RFID기반 전원 관리와 PKI기반 인증이 가능한 보안 카드에 관한 연구

박기웅, 임상석, 석현철, 박규호

한국과학기술원 컴퓨터공학연구실
{woongbak,hcseok,sslim,kpark}@core.kaist.ac.kr

요 약

본 논문에서는 유비쿼터스 서비스 제공을 위한 보안카드를 구현하는데 따르는 이슈와 문제점에 대하여 논하고 이를 극복하기 위한 초저전력 보안카드를 제시한다. 제시된 보안카드는 PKI 기반의 인증이 가능하며 RFID기반의 전원 관리 메커니즘을 통하여 전원공급 지속시간을 극대화 시킨다. 이를 실현하기 위하여 제시된 보안카드는 다음과 같은 특징을 가진다. 첫째, Ad-Hoc 통신과 저전력 통신이 가능한 Zigbee 모듈이 장착된다. 둘째, 통신 모듈에 저전력 메커니즘을 적용하기 위한 RFID 모듈 및 전원 관리 모듈을 장착하여 전원공급 지속시간을 극대화 시킨다. 셋째, 인증 지연 시간을 최소화하기 위해 RSA 가속기를 장착한다.

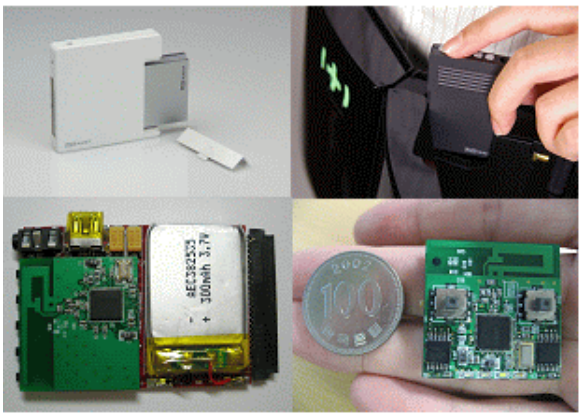
기존 인증장치로서 널리 사용되고 있는 스마트카드 및 RFID 기반의 인증장치의 경우 독립적인 통신 기능과 위치기반 서비스를 제공할 수 없다는 단점을 가지므로 유비쿼터스 서비스를 제공하는데 어려움이 따른다. 본 논문에서는 RFID를 이용한 저전력 메커니즘을 제시하고 이를 활용한 PKI 기반 인증 카드를 제시한다. 본 논문에서 제시한 보안카드의 성능은 인증 지연시간 측면과 전원공급 지속시간 측면에서 성능을 측정하고 분석하였다.

1. 서론

유비쿼터스 컴퓨팅은 환경에 존재하는 컴퓨터 디바이스와 센서들이 전자제품, 생활용품, 가구, 액세서리, 심지어 약품과 음식물에 이르기까지 어디에서나 주변 환경에 부착되고 하나의 네트워크로 연결된다. 이들은 사람에게 쾌적한 생활환경을 제공하기 위해 서로 정보를 주고받거나 스스로 문제를 해결할 수 있는 지능을 가지고 있다.

하지만, 유비쿼터스 컴퓨팅이 일상생활과 컴퓨팅이 유기적으로 접목되어 지능화된 서비스를 제공하는 장점 이면에는 개인정보와 같은 주요 데이터의 노출 위험이 심각하다[1]. 그러므로 유비쿼터스 컴퓨팅 환경에서는 다양한 장치와 단말간의 인증과 이들 간의 통신상의 보안을 확보하는 것이 매우 중요한 문제로 대두된다. 이러한 보안상의 문제를 해결하는데 있어서 인증 시스템은 가장 중요한 역할을 수행한다.

본 논문에서 제시한 초소형 보안카드는 그림1에 나타난다. 제시된 보안카드는 Zigbee를 이용한 위치기반 서비스가 가능하고 웨어러블 컴퓨터에 카트리지 형태로 장착이 가능하여 USB를 통한 통신이 가능하다. 안전한 유비쿼터스 서비스를 제공과 보안카드를 구현하기 위하여 다음과 같은 3가지의 요구사항이 존재한다.



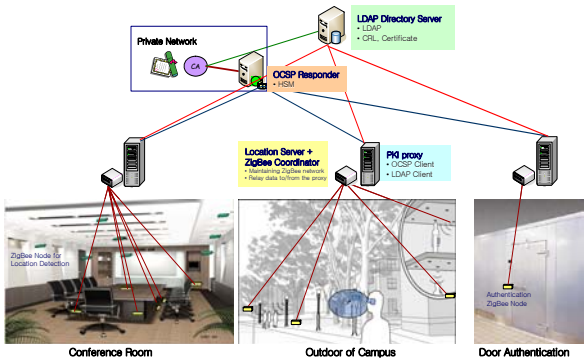
<그림1> : PANDA(Personal Authentication Network Device Architecture), 좌측 : PANDA Ver 1.0 (2005년 개발) 우측 : PANDA Ver 2.0 (2006년 개발)

1)보안카드는 디지털 서명과 인증, 부인 방지 등의 기능이 제공되는 PKI 기반 인증이 가능해야 한다[7]-[9].

