유비쿼터스 환경을 위한 다중 사용자 기반의 안전하고 효율적인 무선 네트워크 관리 기법 제안

서 대 희[†] · 이 임 영[††]

요 약

최근 새로운 형태의 네트워크 환경인 유비쿼터스 컴퓨팅에 대한 연구가 활발하게 진행되고 있다. 특히 유비쿼터스 컴퓨팅에서 중요한 요소는 센서 네트워크로써, 저전력 Ad-hoc 네트워크에 기반한 센서와 센서 노드들로 구성되며, 실제의 환경과 유비쿼터스 컴퓨팅과의 매개 역할을 한다.

현재의 유비쿼터스와 관련된 연구는 주로 RFID를 이용해 경량화된 하드웨어를 통한 네트워크 관리에 대한 연구가 진행중에 있다. 그러나 실생활에 적용하기 위해서는 보다 현실적인 시나리오와 더불어 안전성과 효율성을 고루 갖춘 보안적인 연구가 필수적으로 요구되고 있다. 따라서 본 논문에서는 현재 연구가 진행중인 RFID 이외에 개인 네트워크에서 가장 많은 활용성을 제공하고 있는 PTD를 기반으로 다중 사용자들의 무선 네트워크 구성하고 이를 관리하는 방식을 제안하고자 한다.

제안된 방식은 사용자 주변의 신뢰된 기기를 기반으로 무선 네트워크에서 요구되는 다양한 서비스와 관련된 보안과 효율성을 높이기 위한 방식으로 기존 논문에서 전자 상거래에 사용하던 PTD를 이용해 다양한 서비스를 제공하고 임시 그룹을 설정하여 동적인 환경에 적합한 관리 방식을 제안하였다.

키워드 : 유비쿼터스, 무선 네트워크, 네트워크 관리, 신뢰된 개인용 디바이스

A Study on Secure and Efficient Wireless Network Management Scheme based Multi users for Ubiquitous Environment

Dae-Hee Seo[†] · Im-Yeong Lee[††]

ABSTRACT

Ubiquitous computing, a new type of network environment, has been generating much interest recently and has been actively studied. In ubiquitous computing, the sensor network, which consists of low electric power ad-hoc network-based sensors and sensor nodes, is particularly the most important factor. The sensor network serves as the mediator between ubiquitous computing and the actual environment.

Related studies are focused on network management through lightweight hardware using RFID. However, to apply these to actual environment, more practical scenarios as well as more secured studies equipped with secures and efficiency features are needed. Therefore, this study aims to build a wireless network based on PTD for multi users, which provides the largest utility in individual networks, and propose an appropriate management method.

The proposed method is designed to enhance security and efficiency related to various services required in wireless networks, based on the reliable peripheral devices for users of PTD. Using PTD, which has been applied to electronic commerce transactions in existing papers, this study also proposed an appropriate management method that is suitable for a dynamic environment and setting a temporary group to provide various services.

Key Words : Ubiquitous Environment, Wireless Network, Network Management, PTD

1. 서 론

유비쿼터스 네트워크 환경의 특징이 사용자 중심으로 한 주변 상황이나 환경을 네트워크가 지능적으로 파악하여 사용자 네트워크 환경을 최적화한다. 또한 컨텐츠 사용이 자유롭고, 안전하게 사용할 수 있는 네트워크가 마련되는 것을 특징으로 하고 있다. 유비쿼터스 네트워크를 구성하는 기술로는 유비쿼터스 플렉시블 광대역, 유비쿼터스 텔레포테이션, 유비쿼터스 에이전트, 컨텐츠, 어플라이언스, 유비쿼터스 플렛폼 및 유비쿼터스 센서망 등이 있다. 이들중 유비

※ 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구 결과로 수행되었음.
† 준 회 원 : 순천향대학교 전산학과 박사과정
†† 종신회원 : 순천향대학교 정보기술공학부 교수(교신저자)
논문접수 : 2005년 9월 28일, 심사완료 : 2005년 12월 21일

쿼터스 센서망은 사용자 주변의 유무선 기기가 통신을 수행함으로써 자율적으로 정보를 수집하고 관리하는 필수 구성요소이다.

현재 대중화된 단말기인 노트북, PDA(Personal Digital Assistant), 핸드폰 등은 휴대용 단말기로 향후 최소형화된 칩으로 모든 환경에서 분산 존재할 경우 각종 정보를 취득/저장하여 이용자의 요구에 따라 자유롭게 분배하여 이용할 수 있다. 이와 같이 무선 네트워크 측면에서는 소형화된 디바이스를 이용한 연구가 진행되고 있으며, 최근엔 RFID (Radio Frequency Identification)를 이용해 네트워크를 구성하고 관리하는 연구들이 활발하게 진행되고 있다. 그러나 초소형화된 기기를 이용할 경우 보안적인 측면에서 제한적인 서비스만이 가능하며, 이로 인해 발생될 수 있는 취약성은 사용자 프라이버시 보호에 한계성을 가질 밖에 없다[7].

따라서 현실적인 측면에서 가장 많이 활용되는 모바일 폰 기반의 연구는 적용성과 안전성을 고루 갖춘 연구라 할 수 있다. 특히, 사용자의 신뢰된 디바이스로 무선 네트워크를 구성할 경우 동일한 공간에 다양한 사용자가 네트워크 형성이 가능하고 사용자 프라이버시 정보를 구성하고 관리할 수 있을 뿐만 아니라 기존의 RFID와 같은 소형화 디바이스 연구와는 차별화된 서비스를 제시할 수 있다.

따라서 본 제안방식 2장에서는 유비쿼터스에서 사용되는 무선 네트워크에 대한 일반적인 개요를 살펴보고 3장에서는 PTD(Personal Trust Device) 기반의 무선 네트워크가 형성되었을 경우의 보안적인 요구사항을 제시하고자 한다. 4장에서는 PTD 기반의 기존 네트워크 관리 방식을 분석한 뒤 5장에서는 3장에서 제시한 보안 요구사항을 만족할 수 있는 다중 사용자 기반의 안전하고 효율적인 무선 네트워크 관리 구조를 제안하고, 6장에서는 제안 방식을 분석한 뒤 마지막으로 7장에서 결론을 맺도록 한다.

2. 유비쿼터스 무선 네트워크와 PTD의 개요

본 장에서는 유비쿼터스 무선 네트워크와 PTD에 대한 기술적 개요를 기술하고자 한다.

