INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS
Int. J. Commun. Syst. (2014)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/dac.2769

Improved IPSec tunnel establishment for 3GPP–WLAN interworking

S. Samoui[1], I. El Bouabidi[1], M. S. Obaidat[2], F. Zarai[1,*,†], K. F. Hsiao[3] and L. Kamoun[1]

[1]*LETI Laboratory, University of Sfax, Sfax, Tunisia*
[2]*Computer Science and Software Engineering Department, Monmouth University, West Long Branch, NJ 07764, USA*
[3]*Department of Information Management, Ming-Chuan University, Taoyuan County 333, Taiwan*

SUMMARY

Interworking between wireless local area network (WLAN) and the 3rd Generation Partnership Project (3GPP) such as Long Term Evolution (LTE) is facing more and more problems linked to security threats. Securing this interworking is a major challenge because of the vastly different architectures used within each network. Therefore, security is one of the major technical concerns in wireless networks that include measures such as authentication and encryption. Among the major challenges in the interworking security is the securing of the network layer. The goal of this article is twofold. First, we propose a new scheme to secure 3GPP LTE–WLAN interworking by the establishment of an improved IP Security tunnel between them. The proposed solution combines the Internet Key Exchange (IKEv2) with the Host Identity Protocol (HIP) to set up a security association based on two parameters, which are location and identity. Our novel scheme, which is called HIP_IKEv2, guarantees better security properties than each protocol used alone. Second, we benefit from Mobile Internet Key Exchange protocol (MOBIKE) in case of mobility events (handover). And we extend HIP_IKEv2 to HIP_MOBIKEv2 protocol in order to reduce the authentication signaling traffic. The proposed solution reinforces authentication, eliminates man-in-the-middle attack, reduces denial-of-service attack, assures the integrity of messages, and secures against reply attack. Finally, our proposed solution has been modeled and verified using the Automated Validation of Internet Security Protocols and Applications and the Security Protocol Animator, which has proved its security when an intruder is present. Copyright © 2014 John Wiley & Sons, Ltd.

Received 30 November 2013; Revised 26 January 2014; Accepted 28 January 2014

KEY WORDS: 3GPP LTE; WLAN; Interworking; Security; AVISPA

1. INTRODUCTION

In recent years, the use of wireless communication technologies has been growing, and their use has become more popular in our daily life. However, this huge deployment of wireless technologies has faced many challenges. Indeed, in addition to the risks known of wired networks, several vulnerabilities appear because of the service mobility, in particular, the handover and the integration of multiple technologies in the same terminal.

Hence, interworking between 3rd Generation Partnership Project (3GPP) Long Term Evolution (LTE) and wireless local area networks (WLANs) is advantageous for both service providers and end users; however, securing such interworking architecture is a challenging task [1]. Indeed, this issue has attracted the attention of the worldwide research community. The objective has been to provide practical solutions because integrated mobility and security support are desirable features for the network.

[*] Correspondence to: F. Zarai, LETI Laboratory, University of Sfax, Sfax, Tunisia.
[†] E-mail: faouzi.zarai@isecs.rnu.tn

We focus on, first, securing network layer for heterogeneous network and, second, securing mobility at this layer. Mobile IP (MIP) [2] has been designed to handle mobility at the network layer by managing mobile data communication [3]. MIP was designed by Internet Engineering Task Force in two versions, Mobile IPv4 (MIPv4) [4] and Mobile IPv6 (MIPv6) [5]. The main goal of this protocol is to allow mobile nodes (MNs) to move and change its point of attachment while maintaining its network connections [6].

To have a successful security strategy in wireless networks, there are three objectives that must be met: mutual authentication, data integrity, and confidentiality. It is always desired to establish an efficient and secure key management scheme between authenticated users and different nodes in the network [7]: in this context, many protocols are designed to assure security services. As the aim is to create security services at the network layer and as IP Security (IPSec) [8] is used to protect MIPv6 data and signalization messages, we choose to benefit from it to establish a security tunnel between a WLAN network and 3GPP LTE network.

IPSec is a security framework that operates at the network layer by extending the IP packet header. It provides interoperable, high-quality, cryptographically based security for IPv4/IPv6. The security services offered by IPSec include authentication, integrity, encryption, and flow confidentiality.

With IPSec, both communication endpoints must agree on a set of algorithms and keys to achieve a secure connection [9]. To establish a shared state, hosts can employ Internet Key Exchange (IKEv2) protocol [10]. The shared security context is called a Security Association (SA).

SA is a central concept in IPSec that supports encryption, authentication, or both. They are unidirectional, so in order to protect a duplex channel, two SAs are necessary (an incoming one and an outgoing one).

The IKEv2 exchange is designed to establish and manage SA in four messages. In the first two messages, called IKE_SA_INIT, the communicating entities negotiate cryptographic algorithms, exchange nonce, and make Diffie–Hellman [11] exchange to obtain a shared key. In the last two messages, called IKE_AUTH, both entities authenticate the previous messages and exchanges identity. Finally, the SA established by IKEv2 is based essentially on location.

As already mentioned, our goal is to secure the interworking between the 3GPP LTE and WLAN at the network layer, so that a tunnel full authentication and authorization between them handled by IKEv2 accompanied with the Extensible Authentication Protocol Authentication and Key Agreement (EAP_AKA) is proposed and described in our first previous work, which is called IKEv2/EAP_AKA [7]. Therefore, an IPSec tunnel based on location is established.

In the mentioned work [7], we treat also the case of mobility events. So, when an MN changes its point of attachment and receives a new IP address, IPSec cannot continue normally, and rekeying of the SA must occur. Therefore, the IPSec tunnel established must be changed, and we need to establish a new tunnel with new security associations.

This solution may not be optimal for several reasons. In some cases, creating a new security association may require user interaction for authentication, such as entering a code from a token card or by manual intervention (such as a password). Creating new SAs frequently involves expensive calculations and probably a large number of round trips, so it is too lengthy to ensure session continuity.

Therefore, a mechanism for updating the IP addresses of existing IPSec and IKE SAs is required.

This handover case is handled by the Mobile Internet Key Exchange protocol (MOBIKE) [12]. MOBIKE is a mobility and multihoming extension to the IKEv2 protocol. MOBIKE allows an MN to change its point of attachment while maintaining a Virtual Private Network (VPN) session. Similarly, it allows a multihomed host that has multiple interfaces of attachment to a network to move the traffic to a different interface always on keeping the VPN session.

The MOBIKE protocol solves the mobility problem inherent in IKEv2. Consequently, the node moves from a network to another without re-establishing all security associations, and the existing VPN session still continues without rekeying.

In a second previous work [13], we demonstrate that despite that IKEv2 offers authentication, authorization, and key agreement services to establish a security association between two peers bound to IP addresses, it is still vulnerable to some security problems such as denial of service (DoS) and man in the middle (MITM). Therefore, we have focused to extend the IKEv2 in order

DOI: 10.1002/dac

to enhance authentication, eliminate MITM, and reply attacks and guarantee better security between the two peers. The idea is to benefit from the Host Identity Protocol (HIP) protocol [14] because it is used also to establish a pair of IPSec security associations between two hosts through the HIP Base Exchange (HBE). The HBE consists of four messages (I1, R1, I2, and R2) based on a classic Diffie–Hellman key exchange with an inclusion of a puzzle by the responder node as a cryptographic challenge in order to reduce a DoS attack from an illegitimate node that wishes to saturate the responder node with HIP initiation messages [15]. Finally, the SA established by HIP is based essentially on the host identity name space introduced by this protocol. So, in [13], we have described a proposal that consists of combining the IKEv2 with HIP to set up a security association based on two parameters, which are location and identity. This combination provides better security properties than each protocol used alone. This proposal, named HIP_IKEv2, couples location and identity to define a security association between two peers.

This article presents continuity in this research axis. So, we try to give a new scheme to secure 3GPP LTE–WLAN interworking by the establishment of an improved IPSec tunnel between them. Thus, we have modeled the improved IPSec tunnel using Automated Validation of Internet Security Protocols and Applications (AVISPA) [16] and Security Protocol Animator (SPAN) [17], which has proved its security when an intruder is present. The simulation results confirm that the improved IPSec tunnel is a secure solution that ensures end-to-end authentication, confidentiality, and integrity.

The rest of this article is structured as follows. Section 2 describes an overview of MIPv6. Section 3 summarizes the state of the art related to this work. Section 4 presents motivation and novelty. Next, in Section 5, we describe the adopted interworking architecture. In Section 6, we present the improved IPSec tunnel followed by the security analysis. Afterwards, in Section 7, we compare our scheme to others' protocols. Then, in Section 8, we show verification results of AVISPA and SPAN, and we discuss the results obtained. Finally, in Section 9, the conclusion and future work are drawn.

2. OVERVIEW OF MOBILE IPv6

2.1. Mobile IPv6

Both MIPv4 and MIPv6 support the IP hosts mobility and allow them to utilize two IP addresses: a home of address (HoA), which represents the fixed address of an MN, and a care-of-address (CoA) that changes with the IP subnetwork to which an MN is presently attached.

There are certain issues with MIPv4 such as triangular routing [18], ingress filtering [19], and double crossing [19]. In order to solve these problems, MIPv6 has been proposed with many more enhancements that overcome several shortcomings in MIPv4, offering a larger address space, and route optimization, and improving security [5], which is of great interest to us.

