프라이버시를 제공하고 중계 공격에 안전한 다중-컨텍스트 RFID 상호 인증 프로토콜

정회원 안 해 순*, 종신회원 윤 은 준**, 정회원 남 인 길***°

Privacy Preserving and Relay Attack Preventing Multi-Context RFID Mutual Authentication Protocol

Hae-Soon Ahn* *Regular Member*, Eun-Jun Yoon** *Lifelong Member*, In-Gil Nam***° *Regular Member*

요 약

최근 Selim등은 공개키 암호 기반의 프라이버시를 제공하기 위해 다중-컨텍스트 RFID 인증 프로토콜을 제안하였다. 하지만 Selim등이 제안한 프로토콜은 리더와 태그 간의 인증을 수행하는 과정에서 공개키 기반의 암호 알고리즘을 사용하므로 수동형 태그에는 적합하지 않을 뿐만 아니라 상호 인증 부재로 인한 위장 공격에 취약하다. 위와 같은 효율성 문제와 보안 취약점 해결을 위해 본 논문에서는 각각 다른 영역에서 단일 수동형 태그와 다양한 목적을 제공하는 리더들 간의 상호 인증을 제공함으로써 프라이버시 침해와 태그 위장 공격을 방지하며, 중계 공격과 서비스 거부 공격에 안전한 다중-컨텍스트 RFID 상호 인증 프로토콜을 제안한다. 결론적으로 제안한 프로토콜은 RFID 리더로부터 수집된 공간과 시간의 정보를 토대로 안전한 상호 인증이 수행되고, 수동형 태그 환경에 적합하도록 안전한 일방향 해쉬 함수와 대칭키 암호 연산을 수행함으로써 강한 보안성과 높은 연산 효율성을 제공한다.

Key Words : RFID, authentication, multi-context, privacy, hash function, public key, relay attack

ABSTRACT

Recently, Selim et al proposed public key cryptography based privacy preserving multi-context RFID authentication protocol. However Selim et al's proposed protocol not only doesn't fit into passive tag based RFID system because it uses public key based encryption algorithm to perform authentication between reader and tag, but also is insecure to an impersonation attack because it doesn't provide mutual authentication. In order to eliminate the above described efficiency problem and security vulnerabilities, this paper proposes a new multi-context RFID mutual authentication protocol that can prevent privacy invasion and tag impersonation attack through providing mutual authentication between single passive tag which is located different application space and readers which provide multi-context purposes and can secure against relay attack and denial-of-service attack. As a result, the proposed protocol performs secure mutual authentication based on the collected space and time information from the RFID reader and provides strong security and high computation efficiency because if performs secure one-way hash function and symmetric encryption operations suitable to the environments of passive RFID tags.

* 대구대학교 기초교육원 컴퓨터과정 (ahs221@hanmail.net), ** 경북대학교 전자전기컴퓨터학부 (ejyoon@knu.ac.kr)
*** 대구대학교 컴퓨터·IT공학부 (ignam@daegu.ac.kr), (° : 교신저자)
논문번호 : KICS2011-03-162, 접수일자 : 2011년 3월 30일, 최종논문접수일자 : 2011년 7월 12일

Ⅰ. 서 론

유비쿼터스(ubiquitous) 환경이 도래되면서 무선 신호(radio frequency)를 이용하여 원거리의 개체를 식별하기 위해 사용의 편리성과 효율성에 기인한 다양한 RFID(Radio Frequency IDentification) 애플리케이션들이 각광을 받고 있는 추세이다[1-5]. 특히, RFID 기술은 바코드나 비접촉식 스마트카드와 같은 기술과 비교해보면 근접 인증 및 개체 식별 부분에서 매우 우수하다[6-8]. 왜냐하면 RFID 태그(tag)에 저장될 수 있는 다양한 정보와 양은 이전 기술에 비해 상상할 수 없을 정도로 방대하다. 현재, RFID 시스템은 공급 체인, 지불시스템, 접근 제어 등과 같은 애플리케이션에서 RFID 태그 사용이 매우 폭발적이다[9-13]. 그러나 RFID 기반 애플리케이션들의 특징은 기존에 설계된 리더들이 인증을 하기 위해 태그에게 질의를 할 때 단지 하나의 목적만을 위한 하나의 컨텍스트(context)에서만 사용된다는 것이다. 최근 여러 가지 다른 애플리케이션들에서 단일 RFID 태그와 다목적 리더를 식별하고 인증하기 위한 다중-컨텍스트(multi-context) RFID 인증 프로토콜이 제안되었다. 다중-컨텍스트 RFID 시스템 구조는 그림 1과 같다[14].

동일한 단일 RFID 태그는 다양한 목적을 위해 각각 다른 장소에서 질의를 받을 수 있다. 예를 들어 경찰서에서 어떤 사람에 대한 범죄 기록의 여부를 조회하기 위해 그 사람의 태그와 인증하여 식별할 수 있고, 병원에서는 그 사람에 대한 건강 기록에 대해 알게 됨으로써 응급사태가 발생할 경우 그 사람의 태그를 식별하고 인증하여 응급처치를 할 수 있다. 따라서 이러한 다중-컨텍스트 RFID 시스템에서 단일 태그에 저장된 식별 정보를 검색하고 인증하기 위해 각 분야

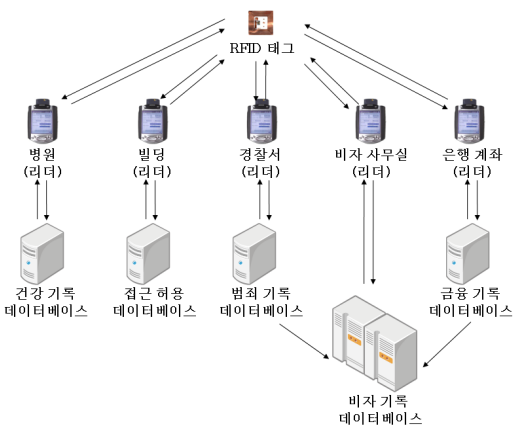

그림 1. 다중-컨텍스트 RFID 시스템 구조

에서 리더들은 태그에게 질의를 함으로써 서로 다른 장소에서 다양한 목적을 충족시킬 수 있다. 또한, 태그와 리더를 인증하고, 접근을 허용함으로써 RFID 태그들의 다용도 목적을 위한 사용이 증가될 뿐만 아니라 프라이버시 침해 방지 및 다양한 공격으로부터 보안의 중요성도 강조되고 있다.

