전자 태그의 보안 레벨을 기반으로 하는 RFID 인증 프로토콜

정회원 오 수 현*, 곽 진**

RFID Tag's Security Level Based RFID Authentication Protocol

Soo-hyun Oh*, Jin kwak** *Regular Members*

요 약

최근 들어 RFID 시스템을 물류·유통 시스템을 비롯한 여러 산업분야에 널리 활용하기 위해 태그에 저장된 정보를 보호하고 임의의 태그에 대한 추적 방지가 가능한 인증 프로토콜에 대한 연구가 활발히 진행 중이다. 본 논문에서는 보안 레벨(security level)의 개념을 이용하여 태그를 인증하기위해 back-end DB에 요구되는 계산량을 감소시킬 수 있는 RFID 인증 프로토콜을 제안한다. 제안하는 방식은 해쉬 함수에 기반하며 재전송 공격, 스푸핑 공격, 트래픽 분석, 위치 프라이버시 등에 대해 안전하다는 장점이 있다.

Key Words : RFID, security level, hash function, authentication, privacy

ABSTRACT

Recently, RFID system is a main technology to realize ubiquitous computing environments. Because RFID system that is an automatic identification technology using radio frequency is a system to read and write the data of the entity. Therefore, many companies are interested in RFID system to reduce supply chain management and inventory control cost. However, for providing secure service, RFID authentication technology secure against tracking by an adversary is researched first. In this paper, we proposed security level based RFID authentication protocol providing reduce computational and communicational workload in the back-end database. The proposed protocol is secure against reply attack, spoofing attack, traffic analysis, and location privacy, since the proposed protocol based on the security of the hash function.

Ⅰ. 서 론

최근 들어 활발히 연구되고 있는 유비쿼터스 컴퓨팅 기술은 단순히 컴퓨팅 환경의 변화뿐만 아니라 기업의 생산, 물류, 판매, 고객관리 등 비즈니스 프로세스를 구성하는 기기나 시스템들이 모두 지능화되고 네트워크로 연결됨으로써 다양한 새로운 비즈니스를 창출하고 있다. 유비쿼터스 비즈니스는 단순한 상거래뿐만 아니라 일반적인 기업경영, 공급망 관리, 유통관리, 안전관리 등 거의 모든 비즈니스 활동에 혁신적으로 적용될 수 있어 이와 관련된 기술과 상품이 미래 IT 시장을 주도할 것으로 예측된다.

유비쿼터스 컴퓨팅 환경에 있어 핵심이 되는 기술이 RFID(Radio Frequency IDentification)이며, 최근 국내에서도 RFID의 중요성을 인식하여 'IT 신성장 동력'의 중점 추진 사업으로 선정하기도 하였다. RFID 시스템은 식별 정보가 저장된 태그(tag)가 부착된 사물을 물리적인 접촉 없이 RF 신호(RF

* 호서대학교 컴퓨터공학부 정보보호 전공 전임강사(shoh@office.hoseo.ac.kr)
** 성균관대학교 정보통신공학부 정보통신보호연구실 박사과정(jkwak@dosan.skku.ac.kr)
논문번호 : KICS2005-05-190, 접수일자 : 2005년 5월 6일

signal : Radio Frequency signal)를 이용하여 개체의 정보를 읽고 기록하는 기술이다. RFID는 기존의 바코드나 자기 인식 장치의 단점을 보완하고 사용의 편리성 향상으로 물류관리, 재고관리 등 소비가 비약적으로 증가되고 있는 차세대 핵심기술로 주목받고 있다.

그러나 RFID를 이용한 개체 인식 기술은 리더(reader)와 칩(chip)을 내장한 태그 사이에 물리적인 접촉 없이 인식 가능하고 태그의 정보가 전송될 수 있으므로, 이로 인한 과도한 정보 노출을 포함한 사용자의 프라이버시 침해를 유발시킨다는 문제점을 가지고 있다. 따라서 RFID 기술을 물류·유통 시스템을 비롯한 여러 산업분야에 널리 활용하기 위해, 태그에 저장된 정보를 보호하고 임의의 태그에 대한 추적 방지 등과 같은 관련 보안 문제를 해결할 수 있는 인증 프로토콜에 대한 연구가 활발히 진행 중이다. 그러나 지금까지 제안된 대부분의 인증 프로토콜은 Backend DB가 태그를 인증하기 위해 데이터베이스에 저장된 모든 태그의 식별정보를 확인해야 하므로, DB에 과도한 연산량이 요구된다는 단점이 있다.

