한국산업정보학회논문지 제13권 제2호(2008. 6)

암호화된 ID를 이용한 다중 객체 접근 방식의 RFID 시스템 연구†

(A Study on RFID System for Accessing Multiple Objects Using Encrypted ID)

정종진*, 김지연*
(Jong-Jin Jung, Ji-Yeon Kim)

요 약 최근 활발히 연구되고 있는 RFID 시스템은 유비쿼터스 환경의 핵심기술로 평가되고 있으며 여러 산업 분야 혹은 개인 생활환경에 있어서 그 응용 범위를 넓혀가고 있으나, 사용자 정보에 대한 추적과 접근이 용이하여 개인 정보 침해의 위험성 또한 증가하게 되는 문제가 제기되고 있다. 본 논문에서는 RFID 환경에서 태그와 단말기 사이에 SEED 암호화 기술을 적용하여 태그에 대한 접근 보안을 유지하고, 하나의 RFID 태그 내에 응용 분야별로 구분된 여러 개의 객체식별자를 가지도록 함으로써 다양한 RFID 시스템으로의 접근을 가능하게 하는 다중 객체 구조의 RFID 태그를 제안한다. 또한, 발생 가능한 여러 가지 유형의 공격으로부터 태그에 저장된 정보를 보호하고 다중 객체에 대한 접근 및 통신을 위한 인증 프로토콜을 제안하며, 기존의 인증 프로토콜과 비교하여 효율적임을 증명한다.

핵심주제어 : RFID 시스템, 다중 객체, RFID 태그, 인증 프로토콜

Abstract RFID systems are being studied and developed in the area of the industry and marketplace. Recently RFID systems are core element of the ubiquitous technologies in individual life and industry. However, RFID systems often cause some serious problems such as violation of privacy and information security because their contactless devices communicate each other by radio frequency. In this paper, we propose multiple objects RFID tag scheme including tag structure and authentication protocol. The proposed RFID tag structure maintains several object IDs of different applications in a tag memory. The tag structure allows those applications to access object IDs simultaneously. The authentication protocol for multiple objects tag is designed to overcome the problems of security and privacy. The protocol has robustness against various attacks in low cost RFID systems. We evaluate the efficiency of proposed scheme and compare security of our scheme with several traditional schemes.

Key Words : RFID system, Multiple objects, Authentication protocol

1. 서 론

현재 정보통신 기술은 언제 어디서나 사용자가 네트워크에 접속 가능한 유비쿼터스 환경으로 진화하고 있으며, 이러한 유비쿼터스 환경은 사용자의 이용 편리성과 함께 경제적인 이익까지도 창출할 수 있다. 이러한 유비쿼터스 컴퓨팅 환경의 핵심 기술이라 할 수 있는 RFID(Radio Frequency IDentification) 시스템은 무선 통신을 이용하여 자

† 이 논문은 2006학년도 대진대학교 학술연구비지원에 의한 것임.
* 대진대학교 컴퓨터공학과

동으로 식별 정보를 제공하는 기술로서 비가시거리의 무선인식이 가능하고 Read/Write가 가능하며, 환경 적응력이 뛰어난 여러 장점으로 인해 교통 카드, 톨게이트 요금 징수, 물류 관리, 출입 통제 등 다양한 분야에서 사용되고 있을 뿐 아니라, 미래에는 더욱 다양한 목적으로 활용될 전망이다. 따라서 각종 물건들에 점점 더 많은 RFID 시스템의 태그가 부착될 것이고, 개인 생활에 있어서도 회사, 집, 차 등 각기 다른 목적으로 사용하기 위한 여러 개의 RFID 태그를 소유하게 되는데, 사용자의 입장에서는 다수의 태그를 소지하고 용도에 따라 구별하여 사용한다는 것이 불편을 초래할 수도 있을 것이다. 또한 많은 태그들에 저장되어지는 개인 정보는 곳곳에 설치될 RFID 리더를 통해 전송하게 되는데, 이 때 무선 통신의 불안정한 특성으로 인해 정보의 유출이나 위치 추적과 같은 사용자 프라이버시를 침해하는 심각한 문제점도 발생시킬 수 있다. 따라서 바람직한 유비쿼터스 환경을 만들기 위한 RFID 시스템은 여러 종류의 응용들 간에 정보 공유와 정보보안을 필요로 한다.

