情報保護學會論文誌
第 21 卷 第 1 號, 2011. 2

모바일 리더의 태그 리스트 재사용을 방지하는 저비용 RFID 태그 검색 프로토콜*

여 돈 구,† 이 상 래, 최 현 우, 장 재 훈, 염 흥 열‡
순천향대학교

A Low-Cost RFID Tag Search Protocol Preventing the Reuse of Mobile Reader's Tag-List*

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

요 약

모바일 환경의 RFID 시스템에서는 백엔드 서버와 리더의 실시간 통신을 보장할 수 없으므로, 리더는 백엔드 서버와 통신이 불가능한 상황에서도 검색하고자 하는 특정 태그를 정확히 검색할 수 있는 능력을 보장할 수 있어야 한다. 모바일 리더 기반의 태그 검색 프로토콜에 대한 최근 연구들은 태그 및 리더의 프라이버시 문제를 다루고 있지만, 리더가 기존에 소유하던 태그 리스트의 재활용함으로써 발생할 수 있는 문제점은 고려하지 않고 있다. 다시 말해, 특정 태그에 대한 권한이 삭제된 리더가 기존에 소지하던 태그 리스트를 재활용함으로써 권한이 삭제된 태그를 검색할 수 있는 문제가 발생할 수 있다. 제안하는 프로토콜은 태그 리스트의 재활용을 방지함으로써 보안성이 향상된 태그 리스트를 제공하고, 모바일 리더 기반의 RFID 환경에 적합한 동적 ID 기반의 효율적인 태그 검색 프로토콜을 제공한다.

ABSTRACT

When a real-time data transfer is not possible between a reader and a back-end server in the mobile environment, the reader should support a capability to search a certain tag without communicating with a back-end server. Some recent papers related to the mobile reader-based tag search protocol have addressed privacy concerns for the reader and the tags. However, to our best knowledge, there are no papers addressing the problem arising from reusing tag lists existed in the mobile reader. In other words, there arise a problem that a mobile reader which has lost an right to access to a specific tag is able to search that tag by reusing a tag list for searching a particular tag. If mobile reader having an unauthorized tag list, the mobile reader can reuse a particular tag list. Our protocol provides the enhanced secure tag lists preventing the reuse of the tag lists and an efficient tag search protocol based on dynamic identity in the mobile reader-based RFID environments.

Keywords: RFID Tag Search Protocol, XOR Chain-based Tag-list

접수일(2010년 11월 29일), 게재확정일(2011년 1월 13일)
*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

최근 일상에서 자유롭게 정보통신 기술을 이용하는 유비쿼터스 환경이 다양하게 구성되고 있다. 이러한 유비쿼터스 환경을 구성하는 기술 중 USN/RFID 기술이 많은 관심을 받고 있다. 최근 연구들은 RFID와 관련된 다양한 취약성 및 프라이버시 문제를 제기하고 있으며, 리더와 태그 간의 안전한 통신 및 프라이버시 보호를 위한 RFID 인증 프로토콜과 태그 검색 프로토콜에 대한 연구가 활발하게 진행되고 있다.

RFID 태그 검색 프로토콜은 리더 소유자가 찾고자하는 특정 태그의 위치를 판별하는데 사용된다. 최근 모바일 환경에서 이동형 리더 기반의 태그 검색 프로토콜들에 대한 연구가 진행되고 있다. 모바일 환경에서는 백엔드 서버와 리더의 실시간 통신을 보장할 수 없으므로, 리더는 백엔드 서버와 독립된 상황에서 검색하고자 하는 태그를 정확히 검색할 수 있는 능력을 보장할 수 있어야 한다. 기존의 유선환경의 RFID 인증 시스템에서는 주로 태그의 프라이버시 문제가 거론되었지만, 모바일 환경의 RFID 검색 시스템에서는 태그의 프라이버시는 물론 모바일 리더에 대한 프라이버시 문제 또한 해결해야 한다.

최근 연구되고 있는 이동형 리더 기반의 태그 검색 프로토콜[1-4]에서는 태그 및 리더의 프라이버시 문제를 고려하고 있지만, 리더가 기존에 소유하던 태그 리스트의 재활용문제는 고려하지 않고 있다. 즉, 특정 태그에 대한 검색 권한이 삭제되었음에도 기존에 소유하던 태그 리스트를 재활용함으로써 권한이 삭제된 태그를 검색할 수 있는 문제가 발생할 수 있다. 본 논문에서는 동적 ID 기반의 모바일 RFID 시스템 환경에서 유연한 리더 권한 관리가 가능하고 효율적인 RFID 태그 검색 프로토콜을 제안하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서 사전 연구로 기존 이동형 리더 기반의 RFID 태그 검색 프로토콜에 대한 보안 요구사항을 정의한다. 3장에서 이동형 리더의 RFID 태그 검색 프로토콜에서 발생할 수 있는 공격자 모델을 정의하고, 기존 연구가 보안 요구사항을 만족하지 못함을 보인다. 4장에서는 제안하는 이동형 리더 기반의 RFID 태그 검색 프로토콜을 기술하고, 보안 요구사항을 만족함을 보인다. 이후 5장에서 기존 프로토콜과의 안전성 및 효율성 분석을 통해 제안하는 프로토콜의 우수성을 확인 한 후 6장에서 결론을 맺는다.