본 논문에서는 보안 레벨(security level)의 개념을 이용하여 태그를 인증하기위해 Backend DB에 요구되는 계산량을 감소시킬 수 있는 RFID 인증 프로토콜을 제안한다. 제안하는 방식은 해쉬 함수에 기반하며 매 세션마다 다르게 생성되는 랜덤 수를 이용하므로 재전송 공격, 스푸핑 공격, 트래픽 분석, 위치 프라이버시 등에 대해 안전하다는 장점이 있다. 본 논문의 구성은 다음과 같다. 먼저 2장에서는 RFID 시스템의 개요와 지금까지 제안된 프라이버시 보호 가능한 RFID 인증 프로토콜에 대해 간략히 설명하고, 3장에서는 RFID 시스템의 보안 요구사항에 대해 설명한다. 다음으로 4장에서는 보안 레벨을 이용하는 제안하는 RFID 인증 시스템에 대해 구체적으로 설명하고, 5장에서는 제안하는 시스템과 기존의 시스템의 안전성과 효율성을 비교·분석한다. 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 관련 연구

2.1 RFID 시스템의 개요

RFID 시스템은 (그림 1)과 같이 태그, 리더, Back-end 데이터 베이스(DB)로 구성되며 각각의 기능은 다음과 같다.[1][12]

- 태그(tag) : 리더의 요청에 응답하는 트랜스폰더(transponder)로 각각의 고유한 식별 정보(identification information)를 저장하고 있다.
- 리더(reader) : 태그에 정보를 요청하고 수신한 데이터를 판독하고 태그를 인식하는 트랜시버(transceiver)로 태그에게 RF 신호를 통해 전원을 공급하는 역할을 한다.
- Back-end 데이터베이스 : 리더가 수집한 정보를 저장하거나 리더 또는 태그 대신 복잡한 연산을 수행하는 안전한 서버이며, 리더에서 수집된 정보의 진위 여부를 판별해주는 역할을 수행한다.

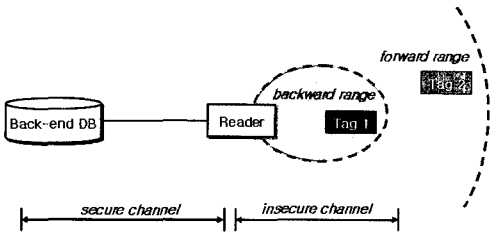

그림 1. RFID 시스템

그림 1에서 forward range는 리더가 RF 신호를 전송할 수 있는 범위를 의미하며, backward range는 태그가 응답 정보를 전송할 수 있는 범위를 말한다. 리더가 태그를 인식하기 위해 보내는 신호를 forward range안에 포함된 tag 1과 tag 2 모두 수신할 수 있지만, backward range 안에 있는 tag1만 응답 신호를 전송할 수 있게 되는 것이다. 그리고 태그와 리더간의 통신은 RF 신호를 이용하므로 공격자에 의한 도청이 가능하므로 안전하지 않은 통신로를 이용하는 것이고, 리더와 데이터베이스 사이의 통신은 안전한 통신로를 이용하게 된다. 태그는 IC 칩과 안테나로 구성되어 있으며, 그 모양과 크기는 다양하게 존재한다. IC 칩의 데이터를 저장하는 메모리의 크기는 25bit에서 512 KB 이상 등 여러 종류가 있으며, 메모리의 형태 또한 읽기 전용, 읽고 쓰기 가능한 형, 한번만 쓰고 여러 번 읽기 가능한 형태 가 있다. 그리고 전력을 공급받는 방법에 따라 능동형 태그와 수동형 태그로 나눌 수 있다.

2.2 RFID 인증 프로토콜

RFID 시스템에서는 리더를 소유한 공격자는 물리적인 접촉 없이 태그의 정보를 읽는 것이 가능하므로, 사용자가 알지 못하는 사이에 태그에 저장된 정보가 노출되거나 태그의 식별 정보를 이용한 사용자의 위치 추적 등이 가능하게 된다. 이러한 문제

점을 해결하기 위해 사용자의 프라이버시를 보호할 수 있는 RFID 인증 프로토콜이 제안되었다. 본 절에서는 지금까지 제안된 사용자의 프라이버시 보호가 가능한 RFID 인증 시스템의 특징 및 장·단점에 대해 간략히 살펴보고자 한다.

