효율적인 공급망 관리를 위한 강화된 RFID 상호 인증 프로토콜

Enhanced RFID Mutual Authentication Protocol on Efficient Supply Chain Management

전준철*

Jun-Cheol Jeon*

요 약

Chen 등은 위조 방지와 프라이버시 보호를 위한 RFID 인증 프로토콜을 제안하였다. 제안된 스킴은 저비용의 RFID 태그 보안을 위하여 XOR 연산과 시프트(shift) 연산을 이용하였다. 그러나, 실제적인 응용 환경을 고려하지 않았기 때문에 보안상의 문제점을 비롯하여 몇 가지 취약점을 보인다. 본 논문에서는 Chen 등의 프로토콜을 분석하고 취약점에 대한 의견을 제시한다. 또한, 기존의 스킴을 보완한 RFID 양방향 인증 프로토콜과 효율적인 공급망 관리를 위한 갱신 프로토콜을 제안한다. 제안된 프로토콜은 기존의 XOR 연산 기반의 RFID 인증 프로토콜과 안전성 및 효율성면에서 비교, 분석하였으며, 높은 안전성과 적은 통신 비용이 요구됨을 확인하였다.

Abstract

Chen et al. proposed a RFID authentication protocol for anti-counterfeiting and privacy protection. A feasible security mechanism for anti-counterfeiting and privacy protection was proposed using XOR and random number shifting operations to enhance RFID tag's security providing a low cost. However, their authentication protocol has some drawbacks and security problems because they did not consider the surrounding environments. We conduct analysis on the protocol and identify problematic areas for improvement of the research. We also provide enhanced authentication and update scheme based on the comment for efficient supply chain management. The proposed protocol was analyzed and compared with typical XOR based RFID authentication protocols and it was confirmed that our protocol has high safety and low communication cost.

Key words : RFID, Authentication, Tag Security

I. 서 론

RFID (radio frequency identification) 기술은 유비쿼터스 기반 환경에서 상품 식별을 위해 중요한 역할을 할 것으로 기대되며, 주로 대량의 상품을 식별하는데 사용되는 차세대 기술로 고려되고 있다. 그리고, 가까운 미래에 기존 광학 바코드 시스템을 대체하게 될 것이다. 태그에 장착된 마이크로 칩은 유일한 식별 정보를 가지고 있으며 공급망 관리 및 재고 관리 등의 여러 분야에 응용된다[1,2].

전형적인 RFID 시스템은 태그(tag)와 리더(reader)로 구성된다. 백엔드 서버(back-end server)는 개별적

* 우석대학교 정보보안학과(Information Security Department, Woosuk University)
· 제1저자 (First Author) : 전준철
· 투고일자 : 2009년 9월 8일
· 심사(수정)일자 : 2009년 9월 9일 (수정일자 : 2009년 10월 23일)
· 게재일자 : 2009년 10월 30일

인 구성 요소로서 일반적으로 RFID 시스템과 함께 운용된다. 태그는 IC 칩과 안테나로 구성되고, 리더들의 질의에 대한 응답으로 저장된 데이터를 리더에게 전송한다. 리더는 무선 신호를 보내고 태그로부터 전달된 데이터를 받는다. 그리고 백엔드 서버에 데이터를 보낸다. 백엔드 서버는 안전하며 리더의 식별자 역할을 하는 태그 정보를 저장하는 데이터베이스를 가진다. 백엔드 서버는 정당한 리더를 경유해서 전달된 정보로부터 각 태그의 식별자를 결정하고, 자신이 가지고 있는 데이터베이스로 부터 리더에게 데이터를 전송한다[3].

RFID 기술은 무선이라는 특성 때문에 과도한 정보 노출뿐만 아니라 사용자 위치 정보 추적과 같은 중대한 프라이버시 침해를 야기한다. 그 이유는 태그의 정보가 리더에게 보내지는 동안 리더와 태그 사이에 물리적인 접촉없이 쉽게 인식할 수 있기 때문이다. 이러한 우려는 RFID 구현에 있어서 방해 요소가 되며, 성공적인 RFID 구현을 위해서 다양한 프라이버시 문제들은 사전에 해결되어야 된다. 따라서 인증 프로토콜에 관한 연구는 태그에 저장된 정보를 보호하고, 태그의 위치 추적과 같은 보안 문제들을 해결하기 위해서 지금도 활발하게 진행되고 있다[4].

