韓國컴퓨터情報學會 論文誌
第15卷 第9號, 2010. 9.

2010-15-9-3-3

이동형 리더의 프라이버시를 보호하는 안전하고 효율적인 RFID 태그 검색 프로토콜

최현우*, 여돈구*, 장재훈*, 염흥열**

A Secure and Efficient RFID Tag Search Protocol Protecting Mobile Reader's Privacy

Hyun-Woo Choi*, Don-Gu Yeo*, Jae-Hoon Jang*, Heung-Youl Youm**

요 약

최근 들어, 특정 RFID 태그들의 그룹 내에서 원하는 태그를 찾기 위한 RFID 태그 검색 시스템에 대한 연구가 활발히 진행되고 있다. RFID 태그 검색 시스템은 물류 및 재고 관리를 비롯하여 미아 찾기, 범죄자의 전자발찌 등 다양한 분야에서 응용될 수 있다. 안전한 RFID 태그 검색 시스템의 구현을 위해서는 태그 추적 문제와 리더 소지자의 프라이버시 문제 등과 같이 다양한 보안 위협들을 고려하여 프로토콜을 설계해야 한다. 기존에 제안된 RFID 태그 검색 프로토콜들은 몇몇 보안 요구사항을 만족시키지만, 리더 소지자의 프라이버시 문제를 해결하지 못했고, 리더 소지자의 프라이버시 문제를 해결했다 하더라도 암호화 연산을 이용하였기 때문에 연산량 측면에서 많은 부하를 가져오게 했다. 따라서 본 논문에서는 리더 소지자의 프라이버시 문제를 해결하면서도 효율적으로 동작하는 RFID 태그 검색 프로토콜을 제안한다.

Abstract

Recently, study on RFID Tag Searching technique which is used to find a specific tag in particular tag group were developed continuously. RFID tag searching technique can be applicate in various fields such as product management, finding children, and electronic anklet. To implement a RFID tag search system, RFID tag searching protocol should be considered various security threats such as reader and tag tracking, privacy, etc. For implementing a safe RFID tag lookup system, it is important to consider the potential security threats such as the tag tracking problem, and the privacy of the owner of the tag reader problem. There exists an RFID tag lookup system that satisfies a few security requirements, but the privacy of the owner of the tag reader problem has still been left unsolved, and even if it were solved, it requires a considerable amount of cryptographic operations to be performed which results in a decrease in performance. This paper proposes a system that does not degrade the performance while solving the privacy of the owner of the tag reader problem.

• 제1저자 : 최현우 교신저자 : 염흥열
• 투고일 : 2010. 08. 06, 심사일 : 2010. 08. 20, 게재확정일 : 2010. 08. 28.
* 순천향대학교 정보보호학과 석사과정 ** 순천향대학교 정보보호학과 교수
※ "본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (NIPA-2010-(C1090-1031-0005))

▸ Keyword : RFID, 태그(tag), 검색(search)

Ⅰ. 서 론

RFID(Radio Frequency IDentification) 시스템은 과거 단순히 태그(Tag)가 부착된 물체를 식별하는 기술에 그치지 않고, 실시간으로 물류의 운송을 추적하는 등 다양한 분야에서 사용되고 있다. 특히, 특정한 RFID 태그들의 그룹 내에서 사용자가 찾고자 하는 태그가 있는지 확인 할 수 있게 해주는 RFID 태그 검색 시스템(RFID Tag Search System)이 최근들어 RFID 응용분야로써 각광받고 있으며, 이에 대한 연구 또한 활발히 이루어지고 있다.

RFID 태그 검색 시스템은 다양한 분야에서 활용될 수 있는데, 도서관에서 책을 찾는다거나 창고에서 특정 재고의 존재 유무를 확인해야 하는 등의 작업에 매우 유용하게 이용될 수 있다. 또한 사회적으로 이슈가 되고 있는 범죄자의 전자발찌에 적용되어 특정 구역을 벗어나는 범죄자를 확인할 수도 있으며, 놀이공원 등 사람이 많은 곳에서 미아를 찾기 위한 방안으로도 적극 활용될 수 있다.

RFID 태그 검색 시스템의 구현을 위해서는 안전한 프로토콜의 설계가 요구되는데, 이는 이동형 RFID 리더가 중앙 서버의 도움 없이 특정 태그를 찾기 위한 연산을 수행하면서 리더 소지자의 프라이버시를 보호해야 하는 등의 보안 요구사항을 충족시켜야 하기 때문이다. RFID 태그 검색 시스템은 고정식의 리더가 아니라 휴대용의 리더를 사용하므로, 리더 소지자는 서버로부터 접근 가능한 태그들의 정보를 내려 받아 리더에 저장하고, 휴대용의 리더를 들고 이동하면서 특정 태그를 검색하게 된다. 이때 리더 소지자의 프라이버시가 보장되지 않는다면 특정 리더 소지자가 찾고자 하는 태그가 무엇인지, 혹은 리더 소지자의 위치가 어디인지 공격자는 알 수 있게 되어 리더 소지자는 프라이버시를 침해당하게 된다. 마찬가지로 태그의 위치가 보호되지 않는다면 공격자는 실시간으로 리더가 찾고자 하는 태그의 위치를 추적할 수 있게 된다.

RFID 태그 검색 시스템의 구현을 위해 고려해야 할 또 한 가지 사항은 RFID 리더 및 태그의 연산량을 최소화해야 한다는 것이다. 이는 RFID 검색 프로토콜의 성능과 직결되는 문제이며, 대량의 RFID 태그들을 상대로 하여도 안정적인 프로토콜의 동작을 보장하기 위함이다. 본 논문의 3장에서는 해쉬(hash) 함수와 XOR (exclusive or) 연산만을 이용한 XOR 체인 기반의 RFID 태그 검색 프로토콜을 제안한다.

