情報保護學會論文誌
第19卷 第5號, 2009. 10

강한 인증과 프라이버시를 보장하는 개선된 초경량 RFID 인증 프로토콜

전 동 호,[1†] 김 영 재,[1] 권 혜 진,[1] 정 선 영,[2] 김 순 자[1‡]
[1]경북대학교, [2]경운대학교

An Enhanced Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Privacy

DongHo Jeon,[1†] YoungJae Kim,[1] Hyejin Kwon,[1]
SeonYeong Jeong,[2] SoonJa Kim[1‡]
[1]Kyungpook National University, [2]Kyungwoon University

요 약

최근, Chein 등에 의해 초경량의 강한 인증과 무결성을 제공하는 프로토콜이 제안되었다. 태그는 단지 간단한 비트연산을 필요로 한다. 태그는 난수를 생성하는 난수생성기를 지원하지 않기 때문에, 공격자는 이전 메시지를 재전송할 수 있고 리더를 가장할 수 있다. 더욱이, 이전의 모든 초경량 인증 스킴들은 비동기, 도청, 가장, 위치추적, 서비스 거부 , 태그 ID 노출, 등의 다양한 공격에 취약성들을 가지고 있다. 이전의 초경량 프로토콜의 취약성을 분석하고, 태그에 난수생성기를 이용하여 보안문제들을 해결한다. 따라서, 본 논문에서는 난수생성기와 비트연산 등을 사용하여 알려진 공격에 안전한 새로운 경량 상호 인증프로토콜을 제안하고 제안된 방식의 안전성과 효율성을 분석하였다.

ABSTRACT

Recently, Chein et al proposed the ultralightweight strong authentication and strong integrity (SASI)protocol, where the tag requrires only simple bitwise operations. Since the tag does not support random number generator to generate a challenge nonce, an attacker can replay old messages and impersonate reader. However, all of the previous ultralightweight authentication schemes are vlunerable to various attacks: de-synk, eavesdropping, impersonating, tracking, DoS , disclosure etc. we analyze the problems of previous proposed ultrlightweight protocols, to overcome these security problems by using PRNG on the tag. Therefore, in this paper we propose a new lightweight RFID mutual authentication protocol that provides random number generator and bitwise operations , a security and an efficiency of the proposed schme analyze.

Keywords: RFID system, Authentication protocol, privacy

I. 서 론

RFID(Radio Frequency Identification) 시스템은 무선 주파수를 이용하여 물리적 접촉없이 정보를 읽고 저장할 수 있는 기술이다. 바코드 시장을 대체할 기술로서 지나 10년 동안 꾸준하게 발전을 해왔으며 유통, 물류, 의료, 교육등의 분야에 적용되고 있다. RFID 시스템의 구성은 데이터베이스를 포함한 서버와 연결된 리더, 태그로 구성되어 있다. RFID의 비접촉 무선인식 기술은 기술적인 유용성은 뛰어나지만, 태그와 리더간의 통신이 무선 채널상에서 이루어지므로 공격자에 의해 태그정보가 노출되거나 사생활

접수일(2009년 5월 27일), 수정일(2009년 7월 28일), 게재확정일(2009년 8월 26일)
† 주저자, jdh0692@korea.com
‡ 교신저자, snjkim@ee.knu.ac.kr

침해 및 보안상의 취약점이 드러나게 되었다[1]. 이는 세계 각국에서 사생활 침해논란으로 인해 RFID 대중화의 저해요소로 작용되고 있다. 리더와 태그간의 무선 통신은 유선 통신에 비해 도청되기 쉽다. 이를 극복하기위해서 암호학적인 방법을 RFID 시스템에 추가하여 보안성을 높이는 연구가 계속 진행되어 왔다. 태그 가격의 한계로 인해 일반 컴퓨터 통신과 같이 연산량이 많은 암호 요소를 쓸 수 없다. 이에 Weis 등은 유선 통신에서 통용되고 있는 공개키나 대칭키 암호보다는 연산량이 적으면서 암호학적 효과를 낼 수 있는 프로토콜을 제안하였다[2]. 그러나 저가의 태그는 제한적인 연산능력과 저장공간의 한계로 인해 대칭키, 공개키, 해시 같은 전통적인 암호기법의 사용이 힘들다. 이러한 저가형 태그를 위한 저비용의 안전한 인증기법과 암호기법의 연구를 필요로 하고 있다. 본 논문에서는 현재까지 제안된 RFID의 초경량의 인증 프로토콜에 대해 살펴보고 기존의 취약점을 개선한 경량 상호인증 프로토콜을 제안한다.

본 논문의 구성은 다음과 같이 구성되어 있다. 2장에서는 현재까지 제안된 RFID 초경량의 인증방법과 보안 요구조건에 대해 살펴보고 3장에서는 제안하는 경량 상호인증 프로토콜을 소개한다. 4장에서는 제안기법에 대한 안전성과 효율성을 살펴보고 5장에서 결론을 맺는다.

II. 연구배경

2.1 기존 초경량 인증 프로토콜의 취약성

현재까지 제안된 RFID 인증기법을 태그에서의 연산능력과 저장능력에 따라 크게 네 가지 형태로 분류하면 첫째, 중량 인증방식은 해시함수, 암호화, 공개키 알고리즘 등 전통적 암호기법을 사용하는 프로토콜이다[4,5]. 둘째, 단순인증 방식은 난수생성기와 일방향 해시함수를 사용하는 프로토콜이다[6-10]. 셋째, 경량인증방식은 EPC class-1 Gen-2 가 PRNG와 CRC만 지원하기 때문에 해시함수를 사용하지 않고 난수생성과 CRC만 사용하는 프로토콜이다[13-17]. 넷째, 초경량 인증방식은 xor, and, or같은 간단한 비트연산만을 사용하는 프로토콜이다[18-21].

