情報保護學會論文誌
第20卷 第1號, 2010. 2

온라인 백-엔드-데이터베이스가 없는 안전한 RFID 상호 인증 프로토콜

원 태 연,[1†] 유 영 준,[1] 천 지 영,[1] 변 진 욱,[2] 이 동 훈[1‡]
[1]고려대학교, [2]평택대학교

Secure Mutual Authentication Protocol for RFID System without Online Back-End-Database

Tae Youn Won,[1†] Young Jun Yu,[1] Ji Young Chun,[1] Jin Wook Byun,[2] Dong Hoon Lee[1‡]
[1]Korea University, [2]Pyeongtaek University

요 약

RFID (Radio Frequency IDentification)는 유비쿼터스 환경에서 바코드를 대체하여 유용하게 사용될 하나의 차세대 자동식별 기술을 말한다. RFID 시스템은 기본적으로 태그(Tag)와 태그 인식을 위한 리더(Reader) 그리고 태그에 대한 정보를 저장하고 있는 백-엔드-데이터베이스(Back-End-Database)로 구성된다. 최근 휴대폰이나 PDA(Personal Digital Assistants)에 모바일 리더 기능을 장착한 모바일 리더를 이용한 RFID 서비스가 급증하고 있으나 이러한 환경에서 안전한 기법에 대한 연구는 아직까지 미흡하다. 기존에 존재하는 고정형 리더를 이용한 기법들을 모바일 리더를 이용한 환경에 적용하기에는 추가적으로 고려해야할 요소들이 존재한다. 모바일 리더 환경에서는 기기의 분실이 쉽고 또한 통신 장애 및 통신 범위 초과와 같은 이유로 백-엔드-데이터베이스와 항상 신뢰하여 연결될 수 없기 때문에 이러한 추가적인 문제들을 고려한 안전한 기법에 대한 연구가 필요하다. 이러한 문제를 해결하기 위해 최근 Han 등이 백-엔드-데이터베이스가 없는 환경에서 RFID 상호 인증 프로토콜을 제안하였다. 하지만 Han 등의 기법은 도청, 스푸핑, 재생 공격을 통한 태그 위치 추적이 가능하다. 또한 저가 기반의 수동형 태그에 부적절하게 많은 통신량을 요구한다. 따라서 본 논문에서는 Han 등의 기법의 취약성을 분석하고 안전성과 효율성 측면에서 향상된 온라인 백-엔드-데이터베이스가 없는 환경에서 RFID 상호 인증 프로토콜을 제안한다.

ABSTRACT

RFID is one of useful identification technology in ubiquitous environments which can be a replacement of bar code. RFID is basically consisted of tag, reader, which is for perception of the tag, and back-end-database for saving the information of tags. Although the usage of mobile readers in cellular phone or PDA increases, related studies are not enough to be secure for practical environments. There are many factors for using mobile readers, instead of static readers. In mobile reader environments, before constructing the secure protocol, we must consider these problems: 1) easy to lose the mobile reader, 2) hard to keep the connection with back-end-database because of communication obstacle, the limitation of communication range, and so on. To find the solution against those problems, Han et al. suggest RFID mutual authentication protocol without back-end-database environment. However Han et al.'s protocol is able to be traced tag location by using eavesdropping, spoofing, and replay attack. Passive tag based on low cost is required lots of communication unsuitably. Hence, we analyze some vulnerabilities of Han et al.'s protocol and suggest RFID mutual authentication protocol without online back-end-database in aspect of efficiency and security.

Keywords: RFID, Privacy, Security, Mutual authentication

접수일(2009년 9월 21일), 게재확정일(2009년 12월 31일)

† 주저자, kucs226@korea.ac.kr
‡ 교신저자, donghlee@korea.ac.kr

I. 서 론

RFID (Radio Frequency IDentification)는 유비쿼터스 환경에서 유용하게 사용될 하나의 차세대 자동식별 기술을 말한다. RFID 시스템은 기본적으로 태그(Tag)와 리더(Reader) 그리고 백-엔드-데이터베이스(Back-End-Database)로 구성된다. 태그는 사람, 동물 및 상품 등에 부착되며, 이들을 식별하기 위해서 고유한 정보(일반적으로 ID)를 칩(Chip)에 저장하고 있다. 리더는 라디오 주파수(RF Signals)를 이용하여 태그로부터 식별 정보를 수신하며, 수신한 식별 정보를 백-엔드-데이터베이스에 전송하는 역할을 한다. 백-엔드-데이터베이스는 사전에 태그와 관련된 모든 데이터를 저장하고 있으며, 리더로부터 수신한 태그의 식별 정보를 검증한다. 이러한 RFID는 바코드(Bar-Code) 기술과 비교하여 많은 장점을 가지고 있다. 바코드는 물체를 식별하기 위해 물리적인 접촉이 필요하며 개개의 물체를 일일이 식별해야 하기 때문에 오랜 시간이 걸린다. 반면 RFID는 라디오 주파수를 이용하여 모든 물체를 한꺼번에 인식할 수 있기 때문에 물리적인 접촉(line-of-Sight)이 필요 없다. 또한 바코드에 비하여 많은 정보를 칩에 저장할 수 있으며 쓰기도 가능하다. 따라서 이러한 장점들 때문에 RFID 기술은 바코드 기술을 대체하여 물류, 유통 및 교통 카드와 전자 여권까지 다양한 곳에서 활용되고 있다. RFID는 앞으로 센서 기술과의 융합을 통하여 차세대 기술로 활용될 것이다.