II. 시스템 구성 및 보안 요구사항

초기 RFID 시스템은 백엔드 서버, 리더, 태그로 나누어지며 백엔드 서버와 리더는 유선구간으로 구성된다. 즉, 백엔드 서버와 리더 사이의 구간을 안전한 채널로 가정함으로써 정당한 리더만이 백엔드 서버로 접속할 수 있다. 유선 RFID 기반 환경에서도 보안성 향상 및 태그 인증 연산의 효율성을 증가시키기 위해 동적 ID 기반 RFID 상호 인증 프로토콜에 대한 연구가 활발히 진행되고 있다[5,6].

최근 스마트폰 및 모바일 기기의 보급이 일반화되면서 무선 환경에서의 이동형 리더에 대한 연구가 지속되고 있다. 사용자는 RFID 리더칩이 내장된 휴대용 단말을 이용하여 사물에 부착된 태그를 읽고, 태그의 정보를 검색할 수 있다[4]. 이동형 리더의 검색 기능을 지원하기 위해서는 일반적으로 백엔드 서버가 없는 독립된 환경에서 리더 소지자가 이동하면서 태그를 검색할 수 있어야 한다. 리더 소지자는 태그 검색 이전에 백엔드 서버로부터 리더 소지자의 권한에 따라 할당된 태그 리스트를 할당 받아야 한다.

본 논문에서 제안하는 태그 검색 프로토콜은 관련 연구[6]의 인증 방식을 고려하여, 리더 ID 갱신 방식을 이용한다고 가정한다.

2.1 시스템 구성 정의

백엔드 서버는 정당한 리더 및 태그의 정보를 저장하고 있으며, 이동형 리더가 독립적으로 태그를 검색할 수 있도록 리더 및 태그의 정보를 이용하여 태그 리스트를 생성한다. 백엔드 서버는 정당한 이동형 리더에게 태그 리스트 정보를 안전한 채널을 이용하여 전달한다. 백엔드 서버의 데이터베이스의 정보는 유효한 것으로 가정하므로, 이동형 리더에게 전달되는 태그 리스트 또한 유효한 정보로 가정한다. 이동형 리더는 태그 검색 이전에 백엔드 서버로부터 이동형 리더의 권한에 맞는 태그 리스트를 수신 받아야 한다. 정당한 이동형 리더는 수신 받은 태그 리스트의 정보를 이용하여 검색하고자 하는 특정 태그를 찾기 위해 쿼리를 브로드캐스트한다. 태그는 이동형 리더로부터 전달받은 쿼리 정보를 이용하여 응답 메시지를 생성하고, 그 결과를 이동형 리더에게 전달한다.

정의1. 서버 독립적인 RFID 검색 시스템의 구성.

- 태그 집합 $T=(Id_{T1},K_{T1}),(Id_{T2},K_{T2}),\ldots,(Id_{Tn},K_{Tn})$

: 백엔드 서버에 등록된 태그 집합으로 각 태그는 Id_T와 K_T를 저장한다.

• 리더 집합 $R=\{Id_{R1}, Id_{R2}, ..., Id_{Rn}\}$: 백엔드 서버에 등록된 이동형 리더 집합으로 각 리더는 리더의 동적ID XId_R, 리더의 태그 리스트 인증키 $LKId_R$, 리더의 태그리스트 LId_R를 저장한다.

• 리더의 태그 리스트 $LId_R=\{LId_{T1}, LId_{T2}, ..., LId_{Tn}\}$: 이동형 리더 Id_R의 권한에 해당하는 태그 리스트 LId_T로 이루어진 집합

• 리더의 태그 리스트 인증키 $LKId_R = h(Id_{T1}\|K_{T1})\oplus h(Id_{T2}\|K_{T2})\oplus ...\oplus h(Id_{Tn}\|K_{Tn})$: 리더 Id_R의 권한에 해당하는 태그의 정보로 계산된 128bit의 키 정보

• 태그 리스트 정보 $LId_{Tn} = LKId_R\oplus h(Id_{Tn}\|K_{Tn})\oplus XId_{Rn}$: 리더 Id_R의 태그 리스트 인증키값 $LKId_R$, 검색하려는 태그의 정보 $h(Id_{Tn}\|K_{Tn})$, 리더의 현 세션의 ID XId_R의 XOR 연산에 의해 계산된 128bit의 정보

• 백엔드 서버 B : RFID 시스템 내의 정당한 리더 및 태그의 정보를 저장하고 있는 데이터베이스로서 이동형 리더 Id_R의 권한에 해당하는 태그 리스트 LId_R를 발급한다.

