Design for Interworking between High-speed Portable Internet and Wireless LANs using different AAA protocols

Sun-Hwa Lim, Yeong-Jin Kim
IP Mobility Research Team, Wireless System Research Group
161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350
KOREA

Abstract: - With the rapid growth of wireless technologies, there will be coexistent heterogeneous wireless networks environment within a few years. For example, there may be coexistent current wireless LAN systems based on widely available IEEE 802.11 and a wireless system based on proprietary wireless standard with different AAA mechanisms such as RADIUS and Diameter. In case of being coexistent the heterogeneous wireless networks, it is imperative for each wireless system to be backwardly compatible with other wireless systems and to be smoothly roamed. First of all, in order to provide wireless Internet service for users who move to other wireless network, users should be either authenticated or, authorized or, both. Accordingly, we propose a scheme being capable of interworking between heterogeneous wireless networks with different AAA mechanisms in the viewpoint of 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 networks.

Key-Words: - Wireless Local Area Network (LAN), High-speed Portable Internet (HPi), interworking, authentication, RADIUS, Diameter

1 Introduction

With the rapid growth of wireless technologies, 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 networks both effective extensions and attractive alternatives to wired networks [1]. Accordingly, there will be coexistent heterogeneous wireless networks environment within a few years. For example, there will be current wireless systems based on widely available IEEE 802.11 and a wireless system based on proprietary wireless standard with different AAA mechanisms such as RADIUS [2] and Diameter [3].

In case of being coexistent heterogeneous wireless networks, it is imperative for each wireless system to be backwardly compatible with other wireless systems and to be smoothly roamed. First of all, in order to provide wireless Internet service for users who move to other wireless network, users should be either authenticated or, authorized or, both. When there may be coexistent RADIUS and Diameter, the efficient protocol conversion is required for interworking between heterogeneous wireless networks.

Accordingly, we propose a scheme being capable of interworking between heterogeneous wireless networks with different AAA mechanisms in the viewpoint of user authentication. We design an interworking gateway which performs a role of gateway for the interworking. In this paper, a wireless system based on proprietary wireless standard is called High-speed Portable Internet (HPi). The interworking gateway shall be operated over a packet access router (PAR) system that is one node of HPi system.

This paper is organized as follows. Section 2 briefly introduces the HPi system, RADIUS, and Diameter. Section 3 describes considerations, network architecture, and protocol stack for interworking between heterogeneous wireless networks. 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 variety of IP-based on 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 on 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 AT to be reachable at its home address even when the AT is not attached to its home network.

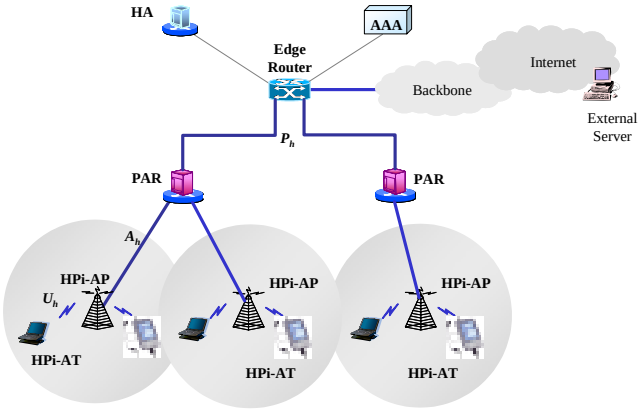

Fig.1 Network architecture for HPi system

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 RADIUS was a limitation because it is 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 Wireless LANs

3.1 Consideration

In order to provide the interworking between heterogeneous wireless networks, the following feature sets should be considered in this paper.

3.1.1 Wireless Access Standards

HPi and wireless LANs environment use different frequencies on PHY/MAC layer. Therefore, in case the AT operated by HPi wireless access standard may move to wireless LAN environment, access to the AP is disallowed. In case the AT operated by existing wireless access standards may move to HPi wireless environment, access to the AP is also disallowed. Accordingly, for being capable of freely moving to heterogeneous wireless networks, 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 and we only consider 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 as shown in the following Table 1.

Table 1 EAP Protocol Comparison

Protocol / Feature	MD5	TLS	TTLS	LEAP
Requirement	User name /password	Certificate	Client:user name /passwordd 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 which is supported by nearly every vendor.

