韓國 컴퓨터情報學會 論文誌
第12卷 第4號, 2007. 9.

2007-12-4-2-1

# 유비쿼터스 환경을 위한 RFID 보안 인증 프로토콜

배 우 식*, 최 신 형**, 한 군 희***

# RFID Security Authentication Protocol for the Ubiquitous Environment

Woo-Sik Bae*, Shin-Hyeong Choi**, Kun Hee Han***

## 요 약

RFID 시스템의 전자 Tag, Reader 간의 무선 통신에서, 기존의 해쉬-락 관련 알고리즘은 스푸핑, 재전송, 트래픽 분석 및 위치 추적등 보안상의 취약점이 존재한다. 본 논문에서는 개인정보 보호를 위한 기존의 해쉬-락 관련 알고리즘을 비교, 분석하였으며 이를 보완하기 위하여 실시간과 매 세션마다 리더로부터 수신한 난수를 이용하여 해쉬 함수를 생성하고 인증 프로토콜을 가지는 새로운 해쉬 기반 보안 인증 알고리즘을 제안하였다. 제안한 알고리즘은 RFID 무선 인증 시스템에서 다양한 유용성을 제공할 수 있으며, 기존의 알고리즘에 비해 계산량을 절감할 수 있는 장점이 있다. 또한 추후 예상되는 주변의 수많은 태그 중 필요한 태그만 선별하여 사용하며, 시간 기반으로 불필요 태그의 동작을 종료시켜 서버부담을 줄이는 방법이 될 것으로 기대된다.

## Abstract

On the wireless communication between RFID Tag and Reader, there are some existing problems with weaknesses of security such as spoofing, replay, traffic analysis, position tracking, etc., in the established hash lock related algorithm. This paper has presented the comparison and analysis of the established hash lock related algorithm for privacy and in order to make up for this, also suggested a new security authentication algorithm based on hash which has an authentication protocol and creates hash function by using random numbers received from the reader on real time and every session. The algorithm suggested here can offer a several of usefulness for RFID authentication system and it has an advantage to reduce the amount of calculations compared to established algorithm. It also uses the tags needed among a lot of tags around which are expected later and it is expected to reduce a responsibility of the server by ending unnecessary tags' operation with time based.

▸ Keyword : Radio Frequency IDentification, Hash Lock, Ubiquitous

• 제1저자 : 배우식
• 접수일 : 2007. 7.9, 심사일 : 2007. 8.4, 심사완료일 : 2007. 8.14
* 충북대학교 컴퓨터교육과 박사과정 ** 강원대학교 제어계측공학과 조교수
*** 백석대학교 정보통신학부 교수

# Ⅰ. Introduction

RFID(Radio Frequency IDentification) is being expected to use all fields of personal and industrial area with improvement of using convenience and there have been being a lot of researches progressing home and internationally. However, RFID technology has a lot of disadvantages such as Eavesdropping, Traffic Analysis, Denial of Service Attack, Message Loss, Tracking Attack, and Spoofing Attack because it reads information which is built in inside microchip by using radio frequency, so it could cause problems of security and privacy. Therefore, there should be a solution of security in order to activate RFID system.

This paper has presented an authentication protocol in order to solve the problem of privacy of RFID. It can protect privacy of user safer and more effective through analyzing problems that cannot be solved by established schemes like Hash Lock Scheme[1,2], Randomized Hash Lock Scheme[3,4], Hash Chain Scheme, Hash based ID variation[5,6] and so on. This protocol is safe from the attack by attacker because of using hash functions, random numbers and real time, and it suggests a method that reduces load problems which are caused in the system by lots of tags unneeded which can be expected later by using real time. It is also available to apply distributed database and suggests a mechanism which offers various securities and applicability.

# Ⅱ. RFID System

RFID system is generally consisted of tag, reader, and back end database.

## 2.1 Tag

A tag is consisted of microchip and antennae, and is a device to send/receive its own information from itself to reader by request of the reader or the situation because it has been stored identification code and information. There are two types of tags now.

