한국산학기술학회논문지
Vol. 10, No. 2, pp. 313-319, 2009

# 물류 시스템에 적합한 RFID 다중 인증방법

배우식[1], 이종연[2*]

# A RFID Multi-Authentication Method for Logistics Systems

**Woo-Sik Bae[1] and Jong Yun Lee[2*]**

**요 약** 최근 들어 RFID 시스템은 무선으로 동시에 여러 태그를 인식할 수 있는 장점으로 기존 바코드를 대체할 수 있는 새로운 기술로 부상하고 있다. 또한 산업계에서는 물류, 유통 분야를 비롯하여 널리 사용할 수 있는 보안성이 보장된 태그 및 인증 프로토콜에 대한 연구가 활발히 진행 중이다. 본 논문에서는 RBAC 개념을 인증프로토콜에 접목하고 보안성이 강화된 프로토콜과 보안성을 낮추고 효과적인 대량 인증을 할 수 있는 방법을 제안하며 제안하는 방식은 해쉬 함수를 기반으로 스푸핑공격, 트래픽분석, 재전송공격 등에 대한 안정성이 보장되는 장점이 있다.

**Abstract** Recently the RFID system, which can recognize multiple tags simultaneously through wireless communication, is emerging as a new technology that can replace the barcode system. Furthermore, related industries are carrying out active research on tags and authentication protocols with guaranteed security that are widely applicable to logistics, distribution, etc. The present study proposes a protocol with enhanced security by introducing the concept of RBAC to the authentication protocol, and a method with lower security for effective mass authentication. The proposed method is advantageous in that it guarantees security against spoofing attack, traffic analysis, replay attack, etc. based on hash function.

**Key Words :** RFID, Security, Logistics

## 1. 서론

RFID(Radio Frequency Identification)는 전자 태그(Tag)를 사물에 부착하여, 사물이 주위 상황을 인지하고 기존 IT 시스템과 실시간으로 정보를 교환, 처리할 수 있는 기술이다. 미래에 사용의 편리성 향상으로 개인 및 산업 전반에 활용이 예상 되며 많은 기술 발전과 국내 · 외적으로 많은 연구가 진행되고 있다. 그러나 마이크로칩에 내장된 정보를 무선주파수를 이용하여 읽어내기 때문에 RFID 기술은 도청, 트래픽분석, 서비스거부공격, 메시지유실, 트래킹공격, 스푸핑공격 등 무선 네트워크상의 많은 취약점 들을 지니고 있다. 따라서 RFID 시스템이 활성화되기 위해서는 리더와 태그 사이의 안전한 상호인증이 매우 중요하다.

본 논문에서는 RFID의 프라이버시 문제를 해결하기 위한 기존 제안된 해쉬-락 기법[1,2,3], 확장된 해쉬-락 기법[4,5] 등이 해결하지 못한 문제점 분석을 통해 보다 안전하고 효율적으로 태그 데이터를 보호할 수 있는 인증 프로토콜을 제안한다. 제안하는 프로토콜은 리더의 역할 기반접근제어로 불필요한 데이터의 송수신을 줄여 주며 태그의 일정한 데이터를 송신하는 것을 바탕으로 한다.

## 2. 관련연구

### 2.1 RFID 태그 코드

RFID 코드체계는 국제적으로 ISO/IEC 15459, ISO/IEC 15963, ISO/IEC 11784(동물코드), ISO/IEC 10374(컨테이너 코드), EPC, ucode 등이 있다. 국내 모바일 환경에서 RFID 서비스 제공을 위한 모바일 RFID 코드체계 및 국내 RFID 산업에 적용을 위한 국제 표준 규격인 ISO/IEC 15459 기반 IOS/IEC KKR 코드 체계가 있다. EPC 코드