2.2.1 해쉬 락(Hash lock) 프로토콜

해쉬 락 프로토콜은 "locked" 상태에서는 태그가 자신의 실제 ID 값이 아닌 metaID 값을 전송하고, "unlocked" 상태에서만 실제 ID를 전송함으로써 사용자의 프라이버시를 보호하는 방식이다[9]. 이 방식에서 metaID = hash(key)이며, DB는 각 태그에 대해 키(key) 값과 metaID를 저장해야 한다. 태그는 리더로부터 자신의 키 값을 정확히 전송받은 경우에만 정당한 쿼리로 간주하여 자신의 ID 값을 전송하며, 공격자의 공격을 방지하기 위해 "unlocked" 상태는 아주 짧은 순간에 이루어지도록 해야 한다. 그러나 RFID 시스템에서 태그와 리더간의 통신은 불안전한 통신로를 이용하므로 누구나 도청이 가능하다. 따라서 이 방식에서 공격자는 리더와 태그간의 통신을 도청하여 태그의 ID를 얻는 것이 가능하고, 또한 metaID가 항상 동일한 정보이므로 리더나 공격자에 의한 트래킹이 가능하다는 문제점이 있다.

2.2.2 확장된 해쉬 락 프로토콜

이 방식은 해쉬 락 프로토콜을 개선한 방식으로 랜덤화 된(randomized) 해쉬 락 프로토콜이라고도 한다.[10] 이 방식에서 태그는 해쉬 함수를 이용하며 매 세션마다 전송되는 값을 변형하며 공격자나 리더를 포함한 허가받지 않은 개체에 의한 트래킹을 방지할 수 있다는 장점이 있다. 그러나 이 방식은 프로토콜의 마지막 부분에서 RFID 리더가 ID를 전송함으로써 ID가 노출되어 공격자에 의한 프라이버시를 침해받을 수 있다는 단점이 있다.

2.2.3 외부 재 암호화(Re-encryption)을 이용하는 방식

이 방식은 EURO banknote에 RFID 시스템을 이용하여 합법적인 트래킹이 가능하도록 하기 위해 제안된 방식이다[3]. 이 방식에서 태그의 메모리는 optical contact area와 RF contact area로 나누어지며, 리더에 의해 태그가 인식된 후에 재 암호화를 이용하여 태그에 저장된 정보를 재 기록하는 방법이다. 이 방식은 사용자가 인식하지 못하는 사이에 물리적인 접촉 없이 리더가 태그의 정보를 읽거나 쓰는 것을 방지할 수 있으며, 필요한 경우에 법 집행기관 같은 합법적인 기관에 의한 트래킹은 가능하다는 장점이 있다. 그러나 공개키 암호 방식과 디지털 서명 방식을 이용하므로 재 암호화에 많은 양의 계산을 요구하므로 현실적으로 구현하는데 많은 어려움이 있다.

2.2.4 해쉬 체인(Hash-chain)을 이용하는 방식

해쉬 체인을 이용하는 방식은 두 개의 해쉬 함수를 이용하여 리더의 query에 대해 태그가 매 세션마다 서로 다른 응답을 전송하고, 이를 이용하여 태그를 인증하는 방식이다[10]. 이 방식에서 동일한 태그라 할지라도 매번 다른 값을 전송하여 인증을 받으므로, 공격자가 태그의 응답들을 이용하여 동일한 태그인지 아닌지를 구별하는 것이 불가능하다. 그러나 태그의 정당성을 확인하기 위해 back-end DB가 수행해야 하는 연산량이 매우 많다는 단점이 있다.

2.2.5 해쉬 기반 ID 변형 프로토콜

해쉬 기반 ID 변형 프로토콜은 매 세션에서 난수를 생성하고 이를 이용하여 인증 정보를 매번 갱신하므로 공격자로부터 프라이버시를 보장 받을 수 있다.[11] 또한 프로토콜에 사용되는 TID(Transaction ID)와 LST(Last Successful Transaction)도 매 세션마다 갱신되므로 재전송 공격을 막을 수 있다. 이밖에도 물리적인 공격에 의해 전송되는 메시지가 손실되어도 AE(Associated DB Entry)를 통해 복구가 가능하다는 장점을 가지고 있다.

이 프로토콜은 공격자가 정당한 리더로 가장하여 RFID 태그가 전송하는 메시지를 획득하는 경우, 정당한 RFID 리더와 RFID 태그가 다음 세션을 진행하기 전에 이 메시지를 이용하면 정당한 RFID 태그로 인증 받을 수 있다. 이와 같은 스푸핑 공격이 가능한 이유는 정당한 RFID 태그는 프로토콜 마지막 과정에서 메시지를 받지 못하는 경우 정보가 유실되었다고 판단하여 기존의 RFID 태그의 ID를 갱신하지 않기 때문이다. 또한 프로토콜 수행 중에 발생할 수 있는 메시지 유실의 피해를 줄이기 위해 사용되는 AE와 관련 정보는 back-end DB에게 부담을 줄 수 있다.

