u-City를 위한 통합 인증 시스템 모델

안 현 섭
고려대학교 컴퓨터정보통신대학원
hsan@dongbu.com

Modeling of unified authentication system for u-City

Hyeonseob An
Korea Graduate of Computer and Information Technology

요 약

유비쿼터스 사회가 도래함에 따라 유비쿼터스 기술을 도시에 적용한 u-City가 개발되고 있다. u-City는 다양한 정보화 기기들이 존재하며 정보화 기기 사이를 연결하는 다양한 네트워크 기술이 상존한다 u-City의 핵심 요소인 uMC(ubiquitous Management Center)는 u-City 내의 모든 서비스를 처리하도록 설계되었으며 도시를 통제하는 중요한 기능을 수행한다. 따라서 사용자의 인증 및 보안을 처리하기 위한 기술이 요구되며 이러한 기술은 uMC에 필수적으로 구현되어야 한다. 본 논문에서는 기존의 인증 기술에 대해 설명하고, u-City 네트워크 환경에 적합한 인증 방법과 절차를 제안한다 제안된 u-City 통합 인증 시스템은 u-City에 존재하는 정보화 단말기와 사용자를 인증하여 정당한 사용자에게만 IP를 할당하고, 할당된 사용자에 대해 정책에 따라 차별화된 권한을 부여 할 수 있으며, 따라서 uMC의 보안에 중요한 역할을 한다.

I. 서 론

현대 사회는 정보의 중요성이 부각되고, 유무선 네트워크 기술의 발전함에 따라 이동 중에 통신서비스가 가능한 환경으로 변화하고 있다. 특히 정보화 기기의 소형화 지능화됨에 따라 정보기기 들이 자유롭게 네트워크에 연결되어 정보를 공유할 수 있는 유비쿼터스(ubiquitous) 환경의 필요성은 더욱 증가하고 있다.

최근 이런 추세에 맞추어 다양한 네트워크를 통합하고 동일한 인증 절차를 갖는 네트워크 환경을 도시에 적용한 u-City(ubiquitous City)가 건설되고 있다[1][2][3][4].

유비쿼터스 환경은 다양한 정보화 기기들이 존재하며, 그 기기들 사이를 연결하는 다양한 네트워크 기술이 상존한다. 따라서 사용자의 접속 인증 및 보안을 처리하기 위한 요소를 필요로 하며, 이런 이유로 u-City에는 도시통합 관제 센터(uMC : ubiquitous Management Center)가 존재한다. uMC는 도시의 모든 기반 시설물을 관리, 관제하고 운용하는 새로운 개념의 관제 센터로 기존의 소방 방재 센터, CCTV, 경찰청, 등의 단위 시스템별 관제 센터 등을 물리적으로 통합하고 모든 시설물과의 네트워크 통신 등을 통합 관리하는 도시 관리의 중추적인 역할을 한다[3].

uMC는 u-City내의 발생가능한 모든 서비스를 처리하도록 설계되어 있으며, 도시를 통제 하는 중요한 기능을 수행함으로 내, 외부의 악의적인 공격자로부터 해킹 및 서비스 공격 등의 목표가 될 경우 심각한 문제를 일으키게 된다. 특히 모든 정보화 기기 및 주민들과 네트워크로 밀접히 연결되어 있기 때문에 네트워크 접근을 통한 서비스 거부 공격, 스니핑 공격, 변조 공격 등 보안 취약점은 더욱 커진다[4].

따라서 uMC는 접근 가능한 모든 사람 및 PC, 모바일 폰, PDA등 이기종 기기에 대한 다양한 인증 및 보안 정책을 적용할 수 있어야 한다. 뿐만 아니라, 접속기기에 대한 인증 뿐 아니라 접속된 기기를 사용하는 사람에 대한 인증을 수행해야 한다.

현재까지는 u-City의 다양한 이기종 노드 및 사람에 대한 인증을 처리할 수 있는 방법은 제시되어 있지 않으며, 기존의 인증기술은 단말기만을 인증하는 MAC 인증, IP 인증 등의 개별적 인증 처리 방법만 존재하고 있는 상황이다[5].

