Interworking between High-speed Portable Internet and Existing Wireless LANs using Different AAA Protocols

SUN-HWA LIM, YEONG-JIN KIM

Wireless System Research Group

Electronics and Telecommunications Research Institute

161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350

KOREA

Abstract: - With the growth of wireless technologies rapidly, there will be coexist heterogeneous wireless LANs environment within a few years. For example, there may be coexist current wireless LAN systems based widely available 802.11 and a wireless LAN system based proprietary wireless LAN standard with different AAA mechanisms such as RADIUS and Diameter. In case of being coexisted the heterogeneous wireless LANs, it is imperative for each wireless LAN system to be backwardly compatible with other wireless LAN systems and to be smoothly roamed. First of all, to provide wireless Internet service for users who move to other wireless LANs, users are to be authenticated only, authorized only or both. Accordingly, we propose a scheme being capable of interworking between heterogeneous wireless LANs with different AAA mechanisms in the viewpoint for user authentication. We design an interworking gateway which performs a role of gateway for the interworking. The scheme presented in this paper makes it easy to develop the interworking gateway for interworking heterogeneous wireless LANs.

1 Introduction

With the growth of wireless technologies rapidly, wireless LANs allow for fast and easy Internet or Intranet broadband access from public hot spots like airports, hotels and conference centers. Flexibility and mobility make wireless LANs both effective extensions and attractive alternatives to wired networks [1]. Accordingly, there will be coexist heterogeneous wireless LANs environment within a few years. For example, there will be current wireless LAN systems based widely available 802.11 and a wireless LAN system based proprietary wireless LAN standard with different AAA mechanisms such as RADIUS and Diameter.

In case of being coexisted heterogeneous wireless LANs, it is imperative for each wireless LAN system to be backwardly compatible with other wireless systems and to be smoothly roamed. First of all, to provide wireless Internet service for users who move to other wireless LANs, users are to be authenticated only, authorized only or both. When there may be coexisted RADIUS [2] and Diameter [3], the efficient protocol conversion is required for interworking between heterogeneous wireless LANs.

Accordingly, we propose a scheme being capable of interworking between heterogeneous wireless LANs with different AAA mechanisms in the viewpoint for user authentication. We design an

interworking gateway which performs a role of gateway for the interworking. In this paper, a wireless LAN system based proprietary wireless LAN standard is called High-speed Portable Internet (HPi). The interworking gateway shall be operated over a Packet Access Router (PAR) system that is one of HPi system.

This paper is organized as follows. Section 2 briefly introduces the HPi system, RADIUS, and Diameter as related works. Section 3 describes considerations, network architecture and protocol stack for interworking between heterogeneous wireless LANs. Section 4 presents design for establishment of a desired interworking gateway. Finally, section 5 presents the concluding remarks.

2 Related works
2.1 HPi System
The goal of developing HPi system should provide portability, mobility, low-cost and a verity of IP-based wireless Internet services in 2.3GHz bandwidth. Figure 1 shows network architecture for HPi system. There are a portable Access Terminal (AT), an Access Point (AP), a Packet Access Router (PAR), an Authentication, Authorization, and Accounting (AAA) Server and a Home Agent (HA). The AT can transfer/ receive high packet data to/from the AP with proprietary wireless standards. The AP shall process wireless signals and handle wired signals. Additionally, the AP can perform a handoff control between sectors. The PAR is able to connect a few of APs based IP and access IP Core Network. The PAR can perform authentication routing, mobile IP, and handoff controls between APs or PARs. The AAA Server performs an Authentication, Authorization, and Accounting for a user. The HA effectively causes the mobile node to be reachable at

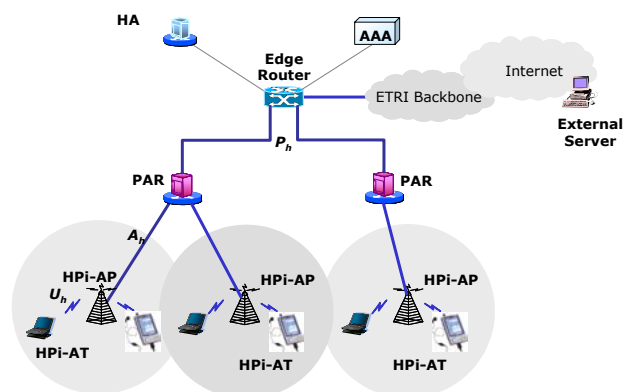its home address even when the mobile node is not attached to its home network.