Ⅲ. RFID 시스템의 보안 요구사항

RFID 인증 시스템에서 리더와 태그간의 통신은 RF 신호를 이용한 불안전한 채널을 통해 이루어지므로 공격자에 의한 도청이 항상 가능할 뿐만 아니라, 물리적인 접촉없이 태그에 저장된 정보를 판독

하는 것이 가능하므로 다음과 같은 보안 요구사항을 만족하도록 시스템을 설계하여야 한다.[11][12]

3.1 재전송 공격

수동적 공격자가 리더와 태그 사이에 주고받는 메시지를 도청한 후, 이를 재 전송(replay)함으로써 정당한 태그나 리더로 인증 받으려는 공격을 재 전송 공격(replay attack)이라 한다. 재 전송 공격에 대해 안전하기 위해서는 매 세션마다 태그가 전송하는 정보가 변경되도록 해야하고, 전송 정보로부터 태그의 식별 정보를 구하는 것이 불가능하도록 해야한다. 즉, 공격자가 이전 세션의 모든 리더와 태그간의 통신 내용을 도청하여 저장하더라도, 이를 이용하여 리더가 정당한 태그로 인증할 수 있는 새로운 값을 생성하는 것은 불가능해야 한다.

3.2 스푸핑 공격

스푸핑 공격(Spoofing Attack)은 공격자가 정당한 RFID 리더로 가장하여 RFID 태그로부터 인증에 필요한 정보를 획득하고, 이 정보를 이용하여 정당한 RFID 태그로 위장하는 공격방법을 말한다. 이 공격을 수행하는 경우, 위치를 추적하고 싶은 RFID 태그에게 계속하여 질의를 전송함으로써 RFID 태그를 소유하고 있는 주체의 위치를 파악할 수 있어 프라이버시를 침해할 수 있다. 이를 예방하기 위해서는 공격자가 정당한 RFID 리더로 가장하는 것이 어려워야 하며, 세션마다 RFID 태그의 응답이 변화할 수 있도록 난수 등을 이용해 프로토콜을 설계해야 한다.

3.3 트래픽 분석

트래픽 분석(Traffic Analysis Attack)은 RFID 리더와 RFID 태그간의 정보를 도청할 수 있는 공격자가 도청된 내용을 이용하여 인증 프로토콜에 필요한 비밀 정보를 분석하는 공격 방법을 의미한다. 이를 방지하기 위해서는 공격자가 도청된 정보를 이용하여 비밀 정보와 그렇지 않은 정보를 구분할 수 없어야 한다.

3.4 위치 프라이버시

RFID 시스템에서 RFID 태그는 물리적인 접촉없이 인증이 가능하므로, 사용자가 인식하지 못하는 사이에 자신의 위치 정보를 불법적인 RFID 리더에게 전송함으로써 RFID 태그 소유자의 프라이버시를 침해할 수 있다. 따라서 이를 방지하기 위해서는 매 세션마다 갱신되는 RFID 태그의 ID를 사용함으로써 공격자로부터 프라이버시를 보호하여야 한다. 또한 두개의 서로 다른 응답메시지에 대해서 공격자는 동일한 RFID 태그로부터의 응답인지 구분할 수 없어야 한다.

Ⅳ. 제안하는 시스템

RFID 시스템은 리더와 태그 사이의 물리적인 접촉없이 인증이 가능하므로, 사용자가 인식하지 못하는 사이에 사용자의 위치 정보나 상품 구매 정보가 유출될 수 있어 프라이버시를 침해할 수 있는 문제점을 가지고 있다. 따라서 이러한 문제점을 해결하기 위해 사용자의 프라이버시를 보호할 수 있는 인증 프로토콜에 대한 연구가 활발히 진행되고 있다.

사용자의 프라이버시를 보호할 수 있는 인증 프로토콜은 물리적인 기법과 암호학적인 기법으로 나눌 수 있다. 이중, 암호학적인 기법을 사용하는 프로토콜들은 태그의 식별 정보가 직접 전송되지 않고 매 세션마다 전송되는 인증 정보를 변경함으로써 위치 추적이나 트래픽 분석, 트래킹에 대한 안전성을 제공한다.

그러나 대부분의 시스템에서 back-end DB가 리더가 전송한 정보를 이용하여 태그의 정당성을 확인하기 위해서는 모든 태그의 식별 정보를 비교해야 하므로, 과도한 계산량을 요구한다는 단점이 있다. 본 절에서는 보안 레벨을 이용하여 DB에 요구되는 계산량을 감소시킬 수 있는 개선된 프로토콜을 제안한다.

