uMC에서의 인증방안에 관한 연구

진광윤*, 서장원**, 최신형***
*강원대학교 컴퓨터공학과, **동서울대학 컴퓨터소프트웨어과
***강원대학교 전기제어공학부
e-mail:kyjin@kangwon.ac.kr

A Study about Authentication Method on the uMC

Kwang-Youn Jin*, Jang-Won Suh**, Sin-Hyeong Choi***
*Dept. of Computer Engineering, Kangwon National University
**Dept. of Computer Software, Dong Seoul College
***Division of Electrical & Control Engineering, Kangwon National University

요 약

현대 사회는 정보의 중요성이 부각되고, 유무선 네트워크 기술이 발전함에 따라 이동 중에 통신 서비스가 가능한 환경으로 변화하고 있다. 특히, 정보화 기기가 소형화, 지능화됨에 따라 이 기기들이 자유롭게 네트워크에 연결되어 정보를 공유할 수 있는 유비쿼터스(ubiquitous) 환경의 필요성은 더욱 증가하고 있다. uMC는 도시의 모든 기반 시설물을 관리, 관제하고 운용하는 새로운 개념의 도시 통합 관제 센터로 기존의 소방 방재센터, CCTV, 경찰청 등의 단위 시스템별 관제 센터 등을 물리적으로 통합하고 모든 시설물과의 네트워크 통신 등을 통합 관리하는 도시 관리의 중추적인 역할을 수행한다. 본 논문에서는 uMC에 접속하는 과정에서 접근 및 보안성을 강화하기 위해 네트워크상에 존재하는 단말기기에 효율적으로 IP를 할당하고 인증 할 수 있는 방안을 연구한다.

1. 서론

IT기술의 발달로 인해 어린학생부터 노인까지 모든 연령층에서 휴대폰은 하나씩 가지고 있으며, 이를 응용한 다양한 서비스가 제공되고 있다. 이와 더불어 현대 사회는 정보의 중요성이 부각되고, 유무선 네트워크 기술이 발전함에 따라 이동 중에 통신 서비스가 가능한 환경으로 변화하고 있다. 특히, 정보화 기기가 소형화, 지능화됨에 따라 이 기기들이 자유롭게 네트워크에 연결되어 정보를 공유할 수 있는 유비쿼터스(ubiquitous) 환경의 필요성은 더욱 증가하고 있다.

최근 들어, 이러한 추세에 맞추어 다양한 네트워크를 통합하고 동일한 인증 절차를 갖는 네트워크 환경을 도시에 적용한 u-City(ubiquitous City)가 많은 지자체를 중심으로 다양하게 건설되고 있다[1].

유비쿼터스 환경에는 너무나 많은 정보기기들이 존재하며, 그 기기들 사이를 연결하는 다양한 네트워크 기술은 필수적이라고 할 수 있다. 여기서는 사용자의 접속 인증 및 보안을 처리하기 위한 요소를 필요로 하며, 이런 이유로 인해 u-City에는 uMC(ubiquitous Management Center)가 존재한다. uMC는 도시의 모든 기반 시설물을 관리, 관제하고 운용하는 새로운 개념의 도시 통합 관제 센터라고 정의할 수 있다. 그 기능으로는 기존의 소방 방재센터, CCTV, 경찰청 등의 단위 시스템별 관제 센터 등을 물리적으로 통합하고 모든 시설물과의 네트워크 통신 등을 통합 관리하는 도시 관리의 중추적인 역할을 수행한다[2].

uMC는 u-City 내의 발생가능한 모든 서비스를 처리하도록 설계되어 있으며, 도시를 통제하는 중요한 기능을 수행함으로 내·외부의 악의적인 공격자로부터 해킹 및 서비스 공격 등의 목표가 될 경우 심각한 문제를 일으키게 된다. 특히, 모든 정보화 기

기 및 주민들과 네트워크로 밀접히 연결되어 있기 때문에 네트워크 접근을 통한 서비스 거부 공격, 스니핑 공격, 변조 공격 등 보안 취약점은 더욱 커진다[3].

따라서, 본 연구에서는 uMC에서의 인증 및 보안 방안에 대해 알아본다.

2. 관련연구

기존에 제시된 인증기술은 크게 단말 및 사용자 인증, 망 접속 및 서비스 인증으로 나눌 수 있다.

첫째, 단말 및 사용자 인증은 다음과 같이 정리할 수 있다.