한편, Chen 등은 위조 방지와 프라이버시 보호를 위해 RFID 인증 프로토콜을 제안하였다[5]. 이 연구의 주된 연산은 XOR 연산과 몇 가지 가정을 기반으로 한 시프트(shift) 연산을 사용하는 것이다. 그러나 그들의 가정과 연산은 몇 가지 취약점과 보안 문제점을 야기한다. 첫째, 정당한 리더의 ID가 갱신절차 없이 태그의 메모리에 영구 저장된다고 가정하였다. 둘째, 태그와 백엔드 서버 간에 단방향 인증을 제시하였다. 셋째, 주된 연산 중의 하나인 시프트 연산은 보안상의 문제점을 가진다. 그리고 넷째, 모든 절차가 백엔드 서버로부터 시작된다. 본 논문에서는 위에서 언급된 몇 가지 취약점을 분석하고, 효율적인 공급망 관리를 위한 향상된 스킴을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 RFID 인증 프로토콜의 안전성 및 효율성의 요구사항을 알아본다. 3장에서는 Chen 등이 제안한 RFID 인증 프로토콜을 살펴보고 취약점을 분석한다. 4장에서는 분석한 취약점을 바탕으로 향상된 인증 스킴을 제안한다. 5장에서는 제안한 RFID 인증 프로토콜의 안전성 및 효율성을 보여주고, 마지막으로 6장에서 결론을 맺는다.

Ⅱ. RFID 인증 프로토콜 요구사항

2-1 안전성 요구사항

RFID의 특징에 의해 위치 추적과 도청이라는 개인 프라이버시에 대한 새로운 보안상 취약점을 가지게 된다. 이러한 다양한 종류의 위협과 그로부터 안전하기 위해 필요한 조건은 다음과 같다[6,7].

1) 도청 공격: RFID 시스템에서 리더와 태그 간의 통신은 무선으로 이루어지고, 또한 태그는 리더의 요청을 받으면 리더에 대한 인증과정 없이 응답을 하게 된다. 따라서 공격자는 별 다른 노력 없이 쉽게 정당한 태그의 응답을 얻을 수 있다. 그러므로 안전한 RFID 시스템은 공격자가 정당한 메시지를 얻더라도 그로부터 어떠한 유용한 정보도 얻을 수 없게 설계되어야 한다.

2) 재전송 공격: 재전송 공격이란 과거에 정당한 개체간의 통신 메시지를 도청한 후, 이후에 그 메시지를 재사용하는 것을 뜻한다. 이 공격은 이전 세션에서 도청한 메시지를 현재 세션에 사용함으로써 정당한 사용자로 사칭할 수 있다. 따라서 메시지는 세션마다 불규칙적으로 변경되어야 한다.

3) 위장 공격: 위장 공격이란 스푸핑(spoofing) 공격이라고도 하며 정당하지 않은 개체를 정당한 것처럼 속여 인증과정을 통과하는 방법이다. 스푸핑은 그 대상에 따라 두 가지로 구분할 수 있다. 먼저 공격자가 태그로 위장하여 정당한 리더를 속이는 방법과, 반대로 공격자가 리더로 위장하여 태그를 속이는 방법이 있다. 따라서 통신에의 사용된 메시지를 통하여 키 값 또는 난수 값 등을 추출할 수 없어야 한다.

4) 위치 추적: 위치 추적은 공격자가 특정한 태그로부터 동일한 정보나 특정 태그를 구별할 수 있는 정보를 찾아 태그 소유자의 위치를 추적하는 공격을 의미이다. 이 공격은 세션마다 동일한 정보가 나오

는 RFID 시스템은 위치 추적이 가능하다는 것을 의미한다. 따라서 위치 추적에 안전하려면 리더와 태그와의 통신에서 오가는 메시지가 일정하거나 규칙적으로 생성되어 공격자가 메시지를 보고 태그를 쉽게 추측할 수 없어야 하고, 또한 현재의 정보를 토대로 이전의 정보를 추측할 수 없어야 한다.

5) 비동기화 공격: 태그의 비밀 정보가 갱신되는 프로토콜에서 통신상의 문제가 발생할 경우, 백엔드 서버와 태그사이에 내부 정보가 불일치할 수 있다. 이러한 점에 착안하여 공격자가 고의로 통신을 방해하여 백엔드 서버와 태그의 정보 불일치를 유도하는 것을 비동기화 공격이라 한다. 이러한 공격으로부터 안전하려면 정보 불일치가 일어나더라도 기존의 값을 회복할 수 있도록 설계하여야 한다.

2-2 안전성 요구사항

데이터베이스에서 태그를 찾는 알고리듬의 효율성은 데이터베이스에서 저장하고 있는 태그의 ID 개수가 증가하더라도 데이터베이스의 식별 과정중의 계산량이 일정 수준 이하로 유지되어야 한다는 데이터베이스의 확장성(scalability)과 관련된 문제이다. RFID 시스템은 데이터베이스가 동시에 여러 태그를 인증하는 환경에 있는 시스템이므로 안전한 인증방식도 중요하지만, 해당 태그를 빠르게 찾아 인증하는 것도 프로토콜 설계 시 중요한 고려 요소가 된다.

