무선 환경에서의 사용자 인증을 지원하는 QoS 제어 게이트웨이 구현

오민철° , 송병훈, 정광수
광운대학교 전자공학부 컴퓨터통신연구실
mcoh@adams.gwu..ac.kr, byungh@adams.gwu.ac.kr, kchung@daisy.gwu.ac.kr

Design and Implementation of the QoS Control Gateway with User Authentication in Wireless Networks

Mincheol Oh° ,Byunghun Song, Kwangsue Chung
School of Electronics Engineering, Kwangwoon Univ.

요 약

최근 무선랜 기술이 타 무선솔루션에 비해 비용이 저렴하고 사용하기 쉽다는 장점으로 큰 인기를 끌면서 급속히 확산되고 있다. 무선랜은 캠퍼스 크기의 서비스 지역에서 다양한 인터넷 서비스를 제공하는 기본 인프라로 사용하기에는 적당하나 아직 인증이나 트래픽 제어에 관한 많은 부분에서 개선할 필요가 있다. 기본적으로 무선 서비스 망은 유선 망과의 연동을 위해서 게이트웨이 기반 모델을 사용한다. 본 논문은 유, 무선을 연결하는 게이트웨이 기반의 사용자 인증 및 트래픽 제어를 제공하는 시스템을 구현하여 현재의 무선망에서의 차등화된 QoS 네트워크 서비스를 제공하였다. 구현한 게이트웨이는 향후 다양한 서비스 모델을 수용 할 수 있도록 확장성을 제공한다.

1. 서론

최근 네트워크 솔루션이 다양하게 발전해 가면서 가입자 망이나 컴퍼스 크기의 서비스 영역에서 무선의 사용이 증가지고 있다. 특히 무선랜은 이러한 추세에 가장 앞장서 있는 솔루션이라 말 할 수 잇다. 무선랜은 성공한 인프라인 유선랜 기술을 근간으로 사용과 확장성을 높이는 무선의 개념이 결합된 솔루션이다. 그렇게 때문에 무선랜을 설치하는 장소가 점점 늘어나고 있다. 그러므로 무선랜 네트워크 인프라에서 기존의 인터넷 서비스를 포함한 다양한 네트워크 서비스를 효과적으로 제공하기 위한 연구들이 최근 많이 늘어나고 있다.

사용자 인증은 가장 먼저 생각될 수 있는 무선랜의 서비스 기술이다. 무선이라는 특징 때문에 언제 어디서든 누구나 네트워크에 접근을 할 수 있기 때문에 어떠한 네트워크 보다 사용자인증이 중요하다. 현재 주목받고 있는 인증 기술로는 IEEE 802.1x 기술과 기본적인 랜 인증 방법인 MAC 기반 인증 방법, 그리고 인증 전용 프로그램을 이용한 인증 방법등이 활발히 연구되고 있다. 특히 전용 프로그램을 이용한 방법은 인증과 동시에 추가적인 서비스를 제공 할 수 있기 때문에 새로운 유형의 서비스 모델을 만들 수 있다. 관련 연구로는 스웨덴의 TSLab에 의해 진행되었던 FlyingLinux 프로젝트가 있다 [1][2].

본 논문에서 제안하는 QoS 제어 게이트웨이(QCG)는 전용 무선 인증 방법을 지원하는 시스템으로서 사용자인증 후 이에 따른 사용자 서비스 등급에 따른 차별적인 인터넷 접근 서비스를 제공한다. 제안한 서비스 모델은 특히 과금에 따라 무선 서비스를 제공할 수 있도록 확장할 수 있으며 추가적인 부가 서비스와의 연동을 쉽게 구현 할 수 있다.

본 논문은 총 5장으로 기술되었으며 2장에서는 무선랜에서의 인증을 위한 연구들에 대해서 기술하였고, 3장에서는 구현한 QCG의 구성 및 기능에 대해서 기술하였다. 4장에서는 QCG의 기능을 시험하기 위한 시험 망의 구성 및 시험결과에 대해 기술하였고 마지막으로 5장에서는 결론 및 향후 연구과제에 대해 논의하였다.

2. 관련 연구

2.1 무선랜

1997년을 기점으로 2Mbps 속도로 시작한 무선랜 시장은 초기 투자비용이 높음에도 불구하고 이동성과 인테리어를 요하는 POS(Point of sale System) 시장을 중심으로 막을 열었다.

무선랜은 기지국 역할을 하는 AP(Access Point)와 PC나 노트북 등에 내장되어 있는 무선랜카드 그리고 PDA와 같은 모바일 단말 등으로 구성되고 네트워크 측면에서는 일반 유선랜의 구성과 비슷하다.

