RFID 시스템에서 DoS 공격을 포함한 다양한 공격에 대처하는 인증 기법

An Authentication Scheme against Various Attacks including DoS Attack in RFID System

이 규 환, 김 재 현*
(Kyu Hwan Lee and Jae Hyun Kim)

Abstract: The RFID system is very useful in various fields such as the distribution industry and the management of the material, etc. However, the RFID system suffers from various attacks since it does not have a complete authentication protocol. Therefore, this paper propose the authentication protocol that used key server to resist various attacks including DoS(Denial of Service) attack. For easy implementation, the proposed protocol also uses CRC, RN16 generation function existing in EPCglobal class 1 gen2 protocol. This paper performed security analysis to prove that the proposed protocol is resistant to various attacks. The analytical results showed that the proposed protocol offered a secure RFID system.

Keywords: RFID, Security, Authentication, Key

I. 서론

RFID(Radio Frequency IDentification)란 사물(objects)에 부착된 전자 태그(tags)로부터 무선 주파수를 이용하여 태그 내에 저장되어 있는 태그의 *ID*나 주변 환경 정보(센싱정보)를 송수신하여 기존 IT 시스템과 실시간으로 정보를 교환하고 이를 처리하는 기술을 의미한다. 이러한 RFID 시스템을 이용하면 각종 물품에 전자태그를 부착해 스캐너로 하나씩 읽을 필요 없이 이동 시 자동으로 물품 명세와 가격, 유통경로 및 기한 등을 파악할 수 있기 때문에 유통 및 물류 분야뿐 아니라 자재관리나 인력 관리등에 RFID 시스템이 많이 사용되고 있다. 그러나 RFID 시스템은 EPC code가 암호화 되어 전송되지 않고, 리더-태그 간 상호 인증을 제공하지 않기 때문에 다양한 공격에 노출 되기 쉽다. 또한 고정된 *ID*를 사용하게 되면 고정된 *ID*를 이용하여 태그의 위치를 추적할 수 있기 때문에 개인의 사생활 침해를 야기 시킬 수 있다[1].

이러한 문제점을 해결하기 위하여 데이터베이스(Database)와 태그가 *ID*또는 공유키를 공유하고, Session마다 새롭게 *ID* 또는 인증키를 갱신하는 방법을 사용하는 인증기법들이 제안 되었다[2]-[5]. 하지만 기존의 기법들은 RFID시스템에서 구현이 어렵고, 태그가 *ID* 또는 인증키를 갱신하는 과정에서 악의적인 노드가 DoS공격을 실행하여 그 과정을 방해하게 된다면 태그와 데이터베이스 간에 ID 또는 인증키의 비동기화가 발생할 수 있다.

* 책임저자(Corresponding Author)
논문접수 : 2008. 08. x., 채택확정 : 2008. 08. xx.
이규환, 김재현 : 아주대학교 전자공학과
(lovejiyoon7@ajou.ac.kr , jkim@ajou.ac.kr)
※ 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업(IITA-2008-C1090-0801-0003)의 연구 결과와 "건설생산성 향상을 위한 건설자재 표준화 연구" (과제번호 : 06기반구축A02)의 일환으로 국토해양부 건설기술기반구축사업의 연구비지원에 의해 수행되었음

그러므로 본 논문에서는 구현의 용이함을 위해 EPCglobal class 1 Gen2 프로토콜의 *CRC*(Cyclic redundancy check)함수와 *RN16*(16-bit random or pseudo-random number)생성 함수를 사용하여 인증을 수행하고, 기존의 RFID 시스템에서의 발생할 수 있는 보안 문제 뿐 아니라 DoS 공격을 감지하여 대처할 수 있는 인증 프로토콜을 제안한다.

본 논문의 구성을 살펴보면 Ⅱ장에서는 기존의 RFID 시스템에서의 인증 프로토콜을 살펴보고, Ⅲ장에서는 RFID 시스템에서 DoS공격을 포함한 다양한 공격에 대하여 대처 가능한 프로토콜을 제안하며 Ⅳ장에서 제안하는 인증프로토콜의 Security 분석을 수행 하고 Ⅴ장에서 결론을 맺는다.

II. 관련 연구

RFID 시스템의 보안을 강화하기 위하여 hash 함수를 이용한 여러 가지 인증 기법들이 제안되었다[2]-[5].