Active tag: it sends and receives data by using installed battery inside tag. It is possible to remote data sending and receiving, but it is more expensive, bigger than passive tag and it stops working when the battery runs out.

Passive tag: it gets power by using induced current by electromagnetic wave received from the reader. It can only be available within short distance compared to active tag, but is cheaper, smaller and no limit for life.

## 2.2 Reader

A reader is a device to send a signal to a tag or transmits data received from the tag to the server and has main functions such as activation and deactivation, supplying power to passive tag, encoding data sent to tag, decoding data received from tag, and so on.

## 2.3 Back end Database

It is also generally called host computer and stores information collected by reader and operates complex computing instead of reader of tag that have low computing ability. Figure 1 shows a general model of RFID authentication protocol.

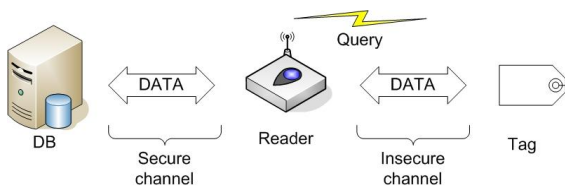


Fig 1. Model of RFID Authentication Protocol
그림 1. RFID 인증 프로토콜 모델

## III. Related Work

### 3.1 Hash Lock Scheme

Hash Lock[1,2,3] protocol is supposed to be shared a Key in the way suggested by MIT by consideration of low cost tag with database safely in advance. The process of authentication is as followed.

1) Locking process of Hash Lock

① Reader R selects a key randomly and computes hash(key) by metaID value.
② R records metaID on tag T.
③ T goes into locked state.
④ R stores (metaID, key).

2) Unlocking process of Hash Lock[Figure 2]

① Reader R asks T's metaID of tag T.
② R investigates (metaID, key) in the database.
③ R transmits key to T.
④ If there is an identification between hash(key) and metaID, T will be out of locked state.

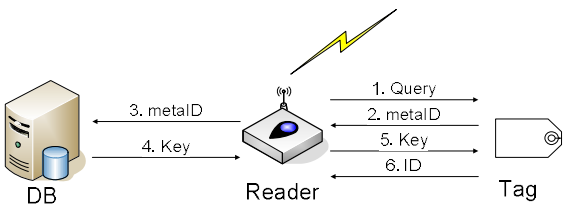


Fig 2. Hash Lock Scheme
그림 2. 해쉬-락 기법

MetaID, identifying value of tag, is fixed in this method, so output data are the same. It makes to check if data have been transmitted from the right tag. And communication channel between reader and tag can be eavesdropped, so that a malicious attacker gets an authentication by producing metaID with computing hash after achieving key. Also the third part can get an authentication by replaying fixed metaID, and there will be possible to have spoofing attack or tracking users because metaID is used as like an identifier.

### 3.2 Randomized Hash Lock Scheme

It is to prevent possible tracking users in Hash Lock scheme. The tag does not give answers which are expected to unauthenticated users, but it should still be identified by legal reader. For this scheme, there should be working directed hash function and random number generator in the tag. Figure3 shows the protocol that makes the tag unlocked state.

① Reader R sends an inquiry to tag T.
② T generates random numbers randomly and computes the value of hash(ID || R).
③ T transmits (R, hash(ID || R)) to R.
④ R computes hash(IDi || R) for the all known value of IDi.
⑤ If it finds the value of IDi which satisfies the condition hash(IDi || R) == hash(ID || R), R transmits IDi to T.
⑥ If IDi identifies ID, T will be out of unlocked state.

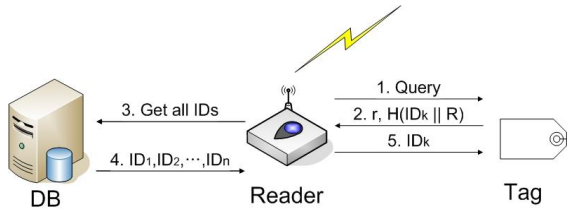


Fig 3. Randomized Hash Lock Scheme
그림 3. 확장된 해쉬-락 기법

This method is strong in spoofing attack because its information from tag to reader changes every session by using random numbers, but the value of IDk is exposed and it makes tracking location possible. And in the case that reader attacker retransmits r,H(IDk || r) after eavesdropping it, it will pretend as a right tag, so it is weak from replay attack.

