J Supercomput (2014) 70:1036–1050
DOI 10.1007/s11227-013-1080-y

Design and analysis of secure host-based mobility protocol for wireless heterogeneous networks

**Imen El Bouabidi · Faouzi Zarai ·
Mohammad S. Obaidat · Lotfi Kamoun**

Published online: 21 January 2014

Abstract Mobility protocols allow hosts to change their location or network interface while maintaining ongoing sessions. While such protocols can facilitate vertical mobility in a cost-efficient and access agnostic manner, they are not sufficient to address all security issues when used in scenarios requiring local mobility management. In this paper, we propose a new scheme that makes Host Identity Protocol (HIP) able to serve as an efficient and secure mobility protocol for wireless heterogeneous networks while preserving all the advantages of the base HIP functions as well. Our proposal, called Heterogeneous Mobility HIP (HMHIP), is based on hierarchical topology of rendezvous Servers (RVSs), signaling delegation, and inter-RVS communication to enable secure and efficient network mobility support in the HIP layer. Formal security analysis using the AVISPA tool and performance evaluation of this method are provided; they confirm the safety and efficiency of the proposed solution. HMHIP reduces handover latency and packet overhead during handovers by achieving registration locally.

Keywords Component · Mobility · Host identity protocol · Rendezvous server · Security · Reply

I. El Bouabidi · F. Zarai (✉) · L. Kamoun
University of Sfax, Sfax, Tunisia
e-mail: faouzifbz@gmail.com; faouzi.zarai@isecs.rnu.tn

I. El Bouabidi
e-mail: imen_bouabidi@yahoo.fr

M. S. Obaidat
Monmouth University, Monmouth, USA
e-mail: msobaidat@gmail.com

M. S. Obaidat
Khalifa University, Abu Dhabi, UAE

1 Introduction

The rapid growth of diverse wireless communication networks, each with its own unique characteristics, led to proliferation of the wireless heterogeneous network concept. Mobility management emerges as one of the most important and challenging problems for wireless mobile communication over the Internet. Mobility and multihoming protocols allow hosts to change their location or network interface while maintaining ongoing sessions. Mobile Nodes (MNs) may move locally within one domain or extend their movements outside their domains. Mobility management protocols in the new generation of wireless networks can be broadly classified into two categories:

- Network-based mobility: The network detects the node mobility and initiates the required mobility signals. Example is Proxy Mobile IPv6 (PMIPv6) [1].
- Host-based mobility: It permits the MN to directly update the Correspondent Node (CN), when it has changed its IP address. In response, the CN sends its packets to MN's new address. Some host-based protocols support multihoming scenarios, where the host announces multiple IP addresses to its CNs as alternative routing paths. The protocols of this category are inherently less secure because trust relationships are usually unavailable to protect the mobility signaling messages. Examples include the Host-Identifier Protocol (HIP) [2], Stream Control Transmission Protocol (SCTP) [3], and SHIM6 [4].

Multihoming and mobility affect the security of transport protocols in several ways. First, existing security mechanisms are often based on implicit assumptions of a static network topology and unchanging addresses. When the assumptions are invalidated, the existing security mechanisms may become ineffective. Second, it is possible to misuse mobility signaling. Potential attacks include denial of service by preventing legitimate communication, connection hijacking, spoofing and intercepting data, and redirecting packet flows to the target of a flooding attack [5].

The available mechanisms to protect against such redirection attacks depend on the mobility technology. The current mobility standards such as long-term evolution (LTE) [6] and WiMAX use network-based mobility. These technologies employ network-side anchors to relay all traffic between the mobile node and its peers. Since the mobility-related signaling is exchanged between MN and the network, it can be secured using trust relation handovers that exist between subscriber and service provider. Since host-based mobility protocols are applied by the end nodes of traffic connections, trust relation handovers are usually unavailable to protect the mobility-related signaling messages. Therefore, many protocols [7–16] have pursued methods of weak authentication, inefficient routing, overhead, and lack of multihoming support.

In this article, we propose a new scheme that makes Host Identity Protocol (HIP) able to serve as an efficient and secure mobility/multihoming protocol for wireless heterogeneous networks while preserving all the advantages of the base HIP functions as well. Our proposal is based on hierarchical topology of Rendez-vous servers (RVSs) [17], signaling delegation, and inter-local RVS (LRVS) communication to enable secure and efficient network mobility support in the HIP layer.

The rest of the article is organized as follows. Section 2 discusses mobility and security solutions. Section 3 presents our solution to secure host-based mobility protocol and keep network performance at optimum levels. In Sect. 4, the evaluation results based on qualitative metrics is presented. The handover latency and overhead metrics are used to compare the proposed protocol HMHIP and the basic HIP specification. Section 5 provides the results of the security analysis. The conclusion in Sect. 6 summarizes the work.

2 Mobility and security solutions

2.1 Host Identity Protocol and attacks

The Host Identity Protocol (HIP) is a multi addressing and mobility solution for the IPv4 and IPv6 Internet [2,9]. It is proposed within the Internet Engineering Task Force (IETF) to separate the host identity and location identity. The IP address will continue to be the location identity, while HIP will carry the host identification function. HIP is also a security protocol that defines host identifiers for naming the endpoints and performs authentication and creation of IPSec security associations between them. A new protocol layer is added into the TCP/IP stack between the network and transport layers.

