# 특정 태그 검색기능을 지원하는 향상된 안전성의 RFID 인증 프로토콜

함 형 민*, 오 희 국*, 김 상 진**

*한양대학교 컴퓨터공학과

**한국기술교육대학교 인터넷미디어공학부

e-mail:hmham@infosec.hanyang.ac.kr

# Enhanced Secure RFID Authentication Protocol with Searching Specific Tag

Hyoungmin HAM*, Heekuck Oh*, Sangjin Kim**

*Department of Computer Science a Engineering, Hanyang University
**School of Internet Media Engineering, Korea University of Technology and Education

요 약

본 논문에서는 RFID시스템에서 일어날 수 있는 위험요소들을 나열하고, 이에 맞는 해결책으로 RFID 인증프로토콜을 제시하며, 일반적인 RFID 인증프로토콜에서 볼 수 없었던 RFID 검색 프로토콜에 관한 소개와 검색 프로토콜이 갖는 새로운 요구사항을 제시한다. 또한 기존에 제안된 RFID검색 프로토콜보다 향상된 보안성을 지원하는 프로토콜을 제안하며 앞으로 연구할 방향을 제시한다.

## 1. 서론

RFID(Radio Frequency IDentification)기술은 무선 주파수를 이용한 객체 식별을 제공한다. 무선 주파수를 이용해 사물이나 사람에 부착된 태그를 인식, 태그에 담긴 정보를 주고받을 수 있도록 하는 비(非)접촉식 정보인식기술인 RFID는 현재 대형마트의 상품정보 처리 같은 기초적 단계부터 모든 사물에 태그를 부착해 네트워크 망을 만들어 모든 정보를 관리한다는 USN(ubiquitous sensor network) 시대를 열어줄 핵심기술로 주목받고 있다.[2]

하지만 RFID 시스템에서 태그와 리더 사이의 통신은 안전하지 못한 채널을 통해 이루어지며 이러한 취약점 때문에 적절하지 못한 도청, 수정, 정보의 분석에 노출되게 된다. 특히나, 수동태그의 경우, 낮은 계산 능력과 저장공간을 갖으며, 이렇게 노출된 데이터는 프라이버시 문제, 태그의 위조 같은 또 다른 위험요소를 발생시키게 된다. RFID 프로토콜은 이러한 위협으로부터 안전을 보장하기 위해 구별 불가능성(Indistinguishabilty), 전방향 안정성(Foward Security), 재전송 공격(Replay Attack)등의 요구사항을 고려해야 한다.

본 논문은 저사양의 수동태그 환경에서의 보안요구사항을 제시하고, 이를 충족하는 RFID인증프로토콜을 제안하며, 특정 태그를 검색하는 기능을 갖는 기존의 RFID인증프로토콜을 소개하고, 문제점을 분석한 뒤, XOR와 해쉬함수, 그리고사전 공유된 비밀키를 이용하여 효율적인 위치 프라이버시를 제공하는 특정 태그의 검색프로토콜을 제안한다.

* 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터(홈네트워크연구센터) 육성・지원사업의 연구결과로 수행되었음.

† 주저자, hmham@infosec.hanyang.ac.kr, hkoh@hanyang.ac.kr

‡ 교신저자, sangjin@kut.ac.kr

## 2. 제안하는 RFID 인증 프로토콜

### 2.1 요구사항

- 데이터 프라이버시: 리더는 태그를 인증할 수 있지만 태그는 리더를 인증할 방법이 없다. 태그는 일방적으로 리더가 보내는 시작 질의를 받고 그에 응답해 주는 것뿐으로, 공격자가 태그자체로부터 정보를 알아내지 못하도록 하드웨어적으로 구현하기에는 비용적 측면에서 무리가 있다[3]. 태그는 요청에 따라 고유정보를 공개채널로 전송해야 하며, 전송되는 정보가 보호되지 않으면 위장공격 등에 노출되게 된다.

