2006

Low-cost RFID identification variation

Koong Lin

Tzu-Chang Yeh

Yao-Yuan Liu

Chad Lin
Edith Cowan University

10.2991/jcis.2006.14
Originally published as: Liu, Y. Y., Lin, K. H. C., Yeh, T. C., & Lin, C. (2006, October). Low-Cost RFID Identification Variation. In *JCIS*. Original article available here

Low-Cost RFID Identification Variation

Koong Lin[1] Tzu-Chang Yeh[2] Yao-Yuan Liu[2] Chad Lin[3]

[1]Computer Center, Tainan National University of The Arts
[2]Dept. of Information Management, Ming Hsin University of Science and Technology
[3]Edith Cowan University, Australia

Abstract

Interests continue to grow in recent years for the adoption of Radio Frequency Identification (RFID) in many different areas including transportation and supply chain management. Those RFID-included objects can be targeted more efficiently by real-time tracking and instant management. However, because of the contact-less type of RFID remote retrieval, the transmission of data in the air is very vulnerable to eavesdropping or appropriation. A primary security concern surrounding RFID technology is the illicit tracking of consumer location and analyzing of their shopping habits or behavior.

This paper proposes a more secure and lightweight RFID variation protection protocol which enhances the security of the transmission of information as well as the consumer privacy protection by using randomized control access and two-way identification. In addition, this protocol also improves the overall performance and lowers the cost of RFID tag without any complicated calculation.

Keywords: RFID; LCID variation; Privacy; Security

1. Introduction

RFID is an automatic identification method, relying on storing and remotely retrieving data using RFID tags. RFID system may consist of several components: RFID tags, RFID readers, edge servers, middleware, and application software. An RFID tag is a small device contain silicon chips and antennas that can be attached to or incorporated into any object. Passive tags require no internal power source, whereas active tags require a power source [3, 8].

Because of the contact-less type of RFID remote retrieval, the transmission of data in the air is very vulnerable to eavesdropping or appropriation. In addition, unique means of identification in each RFID tag such as Electronic Product Code (EPC) [5] allows easy tracking of the movement of persons and goods. Moreover, even if the responses of tags are encrypted, the owner can also be identified and tracked by the fixed encrypted code [6].

It is expected that RFID system will carve a place for itself and become widespread in all areas. It will have a great impact on the way we work and live [12]. However, the excessive use of RFID readers can also turn into closely connected monitoring networks that collect all kinds of information including tracking of the movement of goods as well as identifying and analyzing personal information [1, 9 and 10]. For the long-term growth of RFID system, it is critical that the system can provide a mechanism which will address the issues of personal privacy, security, and identity theft.

2. Related works

There have been some approaches to the security and privacy issues in RFID system. The approaches can be classified into four categories.

Disable tags totally or partially

To protect consumer privacy, checkout clerks would "kill" the tags of purchased goods before they are placed in the hands of consumers; no purchased goods would contain active RFID tags [2, 4 and 10].

But it is difficult to ensure that the kill command was properly executed. In addition, partially disable or rewrite tag can not prevent being tracked as tags respond to a fixed output.

Blocker tags

The RSA Blocker Tag technology uses a jamming system designed to confuse RFID readers and prevent those devices from tracking data on individuals or goods outside certain boundaries [10]. It cannot be used, for example, to circumvent theft-control systems or mount denial-of-service (DoS) attacks – only to protect the privacy of law-abiding consumers.

But this kind of solution, only may achieve in the limited safeguard for consumers. It needs consumer's initial cooperation and voluntary purchase of the equipment. In other words, they do not deal thoroughly with the problems of security and privacy.

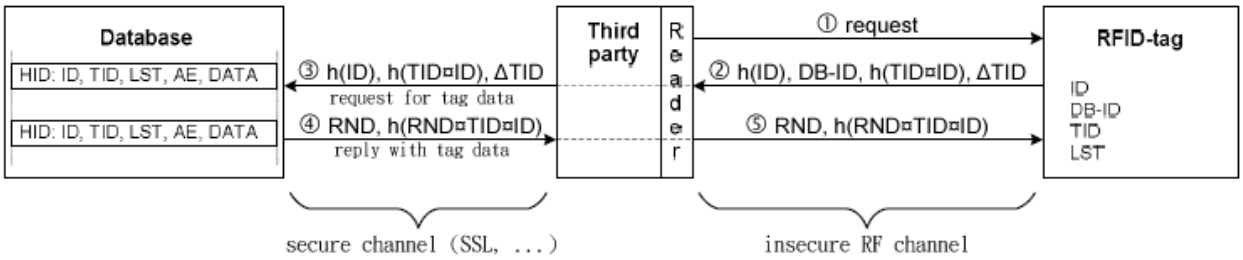

Fig. 1: Dirk's Hash-based ID variation protocol procedure [7]

Hash Lock

With Hash lock, tags only respond to authorized readers. Fixed hash lock stands for an authentication process in which the authentication key is fixed. This scheme offers privacy control at a low cost. All it requires is a hash function and storage for RFID tag's ID. Every reference to RFID tag data was stored in back-end database [4, 11 and 13].