Figure 1 shows the four-way handshake between two hosts wanting to start communication. This is called HIP Base Exchange. First, the client sends a request to the server, asking to establish an association. The request contains the Host Identifier Tags of the Initiator (HIT$_I$) and the Host Identifier Tags of the Initiator (HIT$_R$). In response, the server initiates a Diffe-Hellman key exchange, conducted in the second (R1) and third packets (I2). R1 contains the HIT$_I$, the HIT$_R$, the puzzle (a cryptographic challenge that the Initiator must solve and display the solution in the packet I2), the Responder's Diffie-Hellman key (DH$_R$), the Responder host identity HI$_R$ (i.e., a public key), the proposed cryptographic algorithms for the rest of the base exchange (HIP transforms) and the proposed IPsec algorithms (ESP transforms). All the fields, except HIT$_I$ and the puzzle, are protected by the signature. On receiving R1, the initiator solves the puzzle and creates the message I2. I2 includes the puzzle solution, the Initiator's Diffie-Hellman key (DH$_I$), the HIP and ESP transforms proposed by the Initiator, a security parameter index (SPI) for the Responder-to-Initiator IPsec SA (SPI$_I$), and the Initiator public key (HI$_I$) encrypted using the new session key. The R2

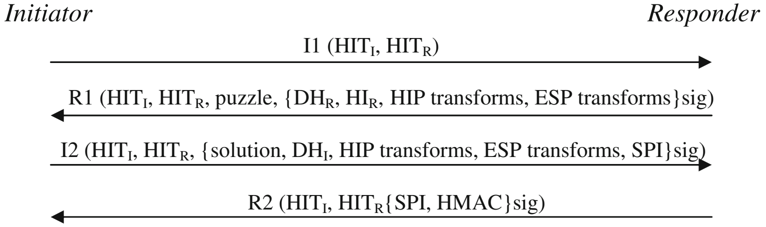

Initiator
Responder
I1 (HIT$_I$, HIT$_R$)
R1 (HIT$_I$, HIT$_R$, puzzle, {DH$_R$, HI$_R$, HIP transforms, ESP transforms}sig)
I2 (HIT$_I$, HIT$_R$, {solution, DH$_I$, HIP transforms, ESP transforms, SPI}sig)
R2 (HIT$_I$, HIT$_R${SPI, HMAC}sig)

Fig. 1 HIP base exchange

packet finalizes the base exchange. R2 contains the SPI for the Initiator-to-Responder IPsec SA (SPI_R), an HMAC computed using the session key, and a signature.

Rendezvous servers improve reachability and operation when HIP nodes are multihomed or mobile by providing a mechanism to locate a host, for example, when two communicating hosts move simultaneously. To employ a rendezvous mechanism, a host first must perform a registration procedure, which is an extended version of the HIP base exchange.

Although HIP provides the best performance, it is vulnerable to various security attacks [8,9]:

- Replays of R1 message: As explained earlier, R1 is partially signed. There is, however, nothing in R1 to prove its freshness.
- Denial of service (DoS): Attacker can replay the signed parts of R1 and trick the Initiator into solving the wrong puzzle. This results in denial of service for the Initiator because the solution is rejected by the Responder.
- Man in the middle (MiTM): Also the rendezvous server may be attacked from many directions. For example, if the computer where the RVS is running is compromised, the malicious administrator can insert harmful data, which enable MiTM and DoS among others.

2.2 Security solutions

Since many protocols on host-based mobility or multihoming have been proposed, a large number of security solutions are available. The following security methods have been applied:

- Strong authentication through pre-shared keys or PKI using trust relation handovers [10,11],
- Session key establishment through Diffie-Hellman exchange [12],
- Weak authentication using random numbers (nonce, cookie, …) [13–15],
- Routability test using challenge/response based on random numbers [16].

Methods of strong authentication are enforced by HIP through the use of Public Key Infrastructure (PKI) and by SHIMv6 via cryptographically generated addresses (CGA) [10] or Hash-Based Addresses (HBA) [11]. Strong authentication is considered cryptographically secure and it protects against redirection attacks. However, it relies on the mutual trust relation handovers between MN and CN as prerequisite, which is usually not available.

The MAST protocol [12] proposes key establishment through elliptic-curve Diffie-Hellman (DH) exchange. The DH key exchange is vulnerable to man-in-the-middle attacks. Also, it demands substantial processing efforts on each host at session beginning. This can become a burden for many mobile devices that have limited processing capabilities.

References [13–15] combine methods of weak authentication with proof of session owner handover. The protection such random identifiers provide can be easily broken through eavesdropping. This allows an adversary to forge Binding update messages for the purpose of interruption or hijacking of traffic connections.

Routability test using challenge/response based on random numbers [16] allows the attacker to receive the challenge and respond on behalf of the victim while spoofing the victim's IP address.

Indeed, these works attempt to improve the performance of the suggested mobility protocols without taking into consideration the level of confidence relation between different technologies from the networks. They have pursued methods of weak authentication, inefficient routing, overhead, and lack of multihoming support. Consequently, our study is characterized by a high level of security without quality of service degradation.

3 Proposed Heterogeneous Mobility HIP Protocol (HMHIP)

To enable the integration of heterogeneous networking technologies into common system architecture a secured mobility protocol is required. In this section, we present the proposed protocol to secure a heterogeneous Mobility HIP protocol, called (HMHIP). It involves a sequence of messages being exchanged between the Mobile Node, the visited network and the home network.

In the proposed protocol, we assume the following:

Each mobility session defines at least one Mobility Association (MA), which is owned by one of the two hosts and provides this host with mobility support.

In case both hosts are mobile, each of them has to support its own MA within the same mobility session.

3.1 The Proposed Heterogeneous Mobility HIP Architecture

In this article, we choose the hierarchical architecture as being the most adapted approach for the study of mobility as well as security. The hierarchical architecture is characterized by the use of a hierarchical function for mobility management. Figure 2 illustrates a general architecture for HMHIP.

In our hierarchical architecture, the network is divided into Radio Access Networks (RANs). For each RAN, we select a unique LRVS to manage Mobile Nodes in the given LRVS entities which serve as gateways, while using functions similar to RVSs [17]. They provide registration service for MNs in a well-defined RAN. Every MN can register its locally valid IP address (referred as local IP address or IP_L in the rest of this article) at the LRVS. The LRVS maps the local IP address of the MNs to a globally routable address (IP_G). This network's decomposition is used to facilitate the study of stations' mobility.

