2006년 2월

석사학위논문

RFID 기반 확장 EPC 코드를 이용한 프라이버시 보호

조선대학교 대학원

컴퓨터 공학과

박 도 준

RFID 기반 확장 EPC 코드를 이용한 프라이버시 보호

Privacy Protection using RFID-based Extended EPC

2006 년 2 월

조 선 대 학 교 대 학 원

컴 퓨 터 공 학 과

박 도 준

RFID 기반 확장 EPC 코드를 이용한 프라이버시 보호

지도교수 이 준

이 논문을 공학석사 학위신청 논문으로 제출함.

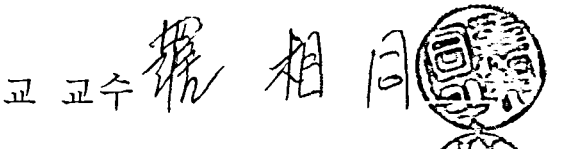
2005 년 10 월

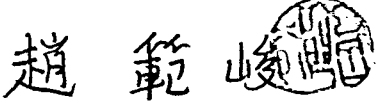
조 선 대 학 교 대 학 원

컴 퓨 터 공 학 과

박 도 준

박도준의 석사학위논문을 인준함

위원장 조선대학교 교수 

위원 조선대학교 교수 

위원 조선대학교 교수 

2005 년 11 월

조선대학교 대학원

< 목 차 >

< 그림 목차 >

< 표 목차 >

ABSTRACT

Privacy Protection using RFID-based Extended EPC

Park Do-Joon

Advisor : Prof., Lee Joon, Ph. D.

Department of Computer Engineering

Graduate School of Chosun University

Radio frequency identification (RFID) is expected to become an important and ubiquitous infrastructure technology. As RFID tags are affixed to everyday items, they may be used to support various useful services. However, widespread deployment of RFID tags may create new threats to user privacy, due to the powerful tracking capability of the tags. There are several important technical points when constructing an RFID scheme. Particularly important is ensuring forward security, data transmitted today will still be secure even if secret tag information is revealed by tampering in the future.

Low cost implementation is another key RFID requirement.

This paper discusses and clarifies the requirements and restrictions of RFID systems. This paper also examines the features and issues pertinent to several existing RFID schemes. Finally, this paper suggests the use of our previously proposed scheme, which protects user privacy using alow-cost one-way hash mechanism.

Ⅰ. 서 론

최근 객체에 RFID(Radio Frequency IDentification)[1]를 부착하여 객체의 정보를 확인하며 주변 상황을 감지하는 RFID 시스템이 미래 IT 시장을 선도할 기술 중 하나로 주목 받고 있다. 이로 인하여 미래의 유비쿼터스 컴퓨팅(Ubiquitous Computing Environment)[2] 환경에서 RFID는 개인의 일상생활 뿐 아니라 기업과 정부의 역할 그리고 사회문화적인 패러다임에도 급격한 변화를 유발하여 새로운 방식의 삶을 창출할 것으로 전망된다. 그런데 RFID가 초래하는 변화는 우리 사회, 기업 및 개인에게 다양한 기회가 되기도 하지만 무분별한 사용으로 인해 야기되는 프라이버시 문제[3] 또한 유비쿼터스의 전통적인 정보 보호 문제들을 뛰어 넘는 새로운 차원의 위협이 될 수도 있다. 특히 RFID는 원천적으로 정보 유출 및 위치 추적 문제[4]가 있다는 점에서 이러한 문제들에 대한 적절한 대책이 강구되지 않는다면 향후 RFID의 확산 및 유비쿼터스 사회로의 진입은 쉽지 않을 것으로 예상된다.

RFID 사용자 프라이버시 보호를 위해서는 세 가지의 기술적인 필수 보안 요건인 기밀성과 불구분성 그리고 전방향 안정성이 있다. 현재 프라이버시 침해 문제를 해결하기 위한 보호 기법으로 몇 가지가 있다. 그러나 이러한 기법들은 보안상 여러 가지 문제점을 가지고 있다.

본 논문에서는 기존의 기법들이 가지고 있는 문제점들을 분석한 후, 일방향 해쉬 함수를 이용하여 세 가지의 필수 보안 요건을 만족하는 RFID 프라이버시 보호 기법에 대하여 연구하고자 한다. 이 기법은 태그 내에 각각 서로 다른 두 개의 해쉬 함수 G 와 H 를 포함하고 있으며, 태그는 초기의 비밀 값 S_i 를 가지고 있다고 가정한다. 리더와의 i 번째 통신에서 리더의 요청신호에 대한 응답으로 태그는 $a_i = G(s_i)$ 값을 리더에게 보내고 이전의 자신의 비밀 값 S_i 를 $s_{i+1} = H(s_i)$ 로 갱신한다.

리더에 대한 태그의 응답이 매번 다르기 때문에 기밀성과 불구분성을 만족하며 i 번째의 비밀 값이 노출 된다 하더라도 해쉬 함수의 일방향 성질로 인하여 i 번째 이전의 정보들이 보호되므로 전방향 안정성도 제공한다[5]. 또한 태그에서 산출되는 결과값 a_i 와 Back-End 서버의 정보를 Auto-ID[6]센터의 기존 EPC[7] 코드 확장을 통해 적용하여 Back-End 서버를 여러 개 분산 시킴으로써 a_i에 대한 Back-End 서버의 높은 해쉬 함수 계산량을 해결 하여 RFID 프라이버시 보호를 연구한다.

Ⅱ. RFID 시스템

2.1 RFID 개요

RFID 시스템은 RF(Radio Frequency)를 이용하며 리더, 태그로 불리는 트랜스폰더, 데이터를 가공할 수 있는 장비 또는 컴퓨터 등 세 가지 구성요소가 결합되어 기능을 발휘하도록 구성되어있다. 또한 태그는 다양한 모양이 가능하며 철제, 목제에 내장할 수 있고 전철이나 버스처럼 외장에 만들 수도 있다. 크기가 다양하며 최근에는 소형화 추세에 따라 플라스틱 카드의 내부나 사람의 피부조직에도 삽입이 가능하며 각종 제품에 내장시키기가 용이하다. RFID의 작동 원리는 태그가 고유한 정보를 담은 신호를 발생하며 이 신호를 안테나를 통해 컨트롤러가 이를 인식하고 분석하여 태그의 정보를 얻는 방식이다.

그림 2.1에서 RFID 태그는 전원 공급방식에 따라 액티브(active) 방식[8] 과 패시브(passive) 방식[9]으로 나눌 수 있으며, 대부분의 읽기전용 태그는 패시브 태그를 사용하며 32비트~128비트의 수정할 수 없는 정보가 내장 되어 있다. 인식거리도 주파수 사용영역 또는 전력 사용량에 따라 센티미터에서 수십 미터까지 매우 다양하게 존재하고 있다. 리더는 태그로부터 송신된 정보를 식별하는 장치로 트랜시버라고도 한다. 데이터베이스를 포함한 Back-End 서버는 태그의 정보를 저장하고 있으며 리더의 요청에 의하여 태그의 정보를 리더에게 전송하는 역할을 한다.

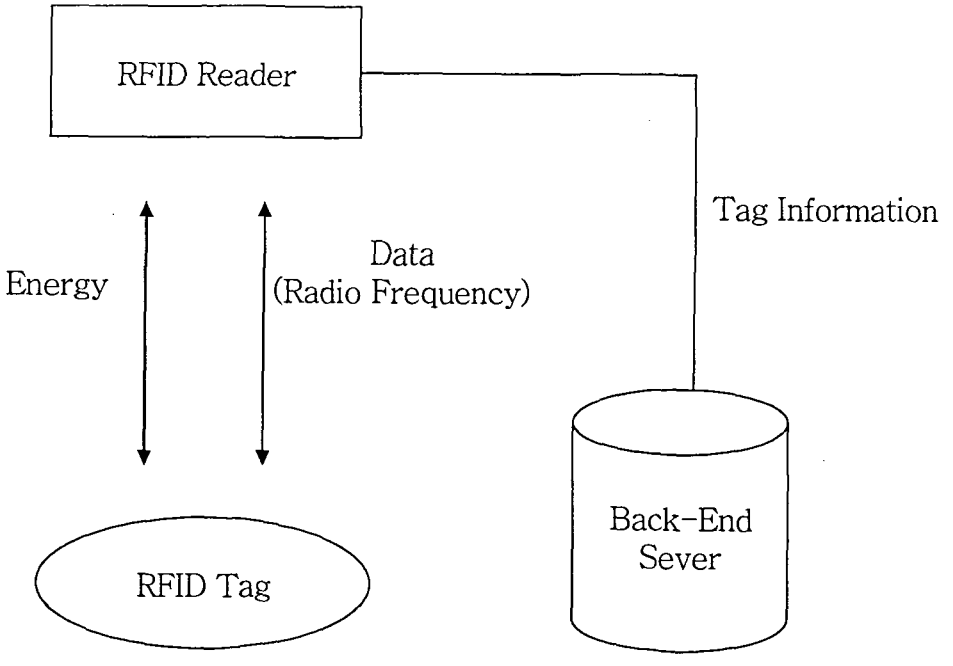


그림 2.1 RFID 시스템

표 2.1에서 카드모양의 기억 또는 기억 매체를 카드 기억 이라고 하는데 카드 기억은 자기 기록 기술을 사용한 자기 카드와 반도체 기술을 사용한 IC 카드, 광 기술 을 이용한 광 ID카드가 있다. 카드 기억은 현금 카드나 신용 카드와 같이 치수가 규격화되어 있으며 소유자 식별과 정보 기억, 정보 처리 등의 기능을 갖는다. ID 시스템은 기존의 자기 카드, 광 ID카드, 바코드 등의 ID 시스템, 전자 유도, 마이크로파 등을 이용한 RFID 시스템으로 구분한다.

RFID 시스템은 Savant[10], ONS(Object Naming Services)[11] 및 PML(Project Markup Language)[12]등이 포함되는 미들웨어 등으로 Back-End[13] 시스템을 구성하며 인터넷 망에 연동되어 응용 서비스를 제공한다. 수동형 태그를 사용하는 시스템에서는 리더가 태그로 전파를 송신하면 태그는 수신 전파로부터 전원을 얻어서 활성화한 후 자신의 ID 정보를 리더로 송신한다. 리더는 읽은 태그 ID 정보를 Savant 서버에 보내 ONS에서 객체정보가 있는 PML의 위치를 확인한 후 PML 서버로부터 객체의 구체적인 정보를 얻는다. RFID는 가상세계와 현실세계를 연결하는 링크로서 유비쿼터스 컴퓨팅 환경에서 필수적인 요소 기술로 모든 상품에 무선 태그를 부착할 수 있다면 다양한 용도로의 활용이 가능하다.