기존에 RFID 태그 검색 프로토콜[1-7]들이 다수 제안되었지만, 리더의 프라이버시 문제를 대부분 해결하지 못했고[1-4,7], 해결했다 하더라도 암호화 알고리즘을 사용하였기 때문에 대량의 태그를 상대로 했을 때는 연산량 측면에서 많은 오버헤드를 갖게 했다[5,6]. 따라서 본 논문에서는 리더 소지자 및 태그의 다양한 보안 요구사항을 만족시키고, 리더 소지지자의 프라이버시 문제를 해결하면서도 효율적으로 동작하는 RFID 태그 검색 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구를 통해 기존 기법들을 분석하고, 3장에서 RFID 태그 검색 프로토콜의 보안 요구사항을 도출한 후, 본 논문에서 제안한 RFID 태그 검색 프로토콜을 기술한다. 4장에서는 제안한 프로토콜과 기존 연구와의 비교를 통해 안전성과 효율성을 분석하고, 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

2.1 관련 연구

RFID 태그 검색 프로토콜은 [그림 1]과 같이 리더(R_i)가 찾길 원하는 특정 태그(T_j)의 id_j를 태그들의 그룹(T^*)으로 브로드캐스트 했을 때(1), 해당하는 id_j의 태그가 응답함으로써 수행될 수 있다(2). 하지만, 이와 같은 단순한 프로토콜은 어떠한 보안성도 제공하지 않는다. 공격자는 단순히 리더와 태그사이의 통신을 도청함으로써 정당한 리더 및 태그로 위장할 수 있게 되는 등 다양한 보안 문제점을 발생시킨다. 그렇기 때문에 RFID 태그 검색 프로토콜을 위해서는 태그가 정당한 리더의 요청인지를 인증할 수 있어야 하고, 리더 또한 정당한 태그의 응답인지를 확인할 수 있어야 한다.

따라서 RFID 태그 검색 프로토콜은 RFID 인증 프로토콜을 확장한 개념이라고 볼 수 있다[9]. 그 이유는 태그 그룹에 속해 있는 모든 태그들에 대하여 각각 인증 프로토콜을 반복적으로 수행함으로써, 인증에 성공한 태그를 사용자가 찾고자 하는 태그로 간주할 수 있기 때문이다. 하지만 인증을 통한 태그 검색은 태그의 수가 늘어날수록 리더 및 태그에 미치는 연산량이 급격히 증가하므로 효율적이지 못하다. 따라서 최근에는 효율적으로 태그 검색을 수행하는 RFID 태그 검색 프로토콜들[1-7]이 제안되고 있다.

$$R_i \rightarrow T* \ : \ id_j \quad (1)$$
$$T* \ : \ \text{If } id = id_j \quad (2)$$
$$R_i \leftarrow T_j \ : \ \text{Reply} \quad (3)$$

그림 1. RFID 태그 검색
Fig. 1. RFID tag search

2.1.1 C.C. Tan 등의 프로토콜

2007년에, C.C. Tan 등은 RFID 태그 검색 프로토콜 [1,2]을 처음으로 제안했다. 문헌 [1,2]에서는 리더 소지자가 휴대용 리더를 이용하여 중앙 서버의 도움 없이 특정 태그를 검색할 수 있도록 하기 위해서, [그림 1]과 같이 검색 권한을 갖는 태그의 목록(Access List)을 중앙 서버(신뢰기관)로부터 휴대용 리더에 내려 받아 저장하게 했다.

$$L_i = \begin{cases} f(r_i,t_1) \ : \ id_1 \\ \quad ... \quad : \ ... \\ f(r_i,t_n) \ : \ id_n \end{cases}$$

그림 2. 문헌 [1,2]의 접근리스트 L_i
Fig. 2. Access list L_i of reference [1,2]

문헌 [1,2]에서, 리더는 식별값 r_i와 [그림 2]에서와 같이 검색 권한을 갖는 태그들에 대한 접근권한 리스트 L_i을 가지며, 태그는 식별값 id_j와 신뢰기관과 공유하는 비밀값 t_j를 가진다. 이때 $f(.)$는 두 파라미터를 연결하여 해쉬하는 해쉬 함수이다. 신뢰기관에 의해 리더는 태그의 비밀값 t_j와 리더의 식별자 r_i를 해쉬한 해쉬값만을 접근리스트로써 저장하기 때문에, 특정 태그에 대한 검색을 수행할 수 있고 리더 측에 태그의 비밀값을 저장할 필요가 없어 보안성을 향상 시킬 수 있다.

$$R_i \rightarrow T* \ : \ h(f(r_i,t_j)\|n_r)\oplus id_j, n_r, r_i \quad (1)$$
$$T* \ : \ \text{Derive } h(f(r_i,t_j)\|n_r) \text{ and XOR with } h(f(r_i,t_j)\|n_r)\oplus id_j \quad (2)$$
$$: \ \text{If } id = id_j \quad (3)$$
$$R_i \leftarrow T_j \ : \ h(f(r_i,t_j)\|n_t\|n_r)\oplus id_j, n_t \quad (4)$$

그림 3. 문헌 [1,2]의 기본 프로토콜
Fig. 3. Basic protocol of reference [1,2]

문헌 [1,2]에서는 1개의 기본 태그 검색 프로토콜과 기본 태그 검색 프로토콜을 기반으로 하여 향상된 3개의 태그 검색 프로토콜을 추가로 제안했다. [그림 3]는 문헌 [1,2]의 기본 프로토콜을 보여준다.

