

논문 2008-45TC-11-6

와이브로 기반의 광대역 무선 액세스 망에서 WiFi 액세스 사용자 인증 방안 설계 및 분석

(User Authentication Scheme for WiFi Access in a WiBro-based BWAN through Nomadic Access Relay Station)

이 용*, 이 구연**

(Yong Lee and Goo Yeon Lee)

요약

와이브로 망을 백홀 링크로 하고, WiFi 무선망을 사용자 액세스 링크로 사용하는 방법은 무선 인터넷 서비스 제공에 관한 비즈니스 영역의 확장 측면에서 최근의 연구 추세이다. 그러나, 이와 같은 연동방법에서는 인가대역을 사용하는 와이브로 망과 비인가 대역을 사용하는 WiFi 망 사이에서의 상이한 사용자 인증방식에 대한 호환 문제의 해결을 필요로 한다. 즉 와이브로 망에서 WiFi 사용자에 대한 제어, 과금 등의 관리를 하기 위해서는 이들 사이의 인증 문제를 해결하는 것이 필요하기 때문이다. 본 논문에서는 이와 같은 사용자 인증 및 과금 등의 제어 관리를 위하여, 두 개의 망을 연결하는 RS인 WiNNERs를 통하여 BWAN 망사업자가 WiFi 사용자를 인증하는 방안을 제안하고, 또한 이에 대한 성능효과를 분석한다.

Abstract

Recently, there have been intensive researches on the wireless Internet access through WiFi WLAN using WiBro network as backhaul link in the Internet service providing business area. However, in the wireless Internet access method, we need to solve the compatibility problem for different user authentications between licensed WiBro network and unlicensed WiFi network for billing and user management. In this paper, we propose an authentication method for WiFi users by BWAN operators through WiNNERs which is RS connecting the two networks, and discuss the effectiveness of the method.

Keywords : 와이브로, WiFi, 사용자 인증, 릴레이 스테이션(RS), 무선랜

I. 서 론

광대역 무선 액세스 망(broadband wireless access network, BWAN) 기술이 진화함에 따라, 이동성 있는 고속 데이터 서비스에 대한 요구가 점점 증가하고 있다. 이에 IEEE 고정망의 광대역 무선 액세스 표준인, 802.16d가 2004년에 발표되었으며 이후에 이동성을 추

가한 802.16d의 보완이 발표되었다^[1~2]. 최근 한국에서는 와이브로 기술을 사용하여 무선 광대역 기반의 고속 데이터 서비스를 시작하였고, 이러한 서비스는 사용자 이동성을 지원하는 WiMAX 기술과 유사하다^[4~5].

BWAN 서비스 제공기술 중의 하나인 와이브로 기술은 이동 사용자가 3세대 통신보다 더 저비용으로 고속의 이동 데이터 서비스를 사용하는 것을 목표로 한다. 그러나 이러한 무선의 광대역 기술은 아직 WiFi와 3G 같은 기존의 무선 데이터 통신 기술을 대체할 상태는 아니다. 대신 이들 망은 미래에 이기종의 무선 망 환경으로 통합될 가능성이 있다. WiFi는 주로 노메딕 데이터 서비스에 사용되는 무선 통신 기술로서 저비용으로 고속의 무선망을 설치할 수 있도록 한다. 이들을

* 정희원, 충주대학교 전자통신공학전공
(Dept. of Electron. and Comm., ChungJu National University)

** 정희원, 강원대학교 컴퓨터학부, 교신저자
(Dept. of Computer Eng. Kangwon National University)

※ 이 논문은 강원도-엘비타주 공동연구의 결과임.
접수일자: 2008년2월4일, 수정완료일: 2008년11월14일

이용하여 특별히 백홀 링크로 WiBro(WiMAX)를 사용하고, 사용자 액세스 링크로 WiFi를 사용하는 무선 메쉬 네트워크를 구성하는 것이 최근의 추세이다^[13]. 이런 메쉬 네트워크는 핫 존(hot zone)이라고 하는 액세스 망을 구성하여 하나의 액세스 포인트 만을 가지는 핫 스팟(hot spot)보다 훨씬 더 넓은 영역에 걸쳐 고속의 무선 데이터 서비스를 제공할 수 있도록 한다. 메쉬 기반의 새로운 WiFi 액세스 망은 사용자에게 데이터 속도와 비용 면에서 만족을 제공한다. 그러나 이런 상황에서 BWAN 기반의 데이터 서비스를 사용하기 위해 데이터 액세스 서비스를 요구하는 가입자는 거의 없는 것이 현실이다. 또한 BWAN에 대한 새로운 퀄리어 플리케이션이 나타날 때까지, 이 새로운 서비스에 대해 가입하는 사용자는 그다지 많지 않을 것으로 예상된다. 그러므로 기존의 비인가대역 WiFi 사용자를 광대역 무선 데이터 서비스에 대한 일반 사용자로서 흡수하는 것은 고려할 만한 것이고 현실적인 비즈니스 모델이 된다. 이 경우에, QoS, 액세스 제어, 과금 등의 기능을 제공하는 것이 필요하며, 비인가대역 사용자 각각을 효율적으로 관리하는 능력은 망 서비스 제공자에게 필수적인 조건이 된다.

