情報保護學會論文誌
第17卷 第1號, 2007. 2

모바일 기반의 RFID 프라이버시 보호 기법*

김 일 중,† 최 은 영, 이 동 훈‡
고려대학교, 정보경영공학전문대학원

A RFID privacy protect scheme based on mobile

Il Jung Kim,† Eun Young Choi, Dong Hoon Lee‡
Graduate School of Information Management and Security, Korea University.

요 약

EPC 네트워크(Electronic Product Code Network) 환경 기반의 RFID 시스템은 사물에 직접적인 접촉을 하지 않고 RF(Radio Frequency) 신호를 이용하여 사물의 정보를 읽어 오거나 기록할 수 있다. 이것은 기존의 바코드 시스템에 비해서 저장능력이 뛰어나며 비접촉식이라는 이점을 갖는다. 이런 RFID 시스템과 모바일 시스템을 접목함으로서 사용자에게 새로운 부가서비스를 제공하는 모바일 RFID 시스템이 만들어지게 되었다. 그러나 비접촉식의 RF(Radio Frequency) 통신을 이용하여 사물의 정보를 가져온다는 이점은 개인의 프라이버시 침해라는 문제점을 발생시킨다. 본 논문에서는 모바일 기반의 RFID 시스템에서의 개인 프라이버시를 보호하는 기법을 제안한다. 제안한 기법은 기존에 제안된 기법들 보다 효율적으로 프라이버시 보호기능을 제공한다.

ABSTRACT

Radio Frequency Identification system based on EPC(Electronic Product Code) Network Environment can read or write information of tagged objects, using RF signals without direct contact. This advantage which is to provide storage ability and contactless property is better than Bar-code system. Mobile RFID system which integrates Mobile system with RFID system will provide new additional service to users. However, an advantage for obtaining information of objects using RF signal causes personal privacy problem. In this paper, we propose techniques that can protect personal privacy based on mobile. Our scheme provides privacy protection of users and is more efficiently than another application service.

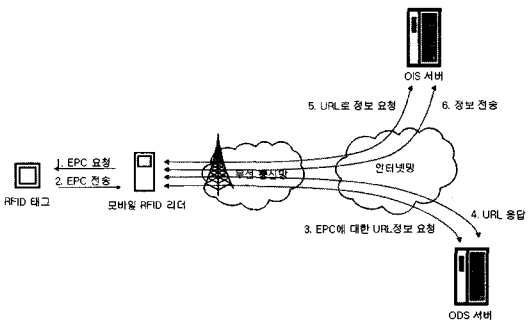
Keywords : *Mobile RFID, RFID system, Privacy, Security*

접수일: 2007년 1월 6일; 채택일: 2007년 1월 27일
* 본 연구는 서울시 산학연 협력사업(10665)의 지원으로 수행된 연구임
† 주저자, wyvern99@korea.ac.kr
‡ 교신저자, donglee@korea.ac.kr

