AUTHENTICATION MECHANISM OF MOBILE IPv6 OVER WIRELESS LAN IN DIAMETER

*Sangkeun Yoo, Dooho Choi, Hyungon Kim and Seungwon Son
AAA Information Security Research Team
Electronics and Telecommunications Research Institute (ETRI)
TEL : *+82-42-860-1685, FAX : +82-42-860-5611
{*lobbi, dhchoi, hyungon, swsohn}@etri.re.kr

Abstract - This paper proposes efficient approach for adaptation of Mobile IPv6 over IEEE 802.11 Wireless LAN using Diameter in roaming environments. We assume that IEEE 802.1x authentication is used to authenticate the user in Wireless LAN and Diameter is used to carry IEEE 802.1x authentication messages between foreign AAA and home AAA. In this paper, Diameter is responsible for supporting IP mobility features such as home agent assignment and key distribution which is needed to securely send BU message to its home agent. Finally, we design authentication mechanism that mobile station can acquire IPv6 mobility support as well as network access to Wireless LAN in roaming environments.

I. Introduction

Recently mobility technology is regarded as indispensable feature in internet area according to widely use of mobile nodes such as notebook computer, internet-accessible mobile phone. Mobile IPv6 is a key protocol that supports mobility in IPv6 network [1]. With the support of Mobile IPv6 mobile user can still use his home address when he locates in foreign network away from his home network.

But Mobile IPv6 specification does not specify how to gain access to network when mobile node is away from its home [2]. Gaining access to foreign network requires that mobile node should be authenticated in foreign network. As shown in [2], mobile node offers its credential to the AAA (Authentication, Authorization and Accounting) infrastructure in order to be granted access to the local network. However foreign network does not have any information about mobile node, it requests authentication to mobile node's home AAA through AAA infrastructure. To offer mobile node's credential to foreign AAA client such as access router (AR), [2] defines several new ICMPv6 messages which are AAA Request, AAA Home Challenge Request, AAA Reply and AAA Teardown. These new ICMPv6 messages convey information which includes mobile node's credential between the mobile node and the AAA client. But [2] does not describe specific AAA protocol used for AAA infrastructure.

Diameter protocol is designed to overcome flaws of RADIUS. It takes into account the network access both in the traditional PPP sense as well as ROAMOPS model, Mobile IP [3, 4, 5 and 6]. Recent Diameter specification deals with IPv6 mobility support [7]. However, [7] does not state any specific protocol to be used between mobile node and AAA client. It describes that ICMP or PANA is suitable to be used to convey information.

This paper proposes efficient user authentication in Mobile IPv6 over IEEE 802.11 Wireless LAN using Diameter in roaming environments. We assume that IEEE 802.1x authentication is used to authenticate the user and Diameter conveys IEEE 802.1x authentication messages between foreign AAA (AAAF) and home AAA (AAAH). In this paper, Diameter is responsible for supporting IP mobility features such as home agent assignment and key distribution which is needed to securely send BU message to its home agent.

The rest of paper is organized as follows. Section 2 shows a brief of AAAv6 protocol introduced in [2] and IEEE 802.1x authentication [9] in Wireless LAN. We will propose authentication method for adaptation of Mobile IPv6 over Wireless LAN using Diameter in section 3. Conclusion will be given in section 4.

II. AAAv6 for IPv6 Network Access and IEEE 802.1x Authentication in Wireless LAN

2-1. AAAv6 for IPv6 Network Access

AAAv6 for IPv6 Network Access [2] proposes a way for IPv6 nodes (client) to present credentials to AAAF in order to be granted access to the foreign network. IPv6 routers are expected to determine whether the client's credentials are valid with the aid of AAA servers. If a client does not supply valid credential, then the router should not forward packets to that client. Such an unauthenticated client should have no access to the other network links adjacent to the router.

When an IPv6 client starts up or enters a foreign network, it receives a Router Advertisement with an AAA Challenge option. The client will construct a tentative IP address and may reply with an AAA Request ICMPv6 message. AAA Request ICMPv6 message includes AAA Credential option constructed by concatenating all of the preceding other options and applying the algorithm specified by the security association between the client and AAAH. The client must perform Duplicate Address Detection (DAD) before sending the AAA Request and the source address of AAA Request must be the chosen IPv6 address.

