Analyses of RFID System Using Lighted Weight Algorithm

Jung-Tae Kim, *Member, KIMICS*

Abstract— In this paper, we propose a general idea about an RFID system which provides lighted weight algorithm. We discuss how RFID could be applied for this kind of system, especially, compact protocol. We evaluate a few protocols that have been suggested for use in passive RFID tagged systems. We can reduce security computation without losing security features by message integration and pre-computation in this paper. And the proposed protocol can be used in low-cost RFID systems that require a small computational load for both the back-end database and the tags

Index Terms— Authentication, RFID, Ubiquitous system, lighted weight algorithm

I. INTRODUCTION

Over the last few years, ubiquitous computing has been integrated into many aspects of our lives because of the evolution of radio frequency identification (RFID) and mobile phone technology. We define a simple RFID as a networked processing device with the following features: an RFID to work actively, a limited number of data transfers, low-bit data transfer, and long-range radio-communication by VHF/UHF frequency.[1,2] The network topology between RFIDs and databases is shown in Fig. 1. There are two key elements within a RFID system:

- RFID tag, or transponder, carries object-identifying data.
- RFID reader, or transceiver, reads and writes tag data. Basically, the tag reader broadcasts a radio frequency signal to access information stored on the tags nearby. This information can range from static identification numbers to user written data or data computed by the tag. Radio frequency identification (RFID) is an automatic identification system that can remotely store and retrieve data about objects by using small devices called RFID tags. RFID systems consist of radio frequency (RF) tags and RF readers. Tag readers can question tags about their contents by broadcasting an RF signal, without physical contact. Radio frequency identification (RFID) technology is expected to become an important and ubiquitous infrastructure technology of supply chain processes and customer service. The low-cost tag, or so-called passive tag will be likely the factor for widespread adoption of the technology. The simple protocol for a single-use RFID requires the following features: high security, lightweight computation, and narrow-band communication. Because the distance between a single-use RFID and RFID reader is a few kilometers, four kinds of security (anonymity, authentication, confidentiality, and integrity) are required to protect against remote attacks by tracking, spoofing, eavesdropping, and altering. Furthermore, a small circuit and small battery is required to implement a single-use RFID on a small mobile objects RFID mutual authentication to protect user privacy and use fewer calculations for tags. There are two key elements within a RFID system:

- RFID tag, or transponder, carries object-identifying data.
- RFID reader, or transceiver, reads and writes tag data. Basically, the tag reader broadcasts a radio frequency signal to access information stored on the tags nearby. This information can range from static identification numbers to user written data or data computed by the tag. Radio frequency identification (RFID) is an automatic identification system that can remotely store and retrieve data about objects by using small devices called RFID tags. RFID systems consist of radio frequency (RF) tags and RF readers. Tag readers can question tags about their contents by broadcasting an RF signal, without physical contact.

Manuscript received January 8, 2009; revised March 5, 2009.

Jung-Tae Kim is with the Department of Electronic Eng, Mokwon University, Taejon, Korea (Tel: +82-42-829-7657, Fax: +82-42-823-8506, Email: jtkim3050@mokwon.ac.kr)

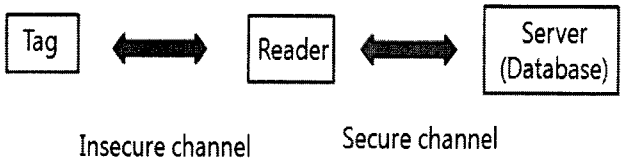


Fig. 1 Basic RFID system

II. RELATED WORK

Many proposals have been proposed to satisfy the security requirements in order to resolve the privacy problems. We have divided the previously proposed protocols into two categories. Hash Function Based Security Protocol Hash-lock protocol and the randomized hash-lock protocol proposed by Weis et al., the hash-based ID variation protocol proposed by Henrici et al. and the hash chain protocol proposed by Okubo et al. are the most interesting and efficient protocol based on hash function. However, these methods are proven to be unsecure and not efficient in those three security requirements aspect. A security protocol based on arithmetic calculation in order to fulfill the low implementation is needed, Juel et al proposed minimalist cryptography using one-time pad scheme for low-cost RFID system and a HB algorithm based protocol.[3,4] However, one-time pad based protocol did not fulfill the implement cost limitation and several security problems of the HB algorithm based protocols have been verified recently. The security factors interested in RFID system is as follows.

A. Anonymity

Synchronization approach is appropriate for the conventional protocol because of its design for simple RFID implementation.

B. Authentication

Authentication is for preventing spoofing. There is much research on authenticating RFIDs and RFID readers by a challenge-response-based protocol.

C. Confidentiality

Confidentiality is for preventing eavesdropping. There is a low-cost implementation of standard encryption/decryption algorithms, such as AES, for RFID

D. Integrity

Integrity is for preventing alterations. In general, generating and validating a message authentication code is required .

III. RISKS OF THE RFID SYSTEM

Confidentiality is for preventing eavesdropping. There is a low-cost implementation of standard encryption / decryption. In RFID system, communications between server and reader generally takes place through a secure channel. However, communications between reader and tag usually occurs via wireless communication which is an insecure channel. Thus adversaries can eavesdrop the transmitted message and attack the system. The main risks of the RFID system are as follows.

