RFID studies, the study on security has been focused on the security between the RF reader and the RFID tag. This means that security vulnerability may occur due to the characteristics of the tag itself when both individual and industrial users avail of services that use the RFID tag [2][4].

Thus, the necessity of the RFID system and its security will be described in Section 2 of this paper. The analysis on the security vulnerability of the existing RFID system will be performed, and the security requirements that can ensure the availability of the services that were not considered in the existing system will be presented in Section 3. The service availability ensuring scheme of the RFID system that satisfies the security requirements suggested in Section 3 will be proposed in Section 4. The proposed scheme will be analyzed in Section 5, and the conclusion will be described in Section 6.

2. Analysis of the RFID System

Under this system, the overview of the RFID system and the necessity for security will be described.

2.1 Overview of the RFID System

RFID is the wireless communication system that consists of the RF reader, which performs read and recode functions, and RF tags, which provide data to the system.

RFID is the system that tags the identification data for individuals, vehicles, freights, etc. By decoding the tagged data through a wireless communication medium without touching it, various applications that have been performed offline previously can now be automated.

The RFID system utilizes the concept of 'the Internet of Things'. This concept provides services to detect tagged items from a distance in real-time through the Internet, or a network similar to the Internet. Therefore, we can predict from it that newer use of Internet will be possible.

Therefore, more than a few billion effective RFID tags and wireless networks will be required every year, and newer software and bar codes or a similar system that can deal with many items may be required, leading to supporting more applications [1].

2.2 Necessity of security for the RFID system

The RF tag has a physical function that is considered most unrealistic in terms of security. Especially, in the case of competitive price tags, there are limitations in the application of various security services. Therefore, the tag shall be able to send and receive data from any reader, and maintain the security for sending and receiving data and safety against various attacks through limited access to unauthorized attackers hovering between the tag and the reader. The problems in the existing RFID system are mainly the security of the data received and sent from the RF tag, and user authentication and privacy protection. In case of security services for the data received and sent from the RFID tag, there is a limitation in the application of various security services due to the characteristics of the RFID tag. Therefore, the service to supplement exposure or change the transmitted data is required. The second problem is user authentication and privacy protection. If the competitively priced RFID tag replaces the existing bar code system, the attacker can easily obtain the user's privacy information, and illegally access the user's privacy data. The related study deals with the availability of the service. The availability of the service is a requirement that must be provided together with the security service when the Ubiquitous computing environment is established, but it was not considered in existing studies. If availability were not ensured, the security service that would address existing problems would be meaningless even though the security service is provided, due to the physical limitation of the RFID tag [1][2].

3. Analysis of the RFID System Analysis on RFID Related Studies and Security Requirements

In this section, the security vulnerability of the existing studies for the RFID system will be analyzed, and security requirements for RFID will be presented to ensure the availability of the service

3.1 The existing studies regarding the RFID systems

The studies related to the tag-based RFID are recently getting more attention in relation to ubiquitous computing, and the representative scheme in the existing study is the MIT Auto-ID center scheme. In the auto-ID center, the protocol in providing the security service by using the Hash function is suggested, and the study in which this is applied is underway.

(a) Hash Lock Scheme: This is the scheme suggested by MIT, and considers lowest price. Each individual is considered to have the Hash function, and the procedures are as follows. First, the RF reader transmits key K to each RFID tag, respectively, and the RFID tag calculates the Meta ID. (Meta ID = Hash (K)) The tag transmits the request message for ID access, and the Meta ID is transmitted as a response to that request. The reader verifies the message, considering relevancy between the pre-allocated key and the Meta ID, and transmits the response to the RFID tag if the verification process is cleared. In this scheme, the authentication process is performed through just the consent given to the transmitted data and the transmission of the ID from the reader [1].

The MIT scheme is restricted to the applicable scheme with competitive pricing through the low-cost and fixed Meta ID, but the tag can be attacked when the Meta ID is opened. Slight differences may exist, depending on the operating system and the requirements, though the Meta ID should not be fixed.

