情報保護學會論文誌
第20卷 第2號, 2010. 4

온라인 서버가 없는 환경에서 이동형 리더의 프라이버시를 보호하는 안전한 RFID 검색 프로토콜*

임 지 환,[1†] 오 희 국,[1] 김 상 진[2‡]
[1]한양대학교, [2]한국기술교육대학교

A Secure RFID Search Protocol Protecting Mobile Reader's Privacy Without On-line Server*

Jihwan Lim,[1†] Heekuck Oh,[1] Sangjin Kim[2‡]
[1]Hanyang University, [2]Korea University of Technology and Education

요 약

최근 Tan 등은 인증 서버와 연결 없이 태그 인증 목록을 가진 이동형 리더가 스스로 태그를 인증할 수 있는 서버없는 RFID 검색 프로토콜을 소개하였다. 서버없는 RFID 시스템은 기존 온라인 서버 모델과 달리 리더의 이동성 및 개인성을 고려해야하기 때문에 태그 뿐 아니라 리더의 프라이버시 보호가 필요하다. 본 논문에서는 서버없는 RFID 검색 시스템을 위한 새로운 보안 요구사항을 정의하고 이를 만족하는 안전한 RFID 검색 시스템을 제안한다. 제안하는 검색 프로토콜은 리더에 저장된 태그의 인증 정보를 매 세션마다 갱신하여 리더의 후방향 위치추적 안전성을 보장하며 검색 프로토콜의 취약점인 재전송 공격을 막기 위해 암호화된 타임스탬프를 사용하였다. 또한 본 논문에서는 서버 없는 RFID 검색 시스템의 분석을 위한 새로운 공격자 모델을 정의하고 이를 이용하여 시스템의 안전성을 증명한다.

ABSTRACT

Recently, Tan et al. introduced a serverless search protocol in which a mobile reader maintains a tag authentication list and authenticates a tag using the list without connecting authentication server. A serverless RFID system is different from general RFID systems which use on-line server models. In the serverless RFID system, since the mobility of a personalized reader must be considered, we have to protect not only the privacy of a tag but also the privacy of a mobile reader. In this paper, we define new security requirements for serverless RFID search system and propose a secure serverless RFID search system. In our system, since tag authentication information maintained by a reader is updated in every session, we can provide the backward untraceability of a mobile reader. Also we use an encrypted timestamp to block a replay attack which is major weakness of search protocols. In addition, we define a new adversary model to analyze a serverless RFID search system and prove the security of our proposed system using the model.

Keywords: Mobile RFID, Serverless RFID Search System, Reader Privacy

접수일(2009년 10월 20일), 게재확정일(2010년 2월 3일)
* 본 연구는 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임. (No. 2009-0080351)
* 이 논문은 2009년도 한국기술교육대학교 교수교육연구진흥비 지원에 의하여 연구되었음.
† 주저자, jihwan.lim@gmail.com
‡ 교신저자, sangjin@kut.ac.kr

I. 서 론

최근 이동형 사용자 단말과 RFID 시스템이 결합한 모바일 RFID 시스템에 관한 연구가 관심을 받고 있다. 모바일 RFID 기술은 RFID 기술을 모바일 단말기 및 무선 인터넷과 접목함으로써, 사용자에게 새로운 부가 서비스를 제공하는 제반 기술이다. 사용자는 RFID 리더칩이 내장된 이동형 휴대 단말을 이용하여 물품 또는 위치에 부착된 태그를 읽고, 태그의 정보를 검색하여 활용할 수 있다. 기존 온라인 서버와 연결된 RFID 환경과 모바일 RFID 환경의 핵심적인 차이점은 리더의 이동성을 고려해야 한다는 점과 인증 서버와 연결 없이 리더 스스로 태그를 인증할 수 있는 환경을 고려해야 한다는 점이다.

• 리더의 프라이버시 노출

모바일 RFID 환경에서 모바일 리더는 더 이상 RFID 시스템의 말단 단말로만 구성되는 것이 아니라 사용자의 개인 이동 단말을 포함하게 된다. 따라서 기존 RFID 시스템에서 리더의 프라이버시를 고려할 필요가 없었던 반면 모바일 RFID 시스템에서는 태그를 소유한 사용자의 프라이버시 뿐 아니라 이동형 리더를 소유한 사용자의 프라이버시가 보호되어야 한다는 것을 의미한다. 만약 리더가 태그를 인증하기 위해 전송하는 질의 메시지에 리더를 식별할 수 있는 정보가 포함되면 이를 확보할 수 있는 공격자는 리더의 위치를 알 수 있다. 특히 리더 신호의 세기는 태그 신호의 세기보다 상대적으로 매우 강하기 때문에 도청에 의한 리더의 위치 프라이버시 노출에 더욱 취약하다.

• 리더 자체 인증 환경

모바일 RFID 시스템에서도 기존 RFID 시스템에서의 온라인 서버 모델을 사용할 수 있다. 즉 리더가 태그를 식별하기 위해서 백엔드 시스템에 접속하여 태그의 질의를 인증 받아 태그를 식별할 수 있다. 하지만 모든 모바일 리더의 온라인 서버까지의 연결이 항상 보장되는 것은 아니며 모바일 리더가 활용될 수 있는 다양한 응용 서비스와 가용성을 고려할 때 태그의 인증 정보를 리더에게 위임할 수 있는 환경에 대한 고려가 필요하다.

최근 Tan [1]등은 이러한 모바일 RFID 환경에 적합한 인증 서버 없는 RFID 검색 프로토콜을 제안하였다. RFID 검색 프로토콜은 모바일 RFID환경에서 더욱 효과적으로 활용될 수 있는 새로운 RFID 응용 모델로서 인증 프로토콜과의 차이점은 리더의 질의 메시지에 있다. 인증 프로토콜이 리더 주변에 존재하는 태그를 인식하기 위해 불특정 다수의 태그를 대상으로 질의를 전송하고 질의에 대한 태그의 응답을 받아 주변 태그를 인증하는 반면, 검색 프로토콜에서 리더는 특정 태그를 대상으로 하는 검색 질의 메시지를 전송하고 해당 태그의 응답을 수신하여 태그의 존재 유무를 판단한다. 즉 인증 프로토콜이 리더 주변에 있는 모든 태그를 인식하는 것이 목적이라면 검색 프로토콜은 특정 태그가 리더 주변에 있는지 유무를 판단하는 것이 목적이다.

II. 시스템 정의 및 보안 요구사항

2.1 정의

RFID 시스템은 태그, 리더, 백엔드 서버 시스템(back-end server system)의 3가지 구성요소를 가진다. RFID 시스템에서 태그는 유일한 식별자를 가진 수동 응답기(passive transponder)다. 일반적으로 저가형 태그는 배터리가 없어 제한적인 계산 능력과 메모리 공간을 가진 것으로 간주되며 생산가격 측면에서 변형 억제(tamper resistant) 기능을 구현할 수 없다고 가정한다. 하지만 최근 저가형 태그에 적합한 암호 알고리즘에 대한 연구가 활발하게 진행되고 있으며 A. Bogdanov[2]등은 저가형 태그를 위한 보안 프리미티브의 요구사항(2000 게이트 이하, $10\mu W$ 이하의 전력 소모, 10,000 clock cycle / operation)[3]을 만족하는 암호학적 해쉬 함수의 구현이 가능하다는 연구 결과를 발표하였고 M. Feldhofer[4]등은 AES(Advanced Encryption Standard) 역시 저가형 태그에 구현가능하다는 연구 결과를 발표하였다.

리더는 백엔드 서버 시스템에 등록된 유효한 태그를 인식하기 위해 질의를 전송하고 응답을 수신하는 송수신기(transceiver) 역할을 수행한다. 일반적인 RFID 시스템에서 리더는 RFID 시스템의 말단 장비로서 백엔드 서버 시스템 또는 클라이언트 응용 시스템과 안전한 통신 채널이 유지하고 있는 것으로 간주한다. 하지만 모바일 RFID 환경에서 리더는 태그와 마찬가지로 유일한 식별자를 가지고 백엔드 서버 시스템에 등록되어 사용되는 이동성을 가진 사용자 단말로 간주한다. 이 리더를 이동형 리더라고 부르며 환경에 따라 시스템으로부터 발급받은 태그 인증 정보를 이용하여 시스템과 연결없이 스스로 태그를 인증하고 인식할 수 있다.

일반적으로 백엔드 서버 시스템은 단일 데이터베이스 또는 동기화된 데이터베이스 군과 안전한 통신 채널을 형성하고 있는 클라이언트 응용 시스템(client application system)을 포함한다. 백엔드 서버 시스템은 데이터베이스에 유효한 태그와 리더 목록 및 공유 비밀 정보를 유지 관리한다. 모바일 리더 환경에서는 이동형 리더에게 인증 가능한 태그 목록 및 태그 인증정보를 발급한다.

정의 1. (RFID 인증 시스템) RFID 인증 시스템은 다음과 같이 구성된다.

- 태그 집합 $T=\{t_1,t_2,...,t_n\}$: 백엔드 서버 시스템에 등록된 태그 집합
- 리더 집합 $R=\{r_1,r_2,...r_l\}$: 백엔드 서버 시스템과 안전한 통신 채널을 유지하고 있는 리더 집합. 일반적인 RFID 인증 시스템에서 리더는 단일 데이터베이스 또는 동기화된 데이터베이스 군으로부터 정보를 수신하여 전달하는 역할을 수행하기 때문에 다수의 리더를 구분할 필요가 없다.
- 백엔드 서버 시스템 *BS*: 등록된 태그 집합을 유지관리하고 인증을 수행하는 주체
- 알고리즘 SetupTag(*ID*,*K*): *BS*가 실행하는 알고리즘으로서 태그의 메모리에 비밀정보 *K*를 저장하고 *BS*의 데이터베이스에 $<ID_i,K_i>$를 저장한다. ID_i는 EPC(Electronic Product Code)와 같은 태그 t_i의 고유 식별자를 의미하고 K_i는 태그의 비밀 정보로서 다수의 비밀정보 $\{k_1,k_2,...\}$로 구성될 수 있다.
- *T*-*BS*간의 인증 프로토콜 *AP*: 리더 *R*을 전달자로 이용하는 *BS*와 태그간에 수행되는 다항시간 대화형 프로토콜로서 *R*이 프로토콜을 개시한다. *R*은 자신 주변에 있는 태그에게 질의문 *Query*를 생성하여 전송하고 *Query*에 대한 태그의 응답 *Resp*을 수신하여 *BS*를 통해 응답한 모든 태그를 인증한다. *BS*에 등록된 태그 t_i의 식별자가 ID_i이고 비밀정보가 K_i일 때, *AP*는 t_i가 K_i를 이용하여 *Query*에 상응하는 합법적인 *Resp*를 생성하여 전송하면 ID_i를 *BS*에게 출력하면서 종료하며 그렇지 않은 경우 $\perp$를 출력하면서 종료한다.

정의 2. (RFID 검색 시스템) RFID 검색 시스템은 정의 1의 RFID 인증 시스템의 태그-*BS*간 인증 프로토콜*AP* 대신 다음의 검색 프로토콜을 가지며 나머지 구성요소는 동일하다.