안전성을 지키는 범위 안에서, 통신되는 메시지는 짧을수록 효율적이며 태그가 부착될 상품이 대량 생산될 경우, 태그가 부착될 상품이 대량 생산될 경우, 태그의 저비용 구성이 중요하므로 저장 공간과 정보 보호를 위한 암호 요소의 연산량을 줄이는 것이 필요하다.

Ⅲ. Chen 등이 제안한 RFID 인증 프로토콜

본 장에서는 논문에서 사용될 기호 표기를 명시하고, Chen 등의 RFID 인증 프로토콜을 살펴본 후, 보안 및 실용적인 측면을 고려하여 몇 가지 취약점을 분석한다.

3-1 용어 및 표기

본 절에서는 기존 논문의 분석과 제안한 인증 프로토콜의 설명을 위해서 사용되는 용어 및 표기를 보여준다.

- H() : 해쉬 함수
- ID_R : 리더의 고유한 식별자
- $NextID_R$: 다음 세션에서의 리더의 고유한 식별자
- ID_T : 태그의 고유한 식별자
- r : 난수
- r′ : 연산 알고리듬에 의해 변경된 난수
- r_R : 리더가 생성한 난수
- r_T : 태그가 생성한 난수
- $\oplus$: XOR 연산
- =? : 비교 연산

3-2 Chen 등이 제안한 프로토콜

Chen 등은 논문[9]에서 위조 방지 및 프라이버시 보호를 위한 RFID 인증 프로토콜을 제안하였다. 그들은 저비용 연산을 위해 해쉬 함수와 같이 복잡한 암호화 알고리듬 대신 XOR 연산을 사용하였다. 먼저 태그의 메모리에 정당한 리더의 ID_R이 저장되어 있다고 가정한다. 그러므로 태그와 리더에 저장된 ID_R에 의해 태그들은 정당한 리더들을 식별할 수 있다. 이 단계에서 태그는 ID_T와 동일한 데이터 길이를 가지는 난수 r을 얻는다.

XOR 연산을 사용하는 주된 목적은 계산 속도를 높이고 태그 비용을 낮추는 것이다. 그림 1은 Chen 등이 제안한 인증 프로토콜을 보여준다. 리더는 백엔드 서버로부터 받은 $ID_R \oplus r$을 태그에게 보낸다. 태그는 ID_R을 이용해 r을 추출하고 r'을 구한다. 그리고, $ID_T \oplus r'$을 리더에게 보낸다. 백엔드 서버는 리더로부터 받은 $ID_T \oplus r'$로부터 ID_T를 구하여 태그를 인증한다.

단계 1. 백엔드 서버는 먼저 난수 r을 생성하고, 데이터베이스로부터 ID_R을 가져와 난수 r과 XOR하여 리더에게 전송한다. 그리고 리더는 $P = ID_R \oplus r$ 메시지를 질의(Query)와 함께 태그에게 브로드캐스트

한다.

단계 2. 태그는 질의에 포함된 P를 받은 후, 태그에 저장된 ID_R과 XOR 연산을 하여 난수 r을 얻은 후, n 비트만큼 왼쪽으로 이동하여 r'을 생성한다. 단, n은 난수 r의 이진 값 1의 개수를 의미한다. 그리고, $Q=ID_T \oplus r'$을 계산하여 리더에게 전송한다.

단계 3. 백엔드 서버는 리더로 부터 Q를 받고, $Q \oplus r'$을 계산하여 ID_T를 얻는다.

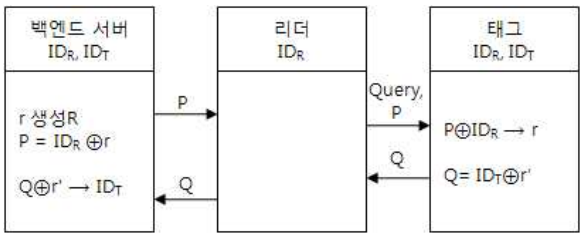

그림 1. Chen 등이 제안한 RFID 프로토콜
Fig. 1. RFID Protocol proposed by Chen et al.

3-3 취약점 분석

언급된 Chen 등의 RFID 인증 프로토콜에서, 보안 및 실용적인 측면을 고려하여 몇 가지 취약점을 분석한다.

