해시함수 기반의 새로운 저비용 RFID 상호인증 프로토콜

배우식† · 이종연†† · 김상춘†††

요 약

최근 들어 RFID 시스템은 바코드를 대체하여 유통 물류, 제조 산업 등 산업전반에 활용되기 시작하였다. 하지만 리더와 태그 간의 통신이 무선구간으로 보안상 취약한 부분이 있어 이 분야의 인증 프로토콜에 대한 연구가 활발히 진행 중이다. 따라서 본 논문에서는 기존 제안된 프로토콜들의 취약성을 보안하여 데이터베이스의 마이크로타임을 전송하는 방식으로, 태그를 인증하기위해 RFID 시스템에서 요구되는 보안 사항을 만족시키며 난수 발생 등 연산량을 최소화 시킬 수 있는 인증프로토콜을 제안한다. 아울러 제안하는 상호 인증 방식은 재전송 공격, 스푸핑 공격, 트래픽 분석, 도청 공격 등에 대해 안전하여 RFID 시스템에 적용 시 태그의 제작비 절감 및 보안성이 우수한 장점이 있다.

주제어 : RFID 보안, 인증 프로토콜, 해시 함수, 마이크로 타임 분할

A New Low-Cost Mutual Authentication Protocol in RFID based on Hash Function

Woo Sik Bae† · Jong Yun Lee†† · Sang Choon Kim†††

ABSTRACT

Recently RFID systems have been introduced in place of barcode systems to industries such as logistics, distribution, and manufacturing. Due to security vulnerabilities in wireless communication between the reader and tags, however, the authentication protocols for the communication have also been researched extensively. In order to solve the vulnerability of previously proposed protocols, this paper thus proposes an authentication protocol that satisfies the security requirements in the RFID system and minimizes the quantity of computation such as random number generation, transmitting the micro time of databases. In addition, it is expected that the proposed cross authentication protocol is safe against replay attack, spoofing attack, traffic analysis, and eavesdropping attack when it is applied to the RFID system. Also, it has advantages such as providing a high level of security at a lower manufacturing cost.

Keywords : RFID security, authentication protocol, hash function, micro time division

† 정 회 원: 충북대학교 컴퓨터교육과 박사과정
†† 종신회원: 충북대학교 컴퓨터교육과 교수 (교신저자)
††† 정 회 원: 강원대학교 공학대학 정보통신공학과 교수
논문접수: 2010년 11월 04일, 심사완료: 2011년 01월 20일

1. 서 론

RFID(Radio Frequency Identification)는 현재 산업 전반에 사용 하고 있는 바코드를 대체하여 전자 태그를 사물에 부착하고, 사물이 주위 상황을 인지하여 기존 IT 시스템과 실시간으로 정보를 교환, 처리할 수 있는 기술이다[1][2]. 이 기술은 앞으로의 유비쿼터스 시대에 사용의 편리성 향상으로 개인 및 산업 전반에 활용이 예상되며 국내·외적으로 많은 연구가 진행되고 있다. 일반적인 RFID 시스템은 태그(Tag), 리더(Reader) 및 데이터베이스의 3가지 요소로 구성된다. 이러한 RFID 시스템은 현재 교통카드, 출입구보안, 재고관리, 물류관리, 동·식물관리, 자재관리등 실생활 및 산업 전반에 응용 및 확산되고 있는 추세이다.

1.1 연구 배경 및 필요성

하지만 RFID 시스템은 태그의 마이크로칩에 내장된 정보를 리더가 무선주파수를 이용하여 읽어내기 때문에 도청, 트래픽 분석, 서비스거부 공격, 메시지유실, 트래킹 공격, 스푸핑 공격 등 무선 네트워크상의 많은 취약점들을 지니고 있어서 보안이나 프라이버시 보호문제에 심각한 문제를 야기할 수 있다[3][4][5]. 따라서 RFID 시스템이 활성화되기 위해서는 리더와 태그 사이의 안전한 상호인증이 매우 중요하다[6][7].

아울러 기존 제안된 프로토콜들을 보면 해시-락기법[8][9][10]은 공격자가 리더와 태그간의 통신을 도청하여 metaID를 얻는 것이 가능하고 metaID가 동일하여 공격자가 트래킹이 가능한 문제점이 있다. 확장된 해시-락기법[11][12]은 태그가 난수를 생성하여 매 세션마다 다른 응답을 리더에게 전송하는 방법인데 이 방법도 재전송 공격과 스푸핑 공격에 취약한 문제점이 있다. 해시 체인기법[13]의 문제는 도청공격과 스푸핑 공격에 취약하며 데이터베이스가 태그를 인증하기 위한 연산량이 과다하다는 단점이 있다. 해시기반 ID 변형기법[14][15]은 스푸핑 공격이 가능하고 데이터베이스가 많은 연산을 수행해야 하는 어려움이 있다. 최근 제안된 Kim-Ryoo[16]는 태그의 해시 연산 4회, XOR 연산 3회의 많은 연산을 하는 프로토콜을 제안하였으나 여전히 스푸핑 공격에 취약하여 보안성과 효율성이 떨어진다. 또한 Park 외 4명[17]이 제안한 대칭키 기반의 인증 프로토콜은 태그에서 AES 암호화 2회, 해시 함수 연산1회, 랜덤 넘버 2회의 많은 연산이 필요하며 통신 라운드 수가 10회로 복잡하여 상대적으로 데이터베이스에서의 연산이 적어 실효성이 부족하다.