[3]의 논문에서는 와이브로 같은 광대역 무선 액세스 망에서 서비스 제공자 기반의 비인가 노메딕 액세스 (unlicensed nomadic access:UNA) 릴레이 스테이션을 적용하여 비인가대역 사용자 각각을 코어망 쪽에서 제어할 수 있도록 하여 그들이 WiBro radio access station(RAS)를 통해 인터넷에 접속할 수 있도록 하는 환경을 고려하는 WINNERS (wireless broadband unlicensed nomadic access relay station)를 제안하였다. 이 시스템은 와이브로 망 서비스 제공자가 코어망 쪽에서 비인가 대역 사용자의 각각을 직접 관리할 수 있는 능력을 제공한다. 이러한 직접적인 관리를 통하여 서비스 제공자는 각 비인가대역 사용자에 대하여 유통성을 가지고 용이하게 QoS, 액세스 제어, 과금 등을 관리할 수 있게 될 것이다. WINNERS의 이러한 목표를 달성하기 위해서는 [3]에서 고려된 연결(connection) 설정 및 관리와 더불어 각기 다른 이종망(BWAN과 WiFi)에서 한 사용자를 인증하기 위해 보안 기술의 연동이 필요하다. 본 논문에서는 비인가(unlicensed) radio band 사용자가 BWAN 무선 환경(예, 와이브로 or WiMax)을 통해 인터넷 접속을 가능하게 하는 기술을 적용할 때 이종의 네트워크 간에 서로 다르게 적용되는 사용자 인증 방법의 연동 문제를 해결하고자 한다. 이

논문에서는 WiFi를 비인가 노메딕(unlicensed nomadic) 무선 액세스 기술로서 고려한다.

이 논문은 다음과 같이 구성된다. II장에서는 이 연구의 동기와 배경을 설명한 후 관련 연구 동향을 살펴보고 III장에서는 [3]에서 제안한 WINNERS를 확장하여 보안기능을 포함하는 WINNERS의 구조를 보여준다. IV장에서는 WINNERS를 통하여 UNA 사용자를 BWAN에서 인증할 수 있는 방안을 제안하고 그 과정을 자세히 설명하고 마지막으로 V장에서 결론을 낼 것이다.

II. 배 경

3G망에서 WiFi 사용자들에게 연결(connectivity)를 제공하기 위해 UMTS-WLAN interworking wireless router 등이 이미 상용화 되어 있다^[3]. 통상 IPv4 환경 하에서의 비인가대역 사용자들을 지원하는 무선 (모바일) 라우터에서는 모두 네트워크 주소 포트 변환 (NAPT) 기능을 사용하고 있다^[9]. 일단 NAPT 기술은 IP의 부족 현상을 고려하여 하나 이상의 public IP 주소를 공유하여 여러 사용자에게 액세스를 제공하기 위해 개발된 기술이다. 즉, 여러 WiFi 사용자들은 각각 하나의 사설 IP 주소를 할당받고 라우터에 주어진 하나의 public IP를 공유하여 인터넷 망에 접속한다. 그림 1과 그림 2에서 NAPT 기반의 무선 라우터를 통하여 WiFi 사용자에게 연결(connectivity)을 제공하는 예와 traffic flow의 흐름을 보여준다.

그림 1의 경우 BWAN이 적용되는 BS-AP 구간과 비인가 대역인 AP-WLAN 사용자 구간에서의 사용자 인증 방안이 서로 다르다. 예를 들면 3G와 WLAN 간에도 보안 스킴이 서로 다를 뿐 아니라, 엄격하게 사용자의 액세스를 제어하여 단말과 사용자 인증을 수행하는 3G에서와 달리 WLAN에서는 802.11i나 802.1X 기반의 사용자 인증 방법을 제공한다.

BS와 AP 구간은 하나의 public IP 주소로 하나의 사용자를 인식하여 인증하고 액세스 권한을 부여하는 반면 실제로 WiFi가 제공되는 구간은 AP와 여러 WLAN 사용자 간에 사설 IP 주소를 통한 액세스가 제공된다. 따라서 BS는 여러 WiFi 액세스 사용자의 존재를 알지 못하고 인증도 할 수 없게 된다.