3.2 Initiation mechanism

If a mobile node joins a new RAN, it physically connects to one of the access routers (AR) of the RAN. Right after detecting the newly established physical connection and getting a serviceable IP address (IP_L), the MN activates the HIP service discovery procedure [18] to detect the visited LRVS (vLRVS) service provided in the visited RAN. The HMHIP steps are described in the following (see Fig. 3).

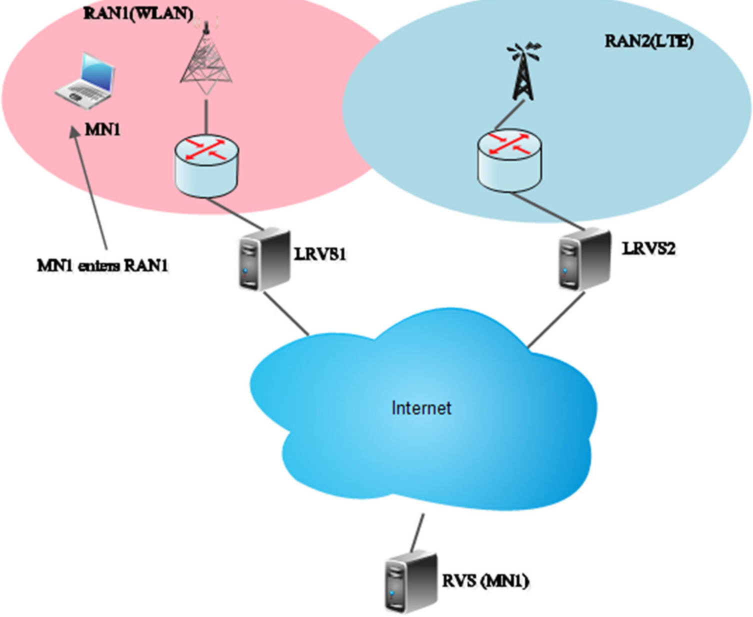


Fig. 2 The architecture of HMHIP

1. The MN starts the Handover Base Exchange by sending the message $I1$ to its RVS and current correspondent nodes (CNs) in order to be reachable for the current and future communication. The $I1$ message contains the local IP address (IP_L), IP address of RVS (IP_{RVS}),nonce N_{MN},Host Identifier Tags of the MN and CN (HIT_{MN}, HIT_{CN}), and *token*. The nonce N_{MN} is added to be used by $R1$ to prove its freshness. The token is used to secure the message $I1$ from the replay and hijacking attacks and to delegate the signaling rights to the vLRVS at which it is registered. In possession of this delegation, the vLRVS is able to securely register or update the RVSs and CNs on behalf of the MNs with IP_G assigned to them. The parameter Time to Live (TL) is added to the token in order to specify its time to live.
2. When a visited local RVS (vLRVS) receives an $I1$ whose destination HIT is not its own, it verifies the $I1$ source HIT and adds its IP address (IP_G) and forwards the message to the RVS of the MN.
3. When a rendezvous Server receives an $I1$ whose destination *HIT* is not its own, it consults its registration database to find a registration for the rendezvous service established by the *HIT* owner. If it finds an appropriate registration, it relays the packet to the registered IP address. If it does not find an appropriate registration, it drops the packet.
4. Once the $I1$ message is received, CN completes the $R1$ with the HIT_{MN} received in the $I1$ and a *PUZZLE* field whose level of difficulty will be adjusted based on level of trust on the MN. Besides the puzzle, $R1$also contains HI$_R$, Diffie-Hellman parameters (DH_R and HIP transforms, ESP transforms) and its signature. When a