1) 정당한 리더의 ID_R이 갱신절차 없이 태그의 메모리에 영구 저장되어 있다고 가정한다; 실제 응용환경에서 리더는 상품의 배포과정 및 처리과정에 의해 변경될 수 있다. 따라서 태그의 메모리에 있는 ID_R은 다음의 배포 및 처리단계에서 언제든지 갱신되어야 한다. 그 이유는 RFID 기반 응용들은 주로 공급망 관리를 위해 개발되었기 때문이다. 예를 들면, 상품이 특정 저장소에서 다른 저장소로 이동될 경우 정당한 리더는 기존 저장소 리더에서 도착지 저장소 리더로 갱신되어야 한다. 따라서, 효율적인 공급망 관리를 위해 ID_R의 갱신 절차를 제공하여야 한다.

다음과 같이, XOR과 해쉬 함수를 기반으로 간단히 갱신 절차를 고려할 수 있다. 리더는 태그로 부터 기존의 ID_R을 받고 백엔드 서버로 그 값을 전송한다. 백엔드 서버는 다음 단계의 ID_R를 동봉하여 태그에게 보낸다. 태그는 리더가 보낸 결과와 기존 ID_R로 부터 다음 단계의 ID_R을 획득할 수 있다.

2) 태그와 백엔드 서버간에 단방향 인증만을 제공한다; 일반적으로 리더와 백엔드 서버간의 통신 채널은 기존 VPN 또는 SSL과 같이 안전한 채널로 고려되어진다. 다른 한편으로 태그와 리더간의 통신 채널은 채널이 무선을 기반으로 하고 있기 때문에 안전하지 않다. 리더는 포켓용 장치일 수도 있고 무선 네트워크 기반의 모바일 장치일 수도 있다. 이와 같이 리더는 TTP(Trusted Third Party)가 아니다. 따라서 태그와 백엔드 서버 사이에는 양방향 인증이 필요하다.

양방향 인증을 제공하기 위해 태그는 자신의 값을 백엔드 서버에게 제공하고, 백엔드 서버는 계산을 통해서 얻은 값을 태그에게 전송한다. 이를 위해 일반적인 방법으로 XOR연산 또는 해쉬 함수를 사용한다. 본 논문에서는 저비용 연산을 위한 XOR 기반의 프로토콜을 고려한다.

3) 주요 연산 중의 하나인 시프트 연산은 보안상의 문제점을 가진다; 태그는 새로운 난수 r'을 생성하기 위해 r을 n 비트만큼 왼쪽으로 순환이동(circular shift)한다. 단, n은 난수 r의 이진 값 1의 개수를 의미한다. 난수들이 좋은 난수 생성기에 의해 생성된다고 가정하자. 이 때 대부분의 난수들은 동일한 비트 내에서 1과 0의 개수가 반반인 경우가 많다. 16비트 난수를 예로 들면, 정확히 1과 0이 반반인 경우가 전체 56,536개 중에 12,870개이다. 이것은 난수의 19.6%가 1과 0이 동일한 개수를 가진다는 것을 의미한다. 이 영역에 있는 1의 개수를 8±2로 약간만 확장하면 일치하는 개수는 65,536개 중에 51,766개로 78.9%가 된다. 이와 같이, 동일한 비트 내의 난수들은 1과 0의 개수가 유사한 비율을 가지는 경우가 많다. 따라서 1의 개수만큼 이동하는 연산은 강력한 보안을 제공하지 않는다.

4) 모든 절차가 백엔드 서버에서 시작한다; 대부분의 경우에 질의는 리더가 태그들의 이동에 즉각적으로 대처해야하기 때문에 리더로부터 시작되어야 한다. 하지만 Chen 등의 스킴에서는 태그가 나타나기 전에 미리 백엔드 서버가 항상 리더에게 $ID_R \oplus r$을 보낸다. 이것은 대량의 태그와의 통신을 위해 바람직한 모델이 아니다.

Ⅳ. 제안하는 향상된 RFID 인증 프로토콜

본 장에서는 앞 장에서 제시한 취약점을 고려하여 향상된 RFID 상호 인증 프로토콜을 제안한다. 그림 2는 제안하는 RFID 상호 인증 프로토콜을 보여준다.

