情報保護學會論文誌
第18卷 第6(A)號, 2008. 12

수동형 RFID 시스템에 적합한 효율적인 상호 인증 프로토콜 설계*

원 태 연[1†], 천 지 영[1], 박 춘 식[2], 이 동 훈[1‡]
[1]고려대학교 정보경영공학전문 대학원, [2]한국전자통신연구원 부설연구소

Efficient Mutual Authentication Protocol Suitable to Passive RFID System*

Tae Youn Won[1†], Ji Young Chun[1], Choon Sik Park[2], Dong Hoon Lee[1‡]
[1]Graduate School of Information Management and Security, Korea University [2]The Attached Institute of ETRI

요 약

RFID(Radio Frequency IDentification) 시스템은 일정한 라디오 주파수 대역을 이용해 무선 방식으로 각종 데이터를 주고받을 수 있는 시스템으로 기본적으로 태그(Tag)와 리더(Reader) 그리고 백-엔드-데이터베이스(Back-End-Database)로 구성된다. 태그에 쓰기(Re-Write)가 가능하고 무선공간에서 다수의 태그를 동시에 인식 가능하다는 장점으로 인해 기존의 바코드 시스템을 대체하여 물류관리, 유통관리, 재고관리 분야에서 널리 사용되고 있다. 그러나 태그와 리더가 무선 주파수를 이용하여 통신하기 때문에 시스템 보안과 개인 프라이버시 침해 문제가 발생한다. 현재까지 RFID 시스템의 이러한 문제를 해결하기 위해 많은 연구가 있었으며 그 결과 다양한 보안 기법들이 제안되었다. 하지만 제안된 많은 보안 기법들은 UHF대역의 국제 표준인 Class-1 Generation-2 태그에는 적용하기 어렵다. 최근에 Chien과 Chen은 Class-1 Generation-2 태그에 적합한 상호 인증 프로토콜을 제안하였지만 이 또한 취약성이 존재하며 데이터베이스에서의 효율성이 떨어지는 문제점이 있다. 따라서 본 논문에서 Chien과 Chen이 제안한 기법을 분석하고 안전성과 효율성을 향상된 새로운 상호 인증 기법을 제안한다.

ABSTRACT

RFID(Radio Frequency IDentification) system is an automated identification system that basically consists of tags and readers and Back-End-Databases. Tags and Readers communicate with each other by RF signal. As a reader can identify many tags in contactless manner using RF signal, RFID system is expected to do a new technology to replace a bar-code system in supply-chain management and payment system and access control and medical record and so on. However, RFID system creates new threats to the security of systems and privacy of individuals, Because tags and readers communicate with each other in insecure channel using RF signal. So many people are trying to study various manners to solve these problems against attacks, But they are difficult to apply to RFID system based on EPCglobal UHF Class-1 Generation-2 tags. Recently, Chien and Chen proposed a mutual Authentication protocol for RFID conforming to EPCglobal UHF Class-1 Generation-2 tags. we discover vulnerabilities of security and inefficiency about their protocol. Therefore, We analyze vulnerabilities of their protocol and propose an efficient mutual authentication protocol that improves security and efficiency.

Keywords : RFID, Gen2, Privacy Problem, Security, Exhaustive Search, Bloom Filter

Ⅰ. 서 론

RFID(Radio Frequency IDentification) 시스템은 일정한 라디오 주파수 대역을 이용해 무선 방식으로 각종 데이터를 주고받을 수 있는 시스템으로 기본적으로 태그(Tag)와 리더(Reader) 그리고 백-엔드-데이터베이스(Back-End-Database)로 구성된다. 리더는 사물에 부착된 태그로부터 고유 식별 정보를 비접촉 방식으로 수집하고, 수집된 정보를 백-엔드-데이터베이스에 전송하여 대상물체를 판독 및 인식한다.

이러한 RFID 시스템은 태그와 리더의 무선 주파수를 이용한 통신으로 인해 물리적인 접촉 없이 통신이 가능하여 인식률이 높고 인식 거리가 길다. 또한 사물의 고유 식별 번호를 저장하고 있는 태그의 반복적인 재-쓰기(Re-Write)가 가능하다. RFID 시스템은 이러한 장점으로 인해 기존의 바코드 시스템을 대체하여 물류관리, 유통관리, 재고 관리 분야에서 사용되고 있다. 2006년 ISO국제표준화 회의에서 EPCglobal에서 제안한 Class-1 Generation-2(이하 Gen2)가 UHF-RFID 규격에 기초한 ISO 18000-6C로 편입됨으로써 표준화 문제도 해결되어 다양한 분야에서의 RFID 산업의 확산이 기대되어 진다[4]. 또한 앞으로 센서 기술과의 융합 및 태그의 제조 기술 발전으로 정보를 능동적으로 획득하고 처리하는 능력까지 갖추게 되면 미래를 이끌어갈 신기술로 더욱더 주목을 받을 것이다.

하지만 RFID 시스템에서 태그와 리더의 무선 주파수를 이용한 통신으로 인해 앞에서 언급한 여러 가지 이익을 얻을 수 있는 반면 정보노출, 위치추적, 위조 및 서비스 장애와 같은 보안 및 사용자 프라이버시 침해 문제가 발생한다[7]. 지금까지 이를 보호하기 위한 많은 기법[2-3,5-6,8-17]들이 제안되지만, 이들 기법은 취약성이 존재하며 태그에서 암호학적 연산(대칭키 암호, 해쉬 함수 등)을 필요하여 저가 기반의 Gen2 태그에는 적합하지 않은 문제가 있다[2,5-6,9-17]. [2,3,6,8]기법들만이 Gen2 기반의 RFID 시스템 환경에서 제안되었다. 가장 최근에는 Chien과 Chen[2]이 Karthikeyan et al.[8]과 Duc et al.[3]이 제안한 인증 기법들을 개선한 Gen2에서 지원하는 의사난수생성(PRNG, Pseudo-Random Number Generator) 함수와 순환중복검사(CRC, Cyclic Redundancy Check) 함수를 사용하는 도전-응답(Challenge-Response) 기반의 상호 인증 기법을 제안하였다. 하지만 이 기법 역시 비동기화 문제가 발생하며 전방안전성(Forward Security)을 만족하지 못하는 문제도 있다. 또한 백-엔드-데이터베이스에서 특정 태그를 인증하기 위해 전수조사(Exhaustive Search)를 해야 하는 비효율적인 문제가 존재한다. 이에 본 논문에서는 Chien과 Chen이 제안한 상호 인증 기법의 취약성을 지적하고 이를 개선한 Gen2 기반에서 안전성과 효율성이 향상된 새로운 상호 인증 기법을 제안한다. 특히 고가의 비휘발성 메모리의 사용을 최소화하고 Gen2에서 지원하는 순환중복검사 함수와 의사난수생성 함수만을 사용하여 RFID 시스템의 보안 및 프라이버시 침해 문제를 해결하는 향상된 도전-응답 기반의 상호 인증 기법을 제안한다. 그리고 백-엔드-데이터베이스에서 특정 태그를 찾기 위해 전수 조사를 해야만 하는 문제를 해결하기 위해서 블룸필터[1]을 사용한 멤버쉽 테스트 방법을 소개한다. 블룸필터를 사용하여 백-엔드-데이터베이스에서 효율성을 향상시키고자 하는 제안은 [16,17]에서 처음 소개되었다.

