情報保護學會論文誌
第16卷 第6號, 2006. 12

분산시스템 환경에 적합한 효율적인 RFID 인증 시스템*

최 은 영†, 이 수 미, 임 종 인, 이 동 훈‡

고려대학교 정보경영공학 전문대학원

Efficient RFID Authentication protocol for Distribution Database Environment

Eun Young Choi†, Su Mi Lee, Jong In Lim, Dong Hoon Lee‡

Graduate School of Information Management and Security , Korea University

요 약

무선 주파수 인식 (RFID: Radio Frequency Identification) 시스템은 원거리 사물 인식 시스템의 중요한 기술로 인식되고 있다. 그러나 RFID 태그의 사용은 시스템 보안과 프라이버시 침해의 문제를 발생시킨다. 저가형의 RFID 시스템은 연산 능력, 전원 공급, 데이터 저장량 등에서 제약을 받는다. 그러므로 RFID 시스템에서의 태그의 연산량은 저가형의 RFID 시스템 환경에서 중요한 요소로 고려되어야만 한다. 본 논문에서는 태그가 단 한 번의 해쉬 연산만으로 상호 인증을 수행하는 효율적인 인증 프로토콜을 제안하며, 제안된 기법은 분산시스템에 적용 가능하기 때문에 유비쿼터스 환경에 적용 가능하다.

ABSTRACT

Radio Frequency identification (RFID) will become an important technology in remotely object identification systems. However, the use of RFID tags may create new threats to the security and privacy of individuals holding RFID tags. These threats bring several problems which are information leakage of a tag, location trace of individuals and impersonation of a tag. Low-cost RFID systems have much restrictions such as the limited computing power, passive power mechanism and low storage space. Therefore, the cost of tag's computation should be considered as an important factor in low-cost RFID systems. We propose an authentication protocol, OHLCAP which requires only one one-way hash function operation and hence is very efficient. Furthermore, our protocol is suitable to distribution database environment. Hence our scheme can be applied to ubiquitous computing environment.

Keywords : *Low-cost RFID system, Privacy, Authentication protocol*

Ⅰ. 서 론

RFID (Radio Frequency Identification) 시스템은 무선 주파수를 이용하여 물리적인 접촉 없이 개체에 대한 정보를 읽거나 기록하는 자동인식

접수일: 2006년 7월 14일 ; 채택일: 2006년 10월 24일
* 본 연구는 과학재단 특정기초연구(R01-2004-000-10704-0) 지원으로 수행되었습니다.
† 주저자, bluecey@cist.korea.ac.kr
‡ 교신저자, donghlee@korea.ac.kr

기술 시스템이다. 이러한 RFID 시스템은 2차 세계대전 당시 영국에서 자국 자동 식별용으로 개발되어 최초로 사용되기 시작하였다. 현재 RFID 시스템은 물류 및 유통 분야에서 사용되던 바코드에 비해서 저장 능력이 뛰어나고 비접촉식이라는 이점을 가진다는 점에서 바코드를 대체할 자동 인식 시스템으로 주목 받으면서 많은 연구가 이루어지고 있다.

RFID 시스템은 리더의 질의에 대하여 사물, 사람 등의 식별 정보를 무선 통신을 사용하여 전송하는 태그, 태그가 전송하는 데이터를 수신하여 태그를 인식하거나 태그에 새로운 정보를 다시 쓰는 역할을 수행하는 장치인 리더, 리더로부터 전송된 임의의 태그의 정보를 통해서 개체를 식별하고 수집된 정보의 진위를 판별하는 기능을 수행하는 데이터베이스로 구성되어 있다. 일반적으로 태그와 리더 사이의 통신 채널은 공격자의 공격에 안전하지 않으며, 리더와 데이터베이스 사이의 통신 채널은 공격자의 공격에 안전하다고 가정한다.

RFID 시스템의 물리적인 접촉 없이도 인식이 가능하다는 특징은 시스템의 안전성과 개인의 정보 노출, 위치 추적 등의 프라이버시 측면에서 여러 가지 문제들을 발생 시킨다. (1) 시스템의 안전성 측면에서, 리더는 태그가 정당한 태그인지를 확인해야 한다. 만약 도둑이 저가의 물건에 태그 인식 정보를 얻는다면 고가의 물건에 탑재된 태그에 이 정보를 입력하여 저가의 가격으로 고가의 물건을 구매할 수 있다. (2) 프라이버시 측면에서, 태그는 리더가 정당한 리더인지를 확인해야 한다. 예를 들어, RFID 태그의 정보가 리더에 전송될 때, 태그와 리더의 통신에 제 삼자가 존재하여서 도청한 정보를 사용하여 사용자의 위치를 추적할 수 있으며, 이것은 사용자의 프라이버시 침해를 야기 시킨다. RFID 시스템의 프라이버시 침해 문제를 해결하기 위해 영구적으로 태그를 무력화 시키는 물리적인 기법과 해쉬 함수, 암호학적 알고리즘 또는 단순한 연산자를 사용하는 다양한 기법들이 제안되었다[1-11,15-17].

본 논문에서는 기존에 제안된 해쉬 기반의 가장 효율적인 기법으로 제안되어 있는, 태그가 두 번의 해쉬 함수를 수행하는 기법보다 효율적인 저가형의 RFID 시스템을 제안하였다. 제안 기법에서 태그를 그룹으로 나누어 관리함으로써, 태그가 단 한 번의 해쉬 연산을 수행하기 때문에 저가의 태그에 적합하다. 또한 제안 기법의 그룹이라는 구조적 특성으로 인해 제안 기법은 분산데이터 베이스에 적합한 구조를 가지게 되므로 유비쿼터스 환경에 적용 가능하다. 본 논문의 구성은 다음과 같다. 2장에서는 기존에 제안된 기법들에 대해 분석하고 3장에서는 제안하는 프로토콜에 대해서 기술하고 4장에서는 제안하는 기법의 안전성과 효율성을 분석한다. 마지막으로 5장에서는 결론을 맺는다.