(1) Eavesdropping: The transmitted message can be easily eavesdropped since communications between tag and reader are via a wireless medium. Eavesdropped information can then be used as the basic information for attack.

(2) Traffic analysis: The attacker may monitor the traffic between tag and reader, and analyze the content of eavesdropped information and predict the response of the tag to the reader's query. Usually, through traffic analysis, it will diminish user's privacy protection.

(3) Replay Attack: Adversaries attack system by retransmitting the eavesdropped information if the system has insufficiency on security.

(4) Position Detection: The attacker can gain identification information from the communications between tag and reader. This is used to locate the user and is a form of privacy invasion of the user. For some VIPs or applications such as E-passport, how to protect privacy is an essential issue.[5] The various security threats resulting from an insecure channel can be categorized as follows:

- Information leakage: One RFID privacy problem is information leakage about a user's belongings. For example, a user may not want certain information known by others, such as ownership of expensive products, identification of personal medicine, and so on.

- Spoofing and replay attack: After an adversary sends a malicious query to a target tag, they collect the responses emitted by the tag. The attacker can then impersonate the reader using the messages collected from the tag. Conversely, an adversary can replay the reader's query to impersonate the target tag. An attacker can also impersonate a legal tag or reader by replaying certain useful messages.

- Desynchronization attack:

If the current ID for a tag is different to the one in the database, this is referred to as a state of desynchronization. Thus, if an adversary blocks certain messages transmitted between a tag and the reader, a dysynchronization state can be created in an ID-renewable RFID system. If the ID of a tag is desynchronized, the tag can be easily traced, as one of

the values emitted from the tag will be constant, thereby compromising the location privacy.

- Location tracing attack: Here, an adversary can obtain some useful information on a tag's location. This attack is essentially applied to a rigid RFID in which certain communication messages between the tag and the database are identical to those used in the previous session.

IV. THE PROPOSED ALGORITHM

We propose a new simple protocol especially designed for single-use RFID. The proposed protocol optimizes the conventional protocol for single-use RFID by integrating authentication and data transfer messages and pre-computing transmitting/receiving frames, without losing security features.

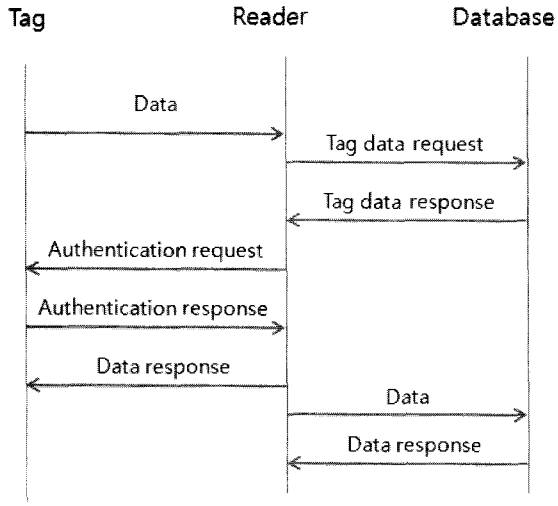


Fig. 2 Conventional protocol

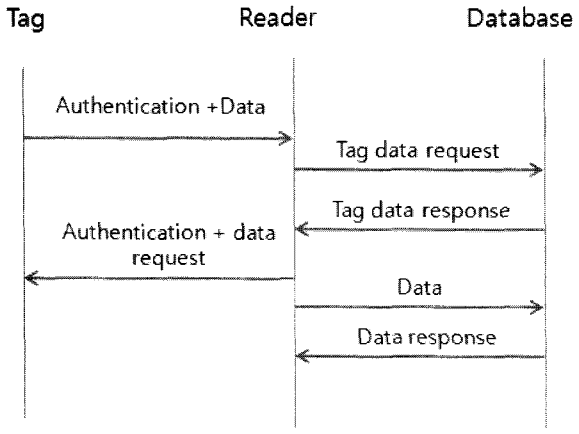


Fig. 3 The proposed protocol

In the initialization stage, tag T is loaded with an initial identifier ID (the identity of a tag), a secret key, and a hash function h(). In the same measure, the back-end database contains the same data stored in tag T; including the ID of the tag, the secret key k and the hash function h(). The back-end database contains fields IDR, K, and Klast, which save the ID, the current k, and the preceding Klast, (the previous secret information which is replaced by the current k), respectively.

We describe the main ideas of our modified protocol to correct problems in previous protocols as follows;

1. To ensure the data privacy and freshness of tag's behavior over a number of requests from reader and the authentication between Tag and Reader, we introduce the Tag's nonce and DataBase's nonce. Therefore a tag needs to have a Random Nonce Generator. Although there are a few literature that a PRN needs more computation capability, it is mandatory that there exits at most one PRN to avoid location trackability of privacy.
2. To ensure the confidentiality of data between agents, we introduce exclusive-or(+) technique into this protocol.
3. To make a secure channel between a reader and a tag, a database and a reader, we introduce Auth value consists of Rkey and DBn like same type of metaID.

