A STUDY ON IMPROVED PKMv2 FRAMEWORK FOR FAST MOBILITY IN 802.16e NETWORKS

GiJun Suh [1], *Seunghwan Yun* [1], *Okyeon Yi* [2], *Sangjin Lee* [1]

[1] Graduate School of Information Management & Security, Korea University, Seoul, Korea
{gjsuh, schneeleopard, sangjin}@korea.ac.kr

[2] Department of Mathematics, Kookmin University, Seoul, Korea
oyyi@kookmin.ac.kr

ABSTRACT

EAP (Extensible Authentication Protocol) is often used as an authentication framework for two-party protocol which supports multiple authentication algorithms known as "EAP method". And PKMv2 in 802.16e networks use EAP as an authentication protocol. However, this framework is not efficient when the EAP peer executing handover. The reason is that the EAP peer and EAP server should re-run EAP method each time so that they authenticate each other for secure handover. This makes some delays, so faster re-authentication method is needed. In this paper, we propose a new design of the PKMv2 framework which provides fast re-authentication. This new framework and usage of the keys which used as a short-term credential bring better performance during handover process.

Keywords: PKMv2 framework, fast authentication, 802.16e, handover

1. INTRODUCTION

There is increasing demand for high speed, wireless communication irrespective of time and place. To fulfill the need, functions of user management and control are necessary. This is the main reason that wireless operators use AAA (Authentication, Authorization and Accounting) [1].

In AAA infrastructure, EAP (Extensible Authentication Protocol) [2] of IETF is the typical two-party protocol for authentication of mobile. Usually, EAP method generates cryptographic material after authentication process and can establish secure communications with this material.

For 802.16e PKMv2 framework based EAP protocol, seamless handover to wireless network user on traveling is a very important technology. Especially, efficient hand-over technology with very high speed communication is crucial. The network using conventional PKMv2 framework of 802.16e standard, however, AAA and MS have to generate another key for a re-authentication.

In this paper, we propose new PKMv2 framework and key usage for fast, seamless handover to overcome this limitation. Furthermore, application of proposed framework to 802.16e [3] network and analysis in standpoint of security will be discussed.

EAP framework and PKMv2 is introduced in section 2 and improvement of proposed framework is discussed in section 3. In section 4, security consideration of proposed framework is explained and concluded in section 5.

2. OVERVIEW

In this section, structure and operation of EAP framework and 802.16e PKMv2 are introduced. (Also, EAP operation in 802.16e network is analyzed.)

2.1 EAP Protocol

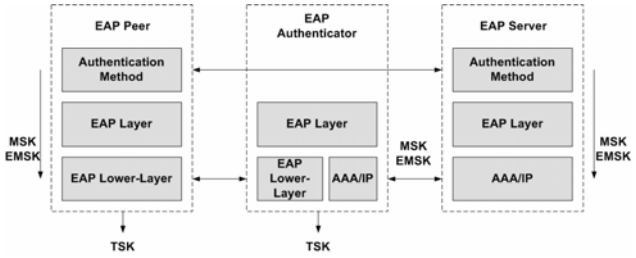

Fig. 1: EAP Framework

EAP is defined in [2] as an authentication protocol which supports multiple authentication algorithms known as "EAP method". EAP was originally developed for run directly over data link layers. It has been applied to IEEE 802 wired networks like 802.1x [4] and wireless networks like IEEE 802.16e. EAP is a two-party protocol between the EAP peer and EAP server. For instance, in 802.16e networks, the EAP peer is located at the MS (Mobile Station) and the EAP authenticator is located in BS (Base Station) and the EAP server is in AAA server.

Fig.1 shows EAP framework and derived keys aimed at positioning EAP elements in the AAA architecture.

Management and distribution of keys are defined by EAP Key Management Framework [5]. First, MSK (Master Session Key) and EMSK (Extended Master Session Key) are generated in the EAP peer and the EAP server is through an EAP method. Then, the EAP server delivers these keys to the EAP authenticator using AAA protocol. The EAP peer and authenticator make security association

by creating TSK (Transient Session Key) based on MSK. EMSK is reserved for future use.

