3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement based on EAP-AKA

Hyeran Mun, Kyusuk Han and Kwangjo Kim
Korea Advanced Institute of Science and Technology (KAIST)
119, Munjiro, Yuseong-gu, Daejeon, 305-732, South Korea
Email:{smartran, hankyusuk, kimkj}@kaist.ac.kr

***Abstract*—The 3rd Generation Partnership Project(3GPP) standard is developing System Architecture Evolution(SAE)/Long Term Evolution(LTE) architecture for the next generation mobile communication system. The SAE/LTE architecture provides secure service and 3G-WLAN interworking [9]. To provide secure 3G-WLAN interworking in the SAE/LTE architecture, Extensible Authentication Protocol-Authentication and Key Agreement(EAP-AKA) is used. However, EAP-AKA has several vulnerabilities such as disclosure of user identity, man-in-the-middle attack, Sequence Number(SQN) synchronization, and additional bandwidth consumption. Therefore, this paper analyzes threats and attacks in 3G-WLAN interworking and proposes a new authentication and key agreement protocol based on EAP-AKA. The proposed protocol combines Elliptic Curve Diffie-Hellman(ECDH) with symmetric key cryptosystem to overcome these vulnerabilities. Moreover, our protocol provides Perfect Forward Secrecy(PFS) to guarantee stronger security, mutual authentication, and resistance to replay attack. Compared with previous protocols which use public key cryptosystem with certificates, our protocol can reduce computational overhead.**

I. Introduction

The next generation mobile communication system is being developed for secure and fast communication. The SAE/LTE architecture [11], [12] that is being developed by 3GPP provides more secure communication than Universal Mobile Telecommunication System(UMTS) which is described in [10]. Fig. 1 shows the overall of the SAE/LTE architecture [8].

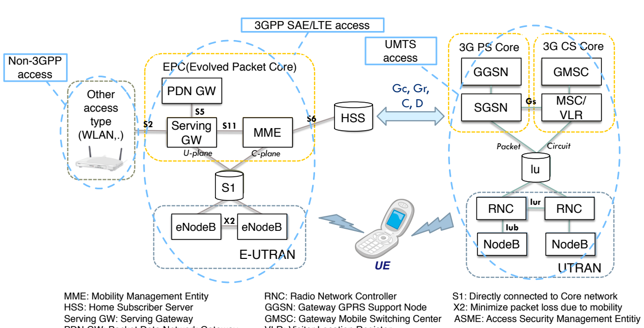


Fig. 1. Overall of SAE/LTE architecture

To provide mutual authentication between User Equipment(UE) and Mobility Management Entity(MME) through E-UTRAN, the SAE/LTE architecture reuses UMTS-AKA [10]. This authentication and key agreement protocol is called Evolved Packet System-Authentication and Key Agreement(EPS-AKA) which generates intermediate key K_{ASME}. Refer to Fig. 2 the K_{ASME} can generate 5 keys for protecting traffic between the UE and the MME, between the UE and the eNodeB, and between the UE and the Serving GW [11].

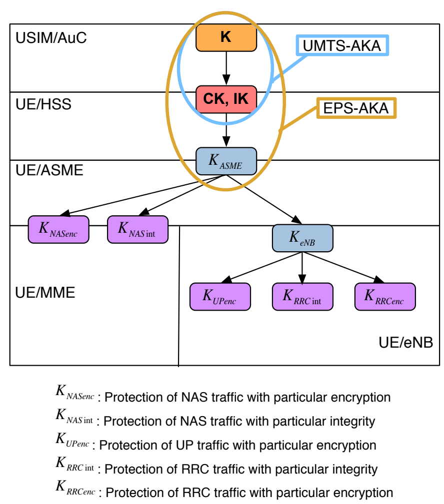


Fig. 2. Key hierarchy in E-UTRAN

Moreover, the SAE/LTE architecture provides 3G-WLAN interworking. 3G networks provide efficient charging management, nearly universal roaming, completed subscriber management, mobility, and wide service area. WLAN provides high bandwidth and data rate, compatibility of the Internet. However, the WLAN provides narrower service area, lower mobility and roaming than 3G networks. Therefore, many researchers have been studying 3G-WLAN interworking because 3G-WLAN interworking has both 3G and WLAN advantages. In 3G-WLAN interworking, both networks require authentication for secure communication.

The SAE/LTE architecture reuses EAP-AKA [4], [14] to

1-4244-2589-1/09/ $20.00 2009 IEEE

provide secure 3G-WLAN interworking. When a subscriber attempts to access WLAN, he sends International Mobile Subscriber Identity(IMSI) through Network Access Identifier(NAI) to the Access Point(AP). EAP-AKA is based on UMTS-AKA. For this reason, EAP-AKA can have not only vulnerabilities of UMTS-AKA but also vulnerabilities in 3G-WLAN interworking.