Ⅰ. 서 론

EPC 네트워크(Electronic Product Code Network) 환경 기반의 RFID(Radio Frequency IDentification) 시스템은 칩을 내장한 태그를 사물에 부착하여 태그에 저장된 데이터를 무선 주파수(Radio Frequency)를 통해 자동 인식할 수 있도록 하는 시스템이다.[1] RFID 시스템은 바코드 시스템과는 달리 무선 주파수를 이용한 비접촉 통신과 많은 데이터를 저장할 수 있으며 이러한 이점을 이용한 많은 연구가 이루어지고 있다.[2,3,4,10,13] 모바일 RFID 시스템은 RFID 시스템과 모바일 기기 및 무선 인터넷을 접목한 것으로 RFID 시스템의 이점과 모바일 기기의 이점을 모두 가지며 다양한 분야에 적용 가능하다. 하지만 모바일 RFID 시스템이 갖는 이점들은 사용자의 프라이버시 침해라는 문제를 야기시킬 수 있다. 그 이유는 모바일 기기가 보편화됨으로써 많은 사람들이 모바일 리더를 소유하게 되어 개인 프라이버시 침해 기회가 크게 증가하기 때문이다. 모바일 리더를 소유한 사람이라면 누구든지 다른 사람이 소유한 상품의 정보를 알 수 있으며 또 특정 상품의 EPC를 추적하여 상품을 소유한 사람을 추적할 수 있다. 이런 문제점을 해결하기 위해서 많은 연구들이 여러 기법들이 제안되었다.[5,7,12] 모바일 RFID 시스템의 문제점을 보안하기 위해서 많은 기법들이 연구되었다. Kill command는 그 중에서 물리적이며 가장 간단한 방법이다. Kill command는 태그에 Kill 명령어를 이용하여 EPC를 제거하는 방법으로 정보유출, 위치추적을 예방한다. 하지만 Kill command는 간단하면서도 강력한 프라이버시 보호 방법이지만 EPC를 제거 후에는 RFID 시스템을 사용하지 못한다는 단점이 있다. [12]에서 제안된 기법은 가디언(Guardian)이라는 모바일이나 PDA를 이용하여 사용자가 소유한 물건에 외부의 리더가 접근하는 것을 모두 컨트롤 하는 기능을 수행한다. 이 기법은 강력한 프록시(Proxy)를 사용하여 RFID 시스템에서 발생 할 수 있는 문제점들을 해결하려고 하였다. 또한 가디언과 유사한 기능을 제공하며 향상시킨 High-Power 프록시 REP(RFID Enhancer Proxy)가 Juels 등에 의해서 제안되었다.[5] 이 기법은 기존에 제안된 가디언 기법과 유사하며, 이것은 외부에서 태그에 의미 없는 값을 써 넣는 공격을 해결하기 위해서 프록시인 REP가 자체적으로 태그의 정보를 갱신하는 방법을 제안하였다. 그러나 이 두 기법은 프록시가 외부의 모든 신호를 감지 가능하다는 강력한 가정을 기반으로 하므로 실질적으로 RFID 시스템의 문제 해결을 하기에는 부적합하다. [7]에서 제안한 기법인 MARP는 [5,12]에서 제안한 기법처럼 강력한 조건이 요구되지 않으나 리더와 태그 그리고 프록시의 키를 관리해주는 공개키 센터와 같은 신뢰성 있는 기관 또는 장치가 요구된다.

본 논문에서는 RFID 시스템에 부가적인 장치인 프록시가 아닌 RFID 시스템의 일부분으로 모바일 리더를 사용하는 실질적으로 RFID 시스템의 문제 해결을 하기 위한 모바일 기반의 RFID 프라이버시 보호 기법을 제안한다. 제안 기법은 [5,7,12]에서 제안한 기법들처럼 리더와 태그사이의 통신을 모두 감지하여 관리할 필요가 없다. 그리고 [7]에서 제안한 기법은 추가적인 공개키 센터가 필요한 반면에 제안하는 기법은 추가적인 장치가 필요 없이도 사용자의 프라이버시를 보호할 수 있으며 해쉬 함수의 사용을 줄여 더 효율적이다. 제안하는 기법은 상품을 구매하기 전에는 매장 내에서 상품의 기업에서 발행한 인증서를 사용하여 상품에 대한 정확하고 신뢰성 있는 정보를 얻고 상품을 구매 후에는 해당 태그에 대한 키를 소유하여 태그가 모바일 리더에게 항상 랜덤한 값을 응답하더라도 소유자의 모바일 리더는 태그의 ID(EPC)를 알 수 있게 한다. 태그가 모바일 리더에게 항상 랜덤한 값을 응답하기 때문에 제 삼자가 이것을 도청하더라도 상품의 정보를 알아낼 수 없다. 그리고 태그의 응답을 특정한 상품과 연결시킬 수 없게 되어 추적이 불가능하게 된다. 본 논문의 구성은 다음과 같다. 2장에서는 모바일 RFID 네트워크에 대하여 설명하고 3장에서는 모바일 RFID 시스템에서 해결해야할 보안 및 프라이버시 문제점에 대하여 설명한다. 그리고 4장에서는 모바일 기반의 RFID 프라이버시 보호 기법을 제안하고 5장에서는 제안 기법의 안전성과 효율성에



