태그상태 변경과 마스터리더 지정을 통한 RFID 프라이버시 보호 방안

정회원 김 은 진*, 종신회원 노 병 희**°

Methods for Change of Tag States and Assignment of Master Leaders to Protect RFID Privacy

Eunjin Kim* ***Regular Member***, Byeong-hee Roh**° ***Lifelong Member***

요 약

프라이버시 문제는 RFID 응용 확산의 가장 큰 요인들 중의 하나로 인식되고 있다. 본 논문에서는RFID 응용에서의 프라이버시 보호를 위한 태그상태 변경 방법과 마스터리더를 지정하는 방안을 제안한다. 태그상태의 변경을 통하여, 태그 정보의 획득을 모든 리더가 가능하도록 할 수도 있고, 특정 리더(마스터리더)로 제한할 수 있다. 또한, 태그의 소유주의 변경에 따라 태그의 정보를 취득 가능한 마스터리더를 지정케 함으로써 타인에 의한 물품 정보의 취득을 제한하도록 할 수 있다. 이들 제안 방법을 통하여, 개인이 소유한 태그들의 정보가 불법적으로 노출되는 것을 방지하여 프라이버시 문제가 해결 가능할 것으로 기대한다.

Key Words : RFID Privacy, RFID Security, RFID Tag, RFID Reader, Master Reader

ABSTRACT

The problem of privacy is considered one of the main concerns to deploy RFID applications. In this paper, we propose methods to change a tag state and assign a master leader for the protection of privacy. By changing a tag state, we can limit the range for the information retrieval of the tag to all leaders or a specific leader (mater leader). Whenever the owner of a tag changes, with the master leader assignment method for the tag, we can make only the master leader get the information for the tag. With the proposed methods, it is expected that the privacy problems can be solved by preventing the private information of tags that persons have from being exposed by illegal leaders.

Ⅰ. 서 론

RFID(Radio Frequency IDentification)는 유비쿼터스 컴퓨팅의 실현을 위한 가장 핵심적인 기술들 중의 하나로 인식되고 있다. RFID 기술은 인간의 생활 전반에 활용되어 무한한 부가가치 창출이 가능하며, 향후 전 세계적인 산업구조, 시장구조의 변화뿐만 아니라 인간의 삶의 형태까지 변화시킬 것으로 예상된다. 그러나 RFID 기술의 확산은 개인 신상 정보 노출에 따른 개인의 사생활 침해와 같은 문제를 야기할 것으로 우려되고 있다. 이것은 RFID 기술에서 정보접근의 매개역할을 하는 태그 정보가 개인이 알지 못하는 사이에 당사자의 허가 없이 오용될 가능성을 내재하고 있기 때문이다.

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업(IITA-2007-(C1090-0701-0003))과 아주대학교 교내 일반 연구비의 지원으로 수행되었음.

* 엔씨소프트 (moonk7@ncsoft.net) ** 아주대학교 정보통신전문대학원 (bhroh@ajou.ac.kr)(° : 교신저자)

논문번호 : KICS2007-03-096, 접수일자 : 2007년 3월 2일, 최종논문접수일자 : 2007년 11월 26일

기존의 정보시스템을 대상으로 한 정보보호를 위한 기술적 방안들이 제시되어 있으나, 이를 RFID 기술을 위하여 그대로 적용하는 데는 많은 문제점을 갖고 있다. 기존의 정보시스템은 사용자이름(Username), 암호(Password)등과 같은 개인의 식별정보가 정보접근의 직접적인 수단을 제공하지만, RFID 정보시스템의 경우에 사용되는 태그 식별정보는 개인과는 무관한 개인이 사용하는 제품의 정보로써, 이 정보는 여러 단계의 개인화되는 과정을 거치게 되는 근본적인 차이를 갖고 있기 때문이다[1]. RFID 태그의 정보가 불법적인 리더들에 의하여 도청되는 것을 방지하기 위한 다양한 방법들이 제안되었다[2]. 이들 여러 방법들 중에서, Henrici등[3]이 제안한 태그-리더간 트랜잭션 발생시 마다 태그의 ID를 변경하는 방식은 태그 ID 노출에 따른 프라이버시 문제 해결에 더 효율적인 방식으로 여겨진다. 그러나 이 방법은 태그 ID 정보의 변경 과정 중에 공격자가 태그 정보 요청시 태그 ID 정보가 변경되는 과정이 또다시 발생하게 되어 태그 ID 정보를 관리하는 DB의 불일치가 발생할 위험성을 갖고 있다.