본 장에서는 비트연산에 기반을 둔 초경량 인증방식에 대해서만 중점적으로 살펴본다. 현재까지 다수의 RFID 시스템에서의 인증 프로토콜이 제안되었는데 경량 프로토콜의 진보된 형태로 Peris-lopez는 EMAP[20]를 제안하였는데, XOR, AND, OR 등의 단순한 비트연산만으로 구성되어 있고 480비트의 EEPROM과 96비트의 ROM만 요구하는 매우 효율적인 상호 인증 프로토콜이다. 대부분 저가의 태그는 수동형이기 때문에 연산이 많이 필요한 곱셈 연산이나 해쉬함수는 사용하지 않고 난수 생성조차 리더측에서 수행된다. 태그의 IDS(Index-Psedonym)는 태그의 모든 정보가 저장되는 테이블의 색인으로 사용되고 키는 각각 네부분의 96비트 서브키로 이루어져 있으며 IDS와 키는 상호인증 성공 후에 업데이트 된다. EMAP는 상호인증의 형태를 취하고 있지만 리더가 수신한 메시지 D||E 에 대한 검증절차가 없어 성공적으로 수신되었거나 검증되었는지 알 수 없고, 수신이 실패하였을 경우 IDS와 키의 업데이트 또한 비동기화 될 우려가 있다. EMAP는 전자태그가 특정 리더에 구속되지 않는다고 가정을 하고 있는데, 즉 프로토콜의 실행상태를 기억하지 않기 때문에 어떤 태그와도 불안전한 프로토콜을 수차례 반복적으로 수행할 수 있게 된다. 하지만 이러한 태그의 비구속성 때문에 태그의 비밀정보가 완전히 노출 될 수 있다[3].

LMAP[18]와 M2AP[19]는 거의 유사한 형태의 프로토콜로 M2AP는 LMAP프로토콜에서 응답메시지 E를 추가하였다. 각 태그는 단일한 ID와 IDS, 비밀키(K1,K2,K3,K4)를 가지고 있고 XOR, OR, AND의 단순연산만 수행한다. 상호인증 성공 후에는 IDS와 비밀키 업데이트 과정을 거친다. M2AP의 비트연산에서 모든 비트는 주어진 비트의 왼쪽에 있는 비트에게만 영향을 끼치는데, 각 비트는 동일하거나 큰 색인의 비트에 의존하게 되는 것이다. 즉, 비트연산과 법 2에 대한 덧셈연산만 수행하며 최하위 비트만 고려했을 때 XOR연산은 법2에 대한 덧셈은 동일한 결과값을 산출한다. 메시지 B와 D에서 OR과 AND 비트연산에서 공격자는 IDS를 재설정할 수 있어 난수 N1, N2의 모든 정보를 쉽게 획득할 수 있다. 우측의 모든 비트를 획득한다 법 2에 대한 덧셈을 알아내는 것은 어려운 일이 아니다. D에서 공격자는 몇 번의 연속적인 도청을 통해 태그ID나 비밀키를 획득하고 더 많은 횟수의 도청을 하면 결국 모든 정보가 누출되고 정당한 태그 또는 리더로의 위장이 가능하다. 또한 LMAP와 M2AP의 태그와 리더간 상호인증은 키와 IDS의 동기화후에 이루어져야 하는데, 공격자가 태그의 응답메시지 D를 가로채면 동기화는 쉽게 무너진다[3,23,24].

SASI 또한 비트연산과 위치교환 함수에 기반한 초

경량 인증 프로토콜이다. 태그의 식별자 ID와 두개의 키(K1, K2)가 태그와 서버에 저장되어 있고 비트연산에 의한 메시지를 생성해 전송하고 검증하는 방식이다. 공격자는 리더의 응답 메시지 D를 강제적으로 중단시켜 서버측의 데이터베이스 업데이트를 방해하는 공격으로 비동기화 오류를 발생시킬 수 있다. 또한 공격자가 메시지를 탈취해 재전송할 경우 태그의 IDS를 획득할 뿐만 아니라 변조 메시지로 인증하게 된다 [3,21,25].

초경량 인증프로토콜은 공통적으로 저가 수동형 태그를 고려하여 설계되었기 때문에 EPC global 의 태그 저장 공간 및 연산 능력 등의 요구조건을 만족하는 효율적인 기법들이다. 하지만 EMAP, M2AP 등의 초경량 인증기법은 이미 전송메시지의 탈취 및, 재전송 공격, 비동기화 태그 정보 누출 등의 공격 위협에 노출되었고 보완된 형태 또한 이러한 위협에 취약성이 드러났다. 비트연산방식에 기반한 경량 및 초경량 인증프로토콜은 메시지생성 및 인증을 위한 검증과정에서 비트연산에 의해 메시지를 생성하는데 이는 연속적인 도청에 의해 식별자 및 키 노출이 불가피하고, 획득한 기본 정보는 태그정보의 완전 노출 및 태그 복제, 위장 공격으로 쓰이는 등 한계를 드러내고 있다 [3,22].

2.2 보안 요구 조건

RFID 시스템의 태그와 리더는 무선 주파수 통신을 사용하기 때문에 불법적인 3자의 공격에 취약할 수 있다. RFID 시스템에서 발생할 수 있는 보안 위협의 요구 조건에 대해 설명한다.

2.2.1 상호 인증(Mutual Authentication)

RFID 시스템에서 데이터베이스와 연결된 리더와 태그 모두 합법적인지를 명시적인 인증을 통해서 확인하는 과정이다. 태그와 리더간의 공유한 비밀 값을 확인하여 인증하거나 동일한 값을 생성함으로써 상대방을 인증한다.

