한국산학기술학회논문지
Vol. 8, No. 1, pp. 41-49, 2007

RFID tag 설계 및 프라이버시 보호에 관한 연구

백현옥[1*], 조태경[1], 유현중[1], 박병수[2]

Study on RFID tag Design and Privacy Protection

Hyun-Ok Baek[1*], Tae-Kyung Cho[1], Hyun-Joong Yoo[1] and Byoung-Soo Park[2]

요 약 RFID는 초소형 IC 칩에 식별정보를 입력하고 무선주파수를 이용하여 칩이 부착된 각 사물의 정보를 인식하고 추적, 관리할 수 있는 유비쿼터시대의 핵심기술이다. 그러나 RFID 시스템은 사용자가 의식하지 못하는 사이에 타인에 의해 개인정보는 물론 상황정보까지 수집되고 이용될 수 있기 때문에 프라이버시침해 문제와 정보보안의 대책이 시급한 실정이다. 뿐만 아니라, 유선상에서 사용되는 보안강도가 높은 여러 암호화 알고리즘은 태그의 다양한 제약 때문에 직접 적용되기 어렵다. 본 논문에서는 국제 표준화에 따른 ISO/IEC 18000-6의 표준안을 바탕으로 RFID 태그의 설계와 설계 과정에서 드러난 RFID 시스템이 가지고 있는 문제점을 분석해보았으며 또한 설계한 태그에 적용할 수 있는 암호화 알고리즘에 대해서 고찰하였다.

Abstract RFID in which subminiature IC chip with the indentified information is built a core technique that can recognize, trace and manage various information of an object using radio frequency in the age of Ubiquitous. Several pressing matters about an infringement of Privacy and a security of private information should be settled as soon as possible because an information of specific circumstance can be collected and used without any awareness by others as well as a private information. In addition, various algorithms with high level of security, which is normally used in wire, can be hardly applied to RFID tag because of a lot of restrictions of tag. In this report, designed-RFID tag based on the standard of ISO/IEC 18000-6 and the problems which originated from the technical procedure of that design were analyzed, and the algorithm which could be applied to the designed-tag was also investigated.

Key Words : RFID, tag 설계, 프라이버시 보호, 암호화알고리즘

1. 서론

최근 유비쿼터스 환경 구현에 있어 핵심적인 기술로서 주목받고 있는 RFID(Radio Frequency Identification) 시스템은 전파식별이라고 하여 사물에 초소형 칩을 부착하여 안테나를 통해 사물 및 주변 환경정보를 무선으로 전송하고 처리하는 일종의 비접촉식 식별기술이다. RFID 시스템은 바코드를 대체할 차세대 기술일 뿐만 아니라 정보통신 분야 외에도 물류, 유통, 교통, 환경 등 다양한 분야에 적용될 수 있으며 RFID를 이용함으로써 상품의 제조, 유통, 판매에 이르는 전 과정을 네트워크화, 지능화하고 이를 통해 생산 비용 절감과 효율성 향상 결과를 가져올 수 있다. RFID 시스템은 많은 장점에도 불구하고 본격적인 상용화까지 해결해야 될 문제를 가지고 있다. 유비쿼터스의 특징인 "anytime, anywhere, anything" 통신이 가능한 환경은 사람, 사물, 다양한 콘텐츠의 이용과 더불어, 의식하지 못하는 사이에 개인정보는 물론 상황정보까지 누군가에 의해 정보를 실시간 수집, 이용될 수 있기 때문에 개인의 프라이버시침해 문제와 정보보안의 확보에 대한 대책이 시급한 실정이다. 실제로 월마트와 베네통사에서는 RFID 시스템을 도입하려다가 소비자의 반발로 인해 취소가 된 사례가 있다. 따라서 본 논문에서는 RFID 태그를 직접 설계해 봄으로서 RFID가 가지는 문제점을 파악하고 정보보안의 확보를 위해 태그에 적용할 수 있는 기존의 알고리즘을 통하여 해결책을 찾고자 한

연구보고서는 정보통신부의 출연금 등으로 수행한 정보통신연구개발사업의 연구결과입니다.
[1]상명대학교 정보통신공학과
[2]상명대학교 컴퓨터시스템공학과
*교신저자: 백현옥(roll23@smu.ac.kr)

다. RFID 태그는 ISO/ISE 18000-6 표준안에 따라 디지털 파트만 설계하였다. 설계툴로는 Xilinx 7.1i 버전을 사용하였고 시뮬레이터로는 ModelSim을 이용하여 확인하였다.

본 논문의 2장에서는 RFID 시스템의 전반적인 내용에 대하여 살펴보고 3장에서는 RFID 태그의 설계에 대해서 알아본다. 그리고 4장에서는 태그의 전체 시뮬레이션을 통하여 동작을 확인하고 태그가 가지고 있는 문제점에 대해서 분석한다. 5장에서는 기존에 제시된 보안대책과 연구된 암호화 알고리즘을 살펴보고 마지막으로 6장에서 결론을 내린다.