So, MIPv6 is a host-based solution for handling the global mobility of hosts in IPv6 networks [20]. MIPv6 is composed of three main entities: MN, correspondent node (CN), and home agent (HA). MN is allocated a permanent address called Home of Address (HoA) at home network, which indicates the MN's IP address and its identity in its home network, and it will obtain a temporary address called a CoA, when it moves to a foreign network. When an MN moves from its home network and visits a foreign network, it will discover the default router of the visited network and determines its CoA. Subsequently, the MN forwards a binding registration message to its home network to communicate it about its current CoA. After that, the HA updates the mapping of MN's HoA and CoA, and security associations (bidirectional tunneling) are established between MN and its HA [21].

A CN not aware of the movement of the MN wants to communicate with it. Hence, the packets sent by CN and destined to MN are first routed to MN's home network. The HA will intercept those packets and forward them to the MN. So the HA is in charge of redirecting packets to MN. Such packet forwarding procedure through HAs is called triangular routing, which causes critical latency because of the transfer in HA.

Triangular routing is performed in MIPv4 as MN directly sends messages to CN, but CN sends messages to MN via HA [19], Although MIPv6 removed this triangular problem by the introduction of the Binding Update (BU) message, which enables an MN to update its current location information to the CN. Then, CN is capable of communicating directly with MN. So, a Return Routability (RR) procedure [5] was proposed to assist CN and MN in agreeing on a shared secret key to protect the integrity of the BU message [21].

The basic objective of developing MIPv6 is security against some different types of attacks such as DoS, connection hijacking, MITM, and impersonation attacks. The security objective is to safely create routing changes because all threats are reasoned by the changed routing used to allow mobility in the network. There are several threat categories for MIPv6 such as threat between HA and CN, threat between CN and MN, and threat between HA and MN, which are of major interest to us [22].

The MIPv6 protocol has solved some security problems found in MIPv4 networks but not in all. For example, the mandatory inclusion of IPSec in the MIPv6 protocol, which makes it fundamentally more secure than the MIPv4 scheme. However, given its flexibility, MIPv6 protocol introduces new problems. In spite of using IPSec for establishing security association and secure tunnel between an MN and its HA, communication between the MN and the HA still suffers from others attacks.

2.2. *Security flaws*

IPSec uses IKEv2 for key exchange service to establish security association. IKEv2 offers authentication, authorization, and key agreement services, but it is still vulnerable to some security flaws. In this section, we will enumerate some of these. First, IKEv2 uses Diffie–Hellman cryptographic protocol for establishing secret keys. Payloads required for generating keys are expressly transferred, so a MITM attack can easily occurs. Second, this protocol requires complicated exponential computation. Indeed, this operation occupies many resources. In addition, the intruder tries to exhaust server's resources, for example, the HA is forced to do falsified request; therefore, legal MN and HA fail to connect with the server, and subsequently, a DoS attack occurs. Moreover, exchanged messages have no freshness; consequently, this allows for launching DoS attack by replying messages.

Finally, with IKEv2, the identity of peers is their IP address, and the SA established after the IKEv2 process is based essentially on the network address. This leads to two problems: (i) the identity of a peer may be not available at the beginning of the IKEv2 exchange, and (ii) when there is an IP conflict problem, the initiator will communicate with two different peers.

3. RELATED WORK

MIPv6 presents some security vulnerabilities when used in heterogeneous wireless networks. For this reason, many security solutions are still in progress. Several of them offer enhanced security in MIPv6. However, there are areas still prone to attacks. So, many researchers focus on this issue. In this section, we will present some related work that treat this idea, some of them give a general solution of possible threats, and authors give specific solutions for control signaling messages, but few works focused on securing data traffic.

In [23], Celentano analyzed the security threats for mobility management in MIPv6 and proposed a solution to secure them, assuming that the communicating nodes are attached to a MIPv6-enabled IP Multimedia Subsystem (IMS) network.

The IMS centralized an Authentication Authorization and Accounting (AAA) server [24] that will be the responsible for generating, managing, and distributing the MIPv6 authentication keys required in the BU procedures. Therefore, increasing security and mobility-related information will be accessible to mobile network operator. With the assumption that peers are attached to the IMS, the costly MIPv6 RR procedure is eliminated, which greatly increases the overall MIPv6 security level and the vulnerability in the HA–CN link is avoided. Moreover, the number of exchanged messages during handover between terminals and network is reduced, and consequently, the handoff latency is minimized. So it improves the security level of MIPv6 signaling messages exchanged in order to allow seamless session continuity in case of mobility.

DOI: 10.1002/dac

In [25], the authors worked in securing control signaling messages in MIPv6 when the network attachment point of the MN is changed. They proposed an approach for implementing Identity-Based Encryption (IBE) authentication between HA and MN as well as between CN and MN.

Environments taken into account are where the MN and the CN use the same Public Key Generator (PKG) and where they use different PKGs. They estimate also the performance of some proposed signaling protocols. Indeed IPSec Encapsulation Security Payload (IPSec ESP) in transport mode is the standardized method for securing BUs and other control messages sent in the home registration process. Mutual authentication, dynamic key management, and negotiation of cryptographic algorithms are handled by the IKEv2 protocol. The authentication method is based on a shared secret, X.509 certificates or EAP [26]. The authors outline how IBE can be applied by replacing X.509 certificate based authentication with IBE-based authentication in the four-way IKE handshake or by embedding an IBE-based key agreement method in EAP. They show also how X.509 certificate-based authentication can be replaced with IBE authentication in both proposals by replacing Public Key Infrastructure (PKI) signatures with IBE signatures and PKI encryption with IBE encryption. A third IBE-based method is presented for mutual authentication between an MN and a CN, which uses IBE-based key agreement in a multi-PKG environment. A fourth IBE-based method integrates IBE with the use Cryptographically Generated Addresses for MN Home Addresses.

In [27], Sunguk Lee proposed a security mechanism based on using Transport Layer Security (TLS) to establish keying material to protect MIPv6 signaling and data traffic between HA and MN. He illustrated the security mechanism using IPSec and IKEv2 with AAA infrastructure, and he optimized IKEv2-based operation for HA in visited domain. These mechanisms use an IPSec/IKEv2 to secure the communication between MN and HA. Instead of using IKEv2 to establish security associations, the proposed solution is based on TLS-protected messages to exchange keys and bootstrapping parameters between the MN and the HA controller (HAC). Using TLS and HAC offers advantages over IPSec and IKEv2 in implementation and support of Dual-Stack MIPv6.

In [22], Moravejosharieh focused on MIPv6 security, possible threats, and security considerations. He detailed how IPSec works and presented a simple table where he proposed a solution for each threat such as the authentication of control message for MITM attack, the line encryption for eavesdropping thread, and the user authentication and access lists for unauthorized access.

4. MOTIVATION AND NOVELTY

As described in the preceding section, there are some works that search on securing MIPv6 data. However, they lack precision. For example, no work specifies the discussed architecture. Also they lack performance simulation analysis and results. Furthermore, there is no available work that deals with heterogeneous networks, which is our interest.

Hence, our motivation in this article is to present a detailed solution for securing 3GPP LTE_WLAN interworking architecture. We try to adapt HIP_IKEv2 [13] described previously accompanied with the EAP_AKA protocol to improve the IPSec tunnel established for 3GPP/WLAN interworking [7]. The solution presents an improved IPSec tunnel to secure exchange between the User Equipment (UE) and the evolved Packet Data Gateway (ePDG). We want to benefit from MOBIKE protocol in case of mobility events to extend HIP_IKEv2 to HIP_MOBIKEv2 protocol so as to reduce the authentication signaling traffic. The solution is validated by simulations results.

5. INTERWORKING 3GPP/WLAN ARCHITECTURE

For 3GPP/WLAN interworking, there are two main architectures: loose coupling and tight coupling. As shown in Figure 1, we describe the interworking loose coupling architecture between 3GPP and WLAN [7].

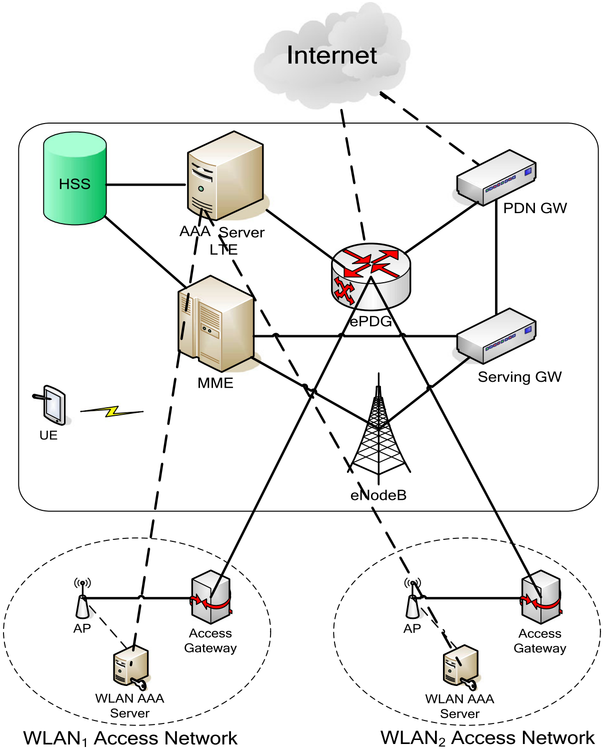


Figure 1. Interworking 3GPP/WLAN architecture.