본 논문에서는 Henrici등의 방법[3]의 문제점을 해결하면서 RFID 응용에서의 개인 프라이버시 보호를 위하여 물품에 부착된 태그를 관리하는 마스터 리더를 지정하는 방법을 제안한다. 제안 방법은 태그의 소유주의 변경에 따라 태그의 정보를 취득 가능한 리더를 지정케 함으로써 타인에 의한 물품 정보의 취득을 제한 가능하여, 개인의 정보가 노출되는 것을 방지하여 프라이버시 보호가 가능하다.

본 논문의 구성은 다음과 같다. 제Ⅱ장에서는 본 논문의 배경에 대하여 기술하고, 제Ⅲ장에서는 제안 방법의 시스템 구조와 기본 통신 과정에 설명하고, 이를 적용하여 태그상태와 마스터리더를 변경함으로써 프라이버시를 보호하기 위한 방법을 제Ⅳ장에서 설명한다. 그리고 제Ⅴ장에서는 결론을 맺는다.

Ⅱ. RFID 프라이버시 문제의 고찰

2.1. RFID 응용 시스템 구조

그림 1은 RFID 태그가 부착된 물품에 대한 정보 획득을 위한 전형적인 RFID 응용 시스템 구조를 보여준다[1]. 리더는 태그에게 태그의 UII (Unique Item Id)[4]를 요청하여 읽어들인 후①, 태그의 UII에 대한 자세한 정보를 갖고 있는 정보서버 (Information Server)의 주소를 디렉터리 서버(Directory Server)에 질의하여 알아온다②. 리더는 정보서버에 접속하여 물품의 자세한 정보를 찾아낸다③. 정보서버는 모든 태그들의 정보를 저장하는 데이터베이스의 역할을 한다.

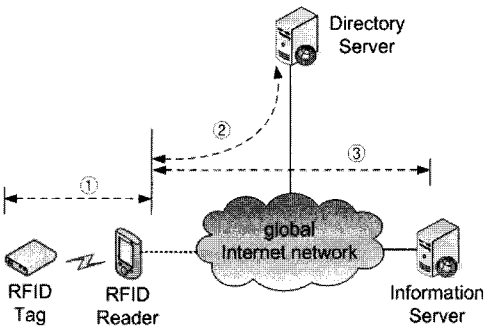


그림 1. RFID 응용 시스템 구조 및 정보 획득 과정

2.2 RFID 개인 프라이버시 침해 문제

RFID 태그를 개인 소유의 물품에 부착하여 응용시 우려되는 개인 프라이버시 침해의 문제는 다음과 같은 상반된 특성을 보여준다. 즉, RFID 응용을 위하여는 RFID 리더를 사용하여 태그가 부착된 물품의 정보를 획득할 수 있어야 하지만, 개인의 프라이버시 보호를 위해서는 개인이 소유한 태그의 정보를 다른 사람이 얻지 못하도록 해야 한다는 것이다. 예를 들어, 소비자들은 상점의 진열된 물품의 정보를 얻기를 원할 것이다. 이 경우, 태그의 ID는 그대로 모든 리더에게 공개되는 것이 바람직할 것이다. 하지만 소비자가 물품을 사서 밖으로 나가는 순간 다른 사람에 의해 자신이 산 물건에 대한 정보가 공개되는 것을 원치는 않을 것이다.

