모바일 RFID 프라이버시를 위한 프락시 시스템 설계

송민근 전문석
숭실대학교 컴퓨터학과
mnmks@hanmail.net

Design of Proxy System for Mobile RFID Privacy

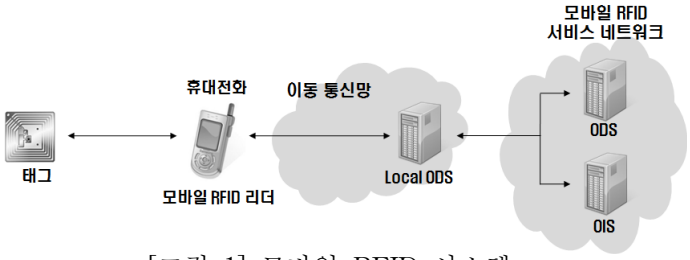
Min-Keun Song, Moon-Seog Jun
Dept of Computer Science, Soongsil University

요 약

현재의 모바일 RFID 서비스는 RFID 리더가 장착된 휴대폰로 누구나 태그에 대한 접근이 가능하므로, 태그 정보가 불법적으로 수집될 수 있으며 추적이 가능하다. 특히 PAN을 구성하는 기본장치 뿐만 아니라 사용자의 소지품에 부착된 각종 RFID에 의한 정보 유출 및 사생활 침해가 큰 문제가 될 것으로 우려된다. 왜냐하면, 기존의 고정형 RFID의 경우, 리더기는 항상 고정되어 있고(예를 들면, 상점의 계산대), RFID 태그만 이동되었으나, 모바일 RFID의 경우는 "휴대폰=RFID 리더기"이므로 사생활 침해 요소가 더욱 심각해지게 된다. 따라서, 본 논문에서는 선택적인 태그 블록킹과 인가된 리더에게는 태그를 대신하여 모바일 리더가 응답하는 프락시 기능을 가진 모바일 RFID 프락시 시스템을 설계하고, 제안 시스템의 기능 및 구조적 특징을 기존 기법들과 비교 분석한다.

I. 서 론

모바일 RFID (Radio Frequency IDentification) 서비스는 우리나라에서 이동통신 인프라를 바탕으로 휴대전화를 이용하여 사물과 사람 사이의 직접적 정보소통 관계를 제공하기 위하여 시작된 융합 서비스이다. 모바일 RFID 서비스 네트워크에 존재하는 ODS (Object Directory Service) 서버는 RFID 태그 식별자와 관련된 제품정보가 있는 OIS (Object Information Service) 서버의 위치를 알려주는 역할을 하는데, OIS 서버는 RFID 태그 식별자와 관련된 제품의 주요 정보를 저장하고 관리하는 역할을 한다([그림 1] 참조). 이러한 서버들과 휴대전화와의 통신은 이동통신망을 통해 수행된다.



[그림 1] 모바일 RFID 시스템

모바일 RFID 서비스는 최종 사용자를 대상으로 한 B2C 서비스이기 때문에 필연적으로 개인 프라이버시 침해 문제가 발생할 수 있으며, 이에 대한 해결책을 마련하여야 한다. 모바일 RFID 리더가 장착된 휴대전화를 소유한 개인 사용자가 타인의 RFID 태그 정보를 쉽게 획득할 수 있게 되면, 누가 어떤 물품을 소유하고 있는지가 노출되고 이는 곧 프라이버시 침해와 직결된다.

따라서, 기존 RFID 서비스와 달리, 모바일 RFID 서비스에서는 휴대단말을 가진, 즉 모바일 RFID 리더기를 가진 개인 사용자가 자신의 태그정보에 대한 접권 권한에 대한 제어권을 가져야 한다. 다시 말하면, 신뢰할 수 있는 타인의 리더기가 접근할 경우에만 나의 태그정보를 읽을 수 있도록 하고, 그 외의 단말기가 읽기 시도를 할 경우 해당 정보를 제공하지 못하도록 하는 기술이 필요로 한다.

모바일 RFID 환경에서 이러한 개인 RFID 태그 정보의 선택적 접근제어를 위한 모바일 RFID 프라이버시 보호 기술을 제안한다.

