情報保護學會論文誌
第20卷 第2號, 2010. 4

개선된 프라이버시와 재동기화를 제공하는 RFID 상호인증 프로토콜

김 영 재,† 전 동 호, 권 혜 진, 김 순 자‡
경북대학교

RFID Mutual Authentication Protocol Providing Improved Privacy and Resynchronization

Young-Jae Kim,† Dong-Ho Jeon, Hye-jin Kwon, Soon-Ja Kim‡
Kyungpook National University

요 약

Ha 와 M.Burmester등에 의해 제안된 RFID 프로토콜들은 전방향 안정성을 보장하기 위해 세션의 정상 종료 후에는 태그의 ID는 일방향 함수인 해시 함수를 이용해 업데이트 된다. 본 논문에서는 Vaudenay가 제안한 프라이버시 게임 모델을 적용해 두 프로토콜의 프라이버시 측면에서의 문제점과 태그의 저가 구현과 효율적인 재동기화를 방해하는 원인에 대해 분석한다. 본 눈문 에서는 이러한 문제점들을 해결하기 위해 두 프로토콜의 장점을 접목한 새로운 해시 연산 기반 상호 인증 RFID 프로토콜을 제안한다. Ha등이 제안한 프로토콜들의 태그와 리더 간 공유 정보의 재동기화 알고리즘을 기반으로 M. Burmester가 제안한 프로토콜의 순환 카운터보다 간단하고 구현하기 쉬운 연속적인 비동기 발생 횟수를 기록하는 간단한 카운터를 적용한다. 프라이버시 역시 두 프로토콜에 적용하였던 프라이버시 게임을 제안 프로토콜에 수행하여 프라이버시가 개선되었음을 보인다.

ABSTRACT

Hash based RFID protocols proposed by Ha and M.Burmester is a scheme that tag's ID is updated using hash function to provide forward secrecy after session end. But this protocols have a problem both privacy and efficiency. This paper analyze a problem for privacy to apply a privacy game model proposed by Vaudenay. we analyze the cause that these scheme is difficult with tag's cheap implementation and efficient resynchronization. To solve these problems, we proposed a new hash based mutual authentication protocol which apply only two protocol's advantages. this protocols is based of resynchronization algorithm for Ha et al.'s protocol and added a new simple counter to record the numner of continuous desynchronization between tag and reader secret informations. this counter is more simple than cyclic counter proposed by M. Burmester's protocol. Also, we prove that proposal protocol improve a privacy against a privacy attack which is executed for Ha and M. Burmester's protocols.

Keywords: RFID, Security, Privacy, Adversary, Resynchroinzation

I. 서 론

RFID(Radio Frequency Identification) 기술은 사물에 부착된 태그로부터 전파를 이용하여 사물의 정보 및 주변 환경을 인식하여 각 사물의 정보를 수집, 저장, 가공, 추적함으로써 사물에 대한 측위, 원격 처리, 관리 및 사물간 정보 교환 등의 다양한 서비스를 제공할 수 있다. [1-2] 이러한 기술은 기존의 바코드를 대체하여 물품관리를 네트워크화 및 지능화함으로써 유통 및 물품 관리뿐만 아니라 보안, 안전, 환경

접수일(2009년 5월 27일), 수정일(1차: 2009년 10월 28일, 2차: 2010년 1월 13일), 게재확정일(2010년 2월 12일)
† 주저자, saroosa@naver.com
‡ 교신저자, snjkim@ee.knu.ac.kr

관리 등에 혁신을 선도할 것으로 전망되며, 이전에 존재하지 않았던 거대한 새로운 시장을 형성할 것으로 기대된다.[1-3] 그러나 이러한 장점은 곧 RFID 시스템의 보안상 위협으로 이어진다. 리더와 태그간의 무선 통신은 유선 통신에 비해 도청되기 쉽고, 대량생산 환경에서 태그 가격의 한계로 인해 일반 컴퓨터 통신과 같이 연산 량이 많은 암호화 알고리즘을 쓸 수 없다.[4-5] 이에 Weis 등은 유선 통신에서 통용되고 있는 공개키나 대칭키 암호보다는 연산 량이 적으면서 암호학적 효과를 낼 수 있는 해시를 사용하여 태그의 정보를 숨기는 프로토콜을 제안하였다[6]. 이후 여러 연구자들에 의해 해시를 이용한 인증 프로토콜이 다양하게 제안되면서 해시 함수는 RFID의 보안 및 프라이버시 위협을 보호할 수 있는 차세대 프로토콜로 각광 받아왔다.

2007년, Ha등이 제안한 프로토콜들[7,13-14]은 전방향 안정성을 보장하기 위해 태그와 리더간의 공유 비밀정보는 세션의 정상 종료 후에 업데이트 된다. 만약 통신 중 비정상 종료가 발생하면 다음 세션에서는 정상 상태일 때와는 다른 태그 인증 알고리즘을 사용용하여 프로토콜을 수행한다. 따라서 공유 정보의 비동기가 생기더라도 다음 세션에서 태그 인증이 가능해 리더로부터 합법적인 태그로서 인식 받을 수 있다. 하지만, 이러한 비동기가 발생 하면 다음 세션에서는 태그인증을 위해서 데이터베이스에 등록된 모든 ID에 대한 해쉬연산을 요구함으로서 태그 검색 시간이 정상 상태에 비해 비약적으로 늘어나는 단점을 가진다. 또한, Vaudenay가 제안한 프라이버시 게임 모델을 이용해 공격 모델을 설계하여 특정 공격에 의해 프라이버시를 보장하지 못함을 보일 것이다.

2008년, M. Burmester가 제안한 프로토콜[8]은 태그와 데이터베이스에 동일한 순환 카운터를 저장해서 비동기가 발생 할 시 태그 ID 검색에 사용되는 메시지를 순환 카운터를 이용해 생성한다. 이를 이용하여 데이터베이스는 비동기 발생 시 태그 인증에 사용될 메시지를 세션 시작 전에 미리 계산하여 저장할 수 있다. 따라서, 공유 정보의 연속적인 비동기 발생 시에도 정상상태 일 때와 동일한 태그 검색 시간만을 요구한다. 하지만, 순환 카운터의 구현은 태그에 많은 저장 공간을 요구 하여 태그의 저가 구현을 방해하는 요소가 된다. 또한, 이 프로토콜 역시 특정 공격에 의해 프라이버시를 보장하지 못함을 보일 것이다.

본 논문에서는 두 프로토콜의 장점을 접목시킨 새로운 해시 연산 기반 상호 인증 RFID 프로토콜을 제안한다. Ha등이 제안한 프로토콜들[7,13-14]의 태그와 리더간의 비동기 상황에서의 재동기화 알고리즘을 기반으로 M. Burmester가 제안한 프로토콜[8]의 순환 카운터(cyclic counter)보다 간단하고 구현하기 쉬운 연속적인 비동기 발생 횟수를 기록하는 간단한 카운터(simple counter)을 적용한 새로운 프로토콜을 제안한다. 프라이버시 역시 두 프로토콜에 사용했던 프라이버시 게임을 제안 프로토콜을 대상으로 수행하면 두 프로토콜과는 다른 개선된 결과를 보임으로서 제안 프로토콜의 프라이버시가 향상 하였음을 보일 것이다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 기존 RFID 프로토콜을 분석하기 위한 관련 연구에 대해 설명하고 3장에서는 기 제안된 프로토콜을 소개하고 각 프로토콜들의 취약점을 분석한다. 4장에서는 이러한 취약점들을 개선한 새로운 해시 연산 기반 상호 인증 RFID 프로토콜을 소개한 뒤 5장에서 제안 기법에 대한 안전성과 효율성을 분석하여 6장에서 결론을 맺는다.

II. 관련 연구

2.1. RFID 시스템의 구성

RFID 시스템은 태그(tag), 리더(reader), 백엔드 데이터베이스(back-end database)의 세 가지 요소로 구성된다. 태그는 상품이나 물건에 부착되어 리더와 교신하여 상품 및 물건 과 관련된 데이터를 무선으로 리더에 전송한다.[1-3] 리더는 주파수 발신을 제어하고 무선인터페이스를 통해 태그로부터 수신된 데이터를 백엔드 데이터베이스에 전달하고, 백엔드 데이터베이스로부터의 응답을 다시 태그에 전달하는 중재자 역할을 한다. 일반적으로 리더와 태그사이의 프로토콜은 무선 상으로 서로 교신하기 때문에 공격자(adversary)의 도청이 가능하다. 백엔드 데이터베이스는 백엔드 서버(back-end server)라고도 불리며 한 개 또는 다수의 태그로부터 읽어 들인 데이터를 처리하며 분산되어 있는 다수의 리더 시스템을 관리하며, 리더를 대신해 대량의 데이터를 저장하고 복잡한 계산을 수행해 태그를 인증하는 역할을 한다. 본 논문에서는 백엔드 데이터베이스를 서버 혹은 *DB*로 간단하게 칭한다. 리더와 백엔드 데이터베이스간의 통신은 유선 상에서 이루어지며, 일반적으로 안전하다고 가정한다.[4-5] 따라서 본 논문에서는 리더와 백엔드 데이

터베이스간의 프로토콜에 대해서는 고려하지 않는다.