2. RFID 시스템

RFID는 자동인식기술의 한 종류이다. 사물에 대한 식별정보를 가지고 있는 IC 칩을 내장한 태그, 라벨, 카드 등에 저장된 데이터를 무선주파수를 이용하여 비접촉으로 읽는 기술로 태그 반도체 칩과 안테나는 이러한 정보를 무선으로 수m에서 수십m까지 보내며 리더는 이 신호를 받아 정보를 해독한 후 컴퓨터로 보낸다. 리더와 태그 사이의 통신은 미리 정해진 RF(Radio Frequency)와 3가지 신호(data, clock, power) 신호에 기반을 둔 request-response 프로토콜을 사용한다[1].

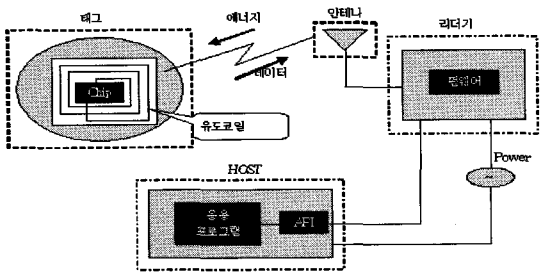

그림 1. RFID 구성도 (Passive Type)

2.1 RFID 구성

RFID 태그는 정보축적과 발신기능을 가지는 매우 작은 칩으로 해당 상품의 세부 정보를 담고 있으며, RF 신호를 받으면 내장된 정보를 전송하는 방식으로서 크게 3개의 구조로 나뉘며 구성요소가 조합되어야 제 기능을 발휘한다.

가. RFID 리더

RFID 리더는 태그의 정보를 읽어내기 위해 태그와 송수신하는 기기이며, 태그에서 수집된 정보를 미들웨어로 전송하는 기능을 한다. RFID 리더에는 태그를 향하여 전파를 주고받는 전자회로 부분을 가지고 있으며 리더 내에 마이크로프로세서는 태그로부터 들어오는 신호를 바꿔주거나, 그 데이터의 신호를 검증하면서 기억장치인 메모리에 저장하기도 하며 필요에 따라서는 나중에 송신하기도 한다.

나. RFID 태그

태그는 물체, 동물, 사람 등에 부착되어서 그 물건에 대한 직접적이거나 간접적인 식별, 인식 정보를 송신하는 장치이다. 일반적으로 한 개의 IC 칩과 한 개의 안테나로 만들어 진다. RFID 태그는 배터리 내장여부에 따라 능동형 태그(Active Tag)와 수동형태그(Passive Tag)로 분류된다. 능동형 태그는 내장된 배터리의 전원으로 동작을 한다. 리더의 필요전력을 줄이고 리더와의 인식거리를 멀리 할 수 있다는 장점이 있으나, 배터리를 사용함으로서 작동시간의 제한을 받으며 수동형에 비해 고가라는 단점이 있다. 수동형 태그는 리더로부터 나오는 전자기장에 의하여 작동 에너지를 얻게 된다. 능동형 태그에 비해 매우 가볍고 가격도 저렴하면서 반영구적으로 사용할 수 있지만, 인식거리가 짧고 리더에서 더 많은 전력을 소모한다는 단점이 있다[2].

다. RFID 미들웨어

RFID 미들웨어란 RFID 시스템 상 중간에 위치하여 리더기 등의 장비를 관리하거나, 이기종 RFID 환경에서 발생하는 대량의 가공되지 않은 데이터를 수집하고 필터링하여, 의미 있는 정보로 변환하여 응용 소프트웨어 등에 필요한 정보를 제공하는 소프트웨어 플랫폼으로 정의할 수 있다. 즉 RFID 미들웨어는 리더에서 계속적으로 발생하는 식별코드 데이터를 수집, 제어 관리하는 기능을 하며, 모든 구성요소와 연결되어 계층적으로 조직화되고 분산된 구조의 미들웨어 네트워크를 구성하여 서로 통신한다.

2.2 RFID 동작원리

RFID 시스템은 기본적인 동작 원리는 다음과 같다. 우선 RFID 태그가 안테나의 전자기장 내를 통과하면 리더로부터 신호를 감지하여 전파를 수신하고 RFID 태그 안에 내장된 IC 칩이 기동하여 태그 내에 저장된 데이터를 리더로 전송한다. 태그로부터 데이터를 수신한 리더는 신호를 변환하여 정상적인 데이터 인지를 검증한 후 정상적인 경우 RS-232, RS-422 및 RS-485 등을 통하여 컴퓨

터와 다른 컨트롤러 호 전송에 필요한 정보를 가공한다 [2].

