情報保護學會論文誌
第19卷 第5號, 2009. 10

이동형 리더 소지자의 프라이버시를 보호하는 RFID 태그 검색 프로토콜

천 지 영,[1†] 황 정 연,[2] 이 동 훈[1‡]
[1]고려대학교 정보경영공학전문대학원, [2]한국전자통신연구원

RFID Tag Search Protocol Preserving Privacy of Reader Holders

Ji Young Chun,[1†] Jung Yeon Hwang,[2] Dong Hoon Lee[1‡]
[1]Graduate School of Information Management and Security, Korea University
[2]Electronics and Telecommunications Research Institute

요 약

사용자가 특정 태그를 찾기 위해 사용하는 RFID 태그 검색 시스템은 재고관리, 물류, 유통, 미아 찾기 등 다양한 환경에 사용될 수 있으며 이 기법은 RFID 시스템을 이용한 응용 분야 중 하나로 연구가 활발히 진행되고 있다. 기존의 RFID 시스템을 이용한 다른 기법들과는 달리 RFID 태그 검색 기법에서는 특히 특정 태그를 찾기 위해 리더의 이동성이 강조되어지는데, 만약 이동형 리더를 가지고 무선 통신이 불가능한 지역에 가게 되었을 경우 중앙 데이터베이스로부터 태그에 대한 정보를 얻어올 수 없어 실시간 검색이 불가능한 상황에서도 검색이 가능해야 한다. 또한 RFID 태그 검색 프로토콜에서는 사용자가 태그가 아닌 이동형 리더를 소지하기 때문에 이동형 리더 소지자에 대한 프라이버시가 고려되어야 한다. 리더의 신호는 태그의 신호보다 도청이 수백 배 더 쉽기 때문에 이동형 리더 소지자의 프라이버시 문제는 매우 중요하다. 최근 이러한 문제를 해결하기 위한 RFID 태그 검색 기법들이 제안되고 있으나 이 기법들은 모두 이동형 리더 소지자에 대한 프라이버시 문제를 고려하지 않음으로써 이동형 리더 소지자의 프라이버시 침해가 심각하다. 따라서 본 논문에서는 이러한 이동형 리더 소지자의 프라이버시 문제를 해결하면서도 수동형 태그에 적합한 안전한 태그 검색 프로토콜을 제안한다.

ABSTRACT

RFID tag search system which is used to find a specific tag has an application such as asset management, supply chain, and this search scheme has been given much attention so far. In RFID tag search system, especially, mobility of the reader is important in order to search tags. Therefore, even though the handheld reader cannot connect with the central database because of unreliable wireless connection or remote location, handheld reader should search the specific tag without help of the central database. In addition, in RFID tag search system, users hold not the tag but the reader, the privacy of users should be considered. Since the signal strength of the reader is stronger than that of the tag, the privacy of the reader holder is very important. Recently, in order to solve these problems, a number of RFID tag search schemes have been proposed. However, since these schemes did not consider the privacy of reader holders, there are serious privacy breaches of reader holders. In this paper, we propose efficient RFID tag search protocol for passive tags. Our proposed scheme preserves the privacy of reader holders.

Keywords: RFID, Privacy, Security, Search protocol, Passive tag

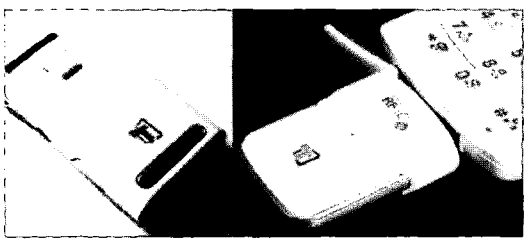
접수일(2009년 4월 28일), 수정일(2009년 8월 14일), 게재확정일(2009년 9월 10일)

† 주저자, jychun@korea.ac.kr
‡ 교신저자, donghlee@korea.ac.kr

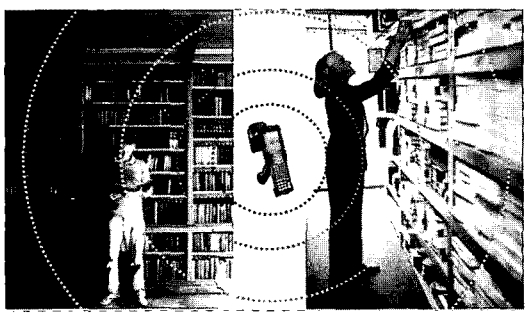
I. 서 론

RFID(Radio Frequency IDentification) 시스템은 기존의 바코드 시스템을 대체할 미래형 인증 기술로 각광받고 있으며 현재 다양한 응용분야에서 사용되고 있다. 최근에는 핵심 응용분야 중 하나로 태그(Tag)가 부착된 사물을 찾기 위한 RFID 태그 검색 시스템(RFID Tag Search System)이 활발히 연구되고 있다. RFID 태그 검색 시스템은 사용자가 찾고자 하는 특정 태그가 리더(Reader)로부터 일정 범위 내에 존재하는지를 확인할 수 있는 시스템이다. 기존의 RFID 인증 기법들[1-12]과는 다르게 RFID 태그 검색 시스템에서는 (특정 태그를 효율적으로 찾기 위해) 리더의 이동성이 강조되어진다. 이동형 리더 기능은 휴대가 간편한 휴대폰이나 PDA(Personal Digital Assistants) 등에 장착되어 사용될 수 있으며[그림 1], 이미 통신회사 등에서 시범서비스를 실시하고 있다.

다양한 부가 서비스를 창출할 수 있는 RFID 태그 검색 시스템은 [그림 2]와 같이 도서관에서 읽고 싶은 책을 찾는 경우 또는 창고에 있는 물건들에 대한 재고관리 등에 사용될 수 있으며 교보문고에서는 이미 모바일 RFID(동글)를 이용하여 도서 정보 조회 서비스를 시범적으로 실시하고 있다.



[그림 1] 모바일 RFID (동글)



[그림 2] RFID 태그 검색 시스템

또한 최근 상습 성범죄자의 위치를 추적·감시할 수 있도록 전자발찌를 찬 사람들이 출소 되었는데 이러한 상습 성범죄자가 일정한 범위 내에 존재하는지를 확인하기 위해 RFID 태그 검색 시스템이 이용될 수도 있다. 그리고 이러한 시스템을 통해 국외로 반출이 금지된 물품이 공항 검색대를 통과하는지도 알아낼 수 있을 것이다.

