EPCglobal RFID 시스템에서 Key server를 사용하는 인증 프로토콜

준회원 이 규 환*, 정회원 김 재 현*

An Authentication Protocol using the key server in the EPCglobal RFID System

Kyu-Hwan Lee *Associate Member*, Jae-Hyun Kim *Regular Member*

요 약

본 논문에서는 EPCglobal RFID 시스템에서 Key server를 사용하는 인증 프로토콜을 제안한다. 제안하는 인증 프로토콜은 RFID 시스템에서 발생할 수 있는 보안적 문제점들과 DoS공격에 대처하기 위하여 Key server를 사용하고, 구현의 용이함을 위하여 추가적인 hash함수 등의 구현 없이 EPCgloal class 1 gen 2 프로토콜에서 제공하는 함수를 이용한다. 본 논문에서는 성능 분석을 위하여 GNY 분석과 Security 분석을 수행하였다. 우선 GNY 분석을 통하여 프로토콜의 신뢰성을 증명하였으며, Security 분석을 통하여 제안하는 인증 프로토콜이 DoS공격을 포함한 다양한 공격에 안전하다는 것을 보였다. 이러한 성능 분석 결과, 제안하는 인증 프로토콜은 안전한 RFID 시스템을 제공한다는 것을 입증할 수 있었다.

Key Words : RFID, Security, Authentication, EPCglobal class 1 gen2

ABSTRACT

This paper proposes an authentication protocol using the key server in the ECPglobal RFID system. The proposed authentication protocol uses the key server and the time-out mechanism to resist various attacks including DoS(Denial of Service) attack. For easy implementation, the proposed protocol also uses the function existing in EPCglobal class 1 gen2 protocol without additive function such as hash function. The proposed protocol is evaluated through two analytical methods. The correctness of the proposed protocol is proved using the GNY analysis. By the security analysis, this paper showed that the proposed protocol is resistant to various attacks including DoS attack. The analytical results demonstrated that the proposed protocol offered a secure RFID system.

Ⅰ. 서 론

RFID(Radio Frequency IDentification)란 사물(objects)에 부착된 전자 태그(tags)로부터 무선 주파수를 이용하여 태그 내에 저장되어 있는 태그의 ID나 주변 환경 정보(센싱정보)를 송·수신하여 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,

※ 본 연구는 한국전자재시험연구원에서 주관하는 "건설생산성 향상을 위한 건설자재 표준화 연구" (과제번호 : 06기반구축A02)의 일환으로 국토해양부 R&D정책·인프라사업의 연구비지원에 의해 수행되었습니다.
* 아주대학교 전자공학과 무선 인터넷 연구실({lovejiyoon7 and jkim}@ajou.ac.kr)
논문번호 : #KICS2009-03-080, 접수일자 : 2009년 3월 2일, 최종논문접수일자 : 2009년 10월 15일

유통경로 및 기한 등을 파악할 수 있기 때문에 유통 및 물류 분야뿐 아니라 자재관리나 인력 관리 등에 RFID 시스템을 많이 사용하고 있다[1]. 그러나 RFID 시스템은 전자상품코드(EPC : Electronic Product Code)가 암호화되어 전송되지 않고, 리더-태그 간 상호 인증을 제공하지 않기 때문에 다양한 공격에 노출되기 쉽다. 또한 고정된 태그 ID를 사용하게 되면 고정된 ID를 이용하여 태그의 위치를 추적할 수 있기 때문에 개인의 프라이버시 침해를 야기 시킬 수 있다[2].

이러한 문제점을 해결하기 위하여 데이터베이스(Database)와 태그가 ID 또는 공유키를 공유하고, Session마다 새롭게 ID 또는 인증키를 갱신하는 방법을 사용하는 인증기법들이 제안 되었다[4]-[9]. 그러나 기존의 기법들을 RFID시스템에서 적용하기 위해서는 태그와 리더에 추가적으로 hash함수를 구현해야 되고, 태그가 ID 또는 인증키를 갱신하는 과정에서 악의적인 노드가 DoS공격을 실행하여 그 과정을 방해하게 된다면 태그와 데이터베이스 간에 ID 또는 인증키의 비동기화가 발생할 수 있다.