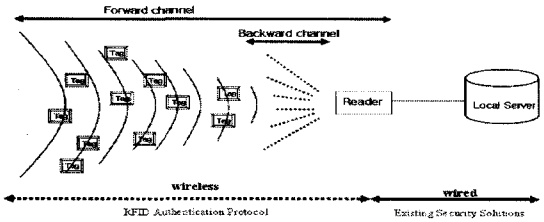

그림 2. RFID 시스템의 전체적 구조

3. RFID tag 설계

3.1 ISO/IEC 18000-6 표준 정의

ISO/IEC 18000 규격은 각 주파수 대역별로 ISO/IEC 18000-1부터 ISO/IEC 18000-7까지 6개 파트로 구성되어 있다((ISO/IEC 18000-5는 없음). 그 중에서 ISO/IEC 18000-6 규격은 860MHz~960MHz의 ISM 대역에서 품목 관리의 응용 분야에 사용되는 RFID 장비의 에어 인터페이스를 정의하며, 이 규격은 유통물류 분야에서 사용할 수 있는 저가의 태그를 제공할 수 있는 유력한 기술로 평가받고 있다. ISO/IEC 18000-6 표준은 Type A, Type B, Type C의 세 가지 형식을 가진다. 특히 EPCglobal의 Class1 Gen2 기술을 Type C로 포함시킨 ISO/IEC 18000-6 AM1(Amendment1) 문서가 2006년 6월에 최종 승인되면서 그 상용화 가능성이 훨씬 높아졌다.

3.2 Verilog HDL 모델링

ISO/IEC 18000-6 표준을 기반으로 Type B를 설계하였으며 Type B는 Manchester coding을 통해 부호화를 하고 Binary tree protocol을 통해서 태그를 식별해 낸다. 그에 대한 응답은 FM0로 부호화 하여 다시 리더에게 전송하게 된다. 이 과정을 Packet Detector module, Manchester Decoder module, CRC16 module, CORE module, FM0 module로 나누었으며 2개의 CRC16 module 을 포함해서 총 6개의 모듈로 나누어 설계하였다. 그림 3 에 태그의 전체 block diagram 을 나타내었고 그림 4는 GROUP_SELECT에 대한 샘플 명령어/응답 패킷을 나타내었다.

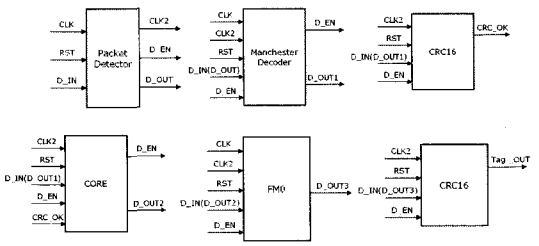

그림 3. RFID 태그 블록도 (Type B)

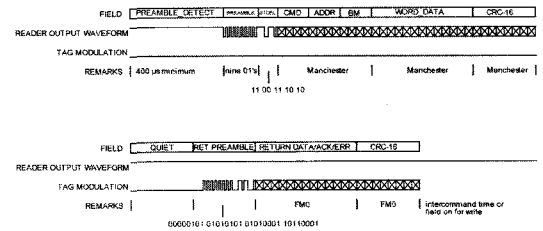

그림 4 GROUP_SELECT에 대한 샘플 명령어/응답 패킷

3.2.1 Packet Detector Module

Reader로부터 전송되는 ASK변조된 일반적인 명령어 포맷은 그림 5에 나타냈듯이 Preamble Detect, Preamble, Delimiter, Command, Parameter, Data, CRC-16으로 구성된다. preamble detect 필드는 최소한 400us 동안 변조되지 않은 일정한 반송파로 구성되어 있으며 이것은 40kbit/s의 통신 속도에서 16비트에 상응한다. preamble은 NRZ(Non Return to Zero)형식에서 9비트의 맨체스터 0과 같은 010101010101로 구성되어 있다. Delimiter는 총 4개로 구성된다. 본 논문에서 설계한 태그에는 Start delimiter 1일 이용하였고 그의 값은 "11 00 11 10 10"이다. Start delimiter의 10개의 bit가 끝난 후에 실제로 command가 시작된다. command부터 Manchester Coding을 하므로 Packet Detector Module의 역할은 preamble detect와 preamble, delimiter를 검출해서 다음 data 부터가 Manchester coding 하게 될 실 data임을 알려주는 것이다. 즉, Command, Parameter, Data, CRC-16일 때 D_EN 신호를 주어 실data 임을 알리고 Manchester coding을 하게 된다[3].

3.2.2 Manchester Decoder Module

Manchester Decoder Module에서는 Packet Detector에서 검출된 data를 data 부호화 하는 역할을 한다. 논리 0

Preamble Detect	Preamble	Delimiter	Command	Parameter	Data	CRC-16

그림 5. 일반적인 명령어 포맷

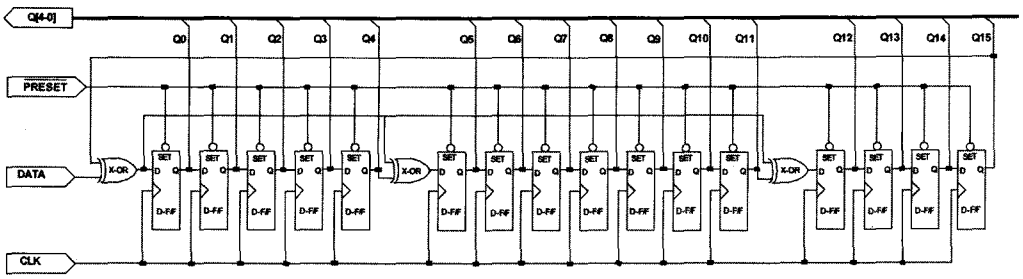

그림 6. CRC-16 누산기의 시프트 레지스터 구현

이 양의 변화(0에서 1로의 변화)로 정의되고, 논리 1이 음의 변화(1에서 0으로의 변화)로 정의된다.