무선랜이 최근 주목받고 있는 이유는 IEEE 802.1b가 등장하면서 속도가 최대 11Mbps까지 가능한데다 장비가격이 급속도로 하락해 유선으로 랜을 구축하는 것에 비해 큰 차이가 없어졌기 때문이다.

2.2 무선랜에서의 인증방법

2.2.1 MAC 주소를 이용한 방법

802.11b는 1999년 9월에 무선 LAN 표준으로 승인되었으며, 최근에 활발한 연구가 진행되고 있는 802.11a와 함께 현재 큰 관심을 모으고 있다.

AP와 모바일 단말의 MAC 주소와의 인터페이스를 통한 인증 방법을 취하고 있다. MAC 주소를 AP에 직접 등록하는 방법 이외에도 RADIUS와 같은 외부 인증 서버와 연계해 관리할 수 있는 기능이 있는 AP도 있으므로 소규모 네트워크 뿐 아니라 대규모 사업장에서도 이용이 가능하다.

그러나, 사용자인증이 아니라 단말인증이므로 단말이 여러 사람에게 공유되어 사용되는 경우 도용이 가능하며, 랜카드가 분실되었을 때, 아무런 제약 없이 침입자에게 네트워크가 노출될 수도 있다는 단점이 있다.

2.2.2 IEEE 802.1x

IEEE 802.1x는 원래 스위치 장비에서 포트별 액세스 컨트롤을 위해 표준화가 진행되고 있었으나 무선랜의 보안문제가 대두되면서, 무선망 보안을 위한 표준으로 더 많이 알려졌다. 이 표준의 핵심은 EAP(Extensible Authentication Protocol)로 구성원인 인증자(Authenticator: AP), 단말(Supplicant), 인증서버(보통 RADIUS 서버) 사이에서 많은 인증 프로토콜이 구동 될 수 있는 프레임워크를 제공하고 있다. 현재 윈도 XP에 802.1x가 탑재되어있다.

기업 환경에서는 인증서를 사용하는 EAP-TLS가 큰 이점을 갖고 있으나, 아직은 일반 사용자들에게 인증서는 다루기 어려운 방식이라는 점과 윈도 XP 이외에는 구현 사례가 부족하다는 단점이 있다.

3. 구성 및 기능

QCG는 사용자인증 기능을 담당하는 ADHCP(Authentication DHCP)가 주요 구성요소라고 할 수 있으며, NAT의 IP 테이블를 이용하여 내부망과 외부 인터넷망을 권한에 따라 접근할 수 있도록 DLNAT(Differentiated Level NAT) 기능을 수행한다. 액세스 서버 에이전트를 두어 사용자를 효과적으로 관리하면서 ADHCP와 DLNAT를 제어한다.

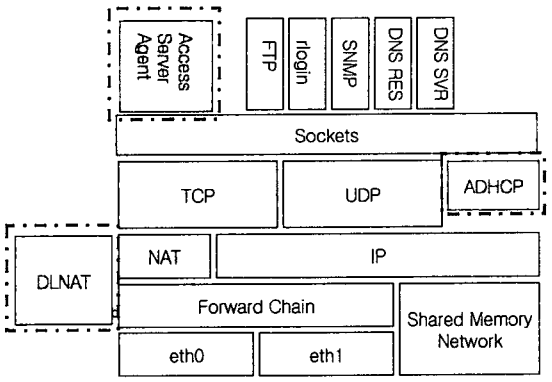

그림 1. QCG Architecture

3.1 ADHCP(Authentication DHCP)

ADHCP는 모든 유무선랜 환경에서 사용자에게는 네트워크 접속 편의성을, 관리자에게는 인증 및 과금 기능을 손쉽게 구현할 수 있도록 지원하는 솔루션으로 '플러그 앤 네트워킹(plug & networking)' 기술을 적용해 유무선랜 사용자들이 네트워크 환경이 바뀌어도 네트워크 설정 변경 없이 손쉽게 네트워크 기능을 사용할 수 있게 된다.

따라서 이 솔루션은 호텔, 공항, 터미널, 콘퍼런스홀 등의 사용자들이 밀집한 핫스폿(hot spot) 지역에서 이동단말기 사용자들에게 매우 유용하다.

이 솔루션은 무선랜 표준규격인 802.11b와 호환가능하고 사용자 권한에 따른 차등화된 서비스 제공이 가능하기 때문에 다양한 과금체계를 처리할 수 있다.

3.2 사용자 인증 기능

ISC dhcp-2.0p15를 기초로 소스를 수정하여 DHCP의 기본 메시지에 인증을 위한 동작을 추가하여 간단하면서도 효과적인 사용자인증이 가능하도록 구성하였다.