2.2 EAP based PKMv2 Framework

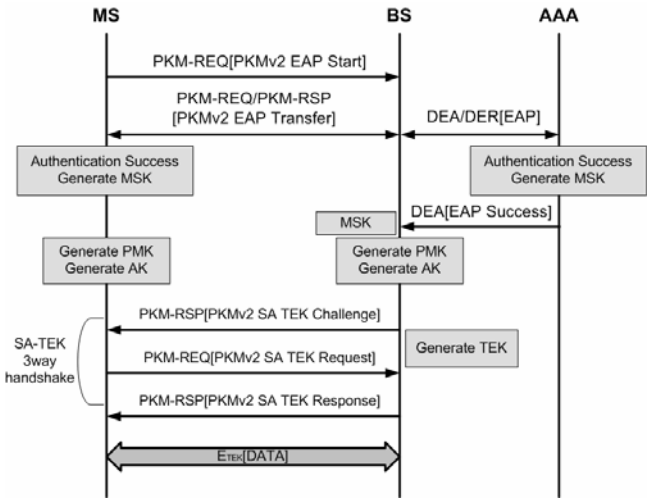

Fig. 2: EAP based PKMv2 framework

802.16e network is a technology for combination of fast communication speed and mobility which are advantages of 802.11 and 3G networks, respectively. Current authentication protocol of 802.16e is PKMv2.

Among the PKMv2 protocols, using EAP as an authentication protocol is discussed in this paper.

One-way authentication, the drawback of PKMv1, is improved to two-way in 802.16e PKMv2. Both RSA-based and EAP-based authentication is feasible in PKMv2. In this paper, EAP-based PKMv2 is chosen. As shown in figure 3, PKMv2 consists of MS (Mobile Station), BS (Base Station), and AAA protocol. MS and BS use PKM-REQ, PKM-RES messages, and BS and AAA sever use Diameter protocol for communication. After authentication MS and AAA generate MSK (Master Session Key), and AAA delivers the MSK to BS. Then, TEK used for communication is generated through SA-TEK 3-way handshake using PMK (Pairwise Master Key) and AK(Authentication Key) generated by MS and BS.

2.3 Problems

Current EAP standard does not consider the efficiency of handover, which causes many problems. These problems will be shown in this section.

2.3.1 Inefficient Re-authentication Process

During handover, or when a mobile device changes the access point (i.e network access server or BS in 801.16e), the EAP peer and the EAP server should rerun EAP method and keying material that should be authenticated again. This process results in long delay and can be a serious problem to provide seamless services.

2.3.2 EAP server manages too many EAP authenticators

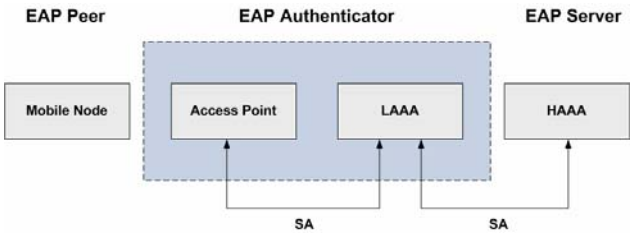

Fig. 3: Separation and Relations of AAA

EAP standard defines that EAP server on the EAP authenticator and AAA server should make SA to protect keying material. It indicates that an EAP server have to control too many EAP authenticators. In reality, therefore, it is efficient that the EAP authenticators makes SA with LAAA (local AAA) of each domain and let HAAA (home AAA) control each LAAA as shown in figure 3. [6]

2.3.3 Lack of extension keys

Recently, HOKEY (handover key) for rapid handover has been studied actively. HOKEY is investigated in HOKEY WG of IETF and is focused on Low-latency re-authentication, Handover key management and pre-authentication. Moreover in current standard there is no extended key that can be used externally except for EMSK. To solve the lack of extension and for HOKEY management EAP extension protocol such as EAP-EXT [7], EAP-ER [8] are proposed and studied. USRK (Usage Specific Root Key) is a study about key generation for extension. [9] This paper proposes the way of raising the efficiency of authentication through USRK generated from EMSK.

3. IMPROVED PKMv2 FRAMEWORK

In this section, PKMv2 framework is proposed which solves the problems indicated in section 2.3.

3.1 Improved PKMv2 Framework in 802.16e

Figure 4 shows the proposed PKMv2 framework. The process is as follows.

Step 1. (MS => BS)
PKM-REQ[PKMv2 EAP Start]

A mobile asks for the start of authentication by sending PKMv2 EAP start message. BS which receives the EAP start message starts authentication process and plays a role of relay by connection to authentication server.

Step 2. (BS => MS)
PKM-RSP[EAP Request/Identity]

BS which receives the EAP start message sends a message for ID request to mobile.

