한국산학기술학회논문지
Vol. 11, No. 2, pp. 576-583, 2010

통합관리센터를 이용한 인증 모델에 관한 연구

진광윤[1], 최신형[2*], 서장원[3]
[1]강원대학교 컴퓨터공학과, [2]강원대학교 제어계측공학과, [3]동서울대학 컴퓨터소프트웨어과

A Study on the Authentication Model using Integrated Management Center

Kwang-Youn Jin[1], Shin-Hyeong Choi[2*] and Jang-Won Seo[3]
[1]**Dept. of Computer Engineering, Kangwon National University**
[2]**Dept. of Control & Instrumentation Engineering, Kangwon National University**
[3]**Dept. of Computer Software, Dong Seoul College**

요 약 u-City에는 다양한 정보화 기기들이 존재하며, 정보화 기기 사이를 연결하는 다양한 네트워크 기술이 존재한다. u-City의 핵심 요소인 통합관리센터는 u-City 내의 모든 서비스를 처리하도록 설계되었으며, 도시를 통제하는 중요한 기능을 수행한다. 따라서 사용자의 인증 및 보안을 처리하기 위한 기술이 요구되며 이러한 기술은 통합관리센터에 필수적으로 구현되어야 한다. 본 논문에서는 기존의 인증 기술에 대해 설명하고, u-City 네트워크 환경에 적합한 인증 방법과 절차를 제안한다. 제안된 u-City 인증 모델은 u-City에 존재하는 정보화 단말기와 사용자를 인증하여 정당한 사용자에게만 IP를 할당하고, 할당된 사용자에 대해 정책에 따라 차별화된 권한을 부여함으로써, 통합관리센터의 보안에 중요한 역할을 한다.

Abstract U-City includes various information devices and network techniques, which connect among several information devices. Integrated Management Center, which is the core element of u-City, is designed to manage all services of u-City and carry out the control function for a city. Accordingly, u-City needs the methods of user authentication and security, so these methods must be implemented to integrated management center. This paper is devoted to describe some conventional authentication techniques, and authentication methods and procedures that may be available to u-City network context. Proposed u-City integrated authentication model assigns IP to only right user after authenticating information terminals and users in u-City and authorizes users according to the policy, so this model plays an important role for the security of integrated management center.

Key Words : U-City, Information Device, Authentication Model

1. 서론

최근 정보화 기기가 소형화, 지능화됨에 따라 이 기기들이 자유롭게 네트워크에 연결되어 정보를 공유할 수 있는 유비쿼터스(ubiquitous) 환경의 필요성은 더욱 증가하고 있다. 이러한 추세에 맞추어 다양한 네트워크를 통합하고 동일한 인증 절차를 갖는 네트워크 환경을 도시에 적용한 u-City(ubiquitous City)가 다양하게 건설되고 있다[1-3].

유비쿼터스 환경은 다양한 정보화 기기들이 존재하며, 그 기기들 사이를 연결하는 다양한 네트워크 기술이 존재하므로 사용자의 접속 인증 및 보안을 처리하기 위한 요소를 필요로 하고, 이런 이유로 인해 u-City에는 통합관리센터가 존재한다. 통합관리센터는 도시의 모든 기반시설물을 관리, 관제하고 운용하는 새로운 개념의 도시통합 관제 센터로 기존의 소방 방재센터, CCTV, 경찰청 등의 단위 시스템별 관제 센터 등을 물리적으로 통합하고 모든 시설물과의 네트워크 통신 등을 통합 관리하는

*교신저자 : 최신형(cshinh@kangwon.ac.kr)
접수일 10년 01월 12일 수정일 10년 02월 17일 게재확정일 10년 02월 24일

도시 관리의 중추적인 역할을 수행함으로 내・외부의 악의적인 공격자로부터 해킹 및 서비스 공격 등의 목표가 될 경우 심각한 문제를 일으키게 된다[4,5]. 따라서 통합관리센터는 접근 가능한 모든 사람 및 컴퓨터, 모바일 폰, PDA 등 이기종 정보 기기에 대한 다양한 인증 및 보안 정책을 적용할 수 있어야 한다. 뿐만 아니라, 접속기기에 대한 인증과 접속된 기기를 사용하는 사람에 대한 인증도 반드시 수행해야 한다.

