다중 객체 지원을 위한 RFID 시스템에서 보안 레벨 기반의 인증 기법에 관한 연구

A Study on Security Level-based Authentication for Supporting Multiple Objects in RFID Systems

김지연(Ji-Yeon Kim)*, 정종진(Jong-Jin Jung)**,
조근식(Geun-Sik Jo)***, 이균하(Kyoon-Ha Lee)***

초 록

RFID 시스템은 비가시 거리에서의 무선통신을 이용한 자동식별 기능을 제공하고 다양한 환경 변화에 대해 적응력이 뛰어난 기술로서 최근 여러 산업분야와 개인 생활환경에 있어서 응용범위를 넓혀가고 있다. 그러나 기존의 RFID 응용시스템들은 하나의 태그에 하나의 객체 식별정보가 저장되는 구조를 기반으로 하고 있기 때문에 RFID 시스템의 응용이 증가될수록 많은 태그들이 혼재하게 되어 사용자 관점에서의 불편을 초래하게 된다. 또한 많은 태그들에 저장되는 개인정보가 RFID 무선통신의 불안정성으로 인하여 공격에 노출됨으로써 심각한 사생활 침해의 문제를 종종 야기하고 있다. 따라서 RFID 시스템의 확대 발전을 위해서는 안정적인 정보보안을 바탕으로 한 응용들 간의 효율적인 정보공유 방법이 요구된다. 이러한 측면에서 본 논문에서는 하나의 태그로 다수 개의 RFID 응용 객체에 접근할 수 있도록 하는 다중 객체 접근 방식의 RFID 태그 구조를 설계하고, 이에 적합한 인증 프로토콜을 제안한다. 제안된 인증 프로토콜은 저사양의 태그 구조 하에서도 통신을 방해하는 다양한 공격에 강인하도록 설계되었다. 특히 본 논문에서는 여러 개의 리더에 대한 인식 동작을 효율적으로 수행하기 위해 응용 객체별로 보안 레벨을 부여하고, 보안 레벨에 따라 각각 다른 인증 절차를 수행하도록 한다. 마지막으로 다양한 실험 및 분석을 통하여 제안한 인증 기법이 기존의 방법들과 비교하여 효율적임을 증명한다.

ABSTRACT

RFID systems provide technologies of automatic object identification through wireless communications in invisible ranges and adaptability against various circumstances. These advantages make RFID systems to be applied in various fields of industries and individual life. However, it is difficult to use tags with distinction as tags are increasingly used in life because a tag usually stores only one object identifier in common RFID applications. In addition, RFID systems often make serious violation of privacy caused by various attacks because of their weakness of radio frequency communication. Therefore, information sharing methods among applications are necessary for expansive development of RFID systems. In this paper, we propose efficient RFID scheme. At first, we design a new RFID tag structure which supports many object identifiers of different applications in a tag and allows those applications to access them simultaneously. Secondly, we propose an authentication protocol to support the proposed tag structure. The proposed protocol is designed by considering of robustness against various attacks in low cost RFID systems. Especially, the proposed protocol is focused on efficiency of authentication procedure by considering security levels of applications. In the proposed protocol, each application goes through one of different authentication procedures according to their security levels. Finally, we prove efficiency of th proposed scheme compared with the other schemes through experiments and evaluation.

키워드 : 다중 객체, 보안 레벨, 인증 프로토콜, RFID 시스템
Multiple Object, Security Level, Authentication Protocol, RFID System