본 논문은 2008년도 지식경제부 성장동력기술개발 사업의 일환으로 (주)메타비즈의 위탁과제로 수행되었음.
[1]충북대학교 컴퓨터교육과 박사과정
[2]충북대학교 컴퓨터교육과 교수
*교신저자: 이종연(jongyun@chungbuk.ac.kr)
접수일 09년 01월 01일 수정일 09년 02월 01일 게재확정일 09년 02월 18일

체계는 그 종류에 따라 구조가 상이하나, 한 가지 동일한 구조는 바로 Header 부분인데, 이를 통해 EPC 코드 종류를 파악할 수 있다. 즉 EPC 코드 체계는 Header 8비트에 따라 나머지 비트의 구조 체계가 상이하며, 현 코드 체계에 따르면 이론상 256개의 종류가 생성 가능하며, EPC Header 확장시 256개 이상의 종류도 생성 가능하다.

EPC 코드는 총길이(비트)에 따라 그 구성 형태가 상이하게 되는데. SGTIN-64, SGTIN-96, STGIN-128 등은 각각 SGTIN이며 64비트, 96비트, 128비트 체계를 갖는다.

### 2.2 GID-96

GID(General Identifier)는 기존 코드 체계와는 관계없이 새롭게 정의된 96비트 EPC 코드체계이다. GID는 관리자 번호, 오브젝트 클래스, 일련번호의 세 필드로 구성되며 인코딩은 [표 1]과 같이 EPC 이름공간에서 유일성을 확보하기 위해 네 번째 필드인 헤더를 포함한다.

**[표 1]** GID-96

| | 헤더 | 업체코드 | 오브젝트 클래스 | 일련번호 |
|---|---|---|---|---|
| GID -96 | 8 | 28 | 24 | 36 |
| | 0011 0101 (2진값) | 268,435,455 (최대10진값) | 16,777,215 (최대10진값) | 68,719,476,735 (최대10진값) |

업체코드는 오브젝트 클래스와 일련번호를 관리할 주체를 식별하며 관리자 번호의 유일성이 있다. 오브젝트 클래스는 상품의 종류나 유형을 식별하기 위해 EPC 관리 주체에 의해 사용 된다. 일련번호는 각 오브젝트 클래스 내에서 유일하게 할당 된다. 관리자는 오브젝트 클래스 내에서 중복되지 않는 고유한 일련번호를 할당해야 한다.

#### 2.2.1 GID-96 인코딩 절차

주어진 값 : EPC 관리자 번호 M $(0 \le M < 2^{28})$, 오브젝트 클래스 C $(0 \le C < 2^{24})$, 일련번호 S $(0 \le S < 2^{36})$

절차 : 최상위 비트로 부터 최하위 비트 방향으로 다음에 나열하는 필드를 연결시켜 인코딩 한다.

- 헤더 00110101, 관리자번호 M (28비트), 오브젝트 클래스 C (24비트), 일련번호 S(36비트).

#### 2.2.2 GID-96 디코딩 절차

주어진 값 ; $00110101b_{87}b_{86}\cdots b0$ 96비트열인 GID-96 (처음 8비트 00110101은 헤더)

결과 : 관리자번호, 오브젝트 클래스, 일련번호

절차 :

1. 부호없는 정수인 $b_{87}b_{86}\cdots b_{60}$ 비트는 EPC 관리자 번호
2. 부호없는 정수인 $b_{59}b_{58}\cdots b_{36}$ 비트는 오브젝트 클래스
3. 부호없는 정수인 $b_{35}b_{34}\cdots b_0$ 비트는 일련번호

### 2.3 기존 프로토콜

#### 2.3.1 해-쉬락 기법

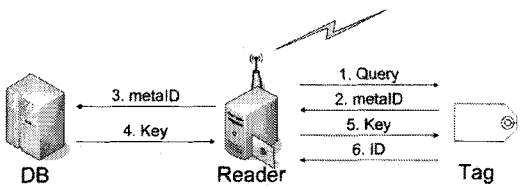
해쉬-락 프로토콜은 낮은 태그 가격을 고려하여 MIT에 의해 제시된 방식으로 Key를 태그, 데이터베이스와 사전에 안전하게 공유되어 있다고 가정하며 인증과정은 다음과 같다.