이동형 리더의 사용은 사용자의 편의성을 증대시키는 반면 기존의 고정형 리더(Static Reader)의 사용에 비해 추가적으로 고려해야할 보안 문제들을 발생시킨다. 가장 중요한 보안 문제 중 하나는 이동형 리더 소지자의 프라이버시 문제이다. 리더 신호의 세기는 태그 신호의 세기보다 수백 배 강해서 도청이 훨씬 더 쉽기 때문에 이동형 리더 소지자의 동선(動線, Traffic Line)이 쉽게 노출될 수 있다. 따라서 이동형 리더 소지자에 대한 프라이버시 문제는 매우 중요하게 다루어져야 한다.

또한 사용자가 이동형 리더를 가지고 무선 통신이 불가능한 지역에 가게 되었을 경우 또는 시스템 과부하 등으로 인해 중앙 데이터베이스로부터 태그에 대한 정보를 얻어올 수 없어 실시간 검색이 불가능한 상황에 대해서도 시스템 가용성(Availability)을 보장해야 한다. RFID 시스템 가용성은 미국 국가표준기술연구소(NIST, National Institute of Standards and Technology)에서 발표한 RFID 보안 가이드라인[13]에 포함된 RFID 시스템에 대한 주요 보안 측정(Security Measures) 요소 중 하나이다.

마지막으로 이동형 리더는 분실이 쉽기 때문에 분실 시 데이터 노출에 대한 안전성(Leakage Resilience)도 고려되어야 한다. 분실된 리더에 저장되어 있는 태그 정보를 이용하여 태그를 위조하고 위조된 태그로 정당한 리더와의 인증을 통과하는 공격은 분실이 잦은 이동형 리더 환경에서 쉽게 일어날 수 있다. 이동형 리더는 많은 태그들에 대한 정보를 저장하고 있기 때문에 데이터 노출에 대한 안전성이 보장되지 않는다면 다량의 위조 태그를 생성할 수 있게 되어 심각한 보안 문제를 초래하게 된다.

최근 RFID 태그 검색 기법들[14-16]이 제안되었으나 이동형 리더 소지자에 대한 프라이버시 문제 등을 고려하지 않음으로써 심각한 보안취약점을 가지고 있다. 또한 알려진 기법들은 다중 이동형 리더를 사용하는 환경에서는 적합하지 않다. 본 논문에서는 기존 RFID 태그 검색 기법에서 고려하지 않은 이동형 리더 사용 시 추가적으로 발생하는 문제들에 대해 분석

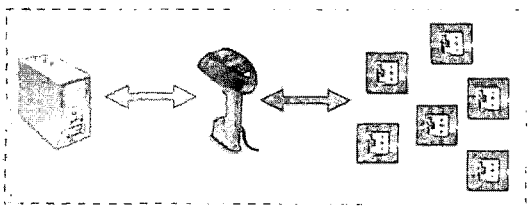
하고 이러한 문제들에 안전한 효율적인 RFID 태그 검색 프로토콜을 제안한다.

본 논문의 공헌은 다음과 같다. 본 논문에서 제안하는 기법은 이동형 리더 소지자의 프라이버시 문제를 해결한 최초의 태그 검색 기법이다. 제안하는 기법은 전력 소비, 저장량, 연산 속도 측면에서 수동형 태그에 가장 적합한[17] AES-128(Advanced Encryption Standard)을 사용하여 이동형 리더가 항상 같은 정보를 내보내 동선이 노출되는 문제를 해결하였다. 그리고 각각의 리더가 중앙 데이터베이스에 접속하지 않고 태그를 검색할 수 있도록 태그 검색을 위해 필요한 값들을 저장하게 함으로써 가용성 문제를 해결하였다. 마지막으로 리더 분실에 대한 안전성을 보장하기 위해 각각의 리더가 같은 태그 검색을 위해 저장한 값을 모두 다르게 함으로써 리더 분실 시 다량의 태그 위조 가능성을 막았다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구에 대해 살펴보고 3장에서는 RFID 태그 검색 프로토콜을 제안한다. 4장에서는 제안하는 프로토콜의 안전성과 효율성을 분석한 후 5장에서 결론을 맺는다.

II. 관련 연구

특정한 태그를 찾기 위해 기존에 제안된 RFID 인증 프로토콜들[6-11]을 사용할 수 있다. 리더가 주위 태그들에게 신호를 보내 태그들을 모두 인증하여 찾고자하는 태그가 있는지를 확인함으로써 태그에 대한 검색을 할 수 있다. 하지만 [그림 3]과 같은 인증 프로토콜의 경우 하나의 태그를 검색하기 위해 일반적으로 최대 데이터베이스 내에 있는 태그 수만큼의 연산이 필요하게 되는데 이는 태그의 익명성 보장을 위해 필요하다. 만약 데이터베이스가 저장하고 있는 태그의 수를 n개라고 하고 리더 주위에 있는 태그의 수를 k개라고 하면 리더는 최대 $k \times n$번의 연산을 수행해야 하기 때문에 인증 프로토콜을 그대로 적용하여 검색 프로토콜을 구성하는 것은 효율적이지 못하다.



[그림 3] RFID 인증 프로토콜

최근 효율적이고 안전한 RFID 태그 검색을 위한 프로토콜들[14-16]이 제안되고 있다. 문헌 [14,15]에서는 신뢰기관인 CA(Certificate Authority)가 모든 태그 T_i에 대한 비밀키 t_i를 저장하고 있고 정당한 리더 R_j와 안전한 채널을 통해 통신한다고 가정한다. 각각의 리더 R_j는 자신의 식별자인 r_j와 검색 권한을 갖는 태그에 대한 접근 리스트(Access List)인 L_j를 갖는다. 각각의 태그 T_i는 자신의 식별자인 id_i와 비밀키 t_i, 그리고 해쉬함수인 $h(.)$를 저장한다.

이동형 리더가 중앙 데이터베이스와 통신할 수 없는 상황에서의 검색 문제를 해결하기 위해 각각의 리더들은 자신의 검색 권한에 따라 CA로부터 태그를 검색할 수 있는 값들을 받아온다. 하지만 이동형 리더는 쉽게 분실될 수 있기 때문에 태그의 비밀키 값을 리더에 직접 저장하는 건 위험부담이 크다. 따라서 각각의 리더 R_j는 접근 권한을 갖는 태그들에 대한 정보를 담은 접근 리스트(Access List)인 L_j를 CA로부터 다음과 같이 받아온다[그림 4]. 이 때, 함수 $f(.,.)$는 해쉬함수이다.

$$L_j = \begin{cases} f(r_j,t_1) & : id_1 \\ \cdots & : \cdots \\ f(r_j,t_n) & : id_n \end{cases}$$

[그림 4] 접근리스트 L_j

따라서 리더 R_j는 해쉬함수의 일방향성(One-way)으로 인해 태그의 비밀키인 t_i값을 알지는 못하지만 접근 리스트를 이용하여 특정 태그에 대한 검색을 할 수 있게 된다.