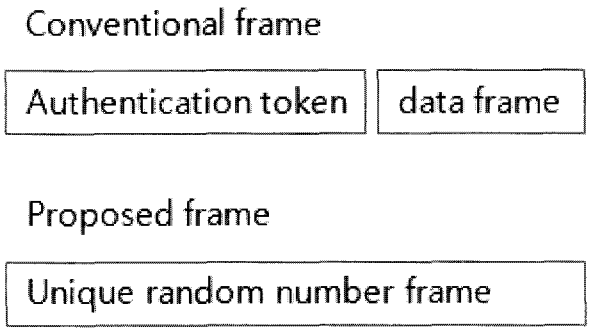


Fig. 4 Comparison of frames

V. PERFORMANCE ANALYSES

The protocol has three main stages: tag identification, mutual authentication and updating.

We evaluate the impact of increasing the stored information, which is the main drawback of the proposed protocol. Analyses show the stored information of the RFID and RFID reader/database. From the Fig. 1, there are mainly three parties involved in our RFID mutual authentication scenario. They are database, the reader and the tag. However,

we assume only two roles in our simplified model, namely the reader (maintaining the database, where all tags' records are indexed and stored in a table); and the tag (to be authenticated). Before a tag is dispatched, it must be written with its identifier (in ROM), its pseudo-ID (in EEPROM) and several secret values (for authentication purpose).[6] We summarize the promising properties of our scheme as follows:

Privacy: a tag's ID is never disclosed in clear text nd its pseudo-ID is changed after every successful protocol round.

Security: the scheme defends against a variety of attacks such as: replay attack, eavesdropping, spoofing attack, skimming attack and active man-in-the-middle attack.

Compact: the 3-pass authentication protocol uses only ultra lightweight functions, whose hardware implementations require only hundreds of gates.

Instead of storing various security parameters as an RFID in the conventional protocol does, an RFID in the proposed protocol stores only transmitting/ receiving frames. In the proposed protocol, the number of possible transmitting frames and expected receiving frames depends on data variation and the number of sequences.

A. Conventional protocol

Information in Tag
- ID Hash Seed
- ID Hash Parameter
- Secret for Authentication
- Secret for Message Authentication
- Secret for Encryption
- Sequence Number

Information in Reader and Database
- ID
- ID Hash Seed
- ID Hash Parameter
- Secret for Authentication
- Secret for Message Authentication
- Secret for Encryption
- Sequence Number

B. Proposed protocol

- Possible Transmitting Frames
- Expected Receiving Frames

Therefore, the compact protocol can communicate its information from tag to server's database. We can reduce security computation without losing security features by message integration and pre-computation. Future work for the proposed protocol by taking into consideration of security properties will be conducted as follows.

A. Security Analysis
- Confidentiality
- Tag anonymity
- Tag/reader authenticity

B. Performance Analysis
- Computational overhead
- Storage overhead
- Communication overhead

VI. CONCLUSIONS

RFID is an emerging technology which will replace lots of the existing Auto-ID technologies. Security is a very important of RFID Systems. The security functions to be adopted in a system, strongly depend on the application contest. We followed another approach and proposed a lightweight challenge-response protocol that can be easily adapted to the limited resource criteria of a passive tag. In conclusion, the proposed protocol can be used in low-cost RFID systems that require a small computational load for both the back-end database and the tags. The work presented in this paper is an ongoing work as denoted by future work section.

REFERENCES

[1] P. Ekdahl, and T. Johansson, "Another attack on A5/1", IEEE Transactions on Information Theory, V.49, N.1, pp.284-289, 2003.Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa,

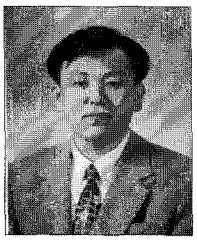
[2] S. A. Weis, etcs, "Security and privacy aspects of low cost radion frequency identification systems", security in pervasive computing, 2003. (Journal Online Sources style) K. Author. (year,

[3] H. Chan, etcs, "Security and Privacy in sensor networks," IEEE Computer, V.36, N.10, pp.103-105, Oct. 2003.

[4] S. Sarma, S. Weis, D. Engels, "RFID systems and Security and privacy implications", in: Workshop on Cryptographic Hardware and Embedded Systems(CHES) 2002, LNCS No. 2523, 2003, pp. 454-469.

[5] S. A. Weis, S. E. Sarma, R. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in Proc. 1st Security Pervasive Comput., 2003, vol. 2802, Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, pp. 201–212.

[6] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in Proc. WorkshopCryptographic Hardware Embedded Syst. (CHES 2004), Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, vol. 3156, pp. 357–370.



Jung-Tae Kim
received his Ph.D. degrees in Electrical and Electronic Engineering from the Yonsei University in 2001. From 1991 to 1996, he joined at ETRI, where he worked as senior member of technical staff. In 2002, he joined the department of electronic engineering, Mokwon University, Korea, where he is presently professor. His research interest is in the area of information security system technology that includes network security system design, chaos cryptosystem and RFID security protocol.