기존의 많은 RFID 응용들은 하나의 리더에 대하여 여러 RFID 태그를 인식하는 기술구조를 기반으로 개발되어 왔으나, 본 논문에서는 하나의 태그를 서로 다른 응용에서 공유하여 사용하기 위한 다중 객체 접근 RFID 태그의 구조를 설계하고, 이러한 태그 구조에 적합한 RFID 인증 프로토콜을 제안하고자 한다. 제안하는 인증 프로토콜은 기존의 연구들에서 거의 프로세서 수준의 태그의 연산 능력을 요구하는 것과는 달리, 저사양의 태그 구조 하에서도 통신을 방해하는 다양한 공격에 강인하도록 설계하였다.

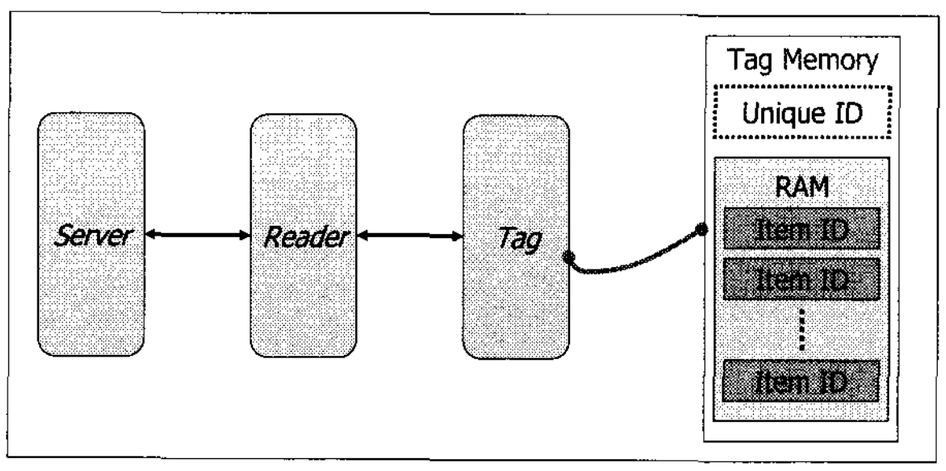
본 논문의 구성은 먼저 2장에서 RFID 시스템의 기술 개요 및 요구 사항을 살펴보고, 3장에서는 기존의 관련 연구들을 분석한다. 4장에서 제안하는 기법에 대해 소개하고, 5장에서는 제안 방식의 성능을 기존 방식과 비교하여 분석하고, 6장에서 결론을 내리기로 한다.

2. 기술 개요 및 요구 사항

RFID는 무선 주파수를 이용한 비접촉식 자동 인식 기술로서, 태그와 리더, 서버로 구성된다. 태그는 데이터를 저장하고 있으며, 리더의 요청에 의해 정보를 송수신하는 기능을 수행한다. 리더는 태그가 송신한 정보에 의해 태그를 인식하고, 태그에 정보를 기록할 수 있다. 서버는 리더에 의해 수집된 정보를 해독하는 연산을 수행하고, 수집한 정보를 데이터베이스에 저장한다. 이러한 RFID 시스템의 구성요소들 중에서도 핵심 요소인 태그는 무선 주파수의 대역별로 분류하거나, 태그의 전력을 공급받는 방법에 따라 분류할 수 있다. 또한, 태그의 데이터 저장 기능에 따라 읽기 전용, Write Once Read Many(WORM), 읽기/쓰기 등의 형태로 구분할 수 있으며, 단순한 인식소자 기능에서 데이터의 읽기/쓰기가 가능한 형태로 점차 발전하는 추세이다. 현재 개발되고 있는 태그는 약 10Mbits/sec의 데이터 전송 속도와 1Mbyte 이상의 메모리 용량을 실현할 수 있는 수준이고, 향후 프로세서를 포함한 태그로 발전 가능할 것이라 예측된다.

RFID 태그의 표준화는 ISO와 IEC가 공동 설립한 JTC1과 GSI 기구에서 설립한 EPC Global Inc.에서 이루어지고 있다. 태그의 ID는 리더와 태그 간 통신과정에서 태그를 고유하게 식별하기 위한 번호로서, 이러한 ID는 국제 표준을 따르고 한국 환경에 맞는 ID를 부여하도록 하는 표준화 방안을 규정하고 있다. RF 태그의 생산자 또는 제조자에 의해 태그 내에 고정 기록되는 식별 번호인 불변 유일 식별자(Permanent Unique Identifier)는 칩 ID 또는 태그 ID라고 하며, ISO/IEC 15963 형식[8]에 의해 번호화된다. 사물 식별자(Item Identifier)는 RF 태그를 부착한 사물 자체를 구별하기 위한 식별자로서, RF 태그 이용자에 의해 태그의 데이터 기록 공간에 저장되는 식별자이다. 사물 식별자는 (그림 1)에서 보인 것처럼 아이템 ID로 불리며, ISO/IEC JTC1 SC31, EPC Global 등의 국제 표준화 단체에서 표준화 작업이 진행 중이다[9].