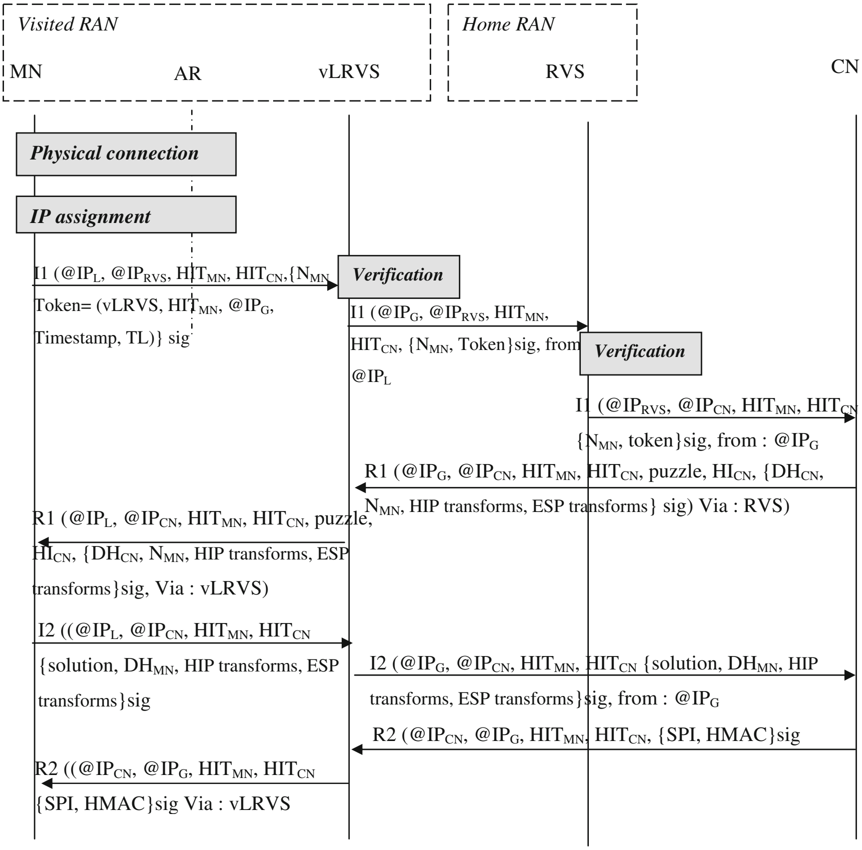

Visited RAN
Home RAN
MN
AR
vLRVS
RVS
CN
Physical connection
IP assignment
I1 (@IP$_L$, @IP$_{RVS}$, HIT$_{MN}$, HIT$_{CN}$,{N$_{MN}$
Token= (vLRVS, HIT$_{MN}$, @IP$_G$,
Timestamp, TL)} sig
Verification
I1 (@IP$_G$, @IP$_{RVS}$, HIT$_{MN}$,
HIT$_{CN}$, {N$_{MN}$, Token}sig, from
@IP$_L$
Verification
I1 (@IP$_{RVS}$, @IP$_{CN}$, HIT$_{MN}$, HIT$_{CN}$
{N$_{MN}$, token}sig, from : @IP$_G$
R1 (@IP$_G$, @IP$_{CN}$, HIT$_{MN}$, HIT$_{CN}$, puzzle, HI$_{CN}$, {DH$_{CN}$,
N$_{MN}$, HIP transforms, ESP transforms} sig) Via : RVS)
R1 (@IP$_L$, @IP$_{CN}$, HIT$_{MN}$, HIT$_{CN}$, puzzle,
HI$_{CN}$, {DH$_{CN}$, N$_{MN}$, HIP transforms, ESP
transforms}sig, Via : vLRVS)
I2 ((@IP$_L$, @IP$_{CN}$, HIT$_{MN}$, HIT$_{CN}$
{solution, DH$_{MN}$, HIP transforms, ESP
transforms}sig
I2 (@IP$_G$, @IP$_{CN}$, HIT$_{MN}$, HIT$_{CN}$ {solution, DH$_{MN}$, HIP
transforms, ESP transforms}sig, from : @IP$_G$
R2 (@IP$_{CN}$, @IP$_G$, HIT$_{MN}$, HIT$_{CN}$, {SPI, HMAC}sig
R2 ((@IP$_{CN}$, @IP$_G$, HIT$_{MN}$, HIT$_{CN}$
{SPI, HMAC}sig Via : vLRVS

Fig. 3 Initiation mechanism in the proposed protocol

CN replies to an $I1$ relayed via an RVS, it will append to the regular $R1$ header a *Via RVS* parameter containing the IP addresses of the traversed RVS's.

5. Then, the RVS sends the $R1$ message to the IP_G address.
6. After that, the MN continues the service discovery by completing the registration with the final $I2 - R2$ sequence.

3.3 Handovers management

3.3.1 Intra-domain handover procedures

If a mobile node which had performed the initialization mechanism, moves to a new RAN of the same vLRVS, after receiving the IP$_L$ from the new serving AR, it simply updates its registration with its new local IP address at the new vLRVS. The intra-domain handovers are hidden from the outside world in order to keep network performance at optimum levels (handover latency, signaling overhead and packet loss rate).

3.3.2 Inter-domain handover procedures

While MN changes its old LRVS, it has to update its RVS and all the correspondent nodes with ongoing communication. The first thing to do is to update the old LRVS to make it able to forward packets sent to the MN's old globally routable IP address as long as the MN has not finished updating the RVS and all of its CNs. After the old LRVS is updated, MN updates its CNs and at last the RVS. When the MN finishes all of the required updates [19], it removes the registration association at the old LRVS.

4 Performance analysis

To evaluate performance of our proposed protocol, we have used the network simulator developed using Java language [20]. The simulated network is depicted in Fig. 4. It is composed of two networks LTE and WLAN.

In our simulation, the number of stations in WLAN networks is fixed to 200 and their positions are uniformly distributed in nine APs at the starting time of simulation. The number of MNs in LTE cell is not fixed. APs receive handover arrivals from LTE cell according to Poisson process with mean rate λ_h. The mobility model is considered as random-walk model in which the MN initially chooses a speed that is uniformly distributed over interval [0, 4 km/h]. It also chooses a direction for motion, which is uniformly distributed over [0, 360]. Service requests arrive at eNB as Poisson processes with parameter λ_n and service time is determined by an exponential distribution with mean $1/\mu_n$. Two types of flows were used in the simulations: voice over IP and data flows. The parameter settings in our simulation are listed in Table 1.

The two most important metrics which can measure the performance are:

Fig. 4 The simulated network

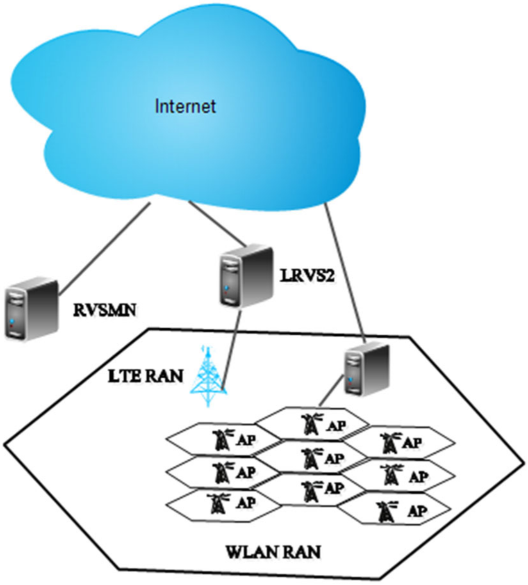


Table 1 General simulation parameters

Parameters	Values
Number of APs	9
Border covered by AP	100 m
Border covered by eNodeB	500 m
Velocity of UEs	4Km/h
Max eNodeB transmit power	46 dbm
Handover arrivals from LTE cell(λ_h): VoIP; data	1 call/h/user; 1 calls/h/user
WlAN IEEE 802.11n data rate	100 Mbps (Frequency band 2.4 GHZ)
Packet size: Voip; data	120 bytes; 1,500 bytes
New call rate (λ_n): VoIP; data	2 call/h/user; 2 calls/h/user
Average connection holding time: voice; data	3 min; 9 min

1. Handover latency: We define the handover latency as the amount of time measured from the moment when the MN disconnected from the old AR to the moment when it receives the first packet from the new AR. This metrics can be seen as the aggregation of the following delays:
   (a) The delay of IP assignment in the visited RAN,
   (b) The transmission delay, and
   c) The delay of the signature verification operation, which is done on LRVS and RVS servers.
2. The overhead that is induced on the network by requests and responses. These metrics are mainly dependent on the number of registration requests by mobiles.