2.1 유비쿼터스 무선 네트워크 개요

유비쿼터스 환경은 누구나 언제, 어디서나 어떠한 경로를 통해서라도 자신이 원하는 일을 처리할 수 있도록 모든 IT 디바이스가 유무선 네트워크로 연결된 서비스를 제공한다. 웨어러블 컴퓨팅과 네트워크의 이동성을 극대화해 어디서든 컴퓨터를 사용할 수 있게 하는 노매디(Nomadic)컴퓨팅, 그리고 모든 사물에 컴퓨터를 이식해 도처에 컴퓨터가 편재될 수 있도록 하는 퍼베시브(Pervasive)컴퓨팅 등이 그 사례이다.

유비쿼터스 네트워크는 휴대전화 및 PDA, 노트북등을 가지고 실내 및 실외에 관계없이 통신이 가능한 네트워크 환경을 의미한다. 따라서 모바일 디바이스가 근거리에서 인터넷 망 또는 주변 네트워크에 언제 어디서든 통신하고 빠른 시간에 네트워크를 형성하기 위한 기술들이 요구되며, 이와 관련된 연구로는 802.11, Bluetooth, HomeRF(Home Radio Frequency), WPAN(Wireless Personal Area Networks)등의 기술이 연구되고 있다.

그러나 802.11, Bluetooth, HomeRF 등의 근거리 무선 통신 기술들은 사용자가 증가하면서 사용자간의 충돌성과 이로 인해 발생되는 서비스의 질 저하 문제 뿐만 아니라 서비스의 종류에 따라 지원이 불가능하다. 또한 보안적인 측면에서 ACIN(Authentication, Confidentiality, Integrity, Non-repudiation)과 관리 측면에서의 문제성이 지적되고 있다.

이를 보완하기 위해 WPAN에서는 기존의 근거리 무선 통신들의 차별성을 통합화하고 사용자 주변의 무선 네트워크 구축을 위한 연구로서 현재 IEEE(Institute of Electrical and Electronics Engineers) 802.15에서 표준화가 이루어지고 있다.

그러나 보안적인 측면에서는 많은 연구가 진행되고 있지 않다. 따라서 사용자 프라이버시 보호 서비스가 이루어지지 않을 경우 증가되는 정보의 양에 따라 조작된 정보나 불법적인 정보에 대한 취약성으로 발생되는 문제는 매우 크다고 할 수 있다. 현재 유비쿼터스에서 무선 네트워크 구성시 서비스 측면과 보안적 측면을 모두 고려한 연구가 요구되나 이를 위한 연구는 매우 미흡한 실정이다. 이는 다양한 서비스를 고려한 보안 서비스를 제공하기 위한 연구가 고려되지 않았기 때문이다[2, 7].

2.2 PTD의 개요

인터넷의 고도화는 모바일 환경에 대한 급속한 발전을 이루고 있다. 이와 관련하여 RUIM(Removable User Identity Module), GPS(Global Positioning System), MPEG4(Moving Picture Experts Group 4), Bluetoooth등 모바일 디바이스를 이용한 새로운 기술이 등장하고, 표준화가 이루어지고 있다.

특히, 모바일 디바이스의 경우 사용자 중심으로 다양한 데이터를 처리하는 보편적 기기로 개인정보 데이터를 처리하는 중요한 하드웨어 장치이다.

모바일 디바이스는 사용층과 목적에 따라 단순한 음성통화에서 고속 컴퓨팅 기능을 탑재한 PDA(Personal Digital Assistant)에 이르기까지 더욱더 세분화되고 다양해 질 전망이다. 따라서 다양한 디바이스의 플랫폼을 효율적으로 수용할 수 있는 범용적인 통합 환경의 구현 및 OEM(Original Equipment Manufacturer) 사양의 대응을 위한 개방형 설계와 더불어 사용자 프라이버시 보호를 위한 서비스가 고려되어야 한다[3, 11].

MeT(Mobile Electronic Transactions)에서 안전한 모바일 통신을 위해 제시된 PTD(Personal Trusted Device)는 사용자의 신뢰할 수 있는 디바이스를 의미하며 무선 통신상에서의 안전성을 제공해 줄 수 있다고 정의하고 있다.

따라서 기존의 모바일 디바이스가 무선 통신상에서 안전한 서비스를 제공하기 위해서는 공개키 암호 알고리즘의 적용과 더불어 WAP(Wireless Application Protocol)과 같은 프로토콜 적용이 필수적으로 요구된다. 이에 WAP 포럼에서

는 사용자의 프라이버시 보호를 위한 모바일 디바이스를 암호 알고리즘이 내장되고 이에 기반한 보안 프로토콜을 적용시킬 수 있는 모바일 디바이스를 PTD로 규정하여 이를 위한 연구가 진행중에 있다[4, 16].

MeT에서 제시되는 PTD는 모바일폰으로 개인키와 같은 중요 데이터에 대한 보관 뿐만 아니라 개인에 대한 인증용으로 사용하여 뱅킹, 지불, 보너스 프로그램과 같은 응용프로그램 플랫폼에서 활용 할 수 있는 디바이스를 의미하며, 추가적으로 사용자 ID에 기반해 전송 데이터에 대한 인증과 인가 과정을 수행할 수 있는 모바일 디바이스를 의미한다.

이에 WAP 포럼에서는 PKI(Public Key Infrastructure)와 WPKI(Wireless Public Key Infrastructure)와 같은 어플리케이션을 PTD에 적용시키기 위해서 하드웨어적 측면에서는 작은 컴퓨팅 CPU와 메모리 그리고 제한된 소비 전력과 디스플레이등을 제시하고 있다. 또한 보안적 측면에서는 키의 생성과 등록, 사용자의 인증과 관리, 암호화/복호화 메시지의 전송과 수신등을 고려한 연구가 진행중에 있다[4].

3. 유비쿼터스 무선 네트워크 보안 사항

본 장에서는 유비쿼터스 무선 네트워크에서 보안의 필요성과 요구되는 보안 요구사항에 대해 논하고자 한다.

3.1 유비쿼터스 무선 네트워크에서 보안의 필요성

유비쿼터스 네트워크는 사용자의 프라이버시 뿐만 아니라 비즈니스, 나아가 사회 전반을 변화 시킬 수 있는 가장 큰 핵심 요소 기술이다.

유비쿼터스 환경의 특성상 모든 컴퓨터와 사물이 하나로 연결된 네트워크로서 누구든지 사용자의 정보에 접근할 수 있다. 이와 같이 고도화된 네트워크 환경의 보안적 취약점은 고의적인 제 3자의 공격자로부터 정보 도용을 통한 프라이버시 침해로 이어질 수 있다는 것이다[2], [6]. 그러나 유비쿼터스 네트워크에서 보안 기술을 적용하기 위해서는 하드웨어적으로 제한된 시스템에 보안 서비스를 제공해야 하기 때문에 일반적인 인터넷 환경에서 제공되는 보안 서비스보다 구현하기 어려운 측면도 있다.