Three particular elements constitute this interworking architecture:

- *The 3GPP network (LTE)*: Which presents the home network that consists of many components such as the AAA server, the ePDG entity, the Home Subscriber Server/Authentication Center (HSS/AuC), the Mobility Management Entity, in addition to the Public Data Networks, and finally the Serving Gateway. We will not detail all these components, and we will only detail the security architecture. Hence, the main function of the ePDG is to secure the data transmission with a UE connected over an untrusted non-3GPP access. For this purpose, the ePDG acts as a termination node of IPSec tunnels established with the UE. The AAA server guarantees the authentication between 3G and non-3GPP networks by ensuring the access through ePDG entity and allots registration information such as International Mobile Subscriber Identity (IMSI), which will be safeguarded in the database HSS/AuC. The HSS is a central database containing information about user and subscription. It includes different functionalities such as user authentication, access authorization, call and session establishment support, and mobility management [28].
- *The WLAN access network*: This consists of Access Points (APs), AAA servers, and Access Gateways. The WLAN AAA manipulates AAA traffic, and the Access Gateway manipulates the data traffic.

6. IMPROVED IPSEC TUNNEL ESTABLISHMENT

6.1. Requirement of a secure and efficient 3GPP/WLAN interworking

Interworking between WLAN and 3GPP/LTE networks is a challenging task, and it can open the door to various attacks. Hence, in order to guarantee an adequate level of security and quality of service for an efficient and secure interworking, many requirements must be ensured. These requirements may concern signaling exchanges or end-to-end data exchanges.

In order to secure data exchange, we need to talk about the following features:

- Mutual authentication between communicating entities.
- Integrity protection of exchanged messages.

- Confidentiality of exchanged data and shared secret keys.
- Freshness of messages and keys.
- Replay attack protection.
- DoS protection.
- MITM protection.

In order to have satisfactory quality of service, we need to reduce handover latency.

6.2. *Improved IPSec tunnel establishment*

As already mentioned, our goal is to secure 3GPP/WLAN interworking on the network layer and then reduce handover latency in case of mobility event. We focus especially on securing MIPv6 data traffic between an MN and his HA. The considered scenario is that a UE, which is subscribed to the LTE network, wants to be connected first to a WLAN_1 access network. Second, it moves from this WLAN_1 access network to a WLAN_2 access network. According to this scenario, we have first a heterogeneous interworking scenario between a 3GPP/LTE and a WLAN network. Second, we have a handover between two untrusted non-3GPP IP access connected to the same ePDG, which need to provide authentication, confidentiality, and integrity protection.

We think about adapting HIP_IKEv2 [13] accompanied with EAP_AKA protocol to establish an improved IPSec tunnel between the UE connected to WLAN_1 and the ePDG. But, when the UE moves, the improved IPSec tunnel established must be changed, and we need to establish a new tunnel with new security associations because the SA already established is based on two parameters: the host identity tag, which is constant, and the IP address, which is variable. This solution may not be optimal for several reasons. Frequently, creating a new security association requires user intervention for authentication, such as entering a password. Creating new SAs often involves expensive calculations and perhaps a big number of round trips. Therefore, a mechanism for updating the IP addresses of existing security association is needed.

The mobility problem found in IKEv2 is solved by MOBIKE protocol by decoupling the SA established from the IP address. In the same way, we think to extend the HIP_IKEv2 protocol to HIP_MOBIKEv2 in order to reduce the authentication signaling traffic. Hence, when the IPSec tunnel is established, the IPSec SA is based on the IP address in the HIP_IKEv2 SA instead of the IP address in the header of HIP_IKEv2 message. Therefore, the handover case is handled by HIP_MOBIKEv2. So the UE moves from a network to another without re-establishing all security associations. The next section describes the HIP_MOBIKEv2 exchange.

6.2.1. HIP_MOBIKEv2 protocol. HIP_IKEv2 does not provide any mobility support. That is why HIP_MOBIKEv2 is defined as an extension to the first one to provide secure mobility. The main scenario for HIP_MOBIKEv2 is enabling a VPN user to move from one address to another without re-establishing all security associations with the second VPN part. HIP_MOBIKEv2 updates only IP address in the header of IPSec SAs, and the addresses and other parameters used inside the tunnel stay unchanged. Therefore, HIP_MOBIKEv2 allows a peer to have several IP addresses. In addition, it allows traffic movement between different networks interfaces if the used one stops working while maintaining a VPN session.

The initiator establishes a HIP_IKEv2 SA with the responder by means of the HIP_IKEv2_INIT exchange. This exchange is similar to the initial exchange in HIP_IKEv2 messages, in which peers negotiate cryptographic algorithms and exchange nonces, HITs, and Diffie–Hellman parameters to generate keying material for the HIP_IKEv2 SA.

However, in the HIP_IKEv2_AUTH exchange, there is a small difference. In addition to exchange identities, certificate, traffic selectors (TS), and other habitual payloads are also exchanged. HIP_MO BIKEv2 introduces two INFORMATIONAL notification payloads: the HIP_MOBIKEv2_S UPPORTED payload to inform the other peer that supports MOBIKE; and the ADDITI ONAL_IP_ADDRESSES, which contains others available IP that can be used. Finally, a HIP_IKEv2 and IPSec SAs have been established between the first IP address of the initiator IPi1 and the IP address of the responder IPr1. When the initiator wants to change its IP address to IPi2, HIP_MOBIKEv2 defines two other notification payloads to be used: the UPDATE_SA_ADDRESSES notification payload sent using the new IP address accompanied by the host identity tag to guarantee the legitimacy of the sender and the COOKIE2 notification payload used to ensure RR check purposes. If the INFORMATIONAL request includes COOKIE2 sent by the responder, the initiator must copy the notification to the response message.

Figure 2 shows the HIP_MOBIKEv2 handover procedure. The notation is based on HIP_IKEv2 protocol [13].

6.2.2. Hypothesis and notations. In our scheme, we assume the existence of the following keys:

K_{UE_HSS}: Symmetric key (SK) shared between UE and HSS.
$K_{ePDG\_3GPPAAAserver}$: SK shared between ePDG and 3GPP_AAA server.

Our scheme is described with the notation summarized in Table I.

6.2.3. Proposed scheme. In addition to HIP_IKEv2 protocol to establish IPSec security associations, the proposed solution is based also on EAP_AKA to enhance the authentication and authorization procedure and therefore minimize security threats. The EAP_AKA [29] within HIP_IKEv2 must be used to authenticate UEs [30]. The authentication of the UE terminates in the 3GPP AAA server.

The tunnel full authentication and authorization are described in Figure 3. All steps are detailed as follows:

Step 1 (UE ➔ ePDG): HIP_IKEv2_SA_INIT_Req: [HDR, SAi_1, $\{KE_{UE}\}_{PK\_ePDG}$, $\{N_{UE}\}_{PKe\_PDG}$, HIT_{UE}, Ts, HASH_1].

With HASH_1 = $\{H(SAi_1||KE_{UE}||N_{UE}||\ HIT_{UE}\ ||Ts)\}_{PR\_UE}$

The UE sends to the ePDG the IKE header (HDR), the SAi_1 that denotes the set of cryptographic algorithms for the HIP_IKEv2_SA that it supports, and the $\{KE_{UE}\}_{PK\_ePDG}$ that represents the Diffie–Hellman value encrypted with the public key of the ePDG, in addition to $\{N_{UE}\}_{PK\_ePDG}$ that represents the nonce (used as input to the cryptographic functions to protect against replay attacks by guarantying the liveliness of the keying material) encrypted with the public key of the ePDG. This message contains also the UE's host identity tag HIT_{UE} and a time stamp ticket. The HIP_IKEv2_SA_INIT_Req ends with a HASH_1 payload.

Once received, the ePDG uses its private key to decrypt KE_{UE} and N_{UE} payloads. Moreover, it uses the public key of the UE to decrypt HASH_1 and therefore obtain $H(SAi_1||KE_{UE}||N_{UE}||Ts||\ HIT_{UE})$. After that, the ePDG applies the same hash function on $(SAi_1||KE_{UE}||N_{UE}||\ HIT_{UE}\ ||Ts)$

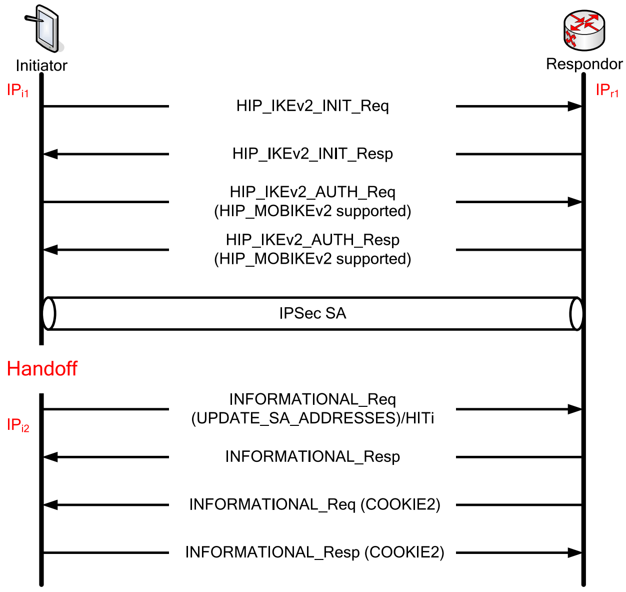


Figure 2. HIP_MOBIKEv2 handover procedure.