[그림 3]에서 리더는 난수 n_r를 이용하여 매번 다른 값으로 태그 검색을 요청하지만(1), 공격자는 요청 메시지 도청하여 재생공격을 시도함으로써 리더가 찾고자 하는 태그로부터 정상적인 응답을 받을 수 있다. 문헌 [1,2]에서는 이와 같은 재생공격을 지적하여 개선된 3개의 프로토콜을 추가로 제안했다. 개선된 첫 번째 프로토콜은 다음 [그림 4]와 같다.

$$R_i \rightarrow T* \ : \ h(f(r_i,t_j)\|n_r)\oplus id_j, n_r, r_i \quad (1)$$
$$T* \ : \ \text{Deriving } h(f(r_i,t_j)\|n_r) \text{ and XOR with } h(f(r_i,t_j)\|n_r)\oplus id_j \quad (2)$$
$$: \ \text{If } id = id_j \text{ and } n_r \neq \text{old}n$$
$$: \ \text{update old}n = n_r \quad (3)$$
$$R_i \leftarrow T_j \ : \ h(f(r_i,t_j)\|n_t)\oplus id_j, n_t \quad (4)$$

그림 4. 문헌 [1,2]의 개선 프로토콜 1
Fig. 4. Advanced protocol 1 of reference [1,2]

[그림 4]에서 태그는 이전에 요청된 리더의 랜덤값(n_r)인 old$n$을 저장하고 있기 때문에, 태그 자신의 id와 계산 해낸 id_j가 같더라도 현재 랜덤값 n_r이 바로 전의 요청메시지에 포함된 랜덤값 old$n$과 같다면 응답을 하지 않는다. 이로 인해 바로 이전의 요청메시지를 이용하는 공격자의 재생공격을 막을 수 있게 된다. 하지만, old$n$ 이전의 요청메시지로 재생공격을 시도하는 공격자는 막을 수가 없기 때문에 재생공격의 근본적인 해결책이 될 수 없다.

문헌 [1,2]의 첫 번째와 두 번째 프로토콜은 리더가 찾는 태그만이 리더가 정당한지를 검증한 후 응답 메시지를 발생시킨다. 따라서 리더가 특정 태그 그룹에서 찾고자 하는 태그가 존재하는 경우에는 1개의 응답 메시지만이 존재하게 된다. 이것은 공격자가 응답 메시지의 내용을 모르더라도, 응답 메시지의 존재만으로도 리더가 찾고자 하는 태그의 존재 유무를 알 수 있기 때문에, 주기적으로 요청메시지를 태그의 그룹에 전송하여 찾고자 하는 태그의 위치를 추적할 수 있게 된다. 따라서 문헌 [1,2]의 세 번째 및 네 번째 프로토콜에서는 id_j가 같은 태그뿐만 아니라, id_j가 같지 않더라도 응답 메시지를 발생 시킬 수 있도록 하는 프로토콜을 제안 했다.

다음 [그림 5]는 문헌 [1,2]의 두 번째 개선된 프로토콜을 나타낸다.

$R_i \rightarrow T*$: Broadcast $[id_j]m, r_i, n_n$ (1)

$T*$: If $idm = [id_j]m$ (2)

$R_i \leftarrow T_j$: $h(f(r_i,t_j) \| n_r \| n_t) \oplus id_j, n_t$ (3)

R_i : Determines $f(r_i,t_j)$ from L, obtain id_j (4)

그림 5. 문헌 [1,2]의 개선 프로토콜 2
Fig. 5. Advanced protocol 2 of reference [1,2]

[그림 5]에서 리더는 찾고자 하는 태그(id_j)의 처음 m 비트만($[id_j]m$)을 태그의 그룹으로 브로드캐스트 한다. 리더의 요청메시지를 수신한 태그들은 $[id_j]m$이 자신 id_j의 처음 m비트와 같다면 응답메시지를 계산하여 리더로 전송한다. 따라서 리더와 태그 그룹 사이에는 랜덤한 수의 응답이 존재하기 때문에 공격자는 리더가 찾고자 하는 태그의 존재 유무를 알 수가 없게 된다. 하지만 [그림 5]의 프로토콜 안전성은 특정 태그 그룹에 포함되는 태그의 수에 비례함을 알 수 있다. 즉, 태그 그룹에 포함된 태그의 수가 적을 때에는 처음 m비트를 가지는 태그가 1개만 존재할 가능성이 있기 때문에 공격자는 태그의 존재유무를 파악할 수 있게 된다.

마지막으로 문헌 [1,2]의 개선된 세 번째 프로토콜은 [그림 6]과 같다.

$R_i \rightarrow T*$: Broadcast $h(f(r_i,t_j) \| n_r) \oplus id_j, n_r, r_i$ (1)

$T*$: Derive $h(f(r_i,t_j) \| n_r)$ and XOR with $h(f(r_i,t_j) \| n_r) \oplus id_j$ (2)

: If $id = id_j$:

$R_i \leftarrow T_j : h(f(r_i,t_j) \| n_t) \oplus id_j, n_t$ (3)

: Else :

$R_i \leftarrow T_j : (rand, n_r)$ $with$ $prob.\lambda$ (4)

그림 6. 문헌 [1,2]의 개선 프로토콜 3
Fig. 6. Advanced protocol 3 of reference [1,2]

[그림 6]에서 λ는 리더가 찾고 있는 id_j와 태그의 id가 일치 하지 않더라도 태그가 응답메시지를 발생할 확률을 의미한다. 따라서 검색 프로토콜이 동작하는 리더와 태그 간에는 랜덤한 수의 응답 메시지가 존재하게 되며, 태그 추적 등과 같은 공격을 막을 수 있게 된다. 하지만, 개선된 프로토콜 2와 마찬가지로 태그의 수가 적을 경우에는 안전하지 않다.