II. 기존에 제안된 기법들에 대한 분석

본 장에서는 제안 기법과 관련된 해쉬 기반의 기존 기법들에 대해 안전성과 효율성 측면에서 분석하고 한다. 우선, RFID 시스템의 문제점에 대해 간략히 알아보고, 제안 기법과 관련된 해쉬 기반의 기법들에 대해 알아본다.

2.1 RFID 시스템 구성

RFID 시스템은 세 가지 요소, 태그 (트랜스폰더), 리더 (트랜시버), 데이터베이스 로 구성되며, 각각의 기능은 다음과 같다. (그림1) 은 RFID 시스템의 구성을 나타낸 것이다.

○ 태그 (Tag) 또는 트랜스폰더 (Transponder) : 태그는 RFID 시스템에서 리더의 질의에 대하여 사물, 사람 등의 식별 정보를 무선 통신을 사용하여 전송하며, 태그의 구성은 무선 통신을 위한 안테나와 연산을 수행하고 정보를 저장하는 마이크로 칩으로 이루어져있다. 태그는 전력을 공급받는 방법에 따라 능동형 태그 (active tag) 와 수동형 태그 (passive tag) 로 분류된다.

- 능동형 태그 (active tag) : 능동형 태그는 자체 내장된 배터리를 통해서 전력을 공급한다. 자체 내장된 배터리를 사용하기 때문에 원거리 정보 전송이 가능하다. 하지만 자체 내장 배터리가 내장되어 있어서 태그의 가격이 비싸며, 태그의 수명도 배터리에 종속적이라는 단점을 갖는다. 능동형 태그는 토목·건축분야, 의료분야 등에 사용된다.
- 수동형 태그 (passive tag) : 수동형 태그는 리더로부터 수신한 전자기파로부터 유도한 전류를 전원으로 사용한다. 태그의 전송 전력이 리더에 비해 낮기 때문에 근거리 통신이 가능하다. 수동형 태그는 배터리를 내장하고 있지 않기 때문에 능동형 태그 보다 가격이 싸며, 태그

의 수명이 반영구적이다. 수동형 태그는 물류관리, 전자 상거래, 교통 분야, 전자물체감시(EAS) 시스템 분야 등에 사용된다.

○ 리더 (Reader) 또는 트랜시버 (Transceiver) : 리더는 태그가 전송하는 데이터를 수신하여 태그를 인식하거나 태그에 새로운 정보를 다시 쓰는 역할을 수행하는 장치이다. 리더가 태그에 무선 통신을 사용하여 태그에 정보를 요청하고 받은 정보를 데이터베이스에 전송한다.

○ 데이터베이스 (Database) : 데이터베이스는 태그에 관련된 정보를 저장하고 관리하는 역할을 한다. 데이터베이스는 정당한 리더로부터 전송된 임의의 태그의 정보를 통해서 개체를 식별하고 수집된 정보의 진위를 판별하는 기능을 수행한다. 데이터베이스는 연산 능력이 낮은 리더나 태그를 대신하여 연산을 수행하기도 한다.

RFID 시스템은 기본적으로 리더와 데이터베이스 사이는 미들웨어를 사용하여 안전한 채널을 통해 통신이이루어진다. 이와 달리 RFID 시스템에서 리더와 태그는 비 접촉의 무선 통신으로 데이터를 주고받기 때문에 불안전한 통신으로 가정한다.

2.2 RFID 시스템의 문제점

RFID 시스템은 리더와 태그 간에 무선 통신을 사용하며 태그의 고유 정보에 대한 무분별하게 전송하는 동작 으로 인해서 여러 위협에 노출되기 쉽다. 이러한 취약점들은 공격자가 기존의 다른 시스템에서 보다 적은 노력으로 원하는 정보를 얻을 수 있게 한다. RFID 시스템에서 공격자들은 리더와 태그간의 통신 도청, 태그 위조 등의 공격을 수행 할 수 있다. 이러한 공격을 통해서 공격자는 사용자의 프라이버시를 침해 할 수 있다. 그러므로 다음과 같은 문제점들을 고려하여 RFID 시스템을 설계하여야 한다.

1) 사용자의 개인정보 노출 문제점(프라이버시 침해)
: RFID 시스템이 널리 사용됨에 따라 사람들은 개체에 태그가 내장된 다양한 물건들을 지니게 될 것이다. RFID 시스템은 주위의 리더의 질의에 무분별하게 태그 고유의 정보를 전송하기 때문에 물건에 내장된 태그는 사용자가 다른 사람에게 알리고 싶지 않은 정보, 예를 들면, 고가의 물건의 소유, 특정 병력에 관한 약품 소지 등에 대한 정보를 제 삼자에게 제공할 수 있다. 그래서 사용자에 대한 다양한 정보가 사용자의 동의 없이 누출될 수 있다. 그러므로 안전한 RFID 시스템을 설계하기 위해서는 무선 통신을 사용하더라고 사용자의 프라이버시를 침해할 수 없도록 설계하여야 한다.

2) 사용자의 위치 추적 문제점 (프라이버시 침해)
: 사용자가 태그가 내장된 물건을 구매할 때, 공격자는 사용자와 태그의 고유 정보에 연관성을 줄 수 있다. 더구나 사용자는 태그가 내장된 물건을 지니고 다니기 때문에 공격자는 태그 고유 정보를 이용하여 사용자의 이동 경로를 추적할 수 있다. 이러한 문제점을 해결하기 위해서 RFID 태그의 질의에 대한 응답은 제 삼자에게 랜덤하게 보여서 구별 불가능 하여야 한다.