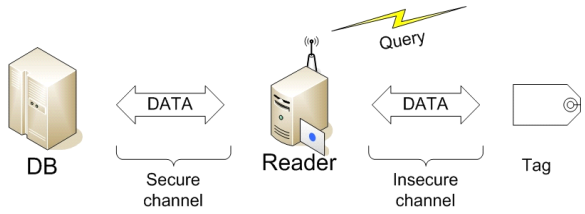
1.2 학문적 기여

따라서 본 논문에서는 RFID의 보안 문제를 해결하기 위해 난수 및 마이크로 타임을 분할하여 암호화 하는 방법으로 한 새로운 인증 프로토콜의 제안을 연구목표로 한다. 기존에 제안된 해시 관련 인증 프로토콜들에 비해 복잡한 연산을 하지 않고 데이터베이스 시간을 이용하여 해시함으로써 보안성을 강화하고 비용을 줄여 효율적으로 RFID 시스템을 보호할 수 있는 인증 프로토콜을 제안한다. 아울러 그 세부적인 연구내용은 다음과 같다. 첫째, 기존의 해시 관련 제안 프로토콜을 알아보고 문제점을 확인한다. 둘째, 제안 프로토콜을 검토하고 세부 동작과정을 단계별로 요약한다. 셋째, 안전성 및 효율성을 분석하여 기존 프로토콜대비 제안하는 프로토콜의 우수함을 입증한다. 끝으로 본 논문의 연구결과는 태그가 소형인 점을 감안하여 최소한의 연산으로 보안성이 높은 인증 프로토콜임을 알 수 있다.

본 논문의 구성은 다음과 같다. 2절 에서는 관련 연구에 대해 기술하고, 3절에서는 제안 프로토콜과 안전성에 대해 설명한다. 4절에서는 제안 프로토콜의 효율성을 검증한다. 마지막으로 5절에서 결론과 향후 관련연구 방향에 대해 제시한다.

2. 관련 연구

RFID 시스템은 크게 DB, 리더, 태그의 세부분으로 구성되며 <그림 1>은 일반적인 RFID 인증 프로토콜 모델 이다. DB와 리더구간의 통신은 통상 안전한 유선방식이며 리더와 태그 구간은 무선 구간으로 구성되어 있다.

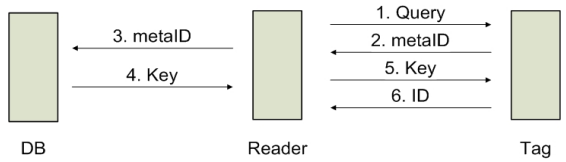


<그림 1> RFID 인증 프로토콜 모델

아울러 기존의 RFID 인증 프로토콜에는 해시-락 기법[8][9][10], 확장된 해시-락 기법[11][12], 해시 체인 기법[13], 해시 기반 ID 변형기법[14][15], Kim-Ryoo의 상호인증 프로토콜[16], Park 외 4명의 대칭키 기반의 인증프로토콜[17]등의 다수 연구가 있다. 다음은 이의 주요 프로토콜에 대해 간략히 알아보도록 한다.

2.1 해시-락 기법

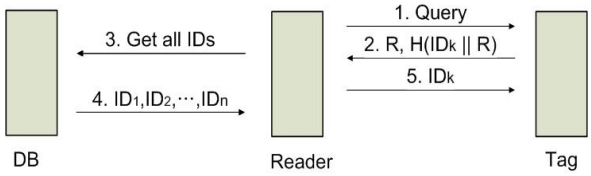
해시-락 프로토콜은[8][9][10] 낮은 태그 가격을 고려하여 MIT에 의해 제시된 방식으로 <그림 2>와 같이 Key를 태그, 데이터베이스와 사전에 안전하게 공유되어 있다고 가정하며 한번의 해시 함수로 인증하기 때문에 저가로 구현된다. locked 상태에서는 태그가 자신의 실제 ID 값이 아닌 metaID 값을 전송하고, unlocked 상태에서만 실제 ID를 전송함으로써 프라이버시를 보호하는 방법이다. 이 방법은 태그의 식별 값인 metaID가 고정되어 있어, 출력되는 데이터가 같아 해당 태그로부터 데이터가 전송 되었는지 확인할 수 있게 된다. 그리고 리더기와 태그사이의 통신채널은 도청이 가능하기 때문에 악의적인 공격자는 키(Key)를 획득한 후, 해시 연산하고 metaID를 산출하여 인증을 받을 수 있다. 또한 제 3자가 고정된 metaID를 재전송함으로써 인증 받을 수 있으며, metaID가 식별자처럼 사용되기 때문에 스푸핑 공격 및 사용자 추적이 가능하다.



<그림 2> 해시-락 기법

2.2 확장된 해시-락 기법

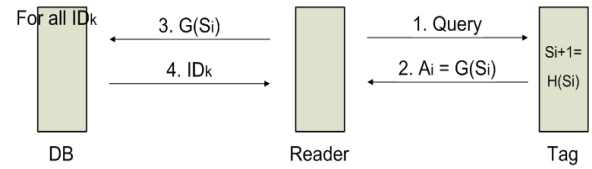
Hash Lock 기법에서 가능한 사용자 추적을 방지하기 위해 개선한 방식이다[11][12]. 태그는 인가되지 않은 사용자에 의한 질의에 대하여 예상 가능한 응답을 하지 않지만, 합법적인 리더기에 의해서는 여전히 식별 가능해야 하는 방식이다. <그림 3>과 같이 이 기법에서는 태그에 단방향 해시 함수와 난수발생기가 구축되어 있어야 한다. 이 방식은 난수를 이용하여 태그에서 리더로 가는 정보가 매 세션마다 바뀌므로 스푸핑 공격에는 강하지만 IDk 값이 노출되어 위치 추적이 가능하며 리더의 공격자가 R,H(IDk || R)을 도청하여 정당한 태그로 가장하여 재전송할 경우 공격에 취약하다.



