韓國컴퓨터情報學會 論文誌
第15卷 第10號, 2010. 10.

2010-15-10-3-4

ID 검색 개선을 위한 비보호채널상의 RFID 상호인증 프로토콜

박 미 옥*, 오 기 욱**

RFID Mutual Authentication Protocol on Insecure Channel for Improvement of ID Search

Mi-Og Park*, Gi Oug Oh**

요 약

본 논문에서는 데이터베이스, 리더 그리고 태그 간의 모든 통신 채널이 안전하지 않은 비보호 채널(insecure channel)임을 가정하여 비보호 채널상의 안전한 RFID 상호인증 프로토콜을 제안했다. 제안한 프로토콜은 안전한 단방향 해쉬함수를 사용했고, DB에서 태그 ID를 검색하는데 걸리는 시간과 해쉬 연산량의 부담을 개선하는 것이 목적이다. 또한, RFID 상호인증 프로토콜이 보장해야 할 기본적인 보안사항들뿐만 아니라 전방향 안전성(Forward Security)도 함께 제공하며, 태그에서 난수를 생성하지 않음으로써, 태그에서의 처리량의 부담을 줄이고자 한다.

Abstract

In this paper, we proposed a new secure RFID(Radio Frequency IDentification) mutual authentication protocol on insecure communication channel which assumed that all communication channels between the database, the reader and the tag are insecure communication channels. The proposed protocol used a secure one-way hash function and the goal is to improve search time of a tag ID and overload of hash calculational load in DB. In addition, the proposed protocol supports not only basic security requirements to be provided by RFID mutual authentication protocol but also forward secrecy, and the tag does not generate a random number to reduce overload of processing capacity in it.

▸ Keyword : RFID, 전방향 안전성(Forward Security), 상호인증(Mutual Authentication), 비보호 채널(Insecure Channel)

• 제1저자 : 박미옥 교신저자 : 오기욱
• 투고일 : 2010. 07. 29, 심사일 : 2010. 08. 16, 게재확정일 : 2010. 08. 26.
* 성결대학교 컴퓨터공학부 전임강사 ** 안양대학교 교양학부 조교수

Ⅰ. 서 론

RFID(Radio Frequency IDentification)란 모든 사물에 전자태그를 부착하고 무선통신 기술을 이용하여 사물의 정보 및 주변 상황정보를 감지하는 인식기술이다. RFID 시스템의 구성은 기본적으로 태그(Tag)와 리더(Reader) 그리고 데이터베이스를 갖춘 백-엔드-서버(Back-End-Server)로 구성된다. 리더는 사물에 부착된 태그로부터 고유 식별정보를 무선 주파수 통신으로 수집하고, 수집된 정보를 백-엔드-데이터베이스에 전송하여 대상물체를 판독 및 인식한다. 무선 주파수를 이용한 RFID 시스템의 이러한 장점은 바코드 시스템을 대체하여 일상생활 속의 교통가드나 출결 카드에서부터, 물류나 유통관리 및 재고 관리 분야에까지 널리 사용되고 있으나, 리더와 태그간의 무선 주파수 통신은 정보노출, 사용자의 위치추적(Location tracking), 위조와 같은 보안 및 사용자 프라이버시(Privacy) 침해 등의 심각한 문제를 발생할 수 있다[1][2][3]. 이러한 보안 안전성 문제해결을 위해, RFID 시스템에서는 리더와 태그간의 다양한 인증(Authentication) 메커니즘들이 제안되었으며, 대부분의 많은 논문들이 안전한 해쉬 함수를 사용하고 있다. 또한, 해쉬 함수를 사용하는 대부분의 논문들은 DB와 리더간의 통신 채널을 안전한 채널(Secure channel)로 가정하고 있다[4][5][6].

그러나, 최근에는 응용환경에 따라 휴대폰이나 PDA와 같은 모바일 장치에 리더를 장착하여, DB와 리더간에 무선 채널을 통한 데이터의 송수신환경이 가능해짐에 따라, DB와 리더간의 통신 채널을 안전하지 않은 채널(insecure channel) 즉, 비보호 채널로 가정한 논문들이 제안되어오고 있다. DB와 리더, 그리고 태그간의 모든 통신 채널이 안전하지 않은 비보호 채널이라고 가정할 경우, 리더와 태그간의 통신 채널에서 발생할 수 있는 재전송 공격(Replay attack), 도청 공격(Eavesdropping attack), 스푸핑 공격(Spoofing attack)과 같은 여러 공격에 취약할 수 있으며, 이러한 보안 취약성으로 인해 DB와 리더간에도 안전한 상호인증 메커니즘을 사용한다[7][8][9].