문헌 [14,15]에서는 4가지 검색 프로토콜을 제안하였다. 첫 번째 검색 프로토콜은 다음 [그림 5]와 같다.

$$R_j \rightarrow T^* : h(f(r_j,t_i) \| n_r) \oplus id_i, n_r, r_j$$

$$T^* : Derive\ h(f(r_j,t) \| n_r)\ \text{and}\ XOR\ with\ h(f(r_j,t_i) \| n_r) \oplus id_i$$
$$: If\ id = id_i$$

$$R_j \leftarrow T_i : h(f(r_j,t_i) \| n_t \| n_r) \oplus id_i, n_t$$

[그림 5] 문헌 [14,15]의 첫 번째 프로토콜

리더는 자신이 검색할 태그에 대한 값을 만들어 주위의 태그들에게 보낸다. 리더 주위의 모든 태그들은

리더로부터 온 값을 계산하여 자신의 id_i와 일치하면 리더에게 인증값을 생성하여 보내준다. 이 프로토콜은 문헌 [14,15]에서도 지적되었듯이 재생공격이 가능하다. 공격자가 리더가 태그에게 보냈던 값을 저장해 두었다가 재사용하게 되면 항상 같은 태그가 대답하게 되므로 어떤 태그인지는 알지 못하지만 특정 태그에 대한 검색이 가능하게 된다. 따라서 첫 번째 검색 프로토콜의 재생공격에 대한 취약성을 개선하고자 3가지 개선된 기법을 추가적으로 제시한다. 리더의 질의에 대해 하나의 태그가 대답하는 것 자체가 태그를 식별하는데 사용될 수 있기 때문에 리더의 질의에 대해 하나의 태그가 대답하는 한 재생공격을 막기는 어렵다. 따라서 리더의 질의에 대해 리더 주위 태그 중 일부의 태그가 동시에 대답하게 함으로써 재생공격을 막는 기법으로 프로토콜 3과 프로토콜 4를 제안하였다.

재생공격을 막는 방법 중 하나로 타임스탬프를 사용하는 방법이 있으나 저가의 태그에 타임스탬프 기능을 추가하는 것은 현실적으로 어렵다. 따라서 난수의 재사용을 체크하여 재생공격을 막는 방법을 이용한 프로토콜 2를 제안하였다. 이 기법을 사용하기 위해 태그가 이전 검색에서 리더에 의해 사용되었던 난수를 최대 m개 저장하고 있어야하는데 이 방법은 저장량이 작은 태그에서 사용하기 어렵고 또한 문헌 [14,15]에서 지적한 대로 저장되기 이전에 사용되었던 난수 값으로 재생공격을 하게 되면 재생공격에 취약하게 된다.

앞에서 지적한 바와 같이 문헌 [14,15]에서 제안된 기법은 리더 소지자의 프라이버시 침해 문제를 발생시킨다. 제안된 4가지 기법들 모두 리더가 태그를 찾기 위한 질의에서 r_j를 사용하는데 이는 이동형 리더에 대한 식별자로 고정된 값이다. 따라서 r_j 값을 추적함으로써 이동형 리더 소지자의 위치 추적이 가능하게 된다. 리더 신호에 대한 도청이 태그 신호에 대한 도청보다 훨씬 쉽기 때문에 심각한 프라이버시 문제를 발생시킨다.

[14,15] 기법 이후 이를 개선한 기법이 제안되었다 [16]. 이 기법은 [14,15] 기법이 만족하지 못하는 전방향 안전성(Forward Secrecy) 문제를 해결하고 응용환경을 제시하였으나 이 기법 역시 리더 소지자의 프라이버시 문제를 해결하지 못하였다. 또한 전방향 안전성을 위해서 리더와의 정상적인 통신이 이루어진 후 일방향 함수(One-way Function)를 이용하여 태그의 비밀값을 갱신(Update)하는데 이 때 태그와 리더 사이의 동기화 문제가 발생하게 된다. 문헌 [16]은 이러한 비동기화 문제를 해결하기 위해 태그와 리더가 상호 인증이 이루어진 후에 서로의 값을 갱신하도록 설계하였다. 하지만 이러한 방법에서는 리더의 개수에 제약이 따른다. 여러 개의 리더를 사용하여 태그를 검색하는 경우 A 리더와의 통신 후 태그가 값을 갱신하였다고 하면 A 리더 이외의 다른 리더들은 갱신된 사실을 알 수 없기 때문에 비동기화 문제가 발생하게 된다. 따라서 [16] 기법은 여러 개의 리더를 사용하는 환경에는 적합하지 않다.

III. RFID 태그 검색 프로토콜

3.1 시스템 가정 사항

RFID 태그 검색 시스템은 [그림 6]과 같이 중앙 데이터베이스를 가진 신뢰기관과 이동형 리더 그리고 태그로 구성된다. 신뢰기관과 이동형 리더 사이의 통신 채널은 안전한 채널이고 이동형 리더와 태그 사이의 통신 채널은 안전하지 않은 채널이라고 가정한다. 신뢰기관의 서버와 이동형 리더는 무선 통신을 하긴 하지만 둘 다 강력한 컴퓨팅 파워를 갖기 때문에 암호학적인 방법을 통한 안전한 채널의 형성이 가능하므로 안전한 채널이라고 가정한다. 하지만 태그와 이동형 리더의 무선 주파수를 이용한 통신은 태그의 자원 제약성 때문에 안전한 채널을 가정하기 힘들다. 따라서 안전하지 않은 채널에서 태그와 리더사이의 통신에 안전성을 주기위한 프로토콜의 설계가 필요하다.

[그림 6] 시스템 구성도

3.1.1 신뢰기관(TTP: Trusted Third Party)

신뢰기관은 항상 신뢰되는 기관으로 태그에 대한 정보들을 저장한 중앙 데이터베이스를 가지고 있다. 신뢰기관은 이동형 리더들에게 태그 검색이 가능하도록 하기 위해 태그의 비밀키를 가공한 값을 전달한다. 따라서 신뢰기관은 항상 온라인일 필요가 없기 때문에 태그의 정보들은 좀 더 안전하게 보호되어질 수 있다.

3.1.2 이동형 리더(Handheld Reader)

이동형 리더는 신뢰기관으로부터 받은 값을 이용하여 찾고자하는 태그가 일정한 통신 반경 내에 존재하는지를 검색한다. 리더는 태그의 동작에 필요한 전원을 공급하기 위해 전파의 세기가 강해야 하며 보통 리더의 통신 반경은 100m라고 가정한다[18].