그러므로 본 논문에서는 구현의 용이함을 위해 추가적인 함수 구현 없이 EPCglobal class 1 gen2 (Gen2) 프로토콜의 함수를 사용하여 인증을 수행하고, 기존의 RFID 시스템에서 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, Ⅲ장에서 Gen 2프로토콜에서의 보안상 문제점을 분석한다. Ⅳ장에서는 EPCglobal RFID 시스템에서 Key server를 사용하는 인증 프로토콜을 제안하고 Ⅴ장에서 제안하는 인증프로토콜을 분석하며 Ⅵ장에서 결론을 맺는다.

Ⅱ. 관련 연구

RFID 시스템의 보안을 강화하기 위하여 hash 함수를 이용한 여러 가지 인증 기법들[4]-[9]이 제안되었다.

2.1 Hash locked 프로토콜

Hash locked 프로토콜[4]은 태그가 자신의 *ID*를 hashing한 *MetaID*를 이용하여 인증을 수행하며, 태그는 인증이 되기 전에는 lock 상태로 있다가 인증을 수행하면 unlock 상태로 변환하여 태그 자신의 ID를 리더에게 전송한다. 그러나 Hash locked 프로토콜에서는 *MetaID*를 사용하여 *ID*가 노출되는 것을 방지할 수 있지만 고정된 *MetaID*를 사용하기 때문에 태그 위치 추적이 가능하다. 또한, 인증키와 *ID*가 암호화 되어 전송되지 않고 리더-태그 간 상호 인증을 수행 하지 않기 때문에 악의적인 노드의 도청이나 속임수 공격 등의 다양한 공격에 노출될 수 있다.

2.2 Randomized hash lock 프로토콜

Randomized hash lock 프로토콜[4]은 고정된 *ID*로 인한 태그 추적을 방지하기 위하여 매회 인증 과정마다 랜덤변수를 이용한 다른 *MetaID*를 사용한다. 그러나 Randomized hash lock 프로토콜에서는 태그 추적을 방지할 뿐 Hash locked 프로토콜과 같이 인증키의 도청이나 속임수 공격 등의 다양한 공격에 노출되기 쉽다.

2.3 Henrici의 인증 프로토콜

Henrici가 제안한 인증 프로토콜[5]은 태그 위치 추적 방지와 보안의 향상을 위하여 태그와 데이터베이스 간에 *ID*와 *Session number*를 공유하고 session마다 *ID*와 *Session number*를 갱신을 수행하며 hash 함수를 이용하여 메시지의 무결성을 제공하는 인증을 수행한다. 하지만 Henrici가 제안한 인증 프로토콜에서는 리더-태그 간에 상호인증이 제공되지 않기 때문에 악의적인 노드가 합법적인 리더 행세를 하는 속임수 공격이 발생할 수 있다.

2.4 Dimitriou의 인증 프로토콜

Dimitriou가 제안한 인증 프로토콜[6]은 태그와 데이터베이스 간에 *ID*를 공유하고 매회 *ID* 갱신을 수행 할 뿐만 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 충동할 가능성이 있다.

2.5 Duc과 Cai의 인증 프로토콜

Duc이 제안한 인증 프로토콜[7]과 Cai가 제안한 인증 프로토콜[8]은 기존의 RFID 시스템의 표준 문서를 고려하여 RN16 생성함수와 CRC함수를 이용하여 인증 과정을 수행한다. Duc이 제안한 인증 프로토콜은 기존의 RFID 시스템에서 발생할 수 있는 보안의 문제점들을 해결할 뿐만 아니라 기존의 RFID 시스템의 표준 문서도 고려했지만 리더 인증을 수행하지 않기 때문에 속임수 공격에 취약하다.

또한 인증 과정에서 손실 되는 시간이 많다. Cai가 제안한 인증 기법은 EPCglobal RFID 시스템에서 간단한 태그-리더 간 상호 인증을 제공한다. 하지만 Cai가 제안한 인증 기법은 메시지의 무결성을 제공하지 않기 때문에 메시지 변조 공격에 취약하다.

2.6 SPA 프로토콜

SPA[9]는 비밀 키 탐색의 효율을 높이기 위하여 트리 기반 키 분배를 사용하고 비밀 키 유출을 방지하기 위해 주기적인 비밀 키 갱신을 수행하지만 메시지의 무결성을 제공하지 않기 때문에 메시지 변조 공격에 취약하다. 기존 인증프로토콜들의 안전성 평가는 표 1에 정리되어 있다.