표 2.1 기억매체 종류

	바코드	자기 카드	IC 카드	RFID
인식 방법	비접촉식	접속식	접촉식	비접촉식
인식 거리	0~50cm	리더에 삽입	리더에 삽입	0~5m
인식 속도	4 초	4 초	1초	0.01~0.1초
인식율	95% 이하	99.9% 이상	99.9%	99.9%
투과력	불가능	불가능	불가능	가능(금속제외)
사용기간	-	1만번 이내(4년)	1만번(5년)	10만번(60년)
Data Write	불가능	가능	가능	가능
Card 손상율	매우 잦음	잦음	잦음	거의 없음
태그 가격	가장 저렴	저렴	높음($10이상)	보통($0.5~$1)
보안 능력	거의 없음	거의 없음	복제 불가	복제 불가
재활용	불가능	불가능	가능	가능

2.1.1 RFID 태그

다양한 객체에 부착되는 RFID 태그는 IC 칩과 안테나 및 전원 공급 장치로 구성되어 있으며 다양한 모양과 크기가 있다. 칩에는 객체의 유일한 식별코드나 정보를 적게는 64비트에서 많게는 8천 비트 정도까지 저장하며 리더의 요청에 의해 또는 상황에 따라 스스로 외부에 정보를 전송하거나 수신한다. 저가의 RFID 시스템 구현을 위해서는 이 태그를 얼마나 저렴하게 만들 수 있는가가 중요하기 때문에 태그는 하드웨어적으로 상당히 제한적일 수밖에 없으며 간단한 명령을 수행할 수 있을 정도이다. 또한 태그는 특징에 따라 세 가지로 분류한다.

첫째 전원의 공급 형태에 따른 RFID 태그의 구분은 표 2.2와 같다.

둘째 칩의 유무에 따라 분류하는데 칩이 없는 태그는 제조비용이 저렴하고 24비트 정도의 정보를 저장할 수 있다. 이 정도의 저장 능력은 상점, 창고 등 회사 내부 사용으로는 적합하나 대량 판매 시장에는 충분하지 않다. 리더가 모든 제조 항목을 식별하기 위해서 태그는 많은 객체를 식별하도록 설계된 매우 큰 ID 식별번호를 저장할 수 있을 만한 저장 공간을 가지고 있어야하며 자신의 범위 및 인접해 있는 다수의 태그를 읽을 수 있어야 한다. 칩이 있는 태그 시스템은 일련번호 혹은 제품 코드번호 등과 같은 데이터를 저장할 수 있으며 특정 어플리케이션을 이용하여 데이터를 처리해주는 리더에게 데이터를 전달할 수 있다. 일반적으로 96비트의 데이터를 저장 할 수 있으며 제조자 이름, 제품 이름, 제품에 할당될 수 있는 유일한 식별 번호 등이 포함 된다.

표 2.2 전원 공급 방식에 따른 RFID 태그의 구분

구분	Active	Passive
특징	-태그에서 자체 RF신호 송신 가능 -배터리에서 전원 공급	-리더의 신호를 변형 반사 -리더의 전파 신호로 전원 공급
장점	-장거리(3M)이상 전송가능 -센서와 결합 가능	-배터리 없으므로 저가격 구현가능 -배터리 교체 비용 없음
단점	-배터리에 의한 가격 상승 -동작시간 제한	-장거리 전송 제한 -센서의 모듈 추가 제한
적용분야	-환경 감시, 군수, 의료, 과학 분야	-물류 관리, 교통, 보안, 전자 상거래 분야

셋째 표 2.3과 같이 주파수범위에 따른 분류이다. 낮은 주파수는 짧은 범위를 갖고 있으나, 높은 인식율을 갖는다. 높은 주파수는 낮은 주파수에 비하여 넓은 범위를 갖으나, 인식율에서 객체나 지형 및 여러 가지 상황에 따른 요소에 의해 영향을 받는다.

RFID 태그는 이미 다양한 분야에서 사용되고 있으며 특히 유통, 물류 분야여서 정확한 재고 관리와 전체 SCM(Supply Chain Management)의 효율성 그리고 경쟁력을 극대화 시킬 수 있는 기술이다.

표 2.3 주파수별 RFID 구분 및 특성

주파수	저주파	고주파	극초단파		마이크로파
	125.134KHz	13.56KHz	433.92KHz	860~960KHz	2.45GHz
인식거리	60Cm미만	60Cm까지	50~100m	3.5~10m	1m이내
일반특성	● 고가 ● 성능저하 거의없음	● 저주파 보다 저가 ● 짧은거리, 다중인식	● 장거리 인식 ● 실시간 추적 ● 컨테이너 내부습도	● 가장저가 ● 태그성능 이뛰어남	● 900대역 태그유사 ● 환경영향 많이받음
동작방식	수동형	수동형	능동형	능동/수동형	능동/수동형
적용분야	● 공정 자동화 ● 출입통제 / 보안 ● 동물관리	● 수화물 관리 ● 대여물품 관리 ● 교통카드	● 컨테이너 관리 ● 실시간 위치추적	● 공급망 관리 ● 자동통행 료징수	● 위조방지
인식속도	저속 ~~ 고속				
환경영향	강인 ~~ 민감				
태그크기	대형 ~~ 소형				

2.1.2 RFID 리더

리더는 RF 신호의 발신 및 수신과 데이터 디코딩을 하는 부분을 포함하고 있으며 그 외에 호스트 컴퓨터와의 통신을 수행하기 위한 직렬 통신, USB, 이더넷 등으로 구성 된다.

RF전송 부분은 안테나 회로와 동조 회로, 변복조기를 포함하여 안테나 동조회로와 안테나가 최상의 성능을 발휘하기 위해서 적절하게 동조를 맞출 수 있도록 설계되어야 한다. 수신된 신호는 마이크로 컨트롤러를 통해 디코딩되어서 데이터를 얻을 수 있으며 마이크로 컨트롤러 내의 펌웨어 알고리즘은 RF신호를 발신하고 수신한 데이터를 분석하며 호스트 컴퓨터와 통신을 한다.

그림 2.2에서 리더와 태그는 여러 가지 디지털 방식의 부호화를 이용하여 기저대역의 데이터를 처리한다. 무선신호는 기본적으로 세 가지 디지털 변조방식[14] 즉 ASK (Amplitude Shift Keying), FSK (Frequency Shift Keying), PSK(Phase Shift Keying)를 이용하여 기저신호를 고주파 신호로 변환하여 전송한다. 그러나 특정 주파수 대역에서는 전자파의 인체영향이나 다른 통신시스템과의 간섭을 줄이기 위하여 특정 변조방식만을 사용하도록 요구 되며, 가장 많이 쓰이는 것이 주파수 확산(Spread Spectrum, SS)방식이다. 주파수 확산방식 중 CDMA 모바일 폰이나 무선랜에 이용되는 직접 시퀀스(Direct Sequence, DS)와 블루투스에 이용되는 FH(Frequency Hopping)등이 사용된다.

그러나 주파수확산 변조방식[15]을 태그에 적용하면 그만큼 복잡한 회로가 필요하여 가격이 상승하므로 실제는 리더만이 이러한 변조방식을 사용한다. 그리고 태그는 주파수확산의 전체 주파수를 커버하도록 광대역으로 만들며 ASK 등을 이용하여 신호를 전송한다.

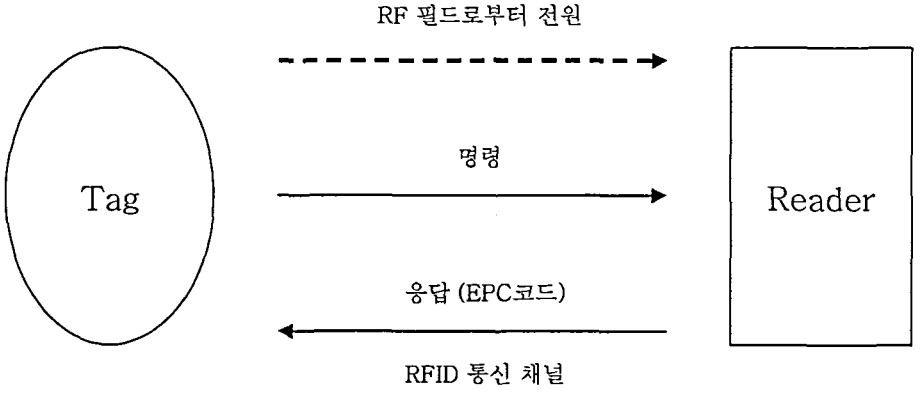


그림 2.2 RFID 태그와 리더의 상호 작동 원리

또한 데이터 정보의 신뢰성을 높이기 위해 여러 신호 처리가 수행되는데, CRC(Cyclic Redundancy Check)등의 방법을 사용하는 에러율 감소 방법, 여러 개의 태그를 구별하기 위하여 무선랜 등에서 사용되는 Aloha나 CSMA(Carrier Sense Multiple Access)와 비슷한 방식을 사용하는 충돌 방지 방법, 데이터의 보호를 위하여 대칭 또는 비대칭 암호 알고리즘을 사용하는 데이터 보안 방법 등이 적용된다.

리더는 휴대 가능한 터미널일 수 있으며 요금 정산소와 같은 입구에 설치되어 있는 고정된 디바이스일 수 있다. 또한 회사나 공장, 상점 등에 설치하기 위해서는 많은 리더들이 필요하고 이들은 보통 하나의 RF로 작동된다. 그러나 서로 다른 제조업자들이 만든 태그가 각각 다른 주파수를 사용한다면 유통업자는 필요한 위치마다 다양한 리더가 필요할 것이다. 즉 RFID 프로토콜에 대한 표준이 통일되지 않아 여러 가지 프로토콜이 사용되고 있으며 앞으로도 멀티 프로토콜이 요구된다. 또한 이러한 기능의 리더를 구현하기 위해 디지털 RF 및 SDR(Software Defined Radio)[16]기술이 적용되며 지능형 리더가 출현될 전망이다. 그리고 리더의 기술 응용은 현재 단순 인식 기능 적용 분야로부터 다량의 정보를 동시에 수집할 수 있는 분야로 확산됨에 따라 동시에 수백 개 이상의 태그를 인식할 수 있는 다양한 방식의 신호 전달 알고리즘이 개발될 전망이다.

2.2 RFID 시스템의 프라이버시

현재 사용되고 있는 RFID 태그는 일반적으로 태그마다 일정한 분류 체계를 가진 고유한 ID 값을 가지거나, 사용하는 업체에서 제품명, 제품번호, 회사명, 생산일자 등의 직접적인 식별 정보를 입력하기도 한다. 따라서 각 각의 태그는 항상 동일하며 고유한 값을 송신하게 되며, 태그의 정보를 읽어 내는 기능을 하는 RFID 리더가 적합한지를 판단하는 과정 없이 모든 RFID 리더에게 송신을 하게 된다. 다시 말해서, 현재의 RFID 태그는 각각의 고유한 값을 아무 리더에게나 송신한다는 것이다. 이러한 RFID 태그의 성질은 태그가 삽입된 물품을 가진 사람에 대한 프라이버시가 침해 문제를 발생시킨다. RFID 리더를 가진 사람이라면 누구나 태그의 정보를 읽어 낼 수 있기 때문에 태그가 삽입된 객체를 소유한 사람의 프라이버시가 침해당할 수 있다.