제안하는 RFID 시스템에서 사용하는 태그는 다중 객체 접근 구조의 RFID 태그이며, 태그 식별자 중 사물 식별자를 이용하여 접근 가능한 다중 객체의 ID를 저장한다.



(그림 1) 태그 식별자의 개념

RFID 시스템은 물리적 접촉 없이 인식이 가능하므로 개인 정보보호(프라이버시)와 안전성 측면의 여러 문제점들을 야기할 수 있다. 특히 리더와 태그 간의 인증 과정에서 사용되는 무선 채널에서 발생 가능한 여러 가지 공격들로 인해 RFID 시스템의 안전성이 위협받을 수 있으며, 이 점은 RFID 시스템의 사용 자체를 부정적으로 인식하게끔 할 가능성이 있다. 가능한 공격들의 유형과 그에 대해 RFID 시스템이 갖추어야할 안전성 측면의 요구사항을 살펴보면 다음과 같다.

- 도청(Eavesdropping) : 일반적으로 태그에 저장되어 있는 정보는 일련번호나 코드번호로서 본 사물의 세부 정보(제조사, 가격 등)를 알 수 없으나, 리더나 태그로부터 도청한 정보를 재전송하여 RFID 시스템에 접속하여 세부 정보를 알아내거나, 지속적인 도청을 통하여 사용자에 대한 위치 추적을 할 수 있다. 따라서, RFID 시스템은 도청된 정보로부터 어떠한 key 값도 유추할 수 없도록 설계되어야 하며 도청한 정보를 다시 사용하여 재전송하거나, 사용자의 위치를 추적할 수 없도록 하는 인증 프로토콜을 가져야 한다.
- 위치 추적(Location Tracking) : 태그로부터 리더에게 전송되는 정보를 이용하여 태그의 위치나 소비자의 경향 등 트래픽 분석이 가능한 공격의 유형이다. 따라서, 안전한 RFID 시스템은 동일한 태그로부터 수신되는 정보를 매 세션마다 변경함으로써 동일한 태그임을 구분할 수 없도록 설계되어야 한다.
- 스푸핑(Spoofing) : 스푸핑 공격은 공격자가 정당한 리더나 태그로 가장하여 인증 프로토콜에 참여하는 것으로, 수집한 정보를 바탕으로 세부 정보를 획득할 수 있다. 따라서, RFID 시스템은 태그에 저장된 정보를 암호화하거나 태그 접근 권한을 관리할 수 있도록 하여, 공격자가 태그나 리더로부터 수집한 정보를 이용하여 정당한 태그나 리더로 가장하는 것이 불가능하도록 설계되어야 한다.
- 방해 : 방해 공격은 RFID 시스템의 프로토콜에 참여하지 않고 어떠한 정보도 수집하지 않지만 정상적인 정보의 전송을 방해하여 메시지의 유실을 유발할 수 있다. 따라서, 안전한 RFID 시스템은 정보 전송 방해에 대한 공격 탐지 기능을 가져야 한다.

3. 관련 연구

RFID 시스템의 안전성을 위협하는 여러 공격들에 대한 문제점을 해결하기 위한 기존의 방법들로는 Kill 명령어 기법[2], 패러데이 케이지 기법[6], 블로커 태그 기법[5] 등의 물리적 보안 기법들과 암호학적인 방법을 이용한 인증 기법들이 있다. 이들 중 현재 RFID 시스템에서 주로 연구되고 있는 암호학적인 인증 기법들에 대해 간략하게 살펴본다.

