Journal of The Korea Society of Computer and Information
Vol. 18, No. 10, October 2013
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2013.18.10.071

# 다중 컨텍스트 RFID 상호 인증 프로토콜의 보안 취약점 분석

김 영 백*, 김 성 수**, 정 경 호***, 김 수 용****, 윤 태 진**, 안 광 선***

# A Vulnerability Analysis of Multi-Context RFID Mutual Authentication Protocol

Young-Back Kim*, Sung-Soo Kim**, Kyung-Ho Chung***,
Soo-Yong Kim****, Tae-Jin Yun**, Kwang-Seon Ahn***

## 요 약

본 논문에서는 Ahn 등이 제안한 다중 컨텍스트 RFID 상호 인증 프로토콜(MCR-MAP)의 보안 취약점을 공격 시나리오를 통해 분석하고 이를 개선한 MCR-MAP을 제안한다. 제안된 프로토콜은 태그가 인증을 시도할 때 정당한 태그 ID와 서버에서 생성한 타임스탬프를 동시에 요구하도록 개선하였다. 그리고 태그가 신임장(Credential)을 생성할 때 서버와 태그가 공유하는 비밀키와 서버에서 생성한 타임스탬프를 XOR 연산한 값을 비밀키로 사용하도록 개선하였다. 이에 따라 제안된 프로토콜은 안전한 상호 인증을 제공하므로 위장 공격에 안전하며, 전방향안전성을 제공하므로 오프라인 전수 공격에도 안전하다. 본 논문에서는 안전성 분석을 통해서 기존 프로토콜과 제안된 프로토콜의 보안 안전성을 비교·검증하였다.

▸ Keywords : 다중 컨텍스트, RFID, 상호 인증

## Abstract

In this paper, we analyze the security vulnerability through the several attack scenarios for the MCR-MAP(Multi-Context RFID Mutual Authentication Protocol) proposed by Ahn et al. And we propose the secure mutual authentication protocol that improved a prior MCR-MAP. The suggested protocol uses the ID of the legal tag and the timestamp generated by the server, when the tag tries to authenticate. And when the tag creates the credential, we create the new secret key computing the XOR operation between the secret key shared with the server and the tag timestamp generated

•제1저자 : 김영백 •교신저자 : 김성수
•투고일 : 2013. 8. 21, 심사일 : 2013. 9. 2, 게재확정일 : 2013. 9. 10.
* 한국전자통신연구원(Electronics and Telecommunications Research Institute)
** 경운대학교 모바일공학과(Dept. of Mobile Engineering, Kyungwoon University)
*** 경북대학교 컴퓨터공학과(Dept. of Computer Engineering, Kyungpook National University)
**** 영진전문대학 컴퓨터응용기계계열(School of Computer Aided Mechanical Engineering, Yeungjin College)

by the server. As a result, the proposed protocol provides the secure mutual authentication and then is safe to spoofing attack. Also it provides forward-secrecy and then is safe to offline brute-burst attack. In this paper, we compare and verify the security vulnerability of the prior and the proposed protocol through the security analysis.

▸ Keywords : Multi-Context, RFID, Mutual Authentication

## I. 서 론

RFID(Radio Frequency IDentification) 기술은 유비쿼터스 환경의 핵심 기술 중의 하나이다[1]. RFID 시스템은 기존의 바코드 기술에 비해 간단한 연산이 가능한 논리 회로와 저장 공간을 삽입할 수 있는 장점 외에도 인식 속도와 인식 거리 등에서 많은 편리성을 제공한다[2]. 따라서 가까운 미래에는 RFID 시스템이 물류와 유통 분야에서 기존의 인식 시스템을 완전히 대체할 전망이다. 뿐만 아니라 공급 체인, 지불 시스템, 접근 제어 등 여러 분야에서 RFID 시스템의 여러 장점을 활용하기 위한 연구가 활발히 진행되고 있다. 그러나 대부분의 RFID 인증은 특정한 서비스만을 목적으로 리더와 태그를 상호 인증하는 단일 컨텍스트 RFID 기반으로 설계된다. 최근에 위치 상황에 맞는 다양한 서비스를 목적으로 단일 RFID 태그를 다양한 리더로 인증하기 위한 다중 컨텍스트 RFID 상호 인증 프로토콜(MCR-MAP: Multi-Context RFID Mutual Authentication Protocol)이 제안 되었다[3].

그림 1은 다중 컨텍스트 RFID 시스템의 구조를 나타낸다. 다중 컨텍스트 RFID 시스템은 다양한 형태로 응용이 가능하다. 예를 들어 단일 태그를 소지한 사용자가 병원에서 인증하면 건강 기록에 대한 서비스를 받고 빌딩에서 인증하면 출입 허가를 받을 수 있다. 또한 경찰서에서는 범죄 기록 조회용으로, 비자 사무실에서는 비자 기록 조회용으로, 은행에서는 금융 기록 조회용으로 사용될 수도 있다. 그리고 어떤 서비스를 제공하기 위해서는 데이터베이스 서버들 간에 비자 기록 서버와 범죄 기록 서버 및 금융 기록 서버처럼 상호 연동될 수도 있을 것이다. 이와 같이 다중 컨텍스트 RFID 시스템은 사용자와 서비스 제공자에게 다양한 편리성과 유연한 활용성을 가져다준다. 하지만 다중 컨텍스트 RFID 시스템은 다양한 용도의 서비스를 제공하는 만큼 공격자에게는 더 많은 공격 동기를 유발하게 되므로 공격자로부터의 공격 위험성도 크다. 다중 컨텍스트 RFID 시스템이 가지는 특징으로 인해서 보안 취약점 공격으로 사용자와 서비스 제공자가 입게 되는 손실도 크다. 따라서 다중 컨텍스트 RFID 시스템에서는 보다 엄격한 보안 설계가 요구된다.

