Trends in Mathematics
Information Center for Mathematical Sciences
Volume 8, Number 1, June, 2005, Pages 77–85

EFFICIENT MECHANISM FOR THE SETUP OF UE-INITIATED TUNNELS IN 3GPP-WLAN INTERWORKING

SANG UK SHIN

Abstract. We propose an efficient mechanism for the setup of UE(User Equipment)-initiated tunnels in 3GPP(3rd Generation Project Partnership)-WLAN(Wireless Local Area Network) interworking. The proposed mechanism is based on a secret key which is pre-distributed in the process of authentication and key agreement between UE and 3GPP AAA(Authentication Authorization Accounting) server. Therefore it can avoid modular exponentiation and public key signature which need a large amount of computation in UE. Also the proposed scheme provides mutual authentication and session key establishment between UE and PDG(Packet Data Gateway).

1. Introduction

3GPP-WLAN interworking refers to the utilization of resources and access to services within the 3GPP system by the WLAN UE and user respectively. The intent of 3GPP-WLAN Interworking is to extend 3GPP services and functionality to the WLAN access environment. 3GPP considers the following 6 scenarios for 3GPP-WLAN interworking:

(1) Common billing and customer care
(2) 3GPP system based access control and charging
(3) Access to 3GPP system PS(packet switched) based services
(4) Service continuity
(5) Seamless service provision
(6) Access to 3GPP CS(circuit switched) services,

For scenario 3, access to external IP networks should, as far as possible, be technically independent of WLAN Access Authentication and Authorization. However, access to external IP networks from 3GPP WLAN interworking systems shall be possible only if WLAN Access Authentication/Authorisation has been completed first. Scenario 3 requires a combination of both. The PDG supports access to external IP networks, including those supporting 3GPP PS Domain based services.

To setup UE-initiated tunnels between UE and PDG in scenario 3, 3GPP TS [3] is considering that the WLAN UE and PDG use IKEv2(Internet Key Exchange version 2)[8] in order to establish IPsec(Internet Protocol Security) SAs(security

1991 *Mathematics Subject Classification.* Primary 94A60, 94A62, 94A99; Secondary 14G50, 68P25.

Key words and phrases. 3GPP, WLAN, security, authentication, key agreement.

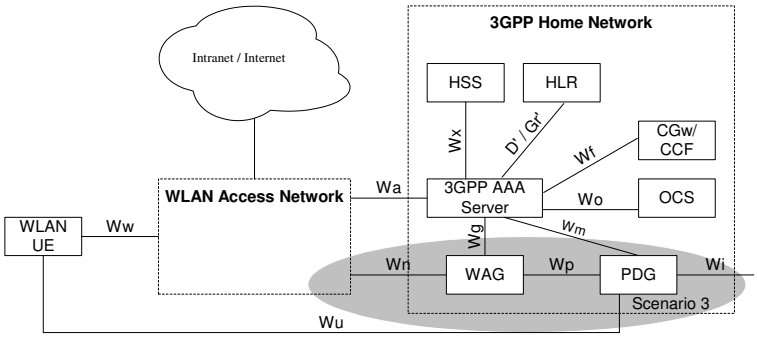

FIGURE 1. Non-roaming reference model

associations). However this mechanism requires the modular exponentiation for Diffie-Hellman key exchange and the public key signature which impose heavy computational overhead on UE.

This paper proposes an efficient mechanism using a secret symmetric key without public key operations, which is pre-distributed in the process of authentication and key agreement between UE and 3GPP AAA server. The proposed mechanism can avoid modular exponentiation and public key signature which need a large amount of computation in UE. Also the proposed scheme provides mutual authentication and session key establishment between UE and PDG.

2. Security architecture and security features for 3GPP-WLAN Interworking

3GPP TS [1] describes three reference models for WLAN interworking, Fig. 1 $\sim$ Fig. 3. In the first reference model(Fig. 1)the home network is responsible for access control and tunnel establishment. In Fig. 2 the home network is responsible for access control and tunnel establishment, and the traffic is routed through the visited network (using the WAG). In Fig. 3, the home network is responsible for access control, but the authorization decision of tunnel establishment will be taken by the 3GPP proxy AAA based on own information plus information received from the home network. The visited network will take part in tunnel establishment (either the WAG or the PDG).