Ⅱ. 관련 연구

RFID 시스템은 일반적으로 리더, 태그 그리고 백-엔드 데이터베이스(back-end database)의 3가지 구성요소로 이루어져 있다. RFID 시스템에서의 태그는 주위의 리더 신호에 반응하여 자신의 고유 정보를 무선 통신 채널을 통해서 리더에게 전송한다. 또한, 리더와 백-엔드 데이터베이스의 연산 능력에 비해 RFID 태그는 연산 능력이 떨어지며, 객체를 유일하게 식별하기 위한 정보만을 가지고 있다. 따라서 리더 주변의 공격자는 사용자의 개인 정보나 위치 정보를 쉽게 얻을 수 있으므로 심각한 프라이버시 침해 문제를 유발시킨다.

현재 RFID 시스템 환경에서 발생할 수 있는 프라이버시 침해 문제를 해결하기 위해 많은 연구자들에 의해 해쉬-락 기법, 확장된 해쉬-락 기법, 해쉬-기반 ID 변형 기법, 개선된 해쉬-기반 ID 변형 기법, 블로커 태그를 이용한 기법, 해쉬-체인 기법 등 다양한 RFID 인증 프로토콜(authentication protocol)들이 최근까지 연구 되고 있다[13, 15-16]. 해쉬-락 기법은 해쉬 함수를 사용하여 저가의 태그에 적용될 수 있지만, 리더와 태그 간에 동일한 해쉬 값인 metaID=h(key)를 사용하기 때문에 공격자가 태그의 위치를 추적할 수 있고[17], 난수 값을 사용하는 랜덤 해쉬-락 기법과 서로 다른 두개의 해쉬 함수를 사용하는 해쉬-체인 기법도 태그의 ID가 노출될 가능성과 재전송 공격 및 스푸핑 공격에 취약하다[13]. 해쉬 함수 이외에도 암호학적 함수를 사용하는 방법으로 재 암호화 접근기법이 있다[15, 18]. 하지만 현재까지 제안되어져 오고 있는 대부분의 RFID 인증 프로토콜들은 태그의 재사용이 불가능하거나, 태그의 위치추적으로 위치 트래킹 공격(location tracking attack)이 쉬우며, 재전송 공격(replay attack)이나 스푸핑 공격(spoofing attack)등 다양한 보안 취약점과 프라이버시 침해 문제들이 많은 연구자들에 의해 발견되어 지고 있다.

2009년에 Selim등[14]은 기존의 단일 태그와 단일 리더와의 인증에서 탈피하고, 공개 키 암호 알고리즘을 기반으로 하여 단일 태그와 다목적을 위한 정보를 저장하여 상황과 용도에 따라 여러 리더들과 인증이

가능한 RFID 시스템의 특징을 고려하여 실용적인 인증 프로토콜을 제안하였다. 하지만 Selim등이 제안한 프로토콜은 다음의 보안 취약점과 연산 효율성 문제를 가진다. (1)리더와 태그 간에 상호 인증을 제공하지 않기 때문에 프라이버시 침해 및 다양한 공격들에 취약하다. (2)공개키 암호 알고리즘의 사용으로 인해 과도한 자원이 요구됨으로써 무엇보다 저전력 수동형 RFID 태그에서는 부적합하다[19].

따라서 본 논문에서는 공개키 암호 알고리즘을 사용하지 않고, 수동형 RFID 태그 환경에 적합한 안전한 일방향 해시 함수[20]와 대칭키 암호 알고리즘[21]을 사용하여 단일 태그와 다양한 목적을 제공하는 리더들 간의 상호 인증을 제공함으로써 태그 위장 공격을 방지하고, 프라이버시 침해 공격 및 서비스 거부 공격, 중계 공격, 그리고 재전송 공격에 안전하고 효율적인 다중-컨텍스트 RFID 상호 인증 프로토콜을 제안한다. 결론적으로 제안한 프로토콜은 RFID 리더로부터 수집된 공간과 시간의 정보를 토대로 안전한 상호 인증이 수행되고, 수동형 태그 환경에 적합하도록 안전한 일방향 해쉬 함수와 대칭키 암호 연산을 수행하여 강한 보안성과 높은 연산 효율성을 제공한다.

본 논문의 구성은 다음과 같다. 3장에서는 Selim등이 제안한 다중-컨텍스트 RFID 인증 프로토콜을 소개하고, 4장에서는 Selim등이 제안한 프로토콜에 대한 상호 인증 및 연산 효율성 문제에 대해 분석한다. 그리고 5장에서는 제안한 다목적 리더들을 위한 단일 태그와의 상호 인증을 제공하는 다중-컨텍스트 RFID 상호 인증 프로토콜에 대해 설명하고, 6장에서는 안전성과 효율성을 분석한 후, 7장에서 본 논문의 결론을 맺는다.