<그림 3> 확장된 해시-락 기법

2.3 해시 체인 기법

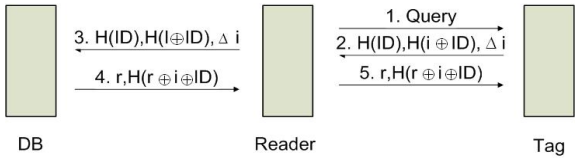
해시 체인 방식은 해시 함수 두 개를 이용하여 리더의 Query에 대해 태그는 매 세션마다 서로 다른 응답을 전송하며 이를 이용한 인증 방식이다[13]. 서로 다른 두개의 해시 함수를 사용하는 해시 체인 기법은 리더의 세션마다 다른 Ai 값을 전송하여 인증하므로 위치트래킹 공격에 안전하다. 하지만 최악의 경우 데이터베이스에서는 모든 Si에 대하여 H와 G를 i번 수행해야 한다. 또한 잘못된 응답이 수신되었을 경우, 데이터베이스는 고유한 모든 ID에 대해 ∞번의 해시를 수행할 가능성이 있는 단점이 있으며 <그림 4>는 해시 체인 기법의 동작 과정 이다.



<그림 4> 해시 체인 기법

2.4 해시 기반 ID변형기법

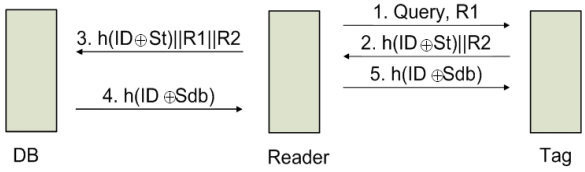
해시 기반 ID 변형기법은[14][15] 해시 체인 기법과 유사하게 태그의 인증정보인 ID를 매 세션마다 바꾸는 기법이다. <그림 5>와 같이 매 세션마다 태그의 ID가 난수 R에 의해 갱신되므로 재전송 공격으로부터 안전하다. 그러나 공격자가 정당한 리더로 가장해 태그로부터 전송하는 H(ID), H(i⊕D), Δi를 획득하는 경우 정당한 리더와 태그가 다음 인증세션을 수행하기 전에 이 정보들을 리더의 질의에 대한 응답으로 이용하면 공격자는 정당한 태그로 인정받아 스푸핑 공격이 가능하다. 정당한 태그는 프로토콜 마지막 과정에서 메시지를 받지 못하는 경우 정보가 유실되었다고 판단하여 기존의 태그의 ID를 갱신하지 않기 때문이다.



<그림 5> 해시 기반 ID 변형 기법

2.5 Kim-Ryoo의 상호 인증 프로토콜

본 상호 인증 프로토콜은[16] <그림 6>과 같이 리더가 태그를 인증하기 위해 난수 R1을 생성하여 태그에게 전송후 태그는 리더를 인증하기 위해 난수 R2를 생성하여 R1, R2를 이용하여 St를 계산하고 R2와 함께 리더에 전송한다. 리더는 수신한 h(ID ⊕ Rt)|| R2 데이터에 R1을 연접하여 데이터베이스에게 전송한다. 데이터베이스는 수신한 h(R1 ⊕ R2)와 비교하여 일치하면 리더가 인증된다. 그리고 데이터베이스는 R2를 이용하여 Sdb를 계산후 리더가 데이터베이스를 인증하기 위한 h(ID ⊕ Sdb)메시지를 리더에게 전송한다. 리더는 수신한 h(ID ⊕ Sdb)를 태그에게 전송하고 태그는 h(ID ⊕ Sdb)데이터를 수신하면 자신이 저장하고 있는 R2와 자신의 ID를 이용하여 h(ID ⊕ Sdb)를 계산한다. 수신된 h(ID ⊕ Sdb) 값과 계산된 h(ID ⊕ Sdb) 값이 일치하면 데이터베이스가 인증되는 방법으로 태그에 해시 4회, XOR 3회등 복잡 하고 많은 계산을 요구한다. 그리고 문제점으로 태그가 리더에게 전송한 난수 R2와 리더가 태그에게 전송한 h(ID ⊕ Sdb)을 도청 하였을 경우 공격자에 의해 스푸핑 공격이 취약한 단점이 있다.



<그림 6> Kim-Ryoo의 상호 인증 프로토콜

2.6 Park 외 4명의 상호 인증 프로토콜

본 상호 인증 프로토콜은[17] 데이터베이스의 연산량보다 태그의 연산이 많은 AES-128 및 해시 함수 SHA-1 기반의 상호 인증 프로토콜로서 태그와 리더간의 상호 인증은 제공하지만 리더와 데이터베이스 간의 상호 인증이 완전하지 않은 단점이 있다. 아울러 통신 라운드 수가 10회 및 태그에 다양한 연산이 집중되어 있어 태그 제작 시 많은 비용이 필요하며 높은 계산능력과 저장 공간이 필요한 비효율적인 방식이다.

3. 제안하는 인증 프로토콜

3.1 구조

본 제안 프로토콜의 리더는 카운트를 갖고 있으며, 리더가 처음 태그에게 질의를 할 때 Rr를 함께 전송한다. 태그는 리더로부터 수신한 Rr를 저장 공간에 저장 후 자신이 가지고 있는 IDt로 해시한 값과 Rdbt를 이용하여 매 세션마다 다르게 응답함으로써 기존 프로토콜들에서 문제점으로 지적되었던 각종 공격에 대하여 안전하다. 제안 프로토콜에서 데이터베이스는 태그의 ID와 관련 데이터를 저장하고 있으며, 태그에서는 해시 함수 1회, 비교연산 1회, 난수발생 1회, XOR 1회의 연산만을 이용하여 데이터베이스와 태그를 상호 인증한다. 리더는 난수 데이터를 생성 후 송신해 주는 것 외에는 연산이 필요하지 않다.