Table I. Notation used in the scheme.

Notation	Description
HDR	IKE header
SAi_n, SAr_n	Cryptographic algorithms
KEx	Key exchange payload of x
Nx	Nonce of x
IDx	Identity of the node x
AUTHx	Authentication payload of x
$\|$	Concatenation operation
SK	Shared key between UE and ePDG
Ts	Time stamp
{M}K	Encryption of message M with key K
H(M)	Hash of message M
f0, f3, f4, f5	Key generation function
f1, f2	Authentication function
G	Diffie–Hellman base
Exp	Exponential function
AMF	Authentication management field
AK	Anonymity key
CK	Cipher key
IK	Integrity key
MSK	Master session key
SQN	Sequence number
RAND	Random number
XRES	Expected result
AUTN	Authentication token
$\oplus$	Exclusive or
TSx	Traffic selectors of x
Puzzle	A cryptographic puzzle
Sol	Solution of puzzle
PK_x	Public key of x
PR_x	Private key of x

and compares it with $H(SAi_1 \| KE_{UE} \| N_{UE} \| HIT_{UE} \| Ts)$. If correct, it means that the first message of this initial exchange comes from a legal UE, and there is no attacker. If not, the ePDG must terminate this exchange.

Step 2 (ePDG ➔ UE): HIP_IKEv2_SA_INIT_Resp: [HDR, SAr_1, $\{KE_{ePDG}\}_{PK\_UE}$, $\{N_{ePDG}\}_{PK\_UE}$, HIT_{ePDG}, Ts, [CERTEQ], Puzzle, HASH_2].

With $HASH\_2 = \{H(SAr_1 \| KE_{ePDG} \| N_{ePDG} \| HIT_{ePDG} \| Ts)\}_{PR\_ePDG}$

The ePDG answers with a message that contains its choice from the set of cryptographic algorithms for the HIP_IKEv2_SA (SAr_1), and its value to complete the Diffie–Hellman exchange encrypted with the public key of the UE $\{KE_{ePDG}\}_{PK\_UE}$, in addition to $\{N_{ePDG}\}_{PK\_UE}$ that represents its nonce encrypted with the public key of the UE, followed by his host identity tag HIT_{ePDG} and a time stamp ticket. The last payload represents a HASH_2 payload.

This second message can contain optionally a Certificate Request Payload (CERTREQ), if the ePDG wants to obtain UE's certificate to authenticate him; also, it contains a cryptographic puzzle to be solved by the UE.

Upon receipt of this message, the UE uses its private key to decrypt KE_{ePDG} and N_{ePDG} payloads. Moreover, it uses the public key of the ePDG to decrypt HASH_3 and therefore obtain $H(SAr_1 \| KE_{ePDG} \| N_{ePDG} \| HIT_{ePDG} \| Ts)$. After that, the UE applies the same hash function on $(SAr_1 \| KE_{ePDG} \| N_{ePDG} \| HIT_{ePDG} \| Ts)$ and compares the results with $H(SAr_1 \| KE_{ePDG} \| N_{ePDG} \| Ts)$. If correct, it means that the second message of this initial exchange comes from a legal ePDG, and there is no attacker. If not, the UE must terminate this exchange.

Next, each node uses the two nonces accompanied with the Diffie–Hellman shared keys as inputs to the cryptographic functions for generating a SK between them.

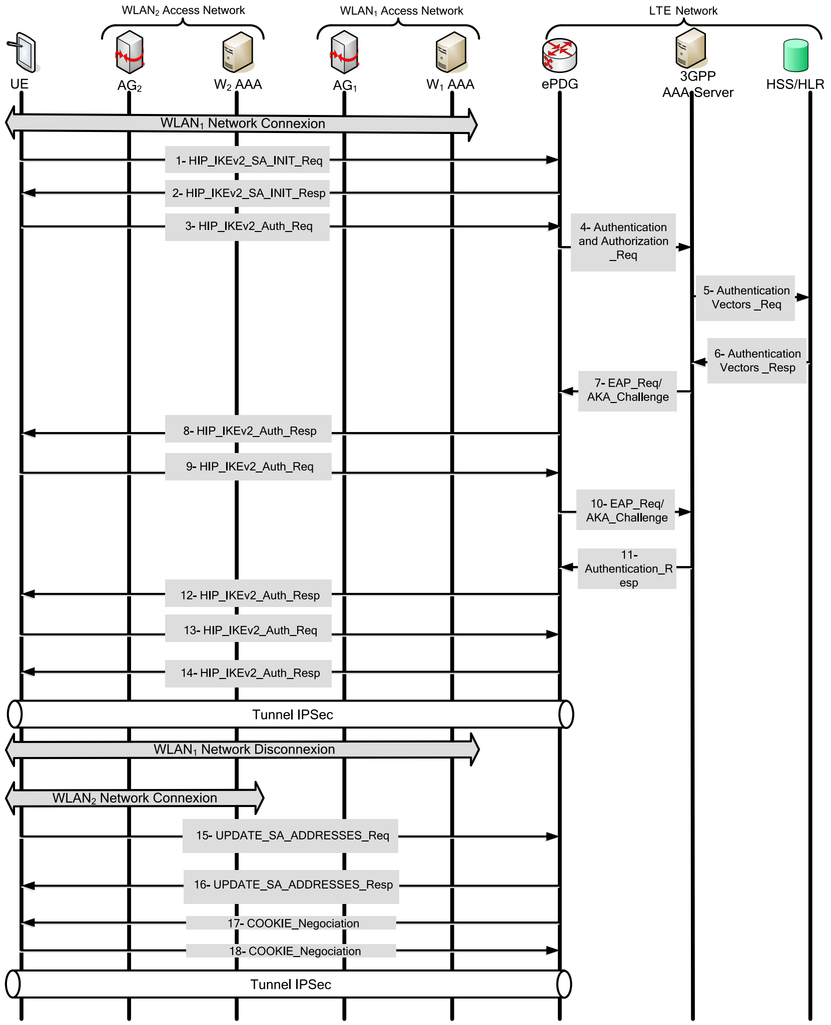


Figure 3. Tunnel full authentication and authorization between UE and ePDG.

$$SK = f_0(N_{UE}||N_{ePDG}||(\exp(\exp(G, KE_{UE}), KE_{ePDG})))$$

Therefore, both the UE and the ePDG share a bidirectional HIP_IKEv2_SA that provides confidentiality and integrity services to the following messages.

Step 3 (UE ➔ ePDG): HIP_IKEv2_AUTH_Req: [HDR, {ID_{UE}, ID_{ePDG}, HIT_{UE}, HIT_{ePDG}, [CERT], [CERTEQ], SAi_2, TS_{UE}, TS_{ePDG}, Sol, Ts, CFG_Req, N (HIP_MOBIKEv2_Supported)$\}_{SK}$]

After the establishment of the HIP_IKEv2_SA, the first message of HIP_IKEv2_AUTH phase is performed. The UE sends to the ePDG a request containing its identity (ID_{UE}), which must be compliant with Network Access Identifier format containing the IMSI, the identity of the ePDG, which is the AP Number (APN) in the (ID_{ePDG}) payload, and begins negotiation of child IPSec security associations. This message can optionally contain the certificate Payload (CERT), which is only necessary if the ePDG sent a CERTREQ. Also, he can send a CERTREQ payload if he wants to obtain a certificate of the ePDG. The UE shall send also the TS that allow the peers to identify the packet flows that require processing by IPSec, and the Configuration Payload Request (CFG_Req) that facilitates the user to obtain a Remote IP address [30]. Finally, UE gives a solution to the cryptographic puzzle and sends a HIP_MOBIKEv2_SUPPORTED notification to indicate that the implementation supports this specification. Only the header of this message is not encrypted with the new SK.

DOI: 10.1002/dac

The UE neglects the AUTH parameter in order to denote to the ePDG that it wants to use EAP over HIP_IKEv2.

The UE must send EAP messages for authentication over HIP_IKEv2 to the ePDG, and therefore, the ePDG must extract this EAP messages received and send them to the 3GPP AAA server.

Step 4 (ePDG ➔ 3GPP_AAAserver): Authentication and Authorization_Req: [$\{ID_{UE}, ID_{ePDG}\}_{KePDG\_3GPPAAAserver}$]

The ePDG decrypts the last message with SK, extracts ID_{UE} and ID_{ePDG}, and forwards them in an Authentication Request message to the 3GPP AAA server after encryption with the shared key $K_{ePDG\_3GPPAAAserver}$.

Step 5 (3GPP_AAAserver ➔ HSS/HLR): Authentication_Vectors_Req: [ID_{UE}]

After obtaining the user's identity, the 3GPP AAA server sends the user's IMSI to the HSS/AuC to fetch the user profile and authentication vectors (if these parameters are not available in the 3GPP AAA server).

Step 6 (HSS/HLR ➔ 3GPP_AAAserver): Authentication_Vectors_Resp: [RAND, XRES, CK, IK, AUTN]

The HSS shall then generate authentication vectors and send them back to the 3GPP AAA server. This generation of this authentication vectors is based on the pre-shared secret key K_{UE_HSS} (between the user and the 3GPP network), which is assigned to the user when it is subscribed to the LTE network.