3) 위 조 : 이 공격은 능동적인 공격자에 의해 이루어지며 공격자는 정당하지 않은 개체를 정당한 것처럼 속여 인증과정을 통과하는 방법이다. 이러한 위조 공격은 두 가지 유형으로 나눌 수 있다.
- 재전송 공격의 경우, 공격자는 리더와 특정 태그 사이의 통신을 도청하여 저장한다. 그 이후 공격자는 리더의 질의에 대해 특정 태그로 임의의 태그를 위장하기 위해서 저장했던 메시지를 전송한다. 즉, 공격자는 임의의 태그를 특정 태그로 위조가능하다.
- 스푸핑 공격의 경우, 공격자는 리더로 위장하여 특정 태그의 정보를 얻는다. 이 과정은 재전송 공격과 달리 태그와 리더 사이의 하나의 세션이 완료되기 전에 필요한 정보를 태그로부터 얻고 그 세션을 종료한다. 공격자는 그 태그로부터 전송받은 데이터를 사용하여 리더를 속여 특정 태그인척 할 수 있다. 예로 들면, 상점에서 태그가 내장된 싼 가격의 상품에 공격자는 리더로 위장하여 인증 받을 수 있는 정보를 얻고 정상적인 인증과정을 위한 과정이 완료되기 전에 통신을 종료한다. 그 이후에 공격자는 고가의 상품을 구매하는 과정에서 싼 가격의 상품에서 얻은 데이터를 사용하여 고가의 상품을 싼 가격의 상품으로 인증 받고 구매할 수 있다.

RFID 시스템에서 공격자의 이러한 공격부터 시스템을 보호하기 위해서 리더와 태그 사이의 통신에서 상호 인증하는 과정이 필요하다.

2.3 기존에 제안된 프라이버시 보호 기법 분석

RFID 시스템의 프라이버시 침해의 문제점을 해결하기 위해 다양한 기법들이 제안되었다. 이러한 기법들은 사용자가 정당한 리더와 데이터베이스는 태그를 이용하여 사용자와 유용한 서비스가 가능하며, 정당하지 않은 개체들은 태그에 대한 어떤 정보도 얻지 못하도록 하여 사용자의 프라이버시를 보호하는 기법들이 제안되었다[2-5,7-10,14-16]. 기존에 제안된 방법들은 해쉬 함수, 암호화 알고리즘과 같은 암호학적 방법들을 사용하는 기법들[2, 4, 7-12, 16-17, 19-20]과 XOR 함수를 사용하는 기법들이 있다[3,18]. 본 절에서는 제안 기법 중에서 본 기법과 관련된 해쉬 함수 기반의 기법들에 대해서 살펴보도록 하겠다.

해쉬 기반 기법은 해쉬 함수의 일방향성 (One-Way)을 이용하여 태그의 정보를 보호하는 기법이다. 해쉬 함수를 사용하는 기법으로 대표적인 것이 해쉬 락 (hash lock) 기법이다[17]. 이 기법은 해쉬 함수를 사용한다는 점에서 저가의 태그에 적용될 수 있다. 그러나 리더와 태그 사이의 통신에서 고정된 해쉬 아이디 (metaID=hash(key)) 를 사용한다는 점에서 공격자가 태그의 위치를 추적할 수 있으며 이로 인해 사용자의 프라이버시도 침해된다. 이러한 문제점을 해결하기 위해, Weis은 태그가 의사 난수 생성기 (pseudo random generator) 사용하여 리더의 질의에 안된 기법들은 공격자의 재전송, 스푸핑 공격에 안전대해서 태그가 항상 랜덤한 값을 응답할 수 있도록 하는 기법을 제안하였다[17]. 그러나 [17]의 논문에 제하지 않다. 그 이외에도 해쉬 함수 기반의 기법이 제안되었으며 다음과 같다.

Ohkubo은 두개의 해쉬 체인을 사용하여 사용자의 프라이버시를 보호하는 기법을 제안하였다[12]. 그러나 이 기법은 데이터베이스가 리더의 질의에 대한 태그의 응답이 정당한 것인지를 확인하기 위해서 계산하여야 하는 해쉬 값이 태그의 수에 의존한다는 문제점을 갖는다. 그 이후, 이 기법의 효율성을 향상시키기 위한 여러 가지 기법들이 제안되었다[2, 16, 19]. 또한 Henrici은 일해쉬 함수를 사용하여 추적될 수 있는 태그의 ID를 변화 시키는 기법을 제안하였으나 공격자의 스푸핑 공격에 취약하다는 문제점을 가지고 있다[9]. 최근에는 해쉬 기반의 스푸핑 공격에도 안전한 기법이 Lee 등에 의해서 제안되었으며[10], 다양한 서비스 제공이 가능한 분산 환경에 적합한 해쉬 기반의 기법도 제안되었으나 이 기법도 데이터베이스가 데이터베이스에 저장된 태그의 수에 의존하여 계산하여야 한다는 점에서 시스템 적용에 문제점을 갖는다[11]. 그 이외에도 DOS 공격과 같은 특정 공격에 안전한 기법들도 제안되었다[8]. [표 1]에서 안전한 RFID 시스템의 요구사항을 고려하여 해쉬 함수 기반 기법들에 대한 안전성에 대해 간략히 나타낸다.

Ⅲ. 제안 프로토콜

본 장에서는 해쉬 기반의 상호 인증 프로토콜을 제안한다. 제안 프로토콜은 태그가 해쉬 연산을 한번

[표 1] 해쉬 함수 기반 기법 ○ : 안전, × : 불안전

기법		위치 추적	위조		태그 해쉬 연산 횟수	분산 시스템 적용
			스푸핑	재전송		
[17]	기법 1	가능	×	×	1	가능
	기법 2	불가능	×	×	1	가능
[12]		불가능	×	○	2	가능
[2,16]		불가능	×	○	2/3	가능
[9]		불가능	×	○	3	불가능
[10]		불가능	○	○	2	불가능
[11]		불가능	○	○	3	가능
[8]		불가능	○	○	2	불가능
[19]		불가능	○	○	4	가능
[20]		불가능	○	○	2	불가능

만 수행하기 때문에 효율적이고 RFID 기법 설계 시에 고려하여야 할 사항들을 만족한다. 제안 프로토콜은 시스템 초기화 단계와 상호 인증 단계로 구성된다.