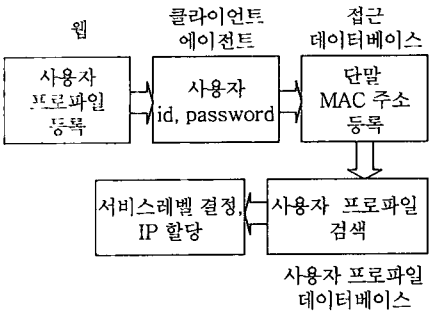

그림 2. 인증절차

사용자가 QCG에 접근하여 사용자 인증과 IP를 할당받는 과정을 그림 2의 순서도에 표현하였다. 이 과정에서 사용되는 두 개의 데이터베이스를 표 1과 표 2에 나타내었다.

표 1. 사용자 프로파일 데이터베이스

ID	패스워드	휴대폰번호	단말기종류	DLnat_level
usr_id	usr_pwd	usr_phoneNo	usr_station	bronze_level=x silver_level=y gold_level=z

(단 x, y, z : 파라미터 값)

사용자는 웹상에서 미리 가입을 하여 표 1의 사용자 프로파일 데이터베이스에 등록함으로써 본 서비스를 받을 수도 있고, Guest 권한으로 내부망 만을 이용할 수 있는 임시 IP 주소를 할당받은 후 가입과정을 거쳐 정식 사용자가 될 수도 있다.

표 2. 액세스 데이터베이스

IP address	MAC address	Adhcp_state	DLnat_level
192.168.0.2	xx:xx:xx:xx:x	init_state=w	bronze_level=x
~	x:xx	ready_state=x	silver_level=y
192.168.0.20		allow_state=y	gold_level=z
		deny_state=z	

(단 w, x, y, z : 파라미터 값)

클라이언트로부터 id와 passwd를 포함한 메시지를 수신하게 되면, 서버는 남은 IP 주소 중에서 할당할 IP를 선택하여 사용자의 MAC 주소와 함께 액세스 데이터베이스 등록하고 사용자 프로파일 데이터베이스를 검색한다. 이때, 사용자는 인증을 기다리는 READY 상태이다. 인증절차가 끝나면 사용자의 프로파일에 따라 ALLOW나 DENY가 결정되고, 동시에 사용자 프로파일의 DLnat_level에 따라 사용자 권한이 결정되어 이용 가능한 서비스를 등급에 따라 제공할 수 있는 상태로 만든다.

3.3 DLNAT(Differentiated Level NAT) 기능

DLNAT는 IP 필터링을 이용하여 사용자 레벨에 따라 차등적인 서비스를 담당하는 부분으로 클라이언트의 내부망 지역서비스 및 인터넷서비스를 선택적으로 제공하기 위한 구성요소이다.

사용자가 본 서비스를 이용하기 위해 가입할 때 원하는 서비스 등급을 선택하면, 해당 등급에 따라 사용자 프로파일의 DLnat_level이 세팅된다. 이 세팅된 값은 접근 데이터베이스의 DLnat_level로 전달되어 사용자의 권한에 따라 내부망 서비스를 이용할 수 있는 브론즈레벨, 내부망 서비스와 유료콘텐츠를 이용할 수 있는 실버레벨, 혹은 내부망 서비스, 유료콘텐츠 그리고 외부 인터넷망을 이용할 수 있는 골드레벨로 나뉘어 서비스 등급이 결정된다.

3.4 단말 에이전트

단말 에이전트는 사용자를 효과적으로 제어하기 위해서 액세스 서버 에이전트와 통신을 하여 사용자로 하여금 쉽게 서비스 초기화를 이룰 수 있도록 한다. 기본적으로 리눅스를 위한 콘솔형과 windows나 wince를 위한 것이 있다.

간단하게 만들어져 작은 디바이스에도 설치하여 쉽게 사용 가능하고, 인증을 위한 정보를 액세스 서버 에이전트에 전달한 후 어떤 서비스를 받을 수 있는지 사용자가 인지 할 수 있도록 표시해주는 기능을 담당한다. 사용자가 자신이 가진 레벨 이상의 서비스 받고자 할 경우 간단한 동작으로 이를 실현할 수 있도록 구현되었다.

4. 시험망의 구성 및 시험 결과

4.1 시험망의 구성

본 QoS 제어 게이트웨이의 사용자 인증절차와 사용자 레벨에 따른 차등화된 서비스 제공을 시험하기 위해 그림 3과 같이 구성하였다. QCG는 레드햇 리눅스 7.2상에서 구현하였고, 단말 에이전트를 위한 구현툴로 GTK+, 윈도상의 MFC, wince SDK가 사용되었다.