Figures 5 and 6 show the influence of our proposed protocol (HMHIP) and of the HIP protocol on handover latency. We notice that handover latency increases when the number of terminals increases in the WLAN system.

The basic HIP specification performs very bad in intra-RAN, which proves that our proposal extremely reduces the latency by 50 % during intra-RAN handovers. This can be justified by the fact that in basic HIP mobility the RVS and all the CNs must be updated after every AR change, while in case of HMHIP only the LRVS should be informed about the fact of intra-RAN handovers.

Figure 7 shows that the HMHIP performance in terms of overhead was very close to that of the basic HIP specification. The number of messages exchanged using our solution HMHIP is 30 % less than that of HIP.

During intra-RAN handovers, HMHIP has lower overhead than the basic HIP specification. This can be justified by the fact that in basic HIP mobility the RVS and all the CNs must be updated after every AR change, while in case of HMHIP only the LRVS should be informed about the fact of intra-RAN handovers. However, during inter-RAN handover, HMHIP has more overhead than the basic HIP specification. In fact, when an inter-RAN handover occurs, an additional registration is needed and there is a need to update both the new LRVS, and the old LRVS.

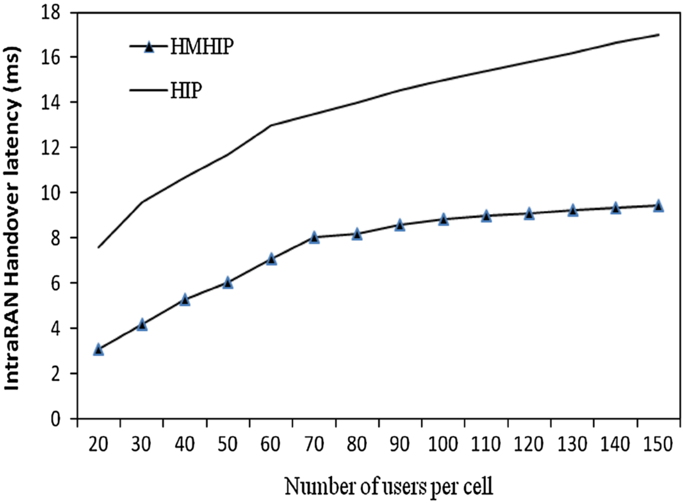


Fig. 5 Intra RAN handover latency

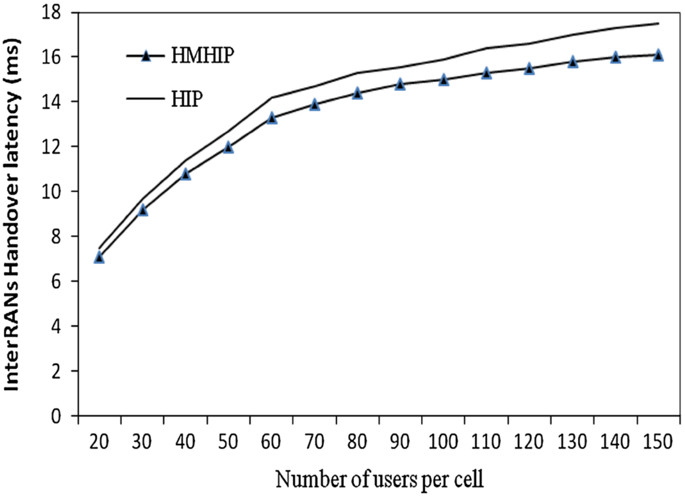


Fig. 6 Inter RANS handover latency

5 Security validation

It can be deduced that HMHIP outperforms the existing approaches at the security level. In fact, many attacks are possible. In the basic HIP specification, attacker can replay the signed parts of R1 and trick the MN into solving the wrong puzzle. This results in denial-of-service for the MN because the solution is rejected by the CN. In our proposed HMHIP protocol, R1 can prove its freshness by adding a nonce of the MN to I1 and to the unsigned part of R1.

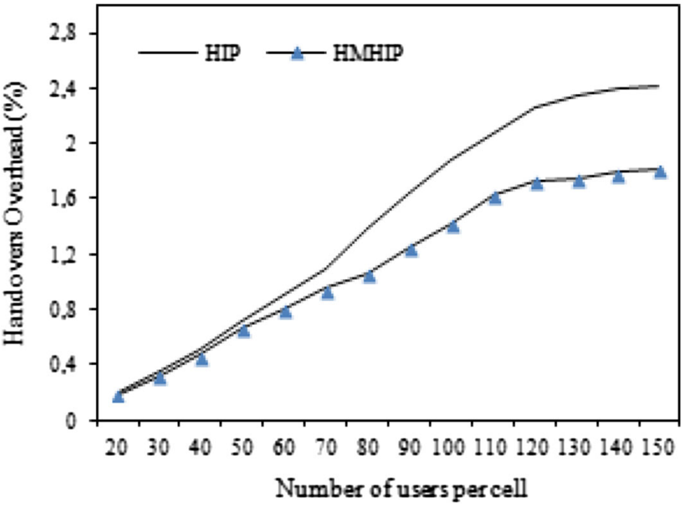


Fig. 7 Handover overhead

Furthermore, the security strength of the proposal is derived from the generic security provided by HIP. In the current Internet where hosts are identified according to their IP addresses, the true advantage we get from HIP is a strong identification based on the public key cryptography. HIP enabled hosts can prove their identity by owning the private key part of their asymmetric Host Identity and signing data with it. With cryptographical identities, HIP enables authentication between end-points. Also, in our proposed HMHIP protocol, we have used the message token which prove the delegation of signaling rights of the MN to the LRVS at which it is registered.