1) 해쉬-락의 잠금 과정

① 리더 R은 랜덤한 키 key를 선택하고,meta ID 값으로 hash(key)를 계산한다.
② R은 metaID를 태그 T에 기록한다.
③ T는 잠긴 상태(locked state)에 들어간다.
④ R은(metaID, key)를 저장한다.

2) 해쉬-락의 풀림 과정[그림 1]

① R은 태그 T에게 T의 metaID를 질의한다.
② R은 DB에서(metaID, key)를 조사한다.
③ R은 T에게 key를 전송한다.
④ 만약 hash(key)와 metaID가 일치하면, T는 잠긴 상태에서 빠져 나온다.




**[그림 1]** 해쉬-락 기법

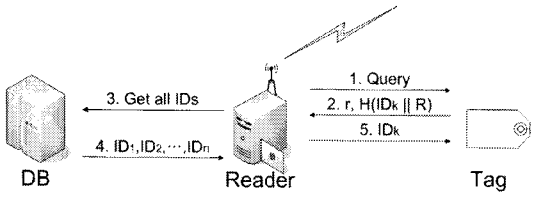
이 방법은 태그의 식별 값인 metaID가 고정되어 있어, 출력되는 데이터가 같아 해당 태그로부터 데이터가 전송되었는지 확인할 수 있게 된다. 그리고 리더기와 태그사이의 통신채널은 도청이 가능하기 때문에 악의적인 공격자는 Key를 획득한 후, 해쉬 연산하여 metaID를 산출하여 인증을 받을 수 있다. 또한 제 3자가 고정된 metaID를 재전송함으로써 인증 받을 수 있으며, metaID가 식별자

처럼 사용되기 때문에 스푸핑 공격 및 사용자 추적이 가능하다.

### 2.3.2 확장된 해쉬-락 기법

해쉬-락 기법에서 가능한 사용자 추적을 방지하기 위한 방식이다. 태그는 인가되지 않은 사용자에 의한 질의에 대하여 예상 가능한 응답을 하지 않지만, 합법적인 리더기에 의해서는 여전히 식별 가능해야 하는 방식이다. 이 기법에서는 태그에 일방향 해시 함수와 난수발생기가 구축되어 있어야 한다. 태그를 풀림 상태로 하는 프로토콜은 [그림 2]와 같다.

① 리더 R은 태그 T에게 질의를 보낸다.
② T는 랜덤 한 난수를 생성하고, hash(ID ‖ R)값을 계산한다.
③ T는 R에게 (R, hash(ID ‖ R))을 전송한다.
④ R은 모든 알려진 IDi값에 대해 hash(IDi ‖ R)을 계산한다.
⑤ 만약 hash(IDi ‖ R) = hash(ID ‖ R)을 만족하는 IDi를 찾는다면, R은 T에게 IDi를 전송한다.
⑥ 만약 IDi와 ID가 일치한다면, T는 잠긴 상태에서 빠져 나온다.

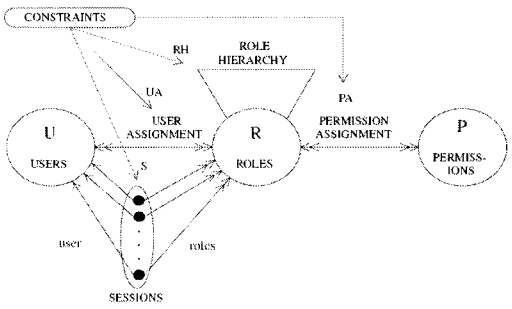



**[그림 2]** 확장된 해쉬-락 기법

이 방식은 난수를 이용하여 태그에서 리더로 가는 정보가 매 세션마다 바뀌므로 스푸핑 공격에는 강하지만 IDk 값이 노출되어 위치 추적이 가능하며 리더의 공격자가 r,H(IDk ‖ r)을 도청하여 재전송 할 경우 정당한 태그로 가장하여 재전송 공격에도 취약하다.