1. 종래 기술 문제점

기본적으로 별도의 사설 주소를 할당받은 여러 WiFi 사용자가 하나의 public IP를 사용하여 public IP

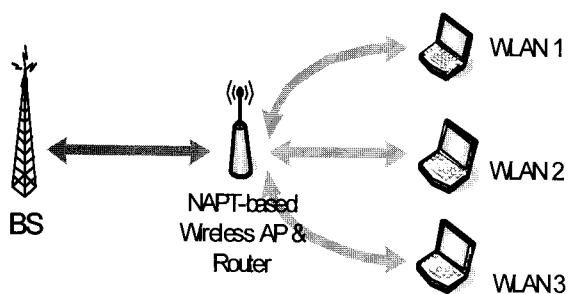


그림 1. NAPT 기반의 무선 라우터를 통하여 WiFi 사용자에게 connectivity를 제공하는 예.

Fig. 1. An example of user connectivity through NAPT-based wireless router.

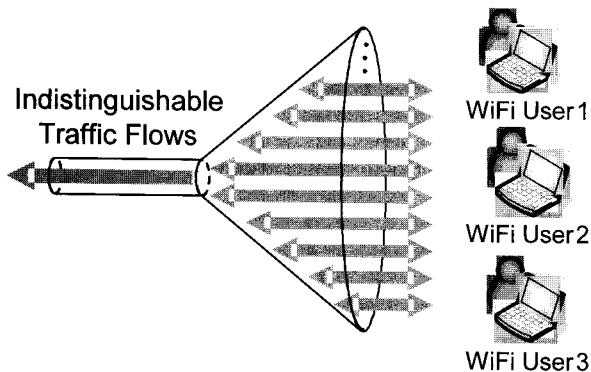


그림 2. NAPT 기반의 traffic flow 예.

Fig. 2. An example of NAPT-based traffic flow.

망(예, 인터넷)을 액세스할 수 있는 기능을 제공할 수 있도록 해주는 환경에서 각 사설 주소를 사용하는 사용자가 public IP 망을 액세스할 때 public 망에서는 이 사용자가 보이지 않게 된다. 이러한 점으로 인해 public 망 액세스를 제공하는 네트워크 사업자에게는 사용자 별 관리의 부실로 그다지 환영받지 못하는 기술이 되었다.

Public IP 주소로 변환된 후에는 사용자 식별이 불가능하며 또 TCP/UDP 포트도 각 사용자의 서비스 별로 변환이 이루어지기 때문에 포트를 이용한 각 사용자 식별도 불가능하다. 물론 NAPT 기반의 라우터에서 사설 주소를 이용하여 사용자별 트래픽 관리 및 QoS 관리가 각 패킷별 처리를 통하여 이루어지는 것이 가능할 수도 있으나, 이는 망 성능에 매우 크게 영향을 미치며 이를 해결하기 위해 H/W 업그레이드 시 비용의 상승이라는 문제로 연결된다. 또한 각 사용자별 access disable 및 enable 기능을 구현하기 위해서는 복잡도가 상당히 높은 문제가 있다.

이러한 문제로 인하여 BWAN 쪽에서는 사용자가 보이지 않아 식별이 불가능한 사용자를 인증해야 하는 어

려움이 발생한다. 보안 스케이프 네트워크 별로 서로 다르게 제공되어 이종 망간에 사용자에게 연결(connectivity)을 제공할 경우, 다른 네트워크에서 넘어온 사용자를 식별하여 인증하는 것은 어려운 문제이다.

와이브로, WiMAX 기반의 BWAN환경에서는 사용자 인증을 위하여 PKM(privacy and key management) 기반의 인증 프로토콜을 사용하고, WLAN 환경에서는 IEEE 802.1X 및 802.11i 기반의 인증 프로토콜을 사용하여 사용자 인증을 수행한다. 따라서 WLAN 액세스 사용자가 BWAN 환경을 통해 연결(connectivity)을 유지할 경우, WLAN의 인증방식을 따르는 사용자를 BWAN에서 인증 하여야 하며 BWAN 환경에 보이지 않는 사용자가 어떻게 사용자 인증을 얻을 것인지는 문제가 된다.

2. 논문의 배경

이 논문의 목적은 와이브로, WiMAX 기반의 BWAN 환경하에서 비인가대역을 사용하는 사용자에게 사업자 지향의 인터넷 연결을 제공하여 BWAN에서 활용할 때 BWAN에서 비인가대역 사용자를 인증 할 수 있도록 함에 있다. 여기서 사용자 지향이라 함은 비록 비인가 대역을 사용하는 사용자라 하더라도 QoS 및 과금(billing) 등 각 사용자 마다의 관리 제공을 의미한다. 본 논문에서는 와이브로와 같은 BWAN에서 비인가 노마딕 액세스(unlicensed nomadic access: UNA)를 제공하기 위하여 각 비인가 대역 사용자의 관리(QoS, 트래픽 제어, 과금 등)를 위한 인증 방법 및 구조를 제안한다. 그림 3에서 본 연구의 배경이 되는 BWAN-UNA Interworking 개념을 와이브로-WiFi Interworking을 예로 보여준다.

