모바일 RFID 프라이버시를 위한 인증 프로토콜 성능 평가

정회원 엄 태 양*, 종신회원 이 정 현**

Performance Evaluation of Authentication Protocol for Mobile RFID Privacy

Taeyang Eom* *Regular Member*, Jeong-Hyun Yi** *Lifelong Member*

요 약

모바일 RFID(Radio Frequency IDentification)은 스마트 폰과 같은 휴대 가능한 장치에 기존의 RFID 리더를 탑재하여, 개인에게 다양하고 편리한 서비스를 제공할 수 있다. 개개인은 제품에 대한 정보를 장소에 구애받지 않고 제공받을 수 있지만, 모바일 리더를 소지한 누구나 타인의 RFID 태그를 읽을 수 있어 개인 프라이버시 침해가 발생할 위험 요소가 존재한다. 이러한 프라이버시 침해 문제를 해결하기 위해 다양한 인증 기술들이 제안되어 왔지만, 대부분은 태그에서 많은 연산을 필요로 하는 솔루션으로 일반적으로 많이 사용하는 수동형 태그에서는 적용할 수 없다. 따라서, 본 논문에서는 모바일 단말의 연산능력을 최대한 활용하여 능동형 태그 뿐만 아니라 일반적인 수동형 태그에도 적용가능한 모바일 RFID 인증 기술을 제안한다. 제안 프로토콜은 태그보호, 위치추적 방지, 트래픽 추적 방지를 위한 보안 요구사항과 경량화를 위한 성능 요구사항을 모두 만족하고, 이의 실용성 검증을 위해 스마트폰과 상용 모바일 RFID 리더기에 제안 프로토콜을 탑재하여 실험한 결과를 제시한다.

Key Words : Mobile RFID, Passive Tag, RFID Authentication Protocol

ABSTRACT

Mobile RFID system, that consists of the existing RFID reader mounted on the mobile devices such as smartphones, is able to provide the users a variety of services and convenience. Although the users can get the information about a certain product anytime anywhere, there is high probability that their privacy may be violated because their belongings with RFID tags can be scanned by other mobile readers at any time. Several RFID authentication schemes have been proposed to deal with these privacy issues. However, since the existing solutions require heavy computation on the tag side, most of them is not applicable to the general low-cost passive tags which do not have any processing unit. In this paper, we propose the efficient authentication scheme for mobile RFID system applicable to the passive tags as well as the active ones by the best use of computing capability of mobile devices. The proposed scheme satisfies the import security issues such as tag protection, untraceability, anti-traffic analysis. We also implement the proposed scheme on top of real smartphone for feasibility and show the experimental results from it.

※ 이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.20090067977).
* 숭실대학교 컴퓨터학부 모바일 보안 연구실(appler@ssu.ac.kr), ** 숭실대학교 컴퓨터학부 교수(jhyi@ssu.ac.kr)
논문번호 : KICS2010-11-539, 접수일자 : 2010년 11월 10일, 최종논문접수일자 : 2011년 5월 11일

Ⅰ. 서 론

모바일 RFID 시스템은 무선 식별 기술로써 태그의 정보를 누구나 읽을 수 있다. 이러한 자유로운 읽기 기능과 무선 인식의 특성상 모바일 RFID 시스템에는 타인이 태그의 정보를 읽음으로써 사용자가 소유한 태그의 정보를 획득하여 발생하는 사생활 침해 문제[16]가 있으며, 태그의 고정적인 ID 값을 네트워크 구간에서의 도청에 의한 사용자 추적 문제가 발생할 수 있다.

이러한 RFID 프라이버시 문제를 해결하기 위해 다양한 해결책[1~5,9,11~13,15,17,18]이 지금까지 제시되어 왔지만, 대부분의 기술들이 태그에 많은 연산을 요구하고 있어, 프로세서가 내장된 고가의 능동형 태그에만 적용할 수 있다. 태그의 가격 상승과 태그 자체의 부피 증가 문제로 인해 주로 물품 등에 부착되는 수동형 태그를 기반으로 하는 모바일 RFID 시스템에서는 실용적으로 활용되지 못하고 있다.

이를 위하여 본 논문에서는 기존 프로토콜들의 고연산 기능을 모바일 단말기에 전가하고, 태그에는 처리 결과값을 저장하는 형태로 수동형 태그만으로 인증 기능을 구현할 수 있는 효율적인 프로토콜을 제안한다. 따라서, 본 논문의 주된 초점은 주로 능동형 태그를 가정하는 기존 RFID 인증 프로토콜의 제약사항을 개선하여, 능동형 태그 사용없이 수동형 태그만으로도 동일한 안전성과 성능을 보일 수 있는 모바일 RFID 인증 기법을 제안하는 데 있다. 제안한 프로토콜은 태그보호, 위치추적 방지, 트래픽 추적 방지를 위한 보안 요구사항과 경량화를 위한 성능 요구사항을 모두 만족하고, 이의 실용성 검증을 위해 스마트폰과 상용 모바일 RFID 리더기에 제안 프로토콜을 탑재하여 실험한 결과를 제시한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 모바일 RFID 시스템의 구성과 보안 및 성능 요구사항에 대해 설명한다. Ⅲ장에서는 이전에 제안된 RFID 인증 프로토콜의 분석내용을 기술하고, Ⅳ장에서는 제안하고자 하는 인증 프로토콜을 설명한다. Ⅴ장에서는 설계한 인증 프로토콜 구현과 실험을 통한 성능 평가 결과를 제시하고, 마지막으로 Ⅵ장에서 결론을 맺는다.

Ⅱ. 모바일 RFID 시스템

2.1 모바일 RFID 시스템 구성

모바일 RFID 시스템은 태그, 휴대용 단말에 내장되거나 부착 가능한 RFID 리더 그리고 데이터베이스로 그림 1과 같이 구성되어 있다.

태그는 칩과 안테나로 구성되어 있으며, 유일한 식별 코드에 해당하는 ID 데이터가 저장되어 있어서 리더의 요청에 의해서 자신의 데이터를 송수신하는 장치이다.

모바일 리더는 태그에게 질의를 보내거나 태그로부터 받은 데이터를 판독하여 서버에게 전송하는 태그 데이터 식별 장치로써, 태그와 데이터베이스 사이에서 중계자 역할을 수행하며, 모바일 RFID 시스템에서의 리더는 유동적이기 때문에 무선망을 통해 통신한다.

마지막으로 데이터베이스는 RFID 리더로부터 전송되는 태그 데이터를 통하여 자신이 가진 정보가 있다면 리더에게 제공하는 역할을 한다.

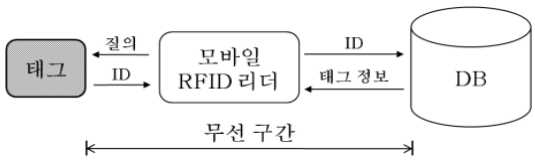

그림 1. RFID 시스템 구성

2.2 모바일 RFID 보안 및 성능 요구사항

모바일 RFID 시스템의 요구사항으로 크게 보안 요구사항과 성능 요구사항으로 분류한다.

2.2.1 보안 요구사항

모바일 RFID 시스템 역시 기존의 RFID 시스템 보안 문제를 더욱 확산 시킬 수 있으므로 아래의 요구사항을 만족해야 한다.

- 태그 보호: 리더의 질의에 대해 응답하는 태그의 데이터가 정보 제공에 사용될 수 있는 ID 값과 같이 어떠한 변화 없이 그대로 전달 되어진다면 태그의 정보에 해당하는 소유자가 가진 물품이 공개되게 된다. 그러므로 허가되지 않은 리더로부터 받은 질의에 대해 태그는 인증 절차 없이 고유한 ID 값을 노출하지 않아야 한다.
- 위치 추적 방지: 태그가 가진 데이터는 RFID 리더에서 해석 되어지며 이 데이터가 무선망을 통해 데이터베이스로 전해지게 되어 정보를 제공받게 된다. 하지만 도청자가 태그와 리더 사이에서 가져가는 데이터는 무의미한 데이터지만 무선망을 통해 전달되는 데이터가 태그가 응답한 데이터와 같다면 이 데이터를 통해 도청자는 위치 추적을 할 수 있다. 그러

므로 추적 문제가 발생할 수 있는 태그의 데이터가 주기적으로 갱신되어야 하며 리더와 데이터베이스 구간에서 태그의 데이터가 그대로 보내져서는 안된다.