따라서 유비쿼터스 네트워크와 같은 새로운 환경에서 기술적인 효율성과 더불어 안전성에 대한 문제가 선행되어 연구되지 않는다면 여러 가지 사회 문제로 양산될 수 있다.

3.2 PTD를 이용한 네트워크 관리의 보안 요구사항 분석

유비쿼터스 네트워크가 사용자 중심으로 구성될 경우 사용자 프라이버시 정보를 이용한 통신을 수행할 수 있다. 특히, 모바일 디바이스의 특성상 나타날 수 있는 정보 시스템과의 연계성으로 인해 사용자 주변의 모바일 디바이스인 PTD는 자율적인 정보를 수집하고 관리하는 구성요소가 반드시 필요하다.

그러나, 모바일 디바이스의 소형화에 따른 물리적인 경량성(낮은 전력과 연산량, 적은 메모리 등등)은 보안적인 연산을 수행할 경우 다양한 요구사항이 고려된다. 따라서 본 논문에서는 기존 방식과 차별화된 유비쿼터스 기반의 다중 사용자를 위한 안전하고 효율적인 네트워크 관리 기법 제안을 위해 다음과 같은 요구사항을 제시한다.

- 상호 인증 : 사용자 중심으로 이루어지는 무선 네트워크의 경우 이동 단말과 인증 서버 혹은 게이트웨이와의 상호 인증을 통해 안전성을 유지할 수 있어야 한다.
- 기밀성과 무결성 : 네트워크 구성 개체간에 사용자 프라이버시 정보를 전송할 경우 전송되는 데이터에 대한 기밀성과 무결성을 제공하여 전송 데이터에 대한 안전성을 유지할 수 있어야 한다. 또한 PTD에 저장된 데이터를 위한 보안 서비스도 반드시 고려되어야 한다.

* 저장 데이터에 대한 기밀성 : 트래픽 보안이 무선 트래픽 상에서 기밀성을 보호하는 것이라면 유비쿼터스 무선 네트워크에서 저장되는 정보에 대한 기밀성 역시 매우 중요하다. 예를 들어 PTD를 분실하였을 경우 패스워드로 PTD 자체를 보호한다 할지라도 PTD에 저장된 정보가 암호화 되지 않고 저장되기 때문에 PTD에 대한 정보를 기반으로 있는 공격자는 저장된 정보를 획득할 수 있다.
* 전송 데이터에 대한 기밀성과 무결성 : 유비쿼터스 무선 네트워크에서 데이터의 전송과 수신에서 전송 메시지의 기밀성과 무결성을 제공하지 않는다면 개인 프라이버시 정보에 매우 취약한 서비스를 제공할 수 밖에 없다. 따라서 이와 관련된 전송 데이터에 대한 보안 서비스가 반드시 요구된다.

- 상태 획득 기술 : 모바일 디바이스 간에 상태가 변경됨에 따라 통신이 설정될 수 있는지를 결정하는 기술로써 다른 디바이스들과의 안전한 정보 전송을 기반으로 정보를 획득하는 기술을 제공해야 한다.
- 자동 서비스 생성 방안 : 일정한 통신량의 이용 빈도가 높을 경우 안전한 형태의 임시 그룹으로의 변환이 가능해야 하며, 일정한 통신량 이하의 서비스 빈도가 나타날 경우 자동적인 임시 그룹 해체 과정을 제공할 수 있어야 한다.
- 효율성 : 모바일 디바이스의 특성상 보안 서비스에서 요구되는 연산의 계산량을 최소화하여 디바이스의 효율을 극대화 시킴으로써 전체 네트워크의 효율성을 높이는 방안이 필요하다.

4. 기존 방식 분석

본 장에서는 기존의 PTD에 기반한 무선 네트워크 관리 기법에 대해 3장에서 제시한 보안 요구사항으로 분석하고자 한다.

4.1 WAP 포럼 방식

WAP 포럼에서는 PTD에 기반한 응용 어플리케이션 개발 연구를 추진하고 있으며, 특히 WTLS(Wireless Transport Layer Security)에 적용하기 위한 연구를 진행하고 있다.

WAP 모델에서는 휴대 단말기와 인터넷 서버 사이에 WAP Proxy라 불리는 WAP Gateway를 두도록 하고 있다. WAP Gateway의 주요 역할은 WAP 프로토콜과 인터넷 TCP/IP 프로토콜을 중간에서 변환해 주는 것이다. 즉, 모든 휴대 단말기의 인터넷 서비스 요구는 WAP Gateway를 거치도록 되어 있고, WAP Gateway는 요청 받은 서비스를 기존 유선 인터넷 망을 통해 다시 서비스를 요청한다. 이에 WAP Gateway가 인터넷 서버로부터 응답을 받고 다시 서비스를 최초 요청했던 휴대 단말기에게 WAP 프로토콜로 전송함으로서 모든 과정이 이루어진다[16]. 그러나 다음과 같은 취약성을 지적할 수 있다.

① 그룹의 자동 서비스 생성 : WAP 포럼에서 제시한 방식의 경우 단순히 개체들간의 통신상의 안전성을 목표로 구성되었다. 따라서 네트워크 구성 이후에 관리 측면에서의 보안 서비스는 고려되지 않았다.

② 상호 인증 : 익명 키 교환의 경우 서버와 사용자가 상호 인증을 수행하지 않아 위장 공격의 위험성을 내포하고 있다.

③ PTD와 서비스 제공자의 보안 : PTD를 WAP 프로토콜에 사용할 경우 추가적인 서비스나 안전한 인증 서비스를 제공할 수 없다. 이는 고려되는 PTD가 WTLS에서 요구되는 키 설정과 인증 과정 이후에 어떠한 보안 서비스도 제공하지 않기 때문이다.

4.2 무선 네트워크상의 정책 기반 네트워크 관리 방식

Leonida등이 제안한 방식으로 이동 IP 환경에서 정책 기반의 네트워크 구성과 동작 절차를 제안하였다[4]. 제안된 방식은 정책 클래스를 기반으로 정책 시나리오를 구성하고 이를 차별화 서비스 네트워크를 구현하기 위한 방식이다. 이는 내부 네트워크와 외부 네트워크를 기준으로 에이전트를 설치해 분석과 감시 기능을 수행하도록 제안되었다.

그러나 본 방식은 다음과 같은 문제성을 내포하고 있다.

① 그룹 자동 서비스 생성 : 제시된 방식에서 에이전트는 내부 정책을 전달하고 관리하는 모바일 개체로 규정하고 있다. 따라서 그룹을 구성하는 개체들은 정책에 관련된 내용을 전달받고 이를 수행한다. 따라서 그룹 내부의 자동적 서비스는 제공되지 않고 중앙서버의 정책에 따라 수동적인 보안 서비스만을 제공하여 내부 공격자에 의한 공격이 수행될 경우 전체적인 네트워크 마비가 발생할 수 있다.