### 3.3 Hash Chain Scheme

Hash chain scheme[6] which uses two different hash functions is safe from location tracking attack by transmitting different Ai value in each session. However, in the worst case, database operates H ad G I times for all Si. And also if there are wrong answers received, it is possible for the database to operates hash ∞ times for the all specific ID. Figure4 shows the operating process of hash chain scheme.

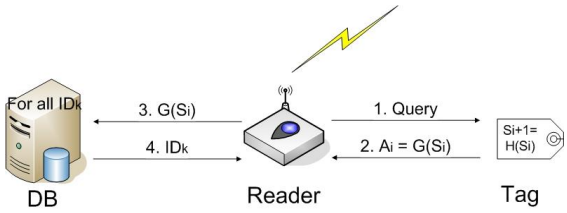


Fig 4. Hash Chain Scheme
그림 4. 해쉬 체인 기법

### 3.4 The Scheme of Hash Based ID Variation

Hash based ID variation scheme[7,8] is the scheme which changes ID, authentication information of tag, in each session similar to hash chain scheme. ID of tag is renewal by random number R in each session like in Figure5, so it is safe from replay attack. However, if an attacker as pretending to be the right reader achieves H(ID), H(I ⊕ID) and Δi, and uses this information as answers to the questions of reader before the right tag operates the next authentication session, the attacker can be recognized as the right tag.

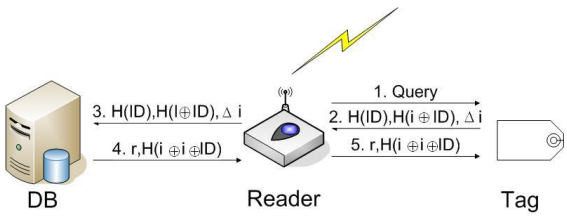


Fig 5. Hash Based ID Variation Scheme
그림 5. 해쉬 기반 ID 변형 기법

## IV. Protocol Proposed

### 4.1 Structure

This protocol proposed transmits both random number and real time when reader asks tag first, tag responds with the value from hash by ID and real time that the tag itself has. By doing that, it should be safe from replay attack and spoofing attack which are meant to be problems in established protocols.

Back end database stores data related to id of tag in the protocol proposed and it authenticates tag by computing only 2 times of hash function.

Reader does not need any computing apart from sending random number and real time data, temporary memory is needed to store information being sent between back end and database.

Parameters used in the protocol proposed are as followed, and Figure6 presents the basic structure of the protocol proposed.

#### 4.1.1 Assumption items

For the protocol proposed, there is an assumption for the followings.

Tag operates activated installed battery.

Tag and database operate computing of hash function.

Tag and database share ID of tag in advance.

Reader has a random number generating function.

Back end database and reader communicate on the safe communication channel.

〔Parameters〕

Query: inquiry, and ask for respond of tag

ID: secret authentication information of tag its own

H( ): working direct hash function

Rt: transmitting DB time(㎲) from reader to tag

Rr: random number that is generated and transmitted by reader to tag

Tt: time(㎲) to store in tag
Rtn: time(㎲) to record on tag
Dn: order transmitted from database to tag
||: concatenate function

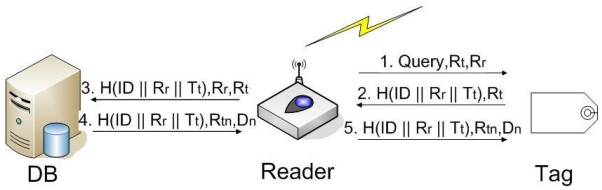


Fig 6. Structure of Protocol Proposed
그림 6. 제안 프로토콜의 구조

## 4.2 Process of Authentication

◎ Step1: reader broadcasts Query with Rt and Rr to tags.