On receiving the AAA Request, the attendant must check if the chosen address is already in use. If the chosen

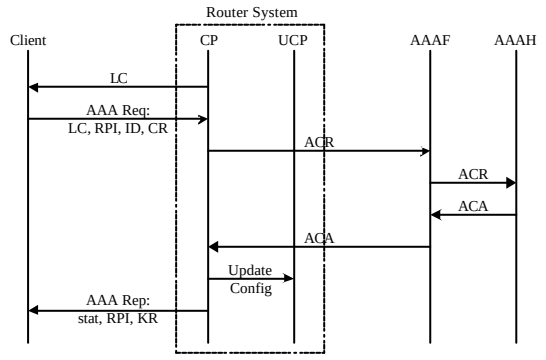
address is not in use, the attendant will extract the AAA field values and forward them to AAAF in an ACR (AAA Client Request) message using an AAA protocol, which is then forwarded to AAAH. The data in each AAA option must be conveyed to AAAH by the ACR message.

In return, AAAH will construct an ACA (AAA Client Answer) message containing information in a suitable form that can be extracted by the attendant and conveyed to the client in an AAA Reply message with appropriate options. AAAH should compute an authenticator, to be included in an AAAH Authenticator option, by concatenating all the preceding options intended for the client, and applying the algorithm specified by the security association between the client and AAAH. If the status of the request is successful, AAAH will send back an ACA message indicating success to AAAF.

AAAF will forward this to the attendant. If there are any keys distributed by AAAH, AAAF must re-encode those keys for the attendant.

The attendant must add an entry for the client in its Neighbor Cache and at the same time update the packet filter with the client's IPv6 address when the AAA verification for the client has been successful. The attendant will extract all information in the ACA message intended for the client and send them back in an AAA Reply ICMPv6 message. The attendant must create security associations for the client corresponding to any keys distributed to it by AAAF.

When the client receives an AAA Reply indicating success, it must verify the AAAH authenticator and the validity of the replay protection indicator. If verification succeeds, and key reply extensions have been included in the Reply, the client must create security associations for the attendant.



LC = Local AAA Challenge
RPI = Replay Protection Indicator used between client and AAAH
CR = AAA Credential
ID = Client Identifier
KR = Key Reply
UCP = Uncontrolled part
CP = Controlled part
ACR = AAA Client Request (using an AAA protocol)
ACA = AAA Client Answer (using an AAA protocol)

Fig. 1. AAAv6 authorization protocol exchanges

Figure 1 depicts AAAv6 authorization protocol exchange between client, AR, AAAF and AAAH.

2-2. IEEE 802.1x Authentication in Wireless LAN

The PPP Extensible Authentication Protocol (EAP) is a general protocol for PPP authentication which supports multiple authentication mechanisms [8]. EAP does not select a specific authentication mechanism at Link Control Phase, but rather postpones this until the Authentication Phase. This allows the authenticator to request more information before determining the specific authentication mechanism. This also permits the use of a "back-end" server which actually implements the various mechanisms while the PPP authenticator merely passes through the authentication exchange.

IEEE 802.1x authentication (Port-Based Network Access Control) [9] defines the encapsulation techniques that shall be used to carry EAP packets between Supplicant PAEs (Port Access Entity) and Authenticator PAEs in a LAN environment. Supplicant means that an entity at one end of a point-to-point LAN segment that is being authenticated by an authenticator attached to the other end of that link, whereas authenticator means that an entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link. This encapsulation is known as *EAP over LANs*, or *EAPOL*. IEEE 802.1x authentication can be used in Wireless LAN as authentication protocol which is called by *EAP over Wireless*, or *EAPOW*. IEEE 802.1x authentication occurs after 802.11 association as follows.

- After association, client and access point have an Ethernet connection
- Prior to authentication, access point filters all non-EAPOL traffic from client
- If 802.1x authentication succeeds, access point removes the filter

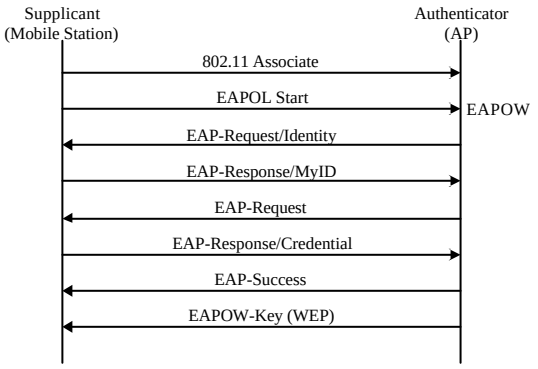


Fig. 2. IEEE 802.1x in Wireless LAN

Figure 2 presents IEEE 802.1x procedure in Wireless LAN. WEP-Key (EAPOW-Key) integration is enabled when authenticator works with AAA server such as RADIUS or Diameter and EAP method is EAP-TLS, EAP-TTLS or PEAP.