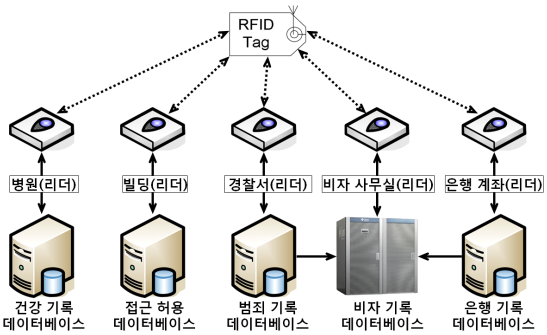



그림 1. 다중 컨텍스트 RFID 시스템 구조
Fig. 1. Multi-Context RFID system architecture

최근 Selim 등은 단일 수동형 태그와 위치 상황에 맞는 다양한 목적의 서비스를 제공하는 리더들 간의 상호 인증을 위한 MCR-MAP를 제안하였다[3]. 하지만 Ahn 등은 Selim 등이 제안한 MCR-MAP에 대해 공개키 암호 알고리즘 사용이 자원 제약적인 수동형 태그에 부적합함을 지적하고 또한 리더와 태그 간에 상호 인증이 제공되지 않음으로 인해 위장 공격이 가능함을 보였고 이를 개선한 MCR-MAP를 제안하였다[4]. 그러나 Ahn 등이 제안한 MCR-MAP는 태그 메시지 인증을 위해 태그 자신의 ID 외에 어떤 정보도 요구하지 않으므로 태그 동일성 확인이 어렵고 또한 인증서 암호화를 위해 비트 구성 정보가 공개되는 태그 ID를 비밀키로 사용함으로 인해 위장 공격과 오프라인 전수 공격을 야기하는 문제가 있다. 이에 따라 본 논문에서는 Ahn 등이 제안한 MCR-MAP의 보안 취약점을 공격 시나리오를 통해 분석하고 안전한 상호 인증과 전방향안전성을 보완하여 위장 공격과 전수 공격에 안전한 개선된 MCR-MAP을 제안한다.

본 논문은 다음과 같이 기술한다. 2장에서 본 논문과 관련

된 연구를 기술한다. 3장에서 Ahn 등이 제안한 MCR-MAP을 살펴보고 4장에서 보안 취약점을 공격 시나리오를 통해 분석한다. 5장에서 개선된 MCR-MAP을 제안하고 6장에서 보안 안전성을 평가한다. 마지막으로 7장에서 결론을 기술한다.

## II. 관련연구

### 2.1 RFID 시스템의 보안 기법

RFID 시스템에서 리더와 태그 구간은 무선 주파수를 사용하므로 보안성이 취약하다[5]. 하지만 수동형 태그의 여러 제약 조건들로 인해서 기존의 보안 분야에서 연구된 다양한 기법들은 그대로 적용되기 어렵다. 특히 태그는 공격자에 의해 정보가 위·변조되거나 복제될 수 있으므로 정당한 태그인지 인증돼야 한다. 또한 태그가 전송하는 정보가 위·변조되거나 불법 도청되지 않도록 태그가 정당한 리더와 통신하고 있는지도 인증돼야 한다. 따라서 안전한 RFID 시스템을 위해서는 리더와 태그의 상호 인증 설계를 필수적으로 고려해야 한다[6].

RFID 시스템의 보안 기법은 크게 물리적 접근 방법과 암호학적 접근 방법으로 분류된다. 초기 RFID 보안 대책으로 물리적 접근 방법이 주로 제안되었으며 KILL 명령어 기법, Active Jamming 기법, Blocker 태그 기법 등이 있다[7]. 그러나 대부분의 물리적 접근 방법은 RFID 시스템의 활용성을 과도하게 제약한다. 최근에는 해쉬 함수 및 암호 알고리즘을 이용하는 암호학적 접근 방법이 활발히 연구되고 있다. 해쉬 기반의 대표적인 보안 기법으로는 S. Weis 등이 제안한 hash-lock 기법과 randomized hash-lock 기법 그리고 M. Okubo 등이 제안한 hash-chin 기법 등이 있다[8-9]. 공개키 기반의 보안 기법으로는 A. Juels와 R. Pappu이 제안한 재암호화 기법과 P. Golle 등이 확장한 재암호화 기법이 있다[10-11]. 하지만 공개키 알고리즘은 수동형 태그의 구현 시 요구사항인 회로 면적 7,000 게이트와 최대 250us 응답 시간(T1 time)에 맞게 구현되기 어렵다[12]. 따라서 외부에 재암호화를 위한 별도의 장비가 필요하다. 반면에 대칭키 알고리즘은 M. Feldhofer 등이 수동형 태그에 적용이 가능한 저전력 AES를 설계하고 이를 이용한 challenge-response 프로토콜을 제안한 이후 경량화 연구들이 다양하게 진행되고 있다[13]. 최근에는 AES-64 구현 연구와 AES-128 구현 연구 결과가 발표된 바 있어 저전력 대칭키 알고리즘의 수동형 태그 적용이 늘어 날 것으로 보인다[14-15]. 암호 알고리즘은 전수 공격을 방지하기 위해서 최소 64 비트 이상이 필요하므로 본 논문에서는 128 비트의 저전력 AES를 사용하는 것으로 가정한다[14].