2.2.2 도청공격(Eavesdropping Attack)에 안전

도청공격은 공격자가 태그와 리더 간에 송수신되는 모든 통신 내용을 엿들은 후 태그에 저장된 비밀정보를 알아내고자 하는 공격이다. 도청을 통해 얻어지는 정보를 이용하여 태그에 대한 비밀 값들을 알아낼 수 없어야 한다.

2.2.3 정보 노출(Information leakage)에 안전

RFID 시스템에서 리더와 태그 간의 통신은 무선으로 이루어지고, 또한 태그는 리더의 요청을 받으면 리더에 대한 인증과정 없이 요청에 대한 응답을 하 대한 인 따라서 공격자는 별 다른 노력 없이 쉽 대정당한 태그의 응답을 얻을 수 있다. 그러므로 안전한 RFID 시스템은 공격자가 정당한 메시지를 얻더라도 그로부터 어떠한 유용한 정보도 얻을 수 없게 설계되어야 한다.

2.2.4 재전송 공격(Replay attack) 및 사칭(Impersonate attack)에 안전

재전송 공격이란 이전 세션에 사용된 메시지를 공격자가 재사용하는 것을 말한다. 이 공격은 주로 사칭과 연관 되는데, 공격자는 이전 세션에서 도청한 메시지를 현재 세션에 사용함으로써 정당한 사용자로 사칭할 수 있다.

2.2.5 스푸핑 공격(Spoofing attack)에 안전

스푸핑 공격은 공격자가 정당한 리더 혹은 태그로 위장하여 상대방을 속이거나 유용한 정보를 얻는 공격이다. 이 공격이 성공하기위해서는 공격자는 상대방의 시도에 정당한 응답을 생성해 낼 수 있어야 한다.

2.2.6 위치추적(Location tracking)에 안전

위치추적공격은 공격자가 여러 지역에 걸쳐 불법적인 리더기를 설치한 상황에서 어떤 태그 소유자의 이동 경로를 추적하는 것을 말한다. 이는 아래의 두 가지 보안조건이 충족되지 않을 때 일어나게 된다.

i)불구분성(Indistinguishability)

불구분성이란 태그에서 나오는 메시지를 토대로 그 메시지의 출처를 알아내지 못하는 성질을 말한다. 이를 만족하기 위해서는 통신 중 특정 태그를 지칭하는 고정 메시지나 규칙적인 성질을 가지는 메시지 전송을 지양하여야한다.

ii)전방향안전성(Forward secrecy)

전방향안전성이란 공격자가 어떠한 공격의 성공으로 그 태그의 현재 정보를 알게 되었을 때라도 그를 이용하여 태그 소지자의 과거 이동 경로를 추측하지 못하는 것을 말한다. 즉, 위치추적공격에 안전하려면 특정 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.

2.2.7 비동기화유도 공격(Desynchronization attack: DoS)에 안전

데이터베이스와 태그사이에 정보 갱신이 이루어지는 프로토콜에서 공격자가 악의적으로 통신상의 메시지를 차단하거나 통신상의 문제가 발생할 경우 두 개체 사이에 정보 불일치가 일어 날 수 있다. 이러한 점에 착안하여 악의적으로 리더와 태그사이의 통신을 차단하여 정보 불일치를 유도하는 것을 비동기화유도 공격이라 한다. 이는 일종의 서비스 거부 공격(DoS, Denial of Service attack)으로 이러한 공격에 안전하려면 정보 불일치가 일어나더라도 그를 회복할 수 있도록 설계되어야 한다.

III. 제안하는 프로토콜

본 장에서는 RFID 시스템의 여러 가지 보안 요구조건을 바탕으로 안전하고 효율적인 저비용 RFID를 위한 경량 상호인증 프로토콜을 제안한다[그림 1]. 데이터베이스(DB)와 리더(Reader)는 안전한 채널 상에서, 리더와 태그(Tag)는 안전하지 않은 무선 채널상에서 통신한다고 가정한다. 또한 리더와 태그는 난수생성이 가능하여야 하며, 데이터베이스와 태그는 비밀키 K를 공유하고 있다. 제안하는 프로토콜은 고정된 ID를 가짐으로서 데이터베이스에서 검색을 빠르도록 하고 데이터베이스와 태그에서 저연산(xor, rot, +)을 이용하여 연산속도를 빠르게 한다. 블로킹으로 인해 태그의 비밀키 K값이 업데이트 되지 않았을 경우, 데이터베이스에서 비밀키 K_{old}를 검색하여 비동기 문제를 해결할 수 있다. 매 세션마다 태그와 데이터베이스에서 연산되는 r_T, r_R, K 값이 바뀌게 되므로 도청, 재전송, 스푸핑, 위치추적 공격에 안전하다. 태그의 ID, K 값이 노출되더라도 계속해서 K값이 업데이트 되므로 전 방향 안전성을 어느 정도 만족한다.

3.1 용어정리

이 절에서는 제안 기법에 사용하게 될 용어를 설명한다.

DB : 백 엔드 데이터베이스
R : 리더.
T : 태그.
r_R : 리더가 생성한 난수.
r_T : 태그가 생성한 난수.
ID : 태그의 식별정보.
K : Tag의 ID.
$rot_L ID, A$: ID를 A비트 왼쪽 rotation.
$rot_R ID, A$: ID를 A비트 오른쪽 rotation.
K_{old} : DB에 저장된 태그의 K값.
K_{new} : DB에 저장된 태그의 K값.
K_1, K_2 : K의 왼쪽 절반, K의 오른쪽 절반
|| : 연접
+ : 2^l-1을 법으로 한 덧셈 연산
$\oplus$: 2을 법으로 한 덧셈 연산

3.2 제안하는 프로토콜

제안하는 프로토콜은 [그림1]과 같으며 초기설정과 상호인증, 키 업데이트 과정으로 나눌 수 있다. 각각의 태그에 대하여 데이터베이스에 ID, 초기 인증키 K_{new}, K_{old} 값을 저장하고 태그에 ID, K 값을 저장한다.