The list below describes the network elements of the 3GPP-WLAN interworking Reference Model:

- A WLAN UE is the UE(equipped with UICC card including (U)SIM) utilized by a 3GPP subscriber to access the WLAN network for 3GPP interworking purpose. For examples, a laptop computer or PDA with a WLAN card, UICC card reader and suitable software applications.
- The 3GPP AAA Proxy represents a logical proxying functionality that may reside in any network between the WLAN and the 3GPP AAA Server.

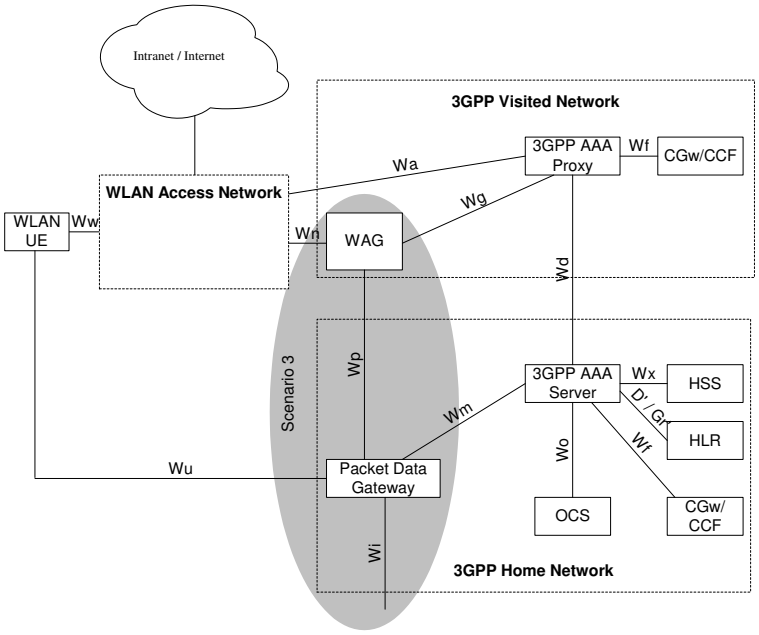

FIGURE 2. : Roaming reference model - 3GPP PS based services provided via the 3GPP Home Network

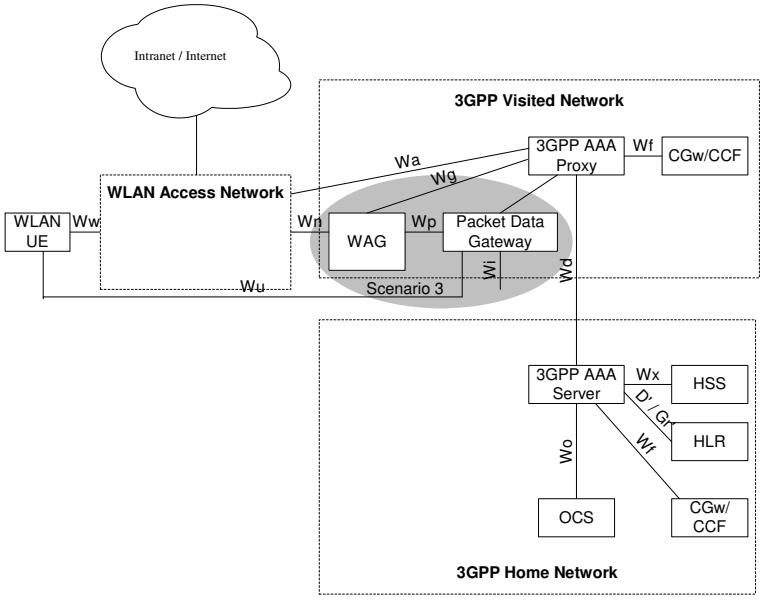

FIGURE 3. Roaming reference model - 3GPP PS based services provided via the 3GPP Visited Network

These AAA proxies are able to relay the AAA information between WLAN and the 3GPP AAA Server.