RFID 프라이버시 침해의 유형은 크게 두 가지로 분류할 수 있다.

첫 번째 유형은 RFID가 부착된 소유물의 정보가 유출 되는 경우로서, 태그의 직접적인 식별 정보나 고유한 ID가 리더를 가진 사람 모두에게 전송이 된다는 것을 의미한다. 예를 들면, 개인이 소지하고 있는 물품은 그 사람의 생활환경, 소득 수준, 소비 경향, 핸디캡, 신체조건 등을 반영하기 때문에 태그의 정보 유출로 인한 프라이버시 침해는 상당한 수준이라고 보아야한다. 태그에 직접적인 식별 정보가 들어있지 않고 고유한 ID가 들어있는 경우에도, 고유한 ID의 분류체계가 정해져 있기 때문에 분류체계에 대한 상세한 정보를 가지고 있는 공격자의 경우에도

비슷한 수준의 정보 획득이 가능하다. 1~2년 정도 후에는 거의 모든 물품에 RFID 태그가 삽입되는 환경이 올 것으로 예상되는 현 시점에서, 태그로 인한 정보 유출과 프라이버시 침해는 큰 문제로 고려되어야 한다. 리더를 가지고 있는 사람이라면 다른 사람이 모르는 사이에 태그를 읽어서 그 사람의 신상 정보를 파악할 수 있게 되기 때문이다. 그리고 프라이버시를 침해하는 수준을 넘어서 범죄에 이용될 가능성도 크다. 태그에 의해 정보 유출이 되면 고소득자 또는 고가 물품 소지자에 대한 식별이 가능하므로 길거리를 지나가는 사람을 목표로 하는 범죄가 늘어날 가능성이 있다. 리더 기능이 수년 내에 휴대폰에도 포함될 것이라는 점에서 심각성은 더 커질 수 있다.

둘째는 동일한 태그의 ID 값으로 인하여 리더를 가진 공격자는 특정 태그의 소유자 위치를 추적할 수 있다. 이것은 싼 가격의 위치 추적 장치를 그 사람에게 달아 놓은 것과 같은 것이다. 예를 들면 리더를 가진 공격자는 수 미터에서 수십 미터 거리를 유지하며 특정 태그의 소유자를 추적해 갈 수 있다. 공격에 가담하는 사람이 여러 명인 경우이거나 다수의 위치에 리더를 설치한 경우에는 추적이 더욱 용이해질 수 있다. 위치 추적은 심각한 프라이버시 침해로 볼 수 있다. 위치 추적을 당하는 경우 태그의 소유자가 위치하는 곳이 공개적으로 밝히기 싫어하는 개인에게 민감할 수 있기 때문에 정보 유출의 문제보다도 오히려 더 심각한 문제로 인식해야 한다.

2.3 RFID 프라이버시 보호를 위한 필수 보안 요건

RFID 시스템에서 프라이버시 보호를 위한 필수 보안 요건을 정의하고자 한다. 정보 유출 문제와 위치 추적 문제를 해결하기 위해서 정의되는 세 가지 필수 보안 요건을 반드시 갖추어야만 한다.

2.3.1 기밀성

기밀성(Confidentiality)이란 정보가 비밀리에 전송되어야 하는 보안 요건이다. 비밀리에 전송하기 위해서 사용되는 방법의 첫 번째는 전용 선로를 이용한 통신이다. 통신 당사자들만 사용할 수 있는 안전한 채널을 이용하는 것이나 사실상 어려운 문제이다. 대부분 인터넷 망이나 공중전화망(PSTN) 또는 무선 통신으로 정보를 전달하는 것이 더 일반적인 경우이다 이런 경우에는 전송되는 정보를 암호 알고리즘을 사용해서 암호화하는 방법을 사용하게 된다.

태그와 리더간의 통신을 살펴보면, 무선을 이용하는 통신이기 때문에 도청의 가능성이 열려 있다. 특히 리더에서 태그로 보내지는 정보는 수십 미터 에서도 도청이 가능하다. 반면에 태그에서 리더로 전송되는 정보는 수 미터 내에서만 도청이 가능하다. 리더에서 태그로 보내는 정보를 획득할 수 있는 거리를 전방 채널이라 하고, 태그에서 리더로 보내지는 정보를 획득할 수 있는 거리를 후방 채널 이라고 한다. 즉 전방 채널 범위 안에

있는 경우는 리더가 태그에게 전송하는 정보를 모두 도청할 수 있다는 의미이며 후방 채널 범위 안에 있으면 리더에서 태그로 전송되는 정보는 물론 태그에서 리더로 전송되는 정보를 도청할 수 있다는 의미이다. RFID 시스템에서의 프라이버시 보호를 위한 기법들 중에서 전방 채널은 보안상 중요하지 않은 정보를 전송하며 후방 채널을 이용해서 보안상 중요한 정보를 전송하는 기법도 존재한다. 그러나 고성능의 리더를 가지고 있는 경우에 후방 채널의 내용도 도청이 가능하기 때문에 후방 채널을 이용한 비밀 정보의 전송을 안전하다고 할 수 없다. 또한 후방 채널을 이용하는 보안 기법은 적합하지 않은 리더가 태그와 정상적인 통신을 할 때에 문제의 발생이 높다. 도청이 아니라 태그와 직접 통신을 하는 경우 태그가 중요한 정보 인증 과정이나 암호화 처리 없이 전송한다면 공격자는 쉽게 태그에 대해서 식별하거나 태그가 삽입된 물품을 가진 사람의 프라이버시 정보를 획득한다.

현재 사용되고 있는 RFID 태그는 삽입된 객체의 정확한 정보가 들어 있는 경우도 있고 단지 서버에서 식별 정보를 찾을 수 있도록 ID가 들어 있는 경우도 있다. 전자의 경우는 기밀성의 상당한 문제가 생길 수 있으며 후자의 경우는 적법하지 않은 리더나 도청자의에게 직접적인 정보는 줄 수 없지만, 사전에 다수의 태그 ID에 대한 정보를 축적한 상태라면 직접적인 식별 정보를 얻은 경우만큼이나 기밀성에 문제가 있다고 할 수 있다.

결국 기밀성을 보장하기 위해서는 태그가 식별 정보를 리더에게 줄 때에 리더가 적합한지 확인하는 인증 프로토콜을 거치는 방법을 사용하던지, 적합한 리더만이 알 수 있도록 암호화해서 전송하는 방법을 사용해야 한다.

2.3.2 불구분성

불구분성(Indistinguishability)이란 태그가 리더에게 정보를 송신할 때, 매번 동일한 값을 주지 않아야 한다는 보안 요건이다. 자세하게 설명하면, 태그는 리더가 정보를 요구할 때마다 다른 정보를 전송해 주어야 하며 이 정보는 리더 측에서는 예측이 불가능해야 한다. 또한 실제 난수(random number)와는 구분이 불가능해야 한다. 이 불구분성을 만족하는 경우에는 여러 태그 중에서 하나의 특정한 태그를 구분해내는 것이 불가능하며 계속적인 정보 요구를 통한 특정 태그의 추적이 불가능하다. 불구분성은 태그 소유자의 위치 정보에 대한 프라이버시를 보호하기 위해서 중요한 보안 요건이다.

결국 불구분성을 보장하기 위해서는 태그가 항상 동일한 정보를 송신해서는 안되며, 태그 내부에서 난수 생성에 준하는 작업을 한 후 결과 값을 전송하거나 태그 외부에서 적법한 리더가 자주 갱신해 준 값을 전송해야 한다. 전자의 경우에 태그 내부에 난수 생성기에 준하는 모듈 구현 가능해야 하며 리더와 Back-End 서버에서는 태그에서 송신하는 값을 가지고서 정상적인 식별이 가능해야 한다.

후자의 경우에는 쉽게 구현은 가능할 수 있겠지만, 적법한 리더가 태그의 정보를 갱신할 때 기밀성을 보장할 수 있느냐와 적법한 리더가 태그의 정보 갱신을 얼마나 자주 해 줄 수 있느냐가 중요한 문제로 인식된다. 그러므로 보안 측면에서는 전자의 경우가 더 높은 안정성을 가진다.

2.3.3 전방향 안정성

전방향 안정성(Forward Security)[17]은 키 분배(key distribution)에서 사용되며 키 분배 프로토콜에서는 장기간 사용되는 키가 있으며 이 키를 기반으로 현재의 세션에 사용될 세션 키(session key)를 만들어 내게 된다. 문제는 현재 시점에서 장기간 사용되는 키가 공격자에게 드러난 경우에라도, 이 키를 기반으로 과거 시점에 만들어진 모든 세션키를 계산해 낼 수 있어서는 안된다. 이처럼 장기간 사용되는 키가 노출 이 된 경우에 이전의 세션키를 계산할 수 없는 경우 전방향 안정성이 보장된다고 한다.

RFID 시스템에서의 전방향 안전성의 의미는 태그가 현재 송신하는 정보를 알아내거나 태그 내부의 저장된 비밀 정보가 노출된 경우에라도 그 정보를 가지고서 과거의 송신 정보를 알아낼 수 없도록 해야 한다는 보안 요건이다. 태그의 현재 정보를 이용해서 과거 송신 정보를 알아낼 수 있다면 태그 소유자의 과거의 위치를 파악할 수 있으므로, 역시 프라이버시 침해가

발생할 수 있다. 예를 들어 공격자가 다수의 리더를 지역 곳곳에 설치해 놓은 채로 일정 기간 동안의 모든 태그들의 정보를 수집해 왔다고 가정하면, 현재의 태그 정보를 획득한 상태에서 과거의 송신 정보를 계산하여 정보를 검색하게 되면 그 태그 소유자의 과거 위치 정보와 시점까지도 모두 파악할 수 있게 된다. 이러한 공격은 다수의 리더 설치와 대량의 정보 데이터베이스 구축이 필요하기 때문에 공격자보다는 정부기관이나 전문 업체에서 시도될 수 있는 프라이버시 침해 공격이다.

태그의 현재 송신 정보를 가지고 과거 송신 정보를 알아낼 수 없게 하기 위해서는 단순히 불구분성만 보장 되면 된다. 그러나 태그는 물리적인 공격으로 인해 내부의 정보가 드러날 수 있기 때문에, 물리적인 공격을 통해서 태그 내부에 있는 현재의 비밀 정보가 드러났을 경우에 대해서도 전방향 안정성이 보장되어야 한다.