2.3 기존의 RFID 프라이버시 보호 방법들

RFID 응용에서 태그 ID의 불법 유출을 방지하여 프라이버시를 보호하기 위하여, 태그를 "Kill Command"를 사용하는 방법[5]과 블로커 태그를 쓰는 방법[6] 등이 제안되었다. "Kill Command" 방식은 AutoID 소비자가 태그가 붙어있는 물품을 구입하자마자 그 태그가 더 이상 리더의 쿼리 요청에도 응답이 없도록 "Kill"하는 방식이다. 하지만 많은 경우 이처럼 태그를 "Kill"하는 것이 바람직하지 않을 수도 있다. 왜냐하면 그 물품을 다시 다른 소비자에게 파는 경우처럼 그 태그가 다시 사용될 필요가 있는 경우를 고려해야 하기 때문이다. 블로커 태그는 태그의 정보를 공개하고 싶지 않은 영역에 블로커 태그를 활성화시킴으로써 태그의 UII를 공개하지 않는 방법이다. 하지만 만약 이러한 블로커 태

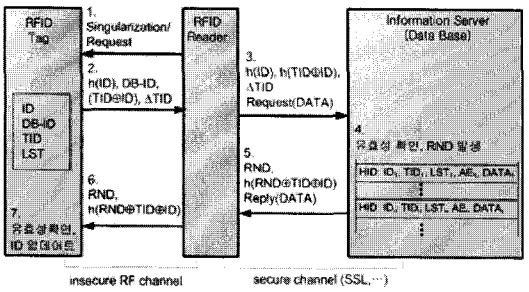


그림 2. 트랜잭션에 따른 태그 ID 변경 방법[3]

그가 악의적으로 이용된다면 모든 태그가 정당한 리더에게 읽히는 것도 방해할 수 있기 때문에 오히려 RFID 시스템의 특성을 해칠 수 있다[4].

Dirk Henrici등은 도청 및 추적 문제를 해결하기 위해 hash-lock 방식을 개선하여 매번 정상적으로 태그와 리더간의 쿼리 전송이 이루어질 때마다 태그의 ID를 바꾸는 방식을 제안하였다[3]. 이 방법에서는 태그와 정보서버의 DB에 다음과 같은 부가적인 요소의 추가를 필요로 한다. 우선, 태그에 추가될 요소들은 데이터베이스 식별자 (DB-ID), 현재 ID (ID), 트랜잭션 번호 (TID), 가장 최근에 성공한 트랜잭션 번호 (LST)등이 있다. 이와 연관되어 정보서버에는 현재 ID의 해쉬값(HID), 현재 ID (ID), 가장 최근에 성공한 트랜잭션 번호 (LST), 관련된 DB 엔트리 (AE), 태그에 대한 실제 정보 (DATA)들이 추가로 필요하게 된다. 트랜잭션에 따른 태그 ID의 변경 과정은 그림 2와 같다.

이 방법을 사용하면 태그가 리더에게 전송하는 값이 매 트랜잭션이 성공적으로 이루어질 때마다 새롭게 바뀌기 때문에 사용자에 대한 추적 문제를 해결할 수 있게 된다. 그러나 악의적인 공격자에 의해 한 태그가 계속적으로 쿼리 요청을 받게 된다면 그 태그의 TID 값을 의도적으로 높게 만들 수 있기 때문에 이 값을 이용해서 여전히 추적당할 문제가 있다[7]. 또한 위의 과정에서 2단계 이상 진행된 상태에서 공격자가 태그에 정보를 요청하게 되면 태그는 요청 받을 때마다 TID 값을 하나씩 증가하게 되므로 데이터베이스와 태그 사이의 관계가 깨질 위험이 있다.

Ⅲ. 제안 시스템의 구조 및 기본 통신 과정

본 논문에서 제안하는 방법의 기본 개념은 다음과 같다. 모든 태그가 물품에 부착된다고 할 때, 모든 물품에는 다 소유주가 있는 것처럼, 물품에 부착된 태그들도 각기 그 소유주가 존재한다고 할 수 있다. 이러한 개념을 RFID 시스템에 도입해보면 리더를 갖고 있는 소유주가 관리할 수 있는 여러 개의 물품 즉, 태그들이 존재할 수 있게 된다. 이와 같이 태그를 관리 가능한 리더를 마스터리더로 설정하고, 태그와 이 마스터리더간에 비밀키를 갖고 있다면 태그의 정보를 마스터리더에게만 공개함으로써 다른 도청자나 리더가 태그의 정보를 획득할 수 없도록 할 수 있을 것이다. 여기에서는 본 논문에서 제안하는 RFID 응용 시스템과 기본 통신 과정에 대하여 설명하기로 한다.

