An Efficient and Secure Mutual Authentication Mechanism in NEMO-based PMIPv6 Networks: A Methodology and Simulation Analysis

Sirine Ben Ameur[1], Salima Smaoui[1], Faouzi Zarai[1], Mohammad S. Obaidat[2] and Balqies Sadoun[3]
[1]*LETIlaboratory, University of Sfax, Sfax, Tunisia*
[2]*Computer Science and Software Engineering Department, University of Monmouth, NJ 07764, West Long Branch, U.S.A.*
[3]*College of Engineering, Al-Balqa' Applied University, Hay Al-Mayamin, As Salt, Jordan*

Keywords: Network Mobility, Proxy Mobile IPv6, Security, AVISPA.

Abstract: Currently, Network Mobility (NEMO) Basic Support protocol enables the attachment of mobile networks to different points in the Internet. It permits session continuity for all nodes in the mobile network to be reachable as the network moves. While this standard is based on the MobileIPv6 standard, it inherits these disadvantages such as security vulnerabilities. To manage the problems of NEMO, many schemes combine it with a network-based approach such as Proxy Mobile IPv6 (PMIPv6). Despite the fact that this latter expedites the real deployment of IP mobility management; it suffers from lack of security. Therefore, we propose an Efficient and Secure Mutual Authentication Mechanism during initial attachment in NEMO-based Proxy Mobile IPv6 Networks called EMA-NEMO based PMIPv6 in order to provide mutual authentication between a mobile router and diameter server during initial attachment of the mobile router to a PMIPv6 domain. Moreover, we evaluate the performance of our scheme using the Automated Validation of Internet Security Protocols and Applications (AVISPA) software which has proved that authentication goals are achieved.

1 INTRODUCTION

In the present Internet environment NEMO Basic Support (V. Devarapalli et al., 2005) is a protocol that enables mobile networks to attach to different points in the Internet. This protocol is based on the Mobile Internet protocol version 6 (MIPv6) (D. Johnson et al., 2011). Consequently, it inherits its disadvantages, such as lack of security and handover latency. Many schemes in the literature (I. El Bouabidi, et al., 2014; S. Smaoui et al., 2014; A.H. A.Hashim et al., 2013) attempt to adapt layer 3 mobility protocols of a terminal for a Mobile Network. Unlike, host-based mobility management schemes such as MIPv6 and Hierarchical MIPv6 (HMIPv6) (J. Kempf, 2007), a Network-based Localized Mobility Management (NETLMM) scheme (H. Soliman et al., 2008), like PMIPv6 (S. Gundavelli et al., 2008), can expedite the real deployment of IP mobility management.

Contrary to MIPv6, by using PMIPV6 the network can be in charge of the mobility of mobile node, and Mobility Access Gateway (MAG) entity can recognize the mobility of L2 connection information, and send the Proxy Binding Update (PBU) message to the Local Mobility Anchor (LMA) on behalf of the mobile node. Hence, without any modifications to the host's TCP/IP Protocol stack, the mobile node can change its point of attachment to the Internet with the same IP address. At the same time, when the mobile node (in our case mobile router) attaches to the MAG, the deployment of security protocols on this link should ensure that the network-based mobility management service is offered only after the authorization and authentication of the mobile node to that service. Authors in (S. Gundavelli et al., 2008), assume that there is an established trust between the mobile node and the MAG before the protocol operation begins. However, they do not specify how this is achieved.

As a first step, we study the security issues related to the PMIPv6 protocol (C. Vogt and J. Kempf, 2007). We can conclude that there are many threats in the link between the MR and the MAG.

After carefully analyzing various pieces of related schemes, we found that the standard in (J. Korhonen

Ben Ameur S., Smaoui S., Zarai F., S. Obaidat M. and Sadoun B..
An Efficient and Secure Mutual Authentication Mechanism in NEMO-based PMIPv6 Networks: A Methodology and Simulation Analysis.
DOI: 10.5220/0005580200130021
In *Proceedings of the 5th International Conference on Simulation and Modeling Methodologies, Technologies and Applications* (SIMULTECH-2015), pages 13-21
ISBN: 978-989-758-120-5

