Pervasive computing에서의 사용자 인증 및 프라이버시 보호 방안 연구

이진우*, 구자범*, 박세현*

*중앙대학교, 전자전기공학부

A Study of User Authentication and Privacy Protection Method in Pervasive Computing

Chin-U Lee*, Ja-Beam Gu*, Se-Hyun Park*

*School of Electrical and Electronic Engineering, Chung-Ang University

요 약

Pervasive computing은 본래의 의미에서 알 수 있듯이 모든 개체들이 네트워크로 연결되어 보다 향상된 서비스 환경을 제공하고자 하는 것이 목표이므로, 작게는 센서들에 의한 네트워크로부터 크게는 인공위성 네트워크까지 다양한 크기와 성능을 갖는 네트워크 개체들이 존재하는 복합 환경을 구성하게 된다. 이와 관련하여 IPv6의 보급, 이동 단말의 성능향상, 다양한 서비스와 어플리케이션 개발을 통해 새로운 네트워크 실현을 가속화하고 있다. 이러한 차세대 네트워크는 많은 사용자와 단말들의 적응적 상호 작용이 주요 핵심 부문이 될 것이다. 따라서 본 논문에서는 이러한 네트워크 구성 요소의 적응적 상호 작용의 신뢰성을 보장하기 위한 보안 체계를 연구하는 것을 목표로 한다.

1. 서론

Pervasive computing 환경에서는 유무선 네트워크의 통합과 다양한 크기의 수많은 네트워크의 구축으로 특정 장소를 불문하고 언제 어디에서나 사용 가능한 통신서비스환경이 구축됨으로써 최상의 QoS를 보장하는 통합 네트워크가 구축될 것으로 기대되고 있다. [1] 이러한 환경 하에서는 사용자의 위치와 context에 따라 사용자가 원하는 서비스 또는 네트워크에서 제공되는 서비스가 결정되고, 사용자는 이러한 환경에서 적응적·능동적으로 네트워크를 구성하게된다.[2][3] 따라서 사용자는 주변의 고정된 네트워크 장치뿐만 아니라 주위의 다른 사용자와도 유기적인 연동을 이루어 다양한 정보를 주고받는 환경을 구성하고, 사용자의 위치, 취향, 요구사항, 스케줄, 주위환경 등 다양한 요소에 따른 context를 구성하여 서비스를 형성하게 된다. 이러한 context 기반의 적응적 서비스 제공에 있어서 무엇보다 중요한 것은 네트워크 구성 시 필요한 접근 제어나 context의 기밀성 또는 무결성을 보장하기 위한 보안 기능이 완비되어 있어야 사용자가 안심하고 서비스를 제공받을 수 있다는 것이다. 뿐만 아니라 pervasive computing을 위한 보안 기술 체계를 국내에서 확보하는 것은 세계적인 기술 변화의 흐름을 선도하고 차세대 네트워크 환경의 선두주자로 나가기 위한 발판을 마련한다는 측면에서 매우 중요한 연구이다.

Pervasive computing은 본래의 의미에서 알 수 있듯이 모든 개체들이 네트워크로 연결되어 보다 향상된 서비스 환경을 제공하고자 하는 것이 목표이므로, 작게는 센서들에 의한 네트워크로부터 크게는 인공위성 네트워크까지 다양한 크기와 성능을 갖는 네트워크 개체들이 존재하는 복합 환경을 구성하게 된다. 이와 관련하여 IPv6의 보급, 이동 단말의 성능향상, 다양한 서비스와 어플리케이션 개발을 통해 새로운 네트워크 실현을 가속화하고 있다. 이러한 차세대 네트워크는 많은 사용자와 단말들의 적응적 상호 작용이 주요 핵심 부문이 될 것이다.[4] 따라서 본 논문에서는 이러한 네트워크 구성 요소의 적응적 상호 작용의 신뢰성을 보장하기 위한 보안 체계를 연구하는 것을 목표로 하고 있다. 인증/보안 체계는 pervasive 컴퓨팅의 주요 기술과 밀접하게 연관되어 신뢰할 수 있는

완벽한 pervasive 컴퓨팅을 실현하는데 필수 요소이다. 논문의 구성은 다음과 같다. Ⅱ장에서는 Pervasive computing에 대한 기술동향, Pervasive computing에서의 문제점 및 Pervasive computing에서의 사용자 인증 및 프라이버시 보호방안에 대해서 설명하고, Ⅲ장에서는 본 논문의 결론을 맺고자 한다.