Hash locked 프로토콜[2]은 태그가 자신의 *ID*를 hashing한 *MetaID*를 이용하여 인증을 수행하며, 태그는 인증이 되기 전에는 lock 상태로 있다가 인증을 수행하면 unlock상태로 변환하여 태그 자신의 *ID*를 리더에게 전송한다. 그러나 Hash locked 프로토콜에서는 *MetaID*를 사용하여 *ID*를 숨길 수는 있지만 고정된 *MetaID*를 사용하기 때문에 태그 추적이 가능해지고, 인증과정에서 인증키와 *ID*가 암호화 되어 전송되지 않기 때문에 악의적인 노드에게 노출 될 수 있다. 또한 *MetaID*를 통한 spoofing공격이 가능하고, 리더-태그 간 상호 인증을 수행하지 않는다. Randomized hash lock 프로토콜[2]은 고정된 *ID*로 인한 태그 추적을 방지하기 위하여 매회 인증 과정마다 랜덤변수를 이용한 다른 *MetaID*를 사용한다. 하지만 Randomized hash lock 프로토콜에서는 태그 추적을 방지할 뿐 Hash locked 프로토콜과 같은 문제점이 발생한다.

Henrici가 제안한 인증 프로토콜[3]은 태그 추적 방지와 보안의 향상을 위하여 태그와 데이터베이스(DataBase)간에 *ID*와 *Session number*를 공유하며 session마다 *ID*와 *Session number*

의 갱신을 수행하고 Hash 함수를 이용하여 메시지의 무결성을 제공하는 인증을 수행한다. 하지만 Henrici가 제안한 인증 프로토콜에서는 리더-태그 간에 상호인증이 제공되지 않기 때문에 악의적인 노드가 리더 행세를 하여 태그의 메시지를 spoofing 할 수 있고, EPCgloabl Class 1 Gen2 프로토콜에 대한 고려를 하지 않았기 때문에 구현하기 어렵다.

Dimitriou가 제안한 인증 프로토콜[4]은 태그와 데이터 베이스 간에 *ID* 공유와 매회 *ID* 갱신을 수행 할 뿐 아니라 리더-태그 간 인증을 통하여 spoofing 공격을 방지 할 수 있고, keyed hash 함수를 사용하여 보안을 향상 시켰다. 그러나 Dimitriou가 제안한 인증 프로토콜은 *ID*를 갱신할 때 다른 태그의 *ID*와 충돌할 가능성이 있다. 예를 들어 $h(A) = B$, $h(B) = D$라 하고, 두 개의 태그가 *ID*를 *A*와 *B*를 가질 때 *ID*가 *A*인 태그가 *ID*를 갱신하여 *B*가 되면 두개의 *ID*가 같으므로 충돌이 발생한다. 또한, Henrici가 제안한 인증 프로토콜과 마찬가지로 EPCglobal class 1 Gen2 프로토콜을 고려하지 않았기 때문에 구현하기 어렵다.

Duc이 제안한 인증 프로토콜[5]은 EPCglobal class 1 Gen2 프로토콜을 고려하여 EPCglobal class 1 Gen2 프로토콜에 있는 *RN16*생성 함수와 *CRC*함수를 이용하여 인증 메시지를 생성하고, 태그와 데이터베이스 간에 *EPC code*와 인증키를 공유하여 리더-태그 간 상호 인증을 수행한다. Duc이 제안한 인증 프로토콜은 기존의 RFID 시스템에서 발생 할 수 있는 보안의 문제점들을 해결 할 뿐 아니라 EPCglobal class 1 Gen 2 프로토콜도 고려했지만 다음과 같은 문제점이 발생한다. 우선, 데이터베이스에서 태그의 *(EPC, K_i)*를 찾기 위해서 brute force method를 사용해야 하므로 손실 되는 시간이 많다. 또한 인증 메시지인 *M*에 여러 개의 *(EPC, K_i)*가 존재하기 때문에 여러 번 인증을 수행해야 하므로 생기는 오버헤드도 크다.