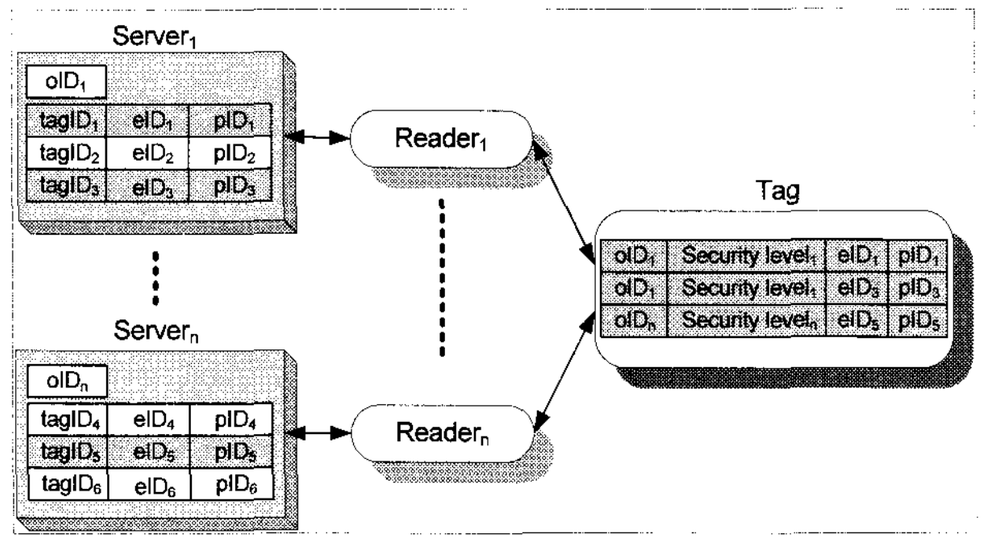
- Hash lock 기법[1] : Hash lock 기법은 태그의 실제 ID 값을 보호하기 위해 metaID를 이용하는 방식으로 해쉬 함수에 의해 metaID를 생성한다. 그러나, metaID의 값이 고정되어 있으므로 공격자가 태그의 위치를 추적할 수 있다. 그리고, 공격자가 metaID를 도청한 후, 이 metaID를 이용하여 태그로 가장하여 리더로부터 key를 획득하는 경우 공격자가 다시 리더로 가장하면 태그의 ID를 얻는 것이 가능하므로 정당한 태그로 가장할 수 있는 스푸핑 공격도 가능하다는 문제점이 있다.
- 확장된 Hash lock 기법[2] : 확장된 Hash lock 기법은 Hash lock 기법을 개선한 방식으로 태그가 난수를 생성하여 매 세션마다 다른 응답을 하도록 함으로써, 공격자에 의한 위치 추적을 방지할 수 있다는 장점이 있다. 그러나 이 기법에서는 리더가 태그에게 ID를 전송하는 인증 프로토콜의 마지막 단계에서 공격자에 의해 ID가 노출될 가능성이 있다.

- Hash chain 기법[3] : Hash chain 기법은 서로 다른 두 개의 해쉬 함수를 이용하여 리더의 질의에 대한 태그의 응답을 매 세션마다 다르게 전송하도록 하는 방식이다. 동일한 태그의 응답이 매번 달라지므로, 공격자가 정보를 도청하더라도 어떤 태그의 응답인지, 서로 다른 응답에 대해서 동일한 태그의 응답인지 아닌지를 알 수 없다. 그러나 공격자가 태그의 응답을 재전송하여 정당한 태그로 가장할 수 있는 스푸핑 공격에 취약하며, 서버에서 태그를 인증하기 위한 해쉬 함수 연산에 대한 연산량이 매우 많고 태그가 서로 다른 두 개의 해쉬 함수를 내장하고 있어야 하므로 태그 가격 상승이라는 문제점이 있다.
- Hash 기반 ID 변형 기법[4] : Hash 기반 ID 변형 기법에서는 태그 ID를 난수에 의해 매번 변경함으로써 안전성을 보장하도록 한다. 매 세션마다 TID(Transaction ID)와 LST(Last Successful Transaction)을 변경시켜 프로토콜에 사용함으로써 다음 세션에서 재전송하여 공격할 수 없도록 한다. 이 기법에서는 프로토콜의 마지막 단계에서 이루어지는 리더로부터의 메시지에 의해 태그를 인증하는데, 메시지 유실이 발생하는 경우 기존 ID를 변경하지 않음으로써 스푸핑 공격이 가능하다.

4. 제안 방식

4.1 RFID 태그의 다중 객체 구조

제안하는 RFID 시스템에서 사용하는 태그는 다기종의 RFID 리더에서 식별 가능한 다중 객체를 포함하는 다중 키 구조를 가진다는 것이 가장 큰 특징이다. RFID 시스템이 적용되는 분야는 산업 분야뿐만 아니라 가정과 직장 등과 같이 다양한 분야 및 생활권에 넓게 분포하며 기존의 RFID 시스템에서는 용도에 따라 각각의 태그가 별도로 사용되고 있다. 하지만, 유비쿼터스 환경이 모든 생활 전반에 걸쳐 점차 확대되고 있는 시점에서 하나의 태그만 사용하여 용도에 따른 여러 종류의 시스템에 적용하게 된다면 정보의 통합과 활용의 용이성을 목표로 하는 유비쿼터스 환경에 더욱 적합할 것이다. 본 논문에서는 (그림 2)와 같이 하나의 태그 내에 사용 분야와 목적에 따라 정의되는 다수 개의 *oID*를 저장한다.