### 2.2 케르크호프스의 원리(Kerckhoffs's principle)

현대 암호 체계의 안전성은 Kerckhoffs의 원리에 기초를 두고 있다[16]. 따라서 보안 시스템은 Kerckhoffs의 원리에 의거 암호 알고리즘이 공격자들에게 알려져 있다는 것을 전제로 설계돼야 한다. 즉 보안 시스템의 안전성은 암호 알고리즘의 비밀에 의해서가 아니라, 키의 비밀을 보호함으로서 보장된다. 비밀키는 가능한 복잡하고 추측 불가능(random)하도록 구성돼야 한다. 유추하기 쉬운 형태의 비밀키는 보안 설계를 쉽게 허물어지게 한다. 대부분의 암호 알고리즘은 이론적으로 전수 공격에 대해 안전하지 못하며, 충분한 시간이 존재한다면 암호화된 정보를 해독하는 것이 가능하다. 전수 공격(brute force attack)은 암호 해독을 위해 키 공간(key space)에 속하는 모든 키 후보를 대입하는 것을 의미한다. 공격 기법 중 가장 난이도가 낮으나 공격 대상에 대한 충분한 정보를 가지고 키 공간의 크기를 줄일 수 있다면 매우 효율적이고 가장 강력한 공격이 될 수 있다. 결과적으로 공격자가 전수 공격에 더 많은 시간을 투입하게 할수록 보안 시스템은 안전해진다.

RFID 태그의 ID는 민간 국제표준화 기구인 EPCglobal에 의해 표준화가 진행되고 있다. 현재 96비트 EPC(electronic product code)인 GID-96이 사실상의 RFID 표준으로 자리를 잡아가고 있다[17]. 그림 2는 EPC 표준인 GID-96 코드를 나타낸다. EPC 코드는〈Version Header, EPC manager, Product Class, Serial Number〉의 계층적 구조를 갖으며 상품 하나하나에 96비트의 EPC 코드를 부여하여 해당 상품에 관한 생산정보나 유통이력 등 상품의 상세정보를 인터넷을 통해 사용자에게 즉시 제공할 수 있다.

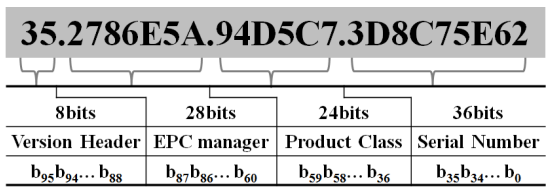



그림 2. GID-96(General IDentifier)의 비트 필드
Fig. 2. The bit field of GID-96(General IDentifier)

그림 2에서 GID의 특징은 개별 상품의 고유한 식별 번호

를 나타내는 Serial Number를 제외한 상위 비트는 거의 고정된다는 것이다. 더구나 Serial Number는 제조 지역이나 제조 일자에 따라 연속적으로 부여되는 경우가 많다. 태그에 부여되는 ID는 EPC 코드 체계를 따르거나 자체 코드 체계를 사용한다. 어떤 경우이든 그림 2에서 보는 것처럼 태그 ID의 비트 구성 정보는 인터넷 등을 통해 쉽게 접근이 가능하다. 결국 공격자는 수집한 사전 정보를 근거로 추정을 통해 키 공간(key space)의 크기를 전수 공격이 가능한 범위 내로 줄일 수 있다. 따라서 태그 ID를 비밀키로 사용하는 것은 Kerckhoffs의 원리에 위배되므로 적절하지 않다. 유추하기 쉬운 형태의 비밀키 사용은 전수 공격에 안전하지 못하며 보안 시스템의 안전성을 쉽게 무너지게 한다.

## III. Ahn 등이 제안한 MCR-MAP

본 장에서는 Ahn 등이 제안한 MCR-MAP를 소개한다[4]. 이 프로토콜을 위한 가정 사항은 Selim 등의 가정 사항과 같다고 전제한다. 먼저 본 논문에서 사용하는 기호와 약어에 대해 간략한 설명을 표 1과 같이 정리하여 나타낸다.

표 1. 기호 및 약어 정리
Table 1. Symbols and abbreviations

| 기호 | 의미 |
|---|---|
| T | RFID 태그 |
| R | RFID 리더 |
| TID | 태그 T의 아이디 값(≥128 비트) |
| RID | 리더 R의 아이디 값(≥128 비트) |
| K | 백 엔드 서버와 태그가 공유한 비밀키(secret key) |
| RK | 백 엔드 서버와 리더가 공유한 비밀키(secret key) |
| RL | 위치 서버가 가지고 있는 리더의 위치 정보 |
| TIT | Ticket 발급 시간 인장(ticket issuance timestamp) |
| NB | 서버가 생성한 난수(nonce) |
| NT | 태그가 생성한 난수(nonce) |
| MACB | 서버 메시지 인증 코드(message authentication code) |
| MACT | 태그 메시지 인증 코드(message authentication code) |
| h( ) | 단방향 해쉬 함수(one-way hash function) |
| E( ) | 대칭키 암호화 함수 |
| D( ) | 대칭키 복호화 함수 |
| PRNG | 의사난수생성기(Pseudo Random Number Generator) |
| x ‖ y | 연접(concatenation) 연산 |
| ⊕ | 배타적 논리합(XOR; eXclusive OR) 연산 |
| (메시지)A | 공격자가 생성한 메시지(attacker side message) |
| (숫자) | 메시지 전송 단계(message transmission step) |
| (알파벳) | 인증 연산 단계(authentication operation step) |

그림 3은 Ahn 등의 프로토콜이 상호 인증을 수행하는 전체 과정을 보여준다. 이 프로토콜은 상호 인증을 위해서 매 세션 마다 메시지 전송 단계 (1)~(12)와 인증 연산 단계 (A)~(F)를 순서대로 수행한다. 이를 기능별로 크게 4개 부분으로 나누어 살펴보면 다음과 같다.