[그림 1] 모바일 RFID 네트워크 구조

〔표 1〕 EPC 구조 설명

항 목	내 용
해더(8bit)	데이터 유형 및 길이를 정의
EPC 관리자 (28bit)	상품에 대한 분류와 일련번호를 관리하는 기관이나 기업을 표시
상품 분류 번호 (24bit)	바코드의 상품 품목 코드에 해당하는 것으로 각 품목 또는 단위를 표시
일련번호 (36bit)	각 상품들에 대하여 부여되는 고유한 식별번호

대해 분석한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 모바일 RFID 네트워크

모바일 RFID 네트워크는 태그(Tag), 모바일 리더(Mobile Reader)와 네트워크 서버(Network Server)로 이루어져 있다. 〔그림 1〕은 모바일 RFID 네트워크의 구조를 나타내고 있다.[8]

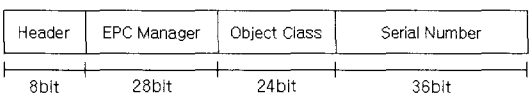
2.1 EPC (Electronic Product Code)[16]

모바일 RFID 시스템에서는 태그의 고유 정보를 EPC 구조로 저장한다. EPC는 해더(Header), EPC 관리자(EPC Manager), 상품 분류 번호(Object Class), 일련번호(Serial Number)로 〔그림 2〕의 구조를 갖는다. 각 항목에 대한 내용은 〔표 1〕과 같다.

2.2 태그 (Tag)

모바일 리더로부터 질의를 받아 상품에 대한 고유정보(EPC)를 RF 신호를 이용하여 전송한다. 태그는 RF 통신을 위한 안테나와 연산과 고유정보를 저장하는 마이크로 칩으로 구성 되어있다. 태그는 전력 공급 방법에 따라 능동형 태그 (Active Tag)와 수동형 태그 (Passive Tag)로 구분된다.

- 수동형 태그 (Passive Tag) : 수동형 태그는 모바일 리더로부터 받은 RF 신호로부터 전력을 공급받아 동작한다. 근거리 통신이 가능하며 복잡한 연산을 수행하기 어렵다. 수동형 태그는 능동형 태그와는 다르게 배터리를 내장하고 있지 않아 수명이 반영구적이며 능동형 태그에 비해 가격이 싸다. 본 논문에 사용된 태그는 EPCglobal Class 1 Generation 2의 표준에서 PRNG (Pseudo Random Number Generator)가 태그 내에 포함될 수 있다는 점에 기반을 두어서 태그가 의사 난수를 생성할 수 있다고 가정한다.[16]
- 능동형 태그 (Active Tag) : 능동형 태그는 태그 자체에 내장되어 있는 배터리를 통하여 전력을 공급받는다. 리더와 원거리 통신이 가능하지만 배터리가 내장되어 있어 가격이 비싸고 배터리가 모두 소모되면 태그의 사용이 불가능하다.



〔그림 2〕 EPC 구조

2.3 모바일 리더 (Mobile Reader)

모바일 리더는 기존의 RFID 시스템의 리더를 모바일 기기에 내장한 것이다. 태그에 질의를 전송하며 태그로부터 전송된 데이터를 인식하거나 태그에 새로운 정보를 다시 쓰는 역할을 한다. 기존의 RFID 시스템의 리더에 비해 연산능력이 뛰어나며 저장 공간 또한 더 크다.

2.4 네트워크 서버 (Network Server)[14,15]

(1) ODS 서버 (Object Directory Service Server)는 DNS 서버(Domain Name Service Server)와 비슷한 형태로 해당 EPC의 정보를 가지고 있는 서버의 URL(Uniform Resource Location)을 알려준다.

- National ODS : 각 기관의 Local ODS의 위치정보 영역 파일 관리
- Local ODS : 소속기관의 OIS 위치정보 관리

(2) OIS 서버 (Object Information Service Server)는 태그의 EPC와 매칭 되는 컨텐츠(Content)를 저장하고 있고 컨텐츠의 요청이 있을 때 컨텐츠를 준다.