3.1 시스템 구조

그림 3은 제안하는 시스템의 구조와 마스터리더를 지정하고 태그에의 권한 부여를 위하여 태그, 리더, 정보서버의 데이터베이스에서 관리되는 파라메터들을 보여주고 있다.

그림 3에서 RFID 태그, 리더, 데이터베이스에서 관리되는 파라메터들의 특징은 다음과 같다.

- UII : 태그의 UID (읽기만 가능)
- Rkey : 마스터 리더와 공유하는 key 값 (읽기/쓰기 모두 가능)
- PW1, PW2 : 데이터베이스와 공유하는 첫 번째와 두번째 비밀 번호 (읽기/쓰기 모두 가능)

리더에서 관리되는 파라메터들은 다음과 같다.

- RID : 리더의 ID
- Rkey : 리더와 태그 간에 공유하는 key 값으로서, 리더 고유의 값

정보서버의 데이터베이스는 기본적으로 태그의 UII와 상세정보를 갖고 있으며, 마스터리더의 정보를 안전하게 관리하기 위하여 다음과 같은 필드들을 추가하게 된다.

- HUIkey : 태그의 아이디인 UII와 Rkey 값을 exclusive-OR한 후 hash function을 사용하여 얻은 값 (즉, HUIkey=h(UII⊕Rkey))
- UII : 태그의 ID

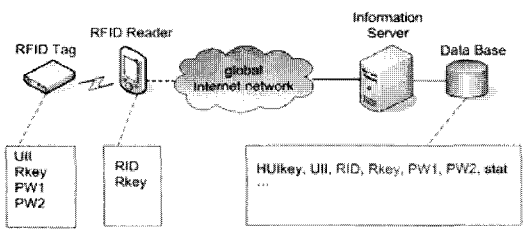


그림 3. 제안 시스템 구성 요소

- RID : 태그를 소유하는 마스터 리더의 ID
- $RKEY_R$, $RKEY_T$: 마스터리더와 태그의 key
- PW1, PW2 : 데이터베이스와 공유하는 첫 번째 , 두 번째 비밀 번호
- stat : 태그의 상태
- DATA : 태그에 대한 실제 정보

3.2 태그 정보 획득 과정

그림 4는 리더가 태그의 정보를 획득하는 과정을 보여준다. RFID 시스템에서 리더와 정보서버간의 통신은 기존의 인프라를 그대로 이용하므로 안전한 채널을 이용하여 통신하는 것이 가능하다. 그러나 리더와 태그간의 통신은 안전하지 않은 RF 채널을 이용하므로 쉽게 도청이 가능하며, 자체 전력을 갖지 않은 태그에서의 연산은 극히 제한적이다. 이를 위하여, 태그 ID의 도청으로 부터의 보호를 위하여 단순한 해쉬함수 기능만 부여하고, 기타 복잡한 연산이나 중요한 알고리즘은 정보서버의 데이터베이스를 사용하여 이루어진다.

그림 4의 정보획득과정을 다음에 설명하였다.

1. 리더는 binary tree-walking과 같은 충돌방지(anti-collision) 방법을 사용하여 여러 태그들중에서 하나의 태그를 지정하게 되고(singularizion)[8], 이 태그에게 ID를 요청(request)하게 된다.
2. 태그는 리더에게 자신의 ID 값인 UII와 $RKEY_T$ 값으로 간단한 exclusive-OR 연산을 한 후 hash 함수를 사용하여 얻은 값인 h(UII $\oplus RKEY_T$)를 리더에게 전송한다.
3. 리더는 태그로부터 얻은 HUIkey 값 (h(UII$\oplus$ $RKEY_T$))과 자신의 RID와 $RKEY_R$ 값을 정보서버에게 보낸다.
4. 정보서버는 데이터베이스에서 리더가 보낸 HUIkey 값으로 검색하여 해당하는 엔트리를 찾아낸 후, 엔트리내의 RID와 $RKEY_R$ 필드의 저장값과 리더가 보내온 값들을 점검하여, 정보를 요청한 리더가 마스터리더가 맞는지를 조사한다.
5. 마스터리더로 확인된 경우, 정보서버는 태그의 정보를 전송하여 정보 획득 과정을 마치게 된다.