3.2 Network Architecture

Figure 2 shows network architecture for interworking between HPi and 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 PAR.

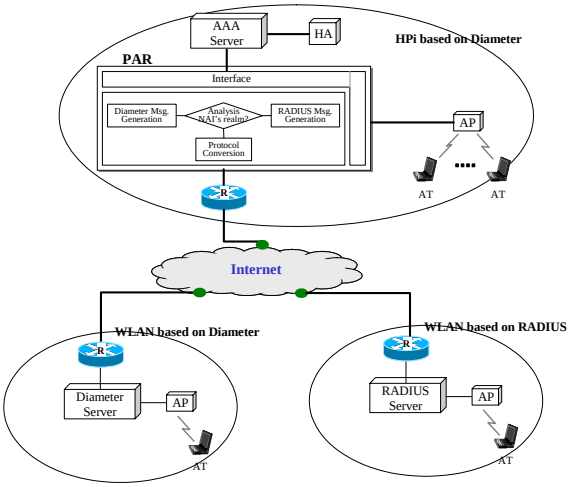

Fig. 2 Network architecture for interworking between HPi and wireless LANs

3.3 Protocol Stack

Protocol stack for interworking between HPi and 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 wireless LANs.

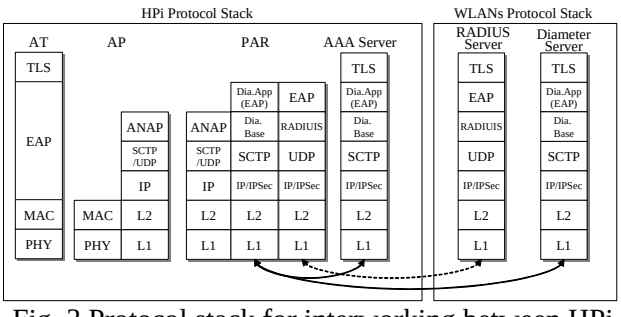

Fig. 3 Protocol stack for interworking between HPi and wireless LANs

4 Proposed Interworking Gateway

4.1 Procedures

Figure 4 shows the procedure for interworking in case of roaming of a user from wireless LANs to HPi.

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. Once initialization access for wireless link and basic capabilities negotiation have 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 an Access-Request message and proxy the message to the RADIUS server.

The Diameter AAA server generates Diameter-EAP-Answer (DEA) message and sends it the PAR. The RADIUS server generate Access-Challenge message and sends it the PAR. In order to authenticate the user, EAP-TLS messages should be transferred between the AT and each AAA server through the PAR. Finally, if the user is authenticated successfully, each AAA server sends EAP-Success message the AT through the PAR.

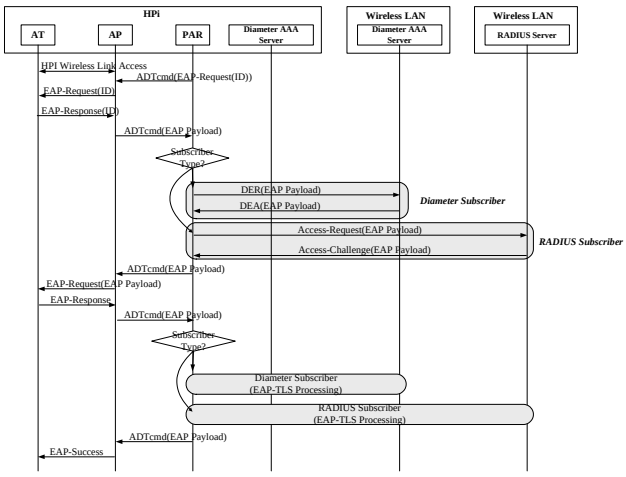

Fig. 4 Procedure for interworking in case of roaming of a user from wireless LANs to HPi

Figure 5 shows the procedure for interworking in case of roaming of a user from HPi to 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 is in home HPi. In case of a subscriber in home HPi, the PAR shall translate a RADIUS message to a Diameter message and transfer it to the AAA server in HPi. In case of the Diameter message, the PAR shall relay the message to the AAA server in HPi.