This paper analyzes threats and attacks in 3G-WLAN interworking and proposes a new authentication and key agreement protocol based on EAP-AKA. Our protocol overcomes several vulnerabilities of EAP-AKA such as violated user's privacy owing to disclosure of IMSI, man-in-the middle attack, SQN synchronization, and additional bandwidth consumption. Furthermore, our protocol provides Perfect Forward Secrecy(PFS) to guarantee stronger security, mutual authentication between the UE and the AAA server and between the UE and the HSS, and resistance to replay attack. Compared with previous protocols which use public key cryptosystems with certificates, our protocol can reduce computational overhead.

The rest of the paper is organized as follows: Section 2 presents brief 3G-Non 3GPP interworking architecture. Section 3 analyze threats and attacks in 3G-WLAN interworking. Section 4 explains overview of EAP-AKA and its vulnerabilities. In Section 5, we propose a new authentication and key agreement protocol based on EAP-AKA. In Section 6, we present analysis of our protocol and comparison of our protocol with previous protocols. Finally, Section 7 offers our conclusion.

II. Architecture of 3G-Non 3GPP Interwoking

Fig. 3 shows how the SAE/LTE architecture accesses Non-3GPP. Refer to Figure3 Non-3GPP consists of trusted Non-3GPP such as WiMax and untrusted Non-3GPP such as WLAN.

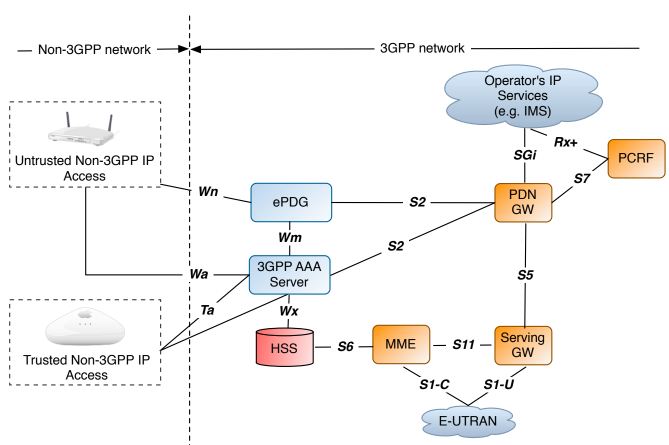


Fig. 3. Architecture of 3G-Non 3GPP interworking

The Authentication, Authorization and Accounting(AAA) server performs mutual authentication between 3G and Non-3GPP as well as accesses Home Subscriber Server(HSS) through *Wx* interface to get subscriber's information such as IMSI and Authentication Vector(AV). Therefore, the AAA server performs important roles during 3G-Non 3GPP interworking. *Ta* interface which was connected with trusted Non-3GPP transmits authentication, authorization, and accounting information to the AAA server. Trusted Non-3GPP transmits subscriber's information to PDN GW through *S2* interface.

In order to access untrusted Non-3GPP, evolved Packet Data Gateway(ePDU) is added in 3GPP network. All traffics which are generated by untrusted Non-3GPP are concentrated on the ePDU. Therefore, the ePDU establishes secure tunnel using IPsec and then securely sends subscriber information. Moreover, *Wm* interface transmits subscriber-related information from AAA server to ePDU [8], [13].

III. Threats and Attacks in 3G-WLAN Interworking

A. Threats

To find threats in 3G-WLAN interworking, identification of trust relationship among participants is important. Fig. 4 shows a simplified trust relationship among three important participants in 3G-WLAN interworking. Details of the trust relationship among the participants are described in [14]. The threats related with each participant are as follows:

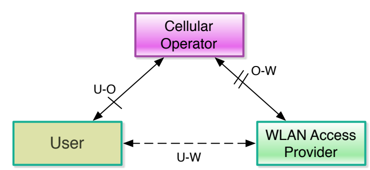


Fig. 4. Trust relationship

1) Cellular Operator:

- An attacker bypasses the access control and authorization mechanisms to get the WLAN service for free.
- An attacker impersonates a legitimate WLAN user. Therefore, the attacker accesses WLAN service for free and then the legitimate user gets charge for the attacker's usage of the service.
- An attacker interferes with the charging mechanism for the WLAN service. As a result, legitimate user's bill is incorrect.
- An attacker may be a legitimate user and then interfere with the charging mechanism to reduce his own bill. In another case, the attacker may be a prepaid user. Therefore, the attacker interferes with the charging mechanism to avoid disconnection despite the expiration of his prepaid account.

2) User:

- When a user accesses WLAN service, an attacker gets information which is either sent or received by the user. This information contains the user's information such as personals and credentials. As a result, the attacker can identify the user and modify the user's information.

- In order to derive a user's personal information, an attacker analyzes the information which is either sent or received by the user. As a result, the attacker can presume he is which service the user is using or where he is located at a given time.
- An attacker gets information about a user's permanent identity such as IMSI and then traces the user using IMSI.