3.2.3 CRC-16 Module

CRC(Cyclic Redundancy Check) 프로시저는 많은 양의 데이터양에 대하여도 충분히 신뢰성이 있는 체크섬을 발생시킬 수 있으며, 유무선 인터페이스를 통한 데이터 전송에서 오류를 검출하는데 매우 적합하다. 또한 연속 데이터 전송에서 오류를 검출할 수 있다는 큰 특징이 있다.

CRC-16을 계산하기 위해 사용되는 다항식은 x16+x12+x5+1이며, 이것은 CRC-CCITT 국제 표준이다. CRC은 명령어의 시작부터 데이터의 끝까지 메시지 내에 포함된 모든 데이터에 대해 계산된다. CRC-16은 리더에서 태그로 향하고, 태그에서 리더로 향하는 경우 모두 사용된다. Reader로부터 명령을 수신하는 경우 태그는 체크섬 또는 CRC값이 유효하다는 것을 확인해야 하며 만일 유효하지 않을 경우, 태그는 프레임을 버리고, 응답도 하지 않으며, 어떤 다른 동작도 취하지 않는다[3].

3.2.4 Core Module

Core Module에서는 실제적으로 태그의 인식과정이 포함되어 있다. 리더로부터 전송받은 데이터를 해석하여 포함된 명령에 따라 동작을 수행하며 command에 해당하는 응답을 하며 명령어에 따라서 태그의 메모리에 저장되어 있는 태그 고유의 UID와 리더에서 전송하는 WORDDATA의 비교를 통해 태그를 식별한다. 태그가 받을 수 있는 명령어는 기능에 따라 mandatory, optional, custom, proprietary의 4개의 그룹으로 나누어진다[3]. 본 논문에서는 4개의 그룹 명령어 중에서 Mandatory command만을 설계하였다. 또한 리더로부터 전송받은 command에 따라서 태그의 상태변화가 이루어지며 Collision arbitration 알고리즘을 사용하여 충돌 중재를 한다. 태그는 충돌 중재를 위해 태그 내에 8 비트 카운터 COUNT 와 난수 발생기(0과 1의 값 중에서 선택)라는 두 개의 하드웨어 요소를 갖추어야 한다[3].

3.2.5 FM0 Module

Core Module에서 Processing 된 데이터는 Bi-Phase Space로 알려진 FM0 기술을 사용하여 부호화되어 리더에게 전송된다. FM0 부호화에서 데이터 변화는 모든 비트 경계와 전송되는 논리 0의 비트 중간에서 발생한다[3]. 이 과정을 통해 부호화된 data는 Return Preamble 뒤에 붙어 전송하게 된다. 여기서 Return Preamble은 리더가 태그 데이터 클럭의 동기를 구하고, 메시지 복호의 시작이 가능하도록 한다.

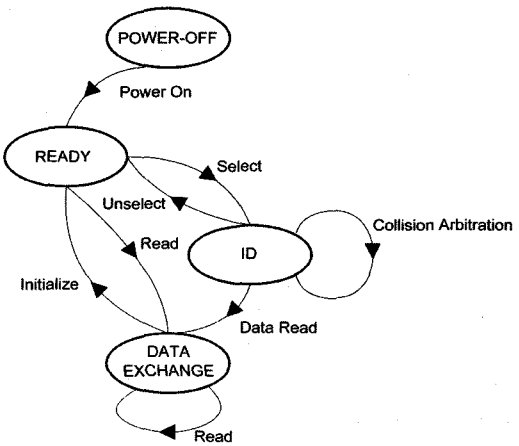

그림 7. 상태 다이어그램

3.3 Tag의 동작 상태 다이어그램

그림 7은 ISO-18000-6 Type B에 제시된 표준 RFID 태그의 상태다이어그램이다. 태그는 리더가 태그를 활성화할 수 없을 때 POWER_OFF 상태에 있으며 리더의 전자계가 형성이 되었을 때 Power_On으로 상태가 변하고 태그는 READY 상태에 있게 된다. 즉, 태그는 리더가 처

음으로 태그에 전원을 공급하였을 때 READY 상태에 있다. GROUP_SELECT나 READ 명령어에 의해 태그가 선택될 경우 Select, GROUP_UNSELECT나 INITIALIZE 명령어에 의해 태그 선택이 해제된 경우 Unselect가 된다. 태그는 자신을 리더에 확인시키려고 할 때 ID 상태에 있으며 리더에 인식되고 선택되었을 때 DATA_EXCHANGE 상태에 있게 된다[3].