2.4 RFID 표준화 동향

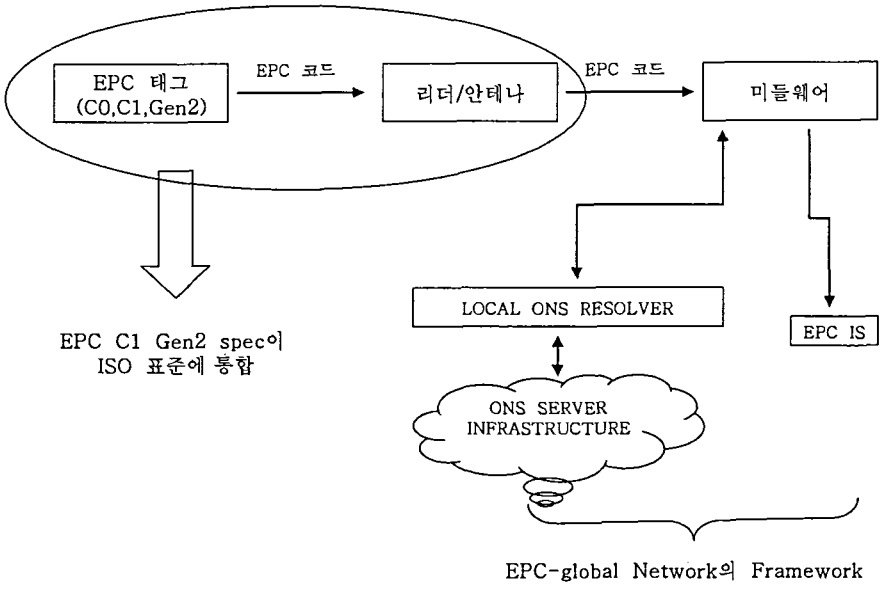


그림 2.3 EPC 시스템과 각 기술영역

RFID 표준화 기구인 Auto-ID 센터와 유비쿼터스 ID 센터는 RFID 표준화 기구의 두 지류를 이룬다. Auto-ID는 EPCglobal로 명칭을 변경하고 결국 GS1(Global Standard Number 1)의 코드 표준 기준은 EPC 체계가 될 것으로 전망했다. EPCglobal은 상품 하나하나에 EPC라는 고유 식별자를 붙여 그 상품에 관한 생산정보나 유통이력 등을 인터넷으로 알 수 있도록 하는 인프라 기술의 표준화를 수행하고 있다. 또한 EPC를 넣은 RFID 태그 기술과 상품에 관한 정보획득 절차를 표준화하여 글로벌 차원의 유통물류 시스템 구축을 목표로 하고 있다. 현재 미국에서는 월마트, 국방성 등이 EPCglobal 회원으로서 EPC 코드를 사용하는 것으로 표명하고 있다. 그림 2.3 EPCglobal에서는 RFID 시스템의 리더 태그 간 통신주파수로서 Class0과 Class1 태그에 대해서는 UHF 대역의 Class 1 Generation2가 Class 0/1을 통합하여 EPCglobal의 RFID Air Interface 표준으로 정착될 전망이다.

EPCglobal은 코드체계 미들웨어의 기술규격1.1을 발표했는데 그 구성요소로서 EPC, Savant, ONS, PML등이 있다. 이들은 Back-End 시스템을 구축하여 리더에서 계속적으로 발생하는 코드 데이터를 수집, 제어, 관리하는 기능을 한다. 그림 2.4에서 Back-End 시스템의 모든 구성요소는 계층적으로 조직화되고 분산된 구조의 미들웨어 네트워크를 구성하여 서로 통신한다. 미들웨어는 다양한 형태의 리더 인터페이스, 다양한 코드 및 망 연동, 여러 가지 응용 플랫폼에 대해서도 상호 운용성을 보장할 수 있어야 한다.

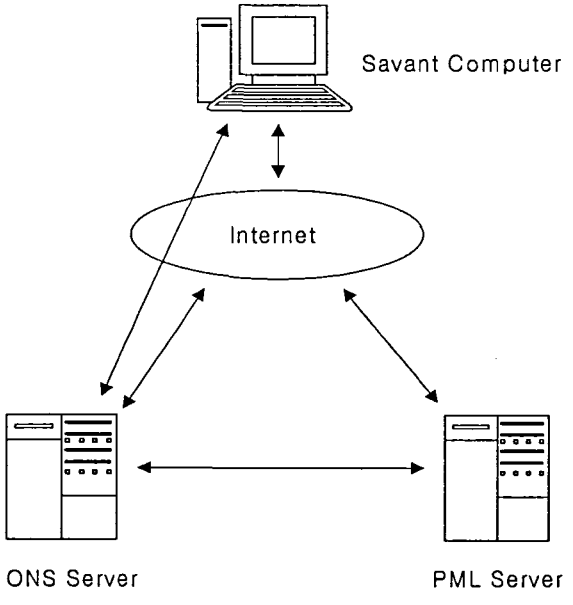


그림 2.4 Back-End 시스템

2.4.1 EPC

EPC는 차세대 바코드로 불리고 있지만 단순한 바코드를 훨씬 넘어서는 것으로 EPCglobal 센터가 개발한 방식이다. 또한 개별상품을 고유하게 식별할 수 있으며 모든 품목에 적용된다. 기존의 코딩 시스템처럼 종이 라벨에 인쇄하는 대신 무선 식별이 가능한 RFID 태그에 기록된다.

EPC는 일종의 인터넷 IP 주소와 비슷한 64 또는 128비트 길이의 아이디 숫자로 구성되어 있으며 각각 4개의 필드로 나뉘어져 있다. 그림 2.5에서 첫 번째 필드는 헤더(Header)이며 코드의 버전 넘버이다. 기존에 정의 되어 있던 다른 코드들과의 호환도 고려하고 있으며, 헤더를 통해 코드들을 구분한다. 또한 미래에 필요하게 될지 모르는 확장을 위해 고안 되었다. EPC 관리자라고 불리는 두 번째 필드는 28비트의 길이를 갖고 있으며 코드에 번호를 매기기 원하는 제품 생산자(vendor)의 정보를 식별해 주는데 대략 2억6천8백만 개의 상품제조업체를 식별가능하다. 상품 그룹은 객체 클래스라고 불리는 세 번째 필드에 의해 인식된다. 이미 존재하는 바코드 시스템의 확장인 마지막 필드는 각 상품을 구별 해주는 일련 번호로 이루어진 필드이다.

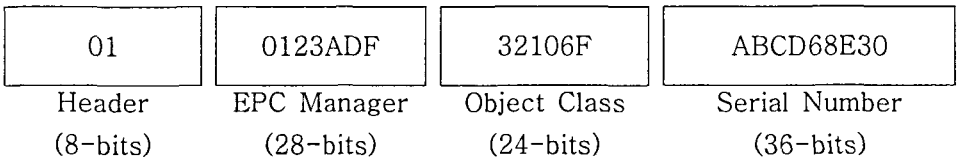


그림 2.5 EPC 코드

2.4.2 Savant

Savant는 서버에 설치되어 있는 공개구조의 소프트웨어로서 현장에서 RFID 태그를 판독하고 각종 객체 정보를 통합하고 제어하는 기능을 제공한다. 즉 Savant는 리더 인터페이스를 통하여 리더와 교신하며 응용프로그램과는 애플리케이션 인터페이스를 통하여 교신한다. 뿐만 아니라 여러 가지 다른 인터페이스를 통하여 다양한 서비스와도 호환될 수 있으며 그 기능을 요약하면 다음과 같이 세 가지로 기술된다. 첫째는 RFID 이벤트 취합 기능이며 둘째는 제어장치 기능 그리고 셋째로는 정보 네트워크 게이트웨이, Savant 내부 애플리케이션, 외부 EPC 네트워크를 연결하는 매개체 역할을 담당한다.

EMS(Event Management System)는 수집된 데이터를 용도에 맞게 분류하고 해당된 일을 처리하는 곳에 배치하는 역할을 수행하며 TMS(Task Management System)는 실제 일을 처리하며 기존의 시스템과 연동하는 역할을 수행한다. 또한 RIED는 실시간으로 발생되는 EPC 데이터를 수집하며 실시간 정보 데이터베이스를 말한다.

2.4.3 ONS

ONS는 디렉토리 역할을 하며, EPC를 인터넷상의 URL로 변환시켜 IP 주소를 찾을 수 있게 하는 역할을 담당 한다.그림 2.6에서 RFID 리더는 Savant에게 EPC 코드로 전달하고 Savant는 ONS 서버에게 EPC 코드로 수행하면 ONS 서버는 IP 주소로 전환하여 Savant에게 전송 된다.

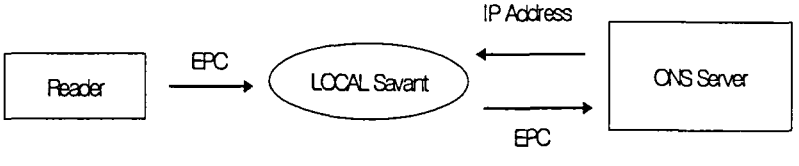


그림 2.6 ONS 개념

2.4.4 PML

PML은 사람과 컴퓨터가 이해할 수 있도록 EPCglobal 센터가 개발한 XML 기반의 언어로서 객체, 시스템 그리고 객체와 관련된 환경을 기술한다. PML의 기능은 RFID 리더에 의해 제품에 대한 정보와 제품에 관련된 기타 정보 등을 Savant를 통해 읽혀 들인 후 PML 서버에서 XML형태로 저장하는 역할을 담당한다. PML의 주된 목적은 RFID 기술이 적용된 물품에 대한 정보를 표준 공통언어로 제공하며 여러 가지 업무와 응용 시스템 등에 이용할 수 있도록 한다. 그리고 PML은 재고 관리, 자동 거래, 공급체인 추적 및 기계 제어 등이 포함된다.

2.4.5 EPC-IS

그림 2.7에서 EPC-IS[18]는 객체 정보를 관리하며 정보제공 요구가 있을 때 PML로 표시하여 제공하는 컴퓨터 시스템이며 높은 수준의 쿼리에도 응답을 제공 한다.

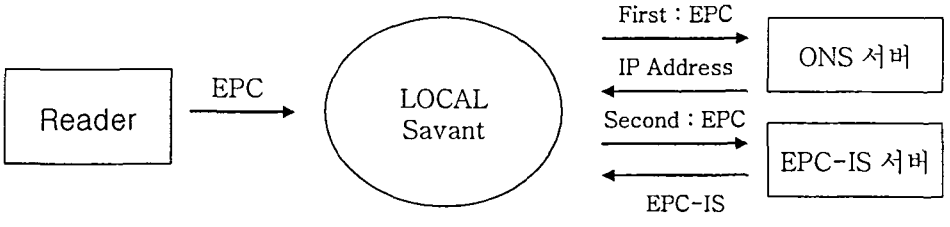


그림 2.7 EPC-IS 개념

Ⅲ. RFID 기반 사용자 프라이버시 보호기법

본 장에서는 RFID 프라이버시 보호를 위한 기존 인증기법들에 대해 알아본다. 기존에 제안된 기법들에는 대표적으로 Kill Tag 기법[19], 재 암호화 기법[20], XOR 기반 일회용 패드 기법[21], 해쉬-락 기법[22], 해쉬-기반 ID변형 기법[23] 등이 있다.