따라서 uMC에 접속하는 과정에서 접근 및 보안성 강화를 위해 네트워크상에 존재하는 단말기기에 효율적으로 IP를 할당하고 인증 할 수 있는 방안을 연구하여 내, 외부로 부터의 스니핑 공격 및 서비스 거부 공격 등으로부터 안전하게 서버와 데이터, 서비스를 보호할 수 있다.

u-City의 경우 다양한 네트워크 기술이 존재함으로 인해 그 복잡성이 높고, 그에 따른 인증 및 접근 과정에 대한 절차가 다양함으로 인해 연구의 범위는 단일 무선랜 기술인 802.11 네트워크 기술로 한정하고, 차후에 다양한 네트워크 기술로 확장을 논의한다.

II. u-City 환경 정의

1. 목적 u-City 네트워크 인프라

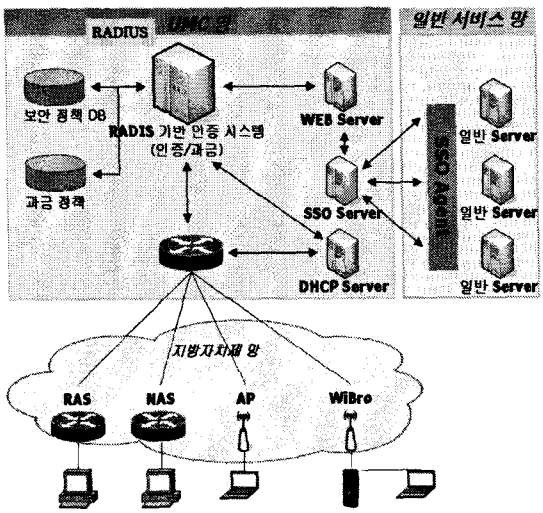
u-City의 네트워크 기술은 USN(ubiquitous Sensor Network) IPv6(IP version 6), BCN(Broadband Conversions Network)등의 인프라로 이루어져 있으며, 최근 기술 개발과 더불어 새로이 등장하고 있는 HSDP, DMB, WiBro 등의 네트워크도 포함될 수 있으나, 범위가 넓고 포괄적일 뿐 아니라, u-City 만의 차별성이 드러나지 않기 때문에 기본 인프라 영역에서는 제외하고, 다만

이를 반영 지원하기 위한 기술적 접근만을 고려한다.

u-City 네트워크를 설계할 때는 공공적인 요소가 중요시되므로, 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 포괄 하도록 구성하고 지리적 위치를 고려해야 한다.

새로 설계되는 신도시의 경우 u-City를 적용할 경우 기존의 네트워크 시설이 존재하지 않으므로, 사용자에게 서비스를 제공하기 위해서는 인증시스템이 필요하며, u-City에서의 네트워크 인증은 사용자 및 단말에 대한 인증을 말단 Edge Router가 AP나 NAS 등으로부터 접속 신호를 받아 인증서버로 전달하여 처리해야한다.

u-City의 네트워크 연동 구조는 [그림 1]과 같으며 네트워크는 지방자치단체의 망으로 자가 망이라 가정하고 제시하였다. uMC의 경우 네트워크 인프라와 내부시설물 들의 서버를 관리하는 운영시스템을 포함한다고 가정하였다. 또한 각 시스템들의 인증 체계는 uMC의 정책 DB 내용에 따라 사용자 별 동일한 정책을 적용 가능하다.