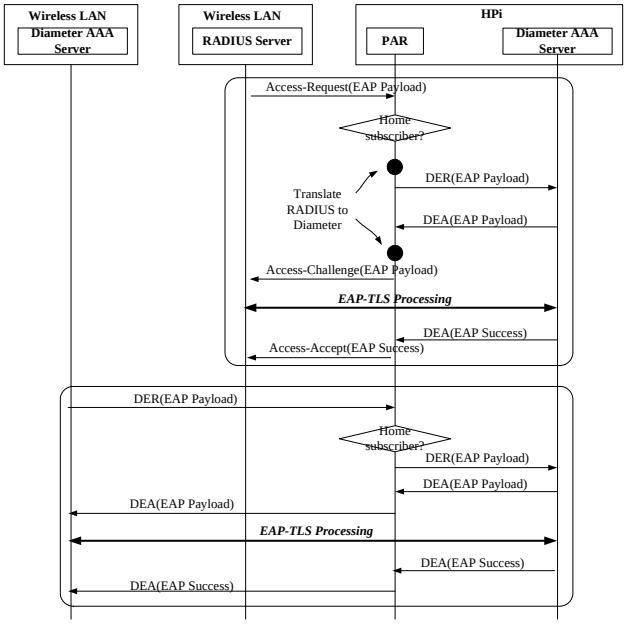

Fig. 5 Procedure for interworking in case of roaming of a user from HPi to wireless LANs

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 follows. Figure 6 shows the function architecture of the interworking gateway.

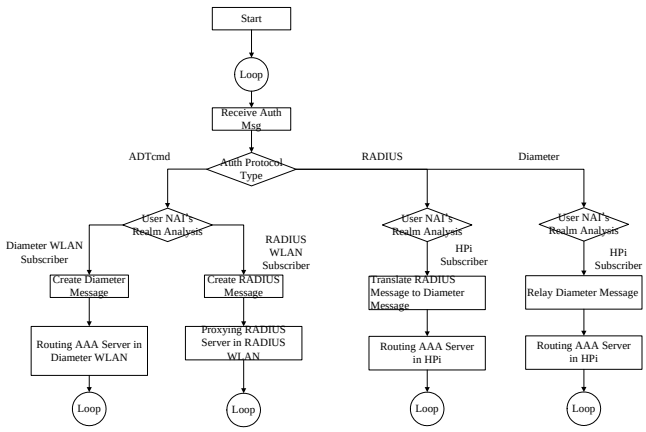

Fig. 6 Function architecture for interworking gateway

4.2.1 Messages Receiving Function

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

4.2.1 Messages Receiving Function

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

4.2.2 Messages Identification Function

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

4.2.3 Home/Visited Determination Function

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

4.2.4 Protocol Conversion Function

In case of roaming of 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. With a few exceptions, it is possible to convert RADIUS authentication attributes to Diameter equivalent ones. However, the following attributes should be considered [10]-[11].

- Although the Destination-Realm AVP is defined in Diameter, no Destination-Realm attribute is defined in RADIUS. Therefore, the Destination-Realm AVP should be created from the realm information of NAI in the RADIUS User-Name attribute.
- The Origin-Host AVP should be created from the information found in the NAS-IP-Address attribute or the NAS-Identifier attribute.
- The Message-Authenticator attribute may be used to sign Access-Requests to prevent spoofing Access-Requests using authentication methods. However, the attribute can not be converted to a Diameter AVP due to not be defined in the Diameter draft currently. Accordingly, in this paper, messages should be secured by using IPSec instead.

4.2.5 RADIUS/Diameter Message Generation Function

In case of roaming of 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.

4.2.6 Messages Transferring Function

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

5 Conclusion

In this paper, we discussed an interworking gateway for interworking between heterogeneous wireless networks 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 networks 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 HPi and 3G mobile telecommunications such as IMT-2000, and UMTS.

References:

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

[10] *Diameter Extensible Authentication Protocol (EAP) Application*, draft-ietf-aaa-eap-03.txt, Oct. 2003.

[11] Sun-Hwa Lim, Jung-MO Mun, Yeong-Jin Kim, and Sun-Bae Lim, Design of protocol conversion gateway based on Diameter for interworking between wireless LANs, *CIC 2002*, Vol. II, 2002, pp. 267-271.