3.1.3 태그(Tag)

태그는 수동형 태그(Passive Tag)로 내장된 전원 없이 리더가 발생시키는 전파로부터 동작에 필요한 전원을 만들어 사용한다. 보통 수동형 태그의 통신 반경은 3m라고 가정하고[18], UHF(UltraHigh Frequency) 대역(800~960MHz)에서 통신한다.

RFID 시스템에서 높은 안전성을 보장하기 위해 암호학적인 알고리즘(Cryptographic Algorithm)의 사용은 불가피하다. 수동형 태그에 적합한 암호 알고리즘들을 구현하여 이를 분석한 Feldhofer 등의 결과를 살펴보면 AES(Advanced Encryption Standard)의 사용이 수동형 태그에 가장 적합하다[17]. [표 1]은 Feldhofer 등의 분석 결과를 나타낸다.

Feldhofer 등은 전력 소비(Imean), 암호 알고리즘 구현을 위해 필요한 칩 영역(Chip Area), 그리고 연산을 위해 필요한 클럭의 수(Clock)의 3가지 측면에서 알고리즘을 분석하였다. 전력 소비의 경우 최대 15μA 이상을 소모하면 통신을 위한 전력까지 소모되어 태그의 통신 반경이 줄어들게 된다. 칩 영역을 제한하는 것은 기술적인 이유보다 경제적인 이유가 큰데 이는 칩의 실리콘 영역(Silicon Area)이 태그의 가격을 결정하기 때문이다. 보통 보안을 위한 칩 영역은 1,000에서 10,000 게이트(gate)정도로 가정한다. 마지막으로, 연산을 위해 필요한 클럭의 수는 태그의 응답 시간(Response Time)에 영향을 미치는데 ISO 15693 표준을 따르는 HF 태그의 경우를 예로 살펴보면 태그가 리더의 요청에 대해 300μs 내에 응답을 해야 하기 때문에 클럭의 수가 알고리즘 분석에서 중요한 요소가 된다.

[표 1] 암호 알고리즘 비교 분석

Algorithm	Security [bits]	Imean [μA@ 100kHz]	Chip Area [GE]	Clock [cycles]
SHA-256	128	5.86	10,868	1,128
SHA-1	80	3.93	8,120	1,274
MD5	80	3.16	8,001	712
AES-128	128	3.0	3,400	1,032
ECC-192	96	18.85	23,600	502,000

향후 모든 사물에 태그를 부착하게 되는 환경에서 태그의 가격은 시스템 구축에 있어서 매우 중요한 요소로 작용하게 될 것이다. 마이크로칩의 밀도가 18개월마다 2배로 늘어난다는 Moore의 법칙에 의해 향후 태그의 성능이 향상되어 수용할 만한 가격으로 수동형 태그에 암호학적인 프리미티브(Primitive)를 구현하는 것이 가능할 것이다. 하지만 기업은 항상 비용이 적게 드는 쪽을 원할 것이고 방대한 양을 사용하는 태그의 가격이 낮으면 낮을수록 좋기 때문에 태그의 기능은 크게 변화되지 않으면서 가격이 떨어지게 될 것이다[7]. 따라서 태그에 최대한 값싼 가격을 지불하면서도 안전한 암호 알고리즘의 구현이 필요하기 때문에 AES-128의 사용이 안전성뿐만 아니라 경제적인 측면에서도 수동형 태그에 적합하다. 따라서 본 논문에서는 수동형 태그에 AES-128 알고리즘이 구현되어 있다고 가정한다.

3.2 보안 및 프라이버시 요구 사항

공격자는 RFID 시스템에 대한 다양한 공격을 통해 보안 및 프라이버시 문제를 발생시킨다. 공격자의 공격 방법에 따라 가능한 공격들은 다음과 같다. 공격자는 태그와 리더 사이의 통신을 도청(Eavesdropping)을 할 수 있고 도청한 데이터를 재전송하는 재생공격(Replay Attack)을 할 수 있다. 또한 정당하지 않은 리더를 사용하여 태그로부터 얻은 정보를 이용해 정당한 리더의 요청에 합리적인 태그로 가장하여 응답하는 스푸핑 공격(Spoofing Attack)도 가능하다. 저가의 태그는 메모리를 보호하는(Tamperproof) 장치가 없기 때문에 공격자는 물리적인 공격(Tampering Attack)을 통하여 메모리에 저장된 값을 모두 알아낼 수도 있다.

위와 같은 공격에 의해 발생할 수 있는 보안 문제 이외에도 사용자가 태그가 내장된 물건들을 몸에 지니게 됨으로써 발생 가능한 사용자 프라이버시 침해 문제로 사용자의 개인 정보 노출과 사용자의 위치 추적 문제가 있다. 태그는 리더의 질의에 대해 자신의 고유 정보를 노출하기 때문에 사용자가 다른 사람에게 알리고 싶지 않은 민감한 정보를 제삼자에게 노출 시킬 수 있고 사용자가 태그가 내장된 물건을 지니고 다니는

동안 태그의 고유 정보를 이용하여 사용자의 이동 경로를 추적할 수도 있다.

이렇게 다양한 공격들을 통해 발생할 수 있는 보안 및 프라이버시 문제 해결을 위해 RFID 프로토콜이 만족해야하는 요구사항은 다음과 같다.

• 기밀성(Confidentiality): 태그와 리더사이의 통신을 도청하더라도 도청된 메시지로부터 어떠한 의미 있는 정보도 알아낼 수 없도록 기밀성을 만족해야 한다.

• 태그에 대한 익명성(Anonymity): 태그에서 리더로 전송되는 통신을 통하여 사물 및 개인에 대한 감시 및 위치 추적이 이루지지 않도록 하기 위해 구별 불가능성(Indistinguishability)과 전방향 안전성(Forward Secrecy)을 만족해야 한다. 구별 불가능성은 태그에서 전송되는 데이터를 보고 어떠한 태그에서 전송되는 값인지를 알 수 없어야 한다는 것이다. 전방향 안전성은 공격자가 현재 태그에 저장된 데이터의 값을 알았다 하더라도 태그가 이전에 생성한 데이터를 추적할 수 없어야 한다는 것이다. 따라서 전방향 안전성을 만족하면 공격자가 현재 알고 있는 태그의 데이터를 이용하여 이전에 태그가 생성하였던 데이터들에 대한 연관성을 줄 수 없다.

• 인증(Authentication): 리더는 자신과 통신하는 태그가 정당한 태그라는 것을 확신할 수 있어야한다. 만약 리더가 태그의 정당성을 인증하는 과정을 수행하지 않는다면 공격자는 재생 공격 등을 통하여 특정 태그로 위장할 수 있다.