정의2. 비동기화 방지 대책 : 동적 ID 방식의 RFID 시스템에서 XId_R 정보 갱신시, 갱신 정보 메시지 손실로 인한 비동기화가 발생하지 않아야 한다. 본 논문에서는 관련연구[6]에서와 같이 인증 프로토콜이 정상 종료될 경우에 백엔드 서버에 의해 리더 ID XId_R 정보가 갱신된다고 가정한다. 즉, 백엔드 서버와 리더 간의 인증이 이루어지지 않은 경우에는 동일한 XId_R를 이용하게 된다.

2.2 모바일 기반 태그 검색 프로토콜 보안 요구사항

백엔드 서버와 독립된 모바일 환경의 RFID 태그 검색 프로토콜은 다음의 요구사항을 만족해야 한다.

• 요구사항1. 태그 위조에 대한 안전성[4] : 이동형 리더가 특정 태그의 검색을 요청할 경우, 정당한 태그 외의 어떠한 개체도 유효한 응답을 만들 수 없어야 한다.

• 요구사항2. 리더 위조에 대한 안전성[4] : 이동형 리더가 특정 태그의 검색을 요청할 경우, 정당한 태그 리스트와 인증키를 소유하지 않은 개체는 유효한 쿼리를 만들 수 없어야 한다.

• 요구사항3. 태그 및 리더 프라이버시 노출에 대한 안전성[4] : 리더의 쿼리 및 태그의 메시지로부터 통신에 참여하였던 각 개체를 구분할 수 없어야 한다. 태그의 위치추적(요구사항3-1) 및 리더의 위치추적(요구사항3-2), 후방향 위치추적(요구사항3-3)과 전방향 위치추적(요구사항3-4)에 안전해야 한다.

• 요구사항4. (동적 ID 방식의 경우)비동기화 발생에 대한 안전성 : 동기화 방식의 RFID 검색 프로토콜에서 키 갱신이 이루어지는 경우, 검색 프로토콜 상의 메시지가 차단되어도 키 갱신이 성공적으로 이루어져야 한다.

III. 기존 연구

본 장에서는 모바일 기반 RFID 태그 검색 시스템에서 발생할 수 있는 공격자 시나리오를 정의하고, 기존 연구들의 안전성 분석을 실시한다.

3.1 공격 시나리오 정의

• 요구사항1에 대한 공격 시나리오 : 공격자는 태그 위조 공격을 통하여 자신이 리더가 찾고자 하는 정당한 태그인 것처럼 응답 메시지를 조작할 수 있다.

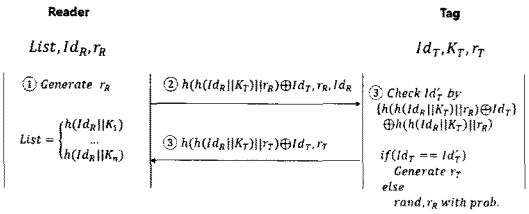
• 요구사항2에 대한 공격 시나리오 : 공격자는 리더 위조 공격을 통하여 자신이 원하는 특정 태그를 검색하기 위해 정당한 리더인 것처럼 요청 메시지를 조작할 수 있다.

• 요구사항3에 대한 공격 시나리오 : 공격자는 리더의 요청 메시지 및 태그의 응답 메시지를 지속적으로 도청하고, 그 결과를 분석하거나 습득한 메시지를 재사용할 경우, 상황에 따라 태그의 위치추적(요구사항3-1), 리더의 위치추적(요구사항3-2), 후방향 위치추적(요구사항3-3) 및 전방향 위치추적(요구사항3-4)이 가능하다.

• 요구사항4에 대한 공격자 시나리오 : 동적 ID 기반의 RFID 검색 시스템에서 통신에 참여한 개체의 갱신정보가 전달 도중에 차단 혹은 공격자에 의해 고의적으로 변조된 경우, 통신에 참여한 개체간의 비동기화가 발생할 수 있다.

3.2 기존 연구에 대한 시나리오 분석

• Tan의 태그 검색 프로토콜[1] : Tan의 논문은 고정 ID 방식 기반의 RFID 태그 검색 프로토콜이다.

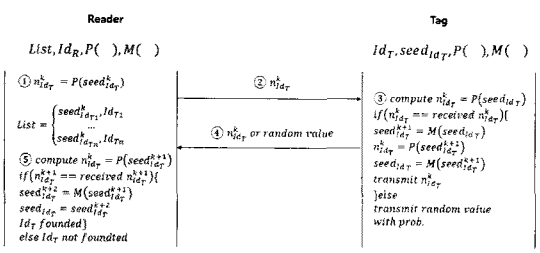


〔그림 1〕 Tan의 3차 태그 검색 프로토콜

이 논문에서는 백엔드 서버에서 리더의 Id_R와 태그의 K_T를 저장하고 있다가 안전한 채널을 통해 리더에게 전달한다. 권한에 맞는 리스트를 수신한 Id_R는 자신이 검색하고 싶은 태그 Id_T의 리스트 정보 $h(Id_R||K_T)$와 리더의 랜덤값 Id_R 정보를 이용해 요청 메시지 ②를 생성한다. 태그는 메시지 ②의 정보와 자신이 소유한 정보 Id_T, K_T를 이용하여 리더가 자신의 Id_T정보를 알고 있는지 확인한다. 태그는 리더가 소지한 Id_T정보가 자신의 Id_T와 일치할 경우에만 메시지 ③을 전송하고, 불일치할 경우, 특정 확률에 따라 랜덤값을 생성하여 전달한다.