4. 결과 분석 및 문제점

본 장에서는 3장에서 소개한 ISO/ISE 18000-6 Type B 태그의 시뮬레이션 결과와 설계하는 과정에서 드러난 RFID 시스템이 가지고 있는 문제점을 분석한다.

4.1 전체 시뮬레이션

그림 8은 GROUP_SELECT_EQ 명령에 대한 시뮬레이션 결과 이다. GROUP_SELECT_EQ를 포함한 GROUP_SELECT를 명령은 ADDRESS, BYTE_MASK, WORD_DATA 이렇게 3개의 파라미터를 갖는다.

그림 9와 같은 GROUP_SELECT_EQ 명령어를 받으면 READY 상태에 있는 태그는 지정된 주소에서 시작하는 8바이트의 메모리 내용을 읽고 리더에서 보낸 WORD_DATA와 비교해야 한다. 메모리 내용이 WORD_DATA와 같은 경우에 태그는 내부 카운터의 카운트를 0으로 설정하고, 그림 10과 같이 UID를 읽고서 되돌려 보낸 후 ID 상태로 들어가야 한다. 그리고 다른 모든 경우에는 태그는 응답을 보내지 않는다[3].

시뮬레이션에서 태그의 UID와 테스트벤치에서 WORD_DATA에 64bit의 값은 정보를 입력해놓았다. 그렇기 때문에 시뮬레이션 결과 태그는 Preamble 후에 ID를 응답하는 것을 확인 할 수 있었다. 또한 리더로부터 받은 CRC값을 태그에서 계산한 결과 오류가 없을 알 수 있었고, 임의로 잘못된 CRC 값을 넣었을 때 태그는 아무런 응답을 하지 않은 것을 확인하였다. 그밖에 GROUP_UNSELECT 명령어와 READ, SUCCESS, FAIL 등의 명령어의 태그의 응답을 확인한 결과 제대로 동작하는 것을 확인할 수 있었고 태그의 상태변화도 확인하였다.

Preamble	ID	CRC-16
	64 비트	16 비트

그림 10. 오류가 없을 때 GROUP_SELECT_EQ 응답

4.2 RFID가 가지는 문제점

태그를 설계하여 각각의 명령어에 따른 시뮬레이션을 수행하였고 명령어에 따른 태그의 응답을 확인하였다. 현재 사용되고 있는 RFID 태그는 일반적으로 태그마다 일정한 분류 체계를 가진 고유한 ID 값을 가지도록 생산되거나, 사용하는 업체에서 제품명, 제품번호, 회사명, 생산일자 등의 직접적인 식별정보를 입력하기도 한다. 따라서 각각의 태그는 항상 동일하며 고유한 값을 송신한다. 태그를 설계하는 과정에서 보았듯이 단지 CRC-16의 과정을 거쳐 오류검출만 할 뿐 그 밖에 어떠한 암호화 과정이 인증 메커니즘이 포함되어 있지 않다. 태그의 정보를 읽어내는 기능을 하는 RFID 리더가 적법한지 아닌지를 판단하는 과정 즉, 인증 프로토콜 없이 모든 RFID 리더에게 송신을 하게 된다. 다시말해서 언제 어디서나 리더를 가진 사람에게 별도의 인증과정 없이 정보를 제공하게 될 것이며 태그가 가지고 있는 고유값을 전달하게 됨으로써 위치추적은 물론 RFID 태그가 부착된 사물을 가진 사람이라면 소유한 사람의 프라이버시가 침해당할 수 있

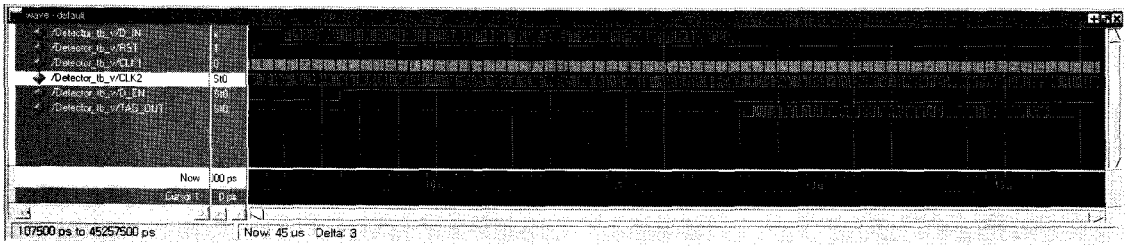

그림 8. GROUP_SELECT명령어의 시뮬레이션 결과

Preamble	Delimiter	Command	Address	Mask	WORD_DATA	CRC-16
		8 bit	8 bit	8 bit	64 bit	16 bit

그림 9. GROUP_SELECT_EQ Command

게 된다. 이것이 RFID 시스템의 편리함과 무한한 가능성에도 불구하고 상용화까지 주춤거리고 있는 이유이다.