위의 일반적인 RFID 시스템이 만족해야하는 요구사항 중 RFID 태그 검색 시스템에서 만족하기 힘든 요구사항은 태그에 대한 전방향 안전성이다. 2장 관련 연구에서 언급하였듯이 전방향 안전성을 만족하기 위해 태그의 비밀값을 일방향성을 만족하는 값으로 계속 갱신하게 되면 모든 이동형 리더들과의 동기화 문제를 해결해야 하는데 이러한 문제를 해결하기는 어려울 뿐만 아니라 추가적인 연산비용이 발생하게 된다. 또한 이동형 리더들과의 동기화를 위해 값을 갱신하지 않는다면 전방향 안전성을 만족하기 힘들다. RFID 태그 검색 시스템은 보통 사용자가 태그가 아닌 이동형 리더를 소지하게 되므로 본 논문에서는 태그에 대한 전방향 안전성은 고려하지 않는다. 태그에 대한 전방향 안전성을 고려하지 않기 때문에 공격자가 태그에 저장된 값을 알아냈을 때 기존의 통신 기록을 이용하여 그 태그가 이전에 생성한 데이터를 추적할 수 있게 된다. 이러한 추적을 통해 태그의 위치를 추적할 수 있게 되긴 하지만 태그 검색 환경은 보통 사용자가 태그를 소지하는 환경이 아니기 때문에 태그 소지자의 프라이버시 문제가 발생하지 않는다.

위에서 언급한 일반적인 RFID 시스템이 만족해야하는 요구사항 외에 RFID 태그 검색 시스템에서는 다음과 같은 추가적인 요구사항을 만족해야 한다.

• 리더에 대한 익명성(Anonymity): 기존 고정형 리더 환경에서는 리더 소지자에 대한 프라이버시를 고려하지 않았지만 이동형 리더 환경에서는 이동형 리더를 사용자가 소지하게 됨으로써 리더 소지자에 대한 프라이버시가 태그 소지자에 대한 프라이버시보다 더 중요시된다. 태그는 통신반경이 $3m$ 이내이고 리더는 $100m$ 이내이기 때문에 태그에서 나오는 신호는 태그 주위에서만 도청이 가능하지만 리더의 경우는 광범위한 영역에서 도청이 가능하다. 태그 신호에 대한 도청이 가능한 영역이 $9\pi m^2$ 라면 리더 신호에 대한 도청이 가능한 영역은 $10{,}000\pi m^2$ 이므로 리더에 대한 도청이 1,000배 가량 더 쉽다. 따라서 리더에서 태그로 전송되는 통신에 대해서도 구별 불가능성과 전방향 안전성을 만족해야 한다.

• 가용성(Availability): 사용자가 이동형 리더를 가지고 무선 통신이 불가능한 지역에 가게 되었을 경우 중앙 데이터베이스로부터 태그에 대한 정보를 얻어올 수 없어 실시간 검색이 불가능한 상황에서도 태그를 검색할 수 있는 시스템 가용성(Availability)을 보장해야 한다.

• 리더 분실에 대한 안전성(Leakage Resilience): 이동형 리더는 분실이 쉽기 때문에 분실 시 데이터 노출에 대한 안전성도 고려해야 한다. 공격자는 분실된 리더에 저장된 태그의 값을 이용하여 다른 정당한 리더에게 정당한 태그인 척 하는 공격(Impersonation Attack)을 할 수 있다. 따라서 공격자의 이러한 공격에 안전한 프로토콜을 설계하여야 한다.

3.3 제안 프로토콜

제안하는 RFID 태그 검색 프로토콜은 초기 설정

단계와 태그 검색 단계로 나뉜다. 초기 설정 단계에서는 중앙 데이터베이스에 접속이 불가하여 검색이 불가능한 상황에서 태그 검색이 가능하도록 하기 위해 이동형 리더가 태그에 대한 접근 리스트를 저장하게 되는데 이러한 방법은 태그의 수가 매우 많을 경우 중앙 데이터베이스가 리더와 태그 사이의 모든 통신에 개입할 때 중앙 데이터베이스의 과부하로 인해 정상적인 서비스가 이루어지지 않는 경우에도 사용이 가능하다.

3.3.1 초기 설정 단계(Setup Phase)

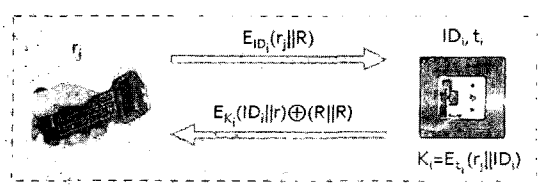
각각의 이동형 리더 R_j의 식별자를 r_j라 하고 태그 T_i의 식별자를 ID_i, 비밀키를 t_i라고 한다. 신뢰기관은 각각의 이동형 리더 R_j에게 〔표 2〕와 같은 접근 리스트 L_j를 안전하게 전송한다. 이 때 $E_t(r\|ID)$는 메시지 $r\|ID$를 비밀키 t로 AES-128 알고리즘을 이용하여 암호화한 암호문을 나타낸다. AES의 평문 길이는 128비트이므로 r과 ID는 64비트이고 비밀키 t는 128비트이다. AES-128의 선택 평문 공격(Chosen Plaintext Attack)에 대한 안전성으로 인해 리더 R_j는 $E_{t_i}(r_j\|ID_i)$로부터 태그 T_i에 대한 비밀키 t_i를 알아낼 수 없다.

〔표 2〕 접근 리스트 L_j

ID	PW
ID_1	$E_{t_1}(r_j\|ID_1)$
...	...
ID_n	$E_{t_n}(r_j\|ID_n)$

3.3.2 태그 검색 단계(Tag Search Phase)

리더 R_j가 태그 T_i를 검색하기 위한 RFID 태그 검색 프로토콜은 〔그림 7〕과 같다. 실제로 리더 주위의 태그들이 모두 리더의 요청에 응답하지만 〔그림 7〕에서는 리더 R_j가 찾고자 하는 태그 T_i의 응답만을 나타내었다.



〔그림 7〕 RFID 태그 검색 프로토콜

1) $R_j \rightarrow T^*: E_{ID_i}(r_j \| R)$

리더 R_j는 태그 T_i를 검색하기 위해 64비트 난수 R을 선택한 후 태그 T_i의 식별자인 ID_i를 비밀키로 하여 자신의 식별자 r_j와 난수 R을 암호화한 암호문 $E_{ID_i}(r_j \| R)$를 생성하여 주위의 태그들에게 전송한다.