* 인하대학교 대학원 정보공학과
** 대진대학교 컴퓨터공학과 교수
*** 인하대학교 컴퓨터정보공학부 교수

1. 서 론

RFID 시스템은 무선 주파수를 이용한 비접촉식 자동인식 기술로서, 태그와 리더, 서버로 구성된다. 이중에서도 RFID의 핵심기능이라 할 수 있는 태그는 물리적 접촉 없이도 인식이 가능하다는 장점을 비롯하여 읽기/쓰기가 가능하고, 환경 적응력이 뛰어난 점 등의 여러 가지 장점으로 인하여 교통카드, 톨게이트 요금징수, 물류관리, 출입통제 등 다양한 분야에서 사용되고 있을 뿐만 아니라, 미래에는 더욱 다양한 목적으로 활용될 전망이다. 따라서 각종 물건들에 점점 더 많은 RFID 시스템의 태그가 부착될 것이고, 개인생활에 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 개인정보는 곳곳에 설치될 리더를 통해 전송하게 되는데, 이 때 무선통신의 불안정한 특성으로 인해 정보유출이나 위치추적과 같은 사용자 프라이버시를 침해하는 심각한 문제점도 발생시킬 수 있다. RFID 시스템에 발생 가능한 공격들에는 도청, 위치추적, 스푸핑, 재전송, 메시지 유실 등이 있으며, 이러한 공격들에 대해 Kill command, 패러데이 케이지, 블로커 태그, Hash lock, Hash chain, Hash 기반 ID 변형 등 여러 방법들이 연구되었다. 물론, 이러한 방법들은 하나의 리더에 대하여 여러 태그를 인식하는 기술구조를 기반으로 하고 있다. 즉, 기존의 RFID 응용 시스템에서 하나의 태그에는 하나의 객체를 식별하기 위한 정보가 저장되어 객체 하나로서 동작하게 되는 것이다. 따라서 이러한 방법들은 RFID 시스템의 보급이 확대될 경우를 적절히 대응하지 못하고 있으며 또한 여전히 일부 공격들에 약점들을 가지고 있다.

본 논문에서는 하나의 태그로 다수 개의 RFID 응용 객체에 접근할 수 있도록 하는 다중 객체 접근 방식의 RFID 시스템 방식을 제안한다. 이에 따라 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 많은 연산량을 요구하는 것과는 달리, 저사양의 태그 구조 하에서도 통신을 방해하는 다양한 공격에 강인하도록 설계하였다. 또한, 여러 개의 태그에 대한 인식 동작을 효율적으로 수행하기 위해 응용 객체의 보안 레벨을 정의하여 보안 레벨에 따라 인증 절차를 다르게 수행하도록 한다. 본 논문의 구성은 먼저 제 2장에서 RFID 시스템의 기술 개요 및 기존의 관련 연구들을 분석한다. 제 3장에서는 제안하는 RFID 태그 구조 및 인증 프로토콜 방식에 대해 소개하고, 제 4장에서 제안 방식의 성능을 기존 방식과 비교하여 분석한다. 마지막으로 제 5장에서 결론을 내리기로 한다.

2. 관련 연구

RFID 시스템은 물리적 접촉 없이 인식이 가능하므로 개인 정보보호와 안전성 측면의 여러 문제점들을 야기할 수 있다. 특히 리더

와 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 인식하게 할 가능성이 있다. 가능한 공격들의 유형과 그에 대해 RFID 시스템이 갖추어야할 안전성 측면의 요구사항을 살펴보면 다음과 같다[8].

- 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 위치추적을 할 수 있다. 따라서 RFID 시스템은 도청된 정보로부터 어떠한 키 값도 유추할 수 없도록 설계되어야 하며 도청한 정보를 다시 사용하여 재전송하거나, 사용자의 위치를 추적할 수 없도록 하는 인증 프로토콜을 가져야 한다.
- 재전송(Replay) : 도청 공격을 통해 리더와 태그 간에 전송되는 정보를 알아낸 후 그 정보를 임의의 태그에 저장하고, 리더로부터 질의를 받았을 때 저장된 메시지를 전송함으로써 임의의 태그를 정당한 태그인 것처럼 가장하는 공격이다. 따라서 도청한 정보를 재전송하더라도 정상적인 세션이 이루어지지 못하도록 인증 프로토콜이 설계되어야 한다.
- 위치추적(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) : 이 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.
- 메시지 유실(Message Loss) : 이 공격은 RFID 시스템이 정상적으로 작동하지 못하도록 하기 위한 공격으로 공격자가 고의적으로 또는 시스템 상의 문제로 인하여 리더와 태그 사이에 발생되는 통신 내용이 유실되는 것이다. 메시지 유실로 인하여 리더와 태그 간 에 동기가 맞지 않을 경우 태그의 사용이 어려워질 수 있다. 따라서 안전한 RFID 시스템은 정보 전송 방해 및 메시지 차단에 대한 공격 탐지 기능을 가져야 한다.