하지만 RFID는 무선 주파수를 이용한 태그와 리더간의 통신(Insecure Channel)으로 인해 RFID 보안 및 사용자의 프라이버시 침해라는 문제점을 야기한다[1]. 현재까지 이러한 문제점들을 해결하기 위해 많은 연구가 이루어지고 있다[2-12]. 이러한 연구는 대부분 고정형 리더(Static Reader)와 백-엔드-데이터베이스를 이용한 안전한 인증 프로토콜들이 대부분이다. 하지만 일반적인 RFID 환경에서 리더는 모바일 장치일 수 있다. 예를 들어 우리는 집에서 슈퍼마켓에서 사온 태그가 부착된 물건들에 대한 정보를 얻기 위해 개인 사용자가 소유한 PDA 또는 핸드폰에 리더 기능을 장착한 모바일 리더(Mobile Reader)를 사용할 수 있다.

이러한 환경에서 모바일 리더는 통신 장애 및 통신 범위 초과와 같은 이유로 인해 필요할 때마다 항상 중앙의 백-엔드-데이터베이스에 안전하게 연결되어 서비스를 받는다는 것이 사실상 불가능하다. 또한 모바일 리더는 분실이 쉽기 때문에 모바일 리더를 분실하였을 때에 대한 안전성도 고려되어야 한다. 이러한 환경에서 RFID 보안 및 프라이버시 문제점을 고려한 연구가 최근에 이루어지고 있다[13-15]. 문헌 [13]에서 Han 등은 문헌 [14,15]에서 제안한 서버가 없는 프로토콜에서의 인증은 태그에 대한 인증만을 고려하고 있다고 지적하고 있다. 또한 리더가 태그의 ID를 그대로 가지고 있기 때문에 익명성(anonymity)이 보장되지 않는다고 말하면서 이를 개선한 새로운 프로토콜을 제안하였다. 하지만 Han 등의 프로토콜은 리더의 요청에 항상 태그가 고정된 값으로 응답하기 때문에 위치 추적이 가능하며, 도청을 통한 재생 공격에 취약하다. 또한 저가 기반의 수동형 태그에 부적절하게 많은 통신량을 요구하고 있다. 따라서 본 논문에서는 Han 등이 제안한 프로토콜에 대한 취약성을 분석하고 이를 개선한 새로운 프로토콜을 제안한다.

본 논문의 공헌. 본 논문의 공헌은 다음과 같다.

1) 모바일 리더 환경에 태그와 리더 모두를 상호 인증하는 향상된 안전성을 보장하는 프로토콜을 제안한다.
2) 저가 기반의 수동형 태그에 적합한 통신량을 고려한 효율적인 방법을 제안한다.

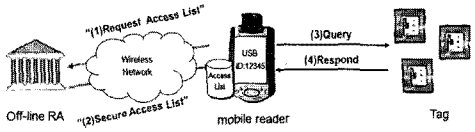
본 논문의 구성. 본 논문의 구성은 다음과 같다. 2장에서는 온라인 백-엔드-데이터베이스가 없는 RFID 시스템에서의 보안 및 프라이버시 요구사항에 대해 살펴보고, 3장에서는 모바일 리더 환경에서 최근에 제안된 기법들의 취약성을 분석한다. 4장에서는 이들을 개선한 보다 안전하고 효율적인 프로토콜을 제안하고, 5장에서 제안한 프로토콜에 대한 안전성과 효율성을 분석한다. 마지막으로 6장에서는 이러한 모바일 리더 환경에서의 해결하기 어려운 문제점에 대해서 언급하고 결론을 짓는다.

II. 온라인 백-엔드-데이터베이스가 없는 RFID 시스템

2.1 시스템 구성 요소

온라인 백-엔드-데이터베이스가 없는 일반적인 RFID 시스템은 [그림 1]과 같이 기본적으로 태그(Tag)와 모바일 리더(Mobile Reader) 그리고 오프라인 등록기관(Off-line Registration Authority)으로 구성된다. 오프라인 등록기관은 모바일 리더와

안전한 채널(Secure Channel)을 형성하지만, 리더와 태그 사이의 통신 채널은 안전하지 않다고 가정한다.



(그림 1) RFID 시스템 구성도

오프라인 등록기관과 리더는 무선 통신을 하지만 둘 다 강력한 계산 능력을 갖고 있기 때문에 암호학적인 방법을 통해 안전한 채널을 형성할 수 있지만, 태그와 리더와의 통신은 태그의 자원 제약성 때문에 안전하다고 가정할 수 없다. 그러므로 프로토콜을 설계함에 있어서 태그와 리더 사이의 통신에 안전성을 부여하는 것이 필요하다.