Ⅱ. Pervasive Computing의 개요

1. 국내·외 기술개발현황

세계 각국은 가까운 미래에 실현될 pervasive computing 사회에 대비하여 IT 관련 분야에서부터 유통, 제조, 서비스 등 다양한 분야에 걸친 전략 및 정책 개발을 위해 국가, 대학, 연구소 및 기업 차원에서 힘을 모으고 있다. 그러나 이러한 연구 활동은 대부분 특정네트워크 및 서비스 모델을 기반으로 하여 기반 기술을 확보하기 위한 연구로 직접적인 보안 관련 연구는 매우 부족한 실정이고, pervasive computing의 dynamic 환경에서 요구되는 trust model, 인증, 프라이버시, 암호화 등에 대한 연구가 국제 워크숍 등을 통해 부분적으로 논의되고 있다. 국내·외의 pervasive computing 관련 연구 동향은 다음과 같다.

◇ 미국의 연구활동

가장 활발한 연구 활동을 보이고 있는 미국은 DARPA, NIST 등의 국가 연구소의 대학 및 기업을 상대로 한 프로젝트 기반 연구에 대한 지원이 눈에 띄며, 기업과 대학 및 연구소 공동 연구와 새로운 패러다임에 편승하기 위한 기업차원의 전략 및 애플리케이션을 개발하고 있다. DARPA는 대표적 프로젝트로 "Smart Dust" 및 "Endeavour 프로젝트(버클리 대학)", "Info-Sphere 프로젝트 (OGI/Georgia Tech)", "Portolano(워싱턴 대학)", "Aura(CMU)" 그리고 "Oxygen (MIT)" 등을 지원하고 있으며 프로젝트의 대부분은 대학을 중심으로 연구되고 있다. NIST는 '스마트 공간 통합 (smart space integration)', 'pervasive 소프트웨어 도구', 'pervasive 네트워킹 기술' 등의 연구 프로그램을 지원하고 있다. 또한 HP, IBM, MS 등의 세계적 기업도 pervasive computing 연구에 동참하여 'EasyLiving 프로젝트(MS)'와 'CoolTown 프로젝트 (HP)' 등을 진행중이다.

◇ 유럽의 연구활동

유럽은 2001년에 시작된 EU의 정보화사회기술계획(IST)의 일환으로 미래기술계획(FET)이 자금을 지원하고 있는 '사라지는 컴퓨팅(disappearing computing)'을 중심으로 pervasive 컴퓨팅에 대한 대응 전략을 모색하고 있다. '사라지는 컴퓨팅'은 정보기술을 일상사물 및 환경 속에 통합하여 인간의 생활을 지원하고 개선하고자 하는 것으로, 우리가 흔히 사용하는 일상 사물에 센서, 구동기, 프로세서 등을 식재하여 사물 고유의 기능에 정보처리 및 교환 기능이 증진된 정보 인공물(information artifacts)의 고안과 정보 인공물 상호간의 지능적이고 자율적인 감지와 무선통신을 통해 새로운 가능성과 가치를 창출하고, 궁극적으로는 인간의 일상 활동을 지원 및 향상시킬 수 있는 환경 구축을 목표로 하고 있다. 이러한 목적을 달성하기 위해 연구소, 대학 및 기업 공동으로 연구하고 있는 Smart Its, Paper++, Grocer 등 16개의 독립 프로젝트를 지원하고 있다.

◇ 일본의 연구활동

일본에서는 물리공간에 존재하는 모든 물체 및 생활 공간 그리고 사람이 착용하는 의복, 안경, 신발, 시계 등의 신변용품 등에 다양한 기능을 갖는 마이크로컴퓨터 칩들이 이식되고 상호간에 연결됨으로써 언제 어디서나 컴퓨터의 능력이 발휘되는 네트워크 구현을 중심으로 한 연구가 산·학·관의 연계에 의해 진행되고 있다.