2.1.1 상호 인증 RFID 프로토콜 (Mutual Authentication RFID Protocol)

리더와 태그간의 리더는 태그에게서 메시지를 수신하게 되면 이를 서버에 전달한다. 서버는 이 메시지를 이용해 태그의 *ID*를 찾*output*아내고 이를 이용해 태그 인증을 수행 한 뒤 을 출력하여 리더인증을 위한 메시지와 함께 리더에전달한다. 서버가 태그 인증에 실패할 겨우 $output = \perp(null)$이 되고, 성공하게 되면 $output = ID$가 된다. $output = ID$일 경우 서버는 태그와의 공유정보를 업데이트한다. 리더가 리더인증을 위한 메시지를 태그에게 전달하면 태그는 이 메시지를 이용해 리더 인증을 수행한다. 태그가 리더 인증에 실패하게 되면 $output = \perp(null)$이고 성공하면 $output = OK$이다. $output = OK$일 경우 태그는 자신의 비밀정보를 업데이트한다.[9-10]

2.2. RFID 시스템 상에서 발생 가능한 공격

RFID 시스템의 태그와 리더는 무선 주파수를 이용해 메시지를 교환 하므로 불법적인 제 3자의 공격에 노출 될 수 있다. 따라서 실제 RFID 시스템에서 발생 할 수 있는 공격 기법 및 위협에 대해서 살펴본다.

2.2.1 도청공격 (Eavesdropping Attack)

태그와 리더 사이의 통신은 무선 방식이기 때문에 안전하지 않은 채널을 통해 공격자는 자유롭게 이러한 메시지들을 도청할 수 있기 때문에 태그 소유자의 신원(identity)을 노출시킬 수 있는 정보를 제공해 줄 수 있다. 따라서 안전한 RFID 시스템은 태그의 신원을 노출시킬 수 있는 비밀정보를 담고 있는 메시지들은 암호화 과정을 거쳐서 전송 되어야한다.

2.2.2 위장 공격(Spoofing Attack)

위장 공격이란 이전 세션들에 사용된 메시지들을 공격자가 도청한 뒤 이를 재전송 또는 변형하여 정당한 리더 혹은 태그로 위장하여 상대방을 속여 태그와 리더간의 인증과정을 통과 하는 공격을 말한다. 안전한 RFID 시스템은 이전 세션에서 통신 되었던 메시지들은 현재 세션에서의 태그와 리더 인증에 유용하게 사용 될 수 없도록 설계 되어야 한다.

2.2.3 위치 추적 공격(Location Tracking Attack)

태그는 리더에 대한 인증과정 없이 리더의 요청에 대해 항상 응답 메시지를 생성하기 때문에 공격자는 불법적인 리더를 여러 곳에 설치하여 임의의 태그의 응답 메시지를 수집 할 수 있다. 위치추적공격이란 공격자가 이러한 불법적인 리더를 이용하여 특정 태그 소지자의 이동경로를 추적하는 공격을 의미한다. 안전한 RFID 시스템은 공격자가 임의의 통신 메시지 내용이 특정한 태그로부터 송신되어졌음을 구분할 수 없어야 한다. 위치추적공격에 안전하기 위해서는 다음의 2가지 조건을 만족해야 한다.

i. 불구분성 (Indistinguishability)

불구분성이란 태그에서 나오는 메시지를 토대로 그 메시지의 출처를 알아내지 못하는 성질을 말한다. 이를 만족하기 위해서는 통신 중 특정 태그를 지칭하는 고정 메시지나 규칙적인 성질을 가지는 메시지 전송을 지양 하여야 한다.

ii. 전방향안전성 (Forward Secrecy)

전방향 안전성이란 공격자가 태그에 대해 물리적 공격을 시도하여 태그의 현재 비밀 정보 값을 획득 하였다 하더라도, 공격자는 획득 정보를 이용하여 태그 소지자의 과거 이동 경로를 추측할 수 없는 성질을 말한다. 따라서 RFID 시스템이 전방향 안전성을 보장하기 위해서는 특정 태그와의 통신에서 사용되는 메시지가 일정하거나 규칙적으로 생성되어 공격자가 메시지를 보고 태그를 쉽게 추측할 수 없어야 하고, 또한, 현재의 정보를 토대로 이전의 정보를 추측할 수 없어야 한다.

2.2.4 비동기화 유도 공격(Desynchronization Attack)

비동기화유도공격이란 공격자가 메시지 위조 또는 가로채기를 통해 프로토콜의 비정상 종료를 유도함으로서 리더와 해당 태그가 공유하는 비밀정보의 비동기화를 유도하거나 해당 태그가 더 이상 합법적인 리더로부터 인증을 받을 수 없게 하는 공격을 의미한다. 이는 일종의 서비스 거부 공격(DoS, Denial of Service)으로 이러한 공격에 안전하려면 태그와 리더간의 비밀정보의 비동기화가 발생 하더라도 다음 세션

에서 해당 태그는 합법적인 리더로부터 인증을 받을 수 있어야 하며, 태그와 리더간의 비밀 정보의 동기 회복이 가능해야 한다.

2.3. 안전성 측면 요구 조건

RFID 시스템을 안전성 측면에서 살펴볼 때 만족해야 할 조건은 크게 정확성(correctness), 보안성(security), 프라이버시(privacy)의 3가지가 있으며, 본 논문에서는 Vaudenay가 제안한 보안 증명 모델 [9-10]에 입각하여 RFID 프로토콜의 안전성을 분석하도록 한다.

2.3.1 정확성 (Correctness)

RFID 시스템의 정확성은 시스템 자체의 오류 가능성을 측정하는 항목이다. 어떠한 공격자의 개입 없이 태그와 리더간의 프로토콜 세션이 실행되었음에도 불구하고, 잘못된 태그와 리더 인증이 발생 한 경우를 말한다. RFID 시스템의 정확성을 증명하기 위해서는 다음의 실험을 수행해야 한다.

1. 리더를 구성한다.
2. 합법적(legitimate) 혹은 불법적(not legitimate)인 ID를 가지는 태그와 리더들을 생성한다.
3. 리더와 태그간의 프로토콜을 수행하여 리더와 태그의 *output*들을 관찰한다.
4. 태그(리더)가 합법적이라면 $output = ID$ (OK)이며, 불법적이라면 $output = \perp$가 되어야 한다.

다음의 세 가지 경우에 RFID 시스템은 정확성을 위반한다.

(1) 잘못된 부정(false negative) : 태그 ID 또는 리더 π 가 합법적임에도 $output = \perp$ 인 경우.
(2) 잘못된 긍정(false positive) : 태그 ID 또는 리더 π 가 불법적임에도 $output \neq \perp$인 경우.
(3) 부정확한 확인(incorrect identification) : 태그 ID가 합법적임에도, $output \notin \{ID, \perp\}$ 인 경우.

이러한 잘못된 부정, 잘못된 긍정 그리고 부정확한 확인이 일어날 확률이 0에 가깝다면, RFID 시스템은 정확성(Correctness)을 가진다.

2.3.2 안전성 (Security)

RFID 시스템에서의 안전성은 공격자의 실제 공격에 얼마나 안전한지를 측정하는 항목이다. 어떠한 공격자가 합법적인 태그(리더)인 것처럼 위장하여 하나의 프로토콜 세션을 수행하여 태그(리더) 인증에 성공하였을 경우 시스템은 불안전(insecure) 하다고 한다. 이러한 상황이 발생할 확률이 0에 가까울 정도로 매우 작다면 RFID 시스템은 안전성을 가진다고 한다. 실제 RFID 시스템에 이러한 안전성을 위협할 수 있는 공격 유형으로는 위장 공격(spoofing Attack)이 있다.

2.3.3 프라이버시 (Privacy)

RFID 시스템은 공격자가 임의의 합법적인 태그들 중에서 특정 태그를 구분할 수 있지 못하게 함으로써 태그의 익명성(anonymity)을 보장해야 한다. 프라이버시를 위협하는 공격으)로는 위치추적공격, 비동기화유도공격 등이 있다. 본 논문에서는 프라이버시의 침해 여부를 판단하기 위해 먼저 공격자(adversary)와 공격자 클래스(adversary class)에 따라 구분하여 다양한 프라이버시 게임을 수행 후 그 결과를 분석하여 해당 공격에 대한 프라이버시 보장 여부를 판단하다.

정의 1. 공격자(Adversary)
공격자는 다음의 오라클들을 사용할 수 있다.

(1) $CreateTag^b(ID)$: 합법적($b=1$) 혹은 불법적($b=0$)인 ID를 가지는 프리 태그(free tag)들을 생성한다. 이 오라클은 태그를 구성하고 $b=1$일 경우에만 리더의 데이터베이스에 태그의 정보를 업데이트한다.
(2) $DrawTag(vtag) \rightarrow (ID, b)$: 프리태그부터 비밀정보 ID를 가지는 $vtag$를 추출한다. 이 오라클은 추출된 태그(drawn tag)의 합법여부를 기록한 b 비트와 $vtag$의 ID를 보관하는 테이블 $\tau(vtag)$를 생성한다.
(3) $Free(vtag)$: $vtag$를 프리태그 집합으로 되돌린다.
(4) $Launch \rightarrow \pi$: 이 오라클은 리더가 새로운 프로토콜 세션 π을 시작하기 위해 사용한다.
(5) $SendReader(\pi, m) \rightarrow m'$: 리더 π에게 메시지 m을 보내서 응답 m'를 받는다.