2.1.1 오프라인 등록기관(Off-line Registration Authority)

오프라인 등록기관은 항상 신뢰되는 기관으로서 태그에 관련된 모든 정보를 가지고 있다. 오프라인 등록기관은 리더들의 태그 인증을 위하여 태그의 비밀키와 같은 고유한 값을 해쉬 함수(Hash Function) 등을 사용한 가공된 값으로 변환하여 전달한다. 그러므로 리더는 태그의 인증을 위하여 등록기관에 매번 요청하지 않고, 주기적으로 전달받은 태그 정보 리스트를 활용하기 때문에 태그의 정보들은 좀 더 안전하게 보호되어질 수 있다.

2.1.2 태그(Tag)

태그는 내장된 전원 없이 리더로부터의 전파로부터 동작에 필요한 전원을 형성하는 수동형 태그(Passive Tag)이다. 수동형 태그는 보통 3m의 통신 반경을 가지며[14], UHF(UltraHigh Frequency) 대역(800~960Hz)에서 통신한다고 가정한다.

2.1.3 모바일 리더(Mobile Reader)

모바일 리더는 오프라인 등록기관에서 받은 태그 정보 리스트를 통해서 찾고자 하는 태그의 정보를 검색한다. 수동형 태그와 통신하는 리더는 100m의 통신반경을 가지고 있으며, 태그에게 충분한 전력을 공급할 수 있도록 전파의 세기가 강하다고 가정한다[14].

2.2 시스템 위협 요소

공격자는 다양한 공격을 시도하여 RFID 시스템에서의 보안 및 프라이버시에 대한 문제를 발생시킨다. 태그와 리더 사이의 무선 통신을 도청(Eavesdropping)할 수 있으며, 정당하지 않은 리더를 이용하여 태그로부터 얻은 정보를 통해 정당한 리더의 요청에 합리적인 태그로 가장하여 응답하는 스푸핑 공격(Spoofing Attack)을 할 수도 있다. 공격자는 도청한 데이터를 재전송하는 재생 공격(Replay Attack)과 메모리에 저장된 정보를 알아내기 위해 별도의 보호장치(Tamperproof)가 없는 저가의 태그에 대한 물리적인 공격(Tampering Attack)을 시도할 수도 있다.

RFID 시스템에는 보안 요구사항 외에도 사용자의 개인정보 노출이나 위치 정보 추적 등의 프라이버시 위협요소도 존재한다. 사용자가 태그가 내장된 물건을 소유한 채 이동할 경우 공격자는 안전하지 않은 태그를 이용하여 사용자의 위치를 추적하고 개인정보를 획득할 수도 있다. 정해진 인증과정만 통과하면 질의에 대하여 자신의 고유한 정보를 노출하기 때문에 프로토콜의 안전성이 보장되지 않는다면 사용자의 민감한 정보가 제3자에게 노출될 수 있으며, 해당 태그만의 고유한 정보를 통하여 위치정보를 획득하는 것도 가능하게 된다.

위와 같은 일반적인 RFID 시스템 위협 요소 이외에 모바일 리더 환경에서는 다음과 같은 위협 요소를 추가적으로 고려해야 한다. 모바일 리더 환경에서는 사용자가 모바일 리더를 들고 어디든 자유롭게 이동하며 태그를 인증할 수 있다는 장점을 갖는다. 하지만 이러한 환경에서는 모바일 리더가 항상 중앙의 백-엔드-데이터베이스에 안전하게 연결되어 서비스를 받는다는 것은 사실상 불가능하다. 모바일 리더를 들고 무선 통신이 불가능한 지역에 가게 되었을 경우 또는 통신 장애와 같은 이유로 인해 백-엔드-데이터베이스와 실시간 통신이 불가능할 수 있기 때문이다. 또한 모바일 리더는 분실이 쉽기 때문에 모바일 리더를 분실하였을 때에 대한 안전성도 고려되어야 한다.

2.3 보안 및 프라이버시 요구사항

위에서 언급된 시스템 위협요소를 해결하기 위하여

RFID 프로토콜이 만족해야하는 요구사항은 다음과 같다.

- 기밀성(Confidentiality): 태그와 리더사이의 모든 통신이 공격자에게 도청되더라도 어떠한 의미 있는 정보도 노출하지 않아야 하는 성질을 말한다. 즉, 공격자는 도청을 하더라도 어떠한 정보도 얻을 수 없어야 한다.
- 태그에 대한 익명성(Anonymity): 공격자가 태그와 모바일 리더와의 통신을 통해서 RFID 태그의 위치를 추적하거나 감시할 수 없어야 한다는 성질을 말한다. 이와 같은 성질을 만족하기 위해서 RFID 프로토콜은 구별 불가능성(Indistinguishability)과 전방향 안전성(Forward Secrecy)를 만족해야 한다. 구별 불가능성이란 태그에서 전송되는 정보를 통해서는 어떠한 태그로 부터의 정보인지 구분할 수 없어야 한다는 것이고, 전방향 안전성은 태그의 현 데이터가 노출되더라도 이전의 데이터가 추적되지 않아야 한다는 성질이다.
- 상호 인증(Mutual Authentication): 상호 인증은 태그와 리더가 서로 정당한 개체임을 확인하는 과정이다. 어느 한 방향의 인증과정이라도 만족되지 않는다면 공격자는 재생 공격이나 스푸핑 공격을 통하여 태그나 리더에 대한 위조가 가능하다.