Fig.1 Network Architecture for HPi System

2.2 RADIUS/Diameter
RADIUS is a software-based security authentication protocol developed by the Internet Engineering Task Force (IETF) RADIUS Working Group. The RADIUS protocol has been widely and successfully deployed to provide AAA services for remote PPP/IP access. The primary functions of RADIUS are authentication, authorization, and accounting. However, the limitation RADIUS was a client/server protocol that required the client to initiate a request. Therefore, Diameter was designed to maximize compatibility with RADIUS and ease migration from RADIUS to Diameter. Characteristics of Diameter are mobile IP and roaming, TCP/SCTP for data transport, proxying, and security supporting IPSec or SSL connections, etc. [4].

3 Architecture for Interworking between HPi and existing Wireless LANs
3.1 Consideration
In order to provide the interworking between heterogeneous wireless LANs, the following feature

sets should be considered in this paper.

3.1.1 Wireless Access Standards

HPi and existing wireless LANs environment use different frequencies on PHY/MAC layer. Therefore, in case the AT operated by HPi wireless access standard may move to existing wireless LAN environment, it is disallowed access to the AP. In case the AT operated by existing wireless access standards may move to HPi wireless LAN environment, it is disallowed access to the AP. Accordingly, for being capable of freely moving to heterogeneous wireless LANs, the AT should be operated over both the HPi wireless access standard and existing wireless access standards. The wireless access layer, that is PHY/MAC layer, is out of scope of this paper. We should consider only application layer in this paper.

3.1.2 EAP Protocols

The PPP Extensible Authentication Protocol (EAP) is a general protocol for PPP authentication which supports multiple authentication mechanisms [5]. Four types of EAP implementations have emerged as "standards." Some of the most commonly deployed EAP authentication types include EAP-MD5, EAP-TLS, EAP-TTLS, and Cisco LEAP [6~9]. They are compared according to a few of features and are shown in the following Table 1.

Table 1. EAP Protocol Comparison

Protocol / Feature	MD5	TLS	TTLS	LEAP
Requirement	user name/ password	Client/Server :certificates	Client : user name/password Server : certificate	user name/password
Key management	No	Yes	Yes	Yes
Authentication	One way	Mutual	Mutual	Mutual
Implement	Easy	Difficult	Moderate	Moderate
Security	Poor	Highest	High	High
RFC/Draft	RFC	RFC	Draft	Proprietary by CISCO

Among EAP protocols presented above for user authentication, we adopt EAP-TLS because of the strongest security and an open standard that's supported by nearly every vendor.

3.2 Network Architecture

Figure 2 shows network architecture for interworking between heterogeneous wireless LANs. Each AAA server shall perform authentication, authorization and accounting for the user based on some user's profile. In order to route authentication messages, the PAR is composed of protocol conversion, Diameter/RADIUS messages generation, and the interface functions for connecting with other systems. The AP shall only relay EAP PDU between the AT and the AAA server.
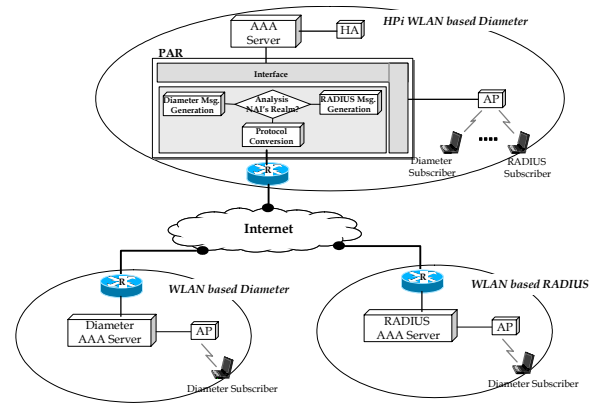