② 상태 획득 기술 : 제안된 방식은 관리자로부터 전송된 정책을 업데이트 함으로써 새로운 공격에 대한 안전성을 보장받고자 하였다. 그러나 유비쿼터스에 적용되기 위한 무선 네트워크에서는 내부 개체의 상태를 파악하고 이를 자동적으로 획득할 수 있는 기술이 필수적으로 요구된다. 따라서 모바일 디바이스의 상태가 변동되었을 경우 이를 확인할 수 있는 방안을 제공하지 못하는 취약성이 존재한다.

③ 기밀성과 무결성 : 제시된 방식은 에이전트와의 통신과정에서 단순한 감시와 분석에 대한 내용을 수행한 결과만을 송수신한다. 따라서 이와 관련된 정보가 노출 될 경우 공격자는 새로운 형태의 공격 수행이 가능하다. 따라서 송수신 데이터 뿐만 아니라 새로운 정책 전달에 따른 기밀성과 무결성 서비스가 필수적으로 요구된다.

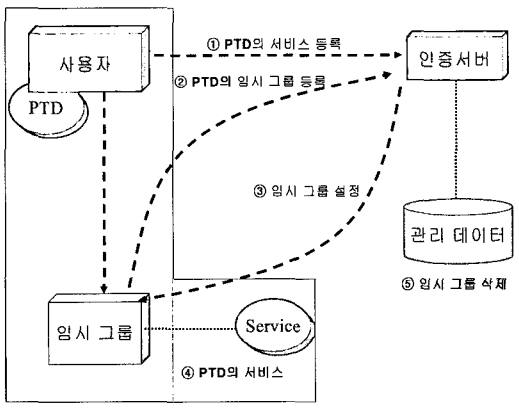
5. 다중 사용자를 위한 안전하고 효율적인 네트워크 관리 구조 방식 제안

유비쿼터스 환경에서는 홈 네트워크와 같이 소규모화된 네트워크 뿐만 아니라 동일한 공간에 많은 사용자들이 이용할 수 있는 공간이 존재할 수 있다. 따라서 다중 사용자들을 위한 공간이 구성될 경우 이를 네트워크로 구성하고 다양한 서비스들을 관리할 수 있는 방식이 요구된다. 따라서 본 논문에서는 다중 사용자를 위한 네트워크 관리 구조 제안을 위해 다음과 같은 시나리오를 제시하고자 한다.

- 일반적인 WPAN(Wireless Personal Area Network)보다는 크고 WLAN(Wireless Local Area Network)보다는 작은 형태로 구성된 네트워크에서 다중 사용자들이 통신을 요구하는 환경이다.
- 다중 사용자들이 동일한 공간에서 활동할 경우(도서관, 극장) 서로 다른 사용자들에 대한 관리가 요구된다.
- 각 사용자들은 신뢰된 모바일 디바이스인 PTD를 소유하고 있다.
- 구성된 네트워크는 수 Mbps 엑세스 링크를 지원하며, 끊김없는 네트워크 접속이 가능하다.

5.1 제안 방식 시나리오

제안 방식은 무선 통신 기능을 갖는 PTD를 소유하고 있는 다수의 사용자들이 무선 네트워크 기반으로 정보 수집을 통해 개인의 프라이버시 정보와 관련된 PTD 어플리케이션 서비스(전자 결재, 인증 등)를 인증 서버에서 이와 관련된 서비스를 등록받고 다중 사용자 네트워크가 구성된 이후 이를 관리하기 위해 지속적인 서비스를 수행하는 과정으로써 제안 방식의 내부 흐름도는 (그림 1)과 같다.



(그림 1) 제안방식 시나리오

① 사용자는 PTD를 기반으로 제공 가능한 서비스를 인증 서버에 등록한다.
② 동일한 서비스를 요구하는 사용자가 다수일 경우를 위한 PTD의 임시 그룹 초기 등록 단계를 수행한다.
③ 인증서버는 동일한 서비스를 요구하는 다수의 사용자에 대한 임시 그룹을 설정한다.
④ 임시 그룹으로 설정된 PTD들의 동일한 서비스 제공을 위한 안전한 통신 과정을 수행한다.
⑤ 동일한 서비스에 대한 서비스가 종료될 경우 인증 서버는 관리 데이터 저장소에서 임시 그룹에 대한 정보를 삭제한다.

제안 방식의 시나리오에서 각각의 개체 및 의미는 다음과 같은 수행 역할을 수행한다.

- 사용자 : 사용자는 PTD를 소유하고 있으며, 인증 서버와 인증을 수행한 후, 서비스를 생성 및 상태를 획득하는 개체.
- 임시 그룹 : 임시 그룹은 동일한 서비스를 요구하는 PTD들이 일정한 개수 이상일 경우 인증 서버에서 생성한 그룹.
- 서비스 : 제안 방식 시나리오에서의 서비스는 사용자 프라이버시 정보가 요구되는 어플리케이션 서비스로서 PTD를 통해 제공.
- 인증 서버 : 유비쿼터스 네트워크 기반의 다중 사용자 소유의 PTD와 상호 인증과정을 수행하는 개체로써 생성한 서비스를 제공하기 위해 게이트웨이와 연동되어 있는 무선 네트워크상의 개체(인증서버는 사전에 PTD의 *ID*리스트를 저장하고 있다).

5.2 시스템 계수

다음은 PTD 기반의 안전하고 효율적인 무선 네트워크 관리를 제안하기 위한 시스템 계수를 기술한다.

(* : S PTD (PTD는 (PTD_1, PTD_2,....,PTD_N)로 구성되며 해당 PTD의 ID는($S_1, S_2, ..., S_N$)), A 인증서버)

n, g : 공개 계수($n = pq$, p : 소수, q : $q|p-1$)

(P_S, Q_S) : PTD의 공개키 개인키 쌍

m_i : 서버에서 사전에 정의 내려져 있는 서비스 고유값으로 PTD와 인증서버가 안전하게 공유한 값 (i=1,...,N)

c_i : 인증 서버에서 m_i를 기반으로 생성된 서비스 제공을 위한 중간값으로 m_i와 일대일 대응 테이블로 저장되는 값

M_0, M_1 : 암호 통신이 필요한 임시 그룹 서비스 요청 메시지

$E()$, $D()$: 암호화, 복호화 함수

r_*, α_*, β_* : 랜덤 수

M_C : 암호화 통신이 필요한 단일 어플리케이션 서비스 메시지

T_* : 타임 스탬프

ID_* : 해당 개체의 ID

M_0, M_1 : 암호 통신이 필요한 그룹 어플리케이션 서비스 요청 메시지

5.3 제안 프로토콜

제안 방식은 특수한 무선 환경이 제공되지 않는 네트워크 상태에서 다수의 모바일 디바이스가 PTD일 경우 이를 이용해 무선 네트워크를 구성하고 안전하고 효율적인 관리 구조를 위해 다음과 같은 흐름을 갖는다.