본 프로토콜은 리더의 태그 리스트가 노출되지 않고 해쉬 연산의 충돌이 없다고 가정한다면, 리더의 Id_R이 노출되므로 리더의 위치추적이 가능하다. 또한, 응답 메시지 ③가 매번 변경되지만 Id_T가 불일치할 경우 태그는 확률에 따라 반응하므로, 공격자가 메시지 ②를 재사용하는 하는 시점에 공격자 주변에 태그 수가 적을 경우 공격에 성공할 수도 있다. 그러므로 요구사항2 및 요구사항3-2을 만족하지 못하며, 리더의 Id_R를 수집하는 경우 요구사항3-3 및 요구사항3-4를 만족하지 못한다.

• Ahamed의 태그 검색 프로토콜[2] : Ahamed의 논문은 동적 ID 방식 기반의 RFID 태그 검색 프로토콜이다. 이 논문에서는 시드값을 의사난수 함수를 이용하여 갱신한다. 과정 ②~④에서 리더가 전달한 시드값을 태그가 확인하고, 동일할 경우에 시드값을 증가하여 리더에게 전달한다. 과정 ⑤에서 리더는 자신의 시드값을 1증가하여 태그가 전달한 시드값과 비교한 후, 시드값이 증가한 경우에 해당 태그를 찾은 것으로 간주한다.

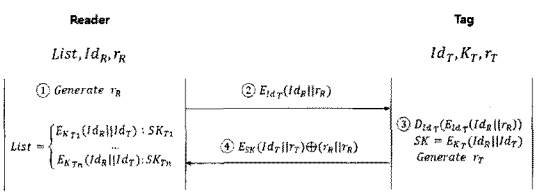


〔그림 2〕 Ahamed의 태그 검색 프로토콜

본 프로토콜은 리더의 태그 리스트가 노출되지 않고 의사난수 생성에 충돌이 없다고 가정한다면, 공격자는 시드값만 노출되므로 요구사항2와 요구사항3을 만족한다고 볼 수 있다. 하지만, 태그로 가장한 공격자가 리더의 전달 메시지 ②의 시드값을 고의로 증가시켜 전달할 수 있으므로 요구사항1을 만족하지 못 한다. 또한, 태그 측에서 시드값을 갱신하여 전달하므로, 메시지 ④가 공격자에 의해 고의적인 갱신되거나 정당한 태그의 응답 메시지가 리더로 전달되지 못하는 경우 비동기화가 발생하게 되므로 요구사항4를 만족하지 못한다.

• 천지영의 태그 검색 프로토콜[3] : 천지영의 논문은 수동형 태그에 적합하게 개발된 AES-128[7] 암호 알고리즘을 사용한다. 제안하는 논문의 태그 리스트 정보는 리더의 Id_R과 Id_T를 연접하여 태그의 비밀키 K_T로 암호화되어 생성된다. 과정 ①~②에서 리더는 검색하고자 하는 리더의 Id_R와 랜덤값 r_R정보를 태그의 Id_T로 암호화하여 전달한다. 과정 태그는 수신한 정보를 자신의 Id_T를 이용하여 복호화 한다. 이후 Id_R과 Id_T정보를 K_T로 암호화하여 메시지 ④에 사용할 암호화 키 SK를 생성한다. 이후 SK를 이용하여 Id_T와 r_R을 암호화하고 $r_R||r_R$을 XOR 연산하여 전달한다.

본 프로토콜에서 리더는 백엔드 서버로부터 Id_T에 해당하는 SK를 사전에 전달 받는다. 리더의 태그 리스트가 노출되지 않는다고 가정하면, 전달되는 메시지 ②와 ④의 위/변조가 불가능하므로 요구사항1, 요구사항2 및 요구사항3을 만족한다고 볼 수 있다. 반면, 메시지 ④의 값 생성시 메시지 ②의 정보와 고정된 태그의 값만 이용되므로 메시지 ④값은 메시지 ②에 의존하게 된다. 공격자는 도청을 통해 메시지 ②의 값을 재사용할 수 있지만, 모든 태그가 동일한 방식 ③~④

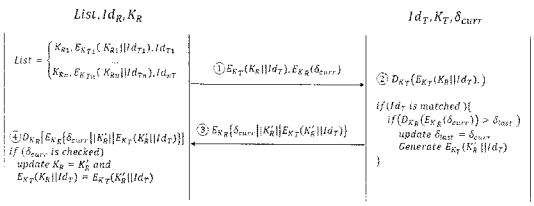


〔그림 3〕 천지영의 태그 검색 프로토콜

을 통해 응답하므로 어떤 태그를 찾고자 하는지 알 수 없게 된다.