- 트래픽 분석 방지: 태그가 가진 인증 데이터만을 가지고 인증 프로토콜 및 서비스에 대해 접근 권한을 가지게 해서는 안되며 태그와 RFID 리더 구간, RFID 리더와 데이터베이스 구간에서 공개 될 수 있는 인증 데이터는 연관 관계나 불법적으로 인증절차에 사용해도 올바른 인증으로 판단되지 않아야 한다. 그리고 태그와 리더, 데이터베이스 사이의 데이터가 태그와 소유자간의 상관관계를 쉽게 파악할 수 없도록 해야 한다.

2.2.2 성능 요구사항

안전하게 정보를 제공받을 수 있으려면 많은 보안 기능이 추가되어야 하지만, 실제 비용측면에서 RFID 응용에서 현실적으로 활용 가능한 태그는 저가의 수동형 태그를 우선 고려하여야 한다. 이를 위한 모바일 RFID 성능 요구사항은 다음과 같이 경량화를 들 수 있다.

- 경량화: 인증 기술과 사용자 프라이버시 문제를 위한 많은 기능을 수행해야 하지만 수동형 태그의 기능은 극히 제한적이다. 바꿔 말하면 태그의 연산 기능은 모바일 단말의 컴퓨팅 능력을 활용하고, 태그는 읽기 쓰기와 잠김 기능만 제공되는 수동형 태그를 활용 할 수 있어야 한다.

위에서 살펴본 모바일 RFID 요구사항을 각 구성별로 정리 하면 태그는 소유자가 가진 물품 정보와 직접적으로 연결되는 데이터를 가지고 있으면 안되며, 주기적으로 변경되어야 하며, RFID 리더는 태그로부터 받은 데이터를 데이터베이스에 전달시에 태그가 가진 ID, 키 에 해당하지 않는 데이터라 할지라도 추적 문제 및 트래픽 분석 방지를 위해 매번 암호화 하거나 랜덤 값으로 변환해서 전달해야 한다.

데이터베이스 역시 보안 요구사항을 만족하려면 추적방지를 위해 RFID 리더가 보내온 데이터와 연결 가능한 데이터를 보내선 안되며 트래픽 분석을 막기 위해 유추할 수 없는 랜덤 값이나 암호화한 값을 전송해야 한다.

Ⅲ. 기존 RFID 인증 프로토콜

RFID 인증 관련한 다양한 연구가 진행되어 왔고, 최근에는 저가의 RFID 태그에 적합한 경량 암호 기반 인증기술[6,8,14]들이 제안 되었지만, 태그에 해쉬함수 또는 유사랜덤함수의 구현 및 실행코드 주입이 필요로 하는 등 수동형 태그에는 실제 적용하지 못하는 기술들이다. 따라서, 본 장에서는 기존의 RFID 인증 프로토콜들 중 가장 대표적인 경량화 기법들을 선택하여 2.2절의 보안 및 성능 요구사항 준수 여부를 분석한다.

3.1 해쉬 락 프로토콜

S. Weis et al.은 RFID 태그가 불법적인 리더에 의해 식별되는 것을 막기 위해 해쉬 함수를 사용한 해쉬 락 프로토콜[19]을 제안 하였다. 이 방법은 낮은 비용의 태그의 리소스 제한을 해결하기 위해 태그에 하드웨어적으로 최적화되어 구현된 해쉬 함수 만을 가정하고 있다. 해쉬 락 프로토콜의 인증 절차는 그림 2와 같다.

불법적인 질의를 통한 태그의 식별을 막기 위해 리더는 키를 사용하여 태그의 ID를 가짜 식별자인 metaID로 변경시키고 데이터베이스에 metaID와 키 집합을 저장한다. 적법한 리더가 잠김 상태인 태그를 식별하기 위해서 태그로부터 받은 metaID를 데이터베이스에 전달하고 데이터베이스는 리더에게 metaID에 해당하는 ID와 키 집합을 리더에게 전달한다. 리더는 태그에게 전송받은 키를 전달함으로써 열림 상태로 변경하고 해당 태그의 진짜 식별자를 통해 태그의 정보를 알아낸다.

이 방법은 일방향 해쉬 함수의 역원을 구하는 어려움에 기반하여 인가되지 않은 리더가 태그의 내용을 읽어내는 것을 방지하는 방법이다. 하지만 이 방법은 metaID가 ID 대신 여전히 식별자의 역할을 수행하기 때문에 사용자가 추적될 수 있는 문제를 완벽하게 해결하지 못한다.

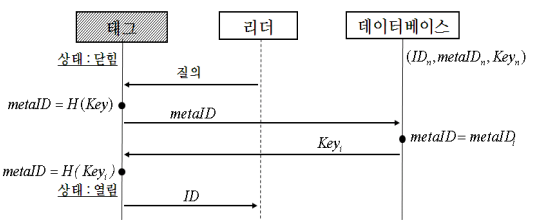

그림 2. 해쉬 락 프로토콜

3.2 랜덤 해쉬 락 프로토콜

S. Weis et al.은 해쉬 락이 metaID에 대한 불법적인 추적이 가능함을 발견하고 이를 보완 하기 위한 방

법으로 랜덤 해쉬 락 프로토콜[19]을 제안 하였다. 이는 리더의 질의 시에 난수 R을 전송시킴으로써 metaID가 아닌 매번 바뀌는 해쉬 값을 통해 태그의 식별이 가능하도록 하는 기술이다. 랜덤 해쉬 락 프로토콜의 인증 절차는 그림 3과 같다.

리더는 태그 식별을 위해 데이터베이스에 있는 모든 ID를 가져와서 자신의 난수 R과 해쉬 값을 비교해 봄으로써 태그의 ID를 알아낸다. 리더는 알아낸 태그의 ID를 태그에 전송함으로써 태그의 상태를 열림으로 변경시키고 진짜 식별자를 통해 태그에 접근한다. 하지만 데이터베이스의 모든 ID리스트를 가지고 와서 연산을 하므로 리더의 연산량 집중 문제가 있다.

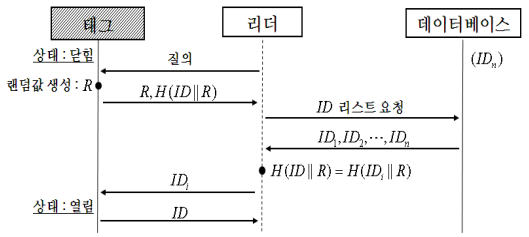

그림 3. 랜덤 해쉬 락 프로토콜

3.3 MW 프로토콜

Molnar et al.은 태그와 리더의 식별이 동시에 가능한 인증 프로토콜을 제안 하였다[7]. MW 프로토콜의 인증 절차는 그림 4와 같다.

리더는 질의 전 자신이 생성한 랜덤 값 R_1을 통해 태그에게 질의를 던진다. 태그는 리더의 질의에 대해 자신이 생성한 랜덤 값 R_2와 ID, R_1을 조합한 σ를 응답한다. 태그의 ID를 인증한 리더는 다시 ID, R_1, R_2를 조합한 τ를 태그에게 전송함으로써 상호 인증을 제공한다.

하지만 이 기술 또한 데이터베이스로부터 받은 ID와 키를 찾는 과정에서 데이터베이스 리스트 전체에 해당하는 연산을 리더에서 해야 한다는 단점이 있다.