본 논문에서는 DB와 리더, 그리고 태그간의 모든 통신채널이 안전하지 않은 무선 채널 즉, 비보호 채널이라고 가정하여, 비보호 채널상의 안전한 RFID 상호인증 프로토콜을 제안한다. 제안한 프로토콜은 비보호 채널상에 전송되는 모든 데이터의 인증과 무결성(Integrity)을 보장하기 위해, 안전한 단방향 해쉬함수를 사용하며, 전방향 안전성(Forward security)을 제공하기 위해, 각 객체의 상호인증 후 DB와 태그는 현재의 비밀키를 다음 세션을 위한 새로운 비밀키로 각각 갱신한다. 또한, 본 논문에서 제안하는 상호인증 프로토콜은 기존의 인증 프로토콜들에서의 태그 ID 검색 및 인증시, DB에서 수행하는 해쉬 연산량의 오버로드를 줄이고, 태그에서 난수를 생성하지 않아, 태그에서의 처리 부담을 줄이고자 한다.

본 논문의 구성은 다음과 같다. 먼저, 2장에서 기존의 프로토콜들을 분석하여, DB에서의 계산로드의 비효율성을 보이고, 3장에서는 이러한 문제를 개선한 새로운 프로토콜을 제안한다. 4장에서는 제안 프로토콜의 안전성과 효율성을 분석한 후, 5장에서 결론을 맺는다.

Ⅱ. RFID 프로토콜 분석

2.1 기존의 프로토콜 분석

본 절에서는 해쉬함수를 기본으로 사용하는 암호학적 접근기법의 대표적인 프로토콜인 해쉬 락과 랜덤 해쉬락 기반의 프로토콜을 살펴보고, DB에서의 비효율성의 문제를 분석한다.

- 해쉬 락 프로토콜 : 이 프로토콜은 [그림 1]과 같이 태그에서 랜덤하게 선택된 key의 해쉬 값인 metaID=h(key)를 이용하여 태그를 인증하는 방법이다. 이 기법은 고정된 metaID의 이용으로 태그의 추적이 가능하며, 재전송 공격에 취약하다[1][3]. 또한, DB에서 태그검색 및 인증시, 일치하는 metaID 값을 찾을 때까지 태그의 모든 key값을 해쉬 함수에 입력하여 계산해야하므로, n*h(key) 번의 해쉬 연산을 수행해야하는 계산로드가 발생한다.

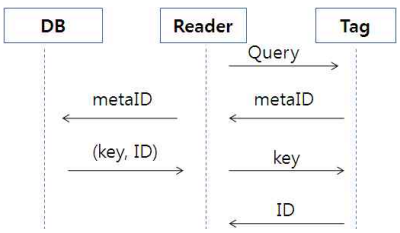

그림 1. 해쉬 락 프로토콜
Fig. 1. Hash Lock Protocol

- 랜덤 해쉬락 프로토콜 : 이 프로토콜은 [그림 2]와 같이 해쉬락 프로토콜의 확장기법으로 태그는 난수 R을 생성하여 h(ID‖R)을 계산한 후, 리더를 통해 DB에게 전달한다. DB는 저장된 모든 ID와 전송받은 R로부터 h(ID‖R)에 대응하는 식별정보를 찾아낸 후, 찾아낸 ID를 태그

에게 전달한다. 이 기법은 마지막 단계에서 태그의 ID가 노출될 가능성이 있고, 공격자가 난수 R과 h(ID‖R)을 획득하여 재전송 공격을 할 수 있다[3][10]. 또한, DB에서 모든 ID와 R을 h(ID‖R) 형식에 대입하여, 일치하는 태그를 검색하므로, n*h(ID‖R) 번의 해쉬연산을 수행하여, DB에서 비효율성의 문제가 발생한다.

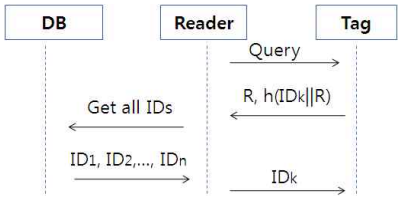

그림 2. 랜덤 해쉬락 프로토콜
Fig. 2. Random Hash Lock Protocol

2.2 비보호채널상의 프로토콜 분석

본 절에서는 비보호 채널상의 프로토콜들이 DB에서 태그 검색 및 인증시, 해쉬연산의 비효율성의 문제가 발생하는지 살펴본다. 본 논문에서 제안하는 프로토콜은 비보호 채널상의 RFID 상호인증 프로토콜인 [9]에 기본을 두고 있으며, 이 프로토콜에서는 비보호 채널이라는 단어 대신, 공개 채널(open channel)이란 단어를 사용했다.

본 절에서 분석하고자 하는 기존 프로토콜들에서 사용된 용어 및 표기는 다음과 같다.