- *T*-*BS*간 검색 프로토콜 *SP*: 리더 *R*을 전달자로 이용하는 *BS*와 태그간에 수행되는 다항시간 대화형 프로토콜로서 *BS*가 프로토콜을 개시한다. *BS*는 *R*을 통해 검색하고자 하는 목적 태그에 대한 질의문 *Query*를 생성하여 전송한다. 이후 태그의 응답 *Resp*을 수신하여 질의에 대한 적법한 응답인지 검증함으로서 목적 태그가 리더 주변에 존재하는지 확인한다. 태그 t_i의 식별자가 ID_i이고 비밀정보가 K_i일 때, *BS*는 t_i를 검색하기 위해 t_i의 비밀정보 K_i를 이용하여 *Query*를 생성하여 전송한다. *SP*는 t_i가 자신의 비밀 정보 K_i를 이용하여 *Query*에 상응하는 합법적인 *Resp*를 생성하여 전송하면 *OK*를 *BS*에게 출력하며 그렇지 않은 경우 $\perp$를 출력하고 종료한다.

검색 프로토콜은 인증 프로토콜의 특별한 형태로 볼 수 있다. 즉 인증 프로토콜을 수행하면 리더 주변에 있는 모든 태그를 식별할 수 있기 때문에 검색하고자 하는 태그가 리더 주변에 존재하는지 여부도 확인할 수 있다. 하지만 특정 태그만을 검색하고자 하는 것이 검색 프로토콜의 목적이라는 점에서 볼 때 주변에 있는 모든 태그를 인증하는 것은 불필요한 작업이며 매우 비효율적이다. 따라서 효율적인 RFID 검색 시스템을 다음과 같이 정의한다.

정의 3. (효율적인 RFID 검색 시스템) 정의 2의 RFID 검색 시스템 중 *SP*가 다음의 추가적인 조건을 만족하면 효율적인 RFID 검색 시스템이라 한다.

- 리더의 질의는 리더가 검색하고자 하는 대상 태그만 식별할 수 있다. 따라서 이 질의를 수신한 검색 대상 태그가 아닌 다른 태그는 아무런 응답을 생성하지 않으며 오직 검색 대상 태그만 리더의 질의에 응답을 전송한다.

정의 4. (서버 없는 RFID 검색 시스템) 서버없는 RFID 검색 시스템은 다음과 같이 구성된다.

- 태그 집합 $T=\{t_1,t_2,...,t_n\}$: 백엔드 서버 시스템에 등록된 태그 집합
- 리더 집합 $R=\{r_1,r_2,...,r_l\}$: 백엔드 서버 시스템에 등록된 이동형 리더 집합
- 백엔드 서버 시스템 *BS*: 등록된 태그, 리더 집합을 유지관리하고 리더에게 인증 가능한 태그 목록 및 식별 정보를 발급
- 알고리즘 SetupTag(*ID*,*K*): *BS*가 실행하는 알고리즘으로서 태그의 메모리에 비밀정보 *K*를 저장하

고 *BS*의 데이터베이스에 $<ID, K>$를 저장한다. *ID*는 EPC와 같은 태그 고유 식별자를 의미하고 *K*는 태그의 비밀 정보로서 다수의 비밀정보 $\{k_1, k_2, ...\}$로 구성될 수 있다.

• 알고리즘 SetupReader(*ID*,*LIST*): *BS*가 실행하는 알고리즘으로서 리더에게 인증할 수 있는 태그 목록을 발급하고 *BS*의 데이터베이스에 $<ID, LIST>$를 저장한다. *ID*는 이동형 리더의 식별자를 의미하고 *LIST*는 이동형 리더가 인식할 수 있는 태그 목록으로 각 태그의 식별자와 각 태그별 식별 정보가 포함된다. 태그 식별 정보는 태그 고유의 비밀 정보 *K*를 이용하여 생성된다.

• 태그-리더간 검색 프로토콜 *SSP*: 이동형 리더와 태그간에 수행되는 다항시간 대화형 프로토콜로서 리더가 프로토콜을 개시한다. 리더는 자신의 인증 가능 태그 목록 *LIST*에서 검색하고자 하는 목적 태그 t_i를 선택하고 t_i의 식별 정보를 이용하여 질의문 *Query*를 생성하여 전송한다. 이후 태그의 응답 *Resp*을 수신하여 질의에 대한 적법한 응답인지 검증함으로서 목적 태그가 리더 주변에 존재하는지 확인한다. 태그 t_i의 식별자가 ID_i이고 비밀정보가 K_i일 때, *SSP*는 t_i가 자신의 비밀 정보 K_i를 이용하여 *Query*에 상응하는 합법적인 *Resp*를 생성하여 전송하면 *OK*를 리더에게 출력하며 그렇지 않은 경우 ⊥를 출력하고 종료한다.

정의 5. (비연결성과 비관찰성) 다수의 개체가 참여하여 생성된 메시지 집합에서 임의로 선택된 서로 다른 두 메시지가 같은 개체에서 생성된 것인지 여부를 확인할 수 없을 때 두 메시지는 비연결성(unlinkability)이 보장된다라고 정의한다. 또한 임의로 선택된 하나의 메시지가 제시된 특정 개체에 의해 생성된 것인지 여부를 확인할 수 없을 때 해당 메시지는 비관찰성(unobservability)이 보장된다라고 정의한다.

정의 5의 비연결성과 비관찰성의 관계는 비관찰성이 비연결성을 포함하는 관계이다. 즉 비관찰성이 만족되지 않으면 비연결성도 만족되지 않으며, 비연결성이 만족되면 비관찰성도 만족된다. 하지만 비관찰성이 만족되더라도 비연결성이 만족되는 것이 아니기 때문에 이 두 개념은 명확히 구분되어야한다. 어떤 프로토콜이 비관찰성은 만족하나 비연결성은 만족하지 않는 경우 어떤 프라이버시 문제가 있겠는가는 문제를 생각해보자. 위치 추적의 안전성 측면에서 비관찰성만 보장하더라도 위치추적에 안전하다고 분석할 수 있다. 하지만 이 경우 비연결성이 보장되지 않은 메시지 중 하나라도 메시지의 비관찰성이 깨지는 순간 연결된 모든 메시지의 비관찰성이 깨지게 된다. 반면 비연결성이 보장된 메시지의 경우 하나의 메시지의 비관찰성이 깨져도 다른 메시지에 영향을 주지 않는다.

정의 6. (강한 프라이버시와 약한 프라이버시) 태그 리더간 전송되는 메시지의 비관찰성과 비연결성을 모두 만족하는 RFID 보안 프로토콜을 강한 프라이버시(strong privacy)를 제공한다고 정의하고 비관찰성만 만족하는 프로토콜을 약한 프라이버시(weak privacy)를 제공한다고 정의한다.

정의 7. (동적/정적 인증정보 기반 RFID 프로토콜) 태그 메모리에 저장된 태그 고유의 비밀 정보가 독립적인 프로토콜 수행 이후 동적으로 갱신되는 프로토콜을 동적 인증정보 기반 RFID 프로토콜이라고 하고, 프로토콜 수행과 관계없이 태그의 비밀정보가 고정되어 변하지 않는 프로토콜을 정적 인증정보 기반 RFID 프로토콜이라고 정의한다.

2.2 서버 없는 RFID 검색 시스템의 보안 요구사항

모바일 RFID 환경에서 인증 서버가 없는 RFID 검색 시스템은 다음과 같은 보안 요구사항을 만족해야 한다.

• 요구사항 1. 태그 위조에 대한 강건성

특정 태그를 검색하는 유효한 질의가 주어졌을 때 질의 대상 태그 외의 다른 개체(태그, 리더, 공격자)는 해당 태그의 내부 상태를 모르는 경우, 질의에 대응되는 유효한 응답을 만들 수 없어야한다.

• 요구사항 2. 리더 위조에 대한 강건성

백엔드 서버 시스템으로부터 특정 태그의 인증 정보를 받지 않은 다른 개체는 해당 태그에 대한 유효한 질의를 만들 수 없어야한다.

• 요구사항 3. 태그 프라이버시

3-1. 질의의 태그 비관찰성: 질의를 생성한 리더와 질의 대상 태그 외에는 해당 질의가 어떤 태그를 대상으로 하는 질의인지 식별할 수 없어야 한다.

3-2. 응답의 태그 비관찰성: 질의를 생성한 리더와 질의 대상 태그 외에는 해당 질의에 대한 응답이 어떤 태그의 응답인지 식별할 수 없어야

〔표 1〕 표기법

T	RFID 시스템의 태그 집합 $T=\{t_1,t_2,...,t_n\}$	K_{AB}	개체 A와 B간의 공유 비밀키
R	RFID 시스템의 리더 집합 $R=\{r_1,r_2,...,r_l\}$	$\{m\}_K$	키 K를 이용한 메시지 m에 대한 AES 암호화
s_x	x번째 프로토콜 수행(세션)	$Challenger$	공격자와 객관적 공격 게임을 수행할 제 3의 개체
$\delta_{curr}, \delta_{last}$	각각 현재의 타임스탬프와 마지막 프로토콜 수행에서 저장한 타임스탬프 값.		
$\Omega_I(T,R)$	태그 집합 T와 리더 집합 R에 대해 세션 구간 I에서 획득할 수 있는 실험 결과 집합, 실험 결과 v_i는 태그로의 질의와 그 응답, 그리고 기타 프로토콜 수행 결과와 관련된 여분 정보들로 구성 $\Omega_I(T,R)=\{v_1,v_2,...\}$		

한다.

3-3. 응답의 비연결성: 질의를 생성한 리더와 질의 대상 태그 외에는 같은 태그의 서로 다른 두 응답을 연결할 수 없어야 한다.

• 요구사항 4. 리더 프라이버시

4-1. 질의의 리더 비관찰성: 질의를 생성한 리더 외에는 해당 질의가 어떤 리더의 질의인지 식별할 수 없어야한다.

4-2. 응답의 리더 비관찰성: 질의를 생성한 리더 외에는 태그의 응답으로부터 어떤 리더에 대한 응답인지 식별할 수 없어야한다.

4-3. 질의의 비연결성: 질의를 생성한 리더 외에는 같은 리더의 서로 다른 두 질의를 연결할 수 없어야한다.

III. 공격자 모델

본 장에서는 [7]에서 정의한 RFID 검색 프로토콜의 공격자 모델을 제안하는 인증 서버 없는 환경에 맞게 확장하며 이를 이용해 기존 프로토콜 및 제안하는 프로토콜을 분석한다. 공격자 모델은 공격의 목적, 공격자의 능력, 그리고 공격 게임으로 정의된다.

3.1 표기법

본 논문에서는 〔표 1〕과 같은 표기법을 사용한다.

3.2 공격의 목적

본 모델에서 공격자는 리더와 태그 구간에서 교환되는 메시지에 대해 다음의 공격을 시도하며 무시할 수 없는 확률로 다음과 같은 성과를 거두었을 때 공격자의 해당 공격이 성공했다고 한다.

• 요구사항 1에 대한 공격(태그 위조): 공격자는 태그를 가장하여 합법적 리더의 유효한 질의에 대해 위조된 응답을 생성하여 해당 태그인 것처럼 인증 받을 수 있다.

• 요구사항 2에 대한 공격(리더 위조): 공격자는 리더를 가장하여 유효한 질의를 생성하고 이를 통해 등록된 태그를 검색할 수 있다.

