情報保護學會論文誌
第20卷 第4號, 2010. 8

서버와 리더의 위장공격 탐지가 가능한 랜덤 ID기반 RFID 상호 인증 프로토콜*

여 돈 구,† 이 상 래, 장 재 훈, 염 흥 열‡
순천향대학교

A Random ID-based RFID Mutual authentication protocol for detecting Impersonation Attack against a back-end server and a reader*

Don-Gu Yeo,† Sang-Rae Lee, Jae-Hoon Jang, Heung-Youl Youm‡
Soonchunhyang University

요 약

최근에 경량화된 해쉬 기반 RFID(Radio Frequency Identification) 상호 인증 프로토콜의 연구결과가 많이 발표되고 있다. 대부분의 프로토콜이 백엔드 서버와 리더 구간을 안전하다고 가정하고 있어, 백엔드 서버와 리더의 위장 공격을 고려하지 않고 있다. 현실적으로 공격자 입장에서는 태그 공격보다는 백엔드 서버나 리더 공격이 공격대비 높은 효율성을 가질 것이다. 본 논문에서는 보다 현실성 있는 해쉬 기반 RFID 상호 인증 프로토콜을 설계하기 위해 전 구간을 안전하지 않은 공개 채널로 가정한다. 기존 연구에서 지원하는 상호인증을 지원하고, 재전송 공격 및 태그와 리더의 위장공격, 태그 위치추적공격, 서비스 거부 공격에 안전하다. 추가로, 모든 개체의 위장 공격으로부터 안전하고, 태그 탐색을 위한 개선된 백엔드 서버 검색률을 지원하는 안전하고 효율적인 RFID 상호 인증 프로토콜을 제안한다. 마지막으로 기존 연구와의 안전성 분석과 효율성 분석을 제시한다.

ABSTRACT

Recently many mutual authentication protocol for light-weight hash-based for RFID have been proposed. Most of them have assumed that communications between a backend server and reader are secure, and not considered threats for backend server and RFID reader impersonation. In the real world, however, attacks against database or reader are more effective rather than attacks against RFID tag, at least from attacker's perspective. In this paper, we assume that all communications are not secure to attackers except the physical attack, and considering realistic threats for designing a mutual authentication protocol based on hash function. And It supports a mutual authentication and can protect against the replay attack, impersonation attack, location tracking attack, and denial of service attack in the related work. We besides provide a secure and efficient RFID mutual authentication protocol which resists impersonation attacks on all of the entities and alow a backend server to search tag-related information efficiently. We conclude with analyzing the safety and efficiency among latest works.

Keywords: Hash-based RFID, Random ID, Mutual Authentication, Self-depence

* 접수일(2010년 4월 13일), 수정일(1차: 2010년 6월 10일), 게재확정일(2010년 7월 10일)
* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음. (NIPA-2010-(C1090-1031-0005))
† 주저자, h7ei@sch.ac.kr
‡ 교신저자, hyyoum@sch.ac.kr

I. 서 론

유비쿼터스 환경에서 RFID(Radio Frequency Identification) 태그를 사물에 부착하여 사물을 식별하고, 정보를 빠르고 편리하게 확인할 수 있어 군사, 물류, 에너지/환경, 융합신산업, 바이오산업 등에서 바코드의 대체 수단으로 이용되고 있다. 하지만, 실생활에서 거의 모든 사물에 RFID 태그가 부착되었다고 본다면 태그의 식별정보 수집으로 인한 이동경로 추적, 금전적 지출 및 사회적 지위 등의 개인 프라이버시와 관련된 정보가 노출될 수 있는 문제점이 있다.

RFID 시스템의 안전성을 위협할 수 있는 공격으로 도청, 트래픽 분석 등의 수동적 공격과 위조, 서비스 거부 공격 등의 능동적 공격들이 있으며, 이런 공격들로부터 안전한 RFID 시스템 설계를 위해서는 전달되는 인증 정보의 기밀성 및 무결성, 태그 식별 정보의 익명성 등의 기본적인 보안 요구사항이 만족되어야 할 것이다. 하지만 RFID 태그의 경우, 연산능력과 저장 능력에 제한이 있으므로 기존의 공개키 방식이나 대칭키 방식의 암호화 알고리즘을 적용하는 것은 적절하지 않다. 초기 RFID 보안 대책으로 kill tag, faraday case, active jamming, blocker tag를 이용한 방식들이 알려졌으며[17]. 이후 해쉬 연산을 이용한 해쉬락, 재암호화, 해쉬 체인 방식 등이 소개되었다. 최근에는 경량화된 대칭키 및 공개키 암호에 대한 연구가 활발히 연구되고 있다[18].

최근 연구된 경량화된 해쉬 기반 인증 프로토콜[2]에서는 고정 ID 방식의 상호 인증을 소개하였고, 임지환의 연구[3]에서는 동적 ID 방식의 상호 인증 프로토콜을 소개하였다. 안전성 분석에 있어서 위 프로토콜들은 백엔드 서버와 리더 구간을 안전하다고 가정하고 있다. 하지만 현실적으로 공격자 입장에서 태그 공격보다는 백엔드 서버나 리더 공격이 공격대비 높은 효율성을 가질 것이다. 안전한 구간을 설정할 경우 추가적인 보안 시스템이 요구되며, 부가적인 비용 또한 증가할 것이다. 본 논문에서는 고정 ID기반의 RFID 시스템이 일반적인 동적 ID 기반 RFID 시스템과 동일한 태그 검색율을 갖고 모든 개체의 위장공격을 탐지 할 수 있는 안전하고 효율적인 RFID 상호 인증 프로토콜을 제안한다. 이 후 논문의 구성은 다음과 같다. 제2장에서 사전 연구로 기존 RFID 상호 인증 프로토콜의 분석 및 요구사항을 정의한다. 제3장에서 시스템 환경과 보안 요구사항을 정의하고, 4장에서는 제안하는 프로토콜을 기술한 후에, 5장에서 각종 공격 시나리오에 대한 대응과 안전성 및 효율성 분석 결과를 기술한 후, 6장에서 결론을 맺는다.

II. 관련 연구

RFID 시스템에는 무선 구간이 존재함으로써 도청, 전파범위 제한에 따른 통신 두절, 간섭 등의 문제점이 발생할 수 있다. 이런 문제점들을 극복하고 경량화된 인증 프로토콜을 제공하기 위해서 해쉬 알고리즘을 이용한 인증 프로토콜들에 대한 다양한 연구들이 수행되고 있다. 본 장에서는 기존에 연구되었던 해쉬 기반 인증 프로토콜들을 분석하고자 한다. 들어가기에

〔표 1〕 프로토콜에서 사용될 기호 및 약어 정리

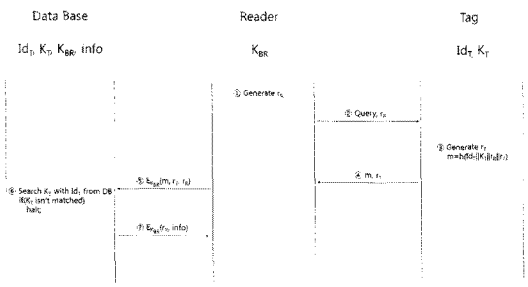
기호	설명	기호	설명
B	백엔드 서버	m	인증 정보
R	리더	m_{Left}	인증 정보의 좌측 절반값
T	태그	m_{Right}	인증 정보의 우측 절반값
▲	B, R, T ∈ ▲	$E_K()$	비밀키 K를 이용한 암호화
Id▲	▲의 식별자	$D_K()$	비밀키 K를 이용한 복호화
r▲	▲의 랜덤값	h()	해쉬연산
c▲	▲의 카운터	_	공격자가 위변조한 정보
Pc▲	▲의 이전 카운터	⊕	eXclusive OR
K▲	▲의 키	$x\|\|y$	x와 y를 연접
PK▲	▲의 이전키	UPDCPL	update complete 메시지
CK▲	▲의 현재키	BF_i	블룸필터[13]
K_{BR}	리더와 백엔드 서버의 공유키	prng()	의사난수함수
K_{TR}	태그와 리더의 공유키	ps_Id_R	관리자 패스워드
XId▲	▲의 OTI(One Time ID)	info	태그의 정보
Xc▲	▲의 OTC(One Time Counter)	sk	세션키

앞서 본 논문에서 사용하는 기호와 약어에 대한 설명을 [표1]과 같이 정리한다.

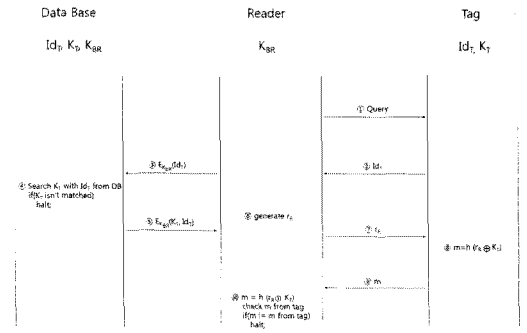
2.1 기존 해쉬 기반 RFID 인증 프로토콜 분석

XOR과 해쉬를 이용한 인증 프로토콜 : 본 프로토콜[1]에서는 백엔드 서버가 사전에 리더에게 K_{BR}를 제공함으로써 백엔드 서버와 리더 구간에 암호화를 지원하고 있다. 리더는 태그로부터 수신한 Id_T를 백엔드 서버로 전달하고, Id_T에 해당하는 K_T를 수신하게 된다. 이후 리더가 prng()를 이용해 r_R을 생성한 후 태그에게 전송하고, $m=h(r_R \oplus K_T)$를 수신한다. 리더는 백엔드 서버로부터 수신한 K_T를 이용하여 m을 계산하고, 태그로부터 수신한 m과 동일한 경우 태그를 인증하게 된다. 인증에 필요한 연산량은 리더는 암·복호화 각 1회, 랜덤값 생성 1회, XOR 연산 1회, 해쉬 연산 1회를 수행하고 태그의 경우, XOR 연산 1회, 해쉬 연산 1회가 수행된다. 총 메시지 전송 횟수는 6회이다.

하지만, 공격자는 태그가 리더를 인증하지 않은 상태에서 리더로 전달되는 Id_T가 그대로 노출된다는 점을 이용하여 도청 공격 및 태그의 위치 추적 공격을 할 수 있다. 도청의 경우 리더와 태그 사이가 무선 구간이므로 전달되는 Id_T를 수집할 수 있다. 설령, 무선 구간을 이용하지 않더라도 유선 근거리통신망 상에 존재하는 내부 공격자가 존재한다면 공격 가능성은 상존한다. 유선 네트워크를 태그의 위치 추적 공격은 태그에게 쿼리를 전달하면 동일한 Id_T가 리턴되므로 가능하다. 또한, 공격자가 리더로 가장하여 사전에 리스트 (Id_T, r_R, m)를 수집하는 경우, 인증 정보 재전송을 통한 태그 위장 공격이 가능할 것이다.



