유비쿼터스 컴퓨팅과 센서 네트워크 보안 기술에 관한 연구

A Study of Ubiquitous Computing and Sensor Network Security Technology

강희조* 방기천**

목 차

Key Words : 유비쿼터스 컴퓨팅, 센서 네트워크, 보안, 객체보호 기술

Abstract

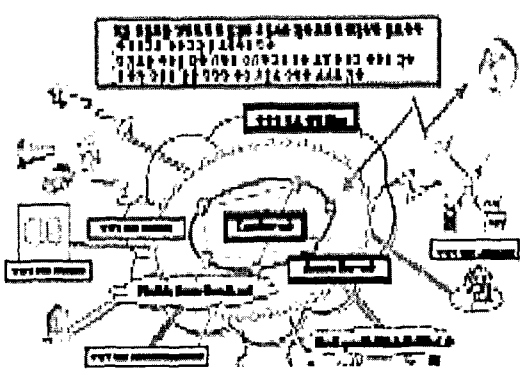
유비쿼터스 컴퓨팅과 센서 네트워크에 대한 보안에 대한 적절한 정의가 필요하고 기존의 보안 개념인 인증, 기밀성, 무결성, 가용성과 유비쿼터스 컴퓨팅과 센서 네트워크 특성을 고려한 보안천이 협약, 에너지 효율성, 메타데이터의 기밀성 메시지와 개체에 대한 무결성, 서비스 거부 공격을 종합적으로 고려한 일반적인 유비쿼터스 컴퓨팅과 센서 네트워크 보안 환경에서 서비스를 보호하기 위한 초경량 객체보호 기술에 대하여 검토하기로 한다.

* 목원대학교 컴퓨터멀티미디어콘텐츠공학부 조교수, hjkang@mokwon.ac.kr, 011-9620-3205
** 남서울대학교 멀티미디어과 교수, bangkc@nsu,ac,kr, 010-9210-0480

Ⅰ. 서론

우리나라에 유비쿼터스 컴퓨팅이 소개되고 발전되는 과정에서 대체로 세가지 형태의 개념으로 조용한 기술로서, 눈에 띠이지 않는 컴퓨팅, 혹은 언제나 사용이 가능한 컴퓨팅, 어디에서나 사용이 가능한 컴퓨터를 가능하게 하는 기술인 유비쿼터스 컴퓨팅이다. 유비쿼터스 컴퓨팅 환경 아래에서는 수많은 컴퓨터 하드웨어, 센서 및 소프트웨어가 네트워크로 결합되면서 인간의 삶은 커다란 변화를 겪게 되었다. 이러한 변화는 컴퓨터나 네트워크를 의식하지 않는 상태에서 구애받지 않고 자유롭게 네트워크에 접근할 수 있는 환경인 유비쿼터스 환경으로 새로운 패러다임의 변화를 일으키고 있다. 유비쿼터스 환경으로의 변화에는 장소에 구애받지 않고 자유롭게 네트워크에 접근할 수 있는 온디맨드 컴퓨팅 기술 이 기반을 이루고 있다. 유비쿼터스 컴퓨팅, 유비쿼터스 네트워크사회에 사용되는 경우 퍼버시브(pervasive)컴퓨팅이라 불리우게 된다[1],[2]. 유비쿼터스 컴퓨팅 환경에서는 모든 정보가 공유될 수 있고 악의 적으로 누구나 쉽게 접근할 수 있는 가능성이 있다. 이러한 측면에서 개인의 정보가 다른 사람에게 쉽게 유출되어 개인적인 사생활의 보장이 유실되는 세계가 될 가능성이 있다. 그 외 크래커에 의한 정보 유출, 바이러스, 컴퓨터 범죄, 프라이버시 침해 등 현재 가상 세계에서 벌어지고 있는 각종 부작용들의 증가로 이어질 수 도 있다. 예를 들어 개인정보나 구매내역이 기업들 사이에서 상업적인 목적으로 공유되고, 통행인의 얼굴을 인식해서 범죄 혐의자와 대조하는 무인 감시카메라에 이르기까지 많은 문제의 소지를 가지고 있다. 유비쿼터서 컴퓨팅 환경에서는 이와 같이 각 개체마다 많은 정보를 갖고 있으며, 또 이에 대한 정보를 수집, 분석하여 필요한 서비스를 알아서 해주는 서버도 필요할 것 이다. 여기서 필연적으로 개인의 정보를 어떻게 보호할 것이며, 필요한 서비스를 어떤 방법으로 안전하게 제공할 것인지에 대한 고려가 필요하다. 무선 인터넷 보안 연구자들은 무선 인터넷의 진보된 개념으로 유비쿼터스 환경 보안을 생각하며, 무선이라는 제약점과 모바일 장치의 제한된 전력을 고려하여 연산량이 적은 인증 프로토콜 개발에 그 초점을 두고 있다.