3.1 Kill Tag 기법

EPCglobal 센터에서 제시한 방법으로 Kill 명령어 접근법에서 각 태그가 8비트의 고유한 패스워드를 포함하며 태그가 이 패스워드와 'Kill'명령을 받을 경우 태그가 비활성화 되는 방식이다. 태그는 내부에 단락 회로가 있기 때문에 이를 끊음으로서 'Kill' 명령을 실행하게 되는데 이렇게 때문에 한번 죽은 태그는 다시 살릴 수 있는 방법이 없다. 이런 경우 태그를 재사용할 필요가 있는 분야에서는 사용이 불가능하다. 아주 간단한 예로써 반품이 가능한 물건에 붙어있는 태그의 경우 이런 'Kill' Tag 명령 방식을 사용할 수 없다. 물론 Read/Write로 설계된 태그의 경우 플래그 비트를 이용하여 태그를 죽였다 다시 살릴 수도 있다. 하지만, 이 경우 또한 여전히 태그에 사용하는 8-bit 암호에 대한 문제가 남는다. 만약 악용하려는 자는 대략 2^8 정도의 계산으로 패스워드를 알아내어 명령어를 남용할 수 있다.

따라서 수많은 제품에 사용될 태그라는 것을 감안하고 보안을 생각한다면 128bit 이상을 암호로 사용해야 하지만 이는 태그에 상당한 부담이 된다. 또한 태그마다 다른 암호를 사용한다면 이를 저장하는 것도 문제이다. 이 방법은 EPCglobal의 EPC Class1 태그에 내장된다.

3.2 재 암호화 기법

재 암호화(Re-Encryption) 기법은 사용자의 프라이버시를 보장하기위해 RFID 시스템에 공개키[24] 암호 인증 방법을 사용한다. 이는 은행 어음에 이용 가능한 RFID 인증 기법으로 은행 어음 태그 식별 번호를 공개키로 암호화하여 태그에 저장한다. 태그에 저장되는 정보는 외부 유닛으로부터 전달된 데이터를 사용자가 사용을 요청할 때 재 기록 한다. 이 외부 유닛은 공개키 암호로 재 암호화를 하는데 있어서 아주 필수적이다. 그 이유는 많은 연산량을 요구하기 때문에 태그만으로는 연산 처리가 어려워 작업은 대체로 리더에 의해서 수행된다. 태그의 결과 값은 각각 재기록 주기 안에 랜덤하게 보이므로 태그의 결과 값을 도청하는 공격자는 긴 시간 주기 동안 태그를 추적할 수 없다. 즉 기밀성이 보장된다. 그러나 이 기법은 공개키 암호화에 따르는 비용이 많이 든다. 특히 RFID 태그가 공개키 암호학적 연산을 수행하는 것이 불가능하며, 리더가 태그의 정보 갱신 문제는 불구분성을 보장하지 못한다.

3.3 XOR 기반 일회용 패드기법

Ari Juels가 제안한 XOR 기반 일회용 패드(One-Time Pad) 기법은 단지 XOR 연산만을 요구하므로, 매우 저렴한 비용을 요구한다. 이 기법에서는 그림 3.1과 같이 리더와 태그가 랜덤 키(Random Key)의 공통 리스트를 공유하고 있으며 여러 번의 통신을 통해 상대방이 동일 목록의 키를 가지고 있음을 확인하여 상호 인증한 후 태그는 ID를 전송한다. 인증 과정 후 일회용 패드는 랜덤 값에 의해 갱신된다. RFID에 XOR 연산을 적용하여 상호 인증을 수행하면서도 태그의 ID가 매번 업데이트되는 형태의 기법으로 실제 적용가능하다. 그러나 다음과 같은 문제점을 가지고 있다.

- 리더와 데이터베이스를 분리하여 생각하지 않아 비현실적이다.
- 태그와 리더 사이의 통신 양이 많다.
- 안전성을 위해서는 공통 목록이 새롭게 재 기록될 필요성이 있다.
- 모든 인증 세션을 도청하는 경우 비밀 정보가 모두 들어난다.

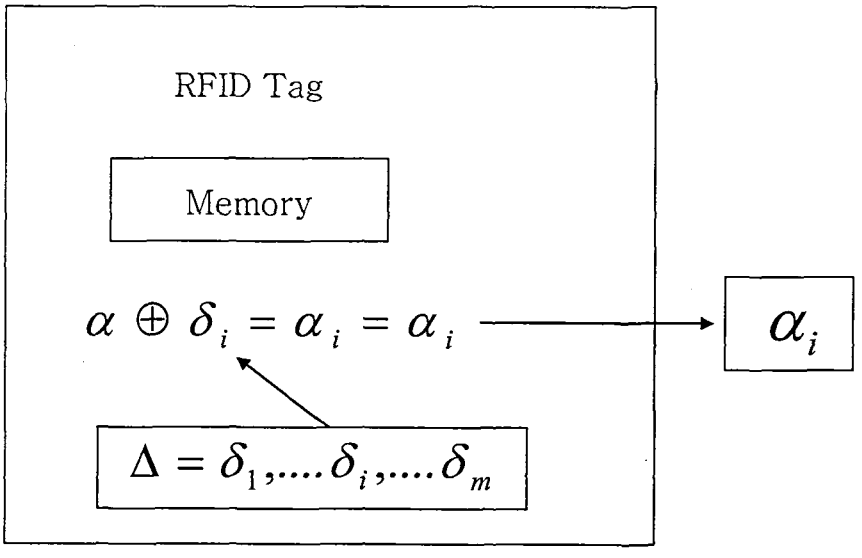


그림 3.1 XOR 기반 일회용 패드 기법

3.4 해쉬-락 기법

Weis가 제안한 해쉬-락(Hash-Lock) 기법의 태그는 수동적이며 오직 읽기 함수를 갖는 몇 백 비트의 메모리를 갖는다. 표 3.1 은 해쉬-락 기법[25] 구성 요소 및 연산 도구 이다. *ID*는 태그의 실질적인 데이터이며 *key*는 랜덤 값이다, 그리고 *metaID*는 키의 해쉬 값, ($= h(key)$)이며, $h()$는 일방향 해쉬 함수를 나타낸다.

표 3.1 해쉬-락 기법 구성 요소 및 연산도구

	필요한 메모리	연산도구
Tag	*metaID, ID*	$h()$
Reader	-	-
Database	*metaID, key, ID*	-

- *ID*: 태그의 실질적인 데이터
- *key*: 랜덤 값
- *metaID*: *key*의 해쉬 값(= ($= h(key)$))
- $h()$: 일방향 해쉬 함수

해쉬-락 기법에서 연산도구로 해쉬 함수를 갖는 태그는 소유자에 의해 자신의 실질적인 데이터 *ID*를 비롯하여 인증과정에서 필요한 일시적인 *metaID* 값을 저장한다. 이때, *metaID*는 랜덤하게 선택된 *key* 의 해쉬값 ($metaID = h(key)$)이다. 이러한 과정을 잠금(Lock) 과정이라 한다.

잠금 과정 후에 태그의 소유자는 *key* 와 *metaID* 를 데이터베이스에 저장 한다. 이는 보안을 위해서 RF 채널이나 물리적인 접촉으로 안전하게 이루어진다. 그림 3.2에서 해쉬-락 기법 인증 과정은 잠금 상태와 열림(Unlock) 상태로 나누어진다. 첫 번째로 태그가 잠금 과정을 거쳐 잠겨 있는 상태에서 태그는 모든 리더의 질의에 *metaID*를 보냄으로써 응답하고 태그가 열림 상태가 될 때까지 다른 함수는 하지 않는다. 그러나 태그는 리더가 보내온 정보인 *key*를 받고 이를 해쉬 해보고 그것이 자신이 가지고 있는 *metaID*와 같다면 그 정보가 타당하다 판단하고 상태가 열림으로 바뀌면서 *ID*를 전송한다. 이때, 열림 상태는 공격자가 *ID*를 도청하는 것을 예방하기 위해서 아주 짧은 순간에 이루어지며 다시 잠금 상태로 돌아간다. 이러한 잠금 기능으로 태그의 사용자 프라이버시는 보장된다.

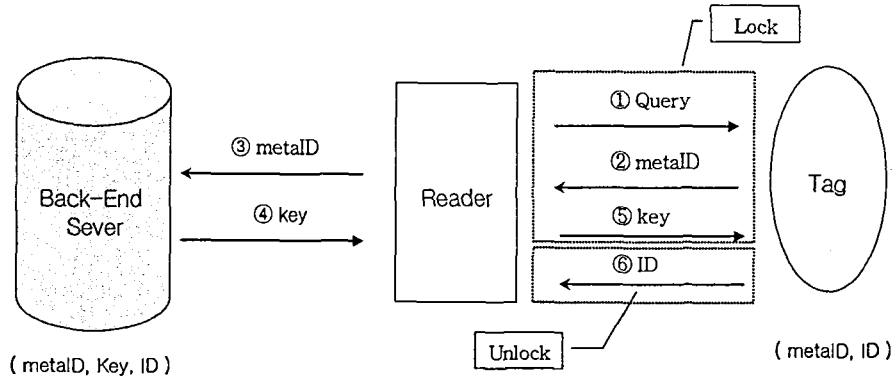

Lock
Back-End
Sever
③ metaID
④ key
Reader
① Query
② metaID
⑤ key
⑥ ID
Tag
Unlock
(metaID, Key, ID)
(metaID, ID)

그림 3.2 해쉬-락 기법

해쉬-락 기법은 태그에 단 한 번의 해쉬 연산이 필요하며 Back-End 서버의 데이터베이스가 안전하다고 가정하면 모든 태그의 *key* 를 관리한다. 해쉬-락 기법의 안전성은 일방향 해쉬 함수에 기반한다. 해쉬 함수의 특성상 *key* 를 모르는 사람이 *metaID* 로부터 *key* 를 알아내는것은 어렵기 때문에 임의의 공격자는 정당한 리더로 가장 할 수 없다.

이 기법은 태그안에 있는 식별 정보를 아무 리더에게나 주지 않고 Back-End 서버에 접근할 수 있는 인증된 리더에게만 주게 함으로써, 기밀성을 보장하는 기법이다. 그러나 공격자가 *metaID*값을 획득한 후, 자기가 태그인척 함으로써 적법한 리더를 통해 *key* 값을 얻어내는 스푸핑 공격이 가능하다. 또한, 잠금 상태에 있는 태그는 항상 *metaID* 값을 송신하기 때문에 불구분성을 만족하지 못한다. 결국 이 기법은 위치 추적을 당하는 문제를 해결하지 못한다.

