해시 함수를 이용한 효율적인 RFID 인증

신효영* · 정계동**

Effective RFID Authentication Using Hash Function

Hyo-Young, Shin* · Gye-Dong Jung**

요 약

최근 RFID 시스템은 유통, 의료, 군사 등 다양한 영역에서 활용하는 기술로 등장하고 있다. RFID 시스템을 여러 가지 응용 서비스에 적용하려면 개인정보를 보호하기 위한 기술이 개발되어야한다. 본 논문에서는 해시 함수를 이용하여 RFID 태그와 데이터베이스간의 상호 인증을 효율적으로 수행할 수 있는 프로토콜을 제안하였다. 제안한 프로토콜은 상호 인증, 익명성, 비밀성, 무결성, 재전송 공격, 위치 추적 등 여러 가지 보안 요구 사항을 만족시키면서, 데이터베이스에서의 해시 연산 횟수를 줄여 전체 인증 시간을 줄일 수 있다.

ABSTRACT

Recently RFID system is used in various fields such as distribution industry, medical industry and military service. The technology for protecting individual privacy is necessary to adapt RFID system in several applications. This paper proposes an authentication protocol which conducts mutual authentication between back-end database and tag using hash function. The proposed protocol satisfies various RFID security requirements : mutual authentication, anonymity, confidentiality, integrity, replay attack, location trace. This protocol reduces the time for authentication minimizing the number of hash operation in back-end database.

키워드

RFID, 인증, 해시 함수, 정보보호

Key word

RFID, Authentication, Hash function, Security

* 경복대학 인터넷정보과 (hyshin@kyungbok.ac.kr)
** 광운대학교 교양학부

접수일자 : 2010. 01. 20
심사완료일자 : 2010. 02. 23

Ⅰ. 서 론

RFID 시스템은 태그, 리더, 데이터베이스로 구성된다. 태그와 리더 사이는 무선으로 통신하며, 리더와 데이터베이스 사이는 유선 혹은 무선으로 통신한다. 리더와 태그사이의 구간은 보안에 매우 취약하여 보호되지 않은 태그가 부착된 물품은 쉽게 모니터링 되고 추적당할 수 있는 위험이 있다.[1,2]

RFID 시스템을 여러 가지 응용 서비스에 적용하려면 개인정보를 보호하기 위한 기술이 개발되어야한다. 현재까지 사용자 정보를 보호하기 위해 개발된 방법에는 Kill 명령어와 같은 물리적인 방법[2], 해시 함수를 기초로 한 방법[3,4,5], XOR 기반의 방법[7], 암호화를 사용하는 방법[8,9]들이 있다.

해시 함수의 일방향성을 이용하여 상호 인증을 제공하기 위하여 여러 가지 프로토콜이 개발되었다. 기존 프로토콜들은 대부분 태그에서의 해시 연산은 가급적 최소화 하였으나 데이터베이스에서 태그 ID를 검색하기 위해 많은 해시 연산을 필요로 하는 단점을 가지고 있다.

본 논문에서는 해시 함수를 이용하여 RFID 태그와 데이터베이스간의 상호 인증을 효율적으로 수행할 수 있는 프로토콜을 제안하였다. 제안한 프로토콜은 상호 인증, 익명성, 비밀성, 무결성, 재전송 공격, 위치 추적 등 여러 가지 보안 요구 사항을 만족시키면서, 데이터베이스에서의 해시연산 횟수를 줄여 전체 인증 시간을 줄일 수 있다.

Ⅱ. 연구 배경

RFID 시스템의 구조와 보안 요구사항, 기존에 수행된 관련 연구들은 다음과 같다.

2.1 RFID의 보안 요구 사항

RFID 시스템이 요구하는 보안 요구 사항들은 다음과 같다.

(1) 인증(authentication)

통신하는 객체들 간의 신원을 검증할 수 있어야 한다. RFID 시스템의 적용 사례에 따라 데이터베이스, 리더, 태그간의 상호 인증이 제공되어야 한다.

(2)익명성(anonymity)

태그로부터 얻은 정보를 가지고 어떠한 태그로부터 전송된 정보인지를 분석할 수 없어야 한다.