- The 3GPP AAA server retrieves authentication information and subscriber profile from the HLR/HSS of the 3GPP subscriber's home 3GPP network, authenticates the 3GPP subscriber based on the authentication information retrieved from HLR/HSS, and communicates authorization information to the WLAN potentially via AAA proxies.
- The HLR/HSS located within the 3GPP subscriber's home network is the entity containing authentication and subscription data required for the 3GPP subscriber to access the WLAN interworking service.
- 3GPP PS based services(Scenario 3) are accessed via a Packet Data Gateway(PDG). The PDG enforces tunnel authorization and establishment with the information received from the 3GPP AAA via the Wm interface.

Security requirements for 3GPP-WLAN interworking are as follows:

- The authentication scheme shall be based on a challenge response protocol and mutual authentication shall be supported.
- All long-term security credentials used for subscriber and network authentication shall be stored on UICC or SIM card.
- The subscriber should have at least the same security level for WLAN access as for his current cellular access subscription in [2].
- Signalling and user data protection shall be supported.
- User identity privacy shall be provided.

3GPP TS describes the following security features in WLAN interworking environment.

(1) Authentication of the subscriber and the network and SA(Security Association) management
   - It supports mutual authentication between WLAN-UE and 3GPP AAA server using IEEE 802.11i[9], EAP(Extensible Authentication Protocol)[6], DIAMETER[11] and RADIUS[10].

(2) Confidentiality and integrity protection
   - In scenario 2, confidentiality protection in the WLAN AN link layer is required. The specification of this feature is, however, out of scope of 3GPP. Confidentiality protection in scenario 3 shall be possible to protect the confidentiality of IP packets sent through a tunnel between the UE and the PDG.
   - Integrity protection is similar to confidentiality protection. The integrity of IP packets sent through a tunnel between the UE and the PDG shall be protected.

(3) User Identity Privacy
   - User identity privacy (Anonymity) is used to avoid sending any cleartext permanent subscriber identification information which would compromise the subscriber's identity and location on the radio interface,

or allow different communications of the same subscriber on the radio interface to be linked.
- User identity privacy is based on temporary identities, or pseudonyms. The AAA server generates and delivers the pseudonym to the WLAN-UE as part of the authentication process.

3. Efficient mechanism for the set-up of UE-initiated tunnels in 3GPP-WLAN interworking

3.1. **WLAN access authentication, key agreement and UE-initiated tunnel establishment mechanism.** In 3GPP WLAN interworking, first it requires to perform mutual authentication between WLAN UE and 3GPP AAA server. It is required that all long-term security credentials used for authentication shall be stored on UICC or SIM card. We consider only the case of UICC in this paper(similarly to the case of SIM card). WLAN UE shall first complete the process of authentication and key agreement(AKA) in order to access 3GPP service. 3GPP TS is considering USIM(Universal Subscriber Identity module)-based WLAN access authentication as Fig. 4 excluding the italic, bold and shaded parts. USIM-base WLAN access authentication is based on EAP(Extensible Authentication Protocol)-AKA. After completing mutual authentication between WLAN UE and 3GPP AAA server, when WLAN UE uses 3GPP PS based service, WLAN UE accesses PDG and then obtains services. In this case, it requires to provide data confidentiality and integrity between UE and PDG. To do this, 3GPP TS [3] is considering that the WLAN UE and PDG use IPsec ESP(Encapsulating Security Payload) tunnel[7]. In this mechanism, IKEv2 is used to allow IPsec ESP SA establishment between the WLAN UE and the PDG. UE requires the public key operations in the process of IKEv2 and needs the exchange of 6 times messages to perform EAP-AKA within IKEv2

3.2. **Efficient mechanism for the set-up of UE-initiated tunnels.** To setup UE-initiated tunnels between UE and PDG in scenario 3, 3GPP TS [3] is considering that the WLAN UE and PDG use IKEv2[8] in order to establish IPsec SAs. However this mechanism requires the modular exponentiation for Diffie-Hellman key exchange and the public key signature which impose heavy computational overhead on UE. This paper proposes an efficient mechanism using a secret symmetric key without public key operations, which is pre-distributed in the process of authentication and key agreement between UE and 3GPP AAA server.