III. Mobile IPv6 over Wireless LAN in Roaming Environments

In this section, we will propose user authentication in Mobile IPv6 over Wireless LAN using Diameter. We assume that IEEE 802.1x authentication is used to authenticate the user in Wireless LAN. Also we assume that Diameter conveys IEEE 802.1x authentication messages between AAAF and AAAH.

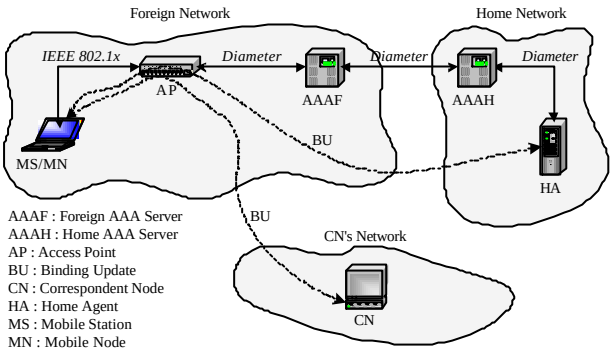


Fig. 3. Mobile IPv6 over Wireless LAN

Figure 3 shows Binding-Update (BU) of Mobile IPv6 over Wireless LAN where IEEE 802.1x and Diameter are used as authentication protocol and AAA protocol respectively. Broker AAA (AAAB) may be placed between AAAF and AAAH if roaming is achieved through roaming consortium by AAAB.

Mobile IPv6 BU may occur in two different types whether BU is sent to HA from MN (Mobile Node) via the AAA infrastructure or sent to HA (Home Agent) directly from MN.

- *AAAH sends BU to HA on behalf of MN*
  It is required to define new EAP-Response and EAP-Success message which can embed BU and Binding Acknowledgement (BA) respectively.

  Case 1. If the MN has a pre-configured HA and knows SA with the HA, it may create the BU message and sends it encapsulated in newly defined EAP-Response to an AAA client such as AP (Access Point). The BU message will be forwarded to the designated HA via the AAA infrastructure. This BU message has the MN's CoA (Care of Address) as the source IP address, the pre-configured HA as the destination IP address and the BU option with the pre-configured Home IP address in the Home address option. When BU is successful in HA, AAAH sends BA encapsulated in newly defined EAP-Success to MN via AAA the infrastructure.

  Case 2. If the MN does not have a HA, it includes some MIP Feature data with the Home-Agent-Requested flag set to 1 and BU which destination address field (HA' address) is empty in EAP-Response message. MN sends EAP-Response to AAA client and EAP-Response will be forwarded to AAAH via AAA infrastructure. The HA will then be assigned by the AAAH, and the BU will be sent by the AAAH to the HA on behalf of the MN. When BU is successful in HA, AAAH sends BA encapsulated in EAP-Success to MN via AAA the infrastructure.

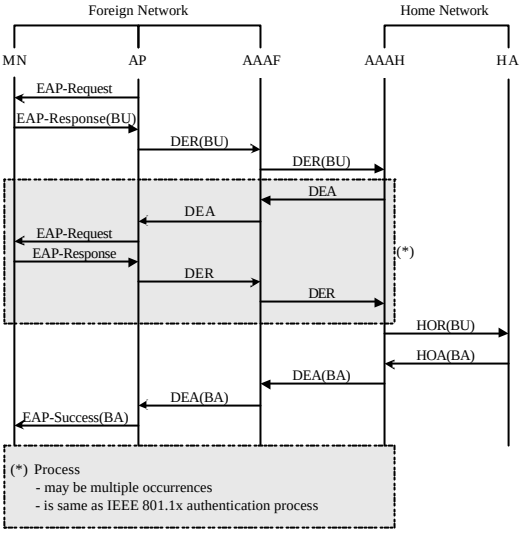


Fig. 4. Indirect Binding Update to HA via AAAH

Figure 4 depicts indirect BU via AAAH. Diameter commands in figure 4 are as follows.

