산업기술연구(강원대학교 산업기술연구소 논문집), 제28권 B호, 2008.
Journal of Industrial Technology, Kangwon Natl. Univ., Korea, No. 28 B, 2008.

광대역 무선 액세스 망에서 WiFi 액세스 사용자 인증

WiFi Access User Authentication in Broadband Wireless Access Network

이 용* 이 구 연**
Lee, Yong Lee, Goo-Yeon

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.

키워드 : 와이브로, WiFi, 사용자 인증, 릴레이 스테이션(RS), 무선랜
Keywords : WiBro, WiFi, User Authentication, Relay Station(RS), Wireless LAN

1. Introduction

With the advent of broadband wireless access network (BWAN) technology, South Korea started rolling out a wireless broadband high-speed data service network using WiBro technology which is similar to WiMAX technology supporting user mobility[1-5]. In [3], the authors proposed WiNNERs (wireless broadband unlicensed nomadic access relay station) scheme which absorbs existing unlicensed radio band WLAN users and controls them at the core network side by applying service provider-based unlicensed nomadic access(UNA) relay station(RS) in broadband wireless access networks like WiBro.

In this paper, we solve the interworking problem for different user authentications between licensed BWAN and unlicensed band network when an unlicensed radio band user connects to the Internet via BWAN. In this paper, we consider WiFi as a unlicensed wireless access technology.

2. Backgrounds

Existing wireless mobile access routers supporting IPv4 exploits the NAPT(Network Address Port Translation) connection-sharing technique to enable multiple WLAN users' Internet access simultaneously using one public IP address. However, on the downside wireless hosts behind a NAT-enabled wireless access router are invisible from the core network side, which causes the need for research to

* 충주대학교 첨단과학기술대학 전자통신공학전공, 교수, 공학박사
** 강원대학교 컴퓨터학부 컴퓨터정보통신전공, 교수, 공학박사, 교신저자

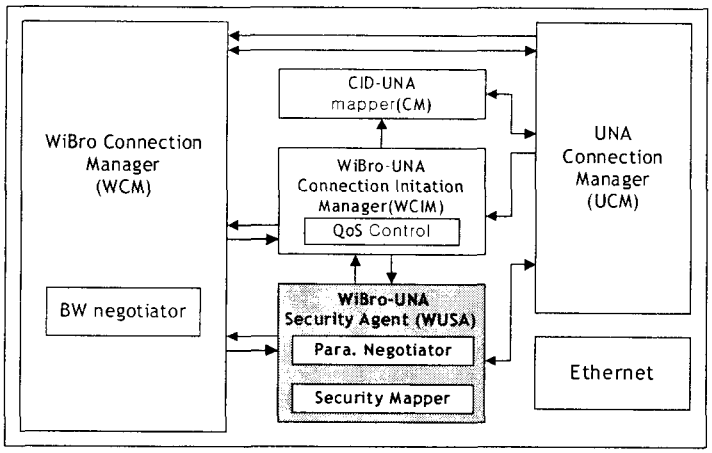

Figure 1. Security Function Block Diagram in WiNNERs for WiBro-WiFi Interworking

distinguish each of the WLAN users at the core network side. Identifying and authentication of the invisible users at the BWAN are difficult.

BWAN such as Wibro, WiMAX, authenticates users by PKM(Privacy and Key Management) and WLAN follows authentication method based on IEEE 802.1X or 802.11i. When WLAN user makes a connectivity through BWAN, BWAN should authenticate the user that has the WLAN authentication scheme. When two heterogeneous networks that have different security scheme from each other give a connectivity to a user, authentication of the user that is from another network with distinct security scheme is critical issue.

This paper proposes security architecture and functions for user authentication at relay station(RS) that connects unlicensed nomadic access(UNA) and BWAN such as WiBRo/WiMAX.

3. Architecture of User Authentication at WiNNERs

In the proposed method, RS authenticates an UNA terminal that requests a connection and maps the authentication parameters of UNA to BWAN authentication parameters. Then, instead of UNA terminal, RS executes the authentication between UNA and BWAN using mapping parameters, exchanges authentication key with BWAN, and forwards the authentication key to the UNA terminal. This method includes the negotiation and mapping of the security parameter between UNA and BWAN. Fig. 1 show the functional block diagram of WiNNERs with security scheme.

Blocks in Fig. 1 are based on the connection setup procedure in [3]. We focus on the functions of security agent and explain the function of each block.