인증 및 키 관리 기술은 무선 랜이나 와이브로, 근거리 접속망 등에서 접속 기기간의 신뢰 문제를 해결하기 위해 연구 되었으며, 대표적으로 PKM(Privacy Key Management)이 있다[4].

PKM 프로토콜은 단말 및 기지국 간의 합법적인 단말 및 사용자를 인증하고, 인증된 단말 및 사용자의 세션키 및 데이터 암호화 키를 관리하는 기능을 가지고 있다.

또한, PKM은 단말/사용자 인증과 단말/기지국 간의 인증을 수행하며, 합법적인 사용자인지를 인증하여 네트워크 서비스를 이용할 수 있도록 한다.

PKM의 초기 버전인 PKMv1은 단방향 인증 방식이며, 재연 공격이 가능하고, 인증키 전송시 보안 위협이 존재한다는 등의 단점이 내재되어 있다. 이후 이를 개선한 PKMv2가 발표되었다[5].

둘째, 망 접속 및 서비스 인증은 다음과 같은 특징을 가진다.

현재 서비스 되고 있는 대부분의 가입자 망의 경우 xDSL, 이더넷, PPP 등의 서비스가 존재하며, 해당 접속 방식에 따라 인증 방법의 차이가 존재한다. 일반적으로 아이디와 패스워드를 이용한 인증 처리 방식과 인증을 하지 않고 회선만으로 인증을 대신하는 방식으로 나뉜다. 이 두 가지 방법 중 하나를 이용하여 네트워크 인증을 마친 사용자는 서비스를 받고자하는 서버에 접속하여 해당 서버의 인증 시스템으로부터 인증을 요청하고, 인증 처리 후 시스템의 서비스를 받게 된다.

이때, 네트워크에서 별도의 인증 절차를 거친 후에 서버에서 독립적으로 다시 인증 절차를 수행하는 것은 인증 절차가 각기 다르고 일관성이 없어 되풀이 공격(replay attack) 이나 스푸핑 공격(spoofing attack) 등에 대한 보안 취약점이 존재하기 때문이다.

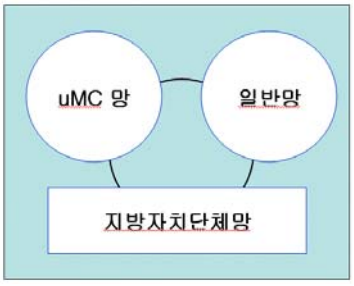
3. uMC에서의 인증방안

u-City에서의 네트워크 기술은 USN(Ubiquitous Sensor Network)과 IPv6 그리고 BCN(Broadband Conversions Network) 등의 인프라로 이루어져 있다. 최근에는 기술 개발과 더불어 새로이 등장하고 있는 HSDP, DMB, WiBro 등의 네트워크도 u-City 인프라에 포함될 수 있으나, 범위가 넓고 포괄적일 뿐만 아니라 u-City만의 차별성이 드러나지 않기 때문에 기본 인프라 영역에서는 제외한다. 다만 이를 반영 지원하기 위한 기술적 접근만은 고려한다.

u-City 네트워크를 설계할 때는 공공적인 요소가 중요시 된다. 따라서, 공공 시설물 및 센서의 위치를 고려하고 센서에서 발생하는 이벤트와 상시 발생 트래픽의 크기와 빈도 등을 감안하여 네트워크 설계를 하게 된다. 일부 서비스만을 위한 네트워크 인프라가 정의되는 경우도 있으며, 네트워크 인프라는 서비스의 범위를 포함하도록 구성하고 지리적인 위치도 고려해야 한다.

새로이 설계되는 신도시에서는 u-City를 적용할 경우 기존의 네트워크 시설이 존재하지 않으므로, 사용자에게 서비스를 제공하기 위해서는 인증 시스템이 필요하다. 그러므로, u-City에서의 네트워크 인증은 사용자 및 단말에 대한 인증을 말단 ER(Edge Router)이 AP나 NAS 등으로부터 접속 신호를 받아 인증 서버로 전달하여 처리해야 한다.

u-City의 네트워크 연동 구조는 다음의 [그림 1]과 같다.