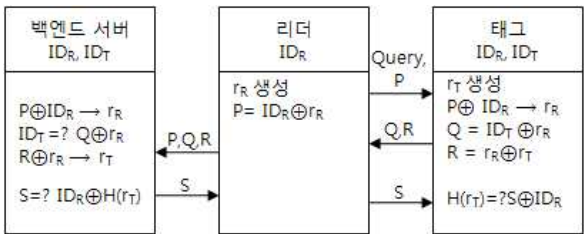

그림 2. 제안된 RFID 상호 인증 프로토콜
Fig. 2. Proposed RFID mutual authentication protocol

백엔드 서버와 각 태그는 ID_R과 ID_T를 가지며, 각 난수는 각각의 세션에서 생성된다고 가정한다. 리더는 r_R을 생성하고 P 메시지를 브로드캐스트한다. 메시지를 받은 태그는 ID_R을 이용하여 r_R을 구하고 r_T를 생성한다. 그리고 태그는 자신과 리더의 인증을 위해 Q과 R을 리더에게 전송한다. 리더는 태그로부터 받은 값을 백엔드 서버에게 전송하고, 백엔드 서버는 ID_T를 추출하여 데이터베이스에 동일한 ID_T가 있는지 확인함으로써 태그를 인증한다. 다음 단계로 백엔드 서버는 리더 인증을 위해 태그로부터 받은 R에서 r_T를 추출하여 리더에게 S를 전송하고, 리더는 백엔드 서버로부터 받은 값을 태그에게 전송한다. 그리고 태그는 $H(r_T)$를 추출하여 리더를 인증한다. 자세한 인증과정은 아래와 같다.

단계 1. 리더는 r_R을 생성하고 질의I(Query)와 함께 $P = ID_R \oplus r_R$ 메시지를 태그에게 브로드캐스트한다.

단계 2. 태그는 r_T를 생성하고, $P \oplus ID_R$을 계산하여 리더가 생성한 난수 r_R을 추출한다. 그리고 태그는 $Q = ID_T \oplus r_R$과 $R = r_R \oplus r_T$를 계산해서 리더에게 전송한다.

단계 3. 리더는 P와 함께 태그로부터 받은 Q와 R을 백엔드 서버에게 전송한다.

단계 4. 백엔드 서버는 $P \oplus ID_R$을 계산해서 r_R을 추출하고, $Q \oplus r_R$을 계산해서 ID_T를 추출한다. 그리고 데이터베이스에 ID_T가 있는지 검색한다. ID_T가 존재하면 태그는 인증되고, 그렇지 않다면 이 세션은 종료된다. 그리고 백엔드 서버는 $R \oplus r_R$을 계산하여 r_T를 추출하고, $S = ID_R \oplus H(r_T)$를 계산한 후 리더에게 전송한다.

단계 5. 리더는 백엔드 서버로부터 받은 S를 태그에게 전송한다.

단계 6. 태그는 $S \oplus ID_R$의 결과 값과 $H(r_T)$를 비교한다. 두 값이 같으면 리더는 인증되고, 그렇지 않다면 이 세션은 종료된다.

효율적인 공급망 관리를 위한 태그 메모리의 ID_R 갱신 절차는 다음과 같다. 태그는 U를 계산하여 리더에게 전송하고, 리더는 태그로부터 받은 값을 백엔드 서버로 전송한다. 백엔드 서버는 해당 리더의 ID_R로부터 $H(H(ID_R))$을 구하고, 태그로부터 받은 값을 비교하여 정당한 ID_R을 찾는다. 해당되는 ID_R이 백엔드 서버에 존재할 경우 V를 계산하여 태그에게 전송한다. 마지막으로 태그는 $NextID_R$을 추출하여 기존의 ID_R을 갱신한다. 자세한 과정은 아래와 같다.

단계 1. 태그는 $U = H(H(ID_R))$을 계산하여 리더에게 전송한다.

단계 2. 리더는 U를 백엔드 서버로 전송한다.

단계 3. 백엔드 서버는 가지고 있는 ID_R로 부터 $H(H(ID_R))$을 계산하고, 리더로부터 전송받은 U를 비교하여 정당한 ID_R을 찾는다. 해당되는 ID_R이 존재할 경우 $V=NextID_R \oplus ID_R$을 계산하여 태그에게 전송한다.

단계 4. 리더는 백엔드 서버로부터 받은 $V=NextID_R \oplus ID_R$을 태그에게 전송한다.

단계 5. 태그는 $V \oplus ID_R$을 계산하여 $NextID_R$을 추출한다. 기존 ID_R은 새로운 $NextID_R$로 갱신된다.

Ⅴ. 제안된 프로토콜의 안전성 및 효율성

5-1 안전성 분석

RFID 인증 프로토콜에서 리더와 태그 사이의 통신은 안전하지 않은 채널을 이용하므로 공격자에 의

한 도청 뿐 만 아니라 물리적인 접촉 없이 태그에 저장된 정보를 알 수 있으므로 몇 가지 보안 요구사항을 만족하여야 한다. 본 절에서는 제안된 RFID 인증 프로토콜의 보안 요구사항에 대해 분석한다.

