IEICE TRANS. COMMUN., VOL.E105–B, NO.2 FEBRUARY 2022

PAPER

An IKEv2-Based Hybrid Authentication Scheme for Simultaneous Access Network and Home Network Authentication

MyeongJi KO[†], **Hyogon KIM**[†], ***Nonmembers***, ***and*** **Sung-Gi MIN**[†a)], ***Member***

SUMMARY To access Internet services supported in a home network, a mobile node must obtain the right to use an access network, and it must be able to contact a home network gateway to access the Internet in the home network. This means that the device must be authenticated by an AP to use the access network, and it must additionally be authenticated by the home network gateway to access its home network. EAP-PEAP is currently the most commonly used authentication protocol in access networks, and IKEv2 is common security protocol for mutual authentication on the Internet. As the procedures in EAP-PEAP and IKEv2 are quite similar, EAP-PEAP can be replaced by IKEv2. If the access network authentication uses IKEv2-based protocols and the home network authentication also uses IKEv2, the IKEv2 messages exchanged in each authentication become duplicated. However, it should be noted that EAP-IKEv2 is not able to carry EAP exchanges. We propose a hybrid authentication mechanism that can be used to authenticate a mobile node for both networks simultaneously. The proposed mechanism is based on the IKEv2-EAP exchanges instead of the EAP exchanges currently used to authenticate the access network, but our scheme adopts the encapsulation method defined by EAP-IKEv2 to transport the IKEv2 message over IEEE 802.11 so as not to change the current access network authentication architecture and the message format used by the authentication protocols. The scheme authenticates both networks through a single IKEv2 authentication, rather than two authentication procedures - one for the access network and one for the home network. This reduces the number of exchanged messages and authentication time.

key words: *authentication, EAPOL, IKEv2, EAP*

1. Introduction

When a mobile node (MN) wants to connect to an access network for Internet access, the MN must be authenticated and authorized by the Access Point (AP) in the access network to access the Internet. The home network of the MN is connected to the Internet via the gateway called the home network gateway. The MN must be authenticated and authorized by the home network gateway to use services provided by the home network, such as VPN or 5G services.

One of the most common wireless access networks is wireless LAN (WLAN), which uses IEEE 802.11 [1] technology. In an IEEE 802.11 access network, a MN must be authenticated by an AP to which the MN is attached. If the MN uses the IEEE 802.1X [2] Authentication and Key Management (AKM) method, the AP starts the EAP authentication [3] with the MN. Then, the AP relays the EAP messages between the MN and the Authentication Server (AS). The AP uses IEEE 802.1X EAPOL-EAP to transport EAP messages between itself and the MN, and RADIUS [4] for the AS. The actual authentication is carried out between the MN and the AS using the specific EAP method, e.g., EAP-PEAP [5], selected by the AS.

EAP-Protected EAP (EAP-PEAP) [5] is an EAP-based authentication method that is widely used by access networks. It consists of two phases: In the first phase, the MN and the AS establish a secure Transport Layer Security (TLS) [6] tunnel to protect the EAP messages exchanged between them. In the second phase, the specific EAP authentication is performed between the MN and the AS.

For home network access, the MN must contact its home network gateway via the Internet. The home network gateway requests authentication for the MN to access its services. The IKE version 2 (IKEv2) [7] and IP security [8] are common security protocols for mutual authentication and secure data transfer on the Internet. IKEv2 also supports an EAP authentication procedure. We call this IKEv2-EAP. IKEv2 consists of two phases: the IKE_SA_INIT exchanges and the IKE_AUTH exchanges. In the IKE_SA_INIT exchanges, the initiator and the responder establish the IKE_SA, which protects all IKEv2 messages exchanged between them. In the IKE_AUTH exchanges, they authenticate each other, so that, if they are used, the EAP authentication procedure is executed in this phase.

It is of note that the EAP-PEAP and IKEv2 authentication methods are quite similar. They both consist of two phases: In the first phase, the MN and the AS establish a secure channel to protect subsequent authentication messages. In the second phase, they exchange their real identities and authenticate each other. In other words, EAP-PEAP can be replaced by IKEv2. However, there is no method for directly transporting IKEv2 over WLAN. There is an EAP method for IKEv2 [10], which is called EAP-IKEv2. EAP-IKEv2 can be used for access network authentication. When the MN uses a service in the home network via an access network, it should execute the IKEv2 for the home network authentication, even though EAP-IKEv2 and IKEv2 share the same authentication information. Also, it carries out public-key authentication twice. The public-key authentication consumes the most computational resources and time on the MN and on the AS during authentication [9]. This can be a problem in a 5G network environment with ultra-low latency characteristics [11] or in an IoT environment with resource-constrained devices [12]. In addition, EAP-IKEv2 does not carry EAP exchanges, as explicitly described in

Manuscript received April 20, 2021.
Manuscript revised July 13, 2021.
Manuscript publicized September 1, 2021.

[†]The authors are with Department of Computer Science and Engineering, Korea University, Seoul, South Korea.
a) E-mail: sgmin@korea.ac.kr (Corresponding author)

DOI: 10.1587/transcom.2021EBP3066

Copyright © 2022 The Institute of Electronics, Information and Communication Engineers

[10].

In this paper, we propose a hybrid authentication scheme that can be used to either authenticate a mobile node for the access network only or can simultaneously authenticate a MN for the access network and home network. This scheme is based on the IKEv2-EAP procedure for authentication, and it uses the EAP-IKEv2 encapsulation method to transport the IKEv2 messages directly over a wireless link. All message flows exactly follow IKEv2-EAP exchanges. In IEEE 802.1X, the AP relays the EAP messages between the MN and the AS. In the proposed scheme, the home network gateway acts as the AS for the AP, and all IKEv2 messages are encapsulated in the EAP-IKEv2 packet format. Therefore, the AP can handle IKEv2 messages like EAP messages and forward them via RADIUS to the AS, without the need for any modifications for AP operation. However, encapsulating in the EAP-IKEv2 packet format involves as much overhead as EAP-IKEv2 header size. Still, it is negligible because it is a small number of bytes compared to the reduced number of messages exchanged. When the specific EAP authentication has been successfully completed, the home network gateway supplies the Master Shared Key (MSK), which is used for IEEE 802.11 4-way handshaking, to the AP if the EAP authentication has been completed successfully. The scheme authenticates both networks through a single IKEv2 authentication, so it reduces the number of message exchanges and the mutual authentication time compared to the two independent authentications conventionally required by the access network and home network. Also, it can provide more faster services in the home network, such as VPN, to users.