지금까지 분석한 내용을 토대로 C.C. Tan 등이 제안한 4개의 RFID 태그 검색 프로토콜은 재생공격 및 태그 추적 공격에 안전하지 않다는 것을 알 수 있다. 게다가 4개의 프로토콜 모두는 리더 소지자의 프라이버시 침해를 발생시킬 수 있는 문제점이 존재한다. 리더가 태그를 검색하기 위해 보내는 요청메시지에는 리더의 고정된 식별자 값인 r_i가 평문으로 노출되어 있기 때문에, 만일 공격자가 도청을 통하여 이동하는 리더의 식별자를 계속해서 확인할 수 있다면, 리더 소지자의 위치를 추적할 수 있게 된다.

2.1.2 천지영 등의 프로토콜

천지영 등이 제안한 참고 문헌 [6]에서는 r_i 값의 평문 노출을 막고자 AES(Advanced Encryption Standard) 암호 알고리즘을 사용해 리더와 태그 구간을 암호화 하는 RFID 태그 검색 프로토콜을 새롭게 제안했다. 문헌 [6]의 프로토콜에서는 수동형 태그에 적합한 암호 알고리즘을 구현하여 이를 분석한 Feldhofer 등[8]의 결과를 통해 AES-128 암호 알고리즘을 태그 검색 프로토콜에 적용 했다.

앞 절의 관련연구에서처럼 문헌 [6]에서도 [그림 7]과 같이 초기 설정 단계에서 신뢰기관으로부터 검색 가능한 태그의 접근 리스트 L_i를 내려 받아 저장하고 있다. 각각의 리더 R_i의 식별자를 r_i라 하고, 태그 T_j의 식별자를 ID_j, 비밀키를 t_j라고 한다. 이때 $E_{t_n}(r_i \| ID_n)$은 각 64비트의 r_i와 ID_n을 연결한 $r_i \| ID_n$를 128비트 길이의 비밀키 t_n를 이용하여 AES 암호 알고리즘으로 암호화한 암호문을 나타낸다.

$$L_i = \begin{cases} E_{t_1}(r_i \| ID_1) & : ID_1 \\ \quad \ldots \quad : & \ldots \\ E_{t_n}(r_i \| ID_n) & : ID_n \end{cases}$$

그림 7. 문헌 [6]의 접근 리스트 L_i
Fig. 7. Access list L_i of reference [6]

문헌 [6]에서, 리더 R_i가 특정 태그 T_j를 검색하기 위한 RFID 태그 검색 프로토콜은 [그림 8]과 같다.

$R_i \rightarrow T*$: Broadcast $E_{ID_j}(r_i \| R)$ (1)

$T*$: Decrypt $E_{ID_j}(r_i \| R)$ and Compute $K_i = E_{t_j}(r_i \| ID_j)$ (2)

$R_i \leftarrow T*$: $E_{K_i}(ID_j \| r) \oplus (R \| R)$ (3)

그림 8. 문헌 [6]의 RFID 태그 검색 프로토콜
Fig. 8. RFID tag searching protocol of reference [6]

〔그림 8〕의 (1)단계에서, 리더 R_i는 태그 T_j를 검색하기 위해, 자신의 식별자 r_i와 64비트 난수 R을 평문으로 하고 찾고자하는 T_j의 식별자인 ID_j를 비밀키로 하는 암호문 $E_{ID_j}(r_i \| R)$을 태그 그룹으로 브로드캐스트 한다. (2)단계에서, 브로드캐스트 메시지를 수신한 태그들은 자신의 ID_j를 이용하여 $E_{ID_j}(r_i \| R)$를 복호화 한 후, r_i과 R을 각각 64비트씩 분리해 낸다. 동시에 r_i과 ID_j를 입력으로 하고, t_j를 비밀키로 하는 암호문 $K_i = E_{t_j}(r_i \| ID_j)$를 생성해 낸다. (3) 단계에서, 각각의 태그들은 난수 r을 선택하여 응답 메시지 $E_{K_i}(ID_j \| r) \oplus (R \| R)$를 생성하여 리더에게 전송한다. 리더는 태그들로부터 수신한 $E_{K_i}(ID_j \| r) \oplus (R \| R)$를 자신이 선택했던 난수 $R \| R$과 XOR 연산을 수행하고, 생성된 결과값인 암호문 $E_{K_i}(ID_j \| r)$에 대해서 접근 리스트의 $E_{t_j}(r_i \| ID_j)$를 키로 취하여 암호문을 복호화 한다. 복호화 후 추출된 ID_j값이 자신이 찾고자 했던 태그의 식별자와 같다면 리더는 특정 태그 그룹에 찾길 원하는 태그가 존재한다는 것을 알 수 있다.

이와 같이 문헌 〔6〕에서 제안한 RFID 태그 검색 프로토콜은 암호화 알고리즘을 이용해 어떠한 평문도 리더와 태그사이에 노출시키지 않음으로써, 리더 소지자의 프라이버시 침해 문제를 해결하였다. 마찬가지로 리더의 요청메시지에 대해 모든 태그가 응답메시지를 발생시키기 때문에 태그의 추적 문제 또한 해결하였다. 하지만 찾고자 하는 태그 그룹에 많은 태그가 존재한다면, 각각의 태그가 발생시키는 모든 응답 메시지에 대해 암·복호화 과정을 거쳐 메시지를 검증해야 하므로, 리더가 가지는 부하는 브로드캐스트 그룹 내의 태그 수에 비례한다고 볼 수 있다. 따라서 본 논문의 3장에서는 해쉬 함수와 XOR 연산만을 이용하여 효율적으로 동작하면서도 추적문제와 같이 리더의 프라이버시 침해 문제를 해결할 수 있는 RFID 태그 검색 프로토콜을 제안한다.