1) 도청 공격: 공격자가 리더와 태그간의 통신 정보는 도청할 수 있어도 이를 통하여 비밀 정보를 얻을 수 없어야 한다. 제안된 프로토콜에서 태그와 리더간에 전송되는 모든 정보는 XOR 연산과 일방향 해쉬 함수를 사용한다. 따라서 공격자는 태그와 리더 사이의 통신을 도청하더라도 전송 정보로부터 ID_R, ID_T, r_R, r_T 등을 알아내는 것은 계산상으로 불가능하다.

2) 재전송 공격: 공격자가 재전송 공격을 하기 위해서는 통신되는 메시지 중에 P, Q, 또는 R 의 값을 이용하여 다음 세션에 재전송하여야 한다. 하지만 이 값들은 r_R 또는 r_T 등의 난수를 각각 포함하고 있으므로 매 세션마다 다른 값들로 불규칙적으로 변경된다. 따라서 공격자가 재전송 공격을 이용하여 정당한 사용자로 사칭하는 것은 불가능하다.

3) 위장 공격: 제안된 프로토콜에서 위장 공격은 두 가지 경우가 있다. 첫 번째로 공격자가 리더에서 태그로 전송하는 첫 번째 통신에서 도청하고, 이것을 이용하여 리더에게 정당한 태그로 위장하여 두 번째 통신을 생성하는 것이다. 다시 말해 공격자는 P를 도청하고, 이 정보를 이용하여 정당한 태그로 인증받기 위해서 새로운 응답을 생성하여 태그에게 전송하려고 한다고 가정하자. 이 경우 두 번째 통신에서 정당한 태그로 인증받기 위해 ID_R을 알아내서 난수 r_R을 추출하고, 이것을 이용하여 $ID_T \oplus r_R$을 리더에게 보내야 한다. 하지만 제안된 인증 프로토콜에서 공격자가 도청한 값, P로부터 ID_R 또는 r_R을 알아내는 것은 계산상 불가능하다.

두 번째의 경우 공격자가 태그에서 리더로 전송하는 두 번째 통신에서 도청하고, 이것을 이용하여 태그에게 정당한 리더로 위장하여 세 번째 통신을 생성하는 것이다. 즉, 이 경우에 공격자는 도청한 Q와 R을 이용하여 r_T를 추출해야한다. 하지만 제안된 프로토콜에서 공격자가 도청한 값, Q 또는 R로부터 r_T를 추출하는 것은 계산상 불가능하다.

4) 위치 추적 공격: 제안된 프로토콜에서는 리더의 요청에 대한 태그의 응답으로 난수 r_T를 생성하고 XOR연산을 이용하여 Q와 R을 계산해서 리더에게 전송한다. 따라서 응답 메시지는 이전 세션과 동일하거나 규칙적으로 변하는 것이 아니므로 공격자가 과거 통신 내용을 모두 알고 있는 상황이더라도 현재 통신 중인 태그가 어떤 특정 태그라고 단정할 수 없다. 또한, 매 세션마다 태그가 r_T를 생성하므로 현재의 정보를 토대로 과거 이동 경로를 유추하는 것은 어렵다.

추적성을 피하기 위한 가장 근본적인 방법은 ID를 갱신하는 것이다. 제안된 프로토콜은 추적성을 피하고 효율적인 공급망 관리를 위한 ID갱신 과정을 제공한다. 제안된 스킴에서는 이중해쉬와 XOR연산을 통하여 태그 메모리의 ID 갱신과정을 제공함으로써, 위치 추적 공격에 대한 강력한 보안을 한번 더 제공한다.

5) 비동기화 공격: 제안된 상호 인증 프로토콜에서 공격자가 태그와 리더 사이의 통신을 차단하였다 하더라도 인증과정 중에서의 백엔드 서버 또는 태그 내부 정보의 갱신이 일어나지 않으므로 비동기화 공격에 매우 안전하다. 하지만, 백엔드 서버와 태그 메모리 내에 있는 리더 ID_R의 갱신 과정 중에 생길 수 있는 비동기화를 위하여 ID_R 복구의 위한 동기화 과정을 제시하여야 한다.

예를 들어, 현재 백엔드 서버에 있는 리더의 ID_R이 $NextID_R$으로 바뀐 후, 태그 메모리의 리더 ID_R가 갱신되기 전에 리더와 태그간의 통신이 차단이 되었다고 가정하자. 현재 백엔드 서버에 저장된 리더의 ID_R와 태그 메모리의 리더의 ID_R는 다른 값을 가지게 된다. 따라서, 제안된 프로토콜에서는 백엔드 서버의 갱신 후에 태그 메모리의 갱신이 일어남으로 백엔드 서버의 ID_R의 복구과정이 필요하다.