• 요구사항 3에 대한 공격(태그 프라이버시 침해): 리더의 질의 메시지나 태그 응답 메시지에 포함된 검색 대상 태그 신원의 관찰성을 확보하거나 같은 태그의 응답 메시지들 간의 연결성을 확보하여 태그의 행적을 추적할 수 있다.

• 요구사항 4에 대한 공격(리더 프라이버시 침해): 리더의 질의 메시지나 태그 응답 메시지에 포함된 질의문을 생성한 리더 신원의 관찰성을 확보하거나 같은 리더의 질의 메시지들 간의 연결성을 확보하여 리더의 행적을 추적할 수 있다.

태그 및 리더의 행적은 전방향(forward)과 후방향(backward)로 구분할 수 있다. 공격자가 메시지의 관찰성을 확보하여 공격 대상의 이전 행적을 추적할 수 있는 경우 후방향 위치 추적이 가능하다고 정의하고 앞으로의 행적을 추적할 수 있는 경우 전방향 위치 추적이 가능하다고 정의한다.

3.3 공격자의 능력

일반적으로 RFID 시스템에서 구분하는 공격자 유형은 태그를 포획할 수 있는 능력이 있는 강한 공격자와 그렇지 않은 약한 공격자로 구분한다. 제안하는 서버 없는 RFID 검색 환경에서는 시스템에 등록된 리더가 잠재적으로 공격자가 될 수 있기 때문에 다음의 4가지로 공격자 유형을 분류할 수 있다.

• 단순 공격자 SA: 태그나 리더를 포획할 능력이 없는 공격자

• 태그 포획이 가능한 공격자 TCA: 태그만 포획할 수 있는 공격자

• 리더 포획이 가능한 공격자 RCA: 리더만 포획할 수 있는 공격자

• 태그와 리더 포획이 가능한 공격자 TRCA: 태그와 리더를 모두 포획할 수 있는 공격자

SA는 시스템에 등록된 리더가 아니면서 단순히 도청, 메시지 수집 등의 방법으로 공격을 시도하는 공격자를, RCA는 시스템에 등록된 리더가 공격자로 활동하는 경우, 즉 일부 태그 집합의 인증 정보를 가지고 있는 시스템 리더가 다른 리더와 태그를 대상으로 공격을 시도하는 것을 모델링한다. TCA의 경우 태그를 물리적으로 포획할 수 있는 공격자를 모델링한다.

리더나 태그를 포획 가능한 공격자가 포획한 개체에 대해 위조 공격을 시도하거나 앞으로의 행적을 추적하는 것은 이미 해당 개체를 포획한 공격자에게 의미가 없으므로, 일반적으로 공격자의 개체 포획은 공격 대상 태그를 직접 포획하는 것을 고려하지 않는다. 다만 개체의 후방향 위치 추적 안전성을 분석하기 위해 공격자가 공격 대상 개체를 직접 포획하는 상황을 고려해야할 필요가 있다. 이 경우 해당 공격자를 T^*CA, R^*CA로 나타낸다. 즉 T^*CA는 공격 대상 태그를 포함한 모든 태그를 포획할 수 있는 공격자를 R^*CA는 공격 대상 리더를 포함한 모든 리더를 포획할 수 있는 공격자를 의미한다. 여기서 공격 대상이란 위조 공격의 대상이 되는 태그 또는 리더, 그리고 수 있는 공실험을 위해 공격자가 *Challenger*에게 요청한 값의 생성에 관여한 리더를 의미한다.

각 공격자는 자신의 능력에 맞게 공격에 필요한 정보를 *Challenger*에게 요청할 수 있다. *Challenger*는 검색 시스템에 대한 실험 수단으로 아래 오라클을 호출할 수 있으며 공격자에 능력에 맞게 공격자의 요청을 수락하고 아래 오라클을 호출하여 그 결과를 전달한다.

• Listen$(T,R,I) \rightarrow \Omega_I(T,R)$: 세션구간 $I \subset \{s_1,s_2,...,s_c\}$에서 발생하는 태그 집합 T와 리더 집합 R간의 통신 메시지를 도청하는 것을 모델링하며 전송된 메시지 집합 $\Omega_I(T,R)$를 출력한다.

• Search$(t_i,m,s_x) \rightarrow 1$ or $\varnothing$: 세션 s_x에서 태그 t_i를 검색하는 질의 메시지 m을 전송하는 것을 모델링 한다. 합법적인 질의 메시지 m을 이용한 Search 호출은 1을 출력하고 그렇지 않은 경우 아무것도 출력하지 않는다.

• Response$(r_j,m_1,m_2,s_x) \rightarrow 1$ or $\varnothing$: 세션 s_x에서 리더 r_j의 검색 질의 메시지 m_1에 대한 응답 m_2를 전송하는 것을 모델링한다. 리더 r_j의 합법적 질의 메시지 m_1과 응답 메시지 m_2를 이용한 Response 호출은 1을 출력하며 그렇지 않은 경우 아무것도 출력하지 않는다.

• Corrupt$(B,s_x) \rightarrow K_B$: 세션 s_x에서 개체 B를 포획하는 것을 모델링한다. 오라클 Corrupt의 호출은 개체 B가 태그인 경우에는 태그의 식별자 t_B와 비밀 정보 K_B를 출력하며 개체 B가 리더인 경우에는 B의 태그 인증 정보 리스트 L_B를 출력한다.

• Link$(v_i,v_j) \rightarrow 1$ or 0: 실험 결과 v_i와 v_j가 같은 개체에서 생성된 실험 결과인지 여부를 판단하는 것을 모델링한다. 두 실험 결과 v_i와 v_j가 같은 개체에서 생성된 실험 결과이면 1을 그렇지 않으면 0을 출력한다.

3.4 공격 게임

공격자의 태그 및 리더 위조, 프라이버시 침해 공격은 다음과 같이 *Challenger*와 공격자간의 공격 게임으로 정의 할 수 있다. 공격자 TRCA의 경우 각 게임에서 별도로 정의하지 않아도 공격자 *TCA*와 *RCA*가 할 수 있는 *Challenger*에 대한 요청을 모두 할 수 있다.

(게임 1) 태그 위조: 게임 참여 가능 공격자 - SA, TCA, RCA, TRCA

1. 공격자는 세션 구간 $I \subset \{s_1,s_2,...,s_p\}$에서 생성된 트랜스크립트 집합 $\Omega_I(T,R)$을 *Challenger*에게 요청하고 *Challenger*는 Listen(T,R,I)를 호출하여 그 결과를 공격자에게 전달한다.
2. *Challenger*는 세션 $s_c(c>p)$에서 공격 대상 태그 $t_i(i \in_R \{1,2,...,n\})$와 t_i를 검색할 수 있는 리더 $r_j(j \in \{1,2,...,l\})$를 선정하여 r_j의 t_i에 대한 유효한 질의문 *Query*를 공격자에게 제시한다.
3. *RCA*는 원하는 만큼 리더 포획을 요청할 수 있으며, *RCA*의 요청이 있을 경우 Challenger는 t_i를 검색할 수 있는 리더 r_x $(x \neq j(\in 1,2,...,l))$를 선정하여 Corrupt$(r_x, s_c)$를 호출하고 그 결과를 공격자에게 전달한다.
4. *TCA*는 원하는 만큼 태그 포획을 요청할 수 있으며, *TCA*의 요청이 있을 경우 *Challenger*는 $t_y(y \neq i)$를 선정하여 Corrupt(t_y, s_c)를 호출하고 그 결과를 공격자에게 함께 전달한다.
5. 공격자는 단계 1, 3, 4에서 획득한 정보를 이용

하여 *Query*에 대한 응답 *Resp*를 생성하여 *Challenger*에게 제시한다.

6. *Challenger*는 Response(r_j, *Query*, *Resp*, s_c)를 호출하고 그 결과가 1이면 공격자의 공격은 성공한다.

단계 3은 시스템에 정상적으로 등록되어 t_i의 인증 정보를 가진 리더가 태그 위조를 시도하는 것을 모델링한다. 시스템에 등록된 리더가 공격자가 될 경우 공격자는 t_i의 인증 정보를 가지고 있을 수도 있고 아닐 수도 있다. t_i의 인증 정보를 가지지 않은 리더는 단순 공격자와 차이가 없기 때문에 단계 3에서 *Challenger*는 t_i의 인증 정보를 가진 리더에 대해 Corrupt를 호출하고 그 결과를 공격자에게 전달한다.

(게임 2) 리더 위조: 게임 참여 가능 공격자 - SA, TCA, RCA, TRCA

1. 공격자는 세션 구간 $I \subset \{s_1, s_2, ..., s_p\}$에서 생성된 트랜스크립트 집합 $\Omega_I(T,R)$을 *Challenger*에게 요청하고 *Challenger*는 Listen(T,R,I)를 호출하여 그 결과를 공격자에게 전달한다.
2. *Challenger*는 공격 대상 태그 $t_i \in T$를 선정하고 공격자에게 제시한다.
3. *RCA*는 원하는 만큼 리더 포획을 요청할 수 있으며, *RCA*의 요청이 있을 경우 *Challenger*는 t_i를 검색할 수 없는 리더 $r_j (j \in \{1,2,...,l\})$를 선정하여 Corrupt($r_j$, s_c)를 호출하고 그 결과를 공격자에게 함께 전달한다.
4. *TCA*는 원하는 만큼 태그 포획을 요청할 수 있으며, *TCA*의 요청이 있을 경우 *Challenger*는 $t_y (y \neq i)$를 선정하여 Corrupt(t_y, s_c)를 호출하고 그 결과를 공격자에게 함께 전달한다.
5. 공격자는 획득한 정보를 이용하여 t_i에 대한 검색 질의문 *Query*를 생성하고 *Challenger*에게 제시한다.
6. *Challenger*는 Search(t_i, *Query*, s_c)를 호출하고 그 결과가 1이면 공격자의 공격은 성공한다.

리더 위조 공격의 경우 공격 대상 태그 t_i를 검색할 수 있는 능력이 있는 리더는 다른 리더를 가장하여 t_i를 위한 검색 질의를 생성할 필요가 없다. 따라서 *Challenger*는 공격자에게 t_i를 검색할 수 없는 리더에 대해 Corrupt를 호출하고 그 결과를 공격자에게 전달한다.