III. 사용자 보안 기능을 포함하는 WINNERs의 구조

본 논문은 비인가대역의 사용자(이후, unlicensed nomadic access, UNA라 부른다)와 와이브로/WiMAX 등의 BWAN을 연결하는 릴레이스테이션(RS)에서의 사용자 인증을 위한 보안 구조 및 기능을 제안한다. 제안하는 방법은 UNA로부터 네트워크 접속에 대한 요청이 있을 경우에 RS에서는 UNA 단말을 인증한 후에, UNA의 인증 파라미터를 BWAN의 인증 파라미터로 맵핑하여 UNA와 BWAN 간의 인증을 대행한 후 UNA를 대신하여 BWAN과 형성한 인증키를 UMA로 전송

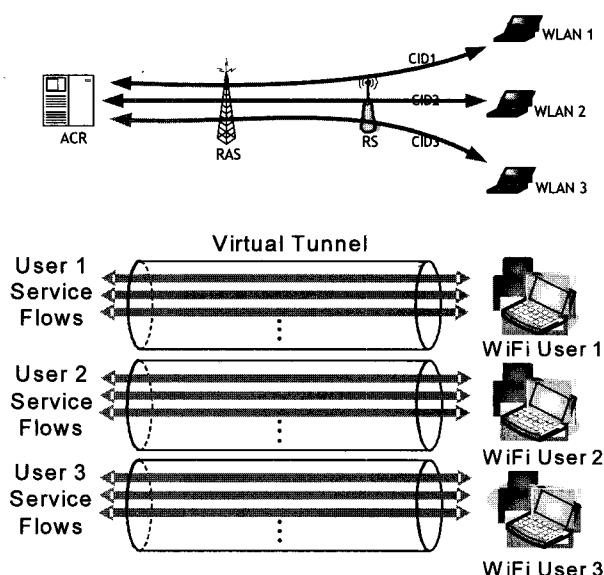


그림 3. WiBro-WiFi Interworking 개념도
Fig. 3. WiBro-WiFi internetworking diagram.

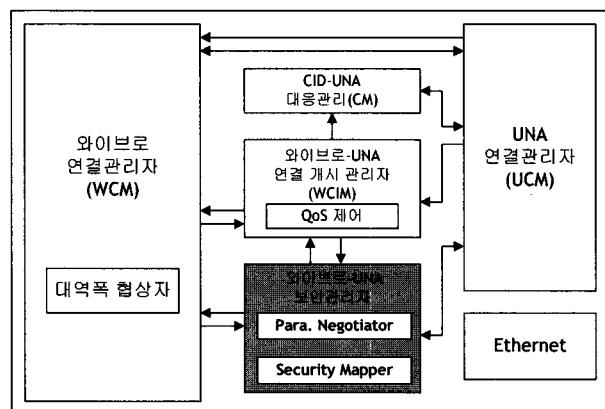


그림 4. WiBro-WiFi Interworking을 위한 WINNERs내의 보안 관리자 구조
Fig. 4. Security management structure in WINNERs for WiBro-WiFi Interworking.

하는 기능을 포함한다. UNA와 BWAN간에 보안에 관련된 파라미터를 협상하는 부분과 맵핑하는 부분으로 구성된다. 이 부분은 [3]의 WINNERs를 확장하여 전체적인 BWAN-UNA 레이스테이션의 기능 블록도 내에 그림 4에서와 같이 포함된다.

그림 4의 구조도에 나타나는 각 블록은 [3]에서 설명된 연결설정과정을 기반으로 한다. 여기서는 [3]에서 설명된 각 블록의 기능에 더하여 보안 관리자의 기능이 추가되었을 때를 중심으로, 각 블록의 기능에 대하여 설명한다.

- UNA 연결관리자(UCM) : 이것은 WiFi 사용자와 와이브로 연결개시요청자의 액세스 포인트로서 동작한다. WiFi 사용자가 연결요청을 할 때, UCM은

먼저 WiFi 사용자를 인증하고 인증 파라미터 및 인증결과를 포함하여 WCIM으로 사용자에 대한 와이브로 연결요청을 보낸다. WCIM으로부터 성공적인 연결결과를 받은 후에 사용자에게 연결결과를 알려준다. 다음에 사용자에 대한 IP 주소를 획득한 후에 와이브로 연결 요청을 보낸다. 마지막으로 CM으로부터 성공적인 CID 매핑 결과를 받으면 사용자에게 DHCP 응답을 보낸다.