2)주변에 존재하는 디바이스와 다른 보안카드 간 ad-hoc 통신이 가능해야 한다[10]. 이와 같은 기능은 보안카드를 통하여 안전한 통신 채널을 맺고 이를 통해 명함과 문서 등의 정보 교환을 가능하게 만든다.

3)위치기반 서비스가 가능해야 한다. 유비쿼터스 환경에서 사용자는 지속적으로 이동하며 환경에 존재하는 여러 디바이스와 동적으로 통신을 하게 된다. 이와 같은 이동성으로 서비스를 제공하는 디바이스는 현재 통신하고 있는 보안카드와의 지속적인 인증이 필요하게 된다. 이러한 기능을 제공하기 위하여 사용자가 소지하고 있는 보안카드의 신호세기(RSSI[11])를 활용할 수 있다. 또한, 만약 사용자가 현재 사용하고 있는 서비스 디바이스와의 서비스 세션을 종료하였을 경우 해당 디바이스는 자동적으로 해당 사용자와 맺고 있는 보안 채널을 종료하는 인증 메커니즘이 필요하다.

위와 같은 요구사항을 만족시키기 위한 기존의 해결 방법으로서 스마트카드와 Passive 형태의 RFID가 있다. 스마트카드와 Passive 형태의 RFID의 경우 서비스 디바이스와의 물리적인 거리에 따른 반응



<그림2> : 전반적인 보안 인프라 구성도

메시지를 통해 이를 실현할 수 있다. 하지만 이를 통한 물리적 위치 측정은 물리적인 제약사항이 뒤따르므로, 위치기반 인증을 실현하는데 있어서 많은 어려움이 따르게 된다[14]. 게다가 RFID와 스마트카드의 경우 내부의 독립적인 전원을 사용하지 않아 Ad-hoc 기반의 통신이 불가능하고 보안 정책의 변화에 따라 사용자가 소지하고 있는 보안카드의 교체가 따르는 단점들을 가지고 있다.

이러한 문제점을 극복하기 위하여 본 논문에서는 기존의 RFID와 스마트카드가 가지고 있는 단점을 극복하고 제시된 요구사항을 만족시키는 보안카드를 제시한다. 아울러, 제시된 보안 카드의 이름은 PANDA[1]로 명명한다.

본 논문의 구성은 다음과 같다. 제2장에서는 본 논문에서 제시하는 보안카드의 요구사항에 대하여 논한다. 제3장에서는 전체적인 시스템 구성도와 본 논문에서 제시한 보안카드에 따른 Zigbee 센서 네트워크 및 PKI 구조를 나타내었고, 제4장에서는 PANDA의 디자인과 전력 관리 기술에 대하여 논한다. 제5장에서는 성능 측정에 대하여 논하고 6장에서 결론을 맺는다.

2. 시스템 요구사항

본 논문에서 제시하는 보안카드(PANDA) 및 그에 따른 보안 시스템은 두 가지의 해결해야 할 문제점이 존재한다.

1) 인증 지연시간 최소화 : 높은 보안성을 제공하더라도 사용자가 환경에 존재하는 디바이스와 인증을 위하여 오랜 시간을 기다려야 한다면 실질적인 구현에 있어서는 현실성을 매우 떨어뜨리는 결과를 초래하므로 사용자의 인지 시간을 고려한 끊김 없는 인증이 제공되어야 한다[16]. 인증 지연시간을 최소화하기 위하여 본 논문에서 제시한 PANDA는 RSA 알고리즘 연산에 따른 지연시간을 감소시키기 위하여 암호연산 가속기[15]를 장착하였다. 암호연산 가속기는 개인키의 안전한 저장과 RSA 연산 및 해시함수의 가속기능을 제공한다. 또한, Zigbee의 채널 탐색 시간[17]에 따른 지연을 막기 위하여 정적인 인증 채널 할당을 통하여 채널 탐색에 의한 지연을 최소화 시켰다.

2) 장기적인 전원공급 지속시간 : PANDA는 내부적으로 장착된 전원공급 장치에 의하여 작동을 하게 된다. 그러므로 만약 사용자가 환경에 존재하는 여러 디바이스와의 인증을 위하여 빈번한 충전을 해주어야 한다면 사용성을 매우 저하시키는 결과를 초래한다. 본 논문에서는 전원공급 지속시간을 극대화하기 위하여 RFID를 이용한 전원 관리를 제안한다. PANDA는 인증연산이 이 수행되지 않는 유휴시간에는 초절전 모드로 대기하게 되고 인증이 필요한 시간에는 RFID 리더기에 의해 발생된 신호를 이용하여 PANDA를 절전 모드에서 인증 모드로 전환하여 전원을 공급하게 됨으로서 전원공급 지속시간을 극대화 하였다.