Ⅲ. 보안 및 프라이버시 문제점

모바일 RFID 시스템의 특성상 모바일 리더와 태그는

〔표 2〕 용어 정의

용 어	정 의
$request_p$	상품을 구매하기 전에 매장 내에서 모바일 리더가 태그로부터 ID를 읽어올 때 사용하는 요청 신호
$request_c$	상품을 구매 후 태그로부터 PID, KID를 받기 위한 요청 신호
ID	태그의 EPC
K	태그의 키(Key) 값
K_j	모바일 리더가 소유한 키들
r_i	모바일 리더의 난수 생성기(PRNG)로 생성한 랜덤 값
r_T	태그가 생성한 랜덤 값
$h_K()$	키드 해쉬(keyed hash function)
Certificate(C_i)	상품에 대한 신뢰성있는 정보를 확인하는데 사용되는 인증서로 인증용 값(C), EPC에 해당하는 정보를 가지고 있는 서버의 위치 정보 포함
$list_c$	인증용 값의 리스트
⊕	exclusive-OR

직접적인 접촉이 없이 RF 통신을 이용하여 데이터를 주고받는다. 태그는 모바일 RFID 리더의 신호에 반응하여 자신의 고유정보(EPC)를 모바일 리더에 전송한다. 이러한 태그와 모바일 리더의 통신방법은 태그가 고유정보를 요청하는 모바일 리더의 정당성을 확인하지 않기 때문에 주변의 제 삼자가 손쉽게 사용자가 소유하고 있는 상품의 정보와 위치정보를 알아낼 수 있어 사용자의 프라이버시 침해 문제가 발생하게 된다. 결국 RFID 시스템은 기존의 RFID 시스템의 문제점을 가지게 되며 구체적은 내용은 다음과 같다. 모바일 RFID 시스템에서 사용자 프라이버시 침해 문제는 다음과 같이 나타난다.[6,9,13]

- 정보의 누출 (Information Leakage)

상품을 구매하기 전에, 누구든지 상품의 정보를 모바일 리더를 사용하여 읽어오는 것은 문제가 되지 않는다. 그러나 상품을 구매한 후에 제 삼자가 상품을 소지한 사용자에게 정보를 읽어오는 것은 사용자의 프라이버시를 침해하게 된다. 예를 들어 고가의 상품이나 특정 병력에 대한 약품 등을 소지하고 있을 때 제 삼자가 모바일 리더를 사용하여 사용자가 소유하고 있는 물품의 정보를 쉽게 얻을 수 있어 개인의 정보 유출이 가능하다.

- 추적 가능 (Tracability)

모바일 RFID 시스템은 EPC 체계를 사용하는데 EPC는 태그에 대한 고유한 식별정보를 나타내며 모바일 RFID 리더는 태그로부터 EPC를 읽어 상품에 대한 정보를 얻는다. EPC가 태그의 고유한 정보를 나타내며 어떤 리더가 질의하던지 자신이 저장하고 있는 EPC를 전송한다. 그러므로 사용자가 특정 상품을 가지고 있다면 제 삼자는 특정 상품의 EPC를 추적하여 사용자를 추적할 수 있다.

- 재전송 공격 (Replay Attack)

제 삼자(공격자)가 리더와 태그 사이의 통신을 도청하여 정보를 저장한다. 제 삼자는 도청한 태그의 정보를 이용하여 리더가 태그에게 정보를 요청할 때 대신 응답한다. 제 삼자가 진짜 태그인 것처럼 리더를 속일 수 있다.

- 스푸핑 공격 (Spoofing Attack)

제 삼자(공격자)는 태그에게 리더인 척하여 태그의 정보를 얻는다. 제 삼자는 정보를 받고 태그와의 통신이 정상적으로 끝나기 전에 세션을 종료한다. 제 삼자는 태그로부터 얻어낸 정보를 이용하여 리더를 속일 수 있다.

Ⅳ. 모바일 기반의 RFID 프라이버시 보호 기법

본 절에서는 모바일 RFID 기반의 RFID 프라이버시 보호 기법을 제안한다. 제안한 시스템은 상품을 구매하기 전과 상품을 구매 후에 상품의 정보를 확인할 수 있는 두 과정으로 이루어져있다.

4.1 용어 정의

〔표 2〕는 제안한 기법에서 사용하는 용어들의 정의를 나타낸 것이다.

4.2 상품 구매 전 상품 정보 확인 과정

상품을 구매하기 전에 매장 내에서 상품에 대한 신뢰성 있는 정보를 확인하는 과정으로 각 매장은 로컬 서버(Local Server)를 소유하게 된다. 모바일 리더와 서버 사이의 통신은 기존의 무선 통신을 사용하기 때문에 안전하다. 〔그림 3〕은 제안한 기법의 흐름도를 표현한 것이다.