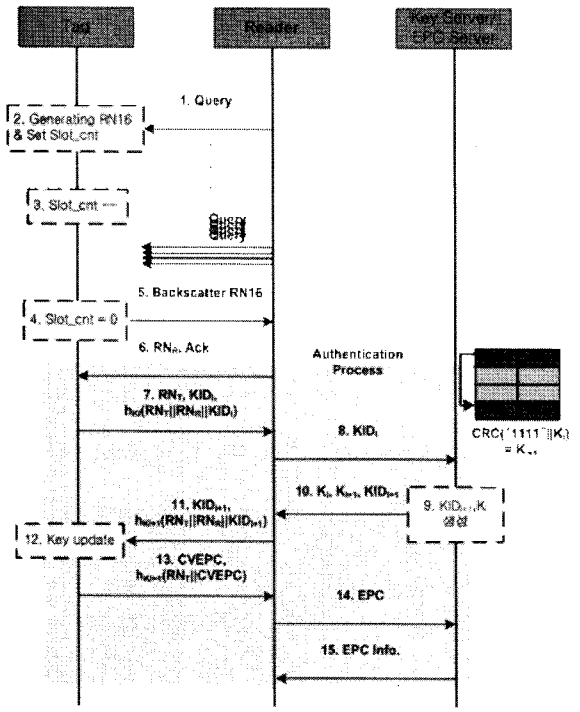

그림 1. 제안 하는 인증 프로토콜의 수행 과정

Fig. 1. The procedure of the proposed authentication protocol

표 1. 제안하는 인증 프로토콜에서 사용하는 파라미터

Table 1. The parameters of the proposed authentication protocol

Parameter	Description
KID	인증키 *K*의 *ID*
K_i	현재 세션에 사용하는 인증 키
K_{i+1}	다음 세션에 사용하는 인증 키
RN_X	*X*에서 생성한 랜덤상수
CVEPC	*EPC* xor *K*
$h_K(M)$	*CRC(K,M)*

앞에서 설명한 여러 가지 인증 프로토콜들은 공통적으로 태그가 ID 또는 인증키를 갱신하는 과정에서 악의적인 노드가 DoS공격을 실행하여 그 과정을 방해 하면 데이터베이스와 태그 간에 인증키나 ID의 비동기화(Desyncronization)가 발생할 수 있다. 그리고 RFID 시스템에 대한 고려가 적고 현실적으로 구현하기가 어렵다. 그러므로 본 논문에서는 EPCglobal class 1 Gen2 프로토콜에 기초하여 기존의 RFID 시스템에서의 발생할 수 있는 보안 문제 뿐 아니라 DoS 공격을 감지하여 대처할 수 있는 인증 프로토콜을 제안한다.

III. 제안하는 인증 프로토콜

제안하는 인증 프로토콜은 구현의 용이함을 위하여 EPCglobal class 1 Gen2 프로토콜에 존재하는 *CRC*함수와 *RN16*생성 함수[6]를 사용하여 인증을 수행하고 DoS공격에 의한 *ID* 또는 공유키의 비동기화를 방지하기 위하여 타임아웃*(Time-out)*기법과 Key server를 이용한다. Key server는 KID_i에 해당하는 비밀키 K_i를 소유하고 있을 뿐, 태그와 비밀키가 동기화 되어 있지 않기 때문에 DoS 공격에 의한 *ID* 또는 공유키의 비동기화를 방지 할 수 있다. 제안하는 인증 프로토콜의 동작과정은 그림 1과 같다. 제안하는 인증 프로토콜은 리더가 다수의 태그를 인식하는 과정에서 하나의 태그가 자신의 *RN16*을 backscattering하여 리더가 하나의 태그를 인식한 후부터 진행된다. 인증에서 사용되는 파라미터는 표 1과 같고 인증 과정은 다음과 같다.

단계1: 리더는 인증 시작을 알리는 *ACK*와 RN_R을 태그에게 전송한다. 이때 RN_R은 리더에서 생성한 *RN16*을 의미한다.

$$R \rightarrow T : RN_R, ACK \tag{1}$$

단계2: 메시지 (1)을 받은 태그는 다음과 같은 인증요청 메시지를 보낸다.

$$T \rightarrow R : RN_T, KID_i, h_{k_i}\left(RN_T, RN_R, KID_i\right) \tag{2}$$

RN_T는 태그에서 생성한 *RN16*을 의미하고, KID_i는 비밀키 K_i의 *ID*를 의미한다. KID_i는 Key server에서 K_i 정보획득에 사용한다. $h_{k_i}(M)$ 은 $CRC(K_i||M)$한 값으로 메시지의 무결성(integrity)과 인증에 사용한다.