(6) $SendTag(vtag, m) \rightarrow m'$: $vtag$에게 메시지 m을 보내서 응답 m'를 받는다.

(7) $Execute(vtag) \rightarrow (\pi, transcript)$: 리더와 $vtag$ 간의 프로토콜 π를 실행한다.

(8) $Result(\pi) \rightarrow x$: 프로토콜 세션 π의 수행 후 $output \neq \perp$ 이면 1을 반환, 그렇지 않으면 0을 반환한다.

(9) $Corrupt(vtag) \rightarrow S$: 태그의 현재 비밀 값 S를 반환한다. 만약 이 오라클의 호출 후에 $vtag$가 더 이상 사용되지 않는다면 $vtag$는 파괴되었다고 한다.

공격자는 다음의 공격자의 분류에 따른 규칙에 준수하여 오라클을 사용하여 게임을 수행한 뒤 $output$을 출력한다. 그러한 규칙에 따라서 공격자는 게임에서 승리할 수 도 있고 패배할 수도 있다. 주의 할 점은 이러한 게임의 승리 혹은 패배가 프로토콜의 프라이버시 보장 여부를 판단하는 잣대는 아니라는 점이다.

정의 2. 공격자의 분류

RFID의 프라이버시를 위협하는 공격자의 클래스는 다음 분류에 따라 나눌 수 있다

1) *Strong Adversary* : 모든 오라클을 자유롭게 사용할 수 있는 공격자.
2) *Destructive Adversary* : *Corrupt*(*vtag*) 오라클을 사용한 *vtag*는 절대 다시 사용할 수 없는 공격자.
3) *Forward Adversary* : *Corrupt* 오라클을 사용한 뒤에는 어떠한 오라클도 사용할 수 없는 공격자.
4) *Weak Adversary* : 태그에 대한 물리적인 공격, 즉 *Corrupt* 오라클을 사용할 수 없는 공격자.

정의 3. 프라이버시 게임 (Privacy Game)

RFID 시스템을 위협하는 공격자는 정의 1에 의해 정의된 9개의 오라클을 정의 2에 의해 분류된 4개의 클래스 규칙에 의거해 사용 함으로서 프라이버시 게임을 수행한다. 만약 해당 클래스의 특정 공격자가 다음 정의 4에 의해 무의미한 공격자(trivial adversary)라면 RFID 시스템은 해당 클래스의 프라이버시 공격에 대해 안전하다.

정의 4. 블라인더, 무의미한 공격자 (Blinder, Trivial Adversary)

블라인더 공격자 A^B는 게임을 수행할 시 A와 동일한 게임을 수행하면서도 *Launch*, *SendReader*, *SendTag*와 *Result* 오라클을 사용하지 못하는 공격자를 말한다. 즉, 이러한 공격자는 게임의 결과 값을 임의로 도출 해낼 수밖에 없다. $|\Pr[A\ wins] - \Pr[A^B\ wins]|$이 0에 가까운 매우 작은 값을 가진다면, 즉 공격자 A가 게임에서 승리할 확률과 공격자 A^B가 게임에서 승리할 확률이 동일하다면, 공격자 A의 프라이버시 게임은 아무 의미를 가질 수 없게 되므로 무의미한 공격자(trivial adversary)가 된다. 현재까지 제안된 대칭키 및 해시 연산 기반 RFID 프로토콜은 weak privacy를 넘어서는 즉, 태그에 대한 물리적 공격으로 인한 비밀정보의 유출에 대해서는 프라이버시를 보장하지 못하므로 본 논문에서는 프로토콜이 특정 weak adversary의 공격에 프라이버시를 보호할 수 있는지를 살펴본다. 즉, 해시연산 기반 RFID 프로토콜은 다양한 weak privacy 공격에 대해서는 항상 안전해야 한다.

III. 기존 RFID 인증 프로토콜의 취약점 분석

3.1. Lightweight and Resynchronous Mutual Authentication Protocol (LRMAP)

Ha 등이 제안한 LRMAP[7]는 다음 세션에서 태그가 보낼 메시지를 데이터베이스가 세션 시작 전에 미리 계산할 수 있음으로써 데이터베이스에서의 ID 검색 시간을 최소화 할 수 있고 태그와 리더간의 공유정보의 비동기가 발생 시에도 동기회복이 가능한 상호인증 프로토콜이다. 하지만, 이러한 비동기가 발생하면 동기회복을 위한 태그 검색시간이 비효율적으로 바뀐다. 데이터베이스가 n개의 태그정보를 보관하고 있다고 한다면, 정상 상태일 경우에는 태그 검색을 위해서는 해시 연산이 전혀 필요하지 않지만, 이전 세션에서 비정상 종료로 인한 비동기가 발생했을 경우 데이터베이스가 태그의 ID를 검색하기 위해서는 최대 $2n$번의 해시 연산을 필요로 한다. 프라이버시 측면에서 봤을 때도 다양한 프라이버시 공격 모델중 다음 특정 weak privacy 공격 모델에 약점을 가진다. 따라서 해시함수를 이용함으로써 획득할 수 있는 최대한의 프라이버시 레벨인 weak privacy를 만족하지 못한다.[9-10]

정리 1. (LRMAP: Weak-Privacy Attack). LRMAP는 다음 프라이버시 공격에 취약하여

DB	R	T
[*ID*][*HID*][*PID*]		[*ID*][*SYNC*]
Generate r		
	$Query, r$ ⟶	
		Generate t and Check $SYNC$. If ($SYNC=0$) then $P \leftarrow h(ID)$ else $P \leftarrow h(ID\|\|t)$ $Q \leftarrow h(ID\|\|t\|\|r)$, $SYNC \leftarrow 1$
	⟵ P, $L(Q)$, t	

If($P=HID$) $PID \rightarrow ID$
else if($P=h(ID\|\|t)$) $PID \rightarrow ID$
else if($P=h(PID\|\|t)$) $PID \rightarrow PID$
else halt
$Q' \leftarrow h(PID\|\|t\|\|r)$
If ($L(Q')=L(Q)$)
then $ID \leftarrow h(PID\|\|r)$, $HID=h(ID)$
		$SYNC=0$

	$R(Q)$ ⟶	
		If ($R(Q)=R(Q')$) then $ID \leftarrow h(ID\|\|r)$, $SYNC \leftarrow 0$

[그림 1] Lightweight and Resynchronous Mutual Authentication Protocol (LRMAP)

weak privacy를 만족하지 않는다.

증명) 공격자 A는 $\tau(vtag)=ID_x$이면 공격자가 승리하는 프라이버시 게임을 수행한다.

1: $CreateTag(ID_0)$, $CreateTag(ID_1)$
2: $DrawTag(ID_0) \rightarrow vtag_0$
3: pick random value r_E
4: $SendTag(vtag_0, Query, r_A) \rightarrow (P, L(Q))$
5: $Free(vtag_0)$
6: draw one tag at random and get $vtag$
7: $Launch \rightarrow \pi$
8: $SendReader(\pi) \rightarrow r$
9: $SendTag(vtag, r_R) \rightarrow (\overline{P}, L(\overline{Q}), \overline{t})$
10: replace current P with $\overline{P}$
11: $SendReader(\pi, P, L(\overline{Q}), \overline{t}) \rightarrow R(Q')$
12: $Result(\pi) \rightarrow x$
13: output whether $\tau(vtag)=ID_x$

공격자는 비밀정보 ID_0을 가지는 $vtag_0$을 선택 한다. 공격자는 난수 r_A를 생성해 태그에게 전송해 태그로부터 응답 메시지 $P=h(ID_0)$를 획득한다. 공격자는 획득한 P 값을 이용해 프라이버시 게임을 수행한다. 2개의 태그중 하나를 랜덤하게 선택하여 이를 $vtag$라 한다. 프로토콜을 시작하게 되면 공격자는 리더의 난수 r을 획득한 뒤 이 값을 그대로 $vtag$에게 전송해 응답메시지 $(\overline{P}, L(\overline{Q}), \overline{t})$을 획득한다. 공격자는 $\overline{P}$ 값 대신 공격자가 소유하고 있는 P 값을 $(L(\overline{Q}), \overline{t})$와 함께 리더에게 전송하여 리더 π에게 세션의 결과 값 x을 요청한다. 이 프라이버시 게임은 $\tau(vtag)$와 ID_x가 동일하면 승리하는 게임이다. 즉, $vtag$는 $vtag_1$ 또는 $vtag_0$이므로 나올 수 있는 경우는 두 가지이다.

먼저 $vtag=vtag_0$인 경우를 살펴본다. 이때 $\tau(vtag)=ID_0$이 된다. $P=h(ID_0)$, $L(Q)=L(h(ID_0\|r\|t))$이 리더에게 전송 되고 DB는 태그 인증을 수행한다. P 값과 동일한 HID값이 ID_0 비밀 값에 존재하여 DB는 태그의 신원을 ID_0으로 인식하게 된다. $L(\overline{Q})=L(h(ID_0\|r\|t))=L(Q)$이므로, 태그인증에 성공하게 되며 $output \neq \perp$ 이고 $x=1$이 된다. 따라서 $\tau(vtag) \neq ID_x$이다.