3) WLAN Access Provider:

- The WLAN user cannot usage of WLAN service due to DoS attack, which is against the network or specific user.
- The WLAN user cannot access the legitimate WLAN service and get illegitimate WLAN service set up by an attacker.

B. Attacks

Attackers setting up a rouge AP may attempt to get free access service, modify a legitimate user's traffic, or perform DoS attacks. Furthermore, attacks can be performed remotely over the Internet. Therefore, the attacks are classified according to where the attack is performed/launched [14].

1) Victim's WLAN UE: Open platform terminals can be infected by viruses, Trojan horses, or other malicious software. The software can be operated without the knowledge of the user on his terminal and used for performing different types of attacks.

- If the user uses Universal Subscriber Identity Module(USIM), which stores important information and connects with the user's terminal, Trojan horses residing in the terminal can send fake requests to the USIM and then transmit challenge-response results to another terminal. The owner of the latter terminal could get access with the stolen important information.
- Trojan horses may reside all the usual activities. Therefore, attackers monitor the user's keyboard or sensitive data and then forward the information to another machine using residing Trojan horses.
- Malicious software can be used to perform Distributed DoS(DDoS) attack. In other words, several instantiations of which software synchronize and start a DoS attack simultaneously against the target.
- Malicious software tries to connect with different WLAN for annoying the user.

2) Attacker's WLAN UE and/or AP: An attacker can perform several types of attacks during his access to the terminal and the AP. For example, DoS attack and eavesdropping can occur because control signaling is not protected. This type of attack can cause different threats.

- An attacker can modify the user's traffic or divert the traffic to another network.
- An attacker can falsify a network or a commercial site to get access to credit card information.
- An attacker can perform man-in-the-middle attack and then get credentials of the legitimate user. After getting a legitimate user's information, the attacker can prevent access of the legitimate user.
- An attacker can use fake configuration or control message to redirect a user's traffic.
- In order to interfere or gain access, an attacker performs simply eavesdropping on the traffic around an AP.

3) WLAN Access Network Infrastructure:

- An attacker can perform attacks at WLAN access network infrastructure such as AP, LAN connecting APs, and Ethernet switches.
- If WLAN is partially a wired network, an attacker may hook up part of the network.
- An attacker can interfere with the charging functions, just to increase a user's bill.

4) Other Device on the Internet:

- An attacker can perform a flooding attack sending garbage packets, just to increase the user's bill.

Details of the threats and attacks in 3G-WLAN interworking are described in [14].

IV. Overview of EAP-AKA and its Vulnerabilities

When the UE attempts to access Non-3GPP such as WLAN, the UMTS-AKA protocol cannot be used. Therefore, EAP-AKA [4] is used to support 3G-WLAN interworking. EAP-AKA protocol is based on UMTS-AKA. We will describe EAP-AKA and its vulnerabilities in this section.

A. Generation of Temporary Identity

For hiding user's permanent identity, the AAA server can generate temporary identity such as pseudonyms or re-authentication identity by using Advanced Encryption Standard(AES) in Electronic Code Book(ECB) with 128 bit key sizes. The temporary identity has the same form with IMSI. Fig. 5 shows generation of temporary identity. Generated temporary identity will use next authentication procedure instead of IMSI [14].

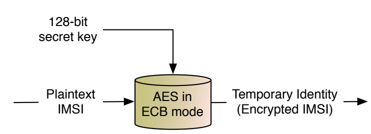


Fig. 5. Generation of temporary identity

B. Procedure of EAP-AKA

EAP-AKA provides mutual authentication between the UE and the AAA server. That is, EAP-AKA performs a procedure of authentication and key agreement between 3G and Non-3GPP. Fig. 6 shows procedure of EAP-AKA.

From Step 5 to 6, the AAA server requests again the user identity because immediate nodes can modify user identity such as IMSI included in EAP Response/Identity message. Therefore, if the UE receives EAP Request/AKA-Identiy message, the UE should send EAP Response/AKA-Identity message which must contain the same user identity included in EAP Response/Identity message to the AAA

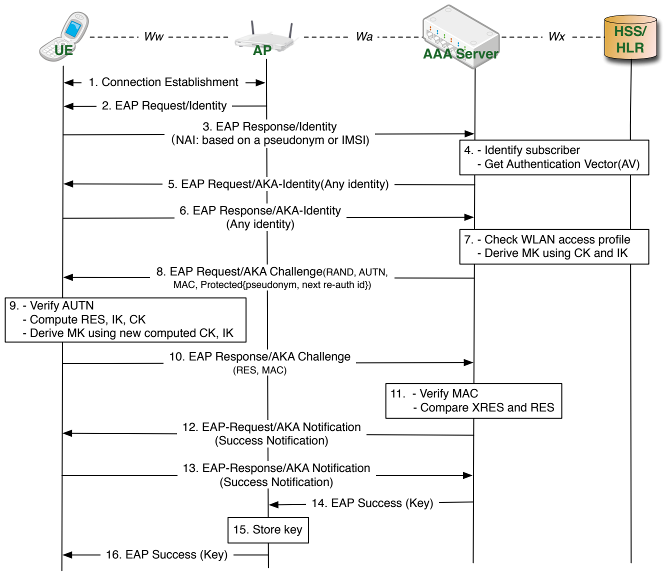


Fig. 6. Procedure of EAP-AKA

server. The AAA server will use user identity received from EAP Response/AKA-Identity message in the rest of the authentication and key agreement procedure. In Step 7, the AAA server checks the WLAN access profile and verifies that the subscriber is authorized to use the WLAN service.