- ID, TID : 태그의 고유정보 ID
- RID : 리더의 ID
- K : DB와 리더간의 공유 비밀키
- G_key : 공유 그룹키
- R, r : 리더가 생성한 난수
- T : 태그가 생성한 난수
- R_r : 생성된 난수의 오른쪽 절반값
- K_1, K_2 : DB와 태그간의 공유 비밀난수
- h(), $h_k()$: 단방향 해쉬함수와 키드 해쉬함수

[표 1-a]는 [7]에서 제안한 두 번째 모델을 나타낸 것으로서, DB가 전송받은 태그의 가상 ID인 metaID와 일치하는 ID를 검색하기 위해, 모든 태그에 대해 태그 ID, TID와 생성된 난수 R의 오른쪽 절반값인 R_r에 대해 XOR 연산($All[TID \oplus R\_r] \stackrel{?}{=} metaID$)을 수행한다. 그러므로, 이 모델도 재생공격과 상호인증은 제공하지만, DB에서 태그인증 과정 시, 모든 태그 ID에 대해 n번의 $[TID \oplus R\_r]$ 을 수행해야 한다. 또한, 이 모델은 전방향 안전성을 제공하지 않기 때문에, 사용자의 프라이버시를 보장하지 못하는 문제점이 발생한다.

[표 1-b]는 [8]에서 제안한 모델로서, 리더는 난수 r을 생성하여, $S = h_k(r)$ 값을 계산하기 위해, 키드 해쉬함수를 실행한다. 리더로부터 $S = h_k(r)$ 값을 전송받은 태그는 이 값을 이용해서 $ID = h(k_1 \oplus S \oplus C)$ 을 계산해 리더에 전송하고, 리더는 (ID, S, r)을 DB에게 전송한다. 리더가 DB에게 (ID, S, r)을 전송할 때, 동일한 ID가 전송되기 때문에, 재생 공격이 가능하고 사용자의 위치가 노출될 수 있는 문제점이 있다[7]. 또한, 다른 비보호 채널상의 모델들처럼, DB에서 일치하는 태그를 검색 및 인증하기 위해 n* $h(k_1 \oplus S \oplus C)$ 번의 해쉬 함수를 계산해야한다.

[표 1]을 통해 분석한 비보호 채널상의 모델들도 DB에서 태그 검색 및 인증시, n번의 해쉬 연산이나 n번의 XOR 연산에 대한 계산로드의 비효율성이 존재함을 알 수 있다. 또한, 태그를 한꺼번에 인식하는 시간이 태그의 수가 증가할수록 비례하는 전수조사 방식이 매우 비효율적이며, RFID 시스템에 적합하지 않다고 [2]에서 지적하고 있다.

표 1. 기존 프로토콜들의 ID 검색 및 인증과정
Table 1. ID Search and Authentication Process of the Existing Protocols

1-a. [7]	1-b. [8]	1-c. [9]
Verify $RID \stackrel{?}{=} G\_key \oplus R\_V1$ Retrieve R_key_i by RID_i then $R\_r = R\_key \oplus R\_V3$ Verify $metaID_i \stackrel{?}{=} All[TID \oplus R\_r]$ then $T\_Value' = h(TID \| R\_r \| T\_key)$ $L[T\_Value] \stackrel{?}{=} L[T\_Value']$	Verify $S \stackrel{?}{=} h_k(r)$ (abort if not) Retrieve $< k_1, k_2, C >$ Verify $ID \stackrel{?}{=} h(k_1 \oplus S \oplus C)$ (abort if not) then $ID' \stackrel{?}{=} h(k_2)$	Verify $h(K \| R)$ (abort if not) Find ID by verifying $h(ID \| R \| T)$ (abort if not) Update $ID_{new} = h(0 \| ID \| R \| T)$

III. 제안하는 프로토콜

본 장에서는 RFID 구성 요소간의 모든 통신채널이 비보호 채널이라는 가정 하에, DB에서의 해쉬 연산량의 계산로드를 개선한 RFID 상호인증 프로토콜을 제안한다. 제안 프로토콜은 ID 검색 및 인증시, DB에서의 비효율성의 문제를 개선하기 위해, 기호 I를 추가하여 I와 ID를 일대일로 매핑시킨다. I와 매핑되는 ID의 관계는 정당한 DB와 정당한 태그만이 알고 있는 비밀정보이다. 태그는 사전에 ID와 자신의 공유 비밀 정보인 I를 DB로부터 발급받아 저장해둔다. 여기서 ID는 각 세션마다 새롭게 갱신함으로써 전방향 안전성을 제공하고, I는 인증 세션을 거치면서 갱신되는 값이다.

제안한 프로토콜은 다음과 같다[그림 3].

[단계1] Reader -> Tag : Query, R

리더는 난수 R을 생성하여, Query와 함께 태그에게 전송한다.

[단계2] Tag -> Reader : I, h(ID‖I‖R)

태그는 전송받은 난수 R을 임시저장소에 저장한 후, R과 자신의 ID, 그리고 DB와의 공유 비밀정보인 I를 이용하여 h(ID‖I‖R)를 계산한다. 계산이 완료되면, I 값과 함께 리더에게 전송한다.