3. 전반적인 시스템 구조

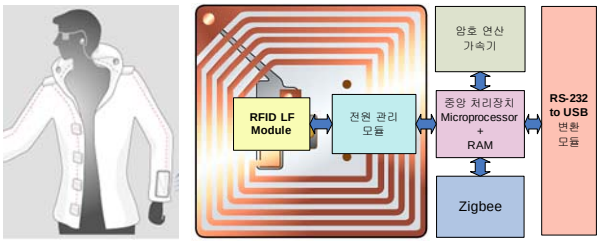
한 학생이 PANDA를 가지고 있다고 가정하자. 학생이 강의실에 입장을 하였을 때 자동적으로 인증 프로토콜이 수행되어 문이 열리게 되고 자동적으로 출석체크가 된다. 학생이 자리에 앉자 수강생 자리에 장착되어 있는 컴퓨터는 학생 인증을 통해 학생의 ID로 로그인이 되며, 그가 이전에 작업했던 컴퓨팅 환경이 그대로 화면에 나타나게 되어 컴퓨팅 작업을 그대로 수행할 수 있게 된다. 수강생의 휴대폰이 울려 자리를 비우게 되었다. 이때 수강생은 자신이 작업하고 있던 컴퓨터 화면을 로그아웃하지 않은 상태로 자리를 비웠지만 학생이 가지고 있는 PANDA는 자동적으로 그 학생의 컴퓨터 화면을 로그아웃 시켜 그 학생의 정보를 보호하게 된다. 이는 유비쿼터스 서비스의 하나의 예이다.

위와 같은 시나리오를 실현하기 위하여 필요한 기술은 다음과 같다. : PKI, Zigbee 기반의 위치기만 서비스, PANDA 등이다. 시스템의 전반적인 구조를 그림2에 도식되었다. 전반적인 구조는 다음과 같이 4가지의 요소로 구성된다.

1) PKI : PKI는 인증서의 보관과 발급을 담당하는 CA와 사용자의 계정 생성과 초기 인증을 담당하는 RA, 인증서의 유효성 여부를 체크하는 OCSP Responder와 인증서의 데이터베이스 역할을 담당하는 LDAP 디렉터리 서버로 구성된다. 사용자의 신원이 CA에 의해 보증되는 인증서와 인증서 폐기 목록을 저장하고 있는 CRL은 LDAP 디렉터리 서버에 저장되며, 인증서의 유효성 여부를 OSCP 장비에 의해 체크할 수 있다.

2) Zigbee Network (Coordinators[19] and sensors) :

[1] PANDA: Personal Authentication Network Device Architecture



<그림3> : PANDA의 블록 다이어그램

Zigbee 네트워크는 위치 기반 서비스 및 서비스 디바이스와 사용자의 PANDA의 신호세기를 측정하고 인증을 수행하는 역할을 담당하게 된다. 환경에 설치되어 있는 수많은 Zigbee 디바이스는 Coordinators 또는 서비스 디바이스로 구성되며 Coordinators는 PKI 프락시 서버에 의해 사용자의 인증연산을 수행할 수 있게 된다. 여기서 본 논문에서 제시한 PKI proxy는 Zigbee기반 PKI 인증연산을 수행하기 위한 TCP/IP와 Zigbee 사이의 프로토콜 컨버터로 동작하게 된다.

3) PKI Proxy : PKI Proxy는 Zigbee로 통신하는 서비스 디바이스가 PKI 인증 연산을 수행할 수 있도록 교량역할을 하게 된다. 각각의 Zigbee 디바이스는 인증에 필요한 최소의 기능을 담당하되 PKI 프락시 서버는 인증서, CRL 다운로드 및 인증서의 유효성 여부를 체크하는 역할을 담당하게 한다. 이와 같이 Zigbee 디바이스에서 발생되는 여러 인증 연산을 PKI Proxy에 위임을 시킴으로서 Zigbee 디바이스에서 발생될 수 있는 여러 병목현상을 제거할 수 있다.

4) PANDA : Zigbee 통신 모듈, 암호 연산 가속기와 RFID 기반 전원 관리 모듈이 장착되어 있는 초소형 보안 카드로서 보다 자세한 디자인은 다음 장에서 논한다.

만약 PANDA 소지자가 Zigbee와 RFID 리더기가 장착된 서비스 디바이스에 가까이 다가가게 되면 RFID 리더기는 PANDA의 전원 상태를 초절전 모드에서 인증 모드로 전환시키기 위한 제어 신호를 보내게 된다. 이때 PANDA는 인증 프로토콜을 수행하기 위하여 인증 모드로 전환하게 되고 인증 요청 메시지를 PKI 프락시 서버로 전송하게 된다. PKI 프락시 서버는 사용자의 인증을 수행하기 위하여 PKI에 접속하여 인증 연산을 수행하게 된다. 최종적으로 프락시 서버는 인증 연산에 대한 결과를 Zigbee 통신 모듈이 장착되어 있는 센서 노드에게 전달하게 된다.

4. PANDA 내부구조

이번 장에서는 PANDA의 내부구조에 대하여 분석한다. PANDA의 내부구조는 그림3에 도식되어 있다. PANDA는 전원공급시간의 장기화, PKI 기반 인증과 Ad-hoc 모드 통신을 제공하기 위하여 다음과 같은 구성요소를 가진다.

4.1 PANDA 구성 요소

PANDA는 여섯 부분으로 나눠진다. 그것은 RFID LF module과 전원 관리 모듈, 중앙처리 모듈, 암호 연산 가속기, Zigbee 통신 모듈, RS-232 to USB 변환 모듈로 구성된다.