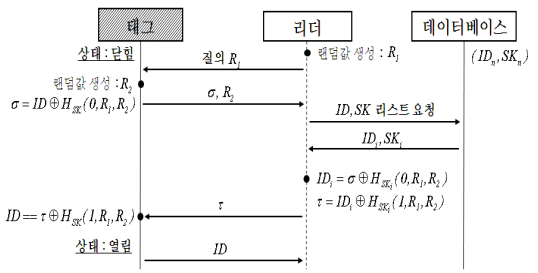

그림 4. MW 프로토콜

위에서 제안된 RFID 인증 프로토콜은 보안 요구사항에 대해서 일부 만족하거나 그렇지 않다. 그리고 성능 요구사항에 대해서는 모두 만족하지 않는다. 이는 제안한 프로토콜의 구성 중 태그의 기능이 별도의 프로세스가 탑재 되어야만 구현할 수 있는 기능이기 때문에 경량화 요구사항을 만족하지 않는다.

Ⅳ. 제안 인증 프로토콜 설계

본 장에서는 해쉬 함수와 XOR 연산만을 활용한 경량 인증 프로토콜을 제안하고, 제안 프로토콜의 안전성과 효율성을 분석한다.

4.1 제안 프로토콜

본 논문에서 사용되는 표기법은 표 1과 같다.

제안 프로토콜은 시스템 초기화 단계와 인증 단계로 구성된다.

표 1. 표기법

표기법	설명
⊕	비트 XOR (exclusive-or)
H	해쉬 함수(Keyed-hash Function)
a	태그에 저장된 ID, 키와 해쉬 값을 XOR한 값
β	DB에서 ID, 키와 해쉬 값을 XOR한 값
Key	태그의 상태 변화를 위한 패스워드 값
SK	DB와 모바일 리더가 공유하는 비밀키 값
ID_{reader}	모바일 리더에 해당하는 ID
ID_{tag}	태그에 해당하는 ID
R_1	모바일 리더가 생성하는 랜덤 값
R_2	데이터베이스가 생성하는 랜덤 값

4.1.1 초기화 단계

초기화 단계에서 태그와 데이터베이스는 ID, α 그리고 키를 저장하고 모바일 리더는 데이터베이스와 인증에 사용할 자신의 ID_{reader}와 SK를 저장한다. 초기화 단계에서 각각의 구성 요소에 저장되는 값은 다음과 같다.

- 데이터베이스: 등록된 모바일 리더에 해당하는 ID_{reader}와 공유할 비밀키 값 SK를 저장한다. 그리고 태그에 대한 ID_{tag}를 획득 후 생성한 키를 저장한 후 등록된 리더로부터 연산된 α를 저장한다.
- 모바일 RFID 리더: 정식으로 데이터베이스에 등록

된 리더는 ID_{reader}와 데이터베이스와의 연산에 사용될 SK를 저장하고 있다. SK는 DB와 모바일 리더가 공유하는 해쉬 함수에 사용하는 비밀키 값이다.

- 태그: 최초의 태그는 순수한 ID만 가지고 있지만 데이터베이스에 등록되면 α 값으로 대체된다. α 값은 인증단계 마다 변경된다. 그리고 수동형 태그의 쓰기 방지 기능을 위하여 키를 가진다.

4.1.2 인증 단계

태그 정보를 인증하기 위한 프로세스는 그림 5와 같다.

단계 1: 모바일 리더가 태그에게 질의를 하면 태그는 사전에 저장된 α 값을 전송한다.

단계 2: α 값을 받은 모바일 리더는 가지고 있는 SK를 사용하여 자신이 생성한 랜덤값 R_1을 해쉬하여 α 값과 XOR 연산한 α' 값을 ID_{reader}, R_1과 함께 보낸다. 데이터베이스는 받은 ID_{reader}가 자신에게 등록되어 있는 리더인지 확인 후 절차를 진행할지 판단한다. ID_{reader}가 확인된다면 그와 쌍을 이루는 SK를 선택한다. 만약 등록되어 있는 모바일 리더라면 보내온 R1 값을 모바일 리더와 공유하고 있는 SK 값으로 해쉬하여 나온 값으로 α'를 XOR 연산하여 원래의 α 값을 구하여 자신이 가진 값이 맞는지 ID_{tag}를 검증한다. 정상적인 태그임이 검증되면 데이터베이스는 난수값 R_2를 생성하여 모바일 리더의 SK를 사용하여 해쉬한 값을 원래의 ID_{tag} 그리고 키를 연접한 값과 XOR 연산한 값 β 를 생성한다. 이렇게 생성된 R_2, β 값은 다시 모바일 리더에게 보내진다.

단계 3: 모바일 리더는 전달받은 R_2, β 값을 가지고 R_2 값은 자신의 SK를 사용하여 해쉬한 값으로 β 와 XOR 연산을 하여 ID_{tag}와 키를 연접한 값을 구한다. 모바일 리더는 태그의 저장 값 변경을 위해 키를 사용한 질의를 통해 데이터베이스가 생성해서 보내준 β 값으로 업데이트를 해주고 인증단계를 마친다.

4.2 제안 프로토콜의 안전성과 효율성 분석

본 장에서는 제안 프로토콜에 대한 안전성과 효율성에 대해 논의한다.

4.2.1 안전성 분석

제안 프로토콜은 2.2.1 절에서 정의한 보안 요구사항을 다음과 같이 만족시킨다.

- 태그 보호: 공격자는 키를 알지 못하기에 수동형 태그를 임의로 수정할 수 없으며 읽어온 값이 직접적으로 태그의 ID에 해당하는 정보가 아니므로 이를 만족한다. 또한 이렇게 읽어온 값 α를 알더라도 정식으로 등록 되어진 모바일 리더가 아니라면 인증을 시도해도 성공 할 수 없으므로 해당 보안 요구사항을 만족한다.

$$\alpha^k = \alpha' \oplus H_{SK}(R_1^i)$$

태그에 저장된 값 α는 이전 인증 단계에서의 저장 값이며, 인증 단계마다 매번 업데이트 되며, 이 인증 값을 도청자가 알게 된다고 해도 실제 ID를 구할 수 없다. 이는 α 값은 인증 단계마다 생성된 랜덤 값을 선택하여 SK를 사용한 해쉬 값을 이용하므로 랜덤 값을 알게 되더라도 SK를 알지 못하면 똑같은 해쉬 값을 구할 수 없으며 이렇게 생성된 값을 가지고 ID 와 XOR 연산을 하여 생성한 값이 α 이므로 매번 알 수 없는 값으로 변경되어 숨겨져 있는 ID 값을 구하지

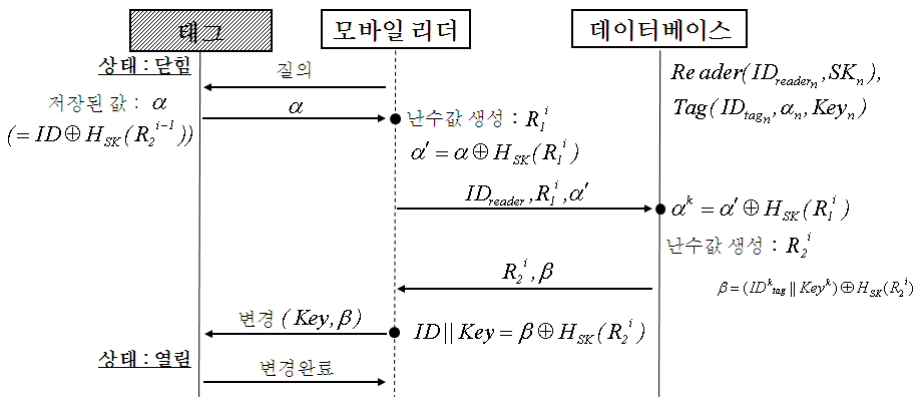

그림 5. 제안 프로토콜

못한다.