4.1 시스템 개요

제안하는 시스템에서는 태그의 정당성을 확인하기 위해 DB에게 요구되는 계산량을 감소시켜 효율적인 인증이 가능하도록 하기 위해, 태그들을 보안 정책에 따라 그룹으로 나누어 각 그룹마다 적당한 보안 레벨을 할당한다. 예를 들어, 물류 관리 방식에서 RFID 시스템을 이용하는 경우 물품의 분류나 가격대에 따라 적절한 보안 레벨을 할당할 수 있다.

본 절에서는 먼저 RFID 시스템의 basic authentication protocol을 설명하고, 보안 레벨을 적용한 Security level based authentication protocol의 동작 과정에 대해 설명한다. 그리고 마지막으로 트래킹, 위치 추적, 트래픽 분석 공격에 안전하도록 개선한 Security level based Randomized authentication protocol에 대해 설명한다.

4.1.1 Basic authentication protocol

RFID 시스템의 기본 인증 방식은 그림 2와 같다.

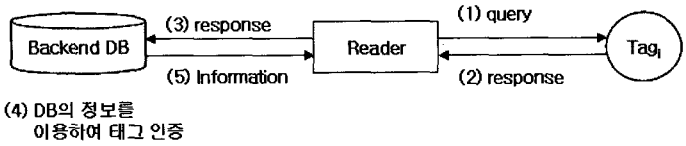

그림 2. Basic authentication protocol

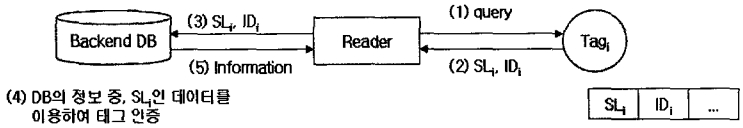

그림 3. Security level based authentication protocol

각 태그는 자신의 식별 정보(ID)를 저장하고 있으며, back-end DB는 모든 태그의 식별정보를 저장하고 있다.

① 리더 R은 태그에 query를 전송한다.
② 태그 T_i는 자신의 ID 정보를 포함하는 response를 리더에게 전송하다.
③ 리더는 response를 back-end DB에 전송한다.
④ Back-end DB는 저장된 정보를 이용하여 response의 정당성을 확인하고, 정당한 태그인 경우 관련 정보를 리더로 전송한다.

Basic authentication protocol에서는 각 태그의 식별정보가 전송되므로 수동적인 공격자들도 도청 공격을 통해 쉽게 태그의 정보를 획득할 수 있으며, 획득한 정보를 이용하여 재 전송 공격을 통한 위장이 가능하다. 또한, 모든 세션에서 전송되는 응답이 동일하므로 태그 소유자의 위치 정보가 노출되고 트래킹 및 스푸핑 공격이 가능하다는 문제점이 있다. 그리고 back-end DB에서 태그의 정당성을 확인하기 위해 저장된 모든 태그의 식별 정보를 비교해야 하므로 많은 계산량을 필요로 한다는 단점이 있다.

4.1.2 Security level based authentication protocol

Security level based authentication protocol은 back-end DB에게 요구되는 계산량을 감소시키기 위해, 모든 태그들을 몇 개의 그룹으로 나누고 각 그룹별로 적절한 보안 레벨을 할당하여 인증하는 방식이다. 이 프로토콜에서 각 태그에는 자신의 식별 정보와 함께 보안 레벨 SL_i 값이 저장되어 있으며, DB에 저장된 정보는 표 1과 같다.

Security level based authentication protocol의 동작과정은 다음과 같다. (그림 3 참조)

표 1. Back-end DB에 저장된 정보

보안 레벨	Tag's ID	information
SL_0	ID_1	*price*|| *valid period* ...
	⋮	*price*|| *valid period* ...
	ID_i	*price*|| *valid period* ...
SL_1	ID_{i+1}	*price*|| *valid period* ...
	⋮	*price*|| *valid period* ...
	ID_j	*price*|| *valid period* ...
⋮	⋮	⋮
SL_n	ID_{k+1}	*price*|| *valid period* ...
	⋮	*price*|| *valid period* ...
	ID_l	*price*|| *valid period* ...

① 리더 R은 태그에 query를 전송한다.
② 태그 T_i는 자신의 security level SL_i와 ID_i 포함하는 response를 리더에게 전송하다.
③ 리더는 response를 back-end DB에 전송한다.
④ Back-end DB는 저장된 정보 중 security level이 SL_i와 일치하는 데이터만을 이용하여 response의 정당성을 확인하고, 정당한 태그인 경우 관련 정보를 리더로 전송한다.