Fig.2 Network Architecture for Interworking between heterogeneous Wireless LANs

3.3 Protocol Stack

Protocol stack for interworking between heterogeneous wireless LANs is shown in Figure 3. In HPi protocol stack, EAP-TLS is used between the AT and the AAA Server. The Access Network Application Part (ANAP) which is newly defined in HPi system is used between the AP and the PAR. The PAR shall process Diameter/RADIUS authentication messages and transfer them to Diameter/RADIUS servers depending on the type of the authentication protocols. Like HPi protocol stack, EAP-TLS is used

between the AT and the AAA Server in existing wireless LANs.
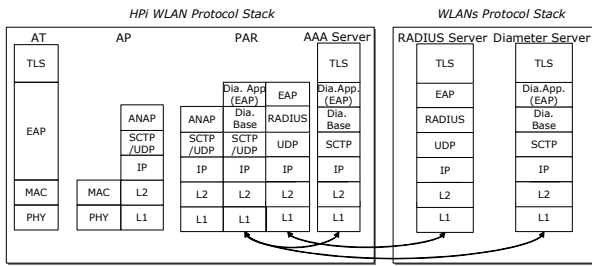

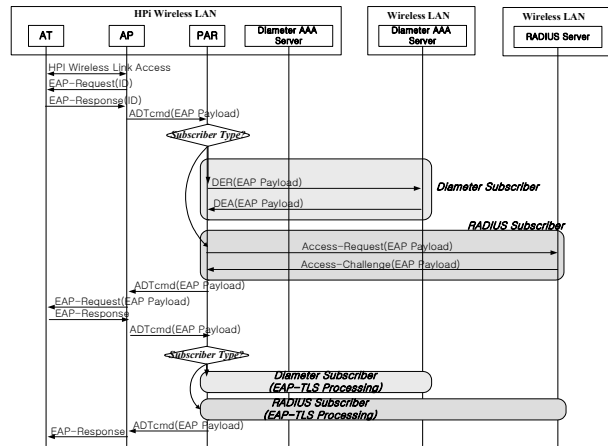Fig.3 Protocol Stack for Interworking between heterogeneous Wireless LANs

Fig.4 Procedure for interworking in case of roaming a user of existing wireless LAN to HPi wireless LAN

4 Proposed Interworking Gateway

4.1 Procedures

Figure 4 shows the procedure for interworking in case of roaming a user of existing wireless LAN to HPi wireless LAN. First of all, the interworking gateway function in the PAR should become the status for being able to receive any messages from the AP in HPi wireless LAN. Once initialization access for wireless link and basic capabilities negotiation has been established between the AT and the AP successfully, the PAR should send an EAP-Request (Identity) message to the AT for requiring the identity of a user through the AP. And then the AT has to send an EAP-Response (Identity) message to the PAR. On receiving an ANAP message including an EAP-Response (Identity) from the AP, the PAR has to determine whether a user is a subscriber in RADIUS wireless LAN or in Diameter wireless LAN with the realm information in NAI of the user. In case of a Diameter subscriber, the PAR shall generate a Diameter-EAP-Request (DER) message and route the message to the AAA server. In case of a RADIUS subscriber, the PAR shall generate a Access-Request message and proxy the message to the RADIUS server.

Figure 5 shows the procedure for interworking in case of roaming a user of HPi wireless LAN to existing wireless LANs. In case of the RADIUS message, the PAR shall interpret the realm information in NAI of the user. And it shall check whether or not a subscriber in home HPi wireless LAN. In case of a subscriber in home HPi wireless LAN, the PAR shall translate a RADIUS message to a Diameter message and transfer it to the AAA server in HPi wireless LAN. In case of the Diameter message, the PAR shall relay the message to the AAA server in HPi wireless LAN.
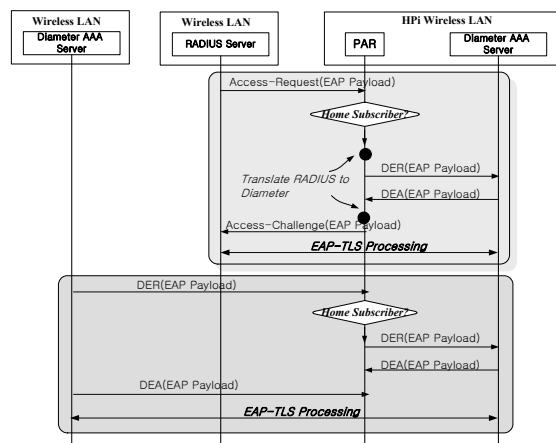