Reader → Tag : Query, Rt,Rr

◎ Step2: after tag concatenates ID and Tt which tag has with Rr, it hashes and transmits it as a respond on Query with Rt to reader.

Tag → Reader : H(ID || Rr || Tt), Rt

◎ Step3: reader transmits Rr, H(ID || Rr || Tt) received from tag, and Rt to back end database.

Reader → Back end Database : H(ID || Rr || Tt),Rr, Rt

◎ Step4: it authenticates tag by comparing the value hashed from concatenating ID stored in back end database, Rt, Rr to H(ID || Rr || Tt),Rr, Rt received from reader.

Back end Database → Reader : calculated H(ID || Rr || Tt),Rr, Rt = received H(ID || Rr || Tt),Rr, Rt. If the authentication is successful, H(ID || Rr || Tt),Rtn, Dn are transmitted to reader.

If it is necessary, Kill command will be sent by period limit tags or unnecessary tags that are input in database.

◎ Step5: reader transmits H(ID || Rr || Tt),Rtn, Dn that are received from back end database to tag.

Reader → Tag : H(ID || Rr || Tt),Rtn, Dn

Tag authenticates back end database by comparing the value hashed from concatenating ID of its own and Rt, Tt which are generated from the authenticating session to H(ID || Rr || Tt),Rtn received from reader. And it records Rtn and operates Dn order if needed, and ends the authenticating session successfully.

## 4.3 Safety of Protocol Proposed

### 4.3.1 Safety on Spoofing Attack

If an attacker pretends to be the right reader and transmits random number Rr and real time Rt with Query to the tag, she/he will be able to achieve H(ID || Rr || Tt) and Rt from the tag. However, when she/he puts this information into malicious tag and sends it to reader as a respond, the information will be out of date already. So, the information with wrong state will be sent with H(ID || Rr || Tt), Rt to back end database. Therefore, she/he cannot get an authentication and there is no way to have spoofing attack.

### 4.3.2 Safety on Replay Attack

Rt and Rr which are sent with Query by the right reader are changed in each session, so also H(ID || Rr || Tt) and Rt which are respond of tag are changed in each session. Therefore, the attacker cannot use H(ID || Rr || Tt) and Rt which are achieved by eavesdropping as respond on next session, so, it is safe on replay attack. In this protocol, attackers would not know tag ID because of random numbering, real time, and hashing, so it is originally impossible to generate right respond H(ID

|| Rr || Tt) and Rt against to Rt and Rr which are changed in every session.

#### 4.3.4 Safety on Interference of Information Transmission

〔Table 1〕 Safety of the Protocol Proposed
표 1. 제안프로토콜의 안전성

| | Hash-lock scheme | Randomized hash-lock scheme | Hash-chain scheme | Hash-based ID variation scheme | Protocol proposed |
|---|---|---|---|---|---|
| Spoofing attack | weak | weak | weak | weak | safe |
| Replay attack | weak | weak | weak | safe | safe |
| Traffic analysis attack | weak | weak | safe | safe | safe |
| Location information exposure | weak | weak | safe | safe | safe |
| Information transmission interfering attack | safe | safe | safe | safe | safe |

#### 4.3.3 Safety on Traffic Analysis and Location Tracking

Even though the attacker pretending the right reader transmits fixed Rt and Rr to tag continuously, in the next session, real time is changed and tag transmits random number Tt by using unknown hashed ID which the attacker would not know and responds H(ID || Rr || Tt) and Rt that are changed in every session. That is why, the attacker cannot discriminate it those different responds are from the same tag. Therefore, the attacker pretending to be the right reader is not able to analyze traffic and to track the location of tag.

The protocol proposed offers mutual authentication so that it detects interfering attack of information transmission. Because of no changing authentication ID information of tag, there is no information loss of database which could be happened in the hash based ID variation protocol that changes ID in every session. Table1 is the comparison of safety to the established protocol.