(b) Randomized Hash Lock Scheme: This is the scheme suggested by MIT, and is an expanded Lock type. This scheme assumes that the RFID tag has safe Hash functions and a random generator, which is different from the existing scheme. Each tag generates a random number, and generates a safe Hash value by using generated random numbers as input values. (r and ID. C=H(ID||r)). The tag transmits C and r to the RF reader.

The reader transmits the received data to the backward database. The database stores received r and corresponding ID, respectively, through the Hash function. The database verifies the C and the ID through relevancy [5].

This scheme is difficult to track since the output information of the RFID tag is changed in every access. However, this scheme provides tracking information on the location of the RFID tag. Especially, if it is related with the secret information of the tag, it cannot be satisfied with forward security. Additionally, the Hash function may be applied to the competitive price tag, but is actually impossible in case of the pseudo-random number generator.

3.2 RFID system security requirements

Several technical problems should be considered beforehand in line with the security of the RFID system. The first one is the problem related with ACIN (Authentication, Confidentiality, Integrity, and Non-repudiation), and is the problem in initial authentication. Many studies

have been conducted regarding authentication. However, the purpose of the existing studies was focused on safe authentication, and the anonymity of the ID was not considered. Therefore, anonymity should be provided through various changes in the ID. However, if ubicomputing were focused on the user in order to provide the service in an actual RFID system, it would be very vulnerable to various attacks due to the characteristics of the RFID. Therefore, despite the problem that is unrealistic, existing studies used various security algorithms to maintain safety against attacks. This paper will propose three security requirements that focus on availability in order to solve potential problems in case the service is not provided due to attacks or the physical failure of the established RFID system, rather than using various applications to enhance security.

- Forward channel security: Forward security is required to generate and provide the service through secure communication between the RFID tag and the RF reader. This is because the attacker can prey on the various information transmitted or received from the RFID tag.
- Secure status acquisition technology: When constructing the RFID-based network, a safe service acquisition process is required to know the status of all RFID tags. This must be performed by checking the current status of all tags in the RFID system in order to ensure the availability of the service against potential physical failure that may happen during DoS attacks or during the construction of the RFID system.
- Availability: When constructing the RFID system, failure in hardware or software may occur due to deliberate action or not. Therefore, if the RFID tag cannot provide service due to attacks or physical failure during the construction of the system, the availability of the RFID system should be provided to restore the service promptly.

4. Proposed Scheme

This section will propose the scheme to ensure the availability of service in the RFID system. The proposed scheme is aimed at providing the service based on the priority of the message, instead of tags that cannot provide the service by the attacker such as DoS (Denial of Service) when the network is established through the service setting of the RF tag and the anonymity ID setting process, after initial authentication is performed.

4.1 Assumptions

The assumptions made to propose the scheme to ensure the service availability of the RFID system are as follows:

① RF tag conducts safe Hash function and XOR operation through passive tags.

② RFID tag and backward server exchanges key beforehand safely.

③ The backward host server can provide all services provided by RFID tags.

④ The backward host server defines the priority among service messages provided by RFID according to the policy priority given to the message, as shown in Table 1.

Table 1. Backward host Server's message level

RFID	Message	Message Policy	RFID information
ID 1	Message 1	3	RF Code 1
ID 2	Message 2	1	RF Code 2
ID 3	Message 3	2	RF Code 3

4.2 System coefficients

The system coefficients needed to propose the scheme to ensure the service availability of the RFID system are as follows:

- HID, RID, RFID : Backward Database Server's ID, RF Reader's ID, RFID Tag's ID
- H(), h : Secure Hash Function, secure hash value
- R : Random number
- M : Service Request Message
- Mres : Service Response Message
- Query(Update_Message) : RAM Update Message of RF Tag

4.3 Protocol

The scheme to ensure the service availability of the RFID system consists of 1) initial authentication protocol, 2) service setting of the RF tag and the anonymity ID setting protocol, and 3) service availability guarantee protocol. The details of the service availability guarantee protocol are also shown below.