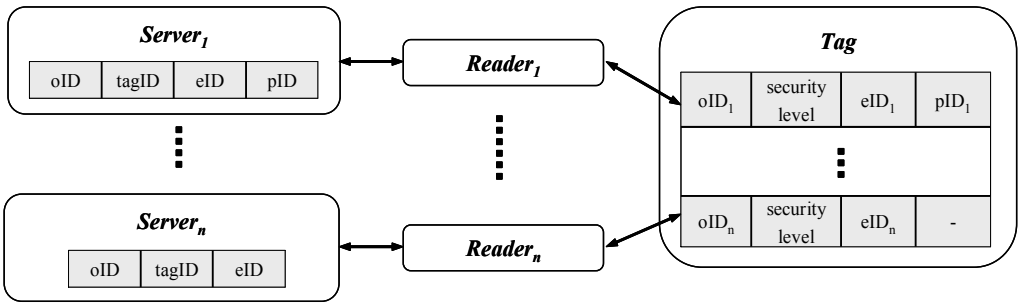
RFID 시스템의 안전성을 위협하는 여러 공격들에 대한 문제점을 해결하기 위한 기존의 방법들로는 Kill 명령어 기법[8], 패러데이 케이지 기법[10], 블로커 태그 기법[2] 등의 물리적 보안 기법들과 암호학적인 방법을 이용한 인증 기법들이 있다. 이들 중 현재 RFID 시스템에서 주로 연구되고 있는 암호학적인 인증 기법들에 대해 간략하게 살펴본다.

- 해쉬 락(Hash Lock) 기법[9] : 이 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 키를 획득하는 경우 공격자가 다시 리더로 가장하면 태그의 ID를 얻는 것이 가능하므로 정당한 태그로 가장할 수 있는 스푸핑 공격도 가능하다는 문제점이 있다.
- 확장된 해쉬 락(Randomized Hash Lock) 기법[9] : 이 기법은 해쉬 락 기법을 개선한 방식으로 태그가 난수를 생성하여 매 세션마다 다른 응답을 하도록 함으로써, 공격자에 의한 위치추적을 방지할 수 있게 된다. 그러나 이 기법에서는 리더가 태그에게 ID를 전송하는 인증 프로토콜의 마지막 단계에서 공격자에 의해 ID가 노출될 가능성이 있다.
- 해쉬 체인(Hash Chain) 기법[7] : 이 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 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.
- 해쉬 기반 ID 변형 기법[6] : 이 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.

3. 다중 객체 기반의 RFID 시스템

3.1 다중 객체 접근 방식의 태그 구조 설계

RFID 시스템이 적용되는 분야는 산업, 가정 그리고 직장 등 다양한 분야와 생활권역에 걸쳐 널리 분포되어 있다. 기존에는 용도에 따라 각각의 RFID 태그를 사용하고 있으나, RFID 시스템 환경이 모든 생활 전반에 점차 확대되고 있는 시점에서 개인 사용자의 편의성을 위해 하나의 태그로 여러 종류의 RFID 시스템에 접근할 수 있도록 하는 것이 더욱 적합할 것이다. 한 개의 RFID 태그만으로 여러 가지 용도의 RFID 객체에 적용하게 되면 정보의 통합과 활용의 용이성을 달성할 수 있다. 본 논문에서는 <그림 1>과 같이 하나의 태그 내에 다수 개의 ID를 저장하도록 설계함으로써 여러 종류의 RFID 시스템 객



〈그림 1〉 제안하는 태그 구조

체에 접근할 수 있도록 한다.

RFID 시스템은 여러 개의 태그들을 서로 구별하기 위하여 고유한 키 값인 *tagID*를 이용한다. 또한, 존재하는 여러 개의 RFID 시스템 요소들은 그 용도에 따라 분류하여 객체의 형태로 정의하고 이 분류된 객체의 번호를 *oID*(object ID)로 정의할 수 있다. 따라서 제안하는 RFID 태그 내에는 고유한 식별자인 *tagID*와 객체를 분류하기 위한 *oID*가 함께 저장된다. *oID*는 고유한 *tagID*와 함께 Fast SEED 알고리즘을 이용한 암호화 과정에 사용되고, 암호화된 결과값을 *eID*(encrypted ID)로 정의한다. 이때 Fast SEED 알고리즘은 기존의 민간 분야의 암호사용을 촉진하기 위해 개발된 SEED 알고리즘을 RFID 태그 환경에 맞게 키 크기를 변경하고 라운딩 횟수를 축소하여 자체 개발한 암호화/복호화 알고리즘으로서, 본 논문에서는 이미 암호화가 수행된 상태에서의 인증 프로토콜에 관해 다루고 있기 때문에 자세한 내용은 생략하도록 한다[3]. 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.