위에서 언급한 일반적인 RFID 시스템에서 요구되는 보안 및 프라이버시 요구사항 이외에도 모바일 리더 환경에서는 다음과 같은 추가적인 요구사항을 고려해야 한다.

- 가용성(Availability): 본 논문에는 백-엔드-데이터베이스가 없는 환경을 가정하기 때문에, 사용자가 중앙 데이터베이스와의 통신이 불가능한 지역에서 모바일 리더를 사용하게 되는 경우도 고려해야 한다. 이러한 경우에도 모바일 리더가 태그와의 상호인증이 가능하도록 가용성이 보장되어야 한다.
- 리더 분실에 대한 안전성(Leakage Resilience): 휴대가 가능한 리더는 이동성이 뛰어난 반면, 분실의 위험이 존재한다. 때문에 분실한 경우 리더의 데이터 노출에 대한 안전성도 고려되어야 한다. 이와 같은 성질이 보장되지 않는다면, 공격자는 리더에 저장된 태그들의 정보를 통하여 정당한 태그인 척 위조할 수 있게 된다.

III. 관련 연구

최근 모바일 리더 환경에서의 상호 인증 프로토콜들[13-16]이 제안되고 있다. 서버가 없는 프로토콜에서의 인증을 최초로 제안한 문헌 [14,15]은 문헌 [13]에서 Han 등이 지적한 대로 태그에 대한 인증만을 고려하고 있다. 또한 리더가 태그의 ID를 그대로 저장하고 있기 때문에 태그 익명성(anonymity)이 보장되지 않는다. 이를 개선한 Han 등의 프로토콜[13]은 앞서 지적한 문제를 해결하였으나 태그가 리더의 요청에 항상 고정된 값으로 응답한다는 문제점을 갖는다. 이러한 문제점으로 인해 태그에 대한 위치 추적이 가능하고 도청을 통한 재생 공격에 취약하다. 또한 태그와 리더 사이의 통신량이 많아 저가 기반의 수동형 태그에 부적절 하다. 이러한 기법들은 모두 태그에 대한 전방향 안전성(Forward Secrecy)을 만족하지 않는다. 따라서 문헌 [16]에서 처음으로 기존의 기법들이 해결하지 못한 전방향 안전성에 안전한 프로토콜을 제안하였다. 하지만 문헌 [16]은 전방향 안전성 문제를 해결하기 위해 다수의 리더 환경이 아닌 하나의 리더만을 사용하는 환경을 고려하였기 때문에 기존의 기법들이 제안된 환경보다는 제약을 받는다.

3.1 Han 등의 프로토콜

본 절에서는 최근 온라인 백-엔드 데이터베이스가 없는 환경에서 제안된 Han 등의 프로토콜을 살펴본 후 취약점을 분석한다.

[표 1] 용어 정의

Notation	Representation
$h(\cdot)$	일방향 해쉬 함수
$\|$	비트 스트링 연결
T	유효한 태그
CA	오프라인 등록 기관
id_T	태그의 고유 ID
$h(id_T)$	T의 Pseudo-identifier
$PRNG$	의사 난수 생성기
β	일방향 해쉬 함수의 결과 길이
$\oplus$	XOR
R	인증된 리더
s	태그와 CA간의 비밀 공유 정보
id_R	리더의 고유 ID
L	리더의 인증 정보

3.1.1 용어 정의

제안된 프로토콜에서 사용되는 용어 정의는 〔표 1〕과 같다.

3.1.2 초기 설정 단계(Initial Setting Phase)

1. CA는 태그 T와의 비밀 공유키 s를 생성하고 태그에 저장한다.
2. CA는 정당한 리더를 인증하고, 인증된 리더의 요청에 따라 〔표 2〕와 같이 접근할 수 있는 태그의 인증 리스트 정보를 생성하여 리더에게 안전하게 전송한다.

〔표 2〕 인증 리스트

...	...
$h(s,id_R)$	$h(id_T)$
...	...

3.1.3 인증 단계(Authentication Phase)

제안된 프로토콜의 인증 단계는 다음과 같다〔그림 2〕.