[그림 1] RFID/USN 환경을 위한 개선된 인증 프로토콜

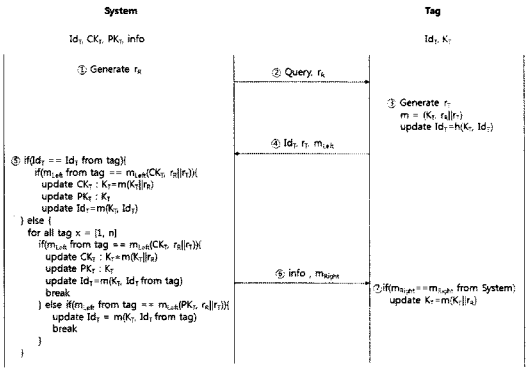


[그림 2] XOR과 해쉬를 이용한 인증 프로토콜

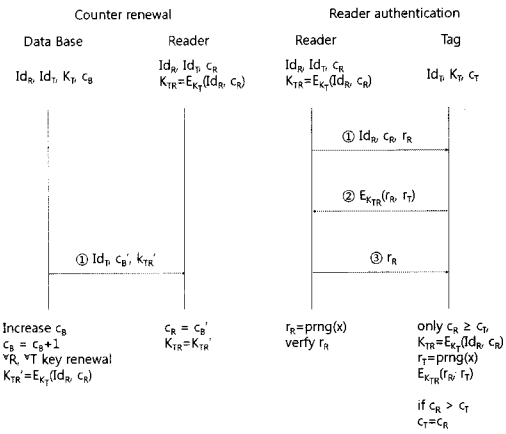
RFID/USN 환경을 위한 개선된 인증 프로토콜 : 본 프로토콜[2]은 신진섭의 연구[1]을 개선한 것으로, 리더가 태그로 쿼리 전송시 r_R을 함께 전달함으로써 재전송 공격이 불가능하도록 개선하였다. 태그의 응답에서 r_T가 포함되므로 태그의 익명성과 위치 추적 공격에 대한 안전성을 제공한다. 태그는 m과 r_T만을 리더로 전송함으로 Id_T와 K_T에 대한 노출을 방지할 수 있다. 인증에 필요한 연산량은 리더의 경우 랜덤 값 생성 1회, 암·복호화 각 1회를 수행한다. 태그의 경우, 랜덤 값 생성 1회, 해쉬 연산 1회로 기존 프로토콜[1] 보다 리더와 태그의 연산 모두 감소하였으며, 라운드 수를 4회로 감소시켰다.

하지만, Id_T와 K_T가 갱신되지 않으므로 공격자가 태그의 그룹에 동일한 _r_R을 쿼리와 함께 반복적으로 요청하는 경우 (_r_R, m, r_T)쌍을 수집할 수 있어 태그의 위치 추적이 가능하다.

동기화 문제를 해결한 새로운 동적 아이디기반 RFID 상호 인증 프로토콜 : 본 프로토콜[3]은 동적 ID를 지원하는 RFID 시스템에 적용한 프로토콜이다. 백엔드 서버와 리더 구간을 안전한 채널로 가정하여 백엔드 서버와 리더를 하나의 시스템으로 표현하고 있다. 태그는 Id_T와 K_T, r_T를, 백엔드 서버에서는 Id_T, CK_T, PK_T, info정보를, 리더는 r_R을 저장한다. 리더가 쿼리와 r_R을 태그로 전송하고, 태그로부터 Id_T, r_T, 인증정보의 좌측 절반 값인 $m_{Left}(K_T, r_R||r_T)$를 응답 받는다. 리더는 이를 수신하여 r_R과 함께 백엔드 서버로 전달한다. 한편, 리더에 인증 정보 전달을 마친 태그는 $Id_T = h(K_T, Id_T)$를 갱신한다. 백엔드 서버는 태그로부터 수신한 Id_T를 식별자로 DB를 검색하여 m_{Left}을 확인하고 인증 된 경우 $K_T=h(K_T||r_R)$와 $Id_T=h(K_T, Id_T)$를 갱신한다. Id_T가 DB에서 색인되지 않을 경우, 전체 태그의 CK_T와 PK_T를 대상으로 m_{Left} 연산을 수행하여 일치하는 경우 CK_T, PK_T, Id_T를 갱신한다. 태그의 키가



〔그림 3〕 동기화 문제를 해결한 새로운 동적 아이디기반 RFID 상호 인증 프로토콜



〔그림 4〕 When Compromised readers Meet RFID 프로토콜

시스템과 비동기화되고 ID까지 비동기화되는 경우 전체 PK_T를 대상으로 m_{Left} 연산을 수행하고, m_{Left}이 일치하는 경우 Id_T만을 갱신한다. 시스템은 태그에게 m_{Right}과 info를 전달하고, 태그는 m_{Right}을 인증한 경우에만 $K_T=h(K_T||r_R)$로 갱신한다. 이와 같은 과정을 통해 위치추적 공격, 서비스 거부 공격 등에 안전하지만, 시스템을 안전한 구간으로 정의함으로써 서버 위장 공격은 고려하지 않았다. 본 프로토콜은 백엔드 서버와 리더 구간에서의 전송 과정을 고려한다면, 리더에서 서버로의 r_R 전송 1회를 포함하여 총 6회의 통신을 거치게 된다. 또한 인증을 위해 리더는 랜덤값 생성 1회만 수행하며, 태그는 1회의 랜덤값 생성과 3번의 해쉬 연산을 수행한다.

본 프로토콜에서는 태그의 ID 갱신을 위해 별도의 통신과정을 두지 않고, 쿼리 응답 후에 스스로 ID를 갱신하도록 하고 있다. 공격자는 이점을 이용하여 태그에게 쿼리와 난수를 브로드캐스트함으로써 손쉽게 시스템과 태그 사이에 ID 비동기화를 발생시킬 수 있다.

ID 비동기화가 발생하게 되면 시스템은 DB에 있는 모든 태그를 대상으로 해쉬 연산을 수행해야만 하므로 동적 ID를 이용한 태그 검색 효율성을 유지할 수 없게 된다. 다만, ID 비동기화는 1회에 한정되므로 시스템과의 통신이 정상적으로 완료되면 동기화가 맞춰진다.

When Compromised readers Meet RFID : 지금까지 살펴본 해쉬 기반 프로토콜〔1-3〕은 기본적으로 백엔드 서버와 리더의 구간을 안전하다고 가정하고 있으므로, 백엔드 서버의 위장 공격이나 리더의 위장 공격으로 발생할 수 있는 메시지 조작 문제를 다루고 있지 않다. 이번에 소개할 논문에서는 동기화 카운터를 이용하여 태그가 비인가된 리더의 공격을 탐지할 수 있도록 하는 기법〔4〕을 소개하고 있다.

본 프로토콜〔4〕은 고정 ID 기반 RFID 인증 프로토콜로 카운터를 이용하여 태그가 비동기화된 리더를 구분함으로써 태그의 인증 정보 노출을 방지하는 방법을 소개하고 있다. 백엔드 서버와 리더 사이를 안전한 구간으로 가정하고 있으며, 백엔드 서버는 시스템에 대한 모든 공격을 탐지할 수 있다는 가정을 둔다. 백엔드 서버는 Id_R, Id_T, K_T, c_B를, 리더는 Id_R, Id_T, c_R, K_{TR}를, 태그는 Id_T, K_T, c_T를 각각 저장하고 있다.

백엔드 서버는 $K_{TR}=E_{K_{TR}}(Id_R, c_R)$을 생성하고 리더에게 전달한다. 리더의 요청시 태그는 Id_R, c_R, r_R를 수신 받고, 암호화 통신을 위하여 $K_{TR}=E_{K_T}(Id_R, c_R)$을 생성하고 태그의 r_T을 암호화하여 $E_{K_T}(r_R, r_T)$ 전달한다. 이를 수신한 리더는 $E_{K_T}(r_R, r_T)$를 복호화 한 후 r_R을 확인함으로써 리더가 태그를 인증하고, 자신의 r_R을 태그로 재전송함으로써 태그가 리더를 인증한다.

공격 탐지시 백엔드 서버는 c_B를 증가시키고 정당한 리더들만 동기화시킨다. 태그는 평상시 사전에 백엔드 서버와 공유하고 있는 c_T값을 유지하고 있다가 리더 요청시, 자신의 정보와 리더의 정보를 이용하여 해쉬 값을 생성하고, 생성된 해쉬 값이 백엔드 서버에서 인증되는 경우에만 정당한 리더로부터 전달받은 카운터로 갱신하는 과정을 거친다. 이후 Id_R과 증가된 c_B를 태그의 키로 암호화함으로써 암호키를 갱신한다.

하지만, 각 태그와 리더 사이에 유일한 K_{TR}을 소유하므로 통신에 대한 안전성을 높일 수 있는 반면, 리

더가 모든 태그의 K_{TR}을 저장해야 한다는 점과, 백엔드 서버가 모든 공격을 탐지할 수 있다는 강력한 가정을 만족해야만 프로토콜이 동작할 수 있다. 리더로 위장한 공격자가 충분히 높은 카운터를 생성하여 전송할 경우 태그 카운터 비동기화 공격이 가능하다. 이와 같은 공격에 의해 비동기화가 발생할 수 있지만 제안된 프로토콜은 재동기화 과정 및 카운터 초기화 방법을 제시하지 않고 있다.

2.2 효율적인 태그 검색을 위한 기존 연구

해쉬 연산을 이용한 초기 RFID 인증 시스템들은 태그의 정보 노출을 막고, 태그와 리더의 연산을 줄이는데 초점이 맞춰져 있다. RFID 시스템에서 태그의 수가 지속적으로 증가한다고 가정한다면, 인증 과정에 있어서 태그와 리더 측면에서의 연산량 감소뿐만 아니라 DB 측면에서 연산량을 줄이는 연구가 진행되어야 한다. 또한 DB 검색 시 DB의 연산량이 태그의 수에 영향을 받는 점 또한 해결해야 할 과제이다. 이번 절에서는 효율적인 연산을 위한 기존 연구들에 대해 살펴보고자 한다.

RFID 시스템은 태그의 ID 갱신 여부에 따라서 태그의 ID를 유지하는 고정 ID 방식과 인증시 태그의 ID를 갱신하는 동적 ID 방식으로 구분될 수 있다. 고정 ID 방식의 경우 태그가 인증을 위해 동일한 ID를 이용하기 때문에 랜덤값을 이용하여 전달되는 정보를 갱신해야 하고, 공격자가 노출되는 정보를 조합할 경우 전방향 안전성을 만족시키기 어렵다. 추가로, 전사적 해쉬 연산[6,10]을 이용한 태그 검색 방식의 연산 횟수를 줄이기 위한 포인터[11], 머클해쉬[12], Bloom Filter[13] 방식들이 제안되었다. 한편, 동적 ID 방식의 경우 인증시 ID 값이 매번 갱신되기 때문에 이를 식별자로 하여 태그를 검색할 경우 백엔드 서버의 해쉬 연산횟수를 줄일 수 있어 전방향 안전성을 만족시키기 쉬운 반면, 갱신되는 인증 정보를 백엔드 서버와 태그 사이에 교환해야 하며 동기화 실패에 대한 대안을 마련해야 한다.

고정 ID 방식을 이용하는 기존 연구[6,10]에서 백엔드 서버는 인증을 위해 최대 n번의 해쉬 연산이 요구되고, 머클해쉬트리 구조를 이용하는 T.Dnimitrin의 연구[12]에서는 log n회의 해쉬 연산이 요구된다. 김익수의 연구[11]에서는 ID의 위치를 나타내는 위치정보(P)를 태그 ID와 함께 저장하기 때문에 DB에서 P를 이용하여 백엔드 서버에서 위치 정보를 검색한 후 2회의 해쉬 연산만 필요하게 된다. 김진호의 연구[13]에서 DB는 태그 당 하나의 BF_I을 수행하고, 이 값을 식별자로써 태그를 검색함으로 최대 p=긍정 오류율(f) × 2n번의 해쉬 연산을 수행하게 된다.

제안하는 프로토콜에서는 고정 ID 방식의 RFID 시스템에 동적 ID의 기능을 구현하기 위해 리더와 태그에 각각 1개의 랜덤ID를 할당한다. 이 값은 백엔드 서버에서 Id_R, Id_T와 랜덤값에 의해 생성된 값으로 매 세션마다 갱신되는 값이다.