• 임지환의 태그 검색 프로토콜[4] : 임지환의 동적 ID 기반 태그 검색 프로토콜 또한 수동형 태그에 적합하게 개발된 AES-128 암호 알고리즘을 사용한다. 한 가지 특징은 메시지의 최신성을 확인하기 위해 타임스탬프 값(δ)를 사용한다는 점이다. 그러므로 리더와 태그는 각각 타임스탬프 값을 추가로 저장해야 한다. 리더는 백엔드 서버로부터 K_R, $E_{K_T}(K_R \| Id_T)$, Id_T 정보로 이루어진 태그 리스트를 수신 받는다. 과정 ①에서 검색하고자 하는 태그의 정보와 함께 암호화된 현재 타임스탬프 값을 태그에게 전달한다. 과정 ②에서 태그는 수신한 태그 정보를 복호화하여 정보가 일치하는 경우에만 타임스탬프 값을 비교하여 메시지의 재전송 여부를 확인한다. 메시지의 최신성이 확인되면 타임스탬프 값을 및 다음번에 사용할 태그 정보를 갱신하고 과정 ③에서 갱신된 정보를 암호화 하여 전달한다. 과정 ④에서 이를 수신한 리더는 메시지를 복호화하고 메시지의 최신성을 확인한 이후 다음번에 사용될 리스트 정보를 갱신한다.

본 프로토콜의 메시지 ①이 태그의 비밀키로 암호화되어 전송되므로 태그 리스트 정보와 암호화 키가 노출되지 않는다고 가정한다면 요구사항2는 만족한다. 또한, 메시지 ①의 K_R이 세션 마다 갱신되며 갱신된 값이 응답 메시지 생성에 사용되므로 요청 및 응답 메시지 분석을 통한 추적이 불가능하므로 요구사항 3-1, 요구사항3-2 및 요구사항3-3을 만족한다고 볼 수 있다. 하지만, 본 프로토콜에서는 하나의 태그만 반응하므로 리더가 전송한 메시지 ①을 도청한 공격자가 다른 지역에서 대상 리더를 찾아낸다면 태그의 정보가 갱신되므로 정당한 사용자는 태그를 찾을 수 없다. 그러므로 요구사항3-4를 만족한다고 볼 수 없다. 또한, 과정 ②에서 태그가 다음 세션의 비밀정보를 갱신한 이후에 메시지 ③을 전달하므로 메시지 ③이 공격자에 의해 고의적인 갱신되거나 정당한 태그의 응답 메시지가 리더로 전달되지 못하는 경우 비동기화가 발생하므로 요구사항4를 만족하지 못한다.



〔그림 4〕 임지환의 태그 검색 프로토콜

IV. 제안하는 태그 검색 프로토콜

이번 장에서는 모바일 환경에 적합한 동적 ID기반 RFID 태그 검색 프로토콜을 소개하고, 2.2절에서 제안한 보안요구사항을 만족함을 보인다.

4.1 보안성이 강화된 태그 리스트 제안

최근 연구된 RFID 태그 검색 프로토콜[1-4]에서 사용되는 태그 리스트 정보는 리더 및 태그의 비밀정보로 이루어진다. 정적 ID 기반의 경우, 리더 혹은 태그의 고정된 ID 정보와 킷값에 의해 생성되거나 고정된 대칭키 기반의 암호화키를 이용한다. 이와 같이 고정된 값을 이용하는 경우, 랜덤값을 생성하여 전달되는 메시지를 변경함으로써 위치 추적 공격을 방지할 수 있다. 동적 ID 기반의 경우에는 리더 혹은 태그의 동적 ID 정보와 킷값에 의해 생성되거나 갱신 가능한 대칭키 기반의 암호화 키를 이용한다. 이와 같이 변경되는 값을 이용하는 경우 세션마다 태그 리스트 정보가 변경되어 추적 공격을 방지하거나 태그 리스트 정보의 노출에 따른 문제를 방지할 수 있다.

하지만, 일반적으로 태그 검색 프로토콜이 요청 및 응답의 2-Way 이루어지므로 응답 메시지의 손실이나 공격자에 의해 메시지가 차단되는 경우 비동기화가 발생할 수 있다. 또한, 기존의 동적 ID 기반의 방식은 태그 측에 다음과 같은 연산부하를 가져온다. 첫째, 태그가 리더를 인증하기 위한 연산이 요구된다. 둘째, 인증된 경우 정보를 갱신하기 위한 연산이 요구된다. 셋째, 갱신된 정보를 노출되지 않고 전달하기 위한 연산이 요구된다.

본 논문에서는 기존 태그 리스트에 대한 새로운 측면의 문제점을 제시하고자 한다. 기존 검색 프로토콜에서 수신 받은 태그 리스트를 업데이트 받는 상황으로 1)리더가 읽을 수 있는 태그가 추가된 경우, 2)기존 태그의 정보가 비동기화 된 경우, 3)리더의 권한이 변경된 경우가 있을 수 있다. 이 중 리더의 권한이 변경된 경우에는 기존에 리더가 가지고 있던 태그 리스트를 재활용한다면 변경 이전의 권한으로 태그를 검색할 수 있는 문제점이 발생할 수 있다.