이때, 태그의 $RKEY_T$ 값의 초기값은 이 태그를 제조한 회사에서 지정하는 마스터리더의 $RKEY_R$ 값으로 초기화된 것으로 가정한다. 마스터리더의 변경에 따른 $RKEY_T$ 와 $RKEY_R$ 값의 변경은 뒤에서 설명하기로 한다.

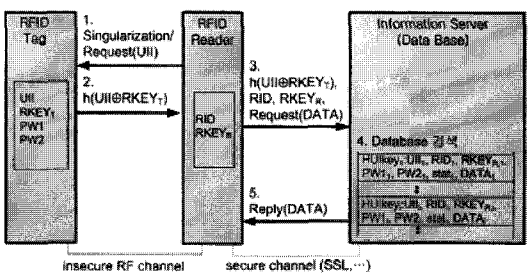


그림 4. 리더의 RFID 태그 정보 획득 과정

3.3 태그 정보 공개의 제한

본 논문에서는 RFID 응용시의 개인 프라이버시 보호를 위한 한 방법으로서 정보서버내 데이터베이스의 각 엔트리의 stat 필드를 사용한다. 이 stat 필드는 태그의 정보를 공개하는 범위를 제한하는데, 이 필드가 필요한 이유는 다음과 같다. 예를 들어, 상점에서 상품 판매시 고객들이 상품에 대한 정보를 획득할 수 있도록 할 필요가 있으며, 이 경우에는 태그에 대하여 마스터리더를 가진 사람이 아니더라도 공개된다. 반대로, 상품을 구입하여 개인 소유가 되면, 상품을 소유한 사람은 상품의 정보가 공개되기를 원하지 않을 수도 있다.

이를 위하여, 태그의 정보 공개에 대한 상태(stat)를 다음의 두 가지로 나누어 데이터베이스에서 관리를 한다. 즉,

- 비공개 상태: 마스터리더만 태그의 정보를 획득가능 하도록 함 (stat=m)
- 공개 상태: 모든 리더들이 태그의 정보를 획득가능 하도록 함 (stat=p)

이들 상태는 그림 4의 태그 정보 획득 과정의 단계-4에서 참고된다. 즉, 데이터베이스에서 리더로부터 받은 HUIkey를 인덱스로 하여 일치하는 엔트리를 찾아내고, 엔트리의 필드중에서 stat의 상태를 확인한다.

i) stat=m인 경우: 리더로부터 받은 RID와 $RKEY_R$ 가 엔트리의 해당 필드의 값들과 비교하여 일치하지 않으면, 정보를 요청한 리더는 해당 태그에 대한 마스터리더가 아니므로, 태그의 정보를 제공하지 않는다. 반대로, 이들 값들이 일치하면, 정보서버는 태그의 정보(DATA)를 리더에게 제공한다.

ii) stat=p인 경우: 이 경우에는 마스터리더 확인 절차를 거치지 않고 바로 태그의 정보(DATA)를 요청한 리더에게 넘겨주게 된다.

또한, 태그와 리더간의 무선구간에서의 도청의 문제를 피하기 위하여 $RKEY_T$와 $RKEY_R$ 가 사용됨에 주의한다. stat=p일 경우 태그의 $RKEY_T$는 리더의 $RKEY_R$ 과 달리 모두 1인 111…1로 설정된다. stat=p일 때, 태그의 $RKEY_T$를 이와 같이 변경하는 절차는 다음 절에서 설명하기로 한다. 따라서 단계-2에서 리더가 태그로부터 받게 되는 값은 $h(UII \oplus RKEY_T)=h(UII)$가 되어, 해쉬 함수에 대한 정보를 아는 모든 리더들은 태그의 UII를 인지할 수 있게 된다. 반면에, stat=m인 경우에는 태그가 제공하는 정보는 $h(UII \oplus RKEY_T)$로서 리더의 키값인 $RKEY_R$ 이 $RKEY_T$와 다른 경우 태그의 UII를 인지할 수 없게 된다.

Ⅳ. 태그 상태와 마스터리더 변경 방법

본 장에서는 Ⅲ장에서의 통신과정을 기반으로 태그상태(stat)의 변경과 마스터리더의 변경 방법을 설명하고, 이를 통하여 RFID 응용시에 개인 프라이버시를 보호하는 과정에 대하여 기술한다.