III. RFID 태그 검색 프로토콜

3.1 보안 요구사항

RFID 태그 검색 프로토콜은 기본적으로 무선구간에서 동작하므로, 공격자는 도청(Eavesdropping Attack)을 통해 전송되는 메시지를 쉽게 훔쳐보는 것이 가능하다. 따라서 도청된 메시지는 공격자의 재생 공격(Replay Attack)에 이용될 수 있어 정당한 리더가 요청한 메시지를 위조하거나 또는 정당한 태그가 응답한 메시지를 흉내 내는데 악용될 수 있다. 또한 리더 소지자는 휴대용 리더를 이용해 이동하면서 태그를 검색해야 하는 경우가 생기는데, 이때 적절한 보안이 보장되지 않는다면 리더 소지자의 위치를 공격자에 의해 추적당할 수도 있다. 마찬가지로 태그를 몸에 지니고 있는 사용자 또한 공격자에 의해 위치를 추적당할 수도 있다.

본 논문에서는 위와 같은 공격을 통해 발생할 수 있는 보안 문제 해결하기 위해, 다음 〔표 1〕과 같이 안전한 RFID 태그 검색 프로토콜이 만족해야 하는 보안 요구 사항을 도출 하였다.

표 1. RFID 태그 검색 프로토콜 보안 요구사항
Table 1. Security requirements of RFID tag searching protocol

보안 요구사항	내용
메시지 기밀성	· 공격자가 도청 공격을 통해 리더와 태그 사이에 전송되는 태그 검색 메시지를 습득했다 하더라도, 그 메시지로부터 어떠한 의미 있는 정보도 알아낼 수 없도록 기밀성이 보장되어야 한다.
개체 인증	· 태그는 리더로부터 수신 한 요청 메시지가 정당한 리더에 의해 생성되었음을 확신할 수 있어야 한다. · 리더는 태그로부터 수신 한 응답 메시지가 정당한 태그에 의해 생성되었음을 확신할 수 있어야 한다.
추적불가능성	· 같은 리더가 생성한 요청 메시지들의 관계를 구별할 수 없게 하여 리더의 위치 추적 공격을 방지해야 한다. · 태그에 의해 발생되는 응답메시지를 랜덤하게 하여 특정 태그의 존재유무를 통한 태그의 위치를 추적 공격을 할 수 없게 해야 한다.
물리공격 안전성	· 공격자는 리더에 저장된 정보를 유출할 수 있고 만일 유출된 정보에 태그의 비밀값이 포함되어 있다면 정당한 태그로써 위장할 수 있게 된다. 따라서 리더에는 태그에 대한 비밀정보가 평문형태로 저장되지 않아야 한다.
재생공격 안전성	· 도청을 통해 리더 및 태그가 전송한 메시지를 저장하고 있다가 다시 재전송시키는 공격자의 재생공격에 대한 안전성이 보장되어야 한다.

$$R_i \rightarrow T^* \ : \ \text{Broadcast} \ \ f(id_j, t_j) \oplus X_i \oplus r_i \oplus n_r \oplus c_r, \ \ h(X_i \oplus r_i \oplus n_r \oplus c_r) \oplus c_r \oplus id_j \quad (1)$$

$$T^* \ : \ temp_1 = h(f(id_{\text{own}}, t_{\text{own}}) \oplus f(id_j, t_j) \oplus X_i \oplus r_i \oplus n_r \oplus c_r), \quad (2)$$

$$: \ temp_2 = id_{\text{own}} \oplus h(X_i \oplus r_i \oplus n_r \oplus c_r) \oplus c_r \oplus id_j$$

$$: \ c_t = (temp_1 \oplus temp_2) + 1$$

$$R_i \leftarrow T^* \ : \ \text{Reply} \ \ h(h(id_{\text{own}} \oplus n_t) \| c_t), \ \ n_t \quad (3)$$

그림 10. 제안하는 RFID 태그 검색 프로토콜
Fig. 10. Proposed RFID tag searching protocol

3.2 제안 프로토콜

제안하는 RFID 태그 검색 프로토콜은 기존 연구[1-7] 에서와 마찬가지로, 리더 측에 검색 가능한 태그들의 접근 리스트를 사전에 저장하고 있다. 이는 휴대용 리더를 통해 리더 소지자가 서버의 도움 없이 이동하면서 태그를 검색할 수 있게 해준다. 따라서 본 논문에서는 사전에 신뢰기관으로부터 접근 리스트를 리더에 안전하게 전송하는 사전 준비 단계와, 실제 RFID 태그를 검색하는 태그 검색 단계로 프로토콜 절차를 분류한다.