1) 중앙처리장치 모듈 : 중앙처리장치 모듈은 마이크로프로세서와 메모리, 인증 시 필요한 S/W로 구성된다. 실제 구현에서는 ATmega128[20]을 채택하였고 마이크로프로세서에서는 인증 프로토콜을 수행하고 Zigbee 통신을 위한 Z-stack 프로토콜 및 유비쿼터스 서비스 제공을 위한 응용 S/W가 적재되어 있다.

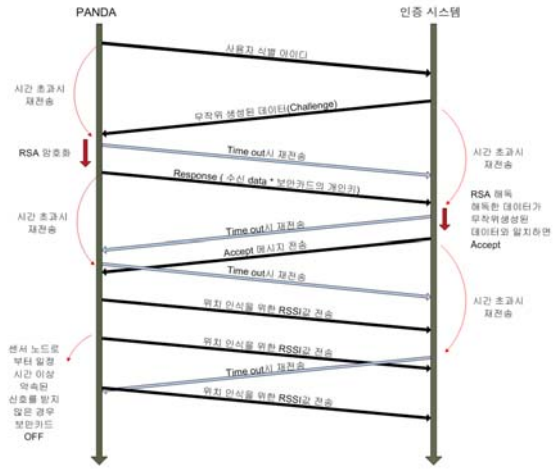
2) 암호 연산 가속기 : PANDA에는 ATMEL사에서 출시된 AT97SC3203S가 장착이 되었고 본 모듈에서는 PKI 기반 인증 시 필요한 RSA 알고리즘 및 Hash 함수 연산의 가속, 사용자의 인증서 및 개인키 저장을 담당하게 된다.

3) RFID LF module[21] : RFID의 안테나에 의해 작동되는 모듈로서, 사용자가 소지하고 있는 PANDA 내부 Zigbee의 MAC 주소와 PKI 인증 시 통신할 채널에 대한 정보를 RFID 리더기로 전송하고 그와 동시에 PANDA를 유휴상태에서 인증 모드로 전환시키는 신호 생성 역할을 담당한다.

4) 전원 관리 모듈 : PANDA의 전원 상태도를 기반으로 전원을 관리하는 기능을 담당한다. 전원 관리 모듈은 RFID LF 모듈로부터 수신한 신호에 따라 전원 상태를 이동하여 PANDA의 모드를 관리하고 통제하는 기능을 담당한다.

5) Zigbee 모듈 : 저전력 무선 통신과 동적인 ad-hoc 기능을 제공한다. 이를 통하여 본 논문에서 제시된 PANDA는 인증 연산을 Zigbee 네트워크를 통하여 수행하도록 하였으며 CC2420[22]을 적용하였다.

6) RS-232 to USB 변환 모듈 : RS-232 to USB 변환 모듈은 PANDA가 웨어러블 컴퓨터에 USB 디바이스의 형태로 장착되는데 사용된다.



<그림4> : PANDA의 인증 프로토콜 다이어그램

4.2 PANDA에서의 PKI 기반 인증

PANDA는 PKI 기반의 Challenge-response 프로토콜

Parameters	Description	Value
T_{Auth_ZigBee}	일반 Zigbee 디바이스의 인증 지연 시간	883.43ms
T_{Auth_PANDA}	PANDA의 인증 지연시간	456.45ms
$T_{Association\_Zigbee}$	일반 Zigbee 디바이스가 인증 시스템과 접속하는데 소요시간	760.00ms
$T_{Association\_PANDA}$	PANDA가 인증 시스템과 접속하는데 소요시간	333.02ms
T_{Comm}	일반 Zigbee 디바이스 또는 PANDA가 인증 프로토콜을 수행하는데 소요시간	123.43ms
T_{Comm_Smart}	스마트카드를 통해 인증 프로토콜을 수행하는데 소요시간	Avg.230ms‡
T_{Infra_delay}	보안 인프라에서 사용자의 신원을 검증하는데 소요시간	35.16ms†
T_{Beacon}	동기화된 메시지 송신을 위하여 기다리는 시간	Avg.250.00ms†
T_{CH}	채널 탐색 시 소요시간	Avg.210.00ms†
T_{ID}	사용자의 ID를 전송하는데 소요시간	Avg.7.81ms†
$T_{Challenge}$	Challenge 메시지를 전송하는데 소요시간	Avg.7.81ms†
T_{RSA}	1024bit RSA 알고리즘을 수행하는데 소요시간	100.00ms‡
$T_{RSA\_SmartCard}$	스마트카드에서 1024bit의 RSA 알고리즘을 수행하는데 소요시간[23]	230.00ms‡
$T_{Response}$	Response 메시지를 전송하는데 소요시간	Avg.7.81ms†
T_{MAC}	PANDA에서 MAC Address를 전송하는데 소요시간	33.00ms‡
T_{PMM}	전원 관리 모듈 지연 시간	0.02ms‡
T_{Assign_Addr}	PANDA 또는 일반적인 Zigbee 디바이스에서 주소를 할당하는데 소요시간.	300.00ms‡

<표1> : 각 디바이스의 인증 지연시간 측정을 위한 파라미터 값 정의

‡는 Spec상으로 측정된 값을 의미하며 †는 실험에 의해 측정된 값을 의미한다.