[단계3] Reader -> DB : R, I, h(K‖R), h(ID‖I‖R)

리더는 자신이 생성한 난수 R과 DB와 공유하고 있는 비밀키 K를 이용하여 h(K‖R)을 계산한 후, R과 h(K‖R), 그리고 태그로부터 전송받은 I 값과 h(ID‖I‖R)을 DB에게 전송한다.

[단계4] DB -> Reader : Inew=h(ID‖I‖T), IDnew = h(ID‖I‖R‖T), h(K‖R‖T)⊕Info, h(K‖R‖T‖Info), h(ID‖T‖R)

DB는 리더와의 공유 비밀키 K와 전송받은 R을 이용하여 h(K‖R)을 계산한 후, 전송받은 h(K‖R)과 같은 값인지 비교한다. 만약 두 값이 동일하면, DB는 리더를 정당한 객체로 인증하고 태그인증을 수행한다. 그렇지 않다면 리더 인증은 실패한 것으로 간주한다. 태그 인증은 먼저, 전송받은 I 값에 매핑되는 ID가 존재하는지 검색하여, 매핑되는 ID가 존재하면 h(ID‖I‖R) 값을 계산한 후, 전송받은 h(ID‖I‖R) 값과 동일한지 체크한다. 두 값이 동일하면, 태그 인증은 성공한 것이고, 그렇지 않다면 태그 인증은 실패한 것으로, 서비스를 중지한다. 태그 인증 성공 후, DB는 난수 T를 생성하여, 태그와의 비밀 정보인 I와 새로운 ID의 갱신을 위해, Inew=h(ID‖I‖T)와 IDnew = h(ID‖I‖R‖T)를 각각 계산한다. 그런 다음 h(ID‖R‖T)를 계산하고, 리더에서 사용할 태그의 정보인 info를 전송하기 위해 h(K‖R‖T)⊕Info와 h(K‖R‖T‖Info)를 계산하여, 난수 T와 함께 리더에게 전송한다.

[단계5] Reader -> Tag : T, h(ID‖R‖T), h(K‖R‖T)⊕Info, h(K‖R‖T‖Info)

리더는 DB로부터 전송받은 난수 T와 DB와의 공유 비밀키 K, 그리고 자신이 생성한 난수 R을 이용하여 h(K‖R‖T)를 계산한 후, DB로부터 전송받은 h(K‖R‖T)⊕Info과

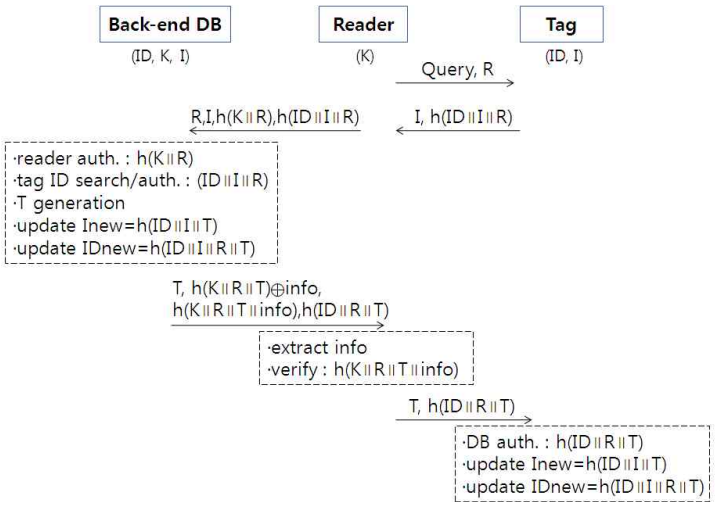

그림 3. 제안한 RFID 상호인증 프로토콜
Fig. 3. Proposed RFID Mutual Authentication Protocol

XOR 연산(h(K‖R‖T)⊕Info⊕h(K‖R‖T))을 수행하여 제품에 대한 정보값 Info를 추출한다. 리더는 얻어진 info 값을 사용해, h(K‖R‖T‖Info)를 계산한 후, DB로부터 전송받은 h(K‖R‖T‖Info)와의 일치여부를 비교하여, DB를 인증하고, Info 정보를 활용한다. DB 인증 성공시, 리더는 DB로부터 전송받은 난수 T와 h(ID‖R‖T)를 태그에게 전송한다. 만약, 두 값이 일치하지 않으면, DB 인증은 실패한 것이고, 과정을 중지한다.