- UNA Connection Manager(UCM) : it serves as an access point of WiFi users and WiBro connection initiation requester. When WiFi user requests a connection, it first authenticates the user and sends the connection request including the authentication parameters and the authentication result to WCIM.
- WiBro-UNA Connection Initiation Manager(WCIM) : it requests a user authentication to WiBro network by sending the authentication parameters and authentication result from UCM to WUSA. After receiving a successful user authentication result from WUSA, it relays the connection request including the parameters to WCM.
- WiBro-UNA Security Agent(WUSA) : it performs authentication procedure for the WiFi user that is relayed from WCIM by mapping WiFi authentication parameters to WiBro authentication parameters. After successful authentication result, it shares authentication key for the user with ACR and

transmits this key to host AP. Also, when WCM negotiates the authentication parameters for WiBo connection initiation, WUCA generates the negotiation parameters.

- WiBro Connection Manager(WCM) : it is defined in [3].
- CID-UNA Mapper(CM) : it is defined in [3].

4. The Proposed method for user authentication through WiNNERs

4.1 User authentication procedure at call connection

Generally, after the interworking system for two heterogeneous networks performs in several connection setups for each network, the system tries to corporate the connection of heterogeneous networks. WiNNERs also accomplish two wireless access setup procedures for BWAN and UNA and then, try the interworking of these connections. This scheme is also applied to user authentication. As BWAN and UNA have each authentication scheme, we need the interworking mechanism of two schemes.

After host AP in WiNNERs finishes the WiFi user authentication, it sends the result to WUSA. WUSA take the place of the user as agent for the user authentication procedure to ACR using this information, acquires a shared key, and sends the key to host AP. Host AP delivers the shared key to the user at the final level of the authentication mechanism. After successfully accomplishing user authentication to ACR through WUSA, WUSA and ACR share an authentication key for the user. WUSA transmits the key to host AP and host AP transmits the key to the user, then ACR and the user can accomplish the key sharing.

After host AP successfully finishes the authentication procedure, it notifies the WiFi user of the successful association. Fig. 2 shows the steps from wireless access request of WiFi user to connection setup by WiBro-WiFi

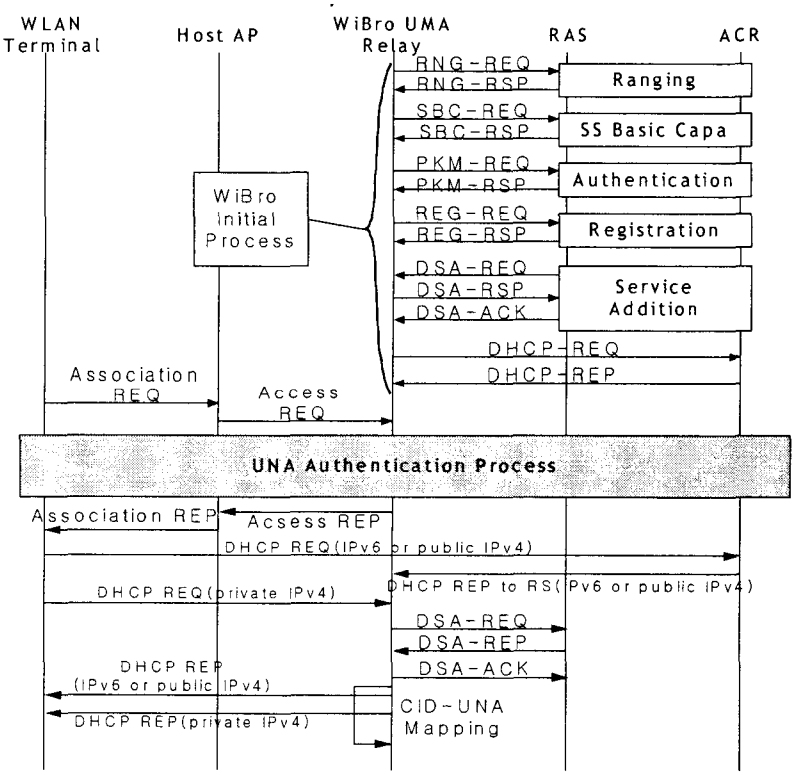

Figure 2. Inter-connection setup procedure of WiBro-UMA for user authentication in WiNNERs

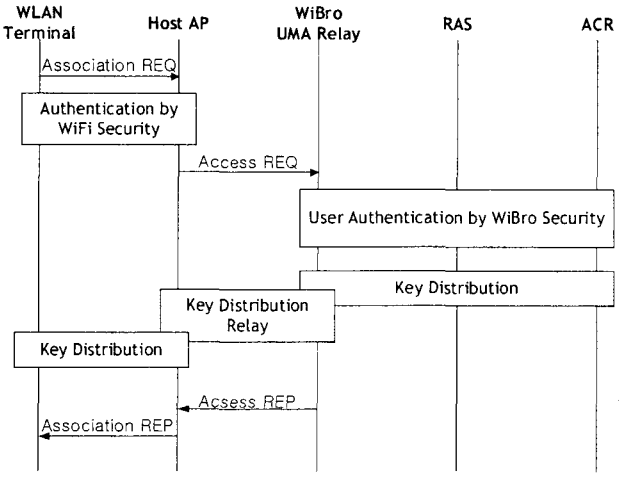

Figure 3. Authentication procedure of WiFi terminal in WiBro-WiFi RS

interworking including user authentication.