- 위치 프라이버시: 보호된 정보는 내용의 노출은 막을 수 있지만, 보호된 정보의 출처를 막을 수는 없기 때문에 해당 태그의 위치가 노출될 위험이 있다. 이점을 이용하여 공격자는 태그가 부착된 상품의 소유자를 추적하는 것이

가능하다.

- 구별 불가능성: 위치프라이버시가 침해공격이 가능한 이유는 태그의 응답이 일정하기 때문이며, 같은 태그가 매번 다른 응답을 할 경우 자연히 이러한 문제를 해결할 수 있게 된다. 한 태그가 매번 다른 응답을 하게 되면, 공격자는 어떤 태그의 응답인지 구별할 수 없고, 결과적으로 위치프라이버시를 만족할 수 있다.

- 전방향 안전성: 태그의 비밀정보가 노출되었을 때, 그 정보가 이전세션에 사용된 비밀정보를 계산할 수 없어야 한다. 태그가 현 시점에 공격당했다 하더라도, 노출된 정보로부터 태그의 과거 행적까지 노출되지 않아야 하며, 이 역시 태그 소유주의 프라이버시 침해와 연관이 있다.

### 2.2. Basic authentication protocol

리더는 태그를 인증할 수 있지만 태그는 리더를 인증할 방법이 없다. 태그는 일방적으로 리더가 보내는 시작 질의를 받고 그에 응답해 주는 것뿐으로, 태그자체로부터 직접 정보를 노출하지 않도록 태그를 구현하기에는 비용적 측면에서 어려움이 있다.

표기법 <표 1>

R: Reader
T: Tag
n: nonce
ID: 태그 고유 식별자
EPC: ID와 매핑 되는 생산 코드 정보
x: 리더와 태그가 공유하고 있는 비밀정보 1
y: 리더와 태그가 공유하고 있는 비밀정보 2
flag: 세션 성공 카운터
⊕: XOR연산
h(): 해쉬연산
Req: 요청메시지
M: 응답 메시지
Sync: 재싱크 정보를 담은 메시지
$data_{c-n}$, $data_c$, $data_{c+n}$:
이전, 현재, 다음 세션의 정보

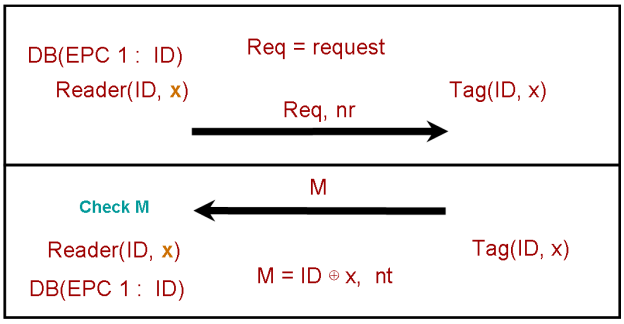
제안하는 프로토콜(그림 1)에서는 이러한 문제를 해결하기 위해 인가된 리더와 태그 간에만 서로 이해할 수 있도록 만든 메시지를 교환하는 방법을 사용한다. 이를 정리하면 다음과 같다.

- 태그가 보낸 응답메시지는 인가된 비밀정보 없이는 해석할 수 없다.

- 응답메시지를 해석할 수 있는 리더는 정당한 권한을 가졌다는 것을 의미하며, 서버로부터 해당 태그의 정보를 얻을 수 있다.

- 응답메시지를 해석할 수 있을 때에만 리더는 올바른 응답메시지를 생성할 수 있다.

리더가 생성한 요청질의의 재사용은 치명적인 문제이다. 리더의 질의 메시지를 도청한 공격자는 연속적인 질의를 통해 태그의 응답에서 일정한 연관성을 이끌어낼 수 있고, 이로 인해 메시지 분석공격이 가능 하게 된다.[1] 이러한 재사용 문제를 해결하기 위해 리더가 보내는 질의의 최신성을 보장하여야 하고, 전방향안전성을 보장하기 위해 동적으로 리더와 태그가 각자의 고유정보를 갱신할 수 있어야 한다.