- 위치 추적 방지: 태그의 데이터는 인증 과정마다 바뀌므로 태그와 리더 사이의 문제점이 없어지며 리더와 네트워크 사이는 무선망이더라도 난수 발생기와 해쉬 함수를 사용하여 매번 다른 추적 불가능한 값이 존재 하므로 해당 보안 요구사항을 만족한다.

$$\beta = (ID_{tag} \parallel Key) \oplus H_{SK}(R_2^{\,i})$$

$$ID_{reader}, R_1, R_2, \alpha', \beta$$

태그로부터 읽어온 값을 모바일 리더는 추적 방지를 위해 자신이 생성한 랜덤 값 R_1을 해쉬한 값과 태그로부터 읽어온 α 값으로 XOR한 값 α'을 전송하므로 매번 전송 시 마다 다른 값이 전송되어 추적 문제를 해결한다. 데이터베이스 역시 자신이 생성한 R_2을 사용한 랜덤한 해쉬 값 β 를 전송하므로 태그에 저장된 값 α를 알고 있다고 해도 추적 문제가 발생하지 않는다.

- 트래픽 분석 방지: 공격자가 전 세션의 데이터를 수집한다고 해도 모바일 리더와 데이터베이스가 공유하는 SK 값을 알지 못한다면 제안 하는 인증 프로토콜을 분석하여 정당하게 인증 받는 것은 불가능하므로 해당 보안 요구사항을 만족한다.

$$ID_{reader}, R_1, R_2, \alpha', \beta$$

모바일 리더와 데이터베이스 구간에 공개 되는 ID_{reader}, R_1, R_2, α', β 값을 도청자가 모두 획득 한다고 해도 ID, 키와 XOR 된 해쉬 값을 구할 수 없으므로 불법적인 인증을 시도할 수 없다. 사용한 해쉬 함수는 SK를 사용하므로 모바일 단말기와 데이터베이스가 공유하는 SK를 가진 정당한 리더가 아니라면 인증을 시도 할 수 없다. 한 예로 모바일 리더가 보내는 값 ID_{reader}, R_1, α'을 저장해 뒀다가 다시 데이터베이스에 보내더라도 데이터베이스가 생성해서 보내는 R_2, β 값을 풀 수 있는 SK가 존재 하지 않기 때문에 도청자는 ID와 키를 구할 수 없다.

이전에 제안된 프로토콜들과의 기능 비교는 표 2에서 볼 수 있듯이 제안 프로토콜은 보안 요구사항과 성능 요구사항을 모두 만족하고 있다. 해쉬락 프로토콜은 태그 보호 기능만을 만족하며, 랜덤 해쉬 락 프로토콜은 태그보호와 위치 추적 방지 기능 만을 만족한다. MW 프로토콜의 경우 보안 요구사항은 만족하지만 경량화 요구사항은 만족하지 않는 반면, 제안 프로토콜은 모든 기능을 만족함을 알 수 있다. 경량화 관련 성능 요구사항 분석은 다음 절에서 상세히 설명하도록 한다.

표 2. 기능 비교표

프로토콜		해쉬락	랜덤 해쉬락	MW	제안
모바일 RFID 요구사항	태그 보호	O	O	O	O
	위치 추적 방지	X	O	O	O
	트래픽 분석 방지	X	X	O	O
	경량화	X	X	X	O

해쉬 함수 및 난수 발생기를 사용하는 제안 프로토콜에서 해쉬 함수에 비밀 값 SK와 함께 입력된 R1 값을 사용 하므로 R1 값을 안다고 하더라도 해쉬 함수에 사용된 비밀 값 SK를 알지 못하므로 똑같은 해쉬 값을 구할 수 없다.

제안 프로토콜의 안전성 검증을 위한 사용된 해쉬 함수의 안전성 증명은 XOR 된 해쉬 값을 구하기 위한 계산량에 의존한다. 해쉬 함수의 공격에서 가장 확률이 높은 공격은 충돌 공격이므로 이를 확인해 보면, 해쉬 함수를 공격자가 충돌 공격을 수행하려 한다면 충돌 알고리즘에서 $2^{160}/2=2^{80}$번의 점검을 해야 한다. 공격자가 초당 2^{30}번의 연산을 할수 있다고 하더라도 충돌 공격을 성공하려면 2^{50}초(약 1만년)가 걸린다. 그리고 난수 발생기는 1024비트의 랜덤 값을 생성하며, 각각의 SK가 다른 모바일 단말에서의 랜덤 값이므로 하나의 모바일 리더가 생성하는 랜덤 값을 가지고 해쉬 된 값을 구할 수는 없다. 반대로 다른 두 리더가 똑같은 랜덤 값을 사용하더라도 사용하는 각각의 모바일 단말이 가지는 SK가 다르므로 숨겨진 인증 정보를 구할 수 없다.

4.2.2 효율성 분석

본 절에서는 2.3.2 절에서 정의한 성능 요구사항과 기존에 제안된 인증 프로토콜들과의 비교를 통하여 제안 프로토콜의 효율성에 대해 살펴 본다.

- 경량화: 우선 기존에 제안된 인증 프로토콜은 수동형 태그가 아닌 능동형 태그에 대한 프로토콜이므로 제안 프로토콜에 비해 태그에 대한 제약이 많다. 랜

덤 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 프로토콜들은 모두 경량화를 만족하지 않는다. 하지만 제안하는 프로토콜은 표 3에서 볼 수 있듯이 데이터베이스에 저장해야 하는 공간은 모바일 단말의 ID와 SK, 태그의 ID, 키와 임의로 저장된 α 값으로 인해 많은 편이지만, 수동형 태그를 사용하며 태그가 수행해야 할 연산들을 모바일 단말이 처리 해 주면서 모바일 보안 요구사항 및 성능 요구사항을 만족하고 있다. 계산량 역시 랜덤 해쉬 락 프로토콜이나 MW 프로토콜은 데이터베이스의 ID 리스트를 전수 조사 해야 하지만 제안 프로토콜은 계산량이 고정되어 있어 성능면에서 좋은 효율을 보여주고 있다. 통신량은 태그-리더 구간, 리더-데이터베이스 구간으로 나눠지며 랜덤 해쉬 락 프로토콜은 리더-데이터베이스 구간에서의 통신량이 고정되지 않는데 이는 모바일 RFID 리더가 판별해야 하는 ID 값이 다를 경우 매번 데이터베이스에 새로운 리스트를 요청해야 하기 때문이다. MW 프로토콜은 리더-데이터베이스 구간의 통신량이 고정적이지만 데이터베이스에서의 계산량이 리더와 공유하는 SK를 찾는 과정에서 많이 요구 된다. 하지만 제안하는 프로토콜은 고정된 통신량만을 필요로 하므로 다른 프로토콜에 비해 효율적이다.

메모리 사용량에서 데이터베이스에 저장해야 하는 저장량을 비교하면 변형된 랜덤 해쉬 락 프로토콜은 n개의 태그 ID에 해당하는 정보와 태그 상태변화에 사용할 패스워드 k로 인해, nlog(t) + nlog(k) = nlog(tk)의 저장량을 필요로 하며, 변형된 MW 프로토콜은 n개의 태그 ID에 대한 정보와 태그의 상태변화에 사용할 패스워드 k, 태그에 저장된 식별값 확인을 위한 h, 그리고 데이터베이스와 모바일 리더 간에 공유되는 비밀키 s를 저장해야 하므로 nlog(t) + nlog(k) + nlog(h) + mlog(s) = mlog(s) + nlog(tkh)만큼의 저장량을 필요로 한다.

제안 프로토콜은 n개의 태그 ID에 대한 정보와 태그의 패스워드 k 그리고 해쉬값 h를 저장해야 하며, 통신할 인가된 모바일 리더 m개로 구성된 리더 식별값 ID_{reader}와 공유할 비밀키 s를 저장해야 한다. 이는 nlog(t) + nlog(k) + nlog(h) = nlog(tkh)와 같은 태그에 대한 정보와 추가적으로 mlog(u) + mlog(s) = mlog(us)인 모바일에 대한 정보를 저장해야 함을 나타내므로 상대적으로 비교된 프로토콜들 보다 사용하는 메모리는 많다.