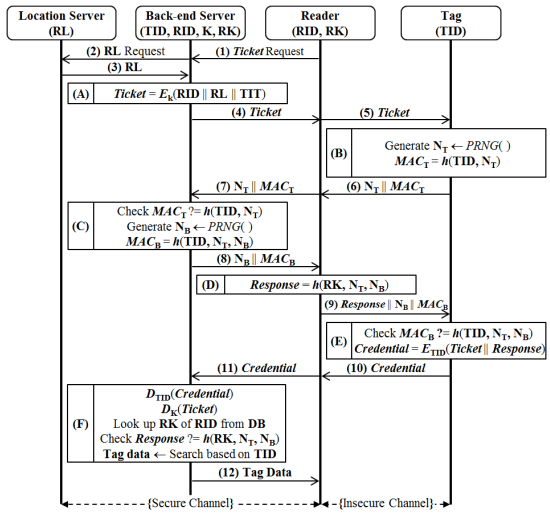



그림 3. Ahn 등이 제안한 MCR-MAP
Fig. 3. MCR-MAP proposed by Ahn et al.

### 1) 서버의 티켓 발급 : (1)~(5)단계

태그가 리더의 인식 영역 내에 접근하면 인증 세션이 시작된다. 먼저 리더는 백 엔드 서버에 *Ticket*을 요청하고, 백 엔드 서버는 위치 서버(Location Server)에 리더의 위치 정보를 요청하여 수신하고, 리더의 식별자 RID와 리더의 위치 정보 RL과 타임스탬프 TIT를 서버와 태그가 공유하는 비밀키 K로 암호화하여 $Ticket = E_K(RID \,||\, RL \,||\, TIT)$을 생성하고, 리더를 거쳐 태그로 전송한다.

### 2) 태그 메시지 인증 코드 검증 : (B)단계~(C)1행

*Ticket*을 수신한 태그는 난수 $N_T$를 임의(random)로 생성하고, 자신의 식별자 TID와 NT를 해쉬하여 태그의 메시지 인증 코드 $MAC_T = h(TID, NT)$를 생성하고, $N_T$와 $MAC_T$를 리더를 거쳐 백 엔드 서버로 전송한다. 그리고 백 엔드 서버는 수신한 태그의 메시지 인증 코드 $MAC_T \stackrel{?}{=} h(TID, N_T)$를 검증한다.

### 3) 서버 메시지 인증 코드 검증 : (C)2행~(E)1행

백 엔드 서버는 난수 $N_B$ 생성하고, TID와 $N_T$와 $N_B$를 해쉬하여 서버의 메시지 인증 코드 $MAC_B = h(TID, N_T, N_B)$를 생성하고, $N_B$와 $MAC_B$를 리더로 전송한다. 리더는 서버

와 자신이 공유하는 비밀키 RK와 태그의 난수 $N_T$와 서버의 난수 $N_B$를 해쉬하여 *Response* = h(RK, $N_T$, $N_B$)를 생성하고, *Response*와 $N_B$와 $MAC_B$를 태그로 전송한다. 그리고 태그는 서버의 메시지 인증 코드 $MAC_B$ ?= h(TID, $N_T$, $N_B$)를 검증한다.

4) 태그의 인증서 발급 및 검증 : (E)2행~(12)단계

태그는 이전 단계에서 수신한 *Ticket*과 *Response*를 태그의 식별자 TID로 암호화하여 인증서 *Credential* = $E_{TID}$(*Ticket* || *Response*)를 생성하고, 리더를 거쳐 백 엔드 서버로 전송한다. 백 엔드 서버는 *Credential*을 태그의 식별자 TID로 복호화 하고, *Ticket*을 서버와 태그가 공유하는 비밀키 K로 복호화 한다. 그리고 DB로부터 리더의 식별자인 RID에 해당하는 리더의 비밀키 RK를 검색하여 *Response* ?= h(RK, $N_T$, $N_B$)를 검증한다. 일치하면 정당한 리더와 태그로 상호 인증에 성공한 것으로 판단하고 식별자 TID의 태그 정보 Tag data를 리더에게 전송하고 인증 과정을 종료한다.

## Ⅳ. Ahn 등이 제안한 MCR-MAP의 보안 취약점 분석

본 장에서는 Ahn 등의 MCR-MAP의 보안 취약점을 제시하고 2가지 공격 시나리오를 통해 분석한다. 첫째, 태그 메시지 인증을 위해 태그 자신의 ID 외에 어떤 정보도 요구하지 않으므로 태그 동일성 확인이 어렵다. 둘째, 인증서 암호화를 위해 비트 구성 정보가 공개되는 태그 ID를 비밀키로 사용함으로 인해 위장 공격과 오프라인 전수 공격을 야기한다. 결국 공격자는 정당한 태그 ID를 알아낼 수 있을 뿐만 아니라 인증까지 수행할 수 있다.

### 4.1 시나리오 ① : 위장 공격

공격자는 사전에 알아 낸 정보로 추정한 정당한 태그 ID의 일부분과 임의로 생성하거나 사전에 수집된 일련의 값을 연접하여 태그 ID를 생성한다. 공격자는 태그 A를 통해 자신이 생성한 태그 ID로 공격을 시도하고 실패하면 같은 방법으로 태그 ID를 갱신하여 여러 세션에 걸쳐서 공격을 반복한다. 그림 4는 공격 시나리오 ①의 수행 과정을 보여준다. 보안 공격에 관여된 단계를 회색으로 표시하였다. 이를 살펴보면 아래와 같다. 인증 연산 (B)와 (E) 외의 단계는 정상적으로 수행된다.

1) (B)단계 : 공격자에 의해 수행됨

공격자 태그 A는 사전에 알아 낸 정보로 추정한 정당한 태그 ID의 일부분과 임의로 생성하거나 사전에 수집된 일련의 값을 연접하여 $TID^A$를 생성한 후 난수 $N_T{}^A$를 임의로 생성하고, $TID^A$와 $N_T{}^A$를 해쉬하여 태그의 메시지 인증 코드 $MAC_T{}^A$ = h($TID^A$, $N_T{}^A$)를 생성한다.