(게임 3) 태그와 리더 프라이버시 침해

(게임 3-1: 질의 및 응답의 관찰성): 게임 참여 가능 공격자 - *SA, TCA, RCA, TRCA*

1. *Challenger*는 세션 s_c에서 공격 대상 태그 t_i ($i \in_R \{1,2,...,n\}$)와 t_i를 검색할 수 있는 리더 r_j ($j \in \{1,2,...,l\}$)를 선정하여 r_j의 t_i에 대한 유효한 질의문 *Query*와 상응하는 응답 *Resp*를 생성하고 공격자에게 제시한다.
2. *RCA*는 원하는 만큼 리더 포획을 요청할 수 있으며, *RCA*의 요청이 있을 경우 *Challenger*는 t_i를 검색할 수 있는 리더 r_x ($x \neq j (\in 1,2,...,l)$)를 선정, Corrupt(r_x, s_c)를 호출하여 그 결과를 공격자에게 함께 제시한다.
3. *TCA*는 원하는 만큼 태그 포획을 요청할 수 있으며, *TCA*의 요청이 있을 경우 *Challenger*는 $t_y (y \neq i)$를 선정하여 Corrupt(t_y, s_c)를 호출하고 그 결과를 공격자에게 함께 제시한다.
4. 공격자는 획득한 정보로부터 공격대상 태그 t_i'와 질의를 생성한 리더 r_j'를 유추하여 *Challenger*에게 제시한다.
5. *Challenger*는 Search(t_i', *Query*, s_c) 또는 Response(r_j', *Query*, *Resp*, s_c)를 호출한다.
6. Search(t_i', *Query*, s_c) 호출 결과가 1이면 태그 관찰 성공, Response(r_j', *Query*, *Resp*, s_c) 호출 결과가 1이면 리더 관찰 성공

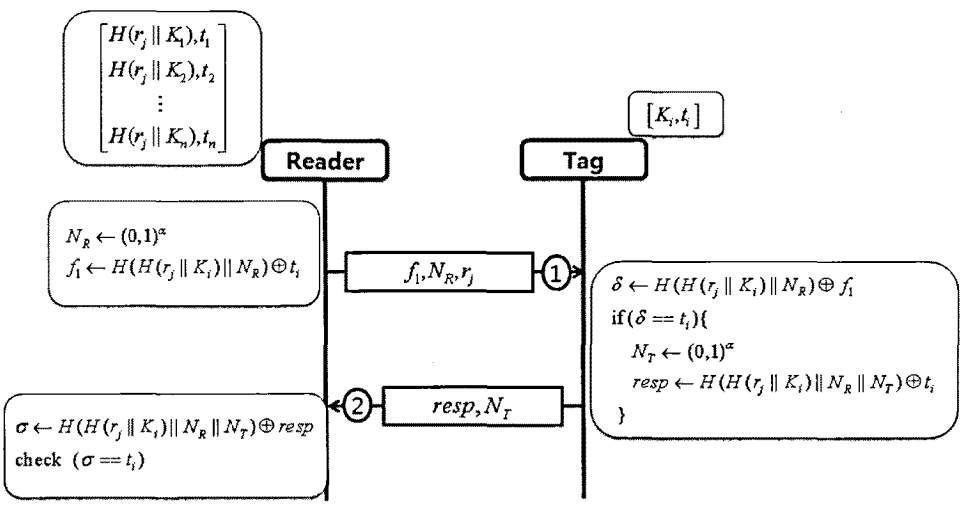
(게임 3-2:질의 및 응답의 연결성): 게임 참여 가능 공격자 - *SA*, T^*CA, R^*CA, T^*R^*CA

1. 공격자는 세션 구간 $I \subset \{s_1, s_2, ..., s_p\}$에서 생성된 트랜스크립트 집합 $\Omega_I(T,R)$을 *Challenger*에게 요청하고 *Challenger*는 Listen(T,R,I)를 호출하여 그 결과를 공격자에게 전달한다.
2. *Challenger*는 세션 s_c에서 공격 대상 태그 t_i ($i \in_R \{1,2,...,n\}$)와 t_i를 검색할 수 있는 리더 r_j ($j \in \{1,2,...,l\}$)를 선정하여 r_j의 t_i에 대한 유효한 질의문 *Query*와 상응하는 응답 *Resp*를 생성하고 공격자에게 제시한다.
3. R^*CA는 공격 대상 리더 r_j의 포획을 한번만 요청할 수 있으며 R^*CA의 요청이 있을 경우 *Challenger*는 Corrupt(r_j, s_c),를 호출하고

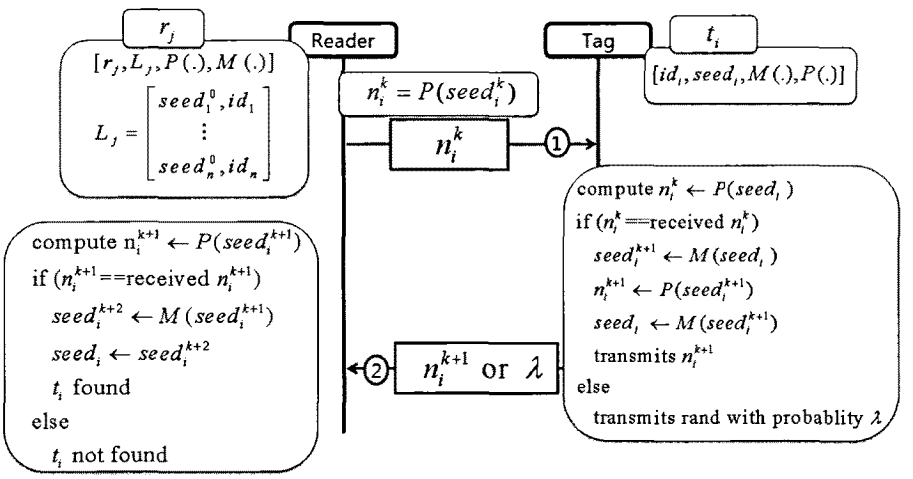
그 결과를 함께 제시한다.

4. T^*CA는 공격 대상 태그 t_i의 포획을 한번만 요청할 수 있으며 T^*CA의 요청이 있을 경우 *Challenger*는 Corrupt(t_i, s_c)를 호출하고 그 결과를 공격자에게 함께 제시한다.
5. 공격자는 획득한 정보로부터 수신한 *Query*, *Resp*와 연결성이 있다고 생각되는 *Query'*, *Resp'*을 $\Omega_f(T,R)$에서 선택하고 이를 *Challenger*에게 제시한다.
6. Challenger는 Link(*Query*, *Query'*) 또는 Link(*Resp*, *Resp'*)를 호출한다.
7. Link(*Query*, *Query'*) 호출 결과가 1이면 질의의 연결 공격 성공, Link(*Resp*, *Resp'*) 호출 결과가 1이면 응답의 연결 공격 성공

게임 3-2의 단계 3, 4에서는 태그 및 리더의 과거 행적(후방향 위치 추적)에 대한 공격자의 프라이버시 침해를 모델링하기위해 공격 대상 태그를 포획하는 공격자를 고려하고 있다. 공격자는 포획한 태그 및 리더의 내부 비밀 정보를 이용, 지나간 세션의 메시지를 분석하여 해당 태그 및 리더의 지난 행적을 알아낼 수 있다.



〔그림 1〕 Tan 등의 기본 검색 프로토콜



〔그림 2〕 Ahamed 등의 동적 인증 정보기반 검색 프로토콜

IV. 사례 연구

4.1 Tan 등의 검색 프로토콜

Tan [1]등은 4가지 서버없는 RFID 검색 프로토콜을 제안한다. [그림 1]은 Tan 등의 기본 검색 프로토콜을 본 논문의 표기법으로 표현한 그림이다. Tan 등의 기본 프로토콜은 정적 인증 정보기반 검색 프로토콜로서 다음과 같은 공격이 가능하다.

- 리더 위조: 공격자 *SA*가 게임 2의 단계 1에서 획득한 태그는 $\Omega_I(T,R)$로부터 t_i를 대상으로 하는 질의문을 구분해 낼 수 있다면 단계 5에서 이를 *Challenger*에게 제시함으로서 게임에서 승리할 수 있다. 즉, 태그는 리더의 질의에 대한 최신성을 검증하지 않아 공격자의 재전송 공격이 가능하다.
- 태그 프라이버시 침해: 질의 및 응답의 연결성 게임 단계 4에서 공격 대상 태그 t_i의 비밀정보 K_i와 t_i를 획득한 공격자 T^*CA는 단계 1에서 확보한 $\Omega_I(T,R)$의 값들을 계산하여 *Challenger*가 제시한 *Resp*와 같은 K_i, t_i를 사용하여 생성된 *Resp'*를 구분할 수 있고 이를 *Challenger*에게 제시하여 게임에서 승리할 수 있다.
- 리더 프라이버시 침해: 질의 및 응답의 관찰성 게임 단계 1에서 *Challenger*로부터 *Query*, *Resp* 값을 수신한 공격자 *SA*는 *Query*에 포함된 리더 아이디 r_j로부터 질의문 생성 리더 r_j'이 r_j라고 유추하고 이를 *Challenger*에게 제시함으로서 게임에서 승리할 수 있다. 리더의 관찰성이 깨지므로 공격자는 게임 3-2의 연결성 게임에서도 승리할 수 있다.

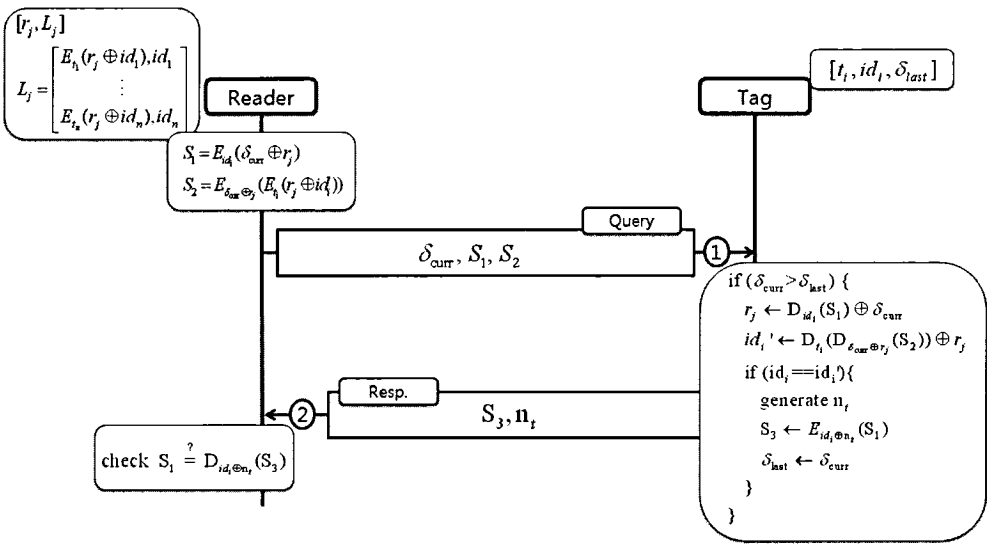
한 가지 언급해야할 것은 제안하는 공격자 모델의 공격자가 리더 위조 게임에서 승리하기 위해서는 확보한 이전 세션의 질의문이 어떤 태그를 검색하는 질의문인지 구분해 낼 수 있어야한다는 점이다. 즉 재전송 공격에 성공하기 위해서는 공격자가 질의문 또는 응답문의 관찰성을 이미 확보했다는 가정이 전제되어야한다. 이는 어떤 프로토콜이 가진 재전송 공격에 대한 취약성은 해당 프로토콜에 대한 공격자의 재전송 공격이 항상 가능하다는 것을 의미하지는 않는다. 하지만 공격자가 특정 태그를 검색하는 질의에 대한 관찰성을 확보하게 되면 공격자는 지속적으로 해당 질의를 재전송하여 특정 태그를 계속 추적할 수 있다.

Tan 등은 이러한 재전송 공격에 취약성을 없애고 개선하고자 3가지 검색 프로토콜을 추가로 제안하였다. 첫 번째 프로토콜은 태그가 이전 세션에서 수신한 리더의 랜덤수 N_R을 저장하여 재전송 공격에 대응하고자 했으나 태그가 모든 리더의 랜덤수를 계속 저장하고 유지할 수 없기 때문에 완전한 해결책이 될 수 없다. 두 번째와 세 번째 프로토콜 역시 리더 검색 질의에 다수의 태그가 함께 응답하거나 인증 프로토콜에서처럼 리더 주변의 모든 태그가 응답하는 등 효율적인 검색 프로토콜로 분류할 수 없어 근본적인 해결책으로 보기 힘들다.