### 4.4 Efficiency of Protocol Proposed

In the protocol proposed in this paper, a tag only stores hash function computing and real time data, so it can be implemented in low cost tags and all tags with developing technology in the future. It

〔Table 2〕 Efficiency of Protocol Proposed
표 2. 제안프로토콜의 효율성

| | Hash-Lock scheme | Randomized Hash-Lock scheme | Hash-Chain scheme | Hash-Based ID variation scheme | Protocol Proposed |
|---|---|---|---|---|---|
| Authentication | Full-duplex | Full-duplex | Half-duplex | Full-duplex | Full-duplex |
| Tag Computing amount | Hash 1 time | Hash 1 time Random 2 times | Hash 2 times | Hash 3 times | Hash once (writing time) |
| Reader Computing amount | - | N times | - | - | Random 1 time |
| Database Computing amount | - | - | n(1+i) times | Hash 3times Random 1 time | Hash 1 time |

also operates only two times of hash function computing during authentication session like [Table 2], so there is not much computing load and it is available to apply to ubiquitous environment which distributed database exists in compared to hash based ID variation scheme that assumes only a database which stores IDs transformed.

This protocol applies random numbers and real time, but other complex computing. Also it does not require a lot of database computing, so it is possible to consist of low cost database, even though there are many tags around. That is why it has high efficiency.

## Ⅴ. Conclusions

The protocol proposed generates a new hash function from the random number and real time in order to transmit different respond in every session. By doing that, it is very safe from replay attack of attacker, spoofing attack, location tracking, and so on. Therefore, we could say that it has high safety and efficiency. In the future, real time data should be recorded continuously on tags even new technology has been applied operation. It will use the tags needed among the tags around and ends unnecessary tags operation. That is expected to be a method that reduces a load of server and manages trash of unnecessary tags.

## References


[1] S. Weis et al., "Security and Privacy Aspects of Low cost Radio Frequency Identification Systems," Security and Pervasive Computing 2003, LNCS2802, pp. 201 202.

[2] S. A. Weis, "Security an Privacy in Radio Frequency Identification Devices" MS Thesis, MIT.May, 2003.

[3] Sanjay E.Sarma, Stephen A. Weis and Daiel W.Engels, "Radio Frequency Identification Systems", In Proceeding of CHES '02, pp. 454 469. Springer Verlag, 2002. LNCS NO.2523.

[4] Weis, S. et al. Security and Privacy Aspects of Low Cost Radio Frequency Identification Systems, First International Conference on Security in Pervasive Computing (SPC), 2003.

[5] Gildas Avoine and Philippe Oechslin "RFID Traceability : A Multilayer Problem", Financial Cryptography, March 2005.

[6] D. Henrici, and P. Muller. "Hash based Enhancement of Location Privacy for Radio Frequency Identification Devices using Varying Identifiers", Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW'04), pp.149 153, IEEE, 2004.


## 저 자 소 개


**배우식**

- 1997년 3월 ~ 현재 : 아주자동차대학 전산소
  2006년 8월 : 백석대학교 정보기술대학원 (공학석사)
- 2007년 : 충북대학교 컴퓨터교육과 (박사과정)

〈관심분야〉 유비쿼터스 DB보안, 컴퓨터 네트워크, 암호 프로토콜/알고리즘

**최신형**

1993년 울산대학교 전자계산학과(학사)
1995년 경남대학교 전자계산학과(석사)
2002년 경남대학교 컴퓨터공학과(박사)
1995년 해군사관학교 전산과학과 전임강사
2003년~현재 강원대학교 제어계측공학과 조교수

〈관심분야〉 임베디드 시스템, 선센서네트워크, 분산시스템 보안, 테스트 및 품질평가

**한군희**

2000년 충북대학교 컴퓨터공학과(공학박사)
2001년~현재 백석대학교 정보통신학부 교수

〈관심분야〉 멀티미디어, 정보보호