- 와이브로-UNA 연결개시관리자(WCIM) : UCM으로부터 받은 인증 파라미터 및 인증결과를 WUSM으로 보내서 와이브로망에 대한 사용자 인증을 요청한다. WUSM으로부터 성공적인 사용자 인증 결과를 받은 후에 WCIM은 이 파라미터를 포함하여 연결요청을 WCM으로 중계한다. 응답으로 CID를 받고나면 이 CID를 CM으로 보낸다.
- 와이브로-UNA 보안 관리자(WUSM) : WUSM은 WCIM으로부터 요청받은 WiFi 사용자에 대하여 WiFi 인증 파라미터를 와이브로망에서 사용되는 사용자 인증 파라미터로 매핑하여 와이브로 인증과정을 수행한다. 인증과정이 성공적으로 완료된 후에 WUSM은 ACR와 공유키(authorization key)를 나눠 갖게 되고 이 공유키를 host AP로 보내준다. 또한 WCM이 와이브로망과의 초기연결설정 중에 인증파라미터에 대한 협상과정이 필요한 경우, WUSM이 협상에 필요한 파라미터를 생성한다.
- 와이브로 연결관리자(WCM) : 이것은 자신이 가입자 단말인 것처럼 초기 연결 설정을 관리한다. 이 초기 연결 설정과정 후에 WINNERs는 비로서 RAS와 통신할 준비가 된다. WCIM으로부터 CID 요청을 받은 후에 WCM은 부가적인 연결 설정과정을 초기화한다. 이에 대해 성공적으로 CID를 받으면, 이 CID를 WCIM으로 넘겨준다.
- CID-UNA 대응기의 기능은 [3]에서와 동일하다.

IV. WINNERs를 통한 WiFi 사용자 인증 방안

1. 호 연결 중 사용자 인증 과정

일반적으로 이종의 네트워크를 연동시키기 위한 장비는 각 네트워크 부분에 대한 연결 셋업이 독자적으로 이루어지고 이종망간의 연결에 대한 연동을 시도한다. WINNERs에서도 BWAN과 UNA를 위한 두 가지의 무선 액세스 셋업 과정이 독자적으로 이루어지고 이 두 가지 액세스 기술에 대한 연동을 시도한다. 사용자 인

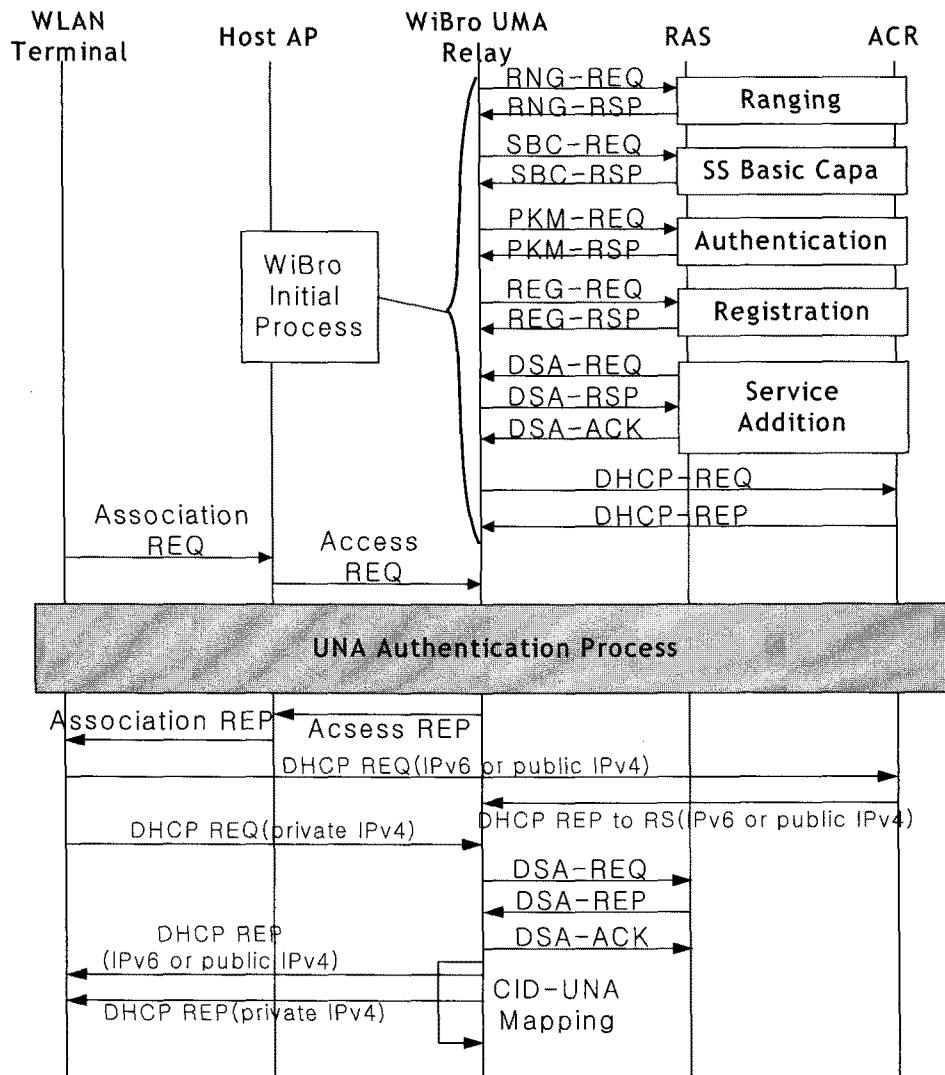


그림 5. WINNERs에서 사용자 인증을 포함한 WiBro-UMA Inter-connection의 설정 과정

Fig. 5. Inter-connection setup procedure of WiBro-UMA for user authentication in WINNERs.