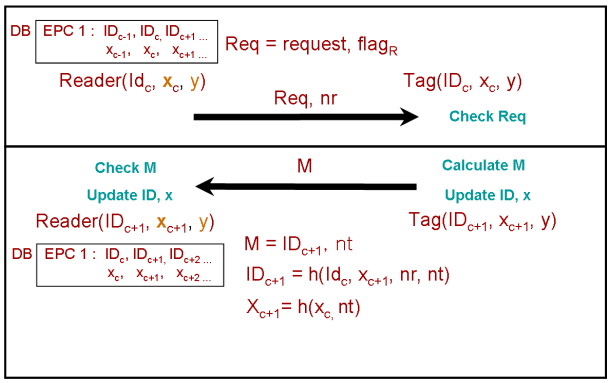



(그림 1) Basic authentication protocol

### 2.3. Authentication protocol using dynamic ID

동적ID기반으로 수정된 프로토콜(그림 2)은 위치프라이버시를 만족한다. 그러나 마지막 세션을 공격자가 임의로 중단하는 세션 중단 공격 시, 위의 조건을 만족하지 못하게 되는 문제가 있다. 이를 해결하기 위 해 이전단계와 다음 업데이트 될 ID를 유지하고 있어야 한다.

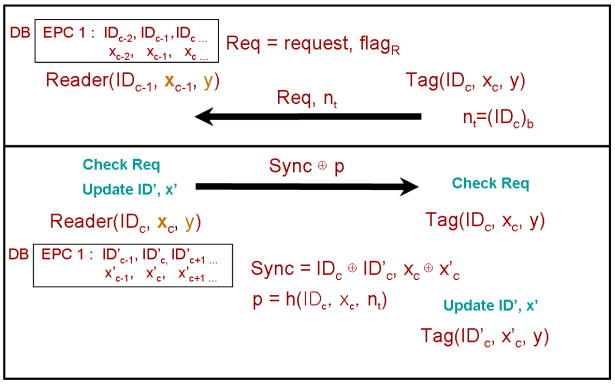
1. 리더는 *Req*를 보낸다.
2. 태그는 Req에 포함된 *flag*를 체크하고 옳으면 *flag*를 1증가시키고 $ID_c$와 $x_c$를 각각 $ID_{c+1}$와 $x_{c+1}$로 갱신한 후 M으로 응답한다.
3. 리더는 태그의 요청을 받아 DB의 정보가 갱신된 경우 *flag*를 1증가시킨다.




(그림 2) 정상세션인 경우

- 마지막 세션이 차단 된 경우

태그는 리더의 요청에 있는 *flag*를 체크하고, 유지하고 있는 *flag*와 맞지 않을 경우, (그림 3)과 같이 자신의 *flag* 정보를 리더에게 보낸다.




(그림 3) Synchronization of authentication protocol

리더는 일정 수만큼의 이전, 다음 세션 정보를 유지하고 있기 때문에 태그의 현재 ID를 알 수 있으며, ID′를 생성하여 태그와 재동기화를 행한다. 추가적으로 비밀정보 x나 ID가 공격자에게 드러났을 경우를 대비해 데이터의 일방향성 유지가 필요한데, 이를 위해 비밀정보 갱신에 해쉬함수를 사용한다.

## 3. RFID search protocol과 요구사항

Chiu C. Tan등이 제안한 RFID search protocol은 기존의 RFID 인증 프로토콜의 응용이다.[1] 다수의 태그 그룹에서 특정 태그의 응답만을 요구하는 것이 특징이며, 이러한 목적을 이루기 위해 요청메시지에 특정 태그의 정보를 포함하는 다소 다른 요청방식을 사용하게 된다. 제안된 인증프로토콜에 안전한 검색프로토콜을 적용하기 위해서는 이러한 차이에서 오는 새로운 보안요구사항이 고려되어야 한다.

### 3.1. RFID 검색 프로토콜 소개

기존에 제안된 서치 프로토콜은 크게 두 가지 유형으로 나눌 수 있다.