그러나 현재까지 u-City의 다양한 이기종 노드 및 사람에 대한 인증을 처리할 수 있는 방법은 낮은 수준이며, 기존의 인증 기술은 단말기만을 인증하는 MAC 인증, IP 인증 등의 개별적 인증 처리 방법만 존재하고 있는 상황이다[6].

본 논문에서는 통합관리센터에 접속하는 과정에서 접근 및 보안성을 강화하기 위해 네트워크상에 존재하는 단말기기에 효율적으로 IP를 할당하고 인증 할 수 있는 방안을 연구한다.

2. 기존 인증 기술

2.1 단말/사용자 인증

인증 및 키 관리 기술은 무선 LAN 이나 Wibro, 근거리 접속망 등에서 접속 기기간의 신뢰 문제를 해결하기 위해 연구 되었으며, 대표적으로 PKM(Privacy Key Management)이 있다[6]. PKM 프로토콜은 단말/기지국 간의 합법적인 단말/사용자를 인증하고, 인증된 단말/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[8].

2.2 망 접속 및 서비스 인증

현재 서비스 되고 있는 대부분의 가입자 망의 경우 xDSL, Ethernet, PPP 등의 서비스가 존재하며, 해당 접속 방식에 따라 인증 방법의 차이가 존재한다. 일반적으로 ID/Password를 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 시스템 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(spoofing attack) 공격 등에 대한 보안 취약점이 존재하기 때문이다.

2.2.1 망 인증 기술

현재 IP를 할당받기 위한 망(network) 인증 기술로는 고정 IP 할당 방식과 가변 IP 할당 방식이 존재한다. 고정 IP 할당 기술의 경우 IP address를 모르면 접속이 불가능하기 때문에 인증 절차를 거치지 않는 무인증 기능을 사용하고 있으며, 사용자가 고정된 장소에 많이 존재할 경우에 적합하다. 또한, 고정 IP 할당 기술은 MAC 인증 방식을 택하고 있는데, 망 접속시 ID/Password 등의 인증 절차 없이 단말기 주소만으로 인증을 처리한다. 이에 비해, 가변 IP 할당 방식은 보통 사용자가 IP address를 할당 받아 일정 기간 혹은 일정 구간 동안 사용하고 사용이 끝난 후 IP address를 반납하는 방식이다. 가변 IP 할당 기술은 무선 구간이나 사용자가 IP 세팅을 일일이 지정하기 어려운 경우에 주로 사용한다. 일반적으로 가변 IP 할당 기술은 DHCP 서버를 사용하여 IP pool을 관리한다[9]. DHCP 프로토콜의 경우 보안이 고려되지 않은 프로토콜로서, 인증되지 않은 사용자가 DHCP 서버를 사용할 경우 보안에 심각한 문제가 발생할 수 있다. 따라서 공격을 예방하기 위해 접근 단말 호스트의 MAC 등을 제한하는 방식으로 IP 할당 정책을 제한할 수 있으나, 서비스 거부 공격 및 접근 공격에는 특별한 대안이 없는 상태이다.

2.2.2 서버 인증 기술

서버 인증 기술은 서비스를 제공하는 인터넷이나 인트라넷에서 독립적으로 관리 및 운영되고 있어 운영 주체마다 인증 방법이 각각 다르다. 가장 일반적인 서버 인증 기술로는 ID/ Password를 요구하는 것이며, 최근에는 보안성 강화를 위해 인증서를 이용해 암호화 하여 전송하는 시스템이 증가하고 있는 추세이다. 인터넷 사용이 급증하면서 사용자들이 접속하는 서버 역시 증가함에 따라 서로 다른 서버에 접속할 때마다 각각의 ID/Password를 관리해야하는 문제점이 발생한다. 특히, 인트라넷의 경우 서버마다 ID/Password가 다를 경우 혼선을 초래할 수 있으며, 반대로 같을 경우 노출의 위험에 직면하게 된다. 따라서 많은 서버에 대한 동일한 인증을 처리해야하는 문제점을 해결하기 위해 SSO(Single Sign On)가 제안되었

다. SSO는 한번 인증으로 인증 정책에 따라 다른 서버에 접속할 때에도 인증 받은 모든 서버에 동일한 권한으로 접속하는 것을 허용한다[10].