〔표 2〕 표기법

표기법	설 명
+	비트 덧셈
⊕	비트 XOR (exclusive-or)
H	해쉬 함수
m‖w	메시지 m과 w 의 연접
m_i	m의 i 번째 세션 메시지

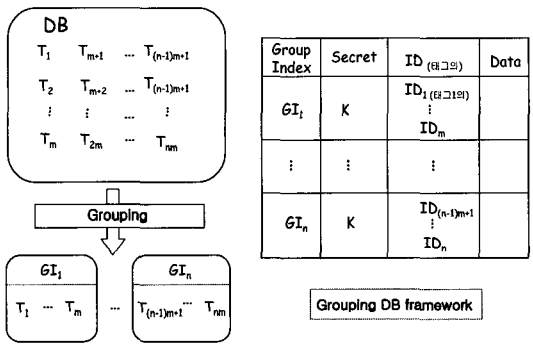
우선, 제안 프로토콜을 설명하기 전에 제안 프로토콜에 사용되는 표시법에 대해 알아보도록 한다. 프로토콜에 사용되는 표기법은 〔표 2〕에서 설명된 것과 같다. 설명된 표시법을 바탕으로 하여 제안 프로토콜에 대해서 알아보도록 한다.

3.1 초기화 단계

초기화 단계에서는 태그와 데이터베이스는 비밀정보와 태그의 ID를 저장한다. 태그, 데이터베이스 및 리더는 다음과 같은 값으로 초기화 된다.

(1) 데이터베이스 : 우선, 데이터베이스는 태그들을 몇 개의 그룹으로 그룹화 한다. 이 과정에서 그룹화는 태그를 랜덤하게 선택한다. 만약 시스템의 태그의 수가 $N(=mn)$이 라면, 데이터베이스는 n개의 태그로 이루어진 m개의 그룹으로 태그의 정보를 관리하고, 각각의 그룹은 GI라는 그룹 인덱스로 식별되어 진다. 〔그림 1〕에서 태그의 그룹화 과정을 나타낸다. 그룹화 후, 데이터베이스의 데이터 필드는 GI, ID, K, S 와 DATA로 초기화 되고, 해쉬 연산 수행을 위하여 해쉬 함수를 가진다. 데이터 필드에 저장된 값들은 아래와 같은 의미를 갖는다.

- GI : ℓ 비트의 태그의 그룹 인덱스이다. 만약 태그가 i번째 그룹에 속하게 되면, 그 태그의 그룹 인덱스는 GIi 이다.
- K : ℓ 비트의 비밀값으로 시스템의 모든 태그에 저장된 값이다. 이 값은 데이터베이스가 리더로부터 전송 받은 값이 어느 태그의 값인지를 효율적으로 구별하기 위해 사용한다.
- S : 각각의 태그가 저장하고 있는 ℓ 비트의 비밀값이다. 이 값은 데이터베이스가 리더로부터 전송받은 값이 실제 그 태그가 전송한 값인지 인증하기 위해 사용한다.
- ID : 각각의 태그가 저장하고 있는 ℓ 비트의 태그 식별코드이다 (Auto-ID 센터에 의한 EPC (Electronic Product Code)의 표준은 태그 ID 의 길이를 64, 96, 256 비트의 상품 체계에 기반하고 있다[6]).
- DATA : 각각의 태그에 대한 태그의 상태와 같은 부가 정보를 저장하고 있다.



〔그림 1〕 데이터베이스의 태그 그룹화 과정

(2) 리더 : 리더는 태그에 질의를 보낼 때마다 ℓ 비트의 값 r을 랜덤하게 선택한다. 올바르게 동작하는 리더는항상 랜덤값 r값을 선택하여 전송하기 때문에 r값으로 0을 전송하지 않는다고 가정한다. 리더는 이외의 다른 작업도 수행하지 않는다. 리더는 단지 태그(데이터베이스)로부터 전송받은 값을 데이터베이스(태그)에 전송한다.

(3) 태그 : 태그의 데이터 필드는 자신에게 해당하는 ID, GI, K, S 와 c 를 저장한다. 이 과정에서 태그가 저장하는 c값은 카운터로서 초기에 ℓ 비트의 랜덤값으로 설정된다. 이 카운터는 리더로부터 질의를 받을 때마다 값을 하나씩 증가시킨다. 이러한 값을 통해서 태그는 매번 다른 값을 리더에 전송한다. 태그는 해쉬 연산을 수행하기 위해 해쉬 함수가 내장된다.

3.2. 상호 인증 단계

이 과정에서는 태그와 리더는 다음의 과정을 통해

서 서로를 인증한다. [그림 2]에서 제안 프로토콜의 동작 과정을 나타내고 있다.

단계 1. 리더는 태그에 질의하기 위해서 랜덤값 $r \in \{0,1\}^{\ell}$ 을 선택하고, Query와 함께 태그에 전송한다.

단계 2. 태그는 리더의 Query(질의)에 응답하기 위해 다음의 과정을 수행한다.

(1) 우선, 리더가 전송한 r이 0인지 확인한다.
- 만약 0라면 이것은 악의적인 리더가 사용자의 정보를 얻기 위한 시도로 판단하여 프로토콜을 멈춘다.
- 그렇지 않다면 태그는 다음의 과정을 수행한다.