The rest of this paper is organized as follows. Section 2 presents related works. Section 3 describes the procedure for IEEE 802.11 with IEEE 802.1X, IKEv2-EAP procedure, and correlation between them. Section 4 describes the proposed hybrid authentication mechanism in detail. Section 5 presents a comparison of the proposed mechanism and authentication protocols for the access and the home network. Section 6 presents a security analysis of the proposed authentication mechanism. Section 7 presents the simulation results. Finally, Sect. 8 concludes this paper.

2. Related Works

The main focus of the proposed hybrid authentication scheme is to perform both access and home network authentication simultaneously without any modification of authentication message format and architecture. However, to our knowledge, there has been no proposed mechanism for simultaneously performing both network authentications.

There have been several proposals [13]–[15] for key exchange protocol. [13] proposed a certificate-less collaborative key agreement technique for IoT which is a variant of the IKEv2 key agreement protocol. [14] proposed TinyIKE, a lightweight adaptation of IKEv2 for the IoT. However, they have proposed a key exchange mechanism using IKEv2 only in a limited environment called IoT, and they do not simultaneously perform access and home network authentication. [15] proposed for improved security of the access network authentication using PEAP. Since PEAP requires digital certificates only in terms of authentication on the server, the client's digital certificates have improved the security of wireless intervals by replacing them with user names and passwords. However, this is only a complementary mechanism to the PEAP mainly used in access networks, not a mechanism that simultaneously performs access network and home network authentication.

3. Standardized Key Exchange and Authentication Protocols

3.1 IEEE 802.11 with IEEE 802.1X

One of the most common non-3GPP networks is the wireless LAN defined in IEEE std 802.11-2016. It supports two authentication mechanisms: One uses a Pre-Shared key and the other uses IEEE 802.1X. Figure 1 shows an IEEE 802.1X authentication flow with the EAP-IKEv2 protocol.

A beacon sent by an AP contains the supported authentication mechanisms in its Robust Secure Network Element (RSNE) of the Beacon message. If a supplicant, which is the same as an MN, requests the IEEE 802.1X authentication, then it includes the IEEE 802.1X method as the AKM method in the RSNE as part of its association message sent to the AP (Messages#1,2,3).

The supplicant and the AP use EAPOL-EAP messages to carry EAP messages. The supplicant may send an EAPOL-Start message to initiate the EAPOL authentication. The AP sends an EAP-request/Identity message to the supplicant (Message#4), and the supplicant responds to the EAP-Request by supplying an identity, which is then used to route the EAP-response to an AS (Messages#5,6). The AS starts a specific EAP authentication for the supplicant. After the specific EAP authentication, the AP receives the MSK encapsulated in a Compounded Secure Key (CSK) component, which is piggybacked on the last EAP-Success message. Then, the supplicant and the AP perform IEEE 802.11 4-way handshaking to establish a secure channel between them using MSK. In this way, the supplicant is allowed

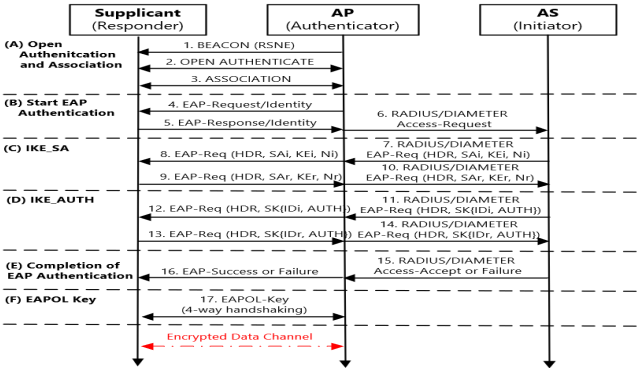


Fig. 1 Flow of EAP authentication using IKEv2 (EAP-IKEv2).

to use the access network.

The EAP-IKEv2 is an EAP mechanism, which is based on the IKEv2 protocol. The EAP-IKEv2 consists of two phases, and IKEv2 messages are encapsulated in the EAP data field of the EAPOL-EAP messages. The first phase is IKE_SA (Messages#7,8,9,10). In this phase, the supplicant and the AS establish an IKE_SA, and this IKE_SA is used to protect all IKEv2 messages exchanged in the second phase. In the second phase, the supplicant and the AS authenticate each other by exchanging their identities and certificates if needed (Messages#11,12,13,14). If this mutual authentication is successful, the AS supplies the MSK to the AP (Messages#15,16). As the AP only requires authentication of the MN, the EAP-IKEv2 mutually authenticates the initiator and the responder, but it does not establish the first child SA like the first phase of the IKEv1 protocol. The roles of the initiator and the responder in the IKEv2 protocol are reversed in the EAP-IKEv2. As a result, the semantics of the payloads sent by the EAP-IKEv2 and IKEv2 are different. For example, in EAP-IKEv2, SAi is the list of cryptography algorithms supported by the AS, but in IKEv2, it is the list of cryptography algorithms supported by the supplicant. In IKEv2, the initiator usually sends the first child SA information and the responder starts the EAP mechanism by sending an EAP payload. As the roles of the initiator and the responder are reserved in EAP-IKEv2, piggybacking this information on EAP-IKEv2 messages at the IKE_AUTH stage is not compatible with the IKEv2 protocol. Further, in IKEv2, the responder may allocate an IP address for the supplicant, and it selects the appropriate IP ranges among the traffic selectors sent by the supplicant. According to the EAP-IKEv2 standard, the EAP-IKEv2 message cannot carry EAP exchanges.

3.2 IKEv2-EAP Procedure

Internet authentication architecture is defined in [16]. It uses IKEv2 as the default authentication protocol and IP Security (IPsec) protocol [17], [18] to protect user traffic. The IKEv2 supports EAP authentication. We call this the IKEv2-EAP procedure. Figure 2 shows the flow of IKEv2-EAP authentication.