2.3 RFID 시스템에 적용 가능한 암호 알고리즘 연구

최근 상호 인증을 제공하는 RFID 시스템에는 백엔드 서버와 리더 구간의 구간을 안전한 구간으로 가정하거나, 암호화를 통하여 전달되는 인증 정보를 노출시키지 않도록 하고 있다[1-3]. RFID 시스템에서 암호화통신을 지원하기 위해서는 RFID 시스템의 리더와 태그가 암호화에 필요한 연산능력, 전력능력, 저장능력을 갖춰야 한다. 현재 널리 사용되고 있는 대칭키 알고리즘으로 NIST(*National Institute of Standards and Technology*)의 AES(*Advanced Encryption Standard*)가 있지만, 자원제약적인 RFID 시스템의 태그에 적용하기에는 현실적으로 어려움이 있어, 경량화에 대한 연구가 활발히 진행되고 있다. 최근에 SHA 보다 적은 자원으로 수동형 RFID에서 보안성 및 프라이버시를 보장하는 AES-64(0.8V, 125kHz, 1.35μW)를 구현한 연구[14]와 3868 gates, 870 clock으로 AES-128를 구현한 연구[15] 결과가 발표된바 있어 RFID 태그에 경량화된 대칭키 알고리즘을 적용한 제품이 늘어날 것으로 보인다. 암호 알고리즘은 Brute-force 공격을 방지하기 위해서 최소 64 비트가 필요하므로[14] 제안하는 프로토콜에서는 백엔드 서버와 리더 구간의 암호 통신 지원 및 갱신되는 인증정보를 보호하는데 128비트의 경량화된 AES를 사용하는 것으로 가정한다.

III. RFID 인증 프로토콜 요구사항

앞서 2장에서 관련 연구 분석을 통하여 기존 RFID 시스템에서 도청 공격, 위장공격, 위치추적 공격 등이 발생할 수 있음을 확인하였다. 본 장에서는 지금까지의 관련 연구들[1-9,19,20]를 통하여 RFID 인증 프로토콜 설계 과정에서 고려해야할 시스템 환경

및 보안 요구사항 등을 정의하고자 한다.

3.1 보안요구사항

관련 연구[1-4]를 통해 RFID 시스템 환경에서 발생할 수 있는 위협들을 같이 정리할 수 있다.

- 도청 공격(Eavesdropping Attack) : RFID 시스템의 무선 구간에서 전파 수신 지역 내에 있는 공격자는 정당한 개체들의 통신 메시지를 수신할 수 있다.
- 위장 공격(Impersonate Attack) : 위장 공격은 도청을 통해 획득한 인증 정보를 재전송하거나 위조함으로써 공격자가 정당한 개체로 인식되도록 하는 공격이다.
- 변조 공격(Spoofing Attack) : 변조 공격은 전달되는 정보를 변경하는 공격을 말한다. 공격자는 위장 공격을 하는 과정에서 메시지 변조 공격을 시도할 수 있다.
- 위치추적 공격(Location Tracking Attack) : 위치추적 공격은 다수의 리더를 설치하여 태그로부터 전달되는 정보의 분석을 통해 태그의 위치를 파악하는 공격을 말한다.
- 서비스거부공격(Denial of Service Attack) : 무선 통신은 주변 환경이나 전파 간섭에 의해 신뢰성이 높은 통신 환경을 제공하지 못한다. 공격자는 고의로 방해 전파를 송신하여 정당한 개체의 통신을 방해하거나, 위장 공격을 통해 정상적인 동기화가 이루어지지 못하도록 방해할 수 있다.

위와 같은 위협에 대응하기 위한 보안요구사항을 다음과 같이 정의 하였다.

- 무결성(Integrity) : RFID 시스템에서 수신자는 상대방이 전달한 데이터가 변경되지 않았음을 확인할 수 있어야 한다.
- 가용성(Availability) : 가용성은 정보, 서비스, 응용들이 합법적인 사용자에게 언제나 사용가능함을 보장해야 한다.
- 통신 보안(Communication Security) : RFID 시스템에서 출발지에서 목적지로 전달되는 정보가 누출되지 않도록 해야 한다.
- 상호 인증(Mutual Authentication) : RFID 시스템에서의 통신에 참여하는 모든 개체가 서로를 인증함으로써 전달하려는 정보가 의도한 개체에게 전달되도록 보장해야 한다.
- 전방향 안전성(Forward Secrecy) : 현재의 데이터가 노출되더라도 과거의 데이터의 안전성을 보장해야 한다. 즉, 현재 세션에서 비인가자가 메시지 분석으로 인증정보를 획득한다 하더라도, 획득된 인증 정보를 이용하여 이전 세션에 참가했던 태그를 구분하거나 태그의 이동 경로를 추적할 수 없음을 보장해야 한다.
- 공격에 대한 복원력(Resilient to Attacks) : RFID 시스템에 각 개체는 공격이 발생한 이후 복원과정을 통해 원래의 상태로 돌아올 수 잇도록 적절한 대응책을 제공해야 한다.
- 부인봉쇄(Non-requdiation) : RFID 시스템에서 어떤 개체가 통신에 참여한 경우, 통신이 종료된 이후 자신의 참여 사실을 부정할 수 없어야 한다.
- 프라이버시(Privacy) : RFID 시스템에서 태그를 소지한 사용자나 개체들의 식별자 및 인증정보를 비밀로 유지되어야 한다.

3.2 프로토콜 설계

기존 RFID 인증 프로토콜[1-2]에서는 백엔드 서버와 리더의 구간을 안전한 구간으로 가정함으로써 백엔드 서버와 리더의 공격을 다루고 있지 않다. 개선된 프로토콜[3-4]에서는 리더의 공격을 다루고는 있지만, 백엔드 서버의 공격은 다루고 있지 않다. 본 논문에서는 RFID 시스템의 모든 구간을 안전하지 않은 구간으로 고려하여 공격자가 백엔드 서버와 리더 그리고 태그로 위장 공격이 가능하다는 가정을 둔다. 이번 절에서는 안전한 RFID 시스템 설계를 위한 요구사항과 시스템 환경에 대하여 기술한다.

[설계요구사항 정의]

- 설계요구사항1. 실용성 있는 프로토콜 설계를 위해서 전 구간에서의 공격을 고려해야 한다.
- 설계요구사항2. 각 구간에서의 정보의 노출을 방지하기 위한 기술을 적용한다.
- 설계요구사항3. 정적 ID 기반의 경우 위치 추적 문제를 해결해야 하며, 동적 ID 기반의 경우 비동기화 문제를 해결해야 한다.
- 설계요구사항4. 태그의 연산 능력을 고려하여 경량화된 프로토콜을 설계해야 한다.
- 설계요구사항5. 백엔드 서버에서 효율적인 태그

검색을 지원해야 한다.

〔시스템 환경 설정〕

- 가정1. 각 개체 사이의 구간은 모두 안전하지 않은 구간으로 가정한다. 다시 말해, 태그 리더와 백엔드 서버간에 무선 전송기술을 이용하여 유선 전송 기술보다 더 취약한 상황을 가정한다.
- 가정2. 각 개체는 해쉬 연산 및 경량화된 암호연산을 지원할 수 있어야 한다.
- 가정3. 리더와 태그가 사용되기 이전에 반드시 사전 등록 단계를 거친다.
- 가정4. 각 개체들이 정상적으로 동기화된 경우, 각 개체의 c_B, c_R, c_T은 모두 동일하다.
- 가정5. 리더가 태그에게 쿼리를 전송하면, 리더의 카운터가 태그의 카운터 보다 크거나 같은 경우에만 동기화가 이루어진 것으로 판단하고 이외의 경우에는 통신을 중단한다.(즉 ,태그는 1차적으로 카운터를 이용하여 리더의 동기화 상태를 확인함으로써 동기화되지 않는 리더의 응답에 불필요한 인증 정보를 전달하지 않는다.)
- 가정6. 리더의 카운터와 K_{BR}이 백엔드 서버와 동기화가 맞지 않는 경우, 리더 동기화 단계를 거쳐 동기화할 수 있다.
- 가정7. 각 개체 사이의 구간에서 메시지 평균 왕복 시간을 임계값(δ)로 설정하고, 메시지 응답 시간이 임계치를 초과하는 경우 통신을 중단한다. 왕복 시간 측정은 태그를 제외한 각 개체가 가지고 있는 타임스탬프 함수에 의해 계산되므로 시스템 내에서 시간동기화를 요구하지는 않는다. 본 논문에서 임계값 설정에 대한 내용은 다루지 않는다.
- 정의1. 변수 크기 정의 및 연산 정의

본 프로토콜에서는 키 생성의 경우 AES-128, HASH-128, eXclusive-OR 연산을 사용하며, 사용되는 파라미터의 크기는 아래와 같다.

- 128 bits의 파라미터 : $Id_▲$, $XId_▲$, ps_Id_R, K_T, $Xc_▲$, m ($▲ \ni_{B,\ R,\ T}$)
- 64 bits의 파라미터 : $r_▲$, $c_▲$, m_{Left}, m_{Right}, ($▲ \ni_{B,\ R,\ T}$)

연산 시 파라미터의 크기가 다른 경우, 아래와 같이 연산한다.

- 암호 연산 : $y=F_K(x)$일 때, $|K|=128$ bits, $|y|=128$ bits의 크기를 갖는다.
- 해쉬 연산 : $h(A||B)$일 때, A=64 or 128 bits, B=64 bits라면 $h(A||B)$ 연산으로 정의한다.
- XOR 연산 : $A \oplus B$ 일 때, A=64 or 128 bits, B=64 bits라면 $A \oplus (B||B)$ 연산으로 정의한다.

- 정의2. 매 세션 마다 갱신되는 변수 정의
  - K_T, $XId_▲$, $Xc_▲$ 값은 매 세션 마다 갱신된다. (단, 정상상태/공격상태에 따라 값을 생성하는 과정이 다르다.)
  - K_{BR}, $c_▲$ 값은 리더 공격이 탐지된 경우에만 갱신되고, 정상 상태에서는 유지된다.

3.3 공격 시나리오

본 논문에서는 공격자가 암호화된 데이터를 습득하여 내부 데이터를 위·변조할 수 있는 능력을 가졌다고 가정한다. 이런 가정은 공격을 더욱 수월하게 하며 공격자에게 유리한 환경을 제공할 수 있다. 이번 절에서는 3.1절에서 언급한 도청공격, 위·변조 공격, 서비스 거부 공격, 위치추적 공격 등의 위협에 대한 공격 시나리오를 살펴보고, 공격자가 각 개체로 위장하여 RFID 시스템의 인증을 우회하는 공격의 시나리오를 제시하고, 이후 4장에서 시나리오별 프로토콜분석을 통하여 제안하는 인증 프로토콜이 각 개체의 위장공격에 안전함을 증명한다.(단 위장 공격에서 물리적 공격은 고려하지 않는다.)

시나리오.1 태그 위장 공격 : 공격자는 자신이 가지고 있는 태그의 인증 정보를 인가된 태그의 인증 정보로 위·변조하여 리더에게 전달하여 할 수 있다. 태그 위장 시나리오의 경우, 공격자는 노출되지 않는 Id_T와 K_T, C_T에 대한 정보를 알 수 없으며, 이전 세션에서 사용되었던 XId_T와 Xc_T는 도청을 통해서 수집할 수 있다.

시나리오2. 리더 위장 공격 : 공격자는 인가된 태그의 정보를 수집하기 위하여 정상적인 리더로 위장 공격을 시도할 수 있다. 리더 위장 시나리오의 경우, 공격자는 노출되지 않은 Id_R과 K_{BR}에 대한 정보를 알 수 없으며, 이전 세션에 이용되었던 XId_R과 c_R은 도청을 통해서 수집할 수 있다. 하지만, 현재 세션에 이용될 XId_R은 암호화되어 전송되므로 획득할 수 없다. (하지만, 본 시나리오에서는 공격자가 XId_R과 K_{BR} 쌍을 알고 있다고 가정한다.)