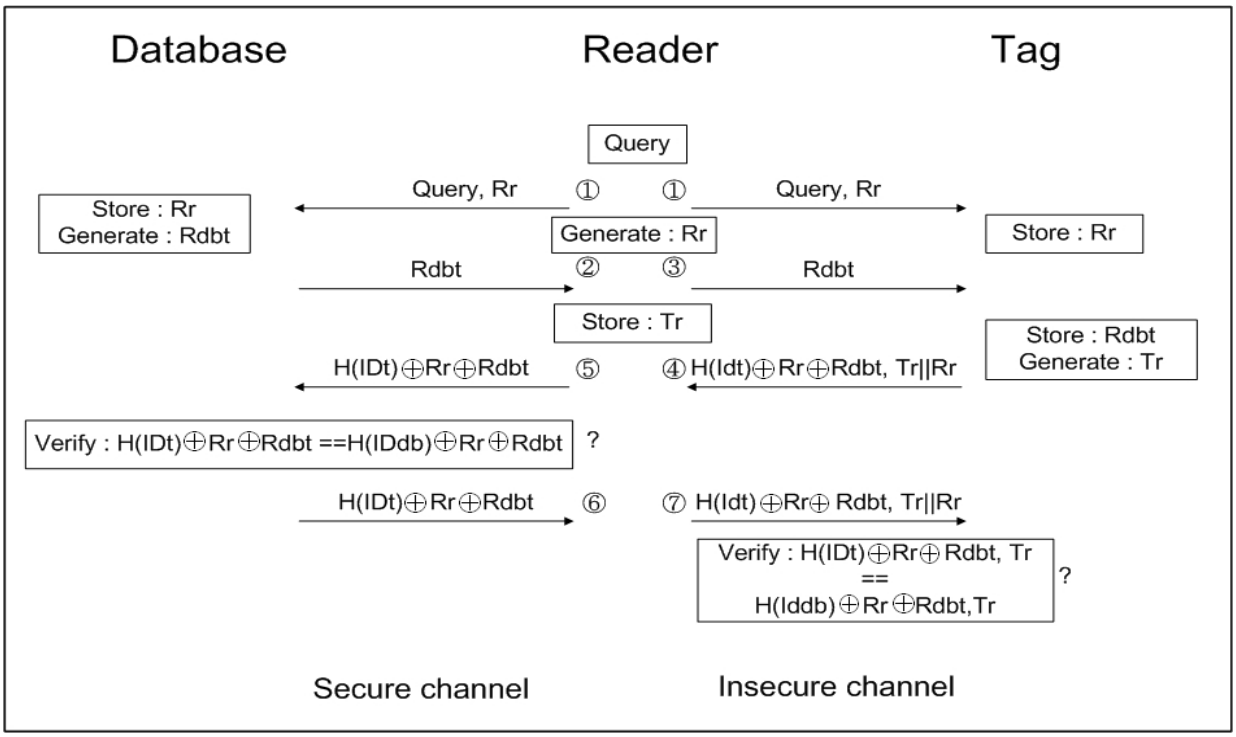
제안 하는 RFID 상호 인증 프로토콜의 전체적인 구성과 동작은 <그림 7>과 같다. 아울러 <그림 7>에서 사용할 기호 정의는 <표 1>과 같으며 <가정 1>은 다음과 같다.

<표1> 기호정의

기호	설명
'Query'	리더의 질의
IDt	태그 고유의 비밀 인증 정보
H(x)	x의 보안 해시 함수(SHA-1)
Rdbt	데이터베이스의 현재시간(μs)
Rr	리더가 생성한 난수
Tr	태그가 생성한 난수
||	연접(Concatenation operation)
→	전송방향

<가정 1> 제안 프로토콜의 가정
- 태그는 수동형이다.
- 태그와 데이터베이스는 해시 함수 연산을 수행한다.
- 데이터베이스는 태그의 IDt를 사전에 공유한다.
- 리더는 난수 생성기능을 갖고 있다.

본 논문에서 제안하는 전반적인 인증 과정은 다음과 같다. 리더는 태그를 인증하기 위해 난수 Rr를 생성하여 'Query'와 함께 데이터베이스와 태그로 전송한다. 태그는 'Query'를 수신한 후 저장 공간에 Rr를 저장한다. 데이터베이스는 리더의 'Query'를 수신한 후 데이터베이스의 Rdbt를 리더에게 전송하고 리더는 태그에게 Rdbt를 전송한다. 태그는 Rdbt를 수신한 후 저장 공간에 저장하고 난수 Tr을 생성한 후 H(IDt)⊕Rr⊕Rdbt, Tr를 계산하여 리더에게 다시 전송한다. 리더는 태그가 보내온 H(IDt)⊕Rr⊕Rdbt, Tr중 Tr을 저장후 데이터베이스에 H(IDt)⊕Rr⊕Rdbt를 전송한다. 데이터베이스는 리더에게 전송 받은 H(IDt)⊕Rr⊕Rdbt의 내용을 데이터베이스의 ID 테이블에 저장된 태그의 IDdb를 이용하여 H(IDdb)⊕Rr⊕Rdbt을 계산한 후 태그로부터 수신한 값과 비교하고 맞는 값이라면 인증한다. 인증한 후 리더에게서 받은 H(IDt)⊕Rr⊕Rdbt을 리더에게 전송한다. 리더는 전송받은 H(IDt)⊕Rr⊕Rdbt값을 확인한 후 데이터베이스를 인증하고, 태그에게 데이터베이스에게서 전송 받은 내용 H(IDt)⊕Rr⊕Rdbt과 임시 메모리에 저장중인 Tr를 이용하여 H(IDt)⊕Rr⊕Rdbt, Tr을 전송하며 태그는 이 값을 이용하여 자신이 가지고 있는 H(IDt)⊕Rr⊕Rdbt, Tr와 확인한 후 맞으면 리더를 인증하는 방식으로써 단



<그림 7> 제안 프로토콜의 구조

계별 세부적인 인증은 다음과 같다.

◎ (단계 ①: 리더)

리더는 인식 범위 내에 태그가 존재하면 카운트 Rr를 생성하여 Query 신호를 데이터베이스와 태그에게 전송한다.

리더 → 태그 : Query, Rr

리더 → 데이터베이스 : Query, Rr

◎ (단계 ②: 데이터베이스)

태그는 Query와 Rr를 수신한 후, 추후 인증을 위해 임시 메모리에 Rr를 저장한다. 데이터베이스는 Query를 수신후 Rdbt를 리더에게 전송한다.

