A Review of 3G-WLAN Interworking

B.Bindusha Reddy[#], Dr Syed Umar [*], M.Satya Anusha[&]

*Assistant. Professor, Department of ECM, KL University, A.P., INDIA.
[#, &]Student, Department of ECM, KL University, A.P, INDIA.

***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 EAPAKA. 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.**

***Keywords*—Routing protocols, 3 G. WLAN, EAP**

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]. 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 KASME. Refer to Fig. 2 the KASME 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]. Moreover, the SAE/LTE architecture provides 3G-WLAN interworking.

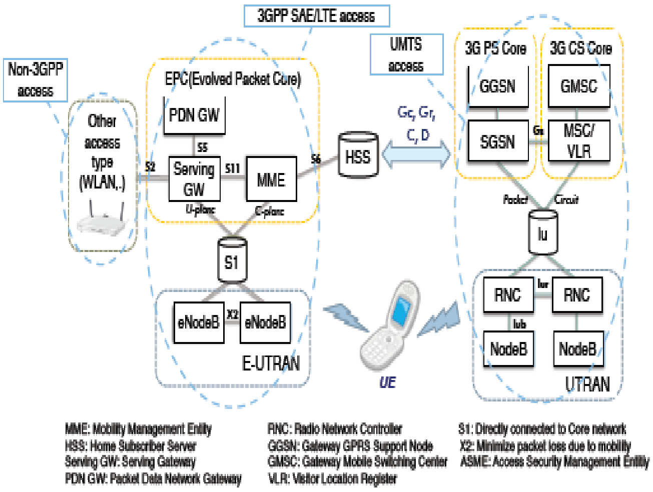
3GPP SAE/LTE access
Non-3GPP access
Other access type (WLAN,.)
EPC(Evolved Packet Core)
PDN GW
S5
S2
Serving GW
S11
MME
U-plane
C-plane
S6
HSS
UMTS access
Gc, Gr, C, D
3G PS Core
GGSN
SGSN
Gs
3G CS Core
GMSC
MSC/ VLR
Packet
Circuit
Iu
S1
eNodeB
X2
eNodeB
E-UTRAN
UE
RNC
Iur
RNC
Iub
NodeB
NodeB
UTRAN
MME: Mobility Management Entity
HSS: Home Subscriber Server
Serving GW: Serving Gateway
PDN GW: Packet Data Network Gateway
RNC: Radio Network Controller
GGSN: Gateway GPRS Support Node
GMSC: Gateway Mobile Switching Center
VLR: Visitor Location Register
S1: Directly connected to Core network
X2: Minimize packet loss due to mobility
ASME: Access Security Management Entity

Fig. 1. Overall of SAE/LTE architecture

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.

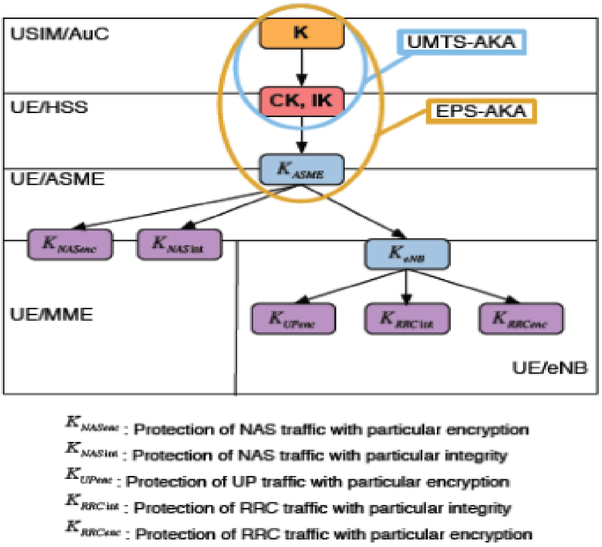
USIM/AuC
K
UMTS-AKA
UE/HSS
CK, IK
EPS-AKA
UE/ASME
K_{ASME}
K_{NASenc}
K_{NASint}
K_{eNB}
UE/MME
K_{UPenc}
K_{RRCint}
K_{RRCenc}
UE/eNB
K_{NASenc} : Protection of NAS traffic with particular encryption
K_{NASint} : Protection of NAS traffic with particular integrity
K_{UPenc} : Protection of UP traffic with particular encryption
K_{RRCint} : Protection of RRC traffic with particular integrity
K_{RRCenc} : Protection of RRC traffic with particular encryption

Fig. 2. Key hierarchy in E-UTRAN

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 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 3GWLAN 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 Interworking

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.

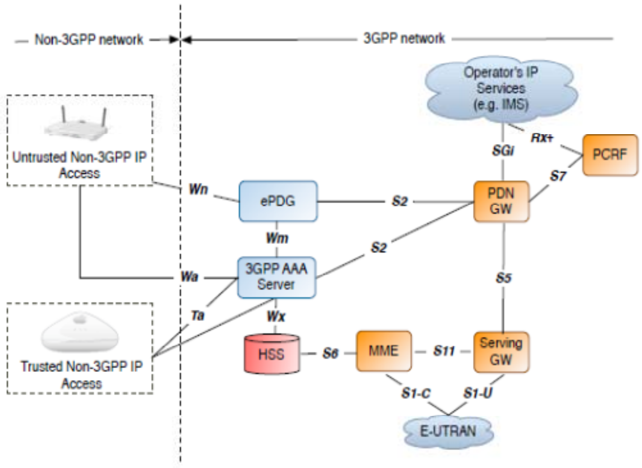

Fig. 3. Architecture of 3G-Non 3GPP interworking

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.