To verify the security protocol, we tested our protocol using the software SPAN Security Protocol ANimator for AVISPA [21]. The first step of the verification consists of modeling the HMHIP using HLPSL formal language of AVISPA. In our HLPSL specification, we defined four basic roles: the MN, LRVS, RVS, and CN. Each of these roles implements its related part of Secure HIP. The simulation of HMHIP is given by Fig. 8.

To make AVISPA tool search for an attack, we have introduced a goals section to define security goals (see Fig. 9):

The security properties defined in the goals section can be divided into:

- Authentication goals (MN/CN, MN/LRVS, MN /RVS).
- The secrecy of the shared key goal.

The first line of the goal section is a command that makes AVISPA tool look for an authentication attack for the witness-request pair defined by constant *auth_1*. The related request goal fact is included in role MN in the transition where the puzzle is received from the CN. The matching witness predicate is in role CN (see Fig. 11) as part of the transition where the signed solution (SPUZZLE) is sent to the MN (see Fig. 10).

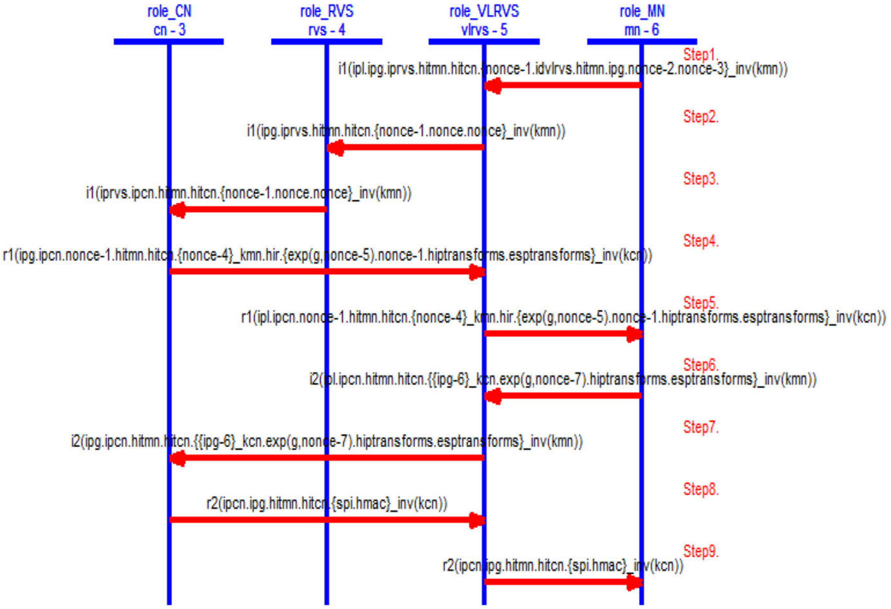
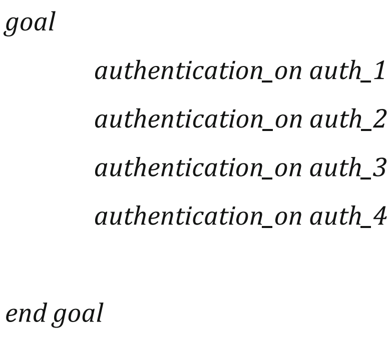

role_CN
cn - 3
role_RVS
rvs - 4
role_VLRVS
vlrvs - 5
role_MN
mn - 6
Step1.
i1(ipl.ipg.iprvs.hitmn.hitcn.{nonce-1.idvlrvs.hitmn.ipg.nonce-2.nonce-3}_inv(kmn))
Step2.
i1(ipg.iprvs.hitmn.hitcn.{nonce-1.nonce.nonce}_inv(kmn))
Step3.
i1(iprvs.ipcn.hitmn.hitcn.{nonce-1.nonce.nonce}_inv(kmn))
Step4.
r1(ipg.ipcn.nonce-1.hitmn.hitcn.{nonce-4}_kmn.hir.{exp(g,nonce-5).nonce-1.hiptransforms.esptransforms}_inv(kcn))
Step5.
r1(ipl.ipcn.nonce-1.hitmn.hitcn.{nonce-4}_kmn.hir.{exp(g,nonce-5).nonce-1.hiptransforms.esptransforms}_inv(kcn))
Step6.
i2(ipl.ipcn.hitmn.hitcn.{{ipg-6}_kcn.exp(g,nonce-7).hiptransforms.esptransforms}_inv(kmn))
Step7.
i2(ipg.ipcn.hitmn.hitcn.{{ipg-6}_kcn.exp(g,nonce-7).hiptransforms.esptransforms}_inv(kmn))
Step8.
r2(ipcn.ipg.hitmn.hitcn.{spi.hmac}_inv(kcn))
Step9.
r2(ipcn.ipg.hitmn.hitcn.{spi.hmac}_inv(kcn))