[단계6] Tag : T, h(ID‖R‖T)

태그는 전송받은 난수 T와 [단계1]에서 전송받아 저장하고 있던 난수 R, 그리고 자신의 ID를 이용하여 h(ID‖R‖T)를 계산한다. 자신이 계산한 h(ID‖R‖T) 값과 전송받은 값이 동일하면, 태그는 [단계1]에서 전송받은 난수 R과 리더 및 DB를 인증하고, 다음 세션을 위해 새로운 비밀값 Inew=h(ID‖I‖T)와 IDnew = H(ID‖I‖R‖T)를 계산하여, 이전의 ID와 I 값을 갱신한다.

Ⅳ. 프로토콜 분석

4.1 안전성 분석

본 절에서는 비보호 채널상의 RFID 상호인증 프로토콜들의 보안사항을 바탕으로, 제안한 상호인증 프로토콜의 안전성 분석한다.

- **상호 인증(Mutual Authentication)**

DB는 [단계4]에서 자신이 계산한 h(K‖R)이 리더로부터 전송받은 h(K‖R)와 동일한지를 검증하여 리더를 인증하고, 자신이 계산한 h(ID‖I‖R) 값이 리더로부터 전송받은 h(ID‖I‖R) 값과 동일한지 검증하여 태그를 인증한다. 리더는 [단계5]에서 DB로부터 전송받은 난수 T를 사용하여, 자신이 계산한 h(K‖R‖T‖Info) 값과 전송받은 h(K‖R‖T‖Info) 값의 동일여부를 검증하여 DB를 인증한다. 태그는 [단계6]에서 리더로부터 전송받은 난수 T를 사용하여, 자신이 계산한 h(ID‖R‖T) 값과 전송받은 h(ID‖R‖T) 값과의 동일여부를 검증하여 리더와 DB를 인증한다. DB와 리더간의 공유 비밀키 K와 DB와 태그간의 공유 비밀정보 I, 그리고 I와 유일하게 매핑되는 ID를 모르는 공격자는 DB, 리더, 또는 태그로 위장하여 스푸핑 공격 등을 할 수 없기 때문에, 제안 프로토콜은 상호인증을 제공한다.

- **도청 공격(Eavesdropping attack)**

공격자는 전송메시지를 모두 도청할 수 있지만, 태그와 DB간의 공유 비밀정보 I로부터 매핑되는 ID를 구할 수 없다. 태그의 ID를 얻기 위해서는 공격자가 도청한 메시지 h(ID‖I‖R)이나 h(ID‖R‖T)로부터 ID 값을 구할 수 있어야 한다. 하지만 난수 R과 T가 계속 변하고, 안전한 단방향 해쉬함수의 성질로 인하여, h(ID‖I‖R)과 h(ID‖R‖T)로부터 태그의 ID를 얻는 것은 불가능하다. 또한, ID는 정당한 태그와 DB에서만 아는 비밀정보이고, 통신채널로 전송되지 않기 때문에, 공격자는 ID 값을 직접적으로 구할 수 없다. 또한, 공격자는 도청한 메시지 h(K‖R‖T)⊕Info나 h(K‖R‖T‖Info)로부터 DB와 리더간의 공유 비밀키 K를 구할 수 있어야한다. 그러나, 단방향 해쉬함수의 안전한 성질과 정당한 DB와 리더만이 K값을 알기 때문에, 공격자는 K 값을 얻을 수 없다. 따라서 제안 프로토콜은 도청공격에 안전하다.

- **재전송 공격(Replay attack)**

제안 프로토콜은 매 세션마다 DB가 생성한 새로운 난수 T와 리더가 생성한 새로운 난수 R을 이용하여 DB와 리더, 그리고 태그간의 상호인증을 수행하기 때문에, 공격자에 의해 재전송된 난수값들은 태그와 리더 그리고 DB간의 상호인증 과정 중에 쉽게 검출된다. 따라서, 제안 프로토콜은 재전송 공격에 안전하다.

- **스푸핑 공격(Spoofing attack)**

공격자는 DB와 태그간의 공유 비밀정보, 태그의 ID가 획득가능하면, DB 또는 태그로의 스푸핑 공격을 수행할 수 있다. 하지만 공격자는 정당한 DB와 정당한 태그 내에 각각 안전하게 저장하고 있는 비밀값, ID를 직접적으로 얻을 수 있는 방법이 없다. 또한, 전송 메시지 h(ID‖I‖R)과 h(ID‖R‖T) 값 내의 ID는 난수 R과 T, 그리고 단방향 해쉬함수에 의해 안전하게 보호되기 때문에, 이러한 전송 메시지로부터 ID를 획득하기 어렵다. 또 다른 스푸핑 공격가능성은, DB와 리더간의 공유 비밀키, K를 획득하면, DB 또는 리더로의 스푸핑 공격을 할 수 있다. 하지만, 공격자는 정당한 DB와 정당한 리더만이 알고 있는 공유 비밀키 K를 직접적으로 얻을 수 있는 방법이 없고, 전송 메시지 h(K‖R‖T)⊕Info와 h(K‖R‖T‖Info) 값 내의 비밀키 K는 난수 R과 T, 그리고 안전한 단방향 해쉬함수에 의해 보호되기 때문에, 이 전송 메시지들로부터 비밀키 K를 획득하기가 어렵다. 따라서, 제안 프로토콜은 스푸핑 공격에 안전하다.