IKEv2 always starts with an IKE_SA_INIT exchange. This establishes an IKE_SA that securely transports all following IKEv2 messages (Messages#1,2). Following the IKE_SA exchange, IKEv2 starts the IKE_AUTH exchanges. If the initiator is intended to use an EAP mechanism for its authentication, it omits the authentication (AUTH) payload in the first message of the IKE_AUTH exchanges (Messages#3,4,5,6). It includes the IDi payload and information for child_SA establishment. By detecting this omission, the responder starts EAP authentication. All EAP messages are encapsulated in the EAP payload element in the IKEV2 messages. The IKEv2 standard suggests that the contents of the IDi payload can be used for AS routing purposes as well as for selecting which EAP method to use. In examining at the flow of IKEv2 using EAP authentication in Fig. 2, we can

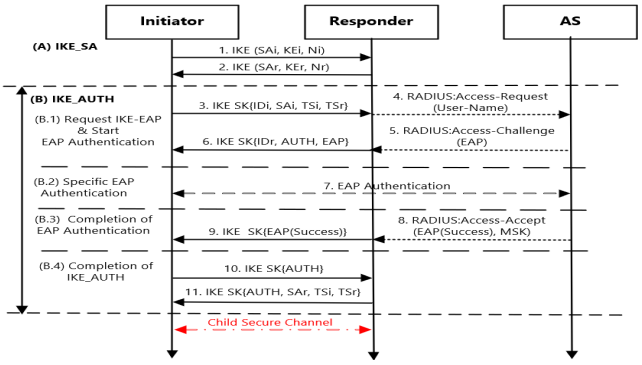


Fig. 2 Flow of IKEv2 using EAP authentication (IKEv2-EAP).

see the content of the IDi payload is used for this purpose, and it is carried in the User-Name attribute of the Radius Access-Request (Message#4). The AS then starts a specific EAP authentication, e.g., EAP-TLS [19], with the initiator (Message#7). If the EAP authentication is successful, the AS may supply an MSK to the responder (Messages#8,9). After receiving the EAP-Success message, the initiator and the responder completes the IKE_AUTH exchanges by exchanging the AUTH payload signed by the MSK (Messages#10,11). The last response message includes the selected child SA information from the child SA establishment, which was sent by the initiator in the first message of the IKE_AUTH exchanges.

3.3 Correlation between IEEE 802.11 with IEEE 802.1X and IKEv2

EAP-PEAP [5] is a commonly used EAP mechanism at IEEE 802.11 with IEEE 802.1X. The EAP-PEAP and IKEv2 authentication methods are quite similar; they consist of two phases: In the first phase, they establish a secure channel to protect subsequent authentication messages. In the second phase, the MN and the AS exchange their real identities and authenticate each other. IKEv2-EAP assumes that the responder may receive an MSK as a result of the IKEv2-EAP procedure. If the AP and the IKEv2 responder cooperate with each other, then a single EAP authentication may mutually authenticate both the MN and the AS. The IKEv2 responder may supply the MSK for the AP on behalf of the AS. Mutual verification between the MN and the AP can be done independently using IEEE 802.11 4-way handshaking, and the mutual verification of the MN and the home network gateway is included in the IKEv2-EAP procedure. This means that the IKEv2 and IKEv2-EAP procedure may be used for the MN authentication on the access network.

4. Proposed Hybrid Authentication Mechanism

4.1 Proposed Hybrid Authentication Architecture

There are a few assumptions in the proposed hybrid authentication scheme. First, the AP and the home network gateway

Fig. 3 Proposed hybrid authentication architecture.

have established secure channels in advance, such as IPSec or L2TP [21]. Secondly, the home network gateway and the AS belong to the same administrative domain. Consequently, the communication channels between the AP and the home network gateway and between the home network gateway and the AS are secure.

The components of the proposed mechanism are the mobile nodes, APs, home network gateways, and the AS. Figure 3 shows the network architecture for the proposed mechanism.

4.1.1 Mobile Nodes

A mobile node (MN) acts as the supplicant for IEEE 802.1X authentication and as the initiator for the IKEv2-EAP authentication. It sends the EAPOL-Start with a NID element for the AP to indicate which AS the succeeding EAP messages should be forwarded to. The sending module of the MN encapsulates an IKEv2-EAP message in an EAP-IKEv2 message, and then it must set the IKEv2-EAP flag in the flag field of the EAP-IKEv2 header. If the MN solely wants to authenticate for the access network and not for the home network, it also sets the Authentication-Only flag in the flag field of the EAP-IKEv2 header. The EAP-IKEv2 message is carried by an EAPOL-EAP message. After the MN receives the EAP-Success message, it executes IEEE 802.11 4-way handshaking with the AP. This establishes a link-level secure channel between them. At this point, the authentication procedure for the access network is completed.

If the MN is going to use services in the home network, it follows the IKEv2 standard to complete ongoing IKE_AUTH exchange. In the last IKE_AUTH exchange, the MNs and the home network gateway exchange the AUTH payload to verify each other and the child SA information to establish the first SA between them.

4.1.2 Access Points (APs)

An AP acts as the authenticator for IEEE 802.1X authentication. It interacts with the MN using EAPOL-EAP and with the AS using RADIUS. When the EAP authentication is successful, it starts IEEE 802.11 4-way handshaking with the MN using the MSK supplied by the AS. In our scheme, the home network gateway acts as an AS for the AP. The AP may use the same operations for an AS to the home network gateway. The home network gateway encapsulates the MSK in the MS-MPPE-Recv-Key [20] attribute of a RADIUS Access-accept message.

After the MN is authorized to use the access network and the AP has completed IEEE 802.11 4-way handshaking, the AP's role in the access network authentication is completed. Therefore, the AP is no longer involved in any ongoing IKE_AUTH exchanges.