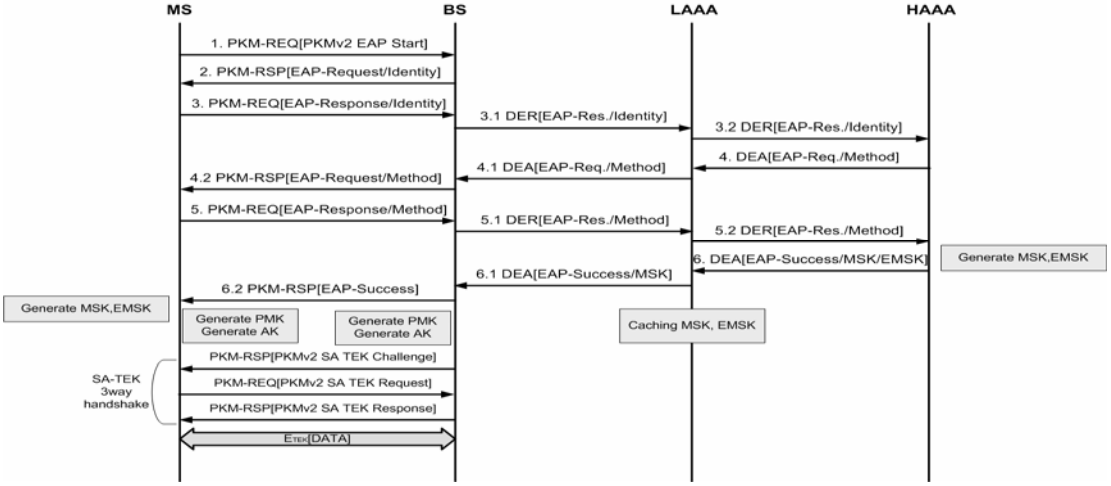

Fig. 4: Improved PKMv2 in 802.16e networks

Step 3. (MS => BS)
PKM-REQ[EAP-Response/Identity]
Step 3.1 (BS => LAAA)
DER[EAP-Res./Identity]
Step 3.2 (LAAA => HAAA)
DER[EAP-Res./Identity]

MS sends unique identity by the form of NAI (Network Access Identifier)[10].

Step 4. (HAAA => LAAA)
DEA[EAP-Req./Method]
Step 4.1 (LAAA => BS)
DEA[EAP-Req./Method]
Step 4.2 (BS => MS)
PKM-RSP[EAP-Request/Method]

The server which receives identity sends the answering message and EAP-method to be used to MS.

Step 5. (MS => BS)
PKM-REQ[EAP-Response/Method]
Step 5.1 (BS => LAAA)
DER[EAP-Res./Method]
Step 5.2 (LAAA => HAAA)
DER[EAP-Res./Method]

After verification of network authentication, MS sends an EAP method to be used to AAA.

Step 6. (HAAA => LAAA)
DEA[EAP-Success/MSK/EMSK]
Step 6.1 (LAAA => BS)
DEA[EAP-Success/MSK]
Step 6.2 (BS => MS)
PKM-RSP[EAP-Success]

HAAA generates MSK and EMSK and sends them to LAAA using AAA protocol. Then, LAAA saves the keys and sends MSK to BS. Finally, BS informs MS of success of EAP protocol by sending EAP-Success message.

Afterwards, MS communicates with BS using MSK generated by MS itself.

3.2 Re-Authentication

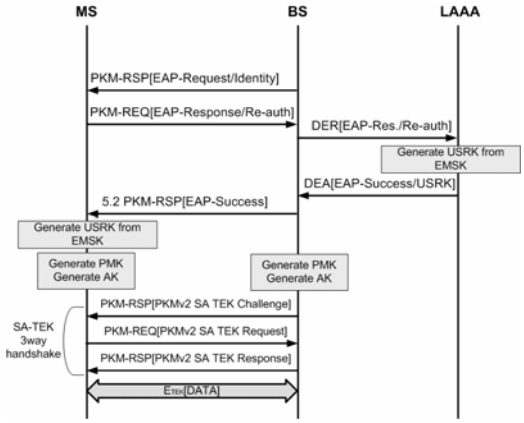

Fig. 4: Re-authentication process of Improved PKMv2

In current PKMv2, new MSK should be generated by AAA when it is authenticated again. It is a very inefficient process in 802.16e network which mobility support is an important factor. We use EMSK and USRK generated by EMSK to make it efficient. As already mentioned in section 2.1.1.2, BS and LAAA have to make SA with LAAA and HAAA, respectively. However, since key distribution is performed in LAAA, it is not necessary to make SA between BS and HAAA. When the MS executes handover to connect other BS, the BS requests a new session key to LAAA. And then, LAAA sends BS USRK which generated from EMSK stored before handover. MS also generate a new USRK as a short-term credential simultaneously.