[Step 1] PTD 1의 서비스 등록 단계(다수의 PTD들중에서 PTD1이 인증 서버에 서비스를 등록하는 단계)

다음 과정은 인증 서버가 PTD들의 서비스 형태를 등록하는 과정을 수행한다.

① 인증 서버는 랜덤하게 선택된 $\alpha_A \in_U Z_n$(n과 서로소인 랜덤수)를 생성하여 c_i(c_i는 m_i와 일대일 매칭되는 고유값)를 계산한 후 이를 모든 PTD들에게 브로드캐스팅한다.

$$c_i = m_i^{\alpha_A} \bmod n \ (\text{i=1,2,....,n})$$

② 임의의 PTD 1은 서버로부터 전송된 c_i 로부터 현재 PTD 1에서 제공할 수 있는 서비스의 고유 번호를 선택한 후 (3개의 서비스를 선택한다면) 이것을 c_1, c_2, c_3라 정의한다. 서비스 형태를 정의내린 PTD 1은 (β_1, β_2, β_3)$\in_U Z_n$(n과 서로소인 랜덤수)를 선택하여 d_i를 계산한 뒤 서버에 전송한다.

$$d_i = c_i^{\beta_i} \bmod n \ (= m_i^{\alpha_A \beta_i} \bmod n) \ (\text{i=1,2,3})$$

③ 인증 서버는 $s = \alpha_A^{-1} \bmod n$을 생성한 뒤 PTD 1의 공개키로 v를 계산하여 이를 PTD 1에 전송한다.

$$v = E_{P_S}(s \| T_A)$$

④ PTD 1은 v를 개인키 Q_{S_1}로 복호화한 후 $t_i = \beta_i^{-1} \bmod n$를 계산하여 f_i를 검증함으로써 그 정당성을 확인한다.

$$f_i = (d_i^{t_i})^s \bmod n (\text{i=1,2,3})$$

이상의 내용을 도식화하면 (그림 2)와 같이 정리할 수 있다.

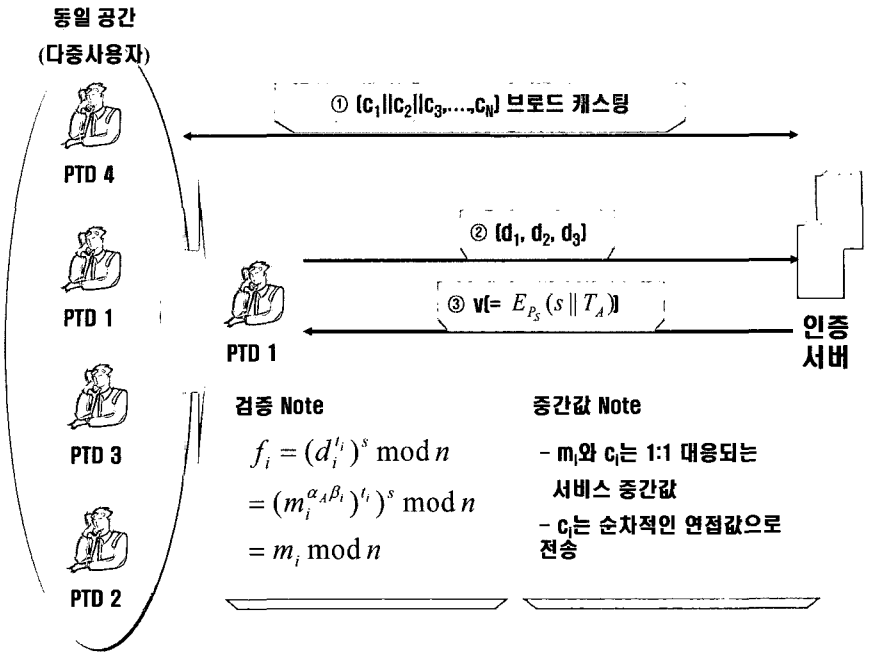
[Step 2] 임시 그룹 설정을 위한 PTD 1의 초기 등록 과정 (동일한 서비스를 요구하는 PTD들중 PTD 1과의 통신)

일정한 개수 이상의 PTD들이 동일한 서비스를 요청할 경우 임시적으로 그룹을 형성하여 통신의 효율성을 높이는 단계이다.

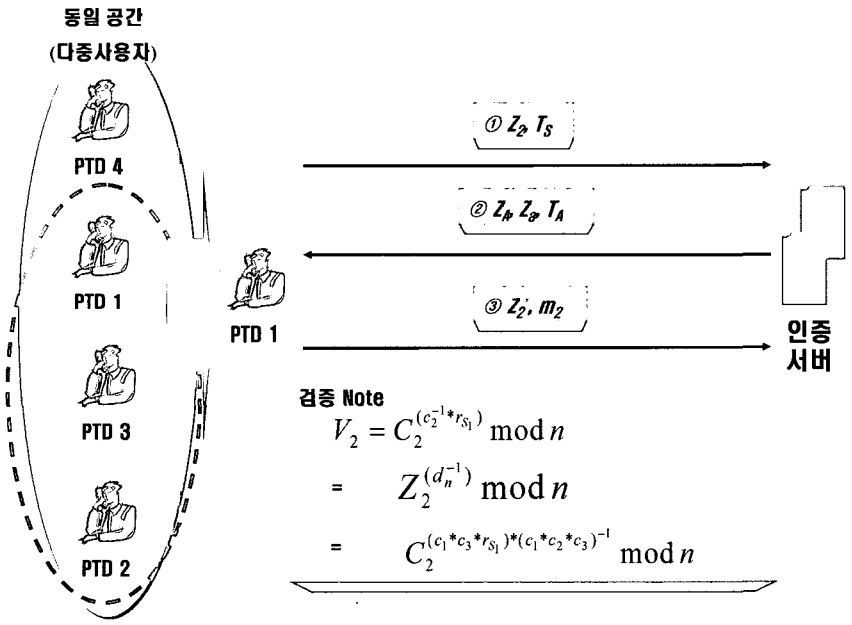
① PTD 1은 [Step 1]에서 설정된 3개의 서비스 c_1, c_2, c_3 중 하나의 서비스를 제공받고자 할 경우(c_2 서비스를 제공 받고자할 경우) 다음을 계산하여 Z_2, T_S를 인증 서버에 전송한다.

$$C_2 = c_2 \oplus m_2 \oplus ID_{S_1},\ d_2 = c_1 * c_3 * r_{S_1},\ Z_2 = C_2^{d_2} \bmod n$$

② 인증 서버는 PTD 1으로부터 전송된 Z_2의 값을 임시 저장한 뒤 PTD 1의 임시 비밀정보 값인 d_n, Z_a값을 다음과 같이 계산하고, 인증 서버의 랜덤수 r_A를 선택하여 Z_A를 계산한 뒤 Z_A, Z_a, T_A를 PTD에 전송한다.