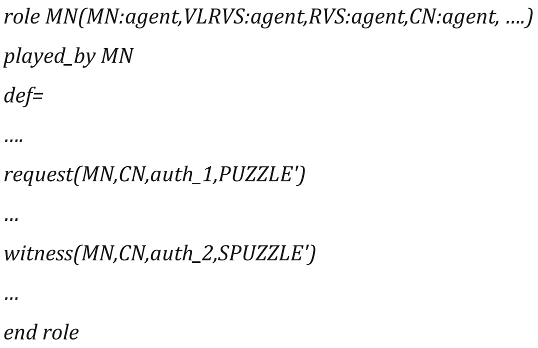
Fig. 8 Protocol simulation

Fig. 9 Section goal



```
goal
        authentication_on auth_1
        authentication_on auth_2
        authentication_on auth_3
        authentication_on auth_4

end goal
```

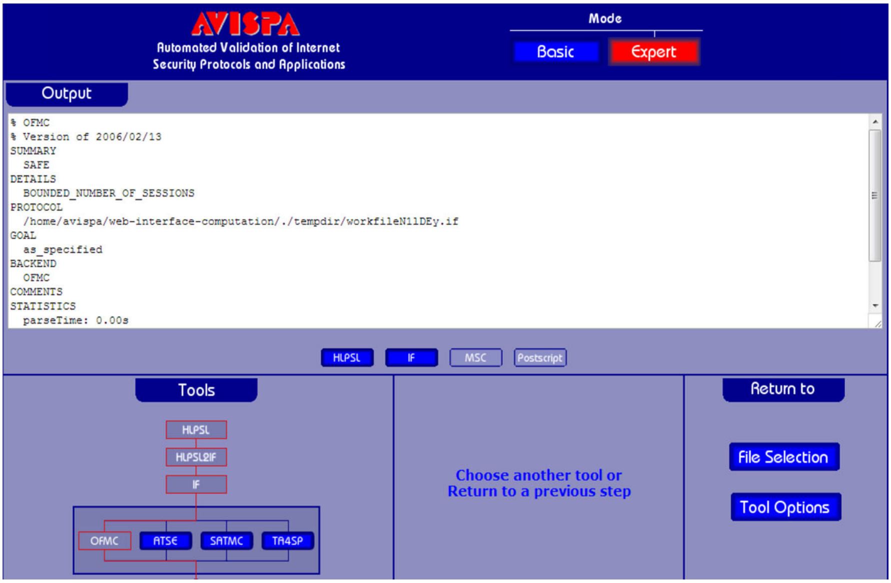
Fig. 10 Location of request goal fact related to authentication on auth_1



```
role MN(MN:agent,VLRVS:agent,RVS:agent,CN:agent, ....)
played_by MN
def=
....
request(MN,CN,auth_1,PUZZLE')
...
witness(MN,CN,auth_2,SPUZZLE')
...
end role
```

Fig. 11 Location of witness goal fact related to authentication on auth_1

```
role CN(CN:agent,MN:agent,VLRVS:agent,RVS:agent,...)
played_by CN
def=
....
witness(CN,MN,auth_1,PUZZLE')
...
request(CN,MN,auth_2,SPUZZLE')
...
end role
```



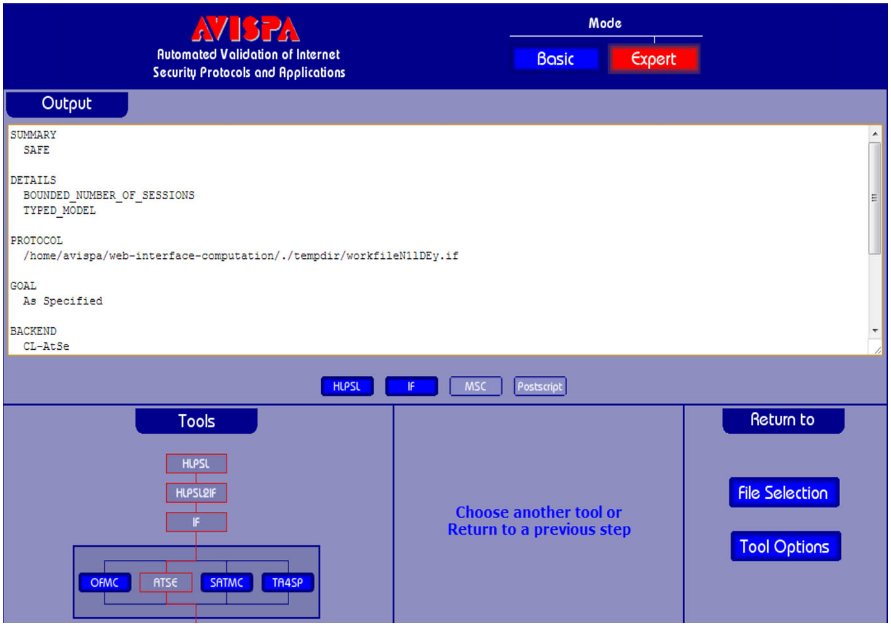
```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/avispa/web-interface-computation/./tempdir/workfileN11DEy.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
```

Fig. 12 Result for HMHIP Protocol with OFMC

In the same way, we have modeled the other defined authentication and secrecy goals in HLPSL. Figures 12, 13, and 14 show the results of the verification tools embedded in AVISPA: OFMC (On-the-Fly Model-Checker) and CL-ATSE (Constraint-Logic-based Attack Searcher). They show that the proposed protocol is safe, which means that no attack was successful in breaking security requirements and the goals set by the protocol specification.