This authentication vector includes a random challenge (RAND), the authentication token (AUTN), the expected response (XRES), the encryption key (CK), and the integrity key (IK).

$$XRES = f2\ (K_{UE\_HSS}, RAND)$$
$$CK = f3\ (K_{UE\_HSS}, RAND)$$
$$IK = f4\ (K_{UE\_HSS}, RAND)$$
$$AK = f5\ (K_{UE\_HSS}, RAND)$$
$$MAC = f1\ (K_{UE\_HSS}, SQN, RAND, AMF)$$
$$AUTN = \langle SQN \oplus AK, AMF, MAC \rangle$$

Step 7 (3GPP_AAAserver ➔ ePDG): EAP_Req/AKA_Challenge: [$\{RAND, AUTN, MAC_{server}\}$ $K_{ePDG\_3GPPAAAserver}$]

After generating and storing the Master Key MK using the CK and IK keys, the 3GPP AAA server calculates a Message Authentication Code (MAC_{server}) and initiates the authentication challenge. The 3GPP AAA server sends the EAP-Request/AKA-Challenge message to the user, which contains the RAND, AUTN, and MAC_{server} payload encrypted with the shared key $K_{ePDG\_3GPPAAAserver}$.

Step 8 (ePDG ➔UE): HIP_IKEv2_AUTH_Resp: [HDR, $\{ID_{ePDG}, HIT_{UE}, HIT_{ePDG}$, [CERT], Ts, EAP_Req/AKA_Challenge(RAND, AUTN, MAC_{server}), N (HIP_MOBIKEv2_Supported)$\}_{SK}$]

Upon receiving the EAP_Req/AKA_Challenge, the ePDG transmits it to the UE after decryption in order to start the EAP procedure over HIP_IKEv2. This response named HIP_IKEv2_AUTH_Resp contains also the identity of the ePDG, a certificate (the ePDG is authenticated to the user using its certificate), a time stamp ticket, and a HIP_MOBIKEv2_SUPPORTED notification to indicate that the implementation supports this specification.

Step 9 (UE ➔ ePDG): HIP_IKEv2_AUTH_Req: [HDR, {EAP_Req/AKA_Challenge (RES, MAC_{user})$\}_{SK}$]

The UE checks the authentication parameters and responds to the authentication challenge after receiving the EAP-Request/AKA-Challenge message. The user executes the AKA algorithms and verifies the AUTN payload; it generates also the IK and CK keys, calculates the

DOI: 10.1002/dac

MK key, and produces the Master Session Key MSK. The user verifies the MAC_{server} value. If this value is correct, it computes its response to the challenge (noted as an RES payload) and sends an EAP-Response/AKA-challenge message to the ePDG that includes the RES and a MAC_{user} value.

Step 10 (ePDG ➔ 3GPP_AAAserver): EAP_Req/AKA_Challenge: [{RES, MAC_{user}} $K_{ePDG\_3GPPAAAserver}$]

The ePDG forwards the EAP-Response/AKA-Challenge message to the 3GPP AAA server. So after receiving the EAP-Response/AKA-challenge message, the 3GPP AAA server verifies the received MAC_{user} value and checks if the received user's response to the challenge (RES) matches with the expected response (XRES) of the selected 3G authentication vector.

Step 11 (3GPP_AAAserver ➔ ePDG): Authentication_Resp: [{EAP_Success, Key material} $K_{ePDG\_3GPPAAAserver}$]

After verification, the 3GPP AAA server sends the Authentication Response including an EAP success and the key material MSK to the ePDG. Now, the MSK shall be used by the ePDG to produce the AUTH parameters in order to authenticate the HIP_IKEv2_SA_INIT phase messages because before, there was no key material available yet, and these two first messages of the HIP_IKEv2_SA_INIT had not been authenticated.

According in [30], the shared secret generated in the EAP exchange (the MSK) is used over HIP_IKEv2 to generate the AUTH (Authentication) parameters.

Step 12 (ePDG ➔UE): HIP_IKEv2_AUTH_Resp: [HDR, $\{EAP\_Success\}_{SK}$]

The EAP Success/Failure message is forwarded to the UE over HIP_IKEv2.

Step 13 (UE ➔ ePDG): HIP_IKEv2_AUTH_Req: [HDR,$\{AUTH_{UE}\}_{SK}$]

The UE takes its own copy of the MSK as input to generate the $AUTH_{UE}$ parameter to authenticate the first HIP_IKEv2_SA_INIT message. The $AUTH_{UE}$ parameter is sent to the ePDG.

Step 14 (ePDG ➔ UE): IKE_AUTH_Resp: [HDR, $\{AUTH_{ePDG}$, SAr_2, HIT_{UE}, HIT_{ePDG}, TS_{UE}, TS_{ePDG}, Ts, CFG_Resp)$\}_{SK}$]

The ePDG check the accuracy of the $AUTH_{UE}$ received from the UE. At this stage, the first message of HIP_IKEv2_SA_INIT is authenticated. Then, it calculates its own $AUTH_{ePDG}$ parameter, which authenticates the second message of HIP_IKEv2_SA_INIT. After that, the ePDG responds with a HIP_IKEv2_AUTH_Resp, which contains $AUTH_{ePDG}$, the second suite of cryptographic algorithms SAr_2, TS, and a time stamp ticket, in addition to the configuration payload (CFG _Resp), which presents the assigned Remote IP address.

Now, the HIP_IKEv2 negotiation terminates.

If the ePDG discovers that an old IKE SA already exist for that APN, it will delete the HIP_ IKEv2 SA and send to the UE an INFORMATIONAL exchange with a Delete payload, as specified in [30], in order to delete the old one.

Finally, an IPSec tunnel is established between the UE and the ePDG that provides security services to the transmitted data.

The following steps describe the procedure of the improved IPSec tunnel updating when the UE moves from $WLAN_1$ to a $WLAN_2$.

Steps 15–16 (ePDG ←→ UE): UPDATE_SA_ADDRESSES: [{HDR,N (UPDATE_SA_ ADDRESSES), $HIT_{UE}\}_{SK}$]

The UE notices a change in its own address and informs the ePDG about this by sending an INFORMATIONAL request containing the UPDATE_SA_ADDRESSES notification accompanied with his HIT. The request is sent using the new IP address. At this point, it also starts to use the new address in its own sent traffic as a source address [12].

DOI: 10.1002/dac

Steps 17–18 (ePDG ←→ UE): COOKIES_Negotiation: $[\{\text{HDR}, \text{N(COOKIES)}\}_{SK}]$

After receiving the UPDATE_SA_ADDRESSES notification, the ePDG registers the new address and performs an RR check of this address. When this test is completed, the ePDG begins to use the new address as the destination for its received ESP traffic [12].

6.3. Security analysis

- Mutual authentication between UE and its Home Network

To minimize security threats such as spoofing attack (for example, the ePDG cannot ensure that IKEv2 messages arrive from a legitimate UE), we propose to enhance the authentication procedure. So benefiting from the EAP_AKA protocol over IKEv2 can be a solution.

The EAP_AKA within IKEv2 shall be used to ensure mutual authentication between the UE and its Home Network. The authentication of the UE terminates in the 3GPP AAA server.

- Secure against MITM attack

First, the UE and the ePDG must exchange the first pair of IKEv2 exchange named IKE_SA_INIT, in which the UE and ePDG negotiate cryptographic algorithms, perform a Diffie–Hellman exchange, and exchange a nonce. These parameters are exchanged in clear text, and therefore, an attacker can easily intercept and obtain info. For instance, an attacker can intercept by replacing the Diffie–Hellman payload of the UE with its own value. So the ePDG, instead of receiving parameters of the UE, receives those of the attacker and vice versa. This exchange has undergone some modifications in order to eliminate this threat and resist MITM attack. The UE and the ePDG should confirm the identity of each other before distributing resources. So the idea in our improvement is based on public key cryptography mechanism.

- DoS attack prevention

Adding a cryptographic puzzle aims to protect the ePDG from DoS attacks. Before committing resources, the ePDG should ask the UE to solve a cryptographic puzzle. Requiring a correct solution of the cryptographic puzzle before allocating resources as precondition can reduce the attack rate, as it is a brute force computation. The puzzle is based on a cryptographic hash function, and it is composed of three components: the puzzle nonce I, the solution J, and the difficulty level K. So if the ePDG wants to defend against a DoS attack, it sends a nonce I to the UE. The UE is asked to find the solution J for which the K lowest order bit for the binary representation of the result $H(I||J)$ is equal to zero. So the UE must every time vary J and apply the hash function to the concatenation of the nonce I with the new J until an appropriate solution is found.

- Secure against reply attack

As time stamping is a way of preventing the replay attack, we propose to add a time stamp ticket to all IKEv2 exchanges between the UE and the ePDG. The two peers accept only messages for which the timestamp is included within a reasonable tolerance. The advantage of this method is that there is no need to generate random numbers.

- Protect user identity

One of the vulnerabilities known in the EAP_AKA protocol is the disclosure of the user identity, which is the IMSI, as it is sent in plaintext.

In our scheme, the user identity is sent by the UE to the 3GPP AAA server over the ePDG.

In the first path, when the UE send his identity to the ePDG, the above is encrypted with the shared key SK between the UE and the ePDG. In the second path, when the user identity is forwarded to the 3GPP AAA server, it is encrypted with the shared key $K_{\text{ePDG\_3GPPAAAserver}}$ between the ePDG and the 3GPP AAA server. Therefore, this problem is solved.