이 프로토콜에서는 back-end DB에서 태그를 인증하기 위해 모든 태그의 식별 정보를 계산할 필요가 없고, 해당 보안 레벨과 일치하는 태그들의 식별정보만을 검사하므로 인증에 요구되는 계산량이 감소된다는 장점이 있다. 그러나 태그의 응답에 보안 레벨과 식별정보가 그대로 포함되므로 수동적 공격자의 도청공격에 대해 안전하지 않다. 또한, 태그가 항상 동일한 response를 전송하므로 트래킹과 스푸핑 공격이 가능하고 위치 프라이버시를 보장하지 못한다는 단점이 있다.

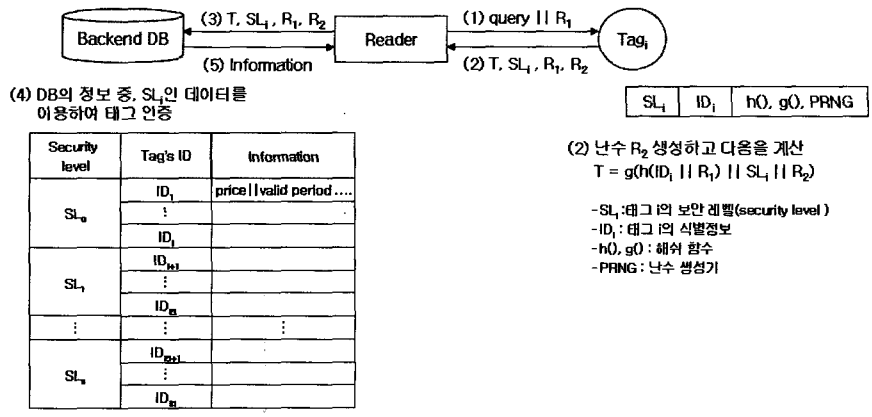

그림 8. Security level based Randomized authentication protocol

4.1.3 Security level based Randomized authentication protocol

Security level based Randomized authentication protocol은 앞에서 설명한 Security level based authentication protocol에 해쉬 함수를 적용한 방식으로, DB의 계산량을 감소시킬 뿐만 아니라 재전송 공격, 트래킹, 스푸핑 공격에 안전하고 태그 소유자의 위치 프라이버시를 보장한다는 장점이 있다. Security level based Randomized authentication protocol의 인증 과정은 다음과 같다(그림 4 참조). 제안하는 프로토콜에서 각 태그는 식별 정보와 보안 레벨 값을 저장하고 해쉬 함수와 난수 생성기를 가지고 있다.

① 리더 R은 태그에 query와 세션마다 다르게 선택한 난수 R_1을 전송한다.

② 태그 T_i는 PRNG를 이용하여 난수 R_2을 생성하고 다음과 같이 T 값을 계산하여, (T, SL_i, R_1, R_2) 값을 리더에게 전송하다.

$$response = g(h(ID_i \parallel R_1) \parallel SL_i \parallel R_2)$$

③ 리더는 (T, SL_i, R_1, R_2)를 back-end DB에 전송한다.

④ Back-end DB는 저장된 정보 중 security level이 SL_i와 일치하는 데이터만을 이용하여 다음 식을 만족하는 식별정보가 존재하는지 확인한다.

$$T \stackrel{?}{=} g(h(ID_i \parallel R_1) \parallel SL_i \parallel R_2)$$

(단, IDn은 security level이 SL_n인 태그의 식별정보)

⑤ ④의 식을 만족하는 태그가 존재하는 경우 관련 정보를 리더로 전송한다.

V. 제안하는 시스템의 비교 · 분석

5.1 안전성

제안하는 security level based Randomized authentication protocol에서는 랜덤 수를 이용하여 태그가 매 세션마다 전송하는 응답이 변경되므로, 수동적 공격자가 태그의 응답을 도청하여 재전송 하더라도 다음 세션에서는 정당한 태그로 인증받을 수 없다. 따라서 재전송 공격에 대해 안전하다. 그리고 태그를 인증하기 위해 리더가 선택한 매 세션마다 변경되는 랜덤 수를 이용하므로, 공격자가 정당한 RFID 리더로 위장하는 경우에도 태그로부터 획득한 인증 정보를 이용하여 정당한 RFID 태그로 위장하는 것이 불가능하다. 즉, 스푸핑 공격에 대해 안전하다. 다음으로 트래픽 분석 공격의 경우, 태그의 응답 정보를 생성하기 위해 암호학적으로 안전한 해쉬 함수를 사용하므로 수동적 공격자가 리더와 태그간의 전송 정보를 도청하더라도 태그의 실제 식별 정보를 추출하는 것은 불가능하다. 따라서, 트래픽 분석 공격에 대해서도 안전한다.