2) (C)단계 : 공격에 상관없이 수행됨

백 엔드 서버는 공격 사실을 감지하지 못하며 태그의 메시지 인증 코드 $MAC_T{}^A$ ?= h(TID, $N_T{}^A$ 검증을 정상적으로 수행한다. 해쉬 연산의 단방향성으로 인해 서버가 관리하는 DB에서 유효한 TID를 순차적으로 가져와 수신한 $N_T{}^A$와 함께 해쉬하여 수신한 $MAC_T{}^A$ 값과 비교하는 검증을 반복한다. 결국 태그 A가 생성한 $TID^A$가 유효한지를 검증하는 것이다. $N_T{}^A$의 값에 상관없이 $TID^A$ = TID를 만족하는 TID가 있으면 검증은 성공한다.

3) (E)단계 : 공격자에 의해 수행됨

공격자 태그 A는 자신이 생성한 $TID^A$와 $N_T{}^A$ 그리고 수신한 NB를 이용해 $MAC_B$ ?= h($TID^A$, $N_T{}^A$ , $N_B$)를 검증해 본다. 검증에 성공한 경우 공격자는 태그 A를 이용하여 공격에 성공한 것이다. 즉 $TID^A$ = TID이므로 정당한 TID를 알아 낸 것이다. 이후 단계에서 태그 A는 정상적인 $Credential^A$ = ETID(*Ticket* || *Response*)를 생성하고 인증 과정을 통과하여 합법적인 태그로 위장할 수 있다. 만일 공격자 태그 A가 (9)단계에서 $MAC_B$를 전송받지 못했거나 $MAC_B$ 검증에 실패한 경우 $TID^A$를 갱신하고 (1)단계부터 다시 시작한다. Ahn 등의 프로토콜에서는 태그 동일성 확인이 어려워 이러한 공격을 감지하거나 걸러낼 수 없으므로 여러 세션에 걸쳐서 반복 공격이 가능하다.

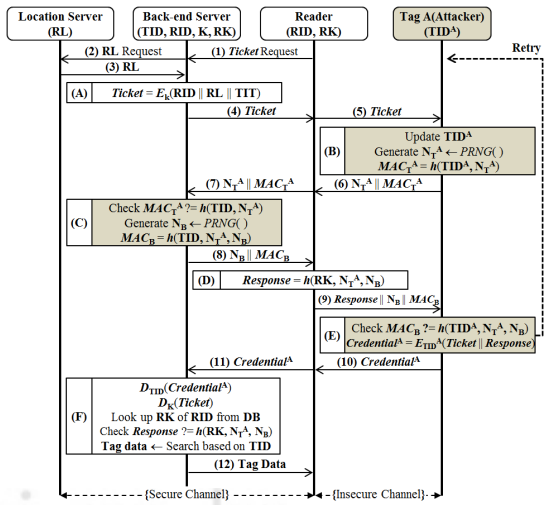



그림 4. 시나리오 ① : 위장 공격
Fig. 4. Scenario ① : spoofing attack

### 4.2 시나리오 ② : 오프라인 전수 공격

공격자 태그 A가 인증 과정에 직접 참여하여 공격하는 시나리오 ①의 경우 프로토콜에 참여하는 각 요소들 간의 물리적 전송 속도와 연산 속도에 제한적일 것이다. 따라서 공격자가 사전에 인터넷 등을 통해 수집한 정보로 추정한 정당한 ID의 일부분이 충분하지 않을 경우 시간적 제약으로 인해 공격이 실효성을 거두기 어려울 수도 있다. 이럴 경우에는 공격자는 정상적인 상호 인증 세션을 충분히 도청한 후 수집된 데이터를 이용하여 오프라인 전수 공격을 시도할 수 있을 것이다.

먼저 공격자는 정상적인 인증 세션을 도청하여 메시지 전송 (5), (9), (10)단계의 *Ticket, Response, Credential* 데이터를 수집한다. 리더와 태그 사이는 비 보안 무선 채널 구간이므로 도청이 가능하다.

오프라인에서 공격자는 연산 속도가 충분히 빠른 다수 워크스테이션에 인증서를 생성하고 검증하는 연산 *Credential* ?= $E_{TID^A}$(*Ticket* || *Response*)을 자동화하여 반복적으로 수행하도록 설치한다. 이때 비밀키 $TID^A$는 공격자가 사전에 알아 낸 정보로 추정한 정당한 ID의 일부분과 임의로 생성하거나 사전에 수집된 일련의 값을 연접하여 반복적으로 생성한다. 공격자가 비밀키 $TID^A$로 생성한 $Credential^A$과 (10)단계에서 도청한 *Credential*을 비교하여 일치하면, 즉 $Credential^A$ = *Credential*이면 공격은 성공한 것이다. Ahn 등의 프로토콜에는 전방향안전성이 없으므로 공격자는 $TID^A$를 이용하여 임의의 세션에서 정상적으로 인증하여 합법적인 태그로 위장할 수 있다.

결국 인증 과정에서 평문 *Ticket*와 *Response* 그리고 암호문 *Credential*이 드러나므로 비밀키 TID를 맞춰보는 전수 공격이 가능하다. 게다가 비밀키로 사용되는 태그의 식별자 TID는 비트 구성 정보가 공개되어 비트 전체가 무작위성을 갖는 것이 아니므로 충분한 사전 정보를 근거로 추정을 통해 키 공간(key space)의 크기를 전수 공격이 가능한 범위 내로 줄일 수 있다.