DOI: 10.1002/dac

- Integrity of messages

The HASH payload included in the IKE_SA_INIT messages of the proposed scheme assures the integrity of the messages. The HASH payload presents always a hash function applied to all messages encrypted with its private key. Hence, when the communication node receives the message, it can calculate the hash value and then compare the result with the HASH payload after decrypting it.

- Post-identified peer

Unlike IKEv2 where peers' identity is their IP address, with HIP_IKEv2 protocol, peers are post-identified by the host identity tag, which can eliminate some problems such as the IP conflict problem.

7. THE NEW SCHEME COMPARED TO OTHER PROTOCOLS

When analyzing security of HIP_MOBIKEv2, it is important to understand key differences from other security and mobility protocols.

The following table presents main features of our scheme (last column) compared to other competing protocols based on some selected criteria.

	IKEv2	MOBIKE	IKEv2/ EAP_AKA [7]	HIP_IKEv2 [13]	HIP_MOBIKEv2	HIPMOBIKEv2/ EAP_AKA
Authentication	Weak	Weak	Strong	Weak	Weak	Strong
MITM resistance	x	x	x	√	√	√
DoS resistance	x	x	x	√	√	√
Reply attack resistance	x	x	x	√	√	√
Message integrity	x	x	x	√	√	√
Mobility	x	√	x	x	√	√

8. FORMAL SPECIFICATION AND VALIDATION OF THE IPSEC TUNNEL ESTABLISHMENT

Because of the nature and sensitivity of security protocols, there has been a renewed emphasis on integrating formal validation in the design and development phase. For this reason, there are several automatic verification tools such as Isabelle, Murphy, FDR, CSP, NRL protocol analyzer, and AVISPA [31, 32]. We have chosen to verify our solution using the AVISPA, because it is the most popular and accurate tool according to many comparatives studies [33, 34].

8.1. AVISPA and SPAN

AVISPA is a push-button tool for building and analyzing security protocols. The AVISPA tool is equipped with a web-based graphical user interface (www.avispa-project.org/software) that supports the editing of protocol specifications and allows the user to select and configure the different back-ends of the tool [31].

AVISPA provides a modular and expressive formal language called the High Level Protocol Specification Language (HLPSL) for specifying intended protocols and formally validating them [35].

In order to help protocol designers in designing and debugging HLPSL specifications, a new feature SPAN [33] was created to facilitate the specification phase by allowing the animation of the language HLPSL [31].

8.2. Specifying the improved IPSec tunnel establishment

We specify the proposed IPSec tunnel establishment between the UE and the ePDG by two different languages, the HLPSL and the cas+ language.

DOI: 10.1002/dac

The specification is composed of several sections:

- The Protocol name.
- The agents that denote participants of the protocol suite.
- A set of identifiers and their types.
- A set of Basic Roles that serves to describe the actions of each agent.
- A Composition Role, which represents the entire protocol and instantiate the Basic Roles.
- The environment role is the top-level role, which describes considered sessions.
- The security goal, which represents the most important feature.

This specification is translated into the lower level language called Intermediate Format (IF) performed by the translator called HLPSL2IF. This step is totally transparent to the user. IF presentation of the protocol is used as an input to the four different back-ends: On-the-fly Model-Checker (OFMC), CL-based Attack Searcher (CL-AtSe), SAT-base Model-Checker (SATMC), and Tree-Automata-based Protocol Analyzer (TA4SP).

8.2.1. Intruder model. The AVISPA tool assumes that the protocol messages are exchanged beyond a network that is below the control of the Dolev_Yao intruder model [36].

This intruder has many capacities over the communication channel. Hence, it can read all messages exchanged between the agents and written in the channel. It can also derive new messages from its initial knowledge and the messages received from honest principals during protocol runs. To derive a new message, the intruder can encrypt and decrypt messages, compose, and decompose, in case he knows the key. The knowledge of the intruder is declared in the environment role, which is the top-level role. In our scheme, the intruder knows the communicating agents (UE, ePDG, and 3GPP_AAA server), their public keys (PK_{UE} and PK_{ePDG}), authentication and key generation function (f0, f1, f2, f3, f4, and f5), and hash function (H and F). The intruder possesses a public key and a private key (PK_I and PR_I). Hence, the intruder knowledge is summarized as follows:

```
   intruder_knowledge= { UE, ePDG,
3GPP_AAA server , PK_UE, PK_ePDG , PK_I, PR_I
,f0, f1,f2,f3,f4,f5, H, F }
```

8.2.2. Security goals. For security goal, we are able to check the mutual authentication between the UE and the 3GPP AAA server, in addition to a second mutual authentication between the UE and the ePDG, and the secrecy of Diffie–Hellman shared key SK, the Cipher Key CK, the Integrity Key IK, and therefore the Master Session Key MSK.

8.2.2.1 Mutual authentication The UE and the ePDG are authenticated on the shared Diffie–Hellman key. The witness and request events are goals related to authentication. So we have modeled this goal in HLPSL as follows:

```
role UE (UE,ePDG,3GPP_AAA server : agent,…)
   played_by  UE
   transition:
   .
   .
   /\ witness (UE,ePDG,SK1,SK)
role ePDG (UE,ePDG,3GPP_AAA server : agent,…)
   played_by  ePDG
   transition:
   .
   .
   /\ request (ePDG,UE,SK1,SK)
```

That is, the UE requests a check of the shared key agreed with the ePDG and identified by SK1. The UE and the 3GPP_AAA server are authenticated on different parameters.

DOI: 10.1002/dac

First, the UE authenticates 3GPP_AAA server on AUTN and $\text{MAC}_{\text{sever}}$. Then the 3GPP_AAA server authenticates the UE on RES. These three parameters are derived from the random number RAND. Thus, we have modeled this goal in HLPSL as follows:

```
role UE (UE,ePDG,3GPP_AAA server : agent,…)
   played_by  UE
   transition:
   .
   .
   /\ witness (UE, 3GPP_AAA server,RAND1,RAND)
role ePDG (UE,ePDG,3GPP_AAA server : agent,…)
   played_by  3GPP_AAA server
   transition:
   .
   .
   /\ request (3GPP_AAA server,UE, RAND1, RAND)
```

The same procedure is adopted to authenticate the UE by 3GPP_AAA server. Then, in the goal section of the protocol, we write the following:

```
  authentication_on SK1
  authentication_on RAND1
```

8.2.2.2 Secrecy of the shared key The Diffie–Hellman shared key must only be known by the UE and the ePDG entities. The secret is the goal fact related to secrecy.

This goal has been modeled in HLPSL as follows:

```
role UE (UE,ePDG,3GPP_AAA server : agent,…)
   played_by  UE
   transition:
   .
   .
   /\ secret (UE, ePDG,SK2,SK)
role ePDG (UE,ePDG,3GPP_AAA server : agent,…)
   played_by  ePDG
   transition:
   .
   .
   /\ secret (UE, ePDG,SK2,SK)
```

Also, the Cipher Key CK and the Integrity Key IK must be a secret between UE and the 3GPP_AAA server to guarantee the secrecy of the Master Session Key MSK.

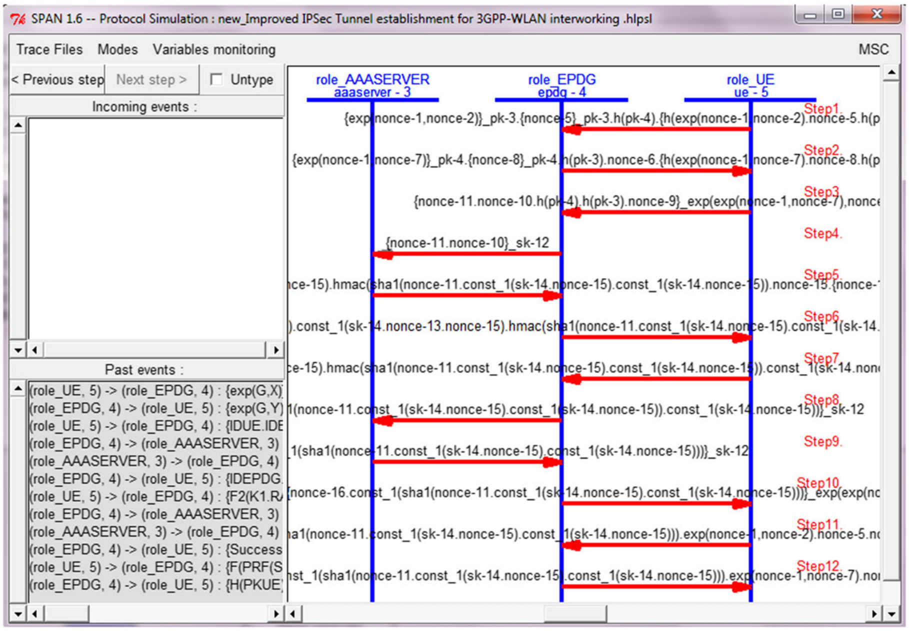
This goal has been modeled in HLPSL, as follows:

```
role UE (UE,ePDG,3GPP_AAA server : agent,…)
   played_by  UE
   transition:
   .
   .
   /\ secret (UE, 3GPP_AAA server,CK1,CK)
   /\ secret (3GPP_AAA server, UE,IK1,IK)
role ePDG (UE,ePDG,3GPP_AAA server : agent,…)
   played_by  3GPP_AAA server
   transition:
   .
   .
   /\ secret (3GPP_AAA server, UE,CK1,CK)
   /\ secret (UE, 3GPP_AAA server,IK1,IK)
```