각 매장의 로컬 서버는 상품들에 대한 인증용 값을 포

함한 인증서들을 서버로부터 미리 받아 저장하고 있다.

(1) 사용자가 매장에 들어가게 되면 매장의 로컬 서버로부터 EPC에 해당하는 정보를 가지고 있는 서버의 위치 정보와 인증용 값(C_i)을 포함한 인증서(Certificate(C_i))를 모바일 리더로 받는다.

(2) 모바일 리더는 (requestp, C_i)를 보내어 상품에 ID를 요청한다.

(3) 태그는 $h_K(C_i)$를 생성하여 ID를 XOR하여 NID를 생성한 뒤 NID를 모바일 리더에게 보낸다.

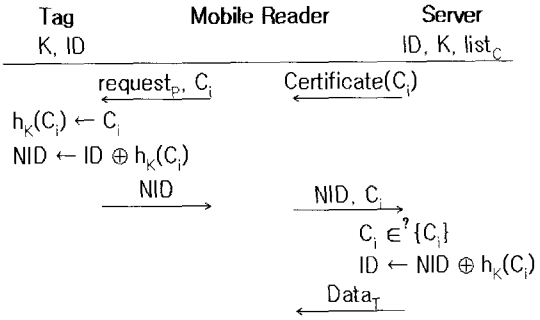
(4) 모바일 리더는 Certificate(C_i)의 안의 OIS 서버의 위치 정보를 이용하여 태그로부터 받은 NID와 C_i를 OIS 서버에게 보낸다.

(5) 서버는 모바일 리더로부터 받은 C_i가 데이터베이스의 $list_C$(={C})에 속하는지 확인하고 속한다면 모바일 리더가 보낸 C_i, NID와 저장하고 있는 K를 이용하여 ID를 생성한다. 생성한 ID에 $Data_T$를 데이터베이스에서 찾아 모바일 리더에게 전송한다.

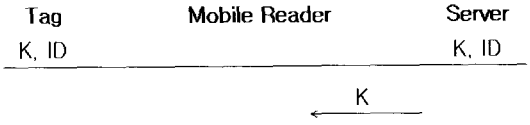
4.3 상품 구매 후 초기설정

모바일 리더와 서버사이의 통신은 기존에 사용되고 있는 안전한 무선 보안 통신을 사용한다. 상품을 구매 후 사용자는 서버로부터 안전한 채널을 통해서 상품에 대한 키(K)를 모바일 리더로 받게된다([그림 4]).

사용자는 서버로부터 받은 키(K)를 모바일 리더에 저장하여 상품 정보를 읽어올 때 사용한다. 모바일 리더를 소유한 사용자는 서버로부터 받은 키(K)를 사용하여 자신의 프라이버시를 보호 할 수 있게 된다. 상품 구매 후 사용자의 프라이버시를 보호하면서 상품의 정보를 확인할 수 있는 방법은 다음에서 설명한다.



[그림 3] 상품 구매 전 상품 정보 확인



[그림 4] 상품 구매 후 초기 설정

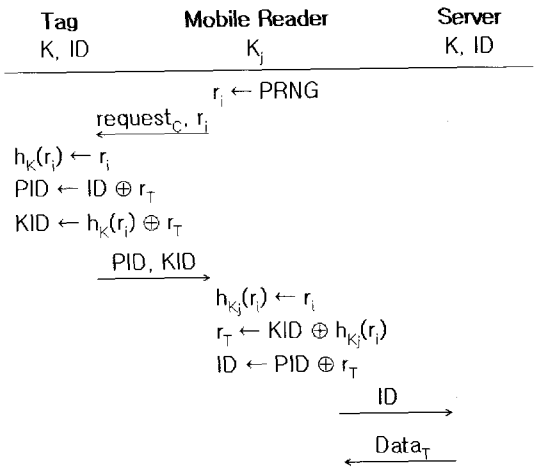
4.4 상품 구매 후 사용자의 프라이버시 보호 및 상품 정보 획득

사용자가 상품을 구매 후 모바일 리더와 상품의 키를 이용하여 사용자의 상품을 관리하고 상품의 정보를 읽어 상품의 정보가 변경되거나 새로운 내용이 갱신되었을 때 항상 안전하게 상품의 정보를 확인 가능하며 사용자 이외의 제 삼자가 상품의 정보를 확인 할 수 없게 하여 구매 후에도 상품에 대한 신뢰성 있는 정보를 확인할 수 있으며 사용자의 프라이버시를 보호할 수 있다. [그림 5]는 상품 구매 후의 상품의 정보를 얻는 방법의 흐름도를 나타낸 것이다.