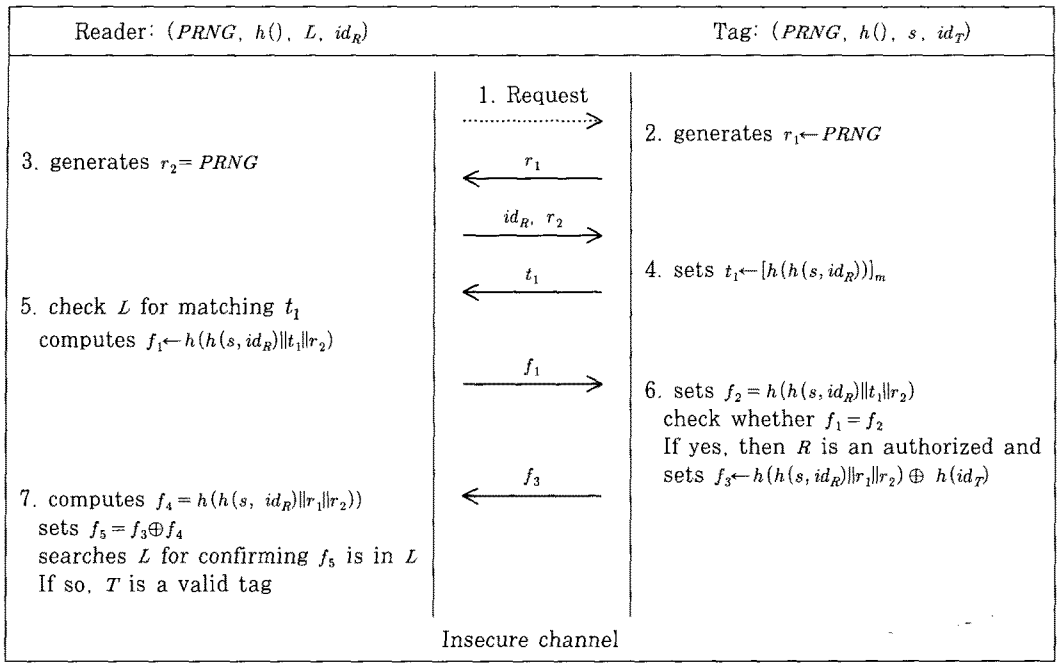
1. 리더 R은 태그 T에 요청 메시지를 전송한다.
2. 태그 T는 난수 r_1을 생성하고 리더 R에게 r_1을 전송한다.
3. 리더 R은 난수 r_2를 생성하고 자신의 id_R과 함께 리더에게 전송한다.
4. 태그 T는 자신의 비밀키 s와 리더로부터 전송된 id_R을 사용하여 $h(h(s, id_R))$을 계산하고 이 값의 처음부터 m 비트 스트링, t_1을 생성하여 리더에게 전송한다.
5. 리더 R은 인증리스트 L안에서 t_1에 일치하는 특정 태그를 찾을 때까지 모든 태그의 비밀값 x를 이용하여 $h(x, id_R)$를 계산한 후 해쉬 값하며 비교한다. 찾으면 $f_1=h(h(s, id_R)\|t_1\|r_2)$를 계산하여 태그 T에게 전송하고 찾지 못했다면 세션을 종료한다.
6. 태그 T는 f_1을 받은 후 자신이 가지고 있는 값을 이용하여 $f_2=h(h(s,id_R)\|t_1\|r_2)$를 계산하고 f_1과 비교 한다. 같다면 리더가 인증되어 졌으므로 $f_3=h(h(s,id_R)\|r_1\|r_2)\oplus h(id_T)$를 계산하여 리더에게 전송한다.
7. 리더 R은 $f_4=h(h(s,id_R)\|r_1\|r_2)$을 계산하고 f_4와 XOR 연산을 수행한다. $f_5=h(id_T)$이므로 인증 리스트 안에 f_5와 일치하는 값이 있는지를 체크한다. 있다면 태그를 인증하고 없다면 태그 인증 실패이므로 세션을 종료한다.

3.1.4 취약점 분석

Han 등이 제안한 프로토콜은 온라인 백-엔드-서버가 없는 환경에서 태그와 리더가 서로를 상호 인증한다. 또한 리더에는 태그의 ID에 대하여 해쉬한 값이 리스트로 저장되기 때문에 능동적인 공격자가 이러한 리스트를 알았다고 할지라도 preimage resistance 성질에 의해 ID를 알 수 없어 익명성을 보장한다.

하지만 제안된 프로토콜은 도청 및 스푸핑 공격과 재생 공격을 통해서도 태그의 위치 추적이 가능하다. 또한 저가 기반의 수동형 태그에는 적합하지 않은 많은 통신량을 가지고 있다.

- 도청: 위의 프로토콜에서 보듯이 태그는 동일한 리더의 요청에 매 세션마다 같은 값인 t_1으로 응답한다. 만약 공격자가 이러한 t_1 값들을 연속적으로 도청한다면 태그를 소지한 사용자의 위치를 추적할 수 있다.
- 스푸핑 공격: 공격자는 자신이 생성한 id_A, r_2를 태그에게 전송한다. 태그는 매번 $t_A=[h(h(s, id_A))]_m$으로 응답하므로 위치 추적이 가능하다.
- 재생 공격: 태그는 리더가 보낸 f_1에 대하여 인증한 후 정당한 리더에게만 f_3을 전송한다. 하지만 공격자는 리더가 태그에게 보내는 id_R, r_2, f_1 값들을 도청하여 가지고 이후 세션에서 재생 공격을 할 수 있다. 태그는 공격자 리더가 전송한 f_1 또한 정당한 값이므로 인증 후 f_3을 계산하여 공격자의 리더에게 전송하게 된다. 따라서 공격자는 재생 공격을 통하여 현재 태그가 주변에 존재하는지를 알 수 있으므로 잠재적으로 위치 추적이 가능하다.
- 통신량: 일반적인 challenge-response 방식의 상호 인증 프로토콜은 기본적으로 3번의 리더와 태그사이의 데이터 통신이 이루어진다. 반면에 Han 등의 프로토콜에서는 태그와 리더의 상호 인증을 위해서 6번의 통신이 이루어진다. 자체적인 배터리를 가지고 있지 않은 저가 기반의 수동



〔그림 2〕 Han 등의 프로토콜

형 태그의 경우 리더로부터 에너지를 받아서 사용하기 때문에 이와 같이 많은 통신량은 적합하지 않다.