4.1 태그 상태(stat) 변경 방법

4.1.1 공개에서 비공개로의 상태 변경 과정

공개 태그에서 비공개 태그(마스터 리더만이 정보획득을 할수 있음)로 변경을 하는 과정을 그림 5에 나타내었다. 그림 5에 나타낸 각 단계를 자세히 설명하면 다음과 같다.

1. 리더는 상태를 변화시킬 태그를 선택하고, 태그의 현재 HUIkey를 요청한다.
2. 태그는 현재 HUIkey 값인 $h(UII \oplus RKEY_T)$를 리더에게 전달한다.
3. 리더는 태그의 현재 HUIkey, RID, $RKEY_R$ 값들과 해당 태그의 상태를 p에서 m으로 변경할 것을 요청하는 메시지를 정보서버에게 보낸다.
4. 정보서버는 데이터베이스에서 HUIkey의 RID와 $RKEY_R$ 값을 확인하고 맞으면 랜덤값 r을 발생시키고, 새로운 키값인 $RKEY_{NEW}$ 를 생성하고, $HUIkey_{NEW}=h(UII \oplus RKEY_{NEW})$를 새로운 인덱스로 하는 임시 엔트리를 생성한다. 태그의 현재 HUIkey를 $HUIkey_{CUR}$ 이라 할 때, 이들의 엔트리는 그림 6과 같다.

$HUIKey_{CUR}$: UII, RID, $RKEY_R$, PW1, PW2, stat=p, DATA	①
$HUIKey_{NEW}$: UII, RID, $RKEY_R$, PW1, PW2, stat=m, DATA	②

그림 6. 현재 엔트리와 새로 생성된 엔트리

5. 정보서버는 리더에게 $(r \oplus PW1 \oplus RKEY_T)$와 $(r \oplus PW2 \oplus RKEY_{NEW})$를 전달하고, 타이머를 설정한다. 타이머가 완료되기까지 리더로부터 정보갱신에 대한 응답이 없으면 $HUIkey_{NEW}$를 인덱스로 하는 임시 엔트리는 제거되고, 태그 상태 변경은 취소된다.
6. 리더는 정보서버로부터 전달받은 정보를 태그에게 전달한다.
7. 태그는 (r⊕PW1⊕RKEYT)로부터 랜덤값 r을 구해낸다. 이것은 태그가 PW1과 $RKEY_T$를 알고 있으므로, 간단한 exclusive-OR 연산을 통하여 구할 수 있다. 그리고 $(r \oplus PW2 \oplus RKEY_{NEW})$로부터 새로 사용할 키값인 $RKEY_{NEW}$를 알아내고, 키값을 $RKEY_T$ 에서 $RKEY_{NEW}$로 변경한다.
8. 태그는 키값을 성공적으로 변경한 사실을 정보서버에게 확인시키기 위해 새로운 HUIkey 값인 $h(UII \oplus RKEY_{NEW})$를 리더에게 전달한다.
9. 리더는 $h(UIIR \oplus RKEY_{NEW})$를 RID, $RKEY_R$ 과 함께 정보서버에게 전달한다.
10. 정보서버는 HUIkey의 RID, $RKEY_R$ 값을 비교하고 맞으면 기존의 $HUIkey_{CUR}$ 엔트리(그림 6의 ①)를 삭제하고, 임시 엔트리인 $HUIkey_{NEW}$ (그림 6의 ②)를 데이터베이스에 갱신하고, 타이머를 해제함으로써 태그의 상태 변경 과정을 마치게 된다.

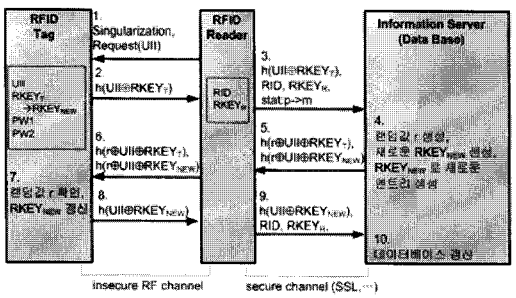


그림 5. 태그 상태의 변경 과정 (p→m)

4.1.2 비공개에서 공개 태그로 상태 변경 과정

비공개 태그에서 공개 태그로의 상태 변경은 그림 5의 절차와 유사하다. 대신에, 단계-4에서 $RKEY_{NEW}$는 비트값이 모두 1로 설정되며, stat 필드는 m에서 p로 바뀌는 것만 다르다.