〈표1〉 서버와 태그에 저장되는 정보

	정보
서버(DB)	tagID, eID, pID
태그	oID, eID, pID

- *tagID* : 태그별 고유한 ID이며, *oID*와 함께 *eID*를 생성하기 위한 키로 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 Fast 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[4]에서 제안한 ID 길이인 128bits를 *eID*와 나누어 사용할 수 있

다. 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 Fast 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.

3.2 보안 레벨을 적용한 인증 프로토콜의 설계

다중 객체를 지원하는 태그는 다양한 종류의 RFID 응용들에 다목적으로 사용된다. 본 연구에서는 [5]를 통하여 다중 객체를 지원하기 위한 인증 프로토콜을 제안하였다. 그러나 [5]에서 제안된 인증 프로토콜은 다수의 RFID 응용들에 대응되는 다중 객체를 지원하는데 반해서 이러한 RFID 응용들이 요구하는 보안 수준의 차이와 인증 절차의 다양성을 반영하지 못하고 있다. 실제 환경에서 RFID 응용 객체들은 금융 시스템과 같이 보안이 매우 중요한 분야와 그렇지 않은 분야로 나뉠 수 있다. 따라서 보안 레벨의 수준을 정의하고, 여러 RFID 응용 객체들을 요구되는 보안 레벨에 따라 각각 분류할 수 있다. 보안 레벨에 따라 RFID 응용 객체들에 대해 인증 프로토콜을 다르게 적용하게 되면 인증 과정에 소요되는 시간과 연산량을 감소시킬 수 있다. 따라서 본 논문에서 제안하는 RFID 시스템의 인증 프로토콜은 다중 객체를 지원하는 태그 구조에 적합하면서 동시에 보안 레벨을 구분하여 동작하도록 설계하였다. 인증 절차가 시작되기 전의 시스템 초기화 단계에서 서버와 태그는 암호와 알고리즘에 의해 생성된 *eID*를 각각 저장한다. 이렇게 태그에 암호화된 값을 저장함으로써 불법적인 태그의 복제 및 정보 해독이 용이하지 않다. 인증 절차가 시작되면, 응용 객체의 보안 레벨에 따라 구분된 프로토콜이 다음과 같이 동작한다.

(1) RFID 리더는 해당하는 응용 객체의 *oID*와 랜덤 값(*RNo*)을 태그에게 전송한다. *RNo* 값은 매 세션마다 생성되며, 다음과 같이 구성된다. 보안 레벨이 낮은 응용 객체의 리더는 oID만 태그에게 전송한다.

$$RNo = R_{Forward_no} || R_{Backward_no}$$

(2) 보안 레벨이 높은 응용 객체의 태그에서는 먼저 전송된 *RNo* 값을 이용하여 *eID*의 변환에 적용할 $R_{Forward}$와 $R_{Backward}$ 값

을 다음과 같이 생성한다.

$$R_{Forward} = R_{Forward_no} \ mod \ (sizeof\ encryptedID/2),$$

$$R_{Backward} = R_{Backward_no} \ mod \ (sizeof\ encryptedID/2)$$

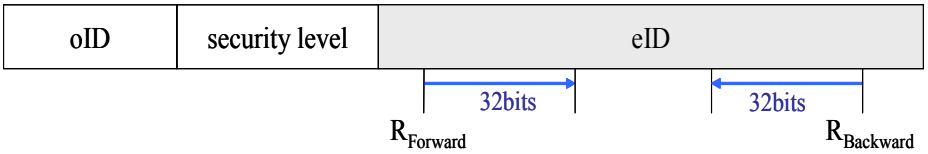
이렇게 생성된 $R_{Forward}$와 $R_{Backward}$는 *eID*에서 bit masking 동작을 수행할 비트의 위치를 의미하며, <그림 2>와 같이 *pID*를 생성한 후, 태그 메모리에 저장한다. 보안 레벨이 낮은 응용 객체의 태그에서는 (2)과정이 생략된다.