(3) 비밀성(confidentiality)

태그와 리더간의 통신시 전송중인 데이터가 불법적으로 도청될 수 있다. 공격자가 리더와 태그간의 통신을 도청하더라도 이 정보를 이용하여 태그에 저장된 비밀정보를 알아낼 수 없어야 한다.

(4) 무결성(integrity)

RFID 시스템의 통신 내용이 불법적인 제 3자에 의해 수정되거나 위조될 수 있다. 이를 방지하기 위하여 암호학적 방법이 제공되어야 한다.

(5) 재전송 공격(replay attack)

공격자가 이전에 일어난 통신 내용을 알고 있다 하더라도 이를 이용하여 현재 세션에서 사용될 정보를 생성해 내는 것이 불가능하여야 한다.

(6) 위치 추적(location tracking attack)

공격자가 태그와 리더사이의 통신 내용을 분석하여 태그나 태그 소유자의 위치 정보를 알아낼 수 없어야 한다.

2.2 관련 연구

현재까지 RFID 시스템에서 사용자 정보보호를 위해 여러 가지 방법들이 제안되었다. 해시 기반의 인증 방법은 해시 함수의 일방향성을 이용하는 것으로 다음과 같은 방법들이 있다.

(1) 해시 락(hash lock) 인증 프로토콜

이 프로토콜은 태그의 실제 ID를 숨기기 위하여 <그림 1>과 같이 태그에서 랜덤하게 선택된 키의 해시 값인 $metaID = h(key)$를 사용한다. 그러나 이 방법은 고정된 $metaID$를 사용하므로 태그의 위치 추적이 가능하고 재전송 공격에 취약한 단점이 있다.

(2) 랜덤 해시 락 인증 프로토콜

해시 락 기법의 태그 위치 추적 문제를 해결하기 위하여 <그림 2>와 같이 제안한 방법이다[4]. 난수 R을 이용하여 태그의 응답 값을 $h(ID \| R)$로 랜덤화 한다. 그러

나 이 방법은 여전히 마지막 단계에서 ID값을 안전하지 않은 채널을 통해 전송하기 때문에 위치 추적 문제와 재전송 공격 문제를 해결하지 못하였다.

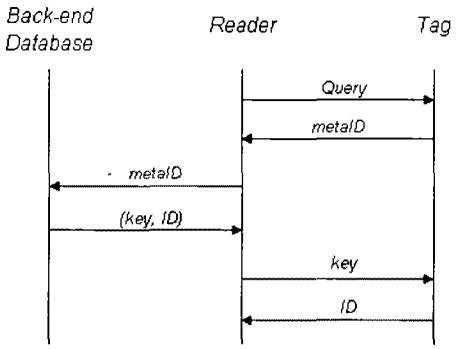

그림 1. 해시 락 인증 프로토콜
Fig. 1 Hash lock authentication protocol

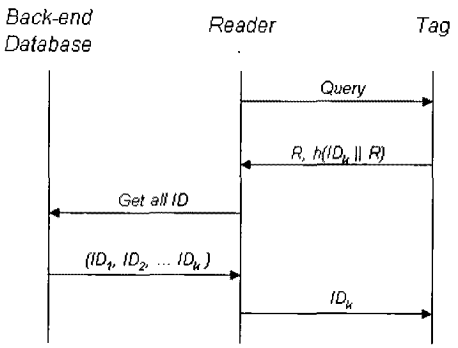

그림 2. 랜덤 해시 락 인증 프로토콜
Fig. 2 Random hash lock authentication protocol

(3) 해시 체인 인증 프로토콜

Ohkubo 등은 <그림 3>과 같이 위치 추적 공격이나 전방향 안전성에 강한 해시 체인 인증 기법을 제안하였다[5]. 해시 체인 인증 프로토콜은 두 개의 해시 함수 H와 G를 사용하여 해시 체인을 구성한다. 그러나 이 방식은 서버가 ID를 검색하는데 많은 시간이 소비되며, 태그로부터 잘못된 응답이 오면 데이터베이스는 무한대의 해시 연산을 수행할 수도 있는 단점이 있다