◇ 국내 연구동향

국내에서는 ETRI를 중심으로 정보기술의 발전에 따라 물리공간과 전자공간의 전략적 연계 공간으로서 제3공간 즉, pervasive computing과 네트워크를 기반으로 하는 공간이 등장할 것이라는 논리 하에 최첨단 pervasive 네트워크의 전국적 구축과 이를 기반으로 교육, 의료, 행정과 국방 등 국가사회의 중추 시스템을 접목시킴으로써 국가경쟁력을 획기적으로 개선하자는 새로운 정보화입국 비전 "u-Korea 21 Grand Strategy"가 제시되고 있다. 이 같은 u-Korea 21 Grand Strategy는 1996년의 제1차 정보화촉진기본계획, 1999년의 Cyber Korea 21과 2002년 4월의 e-Korea Vision 2006 이후 새로운 정보화 패러다임을 선도 할 정보화 기본계획의 밑바탕으로 그 중요성이 매우 크다.

2. Pervasive computing: 문제점

Pervasive computing은 국내·외적으로 아직 개념정립 단계에 있다고 볼 수 있다. 국내·외의 다양한 연구 프로젝트들은 대부분 네트워크 구성이나 서비스에 대한 구체적인 모델을 제시한 경우는 거의 없고, pervasive computing을 실현하기 위한 기반 기술인 광대역 망에 이어질 수 있는 초

고속 액세스 망이나 백본망, 고속 및 광대역 액세스가 가능한 무선통신시스템, 센서기술 등의 연구에 주력하고 있다.

그러나 진정한 pervasive 사회 구현을 위해서는 이러한 통신·어플리케이션 관련 기반 기술뿐만 아니라 언제어디서나 안전하게 정보를 주고받을 수 있는 고도의 보안 및 인증 기술 등이 필요하다. Pervasive computing에서 요구되는 보안 기능을 표 1과 같이 요약할 수 있다. 기존의 네트워크 인증 모델(AAA)의 경우 사용자와 서비스 제공자, 그리고 관리자의 모델로 구성되어 있었으나, pervasive computing 환경은 좀더 세분화되어 글로벌 서비스 관점에서 이동하는 사용자에게 보안 서비스를 제공하기 위한 요소와 로컬 액세스 관점에서 사용자와 주위 환경과의 다양한 상호 작용을 제공하는 관점으로 나뉘어 연구될 필요가 있다. [5]

3. Pervasive computing에서의 사용자 인증 및 프라이버시 보호 방안

현재 가장 보편적으로 사용되고 있는 무선 네트워크인 IEEE 802.11b 무선 LAN은 단말간 링크 수준의 제한적인 인증만을 제공하기 때문에 능동적 서비스 제공에 필요한 보안 메커니즘과 관리 방안이 매우 취약하다. IEEE 802.11b의 인증은 기본 알고리즘인 'open system authentication'과 공유키를 이용한 인증(WEP)으로 구분되지만, pervasive computing에서 필수로 요구되는 개체들 간의 상호인증을 제공하지 않는다. IEEE 802.11b와 더불어 현재 가장 주목받고 있는 유럽식 표준 무선 네트워크인 HIPERLAN/2의 경우에도 Diffie-Hellman 키 교환 방식과 인증을 제공하고 있다. 그러나 제 3의 인증 신용 객체(인증서 등)에 따른 상호인증 기반의 무선 PKI를 사용하지 않을 경우 공개키 분배방식은 정당한 사용자로 가장한 불법의 사용자에 의해 가장공격을 당하거나 데이터의 위조, 변경 등의 심각한 문제를 초래할 수 있다. 이동통신 시스템과 같이 비교적 폐쇄된 환경에서는 대칭키 방식의 보안 구조를 통해서 부분적으로 인증 및 사용자 확인 등의 보안기능을 제공하였으나, 이것은 대칭키 방식의 빠른 속도가 큰 요인으로 작용했기 때문이고, 기존의 시스템이 폐쇄적 환경이라는 점이 대칭키 방식의 단점, 즉 키 관리의 취약점을 보완해 주는 역할을 하여, 최적의 성능을 내면서도 보안성을 유지하는 것이 가능했기 때문이다. 따라서 이러한 방식에서는 네트워크 자체의 폐쇄성에 의해서 각 개체들 간에 필요한 secure association이 보장된다고 가정한 상태에서 인증을 수행하거나 접근을 제어하고 있다. 그러나 이러한 방안은 네트워크가 개방되어 있고 상호인증이 필수인 pervasive computing 환경에 그대로 적용하기에는 서비스 이질성, 사용자와 네트워크 제공자의 다양성 등으로 매우 취약하다. Pervasive computing의 보안 체계는 이러한 환경의 변화와 새로운 보안 요구사항을 만족할 수 있어야 한다.