본 논문의 구성은 다음과 같다. 2장에서 제안 기법에 필요한 배경 지식을 알아보고 3장에서 본 논문에서 제안하는 상호 인증 프로토콜을 소개한다. 4장에서 제안하는 기법에 대한 안정성과 효율성을 언급 한 뒤 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 배경 지식

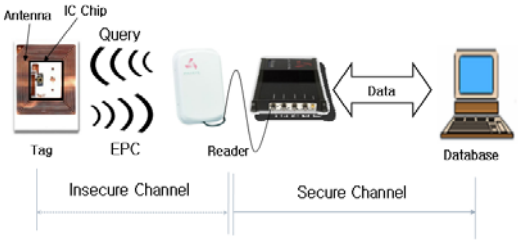
2.1 RFID 시스템

RFID 시스템은 [그림 1]과 같이 기본적으로 태그(Tag)와 리더(Reader) 그리고 백-엔드-데이터베이스 (Back-End-Database)로 구성된다.

2.1.1 태그(Tag)

태그는 기본적인 연산 및 데이터 저장을 위한 IC 칩(IC Chip)과 리더와의 통신을 위한 안테나(Antenna)로

접수일 : 2008년 4월 30일; 수정일 : 2008년 8월 14일;
채택일 : 2008년 9월 25일
* “본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음” (IITA-2008-(C1090-0801-0025))
† 주저자, kucs226@korea.ac.kr
‡ 교신저자, donglee@korea.ac.kr



[그림 1] RFID 시스템 구성도

구성된다. 일반적으로 전력의 공급 방법에 따라 능동형 태그(Active Tag)와 수동형(Passive Tag)로 나뉘는데 수동형 태그는 리더의 전송 요청에 따라 자신 고유 ID(EPC)를 무선 주파수를 이용하여 전송한다. 국제 표준인 Gen2는 수동형 태그로 다음과 같은 기능을 제공하며 이러한 기능은 보안 및 프라이버시 보호를 위해 사용된다.[4].

(a) 16bit 의사난수생성기(16bit-Pseudo-Random Number Generator) : 시드(Seed) 값을 사용하여 16bit 길이의 난수를 생성하며 이전의 결과로부터 다음의 난수가 생성되는 결정적인 함수(deterministic function)이다. 매 세션마다 임의의 난수를 생성하기 위해서 사용된다.

(b) 16bit 순환중복검사(16bit-Cyclic Redundancy Code Checksum) : 태그와 리더사이의 송, 수신되는 데이터에 대한 무결성을 검사한다. 가변 길이의 데이터에 대하여 16bit 길이의 결과 값을 출력하며 해쉬 함수를 대신하여 사용된다.

2.1.2 리더(Reader)

리더는 기본적으로 RF 모듈, 컨트롤 유닛, 그리고 안테나로 구성된다. 리더는 무선 주파수를 이용하여 태그와 통신을 하며 수신 받은 데이터는 백-엔드-데이터베이스에 전송하며 이로부터 사물에 대한 정보를 얻는다.

2.1.3 백-엔드-데이터베이스(Back-End-Database)

백-엔드-데이터베이스(이하 DB)는 각각의 태그와 관련된 데이터를 저장하고 관리하는 장치이다. 리더로부터 전달된 태그의 데이터에 대하여 인증하고 사용자에게 서비스를 제공한다.

2.2 블룸 필터(Bloom Filter)

블룸필터는 주어진 원소가 사전에 정의되어진 집합 안에 포함되어 있는지 여부를 검사하는데 사용할 수 있는 자료 구조이다[1]. 만약 블룸필터가 k개의 독립적인 해쉬 함수($h_1,h_2,.....h_k$)와 n개의 원소를 포함 하는 집합($S=\{s_1,s_2,.....s_n\}$)으로 만들어진 m 비트 스트링이라고 하자(블룸필터의 초기값은 0이다). 각각의 해쉬 함수는 0에서 m-1사이의 값을 갖고 이 값들은 블룸필터의 각각의 비트에 대응된다. m 비트의 블룸필터를 만들기 위해 각각의 원소 $s(\in S)$에 대해서 k개의 해쉬 함수($h_1,h_2,.....h_k$)값 $h_i(s)(1\leq i\leq k)$을 계산한 후 이 값에 해당하는 블룸필터의 비트를 1로 바꾼다. 만약 $hi(s)=t$라고 하면 블룸필터의 t 번째 비트를 1로 바꾼다. 원소 s'($\in S$)의 포함여부를 알아보려면 블룸필터의 $hi(s')(1\leq i\leq k)$ 번째 비트가 모두 1인지 확인한다. 만약 k 비트 모두 1이면 s'가 원소이지만 k개 중 하나라도 0이라면 원소가 아니다.