단계3: 태그의 인증요청 메시지를 받은 리더는 KID_i를 이

용하여 K_i, K_{i+1}, KID_{i+1}의 정보를 Key server에서 획득하여 메시지의 $h_{k_i}(RN_T, RN_R, KID_i)$ 값을 확인하여 본다. 이때, Key server에서는 식 (3)과 같은 과정을 통하여 K_{i+1}과 KID_{i+1}을 계산 할 수 있다. 리더는 인증요청 메시지를 보낸 태그가 합법적인 태그라고 판단하면 인증응답 메시지를 생성하여 전송하고, 타임아웃확인을 위한 타이머를 작동 시킨다.

$$K_{i+1} = CRC("1111" \| K_i) \tag{3}$$

$$R \rightarrow T : KID_{i+1}, h_{k_{i+1}}(RN_T, RN_R, KID_{i+1}) \tag{4}$$

단계4: 리더의 인증응답 메시지를 받은 태그는 K_{i+1}을 계산하여, $h_{k_{i+1}}(RN_T, RN_R, KID_{i+1})$ 을 확인해 보고, 합법적인 리더라고 판단하면 K_i와 KID_i를 각각 K_{i+1}과 KID_{i+1}로 갱신하고 다음과 같은 태그 *ID* 메시지를 리더에게 전송한다.

$$T \rightarrow R : CVEPC, h_{k_{i+1}}(RN_T, CVEPC) \tag{5}$$

*CVEPC*는 *EPC code*와 K_{i+1}을 xor한 값이다.

단계5: 태그의 *ID* 메시지를 받은 리더는 *CVEPC*에서 *EPC*를 계산하여 상품 정보를 획득하고, 다른 태그의 인식을 수행한다. 이때 타임아웃이 발생할 때까지 태그의 *ID* 메시지가 도착하지 않으면 리더는 악의적인 노드의 DoS 공격 또는 채널 에러라 인식하고 단계3부터 다시 시작한다.

IV. Security 분석

본 절에서는 다양한 공격 유형들을 고려하고, 제안한 인증 프로토콜이 이러한 공격들을 어떻게 방어할 수 있는지에 대하여 서술하고 제안한 프로토콜의 안전성을 평가한다.

1. 속임수 공격(Spoofing Attack)

spoofing 공격은 노드 간에 이미 전송된 메시지를 가로채어 수집하여 두었다가 공격자가 이를 그대로 사용하는 공격 유형이다. 제안하는 인증 프로토콜에서는 session 마다 비밀키 *K*가 갱신되기 때문에 리더는 $h_{k_i}(RN_T, RN_R, KID_i)$을 확인해 보고 메시지의 spoofing을 감지할 수 있고 *CVEPC* 메시지를 가로채여 그대로 사용하려 하여도 *CVEPC*는 session마다 다른 비밀키 *K*값을 이용해 생성 되기 때문에 악의적인 노드가 *CVEPC*를 spoofing하여 사용 할 수 없다.

2. 위치 추적(Traceability)

위치추적은 태그의 고정된 아이디를 이용하여 태그의 위치를 추적하는 공격이다. 제안하는 인증 프로토콜에서는 session마다 비밀키 *K*값이 갱신되고 매회 새로운 random number를 생성하기 때문에 태그에서 전송하는 RN_T, KID_i, $h_{k_i}(RN_T, RN_R, KID_i)$ 메시지와 *CVEPC*가 session마다 다른 값을 가지게 된다. 그러므로 태그에서 전송하는 메시지를 통한 태그의 위치 추적은 불가능하다.

3. 메시지 변조 공격(Modification attack)

메시지 변조 공격은 악의적인 노드가 임의로 메시지의 일부분을 수정하는 공격 유형이다. 제안하는 인증 프로토콜에서는 악의적인 노드가 태그나 리더의 메시지를 가로채서 변조 하여도 *hash*값의 무결성 확인을 통하여 메시지 변조를 확인 할 수 있다.

4. 도청(Eavesdropping)

도청은 무선으로 전송되는 데이터의 내용을 공격자가 가로채어 살펴보는 것을 의미한다. 하지만 제안하는 인증 프로토콜에서의 *EPC*는 비밀키 *K*와 xor 연산을 통하여 *CVEPC*로 전송 되기 때문에 도청을 하여도 *EPC*코드를 알 수 없다.

5. 서비스거부 공격(DoS attack)

서비스거부 공격은 대량의 데이터 패킷을 통신망으로 보내서 시스템의 정상적인 동작을 방해하는 공격 수법이다. 하지만 제안하는 인증 프로토콜에서는 그림 2에서 설명된 것처럼 타임아웃기법을 사용하여 DoS 공격을 감지하여 인증 과정을 다시 수행하기 때문에 DoS 공격에 대처할 수 있다.