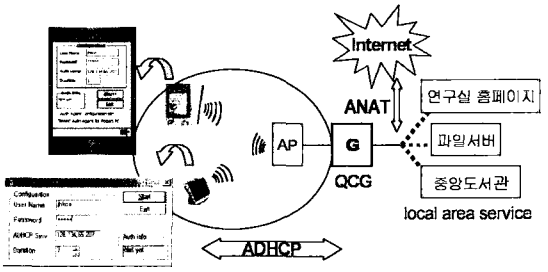

그림 3. 시험망의 구성

4.2 시험 결과

웹상에서 가입절차를 끝낸 사용자가 망으로 진입하여 단말 에이전트를 구동하고 권한에 따라 골드레벨, 실버레벨 혹은 브론즈레벨의 서비스를 기다린다.

그림 4는 인증결과와 사용자 레벨에 따른 서비스 등급의 변화를 보기 위해 액세스 데이터베이스를 모니터한 결과이다.

클라이언트로부터 id와 passwd를 포함한 메시지를 수신하게 되면, 서버는 액세스 데이터베이스에 사용자의 MAC 주소를 등록하고 사용자 프로파일 데이터베이스에서 사용자의 프로파일을 검색한다. 이때, 사용자는 ①과 같이 대기상태에서 인증을 기다린다. 인증절차가 끝나면 사용자의 정보에 따라 ② ③ ④ 중 하나의 상태로 바뀌게 된다

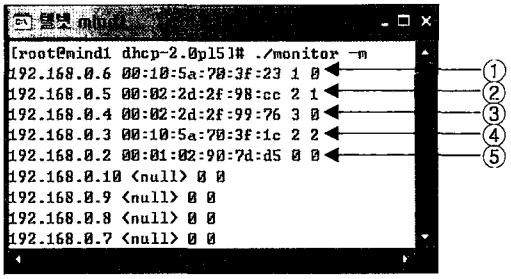

그림 4. 사용자 프로파일에 따른 인증결과 및 서비스 레벨

③과 같이 IP 할당이 거부되거나, ②나 ④ 같이 승인 상태로 바뀌고 IP를 할당받게 된다. 이때 ④상태의 사용자는 실버레벨인 상태이므로 인터넷망에 접속하기 위해서는 추가적인 단계를 거쳐야 하는 반면에, ②상태의 사용자는 모든 서비스를 이용할 수 있는 골드레벨이기 때문에 외부 인터넷망도 바로 접속할 수 있다.

IP를 할당받고 망을 이용하다가 어떤 이유로든 정당한 해제절차 없이 접속이 끊긴 경우 클라이언트의 상태는 ⑤와 같이 바뀌게 된다. 5분내에 재접속 할 경우는 해당 IP를 그대로 할당해주지만 그 이후에는 액세스 데이터베이스에서 삭제되어 처음부터 인증절차를 거쳐야 한다.

5. 결론 및 향후 과제

본 논문에서 구현한 무선 환경에서 사용자 인증을 지원하는 QoS 제어 게이트웨이는 사용자의 프로파일과 단말기의 MAC 주소를 통합하여 관리하기 때문에 사용자인증으로 좀 더 안전한 무선랜 망을 실현하였고, MAC 인증으로 단말을 쉽게 관리 할 수 있는 무선랜 망을 실현하였다. 이 과정에서 사용자 프로파일 데이터베이스와의 연동을 통해 사용자의 레벨에 따라 내부망과 외부 인터넷망을 이용할 수 있도록 차별화 함으로써 차등적인 QoS를 지원할 수 있도록 설계하였다. 간단하고 원하는 기능들을 쉽게 확장시킬 수 있도록 설계되어 목적에 따라 다양한 구현이 가능하다. 단말 에이전트는 편리하고 가볍게 구현하여 낮은 성능의 단말에도 적용 가능하다.

향후 연구 과제로는 사용자가 자신의 레벨에 맞는 네트워크 자원을 사용하고 있는가를 검사하여 적절한 대처를 할 수 있도록 사용자 프로파일에 따른 정책 프로토콜에 대한 연구 그리고 과금체계의 다양화와 컨텐츠의 세분화로 사용자 및 서비스의 레벨을 세분화함으로써 좀 더 차등화된 QoS를 제공할 수 있도록 확장해 나가는 연구가 수행되어야 할 것이다.

참 고 문 헌

[1] A. Escudero, B. Pehrson, E. Pelletta, and P. Wiatr, "Wireless access in Kista - IT University: MobileIPv4 integration in a IEEE 802.11b," IEEE LAN/MAN, March 2001.

[2] FlyingLinux.NET, http://www.flyinglinux.net

[3] G. Anastasi and L. Lenzini, "QoS provided by the IEEE 802.11 wireless LAN to advanced data applications: a simulation analysis," ACM, February 2000.

[4] IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control, IEEE Std 802.1X 2001.

[5] B. Sadeghi and E. Knightly, "Architecture and Algorithms for Scalable Mobile QoS," ACM, July 2001.

[6] H. Anderson, A. Forbes and M. Nystrom, "Improving Wireless LAN Authentication," RSA Lab, January 2002.