데이터베이스 → 리더 : Rdbt

◎ (단계 ③: 리더)

리더는 데이터베이스로부터 수신한 Rdbt를 태그에 다시 전송한다.

리더 → 태그 : Rdbt

◎ (단계 ④: 태그)

태그는 Rdbt를 수신 후 임시 메모리에 Rdbt를 저장한다. 태그는 난수 Tr를 생성하여 자신의 Idt를 해시하고 기 저장된 Rr를 이용하여 H(IDt)⊕Rr⊕Rdbt, Tr를 계산하여 리더에게 전송한다.

태그 → 리더 : H(IDt)⊕Rr⊕Rdbt, Tr

◎ (단계 ⑤: 리더)

리더는 태그로부터 수신한 H(IDt)⊕Rr⊕Rdbt, Tr중 Tr을 임시메모리에 저장후 H(IDt)⊕Rr⊕Rdbt를 데이터베이스에게 전송한다.

리더 → 데이터베이스 : H(IDt)⊕Rr⊕Rdbt

◎ (단계 ⑥: 데이터베이스)

데이터베이스는 ID 테이블에 저장된 태그의 IDdb를 이용하여 H(IDdb)⊕Rr⊕Rdbt를 계산한 후, 태그로부터 수신한 H(IDt)⊕Rr⊕Rdbt와 일치 여부를 비교한다. 만약 두 값이 일치한다면, 데이터베이스는 태그를 인증하고 상호 인증을 위해 H(IDt)⊕Rr⊕Rdbt를 리더에게 전송한다. 만일 그렇지 않다면 인증되지 않은 데이터를 데이터베이스에 저장하여 추후 동일한 태그 신호가 들어올 시 공격률을 분류하여 무시하거나 적절한 대응을 한다.

데이터베이스 → 리더 : H(IDt)⊕Rr⊕Rdbt

◎ (단계 ⑦: 리더)

리더는 데이터베이스로부터 수신한 H(IDt)⊕Rr⊕Rdbt와 임시메모리에 저장중인 Tr를 태그에게 전송한다.

리더 → 태그 : H(IDt)⊕Rr⊕Rdbt, Tr||Rr

◎ (단계 ⑧: 태그,리더)

태그는 H(IDt)⊕Rr⊕Rdbt, Tr||Rr를 수신 하고 일치 여부를 확인한다. 만약 두 값이 일치한다면, 태그는 리더를 인증하고 계속되는 과정을 수행한다. 그렇지 않다면 인증과정을 중지한다.

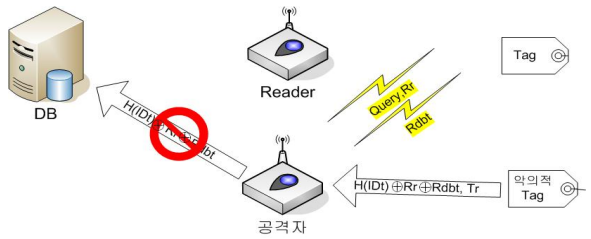
3.2 제안 프로토콜의 안전성 분석

RFID 시스템에서는 리더와 태그간의 무선구간이 존재하며 이 구간이 보안상 취약한 문제점이 있다. 무선구간의 정보를 보호하기위한 방법 및 공격 유형은 스푸핑 공격(Spoofing Attack), 재전송 공격(Replay Attack), 도청 공격(Eavesdropping Attack), 상호인증(Mutual Authentication), 트래픽 분석 공격(Traffic Analysis Attack), 서비스 거부 공격(Denial of Service Attack)등이 있는데 RFID 시스템은 이러한 보안 문제들을 고려하여 설계되어져야 한다[3][4][6][7]. 다음은 각 공격 유형에 대한 안정성 분석이다.

3.2.1 스푸핑 공격(Spoofing Attack)

제안한 프로토콜에서 공격자가 데이터베이스와 태그간에 H(IDt)⊕Rr⊕Rdbt값을 해독하여 얻을 수 있으면, 스푸핑 공격을 성공할 수 있다. 하지

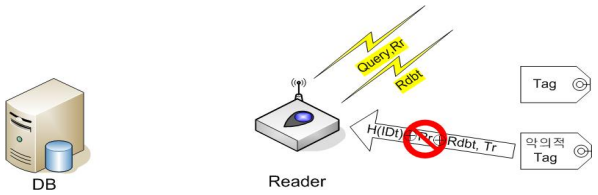
만 <그림 8> 과 같이 공격자는 데이터베이스와 태그내에 각각 안전하게 저장하고 해시한 값으로 매 세션마다 다른 값으로 전송되어지는 H(IDt)⊕Rr⊕Rdbt을 직접적으로 얻고 신속히 해독을 할 수 있는 방법이 없다. 또한 공개된 통신 채널 상으로 송수신 되는 통신 메시지 H(IDt)⊕Rr⊕Rdbt는 매 시간, 매 세션마다 새로 생성되어 사용되어지는 다른신호와 H(IDt)⊕Rr⊕Rdbt,Tr에 의해 태그정보는 보호되어져 있다. 그러므로 제안한 프로토콜은 스푸핑 공격에 안전하다.



<그림 8> 스푸핑 공격의 거부

3.2.2 재전송 공격(Replay attack)

제안한 프로토콜에서는 매 인증 세션마다 데이터베이스와 리더간 Rdbt, Rr을 생성하고, 태그와 리더간 Rdbt, Rc 그리고 태그가 새로운 난수 Tr을 생성하여 단계 ⑥에서와 같이 태그로부터 수신한 H(IDt)⊕Rr⊕Rdbt와 일치 여부를 비교한다. 만약 두 값이 일치한다면, 데이터베이스는 태그를 인증하게 된다. 그렇지 않다면 인증되지 않은 내용을 데이터베이스에 저장하여 추후 동일한 태그 신호가 들어올 시 무시하는 방법의 상호인증을 수행하기 때문에 <그림 9>와 같이 과거 태그의



<그림 9> 재전송 공격의 거부

공격자에 의해 재전송된 H(IDt)⊕Rr⊕Rdbt 값들은 태그, 리더 및 데이터베이스간의 상호인증 과정 중에 세션 진행시 Rr과 Rdbt 값이 변경 된다. 따라서 제안한 프로토콜은 재전송 공격에 안전함이 입증된다.