(그림 2) PTD의 서비스 등록 단계



(그림 3) PTD의 임시 그룹 설정을 위한 초기화 단계

$$d_n = c_1 * c_2 * c_3$$
$$Z_a = Z_2^{d_n^{-1}} \ mod \ n$$
$$Z_A = Z_a^{r_A} \ mod \ n$$

③ PTD 1은 인증서버로부터 전송되는 $Z_a = V_2$이면 Z_2', m_2를 인증 서버에 전송한다.

$$V_2 = C_2^{c_2^{-1} * r_{S_1}} \ \mathrm{mod} \ n$$
$$Z_2' = Z_A^{r_{S_1}} \ mod \ n$$

⑤ 인증 서버는 PTD 1에서 전송된 Z_2'의 값을 이용해 현재 PTD 1이 요구하는 서비스에 대한 임시 비밀 정보 y_2를 저장한다.

$$y_2 = Z_2'^{(r_A^{-1})} \ mod \ n$$

(검증 $Z_2'^{(r_A^{-1})} = Z_A^{(r_A^{-1}) * (r_{S_1})} = Z_a^{(r_A^{-1})(r_{S_1})(r_A)} = Z_2^{(c_1 * c_2 * c_3)^{-1} * r_A^{-1} * r_{S_1} * r_A} =$
$C_2^{(c_1 * c_3 * r_{S_1})(r_A^{-1} * r_{S_1} * r_A)(c_1 * c_2 * c_3)^{-1}} = C_2^{(c_2^{-1} * r_{S_1}^2)}$)으로 검증이 가능하다.

[Step 3] 임시 그룹 설정 단계

인증 서버는 [Step 2]에서 PTD의 비밀 정보 y_i와 [Step 1]에서 전송되어온 m_i를 확인하여 같은 서비스를 제공 받고자 하는 PTD들이 일정한 개수 이상이거나, 동일한 서비스에 대한 빈도가 높을 경우이거나, 동일한 통신량이 증가할 경우 해당 PTD들의 임시 그룹 설정을 위한 과정을 수행한다.

① 인증 서버는 동일한 서비스를 제공 받고자 하는 PTD들의 비밀정보 $(y_1, \ldots, y_N)$으로 정의하고 각각의 y_i에 대한 D_i를 대응하여 생성한 뒤 이를 임시 보관한다. 또한 임시 그룹 설정($ID_{S_1}, ID_{S_2}, ID_{S_3}$)들을 임시 그룹으로 설정하고 m_2에 해당되는 서비스에 대해 서비스 빈도가 높을 경우)을 위해 PTD 1에 s_2, c_2, T_A를 전송한다.

$$D_2 = H(c_2 \| y_2)$$
$$s_2 = g^{D_2} \bmod n$$

② PTD 1은 인증 서버로부터 전송되어온 c_2, s_2에서 c_2를 이용해 y_2^{-1}을 계산하여 세션키 $K_{G_{temp}}$를 생성하고 이를 기반으로 암호 통신이 필요한 어플리케이션 서비스 메시지 M_C를 $K_{G_{temp}}$로 암호화하여 V_{S_1}, T_{S_1}을 인증 서버에 전송한다.

$$K_{G_{temp}} = s_2^{(y_2^{-1})} \bmod n$$
$$V_{S_1} = E_{K_{G_{temp}}}(M_C \bmod n)$$

③ 인증 서버는 전송되어온 V_{S_1}의 검증을 수행하기 위해 $K_{G_{temp}}$를 생성한 뒤 V_S를 복호화한 뒤 암호 통신이 필요한 어플리케이션 서비스 확인한다.

$$K_{G_{temp}} = s_2^{(y_2^{-1})} \bmod n$$

서비스 확인을 마친 인증 서버는 $K_{G_{temp}}$를 임시 그룹원들과의 세션키로 정의하고 $K_{G_{temp}}$리스트를 안전하게 보관한다(그림 4 참조).

- 이상의 과정 [Step 3]는 임시 그룹 설정을 위해 동일한 서비스를 요구하는 모든 그룹원들이 동일하게 수행한다.

[Step 4] 임시 그룹의 서비스 요청단계

다음은 서비스 등록이 완료된 PTD들이 동일한 형태의 서비스를 제공 받기 위해 그룹을 형성하였을 경우 임시 그룹원인 PTD 1은 1-out-2 분실 통신을 이용하여 서버에 서비스를 요청하는 단계이다.

(현재 통신을 요구하는 PTD 1이 임시 그룹원으로 속해 있을때 다음의 통신 과정을 수행한다. 또한 1-out-2 분실 통신을 수행하는 것은 전송되는 정보가 소실되거나 전송 실패 되었을 경우를 고려하여 PTD 1의 전력 효율을 높이기 위함이다.)

① PTD 1은 랜덤값 r_{S_1}', r_{S_1}''을 서버에 전송 한다.

② 인증 서버는 PTD 1으로부터 수신된 r_{S_1}', r_{S_1}''을 임시 저장하고 랜덤하게 Z_i와 x_{Z_i} (Z_i={0, 1}, $x_{Z_i} \in_U Z_n$)를 선택하고 다음과 같이 w, T_A를 계산하여 PTD 1에 전송한다.