본 논문에서의 구성은 다음과 같다. 2장에서는 모바일 RFID 보안요구사항과 기존 프라이버시 보호 기술들을 살펴보고, 3장에서 제안 시스템의 구성요소와 프로토콜을 소개하고 4장에서 결론을 맺는다.

II. 관련 연구

본 장에서는 모바일 RFID의 보안 위협요소와 이에 따른 보안 요구사항을 정의하고, 본 논문과 연관된 기존 연구들을 간략하게 요약 정리한다.

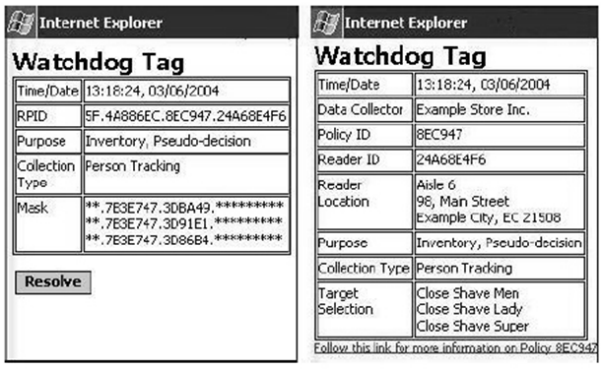
2.1. 모바일 RFID 보안 요구사항

현재의 모바일 RFID 서비스는 RFID 리더가 장착된 휴대전화로 누구나 태그에 대한 접근이 가능하므로, 태그 정보가 불법적으로 수집될 수 있거나 추적이 가능하다. 특히 PAN (Personal Area Network)을 구성하는 기본장치 뿐만 아니라 사용자의 소지품에 부착된 각종 RFID에 의한 정보 유출 및 사생활 침해가 큰 문제가 될 것으로 우려된다. 왜냐하면, 기존의 고정형 RFID의 경우, 리더기는 항상 고정되어 있고(예를 들면, 상점의 계산대), RFID 태그만 이동되었으나, 모바일 RFID의 경우는 "휴대폰=RFID 리더기"이므로 사생활 침해 요소가 더욱 심각해지게 된다. 이러한 모바일 RFID 서비스에서의 보안 요구사항들을 살펴보면 다음과 같다.

- **태그 블록킹:** 인가된 리더만 태그의 정보를 읽을 수 있고, 그 외의 비인가된 리더는 태그의 정보를 습득할 수 없어야한다.
- **프락시 모드 지원:** 인가된 타인의 리더가 태그 접근하여 읽기요청이 있을 경우, 태그 소유자는 리더기 인증이 확인될 경우 태그를 대신하여 태그 정보를 전송한다.
- **프라이버시 권한 제어:** 태그의 소유자는 상황및 상태에 따라 각각 인가된 리더에 차별화된 접근권한을 설정할 수 있다.
- **데이터 무결성 제공:** RFID 시스템에서 실제 태그정보는 리더기와 OIS 서버 사이의 기존 통신망 구간에서 전송되는데, 이때 전송되는 정보의 위변조 유무를 확인 할 수 있는 기능이 제공되어야 한다.
- **태그 모니터링:** 모든 리더는 태그에 접근하여 읽기/쓰기 등을 명령이 수행될 때 마다 사용자 단말의 UI를 통해 이를 확인 할 수 있어야 한다. 이는 보조적인 수단이지만, 태그 소유자가 직접 눈으로 확인 할 수 있기 때문에 매우 실용적인 요구사항이라 할 수 있다.