제안하는 태그 리스트 구조는 〔그림 5〕와 같다. $LKId_R$값은 리더의 권한을 의미하며, 리더의 권한에 따라 읽을 수 있는 태그들의 비밀정보들을 XOR 연산으

$$LKId_{R1} = h(Id_{T1}||K_{T1}) \oplus \cdots \oplus h(Id_{Tn}||K_{Tn})$$

$$List = \begin{cases} LKId_{R1} \oplus h(Id_{T1}||K_{T1}) \oplus XId_{R1} & : LId_{T1} \\ \cdots & \\ LKId_{R1} \oplus h(Id_{Tn}||K_{Tn}) \oplus XId_{R1} & : LId_{Tn} \end{cases}$$

〔그림 5〕 제안하는 태그 리스트 구조

로 연결한 체인 값이다. 백엔드 서버는 리더 Id_R의 태그 리스트를 생성시 $LKId_R$와 읽으려는 태그의 비밀정보 $h(Id_T||K_T)$ 그리고 리더의 동적 ID XId_R를 XOR로 연산한 결과를 태그 Id_T의 리스트 LId_T로 표현한다. 제안하는 검색 프로토콜에서는 관련연구[6]에서 제안하는 인증방식에 의해 태그 인증이 성공한 경우에 변경되는 XId_R를 이용한다. 이렇게 생성된 태그 리스트는 다음과 같은 특징에 의해 태그 리스트의 보안성을 강화할 수 있다.

• 특징1 : LId_T가 노출되어도 $LKId_R$와 XId_R정보를 가지고 있지 않은 공격자는 태그의 비밀정보 $h(Id_T||K_T)$를 알아낼 수 없다.

• 특징2 : 태그 리스트 정보는 리더 Id_R가 인증에 참가하는 경우 갱신되므로 리더는 태그 검색이 필요한 시점 이전에 백엔드 서버로부터 태그 리스트를 재전송 받아야 한다.

• 특징3 : 특징2에 따라, 태그 검색 리스트가 노출되어도 XId_R와 $LKId_R$를 모르는 공격자는 태그 검색 리스트 정보를 활용할 수 없다.

• 특징4 : 권한이 변경된 리더 Id_R는 $LKId_R$ 및 XId_R가 갱신되므로 기존 태그 리스트의 정보를 활용할 수 없다.

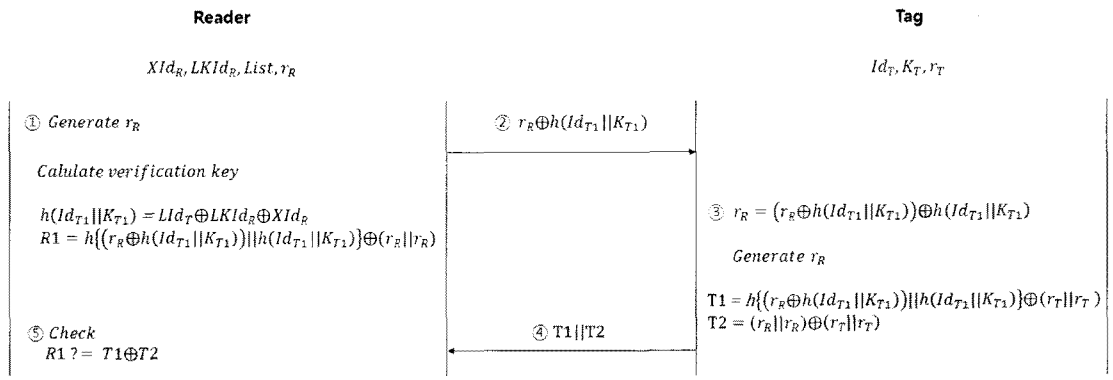
4.2 태그 검색 프로토콜 제안

리더는 태그 검색 이전에 백엔드 서버로부터 XId_R, $LKId_R$, $List$를 전달 받는다. 태그는 연산 능력이 적은 수동형 태그로 가정하며 Id_T, K_T을 갖는다. 과정①에서 리더는 검색하고자 하는 태그의 정보를 추출하기 위해 $List$상의 해당 태그의 정보 LId_T, $LKId_R$, XId_R를 XOR 연산한다. 과정②에서 리더는 랜덤값 r_R을 생성하여 추출한 태그 정보와 XOR 연산하여 브로드캐스트한다. 과정③에서 요청 메시지를 수신한 태그는 자신의 Id_T와 K_T를 해쉬 연산한 후 메시지 ②와 XOR 연산을 통해 리더가 전송한 랜덤값 r_R을 추출한다. 태그는 메시지 ②와 계산했던 Id_T와 K_T를 해쉬 연산값을 연접하여 해쉬 연산한다. 이후 랜덤값 r_R과 XOR 연산하여 $T1$값을 생성한다. 태그가 생성한 랜덤값을 숨기기 위해 r_R과 XOR 연산하여 $T2$를 연산하여 리더에게 응답한다. 각 태그가 과정③~④를 연산하는 동안 리더는 메시지②와 $h(Id_T||K_T)$를 연접하여 해쉬 연산 후 r_R과 XOR 하여 $R1$값을 사전에 연산해둔다. 과정⑤는 각 태그들로부터 전달 받은 메시지 ④를 확인하는 과정으로 태그마다 $T1$, $T2$값을 XOR하여 확인할 수 있다.