계산량은 리더와 데이터베이스 두 영역으로 나눠지며 변형된 랜덤 해쉬 락 프로토콜은 데이터베이스에서의 계산량은 없지만 모바일 RFID 리더에서의 계산량은 (n/2+1)h+r로 데이터베이스로부터 받아오는 전체 n개의 태그 리스트 중 올바른 식별 값을 찾기 까지의 해쉬 계산량과 추가적으로 해쉬 함수 1회, 난수 발생 1회를 고정적으로 수행한다. 변형된 MW 프로토콜은 모바일 RFID 리더에서 3h+r의 고정된 계산량을 가지고 이는 해쉬 함수 3회, 난수 발생기 1회에 해당한다. 그리고 데이터베이스에서의 계산량은 (n/2+2)h+r로 저장된 태그 n개중 하나의 태그를 식별하기 위한 해쉬 계산량과 해쉬 연산 2회, 난수 발생 1회의 추가적인 연산을 수행한다. 하지만 제안 프로토콜은 모바일 RFID 리더와 데이터베이스의 연산량이 각각 2h+r 만큼의 연산인 해쉬 연산 2회, 난수 발생 1회를 수행하면 되므로 비교된 프로토콜에 비해 계산량이 적다.

통신량은 태그와 리더 사이의 통신량과 리더와 데이터베이스 사이의 통신량으로 구분된다. 우선 태그와 리더 사이의 통신량은 비교된 표와 마찬가지로 세 프로토콜 모두 통신량이 같다. 하지만 리더와 데이터베이스 사이의 통신량에서 변형된 랜덤 해쉬 락 프로토콜은 전체 태그 개수 n에 대한 식별 값 t의 통신량과

표 3. 성능 비교표

프로토콜		변경된 랜덤 해쉬락	변경된 MW	제안
메모리 (bit)	태그	$\log(kh)$	$\log(kh)$	$\log(kh)$
	리더	$\log(tkh^2r)$	$\log(tkh^2r^2s)$	$\log(tkh^2rs)$
	DB	$n\log(tk)$	$n\log(tkhs)$	$m\log(us)+n\log(tkh)$
계산량	리더	$(n/2+1)h+r$	$3h+r$	$2h+r$
	DB	-	$(n/2+2)h+r$	$2h+r$
통신량 (bit)	태그-리더	$\log(kh^2)$	$\log(kh^2)$	$\log(kh^2)$
	리더-DB	$(n/2+1)\log t+\log(rk)$	$\log(h^3r^2)$	$\log(uh^2r^2)$

난수값 r과 태그 상태제어를 위한 패스워드 k를 전달함으로서 (n/2+1)log(t)+log(rk)로 다른 프로토콜들에 비해 많은 통신량을 가진다. 변형된 MW 프로토콜은 해쉬값 h의 3회 전송과 난수값 r의 2회 전달로 log(h3r2)의 통신량을 가진다. 제안 프로토콜은 모바일 RFID 리더의 식별 값에 해당하는 u와 해쉬 값 h의 2회 전송과 난수값 r의 2회 전송으로 전체 log(uh2r2)의 통신량을 가진다. 여기서 리더 식별자 u는 64 비트의 크기를 가지며 해쉬값 h는 160 비트의 크기를 가지므로 비교된 프로토콜들 보다 적은 통신량을 가진다.

V. 제안 시스템 구현 및 성능 평가

본 장에서는 4장에서 비교한 안전성과 효율성을 바탕으로 제안 프로토콜을 실제 스마트폰에 구현하여 성능을 평가하고 결과를 기술한다.

5.1 제안 시스템 구현

본 절은 모바일 RFID 인증 프로토콜의 구현을 위해 제안 시스템 설계와 구현 환경에서는 인증 프로토콜에 사용되는 장치 및 재원에 해당하는 내용을 구현 내용에서는 장치 제어를 위한 내용으로 구성 된다.

5.1.1 제안 시스템 구성

구현을 위한 재원 및 디바이스는 태그, 모바일용 RF 리더, 모바일 기기, 데이터베이스로 그림 6과 같이 구성되며 각각의 구성이 가지는 기능은 다음과 같다.

- 태그: 모바일 리더로부터 주어지는 인증에 대한 α 값을 저장할 수 있는 공간과 ID에 해당하는 정보를 저장할 공간 그리고 메모리 쓰기 방지 기능이 제공되어야 한다. 제안 시스템에서 사용할 태그의 저장 공간은 ID에 해당하는 12바이트 공간은 Bank 01에 해당하는 EPC 공간을 사용하고, 해쉬 값에 해당하는 40byte는 Bank 11에 해당하는 User공간을 사용한다. 이러한 기능은 EPC Class-1 Gen-2 태그에서 제공하는 기능으로 만족하므로 수동형 태그를 사용한다[10].
- 모바일 RFID 리더: 태그가 저장하고 있는 저장값에 대한 읽기 기능과 인증 과정에서 생성되는 인증 값을 태그에 저장하기 위한 질의 기능이 제공 되어야 하고 데이터베이스와의 통신 구간에서 사용할 인증 절차에 사용되는 인증정보를 숨기기 위해 난수 발생기와 키를 사용한 해쉬 함수 기능이 구현되어야 한다. 그리고 데이터베이스로 정보를 전송하기 위해 통신 프로토콜을 사용한다.
- 데이터베이스: 모바일 RFID 리더로부터 전송되어 오는 정보 처리를 하기 위해 태그에 대한 ID에 대한 값과 인증 절차 마다 업데이트 되는 정보 α와 인증에 사용되는 모바일 RFID 리더와 공유하는 SK를 가진다. 공유하는 SK로 모바일 RFID 리더와 데이터베이스 사이에 전달되는 인증 정보를 감춰 주기 위해 난수 발생기로 생성한 난수값을 해쉬 함수의 입력 값으로 사용하여 나온 값을 인증 값과 XOR 하게 된다. 위 절차를 수행하기 위한 기능은 난수 발생기와 해쉬 함수 그리고 값을 저장하기 위한 데이터 관리 테이블을 가진다.

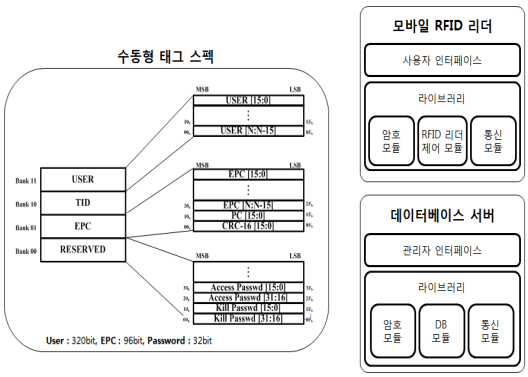

그림 6. 제안 시스템 구성

5.1.2 구현 환경

우선적으로 실험을 위한 재원은 데이터베이스 서버 역할을 할 데스크탑 1대, 모바일용 RF 리더제품은 Nesslab의 900Mhz UHF 모바일용 RF 리더[20]를 사용했다. 모바일용 RF 리더를 제어할 코드가 올라갈 스마트 폰은 삼성 SCH-490 모델을 사용했다. 스마트 폰 스펙은 CPU는 Marvall Monahans PXA 312 806Mhz가 사용되며, 시각적 제어를 위한 LCD 사이즈는 3.3 Inch 이다. 또한 무선 접속을 위한 Wi-Fi 기능이 제공되며, 내부 저장공간은 160MB를 제공한다. 모바일 OS는 Windows Mobile 6.1.4를 지원하므로 개발 PC에서는 해당 SDK를 받아 설치하여 구현 하였다. 사용할 태그는 EPC Class-1 Gen-2 프로토콜 표준을 만족하는 Power-ID 사의 Empowering RFID 제품군중 Power G2 제품을 사용하였다. 사용한 수동형 태그의 저장 공간은 96 비트 EPC 공간과 720 비트 User 메모리 공간과 64 비트 태그 ID 공간을 가지며, 각각 32 비트 접근 키 및 킬 패스워드 공간을 가진다. 인증 프로토콜을 개발하기 위해 각각 구현한 모듈은 아래와 같다.