(그림 2) 제안하는 태그 및 시스템 구조

*oID*는 고유한 태그 ID와 함께 SEED 알고리즘을 이용한 암호화 과정에 사용되고, 암호화된 결과값을 *eID*로 정의한다. RFID 시스템의 서버와 태그 에는 이러한 *eID*가 저장된다. 특정 리더로부터의 질의에 대해 태그에서는 태그에 저장되어 있는 *oID*의 값으로 인덱스된 *eID*를 사용하여 가변적인 값을 생성하여 응답하게 된다. 본 논문에서 제안하는 RFID 시스템은 하나의 태그 내에 여러 개의 ID를 포함하지만, 이러한 *oID*와 *eID*의 인덱스 구조는 리더의 질의에 대한 태그의 응답 시간을 최소화할 수 있으며 효율적인 동작을 가능하게 한다.

RFID 시스템 서버의 Back-end 데이터베이스와 태그에 저장되는 정보는 <표 1>과 같다.

<표 1> 서버 및 태그의 저장 정보

	정 보
서버(DB)	tagID, eID, pID
태그	oID, eID, pID

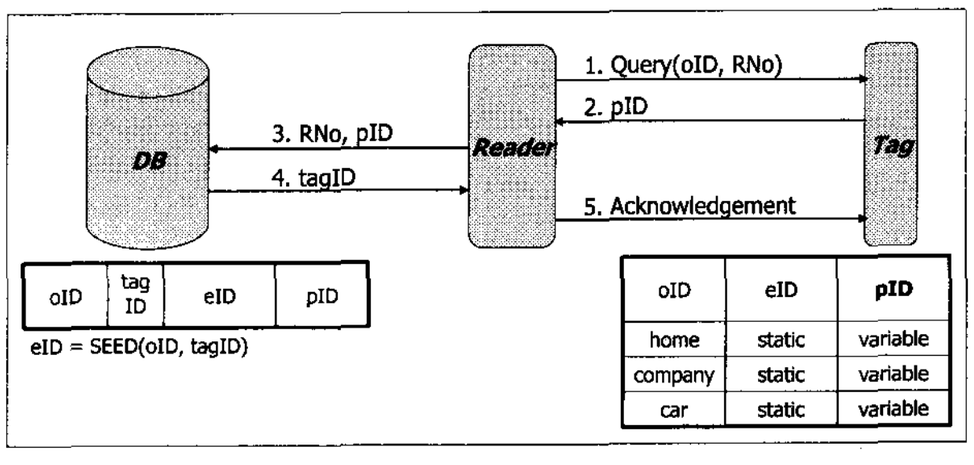
- *tagID* : 태그별 고유한 ID이며, *oID*와 함께 *eID*를 생성하기 위한 key로 사용된다. 제안하는 시스템에서는 다중 객체에 대한 정보가 하나의 태그 내에 저장되므로 한 개의 태그가 여러 *tagID*를 가질 수 있으나, 태그에서는 *tagID*를 저장하지는 않고 SEED 알고리즘을

통해 암호화된 값인 *eID*를 태그 메모리에 저장한다.

- *oID*(object ID) : 이종의 RFID 시스템에서 각 객체의 종류를 구별하기 위한 ID로서, 유비쿼터스 ID 센터[7]에서 제안한 ID길이인 128bit를 *eID*와 나누어 사용할 수 있다. 제안하는 RFID 시스템에서는 리더의 질의문에 *oID*를 포함시켜 다중 객체 ID를 가진 태그 내에서 해당 리더의 객체 타입을 구별하게 하고 해당하는 ID를 검색해 낸다.
- *eID*(encrypted ID) : *oID*와 태그의 고유한 ID인 *tagID*를 사용하여 SEED 암호화 알고리즘에 의해 암호화하여 생성된 값으로서, 시스템 초기화 시 서버와 태그에 각각 저장된다. 하나의 태그 내에 여러 개의 *eID*가 저장되며, 각 *eID*는 *oID*에 의해 구별되어 해당하는 리더의 질의에 대한 응답으로 해당 *eID*를 검색할 수 있게 된다.
- *pID*(partial ID) : 리더를 통한 서버와 태그 사이의 인증이 성공적으로 수행되는 경우의 최종적인 값으로서 매 세션마다 태그에서 응답하는 가변적인 값을 서버와 태그에 저장하도록 한다. 공격자로부터 이전 세션에서 도청된 정보를 이용한 스푸핑 공격이 행하여졌을 경우 서버에서는 *pID*와 비교함으로써 정상적인 인증 프로토콜이 수행되지 않음을 감지할 수 있다. 또한, 리더를 가장하여 태그에게 질의하는 경우에 태그에서는 정당하지 않은 리더로부터 전송되는 랜덤 값이 이전 세션에서 사용된 값임을 *pID*를 비교해 봄으로써 알 수 있게 된다.