그림 1은 기존의 유선 망에서 적용되는 상호인증 구조를 무선 이동통신에 적용한 구조이다. 그림에서 T_{req1}이나 T_{req2}는 이동 단말과 각 개체간 전송 지연을 나타내고 있다. 과거 유선 망이나 무선 LAN과 같은 환경에서는 이러한 전송 지연을 최소화하기 위한 방안에 대한 연구가 중점적이었으나, pervasive 컴퓨팅 환경에서는 이러한 전송지연 뿐만 아니라 T_{MT}, T_{DC}, T_{HE}로 표현된 상호인증 과정의 소요시간을 최소화하기 위한 방안이 필요하다. 특히 T_{MT}는 이동 단말에서 요구되는 지연시간으로 이 시간동안 이동 단말은 상호인증을 위한 인증정보(DC의 인증서와 인증서 폐기 목록)를 획득하고 이것을 검증해야 한다. 따라서 이동 단말의 부하를 최소화하기 위한 방안이 추가적으로 요구된다. 더욱이 이동단말에 대한 네트워크 사용 권한 부여가 이루어지기 이전에 이러한 인증정보 획득 과정이 필요하므로, 자원이 상대적으로 부족한 무선링크를 비효율적으로 사용하는 문제가 발생하여 이에 대한 대책이 요구된다. 또한 인증 구조가 이러한 서버-클라이언트 구조가 아닌 peer-to-peer 구조로 일어날 수 있고, 사용자의 이동 단말이 서버로 동작하여 서비스를 제공하는 경우도 발생할 수 있어 이러한 유·무선망에서 적용되던 인증 구조가 적합하지 않음을 알 수 있다.

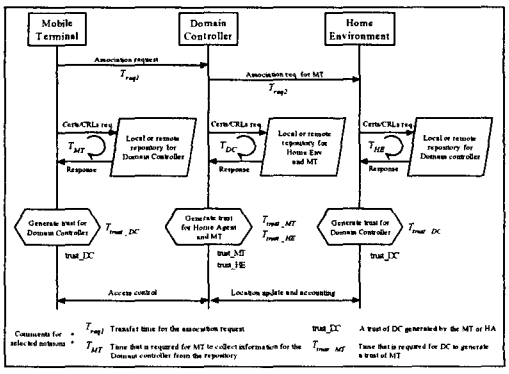

그림 1. 유선의 Secure Association에 의한 상호인증 모델을 적용한 구조

이러한 문제점을 본 논문에서는 무선 PKI에 기반한 공개키 기반 키분배와 AAAv6 프레임워크를 변형한 새로운 보안 체계에서 해결하고자 한다. 그림 2는 PKI 기반의 사용자 인증에 의한 접근제어를 WLAN 구조상에서 구현한 예이다. 이러한 기반 구조에서의 인증은 사용자와 서비스 제공자 간에 공개키를 이용하여 인증이 수행되므로 사용자가 어느 곳에 위치하더라도 인증이 가능하다는 장점이 있다. 다만 공개키는 시스템 자원의 낭비가 매우 크다는 단점을 갖고 있어 본 연구를 통해 효율적인 상호인증과 키분배 방법에 대한 연구 지속적으로 진행 되야 할 것이다.