- 암호 모듈: OpenSSL에서 제공하는 라이브러리를 가지고 모바일 RFID 리더와 데이터베이스가 사용할 암호 함수 구현하였다. 난수 발생기는 매번 통신 과정에서 변경되어야 하므로 1024비트의 길이를 가지는 난수를 발생하도록 구현하였다. 이렇게 생성한 난수값을 해쉬 하는데 사용하는 해쉬함수는 SHA-1을 사용하며 공유할 SK를 사용하여 같은 입력 값이라면 똑같은 해쉬 값을 생성할 수 있다.
- RFID 리더 제어 모듈: 태그의 값 저장 및 읽기 기능을 위해 태그에게 질의하고 태그의 정보를 해석할 수 있는 모바일용 RF 리더를 제어하기 위해 제어코드를 구현하였다. 구현한 제어코드에는 태그의 각 저장 공간을 선택적으로 읽을 수 있는 명령을 지원하며 EPC Class-1 Gen-2 표준에서 지원하는 그림 7과 같은 저장 공간의 Lock 기능을 제공한다. 이를 활용하여 데이터베이스에서는 키를 생성하고 이를 전달 받은 모바일 RFID 리더는 태그의 저장공간에 키를 저장 후 Lock 시켜둔다. 한번 Lock 상태가 된 태그는 상태 변화 코드가 들어오기 전까지는 항상 키를 사용한 쓰기를 시도해야 한다. 즉 읽을 수는 있지만 그 값을 변화시키는 것은 키를 알기 전까지 불가능 하게 된다. 그리고 인증 과정 중에 업데이트 값 생성시 해당 값을 선택 영역에 쓰는 기능을 제공한다.
- 통신 모듈: 태그로부터 읽어온 정보나 제공할 정보를 받기 위해 모바일 RFID 리더는 TCP/IP 소켓 통신을 하게 된다. 모바일 RFID 리더는 Wi-Fi를 사용한 무선 액세스 망에 접속하여 데이터베이스에게 정보를 전달하게 되고, 데이터베이스는 역으로 무선 액세스 망에서 Wi-Fi로 연결되어 있는 모바일 RFID 리더에게 정보를 전달하게 된다. 소켓 통신 과정에는 패킷 타입과 인증 단계를 식별할 수 있는 정보가 포함되어 전달된다.
- 데이터베이스 모듈: ODBC(Open Database Connectivity)를 사용하여 관리할 데이터베이스에 연결, 검색, 저장, 업데이트등의 데이터 처리를 지원한다. 태그 정보에 대한 식별 값 유무 판단과 모바일 RFID 리더가 등록된 리더인지 등록되어 있다면 공유할 SK는 어떤 것인가를 판단 할 수 있도록 지원한다. 추가적인 정보로 태그에 대한 현재 식별 값을 저장해 두었다가 인증 단계마다 모바일 RFID 리더로부터 넘어온 정보가 현재 가지고 있는 정보와 같은지 비교 판단한다.

Figure 6.24 – *Lock* payload and usage

그림 7. 락 페이로드와 사용법

실제 구현에서의 제안 프로토콜 초기화 단계는 그림 8과 같다.

원래의 태그 ID를 데이터베이스에 전달하면 데이터베이스는 태그의 키와 저장값 α를 전해 주게 된다. 이 정보를 태그에 성공적으로 업데이트 하면 데이터베이스는 인증단계를 수행할 준비를 마치게 된다.

그림 9의 인증 단계는 태그에 저장된 α 값을 읽어서 모바일 RFID 리더에서 새로운 값 α'으로 변경 후 인증을 시도한다. 데이터베이스에서는 모바일 리더와 공유하고 있는 비밀키 값 SK를 사용하여 자신이 저장하고 있는 태그에 저장된 α 값을 확인하면, 다시 β 로 ID와 키 정보를 모바일 리더에 제공하게 되며 모바일 리더에서 식별값을 확인한 다음 태그에 새로운 값 β를 저장 후 인증 단계를 마치게 된다.

위에서 구현한 모듈을 가지고 서버에는 휴대용 단말과 통신을 위한 통신 모듈과 휴대용 단말과 서버 사이에서 통신하는 내용의 암호화 및 비식별을 위한 암호 모듈을 사용한다.

그리고 현재 태그 상태에 해당하는 인증값을 식별하기 위한 데이터베이스 모듈을 사용한다. 클라이언트

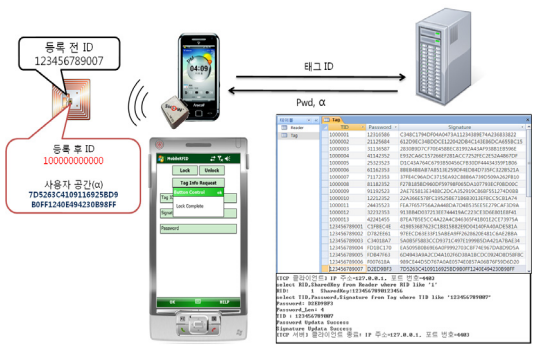

그림 8. 구현 프로토콜 초기화 단계

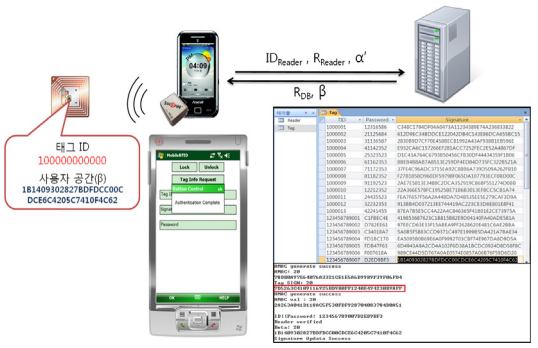

그림 9. 구현 프로토콜 인증 단계

는 휴대용 단말에 해당되며 실제 데스크톱 환경에서 구현해서 확인한 코드를 모바일 버전으로 변경하여 탑재한다. 서버와의 통신을 위한 통신 모듈을 사용하고 보내는 인증 정보의 암호화 및 비식별을 위해 암호 모듈을 사용한다. 휴대용 단말에는 태그 질의 및 상태 제어를 위한 RF 리더가 탑재 되며 이를 제어하기 위한 RFID 리더 제어 모듈을 사용한다.

5.2 성능 평가

제안 하는 인증 프로토콜과 이전 인증 프로토콜들의 효율성을 분석하기 위해 모바일 RFID 환경에 맞게 변경해 보았다. 각각의 프로토콜은 초기화 단계와 인증 단계로 2 단계로 이루어 진다. 초기화 단계는 순수한 상태의 태그의 정보를 취득하고 태그가 가지고 있는 정보를 변경하거나 혹은 다른 추가 적인 값을 저장하는 단계로서 인증 프로토콜 절차를 거치기 위한 인증 정보를 저장하는 단계로 볼 수 있다. 인증 단계는 태그의 상태가 변화되어 있고 그에 해당 하는 인증 정보를 가져와서 실제로 인증을 하는 단계이다.

태그로부터 획득한 인증 정보를 가지고 모바일 리더는 데이터베이스에 인증 정보를 암호화 및 비식별 값으로 변경 후 전송한다. 그리고 서버는 인증 정보를 확인하기 위해 복호화 및 식별 가능한 값으로 변경 하게 된다. 그리고 자신이 확인 할수 있는 인증 정보가 제대로 보내어 졌다면 인증을 마치고 제공하거나 다시 한번 암호화하여 데이터를 보내게 된다. 이를 확인한 모바일 리더는 인증이 이루어 졌음을 데이터를 통해 확인하거나 어떤 응답에 대해 확인하게 된다.

모바일 RFID 시스템에서는 이전에 태그에서 이루어 져야 했던 연산들을 모바일 단말에서 처리해줌으로써 태그에 별도의 추가 기능 구현이 없고 태그는 EPC Class-1 Gen-2 표준만 만족하는 태그이면 가능하다. 그러므로 성능평가에서 고려되지 않는 항목은 태그와 RF 리더가 주고 받는 통신량이 크거나 저장량이 태그 용량을 수용하지 못한다면 성능평가 항목에서 제외한다. 성능평가에서 주목할 점은 태그에 모바일 RF 리더가 질의를 할때에는 어떠한 정보 제공을 필요로 하거나, 데이터베이스의 요청에 의해서 혹은 데이터베이스로부터 받은 값을 정확하게 검증했으며 저장 값을 업데이트 시에 질의를 하게 된다. 즉 태그의 현재 값 확인 단계 후와 확인 후 태그에 대한 업데이트 단계 전 까지의 모바일 RFID 리더의 인증 수행 과정을 비교하도록 한다.