4.2 다중 객체 기반 RFID 시스템의 인증 프로토콜

제안하는 다중 객체를 갖는 RFID 시스템의 인증 프로토콜에서는 (그림 3)과 같이 서버에서 SEED 암호화 알고리즘에 의해 암호화된 ID(*eID*)를 각 태그와 서버의 데이터베이스에 먼저 저장한다. 암호화 알고리즘에 *oID*와 *tagID*를 사용할 수 있으며, 태그에 저장되는 SEED 암호화 알고리즘에 의해 생성된 *eID* 값은 물리적인 복제 및 해독이 용이하지 않으므로, 이러한 *eID*의 장점을 이용하고 위치 추적 및 스푸핑과 같은 공격으로부터 안전한 인증 프로토콜을 설계한다. 또한, 저가의 태그에서도 구현 가능하도록 태그 내에서는 랜덤 값에 의한 비트마스킹(Bit Masking)으로 세션마다 가변적인 정보를 생성하여 리더 질의에 응답하도록 연산량을 최소화함으로써 응용분야를 다양화할 수 있는 장점이 있다.



(그림 3) 제안된 인증 프로토콜

제안하는 인증 프로토콜에서의 세부적인 인증 절차는 다음과 같다.

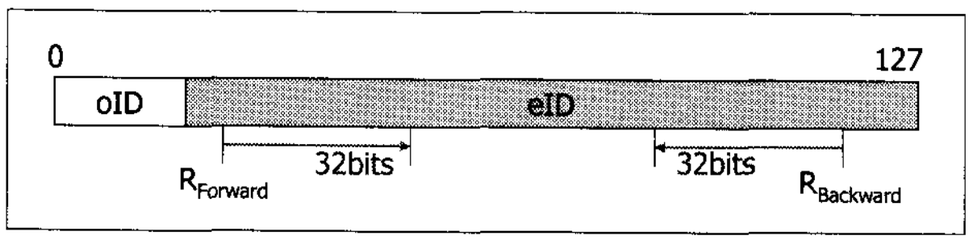
(1) 리더는 해당 *oID*와 세션마다 다르게 생성한 랜덤 값을 태그에게 전송한다. 랜덤 값은 다음과 같이 구성되며, 위치 추적 공격에 대해 태그의 응답을 매 세션마다 다른 값으로 생성하기 위하여 이용한다.

$$RNo = R_{Forward\_no} || R_{Backward\_no}$$

(2) 태그는 *oID*와 전송된 랜덤 값으로 *eID*의 변형된 값인 *pID*를 생성한다. 메모리 블록의 크기가 128bits인 태그를 가정할 경우 (128-*oID*의 bit수)/2의 값을 $R_{Forward_no}$와 $R_{Backward_no}$에 modular 연산을 하면 그 값이 각각 *eID*의 실제 추출 시작 위치인 $R_{Forward}$와 $R_{Backward}$가 된다.

$$R_{Forward} = R_{Forward\_no} \bmod (sizeof\ eID\ /\ 2),$$
$$R_{Backward} = R_{Backward\_no} \bmod (sizeof\ eID\ /\ 2)$$

(그림 4)와 같이 *eID*의 전체 bit 중 $R_{Forward}$에 해당하는 bit부터 32 bits와 $R_{Backward}$ 위치에 해당하는 bit부터 32 bits를 조합하여 64bits 크기의 *pID*를 생성한다.



(그림 4) pID의 생성 방법

태그는 현재 세션에서 생성한 pID_n값과 태그 내에 저장되어 있는 이전 세션에서의 pID_{n-1}를 비교한다. 두 값이 같지 않으면 현재의 리더를 정상적인 리더로 판단할 수 있으며, 태그는 현재 세션에서 생성한 pID_n와 이전 세션에서의 pID_{n-1}를 XOR 연산하여 리더에게 전송하기 위한 *pID*를 생성한다.

$$pID = (pID_n)\ XOR\ (pID_{n-1})$$

만약 현재 세션의 pID_n와 이전 세션에서의 pID_{n-1}이 같은 경우, 리더로 가장한 공격자가 이전 세션에서 도청한 정보를 태그에게 재전송하였다고 판단하여 리더에게 *pID*를 전송하지 않는다.

(3) 리더는 해당 리더와 연결되어 있는 서버에게 랜덤 값 *RNo*와 태그로부터의 응답받은 *pID*를 전송한다.