Step 1. Reader --〉 Tag : r_R

리더는 태그를 인식하여 랜덤값 r_R을 생성하여, Query와 함께 태그에게 전송한다.

Step 2. Tag --〉 Reader : S'

태그는 리더로부터 Query와 r_R를 수신한 후 , 랜덤값 r_T를 생성하고, 데이터베이스와 공유 비밀값 $K(K_1, K_2)$를 절반으로 나누어 K_1, K_2를 다음 연산에 사용한다. 태그는 $S_1 = (rot_L ID, r_R) + (K_1 \oplus r_T)$과 $S_2 = (rot_R ID, r_T) + K_2$를 연산한 결과인 S_1과 S_2를 XOR 연산하여 S'를 r_T와 함께 리더에게 전송한다.

Step 3. Reader --〉 DB : S', r_T, r_R

리더는 태그로부터 받은 S' 와 r_T 자신의 랜덤값 r_R 과 함께 데이터베이스에게 전송한다.

Step 4. DB --〉 Reader : S''

데이터베이스는 리더로부터 S', r_T, r_R을 받아서 태그에 대한 검증과정을 거친다. 데이터베이스는 $S_1=(rot_L ID, r_R)+(K_1 \oplus r_T)$ 연산과 $S_2=(rot_R ID, r_T)+K_2$를 연산한다. S_1과 S_2를 XOR 연산하여 S'를 만족하는 $K_{new}(K_1,K_2)$를 가진 ID를 찾는다. S'값과 일치하는 ID를 찾지 못한다면 $K_{old}(K_1,K_2)$를 적용하여 S'값을 만족하는 ID를 찾는다. 일치하는 결과가 없다면 데이터베이스는 가짜 태그 또는 공격을 하는 태그로 인식하여 통신을 종료한다. 태그를 검증한 후 데이터베이스는 $K_{new}(K_1,K_2)$또는 $K_{old}(K_1,K_2)$를 이용하여 태그가 데이터베이스를 인증하기 위한 S''를 생성하는 과정과 업데이트 과정을 진행한다. 데이터베이스는 r_T, r_R, K_1 , K_2 를 이용하여 $S_3=(rot_L ID, r_R+r_T)+(K_1 \oplus r_T)$ 와 $S_4=(rot_R ID, r_R-r_T)+K_2$ 를 연산한다. 연산한 결과인 S_3 ,S_4를 XOR 연산하여 S''를 생성하고 $K_{new}(K_1,K_2)$를 업데이트 한다. 데이터베이스는 리더에게 S''를 전송한다.

Step 5. Reader --〉 Tag : S''

리더는 데이터베이스에서 수신한 S''를 태그에게 전송하고 태그는 데이터베이스를 검증하기 위한 과정과 검증이 완료된 후 $K(K_1,K_2)$를 업데이트 한다. $S_3=(rot_L ID, r_R+r_T)+(K_1 \oplus r_T)$와 $S_4=(rot_R ID, r_R-r_T)+K_2$를 연산하여 결과인 S_3 ,S_4를 XOR 연산하여 S''를 생성하고 태그는 $K(K_1,K_2)$를 업데이트 한다.

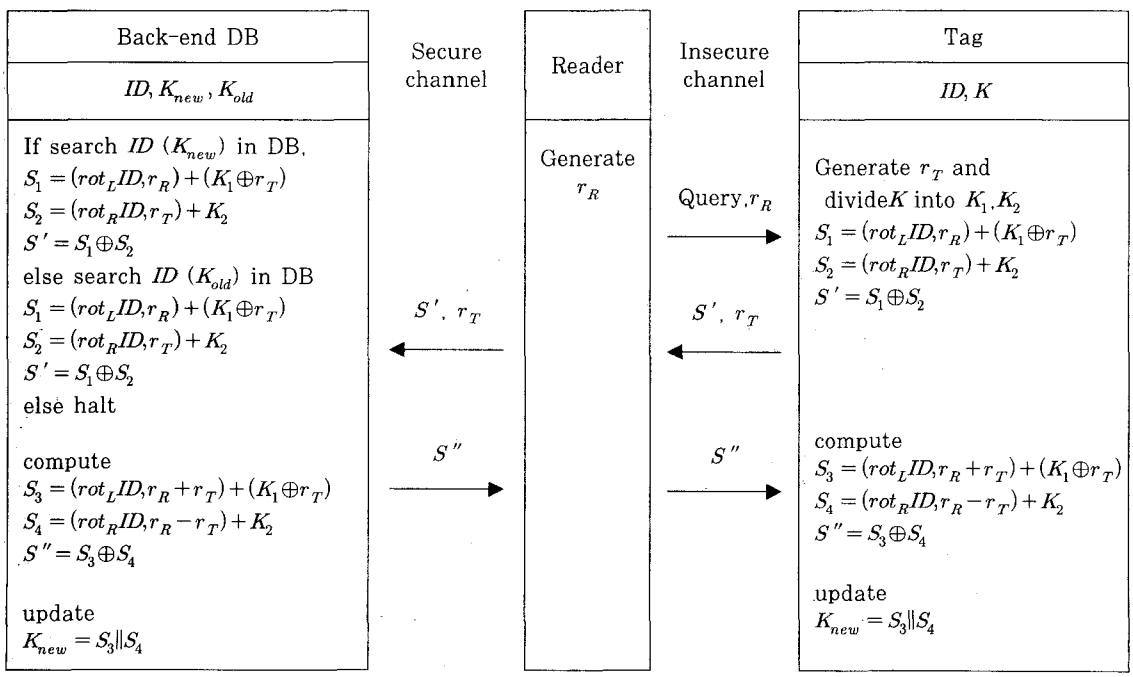
IV. 제안 프로토콜 분석

본 장에서는 앞서 소개된 여러 가지 RFID 보안 요구조건을 바탕으로 Ⅲ장에서 제안한 상호 인증 프로토콜의 안전성과 구현의 효율성에 대하여 분석 한다. 리더와 데이터베이스는 안전한 채널이고 리더와 태그는 안전하지 못한 채널이다. 공격자는 도청이 가능할 뿐 아니라 메시지에 대한 인터럽트도 가능하다고 가정한다. 제안하는 프로토콜은 다음과 같이 상호인증을 통하여 재 전송공격, 스푸핑 공격, 위치추적공격, 서비스 거부 공격, 비동기화 유도 공격 등에 안전하고 전 방향 안정성에 부분 만족한다.