- **트래픽 분석 공격(Traffic Analysis attack)**

h(ID‖I‖R)과 h(ID‖R‖T) 값은 난수 R과 T에 의해 매 세션마다 변경되기 때문에, 공격자는 현재 세션에서의 태그 응답값 h(ID‖R‖T)와 과거 세션에서 도청에 의한 태그 응답값이 동일한 태그로부터 전송된 것인지의 여부를 쉽게 구별할 수

없다. 따라서, 제안 프로토콜은 트래픽 분석 공격에 안전하다.

- **위치트래킹공격(Location Tracking attack)**

제안 프로토콜에서는 위치트래픽분석 공격과 마찬가지로 난수 R과 T를 사용해 계산된 h(ID‖I‖R)과 h(ID‖R‖T) 값은 매 세션마다 변경되기 때문에, 공격자가 특정한 태그를 식별할 수 없어 위치 트래킹이 어려워, 사용자의 프라이버시를 보호할 수 있다.

표 2. 안전성 분석
Table 2. Safety Analysis

공격 유형 \ 프로토콜	[1]	[4]	[9]	제안 프로토콜
도청 공격	X	X	O	O
재전송 공격	X	X	O	O
스푸핑 공격	X	X	O	O
트래픽 분석공격	X	O	O	O
위치 추적 공격	X	O	O	O
서비스거부 공격	O	O	O	O
전방향 안전성	X	X	O	O
DB와 Tag 상호인증	O	O	O	O
DB와 Reader상호인증	X	X	O	O

- **서비스거부 공격(Denial of Service attack)**

제안 프로토콜에서는 매 세션마다 DB와 태그간에 상호인증 완료 후에, 다음 세션에서 사용될 새로운 비밀키 값, IDnew=h(ID‖R‖T)로 갱신하기 때문에, 공격자에 의한 서비스 거부 공격은 쉽게 발견되어 질 수 있다. 또한, 리더와 태그간의 상호인증은 단방향 해쉬함수 연산만을 이용하기 때문에, 태그측에 서비스 거부공격을 수행할 만큼의 많은 연산량을 요구하지 않는다. 따라서, 제안 프로토콜은 서비스 거부 공격에 안전하다.

- **전방향 안전성(Forward Secrecy)**

기존의 많은 RFID 인증 프로토콜들은 매 세션마다 동일한 하나의 태그 ID만을 이용하여 상호인증을 수행함으로써, 공격자가 부채널 공격(Side-channel attack) 등을 통해 폐기되어진 태그로부터 비밀키 값인 태그의 ID를 얻을 수 있으며, 이로 인해 해당 태그와 리더간에 전송된 과거의 모든 메시지들의 무결성과 기밀성을 보장받을 수 없다. 그러나, 제안 프로토콜에서는 DB와 태그간에 상호인증 수행 후, DB와 태그가 이전의 ID를 다음 세션을 위한 새로운 비밀값, IDnew = h(ID‖I‖R‖T)로 각자 갱신하여 사용하기 때문에, 공격자가 현재의 비밀 값, IDnew = h(ID‖I‖R‖T)를 알더라도 안전한 단방향 해쉬함수의 성질에 의해 과거에 사용된 ID 값을 얻을 수 없으며, 태그의 과거 메시지들을 추적할 수 없다. 따라서, 제안 프로토콜은 전방향 안전성을 제공한다.

[표 2]는 앞에서 언급한 보안사항을 기본으로하여, 제안 프로토콜과 해쉬연산 기반의 해쉬락[1]과 랜덤해쉬락[4], 그리고 공개채널상의 상호인증 프로토콜의 안전성을 간단히 비교·분석한 것이다. [표 2]에서와 같이, 제안 프로토콜은 기존의 프로토콜들과 비교할 때, 도청 공격, 재전송 공격, 스푸핑 공격, 트래픽 분석 공격, 위치 트래킹 공격, 서비스 거부 공격 등에 안전하며, 비보호 채널상의 상호인증 프로토콜들이 보장해야하는 전방향 안전성도 제공하여 사용자의 프라이버시를 보호할 수 있다. 또한, 제안 프로토콜은 DB와 리더간의 상호인증과 DB와 태그간의 명시적인 상호인증을 제공하며, 비보호 채널상의 상호인증 프로토콜이 보장해야하는 각 객체간의 상호인증을 제공하기 때문에 기존의 프로토콜들에 비해 더 향상된 안전성을 제공한다고 할 수 있다.