다음으로 $vtag=vtag_1$, 즉 $\tau(vtag)=ID_1$인 경우를 살펴본다. $P=h(ID_0)$, $L(\overline{Q})=L(h(ID_1\|r\|t))$이 리더에게 전송 되고 DB는 태그 인증을 수행한다. P 값과 동일한 HID값이 ID_0 비밀 정보 내에 존재하기 때문에 DB는 태그의 신원을 ID_0으로 인식하고 태그 인증을 시도 하지만 $L(\overline{Q})=L(h(ID_1\|r\|t)) \neq L(Q)$이므로 태그 인증에 실패하게 되어 $output=\perp$이고 $x=0$ 이 된다.

따라서 $\tau(vtag) \neq ID_x$이다.

프라이버시 게임의 수행 결과, 두 가지 경우 모두 $\tau(vtag) \neq ID_x$로서 공격자가 프라이버시 게임에서 지게 되므로 공격자 A가 프라이버시 게임에서 승리할 확률, $\Pr[A\ wins]=0$이 된다. $\Pr[A^B\ wins]=1/2$이므로 $|\Pr[A\ wins]-\Pr[A^B\ wins]|=1/2$이고 이는 무시할 수 없는 값이다. 그러므로 이러한 공격을 하는 weak adversary는 무의미한 공격자(trivial adversary)라 볼 수 없다. 따라서 LRMAP는 제안 공격에 대해서 프라이버시를 보장하지 못한다.

이러한 프라이버시게임은 비동기화 유도 공격을 통해 태그의 리더간의 비밀정보의 비동기화를 유도한 뒤 도청공격을 통해 획득한 메시지를 이용해 태그의 불구분성 위반 여부를 판단하는 게임이다. LRMAP는 태그 검색에 사용되는 메시지 P는 $SYNC$에 따라 다르게 생성되지만 태그인증을 위한 메시지 Q는 $SYNC$에 상관없이, 즉 비동기 발생 유무를 알 수 있는 값을 포함하지 않고 메시지를 생성한다. 따라서 태그 인증은 P가 정상상태 혹은 비동기 발생 후의 메시지인지의 구별 없이 이루어진다. 때문에 현재 세션의 메시지 P는 비동기 발생 후 다음 세션의 통신에 사용하더라도 정상적인 태그 인증이 이루어지게 된다. 공격자는 특정 태그의 메시지 P를 입수한 뒤 세션을 비정상 종료시켰다면 임의의 태그와 리더간의 통신상에서 P의 교체만으로도 이 태그가 특정태그와 동일 태그인지 아닌지를 판단할 수 있다. 이는 태그의 불구분성을 위반하는 공격이다.

3.2. Anonymous RFID Authentication supporting Constant-cost key-lookup (CARAP)

M. Bumester 등이 제안한 CARAP[7]는 태그 인증에 사용될 태그 메시지들을 태그와 데이터베이스에 미리 저장한 순환 카운터(cyclic counter)를 이용하여 생성함으로써 각 태그가 보낼 메시지를 데이터베이스가 세션 시작 전에 미리 계산하여 데이터베이스에서의 ID 검색 시간을 줄일 뿐만 아니라 태그와 리더간의 연속적인 비동기가 발생하더라도 빠른 태그검색 및 동기 회복을 보장한다. 하지만, 이러한 순환 카운터의 구현은 태그에 지나치게 많은 저장 공간이 필요함으로써 비현실적이다. 또한, 태그는 t개의 카운터 값을 가지고 이를 순환하여 사용하기 때문에 t번 이상의 연속적인 비동기가 발생할 경우 태그는 이전에 사용했던 카운터 값을 다시 사용하여 태그 인증 메시지를 생성하기 때문에 다음의 프라이버시 공격에 대해서 약점을 노출한다.

정리 2. (CARAP: Weak Privacy Attack). CARAP는 다음 프라이버시 공격에 취약하여 weak privacy를 만족하지 않는다.

증명) 공격자 A는 다음과 같은 weak privacy 공격을 시도한다.

1: $CreateTag(ID_0)$, $CreateTag(ID_1)$
2: $DrawTag(ID_0) \rightarrow vtag_0$
3: pick random value r_A
4: for $i=1$ to t do
5: $SendTag(vtag, r_A) \rightarrow (P, V_1)$
6: $P[i] \leftarrow P$
7: end for
8: $Free(vtag_0)$
9: draw one tag at random and get $vtag$
10: $SendTag(vtag, r_A) \rightarrow (\overline{P}, \overline{V_1})$
11: $x \leftarrow 0$
12: for $i=1$ to t do
13: if $\overline{P}=S[i]$ then
14: $x \leftarrow 1$
15: end for
16: output whether $\tau(vtag)=ID_x$

공격자는 프리태그 집합에서 ID_0 값을 가지는 $vtag_0$을 추출한다. 공격자는 랜덤값 r_A를 선택해 이를 $vtag_0$에게 전송하여 응답메시지 P, V_1을 수신한 뒤 P 값을 배열 P에 저장한다. 공격자는 이러한 과정을 t번 반복수행하여 t열의 배열 P를 획득한다. 공격자는 이 배열을 이용하여 프라이버시 게임을 수행한다.

2개의 태그중 하나를 랜덤하게 선택하여 이를 $vtag$라 한다. 태그는 r_A 값을 태그에게 보내 응답메시지 $\overline{P}$을 획득하게 된다. 공격자는 $\overline{P}$와 동일한 값이 P 배열 내에 존재하는지를 확인해 존재한다면 $x=1$이 되고, 그렇지 않다면 $x=0$이 된다. $\tau(vtag)$와 ID_x가 동일 하다면 공격자가 승리하는 프라이버시 게임이다.

먼저 $vtag_0$인 경우를 살펴본다. 이전 세션에서 $vtag_0$은 이미 t번의 연속적인 메시지 응답을 수행하여 t개의 카운터 값을 모두 소진 했으므로 이전에 사용했던 카운터중 하나를 선택해 응답메시지를 생성한다. 따라서 $\overline{P}$ 값은 P 배열 내의 값들 중 하나의 값과 동

DB	R	T
$[ID][K_N][K_P][q][Q_N^i][Q_P^i]$		$[ID][K][q][\text{mode}][ctr]$
Generate r		
	$Query, r$ →	
		if mode $=0$ then $P \leftarrow K$ else $P \leftarrow h(ID\|q\|ctr)$, update ctr $V_0\|V_1\|V_2 \leftarrow h(ID\|P\|r)$
	← $P,\ V_1$	
if $(P, ID) \notin D$ then $output \leftarrow \perp$ else $V_0'\|V_1'\|V_2' \leftarrow h(ID\|P\|r)$ if $(V_1' \neq V_1)$ then $output \leftarrow \perp$		
if$(P = K_N)$ then $K_P \leftarrow K_N$ and $K_N \leftarrow V_0'$ else if$(P = K_P)$ then $K_N \leftarrow V_0'$ else if$(P = Q_N^i)$ then $q \leftarrow V_0'$, $Q_P \leftarrow Q_N$, $Q_N^i \leftarrow h(ID\|q\|ctr(i))$ else if$(P = Q_P^i)$ then $q \leftarrow V_0'$, $Q_N^i \leftarrow h(ID\|q\|ctr(i))$ $output \leftarrow ID$	V_2' →	if $(V_2 \neq V_2')$ then if mode $=0$ then $K \leftarrow V_0$ else mode $\leftarrow 0$, $q \leftarrow V_0$ else mode $\leftarrow 1$

〔그림 2〕 Anonymous RFID Authentication supporting Constant-cost key-lookup (CARAP)

일하게 되므로 $x=1$이 된다. 따라서 $\tau(vtag) \neq ID_x$이다. 즉 공격자는 프라이버시 게임에서 패배한다.

$vtag$가 $vtag_1$인 경우에는 $vtag_1$의 응답메시지 $\overline{P}$은 공격자가 보유하고 있는 값과는 항상 다르므로 $x=0$이 된다. 따라서 $\tau(vtag) \neq ID_x$이다. 즉 공격자는 프라이버시 게임에서 지게 된다.

두 가지 경우 모두, 프라이버시 게임에서 공격자는 패배하여 $\Pr[A\ wins]=0$이 된다. $\Pr[A^B\ wins]=1/2$이므로 $|\Pr[A\ wins]-\Pr[A^B\ wins]|=1/2$이고 이는 무시할 수 없는 값이다. 그러므로 이러한 공격을 하는 weak-adversary는 무의미한 공격자(trivial adversary)라 볼 수 없다. 따라서 CARAP는 제안 공격에 대해서 프라이버시를 보장하지 못한다.

이러한 프라이버시 게임은 연속적인 메시지 전송 요청을 통해 태그의 순환카운터(cyclic counter)가 t개의 카운터 값을 모두 소비시키면서 응답메시지 P를 획득한 뒤 획득 메시지를 이용해 프로토콜이 태그의 불구분성을 위반하는지의 여부를 판단하는 게임이다. 이러한 CARAP의 약점은 순환카운터를 모두 업데이트 된 뒤의 태그 검색 및 인증 알고리즘이 고려되지 않아 이전에 사용되었던 카운터 값을 사용할 수 밖에 없기 때문에 발생한다. 공격자는 특정 태그에 연속적인 요청으로 응답 메시지 P를 t개 이상 입수 한 뒤 세션을 비정상 종료시켰다면 임의의 태그의 메시지 P와의 획득 메시지의 비교만으로도 임의 태그가 특정태그와 동일한지 아닌지를 판단할 수 있다. 이는 태그의 불구분성을 위반하는 공격인 셈이다.