3.5 해쉬-기반 ID 변형 기법

D.Henrici 의 해쉬-기반 ID 변형(Hash-based ID Variation) 기법의 구성 요소 및 연산 도구는 표 3.2와 같고 태그 안에 해쉬 함수가 들어 있는 것을 가정하며, 프로토콜 수행 중에 태그가 2번의 해쉬 연산을 하게 된다.

표 3.2 해쉬-기반 ID 변형 기법의 구성 요소 및 연산 도구

	필요한 메모리	연산도구
Tag	*ID, TID, LST*	$h()$,$\oplus$
Reader	-	-
Database	*HID, ID, TID, LST, AE, DATA*	$h()$, *R.N.G*

- *ID*: 인증을 위한 랜덤값으로 인증 성공 시 마다 변환
- *HID*: *ID*의 해쉬 값,($h(ID)$)
- *TID*: 현재 진행 중인 인증 세션 번호

  (초기에는 *LST* 와 같은 랜덤 값으로 초기화)
- *LST*: 마지막으로 성공한 인증 세션 번호

  (초기에는 *TID* 와 같은 랜덤 값으로 초기화)
- *AE*: 메모리 연결을 위해 연결된 데이터베이스 엔트리(entry)
- *DATA*: 사용자 정보, 태그 정보와 같은 실질적인 데이터

- $h()$: 일방향 해쉬 함수
- $R.N.G$: 랜덤 숫자 생성기
- $\oplus$: XOR 연산 (Exclusive-or function)

그림 3.3에서 인증 과정은 리더가 태그에게 질의를 보내면 태그는 현재의 ID 값을 해쉬한 값 $h(ID)$, 현재의 인증 세션 번호인 TID 값에 가장 최근에 성공한 인증 세션 번호 LST 를 뺀값 $\triangle TID$, 그리고 $h(TID \oplus ID)$를 리더에게 전송한다. 리더는 이 세 가지 값을 그대로 Back-End 서버에게 전송하게 되며 Back-end 서버는 데이터베이스에서 $h(ID)$ 값이 키 값으로 저장되어 있는 레코드를 찾아낸다. 다른 값과 레코드에 저장되어 값이 일치하는지 계산을 통해서 확인한 후, 임의의 난수 R 을 생성하여 레코드 값을 갱신하고 새로운 데이터베이스 키 값 $h(R \oplus ID)$ 를 가지는 새로운 레코드를 생성하여 함께 보관한다. 그 후 R값과 $h(R \oplus TID \oplus ID)$값을 함께 리더에게 보내고, 리더는 그 두 가지 값을 태그에게 전송하게 된다. 태그는 먼저 전달받은 R 값을 자신의 TID 값, ID 와 함께 XOR 연산을 해서 해쉬한 값이 건네받은 $h(R \oplus TID \oplus ID)$ 값과 같은지를 확인 하여 정상적이라면 자신의 ID를 $ID = TID \oplus ID$로 변경한다.

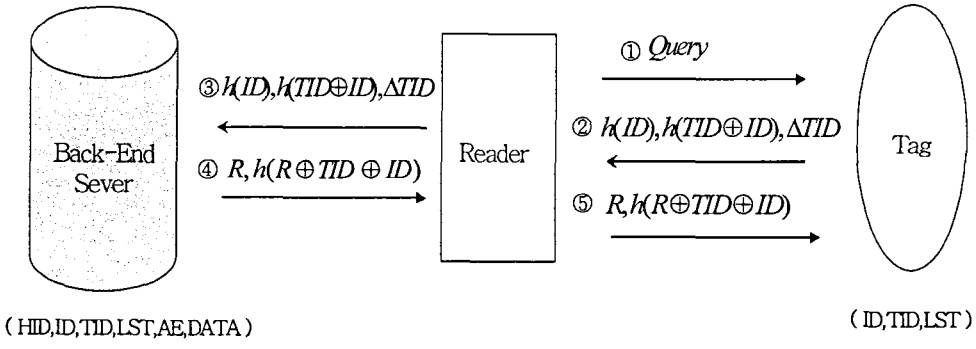


그림 3.3 해쉬-기반 ID 변형 기법

이 기법의 장점은 Back-End 서버에 계산량이 매우 가볍다는 것이다. 그러나 이 기법에서는 많은 보안 허점을 가지고 있으나 일단 기밀성은 보장이 된다. 그러나 불구분성은 몇 가지 관찰과 공격에 의해서 깨어질 수 있다. 첫째로 이 기법에서는 정상적인 절차를 마치지 않으면 계속 같은 $h(ID)$값을 송신하기 때문에 태그를 추적할 수 있다. 둘째로 $\triangle TID$값은 일정하게 증가하는 값이기 때문에 태그의 다음 응답 정보의 일부가 예측 가능하다. 셋째로 공격하는 리더가 계속해서 여러 번에 걸쳐서 태그에게 질의를 하게 되면 $\triangle TID$값이 많이 커져서 다른 태그와 구분이 가능하게 된다. 넷째로 정상적인 리더와 Back-End 서버간의 프로토콜 진행 중간에 공격자가 마지막 단계의 리더의 송신 값을 가로챈 후, 공격자 자신이 고의로 생성한 $R(=0)$값과 이를 이용해서 계산된 $h(R \oplus TID \oplus ID)$값을 태그에게 전송하면 태그는 정상적인 프로토콜로 이해하게 되며 ID를 변경하지만 R 값이 0 이기 때문에 원래의 ID를 유지하게 된다. 결국 서버가 가지고 있는 정보와 태그가 가지고 있는 정보가 일치하지 않는 문제가 발생해서 정상적인 인증 절차를 가질 수 없게 된다. 결국 이 공격 이후로는 태그의 송신 값 $h(ID)$는 항상 고정된 값이 되기 때문에 불구분성이 깨어지고 위치 추적이 더 쉬워진다. 또한 전방향 안정성을 보장 하지 못한다.

Ⅳ. 새로운 RFID 프라이버시 보호 기법 제안

RFID 프라이버시 보호를 위해서 기존 기법들의 문제점 들을 검토한 후 새로운 RFID 프라이버시 보호 기법을 제안한다. 프라이버시를 보호하기 위해서는 몇 가지 기술적인 문제들을 극복해야 한다. 그 중에 하나가 ID 익명화이다. 만약에 태그 ID가 익명으로 유지될 수 있다면, 사용자 소유물에 관련된 정보 유출 문제는 해결 될 것이다. 또 다른 문제는 악의적인 추적을 피하는 것이다. 만약 태그의 결과 값이 고정되어 있다면, 상대방(adversary)은 손쉽게 태그를 추적할 수 있으며, 사용자도 위치 또한 추적할 수 있다. 그러므로 태그의 결과 값은 고정적으로 남아있어서는 안 된다.

필수 보안 요건을 충족시키는 방법 중 하나는 공개키 알고리즘을 사용하는 것이다. 하지만, 공개키 기법은 상당한 계산 능력을 필요로 하는데 이는 일반적으로 태그 비용을 증가시킨다. 따라서 태그에 공개키 연산을 필요로 하는 기법은 실생활에 적용하기는 어렵다. 결과적으로 위의 2장에서 제시한 세 가지 요건들을 저비용으로 충족한다.

4.1 FSPP 기법

제안하는 FSPP(Forward Security Privacy Protection) 기법은 일방향성인 두 개의 해쉬 함수를 사용하여 RFID 프라이버시 침해 보호를 위한 필수 보안 요건 기밀성, 불구분성, 전방향 안전성을 만족한다.

4.1.1 일방향 해쉬 함수

일방향 해쉬 함수(One-way hash function)에 대해서 여기서 언급하는 이유는 제안 기법인 FSPP 기법에서 사용되는 중요한 개념이다. 그리고 RFID 태그에는 공개키 알고리즘과 같은 높은 수준의 암호화 모듈 보다 대칭키 알고리즘이나 해쉬 알고리즘을 포함시키는 것이 더 용이하다.

일반적으로 해쉬 함수는 $h:\{0,1\}^* \rightarrow \{0,1\}^{\ell}$ 의 성질을 가지는 함수이다. 다시 말해서 어떤 길이의 입력 값이 들어와도 출력 값(Hash Value)의 길이는 일정한 값 ℓ을 유지한다는 의미이다. 여기에 일방향성이 더해진 일방향 해시 함수는 입력 값이 주어지면 출력 값을 구하기는 매우 쉽지만, 반대로 출력 값이 주어졌을 때 그에 해당하는 입력 값을 구하기가 매우 어렵다. 일방향 해쉬 함수는 충돌 회피성(collision-free)을 가지고 있어서 같은 출력 값을 가지는 서로 다른 두개의 입력 값을 찾기에 매우 어려운 함수이다.

이러한 일방향 해쉬 함수를 위해서는 출력 값의 길이 ℓ을 적당히 크게 하는 것이 안전성 측면에서 매우 중요하며, 일반적으로 사용되는 길이는 128비트, 160비트, 192비트, 256비트 등이다. 대표적인 일방향 해쉬 함수는 MD2, MD4, MD5, SHA-1, SHA-2 등이 있으며, 대칭키 블록 암호화 알고리즘을 이용해서 일방향 해쉬 함수를 만들어 사용 한다

4.2.2 FSPP 구조 및 인증 과정

표 4.1 FSPP 기법 용어

m	태그 갯수
n	해쉬 값의 길이, 태그가 읽혀지는 횟수를 의미
ID	태그의 식별 정보
H	일방향 해쉬 함수
G	일방향 해쉬 함수. H 와는 서로 다른 분산
S_i	태그의 해쉬값 (비밀값)
t	태그

표 4.1에서 FSPP 기법의 용어를 정리하였고 태그 내부 구조는 그림 4.1과 같다.이 기법은 두 개의 일방향 해쉬 함수 H 와 G 를 가지고 있고 Back-End 서버는 태그 t 에 대한 각각의 식별 정보 ID 값과 임의로 생성한 비밀값 S_i 값을 데이터베이스에 저장하며 각 태그에는 비밀값 S_i 를 가지고 있다고 가정한다.

해쉬 값의 최대 길이 n 값은 정해져 있으며 t 의 범위는 $1 \leq t \leq m$이다. 리더가 질의 할 때마다 태그는 먼저 현재의 자신의 비밀값 S_i 를 해쉬 함수 G 에 입력함으로써 $a_i = G(s_i)$ 를 계산한 후, 이 a_i 를 리더에게 전송해 준다. 그런 다음 태그는 자신의 비밀 값을 스스로 갱신하기 위해서 해쉬 함수 H 를 이용해서 $s_{i+1} = H(s_i)$ 를 계산한다. a_i 값을 수신한 리더는 그 값을 Back-End 서버에게 보낸다.