Ⅲ. Selim등이 제안한 다중-컨텍스트 RFID 인증 프로토콜

본 장에서는 최근 Selim등[14]이 제안한 단일 수동형 태그와 위치 상황에 맞는 다양한 목적을 제공하는 리더들 간의 인증을 위한 다중-컨텍스트 RFID 인증 프로토콜을 소개한다. 그림 2는 Selim등이 제안한 공개키 암호 기반의 다중-컨텍스트 RFID 인증 프로토콜의 전체적인 구성과 동작 과정을 보여준다. 표 1은 본 논문에서 사용할 용어들의 표기법 및 정의를 나타내고 있으며, Selim등이 제안한 다중-컨텍스트 RFID 인증 프로토콜에서의 각 리더는 백-엔드 서버와 함께 키 쌍을 공유하고 리더와 백-엔드 서버 사이에는 인증된 채널과 안전함을 가정한다. 또한, 공격자는 리더를 복

표 1. 용어 정의

기호	의 미
T	RFID 태그
R	RFID 리더
K	백엔드 서버와 태그가 공유하는 비밀키(secret key)
TID	태그 T의 아이디 값($\geq$ 128 비트)
RID	리더 R의 아이디 값($\geq$ 128 비트)
RK	백엔드 서버와 리더가 공유하는 키 값
RL	위치 서버가 가지고 있는 리더의 위치 정보
TIT	$Ticket$ 지급 시간(Ticket Issuance Time)
$E(\ )$	암호화 함수
$D(\ )$	복호화 함수
$h(\ )$	안전한 일방향 해쉬 함수 (Secure One-Way Hash Function)
$PRNG$	의사난수생성기 (Pseudo Random Number Generator)
N_T	태그가 생성한 난수
$\oplus$	배타적 논리합(XOR; eXclusive OR) 연산
$\|$	연접(Concatenation) 연산
pub	공개키
$priv$	비밀키

제할 수 없고, 백-엔드 서버에 의해 리더의 위치 정보가 요청되었을 때 위치 서버의 리더 위치 정보는 신뢰된다고 가정한다. 프로토콜이 수행되는 과정은 다음과 같다.

(1) 리더 → 백-엔드 서버: $Ticket$ 요청

리더는 태그에게 질의하기 위해 백-엔드 서버에게 $Ticket$을 요청한다.

(2) 백-엔드 서버 → 위치 서버: RL 요청

백-엔드 서버는 위치 서버에게 $Ticket$을 요청한 리더에 대한 위치 정보를 요청한다.

(3) 위치 서버 → 백-엔드 서버: RL 전송

위치 서버는 백-엔드 서버에게 리더의 위치 정보 RL을 전송한다.

(4) 백-엔드 서버 → 리더: $Ticket$ 전송

백-엔드 서버는 위치 서버로부터 수신한 RL과 리더의 식별자 RID, 그리고 $Ticket$ 지급 시간(Ticket Issuance Time)인 TIT를 비밀키 K로 암호화하여 $Ticket = E_K(RID \| RL \| TIT)$를 생성한 후 리더에게 전송한다.

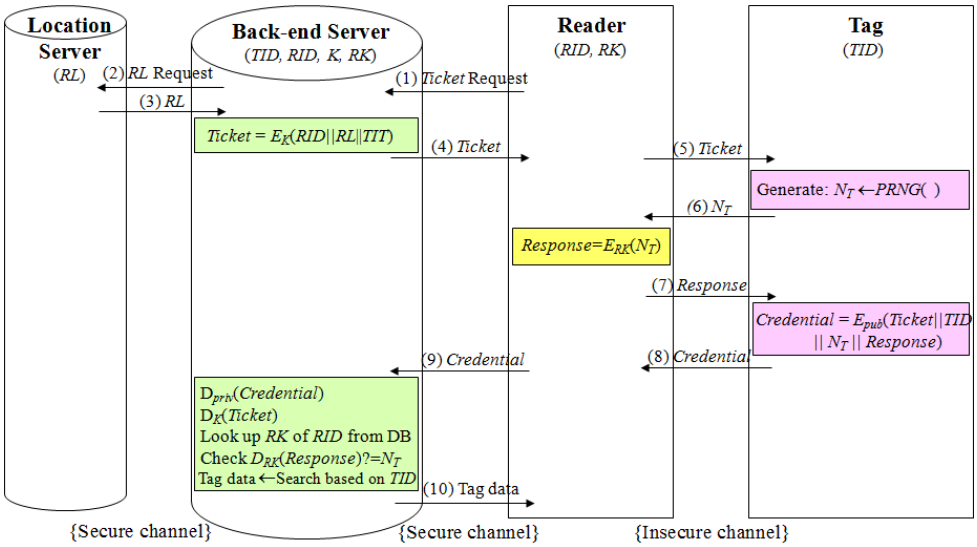

그림 2. Selim등이 제안한 다중-컨텍스트 RFID 인증 프로토콜

(5) 리더 → 태그: *Ticket* 전송

리더는 백-엔드 서버로부터 수신한 *Ticket*을 태그에게 전송하여 질의를 수행한다.

(6) 태그 → 리더: N_T 전송

태그는 난수 N_T를 생성하고, 리더에게 전송한다.

(7) 리더 → 태그: *Response* 전송

리더는 태그로부터 수신한 난수 N_T를 백-엔드 서버와 리더가 공유하고 있는 비밀키 *RK*로 암호화 하여 $Response = E_{RK}(N_T)$ 값을 태그에게 전송한다.

(8) 태그 → 리더: *Credential* 전송

태그는 리더로부터 수신한 *Response*와 (5)번 단계에서 수신한 *Ticket*, 태그 식별자인 *TID*, 그리고 난수 N_T를 공개키 *pub*로 암호화 연산을 수행하여 $Credential = E_{pub}(Ticket \| TID \| N_T \| Response)$를 리더에게 전송한다.

(9) 리더 → 백-엔드 서버: *Credential* 전송

리더는 태그로부터 수신한 *Credential*을 백-엔드 서버에게 전송한다.

(10) 백-엔드 서버 → 리더: *Tag data* 전송

백-엔드 서버는 리더로부터 수신한 *Credential*과 *Ticket*을 복호화한 후 DB로부터 리더 식별자인 *RID*에 해당하는 리더 비밀키 *RK*를 검색한다. 또한 복호화한 *Credential*에서 태그가 암호화하여 전송한 난수 N_T와 리더가 태그로부터 수신하여 암호화한 $Response = E_{RK}(N_T)$를 검색한 *RK*로 복호화하여 두 난수 값이 일치하는지 검증한다. 두 난수가 일치하면 백-엔드 서버는 리더와 태그를 인증하게 되며 *TID*에 대응되는 태그 정보를 리더에게 전송한다.

Ⅳ. Selim등의 다중-컨텍스트 RFID 인증 프로토콜 안전성 및 효율성 문제

본 장에서는 Selim등[14]이 제안한 다중-컨텍스트 RFID 인증 프로토콜이 안전성과 효율성 문제를 가지고 있음을 증명한다.