제안하는 태그 검색 프로토콜은 요구사항1, 요구사항2, 요구사항3 및 요구사항4를 모두 만족한다.

• 요구사항1 : 태그 위조 공격을 위해서는 메시지 ②에서 랜덤값 r_R을 추출해낼 수 있어야 한다. 태그의 Id_R, K_R를 모르는 공격자는 r_R를 유추할 수 없으므로 요구사항1을 만족한다.

• 요구사항2 :메시지 ②에 포함된 태그 비밀정보는 $LKId_R$, XId_R, LId_T를 모두 소유한 정당한 리더만이



〔그림 6〕 제안하는 태그 검색 프로토콜

생성할 수 있는 값이다. 이 값은 매 세션 갱신되는 값이므로 이 정보를 소유하지 않은 리더는 유효한 쿼리를 만들 수 없어 요구사항2를 만족한다.

• 요구사항3 : 메시지 ②는 리더의 랜덤값 r_R에 의해 세션 마다 변경되고 응답 메시지 ④에는 태그의 랜덤값이 추가되므로, 메시지 ②가 공격자에 의해 재활용된다 하더라도 모든 태그가 반응하므로 찾고자 하는 태그를 검색할 수 없으며 태그의 랜덤값이 포함되므로 응답 메시지 ④는 항상 변경된다. 그러므로 요구사항3-1, 요구사항3-2, 요구사항3-3 및 요구사항3-4를 모두 만족한다.

• 요구사항4 : 제안하는 검색 프로토콜에서는 관련연구[6]의 동적 ID 동기화 방식을 이용하므로, 리더 XId_R의 변경시점은 리더가 태그 인증을 시도하는 시점 즉, 백엔드 서버와 리더가 연결되는 시점이다. 그러므로 태그 검색 프로토콜 상에서는 비동기화가 발생할 수 없으며, 태그 리스트가 변경되는 시점은 기존 정적 ID기반의 태그 검색 프로토콜[1,3]보다는 짧고, 동적 ID 방식의 태그 검색 프로토콜[2,4]보다는 길지만, 비동기화로 인한 프로토콜 실패의 위험이 없다.

V. 제안 프로토콜의 안전성 및 효율성 비교

이번 장에서는 관련연구[1-4]의 태그 검색 프로토콜과 안전성 및 효율성 비교를 통하여 제안하는 프로토콜의 우수성을 증명하고자 한다. 비교대상은 3장에서 살펴본 4가지의 검색 프로토콜[1-4]이며 각 프로토콜의 특징을 아래 [표 1]과 같이 정리하였다.

기존 프로토콜은 타입, 암호화여부 구분해볼 수 있다. RFID 타입을 기준으로 살펴보면 태그 리스트, 리더나 태그의 정보가 변경되지 않는 정적ID, 태그의 리스트 정보, 리더나 태그의 정보가 변경되는 동적ID로 구분할 수 있다. 정적ID에는 C.C.Tan[1], 천지영[3]이 해당하고, 동적ID에는 S.I.Ahamed[2], 임지환[4]이 해당한다. 암호화 지원여부로 살펴본다면 암호화를 지원하는 천지영[3], 임지환[4]와 해쉬 연산을 지원하는 C.C.Tan[1], S.I.Ahamed[2]로 구분해볼 수 있다. 제안하는 기법은 태그 테이블 할당시 리더의 동적ID를 사용하므로 동적ID기반으로 분류할 수 있으며, 프로토콜 상에서 암호화 연산은 사용하지 않는다.

기존 프로토콜[1-4] 및 제안하는 프로토콜의 안전

[표 1] 제안 프로토콜의 안전성 및 효율성 비교

	C.C.Tan[1]	천지영[3]	S.I.Ahamed[2]	임지환[4]	제안하는 기법
RFID 타입	정적ID	정적ID	동적ID	동적ID	동적ID
정보갱신 주체	-	-	태그	태그	서버
태그정보 갱신	-	-	O	O	-
리더정보 갱신	-	-	O	O	O
암호화지원 여부	-	O	-	O	-
태그 위장	-	-	취약	-	-
리더 위장	-	-	-	취약	-
태그 프라이버시	△	-	-	-	-
리더 프라이버시	취약	-	-	-	-
비동기화	-	-	취약	취약	-
Tag	3H+R+2X	D+2E+R+X	2P+2M	2D+2E+H+R	2H+R+3X
Server-RQ	H+R+X	E+R	P	E+R	H+R+4X
Server-Tag	-	-	-	D	-
Server-NT	N(H+X)	N(D+X)	N(P+M)	-	N(X)