증 역시 BWAN과 UNA가 독자적으로 구성되어 있으므로 이에 대한 연동 메커니즘이 필요하다. 그러므로 이 논문의 핵심은 이러한 두 가지 인증 기술에 대한 연동에 있다고 할 수 있다.

WiFi 기반 UNA 사용자의 무선 access request로부터 와이브로-UNA interworking을 위한 연결이 셋업되기까지의 동작 순서가 그림 5에 나타난다. WINNERs는 가장 먼저 와이브로 코어망과의 연결 셋업을 수행하여 MAC 관리 메시지 송수신을 위한 basic/primary/secondary ID와 데이터 송수신을 위한 transport IP (TID) 및 IP 주소를 획득한다.(이 과정은 PSS (portable subscriber station)의 데이터 통신을 위한 연결 셋업 과정과 동일하다.) 이렇게 와이브로의 초기 설정 과정이 완료되면 WINNERs와 와이브로 코어망과의 연결 셋업이 완료되고 이제 WINNERs는 WiFi UNA request를

기다린다.

WiFi user가 WiFi 망에 액세스하기 위해 association 요청을 보내면 WINNERs내의 WiFi host AP가 이 사용자의 연결을 인가한다. Association이 이루어지면 host AP는 WiFi의 인증 프로토콜에 따라 UNA 사용자에 대한 인증과정을 수행한다. 사용자 인증이 성공적으로 이루어지면, host AP는 키분배 과정을 보류한 채, 와이브로-UNA 연결개시관리자(WCIM)를 통해 와이브로 망에 대한 access request를 association이 이루어진 사용자의 정보 (예, MAC 주소, 인증 파라미터)와 함께 할당된 TID를 이용하여 상위단으로 보낸다. WCIM은 access request시 보내진 사용자 인증 파라미터를 이용하여 WUSM에게 와이브로 사용자 인증을 요청한다. WUSM은 WCIM에서 받은 WiFi 인증 파라미터를 와이브로 인증 파라미터로 매핑하고 WCM과 연동하여

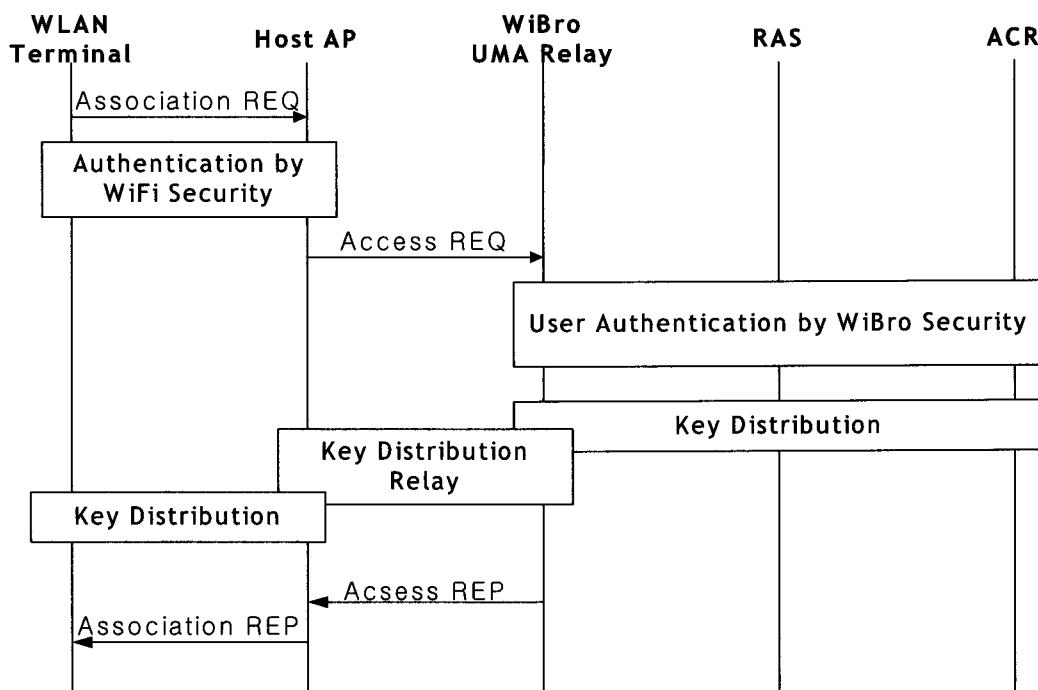


그림 6. WiBro-UNA RS에서의 UNA 단말에 대한 인증 과정

Fig. 6. Authentication procedure of UNA terminal in WiBro-UNA RS.