(2) 태그는 자신의 ID, GI_i, K, r, c 를 사용하여 $A_1 = K \oplus c$, $A_2 = (ID \oplus r) + (GI_i \oplus r \oplus c) \bmod (2^{\ell}-1)$ 을 생성한다. 또한, 태그는 ID, GI_i, r, c, S 를 사용하여 $B = H(ID||(S \oplus GI_i)||r||c)$을 생성한다. 그 후, 태그는 A_1, A_2, B_R을 리더에 전송한다. 여기에서 B_R, B_L은 B값의 $(1/2)\ell$ 비트의 오른쪽, 왼쪽 값을 나타낸다.

(3) 태그는 리더에 A_1, A_2, B_R 값을 전송한 후에, 카운터 c 값을 증가시킨다. 만약 c 값이 $2^{\ell}-1$값을 넘었을 경우에는 c 값을 초기 값으로 초기화 한다.

단계 3. 리더는 태그로부터 A_1, A_2, B_R 을 받았을 때 다음의 과정을 수행한다.

(1) 리더는 데이터베이스에 A_1, A_2, B_R, r을 전송한다.

(2) 데이터베이스는 K를 사용하여 $c = A_1 \oplus K$를 구하고 데이터베이스의 그룹 인덱스들 GI_j, $j \in \{1,\cdots,n\}$을 이용하여 $ID_j = (A_2 - (GI_j \oplus r \oplus c) \bmod (2^{\ell}-1)) \oplus r$ 을 생성한다.

(3) 데이터베이스는 생성한 ID_j, $j \in \{1,\cdots,n\}$값이 데이터베이스에 저장한 값이 있는지 찾아본다. 만약 데이터베이스 저장된 값과 일치하는 값이 있다면, 데이터베이스는 일치하는 ID_i값이 속한 그룹 인덱스와 ID_j를 생성하기 위해 사용한 그룹 인덱스가 일치하는지 확인한다.
- 만약 두 값이 일치한다면, 데이터베이스는 c, r, S, GI_i, 찾은 ID를 사용해서 $H(ID||(S \oplus GI_i)||r||c)$을 생성한다.
- 그렇지 않다면 프로토콜을 멈춘다.

(4) 데이터베이스는 자신이 계산한 $H(ID||(S \oplus GI_i)||r||c)$이 리더로부터 받은 B_R 값과 동일한지를 확인하는 것으로 태그를 인증한다. 두 값이 동일하지 않을 경우 데이터베이스는 프로토콜을 멈춘다.

(5) 데이터베이스는 태그 인증에 성공한 후, 생성한 $H(ID||(S \oplus GI_i)||r||c)$ 값의 왼쪽 반 B_L을 리더에 전송하고 리더는 태그에 B_L 값을 전송한다.

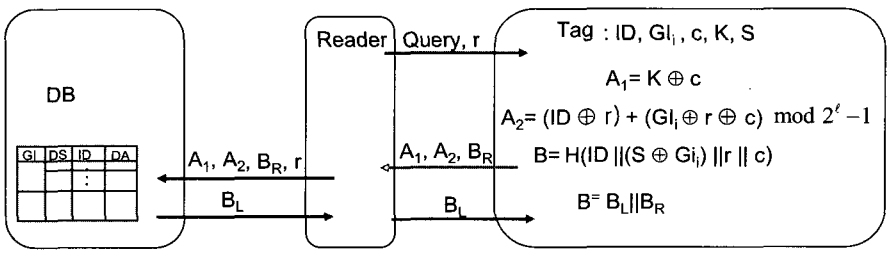
단계 4. 태그는 B_L 값을 받고 이전에 생성한 $H(ID||(S \oplus GI_i)||r||c)$값의 왼쪽 $(1/2)\ell$ 비트와 전송 받은 B_L 값이 동일한지를 확인하는 것으로 태그를 인증한다.

V. 제안 기법의 안전성과 효율성

본 절에서는 제안 프로토콜에 대한 효율성과 안전성에 대해 논의하고자 한다.

5.1. 안전성

제안하는 기법은 2.2 절에서 언급한 안전한 RFID 시스템의 설계 고려사항을 고려하여 분석한



[그림 2] 제안 프로토콜

다. 한 논문에서 제안하는 프로토콜은 공격자의 정보 노출, 사용자의 위치 정보 노출 및 위조 공격에 안전하다.

- 정보 노출 : 공격자는 태그의 정보를 얻기 위해서 제안 기법의 인증 과정을 통과하여야 한다. 제안 기법에서 공격자가 인증 과정을 통과하기 위해 수행 가능한 방법은 다음과 같이 크게 두 가지로 나눌 수 있다.
  - 공격자는 ID, GI_i, K, r, c 의 정보 없이 인증 프로토콜을 통과하기 위해 A_1, A_2, B_R 정보를 모아 분석한 후에 B_L 값을 정확하게 추측하여야 한다. 그러나 해쉬 함수가 일방향성을 제공하기 때문에, 공격자는 A_1, A_2, B_R 로부터 B_L의 정보를 알 수 없다. 구체적으로 설명하면 다음과 같다 : 공격자가 $A_1(=K\oplus c)$값을 도청하더라도 K 값을 알 수 없기 때문에 공격자는 그룹 인덱스 GI값을 알 수 없다. 공격자는 $A_2(=(ID\oplus r)+(GI_i\oplus r\oplus c) \mod (2^{\ell}-1))$ 로부터 어떤 정보도 얻을 수 없다. 공격자는 $\{0,1\}^{(1/2)\ell}$에서 랜덤하게 값을 선택하여야만 한다.
  - 공격자는 공격자가 B_R, B_L 정보들을 도청하여 정보를 모으더라도, 태그 ID에 대한 어떤 정보도 얻을 수 없다. 그러므로 태그의 ID 값을 추측하기 위해 공격자는 해쉬 함수의 입력값 $\{0,1\}^{\ell}$을 랜덤하게 선택하여 한다.