2.7 기존 인증기법들의 문제점 분석

앞에서 설명한 데이터베이스와 태그가 인증키를 공유하는 방식의 인증 프로토콜들은 공통적으로 그림 1에서 보는 것과 같이 태그가 *ID* 또는 인증키를 갱신하는 과정에서 악의적인 노드가 DoS공격을 실행하여 그 과정을 방해하면 데이터베이스에서는 인증키나 *ID*가 갱신되는데 태그에서는 갱신되지 않아서 데이터베이스와 태그 사이에 인증키 또는 *ID*의 비동기화가 발생할 수 있다. 또한, 앞서 설명한 대다수의 인증프로토콜들은 태그 인증에 앞서 하나의 태그를 인식(singulation)하는 과정들은 고려하지 않았고, 기존의 표준 RFID 프로토콜에 적용하기 위하여 추가적으로 hash함수 등을 구현해야한다. 그러므로 본 논문에서는 추가적인 함수 구현 없이 표준 RFID 프로토콜인 Gen 2 프로토콜의 함수를 이용하여 RFID 시스템에서의 발생할 수 있는 보안 문제 뿐 아니라 DoS 공격을 방지하는 인증 프로토콜을 제안한다.

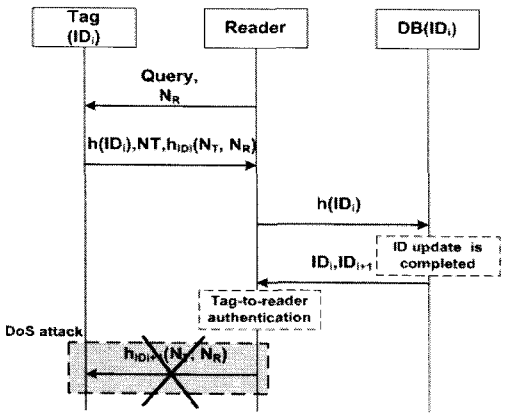


그림 1. DoS 공격에 의해 비동기화가 발생하는 예

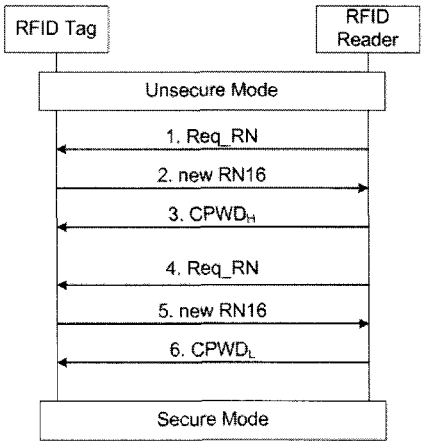


그림 2. EPCglobal class 1 gen2에서 Access command 수행 과정

Ⅲ. EPCglobal class 1 gen 2 프로토콜에서의 보안

Gen2 프로토콜에서는 RFID 시스템의 보안을 위하여 기본적으로 Secure state를 지원한다[3]. Gen2 프로토콜에서는 태그가 리더에게 *EPC code*를 backscattering하여 리더가 태그의 *EPC code*를 인식한 상태인 Open state와 [*read/write/lock command*]를 수행할 수 있는 Secure state가 존재하는데 Open state에서 Secure state로 전환하기 위해서는 [*Access command*]를 태그에게 보내 인증 과정을 수행해야 한다. 인증 과정은 그림 2와 같다. 인증과정에서 [*Req_RN*]은 *RN16* 값을 요청하는 메시지를 의미하고, *RN16*은 16bit random number(16bit의 임의상수)를 의미한다. 그리고 *CPWD*는 태그의 *Access password*와 *RN16*을 XOR 연산한 것을 의미한다. 인증과정은 *Access password*가 32bit이기 때문에 MSB와 LSB로 나누어서 두 번 인증을 수행한다. 그러나 Gen2 프로토콜에서 제공하는 Secure state는 다음과 같은 문제점들을 가지고 있다. *EPC code*가 backscattering되는 과정에서 *EPC code*는 암호화 되어 있지 않기 때문에 그대로 *EPC code*가 악의적인 노드에게 노출 될 수 있고, [*Access command*]를 인증하는 과정에서 *RN16* 메시지가 암호화 되어 전송되지 않기 때문에 *Access password*가 악의적인 노드에게 노출될 수 있다. 또한, Gen2 프로토콜에는 리더-태그 상호 인증을 제공하지 않기 때문에 신뢰할 수 있는 인증이라 볼 수 없다.