3.2.1 사전 준비 단계

다음 [그림 9]는 이동형 리더 측에 저장되는 접근 리스트를 나타낸다.

$$X_i = f(id_1, t_1) \oplus f(id_2, t_2) \oplus f(id_3, t_3) \oplus \cdots \oplus f(id_n, t_n)$$

$$L_i = \begin{cases} f(id_1, t_1) \oplus X_i \oplus r_i & : \ id_1 \\ \quad \cdots & : \ \cdots \\ f(id_n, t_n) \oplus X_i \oplus r_i & : \ id_n \end{cases}$$

그림 9. 제안 프로토콜의 접근 리스트 L_i
Fig. 9. Access list L_i of proposed protocol

[그림 9]에서, 태그의 식별값을 id_j, 그리고 태그의 비밀값을 t_j로 나타낸다. 신뢰기관은 [그림 9]에서처럼 리더가 검색 가능한 각 태그의 식별값과 태그의 비밀값을 연결하여 각각 해쉬하고, 해쉬하여 생성된 각 값들을 XOR 연산하여 최종 결과값인 X_i를 얻는다. 이때 $f(.)$는 두 파라미터를 연결하여 해쉬값을 생성하는 해쉬 함수이다. 그리고 나서 X_i는 태그의 id_n에 매칭 되는 각 $f(id_n, t_n)$와 XOR 연산하여 검색하고자 하는 태그들의 접근 리스트인 L_i를 생성 한다. 접근 리스트 L_i는 태그 검색 프로토콜이 동작되기 이전에 오프라인 상에서 신뢰기관으로부터 리더로 안전하게 전송된다.

3.2.2 태그 검색 단계

다음 [그림 10]은 리더의 요청 메시지와 태그의 응답메시지로 이루어지는 RFID 태그 검색 프로토콜을 나타낸다. [그림 10]에서, 리더는 사전 준비 단계에서 생성한 값들(L_i, X_i)과 리더의 식별값 r_i, 그리고 리더의 카운터값 c_r를 가지며, 태그는 태그의 식별값 id_j와 비밀값 t_j를 가진다. $h(.)$는 해쉬 함수이며, $f(.)$는 두 파라미터를 연결하여 해쉬값을 생성하는 해쉬 함수이다.

리더와 태그가 수행하는 프로토콜의 구체적인 절차는 다음 단계들과 같다.

(1)단계 : 리더 R_i는 특정 태그 T_j를 찾기 위해, 리더의 전파가 도달하는 임의의 태그들에게 $f(id_j, t_j) \oplus X_i \oplus r_i \oplus n_r \oplus c_r$와 $h(X_i \oplus r_i \oplus n_r \oplus c_r) \oplus c_r \oplus id_j$를 포함하는 요청 메시지를 브로드캐스트 한다.

(2)단계 : 리더(R_i)로부터 요청 메시지를 수신한 각각의 태그들(T^*)은, 자신이 가지고 있는 식별값(id_{own})과 비밀값(t_{own})을 이용하여 해쉬값인 $f(id_{own}, t_{own})$를 계산해 내고, 계산된 해쉬값과 요청 메시지의 첫 번째값인 $f(id_j, t_j) \oplus X_i \oplus r_i \oplus n_i \oplus c_r$를 XOR 연산한 후 최종 해쉬한 값인 $temp_1$을 생성해 낸다. 또한 태그 자신의 식별값(id_{own})과 요청 메시지의 두 번째 값인 $h(X_i \oplus r_i \oplus n_r \oplus c_r) \oplus c_r \oplus id_j$를 XOR 연산한 값인 $temp_2$를 생성해 낸다. 이렇게 생성된 $temp_1$과 $temp_2$를 XOR 연산한 후 결과값에 1을 더한 값 $((temp_1 \oplus temp_2) + 1)$이 태그의 카운터 값($c_t$)이 된다.

(3)단계 : 태그들(T^*)은 자신의 식별값(id_{own})과 (2)단계에서 생성한 카운터값(c_t)을 XOR 연산한 후 해쉬한 값에 난수 n_t를 연결하여 한번 더 해쉬한다. 그리고 나서 생성된 해쉬값($h(h(id_{own} \oplus c_t) \| n_t)$)과 난수 n_t를 포함하는 응답 메시지를 요청 메시지를 송신한 리더(R_i)에게 전송한다.

(4)단계 : 임의의 태그들(T^*)로부터 응답 메시지들을 수신

한 리더(R_i)는, 찾고자 했던 태그의 식별값(id_j)과 1이 증가된 카운터 값(c_r+1), 그리고 전달 받은 응답 메시지의 두 번째 값인 난수 n_t를 이용해 수식 $h(h(id_j \oplus c_{r+1}) \| n_t)$를 계산하고, 계산한 결과값이 응답메시지의 첫 번째 값과 일치하는지 검증한다. 만일 일치한다면, 리더는 요청 메시지를 전송한 임의의 태그 그룹 내에 찾고자 했던 태그(T_j)가 존재함을 알 수 있다.

IV. 분석

4.1 안전성 분석

본 절에서는 제안하는 프로토콜이 3.1절에서 도출한 RFID 태그 검색 프로토콜의 보안 요구사항에 만족하는지를 평가한다.

• 메시지 기밀성 : 본 논문에서 제안한 프로토콜에서는, 리더에서 태그로 전송되는 요청메시지와 태그에서 리더로 전송되는 응답 메시지에 포함된 값들을 기본적으로 XOR 연산과 해쉬함수($h(.), f(.)$)를 사용하여 생성하였기 때문에 기밀성을 만족한다. 따라서 공격자는 이들 메시지로부터 리더/태그의 식별값(id_r, id_j)이나 태그의 비밀값(t_j)과 같은 어떠한 의미 있는 정보도 추출해 낼 수 없게 된다.

• 개체 인증 : [그림 10]의 4단계에서, 리더는 자신이 찾고자 했던 태그의 식별값(id_j)과 기대하는 카운터값(c_r+1)을 이용하여 수신한 응답 메시지의 첫 번째 값을 검증함으로써 정당한 태그임을 인증할 수 있다. 한편 제안한 프로토콜에서는 재생공격 및 태그 추적공격 등을 막기 위해 태그 검색 요청 메시지를 수신한 모든 태그들이 응답 메시지를 발생시키게 하였기 때문에 태그 측에서 리더를 인증하지는 않는다.