4.2 Ahamed 등의 검색 프로토콜

Ahamed [5]등은 동적 인증 정보기반의 서버없는 RFID 검색 프로토콜을 제안하였다. Ahamed 등의 검색 프로토콜은 태그의 비밀 정보를 일방향 해쉬 함수를 이용하여 동적으로 갱신하여 공격자의 재생 공격을 막고 후방향 태그 위치추적 안전성을 보장하려고 했다. 하지만 동적 인증 정보 기반의 서버 없는 검색 프로토콜은 다수의 리더가 존재하는 시스템에서 구현될 수 없다. 즉 [그림 2]의 리더 r_j와 태그 t_i간 검색 프로토콜이 성공적으로 종료되면 r_j 와 t_i는 비밀 정보 $seed_i$를 갱신하기 때문에 이후 새로운 등록된 리더 r_{j+1}가 t_i를 검색하고자 해도 t_i의 갱신된 $seed_i'$값을 알지 못하기 때문에 검색에 성공하지 못한다. 5장 분석에서 이를 증명 한다. 또한 Ahamed 등의 검색 프로토콜은 채널 오류나 전송 오류, 공격자의 개입 등으로 마지막 2번 메시지가 차단되면 리더와 태그의 공유 비밀 정보 *seed*값의 동기화가 깨져 리더는 태그를 더 이상 검색할 수 없게 된다. 그림 2는 Ahamed 등의 검색 프로토콜을 본 논문의 표기법으로 표현한 그림이며 다음과 같은 공격이 가능하다.

- 태그 위조: 리더를 포획할 수 있는 공격자 *RCA*는 태그 위조 게임 단계 3에서 *Challenger*로부터 t_i를 검색 할 수 있는 리더 r_x의 인증 정보 리스트 L_x를 넘겨 받는다. L_x에는 t_i의 인증 정보 $seed_i^a$와 아이디 id_i가 포함되어 있으므로 질의문 *Query*가 어떤 태그를 검색하는 질의인지 알고 있는 공격자는 합법적인 응답 *Resp*를 $seed_i^{a+1} = P(Query)$로 계산할 수 있다. 생성한 응답을 단계 4에서 *Challenger*에게 제시한 공격자 *RCA*는 태그 위조 게임에서 승리한다.



〔그림 3〕 Won 등의 정적 인증 정보기반 검색 프로토콜

4.3 Won 등의 검색 프로토콜

Won〔6〕 등은 AES 암호 알고리즘을 사용하는 정적 인증 정보기반 검색 프로토콜을 제안하였다. 〔그림 3〕에서 처럼 Won 등의 프로토콜은 리더의 프라이버시를 보호하기 위해 리더의 아이디를 AES 알고리즘으로 암호화해서 전달한다. AES 알고리즘은 암호학적 해쉬함수와 달리 대칭성을 가진 암호 프리미티브로서 리더가 AES를 이용하여 암호화한 메시지를 태그가 복호화할 수 있어 이 특성을 이용하면 효율적인 프로토콜 설계가 가능하다. 하지만 Won 등의 프로토콜은 태그의 비밀 정보 id_i를 리더가 알고 있고 이를 이용해 리더 스스로 질의 메시지를 생성하기 때문에 다음과 같은 공격이 가능하다.

- 태그 위조: 리더를 포획할 수 있는 공격자 *RCA*는 태그 위조 게임 단계 3에서 *Challenger*로부터 t_i를 검색 할 수 있는 리더 r_x의 인증 정보 리스트 L_x를 넘겨 받는다. L_x에는 t_i의 인증 정보 $E_{t_i}(r_j \oplus id_i)$와 아이디 id_i가 포함되어 있으므로 질의문 *Query*가 어떤 태그를 검색하는 질의인지 알고 있는 공격자는 합법적인 응답 *Resp*를 *Query*에 포함된 S_1값을 이용 $E_{id_t \oplus n_t}(S_1)$, n_t로 생성할 수 있다. 생성한 응답을 단계 4에서 *Challenger*에게 제시한 공격자 *RCA*는 태그 위조 게임에서 승리한다.
- 태그 프라이버시 침해: 게임 3-1의 단계 2에서 획득한 r_x의 L_x로부터 태그의 아이디 집합 $\{..., t_i, ...\}$를 획득한 공격자는 *Challenger*가 제시한 *Resp*를 하나씩 복호화해보고 어떤 태그의 응답인지 구분해 낼 수 있다. 공격자는 t_i를 단계 4에서 *Challenger*에게 제시함으로서 태그 관찰성 게임에서 승리할 수 있다. 또한 게임 3-2 단계 4에서 공격 대상 태그 t_i의 비밀정보 K_i와 t_i를 획득한 공격자 T^*CA는 단계 1에서 확보한 $\Omega_1(T,R)$의 값들을 계산하여 *Challenger*가 제시한 *Resp*와 같은 K_i, t_i를 사용하여 생성된 *Resp'*를 구분할 수 있고 이를 *Challenger*에게 제시하여 태그 연결성 게임에서 승리할 수 있다.
- 리더 프라이버시 침해: 공격자는 게임 3-1의 단계 2에서 획득한 r_x의 L_x로부터 태그의 아이디 집합 $\{..., t_i, ...\}$를 획득한 공격자는 *Challenger*가 제시한 *Query*를 하나씩 복호화해보고 리더 아이디 r_j를 확인할 수 있다. 공격자는 r_j를 *Challenger*에게 제시함으로서 리더 관찰성 게임에서 승리할 수 있다. 리더의 관찬성이 깨지므로 공격자는 게임 3-2의 연결성 게임에서도 승리할 수 있다.

V. 제안하는 서버없는 검색 시스템

제안하는 서버없는 검색 시스템은 다음과 같이 구

성된다.

- 알고리즘 SetupTag(*ID*,*K*): 검색 시스템에 n개의 등록된 태그가 있다고 했을 때 태그의 *ID*는 $ID \in \{t_1, t_2, ..., t_n\}$으로 설정된다. 태그 t_i는 고유 비밀키는 K_i와 메시지 최신성을 판단을 위한 타임스템프 δ_{last}값을 비밀 정보로 가지고 있다. 처음 설정 이후 태그의 δ_{last}값은 합법적 리더에 의해서 갱신된다.
- 알고리즘 SetupReader(*ID*,*LIST*): 검색 시스템에 l개의 등록된 리더가 있다고 했을 때 리더의 *ID*는 $ID \in \{r_1, r_2, ..., r_l\}$로 설정된다. 리더는 고유 식별자 r_j와 최초 *BS*가 발급해주고 이후 태그에 의해서 갱신되는 인증 태그 목록을 가지고 있다. r_j의 인증 태그 목록 L_j는 자신의 비밀 키 K_{ij}와 태그 고유 비밀 정보를 이용하여 AES 암호화된 식별 정보, 그리고 태그 식별자로 구성되며 다음과 같다.

$$L_j = \begin{bmatrix} K_{1j}, \{K_{1j} \| t_1\}_{K_1}, t_1 \\ K_{2j}, \{K_{2j} \| t_2\}_{K_2}, t_2 \\ \vdots \\ K_{ij}, \{K_{ij} \| t_i\}_{K_i}, t_i \end{bmatrix}$$

- 태그-리더간 검색 프로토콜 *SSP*
- 단계 1: 태그 t_i를 검색 하고자 하는 리더 r_j는 L_j로부터 다음의 질의문을 생성해 태그에게 전송한다.

Query:

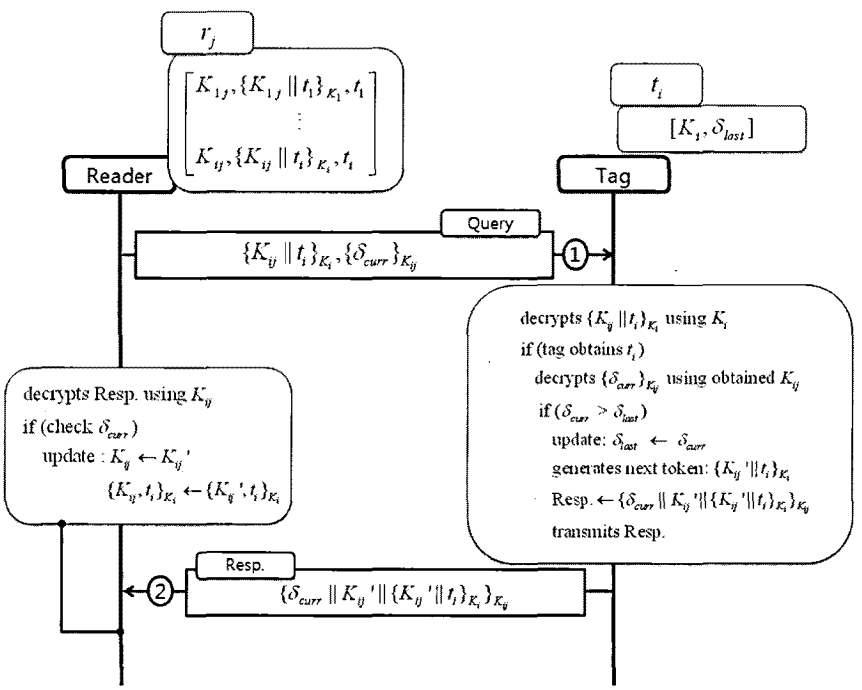
$$\{K_{ij} \| t_i\}_{K_i}, \{\delta_{curr}\}_{K_{ij}} \quad (1)$$

- 단계 2: 리더 r_j의 질의를 수신한 태그 t_i는 자신의 비밀키 K_i를 이용해 식별 정보 $\{K_{ij} \| t_i\}_{K_i}$를 복호화하고 K_{ij}와 t_i를 획득한다. 이후 획득한 K_{ij}를 이용 타임스템프 δ_{curr}를 복호화함으로써 질의문의 최신성을 확인하고 수신한 δ_{curr}를 저장한다. 이후 태그는 리더 r_j가 다음번 질의에 사용할 수 있는 자신의 식별 정보를 새롭게 생성하고 δ_{curr}와 함께 K_{ij}로 암호화하여 리더에게 전송한다.

$$\{\delta_{curr} \| K_{ij}' \| \{K_{ij}' \| t_i\}_{K_i}\}_{K_{ij}} \quad (2)$$

- 단계 3: 태그의 응답을 수신한 리더는 응답을 K_{ij}로 복호화하고 δ_{curr}를 확인하여 질의에 대한 합법적인 응답인지 확인한다. 이후 태그가 생성하여 보낸 새로운 식별 정보로 L_j를 갱신한다.

[그림 4]는 제안하는 태그-리더간 검색 프로토콜을 나타낸다.



[그림 4] 제안하는 검색 프로토콜

제안하는 검색 시스템의 장점은 다음과 같다.