2.2 기존 프라이버시 보호 기술

2.2.1 워치독 태그



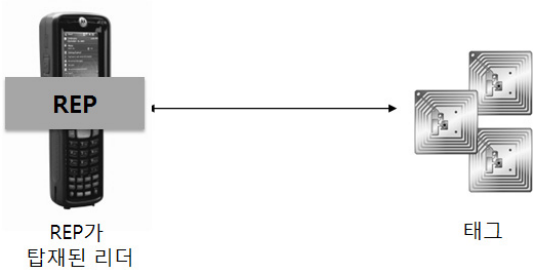
[그림 2] 워치독 시스템

워치독 태그 (Watchdog Tag) [6]는 RFID 프라이버시 보호를 위한 감시 시스템으로써 Floerkemeier et al.에 의해 제안되었다. 워치독 태그는 리더와 태그사이의 구간을 실시간으로 감시하고 있다가 쿼리가 발생되는 순간 작은 스크린을 통하여 사용자에게 정책 ID, 리더 ID등을 개별의 요소를 알려준다.

2.2.2 REP

REP (RFID Enhancer Proxy) [5]는 A. Juels에 의해 제안된 기술로써, 태그에 대한 리더의 접근을 제어하고 필요할 경우 태그를 대신하여 응답하는 디바이스를 사용하여 사용자의 프라이버시를 보호 한다.

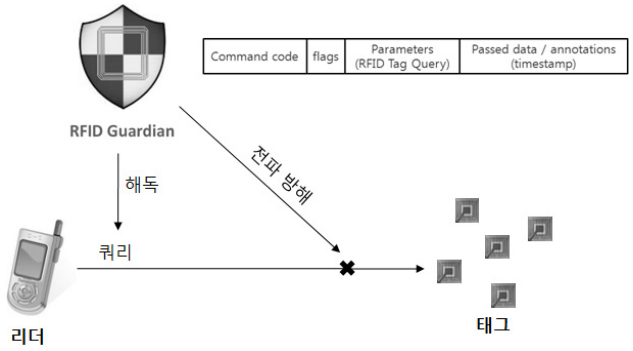
REP는 태그습득, 재암호화, 시뮬레이션, 태그해제의 단계로 구성되어 있는데, 태그 정보의 주기적인 재암호화를 통해 태그의 정보를 보호한다.



[그림 3] RFID Enhancer Proxy 시스템

2.2.3 RFID 가디언

RFID 가디언 (RFID Guardian) [7]은 Rieback et al.이 제안하여 RFID 리더와 태그사이에서, PDA나 기타 휴대용 기기를 사용하여 선택적으로 RFID 전파 방해를 위한 재밍(Jamming) 신호를 발생시켜 비인가된 리더가 허락없이 읽기 시도하는 것을 방지하는 기술이다. 하지만 재밍 신호를 통하여 정당한 리더까지 방해를 받을 수 있는 단점이 있다.



[그림 4] RFID 가디언 시스템

III. 제안 시스템

앞 장에서 기술한 모바일 RFID의 보안 요구사항에 따른 기존 기술들의 제공 기능들을 살펴보면 [표 1]과 같다.

기존의 워치독 태그는 휴대 디바이스를 활용하여 태그 모니터링과 사용자 인터페이스를 제공하지만, 그 이외의 보안 요구사항들을 만족하지 못한다.

REP는 프락시 기능을 지원하고, 재암호화를 통해 태그를 블록킹하여, 태그 정보의 추적성 방지 기능을 제공한다. 하지만 태그 및 리더의 권한별 접근 제어 기능과 사용자 인터페이스를 제공하지 못한다.

RFID 가디언은 주기적인 모니터링과 전파방해를 통해 인가되지 않은 리더에 대해 접근을 막을 수 있고, 상황별 접근 목록을 통해 태그의 접근을 제어한다. 하지만 프락시 기능과 실제 받은 태그의 정보에 대해 데이터 검증을 할 수 없다.

[표 1] MRP 제안 시스템 기능비교

기능	워치독	REP	RFID 가디언	MRP (제안)
태그 블록킹	X	O	O	O
프락시 모드 지원	X	O	X	O
프라이버시 권한 제어	X	X	O	O
데이터 검증	X	X	X	O
태그 모니터링	O	O	O	O

따라서, 본 논문에서는 기존 연구에서 제공하는 기능들을 모두 수용하고 특히, 기존 기술들이 제공하지 못하는 태그 및 리더의 프라이버시 권한별 접근 제어 기능을 제공하도록 하는 모바일 RFID 프락시 (Mobile RFID Proxy: MRP) 시스템을 제안한다.