4.2 효율성 분석

본 절에서는 제안한 프로토콜의 효율성을 분석한다. [표 3]은 [표 2]의 안전성 분석에서 동일한 비도를 가지는 비교모델 [9]과 비교분석한 결과를 간단히 정리한 것이다.

- **DB에 대한 효율**

표 3. 효율성 분석1
Table 3. Efficiency Analysis1
L : 하나의 데이터 유닛에 대한 비트길이

연산 종류 \ 시스템 객체		[9]	제안 프로토콜
해쉬 연산량	DB	n+5	7
	Reader	3	3
	Tag	3	4
XOR 연산량	DB	1	1
	Reader	1	1
	Tag	0	0
난수 생성 횟수	DB	0	1
	Reader	1	1
	Tag	1	0
저장량	DB	2L	3L
	Tag	1L	2L

비교모델에서는 DB에서 일치하는 태그 ID 검색을 위해, h(ID‖R‖T)의 형식에 ID 값을 일일이 대입해서 계산한 후, 그 계산 결과값이 전송받은 h(ID‖R‖T) 값과 일치하는지의

여부를 비교해, 리더 인증을 수행한다. 그러므로 비교모델에서는 일치하는 태그 ID 검색을 위해, n번의 h(ID‖R‖T) 해쉬연산을 수행해야한다. 그러나, 제안 프로토콜은 전송받은 I 값과 일대일로 매핑되는 ID가 존재하는지 일단 검색한 후에, 일치하는 ID가 존재하면 h(ID‖I‖R) 계산을 단 1번만 수행한다. [표 3]의 해쉬연산량은 전체 해쉬연산량을 나타낸 것으로, 비교모델에서는 총 n+5번을 수행해야하지만, 제안 프로토콜은 총 7번만 수행하면 된다. 그러므로 제안 프로토콜은 태그 ID 검색 및 인증시 발생하는 n번의 해쉬 연산량의 로드를 단 1번으로 개선함과 동시에 태그에게 딜레이될 수 있는 응답시간을 신속하게 처리할 수 있는 효율성도 제공한다.

- **태그에 대한 효율**

제안 프로토콜의 태그는 리더가 생성한 난수 R을 자신의 인증을 위한 계산값 h(ID‖I‖R)에 사용한다. 이에 대한 안전성은 DB가 리더 인증이 성공해야만 태그 인증을 수행하기 때문에, 난수 R이 정당한 리더로부터 생성된 값임을 검증할 수 있다. 그러므로 태그에서 리더가 생성한 난수를 대신 사용하는 것에 대한 안전성뿐만 아니라, 태그에서의 난수생성에 대한 처리부담을 줄일 수 있는 효율성도 제공한다고 할 수 있다.

- **해쉬 연산량 및 기타 연산량**

제안 프로토콜은 [표 3]과 같이 태그에서의 해쉬 연산량이, 상호인증을 위한 해쉬연산 2번과 전방향 안전성 제공을 위한 ID의 갱신 1번, 그리고 DB에서의 빠른 태그 ID 검색을 위해 사용한 I 값의 갱신에 1번 사용하여, 총 4번이 해쉬연산이 요구된다. 리더에서는 상호인증과 제품에 대한 정보를 얻기 위한 해쉬연산 3번이 요구되며, DB에서는 상호인증을 위해 4번, 제품에 대한 정보를 처리하기 위해 1번, I값 갱신에 1번, ID 갱신에 1번 사용하여, 총 7번이 요구된다. [그림 4]는 DB가 한꺼번에 인식해야 할 태그의 개수에 따른 해쉬 연산량을 비교한 그래프이다.

그림 4. ID당 검색/인증시의 해쉬 연산량 비교
Fig. 4. Comparison of Hash Computational Load per ID on Search/Authentication

표 4. 효율성 분석2
Table 4. Efficiency Analysis2
Q(쿼리 갯수), h(해쉬연산 횟수), R(난수)

연산 종류	연산량 및 통신라운드
Reader와 Tag간의 전송 메시지	1Q +2R +2h
Reader와 DB간의 전송 메시지	2R +5h
전체 통신 라운드	5

한꺼번에 인식해야 할 태그 갯수를 최대 n개로 설정한 경우는 비교모델II로, n의 절반값으로 설정한 경우는 비교모델I로 표기하여 비교하였다. 한꺼번에 인식해야 할 태그의 개수가 증가할수록, 비교모델은 해쉬연산량이 급증하는 것을 확인할 수 있다.

[표 4]는 객체간의 전송메시지의 연산량과 통신라운드 횟수를 나타낸 것으로, 비교모델과 동일한 결과값을 가지기 때문에 하나의 값만을 표기하였다. 리더와 태그간의 전송메시지 연산량은 1Q+2R+2h이고, 리더와 DB간의 연산량은 2R+5h, 전체 통신라운드 5로서, 비교모델과 동일한 값을 보인다. 그러므로 제안한 프로토콜은 DB에서의 해쉬연산량의 비효율성을 개선했음뿐만 아니라, 강한 보안성과 함께 경량의 통신 트래픽이 요구됨을 알 수 있다.