그림 1은 2010년의 유비쿼터스 네트워크의 전체 모습을 나타내었다. 2010년에는 언제 어디서든지 끊김없이 여러 가지 서비스를 자유로이 이용 가능한 네트워크가 실현되고 수백억개의 PC, 가전제품, 센서 등 다양한 단말기가 네트워크에 접속되고 개인인증이나 단말기의 응답속도가 현재의 수만배 빠른 속도로 실시간 인증이나 단말기 응답이 가능할 것으로 생각된다. 또 이용자 네트워크 이용면에서는 어디서든지 상황에 따라 통신 서비스가 이용 가능할 것으로 생각된다.네트워크 기능 또는 기술면에서는 코아 네트워크가 지금보다 더 유연하면서 대용량을 실현한다. 유비쿼터스 컴퓨팅에 대한 보안의 정의는 아직 개념정립이 정확히 이루어지지 않고 있고, 유비쿼터스 컴퓨팅의 응용분야에 따라서 그 분야에 맞는 보안의 여건이 달라질 수 있다.



<그림 1> 유비쿼터스 네트워크의 미래상 (2010년)

그렇기 때문에 정확한 보안의 개념 정립은 힘들 것이다. 하지만 각 분야에서 연구되어지는 보안의 요건들 중에는 공통된 것들이 많고, 필수적인 것들이 있으므로 이들을 중심으로 유비쿼터스 컴퓨팅과 센서 네트워크 보안의 요구 사항을 살펴보고자 한다. 본 논문에서는 유비쿼터스 컴퓨팅과 센서 네트워크 환경에 대한 보안에 대한 적절한 정의가 필요하고 기존의 보안 개념인 인증, 기밀성, 무결성, 가용성과 유비쿼터스 컴퓨터 특성을 고려한 보안천이 협약, 에너지 효율성, 메타데이터의 기밀성 메시지와 개체에 대한 무결성, 서비스 거부 공격을 종합적으로 고려한 일반적인 유비쿼터스 컴퓨팅 보안 및 센서 네트워크 환경에서 서비스를 보호하기 위한 초경량 객체보호 기술에 대하여 검토하기로 한다.

Ⅱ. 유비쿼터스 컴퓨팅과 센서 네트워크에서의 보안 요구사항

무선 센서 네트워크는 주변의 환경정보를 수집/분석하는 툴로서 매우 민감한 응용들에서 사용된다. 기존의 모든 다른 네트워크에 비해 센서 네트워크만의 매우 독특한 특성은 그 위협요소나 공격 방법, 그리고 이를 위한 보안대책의 면에서도 새로운 연구가 필요하다. 보안상의 관점에서 이슈가 되는 센서 네트워크의 주요 특징으로는 센서 노드의 제한된 능력, 센서 노드들에 대한 물리적 보안의 취약성, 그리고 브로드캐스팅을 주 통신 수단으로 하는 멀티 홉 라우팅 및 데이터 융합 등을 들 수 있다. 센서 네트워크의 실효성을 위해서는 센서들이 매우 제한된 연산, 통신, 저장능력 및 에너지 원만을 가질 수 있어 정상적인 동작을 위한 프로토콜뿐만 아니라 보안 기능의 사용 에도 많은 제약이 따른다. 또 한 센서 네트워크는 사람의 접근이 운영되므로 물리적인 공격에 매우 취약하다. 센서의 제한된 전력과 통신능력은 인접 노드로의 제한된 브로드캐스팅을 주요 통신방식으로 사용하도록 하여 일대일 통신에 비해 훨씬 많은 취약성과 보안상의 어려움을 가중시키고, 특히 전력이나 대역폭의 효율적인 사용을 위해 중간 노드들이 경유 메시지에 대한 부분적인 프로세싱을 해야 하는 특성은 보안을 더욱 더 어렵게 만든다[3]-[5]. 그림 2은 RFID/USN 정보보호 기술 적용 개념도이며 RFID와 USN Ad-hoc Network를 위한 초경량 저전력 RFID/USN 암호 및 인증 기술, RFID/USN 정보보호 미들웨어 및 보안관리 기술, RFID/USN 주문형 프라이버시 보호 기술에 대해서 BcN/IPv6망과의 연관성과 함께 표현하였다.