이전 인증 프로토콜의 모바일 RFID 시스템에 맞게 변경한 내용은 우선적으로 능동형 RFID 태그의 연산을 휴대용 단말에서 수행하도록 하여 태그의 연산량을 제거하였다. 태그는 단순히 읽기, 쓰기 그리고 상태변화와 같은 Lock 기능만을 수행한다. 성능평가에서 해쉬 락 프로토콜은 태그 보호에 해당하는 보안 요구사항 만을 만족하므로 비교 대상에서 제외하였다.

지금부터 설명할 메모리 사용량과 통신량 그리고 인증 처리 시간 비교 그래프는 표 3을 참고하여 작성하였다. 성능 비교 내용은 다음과 같다.

각 프로토콜 별 메모리 사용량에 대한 내용을 비교 그래프로 표현한다. 제안 프로토콜은 다른 프로토콜들에 비해 추가적으로 저장해야 하는 IDreader, SK와 같은 추가적인 데이터가 필요하며, 그래프에서 보여주는 제안 프로토콜의 저장량은 X축의 태그 개수 n에 비례하며, IDreader, SK와 같은 데이터는 1천 만개 정도의 모바일 RFID 리더가 등록 되어있다고 가정하였다. 여기서 메모리 사용량은 각 구성별로 나누어 그래프로 표현하였다.

모바일 RFID 리더의 메모리 사용량에 대한 그래프 그림 10은 태그의 개수 n에 상관없이 고정된 메모리 사용량을 보이며 변형된 MW 프로토콜이 메모리 사용량이 가장 많았으며 그다음으로 제안 프로토콜, 가장 적은 메모리 사용량을 가진 프로토콜은 랜덤 해쉬

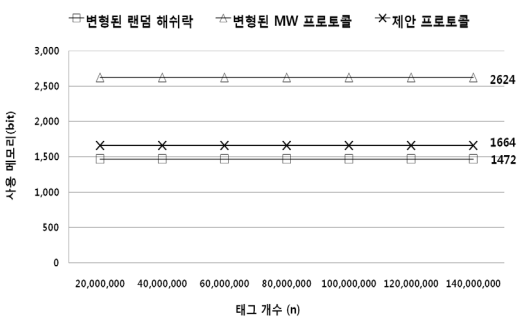

그림 10. 메모리 사용량 비교(모바일 RFID 리더)

락 프로토콜이다. 그림 11을 보면 데이터베이스에서는 추가적인 저장량이 필요한 제안 프로토콜이 5GB 정도의 가장 많은 메모리 사용량을 가졌으며, 변형된 MW 프로토콜과는 아주 근소한 메모리 사용량의 차이를 보인다.

1억 4천개 정도의 태그를 저장하기 위한 제안 프로토콜의 저장량은 약 5GB 정도이며, 변형된 MW 프로토콜 역시 약 5GB, 랜덤 해쉬 락 프로토콜은 약 2GB 정도의 저장량을 필요로 하는 것을 볼 수 있다.

통신량에 대한 비교 그래프는 태그와 모바일 리더 구간, 모바일 리더와 데이터베이스 구간으로 표현하였다. 각 프로토콜의 통신량은 제안 프로토콜과 큰 차이를 보이거나 거의 같음을 볼 수 있다. 태그와 모바일 리더사이의 통신량은 기존의 랜덤 해쉬 락 프로토콜과 MW 프로토콜과는 다르게 모바일 RFID 서비스에서의 경량화를 만족하게 변경하였으므로, 태그의 순수한 저장 공간만을 사용하게 되어 세 프로토콜이 모두 해쉬 함수 기반의 프로토콜이므로 제안 프로토콜과 같은 통신량을 가지는 것을 그림 12에서 확인 할 수 있다.

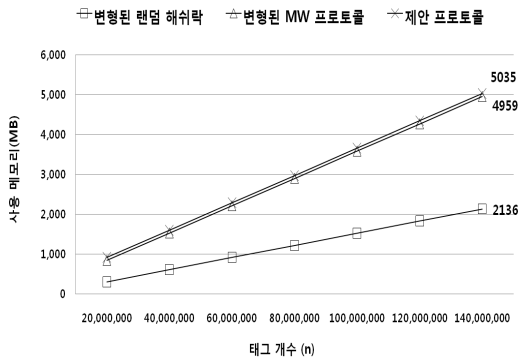

그림 11. 메모리 사용량 비교(DB 서버)

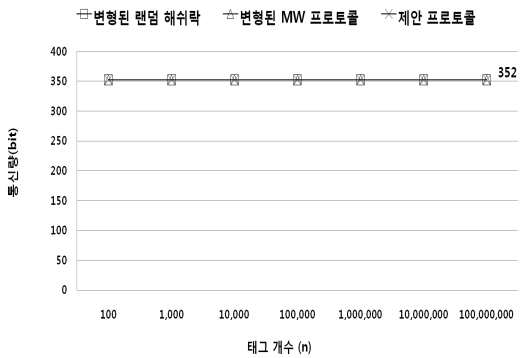

그림 12. 통신량 비교(태그-리더)

모바일 리더와 데이터베이스 사이에서의 통신량은 그림 13과 같이 1억 개의 태그를 저장하고 있는 데이터베이스를 사용시 변형된 MW 프로토콜은 2528 비트의 통신량을 필요로 하며, 변형된 랜덤 해쉬 락 프로토콜은 약 13,440 비트정도의 통신량을 필요로 한다. 그리고 제안 프로토콜은 2432 비트의 통신량만을 필요로 하며 비교 대상중에서 가장 적은 통신량을 가짐을 확인 할 수 있다.

그림 14는 각각의 인증 프로토콜에 대한 인증 수행 시간 비교를 위하여 해당 프로토콜을 모바일 RFID 시스템에서 사용할 수 있도록 변경 한 다음 구현한 내용을 바탕으로 인증 수행 시간을 비교한 그래프이다.

변형된 랜덤 해쉬 락 프로토콜과 변형된 MW 프로토콜은 태그 개수에 비례하여 많은 인증 수행 시간을 필요로 하는 것을 확인 할 수 있었으며 이는 데이터베이스에서 ID 리스트를 제공하던 변형된 랜덤 해쉬 락 프로토콜과 변형된 MW 프로토콜은 인증 값 확인 절차에서 데이터베이스에 존재하는 ID와 휴대용 단말과 데이터베이스가 공유하는 비밀키 SK 값을 검색하는 부분이 추가 되므로 추가적인 데이터베이스 검색 시

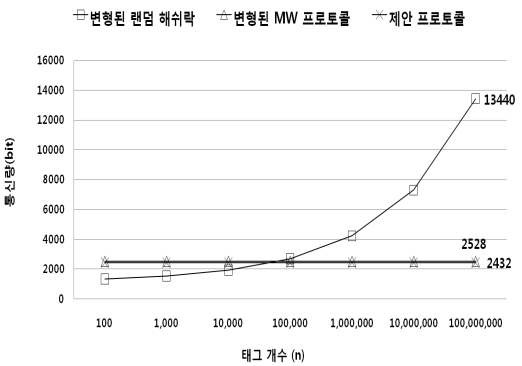

그림 13. 통신량 비교(리더-DB 서버)

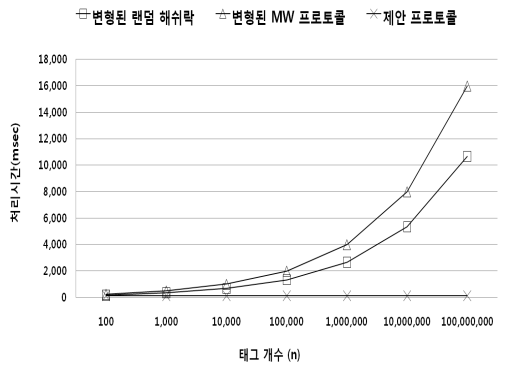

그림 14. 인증 시간 비교

간이 포함된다. 하지만 제안 프로토콜은 고정적인 인증 시간을 보여주고 있다.