ID_R의 갱신 과정없이 다음 단계의 인증을 위하여 인증 프로토콜을 사용한다면, 제안된 인증프로토콜의 단계 2에서 잘못된 Q'와 R'의 값이 생성되고 단계 4에서 백엔드 서버는 태그를 인증하지 못한다. 이때, 리더는 오류 메시지를 보내고, 태그는 다시 갱신 프로토콜을 실행한다. 태그는 U'의 값을 전송하고 백엔드 서버의 이전 세션의 리더 ID_R을 사용하여 갱신 프로토콜을 실행한다. 단, 백엔드 서버는 리더의 ID_R

리스트를 가지고 있다고 가정한다.

본 논문의 효율적인 안전성 비교를 위하여 3장에서 설명한 Chen 등의 논문과 함께 기존의 XOR 기반의 다양한 프로토콜을 비교 대상으로 하였다. 논문 [8]에서 Jules 등은 능동적인 공격에 안전한 HB^+ 기법을 제안하였다. 리더와 태그 간에 추가적으로 특정 값을 비밀 값을 서로 저장하고 임의의 값을 태그가 전송하는 기법이다. Lopez 등은 논문 [9]에서 XOR, AND 그리고 모듈로 덧셈 및 곱셈 연산을 사용한 M^2AP 기법을 제안하였으며, 논문 [10]에서는 해쉬 함수의 사용을 병행한 OHLCAP 상호 인증 프로토콜을 제안하였다. 표 1은 기존 프로토콜과 제안된 프로토콜의 안전성을 비교 분석한 결과이다.

표 1. 안전성 분석
Table 1. Security analysis.

공격구분	Chen[5]	HB^+[8]	M^2AP[9]	OHLCAP[10]	제안구조
도청	×	×	○	○	○
재전송	○	○	○	○	○
위장	×	○	○	○	○
위치추적	○	×	○	○	○
비동기	○	×	×	○	○
상호인증	×	×	○	○	○

○:안전성 제공, ×:안전성 제공안함

논문 [5]에서는 3장에서 언급한 바와 같이 주요 연산 중의 하나인 시프트 연산은 보안상의 문제점을 보였다. 따라서, 도청공격이나 위장 공격에 취약성을 보인다. HB^+ 기법은 1비트의 값으로 태그를 인증하므로 관리환경에서 오류 발생의 확률에 매우 높다. 따라서 다수의 태그 정보를 다루는 환경에서 사용하기에 부적합하며 안전성 측면에서 취약성을 갖는다. M^2AP 기법은 상호인증을 제공하고 위치 추적 공격을 막을 수는 있지만 동기화에 대한 공격에 취약성을 보인다[11].

5-2 효율성 평가

효과적인 효율성 평가를 위하여 태그와 리더에서의 연산량, 태그 메모리 사용량 및 통신횟수를 비교 분석한다. 태그 연산량은 인증을 위해 태그에 요구되어 지는 모든 연산의 의미하며, 태그 메모리의 사용량은 초기에 태그 메모리에 적재된 값들로써, 각 값들은 1비트로 구성되어 있다고 가정한다. 리더 연산량은 리더 뿐만 아니라 백엔드 서버 또는 데이터베이스의 연산량의 총합을 의미하며, 통신횟수는 리더와 태그 사이에 통신을 위해 메시지를 주고 받는 횟수를 의미한다.

Chen[5]과 HB^+[8]의 경우 다른 프로토콜에 비해 적은 연산량을 보인다. 하지만 언급한 바와 같이 상호인증을 제공하지 않고 보안상의 취약점 또는 높은 오류율을 보인다. M^2AP[9]과 OHLCAP[10]의 스킴은 비교적 안전한 프로토콜로 판명되었으나 제안된 구조와 비교하여 높은 연산량을 보인다. 특히, 최소한의 메모리를 사용해야하는 태그의 환경에서 상대적으로 매우 높은 태그 메모리를 사용한다.

표 2. 효율성 평가
Table 1. Efficiency evaluation.

구분	Chen[5]	HB^+[8]	M^2AP[9]	OHLCAP [10]	제안 구조
태그 연산량	2_XOR 시프트 연산	난수 생성 2_XOR 2_mod MUL	1_XOR 1_OR 1_AND 1_mod MUL	5_XOR 2_mod ADD 1_Hash	난수 생성 4_XOR
태그 메모리 사용량	2ι	3ι	6ι	5ι	2ι
리더 연산량	난수 생성 2_XOR	난수 생성	2_XOR 1_OR 1_AND 2_mod ADD	난수 생성 5_XOR 1_mod ADD 1_Hash	난수 생성 5_XOR 1_Hash
통신 횟수	2	3	4	3	3

ι:태그의 비트 수

표 2는 제안된 프로토콜과 기존의 XOR 기반의 인증 프로토콜의 효율성을 비교하였다. #_(XOR, OR, AND, Hash)는 #회의 XOR, OR, AND 그리고 해쉬 연산을 각각 의미하며, #_mod (MUL, ADD)는 #회의 모듈러 곱셈과 덧셈을 각각 의미한다. 표 2에서 보듯이 제안된 프로토콜은 상호인증을 하는 프로토콜 중에서 상대적으로 적은 연산량과 태그 메모리의 사용량을 보인다.