사용자 인증에 관한 요청을 시도한다. 이러한 과정은 그림 5에서 보여준다.

이 때, 사용자 인증 파라미터는 host AP가 사용자 인증에 사용한 정보를 이용하여, WiFi와 와이브로 간 인증 프로토콜과 메시지 포맷이 서로 다르므로, WUSM에서 이를 치환하는 게이트웨이 역할을 수행한다. 즉 host AP는 802.11i나 802.1X 스킴을 이용하여 사용자 인증을 수행하고, 와이브로는 PKMv2 방식을 이용하여 사용자 인증을 수행하는데, WiNNERs 내에서 WUSM은 이 둘 간의 인증 중계역할을 수행한다. WiNNERs 내의 host AP는 정해진 방법에 따라 WiFi 사용자 인증을 수행하고 이에 대한 결과를 WUSM으로 보낸다. WUSM은 이 정보를 이용하여 ACR에 대한 사용자 인증과정을 대행한 후 획득한 공유키를 host AP로 전달한다. 이 공유키는 host AP가 인증 메커니즘의 마지막 단계에 사용자에게 전달한다. WUSM은 통하여 ACR과 사용자 인증이 성공적으로 이루어졌을 경우, WUSM과 ACR은 사용자에 대한 인증키를 공유하게 된다. 이때, WUSM은 이 공유키를 host AP에 전달하고 host AP는 이 키를 사용자에게 전달하여, ACR과 사용자 간의 키 공유가 이루어지도록 한다. Host AP는 인증이 성공적으로 이루어졌을 경우 WiFi 사용자에게 association 완료를 통보한다. 이러한 과정은 그림 6에 보여준다.

이후 사용자는 DHCP를 이용하여 IP를 요청하고 성

공적으로 IP가 할당되면 WiNNERs는 DSA-REQ (Dynamic Service Addition Request) MAC management 메시지를 사용하여 WiFi 사용자 QoS level에 해당하는 전용 CID 할당을 요청한다. WiFi 전용 CID 할당이 완료되면 WiNNERs는 CID - WiFi 사용자와의 맵핑을 시도하고 최종적으로 DHCP REP를 WiFi 사용자에게 전달하여 IP 할당 완료를 통보한다. 이후 WiFi 단말은 와이브로 망에서 요청하는 대로 공유키를 이용하여 데이터를 암호화하여 전송할 수 있게 된다.

2. 사용자 키 정보 관리 방안

와이브로-UNA 보안관리자는 WiNNERs에 접속한 여러 WLAN 단말들의 인증 정보를 관리하여야 하며 UNA 단말과 ACR 간의 공유키도 관리하여야 한다. 이를 효율적으로 관리하기 위하여 사용자 식별 정보가 필요하다. 따라서 인증을 위해 ACR 쪽으로 넘겨주는 보안 파라미터 중에서 사용자 단말에 대한 식별정보인, MAC 주소에 대하여 WUSM에서는 UNA 단말의 식별 정보(예, MAC 주소)와 WiNNERs의 TID를 exclusive OR한 값으로 전송한다. 이렇게 할 경우, WiNNERs에 접속한 여러 WLAN 단말에 대하여 각각 다른 공유키를 생성·관리할 수 있도록 한다. 그림 7은 이러한 과정을 보여준다.

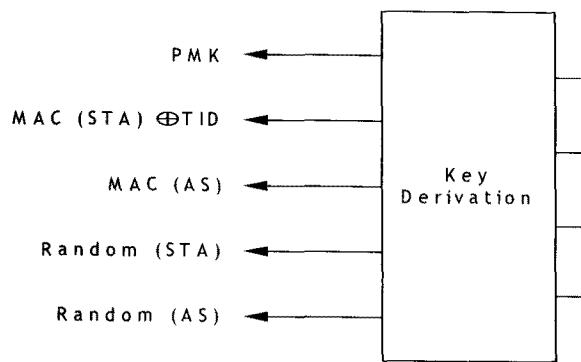


그림 7. 사용자 식별정보로 MAC 주소를 사용하는 경우 키분배 방식

Fig. 7. Key distribution method when MAC addresses are used as user identification information.