IV. 제안하는 프로토콜

이 장에서는 2장에서 제시한 RFID 시스템의 여러 가지 요구조건을 바탕으로 연속적인 비동기 발생 시에도 향상된 프라이버시와 재동기화를 보장하는 프로토콜을 제안한다〔그림 3〕. 먼저 데이터베이스와 리더는 안전한 채널 상에서, 리더와 태그는 안전하지 않은 무선 채널 상에서 통신한다고 가정한다. 또한 리더와 태그는 해시연산 및 난수생성이 가능하여야 한다. 위와 같은 가정 아래 제안하는 프로토콜은 태그에 이전 세션들에서의 연속적인 비동기 발생 횟수(c)를 기록하는

간단한 카운터(simple counter)를 구현함으로 인해 이전 세션들에서 연속적인 비정상 종료가 발생할 시에도 데이터베이스에서 태그를 인식하는 시간이 LRMAP등의 기존의 상태를 기반으로 한 프로토콜보다 상대적으로 줄어들게 설계하였다. 또한, 제안 프로토콜은 심플 카운터가 업데이트 될 수 있는 한계점(threshold)을 설정하고 카운터가 한계점에 이르게 되면, 새로운 태그 검색 및 인증 알고리즘을 실행하여 CARAP에서 발생 할 수 있는 프라이버시 문제점을 개선하였다. 태그검색에 사용되는 메시지 P의 생성에 사용되는 비밀키 K, 카운터 c 그리고 태그 난수 t가 모두 리더 난수 r과 함께 태그인증메시지 Q의 해시 과정에 사용함으로서 LR-MAP의 프라이버시 약점을 해결하였다.

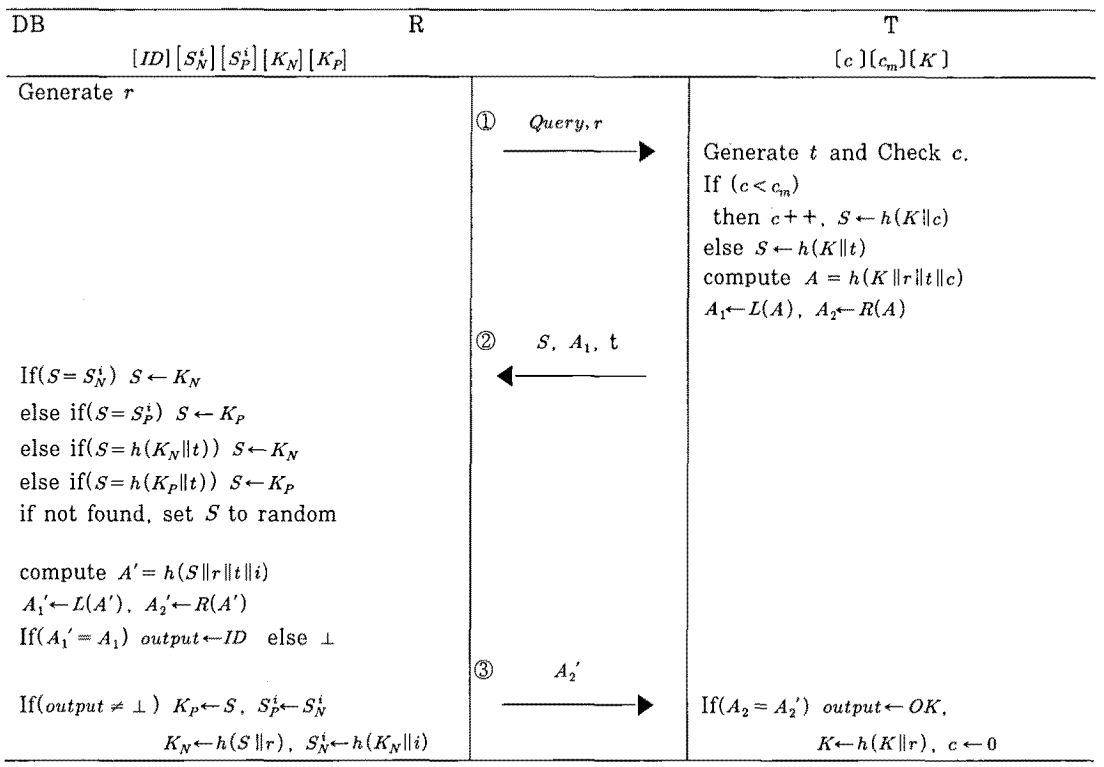
4.1. 용어정리

이 절에서는 여기서는 제안 기법에 사용하게 될 용어를 설명한다.

DB	: 백엔드 데이터베이스
R	: 리더
T	: 태그
r	: 리더가 생성한 난수
t	: 태그가 생성한 난수
c	: 태그와 리더간의 연속적인 비동기 횟수를 기록하는 카운터(simple counter)
c_m	: c가 업데이트 가능한 최대 한계점(Threshold)
$h()$	: 일 방향 해시 함수 $h: (0,1)^* \rightarrow (0,1)^l$
ID	: 태그의 고유식별정보
K_N	: 태그의 인증에 사용되는 비밀키,
K_P	: 이전 세션에서 태그의 인증을 위해 사용된 비밀키
S_N^i	: $S_N^i = h(K_N \| i)$, $i = 1, ..., c_m$
S_P^i	: $S_P^i = h(K_P \| i)$, $i = 1, ..., c_m$
$L()$, $R()$	: 메시지의 왼쪽(오른쪽) 절반
$\|\|$	: 연접

4.2. 프로토콜의 인증 절차

1. 리더는 태그에게 난수 r과 함께 질의를 보낸다.
2. 태그는 난수 t를 생성하고, c를 체크한다.
   - c가 c_m보다 작다면, c를 1 증가시킨 뒤 $A_1 = h(K \| r \| t \| c)$, $A_1 = L(A)$, $A_2 = R(A)$를 생성한다.
   - 그렇지 않다면, $S = h(K \| t)$, $A_1 = h(K \| r \| t \| c)$, $A_1 = L(A)$, $A_2 = R(A)$를 생성한다.
   - t, S, A_1을 리더에게 전송한다.
3. 리더는 태그로부터 받은 메시지를 자신의 난수 r과 함께 데이터베이스에게 전송한다.
4. 데이터베이스는 리더로부터 메시지를 전송받으면, 다음과 같은 5단계의 태그 검색과정을 거친다.
   i. 데이터베이스는 먼저 받은 S 값과 일치하는 값이 있는지를 S_N^i 테이블에서 검색한다. 같은 S_N^i를 찾았다면 S_N^i 포인터가 가리키는 K_N 값을 S에 저장하고 인증과정을 종료한다. 이 과정에서 태그 검색에 성공했다면 태그와 리더간의 비동기가 발생하지 않았거나, ① 또는 ② 메시지 전송 실패로 인한 비동기가 $(i-1)$번 발생했음을 의미한다.
   ii. 데이터베이스는 받은 S 값과 일치하는 값이 있는지를 S_P^i 테이블에서 검색한다. 같은 S_P^i를 찾았다면 S_P^i 포인터가 가리키는 K_P 값을 S 값에 저장하고 인증과정을 종료한다. 이 과정에서 태그 검색에 성공했다면 ③ 번 과정에서의 메시지 전송 실패를 포함한 $(i-1)$번의 비동기화가 발생했음을 의미한다.
   iii. 데이터베이스는 받은 S 값과 일치하는 값이 있는지를 해시함수를 이용하여 검색한다. K_N 값들과 전송받은 t 값을 이용해 $h(K_N \| t)$를 계산하여 S와 일치하는 값이 있는 지를 비교해 본다. 일치하는 $h(K_N \| t)$를 찾았다면 해당 K_N 을 S 에 저장하고 인증과정을 종료한다. 이 과정에서 태그 검색에 성공했다면 ① 또는 ② 과정에서의 메시지 전송 실패로 인한 비동기가 문턱치 값 c_m번 이상 발생했음을 의미한다.
   iv. 데이터베이스는 받은 S 값과 일치하는 값이 있는지를 해시함수를 이용하여 검색한다. K_P 값들과 전송받은 t 값을 이용해 $h(K_P \| t)$를 계산하여 S 와 일치하는 값이 있는 지를 비교해 본다. 일치하는 $h(K_P \| t)$를 찾았다면 해당 K_P을 S 에 저장하고 인증과정을 종료한다. 이 과정에서 태그 검색에 성공했다면 ③번 과정에서의 메시지 전송 실패를 포함한 c_m번 이상의 비동기화가 발생했음을 의미한다.
   v. 태그 검색에 실패했다면 S를 랜덤한 값으로



[그림 3] 제안하는 프로토콜

설정한다.

5. 태그검색이 끝난 데이터베이스는 다음과 같은 태그 인증과정을 수행한다.
   - 데이터베이스는 $A' = h(S \| r \| t \| i)$, $A_1' = L(A')$, $A_2' \leftarrow R(A')$을 계산하여, 전송받은 A_1과 A_1' 값이 일치하는지를 확인한다.
   - 만약 일치한다면 $output = ID$ 를 출력하고, 그렇지 않다면 $output = \perp$를 출력한다.
   - A_2'를 태그에게 전송한다.
6. 태그는 전달 받은 A_2'와 A_2가 일치한다면 $output = ok$를 출력하고 K 값을 $h(k \| r)$로 갱신한 뒤, 정상 종료되었다는 것을 저장하기위해 c를 0으로 초기화 한다.