## V. 개선된 MCR-MAP

다중 컨텍스트 RFID 시스템에서는 보다 엄격한 보안 설계가 요구된다. 본 장에서는 Ahn 등의 MCR-MAP에서 분석된 보안 취약점을 개선하여 안전한 MCR-MAP를 제안한다. 그림 5는 제안하는 MCR-MAP이 상호 인증을 수행하는 전체 과정을 보여준다. 기존의 프로토콜에서 재설계한 부분을 회색으로 표시하였다. 이를 살펴보면 아래와 같다.

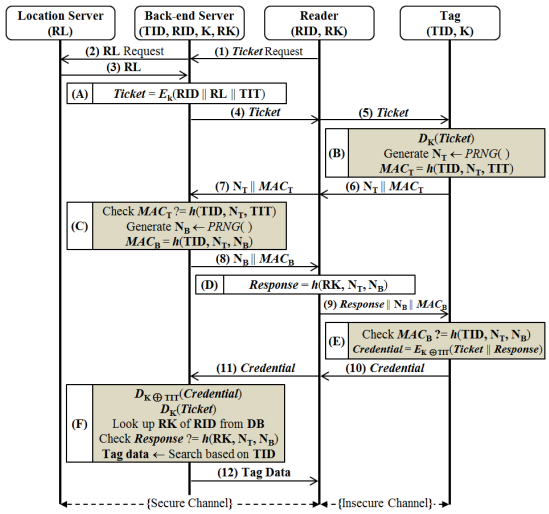



그림 5. 개선된 MCR-MAP
Fig. 5. improved MCR-MAP

#### 1) (B)단계

태그는 서버와 자신이 공유하는 비밀키 K로 $D_K$(*Ticket*)을 복호화 하여 타임스탬프 TIT를 추출한다. 이때 비밀키 K를 가진 정당한 태그만이 타임스탬프 TIT 값을 추출할 수 있다. 이는 향후 인증 과정에서 서버가 인증을 요구하는 태그와 *Ticket* 받은 정당한 태그와의 동일성을 확인하기 위해 사용한다. 그리고 태그는 난수 $N_T$를 임의로 생성하고, 자신의 식별자 TID와 자신이 생성한 난수 $N_T$와 *Ticket*에서 추출한 타임스탬프 TIT를 해쉬하여 태그의 메시지 인증 코드 $MAC_T$ = h(TID, $N_T$, TIT)를 생성한다.

#### 2) (C)단계

백 엔드 서버는 리더로부터 수신한 태그의 메시지 인증 코드 $MAC_T$ ?= h(TID, $N_T$, TIT)를 검증한다. 서버는 유효한 타임스탬프 TIT 값과 정당한 TID를 동시에 만족하는지 여부를 통해 *Ticket*을 받은 정당한 태그와의 동일성과 정당성을 검증한다.

#### 3) (E)단계

태그는 이전 단계에서 수신한 *Ticket*과 *Response*를 서버와 태그가 공유하는 비밀키 K와 타임스탬프 TIT를 XOR 연산한 K⊕TIT 값을 키로 암호화하여 인증서 *Credential* = $E_{K⊕TIT}$(*Ticket* || *Response*)를 생성한다. 특히 암호화 키로 K⊕TIT 값을 설정하여 타임스탬프 TIT에 따라 키의 값이 매 세션마다 갱신되게 함으로써 전방향안전성이 향상된다.

4) (F)단계

백 엔드 서버는 수신한 *Credential*을 서버와 태그가 공유하는 비밀키 K와 타임스탬프 TIT를 XOR 연산한 K⊕TIT 값을 키로 하여 복호화 한다. 정당한 태그의 비밀키 K와 유효한 TIT를 동시에 만족하는지를 확인함으로써 *Ticket*을 받은 정당한 태그와 *Credential*을 발급한 태그의 동일성을 판단한다.

## Ⅵ. 안전성 분석

본 장에서는 제안한 MCR-MAP의 보안 안전성에 대해 분석한다. 먼저 Ahn 등이 제안한 MCR-MAP의 보안 취약점 분석에서 제시했던 공격 시나리오에 대해 제안하는 프로토콜의 안전성을 살펴보고 기존 MCR-MAP와의 보안 안전성을 비교한다.

### 6.1 공격 시나리오 ①에 대한 안전성

제안하는 프로토콜에서는 (C)단계에서 백 엔드 서버는 태그의 메시지 인증 코드 $MAC_T$ ?= h(TID, $N_T$, TIT)를 검증할 때 정당한 TID와 유효한 타임스탬프 TIT를 동시에 만족할 것을 요구한다. 이때 공격자 태그는 (B)단계에서 $D_K$(*Ticket*)을 복호화 할 수 있는 비밀키 K가 없으므로 유효한 TIT를 만들 수 없다. 따라서 공격자가 시나리오 ①을 통해 정당한 TID를 알아내고 정당한 태그로 인증 받는 것은 불가능하다.

### 6.2 공격 시나리오 ②에 대한 안전성

제안하는 프로토콜에서도 인증 과정에서 평문 *Ticket*과 *Response* 그리고 암호문 *Credential*이 드러나므로 *Credential* ?= $E_{(K\oplus TIT)}{}^{A}$(*Ticket* || *Response*)를 수행하여 비밀키 K⊕TIT를 맞춰보는 전수 공격이 가능하다. 그러나 공격자는 비밀키 K⊕TIT에 대한 사전 정보를 수집할 수 없고 비트 전체가 무작위성을 갖고 있으므로 어떤 추정을 통해서도 키 공간(key space)의 크기를 줄일 수는 없다. 더구나 우연히 비밀키 K⊕TIT를 알아낸다 하더라도 매 세션마다 타임스탬프 TIT가 갱신됨에 따라 비밀키 K⊕TIT도 변경되므로 전방향안전성을 가진다. 따라서 공격자가 시나리오 ②를 통해 해당 세션에서 도청한 정보를 통해 다음 세션에서 정당한 태그로 인증 받는 것은 불가능하다.