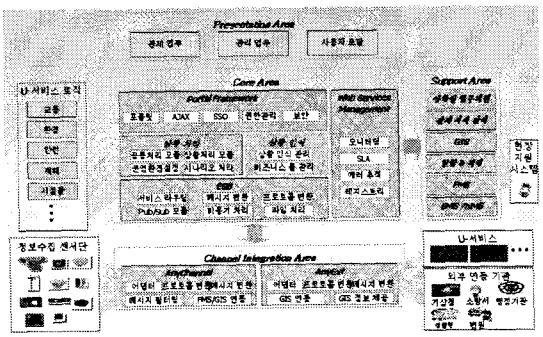
[그림 1] 목적 u-City 네트워트

2. uMC 플랫폼

u-City의 구성요소 중 가장 중요한 요소 중 하나인 uMC는 u-City의 핵심으로 기존 도시에서 서비스 별로 관제하던 방식을 하나의 통합 체제를 사용하여 관리하는 건물, 시스템, 운영 플랫폼을 뜻한다.

uMC는 u-City 내에 설치되어지는 수많은 기기들과 이를 사용하고 관리하는 인력을 인증하고 식별해야하는 기능이 필수적이며, 기존의 다양한 관제 센터의 기능을 한곳에서 수행하기 때문에 매우 복잡하고 정교하게 구성되어야한다.

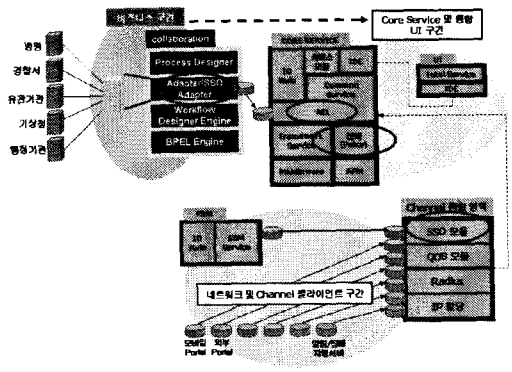
uMC는 가채널을 연계할 수 있는 채널 연계 서비스 영역과 일반 관제센터의 기능을 하는 코어 서비스 영역, 사용자와의 인터페이스를 담당하는 인터페이스 영역, 그리고 외부 시스템과의 연동을 담당하는 외부 연계 영역으로 구성된다, 해당 구성에 대한 플랫폼은 [그림 2]와 같으며, 이는 파주 운정지구에서 추진하고 있는 u-City uMC의 플랫폼이다.



[그림 2] uMC 플랫폼

3. uMC 인증 기술

사용자나 관리자가 u-City 망에 접근한 후 uMC 장비 및 서버에 접근하기 위한 인증 방법으로 SSO[6]를 적용한다. uMC에 적용되는 SSO 인증 구성은 [그림 3]과 같다.



[그림 3] uMC 인증 구성

네트워크에 접속한 단말로부터 채널 및 인터페이스 구간으로 인증이 요구되면 채널 통합 영역을 거쳐 SSO 인증 모듈로 전달되어 인증을 처리하고, 인증이 완료된 시스템에 대해 내부 정책을 적용하여 uMC 내 모든 시스템을 사용할 수 있도록 인증하는 역할을 한다. uMC내부에는 토큰을 인증하고 해석 할 수 있는 SSO adapter가 존재한다.

III. 통합 인증 시스템 설계

1. 구성 요소

1.1. 사용자 단말

사용자 단말은 접근 가능한 AP(Access Point)를 찾아 네트워크에 연결하기 위한 암호화 처리 알고리즘을 가지고

있어야 하며, 유동 IP를 할당받기 위한 DHCP 모듈, 공개키 암호화 기능, PIN Number 입력 기능, Hash 기능을 포함하고 있다.

사용자 단말의 암호화 모듈이 암호화를 처리하기 위한 처리 내용은 다음과 같다.

- 접속 네트워크를 찾기 위한 DHCPDISCOVER /DHCPOFFER 패킷을 브로드캐스트
- 공개키를 통한 SSO 서버로부터 전송된 인증 메시지 해독
- 사용자의 PIN Number 입력 기능과 Hash 기능
- 상대방의 공개키를 이용한 데이터 암호화

1.2. Edge Router

Edge Router는 기존 인증 방법에서는 존재하지 않던 부분으로 사용자 단말의 단말 고유 값을 입력 받아 인증 서버와 단말기의 접근 정보 및 서버의 정책을 입력받아 결정하는 모듈이다. 암호화 기능은 없지만 IP 할당을 위한 DHCP 연결을 위한 기능과 Radius 서버등을 연결하고, DHCP relay를 처리하는 기능을 가진다.