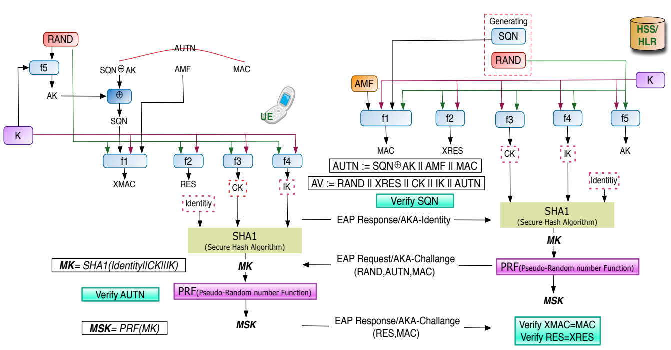


Fig. 7. Generation of MK and MSK

Fig. 7 indicates the procedure of generation of MK and MSK. The AAA server retrieves AV through *Wx* interface. The UE receives EAP Request/AKA-Challenge message with three parameters (RAND, AUTN, and MAC). The UE verifies AUTN and SQN. If AUTN is incorrect, the UE terminates authentication. If SQN is in incorrect range, the UE occurs SQN synchronization procedure. Meanwhile, the AAA server should request again the AV to the HSS. If AUTN is in the correct range, the UE computes RES, Integrity Key(IK) and Cipher Key(CK) using symmetric key K shared between the UE and the HSS. Moreover, the UE computes new MAC value and then sends EAP Response/AKA-Challenge message containing calculated RES and new MAC value to the AAA server. Both CK and IK are used to derive the EAP Master Key(MK), from which EAP Master Session Key(MSK) is derived. Generated MSK is transmitted to the AP and used to protect further communication.

C. Vulnerabilities of EAP-AKA

EAP-AKA is based on UMTS-AKA. For this reason, EAP-AKA can have not only vulnerabilities of UMTS-AKA but also vulnerabilities of 3G-WLAN interworking. Vulnerabilities of EAP-AKA are as follows:

- **Disclosure of IMSI**: Although EAP-AKA uses a temporary identity such as pseudonyms or re-authentication identity, the UE must send a permanent identity such as IMSI to the AAA server on first connection. If an attacker gets IMSI, he can misuse IMSI and can trace subscriber.
- **Man-in-the-middle attack**: EAP-AKA has several factors which can cause man-in-the-middle attacks.
  - As mentioned earlier, IMSI is plaintext on the first connection between the UE and the AAA server. Therefore, an attacker may be waiting for transmission of IMSI and can modify IMSI.
  - Although the UE and the AAA server can be successfully authenticated each other, the AAA server sends EAP Success message with MSK to the AP and the UE without authentication. As a result, an attacker who impersonates the AP can receive EAP Success message with MSK, modify the received message and then send the modified message to the UE or another UE.
- **Perfect Forward Secrecy**: EAP-AKA uses symmetric key K shared between the UE and the HSS to perform authentication and key agreement. The CK, IK, MK, and MSK were generated using K. For this reasion, disclosure of K is equal to the disclosure of all procedure of EAP-AKA. That is, EAP-AKA does not provide Perfect Forward Secrecy(PFS).
- **Bandwidth consumption**: The AAA server requests again the user identity before the challenge/response procedure because immediate nodes can modify user identity. For this reason, EAP-AKA has additional bandwidth consumption.
- **SQN synchronization**: EAP-AKA also uses AV which was used in UMTS-AKA. If received SQN is in the incorrect range, the UE should perform SQN synchronization procedure. Meanwhile, the AAA server should request again AV to the HSS. As a result, bandwidth consumption between the AAA server and the HSS can occur.

V. Proposed Protocol

In this section, we propose a new authentication and key agreement protocol based on EAP-AKA.

A. Notations

Table I shows notations.

TABLE I
NOTATIONS OF PROPOSED PROTOCOL

Notation	Description
U, A, H	Denote the UE, the AAA server, and the HSS, respectively
$_cID_{UE}$	Current temporary ID of UE
ID_x	ID of entity x
T_x	Timestamp generated by entity x
g_K^i	Key generation function using the key K
f_K^1	MAC generation function using the key K
f_K^2	$_cID_{UE}$ generation function using the key K
$RAND_x$	Random number by entity x
K_{xy}	Symmetric key shared between entity x and y
TK	Temporary Key

B. Assumption

In our proposed protocol, we assume the following:

- A secure channel is established between the AAA server and the HSS.
- The UE can identify the ID of AAA server and AP in which it is able to access now.