이러한 정보보호 기술은 RFID/USN 환경에서 사용자의 개인 프라이버시를 보호 및 관리할 수 있어서 안심하고 편리하게 RFID/USN 관련 서비스를 이용할 수 있도록 한다.보안의 목적은 인가되지 않은 사용자가 공유된 정보에 불법적으로 접근하거나, 사용자 공유 정보를 노출 및 변경을 하지 못하도록 하는 것이다. 일반적으로 보안에 대한 요구는 그게 3가지 요건으로 말할 수 있는데, 기밀성(confidentiality), 무결성(integrity), 가용성(availability)이 그 3가지이다[6]. 기밀성은 인증되지 않은 사용자가 중요한 정보를 가로채는 것을 방지하는 것을 말하고, 무결성은 인증되지 않은 사용자가 중요 정보를 변경하는 것을 방지하는 것을 말한다. 또한 가용성은 시스템이 요구되는 수준의 인정한 기능을 수행할 수 있도록 하는 것이다. 예를 들어 Web 수준의 일정한 기능을 수행할 수 있도록 다운되지 않고 정상적으로 동작할 수 있도록 하는 것이다. 위의 모든 방어적 성격이 인증된 사용자와 인증되지 않은 사용자의 구분을 원칙으로 하고 있으므로, 인증(authentication) 또한 중요한 보안적 요소라고 할 수 있다. 그러나 기존의 보안 요건을 그래

도 적용할 경우 유비쿼터스 컴퓨터 환경에서의 적합한 해결안이 될 수 없다. 유비쿼터스 컴퓨팅 환경에서는 모든 정보가 공유될 수 있고, 누구나 악의적으로 쉽게 접근할 수 있는 가능성을 가지고 있다. 즉, 개인의 정보가 다른 사람에게 쉽게 유출되어 개인적인 사생활을 보장이 유실되는 세계가 될 가능성이 있다. 그 외 크래커에 의한 정보 유출, 바이러스, 컴퓨터 범죄, 프라이버시 침해, 저작권 침해 등 현재 가상 세계에서 벌어지고 있는 각종 부작용들의 증가로 이어질 수도 있다. 유비쿼터스 컴퓨팅 환경에서는 이와 같이 각 개체마다 많은 정보를 갖고 있으며, 또 이에 대한 정보를 수집, 분석하여 필요한 서비스를 알아서 해주는 서버도 필요할 것이다. 여기에는 필연적으로 개인의 정보를 어떻게 보호할 것이며, 필요한 서비스를 어떤 방법으로 안전하게 제공할 것인지에 대한 고려가 필요하다. 즉, 인증은 보안 정책모델기반으로 하며, 기밀성은 에너지 효율이 높은 암호 알고리즘 개발이 필요하며, 무결성은 크게 메시지에 대한 무결성과 개체에 대한 무결성으로 나우어 전자는 체이닝 프로토콜, 후자는 tamper protection 기법으로, 가용성은 암호퍼즐 등을 통해서 보장할 수 있다. 일반적으로 계층간 통신이나 분산 시스템에서 보안은 사용자나 개체에 대한 신뢰를 할 수 있는지 또한 주고받는 메시지를 신뢰할 수 있는지에 관한 인증, 주고받는 메시지에 대한 내용을 비밀로 하는 기밀성, 미시지가 통신 중간에 변질 되지 않았음을 검증하는 무결성과 많은 데이터 유입에 대해 어떤 방법으로 시스템의 서비스를 제공할 것인지에 관한 가용성의 관점으로 많이 다루어진다.

1. 인증

유비쿼터스 컴퓨팅 시스템은 일시적으로 네트워크에 연결이 되며, 그 연결은 확실한 연결성을 보장하지 않는다. 유선에서 사용되는 기존의 인증 방법은 인증을 위해 인증 서버나 철회 서버에 온라인 연결을 해야 한다. 유비쿼터스 컴퓨팅환경에서는 일시적이고 불확실한 연결을 제공하므로 인증을 위해 연결을 시도하는 과정에서 연결에 대한 불확실성으로 인해 합법적이지 않은 사용자에 대해 합법적인 사용자로 인증할 가능성이 발생한다. 따라서 불확실한 연결에 대비한 인증 솔루션이 필요하다.