V. 제안 프로토콜 분석

이 장에서는 앞서 소개된 여러 가지 RFID 요구조건을 바탕으로 제안 프로토콜의 보안성과 효율성에 대하여 분석 한다.

5.1. 공격 분석

5.1.1 도청 공격 (Eavesdropping Attack)

제안 프로토콜에서 공격자는 리더와 태그간의 메시지들을 도청할 수 있다. 하지만, 태그 소유자의 신원을 노출시킬 수 있는 정보인 태그 비밀키 K는 해시 함수를 이용해 암호화 과정을 거쳐 전송되기 때문에 공격자가 메시지를 도청하더라도 태그 소유자에 대한 정보를 얻어낼 수 없다. 따라서 제안 프로토콜은 도청공격에 안전하다.

5.1.2 태그 위장 공격 (Tag Spoofing Attack)

제안프로토콜에서 태그 인증에 사용 되는 메시지는 $S = h(K \| c)$ 또는 $h(K \| t)$, $A_1 = L(h(K \| r \| t \| c))$이다. 즉 공격자가 태그 위장 공격을 성공하기 위해서는 이전 세션들에서 획득한 이전 S, A_1 값을 기반으로 해당 세션에서 생성되는 정확한 S, A_1을 예측할 수 있어야 한다. 하지만 A_1은 항상 리더가 세션 내에서 생성한 난수 r과 결합되어 계산된다. 리더 난수 r은 항상 다

른 값을 가지기 때문에 공격자가 이전 세션들을 이용해 현재 세션에서의 A_1을 예측하는 것은 불가능하다. 또한, 현재 세션에서 사용되는 r, t를 획득한다 하더라도, 공격자는 태그 비밀키 K를 알 수 없기 때문에 A_1을 예측하는 것은 불가능하다. 따라서 제안 프로토콜은 태그 위장 공격에 안전하다.

5.1.3 리더 위장 공격 (Reader Spoofing Attack)

제안 프로토콜에서 리더 인증에 사용되는 메시지는 $A_2' = R(h(K\|r\|t\|c))$이다. 즉 공격자가 리더 위장 공격을 성공하기 위해서는 이전 세션들에서 획득한 이전 A_2' 값들을 기반으로 해당 세션에서 생성되는 정확한 A_2'을 예측할 수 있어야 한다. 하지만 A_2'은 항상 태그가 세션 내에서 생성한 난수 t과 결합되어 계산된다. 태그 난수 t은 항상 다른 값을 가지기 때문에 공격자가 이전 세션들을 이용해 현재 세션에서의 A_2'을 예측하는 것은 불가능하다. 또한, 현재 세션에서 사용되는 r, t, A_1을 획득한다고 하더라도, 공격자는 태그 비밀키 K를 알 수 없기 때문에 A_2을 예측하는 것은 불가능하다. 따라서 제안 프로토콜은 리더 위장 공격에 안전하다.

5.1.4 위치 추적 공격 (Location Tracking Attack)

제안 프로토콜은 $c < c_m$ 인 상태에서는 매번 c값이 갱신되므로 S와 A 값은 매 세션마다 다른 값을 가지게 된다. $c = c_m$인 상태에서는 c값은 더 이상 갱신되지 않으므로 태그 난수 t를 이용해 S와 A 값을 계산하며 이 값 역시 매 세션마다 다른 값을 가지게 된다. 따라서 제안 프로토콜은 불구분성을 가진다. 또한, 제안 프로토콜은 매 세션 마다 태그의 비밀 정보 K 값을 해시 이용해 갱신하기 때문에 공격자가 물리적인 공격을 통하여 K 값을 알아냈다고 하더라도 이전 세션에서 사용되었던 태그 비밀 정보 값을 알아내는 것은 불가능하다. 따라서 현재 태그 비밀 정보로 태그 소지자의 과거 이동 경로를 파악할 수 없으므로 제안 프로토콜은 전방향 안전성을 가진다. 그러므로 제안 프로토콜은 위치 추적 공격에 안전하다.

5.1.4 비동기화 유도 공격 (Desynchronization Attack)

제안 프로토콜에서 공격자는 ② 그리고 ③ 과정에서의 메시지 가로채기를 통해 프로토콜의 비동기화 유도 공격을 시도 할 수 있다. 먼저, 공격자가 ②번 과정에서의 연속적인 메시지 가로채기를 통한 연속적인 비동기화 유도 공격을 시도할 경우 태그의 c값이 c_m번까지 증가함으로 인해 비동기가 발생한다. 하지만, 제안 프로토콜은 이러한 비동기 발생을 대비해 데이터베이스에 c값에 따라 예상되는 S 값들을 S_N^i 테이블에 보관해 둠으로서 해당 태그는 다음 세션에서도 합법적인 리더로부터 인증을 받을 수 있으며 동기 회복이 가능하다. 또한, 공격자가 ③번 과정에서의 메시지 가로채기를 통한 비동기화 유도 공격을 시도할 경우 데이터베이스의 태그 비밀 정보는 새로운 값으로 갱신되지만, 태그는 갱신되지 않음으로 인해 비동기가 발생 한다. 하지만, 제안 프로토콜은 데이터베이스는 태그의 이전 비밀정보를 삭제하지 않고 S_P^i, K_P 에 보관해 둠으로서 해당 태그는 합법적인 리더로부터 인증을 받을 수 있으며 동기 회복이 가능하다. 따라서 제안 프로토콜은 비동기화 유도 공격에 안전하다.

5.2. 안전성 분석

이 절에서는 제안 프로토콜의 정확성, 보안성, 프라이버시를 정형적으로 측정함으로서 안전한 상호 인증(safe mutual authentication)과 개선된 프라이버시를 제공함을 보일 것이다.

5.2.1 태그 인증의 정확성 (Corretness of Tag Authentication)

데이터베이스는 항상 합법적인 태그인 경우에 태그를 인증하기 때문에 잘못된 부정은 불가능하다. 따라서 잘못된 긍정과 부정확한 확인이 발생 할 확률이 0에 가깝다면 태그 인증은 정확성을 가진다. 그러한 경우는 비밀키 K를 가지는 태그와 r과 t값이 주어졌을 때 데이터베이스내의 비밀키 $K' \neq K$임에도 $S = S'$이면서 $A_1 = A_1'$인 경우가 존재 하는 경우이다. n개의 합법적인 태그가 있다고 가정해보고 이를 실험태그에 추가한다. 우리는 n개의 태그를 생성하고 태그와 리더 간의 프로토콜을 시뮬레이션 한다고 가정할 때 이러한 부정확한 확인이 일어날 확률은 $2n(c_m+1)2^{-3t/2}$이고, 이러한 확률은 0에 가깝다.

5.2.2 리더 인증의 정확성 (Corretness of Tag Authentication)

리더 인증 역시 태그 인증과 동일하다. 태그 역시

항상 합법적인 리더인 경우에 태그를 인증하기 때문에 잘못된 부정은 불가능하다. 그리고 잘못된 긍정과 부정확한 확인이 발생할 경우는 $K \neq K'$임에도 $R(h(K\|r\|t\|c)) = R(h(K'\|r\|t\|c))$인 경우가 존재 할 때이다. 따라서 부정확한 확인이 일어날 확률은 $2^{-\ell/2}$이고, 이러한 확률은 0에 가깝다.

5.2.3 태그 인증의 안전성 (Security of Tag Authentication)

공격자 A는 한 개의 태그 S를 선택한다. 그리고 p 시각에 $SendReader(\pi) \rightarrow r$와 $SendReader(\pi,(S,A_1,t))$를 차례대로 호출한다. 추가로 A는 $SendTag(ID,r_i) \rightarrow (S_i,A_1^i,t_i)$를 p_i시각에 호출한다. 만약 모든 i에 대해서 $p < p_i$라면 $(r_i,t_i,S_i,A_1^i) \neq (r,t,S,A_1)$일 때 A가 승리할 경우는 $S=h(K\|c)$ 또는 $h(K\|t)$를 만족하면서 동시에 $A_1 = L(h(K\|r\|t\|c))$인 경우이다. $(r_i,t_i) \neq (r,t)$이므로, A가 승리할 확률은 $2(c_m+1)2^{-3\ell/2}$가 되어 0에 가깝다. $p > p_i$인 경우에 A가 승리할 확률은 $\Pr[r_i = r]$인 경우와 같고 이러한 경우가 발생할 확률은 0에 가깝다. 따라서 제안 프로토콜은 안전한 태그 인증을 제공한다.

5.2.4 리더 인증의 안전성 (Security of Reader Authentication)

공격자 A는 한 개의 리더 R을 선택한다. 그리고 p 시각에 $SendTag(T,r) \rightarrow (S,A_1,t)$와 $SendTag(T,A_2')$를 차례로 호출한다. A_2'가 정확하다면 태그는 자신의 비밀키를 업데이트하고 A는 승리한 것이다. 추가적으로 A는 $Execute(vtag) \rightarrow (\pi, transcript)$를 p_i 시각에 호출한다. (단, 마지막 메시지 A_2'가 태그에게 전송되기 전에 프로토콜을 멈춘다.) 만약 $p < p_i$라면 A가 이길 경우는 $A_2' = R(h(K\|r\|t\|c))$인 경우이다. 따라서 A가 승리할 확률 $\Pr[A_2' = R(h(K\|r\|t\|c))] = 2^{-\ell/2}$로서 0에 가까운 확률이다. $p > p_i$인 경우에 A가 승리할 확률 $\Pr[t_i = t] = 2^{-\ell}$ 로서 이는 0에 가깝다.