제안 프로토콜은 데이터베이스의 메모리 사용량 측면에서 상대적으로 비효율적이지만, 통신량은 가장 적은 것을 확인 할 수 있었고, 또한 인증 처리 수행 시간은 항상 태그 개수와 상관없이 동일한 값을 가지는 것을 확인 할 수 있었다. 데이터베이스의 메모리 사용량이 상대적으로 많다고 하지만 태그 개수가 1억개 일 때 데이터베이스에 저장한다면 약 5GB 정도의 저장량이 필요하며 등록된 모바일 단말의 개수가 1천만대라고 해도 약 0.2GB 정도의 저장량을 필요로 하므로 총 5GB 정도의 저장량을 필요로 한다. 하지만 5GB 정도의 저장량은 현재의 데이터베이스 시스템 기술 수준에서는 문제가 되지 않는다. 그리고 연산량 역시 고정적이므로 데이터베이스에 대한 연산 문제 역시 큰 영향을 미치지 못 함을 알 수 있다.

Ⅵ. 결 론

모바일 RFID 시스템은 기존 고정형 RFID 시스템에 비해 사용자가 직접 태그 정보를 획득할 수 있어 편리한 정보 제공 기능을 가지고 있다. 하지만 휴대단말 자체가 RFID 리더기가 되어 RFID 무선 인식이 누구나 쉽게 할 수 있을 경우, RFID 네트워크 인프라 내에 위치하고 있는 태그 부착 제품의 정보 자체가 물품 소유자를 식별하고 소유자의 특성을 알아낼 수 있기 때문에 개인 프라이버시 침해 문제가 발생하게 된다. 따라서 태그 부착 제품을 사용자가 소유한 이후에도 계속적인 서비스가 필요한 경우에는 프라이버시 보호 기능을 제공해야 하며 이를 지원할 수 있는 보안 기능이 필요하다.

따라서, 본 논문에서는 모바일 단말의 연산능력을 최대한 활용하여 능동형 태그 뿐만 아니라 일반적인 50 센트 이내의 수동형 태그에도 적용가능한 모바일 RFID 인증 기술을 제안하였다. 제안 프로토콜은 경량화로 인한 효율성 측면에서 우수성 뿐만 아니라, 태그 보호, 위치추적 방지, 트래픽 분석 방지 등의 보안 요구사항을 모두 만족시킴을 보였다. 또한, 제안 프로토콜을 암호 라이브러리를 활용하여 구현하고 실제 스마트폰에 탑재하여 실용성 검증을 위한 실험을 실시하여 성능을 평가하였다.

제안 프로토콜은 기존 수동형 태그에 추가적인 기능을 요구하지 않으며, 해쉬 함수와 같은 암호 연산은 모바일 리더가 수행하도록 하였다. 단지, 제안 프로토콜은 데이터베이스에 저장 공간을 다른 프로토콜보다 많이 사용하는 단점이 있지만, 통신 오버헤드와 인증 처리시간 측면에서 다른 프로토콜들은 태그의 개수에 비례하는 반면에 제안 프로토콜은 항상 고정된 상수 값을 유지하므로 전체적인 성능이 매우 우수함을 보였다.

제안 프로토콜은 경량 프로토콜이므로 기존 저가의 수동형 태그에 적용가능하기 때문에, 기존의 대부분 RFID 인증 및 프라이버시 보호 서비스에 그대로 적용될 수 있을 것으로 기대된다.

참 고 문 헌

〔1〕 A. Juels, “Minimalist Cryptography for Low-cost RFID Tags,” *International Conference on Security in Communication Networks(SCN ’04)*, pp.149-164, September 2004.

〔2〕 A. Juels and R. Pappu, “Squealing Euros: Privacy Protection in RFID-Enabled Banknotes,” *Financial Cryptography(FC ’03)*, pp. 103-121, 2003

〔3〕 A. Juels, R. Rivest, and M. Szydlo, “The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy,” *ACM Conference on Computer and Communications Security (CCS ’03)*, pp.103-111, October 2003.

〔4〕 A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 2001.

〔5〕 B. Bing. *Broadband Wireless Access*, Boston, Kluwer Academic Publishers, 2000.

〔6〕 Boyeon Song, and Chris J Mitchell, ″RFID Authentication Protocol for Low-cost Tags,″ *ACM Conference on Wireless Network Security (WiSec’08)*, March, 2008.

〔7〕 D. Molnar and D. Wagner, “Privacy and Security in Library RFID: Issues, Practices, and Architectures,” *ACM Conference Commun. Comput. Security(CCS ’04)*, pp. 210-219, 2004.

〔8〕 D. Henrici, P. Muller, “Providing Security and Privacy in RFID Systems Using Triggered Hash Chains,” *IEEE International Conference on Pervasive Computing and Communications (PerCom’08)*, pp.50-59, 2008.

〔9〕 E. Fujisaki and T. Okamoto, “Secure Integration of Asymmetric and Symmetric Encryption

Schemes," *CRYPTO '99*, pp.537-554, 1999.
〔10〕 EPCglobal, "UHF Class-1 Generation-2 Standard v.1.2.0," 05, 2008.
〔11〕 G. Karjoth and P. Moskowitz, "Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced," *ACM workshop on Privacy in the electronic society '05*, pp.27-30, November 2005.
〔12〕 K. Osaka, T. Takagi, K. Yamazaki and O. Takahash, "An Efficient and Secure RFID Security Method with Ownership Transfer," *Computational Intelligence and Security*, pp. 1090-1095, 2006.
〔13〕 M. Ohkubo, K. Suzuki, and S. Kinoshita, "Efficient hash-chain based RFID privacy protection scheme," *International Conference on Ubiquitous Computing (Ubicomp '04)*, September 2004.
〔14〕 Ming Hour Yang and Jia-Ning Luo, "Authentication Protocol in Mobile RFID Network," International Conference on Systems, pp.108-113, 2009.
〔15〕 mClock: Personal / corporate management of wireless devices and technology, 2003. product description at www.mobileclock.com.
〔16〕 S. Garfinkel, "An RFID Bill of Rights, Technology Review," 2002, available at http://www.technologyreview.com/articles/garfinkel1002.asp
〔17〕 S. Inoue and H. Yasuura, "RFID Privacy using User-controllable Uniqueness," *RFID Privacy Workshop*, November 2003. http://www.rfidprivacy.org/papers/sozo_inoue.pdf.
〔18〕 S. Sarma, S. Weis, and D. Engels, "RFID Systems and Security and Privacy Implications," *Workshop on Cryptographic Hardware and Embedded Systems*, pp.454-470, 2002.
〔19〕 S. Weis, S. Sarma, R. Rivest, and D. Engels. "Security and Privacy Aspects of Low-Cost Radio Frequency Identication Systems," In *Security in Pervasive Computing*, pp.201-212, 2004.
〔20〕 UHF RFID Reader Dongle, http://www.nesslab.com/rfid_04_22.php

엄 태 양 (Taeyang Eom) 정회원

2008년 2월 영산대학교 컴퓨터공학과 학사
2008년 9월~2010년 8월 숭실대학교 컴퓨터학과 석사
<관심분야> 모바일 보안, 시스템 보안

이 정 현 (Jeong Hyun Yi) 종신회원

1993년 2월 숭실대학교 전자계산학과 학사
1995년 2월 숭실대학교 컴퓨터학과 석사
2005년 8월 University of California at Irvine, Computer Science 박사
1995년 2월~2001년 8월 한국전자통신연구원 연구원
2000년 4월~2001년 3월 미국 표준기술연구원(NIST) 객원연구원
2005년 10월~2008년 8월 삼성종합기술원 수석연구원
2008년 9월~현재 숭실대학교 컴퓨터학부 조교수
<관심분야> 모바일 보안, 네트워크 보안