4.1.3 Home Network Gateways

The home network gateway acts as the responder for IKEv2-EAP authentication. When the home network gateway receives the RADIUS messages from the AP, it decapsulates the RADIUS messages and then checks the flag field in the EAP-IKEv2 message. If the IKEv2-EAP flag is set, it handles the message in the way defined by our scheme. Otherwise, it handles it according to EAP-IKEv2. If the Authentication-Only flag is set, it completes the authentication procedure after sending an EAP-Success message with the MS-MPPE-Recv-Key attribute. Otherwise, it must complete the ongoing IKE_AUTH exchanges.

4.1.4 The Authentication Server (AS)

The Authentication Server (AS) authenticates the MN using a specific EAP authentication. The AS supplies the MSK to the home network gateway with an EAP-Success message with the MS-MPPE-Recv-Key attribute.

4.2 Proposed Hybrid Authentication Procedure

The proposed mechanism consists of three phases: (1) Open Authentication and Association, (2) IKEv2 Initial Exchange (IKE_SA_INIT), and (3) IKEv2 Authentication Exchange (IKE_AUTH). The third phase consists of six sub-phases. Figure 4 shows the flow of the proposed mechanism.

4.2.1 Open Authentication and Association

This phase follows the open authentication and association procedure defined in the IEEE 802.11-2016 standard (Messages#1,2,3).

4.2.2 IKEv2 Initial Exchange - IKE_SA_INIT

A MN sends the EAPOL-Start with a Network Identity (NID) Set TLV (Message#4). The NID Set TLV includes information for the home network gateway, which the AP should contact. The NID name field in the NID Set TLV contains the address of the home network gateway.

The MN sends the IKE-SA-INIT request message to the AP using EAPOL-EAP (Message#5). Upon receipt of this packet, the AP takes off the EAPOL header, then re-encapsulates it in RADIUS before forwarding it to the home network gateway (Message#6). The home network gateway sends the IKE-SA-INIT reply message to the AP (Message#7), after which the AP forwards it to the MN using an EAPOL-EAP (Message#8). This exchange establishes an IKE_SA. The IKE_SA is used to protect subsequent IKEv2 message exchanges.

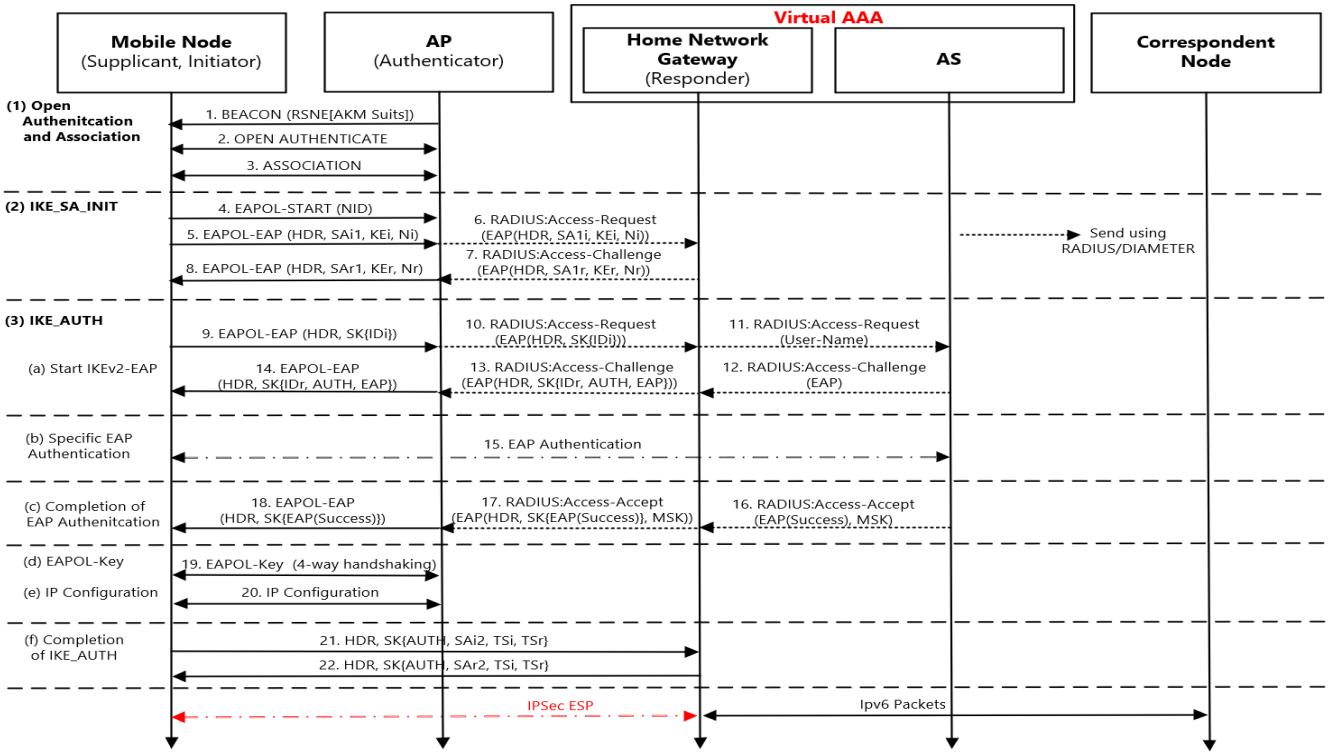


Fig. 4 Flow of proposed hybrid authentication mechanism.

4.2.3 IKEv2 Authentication Exchange - IKE_AUTH

A basic IKE_AUTH exchange is completed with a single message exchange. However, the IKEv2-EAP procedure consists of multiple message exchanges. In the proposed mechanism, the IKE_AUTH process consists of the following six sub-phases, (a)–(f).

(1) Starting IKEv2-EAP

The MN starts the IKEv2-EAP by sending the first IKEv2-request message (Messages#9,10). The IKEv2-request message includes the IDi payload but omits the AUTH payload to indicate its request for the IKEv2-EAP procedure. In our scheme, the first child SA information is also omitted from the first IKEv2-request message.

If the AUTH payload is omitted from the first IKE_AUTH message, the home network gateway knows that the MN will be authenticated with an EAP authentication. The home network gateway uses the content of the IDi payload for AS routing purposes, so it selects the AS using the content of the IDi payload. Then it copies the content of the IDi payload into the value field of the User-Name attribute of the RADIUS Access-request (Message#11). At this point, it forwards the RADIUS Access-request to the selected AS.