3.2.3 도청 공격(Eavesdropping Attack)

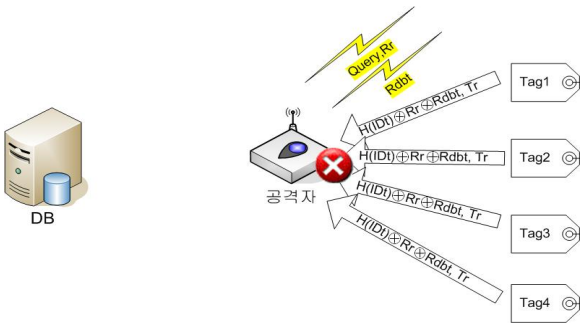
본 논문에서 제안한 프로토콜에서 공격자는 공개된 통신 채널 상으로 송수신되는 통신 메시지 Rr, Rdbt, H(IDt)⊕Rr⊕Rdbt,Tr등을 도청할 수 있다. 하지만 도청한 내용으로부터 공격자는 태그와 리더, 데이터베이스 간에 공유된 비밀키 역할을 하는 식별자인 H(IDt)⊕Rr⊕Rdbt를 얻어내어 해독할 수 있어야 한다. 그러나 보안상 안전한 해시된 H(IDt),Rr와 매 세션마다 바뀌는 Rdbt를 얻는 것은 불가능하며 만일 해독할지라도 Rr⊕Rdbt가 매 세션마다 바뀌기 때문에 공격에 필요 없는 정보가 되므로 제안한 프로토콜은 도청 공격에 안전함을 알 수 있다.

3.2.4 상호인증(Mutual Authentication)

제안한 프로토콜의 단계 ⑥에서 데이터베이스는 태그로부터 수신한 H(IDt)⊕Rr⊕Rdbt와 H(IDdb)⊕Rr⊕Rdbt 동일한지를 비교 검증한다. 태그와 데이터베이스 사이에 공유된 비밀키 역할을 하는 식별자인 H(IDt) 또는 매 세션마다 바뀌는 Rr⊕Rdbt를 모르는 공격자는 태그 또는 리더로 위장하여 공격 등을 수행할 수 없으므로 상호인증이 확인된다.

3.2.5 트래픽 분석 공격(Traffice Analysis Attack)

제안한 프로토콜에서는 Rr⊕Rdbt, Tr은 매 세션마다 변경되므로 공격자는 현재 세션에서 태그의 H(IDt)⊕Rr⊕Rdbt,Tr의 응답이 과거 세션에 도청한 응답들과 동일한지를 비교할 수 없다. 즉, <그림 10>과 같이 매 세션마다 서로 다른 Rr⊕Rdbt와 난수 Tr을 생성함으로 매 세션마다 서로 다른 두 개의 응답들이 과거의 응답들과의 비교를 통하여 동일한 태그로부터 송신된 것인지를 구별할 수 없으므로 태그의 이동경로를 트래킹할 수 없어 제안한 프로토콜은 트래픽 분석 공격 및 위치 추적 공격에 안전이 입증된다.



<그림 10>트래픽 분석 공격의 거부

3.2.6 서비스 거부 공격(Denial of Service Attack)

최근 인터넷상에 이슈화되고 있는 DoS 공격은 단계 ⑥에서와 같이 동일한 신호 또는 이상신호가 들어올시 쉽게 발견되어지며 이때 공격 룰을 분류하여 차단하거나 DB를 우회 하도록 함으로 DoS 공격을 최소화할 수 있다. 아울러 제안한 프로토콜에서 리더와 태그 간에 XOR 및 해시 함수 기반의 연산만을 이용하여 상호인증을 수행함으로 태그 측에 많은 연산량을 요구하지 않는다. 또한 매 세션마다 데이터베이스, 리더, 태그 간에 상호인증 완료 후 갱신되는 값이 없이 변경되는 시간의 경과만 있고 연산이 없기 때문에 제안한 프로토콜은 계산 량이 복잡한 타 프로토콜에 비해 서비스 거부 공격에 대한 영향이 적다.

3.3 기존 프로토콜과의 안정성 비교

제안한 프로토콜과 해시 연산 기반의 프로토콜들인 해시-락 기법[8,9,10], 확장된 해시-락[11,12], 해시 체인기법[13], 해시 기반 ID 변형기법[14][15], Kim-Ryoo의 기법[16], Park 외 4명의 기법과의[17] 안전성을 비교 및 분석 하였다. <표 2>에서 보여주는 것과 같이 해시-락 기법과 확장된 해시-락 기법은 RFID 초창기 제안된 기법으로 많은 보안 취약점들을 가진다. 해시 기반 ID 변형 기법은 상호인증 제공 및 재전송 공격 등에 안전하나 도청 공격, 스푸핑 공격, 위치정보노출 등에 취약하다. Kim-Ryoo의 기법[16]은 처음 태그가 전송한 난수 Nt와 리더가 태그에게 전송하는 h(ID⊕Sdb)를 취득했을 경우 스푸핑 공격, 재전송 공격에 취약하다. Park 외 4명의 기법[17]은 태그에 대부분의 복잡한 계산이 이루어지고 있어 DoS 공격에 문제가 되는 부분을 제외한 대부분의 공격에서 안전하나 데이터베이스와 리더간의 상호 인증이 불완전하다. 또한 과도한 계산량으로 현실성이 뒤떨어진다. 결론적으로 본 논문에서 제안한 프로토콜은 기존의 제안된 프로토콜들과 비교하여 Rr⊕Rdbt를 세션에서 사용함으로써 각종 공격에 강력한 상호인증을 제공함으로써 <표 2>와 같이 스푸핑 공격, 재전송 공격, 도청 공격, 트래픽 분석 공격, 서비스거부 공격 등에 안전함을 알 수 있다.