(1) 모바일 리더는 난수 생성기(PRNG)를 이용하여 난수 r_i를 생성하여 태그에게 데이터를 요청하는 신호와 함께 전송한다 ($request_c$, r_i).

(2) 태그는 모바일 리더로부터 받은 r_i를 K와 해쉬함수를 이용하여 $h_K(r_i)$를 생성한다. 태그는 난수 r_T를 생성하고 이것을 이용하여 PID, KID를 생성한 뒤 모바일 리더에 전송한다.

(3) 모바일 리더는 가지고 있는 모든 키(K_j)를 사용하여 KID로부터 r_T를 추출하고 r_T를 이용하여 PID로부터



[그림 5] 상품 구매 후 상품 정보 확인

〔표 3〕 I : 해쉬 함수의 출력 길이나 키의 길이 또는 ID의 길이, H : 한 번의 해쉬 연산, X : XOR 비트 연산, E : 한 번의 암호화 연산, D : 한 번의 복호화 연산, V : 한 번의 서명 검증 연산, S : 한 번의 서명 연산, M : MARP가 감지할 수 있는 영역 내에 존재하는 태그의 수, N : 모바일 리더가 소유한 키의 수, - : 고려사항 없음

프로토콜		MARP[7] 기법	제안 기법
저장공간	태그	3I	2I
	모바일 리더	7I	1I
	데이터베이스	5I	2I
계산량	태그	2H+3X	1H+1X (구매 전) 1H+2X (구매 후)
	모바일 리더	(3E+1D+2V+2S+1H+1X)*M	- (구매 전) (1H+2X)*N (구매 후)
	데이터베이스	1E+3D+2V+1S+2H+1X	1H+1X (구매 전) - (구매 후)

ID를 추출한다. 추출한 ID중에 EPC의 구조를 가진 ID를 서버에 전송한다.

(4) 서버는 올바른 ID에 대하여 해당하는 데이터를 모바일 리더에 전송한다.

V. 제안한 기법의 안전성과 효율성

본 절에서는 제안 기법에 대한 효율성과 안전성에 대하여 논의한다.

5.1 안전성

제안 기법은 다음과 같이 사용자에게 정확한 상품의 정보를 제공하며 사용자의 프라이버시를 보호한다. 구체적인 내용은 다음과 같다.

- 구매 전 상품 정보에 대한 신뢰성 : 제안 기법에서는 상품의 기업에서 발행하는 인증서를 매장의 로컬 서버가 소유하고 사용자의 모바일 리더에 주어지게 된다. 모바일 리더는 로컬 서버로부터 받은 인증서의 인증용 값(C_i)과 상품의 정보를 가진 서버의 위치 정보를 이용하여 상품의 정보를 얻을 수 있게 되어 상품의 정보에 대한 신뢰성을 보장 받는다.
- 정보 유출 : 제안하는 기법은 태그가 자신의 ID (EPC)가 아닌 ID를 포함한 랜덤한 값을 모바일 리더에게 응답하게 한다. 구매 전에는 (C_i)의 키드 해쉬함수로 ID를 감추어 NID를 전송하고 구매 후에는 모바일 리더와 태그가 생성한 랜덤 값과 키드 해쉬값으로 ID를 감추어 PID를 전송한다. 공격자는 NID, PID 만으로는 사용자가 소지한 상품에 대한 ID를 알아낼 수 없고 또 정보도 알 수 없다.
- 추적 불가능 : 이 특성은 사용자가 상품을 구매한 후에 꼭 제공되어야 하는 특성이다. 제안 기법에서는 사용자가 상품을 구매 후에는 태그의 고유한 키를 받아 모바일 리더로 관리하게 된다. 태그의 고유한 키와 키드 해쉬 함수를 사용하여 태그가 모바일 리더의 응답에 항상 다른 값(PID, KID)으로 응답하게 하여 키를 알지 못하는 사용자는 태그의 ID를 알지 못하게 된다. 구체적으로 설명하면, 모바일 리더의 요청에 태그는 PID, KID를 항상 다른 값으로 전송하기 때문에 특정 상품에 대하여 추적이 불가능함으로 사용자를 추적할 수 없다.
- 태그 위조 불가능 : 제안된 기법에서는 상품을 구매 후에 모바일 리더가 소유한 태그의 고유 키(K)를 통해서 위조 공격에 안전하다. 제 삼자(공격자)가 스푸핑 공격이나 재전송 공격으로 리더와 태그 사이의 통신을 도청하여 정보(PID, KID)를 얻어내더라도 태그의 고유 키(K)를 모른다면 매 세션의 랜덤 값 r_i에 대한 $h_K(r_i)$를 알 수 없기 때문에 태그의 정보가 노출되지 않는다.