4.1 상호 인증 문제

본 절에서는 Selim등이 제안한 다중-컨텍스트 RFID 인증 프로토콜에서 리더와 태그 간에 상호 인증을 제공하지 않음으로 인해 TID_A를 소유한 공격자 태그 Tag_A가 합법적인 태그인 척하여 *TID*를 소유한 태그 위장 공격을 수행할 수 있음을 증명한다. 이로 인해 백-엔드 서버가 리더에게 공격자 태그 Tag_A의 TID_A에 대응되는 $Tag\,data_A$인 잘못된 태그의 정보를 전송하게 되는 문제점을 가지게 된다. 그림 3은 상호 인증을 제공하지 않음으로써 발생하는 태그 위장 공격 시나리오를 보여주고 있다. 리더와 태그 간에는 안전하지 않은 채널을 사용하므로 임의의 세션에서 공격자는 (5)번 단계에서 리더가 태그에게 전송한 *Ticket*을 가로챈다고 하였을 때 다음과 같은 공격을 수행할

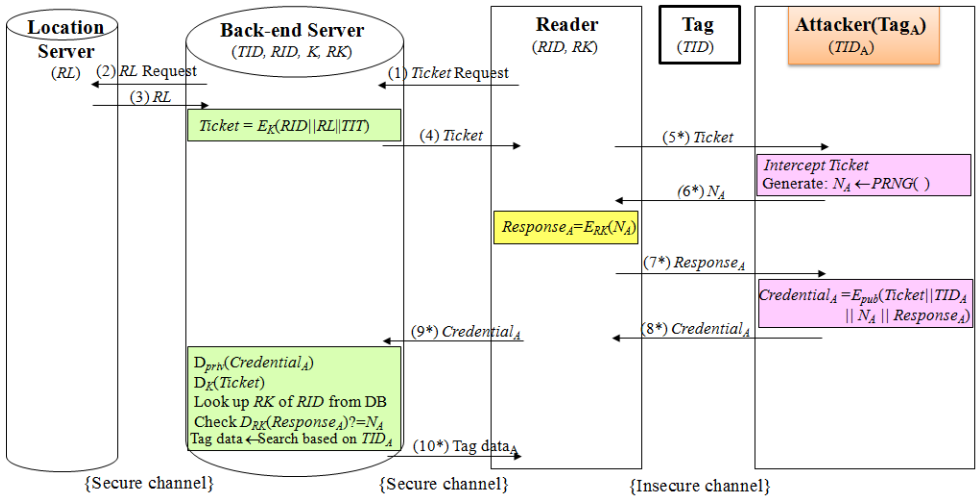

그림 3. 공격자 태그에 의한 태그 위장 공격 시나리오

수 있다.

(1)~(4)의 단계는 정상적으로 수행한다.

(5*) 리더 → 태그: $Ticket$ 전송

리더는 백-엔드 서버로부터 수신한 $Ticket$을 태그에게 전송하여 질의를 수행한다.

(6*) 공격자 Tag_A → 리더: N_A 전송

공격자 Tag_A는 리더가 전송한 $Ticket$을 가로챈 후 난수 N_A를 생성하고, 리더에게 전송한다.

(7*) 리더 → 태그: $Response_A$ 전송

리더는 공격자 Tag_A가 전송한 난수 N_A를 수신한 후 백-엔드 서버와 리더가 공유하고 있는 비밀키 RK로 암호화하여 $Response_A = E_{RK}(N_A)$를 태그에게 전송한다.

(8*) 공격자 → 리더: $Credential_A$ 전송

공격자는 리더가 전송한 $Response_A$를 가로채고, 이전 단계에서 가로챈 $Ticket$, 공격자 Tag_A의 식별자인 TID_A, 그리고 난수 N_A를 공개키 pub로 암호화 연산을 수행하여 아래와 같은 $Credential_A$를 생성한 후 리더에게 전송한다.

$$Credential_A = E_{pub}(Ticket \| TID_A \| N_A \| Response_A)$$

(9*) 리더 → 백-엔드 서버: $Credential_A$ 전송

리더는 공격자가 전송한 $Credential_A$ 값을 수신하여 백-엔드 서버에게 전송한다.

(10*) 백-엔드 서버 → 리더: $Tag\ data_A$ 전송

백-엔드 서버는 리더로부터 수신한 $Credential_A$와 $Ticket$을 복호화한 후 DB로부터 리더 식별자인 RID에 해당하는 리더 비밀키 RK를 검색한다. 또한 복호화한 $Credential_A$에서 공격자 태그인 Tag_A가 암호화하여 전송한 난수 N_A와 리더가 공격자 태그인 Tag_A로부터 메시지를 수신하여 암호화한 값인 $Response_A = E_{RK}(N_A)$를 검색한 RK로 복호화하여 두 값이 일치하는지 검증한다. $Response_A$로부터 복호화하여 얻은 N_A는 $Credential_A$로부터 복호화된 N_A와의 검증 결과는 항상 참이 되기 때문에 백-엔드 서버는 위장한 공격자 태그 Tag_A와의 인증에 성공하게 됨으로써 잘못된 태그 정보인 $Tag\ data_A$를 리더에게 전송한다. 따라서 Selim등이 제안한 다중-컨텍스트 RFID 인증 프로토콜은 상호 인증을 수행하지 않으므로 공격자 태그인 Tag_A는 아주 쉽게 합법적인 태그로 위장하여 잘못된 태그 정보를 리더에게 제공하게 됨으로써 리더는 신뢰할 수 없는 태그 정보 $Tag\ data_A$를 활용하게 된다. 예를 들어 경찰서에서 범죄자의 전과를 조작하기 위해 범죄자와 협업하는 공모자인 공격자는 범죄자의 태그 정보에 기록되어 있는 전과 기록을 범죄 기록이 전혀 없는 태그의 정보로 대체하여 제시한 위장 공격을 수행하여 백-엔드 서버가 리더에게 잘못된 정보를 전송함으로써 리더는 범죄자의 전자 기록이 없는 것으로 식별하게 되는 경우가 발생할 수 있다.