3.3 USRK as Master Session Key for Re-auth.

$$USRK = KDF(EMSK, key\ label, optional\ data, length)$$

The key labels are printable ASCII strings unique for each usage definition with maximum of 255 octets. The length is a 2-octet unsigned integer in network byte order of the

output key length in octets. The default KDF (Key Derivation Function) for deriving from an EMSK is taken from the PRF+ (Pseudo Random Function+) key expansion defined in [11]. In this paper, USRK is used as a session key to be used after re-authentication, or it plays a role of MSK at the first authentication. Because PRF is HMAC-SHA-256, many USRK can be generated using nonce generated by MS in optional data field.

4. CONSIDERATIONS

Optional Data in USRK: In this paper, because USRK is used as a session key for re-authentication, many USRK should be able to be generated and be safe from replay attack, for this reason, we use the sequence number generated by the MS in the optional data field. And the EAP identity message should include a sequence number.

Lifetime of USRK: For safe key use in 802.16e network, the lifetime of USRK should be shorter than that of MSK. If the lifetime of MSK is not defined, it is substituted by PMK lifetime which is set in PMK parameter value.

LAAA Stores MSK, EMSK: LAAA should save MSK and EMSK for fast key generation during handover. Also, LAAA should have the information about SAID for identification of EMSK matched with MS.

4.1 Security Considerations

This section provides an analysis of the proposed protocol in accordance with the AAA key management requirements specified in [13].
We especially analyze security requirements that can be modified when applying USRK to PKMv2.

Table 1: Security Considerations

Requirement	Note
Strong, fresh session key	USRK generated by MS to communicate with new BS is generated newly each time. Because it uses SHA-256, there is no way to find out what another USRK is if one of the USRK is leaked out.
Limit key scope	EMSK generated by HAAA is saved only in LAAA. USRK is saved only in BS on communication that restricts key scope.
Replay detection mechanism	In USRK, calculation includes sequence number of MS and LAAA, it is safe from replay attacks.
Keying material confidentiality	Because MS and BS generate key independently from the same parameter, confidentiality is satisfied.
Prevent the domino effect	One of the compromises in MS does not influence on keying material of another MS. Because USRK is the key used between one MS and one BS, it does not cause the domino effect.
Bind key to its context	All generated USRK use key name of corresponding USRK in key label field.

5. CONCLUSION AND FUTURE WORK

Recently, 'WiBro evolution system' technology is developed in Korea. This technology is planned to be applied to 802.16m on standardization and has an advantage of providing very high speed. Authentication technology for seamless handover in fast communication will be more important. We proposed a fast authentication method during handover in this paper. It will be necessary to study about extension of EAP message for using proposed framework. Study about key management between mains using DSRK (Domain Specific Root Key) is also necessary.

6. REFERENCES

[1] C. de Laat, G. Gross, L. Gommans, J. Vollbrecht and D. Spence. "Generic AAA Architecture," RFC 2903, August 2000.

[2] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. "Extensible Authentication Protocol (EAP)," RFC 3748, June 2004.

[3] IEEE, "Standard for Local and metropolitan area networks-Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems," IEEE Std 802.16e, October 2005.

[4] IEEE, "Standard for Local and metropolitan area networks, port-based network access control," October 2001.

[5] B. Aboba, D. Simon and P. Eronen. "Extensible Authentication Protocol (EAP) Key Management Framework," RFC 5247, August 2008.

[6] R. Lopez and A. Skarmeta et al., "Improved EAP Keying Framework for a Secure Mobility Access Service," IWCMC'06 pp. 183-188 2006.

[7] Y. Ohba, S. Das, and R. Lopez, "An EAP Method for EAP Extension (EAP-EXT) ", Internet-Draft, July 2007

[8] V. Narayanan and L. Dondeti, "EAP Extensions for Efficient Re-authentication", Internet-Draft, January 2007.

[9] J. Salowey, L. Dondeti, V. Narayanan and M. Nakhjiri. "Specification for the Derivation of Root Keys from an EMSK," Internet-Draft, June 2008.

[10] B. Aboba, M. Beadles, J. Arkko and P. Eronen "The Network Access Identifier, " RFC 4282, December 2005

[11] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol," RFC 4306, December 2005.

[12] R. Housley and B. Aboba, "Guidance for Authentication, Authorization, and Accounting (AAA) Key Management," RFC 4962, July 2007.