3.1. MRP 기능 명세

기존의 보안이 적용되지 않은 일반적인 RFID 시스템에서 리더는 공개된 모든 태그에 대해서 읽기 접근이 가능하게 된다. 모바일 RFID 시스템에서는 결국 휴대단말이 리더가 휴대단말을 가진 사람 누구에게나 태그 ID인 EPC (Electronic Product Code) 코드가 노출될 수 있게 되는 프라이버시 침해와 불법적인 추적의 문제가 초래된다. 이런 보안상의 문제점을 해결하기 위해 MRP 시스템은 크게 다음의 2가지 모드를 지원한다.

3.1.1. 블록킹 모드

이 모드에서는 접근 권한이 인가되지 않은 리더가 정상적인 태그 ID를 획득하지 못하도록 태그에 기입력되어 있는 EPC 코드를 랜덤값으로 변경한다. 이 기능을 본 논문에서는 태그 리네이밍(Tag Renaming)이라고 부른다. MRP는 리네이밍을 통해 비인가된 리더기가 태그 EPC를 읽더라도 실제 태그정보는 확보하지 못하도록 하게 된다. 비인가된 리더기가 정확한 태그정보를 획득하기 위해서는 MRP에 자신의 단말기를 등록하는 절차를 따라야 한다.

[그림 5] 블록킹 모드 과정

3.1.2. 프락시 모드

블록킹 모드에 더하여 인가된 리더기가 태그 EPC를 읽기를 시도할 경우, 해당 리더기의 권한이 부합하면 태그의 랜덤값을 전송하는 것이 아니라, MRP가 가지고 있는 태그의 정보를 전송한다. 만약, 비인가된 리더기가 접근할 경우에는 권한제어를 통해 접근이 허용되지 않는다.

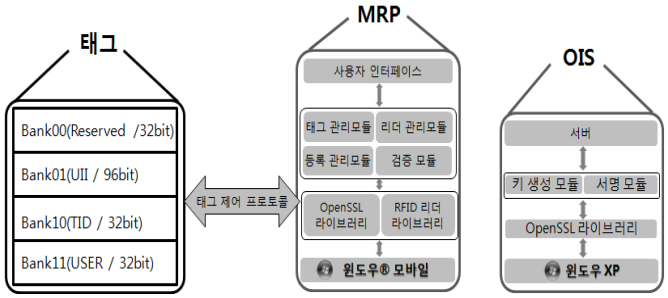
[그림 6] 프락시 모드 과정

3.2 시스템 구조 설계

본 절에서는 MRP 시스템 및 이를 구성하는 OIS 서버에 추가되어야 하는 모듈들에 대한 명세와 태그에서 활용되는 데이터 필드들에 대서 기술한다. 또한, MRP와 태그사이의 제어 프로토콜을 명세한다.

3.2.1 MRP 시스템 구조

MRP 시스템은 윈도우모바일 기반으로 OpenSSL 암호 라이브러리, RFID리더 제어를 위한 라이브러리를 사용하여 각 모듈을 구성하고, GUI 기반의 사용자 인터페이스를 제공한다.



[그림 7] MRP 시스템 구조

MRP 시스템은 각 관리 모듈들은 다음과 같다.