4.3.1 Initial authentication protocol

Initial authentication protocol performs the RF authentication protocol that provides forward security through communication between the reader and the RF tag.

① The RFID reader transmits the initial query message to the RF tag.

② The RF tag generates MID by using the initial reader and the key that is allocated beforehand and stored, and transmits it to the RF reader.

$$MID = H(K)$$

③ The RF reader transmits the received MID and RID, the ID of the RF reader, to the backward database server.

④ The backward database server stores received MID and RID in the corresponding table, and calculates and transmits R_H, V, HID to the reader.

$$V = (H(K) \oplus R_H)$$

⑤ The RF reader identifies HID and transmits RFID to the RF tag together with R_H that is received from the backward database server.

⑥ The RF tag generates h_T by using, R_H , that is received from the RF reader, and transmits it to the RF reader together with the RFID.

$$h_T = H(R_H)$$

⑦ The RF reader transmits the RFID of the RFID tag to the backward database server, and the initial authentication process is performed.

4.3.2 Service setting of the RF tag and the anonymity ID setting protocol

The service setting of the RF tag and the anonymity ID setting process performs service setting for the RF tag and the anonymity ID setting protocol that has completed the initial authentication process.

① The RF reader transmits the query message to the RFID tag.

② The RFID tag that has completed the initial authentication process generates the following response message against the query message for the service setting, and transmits M, RFID, and h_{T_1} to the RF reader.

$$h_{T_1} = H(RFID \oplus K \oplus R_H)$$

③ The RF reader verifies h_{T_1} received from the RF tag, and transmits M and all $RFID$ to the backward database server if the verification process is cleared.

④ The backward database server generates h_H based on the RFID's of all registered tags during process ⑥ of the above 1), and transmits R_H ', the random number, and M_{res} , the response message, according to the priority for M, a service request message, to the RF reader.

$$\text{I list} = (RFID_1, RFID_2, ..., RFID_i, ..., RFID_n)$$
$$h_H = H(I)$$

⑤ The RF reader generates $RFID'$, the anonymity ID of the RFID tag, and transmits M_{res} and R_H ', to the RF tag.

$$\text{I'} = (RFID_1, RFID_2, ..., RFID_{i-1}, RFID_{i+1}, ..., RFID_n)$$
$$RFID' = H(I) - H(I')$$
$$h_R = H(R_H' \| M_{res})$$

Fig. 1 shows the initial authentication protocol, the service setting of the tag, and the anonymity ID setting process.

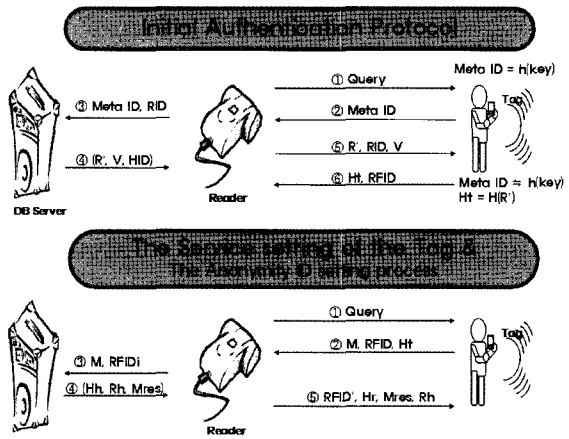

Fig. 1. The initial authentication protocol, and the anonymity ID setting process.

4.3.3 Service availability guarantee protocol

In order to establish the network in the RFID system, and to receive the service based on it, the following detail protocol shall be performed.

① The RF reader transmits the initial query message to the RFID tag.

② The RFID tag calculates and transmits Y together with the service message, M, to the RF reader. (Communication of $RFID_i$)

$$Y = RFID' \oplus H(K \oplus R_H')$$

③ The RF reader extracts RFID' from Y that was received from the RFID tag to verify the anonymity ID, and provide the service by transmitting RID and X to the backward database server if the verification process is cleared.