## 2.4 역할기반 접근제어

RBAC(Role-base Access Control)[6,7]은 접근제어 관리 작업을 단순화하고 역할기반 접근제어를 제공하기 위해 Ravi S. 등에 의해 제안 되었다. RBAC의 핵심은 권한과 역할을 연관시키고 사용자들이 적절한 역할을 할당받도록 하는 것이다. RBAC 정책에서 관리자는 접근제어를 통해 권한이 없는 사용자가 불법적으로 중요 정보의 변조를 방지하는 무결성을 제공 한다. 또한 기밀 정보가 권한이 없는 사용자에게 유출되는 것을 막는 기밀성, 그리고 권한을 부여받은 사용자가 정보를 사용할 수 있도록 보장하는 가용성을 제공할 수 있다. 접근을 통제하기 위해 역할을 사용하는 것은 특성에 맞는 보안 정책을 시행하고 개발하며 보안 관리를 능률화 하는데 효율적인 기법이 된다.




**[그림 3]** RBAC 모델

RBAC96 이라고 불리는 기본적인 RBAC모델은 Sandhu에 의해 정의 되었으며 [그림 3]과 같다.

핵심 RBAC은 사용자(USERS), 역할(ROLELS), 객체(OBS), 조작(OPS)과 허가(PRMS)의 다섯 가지 기본 데이터 요소로 구성되며 추가로 세션(SESSIONS)을 포함하고 있다.[8,9,10]

# 3. 제안 프로토콜

## 3.1 구조

기존 제안 방식의 안전성과 보안성을 강화 하여 R1 프로토콜을 그리고 리더에 수신되는 많은 태그 데이터양으로 불안전한 통신이 이루어짐으로 수신율 저하의 문제점을 해소하기 위해 기존 제안 방식에 전송데이터 양을 감소시킨 R2 프로토콜을 제안한다. RBAC에 바탕으로 그룹별로 구성된 리더를 DB에서 정의해주며 모든 리더에게 태그의 데이터가 모두 전송되지 않고 리더의 권한 내의 태그 데이터를 읽을 수 있도록 구성 되어있다. R1 리더가 처음 태그에게 질의를 할 때 난수와 실시간을 함께 전송하고, 태그는 리더로부터 수신한 난수와 실시간을 자신이 가지고 있는 ID 및 실시간으로 해쉬한 값을 이용하여 RBAC 권한모델에[11,12] 알맞은 내용만 선별 응답하게 된다.

리더는 난수 및 실시간 데이터를 송신해 주는 것 외에는 연산이 필요하지 않으며, 태그와 백-엔드 데이터베이스 사이에서 전송되는 정보를 저장하기 위한 임시메모리만이 요구된다.

제안 R1 프로토콜에서 사용되는 파라미터는 다음과 같으며, [그림 4]는 제안하는 R1 프로토콜, [그림 5]는 제안하는 R2 프로토콜의 기본 구조를 나타낸 것이다.

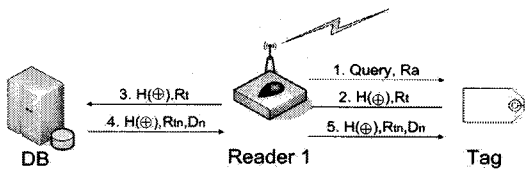
### 3.1.1 가정 사항

본 제안 프로토콜을 제안하기 위하여 다음 사항을 가정한다.