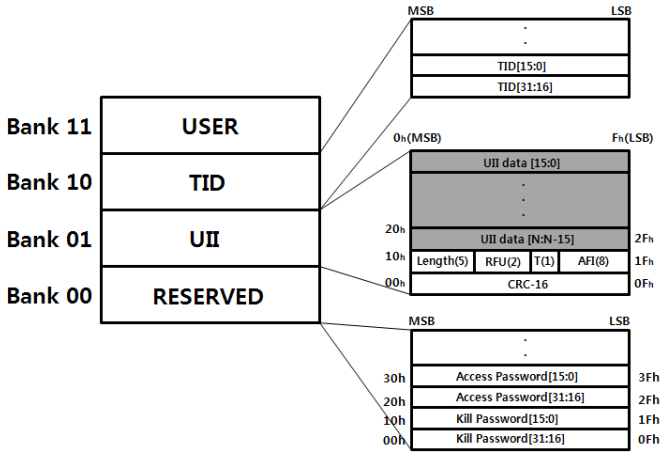
- **등록 관리 모듈:** 본 모듈은 MRP가 초기 본인 소유의 태그를 등록하는 기능을 담당한다. OIS로 부터 등록된 태그 정보와 태그정보에 대한 서명값을 받아와서 인가된 리더에게만 넘겨준다.
- **태그 관리 모듈:** 본 모듈은 등록된 태그의 갱신, 삭제, 권한 수정, OIS로 부터 태그정보 재수신 등의 태그 정보 변경 기능을 지원한다.
- **리더 관리 모듈:** 본 모듈은 인가된 리더의 갱신, 삭제, 권한변경 기능과 비인가된 리더의 인가 등의 리더 정보 변경과 관리 기능을 담담한다. 비인가된 리더는 태그에 접근하기 위해서는 신뢰할 수 있는 리더기 인지를 등록하는 절차를 거쳐야 하며, 리더별로 개별 태그에 대한 접근 권한을 달리 부여할 수 있다.
- **검증 모듈:** MRP 시스템에서는 태그 정보의 무결성 제공을 위해 OIS서버에 태그정보 초기화시 태그정보에 대한 서명값도 같이 생성되는 것을 가정한다. 따라서, 본 모듈은 OIS 서버에 저장된 태그정보가 무선 휴대망을 통해 MRP 전송되는 동안에 태그정보에 대한 위변조 유무를 검증하는 기능을 담당한다.

3.2.2. OIS 구조

MRP 시스템이 제대로 동작하기 위해서는 OIS 서버의 다음과 같은 추가적인 관리 모듈이 필요하다.

- **키 생성 모듈**: 본 모듈은 OIS에서 태그 정보 초기 등록시에 각 태그 정보에 대한 서명 생성시 필요로 하는 개인키, 공개키 쌍을 생성하는 기능을 담당한다.
- **서명 생성 모듈**: 본 모듈은 키 생성 모듈을 통해 생성된 개인키를 사용하여 태그정보 초기 등록시 해당 태그정보에 대한 서명값 생성 기능을 담당한다. 그런 다음, MRP 또는 인가된 리더들에 의해 태그정보 요청시 태그정보와 함께 해당 서명값도 전달한다.

3.2.3 태그제어 프로토콜 및 구조



[그림 8] EPC Gen2 태그 구조

MRP 시스템에서 태그 리네이밍 기능을 실현하기 위해서는 EPC 코드값을 저장할 태그가 재기록하여야 하는데(re-writable), 이를 위해 본 논문에서는 ISO/IEC 18000-6C에 따른 EPC Gen 2 태그를 사용한다. [그림 8]에서 볼 수 있듯이 EPC Gen 2 태그는 Reserved, UII (Unique Item Identifier), TID (Tag IDentifier), USER의 4개의 뱅크로 구성되어 있다. 뱅크 11의 User는 UII를 제외한 모든 정보를 기록하기 위한 사용자 정의 데이터를 저장하는 영역이고, 뱅크 10의 TID는 고유식별번호와 태그 생산자, 시리얼번호, 태그를 식별하기 위한 정보를 포함한다. 뱅크 01의 UII에 EPC 코드가 저장되는데, 본 논문에서 활용되는 랜덤 태그값도 이 영역에 기록된다. 마지막으로 뱅크 00의 Reserved는 kill, access 패스워드를 저장하기위해 사용된다.

MRP 시스템에서 태그 리네이밍을 위해 사용할 뱅크 01의 UII은 CRC (Cyclic Reducdancy Check)-16, PC (Protocol Control), UII data 필드로 이루어져 있다. 이 중에서 MRP 시스템에서 사용할 EPC 코드값은 UII data 필드에 저장되는데, 태그 리네이밍은 기존 태그의 정보를 숨기고 MRP에 의해 28자리수의 랜덤값으로 치환된다.