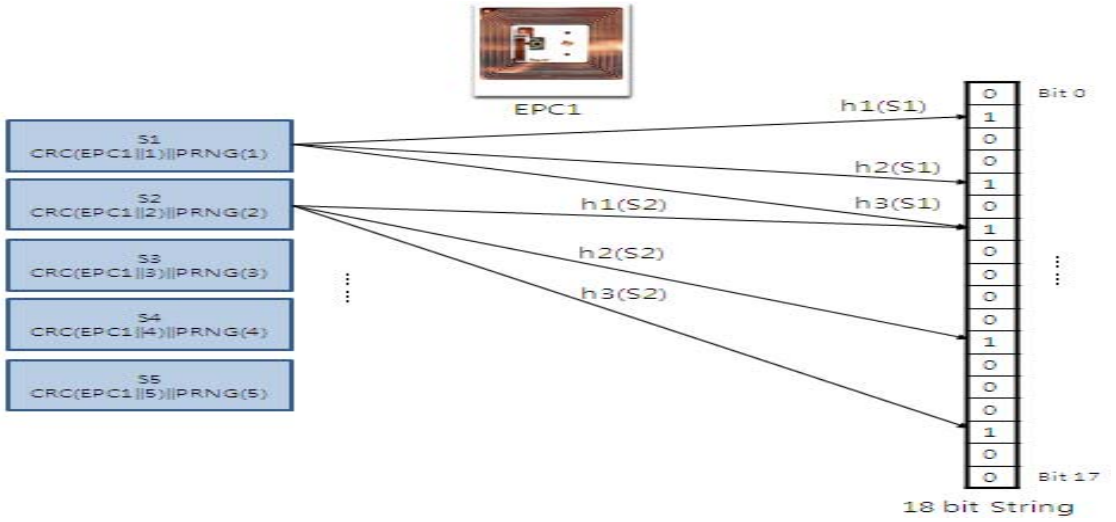
[그림 2]는 식별 정보 EPC1의 값을 가지는 하나의 태그에 대하여 원소의 개수가 5, 서로 다른 함수의 개수 3, 블룸필터 스트링의 크기 m이 18일 때의 블룸필터를 만든 예이다. 태그에서 생성한 $CRC(EPC_1 \| j) \| PRNG(j)$ 값이 리더를 통하여 DB에 전송 되었을 때 DB는 $CRC(EPC_1 \| j) \| PRNG(j)$ 값에 k개의 해쉬 함수를 계산한 값이 m비트의 스트링에서 해당 위치에 모두 1로 되어있는지 체크함으로써 EPC1에 대한 정보를 전수 조사를 하지 않고도 데이터를 쉽게 찾을 수 있게 된다. 보다 자세한 사항은 3절에서 소개하도록 한다.

하지만 블룸 필터는 긍정오류율(false positive error, 집합에 포함되어 있지 않는 원소가 집합 안에 포함되어 있다고 잘못 판단하는 확률)이 존재한다. 다음 식은 긍정오류가 일어날 확률을 말하며 사용하는 환경에 따라 k, n, m의 값을 조정하여 이를 최적화 할 수 있다.

$$f=(1-(1-\frac{1}{m})^{kn})^k\approx(1-e^{-\frac{kn}{m}})^k$$

2.3 이전 기법들에 대한 분석

지금까지는 RFID 시스템의 보안 및 프라이버시 보호를 위해 해쉬 함수 기반의 기법들이 제안되었다. 특히 최근 [17]에서는 위에서 말한 블룸필터를 사용하여 DB



[그림 2] 블룸필터 사용의 예

에서 전수조사를 하지 않고도 특정 태그를 효율적으로 찾을 수 있는 기법을 제안하였다. 하지만 그들의 기법은 현재까지 해쉬 함수가 지원되지 않는 수동형 Gen2 태그에는 적합하지 않으며 전방안전성을 만족하는 구체적인 프로토콜을 제안하고 있지는 않다. 최근에는 Gen2 태그에 적합하면서 보안 및 프라이버시 문제를 해결하기 위한 기법들이 활발히 연구되고 있다. Karthikeyan et al.[8]은 XOR 연산과 행렬(matrix)만을 이용한 인증 기법을 제안하였다. 그러나 이 기법은 인증키를 업데이트하기 위해 리더가 태그에 전송하는 데이터에 대하여 서비스 거부 공격 및 재생 공격을 한다면 비동기화 문제가 발생하며 하나의 세션에서 리더와 태그의 인증이 완료되기 전에 인가되지 않은 리더의 요청에 대하여 태그는 계속 똑같은 값으로 응답하게 되어 위치 추적도 가능하다. 이후 Duc et al.[3]은 Gen2에서 제공하는 의사난수생성 함수와 순환중복검사 함수만을 사용하여 인증하는 기법을 제안하였다. 하지만 이 기법 또한 DB와 태그의 인증키를 업데이트하기 위해서 리더가 태그와 DB에 전송하는 “End Session" 명령어에 대해서 서비스 거부 공격 및 재생 공격을 한다면 비동기화 문제가 발생하게 되어 이후 더 이상 DB와 태그사이에 인증을 할 수 없게 된다. 그리고 물리적 공격을 통하여 태그의 메모리에 저장된 값들을 공격자가 알게 된다면 전방 안전성도 보장하지 못하게 되어 위치 추적을 할 수 있게 된다.

Chien과 Chen[2]은 이러한 Gen2 기반에서의 취약성을 보완한 보다 강력한 도전-응답 기반의 상호 인증 기법을 제안하였다. 하지만 이 기법 역시 취약성이 존재하며 DB에서 효율성이 떨어지는 문제점이 있다. 다음은 Chien과 Chen 기법에 대한 안전성과 효율성을 분석한 것이다.