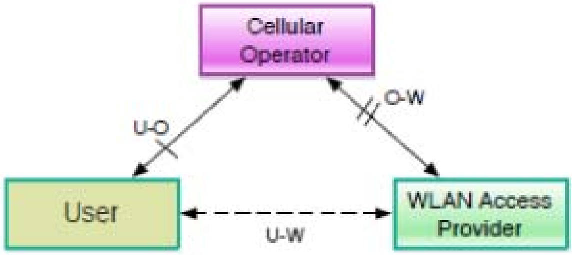

Fig. 4. Trust relationship

Details of the trust relationship among the participants are described in [14].

The threats related with each participant are as follows:

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, EAPAKA [4] is used to support 3G-WLAN interworking. EAPAKA 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 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].

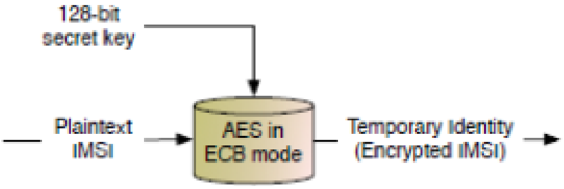

Fig. 5. Generation of temporary identity

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 Identity 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 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

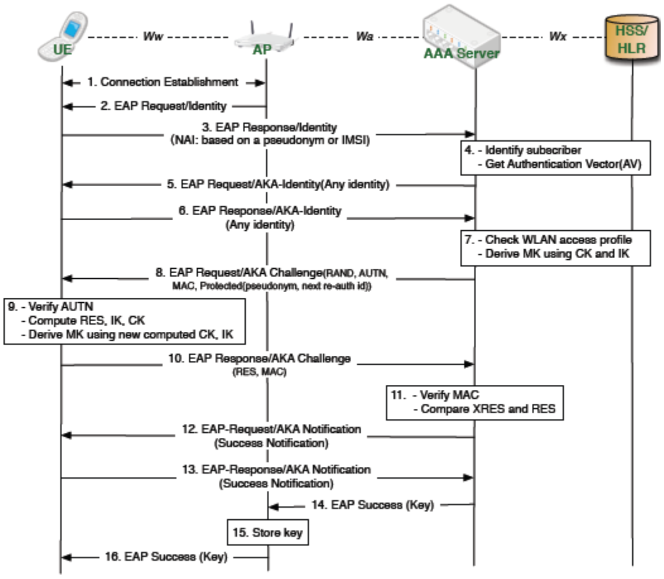
UE
Ww
AP
Wa
AAA Server
Wx
HSS/ HLR
1. Connection Establishment
2. EAP Request/Identity
3. EAP Response/Identity (NAI: based on a pseudonym or IMSI)
4. - Identify subscriber - Get Authentication Vector(AV)
5. EAP Request/AKA-Identity(Any identity)
6. EAP Response/AKA-Identity (Any identity)
7. - Check WLAN access profile - Derive MK using CK and IK
8. EAP Request/AKA Challenge(RAND, AUTN, MAC, Protected(pseudonym, next re-auth id))
9. - Verify AUTN - Compute RES, IK, CK - Derive MK using new computed CK, IK
10. EAP Response/AKA Challenge (RES, MAC)
11. - Verify MAC - Compare XRES and RES
12. EAP-Request/AKA Notification (Success Notification)
13. EAP-Response/AKA Notification (Success Notification)
14. EAP Success (Key)
15. Store key
16. EAP Success (Key)

Fig. 6. Procedure of EAP-AKA

AAA server checks the WLAN access profile and verifies that the subscriber is authorized to use the WLAN service.

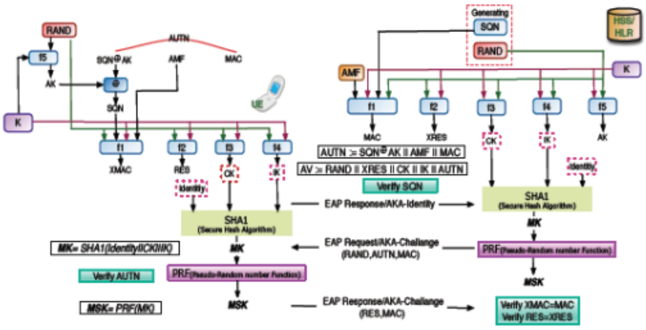
RAND
f5
AK
AUTN
SQN⊕AK
AMF
MAC
⊕
SQN
K
UE
f1
f2
f3
f4
XMAC
RES
CK
IK
Identity
SHA1 (Secure Hash Algorithm)
MK= SHA1(Identity||CK||IK)
MK
Verify AUTN
PRF(Pseudo-Random number Function)
MSK= PRF(MK)
MSK
Generating
SQN
RAND
HSS/ HLR
AMF
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN := SQN⊕AK || AMF || MAC
AV := RAND || XRES || CK || IK || AUTN
Verify SQN
Identity
EAP Response/AKA-Identity
SHA1 (Secure Hash Algorithm)
MK
EAP Request/AKA-Challange (RAND,AUTN,MAC)
PRF(Pseudo-Random number Function)
MSK
EAP Response/AKA-Challange (RES,MAC)
Verify XMAC=MAC
Verify RES=XRES