MRP 시스템이 태그의 뱅크 01 에 있는 UII 필드에 있는 EPC 코드를 읽어 오거나 재기록하기 위해서는 태그 제어 프로토콜이 필요로 한다. 이 태그 제어 프로토콜을 살펴보면 [그림 9]와 같다.

STX(1Byte)	PL(1Byte)	DATA(Variable)	CHECKSUM(1Byte)	ETX(1Byte)

[그림 9] MRP의 패킷 메시지 구조

- STX : 패킷의 시작 (0x7E)
- PL : 패킷의 길이, 데이타+CHECKSUM의 길이
- DATA : 커맨드를 포함한 데이터
- CHECKSUM : DATA의 XOR값
- ETX : 패킷의 끝 (0x7D)

태그제어 프로토콜의 패킷 메시지 구조는 패킷 시작을 알리는 STX (0x7E), 패킷길이를 나타내는 PL, DATA 영역의 XOR값의 CHECKSUM, 패킷 끝은 나타내는 ETX (0x7D)로 이루어진다.

실제 MRP는 DATA영역을 통하여 태그를 제어하게 되는데 One Tag Read 커맨드와 One Tag Write 커맨드를 이용하여 태그 리네이밍 기능을 수행한다. 구체적으로는, One Tag Read 커맨드인 “7E, 03, 60, 65, 05, 7D”를 활용하여 하나의 태그 EPC 정보를 읽어 오거나. 태그 값 모두를 읽기위해서는 Multi Tag Read 커맨드인 “7E, 03, 60, 66, 06, 7D”를 사용한다. 반대로 태그의 EPC를 임의의 랜덤값(예, “1111222233334444”)로 변경하기위해서 One Tag Write 커맨드인 “7E, 18, 60, 77, 20, 31, 20, 34, 20, 31, 31, 31,31, 32, 32, 32, 32, 33, 33, 33, 33, 34, 34, 34, 34, 32, 7D”를 사용하여 태그의 EPC정보를 변경할 수 있다.

3.3 프로토콜 설계

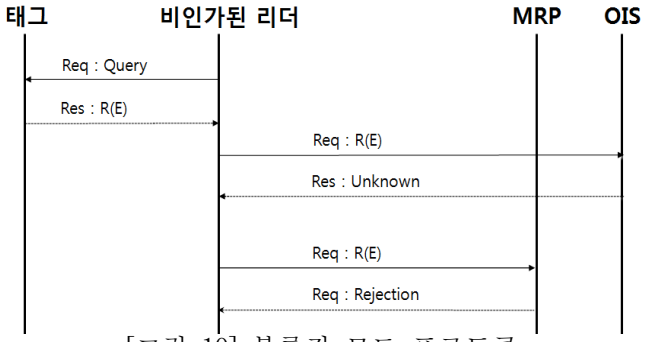
3.1절의 MRP 기능명세에서 볼 수 있듯이 MRP 시스템과 OIS 또는 인가된 리더사이의 프로토콜을 정의하여

야 하는데, 프로토콜 설명을 위해 본 논문에서 사용되는 표기법을 사용하면 [표 2]과 같다.

[표 2] 표기법

기호	설 명
E	태그의 EPC
$R(x)$	x의 리네이밍값
PK_x	x의 공개키
$S_x(m)$	메시지 m에대한 x의 서명값
TI	태그의 정보
RS	등록절차

가. 블록킹모드

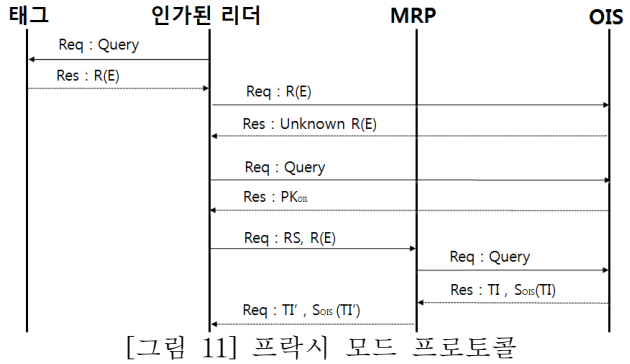


[그림 10] 블록킹 모드 프로토콜

블록킹 모드의 프로토콜은 MRP에 의해 관리되어지는 태그에 대해서 접근을 불가능하게 하여 보호하는 방법이다. [그림 10]의 블록킹 모드 프로토콜에서 보여주는 단계는 다음과 같다.