을 지원하며 이에 대한 흐름도는 그림4에 나타내었다.

1) PANDA 소지자는 RFID 안테나의 인지 범위에 들어가게 된다.

2) RFID LF 모듈은 PANDA의 MAC 주소와 사용자의 ID를 RFID 리더기로 전송하게 된다. RFID LF 모듈은 일반 Zigbee 디바이스가 통신 시 채널을 탐색하는데 발생하는 시간과 Beacon 지연 시간을 줄여준다.

3) PANDA에 부착되어 있는 RFID로부터 읽어온 데이터에 대하여 RFID 리더기는 서비스 디바이스에게 수신한 메시지를 전달한다.

4) 서비스 디바이스는 수신한 MAC 주소에 대하여 채널을 초기화 시키며 PKI 프락시 서버에게 PKI 인증시 필요한 사용자의 인증서와 CRL을 다운로드를 다운로드 받는다.

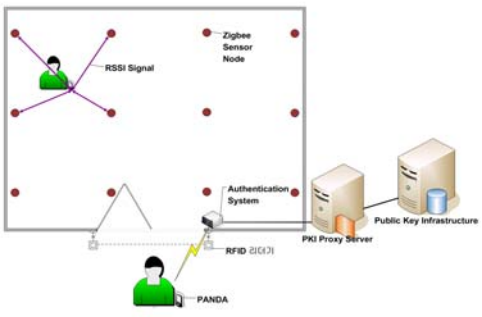
5) 서비스 디바이스는 챌린지 메시지를 생성하여 초기화된 채널을 통해 보낸다.

6) 사용자가 가지고 있는 PANDA는 챌린지 메시지를 자신의 개인키로 암호화 시킨다. 이때 PANDA 내에 있는 암호화 가속기를 이용하여 서명을 수행한다.

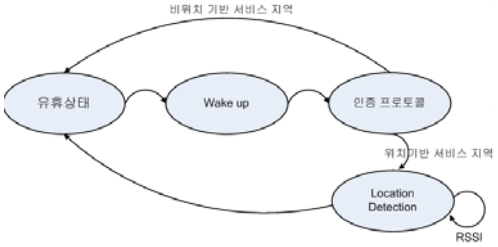
7) 서비스 디바이스는 사용자의 인증을 위하여 사용자에게 보냈던 챌린지 메시지와 응답 메시지를 PKI 프락시에게 전송한다.

8) PKI 프락시는 응답 메시지에 저장되어 있는 서명을 검증하여 인증 연산에 대한 결과를 서비스 디바이스에게 전송한다.

9) 인증 연산의 결과에 서비스 디바이스는 인증결과에 따른 서비스를 제공한다.



<그림5> : PANDA와 보안 인프라의 관계도



<그림6> : RFID 전원 관리 모듈의 상태도

4.3 RFID기반 전원 관리

PANDA와 보안 인프라의 메커니즘과 전원 관리 모듈 상태도가 그림5와 그림6에 각각 도시되었다. PANDA는 평상시 인증 연산이 없거나, 위치기반 서비스가 필요하지 않은 경우에는 유휴상태에 머무르게 된다. 유휴 상태에서 PANDA의 전원 관리 모듈은 전원공급 시간을 극대화하기 위하여 통신 모듈 및 중앙처리 모듈에 대한 전원공급은 차단된다. 이때, 서비스 디바이스에 부착되어 있는 RFID 리더기에 PANDA가 가까이 오게 되면, RFID 리더기는 PANDA에게 현재의 구역이 위치기반 서비스가 필요한 구간인지 아닌지에 대한 여부를 알려주게 된다. 이에 대하여 PANDA의 RFID LF 모듈은 수신한 정보를 PANDA 내의 전원 관리 모듈로 넘겨주게 되며, 전원 관리 모듈은 PANDA의 전원 관리 상태를 유휴 상태에서 wake-up 상태로 이동하게 된다. wake-up 상태에서 전원 관리 모듈은 PANDA의 통신 모듈과 중앙 처리 장치 모듈의 전원을 인가하게 되며, 인증 프로토콜 상태로 전환하게 된다. 이때 구동되는 중앙 처리 장치 모듈은 인증 프로토콜을 구동하기 위한 초기화를 수행하고 인증 프로토콜을 구동하게 된다. 인증 프로토콜이 수행된 후 RFID

$$L_{Zigbee} = \frac{C_{Bat} \times T_{\mathrm{Exp}}}{T_{AuthZigbee} \sum_{s=0}^{2} R_s (I_s + I_{MCU}) + T_{Loc} \sum_{S=0}^{1} R_s (I_s + I_{MCU}) + T_{Idle} (I_2 + I_{MCU})}.$$

s=0 Tx, s=1 Rx, s=2 Ziggee Idle mode (4)

$$L_{PANDA} = \frac{C_{Bat} \times T_{\mathrm{Exp}}}{T_{AuthPANDA} \sum_{s=0}^{2} R_s (I_s + I_{MCU}) + T_{Loc} \sum_{S=0}^{1} R_s (I_s + I_{MCU})}.$$

s=0 Tx, s=1 Rx, s=2 Ziggee Idle mode (5)

리더기로부터 받은 위치 정보에 따라 유휴 상태로 돌아가거나, 위치 정보 제공 상태로 이동하게 된다. 만약 인증을 받은 지점이 위치기반 서비스가 제공되는 지점이라면 인증 프로토콜이 수행된 후 위치 감지 상태로 이동하여 주기 적으로 RSSI 값을 Zigbee 센서 노드로부터 얻게 된다. 위치기반 서비스가 제공되지 않는 곳의 경우에는 다시 유휴 상태로 돌아가게 된다.