SSO의 동작 과정은 Radius 서버를 통해 인증 단계를 수행한 사용자는 도메인 내의 서버들에 접속할 경우 재인증 절차를 거치지 않고 SSO 서버에서 발행한 토큰을 사용하여 인증한다. 이때, SSO 서버에서는 각 사용자의 사용자 접근 제어에 대한 정보를 가지고 있어서 서비스가 선택되면 접근 권한을 부여한다. 또한, 사용자마다 SSO 서버에 개인의 프로파일이 존재하여 다른 서비스를 선택할 수 있는 통합 메뉴를 가지고 있으며, 다른 서비스로 이동할 경우에는 통합 메뉴에서 선택하고 별도의 인증 절차를 거치지 않는다. 인증서 발급은 일회성의 특징을 가지며 웹 브라우저의 쿠키(Cookie)와 같이 세션을 사용하면 사용자 정보를 일정 시간 동안 동일한 도메인만 사용할 수 있고, 특정 시간 동안에 특정 권한을 부여할 수 있다.

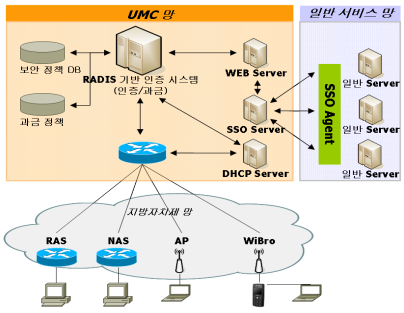
3. u-City 환경 정의

3.1 목표 u-City 네트워크 기반 설계

u-City에서의 네트워크 기술은 USN과 IPv6 그리고 BCN(Broadband Conversions Network) 등의 인프라로 이루어져 있다. 최근 들어, 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 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 1과 같다.



[그림 1] 목표 u-City 네트워크

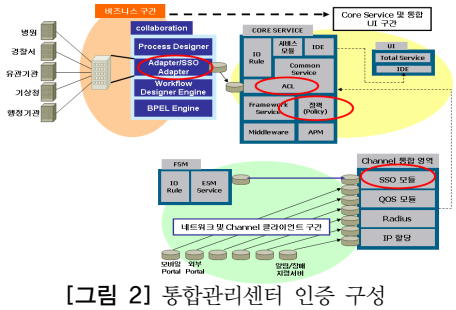
여기서, 네트워크는 지방자치단체의 망으로 자가 망이라 가정하고 제시하였다. 통합관리센터의 경우 네트워크 인프라와 내부 시설물들의 서버를 관리하는 운영 시스템을 포함한다고 가정하였다. 각 모델들의 인증 체계는 통합관리센터의 정책 DB 내용에 따라 사용자 별로 동일한 정책이 적용 가능하다.

3.2 통합관리센터 플랫폼

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

3.3 통합관리센터 인증 기술

사용자나 관리자가 u-City 네트워크에 접근한 후 통합관리센터 장비 및 서버에 접근하기 위한 인증 방법으로 SSO를 적용한다.



[그림 2] 통합관리센터 인증 구성

그림 2에서 통합관리센터 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 통합관리센터 내 모든 시스템을 사용할 수 있도록 인증하는 역할을 한다. 이를 위해 통합관리센터 내부에는 토큰을 인증하고 해석할 수 있는 SSO Adapter가 존재한다.

4. 인증 모델 설계

4.1 구성 요소

4.1.1 사용자 단말

사용자 단말은 접근 가능한 AP를 찾아 네트워크에 연결하기 위한 암호화 처리 알고리즘을 가지고 있어야 한다. 또한, 가변 IP를 할당 받기 위한 DHCP 모듈, 공개키 암호화 기능, PIN Number 입력 기능, Hash 기능을 포함하고 있어야 한다.

4.1.2 ER

ER(Edge Router)은 기존 인증 방법에서는 존재하지 않던 부분으로 사용자 단말에서의 단말 고유 값을 입력받아 인증 서버와 단말기의 접근 정보 및 서버의 정책을 결정하는 모듈이다. 이것은 암호화 기능은 없지만 IP Address 할당을 위한 DHCP 연결 기능과 Radius 서버 등을 연결하고, DHCP relay를 처리하는 기능을 가진다.

