# 수동형 태그를 활용한 경량 모바일 RFID 인증 프로토콜 설계

엄 태 양[1O], 김 춘 수[2], 박 용 석[2], 이 정 현[1]
[1]숭실대학교 컴퓨터학부, [2]한국전자통신연구원 부설연구소
appler@ssu.ac.kr, jbr@ensec.re.kr, parkys@ensec.re.kr, jhyi@ssu.ac.kr

# Design of Lightweight Mobile RFID Authentication Protocol Using Passive Tags

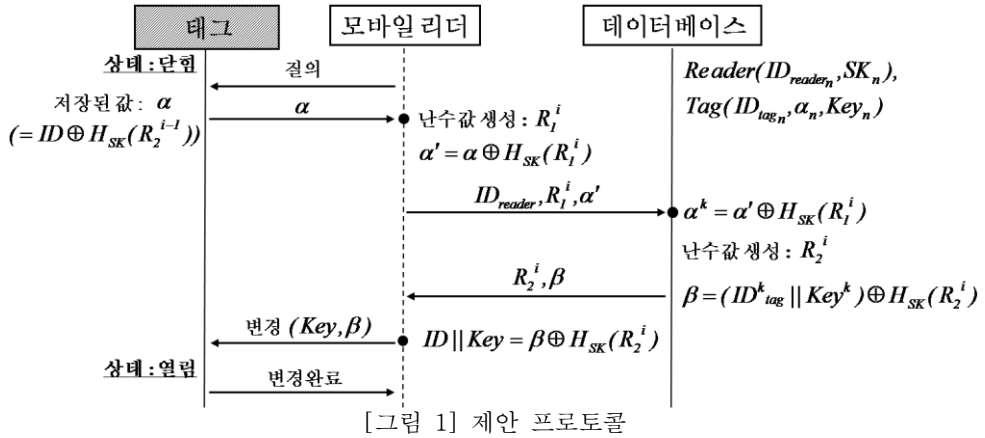
Taeyang Eom[O1], Choon Soo Kim[2], Yongseok Park[2], Jeong Hyun Yi[1]
[1]Soongsil University, School of Computing, [2]The Attached Institute of ETRI

## 1. 서론

모바일 RFID 시스템은 기존 RFID 시스템의 리더를 휴대용 모바일에 탑재하여 사용자 개인에게 보다 편리하고 다양한 서비스를 제공할 수 있다. 사용자는 휴대하고 있는 단말을 가지고 필요한 정보를 편리하게 제공 받지만, 기존의 RFID 시스템에서 발생할 수 있는 보안 취약점이 그대로 모바일 RFID 시스템으로 넘어오면서 사용자 편리성에 비례하여 많은 문제가 발생하게 된다. 이러한 보안 문제를 해결한 이전의 연구들은 프로세서가 없는 수동형 태그 보다는 능동형 태그에 적합한 기능들이었다. 따라서, 저가의 수동형 태그 사용과 모바일 단말의 연산 능력을 활용하여 모바일 RFID 시스템에서의 보안 문제를 해결 할 수 있는 모바일 RFID 인증 프로토콜을 제안한다.

## 2. 제안 프로토콜

제안 프로토콜은 태그의 기능은 수동형 태그를 그대로 활용하고, 모바일 단말의 연산 기능을 최대한 활용하여 해쉬와 XOR 연산만을 활용한 모바일 RFID 보안 및 성능 요구사항을 충족시킨다. 제안 프로토콜은 시스템 초기화 단계와 인증 단계로 구성되며 초기화 단계에서 태그와 데이터베이스는 *ID*, $\alpha$ 그리고 *Key*를 저장하고 모바일 리더는 데이터 베이스와 인증에 사용할 자신의 $ID_{reader}$와 *SK*(Secret Key)를 저장한다. 태그 정보를 인증하기 위한 단계는 [그림 1]과 같다.