• 추적불가능성 : 기존 선행연구[1-2,3-4,7] 에서는 리더의 식별자(r_i)가 평문으로 전송되기 때문에 요청 메시지를 전송하는 리더를 확인할 수 있을 뿐만 아니라, 이동하면서 태그를 검색하는 리더 소지자의 위치를 추적할 수도 있었다. 하지만 본 논문에서 제안한 프로토콜은 리더의 식별값을 포함하여 리더를 구별할 수 있는 어떠한 정보도 공격자는 확인할 수 없기 때문에 리더 소지자의 위치 추적을 불가능하게 한다. 마찬가지로 리더의 요청 메시지를 수신한 모든 태그는 응답메시지를 발생시키기 때문에, 응답 메시지로부터 태그를 구별하거나 위치를 추적할 수 없게 된다. 리더의 추적불가능성은 문헌[6]에서도 개선된 사항이지만, 본 논문에서는 암호화 연산을 사용 하지 않음으로써 효율성이 대폭 향상된다.

• 물리공격 안전성 : RFID 태그 검색 프로토콜에서는 사용자가 리더를 소지하여 이동하면서 원하는 태그를 검색하게 되는 경우가 대부분이다. 이때 리더가 분실된다면 공격자는 습득한 리더로부터 저장된 정보를 유출시킬 수 있게 된다. 만일 리더가 검색 권한을 갖는 태그의 비밀값이 평문 형태로 저장되어 있다면, 공격자는 유출한 태그의 비밀값을 이용해 리더의 요청 메시지에 대해 정당한 태그인척 위장할 수 있게 된다. 이와 같은 공격을 방지하기 위해서는 리더 측에 저장되는 태그의 비밀값은 평문 형태가 아니라 비밀값을 검증할 수 있는 검증값 형태로 저장되어야 한다는 것이다. $f(id_j, t_j) \oplus X_i \oplus r_i$값은 제안한 프로토콜에서 태그의 비밀값에 대한 검증값으로 사용된다. 한편, 태그의 물리공격 안전성 측면에서는, 저가의 태그는 공격자의 물리적인 공격에 의해 태그의 비밀값을 노출 시킬 수 있는 가능성이 존재하기 때문에 물리공격 으로부터 안전하다고 볼 수는 없다.

• 재생공격 안전성 : 공격자는 도청을 통해 리더 및 태그가 전송한 메시지를 저장해 뒀다가 다시 재전송하는 공격을 수행할 수 있다. 본 논문에서는 이와 같은 재생공격에 대한 안전성을 보장하기 위해 기본적으로 요청 메시지를 수신한 모든 태그들이 응답 메시지를 발생시키게 하였으며, 또한 카운터값(c_r, c_t)을 이용하게 했다. 먼저, 공격자가 리더의 요청 메시지를 저장하였다가 이를 이용한 재생공격의 경우, 요청 메시지를 수신한 모든 태그들이 응답 메시지를 발생시키기 때문에 요청 메시지를 이용한 재생공격에 안전하게 된다. 만일 공격자가 태그의 응답 메시지들을 이용하여 재생공격을 수행하게 되더라도, 리더는 기대하는 카운터값을 이용하여 응답 메시지를 검증하기 때문에 공격자의 재생공격으로부터 안전하다.

[표 2]는 제안하는 프로토콜과, 선행연구[1-2,6] 와의 안전성을 비교한 표이다. 제안한 프로토콜이 3.1절의 보안요구사항을 만족시킴을 알 수 있다.

표 2. 안전성 비교
Table 2. comparison of security

안전성 항목	[1,2]	[5]	[6]	제안 프로토콜
메시지 기밀성	○	○	○	○
개체 인증	○	○	○	○
추적불가능성	X	△	○	○
물리공격 안전성	△	△	△	△
재생공격 안전성	X	○	○	○

○: 만족함, X: 만족하지 않음,
△: 부분적으로 만족함

4.2 효율성 분석

본 절에서는 제안하는 프로토콜과 선행연구[1-2][5][6]와의 비교 분석을 통해 효율성을 평가 한다. 다음 [표 3]은

선행연구와 제안 프로토콜에서 리더가 생성하는 요청 메시지와 태그가 요청 메시지를 수신하여 응답 메시지를 생성하기까지의 연산량을 비교한 표이다.

표 3. 연산량 비교
Table 3. Comparison of computational complexity

프로토콜	리더	태그
[1-2]	$3T(h)+2T(\oplus)+1T(r)$	$4T(h)+1T(\oplus)+1T(r)$
[5]	$3T(E)+2T(\oplus)+0T(r)$	$4T(E)+4T(\oplus)+1T(r)$
[6]	$2T(E)+1T(\oplus)+1T(r)$	$3T(E)+1T(\oplus)+1T(r)$
제안 프로토콜	$3T(h)+8T(\oplus)+2T(r)$	$4T(h)+4T(\oplus)+1T(r)$

$T(h)$: 해쉬 연산, $T(\oplus)$: 배타적 논리합 연산,
$T(E)$: 암호화 연산, $T(r)$: 난수생성 연산

[표 3]에서 연산량의 비교 결과, [1-2]의 프로토콜은 리더와 태그 측에서 7번의 해쉬 연산과 3번의 XOR 연산, 그리고 2번의 난수생성 연산을 수행한다. 제안 프로토콜에서는 7번의 해쉬 연산과 12번의 XOR 연산, 그리고 3번의 난수생성 연산을 수행한다. 제안 프로토콜이 [1-2]의 프로토콜에 비해 높은 연산량을 필요로 하는 이유는, [1-2]의 프로토콜이 제공하는 못하는 재생공격과 추적공격을 막기 위해 추가적인 연산이 필요했기 때문이다.