Then, in the goal section of the protocol, we write the following:

```
  secrecy_of SK2
  secrecy_of CK1
  secrecy_of IK1
```

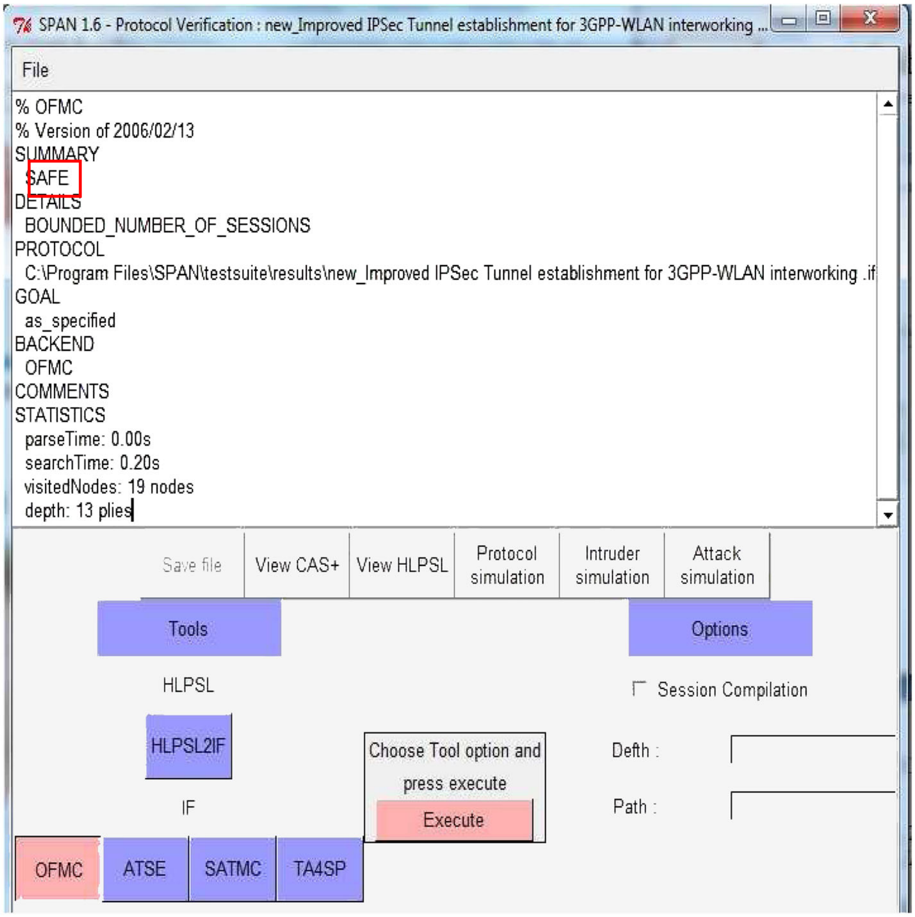
DOI: 10.1002/dac



```
(role_UE, 5) -> (role_EPDG, 4) : {exp(G,X)
(role_EPDG, 4) -> (role_UE, 5) : {exp(G,Y)
(role_UE, 5) -> (role_EPDG, 4) : {IDUE.IDE
(role_EPDG, 4) -> (role_AAASERVER, 3)
(role_AAASERVER, 3) -> (role_EPDG, 4)
(role_EPDG, 4) -> (role_UE, 5) : {IDEPDG.
(role_UE, 5) -> (role_EPDG, 4) : {F2(K1.R/
(role_EPDG, 4) -> (role_AAASERVER, 3)
(role_AAASERVER, 3) -> (role_EPDG, 4)
(role_EPDG, 4) -> (role_UE, 5) : {Success
(role_UE, 5) -> (role_EPDG, 4) : {F(PRF(S
(role_EPDG, 4) -> (role_UE, 5) : {H(PKUE)
```

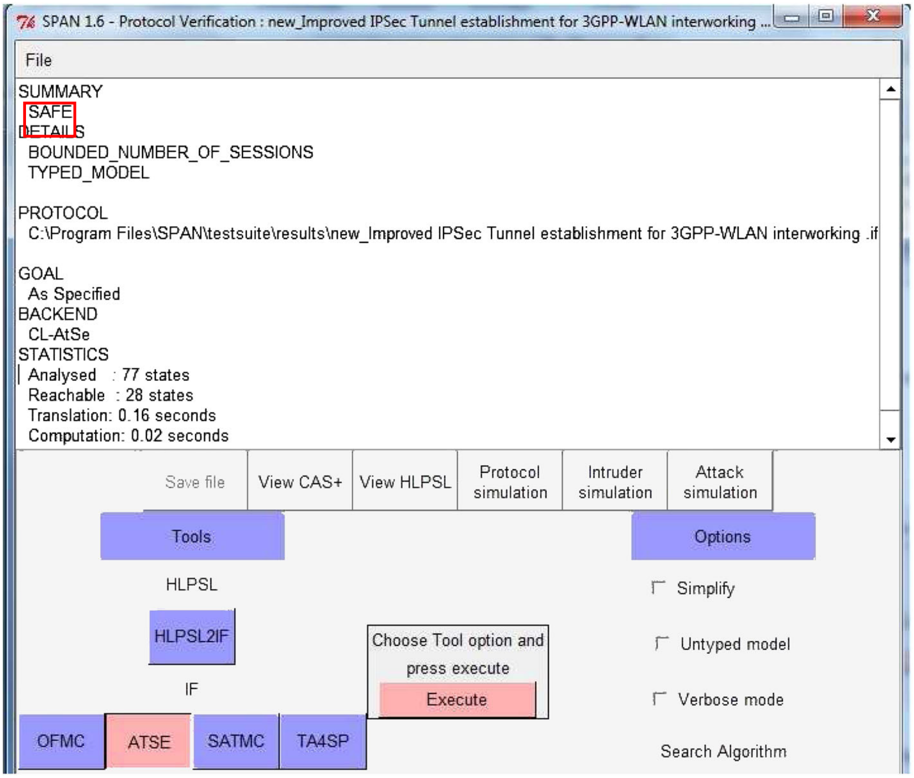
```
{exp(nonce-1,nonce-2)}_pk-3.{nonce-5}_pk-3.h(pk-4).{h(exp(nonce-1,nonce-2).nonce-5.h(p
{exp(nonce-1,nonce-7)}_pk-4.{nonce-8}_pk-4.h(pk-3).nonce-6.{h(exp(nonce-1,nonce-7).nonce-8.h(p
{nonce-11.nonce-10.h(pk-4).h(pk-3).nonce-9}_exp(exp(nonce-1,nonce-7),nonce
{nonce-11.nonce-10}_sk-12
nce-15).hmac(sha1(nonce-11.const_1(sk-14.nonce-15).const_1(sk-14.nonce-15)).nonce-15.{nonce-
).const_1(sk-14.nonce-13.nonce-15).hmac(sha1(nonce-11.const_1(sk-14.nonce-15).const_1(sk-14.
ce-15).hmac(sha1(nonce-11.const_1(sk-14.nonce-15).const_1(sk-14.nonce-15)).const_1(sk-14.non
1(nonce-11.const_1(sk-14.nonce-15).const_1(sk-14.nonce-15)).const_1(sk-14.nonce-15))}_sk-12
_1(sha1(nonce-11.const_1(sk-14.nonce-15).const_1(sk-14.nonce-15)))}_sk-12
{nonce-16.const_1(sha1(nonce-11.const_1(sk-14.nonce-15).const_1(sk-14.nonce-15)))}_exp(exp(nc
ha1(nonce-11.const_1(sk-14.nonce-15).const_1(sk-14.nonce-15))).exp(nonce-1,nonce-2).nonce-5.nc
nst_1(sha1(nonce-11.const_1(sk-14.nonce-15).const_1(sk-14.nonce-15))).exp(nonce-1,nonce-7).no
```

Figure 4. Animation of HLPSL specification with SPAN.



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  C:\Program Files\SPAN\testsuite\results\new_Improved IPSec Tunnel establishment for 3GPP-WLAN interworking .if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.20s
  visitedNodes: 19 nodes
  depth: 13 plies
```

Figure 5. Message returned by SPAN for the improved IPSec tunnel establishment with OFMC.



SPAN 1.6 - Protocol Verification : new_Improved IPSec Tunnel establishment for 3GPP-WLAN interworking ...
File

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  C:\Program Files\SPAN\testsuite\results\new_Improved IPSec Tunnel establishment for 3GPP-WLAN interworking .if

GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed   : 77 states
  Reachable  : 28 states
  Translation: 0.16 seconds
  Computation: 0.02 seconds
```

Figure 6. Message returned by SPAN for the improved IPSec tunnel establishment with CL-AtSe.

8.3. *Verifying the improved IPSec tunnel establishment*

We check the specification by the SPAN. For our verification, we have used the OFMC and the CL-AtSe back-end to search for the attacks on the improved IPSec tunnel establishment.

The output gives details about whether the specification is safe or not. If not, then it also gives the trace of the attack found, to indicate secrecy attack or authentication attack. So even though many properties of the protocol are to be checked, only few can be verified using SPAN.

Only authentication and secrecy goals are supported by AVISPA and SPAN. Figure 4 presents the animation of HLPSL specification with SPAN.