IV. 향상된 익명의 상호인증 프로토콜

본 논문에서는 위에서 분석한 내용을 토대로 Han 등이 제안한 프로토콜을 향상시킨 새로운 상호 인증 방법을 제안한다. 제안 프로토콜은 〔그림 3〕과 같으며 각 단계를 기술하면 다음과 같다.

1. 리더 R은 난수 r_1을 생성하고 자신의 id_R과 함께 리더에게 요청한다.
2. 태그 T는 난수 r_2를 생성한 후 자신의 비밀키 s와 리더로부터 전송된 id_R, r_1을 사용하여 $h(h(s, id_R)||r_1||r_2)$를 계산하고 이 값의 처음부터 m개의 비트 스트링, t_1을 생성한 후 리더에게 t_1, r_2를 전송한다.
3. 리더 R은 인증리스트 L안에서 t_1에 일치하는 특정 태그를 찾을 때까지 모든 태그의 $h(x, id_R)$에 대하여 해쉬 값하며 비교한다. 찾으면 $f_1 = h(h(s, id_R)||t_1)$를 계산하여 태그 T에게 전송하고 찾지 못했다면 세션을 종료한다.
4. 태그 T는 f_1을 받은 후 자신이 가지고 있는 값을 이용하여 $f_2 = h(h(s, id_R)||t_1)$를 계산하고 f_1과 비교 한다. 같다면 리더가 인증되어 졌으므로 $f_3 = h(h(s, id_R)||f_1) \oplus h(id_T)$를 계산하여 리더에게 전송한다.
5. 리더 R은 $f_4 = h(h(s, id_R)||r_1||r_2)$을 계산하고 f_4와 XOR 연산을 수행한다. $f_5 = h(id_T)$이므로 인증 리스트 안에 f_5와 일치하는 값이 있는지를 체크한다. 있다면 태그를 인증하고 없다면 태그 인증 실패이므로 세션을 종료한다.

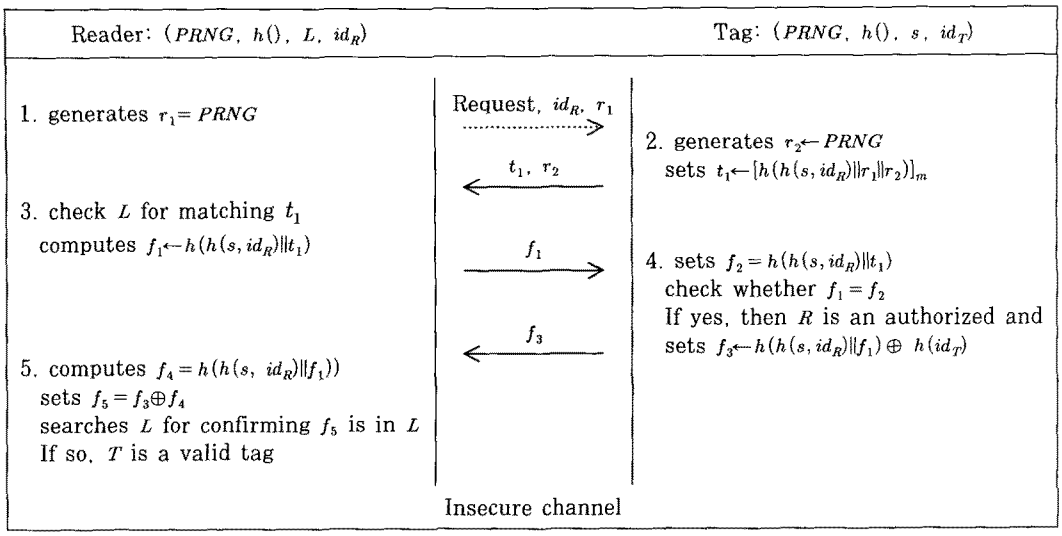
V. 분 석

본 장에서는 제안하는 프로토콜의 안전성과 효율성을 분석한다. 제안하는 프로토콜은 Han 등이 제안한 프로토콜과 비교하여 안전하면서도 효율적이다.

5.1 안전성 분석

본 절에서는 2장에서 언급한 보안 및 프라이버시 요구사항을 만족함을 보인다. 또한, 먼저 Han 등의 기법이 안전성을 만족하지 못했던 도청, 스푸핑, 재생 공격에 대해 안전함을 보인다.

- 도청: 리더의 요청에 태그가 응답하는 값 t_1, r_2,



〔그림 3〕 향상된 익명의 상호 인증 프로토콜

f_3은 매 세션마다 변경된다. 따라서 공격자의 도청을 통한 위치 추적으로부터 안전하다.