(3) 태그는 리더에게 *pID* 또는 *eID*를 전송한다. 보안 레벨이 낮은 응용 객체의 태그에서는 (2)과정을 생략하여 *pID*를 생성하기 위한 연산 시간을 감소하는 대신 리더에게 *eID*를 그대로 전송한다.

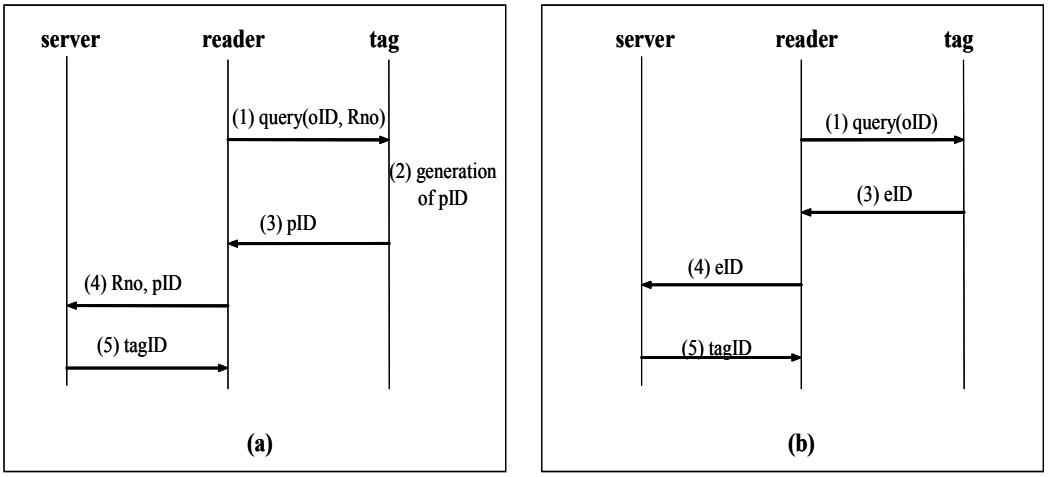
(4) 리더는 해당 응용 객체의 서버에게 랜덤값 *RNo*와 태그에게서 전달받은 *pID* 혹은 *eID*를 전송한다.

(5) 서버에서는 보안 레벨에 따라 전송된 *pID* 혹은 *eID*를 이용하여 복호화 과정을 수행한다. *pID*가 전송될 경우 함께 전송된 *RNo*를 적용하여 일치하는 *eID*를 찾아낸 다음 복호화 알고리즘을 수행해야 한다. 복호화 과정 후 구해진 *tagID*를 통해 사용자 정보를 검색할 수 있고, 현재의 태그가 정당한 태그임을 인증하게 된다.

앞서 설명한 인증 절차를 <그림 3>과 같이 표시할 수 있다.



〈그림 2〉 pID 생성 과정



〈그림 3〉 제안하는 인증 프로토콜 : (a) 고수준 보안 레벨 (b) 저수준 보안 레벨

4. 성능평가

4.1 안전성 평가

제안하는 프로토콜은 다음과 같은 공격에 대해 안전성을 보장할 수 있으며, <표 2>는 기존의 인증 기법들과 안전성을 비교 분석한 표이다. <표 2>에서 기존의 기법들에 대한 안전성 평가는 다수의 논문들에서 공통으로 다루고 있는 결과이다.

〈표 2〉 공격에 대한 안전성 비교
(O : 강함, X : 약함)