A. 교환되는 메시지는 정당한 리더와 태그만 생성할 수 있고, 해석할 수 있다. 이는 사전에 공유하고 비밀키에 의한 것이며, 공격자는 이 비밀키를 알기 위해 리더의 질의에 대해 재사용공격을 시도할 있다. 이를 방지하기 위해 바로 전단계의 난수를 저장해 두고, *flag*로 세션 횟수를 카운트하여 재사용 된 질의인지 확인하는 단계를 거친다.

B. 리더의 질의를 받은 모든 태그들은 리더의 질의가 자신에게 해당하는 것인지를 검사하게 되고, 자신이 아닐 경우에는 의미 없는 값을 생성하여 응답한다. 리더는 질의를 들은 통신범위내의 태그 n개의 그룹에 대해 실제로 모든 응답을 받아, 그 중 찾고자 하는 태그의 응답메시지를 찾게 된다.

### 3.2. 문제점 분석

제안된 기법 A에서 리더의 질의에 대해 다수의 태그 중에서 한 태그만 응답하게 된다는 점은 태그의 응답이 구별 불가능성을 만족해도, 위치프라이버시를 만족하기 어렵게 한다. 태그가 매번 다른 응답으로 구별 불가능성을 만족해도 리더가 매번 특정 태그 검색에 대해 같은 질의를 사용한다면 지속적인 감시로 결국 하나의 태그가 보내는 응답임을 알 수 있기 때문이다.

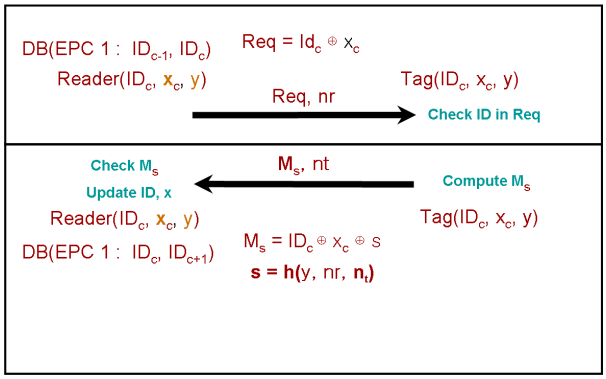
두 번째 기법 B는 하나의 질의에 대해 범위내의 질의를 받은 모든 태그로부터 응답을 받고, 그 중 원하는 응답을 구별하는 방식이다. 이 방식은 기존의 인증프로토콜을 이용해서 DB에서 태그 ID와 매핑되는 EPC를 검색해 내는 것과 크게 다를 바가 없으며, 인증프로토콜이 리더의 범위내의 모든 태그의 응답을 요구하는 반면, 서치프로토콜의 목적에서 볼 때, 이 같은 방식은 불필요한 낭비가 크다.

## 4. 요구사항 및 제안하는 검색 프로토콜

이 논문에서는 위의 두 가지 방법을 절충한 태그검색방식을 제안 하였다(그림 4). 요구사항은 다음과 같다.

(1) 같은 태그의 검색에 대해, 리더의 요청은 매번 갱신되어야 한다.

(2) 리더의 요청에 대해 검색 대상이 되는 특정 태그를 포함한 다수의 태그가 같이 응답 하여야 한다. 위치 프라이버시를 보장하기 위해 태그의 응답메시지는 구별 불가능성과 전방향안전성을 만족해야 한다.




(그림 4) Tag search protocol

1. 조건 (1)을 만족하기 위해 flag를 통해 동기화를 유지하는 서버와 태그는 ID를 매 세션마다 갱신하며, 결과적으로 ID를 포함하는 서버의 Req는 매번 달라진다.

2. 조건 (2)를 만족하기 위해서 태그들은 서버가 검색하고자 하는 대상이 자신이 아니더라도 응답하게 되며, 이때는 x가 아닌 y를 사용하여 가짜 응답 Md를 보내게 된다.

3. 리더는 원하는 태그의 응답을 다음과 같은 형태로 구별한다.