- 태그는 능동형으로 내장된 배터리로 동작한다.
- 태그와 데이터베이스는 해쉬 함수 연산을 수행한다.
- 태그와 데이터베이스는 태그의 ID를 사전에 공유한다.
- 리더기는 난수 생성기능을 갖고 있다.
- 백-엔드 데이터베이스와 리더는 안전한 통신채널로 통신을 하고 있다.
- 태그는 GID-96 코트체계이다
- ID1은 헤더, 업체코드, 오브젝트 클래스, 일련번호
- ID2는 헤더, 일련번호

[파라미터]

- Query : 태그의 응답을 요청
- ID1 : 태그 고유의 전체비밀 인증 정보
- ID2 : 태그 고유의 간소비밀 인증 정보
- H( ) : 일 방향 해쉬 함수
- Rt : 리더가 태그에게 전송하는 DB시간($\mu s$)
- Rr : 리더가 태그에게 전송하는 난수
- Tt : 태그에 저장되어 있는 시간($\mu s$)
- Ra : 상위 권한 리더신호
- H(⊕) : $H(ID1 \oplus R_r \oplus T_t \oplus key)$ 연산
  - Rtn : 태그에 기록될 시간($\mu s$)
- Dn : 데이터베이스에서 태그로 전송되는 명령
- ⊕ : Exclusive OR
- key : DB, 리더, 태그의 공통 비밀키




**[그림 4]** 제안 R1 프로토콜의 구조

## 3.2 R1 인증과정

◎ 1단계 : 리더는 태그들에게 Query, Ra 를 브로드캐스팅 한다.

리더 → 태그 : Query, Ra

◎ 2단계 : 태그는 리더의 등급을 확인 후 ID와 자신이 가지고 있던 $T_t$를 $R_r$와 XOR연산 후 해쉬하여, $R_t$,와 함께 Query에 대한 응답으로 리더에게 전송한다.

태그 → 리더 : $H(\oplus), R_t$

◎ 3단계 : 리더는 $R_r$와 $H(\oplus), R_t$ 를 백-엔드 데이터베이스로 전송한다.

리더 → 백-엔드 데이터베이스 : $H(\oplus), R_t$

◎ 4단계 : 백-엔드 데이터베이스에 저장된 ID를 $R_t, R_r$,key와 해쉬한 값과 리더로부터 수신한 $H(\oplus), R_t$ 를 비교하여 태그를 인증한다.

백-엔드 데이터베이스 → 리더 :

계산된 $H(\oplus), R_t$ =

수신한 $H(\oplus), R_t$

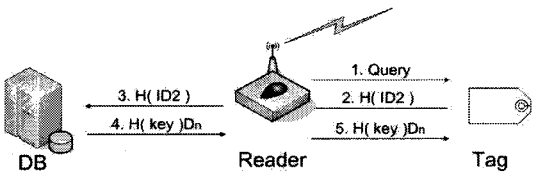
인증이 성공하면 $H(\oplus), R_{tn}, D_n$를 리더에게 전송한다.

◎ 5단계 : 리더는 백-엔드 데이터베이스로부터 수신한 $H(\oplus), R_{tn}, D_n$를 태그에게 전송한다.

리더 → 태그 : $H(\oplus), R_{tn}, D_n$

태그는 백-엔드 데이터베이스의 신호에 인증하고 Rtn을 기록하며 DB 명령에 따라 KILL Command 등 Dn명령을 수행하여 태그동작을 종료하며, 인증 세션을 성공적으로 종료 한다.

## 3.3 R2 인증과정




**[그림 5]** 제안 R2 프로토콜의 구조

◎ 1단계 : 리더는 태그들에게 Query를 브로드캐스팅 한다.

리더 → 태그 : Query

◎ 2단계 : 태그는 리더의 R2 등급을 확인 후 ID2를 해쉬 하여 Query에 대한 응답으로 리더에게 전송한다.

태그 → 리더 : $H(ID2)$

◎ 3단계 : 리더는 $H(ID2)$를 백-엔드 데이터베이스로 전송한다.

리더 → 백-엔드 데이터베이스 : $H(ID2)$

◎ 4단계 : 백-엔드 데이터베이스에 저장된 ID를 해쉬한 값과 리더로부터 수신한 $H(ID2)$를 확인하여 태그에 Dn을 전송 한다.