- 안전성 분석

1) 서비스 거부 공격에 대한 취약성 : Chien과 Chen은 태그와 DB가 인증을 위해 사용하는 인증키 및 접근키의 동기화 유지를 위해서 DB에서 (K_{old}, K_{new}), (P_{old}, P_{new}) 쌍을 유지함으로써 서비스 거부 공격을 통한 비동기화 문제에 안전하다고 주장하고 있다. 하지만 공격자가 제안 기법은 리더에서 태그로 전송하는 M_2에 대하여 한 번의 서비스 거부 공격을 한다면 태그에서 키(K_i)가 업데이트 되지 않더라도 K_{old}에 K_i값이 저장되어 있기 때문에 동기화를 유지할 수 있다. 그러나 두 번 연속으로 서비스 거부 공격을 한다면 DB에 저장된 (K_{old}, K_{new})의 쌍과 태그에 저장된 K_i 사이에 더 이상 공통된 값이 없게 됨으로 동기화가 깨지게 된다. 이는 DB에서 매 세션마다 특정 태그를 인증할 때 K_i의 업데이트 상태를 체크하지 않아 발생하는 문제이다.
2) 전방 안정성에 대한 취약성 : Chien과 Chen은 공격자가 태그 메모리에 저장된 (K, P, EPC_x) 값을 알더라도 전방 안전성을 만족한다고 주장하고 있다. 하지만 공격자가 m번째 세션에서 메모리에 저

장된 값(K_m, P_m, EPC_x)을 알아낸다면 이전 n번째 세션에서 도청하여 저장하고 있는 (M_1, N_1, N_2) 값들과 함께 $M_1 \oplus CRC(EPC_x \| N_1 \| N_2)$을 계산하여 인증키 K_n을 알아 낼 수 있다. 따라서 공격자는 다음과 같이 $K_m = PRNG_{m-n}(K_n)$인지도 계산할 수 있게 되어 m번째 세션의 인증키와 n번째 세션의 인증키의 연계성을 찾을 수 있게 된다. 따라서 전방 안전성을 만족하지 못하며 이로 인해 위치 추적도 가능하게 된다.

- DB에서의 효율성 분석

도전-응답 기반의 기법들은 상호 인증을 위해서 랜덤 값을 사용한다. 따라서 리더의 요청에 태그는 매 세션마다 랜덤 값으로 응답하게 된다. DB는 이러한 기법들에서 특정 태그를 찾기 위해 모든 태그에 대하여 전수조사를 해야 한다. [18]에서 이러한 전수조사 방식에 대한 비효율성을 테스트하였다. 216 태그가 존재할 때 특정 태그 하나를 찾는데 최악의 경우 7.87초가 걸리며 평균은 4.10초가 걸리는 것을 확인할 수가 있다. 만약 100개의 태그를 한꺼번에 인식하기 위해서는 평균 410초가 소요되며, 이러한 인식 시간은 태그의 수가 증가할 수록 비례하여 증가하게 된다. 따라서 이러한 전수조사 방식은 매우 비효율적이며 RFID 시스템에 적합하지 않다.

Ⅲ. 제안하는 상호 인증 프로토콜

3.1 용어 정의

[표 1]은 제안 프로토콜에서 사용되는 용어를 정의한 것이다.

[표 1] 용어 정의

표기법	설 명
BF_x	각 Tag_x의 블룸필터 값
CRC	16비트 순환중복검사 함수
DB	백-엔드-데이터베이스
Data	각 Tag_x와 관련된 사물의 정보
EPC_x	각 Tag_x의 고유 ID
K_{old}	DB 와 Tag_x의 이전 인증키
K_{new}	DB 와 Tag_x의 새로운 인증키
K_i	i번째 세션의 인증키
PRNG	16비트 의사난수생성 함수
Reader	리더
Tag_x	태그

3.2 가정

이전에 제안되었던 기법들과 같이, 태그와 리더사이의 통신 채널은 무선 주파수를 이용한 안전하지 않은 채널이고, DB와 리더의 통신 채널은 안전한 채널이라고 가정한다. 태그는 Gen2 표준을 따르며 순환중복검사 함수와 의사난수생성 함수만을 사용한다.

3.3 공격 모델

제안하는 기법에서 다음과 같은 공격 모델을 고려한다.

- 스푸핑 공격(Spoofing Attack)

공격자는 비 인가된 리더를 사용하여 태그로부터 정보를 수집한다. 이후 정당한 리더의 요청에 수집한 정보로 응답한다. 공격자는 이로부터 태그의 인증과정을 통과할 수 있다.

- 재생 공격(Replay Attack)

공격자는 태그와 리더사이의 전송되는 데이터를 도청한 후 이후 세션에서 재전송 한다. 이로 부터 공격자는 태그의 인증과정을 통과할 수 있다.

- 서비스 거부 공격(Denial of Service)

공격자는 RFID 시스템의 정상적인 작동을 방해하기 위해서 매우 많은 수의 인가되지 않는 메시지를 전송하거나 다른 방법(power interruption, hijacking)으로 태그의 정상적인 작동을 무력화 시켜 비동기화 문제를 야기 시킨다.

- 물리적 공격(Tampering Attack)

태그는 저가 기반에서 제조되었기 때문에 메모리 보호 장치가 없다. 따라서 공격자는 물리적 공격을 통하여 메모리에 저장되어 있는 값을 알아 낼 수 있다. 이러한 물리적 공격으로부터 태그의 복제[1]와 같은 다른 공격이 있을 수 있지만 이는 다른 분야에서 활발히 연구 되고 있으며 이에 대한 내용은 본 논문에서는 고려하지 않는다.

3.4 보안 및 프라이버시 요구사항

본 논문에서 제안하는 기법은 위에서 설명한 다양한

1) 태그의 복제를 막기 위해서 태그의 제조 당시 생성되는 제조 넘버(Serial Number)를 활용하는 방법이 제안되었음.

공격으로부터 다음과 같은 보안 및 프라이버시 요구사항을 고려한다.

- 기밀성(Confidentiality)

태그에서 리더로 전송되는 데이터는 사용자의 프라이버시를 보장해야 한다. 따라서 태그에서 리더로 전송되는 데이터는 정당한 사용자에게만 의미가 있어야하며 허가되지 않은 리더에게는 도청이 되더라도 의미가 없어야 한다.

- 익명성(Anonymity)

태그에서 리더로 전송되는 데이터를 통하여 위치 추적 및 감시가 이루어 지지 않도록 해야 한다. 이를 위해서는 다음과 같이 구별불가능성(indistinguishability)과 전방안전성(forward security)을 동시에 만족해야 한다.

(a) 구별 불가능성

태그에서 전송되는 데이터를 통하여 이것이 어떠한 태그에서 전송된 값인지를 구분할 수 없어야 한다.

(b) 전방 안전성

공격자가 현재 태그에 저장된 데이터 값을 알았다 할지라도 그 정보를 이용하여 이전에 생성한 데이터를 추적할 수 없어야 한다. 즉 공격자가 현재 알고 있는 태그의 데이터를 통하여 이전에 생성하였던 데이터들과 연계시킬 수 없어야 한다.