	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
제안 기법	O	O	O	O

- 도청 공격 : 공격자에 의해 획득된 도청 내용은 스푸핑 공격이나 위치 추적 공격에 활용될 수 있다. 제안하는 프로토콜에서는 도청된 내용을 그대로 이용할 수 없도록 하기 위하여 리더의 질의에 랜덤값(*RNo*)을 포함시키고, 태그는 랜덤값에 따라 매번 달라지는 pID_n 값을 생성하여 전송하도록 하였다. 또한, 태그에 의해 생성되는 가변적인 pID_n 값은 암호화된 *eID*의 임의 추출값으로서 공격자에게 어떠한 ID 정보도 제공하지 않는다.
- 위치추적과 재전송 공격 : 제안하는 프로토콜에서는 리더의 질의에 대한 태그의 응답이 랜덤값(*RNo*)에 의해 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 pID_{n-1} 정보를 이용하여 재전송 공격하는 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. 즉, 공격자가 pID_{n-1} 값을 도청하여 정당한 태그로 가장하고 리더의 인식에 응답하여 재전송 공격을 한다 하더라도 리더가 전송한 *RNo*를 알지 못하고, 또한 *RNo*는 매 세션마다 달라지기 때문에 결국 서버에서의 현재 *RNo*에 의한 pID_n와 이전 *RNo*에 의한 pID_{n-1}의 비교를 통하여 재전송 공격에 대한 방어를 할 수 있게 된다.
- 스푸핑 공격 : 본 프로토콜에서는 공격자가 리더로 가장하는 경우, *oID*를 알고 *RNo*를 랜덤하게 생성하여 태그에게 전송하여야 한다. *RNo* 값의 범위는 태그의 데이터 블록 중 *eID*의 크기 및 범위 값을 바탕으로 연산하여 생성하기 때문에 데이터 블록 크기와 세부 데이터 구조(*oID* 크기 + *security level* 크기 + *eID* 크기)를 모두 알지 못하면 생성할 수 없다. 만약 리더로 가장한 공격자가 이전 세션에서 태그로부터 도청한 pID_{n-1} 값을 그대로 사용한다면 태그와 서버에 저장된 pID_{n-1} 값과 *RNo*에 의해 생성되는 *pID* 값의 비교에 의해 정상적인 인증 절차가 아님을 알 수 있게 된다. 또한 공격자가 태그로 가장하는 경우에는 태그에 저장되어 있

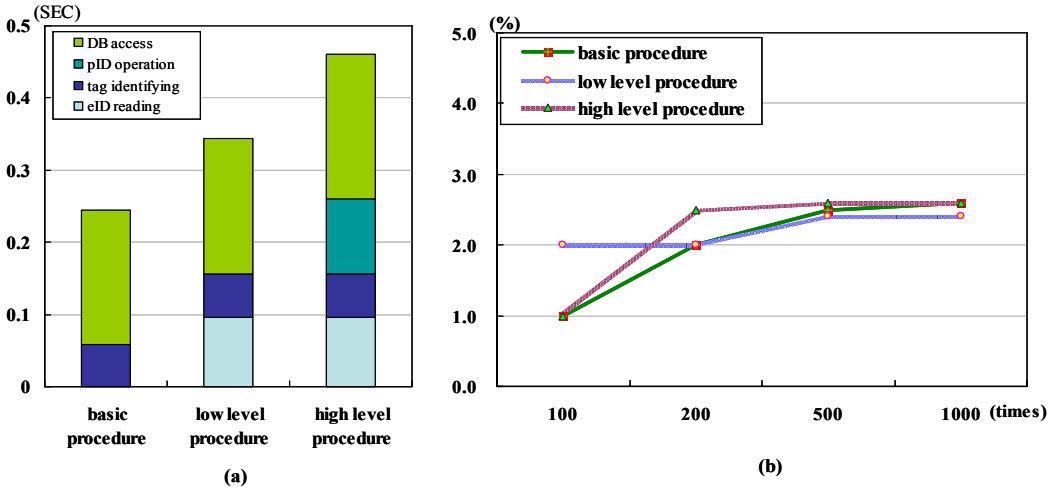
는 *eID*를 알지 못하고서는 올바른 *pID*를 생성할 수 없고, 만약 이전 세션에서 pID_{n-1} 값을 도청하여 알고 있다 하더라도 리더의 질의에 포함되는 *RNo* 값은 매번 변경되므로 도청한 pID_{n-1} 값을 이용할 수 없다.

- 메시지 유실 공격 : 제안하는 프로토콜에서는 태그 내에 저장되는 ID 정보(*eID*)가 고정적인데 반해 서버와 태그 간의 인증 프로토콜 수행 중에 서로 전송하는 정보는 *eID*를 바탕으로 임의적으로 생성하는 *pID* 값이다. 따라서 정보 유실에 의한 복구과정이 불필요하고, 만약 현재 세션이 흐트러지게 되더라도 고정 값인 *eID*를 이용하여 곧 바로 복구할 수 있다.