*Tag : 태그 측에서의 연산량
*Server-RQ : 요청 메시지 생성시 소비되는 연산량
*Server-Tag : 응답 메시지 확인 연산량(1개의 태그만 응답하는 경우)
*Server-NT : 응답 메시지 확인 연산량(N개의 태그가 응답하는 경우)
*△: 확률적 랜덤수 발생은 태그의 수에 따라 취약할 수 있음
*H : 해쉬연산
*R,P,M : 의사난수함수를 이용한 랜덤값 생성
*X : 배타적 논리연산
*E,D : 암/복호화 연산

성 분석은 이미 3장, 4장에 걸쳐 기술하였으므로 연산량 측면의 비교만 언급하도록 한다. 일방향함수를 사용한 의사난수생성을 해쉬 연산과 동일한 연산량이 소모된다고 가정하면, 태그 측면의 연산량은 임지환 > 천지영 > C.C.Tan > S.I.Ahamed > 제안하는 기법 순으로 제안하는 기법의 연산이 태그 측면에서 가장 적은 연산을 소비한다. (임지환의 프로토콜은 하나의 태그만 반응하므로 비교에서 제외하도록 한다.) 리더 측면의 연산량은 천지영 > S.I.Ahamed > C.C.Tan > 제안하는 기법 순으로 제안하는 기법의 연산이 N개의 태그로부터의 응답을 수신하는 경우에 연산량이 가장 적은 연산을 소비한다.

VI. 결론

본 논문에서는 모바일 환경에서의 무선 리더를 대상으로 하는 RFID 태그 검색 프로토콜을 제안하였다. 기존 무선 리더가 소지하는 태그 리스트의 재사용을 방지함으로써 보안성을 강화함으로써 이동이 잦은 모바일 환경에서의 발생할 수 있는 리더 도난, 태그 상태 변경 및 리더의 권한 변경에 유연하게 대처할 수 있도록 하였다. 제안하는 태그 검색 프로토콜은 해쉬 연산과 XOR 연산만을 이용하므로 암호화 기법을 사용하는 기존의 동적 ID기반 태그 검색 프로토콜보다 효율적으로 동작하며 태그 측에서 저장해야하는 정보 또한 최소화할 수 있도록 설계되었다.

참고문헌

[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] S.I.Ahamed, F.Rahman, e.Hoque, F.Kawsar, and T.Nakajima, "S3PR:Secure Serverless Search Protocols for RFID," Information Security and Assurance (ISA), pp. 1870192, Apr. 2008.

[3] 천지영, 황정연, 이동훈, "이동형 리더 소지자의 프라이버시를 보호하는 RFID 태그 검색 프로토콜," 한국정보보호학회, 정보보호학회논문지, 19(5), pp. 59-69, 2009년 10월.

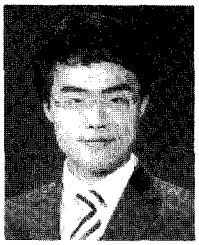
[4] 임지환, 오희국, 김상진, "온라인 서버가 없는 환경에서 이동형 리더의 프라이버시를 보호하는 안전한 RFID 검색 프로토콜," 한국정보보호학회, 정보보호학회논문지, 20(2), pp. 73-90, 2010년 4월.

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

[6] 여돈구, 이상래, 장재훈, 염흥열, "서버와 리더의 위장공격 탐지가 가능한 랜덤 ID 기반 RFID 상호 인증 프로토콜," 한국정보보호학회, 정보보호학회논문지, 20(4), pp. 89-108, 2010년 8월.

[7] M.Feldhofer and J.Wolkerstorfer, "Strong crypto for RFID tags-A comparison of low-power hardware implementations," IEEE International Symposioum on Circuits and Systems(ISCAS), pp. 1839-1842, May 2007.

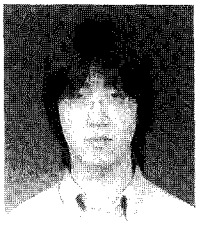
〈著者紹介〉



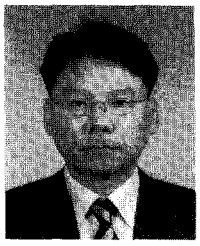
여 돈 구 (Don-Gu Yeo) 학생회원
2009년 2월: 순천향대학교 정보보호학과 졸업
2011년 2월: 순천향대학교 정보보호학과 석사졸업
〈관심분야〉 정보보호, USN 보안, 클라우드 컴퓨팅 보안, IPTV 보안, 역추적

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

최 현 우 (Hyun-Woo Choi) 학생회원
2009년 2월: 순천향대학교 정보보호학과 졸업
2011년 2월: 순천향대학교 정보보호학과 석사졸업
〈관심분야〉 IPTV 보안, 스마트그리드 보안, USN 보안, 역추적



장 재 훈 (Jae-Hoon Jang) 학생회원
2009년 2월: 순천향대학교 정보보호학과 졸업
2011년 2월: 순천향대학교 정보보호학과 석사졸업
〈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 회장(현) 총무이사, 학술이사, 교육이사, 총무이사, 논문지편집위원 위원장(역),
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