$Tag \rightarrow Reader: M_{tag}$

$Reader: M_{tag} \oplus (x_c \oplus s) = ID'$

*if*$(ID' == ID_{reder})$

*success*

*else*

*fail*

조건 (2)에서 가짜 응답을 보내는 확률은 리더의 질의 송신 범위내의 노드 숫자를 고려하여 사전에 정의되며, 이것으로 모든 노드가 허위응답을 하지 않게 되어 3.2에서 소개한 기법 B보다 리더와 통신하는 태그의 에너지 손실이 감소하게 된다.

## 5. 안전성 분석

각 요구사항에 대한 안전성 분석은 다음과 같다.

### 5.1. 재사용 공격

ID와 비밀키 x는 매 세션마다 $ID_{c+1}$, $x_{c+1}$로 갱신되므로 리더의 Req와 태그의 응답 M도 매번 새로워지며, 메시지의 재사용 공격이 불가능하다.

### 5.2. 위치추적

추적은 기본적으로 추적대상인 태그의 응답 을 공격자가 알고 있고, 정당한 질의를 보낼 수 있다고 가정했을 때, 반복적인 질의메시지로 응답의 발원지를 추적하는 것이므로, 목표대상이 매번 다른 응답을 하게 되면 메시지의 구별 불가능성을 만족하게 되어 위치추적으로부터 안전하다.

### 5.3. 전방향안전성

공격자가 이전 세션의 메시지를 수집해 놓았고, 현재 세션의 비밀키 $x_c$나, 메시지의 식별정보 $ID_c$를 알아냈더라도, 매 세션마다 일방향해쉬를 사용하여 갱신한 $x$와 $ID$로

부터 이전 세션에서 쓰인 $ID_{c-1}$이나 비밀키 $x_{c-1}$를 알아낼 수 없으므로 전방향 안전성을 만족한다.

### 5.4. 데이터프라이버시

메시지의 ID는 비밀키 $x$와 XOR되어 x를 모르면 알 수 없으며, 리더와 태그간에 교환되는 메시지는 $x$와 $ID$의 갱신으로 구별 불가능성도 만족한다. 만일 공격자가 x를 얻기 위해 분석공격을 시도하더라도 같은 태그의 응답을 구별하여 수집하기 어려우므로 안전하다.

## 6. 결론

본 논문은 저사양의 수동형 태그를 위해 XOR연산과 해쉬연산을 통해 안전성을 보장하는 RFID 인증 프로토콜을 제안하였다. 제안된 프로토콜은 매 세션마다 $ID$와 $x$를 갱신하여 메시지의 구별 불가능성과 위치프라이버시를 보장하였다. 계산량은 적지만 여타 암호알고리즘에 비해 보안성이 떨어지는 XOR연산의 단점은, 매 세션마다 메시지 갱신을 통한 메시지의 구별 불가능성으로 선형 식의 도출을 어렵게 하여 해결하고자 하였다. 메시지의 구별 불가능성을 보장함으로써, 메시지 분석을 위해 선행되어야 하는 수집된 메시지와 태그의 연관성을 찾는 작업을 방지하여, 메시지 도청만으로 $x$나 $ID$를 계산하려는 공격으로부터 안전하다. 또한 리더는 특정 태그 검색 시, 검색하고자 하는 태그의 ID를 포함하는 질의 메시지를 보내며, ID가 일치하는 태그는 다른 태그와 구별된 응답을 하는 태그 검색 프로토콜을 같이 제안 하였다.

## 참고문헌

[1] Chiu C. Tan, Bo Sheng, and Qun Li "Serverless Search and Authentication Protocols for RFID" PerCom'07

[2] M.Ohkubo, K. Suzuki. and S. Kinoshita, "Efficient hashi-chain based RFID privacy protection scheme." Proc of the Workshop on Privacy: Current Status and Future Direction. 2004

[3] T. Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks", IEEE/Create Net Secure Commun., 2005.

[4] Hun-Wook Kim, Shu-Yun Lim, Hoon-Jae Lee, "Symmetric Encryption in RFID Authentication Protocol for Strong Location Privacy and Forward-Security", 2006 International Conference on Hybrid Information Technology - Vol2 (ICHIT'06) pp. 718-723