However, it can not prevent being tracked, because tags respond predictably.

Randomized Hash Lock

Randomized Hash Lock is an extension of hash lock type scheme which uses random number function. Instead of fixed metal ID, RFID tag's response changes with each query. This prevents illegal RFID readers to locate the consumer's position through the fixed value of RFID tag [6, 7 and 13].

Among those solutions deploying the Randomized Hash Lock approach, the Hash-based ID variation protocol proposed by Dirk is most popular, as shown in Figure 1.

3. LCID variation

The Randomized Hash Lock approach provides better protection against the security and privacy problems among the four solutions discussed earlier. However, the high complexity of computation and procedures is not suitable for the low-cost RFID implementation. This study proposes a more secure and lightweight RFID variation protection protocol which is the Low-Cost Identification variation (LCID variation) protocol, to resolve this issue.

3.1. Initial Setup

The size of storing the capacity is one of the important factors to influence the RFID tag cost. Therefore, the objective of this study is to design a protection mechanism that reduces the amount of data fields contained in RFID tags and so the cost can be reduced.

The necessary field of LCID variation protocol is defined as follows:

Each RFID tag needs to contain fields for the following entries:

- RFID tag's ID ("ID")
  read only
- RFID reader's ID ("RID")
  read only, optionally writable
- Additional fields for user data or a master key are conceivable but not required at all

Each RFID reader needs to contain fields for the following entries:

- RFID reader's ID ("RID")
  read only
- Random number ("RND")
  read / write

The DB needs to contain a table with the following entries for each record row:

- RFID tag's ID ("ID"), acting as primary index of the table
- A reference to tag data / user data ("DATA")
  read / write

Each RFID reader has an unique reader identification (RID), and each RFID tag stores an authorized RID to measure the target of communication. RID is used to prevent illegal RFID readers collecting data illegally to analyze consumer's shopping habits. RND is a random number to protect all of transmission of data and to prevent replay attack.

When the RFID tag is embedded into the product and shipped, the data in database should be written into the RFID tag containing related product records for further access and queries.

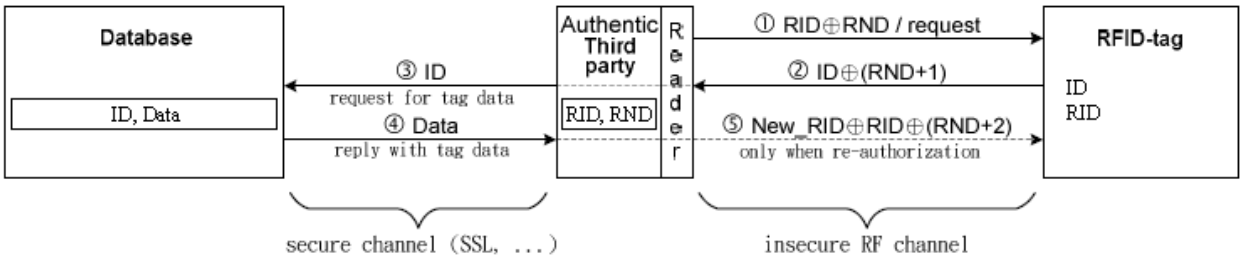

Fig. 2: Low-Cost ID variation protocol procedure

3.2. Normal Operation

There are five steps in the low-cost dynamic RFID security protocol. Figure 2 depicts the brief flow.

1. RFID reader generates a random number RND, and sends a query (RID⊕RND) to RFID tag.
2. RFID tag performs a XOR manipulation on the received (RID⊕RND) and its authorized RID; thus achieves the original RND. And then, it returns the value ID⊕(RND+1) to the RFID reader.
3. RFID reader performs a XOR manipulation on the received ID⊕(RND+1) and its (RND+1); thus obtains the original ID. And then, it uses the ID the query the back-end system.
4. According the above ID, the back-end system accesses the related product information from the database, and returns to RFID reader. In this stage, the ordinary procedure is completed.
5. This step happens only when the RFID reader requests re-authorization. In this situation, RFID reader uses the New_RID (new reader identification) to compute the (New_RID)⊕RID ⊕(RND+2), and sends the value to RFID tag. When RFID tag receives the message, it sequentially performs a XOR manipulation on the received (New_RID) ⊕ RID ⊕ (RND+2), its (RND+2), and RID. The result obtained is the newly authorized New_RID. The RFID tag can overwrite the old RID by the obtained New_RID, and completes the re-authorization procedure.

4. Analysis for LCID variation

In the following, the LCID variation and Hash-based ID variation are compared briefly:

Identification: each RFID tag gets an authorized "RID" which can access the RFID reader data. Thus, RID can protect the data transmitted by RFID tags from being read by unauthorized RFID readers. In addition, fake tags cannot obtain RID, and IDs to compute the RNDs which is used to discriminate a real tag. Therefore, the RFID tag and reader can discriminate each others and achieve the "Two-way identification". On the other hands, the Hash-Based ID variation protocol only provides "One-way identification" for RFID tags; it cannot discriminate the reality of a RFID reader.