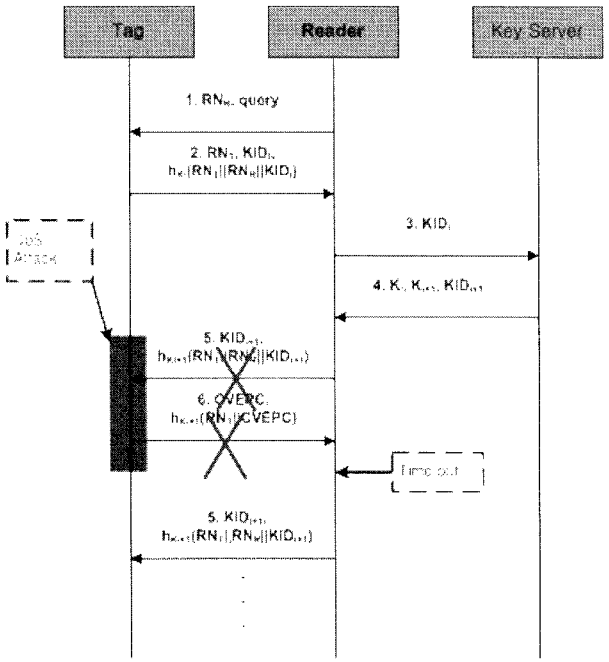

그림 2. 제안하는 인증 프로토콜에서의 DoS 공격에 대처하는 과정

Fig. 2. The procedure against DoS attack in the proposed authentication protocol

V. 결 론

본 논문에서는 DoS공격에 대처 가능한 인증 프로토콜을 제안했다. 제안하는 인증 프로토콜은 EPCgloabal class 1 Gen2 프로토콜에 존재하는 *CRC*함수와 *RN16*생성 함수를 사용하여 인증을 수행하기 때문에 구현에 용이하고 타임아웃기법과 Key server를 사용하여 DoS공격에 의한 *ID* 또는 공유키의 비동기화를 감지하여 대처할 수 있다는 장점이 있다.

제안하는 인증 프로토콜의 Security 분석 결과, 제안하는 인증 프로토콜이 다양한 공격 유형에 대하여 강한 면모를 가지고 있음을 보였다. 그러므로 본 논문에서 제안한 인증 프로토콜은 RFID 시스템에서 안전한 인증 프로토콜로 사용될 수 있을 것으로 기대된다.

참고문헌

[1] A. Juels,"RFID Security and Privacy: A reserch Survey," *IEEE Journal on Selected Areas in Communications*, VOL 24, NO. 2, Feb 2006.

[2] S. Weis, S. Sarma, R. Rivest and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," *Proc. of the First International Conference on Security in Pervasive Computing*, 2003.

[3] D. Hentici and P. Muller,"Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers," *Proc. of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, 2004.

[4] T. Dimitriou, "A Lightweight RFID Protocol to protect against Traceability and Cloning attacks," *Proc. of the First International Conference on Security and Privacy for Emerging Areas in Communiations Networks*, 2006.

[5] D. N. Duc, J. Park, H. Lee, K. Kim,"Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning," *Proc. of the Symposium on Cryptography and Information Security*, 2006

[6] EPCglobal Inc., "Class 1 Generation 2 UHF Air Interface Protocol Standard Version 1.09", 2005.

이 규 환

2007년 아주대학교 전자공학부(공학사). 2007년 ~ 현재 아주대학교 대학원 전자공학과 석사과정 재학 중. 관심분야는 WPAN에서의 보안, 인증, Wireless LAN, Ad-hoc, Mesh network, RFID등임

김 재 현

1991년 한양대학교 전자계산 학과(공학사). 1993년 한양대학교 전자계산 학과(공학석사). 1996년 한양대학교 전자계산 학과(공학박사). 1997년 ~ 1998년 UCLA 전기과 Postdoc 연구원. 1997년 ~ 1998년 IRI Corp. CA, USA. 1998년 ~ 2003년 Bell Labs, Lucent Tech. NJ, USA. 2003년 ~ 현재 아주대학교 정보통신대학 전자공학부 부교수. 관심분야는 무선 인터넷 QoS, MAC 프로토콜, IEEE 802.11/15/16/20, RFID등임