2) $T^*: K_i = E_{t_i}(r_j \| ID_i)$

리더로부터 메시지를 받은 태그들은 자신의 식별자인 ID_i'을 이용하여 암호문 $E_{ID_i}(r_j \| R)$을 복호화한 메시지를 64비트씩 나눈 후 r_j'과 R을 얻는다. 모든 태그들은 자신의 비밀키 t_i'을 이용하여 $K_i' = E_{t_i'}(r_j' \| ID_i')$을 계산한다.

3) $R_j \leftarrow T^*: E_{K_i'}(ID_i' \| r') \oplus (R' \| R')$

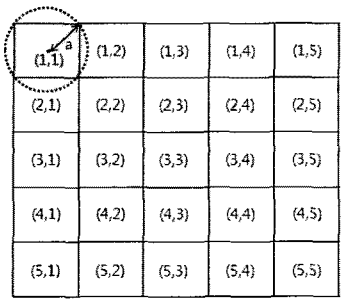
각각의 태그들은 임의의 난수 r'을 선택하여 리더의 요청에 대한 응답 $E_{K_i'}(ID_i' \| r') \oplus (R' \| R')$를 계산한 후 리더에게 전송한다. 실제로 리더 R_j가 검색하고자하는 태그 T_i만이 〔그림 7〕과 같이 정당한 값을 생성하여 보낼 수 있다.

4) $R_j: E_{K_i}(ID_i \| r) \oplus (R \| R)$

리더 R_j는 태그들로부터 받은 값 $E_{K_i'}(ID_i' \| r') \oplus (R' \| R')$에 자신이 선택한 난수 $R\|R$을 XOR 하여 얻은 값을 태그 T_i에 대해 접근 리스트 L_j에 저장된 값 $E_{t_i}(r_j \| ID_i)$을 비밀키 K_i로 하여 복호화 한 후 ID_i를 확인한다. 만약 자신이 찾고자하는 태그 T_i의 식별자 ID_i와 같다면 현재 자신이 위치한 곳으로부터 반경 $3m$ 이내에 자신이 찾고자하는 태그 T_i가 있음을 알 수 있다.

3.4 응용 환경

제안하는 기법은 재고관리, 물류, 유통 등 다양한 환경에 적용이 가능하다. 일례로 RFID 검색 시스템을 기록물 보존소에 적용시킨 예를 살펴보자. 기록물 보존소에는 많은 문서들이 보관되어 있다. 이러한 문서들은 보안등급이 있어 열람자들에게 보안등급별로 문서를 열람할 수 있는 권한이 주어진다. 모든 문서에는 수동형 RFID 태그가 부착되어 있고 열람자들은 자신에게 열람이 허가된 문서들 중 원하는 문서를 찾기를 원한다. 이러한 환경에서는 고정형 리더보다 이



〔그림 8〕 기록물 보존소

동형 리더의 사용이 적합하다. 만약 기록물이 보존되어 있는 장소가 〔그림 8〕과 같다고 가정해보자. 고정형 리더를 설치하여 태그를 검색한다면 수동형 태그의 통신반경이 $3m$ 이내이므로($a \leq 3$) 그림처럼 각각의 셀로 나누고 각 셀의 중심에 고정형 리더를 배치하여야 한다. 〔그림 8〕과 같은 경우 고정형 리더는 25개나 필요하게 된다. 따라서 검색 환경에서 고정형 리더의 사용은 좁은 공간에 고가의 리더가 많이 필요하게 됨으로써 가격 면에서 효율적이지 못하다. 또한 태그가 밀집되어 있지 않은 경우라면 낭비가 더욱 심하게 된다. 따라서 이러한 검색 환경에서는 이동형 리더의 사용이 더 적합하다.

하지만 이동형 리더를 사용할 때는 기록물 보존소의 전 영역을 모두 검색하기 위한 동선(Traffic Line)을 고려해야 한다. 또한 현재 리더가 위치한 곳으로부터 태그의 통신 반경인 $3m$ 이내에 찾고자하는 태그가 존재한다는 것만 알 수 있기 때문에 정확한 위치를 알게 되는 것은 아니다. 하지만 미아 찾기와 같이 태그의 밀도가 낮은 환경에서는 유용하게 사용될 수 있다. 자신의 위치로부터 $3m$ 이내의 미아는 육안으로 확인이 가능하기 때문이다.

또한 제안하는 기법은 재고관리에 더욱 적합하다. 방대한 창고에 특정 물건이 존재하는지를 확인하는 재고관리 환경에서는 정확한 위치에 대한 정보 보다는 존재 유무에 관심이 있기 때문에 태그 검색 기법은 재고관리 환경에서 유용하게 사용될 수 있다.

IV. 분 석

4.1 안전성 분석

본 절에서는 제안하는 기법이 3장에서 분석한 보안 및 프라이버시 요구사항을 만족함을 보인다.

• 기밀성(Confidentiality): 리더에서 태그로 전달되는 값은 리더가 찾고자하는 태그의 식별자로 암호화 되어 있으므로 기밀성을 만족한다. 실제로 리더가 찾고자하는 태그가 어떤 태그인지 공격자 입장에서는 알지 못하기 때문에 공격자는 정당한 값을 복호화할 수 없으므로 이 메시지로부터 어떠한 정보도 알아낼 수 없다. 태그에서 리더로 전달되는 값 역시 정당한 리더와 태그만이 알 수 있는 값으로 암호화되어 있으므로 기밀성을 보장한다.

• 태그에 대한 익명성(Anonymity): 태그는 리더의 요청에 대해 매번 자신이 임의로 선택한 난수 r을 이용하여 응답하므로 공격자 입장에서는 이 값이 어떠한 태그에서 나온 값인지 구별 불가능하기 때문에 구별 불가능성을 만족한다.

• 인증(Authentication): 제안하는 기법에서 리더는 태그와 공유한 값을 통해 자신과 통신하는 태그가 정당한 태그라고 확신할 수 있게 된다. 또한 시도-응답(Challenge-Response) 기법을 사용하여 리더와 태그 모두 자신이 생성한 난수를 사용하기 때문에 재생 공격을 막을 수 있다. 리더가 태그에게 보내는 메시지를 저장한 후 재생 공격에 사용한다 하더라도 리더의 질의에 대해 리더 주위의 모든 태그가 응답하기 때문에 공격자가 알아낼 수 있는 정보가 없다. 만약 공격자가 정당하지 않은 리더를 이용하여 자신이 생성한 값들로 계산한 $E_{ID_i'}(r_j' \| R)$을 보낸다 하더라도 K_i 값을 모르기 때문에 태그의 응답 메시지를 통해 태그를 인증할 수는 없게 된다.