5. 성능 측정 및 모델링

이번 장에서는 PANDA의 성능을 측정하기 위한 모델링을 제시하고 이에 대한 결과를 제시한다. 각 모델링에 사용된 데이터는 Zigbee 스펙[17]과 실제 구현된 하드웨어의 측정치를 이용하여 인증 지연시간과 전원공급 지속시간에 대한 모델링을 하였다.

5.1 인증 지연시간.

인증 지연시간은 T_{auth}로서 이는 통신 결속 시간($T_{Association}$)과 인증 연산시 소요되는 통신시간 (T_{comm})과 인증 연산시 전송되는 정보의 전송에 소요시간(T_{Infra_delay})의 합으로 나타낼 수 있다.

$$T_{Auth} = T_{Asso} + T_{Comm} + T_{Infra\_delay}. \quad (1)$$

Smart Card와 일반 Zigbee 모듈에 대한 인증 지연시간은 수식 1에 근거하여 비교를 하였다. 측정시 사용되었던 파라미터는 표1에 나타내었다.

5.1.1 일반 Zigbee 장치에서의 인증 지연 시간

일반적인 Zigbee 장치는 Zigbee 네트워크 접속을 위하여 MAC 계층을 통한 채널 탐색을 수행하고 접속을 형성한다. Beacon을 사용하는 Zigbee 네트워크의 경우에는 동기적인 통신을 위하여, 최소한 개의 채널이 Beacon 프레임을 전송하기 위한 채널로 할당된다[24]. 그러므로 일반적인 Zigbee 장치에서의 인증 시간은 Beaconing에 의해 발생되는 지연시간 T_{Beacon} 과 채널 탐색 시간 T_{CH}에 의해 결정된다. 그러므로 일반적인 Zigbee Device에서의 인증 지연 시간은 다음과 같이 모델링 될 수 있다.

$$T_{Auth\_ZigBee} = T_{Asso\_Zigbee} + T_{comm} + T_{Infra\ delay},$$
$$T_{Asso\_ZigBee} = T_{Beacon} + T_{CH} + T_{Assign\_Addr},$$
$$T_{comm} = T_{ID} + T_{Challenge} + T_{RSA} + T_{Response}. \quad (2)$$

T_{Beacon}과 T_{CH} 은 0에서 주기까지 유니폼한 분포를 보이기 때문에 랜덤한 Beacon 지연시간과 채널 탐색시간의 평균으로 정의 된다. T_{comm}은 그림4에 나타나 있는 인증 프로토콜 다이어그램에 따라 T_{ID}, $T_{Challenge}$, T_{RSA}, 와 $T_{Response}$의 합으로 모델링 될 수 있다.

5.1.2 PANDA에서의 인증 지연 시간

PANDA는 4장에서 논의된 바와 같이 RFID기반의 전원 관리 모듈을 이용하여 접속시 필요한 정보를 RFID 리더기를 통해 전송하므로, 서비스 디바이스와의 접속시 소요시간은 RFID의 반응 시간(T_{MAC})과 전원 관리 모듈의 반응 시간(T_{PMM})에 의해 결정된다. 제안된 PANDA에서의 인증 지연시간은 다음과 같이 모델링 된다.

$$T_{Auth\_PANDA} = T_{Asso\_PANDA} + T_{comm} + T_{Infra\ delay}$$
$$T_{Asso\_PANDA} = T_{MAC} + T_{PMM} + T_{Assign\_Addr}$$
$$T_{Comm} = T_{ID} + T_{Challenge} + T_{RSA} + T_{Response} \quad (3)$$

수식 (2)에서 제시된 일반적인 Zigbee 장치의 접속시간과 비교하여, 제안된 PANDA에서의 접속 지연 시간(T_{ASSO_PANDA})은 460ms에서 33.015ms로 줄어들게 된다. 감소 요인은 다음과 같다.

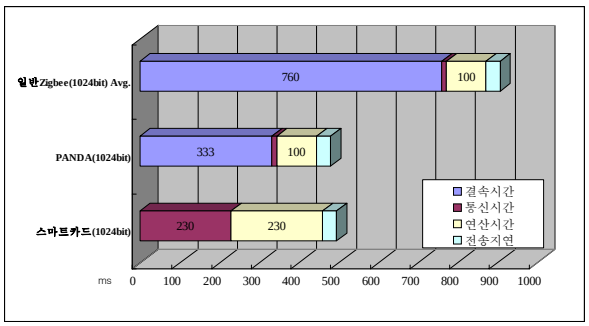
1) 고정된 Zigbee 인증 채널 할당 : 고정된 채널을 통한 인증은 채널 탐색으로 발생되는 오버헤드(T_{CH})를 없애는 효과를 보여준다.