Ⅳ. 제안하는 인증 프로토콜

표준문서에서는 리더가 다수의 태그를 인식하기 위하여 태그들에게 [query]를 전송하면 태그들은 *RN16*을 생성하고 *RN16*값을 이용하여 *Slot_cnt*을 결정한다. 태그의 *Slot_cnt*가 결정되면 이후 리더에게 [query]를 수신할 때마다 태그는 *Slot_cnt*를 1씩 감소시키고 *Slot_cnt*가 0이 되면 자신의 *RN16*값을 backscattering하고 *RN16*을 수신한 리더는 그 태그를 인식한다[3]. 제안하는 인증 프로토콜은 리더가 다수의 태그를 인식하는 과정에서 하나의 태그가 자신의 *RN16*값을 backscattering하여 리더가 하나의 태그를 인식한 후부터 진행된다. 리더와 EPC 서버 간에는 상호인증이 되어 있다고 가정한다. 그림 3은 Key server에서 Key table의 구조를 나타낸다. K_i는 32bit의 비밀 키를 나타낸다. K_i가 32bit인 이유는 CRC함수의 결과 값이 16bit이기 때문에 16배수 값을 가져야한다. 보안성 향상을 위하여 K_i는 48bit나 64bit등으로 16배수의 값을 가질 수 있다. KID_i는 Key table에서 K_i의 인덱스를 나타낸다. KID_i는 Key server에서 Key table 생성 시 임의로 생성한다. i는 K_i와 KID_i의 Key server에서의 인덱스를 나타낸다. 다음 세션의 비밀 키는 16bit 단위로

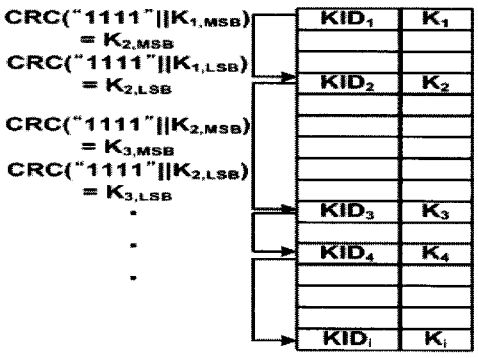


그림 3. Key server에서의 Key table의 구조

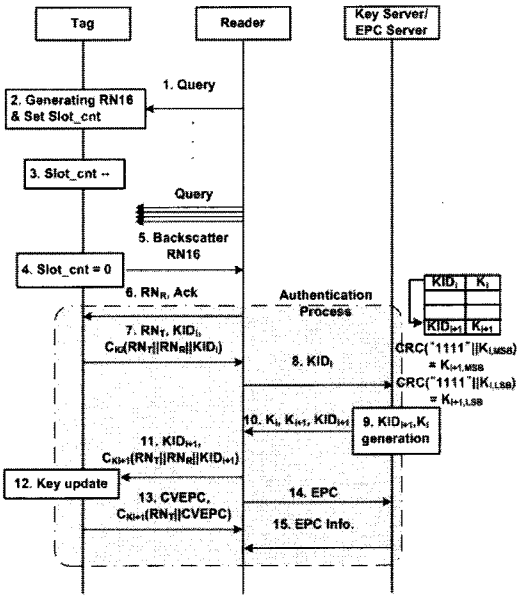


그림 4. 제안하는 인증 프로토콜의 수행 과정

MSB(Most Significant Bit)와 LSB(Least Significant Bit)로 나뉘어 CRC("any constant"|| secret key of current session, K_i)에 의해 계산된다. ||은 메시지의 접합을 의미한다. 본 논문에서는 any constant를 "1111"이라 가정한다. "1111"의 bit를 추가하는 이유는 K_i의 bit수가 CRC 함수의 remainder보다 작기 때문이다. CRC함수의 remainder는 16bit의 결과 값을 내기 위하여 17bit이다. 그림 4는 제안하는 인증 과정을 나타내며 자세한 과정은 다음과 같다.