First, AKA is performed by WLAN UE and 3GPP AAA server. 3GPP TS [3] describes USIM-base WLAN Access Authentication mechanism which is based on EAP-AKA[5]. We modify this mechanism as follows. In the Fig. 4, the italic, bold and shaded parts are included additionally, and other parts are equal to section 6.1.1 of [3].

In the step 3 of the Fig. 4, a “PS_Service” parameter indicates that UE wants to access 3GPP PS Domain based services. In the step 6, it checks the “PS_Service” indicator. If UE want to access 3GPP PS domain based services, a “PS_Key” is

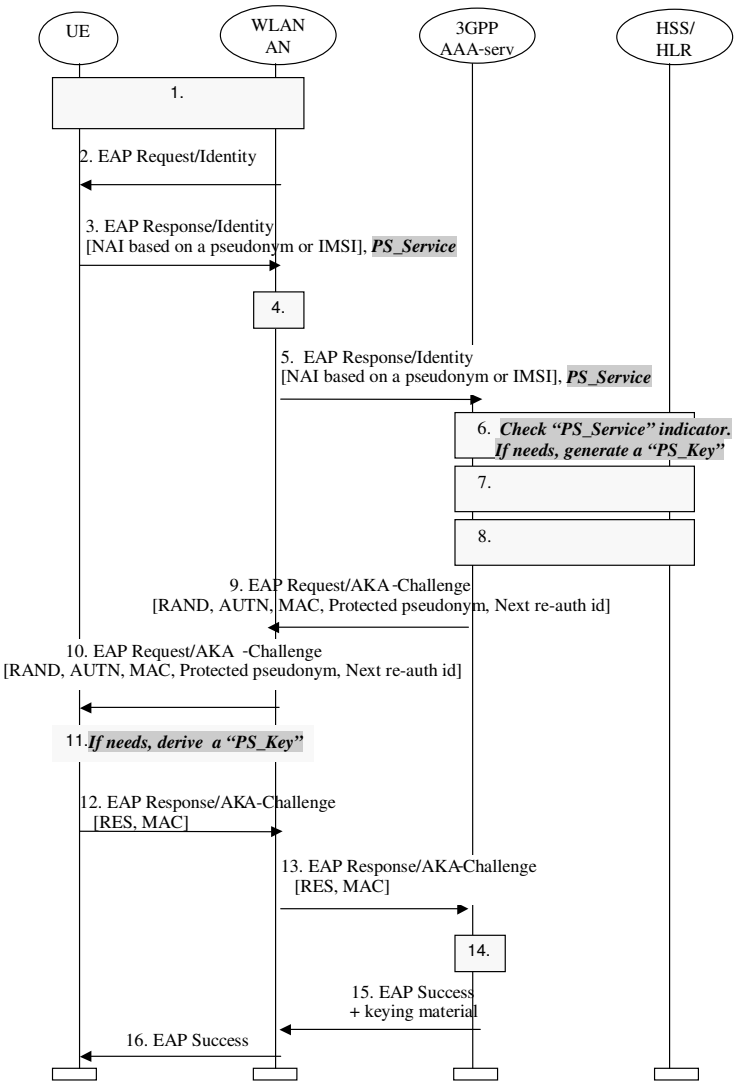

FIGURE 4. Authentication based on EAP-AKA scheme

generated additionally. The "PS_Key" may be generated by using 3GPP MILENAGE algorithm[4] as IK(Integrity Key) and CK(Cipher Key), and will be used to setup UE-initiated tunnels in Scenario 3. In the step 11, the WLAN UE also can derive the "PS_Key" by using the same method.After completing the authentication and key agreement between UE and 3GPP AAA server, WLAN UE can access PDG which provides 3GPP PS Domain based services. To do this, 3GPP TS [3] is considering to use IKEv2 to setup secure tunnels between UE and PDG, which requires public key cryptography. However we provide more efficient method which does not use public key cryptography. The proposed scheme as follows(see Fig. 5).