The AS selects the specific EAP authentication using the content of the User-Name attribute in the RADIUS Access-Request. The AS sends the RADIUS Access-Challenge with an EAP attribute (Message#12). The home gateway relays the EAP attribute in the EAP payload of the IKEv2-response with the first IKE_AUTH IKEv2-request message (Messages#13,14).

(2) Processing a Specific EAP Authentication

The MN and the AS perform the specific EAP authentication, e.g., EAP-TLS (Message#15).

(3) Completing the EAP Authentication

If the EAP authentication is successful, the AS sends the EAP-Success message and MSK to the home network gateway (Message#16). The home network gateway relays the EAP message and the MSK (Message#17). The RADIUS MS-MPPE-Recv-Key attribute may be used to convey the MSK. If the Authentication-Only flag is not set in the EAP-IKEv2 header, the MSK substitutes a “Shared Secret” for the pseudo random function (prf) to generate the AUTH value used in sub-phase (f). The “Shared Secret” and the prf are defined in [7]. The AP stores the MSK for 4-way-handshaking and relays the EAP-Success message to the MN (Message#18).

If the Authentication-Only flag is set in the EAP-IKEv2 header, the home gateway has completed its role as the AS for IEEE 802.1X authentication and the IKE_AUTH exchanges. Otherwise, it continues the IKE_AUTH exchanges for the home network authentication.

(4) IEEE 802.11 4-Way-Handshaking

The AP and the MN execute IEEE 802.11 4-way handshaking. They establish a secure channel between themselves. Upon completion of 4-way handshaking, the MN is autho-

rized to use the access network (Message#19).

(5) Mobile Node IP Configuration

The IP module at the MN initialize its IP module. It obtains its IP address, default gateway lists, and DNS server addresses (Message#20).

(6) Completing IKE_AUTH

When the MN wants to access services in the home network, it continues IKE_AUTH exchanges with the home network gateway. They then execute the last IKE_AUTH exchange. The MN sends the AUTH payload and the first child SA information omitted from the first standard IKEv2-request message in the IKE_AUTH exchanges (Message#21). Next, the home gateway responds by sending an IKEv2-response message (Message#22). At this point, as the MN can use the Internet, it sends the IKEv2 messages directly to the home network gateway. As a result, a child SA is established between the MN and the home gateway.

4.3 Proposed Methods for Compatibility with the Existing Protocol

The proposed authentication mechanism is based on the IKEv2-EAP procedure. There are two problems when IKEv2 is used by the access network. First, there is no method to carry IKEv2 messages over a wired or wireless LAN. To avoid using a new protocol and to provide backward compatibility with the existing standard, the proposed scheme uses the encapsulation method defined by the EAP-IKEv2. The proposed scheme introduces a new IKEv2-EAP flag (bit 6) and an Authentication-Only flag (bit 7) in the flag field of the EAP-IKEv2 message. Figure 5 shows the new flags in the flag field of an EAP-IKEv2 message.

The IKEv2-EAP flag is used to distinguish our scheme at the home network gateway. If the IKEv2-EAP flag is set, it acts as an IKEv2-EAP responder defined in the IKEv2 standard; otherwise, it may act as the initiator defined by EAP-IKEv2. Each IKEv2 message is carried as an EAP-IKEv2 message, and the EAP-IKEv2 messages are encapsulated in the EAP data field of an EAPOL-EAP message. The AP may, as usual, forward the EAP message to the AS using the RADIUS protocol. The Authentication-Only flag indicates whether the MN may access the home network. If the Authentication-Only flag is set, it performs the access network authentication only. The IKEv2-EAP is used to authenticate the MN via the home network gateway. Otherwise, it is intended for the MN to use services in the home network. In this case, the MN and the home network gateway must complete the IKE_AUTH exchange to verify each other by exchanging the AUTH payload and establishing the first child SA information.

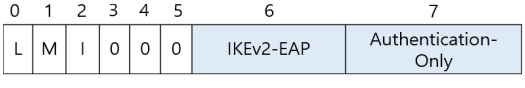


Fig. 5 New flags in the flag field of the EAP-IKEv2 message.

The other problem is that the AP does not know the AS to which the IKEv2-EAP messages must be forwarded. In IKEv2, an initiator identifies a specific responder using its database, such a Peer Authorization Database (PAD), and this allows it to make direct contact using an underlying protocol such as UDP. In the EAP protocol, the initial EAP exchange (the EAP-request/Identity and EAP-response/Identity) is used by the AP to route the following messages to the specific AS indicated by the EAP-response/Identity. To supply the AS information, the scheme uses an EAPOL-Start message with a Network Identity (NID) element. The NID element includes the AS information to which our messages must be forwarded.

In our scheme, the home network gateway supplies an MSK to the AP on behalf of the AS if the mutual authentication between the MN and the AS is successful.

5. Comparison

We compare the number of authentication messages exchanged during access network authentication by the proposed scheme to the number of messages sent using the conventional approaches. For this comparison, we select EAP-PEAP, EAP-IKEv2, EAP-TLS, and our scheme with the Authentication-Only flag set for the access network authentication, and while using the IKEv2-EAP procedure for the home network.

Table 1 shows the number of authentication messages exchanges needed to perform both access and home network authentication. The first row of Table 1 shows the number of authentication messages exchanged for the access network authentication. Note that we do not include the number of messages in the Open Authentication and Association phase. The EAP-PEAP consists of two phases: In the first phase, it exchanges 9 messages. The number of messages, α, exchanged in the second phase depends on the specific EAP authentication method used. As such, EAP-PEAP uses $9 + \alpha$ messages for the access network authentication [22]. The EAP-IKEv2 exchanges 7 messages, as shown in Fig. 1, and the EAP-TLS exchanges 9 messages [23]. Our scheme with the Authentication-Only flag set exchanges $6 + \beta$ messages. The β represents the number of EAP messages exchanged by the specific EAP authentication method in the IKE_AUTH sub-phase(b). The second row shows the number of IKEv2-EAP authentication messages exchanged for the home network authentication. The IKEv2-EAP exchanges $7 + \beta$ messages. As EAP-PEAP, EAP-TLS, and EAP-IKEv2 must perform the IKEv2-EAP procedure again, they exchange an additional $7 + \beta$ messages. Our scheme continues the IKE_AUTH exchanges for the home network authentication, as the MN and the home network gateway retain the authentication information generated at the access network authentication. They only need two messages to verify each other's authenticity by exchanging the AUTH payload.