시나리오3. 백엔드 서버 위장 공격 : 공격자는 보

〔표 2〕 RFID 시스템에서의 일반적인 공격 시나리오

RFID 시스템에서의 도청 공격 - 무선채널 구간의 도청 및 동일한 로컬 네트워크에서의 유선채널 구간의 도청이 있을 수 있다. - 피해 내용 : 통신에 참가하지 않은 비인가자의 데이터 습득이 가능하다. - 대응 방안 : 보안채널을 이용하는 경우와 전달되는 데이터 중 인증정보를 암호화하는 방법이 있다.
위·변조 공격 - 도청을 통해 인증정보를 수집·분석한 후 수집된 인증 정보를 재사용함으로서 다른 개체로 위장하는 공격있을 수 있다. - 피해 내용 : 비인가된 개체가 인증 절차 우회, 권한 상승, 불법 이용 등이 가능하다. - 대응 방안 : 무결성, 기밀성, 신선성을 동시에 유지할 수 있도록 인증절차를 강화해야 한다.
서비스 거부 공격 - 신호 방해를 통한 서비스 거부 공격과 인증정보 변조를 통한 비동기화 공격이 있을 수 있다. - 피해 내용 : 단기적인 통신 두절이 발생할 수 있으며, 인증정보 변조시 지속적인 통신두절이 발생할 수 있다. - 대응 방안 : 재밍 공격을 탐지하는 시스템을 도입하는 방법과 재동기화 방안을 마련하는 경우가 있다.
위치 추적 공격 - 특정 태그나 태그를 소지한 사람에 대한 이동경로를 추적하는 공격이 있을 수 있다. - 피해 내용 : 태그의 검색을 통해 사용자나 물건의 위치 정보를 수집할 수 있다. - 대응 방안 : 태그의 반응을 막을 수 있는 케이스를 이용하는 방식과 인증 프로토콜 상에 태그가 정당한 리더를 구분할 수 있는 능력을 구현하는 방법이 있다.

다 많은 정보를 수집하거나, 서비스 거부 공격을 목적으로 합법적인 백엔드 서버로 위장 공격을 시도할 수 있다. 백엔드 서버 위장 시나리오의 경우, 공격자는 노출되지 않은 Id_R, K_{BR}, ps_Id_R, Id_T, K_T, info의 정보를 알 수 없으며, 이전 세션에서 사용되었던 XId_R, XId_T, Pc_R은 청을 통해 수집할 수 있다. 현재 세션에서 이용될 XId_R, XId_T는 암호화되어 전송되므로 획득할 수 없다. (하지만, 본 시나리오에서는 공격자가 XId_R과 K_{BR} 쌍을 알고 있다고 가정한다.)

위에서 제시한 시나리오에 따른 프로토콜 동작은 4.3절에서 살펴보도록 한다.

IV. 안전하고 효율적인 RFID 시스템을 위한 프로토콜 제안

본 장에서는 3장에서 정의한 요구사항들을 만족하면서 안전하고 효율적인 RFID 시스템 프로토콜을 소개하고자 한다. 4.1절에서 효율적인 태그 검색을 위한 기법을 소개하고 4.2절에서 제안하는 RFID 인증 프로토콜의 인증 절차에 대해 기술한다. 이후 4.3절에서는 제안하는 프로토콜이 3.3절의 공격 시나리오별 공격을 탐지할 수 있음을 보인다. 4.4절에서 동적 ID 방식에서 발생할 수 있는 비동기화를 복구하기 위한 재동기화 프로토콜을 기술한다.

4.1 효율적인 태그 검색 기법

관련 연구에서 알아본 프로토콜들[1-3]들은 태그로부터 전달된 해쉬 값을 인증하기 위해서 최악의 경우 태그의 수만큼 해쉬 연산을 거쳐야한다. 이번 절에서는 고정 ID 방식의 RFID 시스템에서 효율적인 태그 검색을 위해서 리더의 식별자를 이용하는 방식을 소개하고자 한다.

일반적으로 일회용 태그의 경우라도 등록 후에 사용을 해야 하기 때문에, 최소 2번은 동일한 리더에 의해 읽혀질 가능성이 높다. 반복적으로 사용되는 태그

〔표 3〕 백엔드 서버 테이블 정보

테이블명	리더 정보 테이블					
필드명	랜덤 식별자	식별자	암호키	태그 패스워드	이전 세션 카운터	리더 비활성화
값	XId_R	Id_R	K_{BR}	ps_Id_R	Pc_R	0

테이블명	태그 정보 테이블			
필드명	랜덤 식별자	식별자	키	상품정보
값	XId_T	Id_T	K_T	info

테이블명	태그 리스트 테이블	
필드명	랜덤 식별자	랜덤 식별자
값	XId_R	XId_T

가 동일한 리더에 의해 읽혀질 확률은 일회용 태그의 경우보다 더 높다고 볼 수 있다. 제안하는 검색 방식에서는 고정 ID 방식을 사용하는 RFID 시스템의 리더와 태그에 랜덤한 식별자를 할당함으로써 태그검색 효율을 높이고자 한다.

백엔드 서버는 XId_R를 식별자로 K_{BR}를 검색하고, 검색된 키를 이용하여 리더로부터 수신한 메시지를 복호화 한다. 이후 XId_R을 식별자로 [표3]의 태그 리스트 테이블에서 XId_T를 검색하여 검색률을 높인다. XId_R을 식별자로 XId_T를 찾지 못한 경우에만 태그 정보 테이블에서 다른 XId_T 를 검색한다.

이와 같은 방식을 통해 [1,2,3,6,10]처럼 해쉬 값을 알아내기 위해 전체 태그의 ID, K_T 쌍을 이용하여 전제 태그를 대상으로 해쉬 연산을 수행하는 오버헤드를 줄일 수 있다.

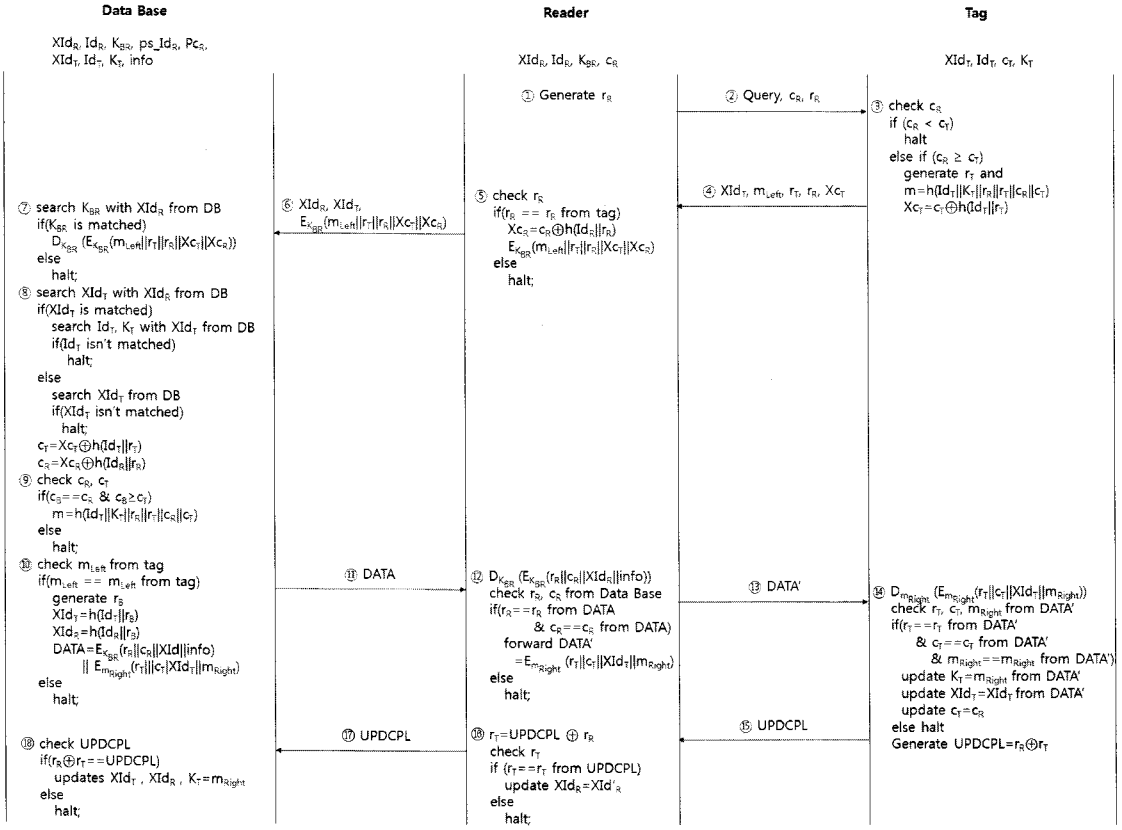
정당한 리더는 자신이 인증했던 태그 리스트 테이블만을 우선적으로 검색하여 태그의 정보를 참조할 수 있다. 정당한 리더는 랜덤 식별자 XId_R와 자신이 가지고 있는 K_{BR}의 신선성을 보장할 수 있어야 한다. 신선성이 보장되지 않는 리더의 경우는 백엔드 서버로부터 인증을 받을 수가 없다. 만일, 백엔드 서버가 인증 과정에서 리더의 인증 정보가 위조된 사실을 알아낼 경우, 리더 정보 테이블의 리더 비활성화 비트를 1로 설정한다. 만일 리더 비활성화 비트가 1로 설정된 리더가 인증 요청을 시도하는 경우, 4.4절의 리더 동기화 단계를 거쳐 인증 정보를 갱신해야만 현재 세션에서 통신이 가능해진다.

4.2 제안하는 프로토콜 인증 과정

[사전 등록 단계]

사전 등록 단계는 사용하지 않았던 리더나 태그를 제안하는 RFID 시스템에서 사용하기 위해 반드시 거쳐야하는 준비과정이며, 오프라인에서 별도의 인증 및 등록 과정을 거친다. 새로운 리더와 태그는 다음과 같은 정보를 백엔드 서버로부터 전달받거나 백엔드 서버에 저장하게 된다.

리더 등록 단계 : 사전 등록 단계에서 리더는 백엔



[그림 5] 제안하는 프로토콜의 인증 단계

드 서버로부터 XId_R, c_R, K_{BR}를 오프라인을 통해서 발급받고, 백엔드 서버에 XId_R, Id_R, K_{BR}, ps_Id_R를 저장한다. 패스워드는 비동기화시 복구를 위한 인증 수단으로 리더 동기화 단계에서 사용된다.

태그 등록 단계 : 사전 등록 단계에서 태그는 백엔드 서버로부터 XId_T, c_T, K_T를 오프라인을 통해 발급받고, 백엔드 서버에 XId_T, Id_T, K_T, 및 태그의 부가정보를 저장한다.

〔인증 프로토콜 단계〕

- 단계 ①~② : 리더는 r_R을 생성한 후 쿼리, c_R, r_R을 태그로 전달한다.
- 단계 ③~④ : 태그는 자신이 가지고 있는 c_T와 리더로부터 수신한 c_R의 크기를 비교한다. 리더의 카운터가 태그의 카운터 보다 작은 경우 통신을 중단한다. 리더의 카운터가 태그의 카운터와 같거나 큰 경우에만 다음 과정을 거친다. 태그는 r_T를 생성하고 리더로부터 수신한 정보(c_R, r_R)과 자신의 정보(Id_T, K_T, r_T, c_T)를 이용해 인증값 m을 생성한다. 카운터 정보를 숨기기 위해 Id_T와 r_T를 해쉬하고 이 값을 c_T와 XOR 연산하여 Xc_T를 생성한다. 태그는 인증을 위해 XId_T, m_{Left}, r_T, r_R, Xc_T 값을 리더로 전달한다.
- 단계 ⑤~⑥ : 리더는 태그로부터 수신한 인증정보의 일치여부를 확인하기 위해서 r_R값을 확인하고 이 값이 동일한 경우에만 Xc_R을 생성한다. 리더는 인증정보 보호를 위해 자신의 정보와 태그의 정보를 K_{BR}로 암호화하고, 리더와 태그를 구분할 수 있는 XId_R, XId_T를 함께 전달한다.
- 단계 ⑦~⑪ : 백엔드 서버는 복호화를 위해 리더로부터 수신한 XId_R를 이용하여 K_{BR}을 백엔드 서버에서 검색한다. 백엔드 서버에 K_{BR}이 없는 경우 통신을 종료한다. 메시지를 복호한 후 XId_R이 가지고 있는 태그 리스트에서 XId_T를 검색하고, XId_T를 식별자로 하여 태그의 정보를 참조한다. 색인된 데이터를 이용하여 Xc_T와 Xc_R로부터 c_T와 c_R을 계산한다. 이 값은 백엔드 서버가 동기화 검사를 하는데 이용한다.