• 리더에 대한 익명성(Anonymity): 리더가 태그에게 보내는 메시지에는 매번 자신이 임의로 선택한 난수 R이 포함되기 때문에 이 값이 어떠한 리더에서 나온 값인지 구별 불가능하게 된다. 제안하는 기법은 리더 구별 불가능성은 만족하지만 리더 전방향 안전성은 만족하지 않는다. 전방향 안전성 가정에 의해 공격자가 리더에 저장된 접근 리스트 L_j와 리더의 식별자인 r_j를 알고 있다고 하자. 만약 태그 검색 후 리더의 식별자 갱신이 없다면 공격자는 이 정보들과 과거에 도청한 $E_{ID_i}(r_j \| R)$을 이용하여 리더가 찾고자하는 태그가 무엇인지 알 수 있게 되고 리더가 이전에 생성한 값들을 추적할 수 있게 된다. 우선 공격자는 접근 리스트 L_j에 저장된 모든 $ID_i (1 \leq i \leq n)$를 이용하여 $E_{ID_i}(r_j \| R)$에 대한

복호화를 수행하고 $r_j' \| R$을 얻은 후 $r_j' = r_j$인지 확인하게 되면 리더 전방향 안전성은 만족되지 않는다. 전방향 안전성을 만족하기 위해서는 일반적으로 태그와 리더가 정상적인 통신을 끝낸 후 일방향 함수 등을 이용하여 비밀값을 갱신하게 되는데 이 때 동기화 문제를 해결해야 한다. RFID 태그 검색 프로토콜 환경은 중앙 데이터베이스가 항상 온라인이라는 가정이 없기 때문에 여러 개의 리더들을 사용하는 환경에서 동기화 문제를 해결하기 어렵다. 리더 전방향 안전성 문제는 리더 R_j가 일정 간격으로 자신의 식별자 r_j를 해쉬함수 $H(\cdot)$를 이용하여 $H(r_j)$로 갱신하게 함으로써 부분적인 해결이 가능하다. 하지만 식별자의 갱신이 있을 때마다 리더는 신뢰기관으로부터 접근 리스트를 새롭게 받아와야 한다. 이 경우 리더는 해쉬함수를 이용하여 식별자를 갱신하므로 해쉬함수의 일방향 성질 때문에 현재 저장된 식별자 r_j로부터 이전 식별자 값을 알아낼 수 없게 되어 리더 전방향 안전성을 만족한다. 만약 리더 소지자의 프라이버시가 매우 중요한 환경이라면 태그 검색 후 리더는 자신의 식별자를 갱신하고 매번 신뢰기관으로부터 접근 리스트를 받아오는 번거로움을 감수해야 한다.

• 가용성(Availability): 사용자가 이동형 리더를 가지고 무선 통신이 불가능한 지역에 가게 되었을 경우 중앙 데이터베이스로부터 태그에 대한 정보를 얻어올 수 없어 실시간 검색이 불가능한 상황에서도 태그를 검색할 수 있도록 하기 위해 각각의 리더들은 접근 리스트를 저장하게 된다. 이러한 접근 리스트를 통하여 리더는 중앙데이터베이스에 접속하지 않고 태그를 검색할 수 있게 된다.

• 리더 분실에 대한 안전성(Leakage Resilience): 제안하는 기법은 공격자가 분실된 리더에 저장된 태그의 값을 이용하여 다른 정당한 리더에게 정당한 태그인 척 하는 공격에 안전하다. 각각의 리더는 자신의 식별자를 포함한 값으로 구성된 접근 리스트를 가지고 있는데 이러한 값으로부터 다른 리더의 식별자를 포함한 값을 생성할 수는 없다. 다른 리더의 접근 리스트를 생성하기 위해서는 태그의 비밀키를 알아야만 하기 때문이다.

〔표 3〕은 제안하는 기법과 비슷한 환경에서 제안된 기법인 [14,15] 기법과의 안전성 비교를 나타낸다. [14,15] 기법은 리더 구별 불가능성을 만족하지 못하여 리더 소지자의 프라이버시 침해가 심각하다.

〔표 3〕 안전성 비교

안전성 항목	[10,11]	제안 기법
기밀성	○	○
태그 구별 불가능성	○	○
태그 전방향 안전성	×	×
인증	○	○
리더 구별 불가능성	×	○
리더 전방향 안전성	×	△
가용성	○	○
리더 분실 시 안전성	○	○

※(○: 만족함, ×: 만족하지 않음, △: 부분적으로 만족함)

4.2 효율성 분석

본 절에서는 제안하는 기법의 효율성을 분석하고 효율성 개선 방안에 대해 살펴본다.

• 태그에 대한 효율성: 태그는 자신의 식별자와 비밀키만을 저장하여 가격이 비싼 비휘발성 메모리의 사용을 최소화 하였으며, 또한 〔표 1〕에서 알 수 있듯이 AES-128의 구현을 위한 칩 영역으로 3,400게이트만을 사용하였기 때문에 메모리 사용량을 줄였다. 태그는 리더의 요청에 응답하기 위해 1번의 복호화와 2번의 암호화를 수행하여야 한다. 이 연산은 총 $9\mu A(\leq 15\mu A)$을 소모하기 때문에 태그의 통신 반경에 영향을 미치지 않는다. 또한 클럭 사이클(Clock Cycle)의 수는 3,096이다.

• 리더에 대한 효율성: 기존 인증기법의 경우 하나의 태그를 인증하기 위해 리더는 최대 저장된 태그 수만큼의 계산량이 필요했으나 제안하는 검색 프로토콜은 리더로부터 통신 반경 $3m$ 이내에 있는 태그 수를 m이라고 하면 m만큼의 계산만이 필요하기 때문에 효율적이다.

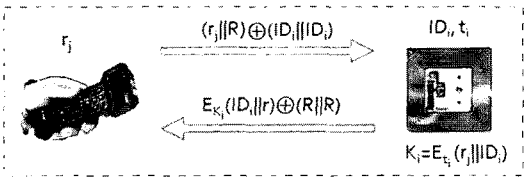
제안하는 기법과 비슷한 환경에서 제안된 기법인 [14,15] 기법과의 효율성을 비교한 결과는 〔표 4〕와 같다. [14,15] 기법에서 태그는 리더의 요청에 응답하기 위해 3번의 해쉬함수 연산을 수행한다. 이 기법은 리더의 연산량을 줄이기 위해 리더 통신 반경에 있

〔표 4〕 효율성 비교

효율성 항목	[10,11]	제안 기법
Imean[μA@100kHz]	11.79	9
Chip Area [GE]	8,120	3,400
Clock [cycles]	3,822	3,096
리더에 대한 효율성	$\leq m$	m

는 모든 태그가 응답하도록 하지 않고 확률적으로 응답하는 방법을 사용하였다. 하지만 [14,15] 기법이 재생 공격에 대해 제안하는 기법과 같은 안전성을 갖으려면 리더에 대한 효율성이 제안기법과 같이 m이여야 한다.