4.2.1 저가 RFID 태그의 제약사항

논문에서 대상으로 하고 있는 수동형 RFID 태그는 하드웨어적으로 제약사항이 있기 때문에 고수준의 암호화를 구현하기가 어렵다. 고수준의 암호화 모듈을 xor 내에 구현 가능하다면, 프라이버시 보호 문제는 간단하게 해결될 수 있으며 백엔드 서버와 태그 간에 공개키, 비밀키 쌍을 나누어 가지기만 하면, 도청에 걱정 없이 보안 필수 요건을 다 만족시키는 프로토콜을 만들 수 있다[4][5]. 그러나 이것은 수동형 태그에는 불가능한 일이며, 수동형 태그는 생산 단가 문제로 인하여 배터리가 장착하거나, 고성능의 범용 CPU(central processing unit)를 장착할 수 없기 때문에 전력 사용량과 논리 게이트의 수, 실행이 되는 클럭 사이클의 횟수 등이 매 제한적이다[6].

표 1. 저가 RFID 태그의 하드웨어적인 제약 사항

	태그 칩 전체에 대한 제약 사항	암호화 알고리즘에 대한 제약 사항
전력사용량	20uA	15uA
게이트 개수	20000GE	5000GE
클럭사이클	1800cycles(18ms)	1000cycles(10ms)
가격	5~10센트	-

5. 프라이버시 해결 및 보안

본 장에서는 앞서 설계한 태그의 프라이버시를 해결하기 위해 RFID 시스템에서 발생가능 한 공격방법을 알아보고 프라이버시를 보호하기 위한 필수 보안 요소를 통하여 한 기존의 연구된 방법을 제시한다. 또한 태그에 직접 적용할 수 있는 방법을 검토하며 프라이버시를 보호할 수 있는 방법을 찾고자 한다.

5.1 RFID 시스템에서 발생 가능한 공격방법 및 위험요인

RFID 시스템에서 태그와 리더는 무선통신으로 정보를 교환한다는 것과 연산능력과 저장능력 등의 제약을 가진 태그로 인해 여러 위협들에 노출되기 쉽다. RFID에서 일어날 수 있는 주요 공격들을 표 2에 나타내었다[5].

표 2. RFID 시스템의 보안 위협

위협의 종류	내 용
도청	- 정보가 암호화되지 않으면 통신 내용이 노출됨 - 리더기로부터 전송되는 신호는 900㎒급 수동형 RFID 시스템의 경우도 100m 이상의 거리에서 측정 가능함
Shooping	- Tag의 내용을 스캔하여 정보를 획득하는 공격 - 휴대용 리더기로 Tag의 내용을 읽어 내고, 위치 추적 등을 할 수 있어 프라이버시 문제를야기함
Spoofing	- 통신상에 관여하여 위장하거나 Tag의 내용을 변조하는 보다 적극적인 공격 - Tag의 내용을 변조하여 상품의 절도에 이용하거나 정당한 리더기로 가장하는 공격이 가능함
서비스 거부 공격	- 강한 전파의 송신 등으로 정상적인 통신을 방해하여 서비스가 이루어지지 못하게 하는 공격

5.2 암호 기술을 이용한 정보보호 방식

일반적으로 기밀성, 인증 등의 서비스를 제공하기 위해서는 블록암호, 스트림암호, 해쉬함수, 공개키 암호가 모두 필요하다. 하지만, RFID 태그의 경우 이를 모두 수용할 수 없기 때문에 새로운 정보보호 방식의 개발이 요구된다.

5.2.1 Hash-Lock 방법

일반적으로 접근 제어메커니즘은 공개키 기반의 방식이나 비밀키 기반의 방식으로 사용되는 경우가 많다. 그러나 RFID 태그가 가진 제약은 연산 능력이나 크키에 영향을 주기 때문에 기존의 접근 제어 메커니즘을 그대로 적용하기 어려운 것이 사실이다. 이로 인해 S.Weis 등의 논문에서 단반향(One-way) 해쉬 함수를 기반으로 하는 접근 제어 메커니즘인 hash Lock 기술이 제안되었다[7]. 태그는 Lock 상태와 Unlock 상태로 2가지 상태를 가지고 있으며 적법한 리더만 Lock 상태의 태그를 열 수 있다. 태그는 Hash 알고리즘을 기반으로 하며 MeteID 정보를 보관할 수 있는 저장공간을 보유하고 있고 Unlock 상태의 태그를 잠그기 위해서는 리더가 임의의 key 값을 선택하고 key에 대한 해쉬 값을 계산하여 meta ID로 지정하고 MetaID 정보를 태그에 저장하면 된다. Lock 상태의 태그는 오직 외부의 요청에 대한 응답으로 MetaID 정보만을 제공하며 다른 정보는 제공하지 않는다. 태그가 정상적으로 작동을 하도록 해주기 위해서는 태그의 상태를 Unlock 상태로 바꿔주어야 하며 태그는 Key 정보를 통한 리더의 요구에 따라 UnLock 상태가 되며 리더에 태그의

정보를 제공하게 된다. Hash Lock 기법은 태그 안에 있는 식별 정보를 백엔드 서버에 접근할 수 있는 인증된 리더에게만 주므로 해쉬함수의 특징인 역 처리의 어려움을 기반으로 하여 허락받지 않은 리더가 태그 정보 획득을 방지할 수 있다. 허락되지 않은 리더는 DB로부터 Key 정보를 획득할 수 없으며, Key 정보가 없으면 태그의 Unlock이 불가능하다[8].