그림 7에서는 WiFi 단말과 와이브로 망과의 공유키 생성을 위하여 PMK(primary master key), WiFi 단말과 AS(authentication server)의 MAC 주소와 랜덤넘버를 사용한다. WiFi 단말은 와이브로 망에 보이지 않는 사용자이므로 실질적으로 PMK는 WiNNERs와 ACR간에 공유한 키이다. 또한 WiNNERs가 와이브로 초기 설정시에 이미 자기의 식별 정보를 이용하여 키를 할당받았으므로 WiFi 단말들이 와이브로 망에 연결을 할때에는 WiFi 단말의 고유 정보가 필요하다. 따라서 여기서는 WiFi 단말의 MAC 주소와 WINNERS의 TID를 exclusive OR한 값을 단말의 식별정보로 사용한다. 이렇게 하여 WiFi 단말과 ACR 간에 고유한 공유키가 생성된다.

V. 결 론

이 논문은 [3]에서 제안한 WiNNERs에 사용자 인증 기능을 추가하였다. WiNNERs는 서비스 제공자들에게 각 비인가 대역 사용자들을 개별적으로 직접 관리할 수 있는 능력을 주기 위해서 제안된 서비스 제공자 위주의 릴레이 스테이션이다. 망 쪽에서 이렇게 직접적으로 각 사용자를 관리하기 위해서는 우선적으로 각 사용자를 인증하는 것이 필요하다. 따라서 이 논문에서는 UNA 액세스 기반의 사용자인 WiFi 사용자가 와이브로 망에 접속할 때에 각기 다른 인증 방법을 사용하는 WiFi 사용자와 와이브로 망간에 인증 과정이 WiNNERs 내에 정의된 WUSM을 통하여 수행되는 과정을 제안하였다. 제안하는 방법은 와이브로 망에는 직접적으로 보이지 않는 WiFi 단말들이 각 단말별로 와이브로 ACR과 공유키를 생성하여 관리할 수 있도록

하여 WiFi 단말이 와이브로 망을 통하여 데이터 서비스를 이용할 수 있도록 한다. 이러한 시스템은 현재 와이브로 망의 확장을 위해 WiFi 사용자를 흡수하는 데 기여할 수 있을 것이다.

참 고 문 헌

- [1] IEEE Standard 802.16-2004, Air Interface for Fixed Broadband Wireless Access Systems, IEEE, October 2004.
- [2] IEEE P802.16e/D7, Air Interface for Fixed and Mobile Broadband Wireless Access Systems: Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, IEEE, April 2005.
- [3] W. Choi, T.S. Shon, H.H. Choi, and Y. Lee, Designing a Novel Unlicensed Nomadic Access Relay Station in IEEE 802.16-based Wireless Access Networks, IEEE VTC07 Spring, pp. 2961 – 2965, 2007.
- [4] Korean Telecommunication Technology Association, Specifications for 2.3GHz Band Portable Internet Service Physical Layer, TTAS.KO-06.0064R1, December 2004.
- [5] Korean Telecommunication Technology Association, Specifications for 2.3GHz Band Portable Internet Service Medium Access Control Layer, TTAS .KO-06.0065R1, December 2004.
- [6] UMA technology, <http://www.umatechnology.org>
- [7] D 2.4 Multi-radio Access Architecture, WWI Ambient Network Project, 2005.
- [8] Kyocera network, <http://www.kyocera-wireless.com>
- [9] K. Wehrle, Linux Networking Architecture, Ch 21, 2005.
- [10] A. Y. Chan and L. Wen-Pai, Architecture of Wireless Access in Vehicles, IEEE VTC, Vol. 5, pp. 3336–3340, 2003.
- [11] IEEE 802.11 WG, <http://www.802wirelessworld.com>
- [12] B. A. Forouzan, TCP/IP Networking, Ch 12, 2000.
- [13] I. F. Akyildiz, X. Wang and W. Wang, “Wireless Mesh Networks : a survey,” Computer Networks, Elsevier, 2005.

저 자 소 개



이 용(정회원)
 1997년 연세대학교 컴퓨터과학과
 (석사)
 2001년 연세대학교 컴퓨터과학과
 (박사)
 1993년~1994년 디지콤정보통신
 연구소

2001년~2003년 한국정보보호진흥원 선임연구원
 2004년~2005년 코넬대학교 방문연구원
 2005년~2007년 삼성전자 통신연구소 책임연구원
 2007년~현재 충주대학교 전자통신공학전공
 조교수

<주관심분야 : Mobile and Wireless Security,
 Ubiquitous Sensor Network, Wireless Mesh
 Network, Mobile Ad hoc network>



이 구 연(정회원)
 1988년 KAIST 전기및전자공학과
 (석사)
 1993년 KAIST 전기및전자공학과
 (박사)
 1993년~1996년 디지콤정보통신
 연구소

1996년 삼성전자
 1997년~현재 강원대학교 컴퓨터학부 교수
 <주관심분야 : 이동통신, 네트워크보안, 초고속통신망, ad-hoc 네트워크>