[그림 1] u-City Network

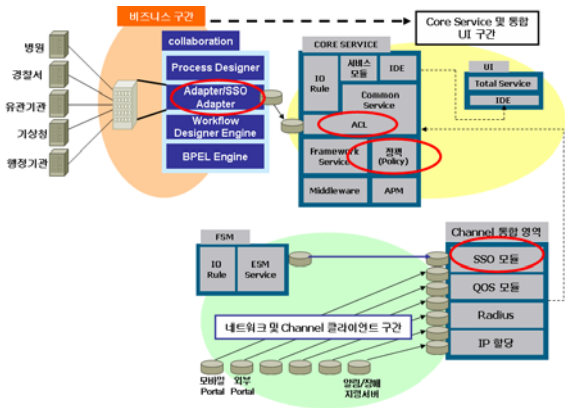
u-City의 구성요소에서 가장 중요한 것 중에 하나인 uMC는 u-City의 핵심요소로서, 기존 도시에서 서비스 별로 관제하던 방식을 하나의 통합 체제를

사용하여 관리하는 건물, 시스템, 운영 플랫폼을 의미한다.

uMC는 u-City 내에 설치되어지는 수많은 기기들과 이를 사용하고 관리하는 인력을 인증하고 식별해야하는 기능이 필수적이다. 그러므로, 기존의 다양한 관제 센터의 기능을 한 곳에서 수행하여야 하기 때문에 매우 복잡하고 정교하게 구성되어야 한다.

이러한 uMC는 가채널을 연계할 수 있는 채널 연계 서비스 영역과 일반 관제 센터의 기능을 하는 코어 서비스 영역, 사용자와의 인터페이스를 담당하는 인터페이스 영역 그리고 외부 시스템과의 연동을 담당하는 외부 연계 영역으로 구성된다.

사용자나 관리자가 u-City 네트워크에 접근한 후 uMC 장비 및 서버에 접근하기 위한 인증 방법으로 SSO를 적용한다. uMC에 적용되는 SSO 인증 구성은 그림 2와 같다.



[그림 2] uMC 인증 구성

uMC 인증 기술은 네트워크에 접속한 단말로부터 채널 및 인터페이스 구간으로 인증이 요구되면 채널 통합 영역을 거쳐 SSO 인증 모듈로 전달되어 인증을 처리한다. 그런 후에, 인증이 완료된 시스템에 대해 내부 정책을 적용하여 uMC 내 모든 시스템을 사용할 수 있도록 인증하는 역할을 한다. 이를 위해 uMC 내부에는 토큰을 인증하고 해석할 수 있는 SSO Adapter가 존재한다.

4. 결론

현대 사회는 정보의 중요성이 부각되고, 유무선 네트워크 기술이 발전함에 따라 이동 중에 통신 서비스가 가능한 환경으로 변화하고 있다. 특히, 정보화 기기가 소형화, 지능화됨에 따라 이 기기들이 자유롭게 네트워크에 연결되어 정보를 공유할 수 있는 유비쿼터스(ubiquitous) 환경의 필요성은 더욱 증가하고 있다. uMC는 도시의 모든 기반 시설물을 관리, 관제하고 운용하는 새로운 개념의 도시 통합 관제 센터로 기존의 소방 방재센터, CCTV, 경찰청 등의 단위 시스템별 관제 센터 등을 물리적으로 통합하고 모든 시설물과의 네트워크 통신 등을 통합 관리하는 도시 관리의 중추적인 역할을 수행한다. 본 논문에서는 uMC에 접속하는 과정에서 접근 및 보안성을 강화하기 위해 네트워크상에 존재하는 단말기기에 효율적으로 IP를 할당하고 인증 할 수 있는 방안을 연구한다.

참고문헌

[1] 황종성, "u-City의 개념과 구현 전략을 위한 이슈 분석", 정보과학회지, 제23권, Nov. 2005.

[2] 김방룡, "u-City 구축에 따른 생산 파급효과 추정", 응용경제, 제8권 3호, 2006.

[3] 한국정보보호진흥원, "u-City 프라이버시 보호 방안 연구", 연구보고서, Dec. 2006.

[4] 안현섭, "u-City를 위한 통합 인증 시스템 모델", 고려대학교 컴퓨터정보통신대학원 석사학위논문, 2008.

[5] S. Xu and C.-T. Huang. "Attacks on PKM protocols of IEEE 802.16 and its later versions", In Proceedings of 3rd International Symposium on Wireless Communication Systems (ISWCS 2006), Valencia, Spain, 2006.