[그림 1] 제안 프로토콜

**단계 1**: 모바일 리더가 태그에게 질의를 하면 태그는 사전에 저장된 $\alpha$ 값을 전송한다.

**단계 2**: $\alpha$ 값을 받은 모바일 리더는 가지고 있는 *SK*를 사용하여 자신이 생성한 랜덤값 $R_1$을 해쉬하여 $\alpha$ 값과 XOR 연산한 $\alpha'$ 값을 $ID_{reader}$ , $R_1$과 함께 보낸다. 데이터베이스는 받은 $ID_{reader}$가 자신에게 등록되어 있는 리더인지 확인 후 절차를 진행할지 판단한다. $ID_{reader}$가 확인된다면 그와 쌍을 이루는 *SK* 를 선택한다. 만약 등록되어 있는 모바일 리더라면 보내온 $R_1$ 값을 모바일 리더와 공유하고 있는 *SK* 값으로 해쉬하여 나온 값으로 $\alpha'$를 XOR 연산하여 원래의 $\alpha$ 값을 구하여 자신이 가진 값이 맞는지 $ID_{tag}$를 검증한다. 정상적인 태그임이 검증되면 데이터베이스는 난수값 $R_2$를 생성하여 모바일 리더의 *SK*를 사용하여 해쉬한 값을 원래의 $ID_{tag}$ 그리고 *Key*를 연접한 값과 XOR 연산한 값 $\beta$를 생성한다. 이렇게 생성된 $R_2$, $\beta$ 값은 다시 모바일 리더에게 보내진다.

**단계 3**: 모바일 리더는 전달받은 $R_2$, $\beta$ 값을 가지고 $R_2$ 값은 자신의 *SK*를 사용하여 해쉬한 값으로 $\beta$와 XOR 연산을 하여 $ID_{tag}$ 와 *Key*를 연접한 값을 구한다. 모바일 리더는 태그의 저장 값 변경을 위해 *Key*를 사용한 질의를 통해 데이터 베이스가 생성해서 보내준 $\beta$ 값으로 업데이트를 해주고 인증단계를 마친다.

## 3. 안전성과 효율성 비교

### 3.1 안전성

- **태그 보호**: 공격자는 *Key*를 알지 못하기에 수동형 태그를 임의로 수정할 수 없으며 읽어온 값이 직접적으로 태그의 *ID*에 해당하는 정보가 아니므로 이를 만족한다. $\alpha$ 값은 인증 단계마다 생성된 랜덤 값을 선택하여 *SK*를 사용한 해쉬 값을 이용하므로 랜덤 값을 알게 되더라도 *SK*를 알지 못하면 똑같은 해쉬 값을 구할 수 없으며 이렇게 생성된 값을 가지고 *ID*와 XOR 연산을 하여 생성한 값이 $\alpha$ 이므로 매번 알 수 없는 값으로 변경되어 *ID* 값을 구하지 못한다.
- **위치 추적 방지**: 태그로부터 읽어온 값을 모바일 리더는 추적 방지를 위해 자신이 생성한 랜덤 값 $R_1$을 해쉬한 값과 태그로부터 읽어온 $\alpha$ 값으로 XOR한 값 $\alpha'(=\alpha \oplus H(R_1^i))$을 전송하므로 매번 전송 시 마다 다른 값이 전송되어 추적 문제를 해결한다. DB 역시 자신이 생성한 랜덤한 해쉬 값 $\beta(=ID||Key \oplus H(R_2^i))$을 전송하므로 태그에 저장된 값 $\alpha$를 알고 있다고 해도 추적 문제가 발생하지 않는다.
- **트래픽 분석 방지**: 모바일 리더와 DB 구간에 공개 되는 $ID_{reader}$, $R_1$, $R_2$, $\alpha'$, $\beta$ 값을 도청자가 모두 획득해도 *ID*, *Key* 와 XOR 된 해쉬 값을 구할 수 없으므로 불법적인 인증을 성공 할 수 없다. 사용한 해쉬 함수는 *SK*를 사용하므로 모바일 단말기와 DB가 공유하는 키를 가진 정당한 리더가 아니라면 인증을 성공 할 수 없다.

이전에 제안된 프로토콜과의 기능 비교는 [표 1]에서 볼 수 있듯이 제안 하는 프로토콜은 보안 요구사항과 성능 요구사항을 만족하고 있다. MW 프로토콜은 보안 요구사항을 모두 만족하지만 경량화 기능은 만족하지 않는다. 여기서 경량화를 만족하고 하지 않고의 성능 요구사항 비교에 해당하는 내용은 다음 절에서 설명 하도록 한다.