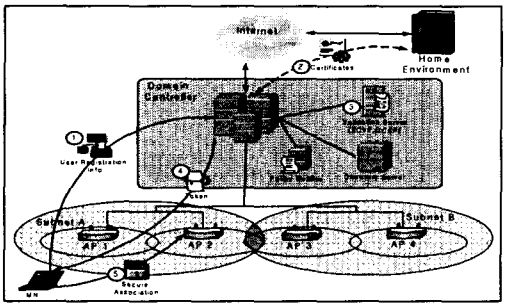

그림 2. PKI 기반의 사용자 인증 및 접근제어

또한 pervasive 컴퓨팅 환경의 네트워크 특성상 사용자의 빈번한 이동에 의해 다수의 서비스 제공자 또는 다른 사용자와 반복적인 인증 과정이 요구된다. 이러한 반복되는 인증과정에서 사용자와 네트워크의 부담을 줄이기 위한 방안으로 "virtual authority"를 이용하는 방안을 제안한다.

Virtual authority는 로컬 도메인의 여러 서비스 제공자, 유동적 사용자들에 대한 인증을 대행하는 노드로, 사용자의 고속 또는 저속 이동 시 효율적인 반복 인증을 제공해 주는 기능을 담당한다. 그림 3는 이러한 인증 대행 관계를 나타낸 것이다.

그림에서 사용자는 virtual authority인 network operator를 통해 다른 서비스 제공자에 대한 인증을 대행하여 각각의 서비스 제공자와 신뢰관계를 형성하는 작용으로 이동 단말의 부담을 최소화 할 수 있기 때문에 단말의 로밍시 seamless한 데이터 전송과 인증에 요구되는 요구사항들에 대한 부하를 최대한 줄일 수 있다.

Ⅲ. 결론

향후 도래할 새로운 네트워크 개념으로서

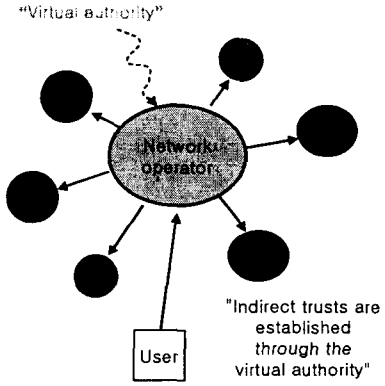

그림 3. Virtual Authority와 서비스 제공자간의 인증 대행 관계

pervasive computing은 현재 국내·외적으로 초미의 관심을 모으고 있다. 이에 따라 세계 각국은 현재 pervasive computing 시대를 주도하기 위해 pervasive 인프라 확보와 관련 핵심 기술의 선개발 및 세계화에 온 힘을 다하고 있으며 동시에 바람직한 pervasive computing 사회의 실현을 위해 국가간의 긴밀한 협력관계가 유지의 필요성을 인식하고 있다. 따라서 본 논문에서 제안하고 있는 사용자 보안 기술은 이러한 새로운 환경을 위한 신뢰성·안전성·상호작용을 보장하여 신뢰할 수 있는 완벽한 pervasive computing 환경 구현의 기틀을 마련할 수 있을 것으로 기대된다.

참고문헌

[1] Lalana Kagal, Tim Finin, and Anupam Joshi, "Trust-Based Security in Pervasive Computing Environments", IEEE Pervasive Computing Mobile and Ubiquitous Systems, December 2001

[2] M. Satyanarayanan, "Pervasive Computing: Vision and Challenges", IEEE Personal Communications, August 2001.

[3] Theo G. Kanter "Hottown, Enabling Context-Aware and Extensible Mobile Interactive Spaces", IEEE Wireless Communications, October 2002.

[4] Asim Smailagic, David Kogan, "Location Sensing and Privacy in a Context-Aware Computing Environment", IEEE Wireless Communications, October 2002.

[5] Adam Stone, "The Dark Side of Pervasive Computing", IEEE Communications Society, 2003.