또한, 태그의 응답 정보에 리더로부터 수신한 랜덤 수 뿐만 아니라 매 세션마다 태그가 다르게 생성한 랜덤 수가 포함되므로, 동일한 태그의 응답이라 할지라도 매 세션마다 달라지는 특징이 있다. 따라서, 태그의 응답 정보를 통해 태그를 소유한 사용자의 위치 정보를 추적하는 것은 불가능하며, 두 개의 서로 다른 응답메시지에 대해서 동일한 RFID 태그로부터의 응답인지 구분할 수 없다. 표 2는 기

표 2. 안전성 비교 · 분석

	재전송 공격	스푸핑 공격	트랙픽 분석	위치 프라이버시
해쉬-락 프로토콜	안전하지 않음	안전하지 않음	안전하지 않음	안전하지 않음
확장된 해쉬-락 프로토콜	안전하지 않음	안전하지 않음	안전하지 않음	안전하지 않음
외부 재 암호화 프로토콜	안전	안전	안전	안전하지 않음
해쉬-체인 프로토콜	안전하지 않음	안전하지 않음	안전	안전
해쉬 기반 ID 프로토콜	안전	안전하지 않음	안전	안전하지 않음
제안하는 시스템	안전	안전	안전	안전

표 3. 효율성 비교 · 분석

	계 산 량		
	태그	리더	Back-end DB
해쉬-락 프로토콜	-	-	-
확장된 해쉬-락 프로토콜	R : 1번 H : 1번	H : T/2 번	-
해쉬-체인 프로토콜	H : 2번	-	H : (T/2) × i 번
해쉬 기반 ID 프로토콜	H : 3번	-	R : 1번 H : 3번
제안하는 시스템	R : 1번 H : 2번	R : 1번 (사전 계산 가능)	H : (|SLi|/2) × 2 번

- R: 난수발생기 연산
- H: 해쉬함수의 연산
- i : 해쉬 함수 적용 횟수
- T : Back-end DB에 저장된 태그의 개수
- |SLi| : Back-end DB에 저장된 태그 중 security level이 SLi인 태그의 개수

존에 제안된 사용자의 프라이버시 보호가 가능한 RFID 인증 프로토콜과 본 논문에서 제안하는 프로토콜의 안전성을 비교 · 분석한 결과이다.

5.2 효율성

본 절에서는 기존에 제안된 사용자의 프라이버시 보호가 가능한 RFID 인증 프로토콜과 본 논문에서 제안하는 프로토콜의 인증 과정에서 요구되는 계산량을 비교한다. 계산량은 태그, 리더, back-end DB로 나누어서 분석하였으며, 외부 재 암호화 기법의 경우, 공개키 암호화 기법을 사용하기 때문에 계산량을 다른 프로토콜과의 정량적 비교가 어려우므로 효율성 분석에서는 제외하였다.

제안하는 시스템의 인증 과정에서 태그에 요구되는 연산량은 1번의 난수 생성과 2번의 해쉬 함수이며, 리더는 한번의 난수 생성이 필요하지만 이는 사전에 계산하여 저장하였다가 랜덤하게 선택하여 전송하는 것이 가능하다. 그리고, back-end DB의 경우 DB에 저장된 모든 태그의 식별 정보에 대해 확인할 필요없이 보안 레벨이 일치하는 태그들에 대해서만 계산을 수행하므로 기존의 방식에 비해 DB에 요구되는 계산량을 감소시킬 수 있다는 장점이 있다. 표 3은 기존에 제안된 사용자의 프라이버시 보호가 가능한 RFID 인증 프로토콜과 본 논문에서 제안하는 프로토콜의 계산량을 비교 · 분석한 결과이다.

VI. 결 론

RFID 기술은 저 비용의 무선 인식 메모리 태그로 인식 속도가 빠르고 바코드에 비해 상대적으로 많은 저장 능력을 가지고 있어, 물류 및 유통 시스템에서 바코드를 대체할 수 있는 차세대 기술로 기대되고 있다. 그러나 RFID를 이용한 개체 인식 기술은 리더와 태그 사이에 물리적인 접촉 없이 인식이 가능하고 태그의 정보가 전송될 수 있으므로, 이로 인한 사용자의 프라이버시 침해를 야기시킨다는 문제점을 가지고 있다. 지금까지 사용자의 프라이버시를 보호할 수 있는 RFID 시스템에 관한 몇몇 연구 결과가 발표되었으나 제안된 방식들은 각각 안전성과 효율성 면에서 몇 가지 문제점을 가지고 있다.