## 4. 제안 프로토콜의 성능

### 4.1 스푸핑 공격에 대한 안전성

R1의 경우 공격자가 정당한 리더로 가장하여 Query와 함께 태그에게 난수 Rr및 실시간 Rt를 전송한다면, 태그로 부터 $H(\oplus), R_t$ 를 획득할 수 있다. 그러나 이 정보를 악의적인 태그에 넣어 리더에 대한 응답으로 보내지게 되면 이미 시간이 지나간 상태의 정보를 백-엔드 데이터베이스에 $H(\oplus), R_t$ 를 전송해야 하기 때문에 인증을 할 수가 없어 스푸핑 공격이 불가능 하게 된다. 그리고 R2의 경우 공격자가 정당한 리더로 가장하여 Query를 전송하여 태그의 식별 값인 ID2가 고정되어 있으며 출력되는 데이터가 같아 전송되었는지 확인할 수 있다. 그러나 전체 데이터가 아닌 헤더와 일련번호만 전송되므로 공격자가 획득해도 사용하지 못하는 불필요한 데이터가 된다.

### 4.2 재전송 공격에 대한 안전성

R1의 경우 정당한 리더가 Query와 함께 전송하는 Rt, Rr는 매 세션마다 변하기 때문에 태그의 응답 $H(\oplus), R_t$ 도 매 세션마다 바뀌게 된다. 그러므로 공격자는 도청으로 획득한 $H(\oplus), R_t$ 를 다음 세션에서는 응답으로 사용할 수 없으므로 재전송 공격에 안전하다. 또한 프로토콜에서 공격자는 태그의 ID를 난수 및 실시간과 해쉬 하기 때문에 알 수 없으므로 매 세션마다 변하는 Rt, Rr에 대하여 정당한 응답 $H(\oplus), R_t$ 을 생성하는 것은 원천적으로 불가능하다.

R2의 경우 공격자가 도청으로 획득한 데이터를 다음 세션에서 사용하게 되면 같은 일련변호가 전송되기 때문에 이에 R1이 동작하여 인증하므로 중복된 일련번호의 태그를 찾아 낼 수 있으므로 재전송공격에 안전하다.

### 4.3 트래픽 분석과 위치 추적에 대한 안전성

R1의 경우 공격자가 정당한 리더로 가장하여 지속적으로 고정된 Rt, Rr를 태그에게 전송하여도 다음 세션에서는 실시간이 바뀐다. 태그는 난수, Tt를 공격자는 알 수 없는 해쉬된 ID를 이용하여 매 세션마다 변하는 응답 $H(\oplus), R_t$ 를 전송하므로 공격자는 서로 다른 응답이 동일한 태그에 의한 것인지를 판별할 수 없다. 그러므로 정당한 리더로 가장한 공격자는 트래픽 분석이 불가능하고 태그의 위치도 추적할 방법이 없게 된다. 그러나 R2의 경우 정당한 리더로 가장한 공격자는 트래픽 분석과 위치 추적을 할 수 있는 단점이 있다.

### 4.4 정보전송 방해에 대한 안전성

R1의 경우 제안 프로토콜은 상호 인증을 제공하므로 정보전송 방해 공격을 탐지할 수 있으며, 태그의 인증 정보 ID는 변하지 않기 때문에 DB의 정보유실은 일어나지 않게 된다.

R2의 경우 정보 전송에 대한 방해 공격에 취약 하다. [표 2]는 기존 프로토콜과의 안전성 비교표이다.