유비쿼터스 네트워크에서는 어떤 개체가 일시적으로 접속을 위한 인증 서비스 요구가 많이 필요하게 될 것이며, 이러한 인증에 대한 요구가 제어 장치나 제어 대상 개체의 변화에 따라서 수시로 바뀔 수 있다. 이를 해결하기 위해서는 보안성인 보장되는 보안 천이 협약이 필요하다[1]. 보안 천이 협약을 구체적으로 설명하면 TV, 오디오, DVD, VCR, 에어컨, 히터 등의 원격 제어 장치가 거실 탁자 위에 놓여 있다고 가정하면, 유비쿼터스 컴퓨팅 환경에서는 모든 가전제품을 모바일 단말기와 같은 하나의 제어 서버를 두고 각 제품을 원격으로 제어할 수 있을 것이다. 만약 하나의 장치로는 모든 디지털 전자 제품들을 제어할 수 있다면, 각 제품의 원격 제어장치는 필요 없다. 그러나 제품을 구매한 후에 모바일 단말기가 각각이 디지털 전자 제품을 제어할 수 있도록 어떤 협약을 설정하는 절차가 필요하다. 이러한 경우에 필요한 보안 사항들을 고려해보자. 손님이 집을 방문했을 때 주인의 허락 없이 전자 제품을 동작시키는 것을 제한할 필요가 있다. 그리고 모바일 단말기가 제어하고 있는 제품들을 교체하거나 처분할 수 있어야 하며, 모바일 단말기가 고장이 났을 때 각각의 전자 제품의 제어 기능을 잃지 않고 다른 모바일 단말기로 교체가 가증해야 한다. 따라서 모바일 단말기가 전제 제품을과 맺은 협약은 수정 가능하고 또는 복구 가능해야 한다. 안전 천이 협약은 기존 환경과는 달리 제어자치, 제어 대상 개체가 수시로 바뀔 수 있으므로 협약

또한 수시로 바뀔 수 있음을 뜻한다. 안전 천이 협약은 기존의 인증 시스템을 기반으로 하여 사용 목적에 맞는 보안 정책을 필요로 한다.

2. 기밀성

인증 서비스에는 인증과 더불어 두 개체 간에 공유키 교환을 하게 되며 이 공유기는 대칭키 암호 시스템 키로 사용된다. 따라서 두 개체 간 인증 단계를 통과하면 안전한 비밀 통신 채널을 제공할 수 있으므로 쉽게 기밀성을 보장할 수 있다. 그러나 유비쿼터스 컴퓨팅 환경에서의 기밀성을 보장하기 위한 컴퓨팅에 따르는 에너지의 사용량이 중요한 고려사항이다.