C. The Workflow of Our Protocol

Our protocol consists of four procedures which are shown in Fig. 8.

1) Initialization:

- **Step 1.** A connection is established between the UE and the AP.
- **Step 2.** To get user identity, the AP sends EAP Request/Identity message to the UE.

2) Registration and Generation of TK:

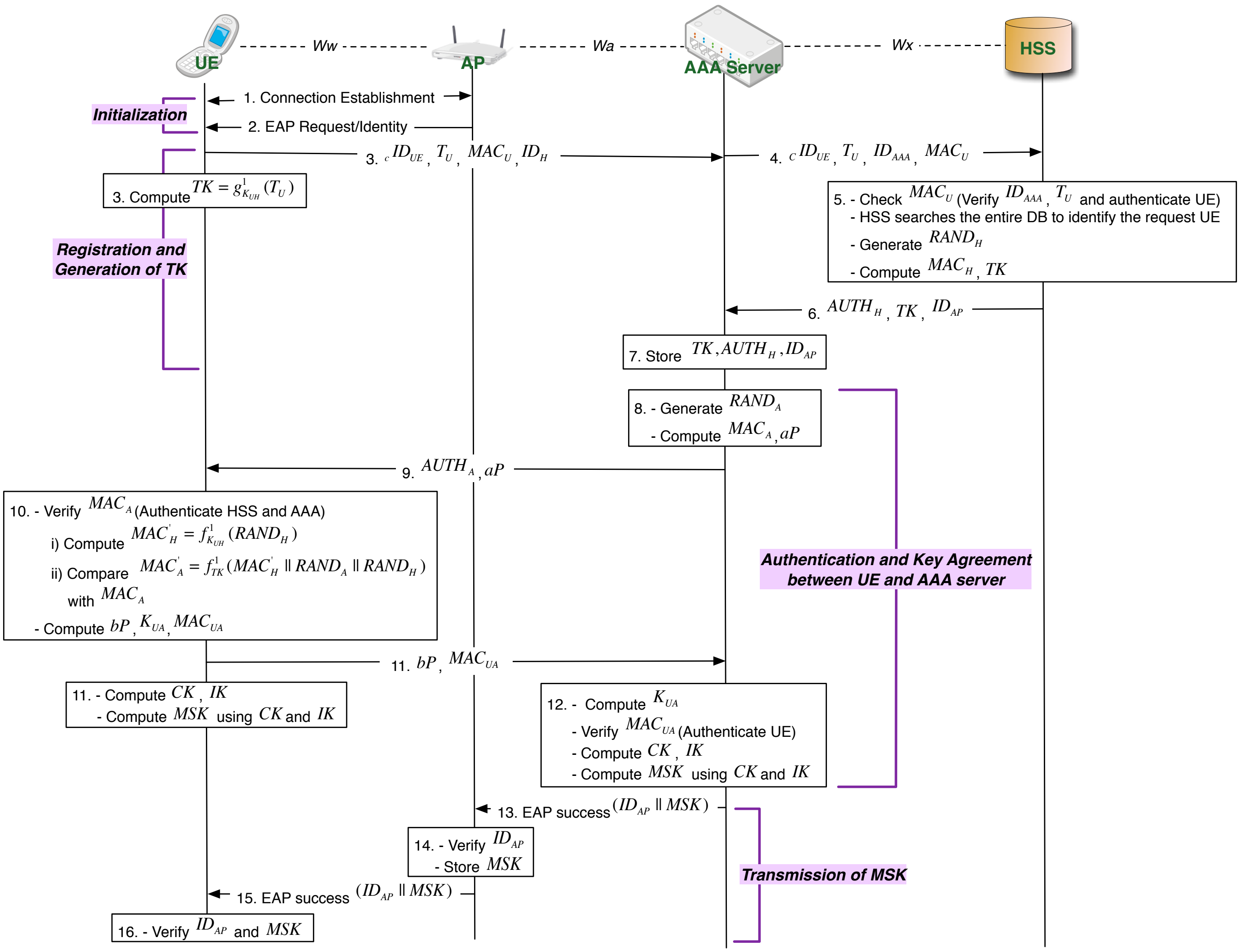
- **Step 3.** The UE generates T_U and computes MAC_U=$f^1_{K_{UH}}$ $(T_U||ID_{AAA}||ID_{AP})$ using the K_{UH}. In addition, the UE computes $_cID_{UE}$ to prevent the disclosure of IMSI. $_cID_{UE}$ can be computed as $f^2_{K_{UH}}(IMSI)$. Therefore, the UE sends $_cID_{UE}$, T_U, MAC_U, and ID_H to the AP. Meanwhile, the UE computes TK=$g^1_{K_{UH}}(T_U)$.
- **Step 4.** The AAA server transmits $_cID_{UE}$, T_U, MAC_U, and ID_{AAA} to the HSS using ID_H received from the UE in Step 3.
- **Step 5.** The HSS checks MAC_U. As a result, the UE can verify ID_{AAA} and T_U and authenticate the UE. The procedure of checking MAC_U is as follows:
  a) The HSS retrieves ID_{AP}, ID_{AAA}, and T_U from MAC_U.
  b) The HSS verifies whether or not ID_{AAA} retrieved from MAC_U equals ID_{AAA} which sent Step 4 message($_cID_{UE}$, T_U, MAC_U, ID_{AAA}) to the HSS.
  c) The HSS verifies whether T_U is in the correct range and then verifies whether T_U retrieved from MAC_U equals received T_U. If the result is correct, the HSS can authenticate the UE and prevent replay attack.