4.1 안전성 분석

4.1.1 상호인증 (Mutual Authentication)

상호인증은 리더와 연결된 데이터베이스와 태그 두



〔그림 1〕 제안하는 프로토콜

당사자가 인증을 통해 서로가 합법적인지 확인하는 과정이다. 제안한 프로토콜은 통신과정에서 ID를 직접 노출 시키지 않고, 데이터베이스와 공유 비밀 값 K와 랜덤 넘버 r_T, r_R를 사용하여 인가된 사용자만이 해당 태그의 ID를 알아 낼 수 있도록 하였다. 데이터베이스에서 매 세션마다 $S' = S_1 \oplus S_2 = \{(rot_L ID, r_R) + (K_1 \oplus r_T)\} \oplus \{(rot_R ID, r_T) + K_2\}$값과 일치하는 ID를 찾아서 태그를 인증하게 된다. 태그 자신이 연산한 결과가 $S'' = S_3 \oplus S_4 = \{(rot_L ID, r_R + r_T) + (K_1 \oplus r_T)\} \oplus \{(rot_R ID, r_R - r_T) + K_2\}$를 만족하는 값이면 데이터베이스를 인증한다. 따라서 제안한 프로토콜은 안전한 상호인증을 제공한다.

4.1.2 도청공격 (Eavesdropping Attack)

도청공격은 무선통신구간인 태그와 리더사이에 송수신되는 내용을 도청하여 태그에 대한 정보를 알아내는 공격이다. 제안한 프로토콜에서 공격자는 r_T, r_R, S', S''를 도청할 수 있다. 하지만 공격자는 도청한 내용을 역으로 연산을 하지 못하므로 태그의 비밀 값 K,ID에 대한 정보를 얻어낼 수 없다. 따라서 제안한 프로토콜은 도청공격에 안전하다.

4.1.3 재 전송공격 (Replay Attack)

재전송 공격은 공격자가 과거에 태그와 리더의 무선통신 구간에서 내용을 도청한 후 이를 재전송하여 합법적인 태그나 리더로 인증 받으려는 공격이다. 제안 프로토콜에 정당한 리더로 가장한 공격방법을 적용하면 공격자는 이전 세션에서 도청을 통하여 r_T, r_R, S', S''를 얻을 수 있지만 이전 세션에서 태그에서 K값이 갱신되어 있고 태그에서 생성된 난수 r_T가 다르므로 이전의 S''와 다르므로 정당한 리더로 인증되지 않는다. 공격자가 정당한 태그로 가장한 경우 세션마다 리더로부터 전송된 r_R값과 태그에서 생성된 r_T값이 $S_1 = (rot_L ID, r_R) + (K_1 \oplus r_T)$연산에 사용되어져 $S' = S_1 \oplus S_2$ 값이 데이터베이스에서 일치하지 않으므로 가짜 태그 또는 공격 태그로 쉽게 검출된다. 따라서 제안한 프로토콜은 재 전송공격에 안전하다.

4.1.4 스푸핑 공격 (Spoofing Attack)

스푸핑 공격은 공격자가 정당한 태그로 위장하여 리더로부터 인증에 필요한 정보를 획득하거나 정당한 리더로 위장하여 태그로부터 인증에 필요한 정보를 획득하여 공격하는 방법이다. 제안 프로토콜에서는 공격자가 정당한 리더로 가장하여 태그를 속이기 위해서는 재전송 공격의 방법과 동일하게 올바른 $S'' = S_3 \oplus S_4 = \{(rot_L ID, r_R + r_T) + (K_1 \oplus r_T)\} \oplus \{(rot_R ID, r_R - r_T) + K_2\}$ 값을 계산해야 하지만 ID나 비밀키 K값을 알지 못하면 정당한 리더로 인증 받을 수 없어 공격에 안전하다. 정당한 태그로 위장하는 경우, 이전 세션에서 도청으로 얻은 정보 S'를 데이터베이스로 이터베이스에서 $S' = S_1 \oplus S_2 = \{(rot_L ID, r_R) + (K_1 \oplus r_T)\} \oplus \{(rot_R ID, r_T) + K_2\}$를 계산하는 과정에서 위장한 태그를 식별해 낼위장한 어스푸핑 공격에 안전하다.

4.1.5 위치추적 공격 (Location Tracking Attack)

위치 추적 공격은 공격자가 태그의 위치변화를 감지하여 태그 소유자의 이동경로를 파악하여 사용자의 프라이버시를 침해하는 공격이다. 태그로부터 매 세션마다 동일한 정보가 나오는 RFID 시스템은 위치추적이 가능하다. 랜덤한 두 개의 태그를 두고 이들을 구별해 낼 수 없으면 불구분성(indistinguishability)을 만족하며 태그의 위치 프라이버시를 보장받을 수 있다. 제안 프로토콜에서는 매 세션마다 r_T, r_R, K 값에 의해 계산된 S'값이 계속해서 바뀌게 되어 이전 세션과 항상 다른 값을 전송하므로 공격자는 특정한 태그를 식별할 수 없으므로 위치추적에 안전하다.