[표 2] 제안프로토콜의 안전성

| | 해쉬락 기법 | 확장된 해쉬락 기법 | 제안 기법 R1 | 제안 기법 R2 |
|---|---|---|---|---|
| 스푸핑 공격 | 취약 | 취약 | 안전 | 안전 |
| 재전송 공격 | 취약 | 취약 | 안전 | 안전 |
| 트래픽 분석 공격 | 취약 | 취약 | 안전 | 취약 |
| 위치정보 노출 | 취약 | 취약 | 안전 | 취약 |
| 정보전송 방해공격 | 안전 | 안전 | 안전 | 취약 |

### 4.5 제안 프로토콜의 효율성

본 논문은 제안한 R1 프로토콜에서 태그는 해쉬 함수 연산 데이터를 저장만 하므로 앞으로의 기술 발전으로 저가 태그 및 모든 태그에서 구현 가능할 것이다. 또한 [표 3]과 같이 인증 세션 동안 1회의 해쉬 함수 연산만을 수행하므로 연산 부담도 크지 않다. 본 R1 기법은 난수 및 실시간만 적용하고 다른 복잡한 연산은 하지 않으며 또한 DB의 연산이 적어 주변에 수많은 태그가 있어도 저가의 DB로도 구성이 가능하기 때문에 효율성 면에서도 우수하다고 할 수 있다. 또한 R2 기법은 태그의 연산이 해쉬 1회로 최소한의 보안을 적용하고 있으며 중복코드 등을 제외하기 때문에 태그가 전송하는 데이터양이 적어 리더의 수신율 향상을 기대 할 수 있다. 따라서 불필요한

데이터가 DB에 저장되지 않아 저장 공간 절약과 전체 시스템의 성능 향상을 가지고 올 수 있다.

[표 3] 제안프로토콜의 효율성

| | 해쉬락 기법 | 확장된 해쉬락 기법 | 제안 기법 R1 | 제안 기법 R2 |
|---|---|---|---|---|
| 인증 | 양방향 | 양방향 | 양방향 | - |
| 태그 연산량 | 해쉬1회 | 해쉬1회 난수 1회 | 해쉬1회 (시간쓰기) | 해쉬1회 |
| 리더 연산량 | - | n회 | 난수1회 | - |
| 데이터베이스 연산량 | - | - | 비교1회 | - |

## 5. 결론

RFID기술의 특성에 기초하여 여러 보안 측면에서 취약성을 분석하고, 취약점을 해결하기 위한 방안을 기존 해쉬-락 연구의 바탕으로 제시 하였다. 이를 위해 기존 태그코드를 분석 하였으며 보안 측면에서 알려진 위협에 대응하기 위해 두 가지의 방법으로 인증 할 수 있도록 했다. 첫째로 인증 방법의 복잡성을 높인 대신 보안능력을 향상시킨 R1 방식 모델이고 둘째가 보안 능력은 떨어지나 프라이버시를 최소한 지켜주며 원활한 통신을 위해 태그에서 불필요 EPC 신호의 송신을 제한하는 R2 방식이다. 제안한 R1 프로토콜은 태그가 리더로부터 수신한 난수 및 실시간으로 부터 새로운 해쉬 함수를 생성하여 매 세션마다 다른 응답을 전송할 수 있도록 함으로써 공격자의 각종공격에 안전한 프로토콜로써 안전성과 효율성이 우수하다. R2 프로토콜은 리더의 Query 신호가 R1와 다른 신호를 보내줌으로써 공격자가 취득 및 조합해도 쓸모가 없도록 불필요 태그 데이터의 송신을 하지 않는다. 이로써 통신 안정성 및 전체 시스템의 효율을 향상시킨 방법으로 추후 지속적인 연구로 RFID 시스템의 성능을 향상시킬 수 있는 방식이다.

## 참고문헌


[1] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. w. Engels, "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems," Security in Pervasive Computing 2003, LNCS 2802, pp. 201-202, Springer-Verlag Heidelderg, 2004.

[2] S. A. Weis, "Security and Privacy in Radio-Frequency Identification Devices" MS Thesis, MIT.May, 2003.

[3] S. E. Sarma, S. A. Weis, D. W. Engels. "RFID systems, Security & Privacy Implications", White Paper MIT-AUTOID-WH-014, MIT AUTO-ID CENTER, 2002.