EdgeRouter의 역할은 다음과 같다.

- 단말 정보를 통한 CLIPS(Clientless IP Session) 생성
- ACL 접근 정보 및 패킷 제어 정책 등 반영
- DHCP 정보 릴레이
- 최초 및 종료 시 접속 경로 redirection
- 인증 후 접속 경로 설정 및 변경

1.3. Radius 서버

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

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

1.4. SSO 서버

SSO 서버 모듈은 사용자 인증을 최종적으로 승인하고 해당 사용자를 인증하는 서버이다. 인증 완료 후 u-City 내의 uMC(u-City Management Center)의 내부 시스템에 인증 토큰을 할당하는 역할을 담당한다. SSO 서버의 역할은 다음과 같다.

- 사용자 기반의 세션키와 공개키를 암호화 하여 단말에 전달
- 사용자의 PIN 기반으로한 단말기 상태인증
- 내부 사용자 접속을 위한 토큰 생성
- 사용자 인증 후 정책의 허용 여부를 Radius 서버와 EdgeRrouter에게 전달

1.5. u-City Management Center(uMC)

u-City의 개발시 가장 중요한 구성요소인 uMC는 u-City의 핵심으로 기존 도시에서 기능을 나누어 관리하던 방식을 하나의 센터로 통합해 놓은 것으로 매우 복잡한 구조를 가지고 있다. 또한 현재 구축되었거나, 구축 예정된 u-City의 특성이 모두 다르기 때문에 다양한 형태의 uMC가 존재할 수 있다. 따라서 본 논문에서는 uMC 구성요소 중 인증 부문만을 다루며, 그 역할은 외부 채널 연계 서비스 영역과 외부 사용자 및 단말기기를 인증하는 부분만으로 한정짓는다. 따라서 uMC 모듈은 기본 적인 암호 모듈과 인증 모듈을 가지고 해당 시스템과 접속 시 암호화 구간을 통해 데이터를 처리한다.

uMC가 인증을 위해 가지고 있어야할 DB의 종류는 인증, 사용자 DB로 다음과 같다.

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 다음과 같은 필드로 구성된다.

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

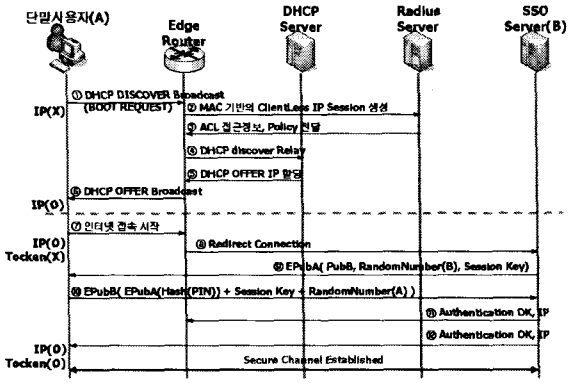
사용자 DB 테이블은 사용자를 식별하고 인증하는데 사용되며, 사용자의 공개키와 인증 정책 등을 담은 필드로 구성된다.

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

필드 중 ACL 필드는 사용자의 접근 정책을 기록하며, EdgeRouter 라우팅 테이블에 적용된다.