4.1.6 서비스 거부 공격 (Dos Attack ;비동기화 유도 공격(Desynchronization attack))

서비스 거부공격은 RFID시스템의 정상적인 작동을 방해하여 비동기화 문제를 일으키는 방법이다. 또한 악의적으로 리더와 태그사이의 통신을 차단하여 정보 불일치를 유도하는 것이 비동기화 유도공격이다. 제안 프로토콜에서 비동기화 유도공격을 시도하려면 안전하지 못한 태그와 리더 사이에서 S'값이 전송된 후 데이터베이스는 일치하는 태그 인증과정을 거친 후 K_{new}값이 갱신되고 기존 K_{new}의 값은 K_{old} 값으로 바뀌게 된다. 데이터베이스에서 태그로 전송되는 S''를 가로채면 태그에서 K값은 갱신되지 않는다. 데이터베이스는 K_{new}, K_{old}값이 업데이트 되고 태그는 K값이 업데이트 되지 않은 비동기 상태가 된다. 그러나 공격받은 태그는 다음 세션에서 K값을 이용하여 연산한 결과인 S'값을 리더에게 전송하면 데이터베이스에서 K_{new}값이 없을 경우 K_{old}값을 검색하고 이 값을 이용하

여 인증과정을 거쳐서 정상적인 K값을 갱신하는 과정이 진행된다. 따라서 S''의 정보가 차단되더라도 다음 통신 세션에서 데이터베이스에 K_{old}값을 통하여 상호인증을 진행할 수 있어 비동기화 유도공격에 안전하다.

4.1.7 전 방향 안전성 (Forward untraceability)

전 방향 안전성은 공격자가 물리적인 공격을 통하여 어떤 태그의 ID, K값을 알아내더라도 이로부터 이전 세션의 정보를 획득할 수 없어야 한다. 제안 프로토콜에서는 공격자가 물리적 공격을 통하여 ID, K값을 알아내더라도 연속적으로 r_R값을 알고 있으면 전 방향 위치 추적이 가능하지만 한번이라도 r_T, r_R값을 알지 못하면, 즉 K를 갱신하는 체인이 끊기면 다음 세션의 K를 유추할 수 없다. 특정 태그의 r_T값을 연속적으로 도청할 수 있는 시점 까지만 전 방향 위치 추적이 가능하므로 부분적으로 전 방향 안전성을 만족한다고 할 수 있다.

기존 프로토콜과의 안전성 비교분석 결과를 정리하면 [표 1]과 같다. Chien 등의 논문에서 분석결과를 인용하면 LMAP, EMAP, M2AP는 상호인증이 가능하지 않다고 되어 있지만 분석한 결과 상호인증이 가능하다. 기존 연구의 SASI 프로토콜의 경우에 공격자는 IDS, A, B, C, D값을 도청할 수 있고 다음 세션에서 정당한 리더로 가장하여 태그에게 A, B, C값을 보내면 태그에서 이전 세션에서 사용하였던 K1old, K2old 값을 이용하여 n1, n2 값을 연산한다. 이를 이용하여 새로운 K1, K2 값을 생성하고 C를 연산하여 리더를 인증한다. 리더 인증과정을 거친 후 태그는 리더를 가장한 공격자에게 D메시지를 보내고 IDS, K1, K2를 업데이트 과정을 거친다. 이와 같은 공격방법으로 공격자는 태그에게 정당한 리더로 인증 받게 된다. 따라서 SASI 프로토콜은 재전송 공격과 스푸핑 공격에 안전하지 않다. 최근 발표된 Cao등의 논문에서 SASI 프로토콜의 취약성을 지적하고 있다[25]. SASI 프로토콜은 위치 추적 공격, 서비스 거부 공격에 취약하며 전 방향 안전성을 만족하지 않는다. 메시지 변조와 물리적 태그 공격이 가능한 공격자는 특정한 태그를 식별할 수 있어 위치추적이 가능하며 비동기화 문제를 일으켜 정상적인 작동을 방해하는 서비스거부공격에 취약하다. 따라서 [표 1]의 안전성 비교에서 SASI 프로토콜은 재전송 공격, 스푸핑 공격, Dos 공격, 위치추적, 전 방향 안전성에 안전하지 않다.

4.2 효율성 분석

기존에 제안된 해시를 사용하지 않는 초경량 프로토콜(LMAP, M2AP, EMAP, SASI)과 효율성 면에서 비교하면 [표 2]와 같다. 비교요소는 통신량, 태그와 데이터베이스의 저장 공간, 연산종류(xor, ∧, ∨, +, -, rotate, PRNG)에 따른 횟수 등이다. 통신량에서 비교해보면 M2AP와 EMAP가 5L의 크기가 필요하고 LMAP와 SASI는 4L의 크기가 필요하다. 제안된 프로토콜에서는 3L의 크기만 필요하므로 기존 프로토콜에 비해 통신량이 줄어든다. 태그와 데이터베이스의 저장 공간을 비교해보면 LMAP, M2AP, EMAP는 모두 6L의 크기가 필요하고 SASI는 데이터베이스에서 5L의 저장 공간만 필요하나 태그에서 7L의 저장 공간이 필요하다. SASI는 데이터베이스에 ID, IDS, K1, K2를 저장해야 하고 태그에 ID, IDS_{old}, $K1_{old}$, $K2_{old}$, IDS_{next}, $K1_{next}$, $K2_{next}$ 를 저장하여야 한다.