- 제안하는 검색 시스템의 검색 프로토콜은 정의 3의 효율적인 검색 프로토콜로서 질의 대상이 되는 목적 태그만 리더의 질의를 식별할 수 있고 응답을 전송하기 때문에 효율적으로 태그를 검색할 수 있다.
- *BS*가 발급하는 인증 태그 목록에는 태그 고유의 비밀 정보가 포함되어 있지 않으며 태그의 응답은 그 비밀 정보를 이용하여 생성되기 때문에 리더가 포획되더라도 태그를 위장하여 태그 행세를 할 수 없다.
- 리더의 질의에는 리더의 아이디가 포함되지 않으며 인증 태그 목록에 포함된 태그 식별 정보는 검색 성공시 태그에 의해서 갱신되기 때문에 리더 질의의 비관찰성 및 비연결성을 보장할 수 있다.

각 항목에 대한 추가적인 분석은 5장 분석 부분에서 자세히 다룬다.

VI. 분 석

본 절에서는 서버없는 RFID 시스템이 태그 포획이 가능한 공격자에 대해 태그 프라이버시 침해에 안전하지 않음을 보이고 제안하는 시스템이 2.2절에 정의한 4가지 보안 요구사항을 만족함을 증명한다.

Lemma 1. 서버없는 RFID 시스템의 정적 인증 정보기반 리더-태그 검색 프로토콜 *SSP*는 태그 포획이 가능한 공격자 A에 대해 전방향, 후방향 태그 프라이버시 보호를 제공하지 못한다.

증명. 정적 인증 정보 기반 프로토콜 *SSP*가 있다고 가정하자.

1) 정의 5에 의해서 *SSP*에 참여하는 태그 t_a는 자신의 비밀 정보 K_a를 갱신하지 않은 채 계속 유지한다.
2) 태그 포획이 가능한 강한 공격자는 태그의 비밀 정보 K_a를 획득할 수 있다.
3) 정의 4에 의해서 모든 태그의 응답은 자신의 비밀 정보 K_a를 이용해 계산되어야 한다.
4) 따라서 K_a를 획득한 A는 태그가 이전에 생성한 응답 메시지와 앞으로 생성할 응답 메시지를 모두 계산해 낼 수 있고 다른 태그의 응답과 구분해 낼 수 있다.
5) 그러므로 서버없는 RFID 시스템의 정적 인증 정보기반 리더-태그 검색 프로토콜 *SSP*는 태그 포획이 가능한 공격자 A에 대해 태그 위치 추적 안전성을 제공하지 못한다.

Lemma 2. 서버없는 RFID 시스템의 리더-태그 검색 프로토콜 *SSP*는 동적 인증 정보기반 프로토콜로 설계할 수 없다.

증명. 동적 인증 정보기반 *SSP*가 있으며 시스템에 등록된 리더 r_a, r_b 그리고 태그 t_c가 있다고 가정하자.

1) 정의 4에 의해서 서버없는 검색 시스템에 등록된 모든 리더는 백엔드 서버 시스템으로부터 발급받은 태그 식별정보를 이용해 동일한 태그를 검색할 수 있어야한다.
2) 리더 r_a가 태그 t_c를 동적 인증 정보 기반 *SSP*를 이용해 검색했다면 정의 5에 의해서 r_a의 검색이 종료된 후 t_c의 비밀 정보 K_c는 새로운 비밀 정보 K_c'으로 갱신되어 저장된다.
3) 이후 리더 r_b가 다시 태그 t_c를 검색하려고 할 때 r_b는 갱신된 t_c의 비밀 정보 K_c'를 알지 못하기 때문에 이전 비밀 정보 K_c를 이용해 질의를 생성하여 검색을 시도한다.
4) t_c는 r_b의 질의를 수신하지만 자신이 현재 저장하고 있는 비밀 정보 K_c'으로 생성된 질의가 아니기 때문에 응답 *Resp*를 생성하지 않는다.
5) 따라서 동적 인증 정보기반 *SSP*는 합법적으로 등록된 리더 r_a와 r_b의 태그 t_c의 검색에 대해 올바른 출력을 하지 못한다.

Lemma 3. 서버없는 RFID 검색 시스템은 태그 포획이 가능한 공격자에 대해 태그 프라이버시 침해에 안전하지 않다.

증명. RFID 프로토콜은 정의 5에서처럼 동적 인증 정보기반 프로토콜과 정적 인증 정보기반 프로토콜로 분류할 수 있다. 그런데 Lemma 1에 의해서 정적 인증 정보기반 검색 프로토콜을 사용하는 서버 없는 RFID 검색 시스템은 태그 포획이 가능한 공격자에 대해 위치 추적 안전성을 보장할 수 없으며 Lemma 2 에 의해서 동적 인증 정보기반의 검색 프로토콜을 이용하는 서버 없는 RFID 검색 시스템은 설계할 수 없으므로 태그 포획이 가능한 공격자에 대해 태그 위치 추적에 안전한 서버없는 RFID 검색 시스템은 설계할 수 없다.

Assumption 1. 제안하는 시스템에서 사용하는

AES 암호 알고리즘은 의미론적 안전성(semantically security)을 제공한다.

Lemma 4. 제안하는 서버 없는 RFID 검색 시스템은 공격자 *TRCA*에 대해 태그 위조에 강건하다.

증명. 3.4절에 정의한 태그 위조 게임을 수행하는 공격자 *TRCA*를 생각해보자. 공격자가 게임에서 승리하기 위해선 Challenger가 제시한 *Query*에 대한 응답 *Resp*를 생성하여 제시할 수 있어야한다. 그런데 *Query*에 상응하는 응답 *Resp*은 *Query*에 사용된 r_j와 t_i 사이의 공유 비밀키 K_{ij}를 이용하여 생성되어야 한다. 즉 *Query*에 포함된 암호화된 타임스탬프 값을 K_{ij}로 복호화하여 획득한 후 응답 *Resp*에 포함 시켜야한다. 하지만 공격 대상 태그가 t_i라고 할 때 공격자가 태그 위조 게임 단계 1, 3에서 얻을 수 있는 정보는 다음과 같다.

- 단계 1: 리더 r_j와 t_i의 공유 비밀키 K_{ij}로 암호화된 타임스탬프 값과 새로운 세션에서 사용하게 될 인증 정보, 태그의 비밀키 K_i로 암호화된 태그 인증정보.

$\{K_{ij} \| t_i\}_{K_i}$, $\{\delta_{curr}\}_{K_y}$,$\{\delta_{curr} \| K_{ij}' \| \{K_{ij}' \| t_i\}_{K_i}\}_{K_y}$

- 단계 3: 리더 집합 $R'(R' \subset R,\ r_j \notin R')$ 에 있는 리더들의 비밀키, 인증 정보
  $r_x \in R'$일 때 r_x의 비밀키 K_{ix}, 태그 비밀키 K_i로 암호화된 태그 인증정보, 태그 아이디

$$L_x = \begin{bmatrix} K_{1x}, \{K_{1x} \| t_1\}_{K_i}, t_1 \\ K_{2x}, \{K_{2x} \| t_2\}_{K_i}, t_2 \\ \vdots \\ K_{ix}, \{K_{ix} \| t_i\}_{K_i}, t_i \end{bmatrix}$$

- 단계 4: 태그 집합 $T'(T' \subset T,\ t_i \notin T')$ 에 있는 태그들의 아이디와 비밀키, 타임스탬프값
  $t_y \in T'$일 때 t_y에 대해 아이디 t_y, 비밀키 K_y , 타임스탬프 δ_{last}

공격자가 획득한 위 정보에는 K_{ij}가 포함되어 있지 않으며, Assumption 1에 의해 의미론적 안전성이 보장되는 개별 정보들을 공격자가 다수 확보했다하여도 공격자에게 아무런 이득이 없다. 또한 획득한 정보로부터 공격자가 전수 공격(brute force)을 통해 K_{ij}를 계산하는 확률은 무시할 수 있으므로 공격자 TRCA는 태그 위조에 성공할 수 없다.

Lemma 5. 제안하는 서버 없는 *RFID* 검색 시스템은 공격자 *TRCA*에 대해 리더 위조에 강건하다.

증명. 3.4절에 정의한 리더 위조 게임을 수행하는 태그 및 리더 포획이 가능한 공격자를 생각해보자. 공격자가 게임에서 승리하기 위해선 게임 단계 1, 3에서 획득한 정보를 이용하여 유효한 질의문 *Query*를 생성할 수 있어야 한다. 유효한 질의문 *Query*에는 질의 대상 태그 t_i와 질의 생성 리더 r_j 간의 공유 비밀정보 K_{ij}로 암호화된 최신성 정보($\{\delta_{curr}\}_{K_y}$)가 포함되어야 한다. 하지만 공격자가 리더 위조 게임 단계 1, 3에서 얻을 수 있는 정보에는 태그 위조 게임에서처럼 공유 비밀키 K_{ij}가 포함되어 있지 않으며 확보한 다수의 암호문들은 Assumption 1에 의하여 K_{ij}를 계산해야하는 공격자에게 아무런 이득이 되지 않는다. 또한 공격자가 이전 세션에 사용된 유효한 질의문을 재전송 할 수 있지만 최신성을 확보하지 못한체 재전송된 질의문은 그림 4에 제시된 태그의 리더 인증 알고리즘을 통과할 수 없다. 공격자가 전수 공격을 통해 K_{ij}를 계산하는 확률은 무시할 수 있으므로 공격자는 리더 위조에 성공할 수 없다.

Lemma 6. 제안하는 서버 없는 RFID 검색 시스템은 단순 공격자 SA에 대해 리더 및 태그 비관찰성을 보장한다.

증명. 3.4절에 정의한 질의 및 응답의 관찰성 게임을 수행하는 단순 공격자를 생각해보자. 공격자가 게임에서 승리하기위해선 *Challenger*가 제시한 *Query*와 *Resp*로부터 질의 대상 태그 t_i나 r_j를 유추할 수 있어야 한다.

1) *Query*와 *Resp*를 통해 리더 r_j를 관찰하기 위해선 메시지에 포함된 r_j 고유의 식별 정보를 확인할 수 있어야한다. 그런데 *Query*와 *Resp*에는 리더 r_j를 식별할 수 있는 r_j만의 고유 정보가 포함되어 있지 않으며 r_j가 자신에게 오는 응답인지 식별하기 위해 사용하는 비밀 공유키 K_{ij}는 공격자에게는 랜덤수와 구별되지 않는다. 더욱이 K_{ij}는 태그의 비밀키 K_i값으로 암호화되어 있기 때문에 공격자는 *Query* 및 *Resp*를 통해 리더를 관찰할 수 없다.
2) *Query*와 *Resp*를 통해 태그 t_i를 관찰하기 위해선 1)과 마찬가지로 메시지에 포함된 공격 대상 태그 t_i의 유일한 식별자를 확인할 수 있어야 한다. 하지만 태그의 식별자 t_i는 자신의 비밀키 K_i로 암호화 되어 있기 때문에 t_i를 획득하기 위

해 공격자는 K_i를 계산할 수 있어야한다. 공격자가 비밀키 K_i를 전수 공격으로 알아내는 확률은 무시할 수 있으므로 공격자는 제시한 *Query* 및 *Resp*로부터 태그 및 리더를 관찰할 수 없다.

Lemma 7. 제안하는 서버 없는 *RFID* 검색 시스템은 단순 공격자 *SA*에 대해 리더 및 태그의 메시지 비연결성을 보장한다.