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, EAPAKA 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 reason, 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^i_K	Key generation function using the key K
f^1_K	MAC generation function using the key K
f^2_K	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

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 TU and computes MACU=f1K UH (TUjjIDAAAjjIDAP) using the KUH. In addition, the UE computes cIDUE to prevent the disclosure of IMSI. CIDUE can be computed as f2K UH (IMSI). Therefore, the UE sends cIDUE, TU, MACU, and IDH to the AP. Meanwhile, the UE Computes TK=g1K UH (TU).

* Step 4. The AAA server transmits cIDUE, TU, MACU, and IDAAA to the HSS using IDH received from the UE in Step 3.

* Step 5. The HSS checks MACU. As a result, the UE can verify IDAAA and TU and authenticate the UE. The procedure of checking MACU is as follows:

a) The HSS retrieves IDAP, IDAAA, and TU from MACU.

b) The HSS verifies whether or not IDAAA retrieved from MACU equals IDAAA which sent Step 4 message (cIDUE, TU, MACU, IDAAA) to the HSS.

c) The HSS verifies whether TU is in the correct range and then verifies whether TU retrieved from MACU equals received TU. If the result is correct, the HSS can authenticate the UE and prevent replay attack. After checking MACU, the HSS derives IMSI from cIDUE using KUH. The HSS searches the entire DB which stored user identity such as IMSI to identify the requested UE. The HSS computes TK=g1K UH

(TU) and generate RANDH. Using RANDH the HSS computes MACH=f1K UH(RANDH).

* Step 6. The HSS sends AUTHH, TK, and IDAP to the AAA server. IDAP was obtain from MACU. 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, AUTHH, and IDAP.

3) Authentication and Key Agreement:

* Step 8. The AAA server generates RANDA and computes MACA. 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 AUTHA=(MAC AjjR AND AjjR AND H) and aP to the UE.

* Step 10. The UE verifies MACA. The procedure of verifying MACA is as follows:

a) The UE computes MAC 0 H=f1K UH (RNADH). The RANDH is derived from AUTHA in Step 9.

b) The UE computes MAC 0 A=f1 TK (MAC 0 HjjR AND AjjR AND H). The RANDH and RANDA are derived from AUTHA.

c) The UE verifies whether MAC 0 A equals MACA or not. If MAC 0 A is not same MACA, 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 MACA. As a result, verifying MACA 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 KUA = g2T K (abP). Finally, the UE computes MACUA = f1K UA (R AND Ajj bP) using KUA shared between the UE and the AAA server.

* Step 11. The UE transmits bP and MACUA to the AAA server and concurrently computes CK and IK.

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 cIDUE using the KUH and then sends cIDUE to the HSS. For this reason, the UE and the HSS can only retrieve user identity such as IMSI included in cIDUE using KUH. 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 cIDUE. Therefore, attackers cannot derive the IMSI and cannot modify IMSI.

b) The AAA server sends the EAP Success message with IDAP jjMSK to the AP. The AP then verifies whether or not received IDAP 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 MACH is generated by the correct HSS by verifying MACA. 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 KUA, our protocol uses aP and bP that are not related with KUH. Therefore, if disclosure of KUH occurs, attackers cannot guess KUA. In other words, guessing KUA 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 MACA in Step 10. Similarly, the AAA server can authenticate the UE by verifying MACUA in Step 12.

b) Between the UE and the HSS: The UE can authenticate the HSS by verifying MACA in Step 10. Similarly, the HSS can authenticate the UE by verifying MACU in Step 5.

* Secure against replay attack: Before generating TK, the HSS must verify whether TU is in the correct range or not. Moreover, our protocol verifies RANDA and RANDH included in MACA. Therefore, our protocol can prevent replay attack.

B. Performance Analysis

* Reduce ban width consumption: Our protocol uses cIDUE 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. Moreover, our protocol has less overhead than their 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 3GWLAN Interworking and proposed a new authentication and key agreement protocol based on EAP-AKA. The proposed protocol combines ECDH with symmetric key cryptosystem to 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. Josefssoni, H. Zhou, G. Zorn, Protected EAP Protocol (PEAP) Version 2, draft-josefsson-pppext-eap-tls-10, IETF, October 2004

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

[3] H. Haverinen, J.Salowey, EAP SIM Authentication, draft-arkko-pppexteap-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] PlanetMathi-Elliptic Curve Diffie-Hellman key exchange, http://planetmath.org/encyclopedia/DiffieHellmanKeyExchange.html

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