(1) UE sends "Tunnel Setup Request" message. This message includes the pseudonym based NAI(Network Access Identifier) which was assigned in the process of the authentication and key agreement between UE and 3GPP AAA server, and the nonce N_UE generated randomly by the UE.
(2) PDG routes "PS_Key Request" message towards proper 3GPP AAA Server based on the realm part of the NAI.
(3) 3GPP AAA server sends the subscriber's PS_Key to PDG.
(4) PDG generates the session master key MK and then derives encryption key MK_C and integrity key MK_I as the following;
    MK = prf(PS_Key, NAI | N_UE | N_PDG),
    (MK_C, MK_I) = prf+(PS_Key, N_PDG | N_ UE | NAI),
    where N_PDG is a randomly generated nonce by the PDG, prf and prf+ are cryptographically secure pseudorandom functions, which may be functions defined in IKEv2[8].
    PDG computes authenticator Auth_PDG using MK_I and sends "Tunnel Setup Response" message to the UE. This message includes N_PDG and Auth_PDG.
    Auth_PDG = MAC(MK_I, NAI | N_ UE | N_ PDG),
    where MAC is a cryptographically secure message authentication code such as HMAC-SHA1.
(5) UE generates the session master key MK and derives encryption key MK_C and integrity key MK_I using the same method as PDG.
    MK = prf(PS_Key, NAI | N_UE | N_PDG),
    (MK_C, MK_I) = prf+(PS_Key, N_PDG | N_UE | NAI).
    UE verifies the received authenticator Auth_PDG. If Auth_PDG is correct, the UE computes authenticator Auth_UE using MK_I and sends "Tunnel Setup Complete" message to PDG, which includes encrypted authenticator, E(MK_C, Auth_UE). A function E denotes a block cipher such as AES(Advanced Encryption Standard).
(6) PDG decrypts the received message and then verifies the authenticator Auth_UE. If it succeeds, PDG allows UE to access the service.

3.3. **Analysis of the proposed mechanism.** Our solution minimally modifies EAP AKA based authentication mechanism which is described in [3]. It includes the parameter "PS_Service" additionally in the step 3 of the Fig. 1, and the generation of PS_Key in the step 6 and the step 11. Therefore it minimizes the communication and computation overhead.For the setup of UE-initiated tunnels, 3GPP TS is considering IKEv2 to establish a SA(Security Association) between UE and PDG. IKEv2 requires modular exponentiation operations to perform Diffie-Hellman key exchange, and public key signature based authentication. However, the proposed scheme is based on only the symmetric key. Therefore it can avoid modular exponentiation and public key signature which need a large amount of computation. Our solution provides mutual authentication between the UE and the PDG. In the step 4 the UE authenticates the PDG by verifying the authenticator Auth_PDG