5.2.5 프라이버시 (Privacy)

지금부터 제안 프로토콜이 LRMAP 와 CARAP에서 사용된 프라이버시 공격에 안전함을 증명한다. 먼저, 정리 1과 동일한 방법으로 제안프로토콜에 프라이버시 게임을 수행한다. 공격자는 동일한 방식으로 $S=h(K_0\|0)$을 획득하여 이 값을 다음 세션의 $\overline{S}$ 값과 바꿔치기 한 뒤 리더에게 전송해 결과를 관찰한다. $vtag$는 $vtag_0$ 또는 $vtag_1$이 될 수 있다.

먼저 $vtag = vtag_0$인 경우를 살펴본다. 즉, $\tau(vtag) = ID_0$이다. $S=h(K_0\|0)$, $\overline{A_1} = L(h(K_0\|r\|t\|1))$ 그리고 $\overline{t}$가 리더에게 전송되면 DB는 태그인증을 수행한다. ID_0테이블 내의 S_N^0이 S와 같은 값을 가지므로 $\overline{A_1}' = L(h(K_0\|r\|t\|0))$이고 이는 $\overline{A_1}$과 다르므로 $output = \perp$이고 $x=0$이 된다. 즉, $\tau(vtag) = ID_x = ID_0$이다. 결국, 공격자는 프라이버시 게임에서 승리한다.

다음으로 $vtag = vtag_1$인 경우를 살펴보자. $S=h(K_0\|0)$, $\overline{A_1} = L(h(K_1\|r\|t\|0))$ 그리고 $\overline{t}$가 리더에게 전송되면 서버는 태그인증을 수행한다. ID_0 테이블 내의 S_N^0 이 S와 같은 값을 가지므로 $S=K_N=K_0$이고 $i=0$이다. DB는 ID_0으로 태그를 인식하므로 $\overline{A_1}' = L(h(K_0\|r\|t\|0))$이고 이는 $\overline{A_1}$과 다르므로 태그인증에 실패하게 된다. 따라서 $output = \perp$이고 $x=0$이 되므로 $\tau(vtag) = ID_1 \neq ID_x = ID_0$이다. 결국, 공격자는 프라이버시 게임에서 패배한다.

그러므로 프라이버시 게임의 수행 결과를 종합하면 공격자가 프라이버시 게임에서 승리할 확률, $\Pr[A\ wins] = 1/2$이다. $\Pr[A^B\ wins] = 1/2$이므로 $|\Pr[A\ wins] - \Pr[A^B\ wins]| = 0$이다. 즉, 이러한 공격을 시도하는 weak adversary는 무의미한 공격자이다. 따라서 제안 프로토콜은 [그림 3]의 공격에 안전하다.

두 번째로, 제안 프로토콜이 CARAP에서 사용된 프라이버시 공격에 안전함을 증명한다. 정리 2와 동일한 방법으로 제안 프로토콜에 프라이버시 게임을 수행한다. 공격자는 $S=h(K_0\|c)$를 배열 S에 저장하는 과정을 c_m번 반복 수행하여 c_m열의 배열 S를 획득하여 다음 세션에서의 응답메시지 $\overline{S}$와 비교한다. $vtag = vtag_0$ 인 경우에는 이전의 세션에서 $vtag_0$은 의 c_m번의 연속적인 메시지 응답을 수행하였기 때문에 $\overline{S}=h(K_0\|t)$이 된다. $\overline{S}$와 같은 값은 S 배열 내에 존재하지 않기 때문에 $x=0$ 이 되고 $\tau(vtag) = ID_x = ID_0$이다. 따라서 공격자는 프라이버시 게임에서 승리한다.

$vtag = vtag_1$인 경우는 응답 메시지 $\overline{S}=h(K_1\|0)$이므로 공격자가 소유하고 있는 배열 S의 값들과는 항상 다른 값을 가지게 된다. 따라서 $x=0$ 이 되고

$\tau(vtag) \neq ID_x$이다. 결국 공격자는 프라이버시게임에서 패배한다.

두 가지 경우의 프라이버시 게임의 수행 결과를 종합하면 공격자가 프라이버시 게임에서 승리할 확률 $\Pr[A\ wins]=1/2$이다. $\Pr[A^B\ wins]=1/2$이므로 $|\Pr[A\ wins]-\Pr[A^B\ wins]|=1/2$이다. 즉, 이러한 공격을 시도하는 weak adversary는 무의미한 공격자이다. 따라서 제안 프로토콜은 [그림 3]의 공격에 안전하다.

5.3 효율성 분석

기존 프로토콜과 제안 프로토콜을 효율성 면에서 비교하면 [표 1]과 같다. 비교요소는 태그와 데이터베이스 내에 요구되는 저장공간 및 최대 해시연산 횟수 등이다. 먼저 태그 및 데이터베이스에 필요한 메모리에 관해 살펴본다. 태그는 저가구현을 위해 연산 및 저장공간이 제한적이기 때문에 최소한의 태그 저장공간과 연산량만 필요로 하게 설계되는 것이 바람직하다. 반면, DB는 태그에 비해 훨씬 고용량의 저장공간과 빠른 연산능력을 가지므로 태그에 비해 구현의 제약이 훨씬 적다.

효율적인 비교를 위해 태그와 DB내의 비밀정보는 모두 ℓ 비트로 구성된다고 가정한다면, LRMAP는 2ℓ 비트, CARAP는 $(c_m+4)\ell$ 비트의 태그 저장공간을 필요로 한다. CARAP는 연속비동기공격에도 빠른 태그인식을 위해 c_m번 까지 업데이트 되는 순환카운터가 태그 내에 저장되기 때문에 c_m 값의 설정에 따라 LRMAP에 비해 최악의 경우 수배~수십 배나 많은 저장공간을 필요로 한다. 이에 반해, 제안 프로토콜은 LRMAP에 비해 ℓ비트의 저장공간이 늘어났지만 CARAP에 비해서는 대폭 줄어든 수치이다. 즉, 태그 메모리는 c_m값에 상관없이 일정한 값을 가지므로 태그의 저가구현에 문제가 없다.

다음으로 프로토콜에서 요구하는 총 해시 연산량을 살펴본다. 태그는 LRMAP, CARAP 와 제안프로토콜이 모두 2~3회 정도의 해시 연산량을 필요로 함으로서 거의 차이가 없다. 반면, DB에서의 총 해시 연산량은 LRMAP는 평상시에는 3번의 해시연산이 필요하지만 비동기가 발생한 경우 동기회복 및 재동기화를 위해서는 $2n$번의 추가 해시를 필요로 한다. 즉, 비동기가 발생하면 해시 연산 횟수가 급격하게 늘어나 비효율적이다. CARAP은 비동기여부에 상관없이 최대 (c_m+1)번의 해시연산만을 요구하여 효율적인 알고리즘으로 보이지만 이는 연속적인 비동기 상황에서의 프라이버시 문제를 고려하지 않았기 때문에 이러한 결과가 나왔다고 볼 수 있다.

제안 프로토콜은 이전의 통신이 비정상적으로 종료되어 비동기가 발생한 경우에도 정상 상태 일 때와 같이 최대 (c_m+2)번만의 해시 연산만을 필요로 할뿐만 아니라, c_m번의 연속적인 비동기까지도 정상 상태 일 때와 다름없는 프로토콜이다. c_m번을 넘어서는 연속적인 비동기가 발생할 경우에는 제안프로토콜은 프라이버시를 보호하기 위해 $2n$번의 추가 해쉬 연산으로 등록된 모든 태그정보에 대한 전수 조사를 통해 태그를 인증하여 동기를 회복한다.

두 번째로 살펴볼 부분은 태그인증의 효율성에 관한 부분이다. 효율적인 상호인증 프로토콜을 위해서는 태그를 인식하여 태그의 신원을 확인하고 리더인증을 위한 메시지를 생성하여 태그에게 전송하는 시간이 짧아야 빠른 인증이 가능하다. 특히, DB정보의 업데이트는 프로토콜이 종료된 후 처리가 가능하기 때문에

[표 1] 효율성 분석

(n : DB의 ID 개수, $n \gg \ell \gg c_m$)

		LRMAP	CARAP	제안 프로토콜
DB 저장량(비트)		$3\ell \cdot n$	$2\ell(c_m+1)\cdot n$	$2\ell(c_m+1)\cdot n$
TAG 저장량(비트)		2ℓ	$(c_m+4)\ell$	3ℓ
TAG 해시 연산		3	2	3
DB 해시 횟수 (최대)	평상시	3	c_m+1	c_m+2
	c_m이내 연속 비동기	$2n+3$	c_m+1	c_m+2
	c_m이상 연속 비동기	$2n+3$	c_m+1	$2n+c_m+2$
ID 검색을 위해 사용되는 해시 횟수 (최대)	평상시	0	0	0
	c_m이내 연속 비동기	$2n$	0	0
	c_m이상 연속 비동기	$2n$	0	$2n$

세션내의 연산에서 제외한다면 여기서는 순수 ID검색에 소요되는 연산량을 비교하는 것도 효율성의 잣대가 될 수 있다.