- 인증(Authentication)

DB와 태그간의 상호 인증은 서로가 정당한 개체인지를 확인함으로써 RFID 시스템이 정상적인 서비스를 행할 수 있게 한다. 이는 스푸핑 공격 및 재생 공격을 탐지할 수 있게 하며 서비스 거부 공격 및 공격자의 데이터 변경을 통한 불법적인 태그의 재-쓰기를 막을 수 있다.

3.5 제안 프로토콜

제안 상호 인증 프로토콜은 [그림 3]과 같으며 다음과 같이 초기 설정 단계와 상호 인증 단계로 나눌 수 있다.

3.5.1 초기 설정 단계

1) 각각의 Tag_x에 대하여 DB는 EPC_x, 초기 인증키 K_0을 생성하고 (EPC_x, K_0)를 Tag_x에 저장한다. 그리고 DB는 Tag_x에 대한 (1) EPC_x (2) 이전의 인증키 $K_{old}(=K_0)$ (3) 새로운 인증키 $K_{new}(=K_0)$ (4) BF(블룸 필터)의 값 (5) Tag_x에 대한 기타 정보 Data를 저장한다.

2) DB에서 특정 태그를 찾기 위해 블룸 필터를 사용할 수 있다. 방법은 2장 블룸필터의 소개에서도 말했듯이 각각의 Tag_x의 EPC_x를 사용하여 원소의 집합을 만든다$\{s_1,s_2,.....,s_n\}$. 그리고 각각의 원소에 대하여 k개의 해쉬 함수의 값을 구하여 m비트의 블룸 필터 BF(CRC(EPC_x ‖ 1) ‖ PRNG(1), CRC(EPC_x ‖ 2) ‖ PRNG(2),.....,CRC(EPC_x ‖ n) ‖ PRNG(n)) 셋을 구성하고 이를 DB에 저장한다. 이후 리더로부터 전송된 T_1에 대한 멤버쉽 테스트를 통하여 원하는 태그의 데이터를 DB에서 쉽게 찾을 수 있으며 효율성을 높일 수 있다.

3.5.2 상호 인증 단계

1) (Challenge) Reader → Tag_x : R_r

리더는 랜덤 값 R_r을 생성하고 Tag_x에 R_r와 함께 질의 요청한다. R_r은 공격자의 스푸핑 공격 및 재생 공격을 막기 위해 사용된다.

2) (Response) Tag_x → Reader : T_1, T_2

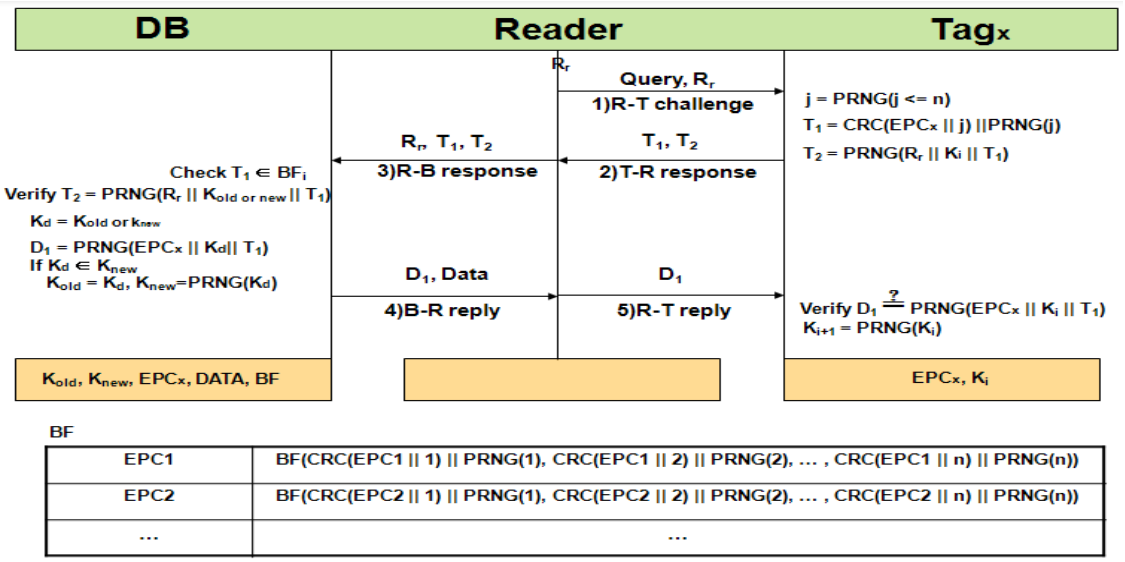
Tag_x는 의사난수생성 함수를 사용하여 난수 j를 생성하고 T_1=CRC(EPC_x ‖ j) ‖ PRNG(j)를 계산한다. 그리고 T_1함께 리더로부터 전송된 랜덤 값 R_r, 인증키 K_i를 사용하여 T_2=PRNG(R_r ‖ K_i ‖ T_1)도 계산한 후 T_1, T_2를 리더에게 전송한다. T_1은 멤버쉽 테스트 시에 사용되며 T_2와 함께 매 세션 변경된다.

3) (Response) Reader → DB : R_r, T_1, T_2

리더는 Tag_x에서 전송된 T_1, T_2와 함께 자신이 생성한 R_r를 DB에 전송한다. 그리고 DB는 다음과 같은 과정을 수행한다.

(1) 멤버쉽 테스트를 행한다($T_1 \in BF_i$).

- DB는 리더로부터 전송된 T_1에 대하여 간단한 연산과 비교과정을 통한 멤버쉽 테스트를 실행하고, Tag_x를 찾는다. 전수조사에 비해 특정 태그를 빠르고 쉽게 찾을 수 있다.



BF

EPC1	BF(CRC(EPC1 || 1) || PRNG(1), CRC(EPC1 || 2) || PRNG(2), … , CRC(EPC1 || n) || PRNG(n))
EPC2	BF(CRC(EPC2 || 1) || PRNG(1), CRC(EPC2 || 2) || PRNG(2), … , CRC(EPC2 || n) || PRNG(n))
…	…

[그림 3] 제안하는 상호 인증 프로토콜

- 찾지 못했다면 세션을 종료한다.