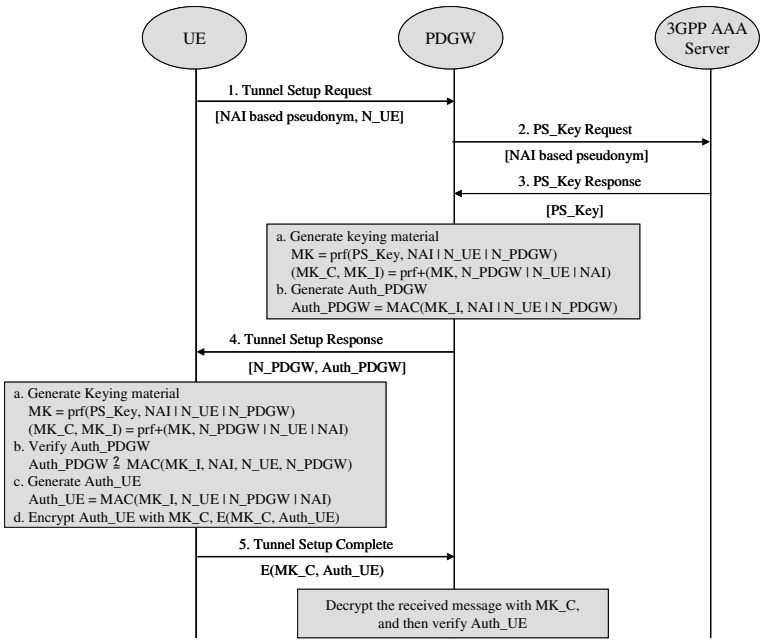

FIGURE 5. The proposed scheme: efficient mechanism for the set-up of UE-initiated tunnels

and in the step 5 the PDG authenticates the UE by checking Auth_UE. Even if keys which were used in previous sessions are revealed, an attacker can not obtain any information about the PS_Key. Also an attacker can not obtain any useful information for current session keys because keys for each session are derived by applying the prf with the PS_Key and random nonces. Therefore the proposed scheme is secure against the known-key attack[12]. It guarantees that generated keying materials are unique by nonces N_UE and N_PDG and cryptographic properties of the prf. Also the proposed scheme provides the user privacy by sending the pseudonym based NAI in the step 1. A replay attack is protected by randomly generated nonces, N_PDG and N_UE for each session.

The security of the proposed scheme depends on the properties of prf, prf+ and MAC function. These functions must be selected in order to guarantee the freshness of a session and session keys, and the randomness of session keys.

4. CONCLUSION

In this paper we introduced the security for 3GPP-WLAN interworking system. According to 3GPP TS 33.234 document[3], the WLAN UE can access the PDG which provides 3GPP PS Domain based services after completing the authentication and key agreement between the UE and 3GPP AAA server. To do this, 3GPP is considering to use IKEv2 to setup secure tunnels between the UE and the PDG. In the process of IKEv2 UE requires the public key operations and needs the exchange

of 6 times messages to perform EAP-AKA within IKEv2. It imposes heavy burdens on the UE and the PDG for authentication and key agreement. Therefore, we proposed the mechanism that a secret key is pre-distributed during WLAN Access Authentication/Authorisation between UE and 3GPP AAA server and then it is used for the set-up of UE-initiated tunnels. The proposed mechanism can avoid modular exponentiation and public key signature which need a large amount of computation in UE. Also the proposed scheme provides mutual authentication and session key establishment between UE and PDG.

References

1. 3GPP TS 23.234: *3GPP system to Wireless Local Area Network (WLAN) Interworking; System Description*
2. 3GPP TS 33.102: *3G Security; Security Architecture*
3. 3GPP TS 33.234: *WLAN Interworking Security*
4. 3GPP TR 35.205: *3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General*
5. draft-arkko-pppext-eap-aka-11, October 2003: *EAP AKA Authentication*
6. draft-ietf-eap-rfc2284bis-06.txt, October 2003: *PPP Extensible Authentication Protocol (EAP)*
7. draft-ietf-ipsec-esp-v3-06.txt, July 2003: *IP Encapsulating Security Payload (ESP)*
8. draft-ietf-ipsec-ikev2-12.txt, January 2004: *Internet Key Exchange (IKEv2) Protocol*
9. IEEE Std 802.11i/D2.0, March 2002: *Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/ MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security*
10. RFC 2865, June 2000: *Remote Authentication Dial In User Service (RADIUS)*
11. RFC 3588, September 2003: *Diameter base protocol*
12. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanston: *Handbook of Applied Cryptography*, CRC Press, 1996

Div. of Electronic, Computer and Telecommunication Engineering, Pukyong National University, Busan, 608-737, Korea

E-mail address: shinsu@pknu.ac.kr