유비쿼터스 컴퓨팅 장치는 주로 작은 장치로 이루어져 있어 이로 인해 새로운 제약 조건이 생긴다. 이러한 특징들은 배터리 전력에 한계가 있어서 빠르고 계산 능력이 뛰어난 프로세서를 유용하게 사용하는데 한계를 가지고 있다. 유비쿼터스 컴퓨팅 장치들은 아주 작은 소형 프로세서들을 갖고 있으며, 이 프로세서들은 공개키 암호와 같은 계산을 하기에는 속도가 늦기 때문에 적합하지 않다. 이러한 제약 조건들은 무선 인터넷이나 블루투스 등이 발달하면서 널리 알려진 사실들이며, 이를 해결하기 위한 방안으로서 사전 계산 등의 방법이 많이 이용되었다. 하지만 배터리는 유한하고 적은 에너지를 갖고 있기 때문에 사전 계산 방법은 그 순간의 처리 속도를 향상시킬 수는 있으나, 배터리의 소모 전력은 사전 계산을 한 것과 하지 않은 것의 차이가 없기 때문에 배터리 전력의 한계를 극복하지 못한다. 따라서 소형장치에 암호 시스템의 효율성을 평가할 때나 암호 시스템을 설계 할 때 초당 비트 처리율 보다 줄(joule)당 비트 처리율을 고려하여야 하며, 줄당 비트 처리율이 좋은 칩 개발과 암호 알고리즘 개발이 필요하다. 아울러 많은 연산량을 갖는 공개키 암호 시스템의 사용을 최대한 줄이는 방향으로 연구가 되어지거나, 효율성이 좋은 공개키 암호 시스템 연구가 필요하다. 개인의 프라이버시의 침해를 막는 것이 중요하다. 그러므로 모바일 단말기와 같이 여러 장치와 통신을 하며 개인의 정보를 모으는 서버장치는 저장된 정보를 비밀로 유지하는 것이 매우 중요하다. 그리고 유비쿼터스 컴퓨팅 환경에서는 꼭 필요한 보안 요구 사항 중의 하나가 메타데이터를 보호하는 것이다. 익명성, 추적성과 트래픽 분석 등과 같은 분야는 지금까지 소홀하게 다뤄진 기밀성의 한 부분이다. 암호화는 주고받는 메시지의 내용이 무엇인지에 대한 비밀유지는 가능하다. 그러나 언제, 누구에게, 누구로부터 전달되는 메시지인지는 비밀로 유지할 수가 없기 때문에 사용자의 프라이버시가 드러날 우려가 있다. 통신 주체가 누구인지 감추는 역명성은 어려운 문제이다. 만약 익명성이 보장될 경우 익명성으로 인한 공격자 추적이 어려울 것이다. 따라서 익명성을 보안 요건으로 고려할 때는 익명성 분장에 따른 공격자 추적 방안도 함께 연구되어져야한다. 그리고 트래픽 분석에 대한 보호대책은 아직 어려운 실정이다. 사용자의 관점에서 사용자의 위치에 대한 프라이버시와 한 사용자에 대한 메시지 트랜잭션을 동일 사용자의 다른 메시지 트랜잭션과 연결짓는 것을 어렵게 만드는 방법도 개인의 프라이버시를 위해 고려되어야 한다. 그렇지 않다면, 우리가 추구하는 유비쿼터스 컴퓨팅 환경이 사용자의 프라이버시를 침해하는 감시자의 역할을 하게 될 것이다.

3. 무결성

기본적인 무결성 문제는 하나의 개체에 다른 개체로 가는 메시지가 제3의 악의적인 공격자에 의해 공격 받지 않게 하는 것이다. 다시 말해서, 상대방 개체와 메시지를 주고받을 때 메시지의 내용이 변경되지 않

은 원본 메시지를 주고받을 때 내용이 변경되지 않은 원본 메시지를 전달하는 것을 보장하는 것이다. 이것은 메시지 인지코드(MAC : message Authentication code)와 같은 잘 알려진 암호학적인 메커니즘을 사용하면 큰 문제없이 메시지 무결성을 보장할 수 있다. 인증을 하기 위해 브로드캐스팅되어지는 데이터에 전자서명을 사용하지 않는다면, 인증을 하기 위해 브로드 캐스트되어지는 데이터를 변경하지 못하도록 전자서명 역할을 대한 할 것이 필요하다. 이는 체이닝 프로토콜로 써 해결이 가능할 것이다.

유비쿼터스 컴퓨팅 환경에서 가장 심각한 무결성 문제는 이동중인 메시지의 무결성이 아니라 유비쿼터스 장치 자체에 대한 무결성이다. 이는 유비쿼터스 장치에 공격자가 사용자의 정보를 유출시키기 위해 인증과는 무관하게 악의적인 조작이 가능할 수도 있고, 장치 자체를 다른 것으로 변경시킬 수도 있다. 어떤 측면에서 인증과 유사한 명이 있지만, 약간의 차이는 있다. 인증에서의 기본 가정은 네트워크는 공격자들의 공격에 노출되어 있고, 안전하지 못하지만, 네트워크에 소속된 개체들은 그들의 비밀을 지킬 수 있는 능력이 있다는 것이다. 유비쿼터스 컴퓨팅 환경에서는 이러한 가정도 받아들이지만, 공격자들이 네트워크에 소속된 개체들을 바꿀 수 있다는 가정도 한다. 이를 해결할 수 있는 방법이 physical tamper protection 솔루션이다. 높은 등급의 tamper resistance를 제공하면, 공격자는 장치 내부에 유지되고 있는 비밀들에 대해 수정이나 접근조차 불가능하게 할 수 있으나 이는 가격이 너무 비싸고 어려운 문제이다. 이러한 이유로 매수를 시도하는 공격자들을 추적할 수 있게 하는 tamper evidence를 이용한다.