4.2 효율성 평가

제안하는 인증 기법에 대한 효율성을 평가하기 위하여 다중 객체 접근 방식의 RFID 태그에 대한 연산시간과 평균 에러율에 대해 시뮬레이션을 수행하였다. 시뮬레이션에 사용된 RFID 시스템은 13.56MHz 밴드의 리더와 2Kbits의 읽기/쓰기 메모리를 가진 태그이며 통신표준은 ISO15693을 따른다. 물론 시뮬레이션용 RFID 시스템은 기존의 단일 객체 접근 방식이기 때문에 리더가 태그 메모리의 특정 블록에 저장된 데이터를 단순히 읽어오는 형태이다. 따라서 본 논문에서는 이러한 단일 객체 접근 방식의 RFID 시스템 환경 하에서 다중 객체 접근 방식의 프로토콜에 대한 시뮬레이션을 수행하기 위하여 <그림 2>에서 보이는 것처럼 태그 메모리에 객체번호 영역(*oID*), 보안 레벨 영역(*security level*), 암호화된 객체 ID(*eID*) 영역 등의 데이터 구조를 정의하고, 이 중 특정 영역의 데이터를 액세스하기 위한 알고리즘의 구현을 통하여 시뮬레이션을 수행하도록 하였다. 총 100개의 태그에 대하여 각 태그마다 7개씩 객체 데이터 예제를 기록하고, 동일한 데이터를 서버의 데이터베이스에 저장하였다. 이 때 객체 ID와 태그 ID를 이용한 암호화는 이미 수행한 상태에서 인증 절차에 대한 연산시간과 에러율에 대해 측정하였다. 연산시간에 대한 실험에서는 인증 프로토콜을 사용하지 않고 서버와 통신하였을 경우*(basic procedure)* 걸리는 시간과 저수준 보안 레벨*(low level procedure)*에 해당하는 RFID 응용 객체에서의 태그와 서버 간 인증에 걸리는 시간, 그리고 고수준 보안 레벨*(high level procedure)*에 해당하는 RFID 응용 객체에서의 태그와 서버 간 인증에 걸리는 시간을 각각 100회씩 반복 수행하여 구하고, 이에 대한 평균 데이터를 비교 분석하였다. 에러율에 대한 실험은 연산시간 측정 동안에 발생된 에러 횟수를 조사한 것이다.

<그림 4>의 분석 결과를 통해 여러 가지 공격에 대해 안전성을 보장하기 위한 고수준 보안 레벨(*high level procedure*) 방식의 인증 프로토콜을 사용하였을 경우에도 서버와의 통신에 걸리는 시간이 비교적 높지 않고, 안정적이라는 사실을 알 수 있다. 평균 에러율에 대한 실험에서는 세 가지 방법 모두 비슷한 결과를 볼 수 있다. 이 사실은 실생활에 적용되는 RFID 시스템에서 리더를 통한 서버와 태그 간의 통신에 인증 프로토콜을 적용하였을 경우 시스템 구현 방법에 영향을 받지 않고도 여러 가지 공격에 대해 안전성을 보장할 수 있다는 것을 보여준다.



〈그림 4〉 효율성 실험 결과 : (a) 연산 시간 (b) 에러율

5. 결론 및 향후 연구

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 태그들을 소유하지 않고 하나의 태그 내에 인증 가능한 정보를 통합 관리할 수 있는 장점을 내포하고 있다. 즉, 하나의 태그 내에 여러 개의 ID를 가짐으로써 사용자의 입장에서 여러 가지 편리한 기능을 제공할 수 있는 것이다. 이를 위해 기존의 암호화 방식인 SEED 알고리즘을 RFID 환경에 맞게 경량화시킨 Fast SEED 알고리즘을 적용하여 태그 구조에 맞게 각 태그 ID에 대한 암호화 ID를 생성하고, 사용자 프라이버시를 보호하기 위한 인증 프로토콜을 본 논문에서 제안하였다. Fast SEED 알고리즘의 암호화에는 많은 비용이 들지만, 이를 시스템 초기화 시에만 서버에서 수행하게 하고, 매 세션마다 이루어지는 인증 프로토콜에서는 랜덤 값에 의한 암호화 ID의 임의 비트 추출 방식으로 태그와 서버의 연산을 효율적으로 수행할 수 있도록 하였다. 특히 제안하는 인증 프로토콜에서는 서로 다른 RFID 응용 시스템들이 요구하는 보안 수준에 따라 다른 인증 절차를 수행하도록 함으로써 저사양의 태그에서도 효율적인 동작이 가능하도록 하였다. 제안 기법의 효율성과 안전성의 평가를 위하여 에러율과 연산시간에 대한 시뮬레이션 실험을 수행한 결과, 제안 기법이 안정적이면서도 RFID 응용 환경에 적용 가능한 수준임을 확인할 수 있었다.