2) Beaconing 지연 시간 제거 : 제안된 PANDA는 RFID 리더기로 자신의 MAC 주소를 전송하여 Beacon 프레임 없이 서비스 디바이스와 접속을 가능하게 만들어 준다.

5.1.3 각 모듈에서의 인증시간 비교

그림 7에서는 PANDA의 인증 지연시간의 감소를 일반적인 Zigbee 디바이스와 비교하여 보여준다. 일반적인 Zigbee 디바이스의 접속 시간은 매우 가변적이기 때문에 일반적인 Zigbee 디바이스의 평균 시간을 이용하여 제안된 PANDA의 인증 지연 시간을 비교하였다. 향상성은 190.96%까지 나타났고 평균적으로 88.92%의 인증 지연 시간의 감소를 볼 수 있다. 이전 장에 나타내었듯이, PANDA의 인증 지연 시간 감소는 고정된 인증 채널 할당과 Beacon 지연 시간의 제거에 기인한 것이다. 다른 한편으로 스마트카드의 인증 지연 시간은 제안된 PANDA보다 비슷한 지연 시간을 보여주고 있다. 결론적으로,

인증 지연 시간은 460ms에서 평균 33.015ms로 감소되는 것을 볼 수 있으며 이는 2장에서 제시되었던 시스템 요구사항과 부합된다.



<그림7> : PANDA와 일반 Zigbee 디바이스 및 스마트 카드의 인증 지연 시간 비교 그래프

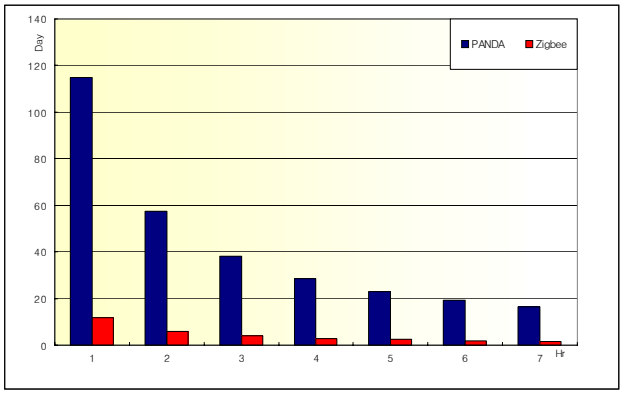
5.2 제안된 PANDA의 전원공급 지속시간

이번 장에서는 일반적인 Zigbee 디바이스와의 전원공급 지속시간을 비교한다. 측정된 전원공급 지속시간은 배터리의 용량과 각 디바이스의 전송 및 수신 모드, 유휴 상태의 비율에 대한 파라미터를 정의하여 이를 모델링 하였고 이를 위한 파라미터는 표2에 나타난다.

Parameters	Description
L_{PANDA}	PANDA의 전원공급 지속시간
L_{Zigbee}	일반 Zigbee 디바이스의 전원공급 지속 시간
T_{Exp}	측정된 전체 시간
T_{Loc}	측정 시간중 위치 기반 서비스가 제공 되는 시간
R_s	상태s의 비율
I_s	상태s에서의 전류 소비량
I_{MCU}	중앙처리장치에서의 전류 소비량
C_{Bat}	배터리 용량

<표2> : 전원공급 지속시간을 측정하기 위한 각 장치의 파라미터

일반적인 Zigbee 디바이스와 PANDA의 전원공급 지속시간에 대한 모델링은 수식 (4)와 (5)에 각각 제시되었다. 전원공급 지속시간을 모델링하기 위하여 3개의 상태(송신모드[Tx]와 수신모드[Rx]와 유휴상태[IDLE])로 나누어 모델링 하였다. 유휴상태(IDLE)는 Zigbee를 통해 통신을 하지 않는 시간을 의미하며 암호 연산 가속기와 중앙 처리장치는 가동이 될 수도 있고 되지 않을 수도 있다. 모델링을 하는데 있어서 전원 소비는 I_x로 모델링을 하였고 각 상태의 비율은 R_s로서 모델링을 하였고 이를 전원공급장치의 용량(C_{BAT})에 근거하여 측정 하였다. 수식(4)에서는 사용자는 인증 및 위치 감지 연산이 필요하지 않은 상태임에도 불구하고 ZigBee 모듈과 중앙 처리 장치 모듈에서는 파워가 소비되는 것을 볼 수 있다(I_2+I_{MCU}). 그러므로 일반 Zigbee 디바이스는 유휴상태에서의 전력 소모로 인하여 전원 지속시간이 떨어지는 것을 볼 수 있다. PANDA에서는 (수식5) 유휴상태시 전원 소모가 전혀 이루어 지지 않는 것을 볼 수 있다. 이는 PANDA의 전원 관리 모듈에서 유휴 상태시 PANDA의 모든 구성요소에 대한 전원을 차단시키는 것에 기인한다. 실제 환경에서 인증 프로토콜 구동시에만 전원의 인가가 필요하므로 PANDA의 유휴상태의 비율을 매우 높다. 그러므로 전원 관리 모듈은 유휴 상태에서의 전원을 차단시킴으로서 전원공급 지속시간을 극대화 시킨다. 그림 8은 본 논문에서 제시한 전원 관리 모듈에 따른 전원공급 지속시간의 향상도를 보여준다. 가로축은 사용자의 하루당 활동 시간을 나타내며, Y축은 전원공급 지속시간을 나타낸다. 그림8에 나타낸 측정 수치는 사용자가 시간당 10번의 인증을 수행한다고 가정하였고 전체 서비스 구역 중 10%가 위치기반 서비스가 제공된다고 가정을 하였다. 전원공급 지속시간은 10배 이상 향상된 것을 볼 수 있다.