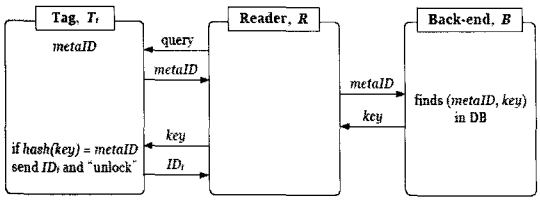

그림 11. Hash-lock 기법

5.2.2 Hash Chain 방법

Hash Chain기법은 두 개의 서로 다른 해시 함수를 이용하는 기법이다. 태그 내부에 두 개의 일방향 해시 함수 H와 G를 가지고 있다고 가정한다. 실제로 해시 함수가 태그 내부에 구현될 가능성은 높다고 볼 수 있다. M. Feldhofer 등이 태그 내에 들어갈 수 있는 AES 모듈을 설계했고 이 AES 모듈을 여러 개의 일방향 해시 함수로 대체하여 사용할 수 있다.

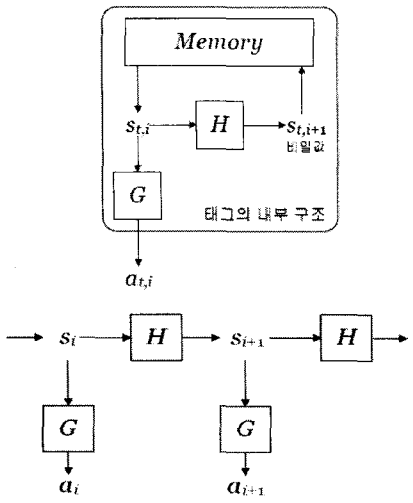

그림 12. 해시 체인 기반 기법의 태그 내부구조와 Ohkubo가 제안한 태그의 연산

H와 G는 해시 함수이다. 리더는 태그로부터 받은 ai값을 백엔드 서버(Back-End Server)에 보낸다. 백엔드 서버는 (ID, S1)의 쌍의 값을 리스트로 가지고 있고, a'i=G(Hi(s1))의 값을 계산해 놓는다. a'i=ai인지 체크를 하고 두 값이 동일하다면 a'i의 쌍인 ID를 리턴하게 된다. 이 방법에서는 따로 리더가 적법한지 아닌지에 대해서 인증 프로토콜을 수행하지 않고 현재의 비밀값 st,i를 해시 함수 G로 계산한 값을 리더에게 주기 때문에 프로토콜이 매우 단순해지며 외부로부터의 값 입력이 없기 때문에 프로토콜의 허점을 이용한 공격이 어렵다[9][10]. 또한 외부에서 태그의 정보 값을 갱신해 주는 방식이 아니라 태그 스스로가 자신의 내부 정보를 갱신하는 방식을 취하기 때문에 도청에 의한 공격으로부터 완전히 자유롭다. 그리고 내부 정보 변경을 일방향 해시 함수를 가지고 계산을 해서 수행하기 때문에 물리적 공격에 의해 내부 정보가 노출되는 경우에라도 일방향 해시 함수의 성질에 의해서 완벽한 전방 보안성을 보장한다. 기본 프라이버시 보호 기법들 중에서 가장 안전한 기법으로 간주되어지고 있으나 백엔드 서버에서 태그를 식별하기 위한 계산 량이 많다[11].

6. 결 론

최근 사물에 전자태그를 부착하여 사물의 정보를 확인하고 주변 상황을 감지하는 RFID 시스템이 등장하여 유비쿼터스 환경의 필수적인 기술로 인식되고 있다. 그러나 RFID 는 태그의 정보 및 이를 소유한 사용자의 위치 정보 등의 개인 정보와 인가된 리더만이 태그 정보에 접근할 수 있는 인증 과정에 취약점을 가지고 있으며, RF를 통한 전송 정보의 불법적인 공격자에 의한 정보가 노출되는 문제를 안고 있다.

본 논문에서는 RFID 시스템에 대한 전반적인 개념과 특성을 살펴보고 직접 태그를 설계하면서 그 과정에서 발견된 RFID 시스템의 보안과 프라이버시 문제점에 대해서 고찰하였다. 태그의 설계과정을 통해서 RFID Type B의 표준에는 태그의 정보를 암호화하는 과정이나 인증 메커니즘이 없어 비인가 된 리더도 태그에 접근하여 정보를 얻을 수 있다는 보안상 취약한 문제점을 발견하였으며 이는 설계한 태그의 동작을 시뮬레이션 하는 동안에도 그대로 드러났다.