  After checking MAC_U, the HSS derives IMSI from $_cID_{UE}$ using K_{UH}. The HSS searches the entire DB which stored user identity such as IMSI to identify the requested UE. The HSS computes TK=$g^1_{K_{UH}}(T_U)$ and generate $RAND_H$. Using $RAND_H$ the HSS computes MAC_H=$f^1_{K_{UH}}(RAND_H)$.
- **Step 6.** The HSS sends $AUTH_H$, TK, and ID_{AP} to the AAA server. ID_{AP} was obtain from MAC_U. We already assumed that a secure channel was established between the HSS and the AAA server. As a result, TK is secure against attackers although TK is plaintext on the air.
- **Step 7.** The AAA server stores TK, $AUTH_H$, and ID_{AP}.

3) Authentication and Key Agreement:

- **Step 8.** The AAA server generates $RAND_A$ and computes MAC_A. Afterward, the AAA server selects random number a and computes aP on E.
  - **Elliptic Curve Diffie-Hellman(ECDH)**: User A and B publicly agree on an elliptic curve E over a large finite field F and a point P on that curve. The user A and B each selects random number a and b, respectively. Using elliptic curve point-addition, user A and B each publicly compute aP and bP on E. Finally, user A and B each compute abP using private and public values. As a result, solving ECDH is a computationally difficult problem [7].
- **Step 9.** The AAA server sends $AUTH_A$=$(MAC_A||RAND_A||RAND_H)$ and aP to the UE.
- **Step 10.** The UE verifies MAC_A. The procedure of verifying MAC_A is as follows:
  a) The UE computes MAC'_H=$f^1_{K_{UH}}(RNAD_H)$. The $RAND_H$ is derived from $AUTH_A$ in Step 9.
  b) The UE computes MAC'_A=$f^1_{TK}(MAC'_H||RAND_A||RAND_H)$. The $RAND_H$ and $RAND_A$ are derived from $AUTH_A$.
  c) The UE verifies whether MAC'_A equals MAC_A or not. If MAC'_A is not same MAC_A, the HSS or the AAA server is not valid. Therefore, the UE terminates the procedure.

  The UE can authenticate the HSS and the AAA server by verifying MAC_A. As a result, verifying MAC_A prevents replay attack and man-in-the-middle attack. The UE selects random number b and computes bP on E. Subsequently, using aP received from the AAA server in Step 9, the UE can compute symmetric key $K_{UA} = g^2_{TK}(abP)$. Finally, the UE computes $MAC_{UA} = f^1_{K_{UA}}(RAND_A||bP)$ using K_{UA} shared between the UE ad the AAA server.
- **Step 11.** The UE transmits bP and MAC_{UA} to the AAA server and concurrently computes CK and IK.



$$_cID_{UE} = f^2_{K_{UH}}(IMSI) \qquad MAC_U = f^1_{K_{UH}}(T_U \| ID_{AAA} \| ID_{AP}) \qquad TK = g^1_{K_{UH}}(T_U)$$

$$MAC_H = f^1_{K_{UH}}(RAND_H) \qquad AUTH_H = (MAC_H \| RAND_H) \qquad MAC_A = f^1_{TK}(MAC_H \| RAND_A \| RAND_H)$$

$$AUTH_A = (MAC_A \| RAND_A \| RAND_H) \qquad K_{UA} = g^2_{TK}(abP) \qquad MAC_{UA} = f^1_{K_{UA}}(RAND_A \| bP)$$

$$CK = g^3_{K_{UA}}(RAND_A) \qquad IK = g^4_{K_{UA}}(RAND_A)$$

Fig. 8. Proposed protocol

Afterward, the UE computes MSK using CK and IK as EAP-AKA.