(4) 서버에서는 전송된 *pID*와 *RNo*를 서버에 저장되어 있는 이전 세션에서의 *pID*에 적용하여 일치하는 *eID*를 찾아낸다. 일치하는 *eID*가 존재하는 경우, SEED 알고리즘의 복호화 과정을 수행하여 *tagID*를 구함으로써 사용자 정보를 검색하고 정당한 태그임을 인증하게 된다. 서버에서는 해당 태그의 ID를 리더에게 전송하고 현재 세션의 *pID*값으로 데이터베이스를 갱신한다.

(5) 리더는 태그에게 프로토콜이 정상적으로 종료되었음을 의미하는 종료 메시지를 태그에게 전송하고, 태그는 현재 세션의 pID_n를 메모리에 저장한다.

5. 성능 평가

5.1 안전성 평가

제안하는 프로토콜은 다음과 같은 공격에 대해 안전성을 보장할 수 있으며, <표 2>는 기존의 인증 기법들과 안전성을 비교 분석한 표이다.

<표 2> 공격 유형에 따른 안전성 비교

(O: 강함, X: 약함)

공격 / 인증기법	위치 추적	스푸핑	재전송	메시지 유실
Hash Lock	X	X	X	X
Randomized Hash Lock	O	X	X	O
Hash Chain	O	O	X	O
Variable ID	O	X	O	X
Proposed Scheme	O	O	O	O

- 도청 : 공격자에 의해 획득된 도청 내용은 스푸핑 공격이나 위치 추적 공격에 활용될 수 있다. 제안하는 방식에서는 도청된 내용을 그대로 이용할 수 없도록 하기 위하여 리더의 질의에 랜덤 값을 포함시키고, 태그의 응답이 랜덤 값에 따라 달라지도록 하였다. 또한, 태그에 의해 생성되는 가변적인 정보는 암호화된 ID의 임의 추출 값으로서 공격자에게 어떠한 ID 정보도 제공하지 않는다.
- 위치 추적과 재전송 공격 : 제안하는 프로토콜에서는 리더의 질의에 대한 태그의 응답이 매번 달라지므로 공격자가 태그의 실제 ID는 물론 각 세션에서의 서로 다른 응답이 동일한 태그에 의한 것인지 판별할 수 없도록 하여 강한 익명성을 보장할 수 있다. 또한, 이전 세션에서 획득한 정보를 이용하여 재전송 하는 경우, 현재 세션에서 만들어진 pID_n와 저장되어 있는 이전 세션의 pID_{n-1} 값을 비교하여 정당하지 않은 상대임을 알 수 있으므로 재전송 공격을 불가능하게 한다.
- 스푸핑 공격 : 본 프로토콜에서는 공격자가 리더로 가장하는 경우, *oID*를 알고 *RNo*를 랜덤하게 생성하여 태그에게 전송하여야 한다. 랜덤 값의 범위는 태그의 데이터 블록 크기와 구조를 알지 못하면 생성할 수 없으며, 만약 이전 세션에서 도청한 값을 그대로 사용한다면

태그와 서버에 저장된 *pID* 값의 비교에 의해 정상적인 인증 절차가 아님을 알 수 있게 된다. 또한 공격자가 태그로 가장하는 경우에는 태그에 저장되어 있는 *eID*를 알지 못하고서는 올바른 *pID*를 생성할 수 없고, 리더의 질의에 포함되는 랜덤 값은 매번 변경되므로 이전 세션에서 도청한 값을 이용할 수도 없다.

- 정보전송 방해 : 제안하는 프로토콜에서는 태그 내에 저장되는 ID 정보(*eID*)가 고정적이므로 서버와 태그 간의 인증 프로토콜 수행 중에 발생하는 정보 유실에 대한 복구 과정이 불필요하다.

5.2 효율성 평가

제안하는 프로토콜 기법에서 태그가 필요로 하는 연산은 리더가 생성한 랜덤 값에 대한 임의의 bits를 추출하는 것이므로, 기존의 기법들에서 사용하는 해쉬 함수 수행이나 랜덤 값 생성과 같은 태그 연산량보다 매우 적은 비용으로 프라이버시를 보호할 수 있다. 또한, 제안 방식에서의 서버는 시스템 초기화 단계에서 SEED 알고리즘에 의한 ID 암호화 연산을 필요로 하며, 인증 세션 동안에는 ID 검색을 위한 평균 n(태그수)/2 회의 비트마스킹을 수행함으로써, 해쉬 함수 수행과 같은 기존 기법에 비해 서버에서의 연산량 또한 효율적으로 개선됨을 알 수 있다. <표 3>은 기존 기법과 제안하는 방식을 효율성에 대하여 비교, 분석한 내용이다.