4.2 연산 효율성 문제

RFID 시스템 환경에서의 수동형 태그는 자체 배터리를 내장하지 않는 대신 리더로부터 전원을 공급받고, 연산을 수행할 수 있는 메모리의 크기가 매우 작다. 그러므로 수동형 태그에서 공개키 암호 알고리즘 연산을 수행하는 것은 연산 오버헤드를 발생시키기 때문에 일반적으로 해쉬 함수나 대칭키 암호 알고즘을 많이 사용한다. 하지만 Selim등[14]이 제안한 다중-컨텍스트 RFID 인증 프로토콜의 태그측 연산에서 $Credential = E_{pub}(Ticket \| TID \| N_T \| Response)$ 값을 구하기 위해 $Ticket$과 태그 식별자인 TID, 난수 N_T, 그리고 $Response$를 공개키 pub로 암호화연산을 수행한다. 따라서 위와 같은 공개키 암호 알고리즘 연산을 수행하는 것은 수동형 태그 측의 연산 효율성을 저하시키는 원인이 된다. 더 나아가서 공격자가 리더인척 위장하여 랜덤한 $Ticket$과 $Response$들을 무한개의 값을 생성하여 단계 (5)와 (7)에서 각각 전송하게 되면 태그는 항상 대응되는 난수 N_T와 $Credential$을 생성하기 때문에 엄청난 공개키 연산 오버헤드로 인해 더 이상 연산을 수행할 수 없는 서비스 거부 상태로 빠질 수 있다. 결론적으로 Selim등이 제안한 프로토콜은 심각한 연산 효율성 문제를 가짐을 알 수 있다.

V. 제안하는 다중-컨텍스트 RFID 상호 인증 프로토콜

본장에서는 태그와 리더 간의 상호 인증을 제공하고, 다양한 공격과 프라이버시 침해를 방지할 뿐만 아니라 공개키 암호 연산을 수행하지 않는 연산 효율성을 보장하는 다목적 리더들을 위한 다중-컨텍스트 RFID 상호 인증 프로토콜을 제안한다. 그림 4는 제안한 프로토콜의 전체적인 구성과 인증 과정을 보여주며 다음과 같이 수행된다.

(1) 리더 → 백-엔드 서버: $Ticket$ 요청

리더는 태그에게 질의하기 위해 백-엔드 서버에게 $Ticket$을 요청한다.

(2) 백-엔드 서버 → 위치 서버: RL 요청

백-엔드 서버는 위치 서버에게 $Ticket$을 요청한 리더에 대한 위치 정보를 요청한다.

(3) 위치 서버 → 백-엔드 서버: RL 전송

위치 서버는 백-엔드 서버에게 리더의 위치 정보 RL을 전송한다.

(4) 백-엔드 서버 → 리더: $Ticket$ 전송

백-엔드 서버는 위치 서버로부터 수신한 RL과 리더의 식별자 RID, 그리고 $Ticket$ 지급 시간(Ticket Issuance Time)인 TIT를 비밀키 K로 암호화하여 $Ticket = E_K(RID \| RL \| TIT)$를 생성한 후 리더에게 전송한다.

(5) 리더 → 태그: $Ticket$ 전송

리더는 백-엔드 서버로부터 수신한 $Ticket$을 태그에게 전송하여 질의를 수행한다.

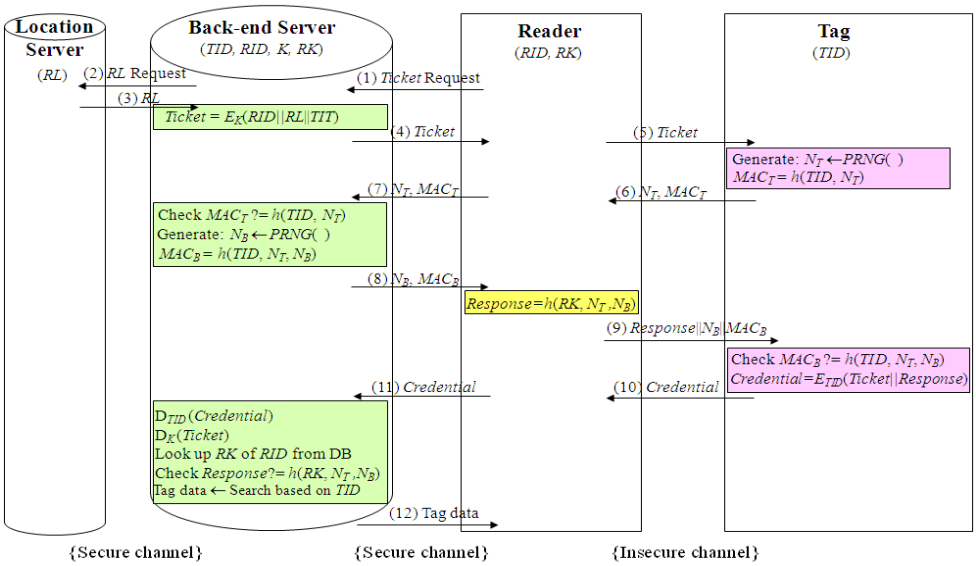

그림 4. 제안하는 다중-컨텍스트 RFID 상호 인증 프로토콜

(6) 태그 → 리더: N_T, MAC_T 전송

태그는 난수 N_T를 생성하고, N_T와 $MAC_T = h(TID, N_T)$ 해쉬 값을 리더에게 전송한다.

(7) 리더 → 백-엔드 서버: N_T, MAC_T 전송

리더는 태그로부터 수신한 N_T와 MAC_T 값을 백-엔드 서버에게 전송한다.

(8) 백-엔드 서버 → 리더: N_B, MAC_B 전송

백-엔드 서버는 리더로부터 수신한 $MAC_T? = h(TID, N_T)$ 값을 검증한다. 또한 난수 N_B를 생성한 후 $MAC_B = h(TID, N_T, N_B)$를 연산하고, 리더에게 N_B와 $MAC_B = h(TID, N_T, N_B)$를 전송한다.