단계1: 리더(R)는 인증 시작을 알리는 *ACK*와 RN_R을 태그(T)에게 전송한다. 이때 RN_R은 리더에서 생성한 *RN16*을 의미한다.

$$R \rightarrow T: RN_R, ACK \quad (1)$$

단계2: 메시지 (1)을 받은 태그는 다음과 같은 인증

표 1. 기존 인증 프로토콜들의 안전성 평가

인증기법	속임수공격	위치추적	메시지변조	도청	서비스거부공격에 의한 비밀 키 갱신 실패
Hash-locked 프로토콜	X	X	X	X	-
Randomized Hash-locked 프로토콜	X	O	X	X	-
Henrici의 프로토콜	X	O	O	O	X
Dimitriou의 프로토콜	O	O	O	O	X
Duc의 프로토콜	X	O	O	O	X
Cai의 프로토콜	O	O	X	O	X
SPA 프로토콜	O	O	X	O	X

요청 메시지를 보낸다.

$$T \rightarrow R: RN_T, KID_i, C_{k_i}(RN_T, RN_R, KID_i) \quad (2)$$

RN_T는 태그에서 생성한 $RN16$을 의미하고, KID_i는 비밀키 K_i의 ID를 의미한다. KID_i는 Key server에서 K_i 정보획득에 사용한다. $C_{k_i}(M)$은 $CRC(K_i||M)$ 값으로 메시지의 무결성과 인증에 사용한다.

단계3: 태그의 인증요청 메시지를 받은 리더는 KID_i를 이용하여 K_i, K_{i+1}, KID_{i+1}의 정보를 Key server에서 획득하여 메시지의 $C_{k_i}(RN_T, RN_R, KID_i)$ 값을 확인하여 본다. 리더는 인증요청 메시지를 보낸 태그가 합법적인 태그라고 판단하면 인증응답 메시지를 생성하여 전송하고, 타임아웃 확인을 위한 타이머를 작동 시킨다.

$$R \rightarrow T: KID_{i+1}, C_{k_{i+1}}(RN_T, RN_R, KID_{i+1}) \quad (3)$$

단계4: 리더의 인증응답 메시지를 받은 태그는 Key server와 동일한 방식으로 K_{i+1}을 계산하여, $C_{k_{i+1}}(RN_T, RN_R, KID_{i+1})$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. DoS 공격에 의해서 인증응답 메시지를 중복해서 받을 수 있기 때문에 태그 자신의 KID_i와 인증응답 메시지의 KID_{i+1}이 일치하면 K_i와 KID_i의 갱신과정은 수행하지 않는다.

$$T \rightarrow R: CVEPC, C_{k_{i+1}}(RN_T, CVEPC) \quad (4)$$

$CVEPC$는 $EPC \otimes K'_{i+1,MSB} \otimes K'_{i+1,LSB}$로 나타낼 수 있고, $\otimes$은 XOR 함수를 의미한다.

단계5: 태그의 ID 메시지를 받은 리더는 $CVEPC$에서 EPC를 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.

제안하는 인증 기법에서의 Key server는 KID_i에 해당하는 비밀키 K_i를 리더에게 제공하지만, 태그와 비밀키가 동기화 되어 있지 않기 때문에 DoS 공격에 의한 ID 또는 공유키의 비동기화를 방지 할 수 있다.

V. 성능 분석

본 절에서는 Security 분석과 GNY 분석을 통하여 제안하는 인증 프로토콜의 안정성과 신뢰성을 평가한다.

5.1 Security 분석

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

5.1.1 속임수 공격

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

5.1.2 위치 추적

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

5.1.3 메시지 변조 공격

메시지 변조 공격은 악의적인 노드가 임의로 메시지의 일부분을 수정하는 공격 유형이다. 제안하는 인증 프로토콜에서는 악의적인 노드가 태그나 리더의 메시지를 가로채어 변조 공격을 시도해도 $C_{k_i}(RN_T, RN_R, KID_i)$, $C_{k_{i+1}}(RN_T, RN_R, KID_{i+1})$, $C_{k_{i+1}}(RN_T, CVEPC)$값의 무결성 확인을 통하여 메시지 변조를 확인 할 수 있다.

5.1.4 도청

도청은 무선으로 전송되는 데이터의 내용을 공격

자가 가로채어 살펴보는 것을 의미한다. 하지만 제안하는 인증 프로토콜에서의 EPC는 비밀키 K의 MSB, LSB와 XOR 연산을 통하여 $CVEPC$로 전송되기 때문에 $CVEPC$를 가로채어 살펴보아도 EPC를 알 수 없다. $CVEPC$는 XOR 연산을 통하여 생성되기 때문에 악의적인 노드가 한 태그의 전송하는 값을 여러 세션에 걸쳐서, 계속 주시한다고 가정할 때 $CVEPC_{i+1}$와 $CVEPC_{i+2}$를 XOR 연산한 값과 $CVEPC_i$와 $CVEPC_{i+1}$ 그리고 $CVEPC_{i+2}$를 XOR 연산한 값을 또 다시 XOR 연산을 한다면 비밀키 K_i의 MSB와 LSB의 XOR한 연산이 노출 될 수 있다. 하지만 이를 통해서는 비밀키 K_i를 유추해낼 수 없으므로 $CVEPC$의 비밀성이 보장된다.