4. 효율성 분석

RFID 시스템에서 리더와 태그 사이의 통신이 효율적인 시스템이 되기 위해서는 전력소비, 연산량 및 저장 공간 등을 줄여 주어야 태그 제작의 비용을 절감 시킬 수 있다. 제안하는 인증 프로토콜의 효율성을 평가하기 위해 인증 과정에서 필요한 난수발생, 해시연산량, 태그의 쓰기연산, 통신라운드수를 기존 인증프로토콜과 비교하였다. <표 3>은 제안한 프로토콜과 기존 연구된 프로토콜과의 효율성을 비교 및 분석한 표이다. 기존

<표 2> 프로토콜의 안전성 비교

	해시-락 기법	확장된 해시-락 기법	해시-체인 기법	해시 기반 ID변형기법	Kim-Ryoo의 기법	Park 외 4명의 기법	제안프로토콜
스푸핑 공격	취약	취약	취약	취약	취약	안전	안전
재전송 공격	취약	취약	취약	안전	취약	안전	안전
도청공격	취약	취약	취약	취약	안전	안전	안전
상호인증	미제공	미제공	미제공	제공	제공	불안정	제공
트래픽 분석 공격	취약	안전	안전	안전	안전	안전	안전
서비스거부공격	안전	안전	안전	안전	안전	불안전	안전

<표 3> 제안프로토콜의 효율성

	해시-락 기법	확장된 해시-락 기법	해시-체인 기법	해시 기반 ID변형기법	Kim-Ryoo의 기법	Park 외 4명의 기법	제안프로토콜
태그 난수발생	-	1	-	-	1	2	1
리더 난수발생	-	-	-	1	1	1	1
태그 Hash 연산량	1	1	2	3	4	1	1
태그에서 연접	-	1	-	1	1	1	-
태그의 쓰기연산	-	-	-	-	-	필요	필요
통신라운드수	6	5	4	5	5	10	8
기타 연산	-	리더의 해시 (태그의 수/2)	-	XOR 4	XOR 3	XOR 1, AES-128 암·복호화	XOR 2

에 제안한 프로토콜과 비교하여 제안한 프로토콜은 태그의 연산량 측면에서 해시 1회, 난수생성 1회, 비교 연산 1회 등의 타 프로토콜에 비해 간단한 연산이 진행된다. 관련 연구에서 해시 기반 ID 변형기법의 경우 태그에서 해시 연산 3회, XOR 연산 4회를 실행하여 비교적 많은 연산을 한다. Kim-Ryoo의 기법[16]은 해시연산 4회, XOR 연산 3회 등의 복잡한 연산을 수행하여 실제 시스템에 적용시 계산량에서 효율성이 떨어진다. 또한 Park외 4명의 기법[17]은 태그 난수발생 2회, AES-128 암·복호화 실행 등 태그에 많은 연산이 집중되어 있어 고가의 태그가 필요하며 통신라운드도 10회로 타 프로토콜에 비해 비효율적으로 동작 한다. 하지만 본 논문에서 제안하는 프로토콜은 통신 라운드 수가 8회 이지만 데이터베이스의 매 순간 변화하는 Rdbt를 해시하여 이용함으로써 보안성은 강화되고 태그에서의 연산량에 있어서 상대적으로 가볍다는 것을 알 수 있다. 최근 계속 연구 발표 되고 있는 해시 관련 무거운 프로토콜은 수동형태그의 저장 공간 및 많은 연산량을 실행시키기 어려운 면이 있어 효율성 측면에서 사용성이 낮은 반면 본 제안 프로토콜은 난수생성, XOR등의 연산을 최소화하고 복잡한 연산이 없어 저비용으로 구축할 수 있다. 아울러 기본적으로 데이터베이스에서 동작중인 Rdbt와 해시 함수를 이용함으로써 다른 프로토콜에 비해 효율성이 우위에 있음을 알 수 있다.

5. 결론

최근 들어 RFID 시스템은 물류, 생산, 재고 관리 분야는 물론 바코드를 대신하여 산업 전반에서 관심을 받고 있다. 향후 점차적으로 바코드를 대체하여 유비쿼터스 환경을 조성하기 위한 분야로 그 발전이 예상되고 있다. 현재 여러 분야에서 연구가 진행되고 있지만 바코드를 대체하기 위해 값이 저렴한 태그의 개발에 많은 연구가 이루어지고 있으며 그에 따른 보안문제도 해결해야 하는 어려운 과제이다. 저가형 태그의 경우 단일의 고정 ID를 저장하고 있고 리더의 신호에 단순히 반응하기 때문에 태그의 위치추적, 이동경로파악, 도청등 보안상 문제가 있으며 각종 공격에 무방비한 상태로 노출되어있다. 이러한 문제를 해결하기 위해 최근 해시-락, 확장된 해시-락, 해시체인, 해시기반ID 변형기법, Kim-Ryoo의 기법, Park외 4명의 기법등 다양한 프로토콜이 제안되고 있다. 대부분 저가형 단순한 방법으로 취약점이 발견되고 있다. 또한 복잡한 계산을 요구하는 방법은 보안상 안전하나 태그 및 RFID 시스템에 많은 부하를 주어 효율성이 떨어진다. 일반적으로 보안 관련한 문제를 해결하기 위해서는 태그의 우수한 계산 능력과 저장 공간이 커야 충족할 수 있다. 그러나 본 논문에서 제안한 프로토콜은 난수와 데이터베이스의 마이크로타임과 ID를 해시하여 이용하는 방법으로 기존 프로토콜에 비해 강력하지만 계산량이 많지 않고 상호 인증이 가능한 프로토콜을 제안하였다. 안전성 분석에서 여러 가지