제안하는 기법은 태그 측면에서 3번의 암·복호화 연산이 요구되는데 효율성을 개선하기 위한 방법으로 [그림 9]와 같은 기법을 고려해 볼 수 있다. 리더의 요청 메시지 $(r_j \| R) \oplus (ID_i \| ID_i)$에 대해 모든 태그는 자신의 ID_i'를 XOR하여 r_j'을 구한 후 이를 이용하여 응답 메시지를 계산한 후 리더에게 전송한다. 이 기법은 태그 측면에서 1번의 복호화 과정을 줄였으나 같은 태그의 검색을 위해 리더가 내보내는 메시지가 항상 같기 때문에 리더가 이전에 검색한 태그와 같은 태그를 검색한다는 정보가 노출되는 단점을 갖는다.



〔그림 9〕 효율성 개선 기법

V. 결 론

본 논문에서는 이동형 리더를 이용한 태그 검색 환경에서의 문제점을 지적하고 이러한 환경에서 필요한 보안 및 프라이버시 요구사항을 분석하였다. 또한 이동형 리더 소지자의 프라이버시를 보호하는 효율적인 RFID 태그 검색 프로토콜을 제안하였다. 향후 태그와 리더에 대한 전방향 안전성을 만족하는 저가의 효율적인 RFID 태그 검색 프로토콜에 대한 연구가 필요하다.

참 고 문 헌

〔1〕 하재철, 백이루, 김환구, 박제훈, 문상재, "해쉬함수에 기반한 경량화된 RFID 인증 프로토콜," 정보보호학회논문지, 19(3), pp. 61-72, 2009년 6월.

〔2〕 정윤수, 김용태, 박길철, 이상호, "RFID를 이용한 IPTV 사용자의 경량화 인증 프로토콜," 정보보호학회논문지, 19(2), pp. 105-115, 2009년 4월.

〔3〕 원태연, 천지영, 박춘식, 이동훈, "수동형 RFID 시스템에 적합한 효율적인 상호 인증 프로토콜 설계," 정보보호학회논문지, 18(6A), pp. 63-73, 2008년 12월.

〔4〕 H.Y. Chien and T.C. Wu, "Improving Varying-Pseudonym-Based RFID Authentication Protocols to Resist Denial-of-Service Attacks," 정보보호학회논문지, 18(6B), pp. 259-269, 2008년 12월.

〔5〕 권혜진, 이재욱, 전동호, 김순자, "데이터베이스에서의 태그 검색이 쉽고 안전한 RFID 상호인증 프로토콜," 정보보호학회논문지, 18(5), pp. 125-134, 2008년 10월.

〔6〕 M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic Approach to "Privacy-Friendly" Tags," In RFID Privacy Workshop, Nov. 2003.

〔7〕 A. Juels and S.A. Weis, "Authenticating Pervasive Devices with Human Protocols," Advances in Cryptology- Crypto, LNCS 3621, pp. 293-308, 2005.

〔8〕 G. Tsudik, "YA-TRAP: Yet Another Trivial RFID Authentication Protocol," Pervasive Computing and Communications(PerCom) Workshops, pp. 640-643, Mar. 2006.

〔9〕 S. Vaudenay, "On Privacy Models for RFID," Advances in Cryptology- ASIACRYPT, LNCS 4833, pp. 68-87, 2007.

〔10〕 H. Gilbert, M. Robshaw, and Y. Seurin, "HB#: Increasing the Security and Efficiency of HB+," Advances in Cryptology-EUROCRYPT, LNCS 4965, pp. 361-378, 2008.

〔11〕 R. Paise and S. Vaudenay, "Mutual authentication in RFID: security and

privacy," ACM Symposium on Information, Computer and Communications Security (ASIACCS), pp. 292-299, Mar. 2008.
[12] M. Burmester, B. Medeiros, and R. Motta, "Provably Secure Grouping-Proofs for RFID Tags," CARDIS, LNCS 5189, pp. 176-190, 2008.
[13] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, and T. Phillips, "Guidelines for Securing Radio Frequency Identification (RFID) Systems," National Institute of Standards and Technology(NIST) Special Publication 800-98, p. 154, Apr. 2007.
[14] C. Tan, B. Sheng, and Q. Li, "Serverless Search and Authentication Protocols for RFID," Pervasive Computing and Communications(PerCom) Workshops, pp. 3-12, Mar. 2007.
[15] 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, Apr. 2008.
[16] 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, Apr. 2008.
[17] M. Feldhofer and J. Wolkerstorfer, "Strong crypto for RFID tags-A comparison of low-power hardware implementations," IEEE International Symposium on Circuits and Systems(ISCAS), pp. 1839 - 1842, May 2007.
[18] "Radio Frequency Identification (RFID): A Focus on Information Security and Privacy," OECD Working Party on Information Security and Privacy, DSTI/ICCP/REG(2007)9/FINAL, p. 70, Jan. 2008.

〈著者紹介〉

천 지 영 (Ji Young Chun) 학생회원
1997년 2월: 이화여자대학교 수학과 학사 졸업
2006년 2월: 고려대학교 정보경영공학과 석사 졸업
2006년 3월 ~ 현재: 고려대학교 정보경영공학과 박사과정
〈관심분야〉 암호 이론, 프라이버시향상기술(PET), 유비쿼터스 보안

황 정 연 (Jung Yeon Hwang) 정회원
1999년 2월: 고려대학교 수학과 학사 졸업
2003년 2월: 고려대학교 정보경영공학과 석사 졸업
2006년 8월: 고려대학교 정보경영공학과 박사 졸업
2009년 4월: 고려대학교 BK21유비쿼터스정보보호사업단 박사후연구원
2009년 5월 ~ 현재: 한국전자통신연구원(ETRI) 선임연구원
〈관심분야〉 정보보호이론, 암호프로토콜, 개인프라이버시보호기술

이 동 훈 (Dong Hoon Lee) 종신회원
1983년 8월: 고려대학교 경제학과 학사 졸업
1987년 12월: Oklahoma University 전산학과 석사 졸업
1992년 5월: Oklahoma University 전산학과 박사 졸업
1993년 3월 ~ 1997년 2월: 고려대학교 전산학과 조교수
1997년 3월 ~ 2001년 2월: 고려대학교 전산학과 부교수
2001년 3월 ~ 현재: 고려대학교 정보경영공학부 교수
〈관심분야〉 암호 프로토콜, 암호 이론, USN 이론, 키 교환, 익명성 연구, PET 기술