5.1.5 서비스거부 공격에 의한 비밀 키 갱신 실패

서비스거부 (DoS) 공격은 대량의 데이터 패킷을 통신망으로 보내서 시스템의 정상적인 동작을 방해하는 공격 수법이다. 그림 5는 DoS 공격이 발생하였을 경우 제안한 인증 프로토콜에서의 대처 과정을 나타낸다. DoS공격이 step 11에서 나타난다고 가정했을 경우에 리더가 step 13의 메시지를 타임아웃이 발생할 때까지 받지 못한다면 리더는 step 11와 13의 메시지를 DoS공격에 의해 손실했다고 생각하고, step 11부터 다시 인증 과정을 수행한다. 그러므로 제안하는 인증 기법에서는 타임아웃 기법에 의해 DoS공격을 탐지할 수 있다. 또한, 악의적인 노드가 step 11의 메시지를 가로채어 태그에 대하여 DoS공격을 시도하여도 인증이 완료된 태그는 인식되기 전 상태로 돌아가기 때문에 리더의 query 메시지에만 응답하고, 다른 메시지에는 응답하지 않기 때문에 악의적인 노드의 태그에 대한 DoS공격은 성공할 수 없다. 리더가 태그의 인증을 완료하면 다른 태그를 인식하기 위하여 query 메시지를 보내기 때문에 query 메시지를 받은 태그는 인식되기 전 상태로 돌아간다.

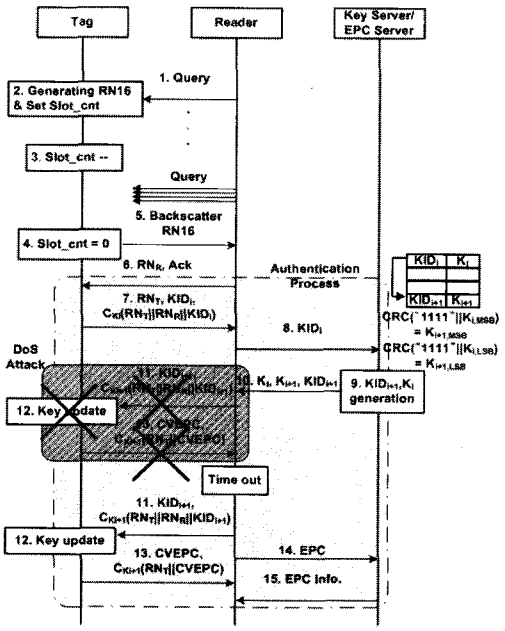


그림 5. 제안하는 인증 프로토콜에서의 DoS 공격

5.2 GNY 분석

제안한 인증 프로토콜의 신뢰성을 분석하기 위하여 GNY logic을 이용한다. GNY logic은 인증 프로토콜의 수행을 이해하기 위한 체계적인 방법으로 GNY logic에 대한 상세한 검증 방법은 참조논문[10]에 기술되어 있다. 본 논문에서 제안한 인증 프로토콜에서 리더가 태그를 인증하는 메시지 (2)와 태그가 리더를 인증하는 메시지 (3)이 직접적인 인증 메시지이므로, 두 메시지를 이용하여 프로토콜의 검증 결과를 보이도록 하겠다.

GNY logic을 통한 검증을 위해서는 먼저 프로토콜의 이상화된 프로토콜을 표현하여야 하며 제안하는 프로토콜을 표현하면 다음과 같다.

5.2.1 이상화된 프로토콜(Idealized protocol)

$$R \lhd *RN_T, *KID_i, *C_{k_i}(RN_T, RN_R, KID_i)$$

$$\hookrightarrow T| \equiv T \xleftrightarrow{K_{i+1}} R$$

$$T \lhd *KID_i, *C_{k_{i+1}}(RN_T, RN_R, KID_{i+1})$$

$$\hookrightarrow R| \equiv R \xleftrightarrow{K_{i+1}} T$$

GNY logic을 통해 검증하고자 하는 인증 목적은 다음 네 가지이다. T가 T와 R이 같은 비밀 키를 공유하고 있다고 믿 키를T는 R이 T와 R이 같은 비밀 키를 가지고 있다는 것을 믿는 것과 R이 R과 T가 같은 비밀 키를 공유하고 있다는 것을 믿고 R은 T가 R과 T가 같은 비밀 키를 가지고 있다는 것을 믿는다는 것이다.