제안 프로토콜에서 데이터베이스에 ID, K_{old}, K_{new}를 저장하므로 3L만큼 저장 공간이 필요하고 태그에서 ID, K를 저장하므로 2L만큼 저장 공간이 필요하다. 제안 프로토콜은 SASI와 비교하여 태그의 저장 공간이 5L 만큼 줄어들어 효율적이다. 데이터베

[표 1] 안전성 비교

(O : 만족, △ : 부분만족, X : 불만족)

	LMAP[18]	EMAP[19]	M2AP[20]	SASI[21]	제안 프로토콜
상호인증	O	O	O	O	O
도청	X	X	X	O	O
재전송	X	X	X	X	O
스푸핑	X	X	X	X	O
Dos(비동기화유도)	X	X	X	X	O
위치추적	X	X	X	X	O
전방향안전성	X	X	X	X	△

〔표 2〕 효율성 비교

(L : 저장 공간, - : 불필요)

		LMAP[18]	M2AP[19]	EMAP[20]	SASI[21]	제안 프로토콜
Total message		4L	5L	5L	4L	3L
Tag memory		6L	6L	6L	7L	2L
DB memory		6L	6L	6L	4L	3L
DB (Reader) operation	xor	14	13	21	10	6
	∧,∨	1	4	4	2	-
	+ , -	9	8	1	4	6
	rotate	-	-	-	2	4
	PRNG	2	2	2	2	1
Tag operation	xor	14	13	20	10	4
	∧,∨	-	2	3	2	-
	+ , -	7	8	-	3	6
	rotate	-	-	-	2	4
	PRNG	-	-	-	-	1

이스에서 연산량을 비교하면 제안 프로토콜은 비트연산의 횟수는 LMAP, M2AP, EMAP에 비해 50% 이상으로 줄어들고 SASI에 비해 26% 정도 줄어든다. rotate 연산은 SASI와 비교하여 2회 많고 랜덤 넘버생성 횟수는 기존 프로토콜에 비해 1회 적다. 태그에서 연산량을 비교하면 제안 프로토콜은 비트연산의 횟수는 LMAP, M2AP, EMAP에 비해 50%이상으로 줄어들고 SASI에 비해 33% 정도 줄어든다. rotate 연산은 SASI와 비교하여 2회 많고 난수생성은 기존 프로토콜은 없지만 1회 생성을 하여야 한다.

제안된 프로토콜은 이전에 제안된 초경량기법들과 비교하였을 때 태그에서 난수생성기 추가를 제외하고 DB와 태그에서 비트연산의 횟수가 감소하였음을 알 수 있다. 물론 난수 생성기를 태그에 추가를 하면 기존의 프로토콜보다는 비용적인 면에서 태그의 비용이 늘어나지만 보안의 취약성을 극복하기 위한 선택적 방법 중의 하나이다. 제안된 프로토콜은 기존에 제안된 해시를 사용하지 않는 초경량 프로토콜에 비해 통신량이 줄어들고 태그와 데이터베이스에서의 저장 공간이 줄어들어 효율적이다. 따라서 제안 프로토콜은 난수생성기를 가지고 있으며 작은 저장 공간과 저 연산의 능력을 가진 태그로 구성된 RFID 시스템에 적합하다.

V. 결 론

최근 저가 태그를 사용한 RFID시스템에 대한 관심이 커지면서 RFID 보안 요구사항이 증대되고 있다. 본 논문에서는 저가 태그 기반의 RFID 시스템에 적용된 기존 제안된 비트연산 기반의 초경량 인증 프로토콜의 취약성을 분석하고 태그에 난수생성을 추가하여 해시를 사용하지 않는 개선된 초경량 인증프로토콜을 제안하였다. 기존에 제안된 초경량 인증 프로토콜이 가지는 보안 취약성을 개선하기 위해 태그에 난수 값과 업데이트된 키 값을 이용하여 연산한다. 매 세션마다 리더에게 전달되는 값이 달라지므로 불구분성을 만족하여 재전송 공격, 스푸핑 공격, 위치추적 공격에 안전하다. 물리적 공격을 통하여 태그에 저장된 정보를 알아내어도 한 번이라도 세션이 끊어지면 다음 세션의 키 값을 알 수 없기 때문에 전 방향 안전성을 부분 만족한다. 데이터베이스와 태그가 동일한 비밀 키를 저장하면서 상호인증 후에 키 값이 업데이트 되므로 서비스 거부 공격이 있더라도 다음 세션에서 데이터베이스에서 이전의 키 값을 찾아 인증을 할 수 있으므로 서비스 거부 공격에도 안전하다. 이전의 초경량 인증 프로토콜과 효율성면에서 비교하여 태그와 데이터베이스에서 통신량과 저장 공간을 줄일 수 있으며 태그와 데이터베이스에서 비트연산의 횟수를 줄여 효율적인 인증 방식이다. 따라서 본 논문에서 제안한 방식은 난수생성기와 작은 저장 공간을 가지는 저 연산 태그가 적용된 RFID 시스템에 적용하여 사용할 수 있다.

참 고 문 헌

〔1〕 K. Finkenzeller, RFID Handbook, John Wiley & Sons, p. 427, May 2003.

〔2〕 S.A. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of

low-cost radio frequency identification systems," Security In Pervasive Computing 2003, LNCS 2802, pp. 201-212, 2004.

[3] 곽민혜, 김광조, "취약성 분석을 통한 경량 RFID 인증 프로토콜 고찰," 2008년도 한국정보보호학회 동계학술대회, pp. 201-208, 2008년 12월.

[4] A. Juels and S.A. Weis, "Authenticating pervasive devices with human protocols," in Advances in Cryptogloy-Crypto '05, LNCS 3126, pp. 293-308, 2005.

[5] 최은영, 이수미, 임종인, 이동훈, "분산시스템 환경에 적합한 효율적인 RFID 인증 시스템," 정보보호학회논문지, 16(2), pp. 25-35, 2006년 12월.

[6] 유성호, 김기현, 황용호, 이필중, "상태기반 RFID 인증 프로토콜," 정보보호학회논문지, 14(6), pp. 57-68. 2004년 12월.

[7] D. Henrici and P. Muller, "Hash-based enhancement of location privacy for radio- frequency identification devices using varying identifiers," Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops. PERCOMW '04, pp. 149-153, Sep. 2004.