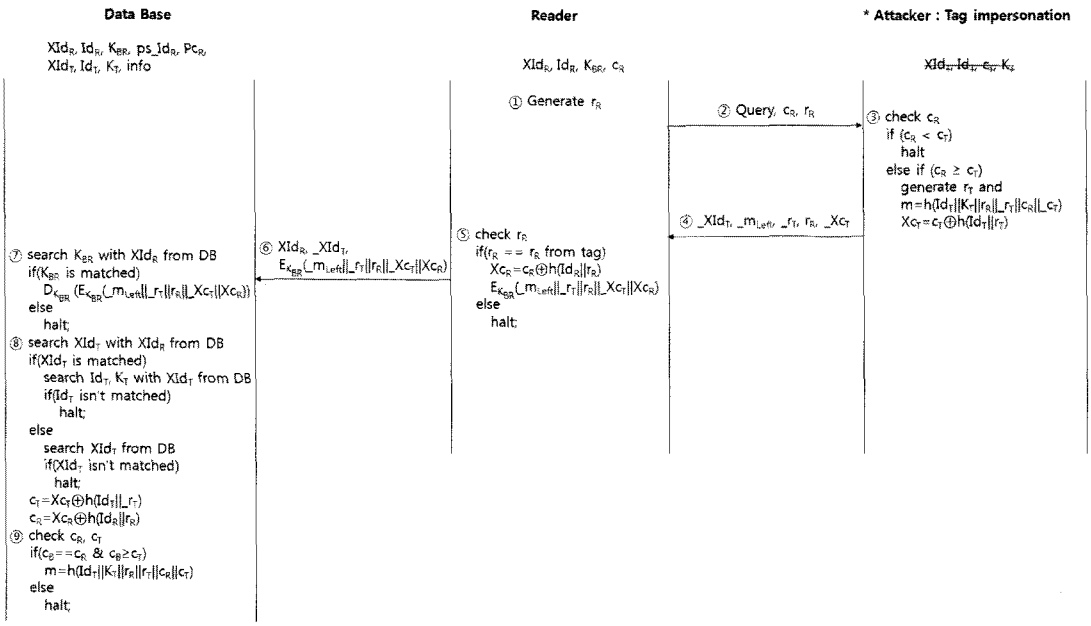
동기화가 맞는 경우에만 m_{Left}의 검증 과정을 거치게 된다. 동기화 및 해쉬 값 검증 과정에서 불일치하는 정보가 있다면 현재 통신을 종료하고 공격 시나리오를 따라 인증정보 갱신 과정이 이루어지게 된다. 동기화 및 해쉬 값 검증이 완료된 경우, 백엔드 서버는 랜덤 값 c_B를 생성하고 XId_T와 XId_R의 갱신 과정을 거친다. 백엔드 서버는 리더가 자신을 인증할 수 있도록 K_{BR}를 이용하여 r_R, c_R, XId_T, 태그의 부가정보를 암호화하여 전달하고, 태그가 자신을 인증할 수 있도록 m_{Right}을 이용하여 r_T, c_T, XId_T, m_{Right}을 암호화하여 전달한다.

- 단계 ⑫~⑬ : 리더는 전달받은 메시지를 복호하고, r_R과 c_R이 검증된 경우에만 DATA'을 태그에게 전달한다.
- 단계 ⑭ : 태그는 리더로부터 전달받은 메시지를 복호하고, r_T, c_T, m_{Right}이 검증된 경우에만 K_T, XId_T, c_T를 갱신한다. (단, DATA'의 cT 값이 0으로 전달된 경우 백엔드 서버가 카운터를 초기화한 것이므로, c_T를 c_R로 갱신하지 않고 0으로 초기화한다.)
- 단계 ⑮ : 태그는 r_R과 r_T를 이용하여 UPDCPL를 생성하고 리더에게 전달한다.
- 단계 ⑯~⑰ : 리더는 수신한 UPDCPL와 자신의 r_R의 XOR 연산 결과가 r_T가 되는지 검증한다. 검증된 경우에만, 수신한 UPDCPL을 백엔드 서버에 전달하고, XId_R을 갱신한다.
- 단계 ⑱ : 백엔드 서버는 Xc_R, Xc_T로부터 계산한 c_R과 c_T를 이용해 UPDCPL을 검증한다. UPDCPL이 일정 기간 동안 도착하지 않을 경우, 사전에 설정된 횟수 동안 DATA 전달 과정을 반복한다.

4.3 시나리오별 프로토콜 동작 과정

시나리오.1 태그 위장 공격 탐지 : 태그 위장 시나리오의 경우, 공격자는 노출되지 않는 Id_T, K_T, C_T에 대한 정보를 알 수 없으며, 이전 세션에서 사용되었던 XId_T와 Xc_T는 도청을 통해서 수집할 수 있다. 하지만, 현재 세션에서 이용될 XId_T는 암호화되어 전송되므로 획득할 수 없다.

- 단계 ①~② : 정당한 리더가 태그로 정보를 요청한다.
- 단계 ③~④ : 태그는 리더의 응답에 $\_XId_T$, $\_m_{Left}$, $\_r_R$, r_R, $_Xc_T$를 회신한다. 여기서 Id_T, K_T, c_T 값을 알 수 없으므로, 정확한 m_{Left}, Xc_T 및 XId_T를 생성할 수 없다.
- 단계 ⑤~⑥ : 리더는 태그로부터 수신한 정보와 자신의 정보를 이용하여 백엔드 서버에 인증 정보를 전달한다.



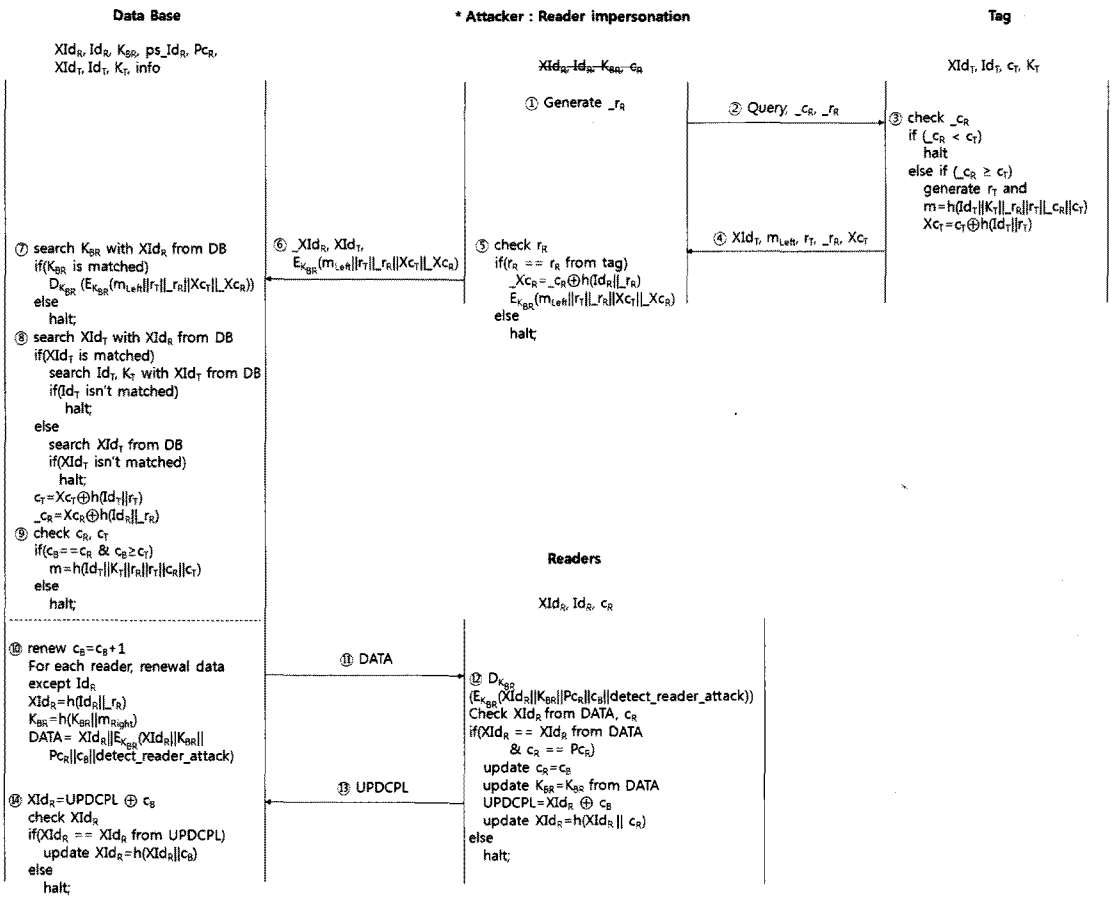
〔그림 6〕 태그 위장 공격 탐지 과정

- 단계 ⑦~⑨ : 리더로부터 인증 정보를 수신한 백엔드 서버는 암호화된 메시지를 복호한 후, c_T, c_R, m_{Left} 검증 단계를 진행한다. Id_T와 K_T를 모르는 태그는 올바른 c_T와 m_{Left}을 생성할 수 없으므로 태그 정보가 위조되었음을 확인할 수 있다. 이런 경우, 백엔드 서버는 통신을 종료한다.

시나리오2. 리더 위장 공격 탐지 : 리더 위장 시나리오의 경우, 공격자는 노출되지 않은 Id_R과 K_{BR}에 대한 정보를 알 수 없으며, 이전 세션에 이용되었던 XId_R과 c_R은 도청을 통해서 수집할 수 있다. 하지만, 현재 세션에 이용될 XId_R은 암호화되어 전송되므로 획득할 수 없다. 하지만, 본 시나리오에서는 공격자가 XId_R과 K_{BR} 쌍을 알고 있다고 가정함으로써 위조된 정보가 정상적으로 백엔드 서버로 전달되더라도 리더 공격을 탐지할 수 있음을 보인다.

- 단계 ①~② : 공격자는 태그에게 위조된 쿼리, $\_c_R$, $_r_R$을 전달한다.
- 단계 ③~④ : 태그는 리더로부터 전달받은 정보를 이용하여 인증정보 m_{Left}, Xc_T를 생성하고, XId_T, r_T, $_r_R$와 함께 리더에게 전달한다.
- 단계 ⑤~⑥ : 공격자는 태그로부터 수신한 정보와 자신이 위조한 정보를 조합하여 생성한 인증 정보를 백엔드 서버로 전달한다.
- 단계 ⑦~⑪ : 리더로부터 인증 정보를 수신한 백엔드 서버는 $_XId_R$을 이용하여 K_{BR}을 검색한다. 정상적인 인증과정에서는 공격자가 K_{BR}을 알고 있다 하더라도 대응되는 XId_R을 알지 못하면 백엔드 서버 측의 인증절차를 수행할 수 없다. (본 시나리오에서는 공격자가 XId_R과 K_{BR} 쌍을 알고 있다고 가정함으로 다음 단계를 수행한다.)