(9) 리더 → 태그: $Response \| N_B \| MAC_B$ 전송

리더는 태그로부터 수신한 난수 N_T와 백-엔드 서버와 리더가 공유하고 있는 비밀키 RK, 그리고 백-엔드 서버가 전송한 난수 N_B의 해쉬 값인 $Response = h(RK, N_T, N_B)$를 연산한다. 리더는 태그에게 $Response \| N_B \| MAC_B$를 전송한다.

(10) 태그 → 리더: $Credential$ 전송

태그는 리더로부터 $Response \| N_B \| MAC_B$를 수신한 후 $MAC_B? = h(TID, N_T, N_B)$를 검증한다. 그리고 (5)번 단계에서 수신한 $Ticket$, $Response$를 태그 식별자 TID를 가지고 암호화 연산을 수행한 아래의 $Credential$ 값을 리더에게 전송한다.

$$Credential = E_{TID}(Ticket \| Response)$$

(11) 리더 → 백-엔드 서버: $Credential$ 전송

리더는 태그로부터 수신한 $Credential$을 백-엔드 서버에게 전송한다.

(12) 백-엔드 서버 → 리더: $Tag\ data$ 전송

백-엔드 서버는 리더로부터 수신한 $Credential$과 $Ticket$을 TID와 K로 각각 복호화한 후 DB로부터 리더 식별자인 RID에 해당하는 리더 비밀키 RK를 검색한다. 검색한 리더 비밀키 RK를 이용하여 $Response? = h(RK, N_T, N_B)$를 검증한 후 검증에서 일치하게 되면 정당한 리더와 태그로 상호 인증에 성공하여 TID에 대응되는 태그 정보인 $Tag\ data$를 리더에게 전송하고 종료한다.

Ⅵ. 안전성과 효율성 분석

본 장에서는 제안한 다중-컨텍스트 RFID 상호 인증 프로토콜의 안전성과 효율성에 대해 분석한다.

6.1 안전성 분석

제안한 다중-컨텍스트 RFID 상호 인증 프로토콜은 다음과 같이 상호 인증을 명시적으로 제공하며, 위장 공격, 서비스 거부 공격, 프라이버시 침해, 재전송 공격 및 중계 공격에 대해 안전성을 제공한다. 표 2는 프로토콜들의 안전성을 비교한 결과를 보여주고 있다. 표 2를 통해 알 수 있듯이 Selim등이 제안한 프로토콜은 상호 인증을 제공하지 않을 뿐만 아니라 위장 공격, 서비스 거부 공격, 프라이버시 침해 공격들에도 안전하지 않다. 더욱이 Selim등이 제안한 프로토콜은 연산 효율성 문제로 인해 비실용적이다. 하지만 제안한 프로토콜은 상호 인증을 제공할 뿐만 아니라 위장 공격, 서비스 거부 공격, 프라이버시 침해 공격들에도 안전하다.

(1) 상호 인증(mutual authentication) 및 위장 공격(impersonation attack): 제안한 프로토콜의 (8)번 단계에서 백-엔드 서버는 태그가 계산한 $MAC_T? = h(TID, N_T)$ 해쉬 값을 검증하고, (9)번 단계에서 태그는 백-엔드 서버가 계산한 $MAC_B? = h(TID, N_T, N_B)$ 해쉬 값을 검증한다. 태그와 백-엔드 서버 사이에 공유된 비밀키 값 역할을 하는 태그 식별자 TID를 모르는 공격자는 합법적인 태그 또는 리더인척 하여 태그 정보를 위조하는 위장 공격을 수행할 수 없게 된다. 따라서 제안한 프로토콜은 안전한 상호 인증을 제공할 뿐만 아니라 위장 공격에도 안전하다.

(2) 서비스 거부 공격(denial of service attack): 제안한 프로토콜에서는 공개키 암호 알고리즘 연산을 수행하지 않고 안전한 일방향 해쉬 함수와 대칭키 암

표 2. 안전성 비교

프로토콜 / 공격유형	Selim 등[14]의 프로토콜	제안한 프로토콜
상호 인증	제공하지 않음	제공함
위장 공격	안전하지 안전	안전함
서비스 거부 공격	안전하지 않음	안전함
프라이버시 침해 공격	안전하지 않음	안전함
중계 공격	안전함	안전함
재전송 공격	안전함	안전함

호 연산을 이용하여 상호 인증을 수행한다. 상호 인증 과정에서 태그는 $MAC_T = h(TID, N_T)$ 해쉬 값을 생성하고, 백-엔드 서버가 생성한 해쉬 값 $MAC_B ? = h(TID, N_T, N_B)$를 검증하기 위해 공개키 암호 연산에 비해 훨씬 빠른 속도로 계산이 가능한 해쉬 함수 연산을 사용한다. 또한 공격자가 리더인척 위장하여 랜덤한 $Ticket$과 $Response$들을 생성하여 태그에게 전송하더라도 태그 측에서는 해쉬 함수 연산의 속도가 빠르기 때문에 연산 오버헤드가 발생하지 않는다. 따라서 제안한 프로토콜은 서비스 거부 공격에 안전하다.

(3) 프라이버시(privacy): 제안한 프로토콜에서는 태그 식별자 TID를 백-엔드 서버와 태그 사이에 안전하게 공유하고 있고, 매 세션마다 새로운 난수 N_T와 N_B를 생성한다. 리더는 난수 N_T, N_B, 그리고 리더 비밀키 RK를 사용하여 $Response = h(RK, N_T, N_B)$ 해쉬 값을 구하여 태그에게 전송하고, 태그는 태그 식별자 TID를 사용하여 대칭키 암호 연산을 수행하여 $Credential = E_{TID}(Ticket \| Response)$ 값을 리더에게 전송하기 때문에 공격자는 도청하여 메시지를 가로 챈다 하더라도 태그 식별자 TID와 리더 비밀키 RK를 모르기 때문에 태그의 정보나 위치 변화를 감지할 수 없다. 이와 같은 이유로 제안한 프로토콜은 태그 소유자의 이동 경로를 파악할 수 없게 됨으로써 위치 트래킹 공격에도 안전하고, 태그 정보에 대한 프라이버시 침해 공격에도 안전하다.