본 논문에서는 보안 레벨이라는 개념을 적용하여 모든 태그들의 몇 개의 그룹으로 나누어 태그를 인증하는데 요구되는 DB의 계산량을 감소시킬 수 있는 효율적인 인증 기법을 제안하였다. 또한 제안하는 방식은 RFID 시스템이 만족해야 하는 보안 요구 사항에 적합하도록 설계되었으며, 재전송 공격,

스푸핑 공격, 트래픽 분석, 위치 프라이버시 등에 대해 안전하다는 장점이 있다. 또한, 본 논문에서 사용하는 보안 레벨을 이용하는 기법은 제안하는 시스템 외에 기존의 다른 RFID 인증 프로토콜에도 적용가능 하므로 보다 효율적인 RFID 인증 프로토콜 설계에 활용될 수 있을 것으로 기대된다.

참 고 문 헌

[1] K. Finkenzeller(1999), RFID Handbook, *John Wiley and Sons*

[2] D. Henrici, P. Muller, "Hash-based Enhancement of Location Privacy for Radio- Frequency Identification Devices using Varying Identifiers", *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops. PERCOMW '04*, pp.149-153, IEEE, 2004

[3] A. Juels and R. Pappu(2003), "Squealing Euros : Privacy protection in RFID-enabled banknotes", *Financial Cryptography'03*, LNCS 2742, pp. 103-121, Springer-Verlag

[4] A. Juels, R. L. Rivest and M. Szydlo(2003), "The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy", *10th ACM Conference on Computer and Communications Security*, CCS 2003, pp. 103-111

[5] M. Ohkubo, K. Suzuki, and S. Kinoshita (2003), "A Cryptographic Approach to "Privacy-Friendly" tag", *RFID Privacy Workshop*

[6] RFID Standardization, http://www.rfidhandbook.de/rfid/standardization.html

[7] S. E. Sarma, S. A. Weis, and D. W. Engels (2002), "Radio-frequency identification systems". *Workshop on Cryptographic Hardware and Embedded Systems, CHES'02*, LNCS 2523, pp. 454-469, Springer-Verlag

[8] S. E. Sarma, S. A. Weis, and D. W. Engels (2003), "Radio-frequency-identification security risks and challenges", *CryptoBytes, 6(1)*

[9] S. A. Weis(2003), "Radio-frequency identification security and privacy", *Master's thesis, M.I.T.*

[10] S. A. Weis, S. Sarma, R. Rivest, and D. Engels(2004), "Security and privacy aspects of low-cost radio frequency identification systems", *In First International Conference on Security in Pervasive Computing 2003*, LNCS 2802, pp. 201-212, Springer-Verlag.

[11] 양정규, 김광조, 표철식, "저가의 RFID에 관한 정보보호 기법 연구", *한국정보보호학회 하계정보보호학술대회 학술지* Vol.14 No.1, 2004

[12] 오수현, 곽진, "유비쿼터스 환경에 적합한 사용자 프라이버시 보호 기능을 제공하는 RFID 시스템", *한국통신학회 논문지*, vol. 29, No. 12C, pp. 1729-1738, 2004. 12

[13] 이근우, 오동규, 곽진, 김승주, 원동호, "Low-cost RFID 시스템을 위한 Improved Hash Chain", *CISC*, Vol.14 No.1, pp.628-632, 2004

[14] 이은곤, "RFID확산 추진현황 및 전망", *정보통신정책* 제 16권 6호, 2004.4

[15] 최동희, 최은영, 이동훈, "유비쿼터스 환경에서의 RFID 프라이버시 보호", *한국정보보호학회 하계정보보호학술대회 학술지*, Vol.14 No.1, 2004

오 수 현 (Soo-hyun Oh) 정회원

1998년 2월 성균관대학교 정보공학과 졸업

2000년 2월 성균관대학교 전기전자 및 컴퓨터공학부 대학원 (공학석사)

2003년 8월 성균관대학교 전기전자 및 컴퓨터공학부 대학원 (공학박사)

2004년 3월~현재 호서대학교 컴퓨터공학부 정보보호 전공 전임강사

<관심분야> 암호 알고리즘/프로토콜, 유비쿼터스 보안

곽 진 (Jin-Kwak) 정회원

2000년 8월 성균관대학교 생물기전공학과 졸업

2003년 2월 성균관대학교 전기전자및컴퓨터공학부 대학원(공학석사)

2003년 3월~현재 성균관대학교 정보통신공학부 박사 과정

<관심분야> 암호 알고리즘/프로토콜, 유비쿼터스 보안