백엔드 서버는 XId_T를 인덱스로 검색함으로써 Id_T와 K_T값을 알 수 있으며, 이 값을 기반으로 c_T, $\_c_R$, $_m_{Left}$의 값을 검증한다. 공격자는 Id_T를 알 수 없으므로 정상적인 c_R과 m_{Left}를 생성할 수 없고, 백엔드 서버에서는 정보의 위조 여부를 확인할 수 있다. 정보가 위조된 경우, $_XId_R$과의 통신을 종료하고 $_XId_R$의 비활성화 비트를 1로 설정한다. (만약, 공격자에 의해서 $_XId_R$값을 갖는 정당한 리더가 비활성화 되었다면 "리더 동기화 과정"을 통해서 다시 세션을 동기화 할 수 있다.) 이와 동시에 백엔드 서버는 c_B를 증가시키고, Id_R을 제외한 모든 리더들의 XId_R과 K_{BR}을 갱신한다. 새로운 XId_R은 각 리더의 Id_R과 백엔드 서버에서 생성한 r_B의 해쉬 연산에 의해 생성되고, K_{BR}은 기존 K_{BR}에 위에서 생성한 정당한 m_{Right}의 해쉬 연산에 의해 생성된다. 정당한 리더들의 업데이트를 위



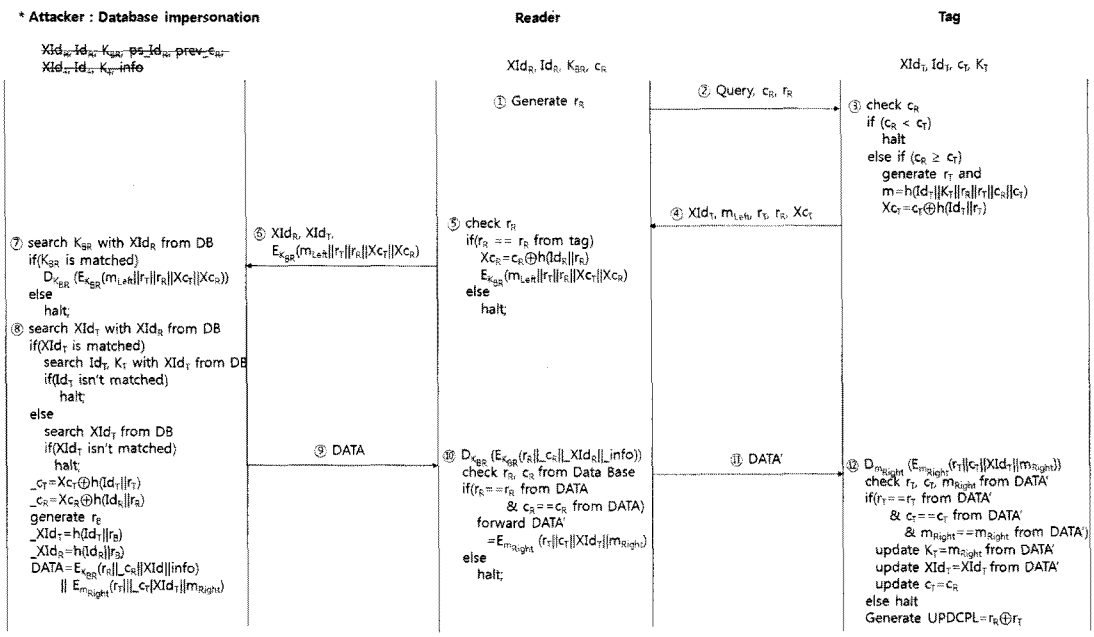
〔그림 7〕 리더 위장 공격 탐지 및 카운터 갱신 과정

해 전달되는 DATA는 메시지 구분을 위한 식별자 XId_R와 암호화된 부분으로 구성된다.

- 단계 ⑫~⑬ : 자신의 식별자 XId_R과 함께 전달된 메시지를 복호한 정당한 리더들은 메시지에서 XId_R과 Pc_R값이 자신의 XId_R 및 c_R값과 동일한지 검증한다. 검증된 경우에만 c_R과 K_{BR}을 갱신한다. UPDCPL 메시지를 생성하기 위해 $c_B = c_B + 1$과 XId_R값을 XOR 연산한 이후에, DATA 전송시 노출되었던 XId_R값을 새로이 갱신한다. 마지막으로 생성된 UPDCPL을 백엔드 서버로 전달한다.
- 단계 ⑭ : 리더의 업데이트를 확인하는 단계로, 백엔드 서버는 전송된 UPDCPL에 갱신된 카운터 c_B를 XOR 연산함으로써 어떤 리더가 데이터 업데이트를 마쳤는지 확인할 수 있다. 확인된 리더가 다음 세션에 사용할 XId_R을 갱신함으로써 리더와 랜덤 ID의 동기화를 맞춘다. UPDCPL이 일정 기간 동안 도착하지 않을 경우, 사전에 설정된 횟수 동안 DATA 전달 과정을 반복한다.

시나리오3. 백엔드 서버 위장 공격 탐지 : 백엔드 서버 위장 시나리오의 경우, 공격자는 노출되지 않은 Id_R, K_{BR}, ps_Id_R, Id_T, K_T, info의 정보를 알 수 없으며, 이전 세션에서 사용되었던 XId_R, XId_T, Pc_R은 도청을 통해 수집할 수 있다. 현재 세션에서 이용될 XId_R, XId_T는 암호화되어 전송되므로 획득할 수 없다. 하지만, 본 시나리오에서는 공격자가 XId_R과 K_{BR} 쌍을 알고 있다고 가정함으로써 정당한 인증 정보가 백엔드 서버로 전달되더라도 백엔드 서버 위장 공격을 리더가 탐지할 수 있음을 보인다.

- 단계 ①~⑥ : 정단한 리더와 태그 사이의 메시지 전송 과정을 보여준다. 리더는 태그로부터 수신한 인증 정보를 이용하여 새로운 인증 정보를 생성하고 이를 백엔드 서버로 전달한다.



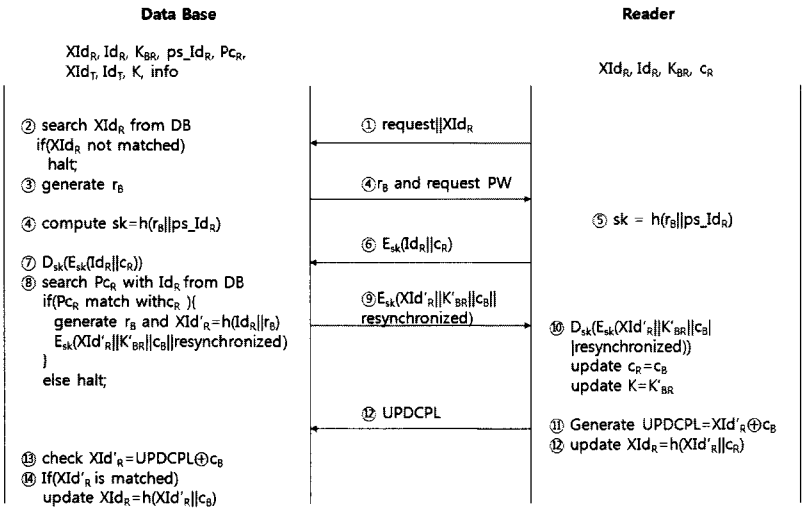
〔그림 8〕 백엔드 서버 위장 공격 탐지 과정

- 단계 ⑦~⑨ : 공격자는 자신이 정당한 백엔드 서버인 것처럼 데이터를 변조하고 이를 리더에게 전달한다. 이 과정에서 Id_R, Id_T, K_T를 모르는 공격자는 정확한 c_T, c_R, m_{Right}을 생성할 수 없다. 하지만, 공격자는 자신이 알고 있는 K_{BR}을 이용하여 거짓 정보를 리더에게 전달할 수 있다.
- 단계 ⑩~⑪ : 리더는 수신한 데이터를 복호하고 r_R과 c_R을 검증한다. Id_R을 모르는 공격자는 정확한 c_R을 생성할 수 없다. 하지만, 도청을 통해 c_R값을 습득할 수 있으므로, 태그로 DATA'를 송신할 가능성이 있다.
- 단계 ⑫ : 태그는 수신한 데이터(DATA')를 복호하고, r_T, c_T, m_{Right}을 검증한다. 공격자가 c_T와 m_{Right}을 검증한다. 공격자가 c_T와 m_{Right}을 생성할 수 없으므로 태그는 통신을 중단한다. 이과 같은 방법으로 거짓 정보를 전송하려는 백엔드 서버 위장 공격을 방지할 수 있다.

4.4 동기화 실패를 위한 재동기화 과정

무선 리더의 경우 이동시 전파 송·수신 상태가 원활하지 않거나, 리더가 오프라인 상태인 경우 백엔드 서버와 통신이 두절될 수 있다. 통신이 두절된 동안 공격이 발생하지 않아 c_B값이 증가하지 않은 경우라면 K_{BR}이 갱신되지 않으므로, 통신이 재개되거나 리더가 오프라인 상태가 되면 추가적인 정보의 갱신 없이 통신이 가능하다. 반면, 통신이 두절된 동안 공격이 발생하여 c_B값이 갱신된 경우에는 c_R보다 c_T가 더 커지는 상황이 발생하므로 태그가 리더의 요청에 반응하지 않게 된다. 또는, 공격자에 의해 XId_R이 도용된 경우 백엔드 서버에서 XId_R을 이용하는 리더를 비활성화시키는 경우가 발생할 수 있다. 이와 같이 정당한 리더가 통신이 불가능해진 경우, 리더 동기화 단계를 통해 백엔드 서버와 동기화를 맞출 수 있다.

- 단계 ① : 통신이 불가능해진 리더는 XId_R을 식별자로 백엔드 서버로 동기화 요청 메시지를 전달한다.
- 단계 ②~④ : 백엔드 서버는 XId_R을 확인하고 존재하는 경우 r_B와 함께 패스워드 요청 메시지를 전달한다.
- 단계 ⑤~⑥ : 리더는 $sk=h(r_B||ps_Id_R)$를 생성하고, 이를 이용하여 Id_R과 c_R을 암호화해 회신한다.
- 단계 ⑦~⑨ : 백엔드 서버는 세션키를 생성하고 수신한 메시지를 복호한다. 패스워드와 Id_R, Pc_R이 동일한 경우에만 $sk(Id_R||c_R)$를 복호화하고 c_R이 Id_R의 이전 세션 정보로 확인되면, XId'_R, K'_{BR}, c_B, 메시지를 세션키를 이용해 암



〔그림 9〕 리더 동기화 단계

호화한 후 리더에게 전달한다.

- 단계 ⑩~⑫ : 리더는 c_R, K_{BR}을 갱신하고, UPDCPL을 생성한 뒤, XId_R을 갱신한다. 마지막으로 UPDCPL을 회신한다.
- 단계 ⑬~⑭ : UPDCPL을 수신한 백엔드 서버는 c_B를 이용하여 이를 검증하고 맞을 경우 다음 세션에서 이용할 XId_R을 갱신한다.

V. 제안하는 프로토콜 안전성 및 효율성 분석

4장에서 공격 시나리오에 대한 프로토콜 분석을 통하여 제안한 프로토콜의 공격 탐지 기능 및 재동기화 기능을 검증하였다. 본 장에서는 제안하는 프로토콜의 안전성 및 효율성 검증을 검증한다. 3.1절에서 정의한 위협에 대해 제안하는 프로토콜이 안전함을 보이고, 기존 인증 프로토콜과 연산량을 비교한다.

5.1 안전성 분석

도청 공격에 안전성 보장 : 도청 공격은 무선 구간에서 전달되는 정보를 수집하여 태그의 정보를 알아내는 공격이다. 도청 공격을 막기 위해서는 도청을 통해 알아낸 정보로부터 다음 세션에 이용되는 인증 정보를 생성하지 못하도록 설계해야 한다. 제안하는 프로토콜의 통신 과정에서는 XId_R, XId_T, m_{Left}, r_T, r_R, Xc_T, Xc_R, c_R, UPDCPL 등이 암호화되지 않고 전달되므로 도청이 가능하다. XId_R과 XId_T는 리더와 태그의 식별자로 매 세션에서 갱신되는 값이며, 갱신된 값은 리더와 태그가 소유한 각각의 키로 암호화되어 전달된다. Xc_R과 Xc_R은 리더와 태그가 소유하고 있는 Id_R과 Id_T을 알고 있어야 생성할 수 있으며, 리더와 태그에 의해 매 세션 갱신된다. 즉, 제안하는 프로토콜에서 암호화되지 않고 전달되는 정보는 모두 다음 세션에 갱신되는 값들이며, 백엔드 서버가 갱신한 정보는 모두 암호화되어 전달되므로 도청 공격에 대하여 안전성을 보장한다고 볼 수 있다.