[8] M. Ohkubo, K. Suzuki, and S. Kinoshita, "A cryptographic approach to privacy-friendly tag," RFID Privacy Workshop, MIT, Nov. 2003.

[9] G. Avoine and P. Oechslin, "A scalable and. provably secure hash-based RFID protocol," IEEE PerSec 2005, pp. 110-114, Mar. 2005.

[10] J.C. Ha, J.H. Ha, S.J. Moon, and C. Boyd, "LRMAP: Lightweight and resynchronous mutual authentication protocol for RFID System," ICUCT'06, LNCS 4412, pp. 80-89, 2006.

[11] A. Juels, "minimalist cryptography for low-cost RFID tags," In The Fourth International Conferece on Security in Communication Networks- SCN 2004, LNCS 3352, pp. 149-164, 2004.

[12] 하재철, 박제훈, 하정훈, 김환구, 문상재, "검색정보 사전 동기화를 이용한 저비용 RFID 인증방식," 정보보호학회논문지, 18(1), pp. 80-89, 2008년 2월.

[13] A. Juels, "Strenthening EPC tag against coning," in ACM Workshop on Wireless Security (WiSe), pp. 67-76, Nov. 2005.

[14] S. Karthikeyan and M. Nesterenko, "RFID security without extensive cryptography," in Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, pp. 63-67, Nov. 2005.

[15] H.Y. Chien and C.H. Chen, "Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards," in Computers Standard & Interfaces, vol. 29, no. 2, pp. 254-259, Feb. 2007.

[16] J. Bringer, H. chabanne, and E. Dottax, "HB++: A lightweight authentication protocol secure against some attacks," in Proc. IEEE Int' Conf Pervasive Service, Workshop Security, Privacy and Trust in Pervasive and Ubiquitous Computing, pp. 28-33, June 2006.

[17] J. Munilla and A. Peinado, "HB-MP: A further step in the HB-family of lightweight authentication protocols," Computer Networks, vol. 51, no. 9, pp. 2262-2267, June 2007.

[18] P.P. Lopez, J.C.H. Castro, J.M.E. Tapiador, and A. Ribagorda, "LMAP: A real lightweight low-cost RFID tags," Proc. Second Workshop RFID Security, pp. 137 -148, July 2006.

[19] P.P. Lopez, J.C.H. Castro, J.M.E. Tapiador, and A. Ribagorda, "M2AP: A minimalist mutual-Authentication Protocol for Low-Cost RFID Tags," Proc. Int' Conf Ubiquitous Intelligence and Computing(UIC '06), pp. 912-923, Sep. 2006.

[20] P.P. Lopez, J.C.H. Castro, J.M.E. Tapiador, and A. Ribagorda, "EMAP: An efficient mutual authentication protocol for low-cost RFID tags," Proc. OTM

Federated Conf and Workshop: IS Workshop, pp. 352-361, Nov. 2006.

[21] H.Y. Chien, "SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity," IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 4, pp. 337-340, Oct.-Dec. 2007.

[22] T. Li and R.H. Deng, "Vulnerability analysis of EMAP-an efficient RFID mutual authentication protocol," in Proc. Second International Conference, Availability, Reliability, and Security (AReS'07), pp. 238-245, Apr. 2007.

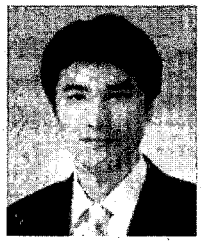
[23] T. Li and G. Wang, "Security analysis of two ultra-lightweight RFID authentication protocols," in Proc. 22nd IFIP TC-11 International Information Security Conference, pp. 109-120, May 2007.

[24] H.Y. Chien and C.W. Hung, "Security of ultra-lightweight RFID authentication protocols and its improvements," ACM Operating System Rev., vol. 41, no. 2, pp. 83-86, July 2007.

[25] T. Cao, E. Bertino, and H. Lei, "Security analysis of the SASI protocol," IEEE Transactions on Dependable and Secure Computing, vol. 6, no. 1, pp. 73-77, Jan.-Mar. 2009.

〈著者紹介〉

전 동 호 (Dong-Ho Jeon) 정회원
2000년 2월: 밀양대학교 컴퓨터공학과 학사
2002년 2월: 경북대학교 정보통신학과 석사
2002년 3월 ~ 현재: 경북대학교 정보보호학과 박사과정
〈관심분야〉 RFID/USN, 네트워크 보안, 정보보호



김 영 재 (Young-Jae Kim) 학생회원
2008년 2월: 경북대학교 전자전기컴퓨터학부 학사
2008년 3월 ~ 현재: 경북대학교 정보보호학과 석사과정
〈관심분야〉 RFID/USN, 정보보호

권 혜 진 (Hye-Jin Kwon) 학생회원
2007년 2월: 경북대학교 수학과 학사
2009년 2월: 경북대학교 정보보호학과 석사
2009년 3월 ~ 현재: 경북대학교 전자공학과 박사과정
〈관심분야〉 RFID/USN, 인증 및 암호기술, 정보보호

정 선 영 (Sun-Young Jung) 학생회원
1987년 2월: 경북대학교 전자공학과 학사
2003년 2월: 경북대학교 정보통신학과 석사
2003년 3월 ~ 현재: 경북대학교 정보통신학과 박사과정
2009년 3월~현재: 경운대학교 디지털전자공학과 전임강사
〈관심분야〉 유비쿼터스, 정보보호

김 순 자 (Soon-Ja Kim) 종신회원
1975년 2월: 경북대학교 수학 교육학과 학사
1977년 2월: 경북대학교 수학과 석사
1988년 2월: 계명대학교 수학과 박사
1993년 4월 ~ 현재: 경북대학교 전자·전기 공학부 교수
〈관심분야〉 정보보호 및 보안기술, 정보보호 응용기술