가능한 공격 상황에 대해 안전함을 보였고, 효율성 면에서는 기존의 해시기반 여러 논문에 비해 우위에 있음을 알 수 있다. 이러한 고기능 RFID 보안 프로토콜은 의료분야, 고가품, 문화재 관리 등 보안 관리의 중요성이 높은 분야에 적용할 수 있다. 본 프로토콜은 해시한 마이크로타임 기반으로 재전송 공격 등이 차단되어 보안상 효과적인 방식이며 시스템에 사용할 시 태그단가를 낮추어 비용절감을 할 수 있으며 많은 적용성이 있을 것으로 예상된다. 향후 보안상 안전성을 해치지 않는 범위 내에서 태그의 연산량을 더욱 줄여 태그의 단가를 낮출 수 있는 다양한 방안에 대한 연구가 필요하다.

참 고 문 헌

[1] Gene Tsudik, YA-TRAP: Yet Another Trivial RFID Authentication Protocol, Proceedings of the 4th annual IEEE international conference on Pervasive Computing and Communications Workshops, p.640, March 13-17, 2006

[2] J. Aragones, A. Martinez-Balleste, and A. Solanas. A brief survey on rfid privacy and security. In World Congress on Engineering, 2007.

[3] Yu Tian-tian, Feng Quan-yuan, "A Security RFID Authentication Protocol Based on Hash Function," ieec, pp.804-807, 2009 International Symposium on Information Engineering and Electronic Commerce, 2009

[4] 이근우, 오동규, 곽진, 오수현, 김승주, 원동호 "분산 데이터베이스 환경에 적합한 Challenge-response 기반의 안전한 RFID 인증 프로토콜", 한국정보처리학회논문지C, 제12-C권, 제03호, pp. 309-316, 2005.

[5] M. Burmester, T. van Le, and B. de Medeiros. Provably secure ubiquitous systems: Universally composable RFID authentication protocols. In Proc. of the 2nd IEEE/CreateNet International Conference on Security and Privacy in Communication Networks (SECURECOMM 2006). IEEE Press, 2006.

[6] He Lei, Gan Yong, Sun Tong, Wang Peng-yuan, "A Revised Efficient Authentication Protocol for Low-Cost RFID System," iitaw, pp.116-118, 2009 Third International Symposium on Intelligent Information Technology Application Workshops, 2009

[7] 김대중, 전문석,"일회성 난수를 이용한 안전한 RFID 상호인증 프로토콜 설계", 정보과학회논문지: 정보통신, 제35권, 제03호, pp. 243-250, 2008.

[8] 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.

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

[10] 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.

[11] 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.

[12] 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.

[13] M. Ohkubo, K.Suzuki and S. Kinoshita, "Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost RFID, "Proceedings of the SCIS 2004, pp. 719-724, 2004.

[14] Gildas Avoine and Philippe Oechslin "RFID Traceability: A Multilayer Problem", Financial Cryptography, March 2005.

[15] D. Henrici, and P. Muller. “Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers”, Procedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops(PERCOMW'04), pp.149-153, IEEE, 2004.
[16] 김배현, 유인태 “반사공격에 안전한 RFID 인증프로토콜”한국통신학회논문지 32권 3호, pp.348-354, 2007.
[17] 박용수, 신주석, 최명실, 정경호, 안광선 “ 해시된 태그ID와 대칭키 기반의 RFID 인증프로토콜”정보처리학회논문지C 제16-C권 제6호, pp. 669-680, 2009.

1999～2003 강원대학교 삼척캠퍼스 정보통신공학과 조교수
2003～현재 충북대학교 컴퓨터교육과 교수
2001～2009 IEEE member
2003～2004 한국정보처리학회 논문지편집위원 데이터베이스분과, 이사 역임
2007～2010 한국산학기술학회 이사 역임
1983～현재 한국정보과학회 종신회원
2010～현재 한국컴퓨터교육학회 이사(현)
2010～현재 한국융합학회장(현)
현재 한국정보처리학회 회원
관심분야: 질의처리 및 최적화, 근사질의응답(AQA), 시공간 데이터베이스, GIS, 데이터 마이닝, 국제물류, u-Learning과 평가방법
E-Mail: jongyun@chungbuk.ac.kr

배 우 식

1997～현재 아주자동차대학 전산소
2006 백석대학교 정보기술대학원 (공학석사)
2009 충북대학교 컴퓨터교육과 박사수료
관심분야: RFID 보안, 컴퓨터 네트워크, 암호 프로토콜/알고리즘, 정보시스템 등
E-Mail: bws@motor.ac.kr

이 종 연

1985 충북대학교 전자계산기 공학과(공학사)
1987 충북대학교 대학원 전자계산기공학과(공학석사)
1999 충북대학교 대학원 전자계산학과(이학박사)
1990～1994 현대전자산업(주) 소프트웨어연구소 주임연구원
1994～1996 현대정보기술(주) CIM사업부 책임연구원

김 상 춘

1986 한밭대학교 전자계산학과 (공학사)
1989 청주대학교 전자계산학과 (공학석사)
1999 충북대학교 대학원 전자계산학과(이학박사)
1983～2001 한국전자통신연구원 정보보호기술연구본부 선임기술원
2001～현재 강원대학교 공학대학 정보통신공학과 부교수
1989～현재 한국정보과학회 종신회원
1989～현재 한국정보처리학회 종신회원, 이사
1989～현재 한국정보보호학회 종신회원, 부회장
2006～현재 개방형컴퓨터통신연구회 종신회원, 상임이사
관심분야: 네트워크보안, IPSec, IPTV 보안, 암호 프로토콜/알고리즘, 보안 시스템 설계 및 구현, RFID 보안 등
E-Mail: kimsc@kangwon.ac.kr