결론적으로, 제안한 프로토콜은 재생 공격이나 스푸핑 공격 등과 같은 다양한 공격에 안전할 뿐만 아니라 각 객체간의 상호인증과 전방향 안전성의 제공, 그리고, DB에서의 태그 ID 검색 및 인증시, n번의 해쉬연산 횟수의 계산로드를 단 1번의 해쉬연산으로 개선함으로써, 비보호 채널상의 RFID 상호인증 프로토콜에 대한 안전성과 효율성을 모두 보장해준다고 할 수 있다.

V. 결론

본 논문에서는 비보호 채널상의 RFID 상호인증 프로토콜을 제안하였다. 제안한 프로토콜은 간단한 기법에 의해, DB에서의 n번의 해쉬 연산을 단 1번의 해쉬 연산으로 감소시킴으로써, DB에서의 전체적인 ID 검색 및 인증시의 연산 처리량뿐만 아니라, 인증시간도 함께 개선하였다. DB에서의 이와 같은 빠른 연산은 태그에 대한 응답시간 딜레이를 최소화하여, 신속한 처리를 원하는 모바일 환경상의 사용자 만족도를 향상시킬 수 있다. 또한, 제안 프로토콜은 태그에서 난수를 생성하지 않아, 태그에서의 처리량에 대한 부담을 감소시켰으며, 기존의 상호인증 프로토콜의 기본적인 보안사항을 모두

만족함으로써, DB와 리더, 그리고 태그간의 모든 객체가 비보호 채널상에 존재하는 모바일이나 유비쿼터스 환경에 적용될 수 있을 것으로 본다.

향후 과제로는 제안한 프로토콜이 실제 모바일 환경에서 얼마나 사용가능성이 높은지를 증명해야 할 것이다. 또한, 제안한 프로토콜을 개선하여 태그뿐만 아니라 모바일 리더에 대한 프라이버시도 함께 보장할 수 있는 모델을 연구하고자한다.

참고문헌

[1] Stephen August Weis, “Security and Privacy in Radio-Frequency Identification Devices,” Master's Thesis, MIT, May 2003.

[2] 원태연, 천지영, 박춘식, 이동훈, “수동형 RFID 시스템에 적합한 효율적인 상호 인증 프로토콜 설계,” 한국정보보호학회논문지, 제 18권, 제 6(A)호, 63-73쪽, 2008년 12월.

[3] 이상렬, “RFID 시스템의 개선된 인증 프로토콜,” 한국컴퓨터정보학회 논문지, 제 12권. 제 6호, 193-200쪽, 2007년 12월.

[4] S. Wies, S. Sarma, R. Rivest, and D. Engels, “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems,” Security in Pervasive Computing 2003, LNCS 2802, pp. 201- 212, 2003.

[5] K. Ree, J. Kwak, S. Kim and D. Won, "Challenge-Response Based on RFID Authentication Protocol for Distributed Database Environment," SPC'05, LNCS 3450, pp.70-84, 2005.

[6] E. Choi, S. Lee and D. Lee, "Efficient RFID Authentication Protocol for Ubiquitous Computing Environment," EUC-2005, LNCS 3823, pp.945-954, 2005.

[7] Soo-Young Kang, Deok-Gyu Lee, Im-yeong Lee, “A study on secure RFID mutual authentication scheme in pervasive computing environment,” pp.4248-4254, Computer Communication 31, 2008.

[8] Jeongkyu Yang, Kui Ren, Kwangjo Kim, “Security and Privacy on Authentication Protocol for Low-cost RFID,” SCIS 2005.

[9] 윤은준, 유기영, "공개 채널 기반의 RFID 상호인증 시스템 설계," 한국통신학회논문지, 제 34권, 제 10호, 946-954쪽, 2009년 10월.

[10] 김성진, 박석천, “접근시간 간격 확인 방식을 이용한 RFID 보안강화 프로토콜 설계,” 한국컴퓨터정보학회 논문지, 제 11권 제 6호, 193-200쪽, 2006년 12월.

저 자 소 개

박 미 옥

1993년 : 숭실대학교 컴퓨터학과 공학석사

2004년 : 숭실대학교 컴퓨터학과 공학박사

2005년 ~ 현재 : 성결대학교 컴퓨터 공학부 전임강사

오 기 욱

1991년 : 경원대학교 전자계산학과 학사

1993년 : 숭실대학교 컴퓨터학과 공학석사

2007년 : 숭실대학교 컴퓨터학과 공학박사

2008년 : 강원관광대학 컴퓨터정보과 조교수

2010년 ~ 현재 : 안양대학교 교양학부 조교수