1) 비인가된 리더는 태그에 R(EPC)를 요청한다.
2) 비인가된 리더는 OIS에게 R(EPC)의정보를 요청하지만 알 수 없는 값을 확인한다.
3) 비인가된 리더는 태그의 소유자인 MRP에게 R(EPC)를 요청하지만 인가된 리더가 아니므로 태그정보(TI)의 습득을 거부당한다.

나. 프락시 모드



[그림 11] 프락시 모드 프로토콜

프락시 모드는 MRP에 의해 관리되어진 태그는 인가된 리더만 접근을 가능하게 하여 보호하는 방법이다. [그림 11]의 프락시 모드 프로토콜에서 보여주는 단계는 다음과 같다.

1) 비인가된 리더는 태그에 R(EPC)를 요청한다.
2) 비인가된 리더는 OIS에게 R(EPC)의 정보를 요청하지만 알 수 없는 값을 확인한다.
3) 비인가된 리더는 OIS에게 공개키(PK_{ois})를 받는다.
4) 비인가된 리더는 MRP에게 인가된 리더로 승인받기 위해 등록절차(RS)를 거치며, 태그의 정보를 요청한다.
4) MRP는 태그의 EPC(E)를 통해 태그의 정보와 서명값을 수신한다.
5) MRP는 인가된 리더에게 태그의 정보와 서명값을 권한에 맞게 송신한다.

IV. 결론

본 논문에서는 휴대폰이 곧 RFID리더기가 되는 모바일 RFID 서비스에서 초래될 수 있는 프라이버시 문제를 해결하기 위해 개인 사용자가 자신의 태그를 타인의 리더기의 불법적인 접근으로부터 보호하기 위한 기술들을 제안하였다. 제안 시스템은 태그의 선택적 블록킹 뿐만 아니라, 인가된 리더의 접근 시도에 대해서는 태그가 아닌 MRP 시스템이 대신 태그정보를 응답하는 프락시 기능을 제공한다.

제안 MRP 시스템은 기존 기술들이 개별적으로 제공하는 기능들을 모두 수용하고 특히, 기존 기술들이 제공하지 못하는 태그 및 리더의 프라이버시 권한별 접근 제어 기능을 제공하도록 하였다.

향후 본 논문에서 제시된 제안 시스템의 설계를 바탕으로 구현과 테스트베드 구축을 통한 실현가능성을 검증할 계획이다.

참 고 문 헌

[1] A. Juels, "RFID security and privacy: A research survey," IEEE Journal on Selected Areas in Communications, 24(2):381 394, February 2006.

[2] A. Juels, "Minimalist cryptography for low-cost RFID tags," International Conference on Security in Communication Networks (SCN'04), pp. 149-164, September 2004.

[3] A. Juels, Private communication, May 2007.

[4] A. Juels, R. Rivest, and M. Szydlo, "The blocker tag: Selective blocking of RFID tags for consumer privacy," ACM International Conference on Computer and Communications Security (CCS'03), pp. 103-111, October 2003.

[5] A. Juels, P. Syverson, and D. Bailey, "High-power proxies for enhancing RFID privacy and utility," Workshop on Privacy Enhancing Technologies (PET'05), June 2005.

[6] C. Floerkemeier, R. Schneider, and M. Langheinrich, “Scanning with a purpose – supporting the fair information principles in RFID protocols,” International Symposium on Ubiquitous Computing Systems (UCS‘04), pp.214-231, November 2004.
[7] M. Rieback, B. Crispo, and A. Tanenbaum, “RFID guardian: A battery-powered mobile device for RFID privacy management,” Australasian Conference on Information Security and Privacy (ACISP'05), pp. 184-194, July 2005.
[8] S. Inoue and H. Yasuura, “RFID privacy using user-controllable uniqueness,” RFID Privacy Workshop, November 2003.