증명. 3.4절에 정의한 질의 및 응답의 연결성 게임을 수행하는 단순 공격자를 생각해보자. 공격자가 게임에서 승리하기위해선 *Challenger*가 제시한 *Query*, *Resp*와 연결성이 있는 *Query'*, *Resp'*을 게임 단계 1에서 획득한 $\Omega_I(T,R)$로부터 구분해 낼 수 있어야한다. 이 증명에서는 키의 갱신을 표현하기 위해 K_{ij}^p, K_{ij}^c, δ_{curr}^p, δ_{curr}^c의 표기법을 사용한다. K_{ij}^p는 이전 세션의 공유 비밀키로 K_{ij}^{p+1}, K_{ij}^{p+2}, ...을 거쳐 현재의 비밀키 K_{ij}^c가 된다. δ_{curr}^p는 세션 p에서의 타임스탬프 값을 δ_{curr}^c는 세션 c에서의 타임스탬프 값을 의미한다.

1) 세션 s_p에서 사용된 r_j의 t_i를 검색하기위한 질의문 *Query*가 $\{K_{ij}^p \| t_i\}_{K_i}$, $\{\delta_{curr}^p\}_{K_{ij}^p}$이라면, 세션 s_c ($c>p$)에서의 질의문 *Query'*는 $\{K_{ij}^c \| t_i\}_{K_i}, \{\delta_{curr}^c\}_{K_{ij}^c}$으로 나타낼 수 있다. 그런데 *Query*의 $\{\delta_{curr}^p\}_{K_{ij}^p}$에 포함된 타임스탬프 값($\delta_{curr}^p$)은 매 세션 갱신되는 값이다. 또한 $\{K_{ij}^p \| t_i\}_{K_i}$값은 태그의 비밀키 K_i로 암호화 되어 있으며 암호화되는 K_{ij}^p가 매 세션 갱신되기 때문에 K_i를 계산 할 수 없는 공격자는 이 값을 통해 메시지 연결성 여부를 확인할 수 없다. 따라서 공격자가 $\Omega_I(T,R)$에서 *Query*와 연결성이 있는 *Query'*을 올바르게 선택할 수 있는 확률은 무시할 수 있으며 따라서 오라클 Link(*Query*, *Query'*)가 1을 출력하는 확률도 무시할 수 있다.

2) 질의문과 마찬가지로 세션 s_p에서의 응답 *Resp*가 $\{\delta_{curr}^p \| K_{ij}^{p+1} \| \{K_{ij}^{p+1} \| t_i\}_{K_i}\}_{K_{ij}^p}$라 할때 s_c에서의 응답 *Resp'*은 $\{\delta_{curr}^c \| K_{ij}^{c+1} \| \{K_{ij}^{c+1} \| t_i\}_{K_i}\}_{K_{ij}^c}$으로 나타낼 수 있다. 이 두 응답의 연결성을 확인하기 위해서 공격자는 K_{ij}^p, K_{ij}^c와 K_i를 알 수 있어야 한다. 하지만 1)과 마찬가지로 K_{ij}^p, K_{ij}^c와 K_i를 알 수 없는 공격자가 $\Omega_I(T,R)$에서 *Resp*와 연결성이 있는 *Resp'* 올바르게 선택할 수 있는 확률은 무시할 수 있으며 따라서 오라클 Link(*Resp*, *Resp'*)가 1을 출력하는 확률도 무시할 수 있다.

1), 2)에 의해서 제안하는 서버 없는 RFID 검색 시스템은 공격자 SA에 대해 리더 및 태그의 메시지 비연결성을 보장한다.

정적 인증정보 기반 프로토콜인 제안하는 태그-리더간 검색 프로토콜 *SSP*는 Lemma 3에서 증명한 것처럼 태그 포획이 가능한 공격자에 대해 태그 비관찰성 및 비연결성을 보장하지 못한다. 즉 공격 대상 태그를 포획한 공격자는 태그의 과거 행적과 앞으로의 행적을 추적할 수 있어 해당 태그의 프라이버시를 침해할 수 있다. 같은 이유로 리더 포획이 가능한 공격자가 특정 리더를 포획하면 이후 해당 리더의 모든 행적을 추적할 수 있다. 하지만 제안하는 프로토콜은 공격자가 공격대상 리더를 포획하여도 해당 리더의 과거 행적을 추적할 수 없는 후방향 리더 프라이버시를 보장한다. 또한 공격자가 공격 대상 리더가 아닌 다른 리더를 포획하여도 확보한 메시지로부터 공격 대상 리더를 관찰하거나 연결할 수 없다.

Lemma 8. 제안하는 서버 없는 RFID 검색 시스템은 공격자 TRCA에 대해 태그 및 리더의 비관찰성을 보장한다.

증명. 3.4절에 정의한 질의 및 응답의 관찰성 게임을 수행하는 공격자 *TRCA*를 생각해보자. 공격자가 게임에서 승리하기위해선 *Challenger*가 제시한 *Query*와 *Resp*로부터 질의 대상 태그 t_i나 r_j를 유추할 수 있어야 한다.

1) *Query*와 *Resp*를 통해 리더 r_j를 관찰하기 위해선 메시지에 포함된 r_j 고유의 식별 정보를 확인할 수 있어야한다. 그런데 *Query*와 *Resp*에는 리더 r_j를 식별할 수 있는 r_j만의 고유 정보가 포함되어 있지 않으며 r_j가 자신에게 오는 응답인지 식별하기 위해 사용하는 비밀 공유키 K_{ij}는 공격자에게는 랜덤수와 구별되지 않는다. 더욱이 K_{ij}는 태그의 비밀키 K_i값으로 암호화되어 있기 때문에 공격자는 *Query* 및 *Resp*를 통해 리더를 관찰할 수 없다.

2) *Query*와 *Resp*를 통해 태그 t_i를 관찰하기 위해선 1)과 마찬가지로 메시지에 포함된 공격 대상 태그 t_i의 유일한 식별자를 확인할 수 있어야 한다. 하지만 태그의 식별자 t_i는 자신의 비밀키

K_i로 암호화 되어 있기 때문에 t_i를 획득하기 위해 공격자는 K_i를 계산할 수 있어야한다. 공격자가 비밀키 K_i를 전수 공격으로 알아내는 확률은 무시할 수 있으므로 공격자는 제시한 *Query* 및 *Resp*로부터 태그를 관찰할 수 없다.

3) *TRCA*가 게임 3-1 단계 2, 3에서 추가로 얻을 수 있는 정보는 공격대상 태그, 리더가 t_i, r_j일 때 다음과 같다.

- 단계 2: 태그 집합 $T'(T' \subset T,\ t_i \notin T')$ 에 있는 태그들의 아이디와 비밀키, 타임스탬프값
  $t_y \in T'$일 때 t_y에 대해 아이디 t_y, 비밀키 K_y , 타임스탬프 δ_{last}
- 단계 3: 리더 집합 $R'(R' \subset R,\ r_j \notin R')$ 에 있는 리더들의 비밀키, 인증 정보
  $r_x \in R'$일 때 r_x의 비밀키 K_{ix}, 태그 비밀키 K_i로 암호화된 태그 인증정보, 태그 아이디
  , $L_x = \begin{bmatrix} K_{1x}, \{K_{1x} \| t_1\}_{K_1}, t_1 \\ K_{2x}, \{K_{2x} \| t_2\}_{K_2}, t_2 \\ \vdots \\ K_{ix}, \{K_{ix} \| t_i\}_{K_i}, t_i \end{bmatrix}$

위 단계 2, 3에서의 획득한 정보에는 K_{ij}, K_i가 포함되어 있지 않으며, 확보한 다수의 암호문들은 Assumption 1에 의하여 K_{ij}, K_i를 계산해야하는 공격자에게 아무런 이득이 되지 않는다. 전수 공격을 통해 K_{ij}, K_i를 계산하는 확률은 무시할 수 있으므로 *TRCA*는 제시한 *Query*와 *Resp*에서 t_i나 r_j를 계산해 낼 수 없다.

1), 2), 3)에 의해서 제안하는 서버 없는 *RFID* 검색 시스템은 공격자 *TRCA*에 대해 태그 및 리더의 비관찰성을 보장한다.

Lemma 9. 제안하는 서버 없는 *RFID* 검색 시스템은 공격자 *TRCA*에 대해 리더 및 태그의 메시지 비연결성을 보장한다.

증명. 3.4절에 정의한 질의 및 응답의 연결성 게임을 수행하는 공격자 *TRCA*를 생각해보자. 공격자가 게임에서 승리하기위해선 *Challenger*가 제시한 *Query*, *Resp*와 연결성이 있는 *Query'*, *Resp'*을 게임 단계 1에서 획득한 $\Omega_I(T,R)$로부터 구분해 낼 수 있어야한다. Lemma 7의 단순 공격자 SA에 비해 공격자 TRCA가 추가로 얻을 수 있는 정보는 다음과 같다.

- 단계 3: 태그 집합 $T'(T' \subset T,\ t_i \notin T')$ 에 있는 태그들의 아이디와 비밀키, 타임스탬프값
  $t_y \in T'$일 때 t_y에 대해 아이디 t_y, 비밀키 K_y , 타임스탬프 δ_{last}
- 단계 4: 리더 집합 $R'(R' \subset R,\ r_j \notin R')$ 에 있는 리더들의 비밀키, 인증 정보
  $r_x \in R'$일 때 r_x의 비밀키 K_{ix}, 태그 비밀키 K_i로 암호화된 태그 인증정보, 태그 아이디
  , $L_x = \begin{bmatrix} K_{1x}, \{K_{1x} \| t_1\}_{K_1}, t_1 \\ K_{2x}, \{K_{2x} \| t_2\}_{K_2}, t_2 \\ \vdots \\ K_{ix}, \{K_{ix} \| t_i\}_{K_i}, t_i \end{bmatrix}$

Lemma 7의 1), 2)와 같이 공격자 *TRCA*가 *Query'*, *Resp'*를 구분하기 위해서는 K_i, K_{ij}와 K_{ij}의 갱신된 키 K_{ij}'을 계산할 수 있어야한다. 위 단계 3, 4에서의 획득한 정보에는 K_i, K_{ij}, K_{ij}'가 포함되어 있지 않으며, 확보한 다수의 암호문들은 Assumption 1에 의하여 K_i, K_{ij}와 K_{ij}'를 계산해야하는 공격자에게 아무런 이득이 되지 않는다. 또한 전수 공격을 통해 이 값들을 계산하는 확률은 무시할 수 있다. 따라서 *TRCA*는 제시한 *Query*와 *Resp*와 연결성이 있는 *Query'*, *Resp'*를 선택할 확률은 무시할 수 있으며 *Challenger*의 오라클 Link(*Query*, *Query'*), Link(*Resp*, *Resp'*) 호출은 1을 출력하지 않는다.

그러므로 제안하는 서버 없는 RFID 검색 시스템은 공격자 TRCA에 대해 리더 및 태그의 메시지 비연결성을 보장한다.

Lemma 10. 제안하는 서버 없는 *RFID* 검색 시스템은 공격자 T*R*CA에 대해 리더의 후방향 비연결성을 보장한다.