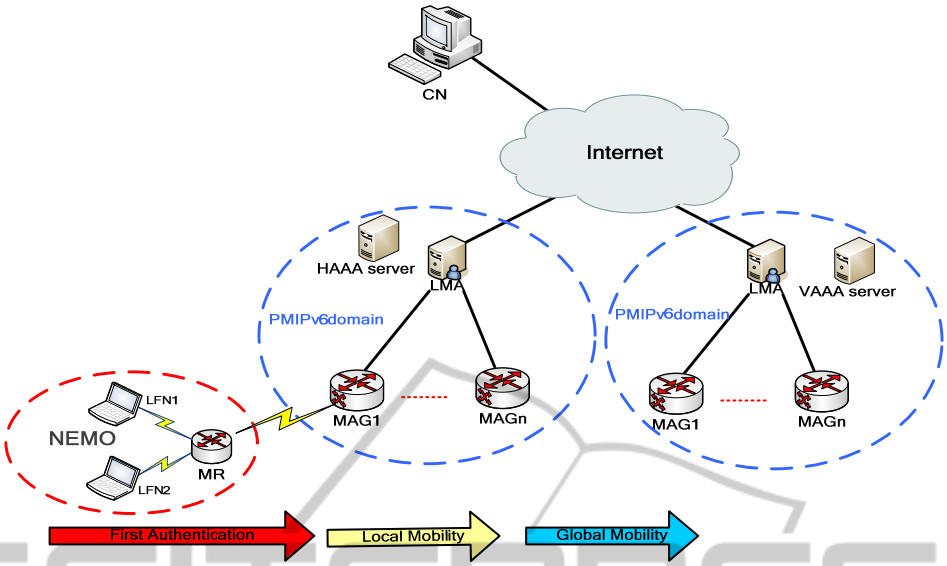

Figure 1: Architecture of EMA-NEMO based PMIPv6.

et al., 2008) gives an example of interaction between different network nodes. This example is based on Extensible Authentication Protocol (EAP). In addition, it uses the Diameter EAP Application for signaling exchanges between the MAG and the HAAA. The LMA uses the Network Access Server Requirements (NASREQ) Diameter Application to authorize the MN with the HAAA server.

At present, several EAP methods are available, but only a few of them are standardized by the Internet Engineering Task Force (IETF). Among these, we can mention the EAP-MD5-Challenge, which is described in (B. Aboba, 2008) and based on the Challenge Handshake Authentication Protocol (CHAP) (W. Simpson, 1996). Despites it does not require a lot of resources for treatment, it is acknowledged as vulnerable to dictionary and brute force attacks. In addition it is a unilateral method.

A second method named Extensible Authentication Protocol Transport Layer Security (EAP-TLS) (D. Simon et al., 2008) based on a password associated with a user name or an identity was proposed. This method offers a good level of security since it allows mutual authentication between the client and the server. However, the major disadvantage is that it relies on Public Key Infrastructure (PKI) for client and server's certificate management. In fact, the PKI is extremely expensive and complex and is not very well applicable to the mobile context.

As a third method we mention the Extensible Authentication Protocol Authentication and Key Agreement (EAP-AKA) used in the 3rd generation mobile networks such as Universal Mobile Telecommunications System (UMTS). It is based on symmetric keys. This method presents also several vulnerabilities as declared in (Y.E.H.E. Idrissi et al., 2012; A. H. Hassanein et al., 2013; B. Yu et al., 2014; H. Mun et al., 2009). Among these vulnerabilities, we mention the disclosure of the International Mobile Subscriber Identity (IMSI) since on the first connection; the user equipment (UE) must send his permanent identity to the AAA server. Therefore, an attacker can abuse the IMSI and seizes a legal subscriber's identity. A man in the middle attack is also present in the EAP-AKA protocol. In fact, when the UE and the AAA server successfully authenticate each other, an EAP Success message including the MSK key must be sent to the Access Point (AP) and the UE without a previous authentication for this AP. Consequently, this MSK key can be received by an attacker who impersonates the AP and then sends a forged key to the UE or sends this legal key to an unauthorized UE. The list of vulnerabilities of EAP-AKA continues with the possibility of disclosure of the all procedure of EAP-AKA. Indeed, only one symmetric key K is used for the generation of the session keys. Therefore, the disclosure of this key brings to the disclosure of all the procedure. For These reasons, and based on the security solutions in (J. Korhonen et al., 2008), we propose in this paper to establish trust relationship between PMIPv6 domain (especially MAGs) and the MR node using diameter server. We have attempted to authenticate and authorize the MR before allowing it to access to the PMIPv6 network in order to eliminate the threats on the interface between the MAG and the MR.

The rest of this paper is structured as follows. Section 2 describes our proposed scheme for initial authentication of NEMO in PMIPv6 domain. Then, section 3, analyses the security aspect of the proposed scheme and evaluates it using the AVISPA and SPAN software. Finally, section 4 concludes the paper.