2. 망 접속 서비스 인증 절차

2.1. 전체 인증 절차



[그림 4] 전체 인증 절차

① 단말 사용자(A)는 네트워크에 접속하기 위해 단말 DHCP Client를 동작시켜 DHCP DISCOVER 패킷을 Broadcast

② 단말로부터 DHCP DISCOVER 메시지를 받은 Edge Router는 단말에서 전송되어진 패킷에서 정보를 받아 MAC 기반의 CLIPS(Client Less IP Session)을 생성하여 Radius 서버에 전송

③ Radius 서버는 해당 MAC Address를 가진 사용자를 DB에서 검색하고 그 사용자에 대한 Policy를 검색하여 ACL 접근 정보 등을 EdgeRouter에 전달

④ EdgeRouter는 전송된 해당 내용을 분석하여 접근 권한을 확인하고 네트워크 연동 정책을 수립, 만약 사용자가 검색되지 않은 경우 메시지를 무시하며 패킷은 버리고 종료한다. ACL에 의해 접근권한이 확인된 사용자 단말의 패킷이라면 DHCP Discover Relay 메시지를 DHCP 서버에 전송

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

⑥ EdgeRouter는 DHCP에서 받은 DHCP OFFER를 사용자에게 전송하고 정책에 반영

⑦ 단말이 인터넷 접속을 시작하면, EdgeRouter는 해당 정책에 따라 네트워크 정책을 적용하고, 초기 접속인 경우, 사용자 인증을 위해 SSO 서버로 접속은 Redirect

⑧ SSO 서버는 Redirect Connection을 전송 받음

⑨ SSO 서버(B)는 ⑧의 정보로부터 단말기 사용자의 DB를 검색하여 공개키를 추출한 Nounce 값, Session Key값, SSO 서버의 공개키 값 등을 추출된 공개키로 암호화하여 단말에게 전송

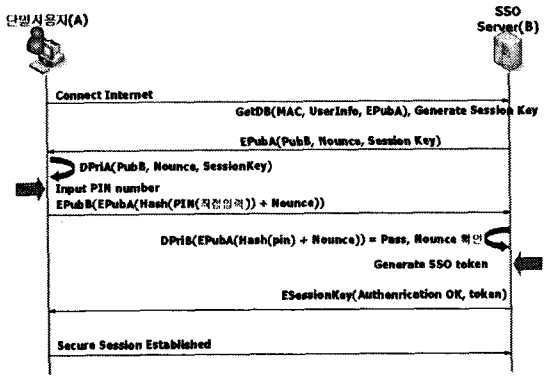
⑩ 단말은 자신의 개인키로 복호화하여 Nounce와 Session Key를 추출하고 사용자의 입력으로부터 PIN Number를 입력받아 해쉬하고, 자신의 공개키로 암호화한 후 SSO의 공개키로 암호화하여 SSO 서버로 전송

⑪ SSO 서버는 자신의 개인키로 복호화하여 사용자가 전송한 PIN Number를 추출하여 사용자를 인증하며 이로서 단말과 사용자가 모두 인증 됨. EdgeRouter와 단말에게 인증완료 패킷을 전송

⑫ 인증완료 패킷을 단말에게 전송, 단말과 사용자 사이의 Session Key로 전송 구간을 암호화한다.

2.2 키 생성 절차

사용자와 SSO 인증 서버 사이의 암호화 전송과 키 생성 및 교환 순서는 다음과 같다.



[그림 5] 키 생성 및 교환 절차

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

전송된 패킷은 사용자가 개인키로 복호화한 후 세션키와 nounce 값, SSO 서버의 공개키 값을 추출하여 저장한다. 추출된 SSO 서버의 공개키 값으로 사용자로부터 직접 입력받은 PIN Number의 해쉬값과 nounce값을 포함하여 암호화 한다. 암호문은 SSO 서버로 전달되어 복호화되고, 사용자 DB에서의 패스워드와 해쉬값을 검증함으로써 인증 여부가 확인된다.

인증이 완료된 사용자의 단말기는 다른 시스템의 별도 인증 절차 없이 사용되기 위해 인증서버로부터 SSO 토큰을 생성 받아 세션키로 암호화된 구간을 통해 안전하게 인증 정보를 전달 받게 된다.