Fig.5 Procedure for interworking in case of roaming a user of HPi wireless LAN to existing wireless LANs

4.2 Function Architecture

Based on above user authentication procedures, we design the interworking gateway which is one of functions in the PAR system and describe the detailed function as the following. Figure 6 shows the function architecture of the interworking gateway.
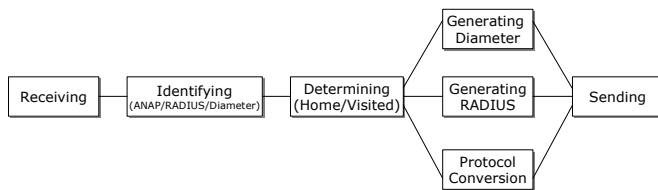

Fig. 6 Function Architecture for Interworking Gateway

- Messages Receiving Function

    The messages receiving function provides facilities for receiving authentication messages from the AP in HPi wireless LAN or a RADIUS/Diameter Server in existing wireless LANs.

- Messages Identification Function

    The messages identification function provides facilities for identifying whether an authentication message is an ANAP or RADIUS or Diameter.

- Home/Visited Determination Function

    The home/visited determination function provides facilities for determining whether a user is a subscriber in home or visited wireless LAN. In this paper, HPi wireless LAN is home wireless LAN and existing wireless LANs are visited wireless LANs.

- Protocol Conversion Function

    In case of roaming a Diameter subscriber to RADIUS wireless LAN, the protocol conversion function provides facilities for translating RADIUS attributes to Diameter AVPs according to RADIUS messages type and inversely translating Diameter AVPs to RADIUS attributes according to Diameter messages type.

- RADIUS/Diameter Messages Generation Function

    In case of roaming a user to visited wireless LANs, this function provides facilities for generating RADIUS or Diameter messages according to the authentication protocol that is supported in visited wireless LANs.

- Messages Transferring Function

    The message transferring function provides facilities for sending RADIUS or Diameter authentication messages to each AAA server in HPi or existing wireless LANs.

5 Conclusions

In this paper, we discussed a interworking gateway for interworking between heterogeneous wireless LANs with different AAA mechanisms. For the interworking gateway, wireless access standards and EAP protocols are considered. And network architecture and protocol stack are designed. Finally, procedures for interworking between heterogeneous wireless LANs are presented and its functions are designed. The scheme presented in this paper makes it easy to develop the interworking gateway. For the further work, we will research into interworking between wireless LANs and 3G mobile telecommunications such as GSM, CDMA, and IMT-2000.

References:

[1] Wireless LAN Overview, http://www.proxim.com/learn/library/whitepaper

s/wp2001-06-what.html

[2] RFC 2865, "Remote Authentication Dial In User Service (RADIUS)," Jun. 2000

[3] draft-ietf-aaa-diameter-17, "Diameter Base Protocol," Dec. 2002

[4] Mobile and Wireless Overview, http://www.wheatstone.net/whatwedo/Portal/Standards/radius_diameter.htm

[5] RFC 2284, "PPP Extensible Authentication Protocol (EAP)," Mar. 1998

[6] RFC 1321, "The MD5 Message-Digest Algorithm," Apr. 1992

[7] RFC 2716, "PPP EAP TLS Authentication Protocol", Oct. 1999

[8] EAP-TTLS, http://www.funk.com/NIdx/draft-ietf-pppext-eap-ttls-01.txt

[9] Cisco LEAP protocol description, http://www.missl.cs.umd.edu/wireless/ethereal/leap.txt