증명. 3.4절에 정의한 질의 및 응답의 연결성 게임을 수행하는 공격자 *T*R*CA*를 생각해보자. 공격자가 게임에서 승리하기위해선 *Challenger*가 제시한 *Query*, *Resp*와 연결성이 있는 *Query'*, *Resp'*을 게임 단계 1에서 획득한 $\Omega_I(T,R)$로부터 구분해 낼 수 있어야한다. 공격자 *T*R*CA*가 공격 대상 리더 r_j를 포획하여 인증 정보 리스트 L_j를 확보하였다고 가정하자. L_j에는 t_i와 r_j간의 비밀키 K_{ij}, t_i의 비밀키로 암호화된 인증정보 $\{K_{ij} \| t_i\}_{K_i}$ 그리고 태그의 식별자 t_i가 포함되어 있다.

1) r_j가 포획된 현재 세션 s_c에서 사용된 r_j의 t_i를 검색하기위한 질의문 *Query*가 $\{K_{ij}^c \| t_i\}_{K_i}$, $\{\delta_{curr}^c\}_{K_0^c}$이라면, 세션 $s_p (p<c)$에서의 질의문

*Query'*는 $\{K_{ij}^p \| t_i\}_{K_i}, \{\delta_{curr}^p\}_{K_0^p}$으로 나타낼 수 있다. 공격자는 리더 포획을 통해 세션 s_c에서의 비밀키 K_{ij}^c를 확보하였지만 세션 s_p에서 사용된 비밀키 K_{ij}^p는 알지 못한다. K_{ij}^p는 t_i가 임의로 생성한 값이기 때문에 공격자가 K_{ij}^c를 알고 있다고 계산할 수 있는 값이 아니다. 따라서 공격자는 메시지 $\{\delta_{curr}^c\}_{K_0^c}$와 $\{\delta_{curr}^p\}_{K_0^p}$로부터 연결성을 확인할 수 없다. 또한 $\{K_{ij}^c \| t_i\}_{K_i}$값은 태그의 비밀키 K_i로 암호화 되어 있으며 암호화되는 공유 비밀 키가 매 세션 갱신되기 때문에 K_i를 계산할 수 없는 공격자는 이 값을 통해 메시지 연결성 여부를 확인할 수 없다. 하지만 세션 s_c 이후 갱신되는 키 K_{ij}^{c+1}, K_{ij}^{c+2} 등은 K_{ij}^c를 이용하여 전달되기 때문에 K_{ij}^c를 알고 있는 공격자는 포획 시점 이후의 모든 메시지에 대해 연결성을 확인할 수 있다.

2) 세션 s_p와 s_c에서의 응답을 각각 *Resp*와 *Resp'*라고 할 때 이들 값은 서로 다른 비밀키 K_{ij}^c, K_{ij}^p,를 이용하여 생성된 값이다. 즉 세션 s_c에서의 응답 *Resp*가 $\{\delta_{curr} \| K_{ij}^{c+1} \| \{K_{ij}^{c+1} \| t_i\}_{K_i}\}_{K_0^c}$ 라고하면 세션 s_p에서의 응답 *Resp'*는 $\{\delta_{curr}^p \| K_{ij}^{p+1} \| \{K_{ij}^{p+1} \| t_i\}_{K_i}\}_{K_0^p}$이라 정의할 수 있다. 그러므로 K_{ij}^p, K_{ij}^c와 K_i를 알 수 없는 공격자가 $\Omega_I(T,R)$에서 *Resp*와 연결성이 있는 *Resp'* 올바르게 선택할 수 있는 확률은 무시할 수 있으며, 따라서 오라클 Link(*Resp*, *Resp'*)가 1을 출력하는 확률도 무시할 수 있다.

1), 2)에 의해서 제안하는 서버 없는 RFID 검색 시스템은 공격자 *T*R*CA*에 대해 리더의 후방향 비연결성을 보장한다.

〔표 5〕는 관련 연구 및 제안하는 프로토콜의 안전성 및 연산 효율성을 보여준다. 공격자는 리더 및 태그의 포획이 가능한 공격자와 포획이 능력이 없는 단순 공격자로 분류하였으며 리더 및 태그의 포획이 가능한 공격자는 공격 유형에 따라 공격 대상 개체를 직접 포획하는 공격자와 공격 대상 개체와 관련 있는 주변 개체를 포획하는 공격자로 다시 분류한다. 주변 개체의 포획이 가능한 공격자는 공격 대상 태그를 검색할 수 있는 리더를 포획할 수 있는 공격자를 의미하며 3.2절에서 언급한 것처럼 시스템에 등록된 리더가 공격자가 되어 다른 리더 및 태그의 프라이버시를 침해하려는 경우를 나타낸다. 공격 대상 개체의 포획이 가능한 공격자는 해당 개체를 포획하여 과거 행적과 앞으로의 행적을 추적하기 위함으로 태그 위조 및 리더 위조의 경우 언제든지 가능하기 때문에 분석에서 제외한다. 각 프로토콜의 분석 4장 사례 연구에서 분석했기 때문에 자세한 설명은 생략한다. Ahamed 등의 프로토콜은 동적 인증 정보 기반의 프로토콜로서 단일 리더, 단일 태그 환경이기 때문에 주변 개체의 포획의 경우를 분석할 수 없다. 표 5에서 확인 할 수 있는 것처럼 제안하는 프로토콜의 경우 공격자 *TRCA*, *SA*에 대해 3장에서 정의한 4가지 보안 요구사항을 모두 만족하며 공격자 *T*R*CA*에 대해 리더의 후방향 위치 추적에 대한 안전성을 보장한다.

연산량 측면에서 제안하는 프로토콜은 태그가 4번, 리더가 3번의 AES 암호화가 필요로 한다. Tan 등의

〔표 5〕 관련 연구 및 제안하는 프로토콜의 안전성 및 효율성 비교.

프로토콜	리더 및 태그의 포획이 가능한 공격자 (*TRCA*, *T*R*CA*)										단순 공격자 (SA)				연산량	
	*T*R*CA*				*TRCA*											
	Req. 3		Req. 4		Req. 3		Req. 4		Req. 1	Req. 2	Req. 3	Req. 4	Req. 1	Req. 2	태그	리더
	후방	전방	후방	전방	후방	전방	후방	전방								
Tan 등[1]	X	X	X	X	O	O	X	X	X	X	O	X	O	X	3H+R	2H+R
Ahamed 등[5]	O	X	O	X	·	·	·	·	·	·	O	O	O	O	*4H*	3H
Won 등[6]	X	X	X	X	X	X	X	X	X	O	O	O	O	O	*4A+R*	3A
제안하는 프로토콜	X	X	O	X	O	O	O	O	O	O	O	O	O	O	*4A*	3A
H: 일방향 해쉬 연산 비용, A: AES 암호화 비용, R: 랜덤수 생성 비용																

프로토콜에서 태그가 3번의 해쉬 연산만을 필요로 하지만 해쉬 연산이 암호화 연산보다 더 비싼 연산이며 랜덤수를 생성하는 비용을 한 번의 해쉬 연산 비용과 동일하다고 간주하면 연산량 측면에서도 제안하는 프로토콜이 가장 효율적이다.

VII. 결 론

본 논문에서는 온라인 서버와 연결없이 이동형 리더가 스스로 태그를 인증하고 검색하는 서버없는 검색 시스템을 제안하였다. 제안하는 서버없는 검색 프로토콜은 2장에서 정의한 정의 3의 효율적인 검색 프로토콜로서 질의 대상이 되는 목적 태그만 리더의 질의에 응답하면서도 3장에서 정의한 모든 보안 요구사항을 만족한다. 기 제안된 서버없는 검색 프로토콜들이 같은 태그에 대한 여러 리더들의 질의가 서로 구분되게 하기 위해 태그 인증정보에 개별 리더의 식별자를 포함시켰으나 이는 리더의 프라이버시를 침해하는 중요한 요인이 된다. 제안하는 프로토콜은 질의 및 응답에 태그와 리더의 식별자를 사용하지 않아 리더 및 태그 메시지의 비관찰성과 비연결성을 보장한다. 또한 리더가 유지하는 태그 인증정보를 매 세션마다 갱신하기 때문에 공격자에 대해 후방향 위치추적 안전성을 보장한다. 리더의 유효한 질의는 태그의 비밀키를 이용해 생성해야하고 질의문 확인과정에서 획득한 리더-태그 간 공유 비밀키를 이용해 응답이 생성되어야 하기 때문에 리더 및 태그 위조 공격에도 강건하다. 본 논문의 안전성 분석에서는 RFID 검색 프로토콜을 위한 새로운 공격자 모델을 제안하였고 이를 이용하여 RFID 검색 시스템 및 제안하는 프로토콜의 안전성을 분석하였다.

참 고 문 헌

[1] C.C. Tan, B. Sheng, and Q. Li, "Secure and Serverless RFID Authentication and Search Protocols," IEEE Transactions on Wireless Communications, vol. 7, no. 3, pp. 1400-1407, Apr. 2008.

[2] A. Bogdanov, G. Leander, C. Paar, and A. Poschmann, "Hash Functions and RFID Tags: Mind the Gap," Proc. of the CHES08, LNCS 5154, pp. 283-299, 2008.

[3] A. Juels and S.A. Weis, "Authenticating Pervasive Devices with Human Protocols," Proc. of the CRYPTO05, LNCS 3126, pp. 293-308, 2005.

[4] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," Proc. of the CHES04, LNCS 3156, pp. 85-140, 2004.

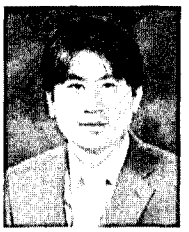
[5] S.I. Ahamed, F. Rahman, E. Hoque, F. Kawsar, and T. Nakajima, "S3PR: Secure Serverless Search Protocols for RFID," Proc. of the ISA08, pp. 187-192, Apr. 2008.

[6] T. Won, J. Chun, and D. Lee, "Strong Authentication Protocol for Secure RFID Tag Search Without Help of Central Database," Proc. of the EUC, pp. 153-158, Dec. 2008.

[7] 임지환, 오희국, 양대헌, 이문규, 김상진, "강화된 사용자 프라이버시를 보장하는 효율적인 RFID 검색 프로토콜," 정보처리학회논문지, 16-C(3), pp. 347-356, 2009년 6월.

〈著者紹介〉

임 지 환 (Jihwan Lim) 학생회원
2005년 2월: 한양대학교 전자컴퓨터공학부(학사)
2007년 2월: 한양대학교 컴퓨터공학과(석사)
2007년 3월~현재: 한양대학교 컴퓨터공학과 (박사과정)
〈관심분야〉 네트워크 보안
URL: http://infosec.hanyang.ac.kr/jhlim/



김 상 진 (Sangjin Kim) 종신회원
1995년 2월: 한양대학교 전자계산학과(학사)
1997년 2월: 한양대학교 전자계산학과(석사)
2002년 8월: 한양대학교 전자계산학과(박사)
2003년 3월~현재: 한국기술교육대학교 인터넷미디어공학부 부교수
〈관심분야〉 암호기술 응용
URL: http://infosec.kut.ac.kr/sangjin/

오 희 국 (Heekuck Oh) 종신회원
1983년: 한양대학교 전자공학과(학사)
1989년: 아이오와주립대학 전자계산학과(석사)
1992년: 아이오와주립대학 전자계산학과(박사)
1993년~1994년: 한국전자통신연구원 선임연구원
1995년 3월~현재: 한양대학교 컴퓨터공학과 교수
〈관심분야〉 암호프로토콜, 네트워크 보안
URL: http://infosec.hanyang.ac.kr/~hkoh/