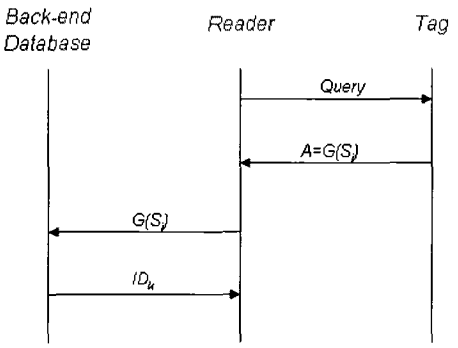

그림 3. 해시 체인 인증 프로토콜
Fig. 3 Hash chain authentication protocol

이 밖에 Kim-Ryoo는 기존의 RFID 인증 프로토콜 분석을 통하여 해시 함수를 이용한 새로운 RFID 상호 인증 프로토콜을 제안하였다[10]. Ahn, Bu 등은 스푸핑 공격에 안전하고, 데이터베이스와 태그가 상호 인증 후 서로 공유된 비밀 값을 안전하게 갱신하게 하여 전방향 안전성을 보장하는 인증 프로토콜을 제안하였다[11].

기존에 제안된 프로토콜은 대부분 태그에서의 연산 횟수를 줄이기 위해 노력하였다. 이는 저가의 태그가 제공하는 낮은 계산 능력 환경을 극복하려는 시도이나 상대적으로 데이터베이스에서의 계산량은 증가하는 단점이 있다. 랜덤 해시 락 프로토콜은 데이터베이스에서 최대 n번의 해시 연산을 수행하고, Kim-Ryoo 프로토콜은 데이터베이스에서 최대 $n+3$번의 해시 연산을 수행하며, Ahn-Bu 등의 프로토콜은 데이터베이스에서 최대 $2n+2$번의 해시 연산을 수행한다.

태그수가 증가하면 데이터베이스에서의 인증에 소요되는 시간 또한 증가하여 전체 시스템에 부하를 주게 된다. 최근 데이터베이스에서의 연산을 줄이고 태그 검색 시간을 줄이기 위해 Bloom filter를 사용하거나 사전에 해시 값을 계산하여 저장한 후 인증과정에서 사용하는 연구가 시도 되었다[12].

Ⅲ. 제안 프로토콜

기존 연구에서는 데이터베이스에서 태그를 검색하기위해 해시 연산을 수행하여 일치하는 값을 찾기 위해 해시 연산의 실행 횟수가 태그 수에 비례하여 증가한다.

본 장에서는 인증 과정에서 데이터베이스에서 태그를 검색하면서 소요되는 해시 연산의 실행 횟수를 줄이는 인증 프로토콜을 제안한다.

3.1 용어 정의

제안 프로토콜에서 사용하는 용어들을 다음과 같이 정의한다.

- $Query$: 태그의 응답을 요청하는 리더의 질의어
- ID : 태그에 할당된 고유의 식별자
- $M_1 \| M_2$: 메시지(M_1, M_2)의 연결
- $h(\,)$: 일방향 해시 함수
- N_r : 리더가 첫 번째 생성한 난수
- N_t : 태그가 생성한 난수
- $\oplus$: 배타적 논리합 연산
- T : $h(ID \| N_r \| N_t)$
- D : $D = h(ID \oplus N_t)$
- KV : $ID \oplus K$

3.2 초기화 단계

제안한 프로토콜을 실행하기 전에 데이터베이스, 리더, 태그에서 초기화해야할 사항들은 다음과 같다.

① 모든 태그에 자신의 식별자로 비밀정보인 ID 값을 저장한다.
② 모든 태그에 비밀 키 정보인 K 값을 저장한다.
③ 리더와 태그에는 의사난수를 생성할 수 있는 난수 생성기를 설치한다.
④ 데이터베이스에는 모든 태그의 식별자인 ID 값과 비밀 값 $KV = ID \oplus K$를 저장한다.

3.3 제안 프로토콜 실행 절차

단계 1. 리더 → 태그 : $Query$, N_r

리더는 난수 N_r을 생성하여 질의어와 함께 태그로 전송한다. 난수 N_r은 태그를 인증하기 위하여 사용된다.