4. 가용성

유비쿼터스 컴퓨팅 환경에서 흥미로운 점은 보안과 전력 소비와의 상관관계 있어서 더욱 세련된 서비스 거부(DoS : denial-of-service)공격이 출현하게 된다는 것이다. 유비쿼터스 장치는 제한된 배터리 에너지를 가지고 있기 때문에, 그것을 아끼기 위해서 필요시에만 깨어 있고 불필요 시에는 휴명 상태에 접어들게 할 수 있다. 이때 효과적인 공격방법은 배터리가 방전될 때까지는 장치를 깨어 있게 하는 것이다. 배터리가 방전되고 나면, 공격자는 유비쿼터스 장치를 사용 불가능하게 만든 후 사라질 것이다. 이러한 잔인한 기법을 일컬어 sleep deprivation torture 라 한다. 인증이 이러한 공격을 막을 수 있을 것이라고는 생각할 수 있으나, 실제적으로는 막을 수가 없다. 인증은 서비스 요구가 있을 때 합법적인지 아닌지를 구분해 준다. 그러나 Web 서버 같은 경우에는 서비스 요구자를 거절 할 수 없다. 서버의 딜레마는 서비스 요구자에게 질의에 대한 응답을 할 것인지 아닌지를 결정하는 것이다. 서버가 서비스 요청이 있을 때, 이 요구를 서비스 거부 공격으로 받아들이고 응답을 주지 않았으나, 실제로는 요청에 대한 응답을 기다리는 순수한 의도의 서비스 요구일 수도 있다. 서비스 거부 공격자들에게 반복적으로 신원확인을 요구하는 것은 효과 없는 일이다. 서비스 요구자의 신분 정보를 쉽게 속일 수 있으며, 분산 서비스 거부 공격도 가능하기 때문이다. 해결 방안으로는 서비스 요구자들에게 우선순위를 부여하는 것이고, 중요하지 않은 요구에 대해 할당할 자원을 줄이고, 중요한 요구에 대한 자원의 할당을 늘리는 것이다. 이것은 좀더 중요한 사용을 위해 서비스의 등급을 보장하는 것이다. 물론 이것은 서비스 사용이 허가된 내부 공격자에 의한 공격에는 취약하다.

또 하나의 접근 방법은 돈을 지불하면 서

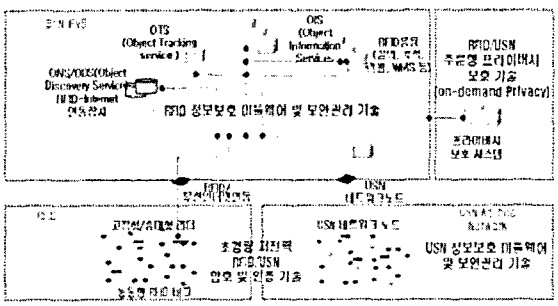
비스를 제공하는 방법이다. 자원에 접근하기 위해 요금을 지불하기 전까지 서버는 클라이언트가 자원을 무분별하게 요청하는 것을 제한할 수 있다. 실제 돈을 요금으로 부과하는 것이 비실용적이라면, 서버는 서비스 교환을 위한 약간의 비용이 드는 자원에 대한 희생을 강요하여 위의 방법과 같은 제한적인 전략을 사용할 수 있다. 서버는 클라이언트에게 암호적 퍼즐을 풀게 하거나, 인간이 대답하기는 쉽고 기계가 하기는 어려운 질문을 하는 방법을 상용할 수 있다. 후자는 계층별 응용에 보다 적합하고 전자는 유비쿼터스 컴퓨팅 환경에 좀더 적합하다.

5. 권한 관리

유비쿼터스 컴퓨터 환경은 요러가지 형태의 서비스가 제공될 것이다. 따라서 공공장소 등에서 여러 사용자가 자원을 공유할 수 있기 때문에 공유된 자원에 대한 접근제어가 필요하며 공유된 장치에 대한 데이터의 비밀성도 보장되어야 한다. 또한 서비스에 따라 자원을 사용하는 것에 대하여 과금할 수 도 있다. 이를 위해서는 서비스 제공자들의 신뢰성을 식별하고 검증하는 객체 식별과 인증이 필수 적이고 서비스 제공의 신뢰 수준에 따라 사용자 정보의 접근정보를 달리하는 사용자 정보 접근제어가 필요하다.