The comparison shows that the proposed authentication mechanism and the EAP-PEAP use a similar number of

Table 1 Total message exchanges that perform network and home authentication.

	EAP-PEAP	EAP-IKEv2	EAP-TLS	Our Scheme
Access Network Authentication	$9 + \alpha^{*}$	7	9	$6 + \beta^{**}$
Home Network Authentication***	$7 + \beta$	$7 + \beta$	$7 + \beta$	2
Total Exchanged Messages	$16 + \alpha + \beta$	$14 + \beta$	$16 + \beta$	$8 + \beta$

* The number of messages exchanged by the specific EAP method at the PEAP Phase 2
** The number of messages exchanged by the specific EAP method at IKE_AUTH sub-phase (b)
*** We assumed that IKEv2-EAP is used for home network authentication

messages for the access network authentication. Unlike other methods, additional message exchanges are not avoidable, as they support the additional EAP procedure. However, our scheme reduces the total number of authentication messages exchanged. Further, our scheme only carries out public-key authentication once. The public-key authentication is required in many commonly used mutual authentication mechanisms, it consumes the most computational resources and time on the MN and on the AS during authentication [9].

As a result, our scheme may decrease the overall mutual authentication time. This reduction in authentication time is meaningful because the delay from 5G authentication has increased by 6.46% compared to that for 4G authentication [24].

6. Security Analysis

The proposed mechanism is based on the existing IKEv2-EAP protocol, except the child SA information is moved from the first request message to the last IKEv2-request message in the IKE_AUTH exchanges. Almost all security concerns are addressed by the IKEv2 protocol. The creation of a child SA is independent of the IKE_AUTH exchanges, and the importance of this is explicitly mentioned in the IKEv2 standard. The proposed mechanism also uses EAP-IKEv2 encapsulation to easily transport IKEv2 messages using the current authentication architecture. Our scheme introduces only two new flags in the flag field of the EAP-IKEv2 header to distinguish our scheme and its roles from the EAP-IKEv2. The EAP-IKEv2 protects its EAP messages using the "Integrity Checksum Data" field in the messages. For these reason, we only discuss the mutual authentications between the components of the proposed mechanism.

6.1 Mutual Authentication

Through the EAP authentication in phase 3-(c), a trust relationship is established between the MN and the AS. We assume that the AP and the home network gateway trust each other. The AP and the MN verify their possession of the MSK through IEEE 802.11 4-way handshaking. If both entities possess the same MSK, the AP's authenticity is guaranteed by the AS. The home network gateway and the MN also verify the possession of the same MSK in phase (f) of the IKE_AUTH exchanges. The MSK is used to generate the AUTH payload they exchange. If both entities verify that they have the same MSK through the AUTH payload, the authenticity of the home network gateway is guaranteed by the AS.

7. Simulator Implementation

We have implemented the proposed scheme on ns-3 simulator version 3.32 [25]. Simplified versions of EAPOL-EAP, IKEv2-EAP, RADIUS and IPSec were implemented to represent the packets used in our scheme. We omitted the specific EAP authentication in the IKEv2-EAP procedure, and we assumed that the EAP authentication was completed successfully and that the MN and the AS generate a common MSK.

Figure 6 shows the network configuration used in the simulation. The link delay for all wired links is set to 10ms and the link delay of the wireless link follows the YansWifiModel, which is predefined in the ns-3 simulator. In that model, propagation delay is calculated using the speed of light. In the experimental environment, the MN is set to be up to 74.33m away from the AP, so the maximum propagation delay that can occur is 250 nanoseconds. This network configuration environment is a scenario in which the MN wants to establish a VPN to the home network gateway.

Wireshark [26] is used to analyze the packet flows of the proposed mechanism and filter out irrelevant traffic such as neighbor discovery from the trace.

Figure 7 shows the packet traces at the AP's wireless interface and wired interface. Figure 7(a) shows the IKEv2-EAP messages that are transported by EAPOL-EAP. EAPOL-Start (Packet#28) is sent to the AP to indicate the start of authentication. Figure 8(a) shows the contents of this packet. It contains a Network Identity (NID) Set TLV, the NID name field of which is the address of the home network gateway (2002:1::200:ff:fe00:02 in the simulation).

Figure 7(b) shows the RADIUS and IKEv2-EAP messages. In Wireshark, the IKEv2 messages are marked as ISAKMP. The IKE_SA exchange is achieved in the first two messages (Packet#5 and Packet#6). The following three packets (Packet#7-Packet#9) show the IKE_AUTH phases (3-a) to (3-c). As mentioned above, IKE_AUTH sub-phase (3-b) is omitted. The newly defined IKEv2-EAP flag and Authentication-Only flag in the flag field of the EAP-IKEv2 header are shown in Fig. 8(b). Here, the IKEv2-EAP flag is set, but the Authentication-Only flag is not set.

The last EAP authentication message (Packet#9) is

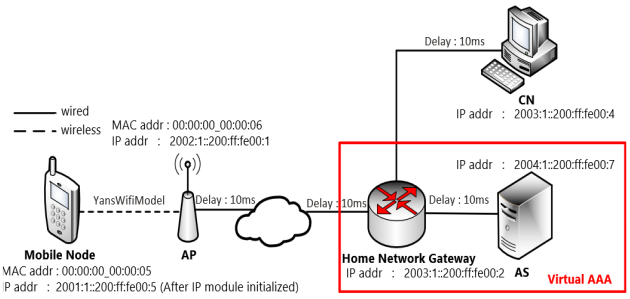


Fig. 6 Network configuration information for the simulation.