- **Step 12.** Using bP received from the UE in Step 11, the AAA server can compute K_{UA}. Then the AAA server verifies MAC_{UA}. In other words, the AAA server verifies whether or not $RAND_A$ included in MAC_{UA} equals $RAND_A$ generated from the AAA server in Step 8. If two values are same, the AAA server can authenticate the UE. The AAA server computes CK and IK. Finally, the UE computes MSK using CK and IK as EAP-AKA.

4) Transmission of MSK:

- **Step 13.** The AAA server sends $ID_{AP}||MSK$ with EAP Success message to the AP. ID_{AP} was received from the HSS in Step 6.
- **Step 14.** The AP verifies whether received ID_{AP} equals AP's own ID or not. If the result is correct, the AP stores MSK. Otherwise the AP does not store MSK and then terminates the execution.
- **Step 15.** The AP sends $ID_{AP}||MSK$ with EAP Success message to the UE.
- **Step 16.** The UE verifies whether or not ID_{AP} received from the AP in Step 15 equals ID_{AP} used in Step 3

to compute MAC_U, and then verifies whether or not MSK received from the AP in Step 15 equals MSK generated in Step 11. If the result is correct, the procedure of authentication and key agreement is successful. Consequently, the UE can securely use WLAN service using MSK.

VI. Analysis and Comparison

In this section, we analyze our protocol and then compare our protocol with the previous protocols.

A. Security Analysis

Our protocol has several security properties as follows:

- **Protect user identity(IMSI)**: In our protocol, IMSI is not exposed by attackers. The UE generates the $_cID_{UE}$ using the K_{UH} and then sends $_cID_{UE}$ to the HSS. For this reason, the UE and the HSS can only retrieve user identity such as IMSI included in $_cID_{UE}$ using K_{UH}. Therefore, our protocol provides strong user identity protection.
- **Secure against man-in-the middle attack**:
  - *a)* The UE and the HSS can only retrieve IMSI from $_cID_{UE}$. Therefore, attackers cannot derive the IMSI and cannot modify IMSI.
  - *b)* The AAA server sends the EAP Success message with $ID_{AP}||MSK$ to the AP. The AP then verifies whether or not received ID_{AP} equals AP's own ID. If two values are not same, procedure of authentication and key agreement fails. Therefore, our protocol prevents man-in-the middle attack compared with EAP-AKA, which sends the EAP Success message with MSK to the AP and the UE without authentication.
  - *c)* The UE can certainly confirm that MAC_H is generated by the correct HSS by verifying MAC_A. As a result, our protocol can prevent man-in-the middle attack.
- **Provide perfect forward secrecy(PFS)**: To provide PFS between the UE and the AAA server, our protocol uses ECDH. While generating K_{UA}, our protocol uses aP and bP that are not related with K_{UH}. Therefore, if disclosure of K_{UH} occurs, attackers cannot guess K_{UA}. In other words, guessing K_{UA} is a computationally difficult problem.
- **Provide mutual authentication**
  - *a)* Between the UE and the AAA server: The UE can authenticate the AAA server by verifying MAC_A in Step 10. Similarly, the AAA server can authenticate the UE by verifying MAC_{UA} in Step 12.
  - *b)* Between the UE and the HSS: The UE can authenticate the HSS by verifying MAC_A in Step 10. Similarly, the HSS can authenticate the UE by verifying MAC_U in Step 5.
- **Secure against replay attack**: Before generating TK, the HSS must verify whether T_U is in the correct range or not. Moreover, our protocol verifies $RAND_A$ and $RAND_H$ included in MAC_A. Therefore, our protocol can prevent replay attack.

B. Performance Analysis

- **Reduce bandwidth consumption**: Our protocol uses $_cID_{UE}$ to prevent disclosure of user identity. As a result, disclosure of user identity does not occur by immediate nodes or attackers despite requesting user identity once. Thus, compared with EAP-AKA which requests again user identity in Step 5, our protocol can reduce bandwidth consumption.
- **Do not occur SQN synchronization**: Our protocol does not occur SQN synchronization as well as does not consume bandwidth between the AAA server and the HSS, because it does not use SQN mechanism and AV. As a result, our protocol can reduce bandwidth consumption.
- **Use Elliptic Curve Diffie-Hellman(ECDH)**: Generally, most of the previous protocols do not use any kind of public key cryptosystem because UEs have power limitation, low-level computational power, and less storage space. However, technology is significantly improving. For this reason, previous protocols consider use of public key cryptosystems with certificates [1], [2], [5], [6]. Therefore, our protocol combines ECDH with symmetric key cryptosystem to provide secure communication between 3G and Non-3GPP. ECDH provides the same security properties and uses fewer resources than other public key cryptosystems with certificates. Therefore, our protocol has less overhead than previous protocols which are based on public key cryptosystems with certificates. In our protocol, the UE and the AAA server only stores and manages a, b, aP, and bP.