5.2 효율성

기존에 제안된 다수의 기법들의[5,7,12] 프록시가 태그와 리더사이의 통신을 모두 관리하는 반면에 제안 기법

은 모바일 기기가 리더이기 때문에 태그의 정보를 읽어 올 때만 모바일 리더가 태그에게 신호를 보내면 된다. [5,12]에서 제안한 기법의 프록시는 강력한 가정을 기반으로 하므로 실질적으로 RFID 시스템의 문제를 해결하기 어렵다. 그래서 제안 기법의 시스템과 유사한 형태를 지니고 실질적으로 RFID 시스템의 문제를 해결하며 가장 낮은 연산으로 프로토콜을 수행하는 Kim등의 MARP 기법[7] 과 제안 기법의 비교를 통해서 제안 기법의 효율성에 대해서 논의한다. 제안 기법은 [표 3]에서 볼 수 있듯이 구매 전에는 상품의 정보를 확인하는 과정에서 모바일 리더는 연산이 필요 없이 태그는 1번의 해쉬 연산과 1번의 XOR 비트 연산이 요구된다. 구매 후의 상품의 정보를 확인하는 과정에서는 태그는 1번의 해쉬 연산과 2번의 XOR 비트 연산이 요구되며 모바일 리더는 모바일 리더가 소유한 키의 숫자만큼 1번의 해쉬 연산과 2번의 XOR 비트 연산이 요구된다. 이런 제안 기법의 계산량은 MARP 기법에서 태그가 2번의 해쉬 연산과 3번의 XOR 비트 연산을 수행하며 MARP가 자신이 감지 가능한 영역의 태그의 수만큼 해쉬 연산과 XOR 비트 연산 이외에도 복잡한 암·복호화 연산과 서명·검증 연산을 수행하는 것에 비해서 계산양이 매우 적고 효율적이다. 또한 제안 기법에서 태그와 모바일 리더에 저장되는 데이터의 양은 MARP 기법에서 저장되는 데이터의 양에 비해 3배정도 작다.

Ⅵ. 결론

모바일 RFID 시스템은 기존의 RFID 시스템과 모바일 시스템이 접목되어 만들어 일상생활에 넓게 이용되게 될 것이다. 모바일 기기가 많은 사람들이 보편적으로 사용하는 만큼 모바일 리더 또한 보편적인 기기가 되어 사용자들의 프라이버시 침해 문제를 발생시킬 것이다. 제안하는 시스템은 태그가 자신의 ID(EPC)가 아닌 ID를 포함한 랜덤한 값을 모바일 리더에게 응답하게 하여 사용자의 프라이버시를 보호하였다. 본 논문에서 제안한 시스템은 기존에 제안된 기법들과 다르게 RFID 시스템에 추가적인 장비인 프록시가 아닌 리더를 사용하고 [5,7,12]처럼 강력한 요구사항이나 추가적인 기관이나 장치가 필요 없다. 그리고 더 낮은 계산량으로 모바일 RFID 시스템의 개인 정보 유출과 위치 추적 프라이버시 문제를 효율적으로 해결하였다.