<그림8> : 일반 Zigbee 디바이스와 PANDA의 전원공급 지속시간 비교 그래프

6. 결 론

본 논문에서는 유비쿼터스 환경에 최적화된 PANDA를 제시하였고 인증 지연시간과 전원공급 지속시간을 극대화시키기 위한 메커니즘을 제시하였다. 본 논문에서는 제시된 저전력 메커니즘과 인증 지연 시간 단축에 대한 성능을 측정하기 위하여 모델링을 하였다. 본 논문에서의 측정 결과에 따르면 다음과 같은 사실을 알 수 있다.

1) 본 논문에서 제시된 RFID 기반의 전원 관리 기법과 고정된 인증 채널은 일반적인 Zigbee 디바이스와 비교하여 월등한 전원공급 지속시간을 보여준다.

2) 제안된 PANDA의 인증 지연시간은 접촉형 스마트카드와 비슷한 반면 Ad-hoc 통신 기능과 위치 기반 서비스 제공이 가능하며, 일반 암호 연산 가속기를 갖춘 디바이스에 비해 평균 2배 정도 빨라진 것을 확인 할 수 있다.

참고문헌

[1] S. L. Jason I. Hong, Jennifer D. Ng and J. A. Landay, “Privacy risk models for designing

privacy-sensitive ubiquitous computing systems," in Proceedings of the 2004 conference on Designing interactive systems: processes, practices, methods, and techniques, 2004.

[3] K. H. Park and U. P. Group, "Ufc: A ubiquitous fashionable computer," in Internation Conference on Next Generation PC, October 2005.

[4] J.-W. Yoo, W.-M. Hwang, S.-H. Baek, and K.-H. Park, "Intuitive interface device for wearable computers,"in Internation Conference on Next Generation PC, October 2005.

[5] K.-W. Park, H.-J. Choi, and K. H. Park, "An interoperable authentication system using zigbee-enabled tiny portable device and pki," in International Conference on Next Generation PC, October 2005.

[6]S.C.Alliance,"http://www.smartcardalliance.org/2006".

[7] J. Myers, RFC 2222: Simple Authentication and Security Layer(SASL). The Internet Society., 1997.

[8] NIST, Entity Authentication Using Public Key Cryptography. FIPS,1997.

[9] I. 9798-3, Entity authentication mechanisms - Part 3: Entity authentication using a public key algorithm. ISO., 1993.

[10] C. Consultannts, Single-chip ZigBee for Indoor Mobile Telemetry. Cambridge Consultannts, 2005.

[11] Z. Alliance, "http://www.zigbee.org/en/index.asp", 2005.

[12] B. D. Noble and M. D. Corner,"The case for transient authentication,"in Proceedings of the 10th ACM SIGOPS European Workshop, September 2002.

[13] C. E. Landwehr,"Protecting unatteded computers without software,"in Proceedings of the 13th Annual Computer Security Applications Conference, 1997.

[14] M. Norris, Location monitoring with low-cost ZigBee devices. Embedded Control Europe, 2006.

[15] ATmel, AT97SC3203 Datasheet. ATmel co, Ltd., 2005.

[16] S. L. Viipull Guptta, Sizzle: SSL on Motes. Sun microsystems., 2005.

[17] Z. A. B. of Directors, ZigBee Specification v1.0. ZigBee Alliance, 2005.

[18] E. S. Hall, D. K. Vawdrey, and C. D.Knutson, "Reducing power and inquiry costs in bluetooth-enabled mobile systems," in Proceedings of International Conference on Computer Communications and Networks, October 2002.

[19] Chipcon, ZigBee Implementer's Guide. Figure 8 Wireless., 2005.

[20] ATMEL, ATmega128(L) Datasheet : 8-bit Microcontroller with 128K Bytes In-System Programmable Flash. ATMEL., 2005.

[21] T. Instruments, Three Channel LF Transceiver(3D AFE) TMS37122 DataSheet. Texas Instruments., 2005.

[22] Chipcon, CC2420 Datasheet 2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver. Chipcon., 2004.

[23] Infinion, infinion SLE66 DataSheet. Infinion., 2006.

[24] J.-S. Lee, "An experiment on performance study of ieee 802.15.4 wireless networks," in Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation, Catania, Italy, vol. 2, 2005, pp. pp. 451-458.