- 스푸핑 공격: 능동적인 공격자는 자신이 임의로 생성한 r_1, id_A를 사용하여 태그에 요청할 수 있다. 하지만 태그는 난수 r_2를 생성하고 이를 사용하여 t_1을 계산하기 때문에 위치 추적을 할 수 없다.
- 재생 공격: 공격자는 이전 세션에서 도청한 $f_1 = h(h(s, id_R)||t_1)$을 재사용하여 태그에 요청할 수 있다. 하지만 현재 세션에서 정당한 태그가 생성 한 $f_2 = h(h(s, id_R)||t_1')$는 f_1과 다르다. 따라서 태그는 응답하지 않으므로 태그의 위치를 추적할 수 없다.
- 기밀성(Confidentiality): 리더에서 태그로, 그리고 태그에서 리더로 전달되는 값은 모두 해쉬 함수의 결과값들로 안전한 해쉬 함수의 성질로 인해 해쉬 함수의 입력값을 알 수 없다. 따라서 공격자는 도청된 메시지로부터 어떠한 의미 있는 정보도 알아낼 수 없다.
- 태그에 대한 익명성(Anonymity): 리더의 요청에 태그는 매번 자신이 임의로 선택한 난수 r_2를 이용하여 응답하므로 응답하는 값 t_1, r_2, f_3은 매 세션마다 변경된다. 따라서 공격자 입장에서는 이 값이 어떤 태그로부터 나온 값인지 구별 불가능하기 때문에 구별 불가능성을 만족한다. 전방향 안전성을 만족시키기 위해 일반적으로 태그는 자신의 비밀값을 매 세션마다 갱신하는 방법을 사용하는데 이러한 경우 다수의 모바일 리더들과의 동기화 문제를 해결하여야 한다. 제안하는 기법은 다수의 모바일 리더를 사용하는 환경에서 제안하는 기법으로 문헌 [13-15]과 같이 전방향 안전성 문제는 고려하지 않는다.
- 상호 인증(Mutual Authentication): 리더와 태그는 서로 공유한 비밀값을 통해 통신하는 상대가 정당하다는 것을 확신할 수 있게 된다. 또한 Challenge-Response 기법을 사용하여 리더와 태그가 모두 자신이 생성한 난수를 사용하기 때문에 상호 인증이 가능하다.
- 가용성(Availability): 모바일 리더들은 자신의 인증 리스트를 이용하여 태그를 인증한다. 이러한 인증 리스트를 통하여 리더는 백-엔드-데이터베이스에 접속하지 않고 태그를 인증할 수 있게 된다. 따라서 사용자가 모바일 리더를 가지고 무선 통신이 불가능한 지역에 가더라도 태그 인증이 가능하다.
- 리더 분실에 대한 안전성(Leakage Resilience): 각각의 모바일 리더는 인증 리스트를 가지고 있는데 이 값들은 모두 해수 함수의 결과값으로 이러한 값으로부터 해쉬 함수의 입력값인 태그 ID, 또는 태그의 비밀값을 알아낼 수 없기 때문에 다른 정당한 리더에게 정당한 태그인 척 하는 공격에 안전하다.

5.2 효율성 분석

Han et al.이 제안한 상호인증 프로토콜은 6번의 리더와 태그사이의 데이터 통신이 이루어진다. 반면에 본 프로토콜에서는 태그와 리더가 서로를 인증하기 위해서 4번의 통신이 이루어진다. 따라서 본 프로토콜은 저가 기반의 수동형 태그에 적용하여 사용할 수 있도록 효율성을 높였다.

VI. 결 론

본 논문에서는 온라인 백-엔드-데이터베이스가 없는 RFID 시스템에서의 보안 및 프라이버시 문제를 해결할 수 있는 향상된 새로운 상호 인증 프로토콜을 제안하였다. 제안한 프로토콜은 Han 등이 제안한 프로토콜과 비교하여 안전하고 효율적이다. 하지만 온라인 백-엔드-데이터베이스가 없는 RFID 시스템에서 다수의 리더를 사용할 경우 태그의 메모리에 저장된 정보가 고정되어야 하기 때문에(전방향 안전성을 만족하기 위해 태그 정보를 갱신하게 되면 다수의 리더에게 이러한 정보를 알리는 추가적인 방법이 필요하다.) 물리적인 공격을 통한 태그의 비밀 정보가 노출될 경우 전방향 안전성(Foward Secrecy)을 만족하기 어렵다. 따라서 이전에 도청한 값들과 함께 사용하여 태그의 위치 추적이 가능하다. 우리는 다수의 리더를 사용하는 온라인 백-엔드-데이터베이스가 없는 시스템에서의 전방향 안전성을 만족하는 안전한 프로토콜에 대하여 연구할 것이다.

참 고 문 헌

[1] A. Juels, "RFID security and privacy: A research survey," IEEE Journal on Selected Areas in Communication, vol. 24, no. 2, pp. 381-394, Feb. 2006.

[2] 하재철, 백이루, 김환구, 박제훈, 문상재, "해쉬함수에 기반한 경량화된 RFID 인증 프로토콜," 정보보호학회논문지, 19(3), pp. 61-72, 2009년 6월.