(4) 중계 공격(relay attack): 제안한 프로토콜은 단일 태그와 다목적 리더들의 상호 인증을 수행하는 다중-컨텍스트 RFID 상호 인증 프로토콜이므로 합법적인 리더는 사용 목적에 맞는 장소 및 태그에게 질의할 수 있는 인증된 지역 내에 위치한다. 리더가 백-엔드 서버에게 $Ticket$을 요청하면 백-엔드 서버는 위치 서버에게 리더의 위치 정보 RL을 요청한다. 위치 서버는 합법적인 리더의 신뢰성 있는 위치 정보 RL을 백-엔드 서버에게 전송하면 백-엔드 서버는 $Ticket = E_K(RID \| RL \| TIT)$ 값을 리더에게 전송한다. 위조한 리더는 합법적인 리더가 태그에게 정당하게 질의할 수 없는 지역 외부에 위치할 뿐만 아니라 메시지의 전송 시간 카운트를 사용하여 주어진 시간 주기 내에 수행되는지 검사하므로 중계 공격을 수행할 수 없다. 그림 5에서는 다중-컨텍스트 RFID 인증 프로토콜에서의 중계 공격 시나리오를 보여주고 있다[14]. 그림에서 보여주듯이 위조한 리더는 합법적인 리더와 태그 간의 전송에서 중간에 중계하여 값을 가로채기 때문에 태그에게 도착하는 응답 값의 지연 시간이 길어지며, 위조한 리더는 단순한 중계 기능만을 수행한다는 것을 알 수 있다. 이러한 이유로 제안한 프로토콜은 중계 공격에 안전하다.

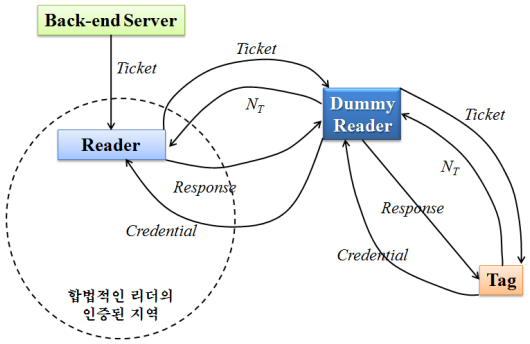

그림 5. 다중-컨텍스트 RFID 프로토콜에서의 중계 공격 시나리오

(5) 재전송 공격(replay attack): 제안한 프로토콜에서는 매 세션마다 태그가 생성하는 새로운 난수 N_T와 백-엔드 서버가 생성하는 새로운 난수 N_B를 이용하여 상호 인증을 수행하기 때문에 과거에 공격자에 의해 재전송된 난수 값들은 태그와 리더, 그리고 백-엔드 서버간의 상호 인증 과정 중에 쉽게 검출된다. 따라서 제안한 프로토콜은 재전송 공격에 안전하다.

6.2 효율성 분석

표 3은 Selim등[14]등이 제안한 다중-컨텍스트 RFID 인증 프로토콜과 제안한 다중-컨텍스트 RFID 상호 인증 프로토콜의 효율성을 비교한 결과를 보여주고 있다.

Selim등이 제안한 프로토콜은 태그와 백-엔드 서버에서 공개키 암호 연산을 각각 1회씩 수행하고, 대칭키 암호 연산은 리더에서 1회, 백-엔드 서버에서 3회를 수행함을 알 수 있다. 그러나 수동형 태그는 한정된 자원을 제공하기 때문에 공개키 암호 연산을 수행하기에는 적합하지 않다. 따라서 본 논문에서는 공개키 암호 연산을 사용하지 않고, 안전한 일방향 해쉬 함수와 대칭키 암호 연산만을 수행한 효율적인 프로

표 3. 효율성 비교

프로토콜 / 연산종류	Selim 등[14]의 프로토콜			제안한 프로토콜		
	서버	리더	태그	서버	리더	태그
공개키 암호 연산	1	0	1	0	0	0
대칭키 암호 연산	3	1	0	3	0	1
해쉬 연산	0	0	0	3	1	2

토콜을 제안하였다. 태그에서는 상호 인증을 위해 해쉬 함수 연산을 2회, 대칭키 암호 연산을 1회 수행하고, 리더는 해쉬 함수 연산만 1회를 수행한다. 또한 백-엔드 서버는 해쉬 함수 연산을 3회, 대칭키 암호 연산을 3회를 수행한다. 해쉬 함수와 대칭키 암호 연산은 공개키 암호 연산에 비해 훨씬 속도가 빠르다. 일반적으로 워크스테이션에서 공개키 암호 연산이 초당 2번 수행되는 반면, 대칭키 암호 연산은 초당 2,000번, 그리고 해쉬 함수 연산은 초당 20,000번 수행될 수 있다[22]. 또한 RFID 시스템 환경에서 공개키 암호 연산이 수행되려면 많은 자원을 필요로 하기 때문에 수동형 태그에는 상당히 비효율적이다. 따라서 제안한 프로토콜은 수동형 태그에서 공개키 암호 연산은 수행하지 않고, 해쉬 함수와 대칭키 암호 연산만을 수행하기 때문에 Selim등이 제안한 프로토콜보다 훨씬 우수한 연산 효율성을 제공한다.

Ⅶ. 결 론

본 논문에서는 Selim등이 제안한 프로토콜이 리더와 태그 간에 상호 인증을 제공하지 않기 때문에 프라이버시 침해 및 다양한 공격들에 취약함을 증명하였다. 또한 Selim등이 제안한 프로토콜은 공개키 암호 알고리즘의 사용으로 인해 과도한 자원이 요구됨으로써 무엇보다 저전력 수동형 RFID 태그에서는 부적합함을 알 수 있었다. 따라서 단일 수동형 태그와 다양한 목적을 제공하는 리더들 간의 상호 인증을 제공함으로써 태그 위장 공격을 방지하고, 프라이버시 보호 및 서비스 거부 공격, 중계 공격, 그리고 재전송 공격에도 안전한 다중-컨텍스트 RFID 상호 인증 프로토콜을 제안하였다. 결론적으로 제안한 프로토콜은 태그들의 합법적인 접근이 RFID 리더로부터 수집된 공간과 시간의 정보를 토대로 상호 인증이 수행되며, 제한된 자원을 제공하는 수동형 태그의 특성에 적합하도록 공개키 암호 알고리즘을 사용하지 않고, 안전한 일방향 해쉬 함수와 대칭키 암호 알고리즘을 수행하기 때문에 높은 안전성과 효율성을 제공한다.