위장 공격 및 위조 공격에 안전성 보장 : 위장 공격은 공격자가 정당한 개체로 인식되도록 하기위해서 전달되는 인증정보를 재전송하거나 위조하는 공격이다. 공격자는 도청을 통해 이전 세션들의 인증정보를 수집할 것이다. 공격자는 전달되는 정보를 위조해야만 정당한 개체로 위장이 가능하지만, 제안하는 프로토콜에서는 암호화되지 않고 전달된 인증정보는 다음 세션에서 사용되지 않는다. 앞서 우리는 각 개체에 대한 위장 공격 시나리오 분석을 통하여 백엔드 서버, 리더, 태그 각각의 위장 공격을 탐지하고 인증정보를 갱신하는 과정을 소개하였다. 따라서 제안하는 프로토콜은 위장 및 위조 공격에 대하여 안전성을 보장한다고 볼 수 있다.

위치추적 공격에 안전성 보장 : 위치추적 공격은 공격자가 도청 공격을 통하여 획득한 인증정보를 수집하여 태그의 위치 정보를 추적하는 공격이다. 위치추적 공격을 막으려면 노출되는 정보를 모두 갱신해야 한다. 제안하는 프로토콜에서는 다음 세션에 이용되는

〔표 4〕 제안하는 프로토콜의 상호인증 요소 분석

B->R	R->B	T->R
XId_R 수신 후 K_{BR}로 암·복호화 Xc_R 수신 후 c_R을 이용한 m_{Left}확인	r_T 전달 후 r_T 수신 Xc_T 전달 후 c_R 수신 XId_R,K_{BR} 쌍을 이용한 암호화	카운터 비교를 통한 동기화 검사 T->B을 인증시 T->R 간접인증
B->T	B->T	T->B
Xc_T 수신 후 c_T를 이용한 m_{Left}확인 m_{Left} 확인 후 m_{Right}로 암호화	r_R 전달 후 r_R 수신 r_R, c_R 정보가 포함된 m_{Left}을 B에서 인증될 경우에만 상품정보 수신	r_T 전달 후 r_T 수신 Xc_T 전달 후 c_T 수신 m_{Left} 전달 후 m_{Right} 수신 m_{Right}로 암호화된 메시지 수신

*기호 설명 : B : Backend-database, R : Reader, T : Tag
B->R : Backend-databese가 리더를 인증하는데 필요한 인증 요소

인증정보가 모두 갱신되도록 설계하였고, 갱신된 정보 또한 암호화되어 전달되므로 이전 인증정보들을 모두 수집하더라도 상관관계를 알아낼 수 없으므로 위치추적이 불가능하다. 따라서 제안하는 프로토콜은 위치추적 공격에 대하여 안전성을 보장한다고 볼 수 있다.

서비스 거부 공격에 안전성 보장 : RFID 시스템에서의 서비스 거부 공격은 두 가지 형태로 나누어볼 수 있다. 첫째, 태그로의 서비스 거부 공격 - 공격자는 태그로 과도한 쿼리를 전송함으로써 태그의 전력을 소비하거나 다른 태그의 요청을 수신하지 못하도록 할 수 있다. 둘째, 거짓 인증정보 갱신을 통한 서비스 거부 공격 - 공격자는 고의로 변조하여 갱신되는 인증정보를 리더나 태그가 수신하지 못하도록 함으로써 각 개체 간의 비동기화를 유발할 수 있다.

제안하는 프로토콜에서는 첫 번째 타입의 공격을 방지하기 위해 카운터를 이용한 동기화 검증 방식[4]을 이용하였다. 태그가 동기화되지 않은 리더를 확인하고 정당한 리더의 요청으로 판단될 경우에만 인증정보를 생성함으로써 무조건적인 인증정보 제공과 태그 전력 소모 공격을 막을 수 있다. 두 번째 타입의 공격의 경우, 백엔드 서버에서 정상적으로 인증이 이루어졌거나, 인증정보 갱신이 필요한 경우에 UPDCPL 메시지를 전송하도록 2번의 통신횟수를 추가하였으며, 메시지가 완전히 수신되기 전까지는 특정횟수 만큼 반복 전송하도록 하였다. UPDCPL 값은 인증된 백엔드 서버, 리더, 태그만이 현재 세션에서 유일하게 생성할 수 있는 값이다. 인증이 완료된 경우 태그가 생성한 UPDCPL을 백엔드 서버와 태그가 인증함으로써 동기화가 이루어졌음을 확인하고, 인증정보가 갱신된 경우에는 UPDCPL을 통해 동기화를 확인한 이후 백엔드 서버에서 XIdR을 갱신한다.

제안하는 프로토콜에서는 공격이나 주변 환경에 의하여 비동기화가 발생한 경우, 리더의 동기화를 위해서 "리더 동기화 단계"를 수행할 수 있도록 하고 있다. 리더 동기화 단계에서 전달되는 정보는 XId_R과 r_B를 제외한 모든 정보는 백엔드 서버와 비동기된 리더 사이의 세션키에 의해 암호화되므로 갱신된 정보를 안전하게 수신하는 것을 보장한다. 따라서 제안하는 프로토콜은 서비스 거부 공격에 대하여 안전성을 보장한다고 볼 수 있다.

상호 인증 보장 : RFID 시스템에서 안전한 통신을 위해 각 개체는 서로의 신분 확인 과정을 거쳐야 한다. 제안하는 프로토콜에서는 백엔드 서버는 리더 및 태그와 상호인증을 제공하고, 리더는 백엔드 서버 및 태그와 상호인증을 제공하고, 태그의 경우 백엔드 서버와의 상호인증을 제공함으로써 리더와의 상호인증은 간접적으로 이루어지게 된다. 각 과정은 〔표4〕와 같다.

부가정보 생성 공격에 대한 안전성 보장 : 위에서 언급한 요구사항을 만족한다하더라도 노출된 정보들을 결합하여 갱신되는 정보에 대한 유추나, 부가적으로 개체 식별이 가능한 인증 정보를 생성할 수 없어야 한다. 즉, 암호화되지 않은 데이터의 취합하여 새로운 정보를 생성할 수 없어야 한다. 제안하는 프로토콜에서 XId_R과 XId_T는 각각의 Id_T와 r_B의 해쉬 연산에 의해 생성되고, 식별자는 개체 식별을 위해서만 사용되며 다른 인증정보에 포함되지 않는다. 이외에 노출되는 정보들은 랜덤하게 생성되는 값이기 때문에 개방된 환경에서 도청된 정보를 통해 각각의 리더와 태그를 구분할 수 없다.

전방향 안전성 보장 : 전방향 안전성은 모든 세션의 정보가 공격자에게 노출되어도 메시지 분석을 통해 태그의 정보가 노출되거나 위치추적이 불가능해야 함을 보장해야 한다. 제안하는 프로토콜에서는 다음 세

〔표 5〕 기존 상호인증 프로토콜과의 안전성 비교

	SP-RFID〔1〕	ABYN-RFID〔2〕	LOK-RFID〔3〕	제안하는 방식
상호인증	리더<->태그, 태그->DB 불가	태그->DB, 태그->리더 불가	모두 가능	모두 가능 + 비동기리더 탐지가능
DB-리더 구간	안전한 채널로 가정	안전한 채널로 가정	안전한 채널로 가정	공개 채널로 가정
재전송/위조 공격	X	O	O	O
위장 공격	X	$\triangle^1$	$\triangle^1$	O
태그 위치 추적 공격	X	X	O	O
서비스 거부 공격	X	X	$\triangle^2$	O
전방향안전성 공격	X	X	O	O
부가정보 생성 공격	X	O	O	O

*부가설명 : $\triangle^1$: DB-리더 구간을 안전한 채널로 가정하여 백엔드 서버의 위조 공격을 고려하지 않음.
$\triangle^2$: 태그-리더 구간의 프로토콜 취약성을 이용한 서비스 거부 공격만을 고려하였음.

션에 이용되는 인증정보가 모두 갱신되도록 설계하였고, 갱신된 정보는 암호화되어 전달되므로 이전 세션의 식별자 XId_R, XId_T와 다음 세션의 식별자 XId'_R, XId'_T의 상관관계를 알아낼 수 없다. 또한, m_{Left}, Xc_T, Xc_R, UPDCPL에는 리더와 태그의 랜덤 값이 포함되어 연관성을 알아내기 어렵다. 따라서 제안하는 프로토콜은 전방향 안전성을 보장한다고 볼 수 있다.

기존 연구들이 제공하는 안전성과 제안하는 프로토콜이 제공하는 안전성을 〔표5〕와 같이 나타낼 수 있다.

5.2 효율성 분석

본 절에서는 제안하는 프로토콜의 효율성에 대해 분석해보고자 한다. 기존에 연구된 인증 프로토콜들〔1-3〕 중 안전성이 가장 뛰어난 LOK-RFID〔3〕와 제안하는 프로토콜의 연산량 분석을 수행하도록 한다. 효율성 분석을 위한 지표로 태그 검색율, 난수 생성 횟수, 대칭키 연산 횟수, 해쉬 연산 횟수, XOR 연산 횟수, 타임스탬프 연산 횟수와 최종적인 통신 라운드 횟수 등을 정하였다. 먼저 LOK의 연산량에 대한 분석을 제시하고 이어서 제안하는 프로토콜의 연산량에 대한 분석을 기술한다.

LOK-RFID는 백엔드 서버와 리더를 하나의 시스템으로 설계〔그림3〕하였으나 백엔드와 서버 구간을 고려할 경우 총6의 통신이 이루어진다. 백엔드 서버의 경우 난수 연산은 수행하지 않으며, 시스템을 안전한 구간으로 가정하였으므로 시스템 내에서 백엔드 서버와 리더 구간에 전달되는 3회의 통신에 대한 암·복호화 3회가 필요할 것으로 보인다. 태그의 인증 메시지 연산을 위해서 사용되는 해쉬 연산은 동적 ID의 상태에 따라 2가지로 분류될 수 있다. 서버에 저장된 ID와 태그의 ID 간에 동기화가 맞는 경우, 인증값 검증에 1회, 인증될 경우 키 갱신에 1회, ID 갱신 1회가 수행되어 총 3회의 해쉬 연산이 수행된다. 서버에 저장된 ID와 태그의 ID 간에 동기화가 맞지 않을 경우, 모든 태그를 대상으로 다음 과정을 수행한다. 현재 키로 생성된 인증값 검증을 위해 1회, 인증될 경우 키 갱신에 1회, ID 갱신에 1회를 수행하므로 총 3회의 해쉬 연산이 수행된다. 만약, 현재 키로 검증되지 않을 경우 이전키로 생성된 인증값 검증을 위해 1회, ID 갱신에 1회가 수행되어 총 2회의 해쉬 연산이 추가로 수행된다. 즉, ID가 동기화된 경우 최소 1회에서 3회의 해쉬 연산이 수행되고, ID가 비동기화된 경우 현재키나 이전키로 인증 여부를 확인하게 되므로 3회의 해쉬 연산이 수행된다. 이는 백엔드 서버의 DB에 n개의 태그가 존재한다고 가정하면 최악의 경우 3n회의 해쉬 연산이 수행될 수 있음을 의미한다. 〔그림3〕의 시스템 상에서 리더는 쿼리 전송시 난수 생성을 1회 수행하고, 이 값을 백엔드 서버로 전송해야 백엔드 서버와 태그 간의 난수 동기화가 필요하다. 또한, 백엔드 서버와 리더의 구간을 안전하다고 가정하였으므로 백엔드 서버와 동일하게 3회의 암·복호화가 필요할 것으로 보인다. 태그는 인증정보 생성 및 키 갱신에 1회의 난수 생성이 필요하다. 인증정보 생성, ID 갱신, 키 갱신에 각각 1회의 해쉬 연산이 수행되므로 총 3회의 해쉬 연산이 필요하다.