4.2 마스터리더 변경 방법

상점에서 물건이 구매를 통하여 개인 소유로 되거나, 또는 개인간의 거래에서 물건의 소유가 변하게 되는 상황이 발생하고, 물건을 소유한 사람이 관리를 위하여 자신은 해당 물건의 정보를 획득할 수 있으나 타인에게 노출되는 것을 방지하기를 원할 수도 있다. 이를 위해서는 물건을 소유한 사람이 자신이 관리하는 리더를 해당 물품에 대하여 마스터리더로 지정함으로써 가능해진다. 그림 7은 물건의 소유 변경에 따른 마스터리더의 변경 절차를 보여준다.

그림 7의 각 과정을 자세히 기술하면 다음과 같다. 여기에서 리더A는 상점에서 물건을 관리하는데 사용되는 RFID 리더 또는 리더 기능을 보유한 물품 관리 시스템이다. 그리고 리더 B는 상점에 물건을 구입하러 온 구매자의 리더를 의미한다. 물건에는 태그(RFID 태그)가 부착되어 있고, 구매전이므로 태그상태는 공개하도록 설정되어 있다고 하기로 한다.

1. 리더B는 태그의 정보를 2.1절에 설명된 일반적인 RFID 응용 절차에 따라 획득해 온다.
2. 리더B는 물품의 정보를 확인 후 구매를 결정하고, 구매절차를 완료한다. 이럼으로써, 물품의 소유는 리더B에게로 넘어가게 된다.
3. 구매한 물품의 소유자는 자신이 보유한 리더B를 통하여만 정보를 획득가능하고, 다른 리더들을 통하여는 정보 획득이 불가능하도록 마스터리더 변경 요청을 한다.
4. 이전 소유자의 리더A는 해당 물품의 태그의 HUIKey를 얻어온다.
5. 리더A는 태그(HUIKey)의 소유를 리더A (RID_A)에서 리더B (RID_B)로의 변경 요청을 정보서버에게 요청한다.

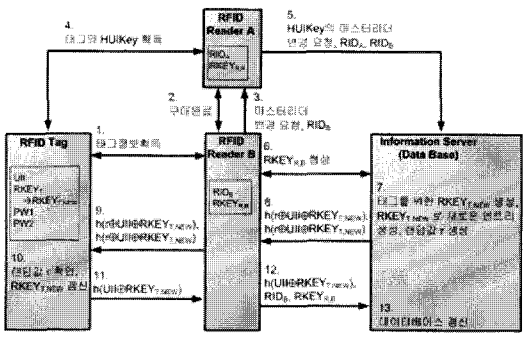


그림 7. 마스터리더 변경 과정

6. 정보서버와 리더B는 태그의 정보획득을 위한 리더B의 키값($RKEY_{R,B}$)을 협상한다. 이것은 리더B가 여러 태그들을 관리하는 경우, 매 태그마다 키값을 달리하기를 원하지 않을 경우, 이전의 키값을 사용하기를 원할 수도 있기 때문이다.
7. 정보서버는 랜덤값 r을 발생시키고, 태그의 새로운 키값인 $RKEY_{T,NEW}$를 생성하고, $HUIkey_{NEW}=h(UII \oplus RKEY_{T,NEW})$를 새로운 인덱스로 하는 임시 엔트리를 생성한다. 태그의 현재 HUIkey를 HUIkeyCUR 이라 할 때, 이들의 엔트리는 그림 8과 같다.

$HUIKey_{CUR}$: UII, RID_A, $RKEY_{R,A}$, PW1, PW2, stat=p, DATA	③
$HUIKey_{NEW}$: UII, RID_B, $RKEY_{R,B}$, PW1, PW2, stat=m, DATA	④

그림 8. 현재 엔트리와 새로 생성된 엔트리

8.~12. 그림 5의 5.~9.와 동일하다.