참 고 문 헌

〔1〕 I. Satoh. Location-based services in ubiquitous computing environments, Service-Oriented Computing-ICSOC 2003, Springer-Verlag LNCS 2910, pp.527-42, November 2003.

〔2〕 L.Srivastava, "Ubiquitous network societies: The case of Radio Frequency Identification, background paper", International telecommunication union (ITU)new initiatives workshop on ubiquitous network societies, Geneva, Switzerland, 2005.

〔3〕 Choi, Eun Young and Lee, Su Mi and Lee, Dong Hoon, "Efficient RFID Authentication protocol for Ubiquitous Computing Environment" In International Workshop on Security in Ubiquitous Computing Systems - secubiq 2005, Volume 3823 LNCS, pp.945-95.

〔4〕 안해순, 부기동, 윤은준, 남인길, "RFID/USN 환경을 위한 개선된 인증 프로토콜," 전자공학회논문지, 제46권, 제CI-1호, pp.1-10, 2009.

〔5〕 S.Shepard, "RFID: Radio Frequency Identification", New York, USA: Mc Graw Hill, 2005.

〔6〕 ISO 14443. Identification cards－Contactless integrated circuit cards－Proximity cards. International Organization for Standardization, Geneva.

〔7〕 ISO 15693. Identification cards - Contactless integrated circuit cards－Vicinity cards. International Organization for Standardization, Geneva.

〔8〕 J.E. Bardram, R.E. Kjær and M.Ø. Pedersen. Context-aware user authentication-Supporting proximity-based login in pervasive computing, UbiComp 2003, LNCS 2864, pp.107-123, Spring-Verlag 2003.

〔9〕 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.

〔10〕 K.Finkenzeller, "RFID handbook: fundamentals and applications in Contactless smart cards and identification", (2nd ed.), Munich, Germany: Wiley, 2003.

〔11〕 S. Garfinkel and B. Rosenberg, "RFID applications, security, and privacy", Boston, USA: Addison-Wesley, 2005.

〔12〕 T. Cao and P. Shen, "Cryptanalysis of two RFID authentication protocols", International journal of network security, In press, 2008.

〔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〕 Selim Volkan Kaya, Erkay Savas, Albert Levi and Ozgur Ercetin. Public key cryptography based privacy preserving multi-context RFID infrastructure. Ad Hoc Networks, volume 7, pages 136-152, 2009.

〔15〕 S. Junichiro, H. Jae-Cheol and S. Kouichi, "Enhancing privacy of universal re-encryption scheme for RFID tags," EUC 2004, Vol. 3207 LNCS, pp.879-890, Springer-Verlag, 2004.

〔16〕 S. A. Weis, S. Sarma, R. Rivest, D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," Security in Pervasive Computing 2003, LNCS 2802, pp.201-212, Springer-Verlag, 2004.

〔17〕 Weis, S. et al, "Security and Privacy in Radio -Frequency Identification Devices", Massac-husetts Institute of Technology, 2003.

〔18〕 A. Juels and R. Pappu, "Squealing euros: privacy protection in RFID-enabled banknotes," In proceedings of Financial Cryptography-FC'03, Vol.2742 LNCS, pp.103-121, Springer-Verlag, 2003.

〔19〕 J. Yang, J. Park, H. Lee, K. Ren, and K. Kim, "Mutual authentication protocol for low-cost RFID", Handout of the Encrypt Workshop on RFID and Lightweight Crypto, 2005.

〔20〕 R. Winternitz, "A secure one-way hash function built from DES," In Proceedings of the IEEE Symposium on Information Security and Privacy, IEEE Press, pp.88-90, 1984.

〔21〕 M. Feldhofer, S. Dominikus, J. Wolkerstorfer, Strong authentication for RFID systems using the AES algorithm, in: M. Joye, J.J. Quisquater (Eds.), CHES 2004, LNCS, vol. 3156, Springer-Verlag, 2004, pp.357-370.

〔22〕 M.S. Hwang, I.C. Lin, and L.H. Li. A Simple Micro-payment Scheme, The Journal of Systems and Software, Vol.55 pp.221-229, 2001.

안 해 순 (Hae-Soon Ahn) 정회원

1996년 2월 경일대학교 컴퓨터공학과(공학사)
2001년 경일대학교 컴퓨터공학과(공학석사)
2010년 대구대학교 컴퓨터정보공학과(공학박사)
2004년~2008년 경일대학교 컴퓨터공학부 전임강사
2008년~현재 대구대학교 기초교육원 컴퓨터과정 초빙교수
<관심분야> 데이터베이스, 정보보안, 데이터베이스 보안, RFID 보안

윤 은 준 (Eun-Jun Yoon) 종신회원

2003년 경일대학교 컴퓨터공학과(공학석사)
2007년 경북대학교 컴퓨터공학과(공학박사)
2007년~2008년 대구산업정보대학 컴퓨터정보계열 전임강사
2008년~현재 경북대학교 전자전기컴퓨터학부 계약교수
2007년~현재 보안공학연구지원센터 보안공학논문지 편집위원
<관심분야> 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜

남 인 길 (In-Gil Nam) 정회원

1978년 경북대학교 전자공학과(공학사)
1981년 영남대학교 전자공학과(공학석사)
1992년 경북대학교 전자공학과(공학박사)
1978년~1981년 대구은행 전산부
1980년~1990년 경북산업대학 부교수
1990년~현재 대구대학교 컴퓨터·IT공학부 교수
<관심분야> 데이터베이스, 데이터베이스 보안, RFID 보안