  제안 기법의 인증 과정을 통과하기 위해서는 공격자가 위와 같은 공격을 시도하여야 한다. 이러한 공격에 대한 공격자의 성공 확률은 최대 $\frac{1}{2^{(\ell/2)}}+\frac{1}{2^{\ell}}$이며, 이 값은 무시할 만한 값이다.
- 사용자의 위치 추적 문제점 : 제안 기법에서는 업데이트 되는 r, c 값을 사용함으로서 사용자의 위치 정보 노출을 막을 수 있다. r 값은 리더가 매 세션마다 다른 값을 선택하여 태그에 전송하며, c 값은 태그 자체적으로 업데이트 한다. 만약에 악의적인 리더가 태그들에 동일한 r 값을 전송할 지라도, 태그가 매 세션마다 c 값을 업데이트 하므로 태그는 리더의 질의에 대해 매번 다른 값을 전송한다. 이와 같은 리더의 악의적인 동작은 시스템 내의 모니터링을 통해서 동작 차단이 가능하므로 고려하지 않아도 된다. 제안 기법에서 사용자의 위치를 추적하기 위해 아래와 같은 두 가지 공격이 가능하다.
  - 공격자는 리더와 추적하고자 하는 사용자가 소지한 태그의 통신에서 A_1, A_2 도청 할 수 있다. 공격자가 K 값을 알 수 없으므로, 카운터 c 값을 추출 할 수 없다. 그러므로 공격자는 A_1, A_2 로부터 태그의 그룹 인덱스 GI를 알 수 없으며, 공격자는 추적 하고자 하는 사용자가 소지한 태그의 ID 정보를 얻는 것이 불가능하다. 즉, 공격자는 추적하고자 하는 사용자의 위치 추적이 불가능하다.
  - 하나의 그룹에 속하는 태그들이 동일한 그룹 인덱스 GI와 K 값을 저장하기 때문에 제안 기법에서는 특정 공격자가 하나의 태그를 물리적으로 공격하여 K 값과 하나의 그룹 인덱스 GI_j, $(j\in\{1,\cdots,n\})$를 획득할 수 있는 경우를 고려하여야 한다[1]. 만약 공격자가 특정 태그와 리더간의 통신을 도청하여 A_1, A_2, B_R 과 B_L를 얻는다면, 공격자가 알고 있는 K 값을 이용하여 A_1로부터 카운터 c' 값을 얻을 수 있고, 갖고 있는 그룹 인덱스 GI_j 을 사용하여 A_2로부터 ID′ 값을 얻을 수 있다. 그러나 공격자는 자신이 얻은 ID′ 값이 특정 태그의 ID 인지 판별하는 것이 어렵다. 왜냐하면, 제안된 기법에서 공격자가 자신이 추출해낸 ID′ 값이 실제 ID 값인지 아닌지를 판별하기 위해서는 도청을 통해서 얻은 $B(=H(ID||(S\oplus GI_i)||r||c)$ 값과 ID′, r, c', GI_j 를 해쉬 함수에 적용해서 얻은 값과 비교하여 확인하여야 한다. 그러나 B값을 생성하기 위해서는 태그마다 다른 값 S와, 태그가 속한 그룹 인덱스 GI 값을 입력값으로 넣어야 한다. 그러나 공격자는 S 값과 그룹 인덱스 GI 값을 모르기 때문에 태그 ID 판별이 불가능하다. 즉, 공격자가 물리적인 공격을 통해 태그들의 공통 변수들을 얻을 지라도 특정 태그의 ID를 알아 낼 수 없다. 그러나 만약 태그 ID가 특정 형태를 지니고 있다면, 이런 경우에는 특정 태그에서 얻은 ID를 통해서 다른 태그들의 ID 정보가 유출 가능하다.
- 위 조 : 제안된 기법은 리더와 태그간의 리더의 태그 인증을 통해서 위조 공격에 안전함을 보장

1) 시스템의 초기화 단계에서, 태그를 랜덤하게 그룹화 하므로 동일한 종류의 상품일 경우에도 태그의 그룹 인덱스 값은 다를 수 있다. 그러므로 상품을 보고 그 상품이 속한 그룹을 판별할 수 없다.

한다. 제안 기법에서는 리더(데이터베이스)가 태그를 인증함으로서, 스푸핑 공격에 안전하다. 제안 기법에서 공격자가 리더인척 하여 태그의 출력 값 A_1, A_2, B_R을 얻을 수 있다. 그러나 리더는 매 세션마다 새로운 r을 전송하고 태그가 그 값을 이용하여 값을 생성하여 전송하는 값으로 태그를 인증하기 때문에 단계 3-(4)을 통과할 수 없다. 그러므로 제안 기법은 스푸핑 공격에 안전하다. 또한 공격자가 리더와 태그와의 통신을 도청하더라도 태그가 매 세션 새로운 r을 사용하기 때문에 다음 세션의 단계 3-(4)를 통과 할 수 없다. 즉, 재전송 공격에 안전하다.

5.2. 효율성

본 절에서는 기존에 제안된 다수의 기법들 중에서 태그가 최소한의 해쉬 함수를 제공하는 Lee 등의 기법 [10]과 제안 기법과 유사한 기능을 제공하는 분산데이터 베이스에 적용 가능한 Rhee 등의 기법 [11]과의 비교를 통해서 제안 기법의 효율성에 대해서 논의 할 것이다. 이전에 태그를 그룹으로 나누어 태그를 인식하는 기법이 제안되었었으나[9], 그 기법은 태그를 그룹으로 관리하여 태그 인식률을 높이는 유사한 기능을 제공하지만 제안하는 기법에 비해서 태그가 4번의 해쉬 연산을 수행하여 하므로 제안 기법과 비교하지 않는다.