4.1.3 Radius 서버

Radius 서버는 CLIPS를 연결한 후 인증 정보를 확인하여 사용자의 정책을 추출하는 역할을 한다. 여기서, 단말 기반의 사용자 정책은 사용자 정책 DB와 단말 DB 정보를 통해 얻는다. Radius 서버의 역할은 다음과 같다.

- ER로부터 CLIPS 연결 처리
- 단말 정보로부터 정보를 추출하여 DB를 통한 사용자의 ACL 정책 정보를 추출하여 전달

4.1.4 SSO 서버

SSO 서버 모듈은 사용자 인증을 최종적으로 승인하고 해당 사용자를 인증하는 서버이다. 인증 완료 후 u-City 내의 통합관리센터 내부 모델에 인증 토큰을 할당하는 역할을 담당한다. SSO 서버의 역할은 다음과 같다.

- 사용자 기반의 세션키와 공개키를 암호화 하여 단말에 전달
- 사용자 PIN을 기반으로 한 단말기 상태 인증
- 내부 사용자 접속을 위한 토큰 생성
- 사용자 인증 후 정책의 허용 여부를 Radius 서버와 ER에게 전달

4.1.5 통합관리센터 구성

통합관리센터는 기존 도시에서 기능을 나누어 관리하던 방식을 하나의 센터로 통합해 놓은 것으로 매우 복잡한 구조를 가지고 있다. 또한, 현재 구축되었거나 또는 구축 예정인 u-City의 특성이 모두 다르기 때문에 다양한 형태의 통합관리센터가 존재할 수 있다. 따라서 본 논문에서는 통합관리센터 구성요소 중 인증 부문만을 다루며, 그 역할은 외부 채널 연계 서비스 영역과 외부 사용자 및 단말기기를 인증하는 부분만으로 한정짓는다. 아울러, 통합관리센터 모듈은 기본적인 암호 모듈과 인증 모듈을 가지고 해당 시스템과 접속 시 암호화 구간을 통해 데이터를 처리한다. 통합관리센터가 인증을 위해 가지고 있어야할 DB의 종류로는 인증 DB와 사용자 DB가 있다.

(1) 인증 DB

인증 DB는 단말기에 대한 정보를 가지고 있는 MAC DB 테이블과 단말기를 소유하고 있는 사용자에 대한 정보를 담고 있는 사용자 DB로 나뉘어 관리된다. MAC DB 테이블은 단말기가 네트워크를 사용할 수 있도록 이미 등록된 기기 인지를 확인하고 등록된 단말이라면 해당 단말을 사용하는 사용자를 식별하는 기능을 하며 표 1과 같은 필드들로 구성된다.

[표 1] MAC DB 테이블 필드

필드	내용
MAC	사용자 기기의 MAC
User_ name	사용자의 이름 혹은 ID
Access	망 인증 및 서버 인증을 사용하는 사용자인지 여부
Service_ID	망 접속 시 부가 서비스를 정의
IPv4/ IPv6	사용할 IP의 종류

(2) 사용자 DB

사용자 DB 테이블은 사용자를 인증하고 식별하는데 사용되며, 표 2와 같이 사용자의 공개키와 인증 정책 등을 담은 필드로 구성된다.

[표 2] 사용자 DB 테이블 필드

필드	내용
User_name	사용자의 이름 혹은 ID
Passwd	사용자의 패스워드(Hash 값)
PKI	사용자의 공개키
Policy	네트워크 사용 정책
ACL	사용자의 접근 허용 정책

4.2 망 접속 서비스 인증 절차

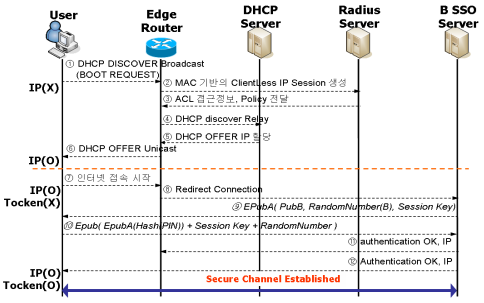
4.2.1 전체 인증 절차

망 접속시 인증을 위한 전체 인증 과정은 다음의 그림 3과 같다.

① 단말 사용자(User)는 네트워크에 접속하기 위해 단말 DHCP Client를 동작시켜 DHCP DISCOVER 패킷을 브로드캐스트 한다.