LRMAP는 정상상태에서는 ID검색을 위해 해시연산이 전혀 필요치 않지만, 비동기 상황에서는 $2n$번의 해시연산을 필요로 함으로서 비효율적이다. CARAP는 ID검색을 위해서는 해시가 전혀 요구되지 않는다. 그러나 이 역시 프라이버시의 문제점을 무시한 알고리즘이었기 때문에 가능한 결과일 뿐이다. 제안 프로토콜은 빠른 태그검색을 위해 연속적인 c_m번의 비동기까지 태그 인증에 사용될 수 있는 태그 메시지가 DB에 미리 계산되어 저장되어 있다. 따라서 제안 프로토콜은 비동기가 발생할 경우에도 해시 함수를 쓰지 않고 데이터베이스에 미리 계산해 둔 값을 태그 검색에 이용하므로 태그 검색시간이 비약적으로 줄어든다. 뿐만 아니라, 악의적인 침입자의 불법 블로킹이나, 통신 환경으로 인한 메시지 유실 등으로 인한 연속적인 비동기가 발생한 경우에도 제안 프로토콜은 c_m번의 연속적인 비동기까지는 빠른 태그 검색을 제공한다. c_m번 이상의 연속적인 비동기가 발생 했을 경우에는 $2n$번의 해시연산을 통해 프라이버시를 보호하면서 태그를 인식한다.

VI. 결 론

본 논문에서는 기존 해시 기반 RFID 시스템의 보안 및 태그 검색 과정에서의 문제점을 알아보고, 그러한 문제점들을 해결 할 수 있는 프로토콜을 제안하였다. 먼저 Vaudenay가 제안한 프라이버시 게임 모델을 사용하여 LRMAP와 CARAP 프로토콜의 프라이버시를 측정하였다. 이러한 프라이버시 게임의 수행결과 LRMAP 과 CARAP 모두 프라이버시에 문제가 있음이 밝혀졌다. 제안 프로토콜은 LRMAP의 프라이버시의 약점을 해결하기 위해 태그 검색에 사용되는 카운터(c) 역시 태그인증에 사용되도록 설계하였다. 또한 CARAP의 프라이버시 약점을 해결 하기 위해 카운터가 한계점에 도달 하게 되면, 새로운 태그 검색 및 인증 알고리즘이 실행 되도록 설계하였다.

프라이버시를 침해하지 않는 범위 내에서 제안 프로토콜은 태그의 저가구현과 태그 검색 및 인증이 효율적으로 실행될 수 있도록 설계하였다. LRMAP가 태그와 리더간의 비동기가 발생하면 태그검색시간이 정상 상태일 때보다 비약적으로 늘어나는 단점을 해결하기 위해 데이터베이스가 해시 연산 없이 태그 검색이 가능한 연속 비동기 횟수의 한계점(c_m)을 설정해 놓아서, 한계점을 넘어서지 않는 연속적인 프로토콜의 비정상 종료가 발생할 시에는 정상상태와 같이 빠른 태그 검색이 가능할 수 있게 설계하였다.

제안프로토콜은 CARAP 프로토콜의 순환 카운터보다 구현하기 쉽고 태그에 많은 저장공간이 필요치 않는 간단한 카운터를 적용함으로써 비교적 적은 태그 저장 공간을 필요로 한다. 또한, 태그의 카운터가 CARAP처럼 공격자의 연속공격에 의해 무한 업데이트 되는 것을 방지하기 위해 c_m을 넘어서는 연속적인 비동기가 발생 할 경우에는 LRMAP와 같이 해시연산을 통한 전수조사를 통해서, 태그와 리더의 태그 검색 및 동기회복이 가능하게 하였다.

즉 이러한 비동기 한계점(c_m)을 얼마로 설정하는 것이 프로토콜의 효율성을 결정하는 중요한 잣대가 된다. 이론적으로는 이러한 한계점을 최대한 크게 잡는 것이 가장 이상적이지만 현실적으로 이 값이 커질수록 데이터베이스는 더욱 많은 저장공간을 필요로 한다. 따라서 데이터베이스의 성능과 통신 환경 등을 고려하여 적당한 한계점 값을 설정해야 한다. 만약 비동기가 거의 발생하지 않거나 데이터베이스의 용량이 크지 않다면, 이 값을 작게 잡는 것이 좋다. 극단적으로 한계점을 1로 설정한다면 제안 프로토콜은 기존의 LRMAP 등과 같은 프로토콜과 거의 같은 성능을 가지게 된다. 반대로 악의적인 침입자의 메시지 블로킹이나 통신 메시지 유실 등으로 인한 비동기가 자주 발생하고, 데이터베이스의 용량이 충분히 크다면, 한계점을 여유 있게 잡는 것도 좋은 방법이다. 이러한 경우, 제안 프로토콜은 CARAP와 같이 연속적인 비동기 발생에도 빠른 태그 검색을 제공함으로써 효율적이다. 반대로, 서버의 성능이나 통신 환경에 대한 고려 없이 비동기 한계점을 설정한다면 프로토콜의 효율성은 장담 할 수 없다. 즉, 태그의 생산 전에 태그가 활용될 시스템의 환경을 고려하여 최적의 비동기 한계점을 도출하는 과정이 선행되어야 할 것이다.

참 고 문 헌

[1] 여준호, 최신 RFID 기술, 홍릉과학출판사, 2008년 8월.

[2] 이용한, 김지영, 정지훈, "무선인식 (RFID) 개인정보보호에 관한 국내외 동향 조사연구," 한국유통물류진흥원, 2006년 6월.

[3] 남상엽, 김근은, 강이철, 박정석, RFID 구현 및

응용, 도서출판 상학당, 2008년 6월.

[4] K. Finkenzeller, RFID Handbook: Fundamentals and Application s in Contactless Smart Cards and Identification, WILEY, May 2003.

[5] S. Garfinkel and B. Rosenberg, RFID : applications, security and privacy, Addison-Wesley, July 2005.

[6] S.A. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," Security In Pervasive Computing 2003, LNCS 2802, pp. 201-212, 2004.

[7] J.C. Ha, J.H. Ha, S.J. Moon, and C. Boyd, "LRMAP: Light weight and Resynchronous Mutual Authentication Protocol for RFID System," Ubiquitous Convergence Technology, LNCS 4412, pp. 80-89, 2007.

[8] M. Bunmester, B. de Medeiros, and R. Motta, "Anonymous RFID authentication supporting constant-cost key lookup against active adversaries," Int. J. Applied Cryptography, vol. 1, no. 2, pp. 79-90, Nov. 2008.

[9] S. Vaudenay, "On privacy models for RFID," Advances in cryptology, ASIACRYPT 2007, LNCS 4833, pp. 68-87, 2007.

[10] S. Vaudenay, "Mutual Authentication in RFID: Security and Privacy," ACM Symposium on Information, Computer and Communications Security (ASIACCS'08), ACM Press, pp. 292-299, Mar. 2008.

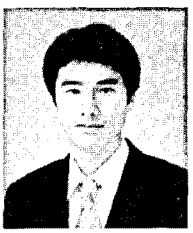
[11] V. Shoup, "Sequences of Gam es: A Tool for Taming Complexity In Security Proofs," IACR ePrint 2004-332, Jan. 2006.

[12] G. Avoine and P. Oechslin, "A Scalable and. Provably Secure Hash-based RFID Protocol," IEEE PerSec 2005, pp. 110-114, Mar. 2005.

[13] D. Henrici and P. Muller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers," Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops. PERCOMW'04, pp. 149-153, Mar. 2004.

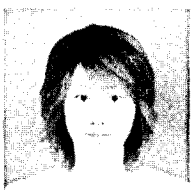
[14] S.M. Lee, Y.J. Hwang, D.H. Lee, and J.I. Lim, "Efficient Authentication for Low-Cost RFID Systems," ICCSA 2005, LNCS 3480, pp. 619-627, 2005.

〈著者紹介〉



김 영 재 (Young-Jae Kim) 학생회원
2008년 2월 : 경북대학교 전자전기컴퓨터학부 학사
2008년 3월~현재 : 경북대학교 정보보호학과 석사과정
〈관심분야〉 RFID/USN, 정보보호

전 동 호 (Dong-Ho Jeon) 정회원
2000년 2월 : 밀양대학교 컴퓨터공학과 학사
2002년 2월 : 경북대학교 정보통신학과 석사
2002년 3월~현재 : 경북대학교 정보보호학과 박사과정
〈관심분야〉 RFID/USN, 네트워크 보안, 정보보호



권 혜 진 (Hye-Jin Kwon) 학생회원
2007년 2월 : 경북대학교 수학과 학사
2009년 2월 : 경북대학교 정보보호학과 석사
2009년 3월~현재 : 경북대학교 전자공학과 박사과정
〈관심분야〉 RFID/USN, 인증 및 암호기술, 정보보호

김 순 자 (Soon-Ja Kim) 종신회원
1975년 2월 : 경북대학교 수학 교육학과 학사
1977년 2월 : 경북대학교 수학과 석사
1988년 2월 : 계명대학교 수학과 박사
1993년 4월~현재 : 경북대학교 전자·전기 공학부 교수
〈관심분야〉 정보보호 및 보안기술, 정보보호 응용기술