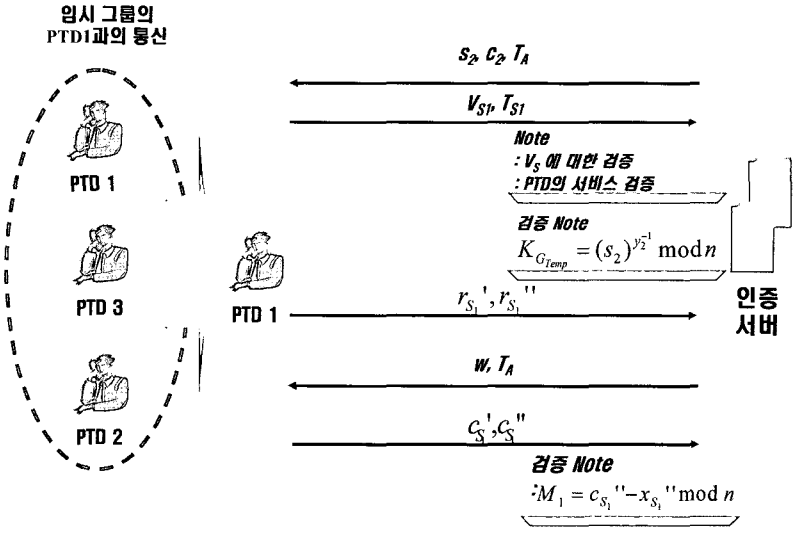
$$w = E_{K_{G_{temp}}}(x_{Z_1}) + r_{S_1}'' \bmod n$$

③ PTD 1은 $x_{Z_1} = D_{K_{G_{temp}}}(w - r_{S_1}'' \bmod n)$을 검증한 뒤 c_{S_1}'와 c_{S_1}''을 다음과 같이 계산하여 서버에 전송한다. (M_0, M_1은 암호 통신이 필요한 임시 그룹 서비스 요청 메시지)

$$c_{S_1}' = M_0 + x_{Z_1}' \bmod n$$
$$c_{S_1}'' = M_1 + x_{Z_1}'' \bmod n$$

④ 서버는 $M_1 = c_{S_1}'' - x_{Z_1}'' \bmod n$을 획득한다.

이상의 [Step 3]와 [Step 4]를 (그림 4)와 같이 요약할 수 있다.



(그림 4) PTD의 임시그룹 설정 및 그룹 서비스 요청 단계

[Step 5] 임시 그룹의 삭제

임시 그룹으로 형성된 PTD들이 임의의 개수 이하가 될 경우 현재 형성된 임시 그룹을 삭제하는 과정을 인증서버는 수행한다.

① 인증서버는 임시 그룹 형성을 위해 PTD들의 임시 저장한 비밀정보($y_1,...,y_N$)과 비밀정보를 기반으로 생성된 D 리스트를 임시 저장정보에서 추출한다.

② 인증 서버는 추출된 값에서 $s_{DEL}=(ID_{S_1},D_{S_1},...,\ ID_{DEL}*D_{S_N})$값을 네트워크 전체에 브로드 캐스팅 한다.

③ 브로드캐스팅된 정보를 수신한 PTD는 자신이 포함된 임시 그룹의 상태를 확인하고, 임시 그룹 삭제를 수신한다.

이상의 과정을 수행하여 동일한 공간에 다중 사용자들을 위한 안전하고 효율적인 네트워크 관리 방식을 수행한다.

6. 제안 방식 분석

본 논문에서는 유비쿼터스 환경을 실현할 수 있는 무선 네트워크에서의 PTD를 이용한 다중 사용자들의 안전하고 효율적인 네트워크 관리 과정을 제안하였다. 제안된 방식을 3장에서 제시한 요구사항을 기반으로 분석할 경우 다음과 같이 정리할 수 있다.

6.1 안전성 분석

제안된 방식은 유비쿼터스 환경에서의 무선 네트워크가 가져야 하는 보안 요구사항을 기반으로 하여 다음과 같은 안전성을 유지할 수 있다.

- 상호 인증 : 사용자 중심으로 이루어지는 무선 네트워크의 경우 이동 단말과 인증 서버 혹은 게이트웨이와의 상호 인증을 통해 안전성을 유지할 수 있어야 한다. 따라서 본 논문에서는 이산대수에 기반한 인증 방식을 이용하였다. 특히 브로드 캐스팅되는 값에서 서비스 값을 계산하여 이를 검증하는 방식을 이용함으로써 네트워크 관리 측면에서 전송의 효율성을 높이는 효과를 가져 올 수 있다.
- 기밀성과 무결성 : 사용자의 프라이버시 정보를 전송할 경우 전송되는 데이터에 대한 기밀성과 무결성을 제공하여 전송 데이터에 대한 안전성을 유지할 수 있어야 한다.

*저장 데이터에 대한 기밀성 : 네트워크상의 개체들은 자동 서비스 생성 개체로써 이와 연관된 비밀값을 안전하고 저장하여야 한다. 따라서 PTD를 이용해 무선 네트워크상에서 이루어지는 연산 과정에 기밀 연산을 수행함으로서 디바이스 저장 정보에 대한 기밀성을 보장하였다. 제안 방식에서는 $V_2=C_2^{(c_2^{-1}*r_S)}\ mod\ n(=Z_2^{(d_n^{-1})}\ \mathrm{mod}\ n=C_2^{(c_1*c_2*r_S)*(c_1*c_2*c_3)^{-1}}\ \mathrm{mod}\ n$의 검증과정을 거쳐 PTD의 비밀값 r_S를 전송하지 않고 기밀 의뢰 연산 방식을 수행하도록 하였다.

*전송 데이터에 대한 기밀성 : 무선 네트워크에서의 전송 데이터의 기밀성은 공개키 암호 알고리즘과 이산대수의 어려움에 기반해 전송 데이터에 대한 기밀성을 유지하였다.

*전송 데이터에 무결성 : 전송 데이터에 대한 무결성의 경우 안전한 해쉬 함수 $H()$를 통해 무결성 서비스를 제공하였다.

- 상태 획득 기술 : 각각의 PTD들은 서비스별로 새로운 비밀정보 y를 재등록해야 한다. 인증서버는 이를 기반으로 다양한 PTD들의 현재 서비스 상태를 확인함으로써 보다 안전한 형태의 통신 서비스가 되도록 하였다
- 자동 서비스 생성 방안 : 일정한 통신량 이상(서비스 이용 빈도)이 높을 경우 안전한 형태의 그룹으로의 변환이 가능해야 하며, 일정한 통신량 이하의 서비스 빈도가 나타날 경우 자동적인 그룹 해체 과정을 제공할 수 있어야 한다. 제안 방식에서의 자동 서비스 생성 방안은 서버에서 제공할 수 있는 서비스 등록에 대한 고유 서비스 i를 기반으로 계산함으로써 서비스 요청의 정당성을 확보하는 자동 서비스 생성 방안을 제안하였다.

이상의 안전성에 대한 분석을 <표 1>과 같이 간단히 요약해 볼 수 있다.