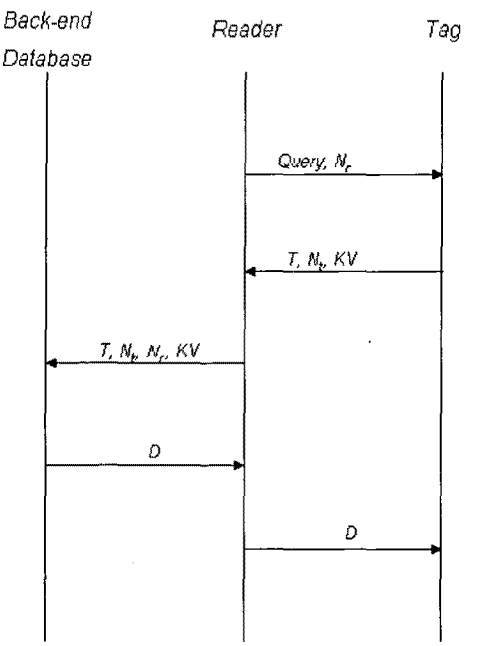

그림 4. 제안 프로토콜 구조
Fig. 4 Structure of proposed protocol

단계 2. 태그 → 리더 : T, N_t, KV

태크는 질의어를 수신한 후 난수 N_t를 생성하고, $T = h(ID \| N_r \| N_t)$을 계산한다.

$KV = ID \oplus K$를 계산한 후 T, N_t, KV를 리더로 전송한다.

단계 3. 리더 → 데이터베이스 : T, N_t, N_r, KV

리더는 태그로부터 수신한 T, N_t, KV를 이전에 생성하였던 난수 N_r과 함께 데이터베이스로 전송한다.

단계 4. 데이터베이스 → 리더 : D

데이터베이스는 저장된 KV 값 중에서 리더로부터 수신한 KV값과 일치하는 KV를 찾는다. 검색한 KV에 K를 XOR 하여 ID값을 추출한다.($ID = KV \oplus K$) $T' = h(ID \| N_r \| N_t)$를 새로 계산하여 $T' = T$인가를 비교한다. 두 값이 같은 경우 데이터베이스는 리더와 태그를 인증한다. $D = h(ID \oplus N_t)$를 계산한 후 리더로 전송한다. 데이터베이스는 $K' = K \oplus D$를 계산하여 비밀

키 K를 새 키 K'로 갱신한다. KV값도 갱신된 비밀 키 K'를 이용하여 재계산하여 갱신한다.($KV' = ID \oplus K$) 이 과정을 알고리즘으로 기술하면 다음과 같다.

```
KV1 = KV from reader
KV2 = KV in database
For each i in KVi
  If KV1 = KV2 Then
    ID = KV1 ⊕ K
  Else
    Send Error Message
      exit
Next i
T' = h(ID ‖ Nr ‖ Nt)
If T = T' Then
  D = h(ID ‖ Nt)
  K' = K ⊕ D
  KV' = ID ⊕ K
  Send D To Reader
Else
  Send Error Message
```

단계 5. 리더 → 태그 : D

리더는 데이터베이스로부터 수신한 D 값을 태그로 전송한다.

단계 6. 태그

태그는 $D' = h(ID \| N_t)$를 계산한 후 $D' = D$인가를 비교한다. 두 값이 일치하면 태그는 데이터베이스와 리더를 인증한다. 태그는 $K' = K \oplus D$를 새로운 비밀 키로 갱신한다.

Ⅳ. 안전성 및 효율성 평가

제안한 프로토콜의 안전성을 RFID 시스템의 보안 요구사항에 따라 분석하고 기존 프로토콜과 비교한 효율성은 다음과 같다.

4.1 안전성

(1) 인증(authentication)

제안한 프로토콜은 데이터베이스에서 리더와 태그를 인증하고, 태그에서 리더와 데이터베이스를 인증하는 기능을 제공한다.

제안 프로토콜의 단계 4에서 데이터베이스는 $T' = h(ID \| N_r \| N_t)$를 계산하여 태그가 전송한 해시 값 $T = h(ID \| N_r \| N_t)$와 비교한다. 비교 결과 T와 T'의 값이 같으면 데이터베이스가 리더와 태그를 인증한다. 단계 6에서 태그는 자신의 ID와 N_t로부터 D'를 계산한다. 태그는 D'와 D를 비교하여 리더와 데이터베이스를 인증함으로써 상호인증을 수행한다.