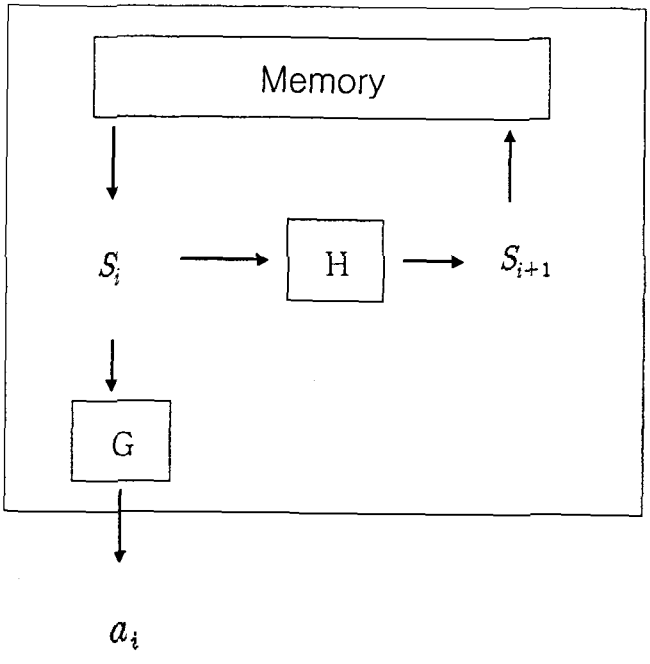


그림 4.1 FSPP 기법의 태그 내부 구조

그림 4.2에서 Back-End 서버는 모든 $1 \le t \le m$와 $1 \le i \le n$ 에 대해서 $a'_i = G(H^i(S_i))$를 계산하여 전송받은 a_i 와 일치하는 S_i 값을 찾아낸다. S_i 값을 찾으면 ID 를 곧바로 알 수 있고 Back-End 서버는 리더에게 식별정보 ID 를 전송해주고 프로토콜을 종료한다.

결국 Back-End 서버는 자신이 가지고 있는 모든 비밀 값을 계산식에 넣어서 특정 태그가 어떤 해쉬 라인에 속해 있는지를 알아낸다. 물론 그 모든 해쉬 라인들의 값을 다 저장하고 있는 방법을 생각할 수 있지만, 태그의 개수 m 이 어느 정도 이상 커지면 불가능 해진다. 이 기법은 따로 리더가 적합한지에 대해 인증 프로토콜을 수행하지 않고 현재의 비밀값 S_i 를 해쉬 함수 G 로 계산한 값을 리더에게 주기 때문에 프로토콜이 매우 단순해지며 외부로부터의 값 입력이 없기 때문에 프로토콜의 허점을 이용한 공격이 어렵다. 또한 외부에서 태그의 내부 정보 값을 갱신해주는 방식이 아니라 태그 스스로가 자신의 내부 정보를 갱신 하는 방식을 취하기 때문에 도청에 의한 공격으로부터 자유롭다. 따라서 기밀성과 불구분성을 모두 보장 한다.

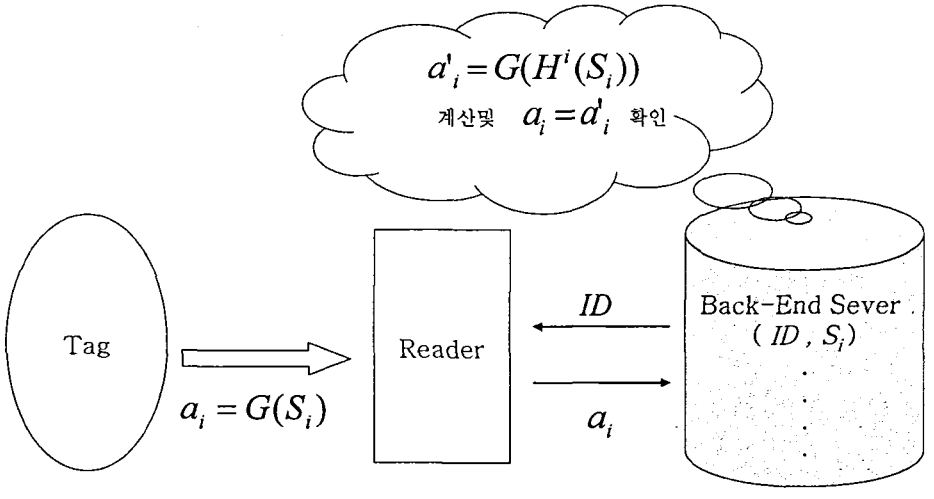


그림 4.2 FSPP 기법의 태그 인증 과정

또한 그림 4.3에서 태그 연산의 내부 정보 변경을 일방향 해쉬 함수를 가지고 계산을 수행하기 때문에 공격에 의해 내부 정보가 노출되는 경우에라도 일방향 해쉬 함수의 성질에 의해서 완벽한 전방향 안전성을 보장한다. 효율적인 측면에서도 FSPP 기법은 작은 게이트 사이즈를 필요로 하는 해쉬 함수 사용으로 낮은 가격의 RFID 태그를 만들 수 있다.

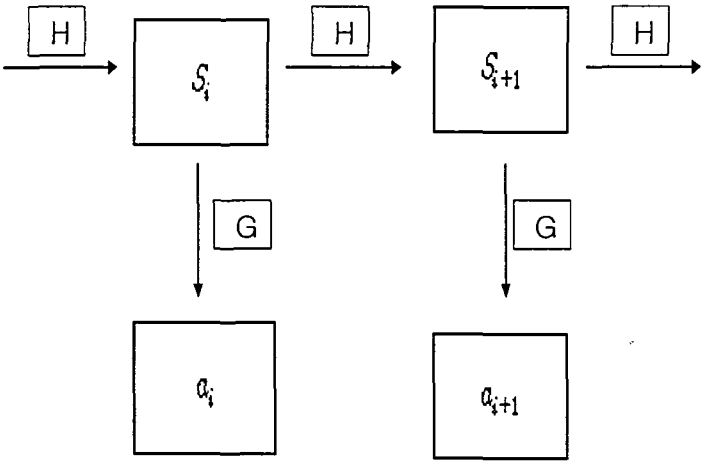


그림 4.3 FSPP 기법의 태그 연산

4.2 EPC 코드의 확장

본 논문에서 제안한 기법은 Back-End 서버의 데이터베이스가 모든 태그에 대한 정보를 가지고 있어야 하며 모든 해쉬 함수를 계산해야 하는 부담을 갖고 있다. 예를 들면 Back-End 서버에서는 하나의 태그를 식별하기 위한 계산에서, $1 \le t \le m$와 $1 \le i \le n$ 에대해서 $a'_i = G(H^i(S_i))$를 계산하는데, 이를 계산적 복잡도로 나타내면 $O(mn)$ 이 된다. 결국 태그의 개수 m 과 태그가 읽혀질 수 있는 횟수 n 에 비례해서 계산량이 늘어나게 된다. n 이 어느 정도 제한적인 범위를 가지는 값이기 때문에 상수항으로 간주한다 하더라도, 태그의 개수 m 에 비례해서 계산량이 늘어나는 것이다. 본 논문에서는 이 문제에 대한 해결 방법으로 기존의 EPCglobal 센터의 EPC 코드를 확장시킴으로써 Back-End 서버 정보를 확장된 EPC 코드 내에 포함시켜 여러 개의 Back-End 서버가 태그를 제어함으로써 계산량을 줄이는 효율적인 기법을 구축할 수 있도록 하였다.

그림 4.4에서 EPCglobal 센터의 EPC 코드에 제안한 기법을 적용했다. 예를 들면 관리자의 원래 영역은 제조업체 코드를 위한 것이다. 그러나 FSPP 기법에서는 이 영역이 Back-End 서버에 관련된 정보를 위해서 사용한다. 또한 객체 코드와 일련번호는 원래 태그 ID용이며 이 영역은 결과값 a_i를 포함한다.

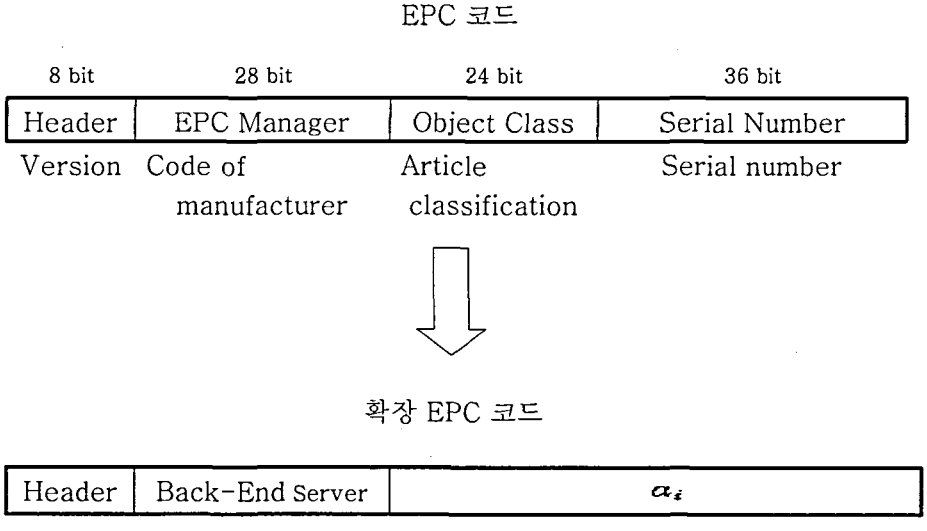


그림 4.4 EPC 코드와 확장 EPC 코드

그림 4.5와 같이 인증 과정을 통해 확장 EPC 코드를 분석할 수 있다.

1. 태그는 리더에게 Back-End 서버의 코드와 FSPP 기법의 태그 결과값 a_i를 포함 시킨 확장 EPC 코드를 전송 한다.
2. 리더는 Back-End 서버의 IP Adress 의 분석을 위하여 ONS 서버로 확장 EPC 코드를 전송한다.
3. ONS 서버는 확장 EPC 코드를 분석하여 다시 리더에 반응을 전송한다..
4. ONS 서버로부터 Back-End 서버의 IP Adress를 획득한 리더는 Back-End 서버에 확장 EPC 코드를 전송한다.
5. 전송받은 확장 EPC 코드를 Back-End 서버는 분석하고 데이터 베이스 내에 리스트로 유지되어 있는 원래의 EPC 코드와의 비교를 통해 일치하는 경우 ID를 리더에 전송한 후 인증 과정을 종료한다.