제안 기법은 해쉬 기반의 기법으로 태그가 인증 프로토콜을 수행하기 위해 한 번의 해쉬 함수 연산을 수행한다. 제안된 기법은 아래 〔표 3〕에서 볼 수 있듯이 이전에 제안된 최소한의 해쉬 연산을 요구하는 기법[10]에 비해 태그의 저장량이 늘어나지만, 태그가 수행하는 해쉬 연산양이 적다 (H :한 번의 해쉬 연산, N: 시스템의 태그의 개수, A : 태그가 수행하는 해쉬 연산 이외의 부가적인 연산 (덧셈, XOR 비트 연산), ε: 데이터베이스가 수행하는 해쉬 연산 이외의 부가적인 연산). 또한, 제안된 기법은 태그의 ID가 매 세션 갱신되지 않기 때문에 분산 데이터베이스 환경에 적용 가능하며, 이전에 제안된 기법의 분산 데이터베이스에 적용 가능한 기법[11]보다 태그의 연산양이 적어 저가형의 RFID 시스템에 더 적합하다. 제안 기법의 분산 데이터베이스 환경에 적용하는 구체적인 방법은 다음과 같다. 우선, 기업의 중앙 서버에서 태그가 내장된 상품에 대한 정보들을 데이터베이스로 구축하고 있으며, 중앙 데이터베이스는 하위 데이터베이스의 질의에 대해 해당하는 태그에 대한 정보들을 하위 데이터베이스에 전송한다. 하위 데이터베이스는 해당 태그에 대한 정보를 중앙 데이터베이스와의 한 번의 통신을 통해 정보를 얻은 후에, 그것으로 하위 데이터베이스들은 자신만의 데이터베이스를 구축하며, 자신의 시스템의 범주 안에서 태그에 해당하는 정보를 식별 가능하다.

더욱이, 제안 기법은 기존의 해쉬 기반의 기법들과 달리 태그에 대한 '소유권 이전' 기능을 제공한다. '소유권 이전' 기능이란 태그를 관리하던 소유자가 변경 될 경우 이전의 소유자는 그 태그들에 대한 어떤 정보, 위치 정보 및 제품 정보들과 같은 것에 대해서 알 수 없어야 한다.

제안 기법은 데이터베이스의 비밀값 K를 태그의 소유자가 변경 될 때마다 변경하여 소유권 이전 기능을 제공 가능하다. 예를 들면, A 대형 마켓에서 소속되어 있던 태그가 B 도매 마켓으로 팔릴 경우, 대형 마켓에서 물건을 계산하는 시점에서 태그에 저

〔표 3〕 제안 기법의 효율성

프로토콜		Lee의 기법 [10]	Ree의 기법 [11]	제안 기법
저장량	태그	1ℓ	1ℓ	5ℓ
	데이터베이스	6ℓ	1ℓ	4ℓ
계산량	태그	2H	3H	1H+A
	데이터베이스	1H	$(\frac{N}{2}+1)$H	1H+ε
통신량	태그 → 리더	$1\frac{1}{2}\ell$	2ℓ	$2\frac{1}{2}\ell$
	리더 → 태그	$\frac{1}{2}\ell$	1ℓ	$\frac{1}{2}\ell$

장되어 A의 데이터베이스의 비밀값 K를 임의의 값 g로 변경하여 저장하고 B 도매 마켓 주인에게 g 값을 알려준다. 그 후 B 도매 마켓에서 A 마켓에서 사온 물건들을 시스템에 등록할 때 g 값을 이용해서 그 물건을 인식하고, 그 시스템의 데이터베이스 비밀값 K'으로 변경하여 저장한다. 이러한 과정을 통해서 이전의 A 대형 마켓의 리더들은 B 마켓의 물건들을 인식 불가능하다. 제안 기법은 '소유권 이전'의 기능을 제공함으로써 기존의 기법들 보다 사용자의 프라이버시 침해 가능성을 줄일 수 있다.

Ⅵ. 결 론

RFID 시스템은 원거리 통신으로 사물을 인식한다는 점에서 물류, 유통, 재고 관리에 유용한 도구가 될 것이다. 그러나 RFID 시스템은 동작 원리의 특성상 사용자의 프라이버시를 침해를 야기 시킨다. 또한, RFID 시스템에서는 리더와 태그 간에 무선 통신을 사용하여 통신하기 때문에 공격자로 인한 도청, 스푸핑 공격, 재전송 공격, 메시지 차단과 같은 공격에 취약하다. 이와 같은 RFID의 문제점을 해결하기 위해서 해쉬 함수, 암호화 알고리즘, 암호학적 함수가 아닌 단순한 연산에 기반하는 여러 가지 프라이버시 보호 기법들이 제안되었다. 본 논문에서는 해쉬 함수 기반의 분산 데이터베이스 환경에 적합한 안전하고 효율적인 프로토콜을 제안한다. 제안 기법은 태그를 그룹화 하여 관리함으로써, 태그의 해쉬 함수 연산의 횟수를 한 번으로 줄임으로써, 기존에 제안된 해쉬 함수의 기법들 중에서 효율적인 기법을 제안하였다. 또한, 제안 기법에서는 태그가 저장하고 있는 값을 변경하여 태그가 내장된 상품의 소유권 이전의 기능을 제공하기 때문에 기존의 기법들 보다 사용자의 프라이버시 침해 가능성을 줄 일 수 있다. 더구나, 제안 기법에서는 태그의 ID를 변경하지 않기 때문에 분산 데이터베이스 환경에 적합하여, '언제 어디서나' 인가된 리더는 태그의 정보를 얻을 수 있어야 하는 유비쿼터스 환경에 적용 가능하다.