(2) Tag_x를 검증한다.(T_2=PRNG(R_r ‖ $K_{old\ or\ new}$ ‖ T_1)

- DB는 K_{old}의 값을 사용하여 인증하였는지 또는 K_{new}의 값을 사용하여 인증하였는지 체크한다. 그리고 K_d에 현재 인증 시 사용한 키(K_{old} or K_{new})를 임시 저장한다.
- 인증하지 못했다면 세션을 종료한다.

(3) 리더와 Tag_x에게 전송할 (D_1, Data)을 생성한다.

- Tag_x에서 공유 인증키 K_i를 업데이트 할 때 정당한 DB를 검증하기 위한 D_1=PRNG(EPC_x ‖ K_d ‖ T_1)를 계산한다.
- DB는 D_1, 태그와 관련된 Data를 리더에게 전송한다.

(4) 인증키(K_{old}, K_{new})를 업데이트 한다.

- DB는 Tag_x를 인증시 K_{new}의 값으로 인증하였다면 다음과 같이 인증키를 업데이트 한다, K_{old}= K_d, K_{new}=PRNG(K_d).

4) (Reply) DB → Reader : D_1, Data

정당한 리더는 Data를 읽고 사물의 정보를 얻는다, D_1은 Tag_x에 전송한다.

5) (Reply) Reader → Tag_x : D_1

Tag_x는 PRNG(EPC_x ‖ K_i ‖ T_1))를 계산하여 리더로부터 전송 받은 D_1의 값과 비교 한다. 같다면 K_i의 값을 K_i+1으로 업데이트 하고 세션을 종료한다(상호 인증 완료), K_i+1=PRNG(K_i). 다르다면 업데이트를 하지 않고 현재 세션을 종료한다.

Ⅳ. 안전성 및 효율성 분석

4.1 안전성 분석

본 절에서는 3장에서 설명한 공격 모델로부터 제안하는 상호 인증 프로토콜이 안전함을 보이고 이로부터 프라이버시 요구사항을 만족함을 보인다.

- 스푸핑 공격에 대한 안전성 : 공격자는 자신이 생성한 랜덤 값 R_r과 함께 태그에 요청하여 (T_1, T_2)를 얻는다. 이 후 합리적인 리더가 자신이 생성한 랜덤 값 Rr‘과 함께 태그에 요청할 때 공격자는 자신이 저장하고 있던 값 (T_1, T_2)로 응답하여 스푸핑 공격을 시도 할 수 있다. 하지만 PRNG(R_r ‖ K_i ‖ T_1) ≠ PRNG(R_r‘ ‖ K_i ‖ T_1) 이기 때문에 공격자는 정당한 태그인척 할 수가 없다. 따라서 본 제안 기법은 스푸핑 공격에 안전하다.
- 재생 공격에 대한 안전성 : 공격자는 리더와 태그사이에서 도청을 통하여 (R_r, T_1, T_2) 데이터를 얻는다. 이후 합리적인 리더의 요청에 도청한 데이터 (T_1, T_2)로 재전송 공격을 할 수 있다. 하지만 이와

같은 경우에도 스푸핑 공격에서와 마찬가지로 DB에서의 인증과정을 통과 할 없다.

- 서비스 거부 공격에 대한 안전성 : 공격자는 상호 인증 5)단계에서 강한 전파의 사용 및 가로채기 공격을 통하여 D_1이 전송되는 것을 막음으로써 태그에서의 인증키 K_i의 K_i+1로의 업데이트를 방해할 수 있다. 하지만 이와 같은 경우가 발생하더라도 이후 세션에서 DB는 이전 공유키 K_{old}를 사용하여 인증하기 때문에 동기화를 유지할 수 있다. 또한 연속적인 서비스 거부 공격을 하더라도 K_{old}의 값으로 인증되었을 경우에는 업데이트를 하지 않기 때문에 동기화를 계속해서 유지할 수 있다.
- 물리적 공격에 대한 안전성 : 공격자의 물리적 공격을 통하여 태그 메모리의 내용이 노출 될 수 있다. 그러나 현재 세션에서의 태그 메모리의 내용이 노출 된다 할지라도 과거 도청한 (T_1, T_2)의 정보를 가지고 이전 인증키를 찾아 낼 수가 없으며 이로부터 현재의 태그와의 연관성을 찾기도 힘들다. 따라서 본 프로토콜은 물리적인 공격에 안전하다.

- 기밀성 보장 : 공격자가 태그에서 DB로 전송되는 정보(R_r, T_1, T_2)들을 도청한다고 할지라도 이는 공격자에게는 의미 없는 값이며 이로부터 태그와 관련된 어떤 정보(EPC) 알아 낼 수 없다. 따라서 기밀성을 보장하며 프라이버시를 보장한다.
- 익명성 보장

(a) 구별 불가능성 : Tagx는 리더가 질의를 할 때마다 매번 랜덤 값으로 응답하기 때문에 리더와 공격자는 수신한 데이터가 어떠한 태그에서 나온 값인지를 알 수 없어 구별 불가능성 만족한다.

(b) 전방 안전성 : 위에서 말한 것과 같이 물리적인 공격을 통하여 태그의 메모리에 저장된 내용을 알아낸다 할지라도 이로부터 이전의 세션 정보를 획득할 수 없으며 현재 세션에서 획득한 정보와의 연관성을 주기도 어렵기 때문에 전방 안전성을 만족하게 된다.

따라서 두 가지 성질을 모두 만족함으로 익명성을 보장한다.

- 상호 인증 보장 : 본 프로토콜은 도전-응답 방식의 DB와 태그가 매 세션마다 랜덤 넘버(R_r, T_1)를 사용함으로서 서로를 상호 인증을 한다. 특히 DB는 매 세션마다 R_r을 포함하여 계산된 T_2 검증을 통하여 태그를 인증하게 되며 이를 통해 현재 세션에서 태그가 프로토콜에 참여하고 있다는 것을 확인 할 수 있다, 그리고 태그도 T_1이 포함된 D_1에 대한 정당성 검증을 통하여 DB를 인증하게 된다.