② 단말로부터 DHCP DISCOVER 메시지를 받은 ER은 단말에서 전송되어진 패킷에서 정보를 받아 MAC 기반의 CLIPS를 생성하여 Radius 서버에 전송한다.

③ Radius 서버는 해당 MAC Address를 가진 사용자를 DB에서 검색하고 그 사용자에 대한 Policy를 검색하여 ACL 접근 정보를 ER에 전달한다.



[그림 3] 전체 인증 절차

④ ER은 전송된 해당 내용을 분석하여 접근 권한을 확인하고 네트워크 연동 정책을 수립한다.

ACL에 의해 접근 권한이 확인된 사용자 단말의 패킷이라면 DHCP Discover Relay 메시지를 DHCP 서버에 전송한다.

⑤ DHCP 서버는 IP 할당을 요청한 단말이 인증 받은 단말로 확인 되었으므로 IP를 할당한다.

⑥ ER은 DHCP에서 받은 DHCP OFFERR를 사용자에게 전송하고 정책에 반영한다.

⑦ 단말이 인터넷 접속을 시작하면, ER은 해당 정책에 따라 네트워크 정책을 적용하고, 초기 접속인 경우에는 사용자 인증을 위해 SSO 서버로 접속은 Redirect 한다.

⑧ SSO 서버는 Redirect Connection을 받아 단말기 사용자의 DB를 검색하여 공개키를 추출하고, Nunce 값, Session Key 값, SSO 서버의 공개키 값 등을 추출된 공개키로 암호화하여 단말에게 전송한다.

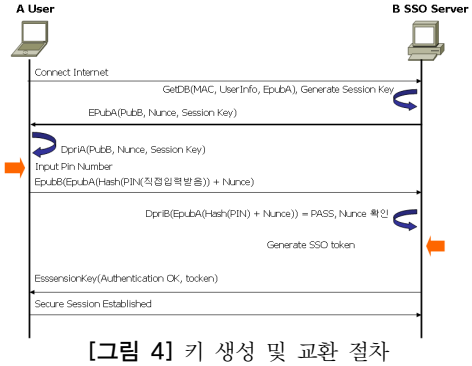
⑨ 단말은 자신의 개인키로 복호화 하여 Nunce와 Session Key를 추출하고 사용자의 입력으로부터 PIN Number를 입력받아 해쉬 후 자신의 공개키로 암호화한 후 SSO의 공개키로 암호화하여 SSO 서버로 전송한다.

⑩ SSO 서버는 자신의 개인키로 복호화하여 사용자가 전송한 PIN Number를 추출하여 사용자를 인증한다. 이로서 단말과 사용자가 모두 인증된다. ER과 단말에게 인증 완료 패킷을 전송하고 단말과 사용자 사이의 Session Key로 전송 구간을 암호화한다.

4.2.2 키 생성 절차

사용자와 SSO 인증 서버 사이의 암호화 전송과 키 생성 및 교환 순서는 그림 4와 같다.

사용자는 IP 할당을 받은 후에 인터넷 및 사이트 접속을 시작하고 해당 트래픽은 Redirect 되어 인증 서버로 전송된다. 이때, 인증 서버는 사용자 단말의 주소로부터 단말기의 소유자 정보를 추출한 후, 해당 사용자의 공개키와 사용자 접근 정보를 추출한다. 그런 후에, 단말과 SSO 인증 서버간의 암호화 구간의 통신을 위한 Session Key를 생성하여 추출된 사용자의 공개키로 암호화 후 단말기로 전송한다.



[그림 4] 키 생성 및 교환 절차

전송된 패킷은 사용자가 개인키로 복호화한 후 Session Key와 Nunce 값, SSO 서버의 공개키 값을 추출하여 저장한다. 추출된 SSO 서버의 공개키 값으로 사용

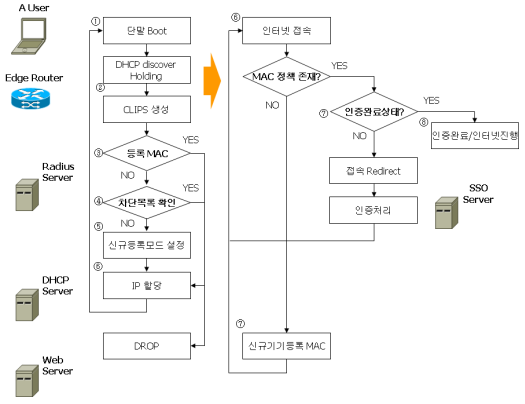
자로부터 직접 입력받은 PIN Number의 Hash 값과 Nunce 값을 포함하여 암호화 한다. 암호문은 SSO 서버로 전달되어 복호화 되고, 사용자 DB에서의 Password와 Hash 값을 검증함으로써 인증 여부가 확인된다.