5.2.2 분석 목적 (Goal)

$$T| \equiv T \xleftrightarrow{K_{i+1}} R, \qquad R| \equiv R \xleftrightarrow{K_{i+1}} T$$

$$T| \equiv R| \equiv R \xleftrightarrow{K_{i+1}} T$$

$$R| \equiv T| \equiv T \xleftrightarrow{K_{i+1}} R$$

5.2.3 가정 사항(Assumptions)

$T \ni RN_T \quad R \ni RN_R \quad T \ni K_i \quad T \ni KID_i$

$T| \equiv R| \Rightarrow R| \equiv * \quad R| \equiv T| \Rightarrow T| \equiv *$

$T| \equiv \#(RN_T), \quad R| \equiv \#(RN_R)$

$T| \equiv \Phi(RN_T), \; T| \equiv \Phi(K_i), \; T| \equiv \Phi(KID_i)$

$R| \equiv \Phi(RN_R),$

$T| \equiv T \xleftrightarrow{K_{i+1}} R$

$R| \equiv T| \Rightarrow T \xleftrightarrow{K_{i+1}} R$

5.2.4 로직 분석(Logical analysis)

메시지 1: R은 T로부터 메시지를 수신하면 규칙 T1에 의해서 다음과 같은 식 (5)를 얻을 수 있다.

$$R \lhd RN_T, KID_i, C_{k_i}(RN_T, RN_R, KID_i) \quad (5)$$

여기서 규칙 P1을 이용하면 $R \ni RN_T, R \ni KID_i$, $R \ni h_{k_i}(RN_T, RN_R, KID_i)$이 성립하고, 규칙 R6에 의해서 식 (6)이 성립된다.

$$R| \equiv \Phi\left(RN_T, KID_i, C_{k_i}(RN_T, RN_R, KID_i)\right) \quad (6)$$

R은 KID_i를 Key Server에게 전송하여 K_i, K_{i+1}, KID_{i+1}을 받아 올 수 있기 때문에 규칙 P1, R6에 의해서 $R \ni K_i, R| \equiv \Phi(K_i)$가 된다. $H_K(M)$는 $H(K,M)$이기 때문에 식 (6)에 규칙 I3를 적용하면 식 (7)을 얻을 수 있다.

$$R| \equiv T| \sim (RN_T, RN_R, KID_i, K_i) \quad (7)$$

식 (7)은 메시지가 T로부터 전송된 사실을 확증하여 T를 인증하였음을 의미한다. 식 (7)에 규칙 J2를 적용하면

$$R| \equiv T| \equiv T \xleftrightarrow{K_i} R \quad (8)$$

식 (8)을 얻을 수 있고, 식 (8)에 규칙 J1을 적용하면 식 (9)를 얻을 수 있다.

$$R| \equiv R \xleftrightarrow{K_i} T \quad (9)$$

결과적으로, K_i를 이용하여 K_{i+1}을 도출할 수 있기 때문에 다음과 같은 식 (10)을 얻을 수 있다.

$$R| \equiv T| \equiv T \xleftrightarrow{K_i} R \quad (10)$$

$$R| \equiv R \xleftrightarrow{K_i} T$$

메시지 2: R은 KID_i를 Key Server에 전송하여 KID_{i+1}, K_{i+1}을 받아 오기 때문에 $R \ni K_{i+1}$, $R \ni KID_{i+1}$이 성립되고 메시지 2를 생성 할 수 있다. R로부터 KID_{i+1}, K_{i+1}을 이용해 생성한 메시지 2를 T가 수신하면, 규칙 T1에 의해서 식 (11)을 얻을 수 있다.

$$T \lhd KID_i, C_{k_{i+1}}(RN_T, RN_R, KID_{i+1}) \quad (11)$$

식 (11)에 규칙 P1, R6을 적용하면

$$T| \equiv \Phi\left(KID_i, C_{k_{i+1}}(RN_T, RN_R, KID_{i+1})\right) \quad (12)$$