[표 2]는 Gen2 기반에서 제안된 기법들에 대하여 안전성을 비교하였다. [표 2]에서 보듯이 본 논문에서 제안하는 기법은 기본의 Gen2에 기반에서 제안된 기법들과 다르게 보안 및 프라이버시 보호를 위한 요구 사항을 모두 만족함을 볼 수 가 있다.

[표 2] Gen2 기반 제안 기법들의 안전성 비교

제안 기법	[3]	[2]	Our Protocol
프라이버시	O	O	O
익명성	X	X	O
스푸핑 공격 저항	X	O	O
재생 공격 저항	X	O	O
DOS 공격 저항	X	X	O
전방 안전성	X	X	O
상호 인증	O	O	O
리더 인증	X	X	O

4.2 효율성 분석

본 절에서는 태그와 DB에서의 효율성에 관하여 분석한다.

- 태그에 대한 효율성 : 제안 기법은 단지 Gen2에서 지원하는 순환중복검사 함수와 의사난수생성 함수만을 사용하여 기존의 기법들이 만족하지 못하는 보안 및 프라이버시 문제를 해결하였다. 또한 태그에서 EPC와 DB와 공유하는 인증키 K값만을 저장함으로 해서 가격이 비싼 비휘발성 메모리의 사용을 최소화하였다.
- DB에 대한 효율성 : 본 논문에서 제안하는 기법의 효율성을 Chien과 Chen의 기법과 비교하기 위해 태그의 개수를 최대 2^{16}개라고 가정한다. Chien과 Chen의 기법에서 태그가 보내는 M_1값의 길이가 중환중복검사 함수의 출력값의 길이와 같기 때문에 만약 태그의 수가 2^{16}개보다 많다면 DB는 태그를 유일하게 결정할 수 없게 된다.

만약 제안하는 기법이 DB에서의 연산을 완전히 없애고 싶다면 각 태그마다 $CRC(EPC_x \| j) \| PRNG(j)$, $(0 \le j \le 2^{16}-1)$ 값을 모두 저장하고 있으면 된다. 이때는

각 태그마다 32×2^{16}비트(256KB)씩 저장해야 하므로 총 $32\times2^{16}\times2^{16}$비트(16GB)의 추가적인 저장 공간이 필요하다. 또한 기존의 기법들과 같이 DB가 값을 추가적으로 저장하지 않는다면 태그가 보내주는 T_1, T_2값을 인증하기 위해 태그를 찾을 때 까지 최대 태그의 수만큼 연산하게 된다.

하지만 블룸필터를 사용함으로써 저장량과 연산량 사이의 Trade-Off를 이용하여 사용 환경에 맞는 시스템을 적절히 구성할 수 있게 된다. 블룸필터의 긍정오류율 계산식

$$f=(1-(1-\frac{1}{m})^{kn})^k\approx(1-e^{-\frac{kn}{m}})^k$$

에서 k, n, m 사이의 최적값을 찾기 위해 다음과 같이 계산한다. $g=\ln(f)$라 하고 양변을 미분하면

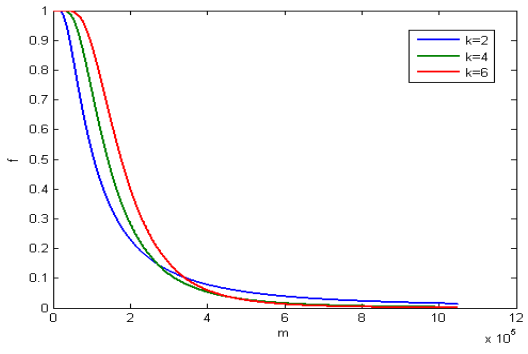
$$\frac{dg}{dk}=\ln(1-e^{-\frac{kn}{m}})+\frac{kn}{m}\cdot\frac{e^{-\frac{kn}{m}}}{1-e^{-\frac{kn}{m}}}$$

이다. k의 최적값을 구하기 위해 $\frac{dg}{dk}=0$ 을 k에 대해 정리하면

$$k=\ln2\cdot\frac{m}{n}\quad\Leftrightarrow\quad\left(\frac{1}{2}\right)^k=(0.6185)^{\frac{m}{n}}$$

이다.

예를 들면 제안하는 기법에서 $n=2^{16}$, $m=2^{19}$이라고 가정할 때 k의 최적값은 6이다. 이 때 $f=0.0216$이므로



[그림 4] k값에 따른 긍정오류율

[표 3] Gen2 기반 제안 기법들의 효율성 비교

프로토콜			[3]	[2]	Our Protocol
저장량	태그		3ℓ	3ℓ	2ℓ
	DB		3ℓ	5ℓ	3ℓ+|BF|
계산량	태그	CRC	3	2	1
		PRNG	2	3	5
	DB	Search	H	H	L
통신량			8	5	5

ℓ : 하나의 데이터 유닛에 대한 비트의 길이
|BF| : 블룸필터 데이터 셋
H : High, L : Low

$0.0216\times2^{16}=1416$개 만큼의 긍정오류가 생긴다. 따라서 블룸필터를 이용하여 선택된 1417개(긍정오류 개수 + 실제 태그)의 태그에 대해서만 T_2값을 계산하면 태그를 인증할 수 있게 된다. 이 때 DB의 연산량은 6번의 해쉬함수와 최대 1417번의 순환중복검사 함수, 의사난수생성 함수의 사용이 요구된다. 또한 블룸필터를 저장하기 위해 추가적으로 요구되는 저장량은 4GB이다($2^{19}\times2^{16}$bit = 4GB).

[그림 4]은 k값에 따른 긍정오류율을 나타낸 그래프이다. 각각의 그래프에서 m값이 커질수록 긍정오류율이 줄어드는 것을 확인할 수 있다. 이와 같은 방법으로 블룸필터를 이용하면 DB에서의 저장량과 연산량의 Trade-Off를 이용하여 사용 환경에 맞는 시스템을 구성할 수 있게 된다.

[표 3]는 Gen2 기반에서 제안된 기법들에 대한 효율성을 분석하였다. 표에서도 보듯이 제안 기법은 태그에서의 비휘발성 메모리의 사용을 하나 줄임으로써 저장량을 최소화 하였다. 또한 기존 기법들과 달리 DB에서 전수 조사 방식을 사용하지 않음에 따라 계산량을 최소화하여 효율성을 높였다. 그리고 상호 인증에서 동기화를 유지하기 위해 필요한 최소한의 통신량을 유지함으로써 통신량에서의 유연함을 보였다.