인증이 완료된 사용자의 단말기는 다른 시스템의 별도 인증 절차 없이 인증 서버로부터 SSO 토큰을 생성 받아 Session Key로 암호화된 구간을 통해 안전하게 인증 정보를 전달 받게 된다. 단말기 및 사용자가 인증을 해결하지 못했을 경우 사용자의 모든 트래픽은 중단되고 패킷은 버려진다. 이와 반대로, 사용자가 인증을 풀었을 경우 Redirect 되었던 트래픽은 다시 전송되어 원활한 접속이 이루어진다.

4.2.3 신규 등록 및 정책 인증 흐름

네트워크에 처음 접속하는 단말은 네트워크를 인식하는 시점부터 IP가 할당되어 사용자 인증이 처리될 때까지 그림 5와 같은 인증 절차를 거친다.

만일, 초기 접속이 아닌 재접속의 경우 이미 인증이 완료된 상태이기 때문에 ER을 통해 더 이상의 Redirection은 발생하지 않고 바로 인증됨으로 네트워크의 접속 속도를 빠르게 할 수 있다.



[그림 5] 신규 등록 및 인증 흐름 절차

① u-City 네트워크 영역에서 단말기를 동작시키면 네트워크에 접속하기 위해 단말은 DHCP DISCOVER 메시지를 전송한다.

② ER은 DHCP DISCOVER 패킷을 DHCP 서버로 전송하지 않고 보류한 상태로 CLIPS를 생 성하여 인증 서버로 전송한다.

③ Radius 서버는 CLIPS를 통하여 전송된 MAC이 이미 등록되어 있는 사용자의 MAC 인지를 확인한다. 만일, 등록되어 있고 사용가능 하다면 IP를 할당한 뒤 정책을 적용하여 인증을 완료한 후에 접속을 허용한다.

④ 등록되어 있지 않다면, 차단 목록을 확인하고 공격자에 의한 차단 목록에 등록되어 있는지 확인한다. 만일, 확인 후 차단 목록에 등록되어 있다면 해당 단말기에서 발생하는 트래픽을 Drop 한다.

⑤ 공격자 목록에서 공격자로 확인되지 않으면, 신규 모드로 처리하여 사용자 등록을 실행하고 사용자의 공개키, 단말기, Password 등을 암호화하여 DB에 기록한다.

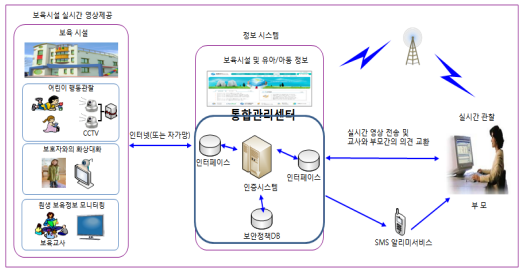
⑥ 신규로 접속시 망 인증 접속을 허가 받고 IP Address를 할당 받은 단말기는 네트워크를 통한 인터넷 접속을 시도한다.

⑦ 신규 등록 장비의 경우 MAC 등록을 처리하며, 신규 등록 장비가 아닌 경우 인증 처리를 위해 경로가 Redirect 처리되어 새로 인증을 실행한다. 이때, 인증 받은 장비는 사용자의 정책에 따라 인증을 수행한다.

⑧ 단말기 인증 및 사용자 인증이 완료된 상태에서 인터넷에 접속한다.

5. 사례적용

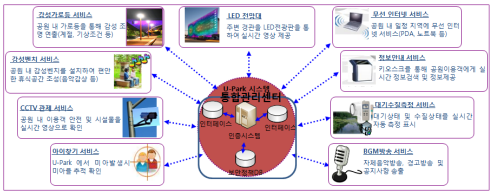
본 논문에서 제안한 통합관리센터를 진행 중인 지자체의 u-City 모델에 적용한 내용을 정리하면 다음과 같다. 적용한 u-City 모델은 총 4개 분야에서 15개의 목표모델을 구축하기 위한 것으로 해당 지자체의 향후 5개년간의 계획에서 제시된 모델로서, 유비쿼터스 지방전자정부구현과 첨단 U-인프라 구축을 목표로 한다. 본 논문에서는 15개의 목표모델 중 u-알리미서비스와 u-Park서비스에 적용해 본다.