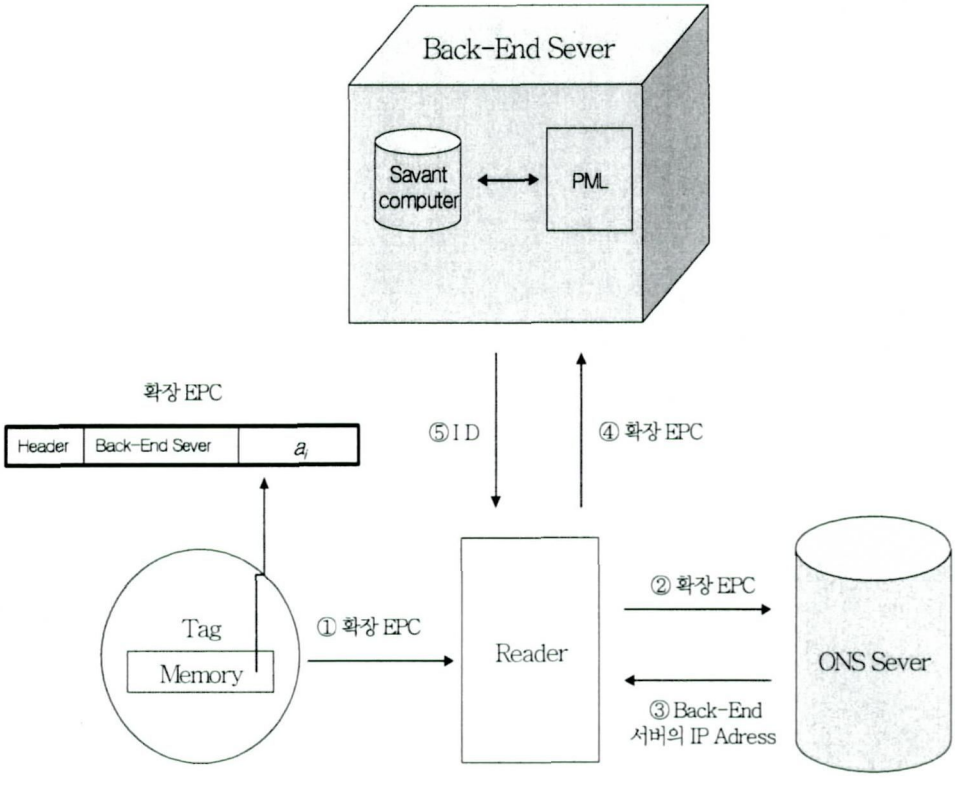


그림 4.5 확장 EPC를 이용한 프라이버시 보호

V. 비교 평가

표 5.1에서 RFID 프라이버시 침해 보호를 위한 기존 인증 기법들과 본 논문을 통해 제안한 FSPP 기법에 대해서 필수 보안 요건인 기밀성, 불구분성, 전방향 안정성 등의 보장 여부를 분석해 보았다.

표 5.1 프라이버시 보호를 위한 필수 보안 요건 비교

프라이버시 보호기법	기밀성	불구분성	전방향 안정성
Kill Tag 기법	X	X	X
재 암호화 기법	O	O	X
XOR 일회용 패드기법	X	O	O
해쉬-락 기법	O	X	X
해쉬 기반 ID 변형 기법	O	X	X
FSPP 기법	O	O	O

표 5.1과 같이 본 논문에서 제안한 FSPP 기법이 3가지 필수 보안 요건을 만족하는 결과를 보였다.

FSPP 기법의 효율성을 기존의 RFID 프라이버시 인증 기법들과 비교는 표 5.2와 같다. 제안 기법의 효율성을 기존의 기법들과 객관적으로 비교하기 위하여 태그 인증에 사용되는 비밀정보 ID, S_j, key 는 모두 j 비트로 가정하였으며 일방향 해쉬함수는 $H: 0,1^* \rightarrow 0,1^l$로 가정하였다.

표 5.2 기존 기법과 FSPP 기법의 효율성 비교

	메모리 (비트)		연산량(회)		
	태그	데이터 베이스	태그	리더	데이터 베이스
해쉬-락 기법	2j	4j	해쉬 함수:1	-	-
해쉬 기반 ID 변형 기법	·3j	8j	해쉬 함수:3	-	난수 생성:1 해쉬 함수:3
FSPP 기법	j	2j	해쉬 함수:2	-	해쉬 함수: (태그 ID의 수)*i

표 5.2와 같이 FSPP 기법은 해쉬 기반 ID 변형 기법이나 해쉬-락 기법에 비하여 태그와 데이터베이스의 메모리량이 적어서 저가의 태그를 구현할 수 있는 장점이 있으며 데이터베이스 구축비용을 낮출 수 있는 장점이 있다. 그러나 FSPP 기법의 데이터베이스 연산량은 기존 기법들에 비하여 태그 *ID* 수와 해쉬 값의 길이에 비례하여 Back-End 서버의 계산량이 많아지는 문제점이 있다. 때문에 본 논문의 4장에서 제안한 기존의 EPC 코드의 확장을 통하여 Back-End 서버의 정보 코드를 포함시켜 Back-End 서버를 분산 시켜야 한다.

V. 결 론

본 논문에서는 최근 여러 가지 환경 요인으로 인해 광범위한 분야에서 사용하고 있는 RFID 시스템에서의 프라이버시 침해 문제인 정보 유출 및 위치 추적 문제에 대해서 다루었다. 또한 RFID 시스템에서의 프라이버시 침해를 막기 위해서 충족되어야만 하는 필수 보안 요건인 기밀성, 불구분성, 전방향 안정성 에 대해서도 정의 하였고 기존의 몇몇 인증 기법들을 분석한 후 보다 더 향상된 기법 FSPP를 제안하였다.

FSPP 기법은 필수 보안 요건을 모두 만족하는 기법으로서 태그 내에 비밀값 S_i가 있음을 가정하고 일방향성 즉 역함수 계산 어려움에 기반하여 두 개의 해쉬 함수 G, H 를 적용하였다. 비밀값 S_i는 해쉬 함수 G 를 통하여 산출된 결과 값 a_i를 리더에 전송하여 정보 유출 문제를 해결 하였고 H 함수를 이용하여 태그의 비밀값을 s_{i+1}로 갱신 함으로써 이전 응답 메시지와 이후 응답 메시지 간에 관계를 공격자로 하여금 추측할 수 없게 하는 위치 추적 문제에 대해서도 해결하였다. 또한 인증 과정에서 예상되는 두 개의 해쉬 함수에 대한 Back-End 서버의 계산량의 증가는 기존의 EPC 코드의 확장을 통하여 Back-End 서버의 정보 필드를 EPC 코드 내에 추가함으로써 다수의 서버로 분산시켜 각 각의 태그를 효율적으로 제어 하도록 하였다.

결과적으로 FSPP 기법은 임의적인 반복기록을 필요로 하지 않고, 외부의 유닛에 의해 동작되는 것이 아니므로 태그 각각의 프라이버시가 저비용으로 보호될 수 있어 유비쿼터스 환경에 유용하다.

향후에는 FSPP 기법의 태그 ID를 Back-End 서버 상호간에 일정하게 분배 할 수 있는 교환 조건 문제와 서버 증가로 인한 전체적인 시스템 크기의 향상으로 보안성 측면을 저하시키는 요인이 될 수 있으므로 이에 대한 연구가 필요하다.

참고문헌

[1] 김성철, 양동훈, 송찬후, 전형순 "RFID 확산에 따른 정보 보호 문제와 기업의 대응 전략", 정보통신 정책연구, 제12권, 제1호, pp.149-168, March 2005.

[2] Peter Tandler, "The BEACH application model and software framework for synchronous collaboration in ubiquitous computing environments" The Journal of Systems and Software 69, pp. 269~296, Dec. 2004.

[3] Stephen A. Weis,"RFID Privacy Workshop" IEEE, March 2004.

[4] Heiko knospe, Hartmut Pobl, "RFID Security" ELsevier Ltd, information security technical report. vol.9, no.4, May 2003.

[5] D. Wagner, "A Generalized Birthday Problem, Proceedings of Crypto" LNCS vol.2442, Oct. 2002.

[6] Sanjay Sarmab, Jin Lung Chirna, "Auto ID systems andintelligent manufacturing control" Engineering Applications of Artificial Intelligence 16, pp.365-376, Nov. 2003.

[7] "EPC Network Architecture" The value of Trust , Internet Dratf, April 2004.

[8] Paul M. Goodrum, "The application of active radio frequency identification technology for tool tracking on construction job sites", Automation in Construction , pp.11-17, May 2005.

[9] http://www.eis.army.mil/AIT/technology/rfid_passive.asp Internet Draft, May 2004.

[10] Mike Allen, " Key Criteria for Making the Right RFID Decisions and Investments" Internet Draft, Acsis Inc. , March 2003.

[11] R.Weinstein, "A Technical Overview and Its Application to the Enterprise" IT Professional , IEEE, June 2005.

[12] Christian Floerkemeier, Ted Osinski, Mark Harrison "PML Core Specification 1.0", http://www.autoidcenter.org/, Internet Draft, 2004.

[13] Harry K.H. Chow, King Lun Choy, W.B. Lee, K.C. Laub, "Design of a RFID case-based resource management system for warehouse operations" Expert Systems with Applications ,Elsevier, pp.1-16, July 2005.

[14] Kohei Mizuno, "A long lifetime transmission-only active RFID Systems, Paper to Workshop on Smart Object Systems in conjunction with UbiComp , Nov. 2005.

[15] Sanjay E.sarma, Stephen A.weis, Daniel W. Engels, "RFID System and Security and Privacy Implications" AUTO-ID center, pp.38-48, Sep. 2003.

[16] http://www.sdrforum.org/, Internet Dratf, Sep. 2005.

[17] Jan Camenischa, Maciej Koprowskib, "Fine-grained forward-secure signature schemes without random oracles" elsevier, Science Direct , March 2005.

[18] "EPC Starter Service" VeriSign, Internet Draft, March 2005.

[19] Ari Juels, Michael Szydlo,"Selective Blocking of RFID Tags for Consumer Privacy" , ACM , pp.27-30, March 2003.

[20] Philippe Golle, Markus Jakobsson, Ari Juels2, Paul Syverson "Universal Re-encryption for Mixnets", Stanford University, Internet Draft, 2005.

[21] Junichiro SAITO, Kouichi SAKURAI "A survey on Cryptographic Techniques for RFID privacy" 정보처리 학회지, 제12권, 제5호, pp.11-16, Sep. 2005.

[22] Qi He, Dapeng Wu, Pradeep Khosla"A Mechanism for Personal Controlover Mobile Location Privacy"University of Florida, http://www.wu.ece.ufl.edu, Internet Draft, Dec. 2003.

[23] Oliver Günther, Dr. Sarah Spiekermann , "RFID & Privacy: Consumer Perspective and Technology Insights" HU-IWI, Sep. 2004.

[24] Zhengtao Jiang, Mingsen Xiang, Yumin Wang"A research on new public-key encryption schemes", Applied Mathematics and Computation, pp.51-61, Oct. 2005.

[25] Michael Roe, "Performance of Symmetric Ciphers and One-way Hash Functions", Cambridge University Computer Laboratory, pp.24-32, June 2001.