6. 안전한 핸드오프

유비쿼터스 컴퓨팅 환경에서 무선 공중망을 이용하여 서비스를 제공할 경우 안전한 핸드오프 기술이 고려되어야 한다. 안전한 핸드오프는 사용자 인증, 키관리 정책, 암호화 알고리즘 협상, 그리고 과금 정책을 포괄적으로 고려하여 구현 되어야 한다. 동일한 서브넷에 위치한 액세스 포인트 사이를 이동할 때 핸드오프 보안이 제공되어야 하고 핸드오프 과정에서 보안 접속 유지와 보안 컨텍스트 정의 및 관리등을 고려하여야 한다. 그리고 무선 센서 네트워크에서 글로벌 로밍 서비스가 제공되기 위해서는 분산 인증 및 실시가 s 패킷 과금에 대한 문제도 해결해야 한다.



<그림 2> RFID/USN 정보보호 기술 적용 개념도

Ⅲ. 유비쿼터스 센서 네트 워크의 보안 기술

무선 센서 네트워크로 널리 사용되어질 수 있는 기술로서 실 세계에서 무선 센서 네트워크 서비스 구성에 대한 연구가 개발이 활발하게 이루어져 왔다. 점차 센서 네트워크 기반의 서비스에 대한 기술이 구체화 되어 지면서 센서 네트워크상에서 보안에 대한 필요성이 대두되어지고 이에 대한 보안 기술에 대한 연구가 활발해지고 있다. 일반적으로 센서 네트워크는 컴퓨팅 환경과 비교해서 제한된 CPU, 저장 공간, 대여폭, 전원 등의 제약 사항을 갖는다. 본 연구에서는 라우팅 프로토콜의 보안용으로 널리 사용되는 SPINS(Security protocols for srnsor networks)[7]에 대해 간략히 살펴본다.

SPINS는 센서 네트워크 보안을 워한 기본적인 보안 도구로 점대점 토신보안을 위한 SNEP(Secure Network Encryption Protocol)과 브로드캐스트 메시지의 인증한 μ

TESLA(Micro Timed Efficient Stream Loss-tolerant Authenti-cation)로 구성되어있다. SNEP은 RC5 CTR 모드와 CBC-MAC을 기반으로 하는 암호화 및 인증을 위한 프로토콜로 두 통신 센서들 간의 공유 카운터를 기반으로 하는 CTR 모드를 사용하여 데이터의 신선도를 보장한다. 통신 효율을 위해 카운터는 메시지와 함께 전송하는 것이 아니라 두 통신 노드가 매 블록마다 공유 카운터를 증가시켜 자체 관리를 하고, 카운터의 초기 공유나 재동기를 위한 별도의 카운터 교환 프로토콜을 제공한다. CTR모드를 사용하므로 암호화로 인한 메시지 팽창은 없으며 8바이트의 MAC이 2바이트의 CRC를 대신하여 6바이트의 오버헤드가 발생한다. SNEP을 위한 키 관리는 베이스 스테이션과 각 노드 사이의 링크키를 기반으로 하며 이 키로부터 각 방향으로의 암호화키와 MAC키를 유도하여 사용한다.

SPINS의 가장 큰 공헌은 브로드캐스트 메시지에 대한 인증기능을 제공할 수 있는 μTESLA 프로토콜을 제안한 것이다. 이는 디지털 서명과 방향 키 체인을 이용한 기존의 TESLA 프로토콜을 제약된 환경의 센서 네트워크에 적합하도록 비밀키 암호 기반으로 수정한 것이다. TESLA 프로토콜의 기본 아이디어는 일방향 키 체인과 키의 지연노출을 이용하여 비밀을 구현할 수 있다는 것이다[9].

우선 송신자는 임의의 비밀키 Kn을 선택하여 길이 n인 키 체인의 초기값으로 삼아 일방향 함수(one-way function) f를 이용하여 n개의 키 체인 Ki=f(Ki+1) (i=n-1, ... 1,0)을 생성하여 저장해 둔다. 키 체인의 마지막 값 K0(key chain commitment)는 모든 수신자들에게 인증 가능한 방법으로 전달한다. 각키 Ki는 time interval i에서의 MAC 키로 사용하며 일정한 지연시간 (최소한 round-trip delay보다는 큰 time interval) 후 Ki를 노출시켜 모든 수신자가 이를 이용하여 이전의 수신 메시지에 대한 MAC을 검증하게 하는 것이다.