〈표 1〉 기존 방식과 비교 분석

보안 요구사항		WAP 포럼 방식	정책 기반 방식	제안 방식
상호 인증		△	○	○
기밀성과 무결성	전송 데이터	△	△	○
	저장 데이터	△	×	○
상태 획득 기술		×	△	○
자동 서비스 생성 방안		×	×	○

(○ : 안전, △ : 부분적인 안전, × : 취약)

6.2 효율성 분석

효율성 측면에서 제안방식은 PTD의 특성상 높은 연산의 계산량을 최소화하여 PTD의 효율을 극대화시킴으로써 전체 네트워크의 효율성을 높이는 방안을 제시하고자 하였다. 따라서 본 논문에서는 통신의 효율을 높이기 위해 1-out-2 분실 통신 방식을 수행하였다. PTD가 전송하는 암호 통신 메시지 c_{S_i}', c_{S_i}''을 서버에 전송함으로써, 하나의 통신 메시지가 분실된다 하더라도 다른 하나를 수신하여 $M_{S_i}=\ c_{S_i}''-x_{S_i}''\ mod\ n$을 획득한다. 따라서 재전송하기 위한 브로드캐스팅 메시지를 최소화 하도록 하여 전체 네트워크의 효율성을 높이고자 하였다. 그러나 본 논문에서는 통신에 대한 효율성이 기존 방식에 비해 전체 프로토콜을 수행할 경우 효율성이 매우 저하되는 문제점과 PTD에서 이산대수의 안전성을 제공하기 위한 높은 연산량을 수행에 따라 계산량의 비효율성의 문제점은 여전히 내포하고 있어 제안된 방식의 다양한 적용성을

저해하는 요소가 된다. 또한 1-out-2 분실 통신의 경우 ad hoc과 같이 서로 상이한 패스를 사용할 경우 두 개의 메시지 모두가 loss될 유효할 수 있으나 본 논문에서 제시한 환경과 같은 일반적인 무선랜과 같은 환경의 경우 연속적인 메시지 전송으로 인해 모두 loss될 확률이 높아지는 문제점도 존재한다.

7. 결 론

최근 정보통신의 급속한 발전으로 개인 정보통신의 수요는 날로 증가하고 있다. 특히, 유비컴퓨팅에 대한 연구는 차세대 IT 기술로써 많은 각광을 받고 있는 기술이다.

유비컴퓨팅 환경의 무선 네트워크 기술은 향후 사용자들에게 아주 많은 편리함을 제공해 줄 수 있는 신기술임에도 불구하고 보안적인 사항이 고려되지 않는다면, 악의적인 목적을 가진 사용자들에 의한 개인 프라이버시 침해와 같은 공격적 취약점을 도출 시킬 수 있다.

특히, 유비쿼터스 환경의 무선 네트워크는 반드시 보안 서비스가 요구되며, 기존의 보안 개념인 인증, 기밀성과 무결성을 비롯하여 새로운 형태의 서비스 제공에 따른 보안 요구사항이 필요하다.

본 논문에서는 기존의 보안 요구사항과 더불어 새로운 보안 요구사항을 제시하여 이를 만족할 수 있는 다중사용자를 위한 네트워크 관리 기법을 제안하였다.

따라서 제안된 방식의 경우 유비쿼터스 상거래와 같은 기반 환경에 활용할 수 있는 구조이다. 이는 향후 추가적인 보안 요소를 정의하고 그에 따른 해결책을 제시함으로써 보다 향상된 네트워크상에서의 보안 서비스를 실현하고자 한다.

참 고 문 헌

[1] D.W. Carman, B.J. Matt and G.H. Cirincione. "Energy-efficient and Low-latency Key Management for Sensor Networks", In Proceedings of 23rd Army Science Conference. Dec., 2-5 2002.

[2] M.Chen, W. Cui, V. Wen and A. Woo, "Security and Deployment Issues in a Sensor Network" http://www.cs.sfu.ca/~angiez/personal/paper/sdissues.pdf#search='Security%20and%20Deployment%20Issues%20in%20a%20Sensor%20Network'

[3] F. Hu, Neerajk, Sharma "Security Considerations in Wireless Sensor Networks", Sensors Expo, San jose, CA, 2004.

[4] L. Lymberopoulos, E. Lupu and M. Sloman, "An Adaptive Policy Based Management Framework for Differentiated Services Networks", proceedings of the Third International Workshop on Policies for Distributed Systems and Networks, pp.147~158, 2002.

[5] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck and M.B. Srivastava. "On communication Security in Wireless Ad-Hoc Sensor Network" Eleventh IEEE International Workshops on Enabling Technologies : Infrastructure for Collaborative Enterprises (WETICE'02) June 10~12, 2002.

[6] W. Du, J. Deng, Y.S. Han, S. Chen and P. Varshney. "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge", To appear in IEEE INFOCOM'04, March 7~11, 2004.

[7] 이송종, "유비쿼터스 네트워크 환경에 적용되는 무선기술", 한국정보과학회 춘계학술발표대회, pp.574~576, 2003.

[8] 이임영 "전자상거래 보안입문", 생능출판사, 2001.

[9] 최용락, 소우영, 이재광, 이임영 "컴퓨터 통신보안", 도서출판 그린, 2001. 2.

[10] Alfred J. Menezes, Paul C.van Oorschot and Scott A. Vanstone "HANDBOOK of APPLIED CRYPTOGRAPHY", CRC.

[11] Ubiquitous Computing http://www.ubiq.com/hypertext/weiser/UbiHome.html

[12] OnlineCertificateStatusProtocol http://www.ietf.org/html.charters/tls-chater.html

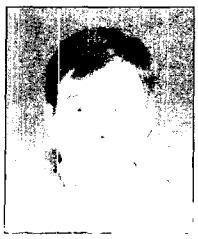
[13] http://www.itu.int/ITU-D/pdf/4597-13.3bis-en.pdf

[14] http://www.iris.re.kr/iwap01/program/download/g07_paper.pdf#search='Secure%20MCommerce%20with%20WPKI'

[15] Project digital Signatures :http://www.law.kuleuven.ac.be/icri/projects/

[16] WAP Forum : Wireless Application Protocol Public Key Infrastructure, Version April, 2001, http://www.wapforum.org

[17] http://crpit.com/confpapers/CRPITV21AZhao.pdf



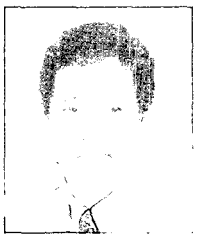
서 대 희

e-mail : patima@sch.ac.kr

2003년 순천향대학교 전산학 전공 석사

2004년~현재 순천향대학교 전산학과 박사과정

관심분야 : 암호이론, 정보이론, 컴퓨터 보안



이 임 영

e-mail : imylee@sch.ac.kr

1981년 홍익대학교 전자공학과

1986년 오사카대학 통신공학 전공 석사

1989년 오사카대학 통신공학 전공 박사

1989년~1994년 한국전자통신연구원 선임연구원

1994년~현재 순천향대학교 정보기술공학부 교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안