Ⅴ. 결 론

본 논문에서는 Gen2 기반의 프로토콜에서 사용자 프라이버시 및 보안 문제를 해결하고 실제 환경에 적용 가능한 효율성이 향상된 새로운 상호 인증 프로토콜을 제안하였다. 특히 최근 Chien과 Chen이 Gen2 기반에서 제안한 프로토콜에 대해서 서비스 거부 공격이 가능하고 전방 안전성을 만족하지 않음을 보이고 이를 개선

하였다. 또한 도전-응답 기반의 프로토콜들이 DB 측면에서 전수 조사를 해야 하는 비효율성을 보이고 이를 개선하기 위하여 블룸필터를 사용한 멤버쉽 테스트 기법을 제안하였다. 이 방법은 전수 조사를 하지 않아도 되기 때문에 효율성이 높다. 따라서 본 논문에서 제안하는 기법은 수동형 RFID 시스템의 보안 및 프라이버시 침해 문제를 해결함과 동시에 실제 환경에서도 적용 가능하도록 태그와 DB에서의 효율성을 높인 새로운 상호 인증 프로토콜이다.

참고문헌

[1] Andrei broder and Michael Mitzenmacher, “Network Applications of Bloom Filters : A Survey”, Internet Mathematics, vol 1, no 4, 2004, pp 485-509(SAC), 2005.

[2] H.Y. Chien and Che-Hao Chen, “Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards”, In Computer Standards & Interfaces, 2006

[3] D.N. Duc, J. Park, H. Lee, K. Kim, “Enhancing security of EPCglobal GEN-2 RFID tag against traceability and cloning”, The 2006 Symposiumon Cryptography and Information Security, 2006.

[4] EPCglobal Inc., "Radio Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960MHz Version 1.0.9., http://www.EPCgloballinc.org

[5] A.D. Henrici, P. MÄuller, “Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers”, In theProceedings of PerSec'04 at IEEE PerCom, 2004, pp. 149-153.

[6] A. Juels, “Strengthening EPC tag against cloning”, To Appear in the Proceedingsof WiSe '05, 2005.

[7] A. Juels, “RFID Security and Privacy: A Research Survey”, IEEE Journal, Vol. 24, Issue:2, pp. 381-394, 2006.

[8] S. Karthikeyan, M. Nesterenko, “RFID security without extensive cryptography”, Proceedings of the 3rd ACM Workshop on Security of AdHoc and Sensor Networks, 2005, pp. 63-67.

[9] D. Molnar, D. Wagner, “Privacy and security in library RFID: issues, practices, and architectures”, Conference on Computer and Communications Security －CCS'04, 2004, pp. 210-219.

[10] M. Ohkubo, K. Suzki, S. Kinoshita, “Cryptographic approach to ‘privacyfriendly’ tags”, RFID Privacy Workshop, 2003.

[11] K. Rhee, J. Kwak, S. Kim, D. Won, “Challenge-response based RFID authentication protocol for distributed database environment”, International Conference on Security in Pervasive Computing －SPC 2005, 2005, pp. 70-84.

[12] S. A. Weis, “Security and privacy in radio-frequency identification devices”, Masters Thesis MIT, 2003.

[13] S.A. Weis, S.E. Sarma, R.L. Rivest, D.W. Engels, “Security and privacy aspects of low-cost radio frequency identification systems”, The Proceedings of the First Security in Pervasive Computing, LNCS, vol. 2802, 2003, pp. 201－212.

[14] J. Yang, J. Park, H. Lee, K. Ren, K. Kim, “Mutual authentication protocol for low-cost RFID”, Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, 2005.

[15] J. Yang, K. Ren, K. Kim, “Security and privacy on authentication protocol for low-cost radio”, The 2005 Symposium on Cryptography and Information Security, 2005.

[16] 김진호, 서재우, 이필중, “멤버쉽 테스트를 이용한 RFID 인증 프로토콜”, 2007년도 정보보호학회 하계학술대회, vol. 17, no. 1, 2007, pp. 93-98

[17] 김진호, 서재우, 이필중, “저비용 RFID 시스템에 적합한 효율적인 인증 방법”, 2008년 정보보호학회논문지, 18권, 제 2호, 2008, pp. 117-128

[18] 원태연, 천지영, 최은영, 이동훈, “RFID 보안시스템에서 전수조사 방식에 대한 성능테스트”, 2007년도 정보보호학회 동계학술대회, vol. 17, no. 2, 2007, pp. 203-206.

<著 者 紹 介>

원 태 연 (Tae Youn Won) 학생회원
2007년 2월 : 고려대학교 전산학과 졸업
2007년 3월~현재 : 고려대학교 정보경영공학전문대학원 석사과정
<관심분야> 정보보호, RFID 보안 기술, 무선 보안, PET 기술

천 지 영 (Ji Young Chun) 학생회원
1997년 2월 : 이화여자대학교 수학과 학사
2006년 2월 : 단국대학교 수학과 석사
2006년 3월~현재 : 고려대학교 정보보호대학원 박사과정
<관심분야> 암호 이론, PET 기술, 유비쿼터스 보안

박 춘 식 (Choon Sik Park) 종신회원
1981년 광운대학교 졸업
1983년 한양대학교 전자통신전공 석사
1995년 일본동경공업대학교 정보보호전공 박사
1982년~1999년 한국전자통신연구원 부장
2000년~현재 한국전자통신연구원부설연구소 책임연구원
<관심분야> : 암호이론, 정보이론, 네트워크보안

이 동 훈 (Dong Hoon Lee) 종신회원
1983년 8월 : 고려대학교 경제학사
1987년 12월 : Oklahoma University 전산학 석사
1992년 5월 : Oklahoma University 전산학 박사
1993년 3월~1997년 2월 : 고려대학교 전산학과 조교수
1997년 3월~2001년 2월 : 고려대학교 전산학과 부교수
2001년 2월~현재 : 고려대학교 정보보호대학원 교수
<관심분야> 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술