#	Time	Source	Destination	Proto	Info
28	00:00:00.947387	00:00:00_00:00:05	00:00:00_00:00:06	EAPOL	Start
30	00:00:01.200446	00:00:00_00:00:05	00:00:00_00:00:06	EAP	Request, Internet Key Exchange v2 EAP (EAP-IKEv2)
32	00:00:01.205510	00:00:00_00:00:06	00:00:00_00:00:05	EAP	Response, Internet Key Exchange v2 EAP (EAP-IKEv2)
34	00:00:01.206184	00:00:00_00:00:05	00:00:00_00:00:06	EAP	Request, Internet Key Exchange v2 EAP (EAP-IKEv2)
36	00:00:01.210708	00:00:00_00:00:06	00:00:00_00:00:05	EAP	Response, Internet Key Exchange v2 EAP (EAP-IKEv2)
43	00:00:01.502229	00:00:00_00:00:05	00:00:00_00:00:06	EAP	Success
50	00:00:01.508634	2001::200:ff:fe00:5	2003::200:ff:fe00:2	ISAKMP	IKE_AUTH MID=03 Initiator Request
52	00:00:01.513231	2003::200:ff:fe00:2	2001::200:ff:fe00:5	ISAKMP	IKE_AUTH MID=03 Responder Response
77	00:00:02.001568	2001::200:ff:fe00:5	2003::200:ff:fe00:2	ESP	ESP (SPI=0x0f2895d3)
79	00:00:02.048595	2003::200:ff:fe00:2	2001::200:ff:fe00:5	ESP	ESP (SPI=0x49b29775)

(a) AP's wireless interface packet capture

#	Time	Source	Destination	Proto	Info
5	00:00:01.200446	2002::200:ff:fe00:1	2002::200:ff:fe00:2	RADIUS	Access-Request id=0
6	00:00:01.205510	2002::200:ff:fe00:2	2002::200:ff:fe00:1	RADIUS	Access-Challenge id=0
7	00:00:01.206184	2002::200:ff:fe00:1	2002::200:ff:fe00:2	RADIUS	Access-Request id=1
8	00:00:01.210708	2002::200:ff:fe00:2	2002::200:ff:fe00:1	RADIUS	Access-Challenge id=1
9	00:00:01.502229	2002::200:ff:fe00:2	2002::200:ff:fe00:1	RADIUS	Access-Accept id=2
10	00:00:01.508634	2001::200:ff:fe00:5	2003::200:ff:fe00:2	ISAKMP	IKE_AUTH MID=03 Initiator Request
11	00:00:01.513231	2003::200:ff:fe00:2	2001::200:ff:fe00:5	ISAKMP	IKE_AUTH MID=03 Responder Response
12	00:00:02.001568	2001::200:ff:fe00:5	2003::200:ff:fe00:2	ESP	ESP (SPI=0x0f2895d3)
13	00:00:02.048595	2003::200:ff:fe00:2	2001::200:ff:fe00:5	ESP	ESP (SPI=0x49b29775)

(b) AP's wired interface packet capture

Fig. 7 Packet result of AP.

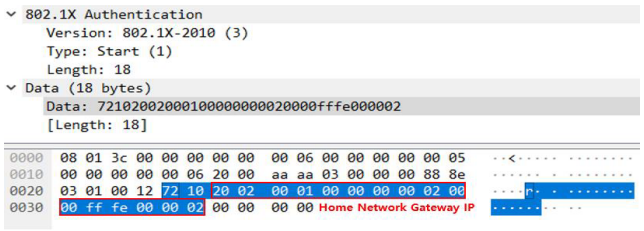
shown in Fig. 8(c). It carries the EAP-Success message and the MSK. The MSK is conveyed by the MS-MPPE-Recv-Key attribute.

IKE_AUTH sub-phases (3-d) and (3-e), consisting of the IEEE 802.11 4-way handshaking and the IP configuration, are omitted from this simulation. We assign 2001:1::200:ff:fe00:05 to the interface of the MN. Then the MN completes the IKE_AUTH phase. The MN and the home network gateway directly exchange the last IKE_AUTH messages, (Packet#50 and Packet#52 in Fig. 7(a) and Packet#10 and Packet#11 in Fig. 7(b)).

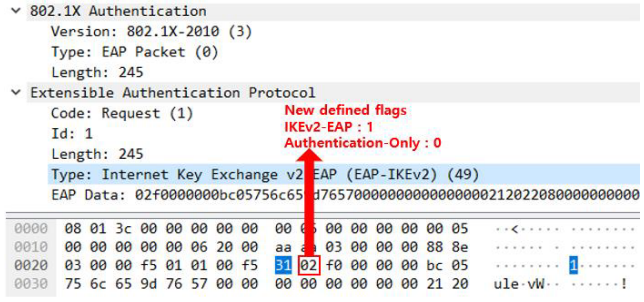
The ESP tunnel established in the IKE_AUTH subphase (f) is used to protect user data packets. Packet#77 and Packet#79 in Fig. 7(a) and Packet#12 and Packet#13 in Fig. 7(b) show the data packets exchanged between the MN and the CN.

8. Conclusion and Future Works

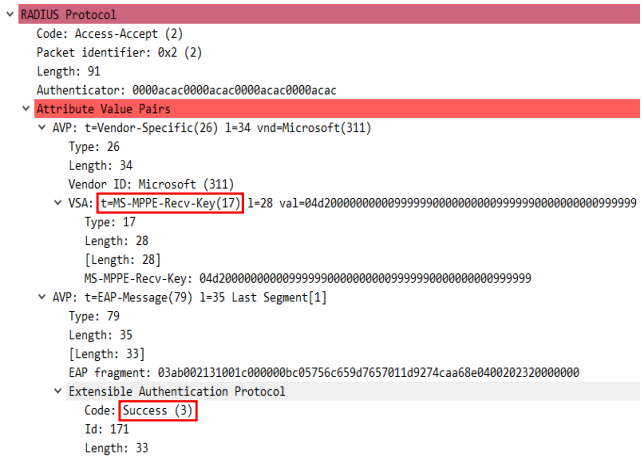
We proposed a hybrid authentication mechanism that simultaneously executes access network and home network authentication. The proposed scheme reduces the number of exchanged messages and the time taken by authentication. We demonstrated the proposed mechanism through the



(a) EAPOL-Start Message (Packet#28 in Figure 8(a))



(b) Newly defined flags in the EAP-IKEv2 header (Packet#30 in Figure 8(a))



(c) RADIUS:Access-Accept with the MSK (Packet#9 in Figure 8(b))

Fig. 8 Contents of captured packet.

simulation.