[표 1] 기능 비교표

| 프로토콜 | | 해쉬 락 프로토콜 | 랜덤 해쉬락 프로토콜 | MW 프로토콜 | 제안 프로토콜 |
|---|---|---|---|---|---|
| 모바일 RFID 요구사항 | 태그 보호 | ○ | ○ | ○ | ○ |
| | 위치 추적 방지 | × | ○ | ○ | ○ |
| | 트래픽 분석 방지 | × | × | ○ | ○ |
| | 경량화 | × | × | × | ○ |

[표 2] 성능 비교표

| 프로토콜 | | 해쉬 락 프로토콜 | 랜덤 해쉬 락 프로토콜 | MW 프로토콜 | 제안 프로토콜 |
|---|---|---|---|---|---|
| 저장량 (bit) | 태그 | $\log(tkh^2)$ | $\log(t^2hr)$ | $\log(tsh^2r^2)$ | $\log(kh)$ |
| | 리더 | $\log(kh)$ | $\log(th^2r)$ | $\log(t^2sh^2r^2)$ | $\log(tskh^2r)$ |
| | DB | $n\log(tkh)$ | $n\log t$ | $n\log(ts)$ | $m\log(us)+n\log(tkh)$ |
| 계산량 (횟수) | 태그 | $2h$ | $h+r$ | $2h+r$ | - |
| | 리더 | - | $(n/2)h$ | $(n/2)h+r$ | $2h+r$ |
| | DB | - | - | - | $2h+r$ |
| 통신량 (bit) | 태그-리더 | $\log(th)$ | $\log(t^2hr)$ | $\log(th^2r^2)$ | $\log(kh^2)$ |
| | 리더-DB | $\log(kh)$ | $(n/2)\log t$ | $(n/2)\log(ts)$ | $\log(uh^2r^2)$ |

h: 해쉬값, r: 랜덤값, m: 전체 모바일 리더의 개수, n: 전체 태그의 개수, k: 태그 패스워드, s: 비밀키, t: 태그 식별값, u: 리더 식별값

### 3.2 효율성

- **경량화**: 기존에 제안된 인증 프로토콜은 능동형 태그에 대한 인증 프로토콜이므로 해쉬 락 프로토콜은 태그에 해쉬 함수를 구현해야 하며 랜덤 해쉬 락 프로토콜은 해쉬 함수와 난수 발생기를 태그에 구현해야 한다. MW 프로토콜 역시 난수 발생기와 키를 찾기 위한 트리 알고리즘이 태그와 리더에 구현 되어져야 하므로 이전 프토토콜은 모두 경량화를 만족하지 않는다. 하지만 제안하는 프로토콜은 [표 2]에서 볼 수 있듯이 데이터베이스에 저장해야 하는 공간은 모바일 단말의 *ID*와 *SK*, 태그의 *ID*, *Key*와 임의로 저장된 $\alpha$ 값으로 인해 많은 편이지만, 수동형 태그를 사용하며 태그가 수행해야 할 연산들을 모바일 단말이 처리 해 주고 있으며 안전성 및 효율성을 만족한다. 계산량 역시 랜덤 해쉬 락이나 MW 프로토콜은 데이터베이스의 *ID* 리스트를 전수 조사 해야 하지만 제안하는 프로토콜은 계산량이 고정되어 있어 성능면에서 좋은 효율을 보여주고 있다. 통신량은 태그-리더 구간, 리더-DB 구간으로 나눠지며 랜덤 해쉬 락 프로토콜과 MW 프로토콜은 계산량이 고정되지 않으므로 매번 리스트를 요청하는 통신량 또한 고정적이지 않다. 하지만 제안하는 프로토콜은 고정된 통신량만을 필요로 하므로 다른 프로토콜에 비해 효율적이다.

## 4. 결론

모바일 RFID 시스템은 기존의 RFID 시스템에 비해 훨씬 편리하고 유용한 정보 제공 기능을 가진다. 하지만 무선 인식에 의한 사용자들의 개인 정보 보호 기능이 충분히 뒷받침 되고 있지 않다. 또한 이전의 문제점이 지금의 모바일 RFID에서는 더욱 큰 문제로 발생 되는 시점에서 인증 기술에 대한 많은 제안들이 나오고 있지만 효율성과 안전성 면에서 몇 가지 문제점을 가지고 있었다. 본 논문에서는 순수한 수동형 태그의 제공되는 기능과 휴대용 단말의 연산능력만으로 해쉬 함수와 난수 발생기를 사용한 RFID 인증 프로토콜을 제안했고 또한 이 프로토콜이 안전성 및 효율성을 만족함을 보였다.