However, the RF tag is very vulnerable to various denial of service or power consumption attacks due to the characteristics of the network construction. Therefore, if the service is not available due to a denial of service attack or a power consumption attack, the detail protocol that will be used to provide the availability of service shall be performed as follows.

[Detail protocol of the service availability guarantee protocol]

① The RF reader transmits the initial query message to the RFID tag.

② The RF reader judges an RFID tag as being attacked through a denial of service or an effect on the power consumption if no response message is received from the RFID tag. The RF reader transmits the recovery message to ensure the availability of service to the

backward database server, and broadcasts the request message for the X information to the entire network.

RF Reader -> Backward Data Base Server : Recovery Service Request

RF Reader -> Broadcasting Message

③ The RFID tags calculate X and Z as follows, and transmits them together with the current service message, M, to the RF reader.

$$Z = H(K \oplus R_H')$$

$$X = RFID_i' \oplus Z$$

④ The RF reader verifies $RFID_i'$, the registered anonymity ID for RFID tags, and transmits the X and Z lists and the RFID of the RFID tag, of which service is paralyzed by the illegal attacker, to the backward database server if the verification process is cleared.

⑤ The backward database service extracts X_i of the RFID tag, which has been affected by the attacker, from the table of the stored data, and transmits X_i and HID of the RFID tag, of which message level is the lowest when compared to the priority of M, the message of the affected tag, to the RF reader.

⑥ The RF reader transmits the message of the RFID tag that has been affected by the attacker to the RFID tag that has the lowest level of service, so as to provide higher message priority.

$$h_R = H(M_i \| RFID_m)$$

$$M_i, h_R, RFID_m, Query(Update\_Message)$$

The RF reader updates the stored anonymity ID list and the corresponding X list, while the backward database server performs the service to ensure the consistent availability of service by updating the X and Z lists. The process above is shown in Fig. 2.

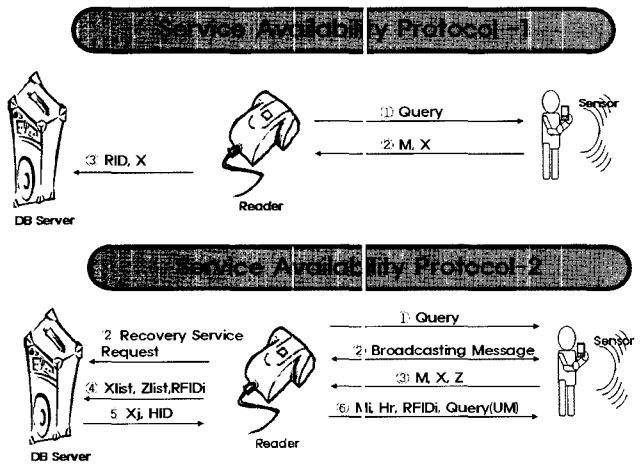

Fig. 2. Service availability guarantee protocol.

5. Analysis of the Proposed Scheme

In this section, the difference from the existing scheme and its security characteristics will be described through the security analysis for the proposed scheme. The proposed scheme has the following degree of effectiveness as well as the security requirements described in Section 3.

5.1 Security Analysis

The proposed scheme satisfies the following for security services against potential attacks to the system.

- Forward channel security: The proposed scheme can ensure anonymity throughout the use of the RFID, which has been a problem in the existing scheme. That means that the attacker cannot obtain relevancy between the opened RFID and the anonymous RFID, and thus, the attacker cannot obtain the tag ID and the data transmitted to the backward host server.
- Secure status acquisition technology: In order to acquire the status for all RFID tags that are included in the RFID system, the proposed scheme used K, X(= RFID' ⊕ Z), and Z(= H(Key ⊕ R_H)) keys that have been allocated beforehand. Z is generated based on the key K, which has been used during the initial allocation of the RFID tag, and R, a random number that was generated and allocated from the backward host server. X is generated based on the anonymous ID of the RF tag and X. This proposed more realistic security type by suggesting the operation scheme which enables the XOR operation in lieu of a random number generator, which is suggested as impossible for the competitively priced RFID tag in the existing scheme.
- Availability: The proposed scheme satisfies the availability requirement for the service that has not been considered in the existing scheme. This ensures the availability of the service message by transmitting message M and the corresponding $RFID_j$ that can provide the service for the tags, of which service is interrupted by an attacker or is paralyzed by physical failure, through the X and Z lists based on the Hash value, which is generated from the RF tag during the status acquisition process for various RF tags, and the random value, R, which is generated from the backward host server.