[3] 정윤수, 김용태, 박길철, 이상호, "RFID를 이용한 IPTV 사용자의 경량화 인증 프로토콜," 정보보호학회논문지, 19(2), pp. 105-115, 2009년 4월.

[4] 원태연, 천지영, 박춘식, 이동훈, "수동형 RFID 시스템에 적합한 효율적인 상호 인증 프로토콜 설계," 정보보호학회논문지, 18(6A), pp. 63-73, 2008년 12월.

[5] H.Y. Chien and T.C. Wu, "Improving Varying-Pseudonym-Based RFID Authentication Protocols to Resist Denial-of-Service Attacks," 정보보호학회논문지, 18(6B), pp. 259-269, 2008년 12월.

[6] 권혜진, 이재욱, 전동호, 김순자, "데이터베이스에서의 태그 검색이 쉽고 안전한 RFID 상호인증 프로토콜," 정보보호학회논문지, 18(5), pp. 125-134, 2008년 10월.

[7] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic Approach to "Privacy-Friendly" Tags," In RFID Privacy Workshop, July 2003.

[8] A. Juels and S.A. Weis, "Authenticating Pervasive Devices with Human Protocols," Advances in Cryptology - Crypto 2005, LNCS 3621, pp. 293-308, 2005.

[9] G. Tsudik, "YA-TRAP: Yet Another Trivial RFID Authentication Protocol," Pervasive Computing and Communications Workshops 2006 (PerCom Workshops 2006), pp. 640-643, Mar. 2006.

[10] S. Vaudenay, "On Privacy Models for RFID," Advances in Cryptology - ASIACRYPT 2007, LNCS 4833, pp. 68-87, 2007.

[11] H. Gilbert, M. Robshaw, and Y. Seurin, "HB#: Increasing the Security and Efficiency of HB+," EUROCRYPT 2008, LNCS 4965, pp. 361-378, 2008.

[12] R. Paise and S. Vaudenay, "Mutual authentication in RFID: security and privacy," ACM Symposium on Information, Computer and Communications Security (ASIACCS 2008), pp. 292-299, Mar. 2008.

[13] S. Han, T.S. Dillon, and E. Chang, "Anonymous Mutual Authentication Protocol for RFID Tag Without Back-End-Database," Mobile Ad-Hoc and Sensor Networks, LNCS 4864, pp. 623-632, 2007.

[14] C. Tan, B. Sheng, and Q. Li, "Serverless Search and Authentication Protocols for

RFID," Pervasive Computing and Communications Workshops 2007 (PerCom Workshops 2007), pp. 3-12, Mar. 2007.

[15] C. Tan, B. Sheng, and Q. Li, "Secure and Serverless RFID Authentication and Search Protocols," IEEE Transactions on Wireless Communication, vol. 7, no. 4, pp. 1400-1407, Apr. 2008.

[16] M.E. Hoque, F. Rahman, S.I. Ahamed, and J.H. Park, "Enhancing Privacy and Security of RFID System with Serverless Authentication and Search Protocols in Pervasive Environments," Wireless Personal Communications, Publised Online: 29, July 2009.

〈著者紹介〉

원 태 연 (Tae Youn Won) 학생회원
2007년 2월: 고려대학교 전산학과 학사 졸업
2009년 2월: 고려대학교 정보경영공학과 석사 졸업
〈관심분야〉 정보보호, RFID 보안 기술, 무선 보안, PET 기술

유 영 준 (Young Jun Yu) 학생회원
2008년 2월: 숭실대학교 수학과 학사 졸업
2008년 3월 ~ 현재: 고려대학교 정보경영공학과 석사과정
〈관심분야〉 암호 프로토콜, VANET, 네트워크 코딩, 응용암호

천 지 영 (Ji Young Chun) 학생회원
1997년 2월: 이화여자대학교 수학과 학사 졸업
2006년 2월: 고려대학교 정보경영공학과 석사 졸업
2006년 3월 ~ 현재: 고려대학교 정보경영공학과 박사과정
〈관심분야〉 암호 이론, 프라이버시향상기술(PET), 유비쿼터스 보안

변 진 욱 (Jin Wook Byun) 정회원
2001년: 고려대학교 전산학과 이학사 졸업
2003년: 고려대학교 정보보호대학원 공학석사 취득
2006년: 고려대학교 정보보호대학원 공학박사 취득
2007년~2008년: 런던대학, ISG, 박사 후 연구원
2008년 3월~현재: 평택대학교 정보통신학과 전임강사
〈관심분야〉 정보보호 프로토콜, 프라이버시 보호 기술, 패스워드 인증, 정보통신 프로토콜

이 동 훈 (Dong Hoon Lee) 종신회원
1983년 8월: 고려대학교 경제학과 학사 졸업
1987년 12월: Oklahoma University 전산학과 석사 졸업
1992년 5월: Oklahoma University 전산학과 박사 졸업
1993년 3월 ~ 1997년 2월: 고려대학교 전산학과 조교수
1997년 3월 ~ 2001년 2월: 고려대학교 전산학과 부교수
2001년 3월 ~ 현재: 고려대학교 정보경영공학부 교수
〈관심분야〉 암호 프로토콜, 암호 이론, USN 이론, 키 교환, 익명성 연구, PET 기술