- Diameter-EAP-Request (DER) [6]
- Diameter-EAP-Answer (DEA) [6]
- Home-Agent-MIPv6-Request Command (HOR) [7]
- Home-Agent-MIPv6-Answer Command (HOA) [7]

- *MN sends BU to HA directly*

  Case 1. If the MN has a pre-configured HA and knows SA with the HA, it may create the BU message and sends it to HA directly after EAP authentication was successful. This BU message has the MN's CoA as the source IP address, the pre-configured HA as the destination IP address and the BU option with the pre-configured Home IP address in the Home address option.

  Case 2. If the MN does not have a pre-configured HA, it includes some MIP Feature data with the Home-Agent-Requested flag set to 1 in EAP-Response message which must be newly defined. The HA will then be assigned by the AAAH and related SA (Security Association) with the HA is selected. AAAH sends MN HA's address and the related SA information encapsulated in EAP-Success which must be newly defined. In turn, MN sends BU to newly assigned HA directly.

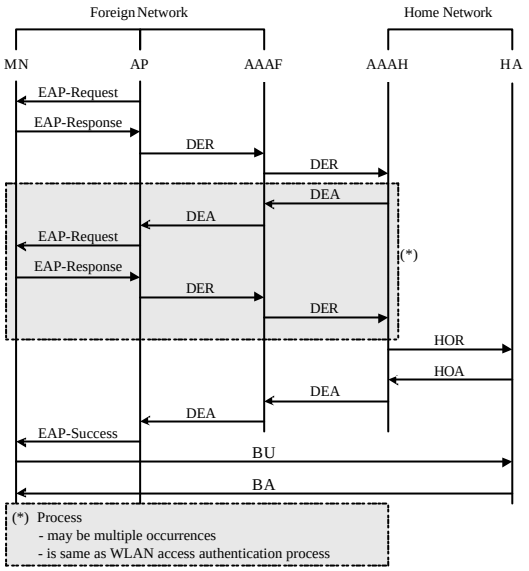


Fig. 5. Direct Binding Update to HA

We propose newly defined EAP-Response message which can embed BU or MIP Feature Data. EAP-Response (Identity) message should be modified to contain BU or MIP Feature Data.

EAP-Response(Identity) Packet Format in RFC 2284

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Code	Identifier	Length
Type	Typed-Data ...	

Where,
Code : 2 (Resonse)
Type : 1 (Identity)
Typed-Data : Identity

Newly Defined EAP-Response(Identity) Packet Format

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Code	Identifier	Length
Type	Sub-Type	Typed-Data ...

Where,
Code : 2 (Response)
Type : 1 (Identity)
Sub-Type :
0 : None (Identity Only)
1 : BU-Embedded
2 : MIP Feature Data-Embedded
3 : BU and MIP Feature Data-Embedded
Type-Data :
Identity / BU / BU and MIP Feature Data

Fig. 6. New EAP-Response Packet Format

- Sub-Type 0
  EAP-Response (Identity) message contains user's identity only.
- Sub-Type 1
  EAP-Response (Identity) message contains user's identity and BU message. Identity-Length indicates the length of identity in Typed-Data field. The remains of Typed-Data filed is BU message. Typed-Data filed is as follows.

Newly Defined EAP-Response(Identity-BU) Packet Format

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Code	Identifier	Length
Type	Sub-Type	Identity-Length
Identity + BU ...		

- Sub-Type 2
  EAP-Response (Identity) message contains user's identity and MIP Feature Data. Identity-Length indicates the length of identity in Typed-Data field. MIP Feature Data field is 32-bit unsigned value. Typed-Data filed is as follows.

Newly Defined EAP-Response(Identity-MIP Feature Data) Packet Format

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Code	Identifier	Length
Type	Sub-Type	Identity-Length
Identity ...		
MIP Feature Data		

- Sub-Type 3
  EAP-Response (Identity) message contains user's identity, BU and MIP Feature Data.

Newly Defined EAP-Response(Identity-BU-MIP Feature Data) Packet Format

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Code	Identifier	Length
Type	Sub-Type	Identity-Length
BU-Length		Typed-Data ...
Identity + BU		
MIP Feature Data		

Fig.7 depicts newly defined EAP-Success message which can embed BA and the address of newly assigned HA in this paper.