Ⅵ. 결 론

본 논문에서는 Chen 등이 제안한 RFID 인증 프로

토콜의 보안 및 실용적인 측면에 있어서 몇 가지 취약점을 분석하였고, 그것을 해결하기 위해 향상된 RFID 인증 프로토콜을 제안하였다. Chen 등의 프로토콜은 낮은 비용 구조와 간단한 계산을 제공하기 위해 XOR 연산, 난수 생성, 시프트 연산을 사용하였다. 그러나 실제적인 응용 환경을 고려하지 않았기 때문에 몇 가지 문제점이 일어날 수 있다. 본 논문에서는 제시된 문제점을 해결하고 실제 응용에서 요구되어지는 상호 인증 프로토콜과 효율적인 공급망 관리를 위한 리더 ID 갱신 프로토콜을 제안하였다. 또한, 다양한 안전성 및 효율성 평가를 통해 기존의 저용량 XOR 기반의 프로토콜에 비해 매우 높은 안전성과 적은 통신비용이 요구됨을 확인하였다. 따라서, 제안된 프로토콜은 효율적인 공급망 관리를 위한 저용량 RFID 통신에 효과적으로 이용될 수 있을 것으로 기대된다.

감사의 글

본 논문은 2009학년도 우석대학교 교내학술연구비 지원에 의하여 연구되었음.

참 고 문 헌

[1] A. Juels, S. A. Weis, Defining Strong Privacy for RFID, RSA lab., 2006.

[2] 백동원, 안병훈, 박상환, 고봉진, 박승엽, “무선랜 기반의 RFID 시스템 구현”, 한국항행학회논문지, 12(3), pp. 227-232, 2008.

[3] 이혜림, 한상환, 이종서, 이찬미, 문일영, “모바일 RFID를 이용한 U-AD”, 한국항행학회논문지, 12(6), pp. 583-590, 2008.

[4] D. Molnar, A. Soppera, D. Wagner, “A scalable delegatable pseudonym protocol enabling ownership transfer of RFID tags”, Selected Areas in Cryptography-SAC 2005, LNCS 3897, pp. 276-290, 2005.

[5] Y. C. Chen, W. L. Wang, M. S. Hwang, “RFID Authentication Protocol for Anti-Counterfeiting and Privacy Protection”, Proceedings of Icact 2007, pp. 255-259, 2007.

[6] 권혜진, 이재욱, 전동호, 김순자, “데이터베이스에서의 태그 검색이 쉽고 안전한 RFID 상호인증 프로토콜”, 한국정보보호학회논문지, 18(5), pp. 125-134, 2008.

[7] 하재철, 박제훈, 하정훈, 김환구, 문상재, “검색정보 사전 동기화를 이용한 저비용 RFID 방식”, 한국정보보호학회논문지, 18(1), pp. 77-87, 2008.

[8] A. Juels, Stephen A. Weis, “Authenticating Pervasive Device with Human Protocols”, Advanced in Cryptology-CRYPTO 2005, LNCS 3621, pp. 293-308, 2005.

[9] P. Peris-Lopez, J. C. Hernandes-Castro, J. M. Estevez-Tapiador, A. Ribagorda, “M2AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags”, UIC 2006, LNCS 4159, pp. 912-923, 2006.

[10] E. Y. Choi, S. M. Lee, D. H. Lee, “Efficient RFID Authentication protocol for Ubiquitous Computing Environment”, LNCS, Proceedings of Secubiq 2005, 3823, pp. 945-954, 2005.

[11] T. Li and G. Wang, “Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols”, IFIP New Approaches for Security, Privacy and Trust in Complex Environments, 232, pp. 109-120, 2007.-153, 2004.

전 준 철 (全俊哲)

2000년 2월 : 금오공과대학교 컴퓨터공학과(공학사)
2003년 2월 : 경북대학교 컴퓨터공학과(공학석사)
2007년 2월 : 경북대학교 컴퓨터공학과(공학박사)
2007년 9월 ~ 2008년 8월 : Humboldt University, post doc.
2009년 3월 ~ 현재 : 우석대학교 정보보안학과 전임강사
관심분야 : 암호응용, 인터넷보안, RFID 등