TESLA/μTESLA는 인방향 키 체인의 지연노출을 기반으로 브로드캐스트 메시지의 인증에서가장 문제가 되는 키 관리 문제를 간단히 해결하였다는 점에서 큰 의의를 가진다. 즉 송신지는 임의의 비밀키를 초기값으로 선택할 수 있고, 단지 key chain의 맨 마지막 값만 모든 수신자들에게 비밀유지가 필요 없이 인증 가능한 방법으로만 전송해 주면된다. 단점이라면 수신자가 메시지의 MAC에 사용된 키가 노출된 때까지 일정한 지연시간 동안 패킷들을 저장하고 있어야 하며(DoS 공격에 취약), 또한 모든 수신자들이 느슨하게라도 클럭의 동기가 맞아야 한다는 점이다.

TESLA에서는 마지막 키 체인 값의 전송을 위해 베이스 스테이션이 디지털 서명을 이용하여 브로드캐스트 하였으나 μTESLA에서는 센서 네트워크의 제약을 고려하여 이를 베이스 스테이션과 노드간의 공유키를 이용한 MAC 기반의 유니캐스트로 수정하였다. 이는 공개키 암호의 사용을 피함으로써 계산이나 통신, 에너지 소모 등의 오버헤드를 상당히 줄였지만 대규모 센서 네트워크에서는 확장성에 있어서 여전히 큰 문제가 될 수 있다. Liu 등은(TESLA를 다단계 키 체인(multi-level key chain) 방식으로 확장하여 초기의 유니캐스트 통신을 제거하고 DoS 공격에 대한 저항성을 가질 수 있는 개선방안을 제안하였다[8].

아직은 많은 문제점이 지적된 수 있으나 TESLA/μTESLA는 애드혹 네트워크의 각종 라우팅 프로토콜의 모안에 필수적인 브로드캐스트 메시지에 대한 인증을 가장 널리 사용되는 프로토콜이다.

Ⅳ. 결론

유비쿼터스 컴퓨팅 환경은 차세대 정보기술로서 미래에 많은 편리함을 가져다 줄 것

으로 많은 사람들이 기대하고 있다. 실생활에 많은 편리함을 가져주는 만큼 악의적인 공격자로 인해서 개인의 정보 유출과 같은 큰 희생을 강요받을 가능성이 존재하는 것이 현실이다.따라서 유비쿼터스 컴퓨팅 환경에 대한 보안에 대한 적절한 정의가 필요하고, 기존의 보안 개념인 인증, 기밀성 무결성, 가용성과 유비쿼터스 컴퓨팅과 센서 네트워크 특성을 고려한 보안 천이 협약, 에너지 효율성, 메타데이터의 기밀성, 메시지와 개체에 대한 무결성, 서비스 거부 공격을 종합적으로 고려한 일반적인 유비쿼터스 컴퓨팅 및 센서 네트워크 보안환경에 적합한 보안 인증 기술은 개별적인 보안 인증 기술을 효과적으로 조합할 수 있는 연구 개발이 적합할 것 이다.

참 고 문 헌

1. M. Weiser, "Ubiquitous Computing," Http://www. ubiq.com/Hypertext/weiser /UbiHome.h tml.
2. Mark Weiser, "Hot Topics : Ubiquitous Computing" IEEE Computer October 1993.
3. H.Chan and A.Perrig. Security and privacy in sensor networks, IEEE Computer, pp. 103-105 Octber 2003
4. F.Hu, J.Ziobro, J.Tillett and N.Sharma, Secure wireless sensor networks: Problems and solutions, J.of SCI, to appear, 2004.
5. A.Perrig, J.Stankovic and D.Wagner, Security in wireless sensor networks, Commun. Of ACM, 47(5), pp. 53-57, June 2004.
6. Stajano, F., Security for Ubiquitous Computing, John Wiley & Sons, LTD., 2002.
7. A.Perrig, R.Szewczyk, J.D.Tygar, V.Wen and D.Culler, SPINS: Security protocols for sensor networks, Wire- less Networks 8, Kluwer Academy Publishers, pp. 521-534, 2002.
8. D.Liu and P.Ning, Efficient distr- ibution of key chain commitments for broadcast authentic cation in distributed sensor networks, NDSS' 03, 2003.
9. A.Perrig, R.Canetti, D.Song and .D.Tygar, Efficient and secure authe-ntication for multicast, NDSS'01, Feb. 2001.