RFID 태그의 경우 프라이버시와 보안 기능 향상을 위해 RFID 태그 내에 암호화 알고리즘을 적용하여 보안과 프라이버시 문제를 해결할 수 있다. 하지만 태그가 가진 제약으로 인해 유선상 뛰어난 여러 알고리즘을 그대로 적용시킬 수 없는 단점이 있다. 그렇기 때문에 최근엔 초경량 암호 알고리즘의 연구가 활발하며 Hash Lock,

Randomize Hash Lock, Hash Chain 등의 변형으로 단방향 해쉬 함수를 사용하여 보안할 수 있는 여러 알고리즘들이 개발되고 있고 하드웨어의 제약으로 구현하기 힘들었던 해쉬 함수를 대체할 AES 함수의 구현으로 RFID 태그의 보안은 점점 강도가 높아지고 있음을 알 수 있었다.

하지만 최근 연구된 변형된 암호 방법들도 프라이버시 보호를 위한 필수 보안 요건인 기밀성, 불구분성, 전방보안성, 후방보안성을 완벽히 만족하는 알고리즘의 구현은 아직까지 이루어지지 않고 있고, 이론상 보안의 강도가 높은 암호화 알고리즘을 태그의 연산량을 줄이고 하드웨어 게이트 수를 줄이면서 RFID 태그에 적합하게 구현하는 것이 연구되어야 할 과제이다.

참고문헌

[1] G. Avoine and P. Oechslin, "RFID Traceability: A Multilayer Problem", In Finacial Cryptography '05, February 2005.

[2] 유승화, "유비쿼터스 사회의 Radio Frequency IDentification", 전자신문사, 2005.

[3] ISO/IEC 18000-6, Part6 : Parameters for air interface communications at 860-960MHz, International Standards.

[4] M. Ohkubo, K. Suzuki, and S. Kinoshita, "A Cryptographic Approachto "Privacy-Frendly" Tag", RFID Privacy Workshop, 2003.

[5] G. Avoine and P. Oechslin, "A Scalabel and Provably Secure Hash-based RFID Protocol", In IEEE PerSec 2005, March 2005.

[6] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm", Springer, In Conference of Cryptographic Hardware and Embeded Systems 2004 Proceedings, 2004.

[7] 박태서, "백워드 채널 보호를 이용한 RFID 정보보호 기법", 석사학위논문, 2005.

[8] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Pravacy Aspects of Low-cost Radio Frequency Identification Systems", In Proceedings of the 1st International Conference on Security in Rervasive Computing, 2003.

[9] 조정환, 여상수, 김성권, "AES를 기반으로 하는 개선된 RFID 프라이버시 보호 프로토콜", 한국정보과학회 학술발표논문집, 2005.

[10] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Efficient Hash-Chain Based RFID Privacy Protection Scheme", In Ubicomp 2004, 2004

[11] 주학수, "RFID 시스템의 보안 및 프라이버시 보호를 위한 기술 분석", KETI, 2004.

백 현 옥(Hyun-Ok Baek) [준회원]

- 2005년 2월 : 상명대학교 정보통신공학과 (공학사)
- 2005년 3월 ~ 현재 : 상명대학교 대학원 정보통신공학과 석사과정

<관심분야>
RFID, Wireless PAN, 차세대 이동통신 기술, Ad-hoc 네트워크

조 태 경(Tae-Kyung Cho) [종신회원]

- 1984년 2월 : 한양대학교 전자통신공학과 (공학사)
- 1986년 2월 : 한양대학교 대학원 전자통신공학과 (공학석사)
- 2001년 2월 : 한양대학교 대학원 전자통신공학과 (공학박사)
- 2003년 9월 ~ 현재 : 상명대학교 정보통신공학과 교수

<관심분야>
초고속통신망, e-Learning

유 현 중(Hyun-Joong Yoo) [정회원]

- 1982년 2월 : 서강대학교 전자공학과 (공학사)
- 1991년 5월 : Missouri University 전기 및 컴퓨터 공학과 (공학석사)
- 1996년 5월 : Missouri University 전기 및 컴퓨터 공학과 (공학박사)
- 1996년 3월 ~ 현재 : 상명대학교 정보통신공학과 교수

<관심분야>
인공신경망응용, 패턴인식, 영상/동영상 처리

박 병 수(Byoung-Soo Park) **[종신회원]**

- 1986년 2월 : 한양대학교 전자공학과 (공학사)
- 1989년 8월 : 한양대학교 대학원 전자공학과 (공학석사)
- 1994년 5월 : 텍사스 A&M (공학박사)
- 1995년 3월 ~ 현재 : 상명대학교 컴퓨터시스템공학과 교수

<관심분야>
임베디드 시스템, 병렬 알고리즘