### 6.3 보안 안전성 비교

표 2는 Ahn 등이 논문 [4]에서 기술한 프로토콜의 안전성 분석과 비교 결과를 기준으로 제안한 프로토콜과의 비교 결과를 요약 정리하여 나타낸 것이다. Selim 등의 프로토콜의 안전성은 Ahn 등이 지적한 바와 같다. 또한 Ahn 등의 프로토콜에서 상호 인증과 위장 공격을 제외한 안전성은 Ahn 등이 주장하는 바와 같다. 제안한 프로토콜은 Ahn 등이 제안한 프로토콜에서 상호 인증과 위장 공격에 대한 보안 취약점을 개선하였다. 이에 따라 각 공격 유형에 대한 보안 안전성이 유지되거나 강화되었다. 표 2에 보안 안전성이 강화된 부분을 회색으로 표시하였다. 이를 살펴보면 아래와 같다.

표 2. 보안 안전성 비교
Table 2. Comparison of security-safety

| 프로토콜 / 공격유형 | Selim 등의 프로토콜[3] | Ahn 등의 프로토콜[4] | 제안하는 프로토콜 |
|---|---|---|---|
| 상호 인증 | × | × | ○ |
| 위치 추적 | × | ○ | ○ |
| 재전송 공격 | ○ | ○ | ○ |
| 위장 공격 | × | × | ○ |
| 중간자 공격 | ○ | ○ | ○ |
| 서비스 거부 공격 | × | ○ | ○ |

Ahn 등의 프로토콜은 정당한 태그에 대해 인증을 제공하지만 공격자의 태그 A에 대해서도 전수 공격을 통해 알아낸 정당한 TID만 보내면 인증을 제공하는 문제가 있다. 게다가 공격자의 태그 A가 인증을 시도할 때 태그 자신이 생성하는 정보 외에 어떤 정보도 요구하지 않으므로 인해 서버가 인증하려는 정당한 태그와 인증을 요구하는 태그와의 동일성을 확인할 수 없었다. 따라서 Ahn 등의 프로토콜은 상호 인증과 위장 공격에 대한 보안 안전성을 제공하지 못한다.

이에 반해 제안하는 프로토콜은 (B), (C), (E), (F)단계에서 타임스탬프 TIT를 적극 활용함으로써 Ahn 등의 프로토콜에 비해 각 공격 유형에 대한 보안 안전성이 유지되거나 강화되었다. (C)단계에서 백 엔드 서버는 태그의 메시지 인증 코드 $MAC_T$를 해쉬하여 태그를 검증하고, (E)단계에서 태그는 서버의 메시지 인증 코드 $MAC_B$를 해쉬하여 서버를 검증한다. 특히 서버가 $MAC_T$ ?= h(TID, $N_T$, TIT)를 검증할 때 타임스탬프 TIT가 (A)단계에서 생성한 값과 일치할 것을 요구한다. 이를 통해 메시지 인증 코드 $MAC_T$를 보낸 태그가 (B)단계에서 *Ticket*을 받은 태그와의 동일한지와 $D_K$(*Ticket*)을 복호화 할 수 있는 비밀키 K를 가진 정당한 태그인지를 확인한다. 또한 (E)단계와 (F)단계에서 *Credential*의 암·복호화 키로 K⊕TIT 값을 설정함으로서

타임스탬프 TIT를 통해 매 세션마다 키를 갱신되게 하고 *Ticket* = $E_K$(RID || RL || TIT)을 받은 태그와 *Credential* = $E_{K \oplus TIT}$(*Ticket* || *Response*)을 발급한 태그의 동일성을 비밀키 K와 타임스탬프 TIT를 통해 검증한다. 따라서 공격자가 각 인증 단계에서 도청이 가능하더라도 정당한 태그로 인증 받거나 위장할 수 없다. 따라서 제안하는 프로토콜은 안전한 상호 인증을 제공하므로 위장 공격에 안전하며 전방향안전성을 제공하므로 오프라인 전수 공격에도 안전하다.

## IV. 결 론

본 논문에서는 Ahn 등이 제안한 MCR-MAP의 보안 취약점을 제시하고 공격 시나리오를 통해 이를 분석하였다. Ahn 등이 제안한 인증 프로토콜은 첫째, 태그 메시지 인증을 위해 태그 자신의 ID 외에 어떤 정보도 요구하지 않으므로 태그 동일성 확인이 어렵고 둘째, 인증서 암호화를 위해 비트 구성 정보가 공개되는 태그 ID를 비밀키로 사용함으로 인해 위장 공격과 오프라인 전수 공격을 야기하는 문제가 있었다. 결국 공격자는 정당한 태그 ID를 알아낼 수 있을 뿐만 아니라 인증까지 수행할 수 있었다. 이에 따라 본 논문에서는 태그의 메시지 인증 코드 검증과 인증서 암·복호화에 백 엔드 서버와 태그가 공유하는 비밀키 K와 타임스탬프 TIT를 활용하여 보안 안전성을 강화한 개선된 MCR-MAP을 제안하였다. 안전성 분석 결과, 개선된 프로토콜은 공격 시나리오를 통한 공격에 안전하며 Ahn 등의 프로토콜에 비해 각 공격 유형에 대한 보안 안전성이 유지되거나 강화되었다. 특히 제안하는 프로토콜은 안전한 상호 인증을 제공하므로 위장 공격에 안전하며 전방향안전성을 제공하므로 오프라인 전수 공격에도 안전하다.

결론적으로 제안한 프로토콜은 위치 상황에 맞는 다양한 목적의 서비스를 제공하는 다중 컨텍스트 RFID 환경에서 합법적인 태그와 리더들 간의 안전한 상호 인증을 수행하므로 실제 응용에서 사용자와 서비스 제공자에게 다양한 편리성과 유연한 활용성을 더욱 증대시켜 줄 것으로 전망한다.