2 PROPOSED PROTOCOL: EMA-NEMO BASED PMIPv6

Based on the given signaling flow example during PMIPv6 using the AAA interactions in the standard (J. Korhonen et al., 2008), we proposed our protocol named Efficient and Secure Mutual Authentication Mechanism in NEMO-based PMIPv6 Networks (EMA-NEMO based PMIPv6).

2.1 Architectural Components and Terminologies

In this paper, we focus on the authenticationmethod used under the network evaluation of integration of NEMO supporting mobility and network-based PMIPv6. Our architecture,is illustrated in Figure 1, and structured as follows:

- Mobile Networks includes:
  -Two Locals Fixed Nodes (LFN) that have no mobility support stack. All handover will be treated with a transparent manner.
  -A mobile router (MR) which acts as a gateway between LFNs and PMIPv6 entities.
- Proxy Mobile IPv6 Domain includes:
  -Local Mobility Anchor (LMA) which is like a Home Agent (HA) for the mobile router in a PMIPv6 domain. It is the topological anchor point that manages the mobile router's binding state.
  -Mobile Access Gateway (MAG) is a function on an access router that manages mobility-related to signaling for the mobile router.
- Diameter server based on Authentication, Authorization, and Accounting (AAA) properties:
  -Home AAA server (HAAA), is responsible for Authentication, Authorization, and Accounting of network entities.

2.2 Hypothesis and Notations

In our protocol, we assume the existence of the following keys:

- PSK: Pre-Shared Key shared between HAAA and MR,
- $ShK_{LMA/HAAA}$: Shared key between HAAA and LMA,
- $ShK_{MAG1/LMA}$: Shared key between MAG1 and LMA,
- KPubS: Public key of the HAAA.

Our scheme is described with the notation summarized in Table 1 shown below.

Table 1: Notations used in the proposed scheme.

Notation	Description
||	Concatenation operation.
N_i	A nonce genereted randomly by i
IDx	Identity of a node x.
$\{M\}_K$	Encrypted message M using the key K.
$Autn_X$	Authentication token, generated by node X.
SQN	Sequence number
$F1,F2,F3,$ $F4,F5$	These functions are used to generate fields used during an authentication session, the choice of their algorithm is specific to the operator.

2.3 Proposed EMA-NEMO

As show in Figure 2, our solution describes the scenario of first authentication of the MR in a PMIPv6 domain.

Step 1: MR ➔MAG1: EAP start

Firstly, the MR sends a message named EAP start (Extensible Authentication Protocol. We can use the EAPOL "Over LAN" message) to initiate the authentication.

Step 2: MAG1➔MR: EAP/Request-Identity

In the second step, the MAG asks for the MR identity.

Step 3: MR➔MAG1: EAP/Response-Identity; $\{ID_{LF1} || ID_{LF2} || SQN || N_{MR} || ID_{MR}\}KPubS || MAC$

In the third step, the link layer identity of the MR (IMSI or MAC address) is encrypted, with generated Random (N_{MR}) and sequence number (SQN), using the public key of the server.
This message must contain the list of the LFNs identifiers linked to the MR.
And to prevent attacks against integrity, we can add a Message Authentication Code ($MAC = F1(PSK|| ID_{LF1} || ID_{LF2} || SQN || N_{MR} || ID_{MR})$.
In the next authentication, the MR must send the temporary identity computed based on the (IMSI or

MAC address) concatenated with the N_{MR} generated in this authentication.

Step 4: MAG1➔HAAA: DER; (ID_{LF1}|| ID_{LF2}||SQN || N_{MR} || ID_{MR})KPubS ||MAC

After receiving the EAP/Response-Identity message, the MAG transfers the encrypted field and integrity code to the server using Diameter-EAP-Request message.