<표 3> 효율성 비교

	태그	리더	서버
Hash Lock	해쉬:1	-	-
Randomized Hash Lock	랜덤화:1 해쉬:1	해쉬:(n/2)	-
Hash Chain	해쉬:2	-	해쉬:(n/2)*i (i:카운트)
Variable ID	해쉬:3	랜덤화:1	랜덤화:1 해쉬:3
Proposed Scheme	비트마스킹:2	랜덤화:1	비트마스킹: n/2

6. 결 론

본 논문에서 제안하는 RFID 시스템의 태그 구조는 다양한 목적에 적용 가능한 다중 객체를 지원할 수 있는 방식으로 구성되며, 이는 RFID 시스템의 기능과 목적에 따라 사용자가 별도의 태그를 소유하지 않고 하나의 태그 내에 인증 가능한 정보를 통합 관리하는 방식이다. 하나의 태그 내에 여러 개의 ID를 가짐으로써 사용자의 입장에서 여러 가지 편리한 기능을 제공하지만, 태그의 위조나 프라이버시를 보호하기 위한 장치를 더욱 철저히 마련해야 한다. 이를 위해, 현재 가장 널리 사용되는 암호화 방식인 SEED 알고리즘을 적용하여 태그 구조에 맞게 각 태그 ID에 대한 암호화 ID를 생성하고, 사용자 프라이버시를 보호하기 위한 인증 프로토콜을 본 논문에서 제안하였다. SEED 알고리즘의 암호화에는 많은 비용이 들지만, 이를 시스템 초기화 시에만 서버에서 수행하게 하고, 매 세션마다 이루어지는 인증 프로토콜에서는 랜덤 값에 의한 암호화 ID의 임의 bits 추출 방식으로 태그와 서버의 연산을 효율적으로 수행할 수 있도록 하였다.

참 고 문 헌

[1] S.A. Weis, "Security and Privacy in Radio-Frequency Identification Devices", Masters thesis, MIT, http://theory.lcs.mit.edu/~sweis/masters.pdf, 2003.

[2] S.A. Weis, S.E. Sarma, R.L. Rivest and D.W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", First International Conference on Security in Pervasive Computing, LNCS 2802, Springer-Verlag, pp.201-202, 2003.

[3] M. Ohkubo, K. Suzuki and S. Kinoshita, "Cryptographic Approach to "Privacy-Friendly" Tags", RFID Privacy Workshop, http://www.frid.edu.com, 2003.

[4] J. Saito and K. Sakurai, "Variable ID

Scheme of Anonymity in RFID tags", The 2004 Symposium on Cryptography and Information Security, Vol. I, pp.713-718, 2004.

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

[6] mCloak: Personal/corporate management of wireless devices and technology, http://www.mobilecloak.com, 2003.

[7] Federal Information Processing Standards(FIPS), "Data Encryption Standard(DES)", NIST, Technical Report 46-2, January 1988.

[8] ISO/IEC/JTC 1/SC 31, Information technology-Radio frequency identification for item management-Unique identification for RF tags, ISO/IEC 15963, 2004.

[9] Telecommunication Technology Association (TTA), "Technical Report on Numbering an RFID tag", *TTA Technical Report TTAR-06.0013*, 2006.

[10] 강수영, 이임영, "난수를 이용하여 동기화를 제공하는 RFID 프라이버시 보호 기법에 관한 연구," *멀티미디어학회 논문지*, 제10권, 5호, pp.623-630, 2007.

정 종 진 (Jong-Jin Jung)

- 1992년 2월 : 인하대학교 전자계산공학과 (공학학사)
- 1995년 2월 : 인하대학교 전자계산공학과 (공학석사)
- 2000년 2월 : 인하대학교 전자계산공학과 (공학박사)
- 1998년 3월~2002년 8월 : 경문대학 인터넷미디어정보과 조교수
- 2002년 9월~현재 : 대진대학교 컴퓨터공학과 부교수
- 2008년 1월~현재 : 한국지능정보시스템학회 이사
- 관심분야 : 전문가시스템, 지능형 에이전트, RFID/센서 네트워크

김 지 연 (Ji-Yeon Kim)

- 1992년 2월 : 인하대학교 전자계산공학과 (공학학사)
- 1997년 2월 : 인하대학교 전자계산공학과 (공학석사)
- 2005년 6월 : 인하대학교 컴퓨터공학부 (공학박사 수료)
- 1997년 1월 ~ 2001년 2월 : LG정보통신 이동교환실 주임연구원
- 2001년 3월 ~ 2005년 8월 : 청강문화산업대학 인터넷비즈니스과 조교수
- 2006년 3월 ~ 현재 : 대진대학교 컴퓨터공학과 강의교수
- 관심분야 : 이동통신, RFID/센서네트워크, 정보보안