(2) 익명성(anonymity)

제안 방식은 해시 함수를 통하여 태그의 ID를 노출하지 않게 한다.

단계 2의 $T = h(ID \| N_r \| N_t)$, 단계 5의 $D = h(ID \oplus N_t)$ 값 모두 ID의 노출을 방지하고 해시 값을 사용함으로써 태그의 익명성을 확보할 수 있다. KV 또한 ID와 비밀 키 K를 XOR하여 전송함으로써 ID의 노출을 방지한다.

(3) 비밀성(confidentiality)

제안 프로토콜은 제 3자에 의해 N_r, N_t, KV 등이 도청될 수 있다. 그러나 태그와 리더의 ID와 비밀 키 K는 외부로 노출되지 않는 비밀정보로 보관된다. 태그와 리더사이에 통신할 경우 ID는 해시 함수로 처리되어 암호키를 알지 못하면 역으로 이 값을 알아낼 수 없다. KV 또한 비밀 키 K로 XOR 하여 ID 값이 노출되지 않는다. 도청한 N_r, N_t, KV값으로부터도 ID 값을 유추할 수 없으므로 제안프로토콜은 비밀성을 제공한다.

(4) 무결성(integrity)

제안 프로토콜은 구성 요소간 통신시 제3자에 의한 데이터 변조가 일어날 때 이를 발견할 수 있다. 데이터베이스와 리더는 자신이 저장한 ID를 이용해 새로운 해시 값을 계산하여, 이를 수신한 해시 값과 비교한다. 전송도중 데이터에 변조가 일어나면 이를 발견하여 데이터의 재전송을 요구하거나 인증을 거부하게 되므로 제안 프로토콜은 무결성을 제공한다.

(5) 재전송 공격(replay attack)

제안 프로토콜은 인증 요구가 발생할 때 마다 리더에서 새로운 난수 N_r과 N_t를 생성하여 사용한다. 공격자가 이전 난수를 도청하여 사용하면 해시 값을 계산하여 비교하는 과정에서 이를 발견할 수 있다. 따라서 제안 프로토콜은 이전 값을 도청하여 재사용하는 공격으로부터 안전하다.

(6) 위치 추적(location tracking attack)

제안 프로토콜은 인증이 시도될 때 마다 태그와 리더간에 주고받는 메시지의 내용은 항상 다르다. 특정 태그가 전송하는 메시지 값과, 다른 태그들이 전송하는 메시지 값들이 다르므로 공격자가 전송하는 내용을 바탕으로 특정 태그를 구분하기 어렵다.

4.2 효율성

RFID 시스템은 데이터베이스, 리더, 태그로 구성된다. 리더는 먼저 태그에 질의를 하고 태그는 이에 대한 응답을 리더로 보낸다. 리더는 데이터베이스로 태그의 응답을 전송한다. 데이터베이스는 사전에 저장한 태그 *ID*를 이용한 계산 값과 태그의 응답 값과 비교하여 일치하는지를 판단하여 태그를 인증한다. 데이터베이스에 등록되어 있는 태그의 수가 많을 경우 데이터베이스에 저장된 태그 정보와 일일이 비교하는 계산량이 많아져 인증에 소요되는 시간이 길어진다.

제안된 프로토콜은 *KV*값을 미리 계산하여 데이터베이스에 전송하고 태그로부터 수신한 *KV*값을 비교한다. 이는 기존의 연구에서 사용하던 데이터베이스에 저장된 태그의 *ID*값마다 해시 값을 계산하여 태그로부터 수신한 해시 값과 비교하는 방식보다 인증 시간을 단축시킨다. <표 1>은 제안 프로토콜과 기존 프로토콜의 연산 효율성을 비교한 것이다.

표 1. 제안 프로토콜의 효율성 비교
Table 1 Effectiveness of proposed protocol

프로토콜 / 연산	RHAP		Ahn-Bu [11]		제안 프로토콜	
	태그	DB	태그	DB	태그	DB
해시 연산량	1	n	3	2n+2	3	2
XOR 연산량	0	0	0	0	2	2
난수 생성수	1	0	1	0	1	0

V. 결 론

RFID 시스템 사용의 증가와 함께 RFID 시스템이 가지고 있는 보안 취약점을 해결하기 위한 기술 개발 또한 요구되고 있다.