EAP-Success Packet Format in RFC 2284

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Code	Identifier	Length

Where,
Code : 3 (Success)

Newly Defined EAP-Success Packet Format

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

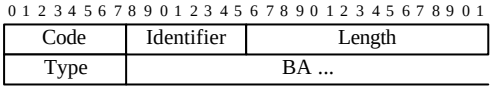
Code	Identifier	Length
Type	Typed-Data ...	

Where,
Code : 3 (Success)
Type :
0 : None (Success Only)
1 : BA-Embedded
2 : BA and HA's Address-Embedded
Type-Data :
BA / BA and HA's Address

Fig. 7. New EAP-Success Packet Format

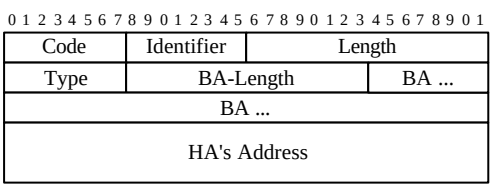
- Type 0
  EAP-Success message only
- Type 1
  EAP-Success message contains BA message. Typed-Data filed is as follows.

Newly Defined EAP-Success(BA) Packet Format



- Type 2
  EAP-Success message contains BA message and the address of newly assigned HA of MN. HA's address field is 128-bit unsigned value. Typed-Data filed is as follows.

Newly Defined EAP-Success(BA-HA's Address) Packet Format



Indirect BU to HA via the AAA infrastructure has advantage in respect of reducing traffic. Because BU can be embedded to EAP authentication message and forwarded to HA via AAA infrastructure, MN needs not to send BU to HA separately. But whenever BU is needed, AAA infrastructure must be involved which may traverse many network nodes. On the other hand, direct BU method needs separate BU from MN to HA without use of the AAA infrastructure. This is additional round-trip compared to indirect BU which is embedded to EAP authentication message and AAA messages. But if fast handoff mechanism is supported such as IAPP [10], this direct BU is far better than indirect BU. Fast handoff mechanism like IAPP enables local re-authentication once MN was authenticated successfully in AAAF. This means that re-authentication caused by handoff does not involve AAAH so the AAA infrastructure is not needed. Direct BU to HA can save network traffic that may traverses many network nodes.

IV. Conclusion

Mobile IPv6 supports mobility in IPv6, but does not specify how to gain access to network when mobile node is away from its home. IEEE 802.1x authentication defines how to authenticate user who wants to gain network access. IEEE 802.1x in the Wireless LAN integrated with AAA enables user to acquire wireless network access in the roaming environments.

In this paper, we give efficient integration of Mobile IPv6 over IEEE 802.1x-based Wireless LAN using Diameter in roaming environments. We assume that Diameter carries IEEE 802.1x authentication messages between foreign AAA and home AAA. To integrate Mobile IPv6 with Wireless LAN, we propose indirect BU which is sent to HA via the AAA infrastructure on behalf of MN when IEEE 802.1x authentication is processed. Also we propose direct BU which is sent to HA by MN without the AAA infrastructure after IEEE 802.1x authentication finished successfully.

References

1. D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", IETF Internet-Draft, draft-ietf-mobileip-ipv6-20.txt.
2. Charles E. Perkins, Ernie Tacsik, Thomas Eklund, "AAA for IPv6 Network Access", IETF Internet-Draft, draft-perkins-aaav6-06.txt.
3. Pat R. Calhoun, John Loughney, Erik Guttman, Glen Zorn, Jari Arkko, "Diameter Base Protocol", IETF Internet-Draft, draft-ietf-aaa-diameter-17.txt.
4. Pat R. Calhoun, Tony Johansson, Charles E. Perkins, "Diameter Mobile IP Application", IETF Internet-Draft, draft-ietf-aaa-diameter-mobileip-14.txt.
5. Pat R. Calhoun, Glen Zorn, David Spence, David Mitton, "Diameter Network Access Server Application", IETF Internet-Draft, draft-ietf-aaa-diameter-nasreq-11.txt.
6. T. Hiller, G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", IETF Internet-Draft, draft-ietf-aaa-eap-01.txt.
7. Stefano M. Faccin, Franck Le, Basavaraj Patil, Charles E. Perkins, "Diameter Mobile IPv6 Application", IETF Internet-Draft, draft-le-aaa-diameter-mobileipv6-03.txt
8. L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", IETF RFC 2284
9. "IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control", IEEE Std 802.1X-2001
10. Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation, IEEE P802.11F/D, January 2003