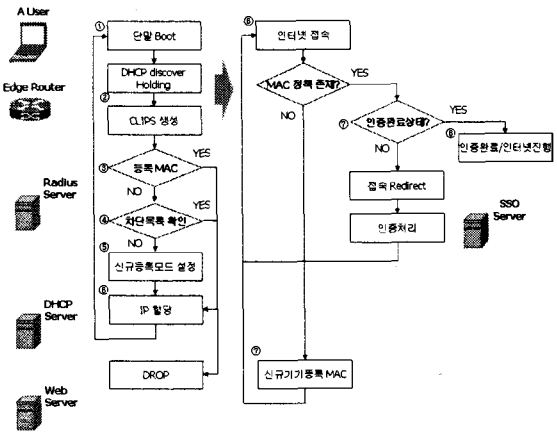
단말기 및 사용자가 인증을 해결하지 못하였을 경우 사용자의 모든 트래픽은 중단되고 패킷은 버려진다. 사용자가 인증을 풀었을 경우 Redirect 되었던 트래픽은 다시 전송

되어 원활할 접속이 이루어진다.

2.3. 신규 등록 및 정책 인증 흐름

네트워크에 처음 접속하는 단말은 네트워크를 인식하는 시점부터 IP가 할당되어 사용자 인증이 처리될 때까지 [그림 4]와 같은 절차를 거친다.

만약 초기 접속이 아닌 재접속의 경우 이미 인증 완료된 상태이기 때문에 EdgeRouter를 통해 더 이상의 Redirection은 발생하지 않고 바로 인증됨으로 네트워크의 접속 속도를 빠르게 할 수 있다.



[그림 6] 신규 등록 및 인증 흐름 절차

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

② Edge Router는 DHCP DISCOVER 패킷을 DHCP 서버로 전송하지 않고 보류한 상태로 CLIPS를 생성하여 인증 서버로 전송

③ Radius 서버는 CLIP를 통하여 전송된 MAC이 이미 등록되어 있는 사용자의 MAC 인지를 확인하여 등록되어 있고 사용가능하다면 IP를 할당한 뒤 정책을 적용하여 인증을 완료 후 접속을 허용

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

⑤ 공격자 목록에서 공격자로 확인되지 않으면, 신규 모드로 처리하여 사용자 등록을 실행하고 사용자의 공개키, 단말기,패스워드 등을 암호화 하여 DB에 기록

⑥ 신규로 접속 시 망 인증 접속을 허가 받고 IP를 할당 받은 단말기기는 네트워크를 통한 인터넷 접속을 시도

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

⑧ 단말기 인증 및 사용자 인증이 완료된 상태에서 인터넷 망에 접속

IV. 결론

u-City는 첨단 IT 기술을 도시에 적용하여 도시 내에서 발생하는 여러 가지 부작용들을 해결하여 시민들의 복지를 향상 시킬 수 있는 새로운 개념의 도시이다.

USN, BCN, IPv6, Wibro 등 네트워크 기술들이 복합적으로 적용되어있고 모바일 폰, UMPC, PDA, PC 등 다양한 형태의 정보화 기기 들을 통해 새로운 형태의 서비스를 이용할 수 있다.

본 논문에서는 다양한 정보화 단말이 무선 인프라를 이용하여 u-City 서비스에 접속하기 위한 인증 방법을 제안하고 그 절차를 명확히 하였다. 제안된 통합 인증 기법을 사용할 경우, 신규 사용자의 IP 할당과 기 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 키관리 기법으로 공개키를 사용하는 PKM을 사용함으로써 확장성이 높고, 기존 시스템에 적용할 경우 새로운 시스템의 추가 없이 AP/NAS 부분에 EdgeRouter 기능을 하는 장비를 추가하고, 인증 시스템만 갖추면 됨으로 적용성과 이식성이 매우 높다.

참 고 문 헌

[1] 황종성, "u-City의 개념과 구현 전략을 위한 이슈 분석," 정보과학회지, 제 23권, Nov. 2005.

[2] 정기섭, 박성수, "u-City 구축과 범죄통제," 사회과학연구(동국대학교) 제 12권 1호, 2005

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

[4] 한국정보보호진흥원, "u-City 프라이버스 보호방안 연구," 연구보고서, Dec. 2006.

[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.