식 (12)가 성립된다. T는 K_i를 이용하여 K_{i+1}을 계산할 수 있기 때문에 $T \ni K_{i+1}$이 되고 규칙 R6에 의해 $T \ni \Phi(K_{i+1})$가 된다. 식 (11), (12)에 규칙 I3을 적용하면 식 (13)을 얻을 수 있다.

$$T| \equiv R| \sim (RN_T, RN_R, KID_{i+1}, K_{i+1}) \quad (13)$$

식 (13)은 메시지 2가 R로부터 전송된 사실을 확증하며, T가 R을 인증했음을 의미한다. 식 (13)에 규칙 J2를 적용하면 식 (14)가 성립한다.

$$T| \equiv R| \equiv T \xleftrightarrow{K_{i+1}} R \quad (14)$$

식 (14)에 J1을 적용하면 식 (15)를 구할 수 있다.

$$T| \equiv T \xleftrightarrow{K_{i+1}} R \quad (15)$$

이러한 결과를 종합하면, 식 (10)에 의해서 R이 T를 인증하고 비밀 키를 공유한다는 것을 알 수 있고, 식 (14), (15)를 통해 T가 R을 인증하고 비밀 키를 공유한다는 것을 알 수 있다. 그러므로 제안하는 인증 프로토콜이 신뢰성 있는 인증을 수행한다는 것을 증명 할 수 있다.

VI. 결 론

본 논문에서는 EPCglobal RFID 시스템에서 Key

server를 사용하는 인증 프로토콜을 제안했다. 제안하는 인증 프로토콜은 구현의 용이함을 위하여 추가적인 함수 구현 없이 Gen2 프로토콜에 존재하는 함수를 인증과정에 사용하고 DoS공격을 포함한 다양한 공격에 대처하기 위하여 타임아웃 기법과 Key server를 사용한다.

제안하는 인증 프로토콜의 성능을 분석하기 위해 GNY logic을 통한 프로토콜 검증과 Security 분석을 하였다. GNY logic을 이용한 일반적인 증명을 통해 프로토콜의 신뢰성을 입증하였고, 다양한 공격 유형에 대하여 제안하는 인증 프로토콜이 어떠한 강점을 갖는지 분석하였다. 따라서 본 논문에서 제안한 인증 프로토콜은 안전한 RFID 시스템을 제공할 것으로 기대된다.

참 고 문 헌

〔1〕 RFID Journal, http://www.rfidjournal.com/.

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

〔3〕 EPCglobal Inc., "Class 1 Generation 2 UHF Air Interface Protocol Standard Version 1.09," 2005.

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

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

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

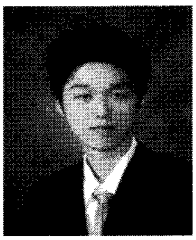
〔7〕 D. N. Duc, J. Park, H. Lee, K. Kim, "Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning," *in Proc. the Symposium on Cryptography and Information Security*, 2006.

〔8〕 C. Qingling, Z. Yiju, and W. Yonghua, "A minimalist Mutual Authentication Protocol for RFID System & BAN Logic Analysis," *in Proc. International Colloquium on Computing, Communication, Control, and Management*, 2008.

〔9〕 L. Lu, J. Han, L. Hu, Y. Liu, and L. M. Ni, "Dynamic Key-Updating: Privacy- Pres erving Authentication for RFID Systems," *in Proc. Pervasive Computing and Communica tion*, 2007.

〔10〕 L. Gong, R. Needham, and R. Yahalom, "Reasoning about Belief in Cryptographic Protocols," *in Proc. the IEEE Symposium on Research in Security and Privacy*, 1990.

이 규 환 (Kyu-Hwan Lee) 준회원



2007년 아주대학교 전자공학부 졸업

2007년~현재 아주대학교 전자공학부 석/박사 통합과정

<관심분야> WLAN, 무선망 QoS, WPAN 보안 인증, Ad-hoc, Mesh network 등

김 재 현 (Jae-Hyun Kim) 정회원

1987년~1996년 한양대학교 전산과 학사 및 석/박사 졸업

1997년~1998년 미국UCLA 전기전자과 박사 후 연수

1998년~2003년 Bell Labs, Performance Modeling and QoS Management Group, 연구원

2003년~현재 아주대학교 전자공학부 부교수

<관심분야> 무선인터넷 QoS, MAC 프로토콜, IEEE 802.11/15/16/20, 3GPP, 국방 전술네트워크 등