본 논문에서는 해시 함수를 이용하여 태그와 데이터베이스가 상호 인증할 수 있는 프로토콜을 제안하였다. 제안 프로토콜은 RFID 시스템에서 요구하는 보안 요구사항인 상호 인증, 익명성, 비밀성, 무결성, 재전송 공격, 위치 추적 등의 안전성을 만족한다. 제안 프로토콜은 기존의 해시 함수를 이용한 인증 프로토콜의 단점인 데이터베이스에서의 과도한 해시 연산 횟수를 줄였다. 기존 프로토콜은 태그 수의 증가에 따라 데이터베이스에서의 해시 연산횟수가 증가하여 인증시간이 길어지는 단점이 있었으나, 제안 프로토콜은 데이터베이스의 해시 연산횟수를 태그 수에 관계없이 3회로 일정하여 태그 수가 증가하여도 데이터베이스의 성능에 영향을 미치지 않는 장점을 갖는다.

태그에서의 해시 연산 횟수도 기존 프로토콜보다 증가하지 않았으나 키 값 관리를 위해 XOR 연산이 2회 요구된다. 이는 전체 시스템 효율에 큰 영향을 미치지 않을 것으로 예상되며, 태그수가 많이 소요되는 대용량 RFID 시스템에 적용할 수 있을 것으로 기대한다.

참고문헌

[1] R. Chandramouli, T. Grance, R. Kuhn, "Security Standards for the RFID Market ", IEEE Security & Privacy, Nov./Dec. 2005.

[2] S. L. Garfinkel, A. Juels and R. Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions", IEEE Security and Privacy, vol.3, pp.34-43, May/June 2005.

[3] S. Weis, "Radio-frequency identification security and privacy", Master's thesis, M.I.T. 2003.

[4] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification System", Security in Pervasive Computing 2003, LNCS 2802, pp. 201-212, 2004.

[5] M. Ohkubo, K. Suzuki and S. Kinoshita, "Hash-Chain Based Forward Secure Privacy Protection Scheme for Low-Cost RFID", Proceedings of the SCIS '04, pp.719-724, Sep. 2004.

[6] A. Juels, "Minimalist cryptography for low-cost RFID tags", In 4th International Conference on Security in Communication Networjs - SCN 2004, Vol. 3352, LNCS pp. 149-164.

[7] S. Karthikeyan, M. Nesterenko, "RFID Security without extensive cryptography", Proc. of 3rd workshop on Security of AdHoc and Sensor Networks, 2005, pp. 63-67.

[8] Ari Juels, Ravikanth Pappu, "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes", LNCS 2742, pp.103-121, 2003.

[9] S. Junichiro, H. Jae-Cheol and S. kouichi, "Enhancing privacy of universal re-encryption scheme for RFID tags", EUC 2004, vol. 3207, LNCS, pp. 879-890, Springer-Verlag, 2004.

[10] 김배현, 유인태, "반사공격에 안전한 RFID 인증 프로토콜", 한국통신학회논문지, 제 32권, 제 3호, pp.348-354, 2007, 3.

[11] 안해순, 부기동, 윤은준, 남인길, "강력한 보안성을 제공하는 RFID 상호 인증 프로토콜", 정보처리학회논문지, 제 16-C권, 제 3호, 2009, 6.

[12] 김익수, "효율성을 고려한 해시 함수 기반의 안전한 RFID 프로토콜", 한국통신학회논문지, 제 34권, 제 4호, pp.428-434, 2009.

저자소개

신효영(Hyo-Young Shin)

1986년 광운대학교 전자계산학과 졸업
1988년 광운대학교 전자계산학 석사
1998년 광운대학교 컴퓨터과학 박사
1988년~1993년 (주)LG 소프트
1994 ~ 현재 경복대학 인터넷정보과 부교수
※관심분야:네크워크보안, 분산시스템

정 계 동(Gye-dong Jung)

1985년 광운대학교 전자계산학과 졸업
1992년 광운대학교 산업정보학 석사
2000년 광운대학교 컴퓨터과학 박사
1993년~2004년 광운대학교 정보과학원 교수
2005년~현재 광운대학교 교양학부 교수
※관심분야: XML 분산시스템, 이동에이전트