Security: The RFID reader randomly generates a RND number at each communication. RND can be used to protect transmitted data, ensure the communication privacy, and avoid replay attacks. On the other hand, Hash-Based ID variation protocol deploys one-way hashing to protect the transmitted data with higher computation complexity and data loading.

Privacy: Employing random numbers makes the data transmitted by RFID tags get a non-fixed value that is unpredictable, and thus can protect the consumer's location from being traced. On the other hand, Hash-Based ID variation changes the RFID tag identification code after each data access.

EPC compatibility: The RFID tag contains a fixed identification number; which is compatible with EPC network. The product related information could be queried via ONS in EPC network. Hash-based ID variation changes the RFID tag identification code after each data access, and thus is not compatible with EPC network that uses single ID number.

Communication performance: This work (LCID variation) simplifies the communication flows and data transmission. There are two types of reading flows in LCID variation protocol: (1) In the ordinary flow, only four times of message passing are needed. (2) In case there is a need to be re-authorized, it takes five times of message passing. In both types, only one single data should be transmitted at each step. Therefore, it retains good performance in the environment where considerable RFID tags access the network simultaneously. On the other side, Hash-based ID variation always takes five times of message passing, and multiple packets of data are sent out in

each message passing. Obviously, this protocol can bring down the overall performance.

Cost: There are two significant cost components for the RFID tag: the computation ability and storage space. These two components are simplified in our security protection mechanism. Because LCID variation deploys only the less-complicated XOR computation, the RFID tag does not need complicated computation capabilities and storage spaces. On the other hand, the RFID tag must handle multiple hashing functions and XOR computation in Hash-based ID variation. In addition, it must store both the old and current record, and thus increases the space demand by two folds.

Table 1 describes the above analysis.

Table 1: Comparative and analysis

		Hash-based ID Variation	*Low-Cost ID Variation*
Data	Identification	One-way	Two-way
	Security	Yes	Yes
	Privacy	Yes	Yes
	EPC compatibility	No	Yes
Performance	Procedure	Complex	Simple
	Calculate	Complex	Simple
	DB record	2 Records	1 Record
	Expand capability	Yes	Better

5. Conclusion

In recent years, the RFID has been widely adopted in many different fields at an increasing rate. Yet, the issues of security and privacy have become the key challenges in promoting the RFID technology. Each of the existing four categories of solutions has its merits and pitfalls. The objective of this research is to propose a secured and lightweight protection protocol to resolve these issues.

This research proposes a low-cost dynamic RFID security protocol, which deploys a randomized protection and two-way identification mechanism. This protocol can provide better protection for data transmission and consumer privacy. In addition, the protocol has an advantage in terms of data transmission performance over other protocols as it does not require encryption technology. Moreover, the protocol lowers the RFID tag costs and is compatible with the existing EPC network. This research demonstrates a new and effective low-cost RFID protocol that can be implemented and introduced to a consumer market that operates in high security environments.

6. References

[1] Alfonsi, Benjamin J., "Privacy Debate Centers on Radio Frequency Identification," *IEEE Security & Privacy*, 2004.

[2] Auto-ID Center, "860Mhz-960Mhz Class I Radio Frequency Identification Tag & Local Communication Interface Specification Proposed Recommendation Version 1.0.0," *Technical Report MIT-AUTOID-TR-007*, 2002.

[3] Bansal, Rajeev, "Microwave Surfing," *IEEE microwave magazine*, 2004.

[4] Bridgelall, Raj, "Enabling Mobile Commerce Through Pervasive Communications with Ubiquitous RF Tags," *IEEE*, 2003.

[5] EPCglobal, At: "http://www.epcglobalinc.org/," Accessed April 10, 2006.

[6] Gao, Xingxin, Zhe Xiang, Hao Wang, Jun Shen, Jian Huang and Song Song, "An Approach to Security and Privacy of RFID System for Supply Chain," *IEEE*, 2004.

[7] Henrici, Dirk and Paul Müller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers," *IEEE*, 2004.

[8] Inoue, Sozo and Hiroto Yasuura, "RFID Privacy Using User-Controllable Uniqueness," *RFID Privacy Workshop@MIT*, 2003.

[9] Inoue, Sozo, S. Konomi, and Hiroto Yasuura, "Privacy in the Digitally Named World with RFID Tags," *Workshop on Socially-Informed Design of Privacy-Enhancing Solutions in Ubiquitous Computing*, 2002.

[10] Juels, Ari, Ronald L Rivest and Michael Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," *CCS'03*, 2003.

[11] Kinosita, Shingo, Fumitaka Hoshino, Tomoyuki Komuro, Akiko Fujimura, and Miyako Ohkubo, "Non-identifiable Anonymous-ID Scheme for RFID Privacy Protection," *Proc. Of CSS'03*, 2003.

[12] Lin, Koong and Huei Leu, "Using AHP Approach to Establish a Decision Analysis Mechanism for Adopting RFID Systems," *Communications of IICM (Institute of Information and Computing Machinery)*, Vol. 8, Num. 4, 2005.

[13] Weis, Stephen A, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," *Proc. of First International Conference on Security in Pervasive Computing*, 2003.