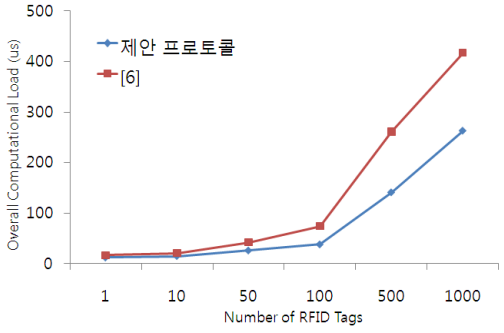

그림 11. 태그수의 증가에 따른 연산량 비교
Fig. 11. Comparison of computational costs on number of tag increase

같은 보안성을 제공하는 제안 프로토콜과 [5][6]과의 비교에 있어서는, 제안 프로토콜이 해쉬 연산과 XOR 연산만으로 이루어졌기 때문에, 5번 및 7번의 암·복호 연산을 수행해야 하는 [5][6]의 프로토콜보다 뛰어난 성능을 보여준다. 게다가 제안 프로토콜과 [6]의 프로토콜은 기본적으로 특정 그룹에 속한 모든 태그들의 응답 메시지를 처리해야 하기 때문에, 리더의 브로드캐스트 영역에 존재하는 RFID 태그의 수가 늘어날수록 [6]의 프로토콜이 필요로 하는 암호화 연산은 급격히 증가하게 된다. 다음 [그림 11]은 암호 연산 회수를 태그의 수로 가정 했을 때, 태그의 수에 따른 연산량을 비교한 그래프이다. [그림 11]에서와 같이, 문헌 [6]에서는 태그의 수가 증가할수록 필요로 하는 계산량이 급격히 증가하는 반면, 본 논문에서 제안한 프로토콜은 문헌 [6]보다 낮은 계산량을 필요로 한다.

V. 결 론

본 논문에서는 휴대용 리더를 소지한 사용자가 이동하면서 특정 태그를 검색할 수 있게 하는 RFID 태그 검색 프로토콜을 제안하였다. 제안한 프로토콜은 본 논문에서 분석한 RFID 태그 검색 프로토콜의 보안 요구사항을 만족한다. 또한 기존 선행연구[1-2]가 가지는 리더의 추적문제를 해결하였고, 해쉬연산과 XOR 연산만을 이용하기 때문에 암호화 연산을 사용하여 리더의 추적문제를 해결한 선행연구[5][6] 보다 효율성이 향상되었다.

향후 본 논문에서 제안한 RFID 태그 검색 프로토콜은 휴대성을 필요로 하는 다양한 RFID 응용 분야에서 적용될 수 있을 것으로 기대된다.

참고문헌

[1] C.C. Tan, B. Sheng, and Q. Li, "Serverless Search and Authentication Protocols for RFID", Pervasive Computing and Communications (PerCom) Workshops, pp. 3-12, March 2007.

[2] C.C. Tan, B. Sheng, and Q.Li, "Secure and Serverless RFID Authentication and Search Protocols", IEEE Transactions on Wireless Communications, vol. 7, no. 4, pp. 1400-1407, April 2008.

[3] 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. 187-192, April 2008.
[4] S.I. Ahamed, F. Rahman, E. Hoque, F. Kawsar, and T. Nakajima, "Secure and Efficient Tag Searching in RFID Systems using Serverless Search Protocol", International Jounal of Security and Its Applications (IJSIA), pp. 57-66, October 2008.
[5] T.Y. Won, J.Y. Chun, and D.H. Lee, "Strong Authentication Protocol for Secure RFID Tag Search Without Help of Central Database", Embedded and Ubiquitous Computing, pp. 153-158, December 2008.
[6] 천지영, 황정연, 이동훈, "이동형 리더 소지자의 프라이버시를 보호하는 RFID 태그 검색 프로토콜", 정보보호학회 논문지, 19(5), 59-69쪽, 2009. 10월
[7] I.C. Lin, S.C. Tsaur, and K.P. Chang, "Lightweight and Serverless RFID Authentication and Search Protocol", International Conference on Computer and Electrical Engineering, pp. 95-99, December 2009.
[8] M. Feldhofer and J. Wolkerstorfer, "Strong crypto for RFID tags - A comparison of low-power hardware implementations", IEEE International Symposium on Circuits and Systems, pp. 1839-1842, May 2007.
[9] 이상렬, "RFID 시스템의 개선된 인증 프로토콜", 컴퓨터 정보학회논문지, 제 12권, 제 4호, 69-75쪽, 2007년. 12월.

저 자 소 개

최 현 우

2009년 2월 : 순천향대학교 정보보호학과 졸업
2009년 3월~현재 : 순천향대학교 정보보호학과 석사과정
관심분야 : IPTV 보안, 스마트그리드 보안, USN 보안, 역추적

여 돈 구

2009년 2월 : 순천향대학교 정보보호학과 졸업
2009년 3월~현재 : 순천향대학교 정보보호학과 석사과정
관심분야 : 정보보호, USN 보안, 클라우드 컴퓨팅 보안, IPTV 보안, 역추적

장 재 훈

2009년 2월 : 순천향대학교 정보보호학과 졸업
2009년 3월~현재 : 순천향대학교 정보보호학과 석사과정
관심분야 : 역추적, IPTV 보안, USN 보안

염 흥 열

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