5.2 Effective Analysis

When compared with the existing scheme, the proposed scheme requires two operations, the safe Hash function operation and the XOR operation. It provides the required degree of effectiveness to maintain the proper level of safety that will be applied to the competitively priced RFID tag, compared to the existing scheme. This may provide lower efficiency when compared with the scheme

that uses only the Hash function considered in a) of Section 3.1. Nevertheless, the proposed scheme provides various types of security services that were not considered in a) of Section 3.1. Also, when compared with b) of Section 3.1, the proposed scheme is more realistic for the low price tag by performing the XOR operation in lieu of an unrealistic random number generator. Therefore, the proposed scheme is considered to be more realistic, and has a higher degree of effectiveness when compared with the scheme in b) of Section 3.1.

6. Conclusion

A study on the safe availability guarantee scheme was performed in this paper, based on RFID among wireless communication technologies for which various studies and commercial development are being made for the application of ubiquitous computing technologies, a next-generation IT-based environment. Specifically, wireless communication technology is necessarily required to build a user-oriented network, such as an ubiquitous computing environment, and security technology is necessarily required to protect the privacy of the users. However, the proposed scheme can remain vulnerable in various attacks, such as protocol modification attacks, physical attacks, and other types of network attacks. Therefore, a study for the authentication method for the security service of the RFID tag, as well as for complementary issues against various security threats, should be performed consistently in future studies.

References

[1] Miyako Ohkubo, Koutarou Suzuki and Shingo Kinoshita, "*Cryptographic Approach to "Privacy-Friendly*" Tag" RFID Privacy Workshop@MIT, Nov, 2003

[2] Sanjay E.Sarma, Stephen A. Weis and Daniel W. Engels, "*Radio-Frequency Identification : Secure Risks and Challenges*", RSA Laboratories Cryptobytes, vol. 6, no.1, pp.2-9. Spring 2003

[3] Sanjay E.Sarma, Stephen A. Weis and Daiel W. Engels, "*Radio-frequency identification systems*", In Pro-ceeding of CHES '02, pp454-469. Springer-Verlag, 2002. LNCS no. 2523.

[4] Sanjay E.Sarma, "*Towards the five-cent Tag*", Technical Report MIT-AUTOID-WH-006, MIT Auto ID Center, 2001.

[5] Stephen A. Weis, "*Security and Privacy in Radio-Frequency Identification Devices*", Masters Thesis. MIT. May, 2003

[6] Stephen A. Weis, Sanjay E.Sarma, Ronald L. Rivest and Daiel W. Engels, "*Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems*", First International Conference on Security in Pervasive Computing, 2003. http://theory.lcs.mit.edu/ sweis/spc-rfid.pdf

[7] MIT Auto-ID Center. http://www.autoidcenter.org

Dae-Hee Seo

He received the M.S degree in Division of Information Technology Engineering from Soonchunhyang University. He is currently a Ph.D Course at the Division of Information Technology Engineering of Soonchunhyang University. His research is interested in information security, wireless internet and mobile network security.

Im-Yeong Lee

He received the B.S degree in electronic engineering from Hongik University and M.S. and Ph.D. degrees in communication engineering from OSAKA University, Japan, in 1981, 1986, and 1989. He is currently a Professor at the Division of Information Technology Engineering from Soonchunhyang University, Korea, His research is interested in Information security, Cryptography and Mobile network security.