[그림 6] u-알리미서비스

u-알리미서비스에서 통합관리센터의 역할은 자녀의 활동상태를 알려주는 CCTV 등 각종 단말기기로부터 수

집된 정보를 해당 학부모에게 모바일 기기를 통해 전달하거나 사용자 인증을 통해 접속한 원격 단말기를 통해 보여준다.



[그림 7] u-Park 서비스

u-Park서비스에서 통합관리센터의 역할은 공원에 설치된 가로등, 전망대 등 각종 단말기기를 정해진 정책에 따라 동작시키며 각종 센서로부터 수집된 정보를 분석하여 인증된 이용자들에게 전달하는 역할을 한다.

6. 결론

본 논문에서는 다양한 정보화 단말이 무선 인프라를 이용하여 u-City 서비스에 접속하기 위한 인증 방법을 제안하고 그 절차를 서술하였다. 제안된 통합 인증 모델을 사용할 경우, 신규 사용자의 IP 할당과 이미 인증된 사용자의 빠른 서비스 접속이 가능하며, 공격자의 경우 차단 목록을 통해 관리됨으로 사전 차단이 가능하다.

특히, 단말과 사용자 인증이 동시에 이루어지므로 보안의 단계를 높일 수 있다. 또한, 키 관리 기법으로 공개키를 사용하는 PKM을 사용함으로써 확장성이 높고, 기존 모델에 적용할 경우 새로운 모델의 추가 없이 AP/NAS 부분에 ER 기능을 하는 장비를 추가하고, 인증 모델만 갖추면 됨으로 적용성과 이식성이 매우 높다.

참고문헌

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

[2] 최창선, 황찬규, 김정욱, "도시공간과 유비쿼터스 기술의 융합에 관한 연구", 한국산학기술학회논문지 제10권 5호, 2009.

[3] 정기섭, 박성수, "u-City 구축과 범죄통제", 사회과학연구(동국대학교), 제12권 1호, 2005.

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

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

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

[7] 황찬규, “건설산업의 새로운 성장동력, 유비쿼터스 건설 분야 전망”, 한국산학기술학회논문지 제9권 2호, 2008.

[8] 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.

[9] D. Johnston and J. Walker, "Overview of IEEE 802.16 security", IEEE Security and Privacy Magazine, vol. 2, no. 3, pp.40-48, May-June 2004.

[10] Vladimir Brik, Jesse Stroik, Suman Banerjee: Debugging DHCP performance Internet Measurement Conference 2004 : 257-262.

진 광 윤(Kwang-Youn Jin) **[정회원]**

- 1984년 2월 : 서울산업대학교 전자계산학과 (공학사)
- 1987년 2월 : 건국대학교 전자계산학과 (공학석사)
- 2004년 2월 : 경남대학교 컴퓨터공학과 (공학박사)
- 1990년 3월 ~ 현재 : 강원대학교 컴퓨터공학과 교수

<관심분야>
정보보안, 임베디드시스템

최 신 형(Shin-Hyeong Choi) **[종신회원]**

- 1993년 2월 : 울산대학교 전자계산학과 (공학사)
- 1995년 2월 : 경남대학교 전자계산학과 (공학석사)
- 2002년 8월 : 경남대학교 컴퓨터공학과 (공학박사)
- 2003년 9월 ~ 현재 : 강원대학교 제어계측공학과 부교수

<관심분야>
정보보안, USN, 임베디드시스템

서 장 원(Jang-Won Seo) **[정회원]**

- 1992년 2월 : 서울산업대학교 컴퓨터공학과(공학사)
- 1996년 2월 : 숭실대학교 대학원 전산공학과(공학석사)
- 2000년 2월 : 숭실대학교 대학원 컴퓨터학과(공학박사)
- 2001년 9월 ~ 현재 : 동서울대학 컴퓨터소프트웨어과 교수

<관심분야>
정보보안, 디지털신호처리