[4] Sanjay E.Sarma, Stephen A. Weis and Daiel W.Engels, "Radio-Frequency Identification Systems", In Proceeding of CHES '02, pp. 454-469. Springer-Verlag, 2002. LNCS NO.2523.

[5] Weis, S. et al. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, First International Conference on Security in Pervasive Computing (SPC), 2003.

[6] R. Laborde, B. Nasser, F. Grasset, F. Barr`ere, A. Benzekri, "A Formal Approach for the Evaluation of Network Security Mechanisms Based on RBAC Policies" Electronic Notes in Theoretical Computer Science 121 2005, pp. 117-142

[7] Andrea Omicini Alessandro Ricci Mirko Viroli, "RBAC for Organisation and Security in an Agent Coordination Infrastructure" Electronic Notes in Theoretical Computer Science 128, 2005, pp. 65-85

[8] XinyuWANG, Member, Jianling SUN, Xiaohu YANG, Chao HUANG,and Di WU "Security Violation Detection for RBAC Based Interoperation in Distributed Environment" IEICE TRANS. INF. & SYST., VOL.E91-D, NO.5 MAY 2008, pp. 1447-1456

[9] Jacques Wainer, Akhil Kumar, Paulo Barthelmess "DW-RBAC: A formal security model of delegation and revocation in workflow systems" Information Systems 32, 2007, pp. 365-384

[10] Celia Li, Cungang Yang, Richard Cheung, "Key management for role hierarchy in distributed systems" Journal of Network and Computer Applications 30, 2007, pp. 920-936

[11] Chiara Braghin, Daniele Gorla and Vladimiro Sassone, "Role-based access control for a distributed calculus Chiara Braghin" Journal of Computer Security 14, 2006, pp. 113-155

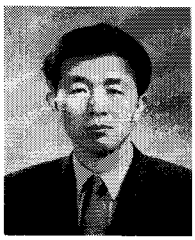
[12] Wei She and Bhavani Thuraisingham, "Security for Enterprise Resource Planning Systems" Information Systems Security, 2007, pp. 152-163

## 배 우 식(Woo-Sik Bae) [정회원]

- 1997년 3월 ~ 현재 : 아주자동차대학 전산소
- 2006년 8월 : 백석대학교 정보기술대학원(공학석사)
- 2007년 3월 : 충북대학교 컴퓨터교육과(박사과정)

<관심분야>
RFID DB보안, 네트워크, 암호 프로토콜/알로리즘, 유통물류

## 이 종 연(Jong Yun Lee) [정회원]



- 1985년 2월 : 충북대학교 전자계산기공학과(공학사)
- 1987년 2월 : 충북대학교 대학원 전자계산기공학과(공학석사)
- 1999년 2월 : 충북대학교 대학원 전자계산학과(이학박사)
- 1989년 : 비트컴퓨터(주) 개발부
- 1990년 ~ 1994년 : 현대전자산업(주) 소프트웨어연구소 주임연구원.
- 1994년 ~ 1996년 : 현대정보기술(주) CIM사업부 책임연구원
- 1999년 ~ 2003년 : 삼척대학교 정보통신공학과 조교수
- 2003년 ~ 현재 : 충북대학교 컴퓨터교육과 부교수
- 2003년 ~ 2005년 : 한국정보처리학회 논문지 편집위원(데이타베이스분과) 역임
- 2004년 ~ 2004년 : Information Journal 편집위원
- 2006년 : 한국정보처리학회 이사역임
- 2004년 ~ 2007년 : 한국멀티미이어학회 이사
- 2007년 ~ 현재 : 한국산학기술학회 상임이사
- 2001년 ~ 현재: IEEE Member

<관심분야>
질의 처리 및 최적화, 시공간 데이터베이스, u-learnimg 및 평가모델, RFID/e-Seal 보안, 유통물류, GIS