13. 정보서버는 기존의 $HUIkey_{CUR}$ 엔트리(그림 8의 ③)를 삭제하고, 임시 엔트리인 $HUIkey_{NEW}$ (그림 8의 ④)를 데이터베이스에 갱신한다. 이럼으로써, 태그의 마스터리더는 리더B로 지정되고, 상태 변경도 비공개로 설정되어, 태그는 리더B에 의하여만 정보획득이 가능하게 된다.

V. 결 론

본 논문에서는 RFID 응용에서의 개인 프라이버시 보호를 위하여 물품에 부착된 태그의 상태와 마스터리더를 변경하는 방법을 제안하였다. 제안 방법은 태그 소유주의 변경에 따라 태그의 정보의 취득을 소유주의 리더를 통하여만 가능하도록 하게 함으로써 타인에 의한 물품 정보의 취득을 못하게 함으로써 개인이 소유한 물품의 정보가 노출되는 것을 방지하여 프라이버시 보호가 가능하다.

RFID 기술을 활용한 응용은 무한한 부가가치 창출이 가능하며, 향후 전 세계적인 산업구조, 시장구조의 변화뿐만 아니라 인간의 삶의 형태까지 변화시킬 것으로 예상된다. 그러나 개인 프라이버시의 문제는 이러한 RFID 응용 확산의 큰 장애 요인중의 하나로 인식되고 있다. 본 논문에서 제안한 방법은 이러한 개인 프라이버시 보호 문제를 해결 가능할 것으로 예상된다.

참 고 문 헌

[1] Eunjin Kim, Sun Ho Kim, Byeong-hee Roh, "Security and Privacy Issues to Deploy RFID-based Services," KINGPC'2005, Seoul, Korea, 2005. 11

[2] Ari Juels, "RFID Security and Privacy: A Research Survey," IEEE Journal on Selected Areas in Communications, Vol.24, No.2, February 2006

[3] D.Henrici, P.Muller, "Hash-based Enhancement of Location Privacy for Radio-frequency Identification Devices Using Varying Identifiers," Workshop on Pervasive Computing and Communications Security, 2004

[4] Yong Hwan Lee, Hee Jung Kim, Byeong-hee Roh, and S.W. Yoo, "Tree-Based Classification Algorithm for Heterogeneous Unique Item ID Schemes," EUC Workshops 2005, LNCS Vol.3823, pp.1078-1087, Dec. 2005

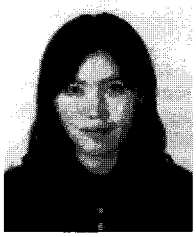
[5] S.E.Sarma, S.A.Weis, D.W.Engels, "RFID systems, security and privacy implications", Technical Report MIT-AUTOID-WH-014, AutoID Center, MIT, 2002

[6] Juels Ari et al, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", 2003

[7] Gildas Avoine, Philppe Oechslin, "RFID Traceability: A Multilayer Problem," The 9th International Conference on Financial Cryptography, LNCS Vol.3570, pp.125-140, 2005

[8] 최원준, 노병희, 유승화, "랜덤화된 트리워킹 알고리즘에서의 RFID 태그 보안을 위한 백워드 채널 보호 방식," 한국통신학회논문지, Vol.30, No.5C, 2005. 5

김 은 진 (Eunjin Kim) 정회원



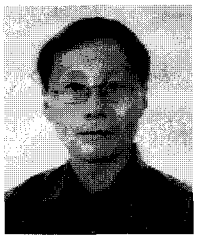
2004년 아주대학교 미디어학부 (학사)

2006년 아주대학교 정보통신전문대학원(석사)

2006년~현재 엔씨소프트

<관심분야> 인터넷 통신 프로토콜 응용 및 서비스, RFID/USN 프로토콜 및 보안

노 병 희 (Byeong-hee Roh) 종신회원



1987년 한양대학교 전자공학과 (학사)

1989년 한국과학기술원 전기및전자공학과(석사)

1998년 한국과학기술원 전기및전자공학과(박사)

1989년~1994년 한국통신 통신망 연구소

1998년~2000년 삼성전자

2000년~현재 아주대학교 정보통신전문대학원 부교수

<관심분야> 모바일 멀티미디어 네트워크 및 응용, BcN QoS 및 트래픽 엔지니어링, 유비쿼터스 센서 네트워크(RFID/USN), 인터넷 보안, 국방전술통신네트워크