C. Comparison

To authenticate WLAN, IEEE 802.1x provides authentication framework based on Extensible Authentication Protocol(EAP). The EAP supports several authentication protocols and each protocol has advantages and disadvantages, respectively. Table II shows comparison of our protocol with previous protocols [5]. Refer to Table II our protocol supports cellular-WLAN interworking and provides strong user identity protection. Moreover, our protocol has less overhead than other protocols(EAP-TTLS, PEAP, and EAP-UTLS) because of using a symmetric key cryptosystem and ECDH. Moreover, our protocol prevents man-in-the middle attack and replay attack. In addition, our protocol provides PFS and does not occur SQN synchronization which occurs in EAP-AKA. Therefore, our protocol provide more efficient and secure 3G-WLAN interworking than previous protocols.

VII. Conclusion

In this paper, we analyzed threats and attacks in 3G-WLAN interworking and proposed a new authentication and key agreement protocol based on EAP-AKA. The proposed protocol combines ECDH with symmetric key cryptosystem to

TABLE II
COMPARISON OF OUR PROTOCOL WITH PREVIOUS PROTOCOLS

	Our protocol	**EAP-TLS [2]**	**EAP-TTLS [6]**	**PEAP [1]**	**EAP-AKA [4]**	**EAP-SIM [3]**	**EAP-UTLS [5]**
Type of cryptosystem	Symmetric and ECDH	Public (Certificate)	Public (Certificate)	Public (Certificate)	Symmetric	Symmetric	Public (Certificate)
Subscriber management	Cellular network provider	WLAN provider	WLAN provider	WLAN provider	Cellular network provider	Cellular network provider	Cellular network provider
Protection of user identity (IMSI)	O	X	O	O	X	X	O
Cellular-WLAN interworking	O	X	X	X	O	O	O
Secure against man-in-the middle attack	O	O	X	X	X	X	O
Secure against replay attack	O	O	O	O	O	O	X
Provide PFS	O	X	X	X	X	X	X
Need for SQN synchronization	X	-	-	-	O	-	-

overcome several vulnerabilities of EAP-AKA such as disclosure of user identity, man-in-the-middle attack, SQN synchronization, and additional bandwidth consumption. Moreover, our protocol provides PFS to guarantee stronger security, mutual authentication between the UE and the AAA server and between the UE and the HSS, and resistance to replay attack. Compared with previous protocols which use public key cryptosystem with certificates, our protocol can reduce computational overhead.

REFERENCES

[1] A. Palekar, D. Simon, S. Josefsson, H. Zhou, G. Zorn, Protected EAP Protocol (PEAP) Version 2, draft-josefsson-pppext-eap-tls-10, *IETF, October 2004*

[2] B. Aboba, S.Simon, PPP EAP TLS Authentication Protocol, RFC 2716, *IETE, October 1999*

[3] H. Haverinen, J.Salowey, EAP SIM Authentication, draft-arkko-pppext-eap-sim-12, *IETE, October 2003*

[4] J. Arkko, H. Haverinen, Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), *IETF RFC 4187, January 2006*

[5] L. Han, A Threat Analysis of the Extensible Authentication Protocol, *Honors Project Report, April 2006*

[6] P. Funk, S.Blake-Wilson, EAP Tunneled TLS Authentication Protocol, draft-ietf-pppext-eap-ttls-05, *IETF, July 2004*

[7] PlanetMath-Elliptic Curve Diffie-Hellman key exchange, *http://planetmath.org/encyclopedia/DiffieHellmanKeyExchange.html*

[8] P.Lescuyer, T.Lucidarme,“ Evolved Packet System (EPS): The LTE and SAE Evolution of 3G “ , *J.Wiley & Sons, 2008*

[9] Third Generation Partnership Project (3GPP) specifications and reports, TR xx.xxx(Technical Report) or TS xx.xxx(Technical Spec.), *http://www.3gpp.org/ftp/Specs/html*

[10] Third Generation Partnership Project (3GPP), 3GPP TS 33.102 v8.0.0 “ 3G Security: Security Architecture (Release 8)” , *June 2008*

[11] Third Generation Partnership Project (3GPP), 3GPP TS 33.401 v8.1.1 “ 3G System Architecture Evolution (SAE): Security architecture (Release 8)” , *October 2008*

[12] Third Generation Partnership Project (3GPP), 3GPP TS 33.821 v1.0.0 “ Rationale and track of security decisions in Long Term Evolved (LTE) RAN/3GPP System Architecture Evolution (SAE) (Release 8)” , *December 2007*

[13] Third Generation Partnership Project (3GPP), 3GPP TS 33.402 v8.3.0 “ Architecture Enhancements for non-3GPP accesses (Release 8)” , *September 2008*

[14] Third Generation Partnership Project (3GPP), 3GPP TS 23.234 v8.1.0 “ 3G security: Wireless Local Area Network (WLAN) Interworking Security (Release 8)” , *March 2008*

[15] Yuh-Min Tseng, USIM-based EAP-TLS authentication protocol for wireless local area networks, *Computer Standards & Interfaces, November 2007*