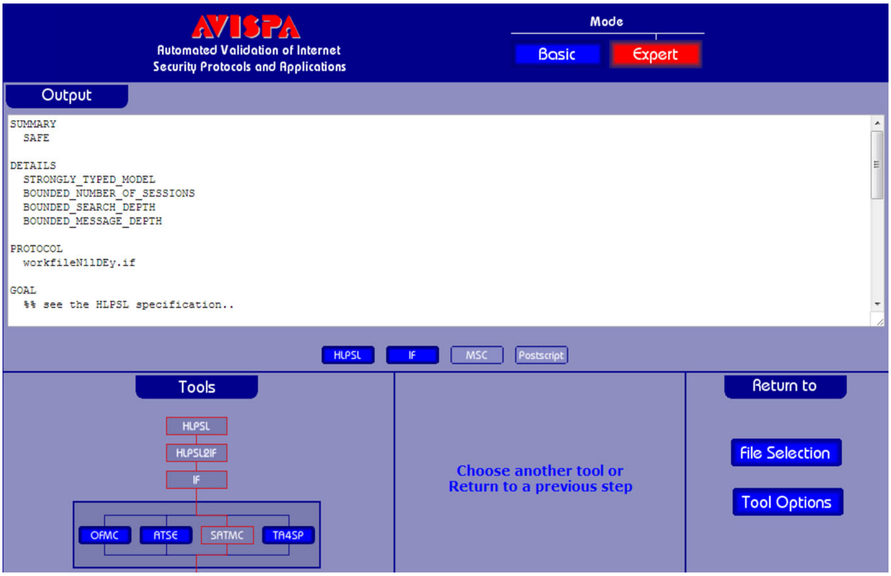
6 Conclusion

In this article, we introduced a new approach to handle mobile networks based on HIP that it can cope with the requirements of wireless heterogeneous networks. Our scheme has introduced some new ideas and concepts such as the use of LRVS servers



```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/avispa/web-interface-computation/./tempdir/workfileN1lDEy.if

GOAL
  As Specified

BACKEND
  CL-AtSe
```

Fig. 13 Result for HMHIP Protocol with ATSE



```
SUMMARY
  SAFE

DETAILS
  STRONGLY_TYPED_MODEL
  BOUNDED_NUMBER_OF_SESSIONS
  BOUNDED_SEARCH_DEPTH
  BOUNDED_MESSAGE_DEPTH

PROTOCOL
  workfileN1lDEy.if

GOAL
  %% see the HLPSL specification..
```

Fig. 14 Result for HMHIP Protocol with SATMC

at each RAN and the protection of replay and hijacking attacks. The performance of the proposed protocol HMHIP and the basic HIP specification was evaluated by simulation analysis. Our proposal presented the lowest handover latency. In addition, HMHIP performance in terms of overhead was very close to that of the basic HIP specification. In the future, we plan to reduce the signaling overhead of our proposal using bulk registrations.

References

1. Gundavelli S, Leung K, Devarapalli V, Chowdhury K, Patil B (2008) Proxy mobile IPv6. IETF, RFC 5213
2. Moskowitz R, Nikander P (2006) Host Identity Protocol (HIP) architecture. RFC 4423, IETF
3. Stewart R, Xie Q, Morneault K, Sharp C, Schwarzbauer H, Taylor T, Rytina I, Kalla M, Xhang L, Paxson V (2000) Stream control transmission protocol. RFC 2960, IETF
4. Nordmark E, Bagnulo M (2009) Shim6: level 3 multihoming shim protocol for IPv6. RFC 5533, IETF
5. Aura T, Nagarajan A, Gurtov A (2005) Analysis of the HIP base exchange protocol. 10th Australasian conference on information security and privacy (ACISP 2005), 481–493. Brisbane, Australia
6. Tritilanunt S, Boyd C, Foo E, González Nieto JM (2007) Cost-based and time-based analysis of DoS-resistance in HIP. Thirtieth Australasian conference on computer science (ACSC '07), 191–200. Darlinghurst, Australia, January 30–February 2
7. Juha S, Mikko S (2010) Risk analysis of host identity protocol: using risk Identification method based on value chain dynamics toolkit. Fourth European conference on software architecture (ECSA), 213–220. Copenhagen, Denmark
8. 3GPP. 3rd Generation Partnerhandover Project; Technical Specification Group Radio Access Network; Evolved Universal terrestrial radio access (E-UTRA); Physical layer procedures (Release8) GPP TS 36.213 V8.8.0 (2009–09)
9. Nikander P, Gurtov A, Henderson TR (2010) Host Identity Protocol (HIP): connectivity, mobility, multi-homing, security, and privacy over IPv4 and IPv6 networks. IEEE Commun Surveys Tutorials 12(2):186–204
10. Aura T (2005) Cryptographically generated addresses (CGA). RFC 3972, IETF
11. Bagnulo M (2009) Hash-based addresses (HBA). RFC 5535, IETF
12. Crocker D (2003) Multiple address service for transport (MAST): an extended proposal. Draft-crocker-mastproposal-01, IETF
13. Vogt C (2005) Credit-based authorization for HIP mobility with concurrent. Draft-vogt-hip-credit-based-authorization-00, IETF
14. Heer T (2007) LHIP lightweight authentication extension for HIP. Draft-heer-hip-lhip-00, IETF
15. Hampel G, Kolesnikov V (2010) Lightweight security solution for host-based mobility and multi-homing protocols. IEEE globecom workshop on seamless wireless mobility
16. Nikander P, Arkko J, Aura T, Montenegro G, Nordmark E (2005) Mobile IP version 6 route optimization security design background. RFC 4225, IETF
17. Laganier J, Eggert L (2008) Host Identity Protocol (HIP) Ren-dezvous extension. Draft-ietf-hip-rvs-04
18. Jokela P, Melen J, Ylitalo J (2006) HIP service discovery. IETF Internet Draft (draft-jokela-hip-service-discovery-00)
19. Laganier J, Koponen T, Eggert L (2006) Host Identity Protocol (HIP) registration extension. IETF Internet Draft (draft-ietf-hip-registration-02)
20. Daly I, Zarai F, Kamoun L (2012) Design and implementation of a simulation environment for the evaluation of authentication protocols in IEEE 802.11s networks. 3rd International ICST conference on mobile lightweight wireless systems, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol 81, Part 4, 206–218
21. The avispa project. Available http://www.avispa-project.org/