Mobility management is generally coupled with an authentication mechanism. In the future, we will make efforts to integrate the proposed mechanism with a current mobility scheme such as access network mobility FT intra-ESS mobility and mobile IKEv2 (MOBIKE) [27].

Acknowledgments

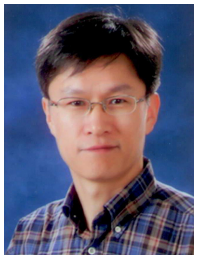
This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ICT Creative Consilience program (IITP-2021-0-01819) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

References

[1] IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area

networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-2016, 2016.
[2] IEEE Standard for Local and metropolitan area networks–Port-Based Network Access Control, in IEEE Std 802.1X-2020, 2020.
[3] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible authentication protocol (EAP)," IETF, RFC 3748, June 2004.
[4] B. Aboba and P. Calhoun, "RADIUS (remote authentication dial in user service) support for extensible authentication protocol (EAP)," IETF, RFC 3579, Sept. 2003.
[5] Microsoft, "[MS-PEAP]: Protected Extensible Authentication Protocol (PEAP)," April 2021.
[6] E. Rescorla, "The transport layer security (TLS) protocol version 1.3," IETF, RFC 8446, Aug. 2018.
[7] C. Kaufman, P. Hoffman, and P. Eronen, "Internet key exchange protocol version 2 (IKEv2)," IETF, RFC 7296, Oct. 2014.
[8] S. Frankel and S. Krishnan, "IP security (IPsec) and Internet key exchange (IKE) document roadmap," IETF, RFC 6071, Feb. 2011.
[9] K.-W. Kim, Y.-H. Han, and S.-G. Min, "An authentication and key management mechanism for resource constrained devices in IEEE 802.11-based IoT access networks," Sensors, vol.17, no.10, 2170, 2017.
[10] H. Tschofenig, D. Kroeselberg, A. Pashalidis, Y. Ohba, and F. Bersani, "The extensible authentication protocol-Internet key exchange protocol version 2 (EAP-IKEv2) method," IETF, RFC 5106, Feb. 2008.
[11] M. Al Khairy, "How 5G low latency improves your mobile experiences," https://www.qualcomm.com/news/onq/2019/05/13/how-5g-low-latency-improves-your-mobile-experiences, Qualcomm, May 2019.
[12] AVSystem, "How to manage resource-constrained IoT devices?," https://www.avsystem.com/blog/what-is-resource-constrained-device, Nov. 2020.
[13] M. Lavanya and V. Natarajan, "Certificate-free collaborative key agreement based on IKEv2 for IoT," 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), July 2017.
[14] S. Raza and R.M. Magnússon, "TinyIKE: Lightweight IKEv2 for Internet of things," IEEE Internet Things J., vol.6, no.1, pp.856–866, Feb. 2019.
[15] T.N. Hidayat and I. Riadi, "Optimation wireless security IEEE 802.1X using the extensible authentication protocol-protected extensible authentication protocol (EAP-PEAP)," Int. J. Comput. Appl., vol.174, no.11, pp.25–30, Jan. 2021.
[16] S. Kent and K. Seo, "Security architecture for the Internet protocol," IETF, RFC 4301, Dec. 2005.
[17] S. Kent, "IP authentication header," IETF, RFC 4302, Dec. 2005.
[18] S. Kent, "IP encapsulating security payload (ESP)" IETF, RFC 4303, Dec. 2005.
[19] D. Simon, B. Aboba, and R. Hurst, "The EAP-TLS authentication protocol," IETF, RFC 5216, March 2008.
[20] G. Zorn, "Microsoft vendor-specific RADIUS attributes," IETF, RFC 2548, March 1999.
[21] W. Townsley, A. Valencia, and A. Rubens, "Layer two tunneling protocol "L2TP"," IETF, RFC 2661, Aug. 1999.
[22] https://mgp25.com/research/infosec/Insecure-PEAP-Networks/
[23] https://m.blog.naver.com/PostView.nhn?blogId=eqelizer&logNo=20156517118&proxyReferer=https:%2F%2Fwww.google.co.kr%2F
[24] L. Song, Z. Xu, Z. Tian, J. Chen, and R. Zhi, "Research on 4G and 5G authentication signaling," J. Phys.: Conf. Ser., vol.1213, 042048, 2019.
[25] https://www.nsnam.org/releases/ns-3-32/
[26] https://www.wireshark.org/
[27] P. Eronen, ed., "IKEv2 mobility and multihoming protocol (MOBIKE)," IETF RFC 4555, June 2006.

MyeongJi Ko received the B.S. degrees in Computer Science and Engineering from Hankyong National University, Korea in 2018. She is currently working toward the Ph.D. degree in Computer Science and Engineering at Korea University, Seoul, Korea. Her interests in research include Future Internet, Vehicle Ad Hoc Networks, mobility protocol design, and performance analysis.



Hyogon Kim received the B.S. and M.S. degrees in computer engineering from Seoul National University, Seoul, Korea, in 1987 and 1989, respectively. He received the Ph.D. degree in computer and information science at University of Pennsylvania in 1995. From 1996 to 1999, he was a Research Scientist at Bell Communications Research (Bellcore). He is now a professor at Korea University. His research interests include wireless communication, vehicular networking, Internet of Things (IoT), and mobile computing.

Sung-Gi Min received the B.S. degree in Computer Science from Korea University, Seoul, Korea, in 1988. He received his M.S. and Ph.D. degrees in Computer Science from University of London in 1989 and 1993, respectively. From 1 January 1994 to 28 February 2000, he worked in LG Information and Communication Research Center, and from 2 March 2000 to 28 February 2001, he was a Professor in the Department of Computer Engineering at Dongeui University, Busan, Korea. Since 2 March 2001, he has been a Professor in the Department of Computer Science and Engineering at Korea University, Seoul, Korea. His research is focused on wired/wireless communication networks, and he is interested in mobility protocols, network architectures, QoS, and mobility management in future networks.