참 고 문 헌

[1] Auto-ID Center, "860Mhz-960MHz Class I Radio Frequency Identification Tag Radio Frequency and Logical communication Interface Specification Proposed Recommendation Version 1.0.0. Technical Report MIT-AUTOID-TR-007", AutoID Center, MIT, 2002.

[2] G. Avoine and Ph. Oechslin, "A Scalable and Provably Secure Hash-Based RFID Protocol", The 2nd IEEE International Workshop on Pervasive Computing and Communication Security - PerSec 2005, IEEE Computer Society Press, Kauai Island, Hawaii, USA, 3, 2005

[3] A. Juels, "Minimalist cryptography for Low-Cost RFID Tags", In The Fourth Internationl Conferecne on Security in Communication Networks-SCN 2004, LNCS 3352, pp. 149-164, Springer-Verlag. 2004.

[4] A. Juels and R. Pappu, "Squealing euros : Privacy protection in RFID-enabled banknotes", In proceedings of Financial Cryptography -FC'03, LNCS 2742, pp.103-121, Springer-Verlag, 2003.

[5] EPCglobal, "EPCTM Tag Data Standards Version 1.1 Rev.1.24 Standard Specification 01", 04, 2004.

[6] A. Juels, R. Rivest and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID tags for Consumer Privacy". In the 8th ACM Conference on Computer and CommunIcations Security, pp. 103-111, ACM Press. 2003.

[7] S. Junichiro, R. Jae-Cheol and S. Kouichi, "Enhancing privacy of Universal Re-encryption scheme for RFID Tags", EUC 2004, LNCS 3207, pp.879-890, Springer-Verlag, 12, 2004

[8] Jeonil Kang and Daehun Nyang, "RFID Authentication Protocol with Strong Resistance against Tracea

bility and Denial of Service Attacks", ESAS 2005, LNCS 3813, pp. 164-175, 2005.

[9] D. Henrici and Paul Muller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", PerSec'04 at IEEE PerCom. pp. 149-153, 2004.

[10] Su Mi Lee, Young Ju Hwang, Dong Hoon Lee and Jong In Lim, "Efficient Authentication for Low-Cost RFID systems", ICCSA 05, LNCS 3480, pp.619-629, 2005.

[11] Keunwoo Rhee, Jin Kwak, Seungjoo Kim and Dongho Won, "Challenge-Response based secure RFID Authentication Protocol for Distributed Database Environment", SPC 2005, LNCS 3450, pp.70-84, Springer-Verlag, 4, 2005.

[12] M. Ohkubo, K. Suzuki and S. Kinoshita, "Efficient Hash-Chain Based RFID Privacy Protection Scheme", Ubcomp2004 workshop.

[13] S. E. Sarma, "Towards the five-cent tag. Technical Report MIT-AUTOID-WH-006, MIT Auto ID Center", 2001. Abailable from http://www. autoidcenter.org.

[14] S. E. Sarma, S. A. Weis and D. W. Engels, "Radio-frequency identification systems". CHES'02, LNCS 2523, pp.454-469, Springer-Verlag, 2002.

[15] S. E. Sarma, S. A. Weis and D. W. Engels, "RFID systems, security and privacy implications. Technical Report MIT-AUTOID-WH-014", AutoID Center, MIT, 2002.

[16] 유성호, 김기현, 황용호, 이필중, "상태 기반 RFID 인증 기법 프로토콜", 정보보호학회논문지, 제 4권, 6호, 12, 2004.

[17] S. A. Weis, S. E. Sarma, S. A. Weis and D. W. Engels, "Security and privacy Aspects of Low-Cost Radio Frequency Identification Systems". First International Conference on Security in Pervasive Computing, 2003. http://theory.lcs.mit.edu/sweis/spc-rfid.pdf.

[18] Istvan Vajda and Levente Buttyan, "Lightweight authentication protocols for low-cost RFID tags", Workshop on Security in Ubiquitous Computing, 2003.

[19] Sang-Soo Yeo and Sung Kwon Kim, "Scalable and Flexible Privacy Protection Scheme for RFID Systems", ESAS 2005, LNCS 3813, pp. 153-163, 2005.

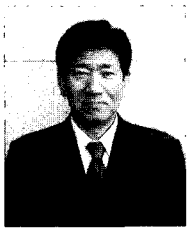
[20] Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren, and Kwangjo Kim, "Mutual authentication protocol for low-cost RFID, Ecrypt Workshop, Workshop on RFID and Lightweight Crypto, pp. 17-24, 2005.

〈著者紹介〉

최 은 영 (Eun Young Choi) 학생회원
2001년 8월 : 고려대학교 수학과 학사
2003년 8월 : 고려대학교 정보보호대학원 공학 석사
2004년 3월~현재 : 고려대학교 정보경영공학 전문대학원 박사과정
<관심분야> 암호 이론, 정보보호 이론, RFID 정보보호 기술, 유비쿼터스

이 수 미 (Su Mi Lee) 학생회원
1995년 2월 : 순천향대학교 화학과 학사
2003년 2월 : 고려대학교 정보보호대학원 공학 석사
2003년 3월~현재 : 고려대학교 정보경영공학 전문대학원 박사과정
<관심분야> 암호 이론, 그룹 키 교환, RFID 인증 시스템

임 종 인 (Lim, Jong In) 종신회원
1980년 2월 : 고려대학교 수학과 졸업
1982년 2월 : 고려대학교 수학과 석사
1986년 2월 :고려대학교 수학과 박사
1986년 9월 ~2001년 1월 :고려대학교 자연과학대학정교수
2001년 2월 ~현재 : 고려대학교 정보경영공학 전문대학원 원장, 고려대학교 정보보호기술 연구센터 센터장
<관심분야> 암호 이론, 암호 정책, PET 기술



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 정보경영공학 전문대학원 교수
<관심분야> 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술