As already mentioned, the improved IPSec tunnel establishment was tested using OFMC and CL-AtSe verification techniques, which assured its security. No attacks or vulnerabilities were found.

Figures 5 and 6 demonstrate the messages returned by OFMC and CL-AtSe, respectively.

As shown in the two figures, the proposed solution is safe to use, and no attacks were found.

9. CONCLUSION AND PERSPECTIVES

The interworking between 3GPP/LTE and WLAN network allows users to benefit from many features that exist in both technologies. However, securing this interworking is a great challenge. Therefore, it has been investigated by researchers. In this article, first, we have focused on securing interworking at the network layer by the establishment of an improved IPSec tunnel between them handled by HIP_IKEv2 protocol to guarantee stranger security properties. Second, we have extended HIP_IKEv2 to HIP_MOBIKEv2 in case of mobility events (handover) in order to reduce the authentication signaling traffic.

The security of the improved IPSec tunnel establishment was verified by AVISPA and SPAN. When our protocol was tested, we found it is resistant to MITM attack, anti-replay attack, and DoS prevention. Future works will be focused on trying to give solution against some other types of attacks such as connection hijacking or impersonation, and trying to give solution for securing new mobility management protocols, such as FHMIPv6 and PMIPv6.

REFERENCES

1. Zarai F, Daly I, Obaidat MS, Kamoun L. Secured and fast handoff in wireless mesh networks. *Security and Communication Networks* 2013; **6**(5):644–657.
2. Perkins C. Mobile networking through Mobile IP. *IEEE Internet Computing* 1998; **2**(1):58–69.
3. Hamad H, Abudalfa S, Sahmoud S. Adaptive mobility management scheme for Mobile IP using ad hoc networks. *International Arab Journal of e-Technology* 2011; **2**(2):65–71.
4. Perkins C. IP mobility support for IPv4. *IETF RFC 3344*, August 2002. (Available from: http://www.ietf.org/rfc/rfc3344) [accessed date January 2013]
5. Johnson D, Perkins C, Arkko J. Mobility support in IPv6. *IETF RFC 3775*, June 2004. (Available from: http://www.ietf.org/rfc/rfc3775) [accessed date January 2013]
6. Cabellos-Aparicio A, Serral-Gracià R, Jakab L, Domingo-Pascual J. Measurement based analysis of the handover in a WLAN MIPv6 scenario. *6th international conference on Passive and Active Network Measurement*, Boston, April 2005; 203–214.
7. Smaoui S, Zarai F, Kamoun L. IPSec tunnel establishment for 3GPP–WLAN interworking. *8th International Conference on Informatics and Systems (INFOS)*, Cairo, May 2012; 74–80.
8. Allard F, Bonnin J. An application of the Context Transfer Protocol: IPSec in a IPv6 mobility environment. *International Journal of Communication Networks and Distributed Systems* 2008; **1**:110–126.
9. Obaidat MS, Boudriga N. *Security of e-Systems and Computer Networks*. Cambridge University Press: The Edinburgh Building, Cambridge CB2 8RU, UK, 2007.
10. Kaufman C, Hoffman P, Nir Y, Eronen P. Internet Key Exchange protocol Version 2 (IKEv2). *IETF RFC5996*, September 2010. (Available from: http://www.ietf.org/rfc/rfc5996.txt) [accessed date December 2012]
11. Nan L. Research on Diffie–Hellman key exchange protocol. *2nd International Conference on Computer Engineering and Technology*, Chengdu, April 2010; 634–637.
12. Eronen P. IKEv2 Mobility and Multihoming Protocol (MOBIKE). *IETF RFC 4555*, June 2006. (Available from: http://www.ietf.org/rfc/rfc4555.txt) [accessed date December 2012]
13. Smaoui S, Zarai F, Obaidat M, Hsiao KF, Kamoun L. HIP_IKEv2: a proposal to improve Internet Key Exchange protocol-based on Host Identity Protocol. *3rd International Conference on Simulation and Modeling Methodologies, Technologies and Applications (SIMULTECH)*, Iceland, July, 2013.
14. Henderson T, Gurtov A. The Host Identity Protocol (HIP) experiment report. *IETF RFC6538*, March 2012. (Available from: http://www.rfc-base.org/txt/rfc-6538.txt) [accessed date June 2013]
15. Arraez L, Chaouchi H, Gurkas Aydin Z. Performance evaluation and experiments for Host Identity Protocol. *International Journal of Computer Science Issues (IJCSI)* 2011; **8**(2):74–83.
16. AVISPA: Automated Validation of Internet Security Protocols and Applications. FET Open Project IST-2001-39252, 2003. (Available from: http://www.avispa-project.org/) [accessed date September 2013]
17. Glouche Y, Genet T, Heen O, Courtay O. A security protocol animator tool for AVISPA. *ARTIST2 Workshop on Security Specification and Verification of Embedded Systems*, Pisa, May 2006.
18. Sanguankotchakorn T, Jaiton P. Effect of triangular routing in Mixed IPv4/IPv6 networks. *Seventh International Conference on Networking*, Cancun, April 2008; 357–362.
19. Doja M, Saggar R. Analysis of token based Mobile IPv6 and standard Mobile IPv6 using CPN tool. *International Journal of Advanced Research in Computer Science and Software Engineering* 2012; **2**(7):125–131.
20. Zhou H, Zhang H, Qin Y, Wang H-C, Chao H-C. A proxy Mobile IPv6 based global mobility management architecture and protocol. *Mobile Networks and Applications* 2010; **15**(4):530–542.
21. Chen Y-C, Yang F-C. An efficient MIPv6 return routability scheme based on geometric computing. *International Journal of Electrical and Information Engineering* 2009; **3**(8):477–482.
22. Moravejosharieh A, Modares H, Salleh R. Overview of Mobile IPv6 security. *Third International Conference on Intelligent Systems Modelling and Simulation*, Malaysia, February 2012; 584–587.
23. Celentano D, Fresa A, Longo M, Postiglione F, Robustelli AL. Secure Mobile IPv6 for B3G networks. *International Conference on Software in Telecommunications and Computer Networks*, Croatia, October 2006; 331–335.
24. Giaretta G, Guardini I, Demaria E, Bournelle J, Lopez R. Authentication, Authorization, and Accounting (AAA) goals for Mobile IPv6. *IETF RFC 5637*, September 2009. (Available from: http://www.rfc-base.org/txt/rfc-5637.txt) [accessed date March 2013]
25. Ehmke M, Forsgren H, Grahn K, Karlsson J, Karvi T, Pulkkis G. Securing control signaling in Mobile IPv6 with identity-based encryption. *Academic journal article, Issues in Informing Science and Information Technology* 2009; **6**:649–667.
26. Housley R, Moore T. Certificate extensions and attributes supporting authentication in Point-to-Point Protocol (PPP) and wireless local area networks (WLAN). *IETF RFC 4334*, February 2006. (Available from: http://www.rfc-editor.org/rfc/rfc4334.txt) [accessed date April 2013]
27. Lee S. Transport Layer Security (TLS) implementation for secured MN-HA communication in Mobile IPv6. *International Journal of Future Generation Communication and Networking* 2011; **4**(3):119–126.

DOI: 10.1002/dac

28. Zarai F, Daly I, Kamoun L. Secured interworking and roaming between 3GPPLTE and wireless local mesh networks. *(IJCNS) International Journal of Computer and Network Security* 2010; **2**(7):75–85.
29. Arkko J, Haverinen H. Extensible authentication protocol method for 3rd Generation Authentication and Key Agreement (EAP-AKA). *IETF RFC 4187*, January 2006. (Available from: http://www.rfc-base.org/txt/rfc-4187.txt) [accessed date December 2012]
30. 3GPP Technical Specification Group Services and System Aspects. 3GPP System Architecture Evolution (SAE); security aspects of non-3GPP accesses. *TS 33.402 (v8.6.0), Release 8*, December 2009.
31. Armando A, Basin D, Boichut Y, Chevalier Y, Compagna L, Cuellar J, Hankes Drielsma P, Heám PC, Kouchnarenko O, Mantovani J, Mödersheim S, von Oheimb D, Rusinowitch M, Santiago J, Turuani M, Viganò L, Vigneron L. The AVISPA tool for the Automated Validation of Internet Security Protocols and Applications. *17th International Conference Computer Aided Verification (CAV)*, Scotland, 2005; 281–285.
32. Glouche Y, Genet T. SPAN—a security protocol animator for AVISPA—user manual. IRISA/Université de Rennes 1, span, 2006. (Available from: http://www.irisa.fr) [accessed date September 2013]
33. Cheminod M, Bertolotti IC, Durante L, Sisto R, Valenzano A. Tools for cryptographic protocols analysis: a technical and experimental comparison. *Computer Standards & Interfaces* 2009; **31**(5):954–961.
34. Lafourcade P, Terrade V, Vigier S. Comparison of cryptographic verification tools dealing with algebraic properties. *Sixth International Workshop on Formal Aspects in Security and Trust (FAST)*, Netherlands, November 2009.
35. Lim S, Bang K, Yi O, Lim J. A secure handover protocol design in wireless networks with formal verification. *5th International Conference, Wired/Wireless Internet Communications (WWIC)*, Berlin Heidelberg, May 2007; 67–78.
36. Dolev D, Yao A. On the security of public key protocols. *IEEE Transactions on Information Theory* 1983; **29**(2):350–357.

DOI: 10.1002/dac