## 참고문헌


〔1〕 M. Weiser, "Some Computer Science Issues in Ubiquitous Computing," Communications of the ACM, vol. 36, no. 7, pp. 74-84, July 1993.

(2) K. Finkenzeller, "RFID Handbook: Fundamentals and applications in Contactless Smart Cards and Identification," Second Edition, John Wiley & Sons Ltd, pp. 195-219, 2003.

(3) Selim Volkan Kaya, Erkay Savas, Albert Levi and Ozgur Ercetin, "Public key cryptography based privacy preserving multi-context RFID infrastructure," Ad Hoc Networks, Vol. 7, pp. 136-152, Jan. 2009.

(4) H.S. Ahn, E.J. Yoon, I.G. Nam, "Privacy Preserving and Relay Attack Preventing Multi-Context RFID Mutual Authentication Protocol," Journal of KICS, Vol. 36, No. 8, pp. 1028-1037, Aug. 2011.

(5) N. Borselius, "Mobile Agent Security," Electronics and Communication Engineering Journal, vol. 14, no. 5, pp. 211-218, Oct. 2002.

(6) A. Juels, "RFID Security and Privacy: A Research Survey," IEEE Journal of Selected Areas in Communications, vol. 24, no. 2, pp. 381-394, Feb. 2006.

(7) A. Juels, R.L. Rivest, M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," 10th ACM Computer and Communications Security Conference (CCS'03), pp. 103-111, Oct. 2003.

(8) S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," In Security in Pervasive Computing, LNCS 2802, pp.201-212, 2005.

(9) M. Ohkubo, K. Suzuki, and S. Kinoshita, "A Cryptographic Approach to "Privacy-Friendly" tag," RFID Privacy Workshop, 2003.

(10) A. Juels, R. Pappu, "Squealing Euros : Privacy protection in RFID-enabled banknotes," Financial cryptography International conference, LNCS 2742, pp.103-123, 2003.

(11) P. Golle, M. Jakobsson, A. Juels, and P. Syverson, "Universal Re-encryption for mixnets," RSA Conference Cryptographers Track '04, LNCS 2964, pp.163-178, 2003.

(12) Y.S. Kang, Y.J. Choi, D.H. Choi, S.Y. Lee,

H.S. Lee, "Design Implementation of Lightweight and High Speed Security Protocol Suitable for UHF Passive RFID Systems," Journal of KICS, Vol. 20, No. 4, pp. 117-134, Aug. 2010.

(13) M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," Cryptographic Hardware and Embedded Systems, LNCS 3156, pp.85-140, 2004.

(14) T. Good, M. Benaissa, "A low-frequency RFID to challenge security and privacy concerns," Proceedings of IEEE 6th International Conference on Mobile Adhoc and Sensor Systems (MASS'09), pp. 856-863 Oct. 2009.

(15) M. Kim, J. Ryou, Y. Choi and S. Jun, "Low-cost Cryptographic Circuits for authentication in Radio Frequency Identification Systems," Proceedings of International symposium on Consumber Electronics (ISCE'06), pp. 1-5, Jun. 2007.

(16) A. Kerckhoffs, "La cryptographie militaire," Journal des sciences militaires, vol. 9, pp.5-83, Jan. 1883. (http://petitcolas.net/fabien/kerckhoffs/)

(17) EPCTM Generation 1 Tag Data Standards Version 1.1 Rev.1.27, EPCglobal, Standard Specification, May 2005.

## 저 자 소 개

김 영 백
1996: 영남대학교 사회학과 문학사
2007: 경북대학교 컴퓨터공학과 공학석사
2010: 경북대학교 컴퓨터공학과 공학박사수료
현 재: 한국전자통신연구원 선임연구원
관심분야: RFID, 정보보호, Lidar 신호처리
Email : realtech@daegu.ac.kr

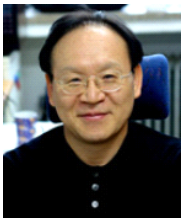
김 성 수
2002: 금오공과대학교 컴퓨터공학과 공학사
2005: 경북대학교 컴퓨터공학과 공학석사
2012: 경북대학교 컴퓨터공학과 공학박사
현 재: 경운대학교 모바일공학 조교수
관심분야: 임베디드 시스템, 정보보호, RFID , 센서 네트워크
Email : ninny@ikw.ac.kr

정 경 호
2000: 대구대학교 컴퓨터정보공학 공학사
2002: 경북대학교 컴퓨터공학과 공학석사
2011: 경북대학교 컴퓨터공학과 공학박사
현 재: 경북대학교 컴퓨터공학과 외래교수
관심분야: 임베디드 시스템, RFID, 정보보호
Email : mccart@knu.ac.kr

김 수 용
1989: 경북대학교 전자공학과 공학사.
1993: 경북대학교 전자공학과 공학석사.
1995: 경북대학교 전자공학과 공학박사수료
현 재: 영진전문대학 컴퓨터응용기계계열 교수
관심분야: 임베디드시스템, 로봇자동화
Email : sykim0622@yjc.ac.kr

윤 태 진

1994: 경북대학교 컴퓨터공학과 공학사
1996: 경북대학교 컴퓨터공학과 공학석사
2012: 경북대학교 컴퓨터공학과 공학박사
현 재: 경운대학교 모바일공학 부교수
관심분야: 임베디드 시스템, 정보보안, 센서 네트워크
Email : tjyun@ikw.ac.kr



안 광 선

1972: 연세대학교 전기공학과 공학사
1975: 연세대학교 전자공학과 공학석사
1980: 연세대학교 전자공학과 공학박사
현 재: 경북대학교 컴퓨터공학과 교수
관심분야: 임베디드 시스템 및 RFID 시스템
Email : gsahn@knu.ac.kr