그러나 본 논문의 실험 결과는 시뮬레이션 실험을 통하여 생성한 값이므로 실제 RFID 환경과는 다소 차이가 발생할 수 있다. 향후에는 다중 객체 태그 구조와 그에 따른 인증 프로토콜을 지원하는 리더를 설계 및 구현하여 제안하는 기법을 실제적인 환경에서 적용할 수 있도록 물리적인 시스템을 구현해야 할 것이다.

참 고 문 헌

[1] Auto-ID Center, 860-930MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation Version 1.0.1, Technical Report, Auto-ID Center, MIT, 2002.

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

[3] Ko, H., Kim, J., Jung, J., Lee, Y., Joe, S., and Chang, Y., "A Study on the RFID Tag Encryption using Fast SEED," Proceedings of the International Conference on Computational Methods in Science and Engineering 2007 (ICCM SE 2007), Vol. 2, Parts B, 2007, pp. 571-574.

[4] ISO/IEC/JTC1/SC31, Information technology - Radio Frequency Identification for Item Management - Unique Identification for RF Tags, ISO/IEC 15963, 2004.

[5] Kim, J., Jung, J., Ko, H., Joe, S., Lee, Y., Chang, Y., and Lee, K., "A Design of Authentication Protocol for Multi-Key RFID Tag," APWeb/WAIM 2007 International Workshops, LNCS 4537, Springer-Verlag, 2007, pp. 644-653.

[6] Saito, J. and Sakurai, K., "Variable ID Scheme of Anonymity in RFID tags," The 2004 Symposium on Cryptography and Information Security, 2004, pp. 713-718.

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

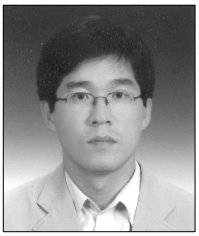
[8] Weis, S. A., Security and Privacy in Radio-Frequency Identification Devices, Masters Thesis, MIT, 2003.

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

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

저 자 소 개

김지연	(E-mail : jini_69@naver.com)
1992년	인하대학교 공학사 (전자계산학)
1997년	인하대학교 공학석사 (전자계산공학)
2002년	인하대학교 컴퓨터정보공학부 박사과정
1997년~2000년	LG정보통신 이동교환실 주임연구원
2001년~2005년	청강문화산업대학 인터넷비즈니스과 조교수
관심분야	이동통신, RFID/센서 네트워크, 정보보안 등



정종진	(E-mail : jjjung@daejin.ac.kr)
1992년	인하대학교 공학사 (전자계산학)
1995년	인하대학교 공학석사 (전자계산공학)
2000년	인하대학교 공학박사 (전자계산공학)
1998년~2002년	경문대학 인터넷미디어정보과 조교수
2002년~현재	대진대학교 컴퓨터공학과 부교수
2008년~현재	한국지능정보시스템학회 이사
관심분야	지능형 에이전트, 지식 기반 스케줄링, RFID/센서 네트워크 등

조근식	(E-mail : gsjo@inha.ac.kr)
1982년	인하대학교 공학사 (전자계산학)
1985년	Queens Colleg/CUNY M.A., Computer Science
1991년	City University of New York, Ph.D., Computer Science
1992년~현재	인하대학교 컴퓨터정보공학부 교수
2006년~현재	BK 21 지능형 유비쿼터스 물류기술 연구사업단장
2008년~현재	한국지능정보시스템학회 회장
관심분야	지능형 전자상거래, 전문가 시스템, 지식 기반 스케줄링, CSP 등

이균하	(E-mail : khlee@inha.ac.kr)
1970년	인하대학교 전기공학과 (공학사)
1976년	인하대학교 전자공학 (공학석사)
1981년	인하대학교 전자공학 (공학박사)
1981년~2007년	인하대학교 컴퓨터정보공학부 교수
2007년~현재	인하대학교 컴퓨터정보공학부 명예교수
관심분야	패턴인식, 지능통신망 등