참고문헌

[1] D. Brock. "The Electronic Product Code - A Naming Scheme for physical Objects", Auto-ID White Paper, 2001.

[2] Eun Young Choi, Su-Mi Lee and Dong Hoon Lee. "Efficient RFID Authentication Protocol for Ubiquitous Computing Enviro- nment", EUC Workshops, 2005.

[3] K. Finkenzeller. "RFID handbook". John Wiley & Sons, 1999.

[4] A. Juels, R. Rivest, and M. Szydlo. "The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy". ACM CCS 2003, pp. 27-30, 2003.

[5] A. Juels, P. Syverson, and D. Bailey, "High-Power Proxies for Enhancing RFID Privacy and Utility", CHACS 2005, LNCS 3856, pp.210-226 ,2005

[6] H. Knospe and H. Pob. "RFID Security". Infomation Security Technical Report, vol. 9, no. 4, pp. 39-50, Elsevier, 2004.

[7] Soo-Cheol Kim, Sang-Soo Yeo, Sung Kwon Kim. "MARP: Mobile Agent for RFID Privacy Protection". 7th Smart Card Research and Advanced Application IFIP Conference (CARDIS'06), Lecture Notes in Computer Science, vol. 3928, pp. 300-312, 2006.

[8] 김용운, 이준섭, 유상근, 김형준. "모바일 RFID 서비스 네트워크 구조 및 표준화 현황". TTA Journal No.102, pp. 44-53

[9] M. Ohkubo, K. Suzuki, and S. Kinoshita. "A Cryptographic Approach to "Privacy-Friendly" tag". RFID Privacy Workshop, 2003.

[10] 박남제. "모바일 RFID 정보보호 표준화 동향 및 전망", TTA IT Standard Weekly, 2005.

[11] Damith Ranasinghe, Daniel Engels, and Peter Cole. "Low-Cost RFID Systems: Confronting Security and Privacy". Auto-ID Labs Research Workshop, 2004

[12] M. Rieback, B. Crispo, and A. Tanenbaum, "RFID Guardian: A Battery-powered Mobile

Device for RFID Privacy Management", ACISP 2005, LNCS 3574, pp. 184-194, 2005

[13] S. A. Weis, S. Sarma, R. Rivest, and D. Engels. "Security and privacy aspects of low-cost radio frequency identification systems". SPC 2004, LNCS 2802, pp. 201-212, 2004.

[14] EPCglobal Inc., "EPCglobal Network : Overview of Design, Benets, and Secutiry", 2004.

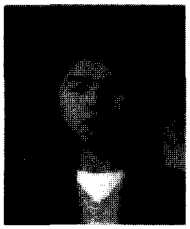
[15] EPCglobal Inc., "EPCglobal Object Name Service (ONS) 1.0"

[16] EPCglobal Inc., "Radio Frequency Identity Protocol Class 1 Generation 2 UHF RFID protocol for communication at 860Mhz-960 Mhz version 1.0.9"

〈著者紹介〉

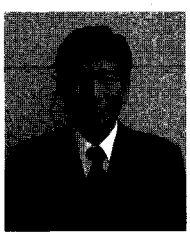
김 일 중 (Il Jung Kim) 학생회원

2005년 8월: 고려대학교 전산학과 졸업
2005년 9월~현재: 고려대학교 정보경영공학전문대학원 석사과정
<관심분야> 정보보호, RFID 정보보호 기술, 유비쿼터스



최 은 영 (Eun Young Choi) 학생회원

2001년 8월: 고려대학교 수학과 학사
2003년 8월: 고려대학교 정보보호대학원 공학 석사
2004년 3월~현재: 고려대학교 정보보호대학원 박사과정
<관심분야> 암호 이론, 정보보호 이론, RFID 정보보호 기술, 유비쿼터스



이 동 훈 (Dong Hoon Lee) 종신회원

1983년 8월: 고려대학교 경제학사
1987년 12월: Oklahoma University 전산학 석사
1992년 5월: Oklahoma University 전산학 박사
1993년 3월~1997년 2월: 고려대학교 전산학과 조교수
1997년 3월~2001년 2월: 고려대학교 전산학과 부교수
2001년 2월~현재: 고려대학교 정보보호대학원 교수
<관심분야> 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술