Fig. 3 illustrates the detail procedure of user authentication. When a WiFi subscriber sends an association request to WiFi network, WiFi host AP in WiNNERs accepts the access of the user. After finishing this association, host AP performs authentication process to the UNA user according to the WiFi authentication protocol. If the user authentication is successfully finished, host AP holds the key distribution procedure to the user and transmits an access request for WiBro network including the user information(ex. MAC address, authentication parameter) to the upper layer using the assigned TID through WCIM.

WCIM requests a WiBro user authentication to WUSM using the user authentication parameters that have been included in the access request. WUSA maps the WiFi authentication parameters obtained from WCIM to WiBro parameters and sends a user authentication request to WCM.

The information that host AP is used when user authentication is used as authentication parameters for interworking. Because the difference of authentication protocols and message formats between WiFi and WiBro, WUSM operates a role as gateway of substitution. That is, host AP performs user authentication using IEEE 802.11i or IEEE 802.1X and WiBro follows PKMv2 scheme for user authentication, therefore WUSM performs a relay of the authentication processes between two different networks.

Then the user requests IP address using DHCP and executes the defined steps in [3] to be assigned IP address. Finally the WiFi subscriber encrypts and transmits data using the share key according to WiBro policy.

4.2 User Key Management Scheme

WUSA manages the authentication information of multiple WLAN terminals that are connected to WiNNERs and the shared keys among UNA terminals and ACR. To efficiently manage them, it needs identifier for each subscriber. MAC address is an identifier for a user terminal among the security parameters that are transmitted to ACR. WUSA uses a result of XOR(exclusive OR) operation for the identifier of the UNA terminal(namely, MAC address) and TID of WiNNERs, instead of MAC address. This makes WUSA generate and manage each shared key for multiple WLAN terminals that are connected to WiNNERs.

Fig. 4 shows the share key generation between WiFi terminal and WiBro network using PMK(primary master key), MAC addresses of WiFi terminal and AS(authentication server) and random number. Because WiFi terminal is invisible to WiBro network, actually PMK is the shared key between WiNNERs and ACR. As WiNNERs is assigned its key using its identifier when WiBro initial connection setup, it needs an unique

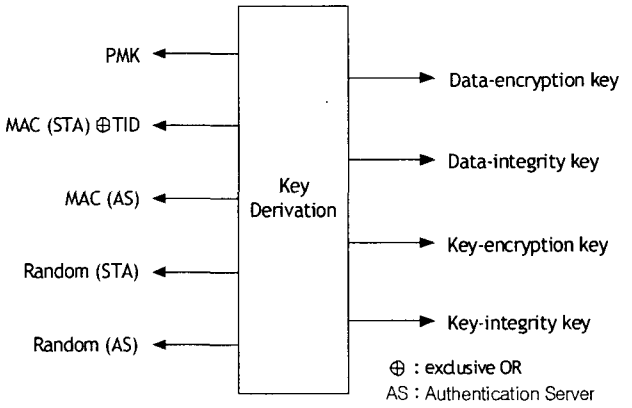

Figure 4. Key distribution method when MAC addresses are used as user identification information.

identifier for a WiFi terminal when the terminal accesses to WiBro. Therefore we use XORing value for a MAC address of a WiFi terminal and TID of WiNNERs as an identifier of the terminal. Finally the unique shared key between WiFi terminal and ACR can be generated.

5. Conclusion

This paper extends for the WiNNERs that has been proposed in [3] including user authentication function. We propose the interworking of authentication procedure between WiFi subscriber and WiBro network that apply each different authentication methods, performing through WUSA in WiNNERs, when WiFi subscriber with UNA accesses WiBro network. In the proposed method, each WiFi terminal that is invisible to WiBro network can generate and manage the shared key with WiBro ACR. Then, WiFi terminal can access WiBro network to use Internet service. This system endows WiFi user with Internet connectivity to extend WiBro network.

References

[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] IEEE 802.11 WG, http://www.802wirelessworld.com