제안하는 프로토콜의 연산량을 살펴보면 다음과 같다. 먼저 백엔드 서버에서는 리더와 태그의 랜덤 ID 갱신을 위해서 1회의 난수를 생성한다. 백엔드 서버와 리더의 안전한 메시지 교환을 위해 2회, 백엔드 서버

〔표 6〕 기존 상호 인증 프로토콜과의 효율성 분석

	SP-RFID〔1〕			ABYN-RFID〔2〕			LOK-RFID〔3〕			제안하는 방식		
태그 타입	정적 ID			정적 ID			동적 ID			동적 ID 특성을 만족하는 정적 ID		
태그 검색율	전사적 해쉬 연산			전사적 해쉬 연산			전사적 DB 검색 후 1회의 해쉬연산			리더 랜덤 ID 기반(m회) DB 검색 후 1회의 해쉬연산		
비동기화시 태그 검색율	-			-			전사적 DB 검색 후 2n회의 해쉬연산			(m+n)회 DB 검색 후 1회의 해쉬연산		
	DB	리더	태그	DB	리더	태그	DB	리더	태그	DB	리더	태그
난수생성	-	1	-	-	1	1	-	1	1	1	1	1
대칭키 연산	2	2	-	2	2	-	3	3	-	3	2	1
해쉬연산	-	1	1	n	1	1	3 3n[1)]	-	3	5 2m+2[2)]	1	1
XOR연산	-	1	1	-	-	-	-	-	-	3	2	2
타임스탬프	-	-	-	-	-	-	-	-	-	1	3	-
통신 횟수	6			4			6			7		

*기호설명 : n : 태그의 수, m : 리더의 수,
1) 태그 검색의 최악의 경우, 3n회만큼의 해쉬 연산이 필요함.
2) 리더 공격이 탐지된 경우, ID와 암호키 갱신을 위해 2m+2회의 해쉬 연산이 필요함.

에서 태그로 전달되는 메시지의 안전성을 위해 1회의 암·복호화가 수행되므로 총 3회의 대칭키 연산이 수행된다. 해쉬 연산의 경우, 리더와 태그의 랜덤 카운터 연산에 각 1회, 인증 정보 검증에 1회, 리더와 태그의 랜덤 ID 갱신에 1회로 총 5회의 해쉬 연산이 수행된다. (단, 리더 공격이 탐지된 경우, 백엔드 서버와 리더 구간의 비밀키 갱신을 위해 m-1회의 해쉬 연산이 수행된다.) XOR 연산의 경우 리더와 태그의 랜덤 카운터 연산에 각1회, UPDCPL 인증을 위해 1회로 총 3회의 XOR 연산이 수행된다. 타임스탬프 연산의 경우, 백엔드 서버가 전송한 메시지의 응답시간을 측정하는데 1회 사용된다. 리더는 쿼리 전송시 난수 생성을 1회 수행하고, 태그로부터 수신 받은 메시지를 백엔드 서버로 전송하는데 1회, 백엔드 서버로부터 전달받은 메시지를 복호화하는데 1회로 총 2회의 암·복호화 연산이 수행된다. 해쉬 연산의 경우 리더가 가지고 있는 카운터를 랜덤 카운터로 변경하는데 1회 수행된다. XOR 연산의 경우 리더의 카운터를 랜덤 카운터로 변경하는데 1회, UPDCPL 값을 검증하는데 1회로 총 2회 연산이 수행된다. 타임스탬프 연산은 태그로 쿼리 전송 후 응답을 측정하는데 1회, 태그의 정보의 인증을 위해 백엔드 서버로 전송하는 과정에서 1회, 인증 후 태그의 정보 갱신을 위해 태그로 전달하는 과정에서 1회로 총 3회의 타임스탬프 연산이 수행된다. 태그는 자신의 인증관련 정보를 생성하기 위해 1회의 난수 생성 과정을 수행하고, 리더가 태그의 정보를 확인하고 백엔드 서버로부터 갱신 정보를 수신하여 암호화된 메시지의 복호화 1회를 수행한다. 해쉬 연산의 경우 인증정보 m을 생성하는데 1회 사용된다. XOR 연산의 경우 랜덤 카운터 생성시 1회, UPDCPL 생성시 1회로 총 2회의 XOR 연산을 수행한다. 타임스탬프 연산은 수행되지 않는다. 마지막으로 통신 횟수의 경우 백엔드 서버와 리더 구간에서 3회, 리더와 태그 구간에서 4회로 총 7회의 통신이 이루어진다.

가장 자원제약적인 태그의 측면에서 살펴보면 해쉬 연산이 3회에서 1회로 줄었다. 반면, 갱신정보의 노출을 방지하기 위한 1회의 복호화 과정이 추가되었으며, 2회의 XOR 연산이 추가되었다. 경량화된 암호 알고리즘〔14,15〕을 적용할 수 있다고 본다면, 2회의 해쉬 연산을 줄임으로써 연산량 부하를 줄이면서 안전성을 높였다고 볼 수 있다. 기존 연구〔1-3〕과의 연산량 비교를 위해 〔표6〕을 제시한다.

VI. 결론

본 논문에서는 현실적인 공격을 고려하기 위해 전 구간을 공개 채널로 고려하여 공격자가 백엔드 서버, 리더, 태그로 가장하는 공격의 시나리오를 제시하였다. 제안하는 프로토콜은 상호인증, 재전송 공격, 위장공격, 태그 위치 추적 공격, 서비스 거부 공격에 안전함은 물론, 고정 ID 방식에 랜덤 식별자와 카운터를 활용하여 공격자가 백엔드 서버, 리더, 태그로 가장하더라도 개체간의 인증 과정에서 공격을 탐지할 수

있다. 한편, 최근 연구[3]와 비교해볼 때, 효율성면에서 인증 과정에서 XOR 연산과 대칭키 암호 연산이 추가되고 통신횟수가 증가하는 단점은 Trade-off 로 작용한다.

하지만 고정 ID 방식의 RFID 시스템에 해쉬 연산을 통해 랜덤 ID 만들어 사용함으로써 백엔드 서버가 갖는 동적 ID의 일반적인 효율적인 태그 검색을 지원하고, 프로토콜 자체 적으로 민감한 인증 정보를 암호화함으로써 별도의 보안 채널을 요구하지 않는다는 점에서 기존 논문들 보다 높은 보안성을 제공한다. 연산량을 증가시키지 않으면서도 RFID 시스템 내에서의 공격 여부를 탐지할 수 있는 추가 연구가 필요하다.

참고문헌

[1] 신진섭, 박영호, "RFID/USN에서의 EXOR과 해쉬 함수를 이용한 인증 프로토콜," 한국산업정보학회논문지, 12(2), pp. 24-29, 2007년 6월.

[2] 안해순, 부기동, 윤은준, 남인길, "RFID/USN 환경을 위한 개선된 인증 프로토콜," 전자공학회논문지, 46(1), pp. 1-10, 2009년 1월.

[3] 임지환, 오희국, 김상진, "동기화 문제를 해결한 새로운 동적 아이디기반 RFID 상호 인증 프로토콜," 정보처리학회논문지, 15-C(6), pp. 469-480, 2008년 12월.

[4] G.Avoine, C.Lauradoux, and T.Martin, "When Compromised Readers Meet RFID," 10th International Workshop, WISA 2009, LNCS 5932, pp. 36-50, Aug. 2009.

[5] 하재철, 백이루, 김환구, 박제훈, 문상재, "해쉬함수에 기반한 경량화된 RFID 인증 프로토콜," 한국정보보호학회논문지, 19(3), pp. 61-72, 2009년 6월.

[6] S.A. Weis, S.E. Sarma, R.L. Rivest and D.W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," First International Conference on Security in Pervasive computing, pp. 50-59, 2004.

[7] M. Burmester, B. Medeiros and R. Motta, "Provably Secure Grouping-Proofs for RFID Tags," Proceeding in 8th IFIP WG 8.8/11.2 International Conference (CARDIS), vol. 5189, pp. 176-190, Sep. 2008.

[8] E.J. Yoon, K.Y. Yoo, "Two Security Problems of RFID Security Method with Ownership Transfer," Proceeding in 2008 IFIP International Conference on Network and Parallel Computing, pp. 68-73, Oct. 2008.

[9] National Institute of Standards and Technology, "Guidelines for Securing Radio Frequency Identification (RFID)," Natl. Inst. Stand. Technol. Spec. Pub. 800-98, Apr. 2007.

[10] K.Rhee, J. Kwak, S. Kim, and D. Won, "Challenge-Response Based RFID Authentication, Protocol for Distributed Database Environment," Proceedings of Second International Conference, SPC 2005, pp. 70-84, Apr. 2005.

[11] 김익수, "효율성을 고려한 해쉬 함수 기반의 안전한 RFID 인증 프로토콜", 한국통신학회논문지, 34(4), pp. 428-434, 2009년 4월.

[12] T. Dimitriou, "A secure and Efficient RFID Protocol that could make Big Brother (partially) Obsolete," Proceedings of 4th Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM'06), pp. 270 - 275, Mar. 2006.

[13] 김진호, 서재우, 이필중, "저비용 RFID시스템에 적합한 효율적인 인증 방법," 정보보호학회논문지, 18(2), pp. 117-128, 2008년 4월.

[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] M. Reldhofer, J. Wolkerstorfer, "Strong

Crypto for RFID Tags - A Comparison of Low-Power Hardware Implementations," Proceedings of IEEE International Symposium on In Circuits and Systems (ISCAS'07), pp. 1839-1842, May. 2007.

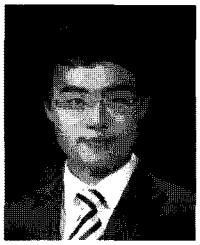
[17] A.Juels, R.L.Rivest, M.Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," 10th ACM Computer and Communications Security Conference (CCS'03), pp. 103-111, Oct. 2003.

[18] 염용진, "RFID시스템을 위한 암호 기술 동향," 정보통신연구진흥원 학술정보-주간기술동향", 1223, 2005년 11월.

[19] International Telecommunication Union, "The 5th revised text on ITU-T X.usnsec-1 | I SO/IEC CD 29180: Security framework for ubiquitous sensor network," ITU-T SG17, 942-PLEN, Apr. 2010.

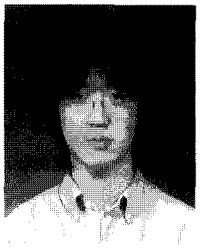
[20] International Telecommunication Union, "Threats and requirements for protection of personally identifiable information in applications using tag-based identification," ITU-T SG17, X.1171, Feb. 2009.

〈著者紹介〉



여 돈 구 (Don-Gu Yeo) 학생회원
2009년 2월: 순천향대학교 정보보호학과 졸업
2009년 3월: 순천향대학교 정보보호학과 석사과정
〈관심분야〉 정보보호, USN 보안, 클라우드 컴퓨팅 보안, IPTV 보안, 역추적

이 상 래 (Sang-Rae Lee) 학생회원
2010년 2월: 순천향대학교 정보보호학과 졸업
2010년 3월: 순천향대학교 정보보호학과 석사과정
〈관심분야〉 정보보호, 클라우드 컴퓨팅 보안, IPTV 보안, 역추적



장 재 훈 (Jae-Hoon Jang) 학생회원
2009년 2월: 순천향대학교 정보보호학과 졸업
2009년 3월: 순천향대학교 정보보호학과 석사과정
〈관심분야〉 역추적, IPTV 보안, USN 보안

염 흥 열 (Heung-Youl Youm) 종신회원
1981년 2월: 한양대학교 전자공학과 졸업(학사)
1983년 2월: 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월: 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월~1990년 9월: 한국전자통신연구소 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월: 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월: 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재: 한국정보보호학회 총무이사, 학술이사, 교육이사, 총무이사, 논문지편집위원 위원장(역), 수석부회장(현)
2005년~2008년: ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월: 정보통신연구진흥원 정보보호전문위원
2009년 5월~현재: 국정원 암호검증위원회 위원
2009년~현재: ITU-T SG17 부의장/SG17 WP2 의장
〈관심분야〉 인터넷보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