Step 5: HAAA ➔ MAG1: DEA (EAP-request); {AutnS|| {SQN||(T-ID_{MR} = F5(ID_{MR}||N_{MR})) ||(Right(N_S)||Left(N_{MR})}$ShK_{LMA/HAAA}$ } $ShK_{MAG1/HAAA}$

When the server receives the message from MAG1, it:

- ✓ Decrypts the encrypted field and verifies the MR identity (ID_{MR}) and its subscription information for authentication,
- ✓ Then, verifies the integrity of the received fields and executes the synchronization procedure using the SQN value.
- ✓ Next, it generates a new nonce (N_S),
- ✓ It computes the authentication token (AutnS) field, when AutnS = MAC ||{ID_{MR}||IDs||N_S} EK_1. The server uses the Message Authentication Code (MAC=F1(PsK||N_S)) field to improve the integrity of the nonce generated, and it uses an encryption key EK_1=F2(PsK||N_{MR}) against brute force attack.
- ✓ Computes an encrypted field using the shared key between the LMA and the server. This field will be used in step 11 to improve that the MR is authenticated via the MAG1 node.
- ✓ Finally, it sends a Diameter-EAP-Answer (DEA)

Step 6:MAG1➔MR: EAP-Request

The MAG1 transmits the AutnS field to MR.

Step 7: MR➔MAG1: EAP-Response

When the MR receives the message from MAG1, it:

- ✓ Computes the encryption key EK1,
- ✓ Decrypts the encrypted field using EK1 and verifies its identity and the identity of the server, then it authenticates the server,
- ✓ Keeps the nonce (NS) and verifies its integrity by checking the MAC value.
- ✓ Finally, it computes the AutnMR value and sends it to the server via the MAG1 using EAP-Response.

$Autn_{MR}$ = F4(NSK|| ID_{MR}||ID_S), when the NSK is a new shared key between the MR and the server. This key is used for the next authentication instead of the key PSK against attacks.

NSK= F3(PsK||N_S||N_{MR})

Step 8: MAG1➔HAAA: DER

The MAG1 transmits the $Autn_S$ field to the server.

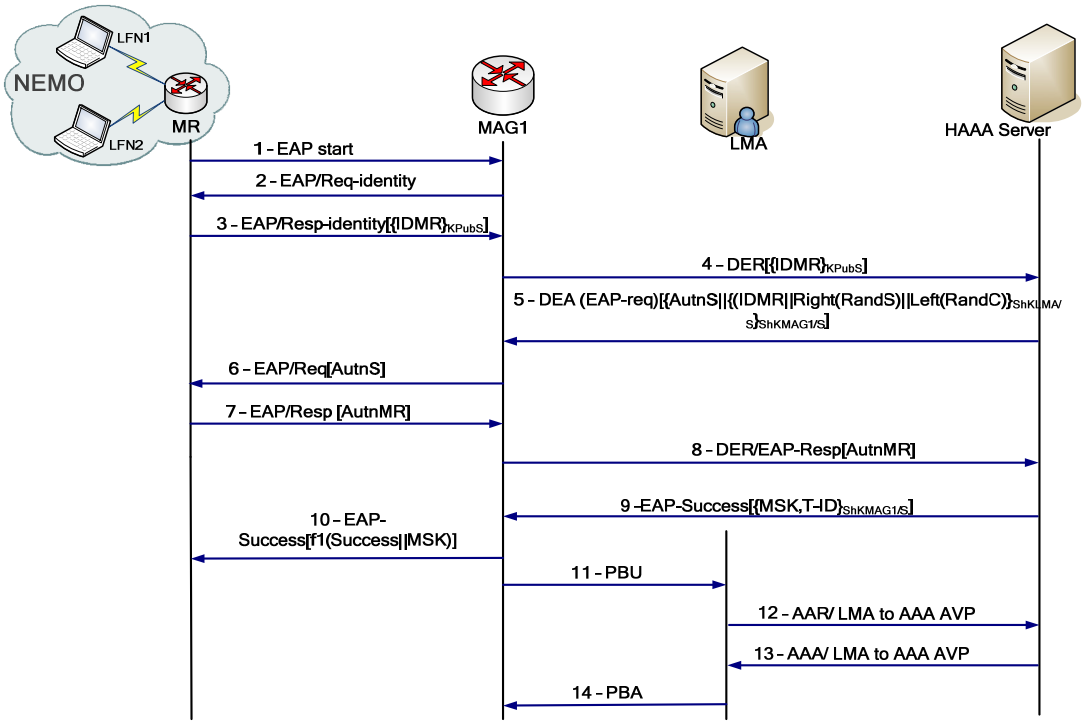

Figure 2: Initial authentication in PMIPv6 domain.

Step 9: HAAA➔MAG1: DEA (EAP-Success);

When the server receives the message from MAG1, it:

- ✓ Calculate the Autn'MR, then it verifies if there are an equality between the calculated and received field to authenticate the MR.
- ✓ If the MR is authenticated, the server must computes a MSK key, and sends it to the MAG1. These keys are used to encrypt data and verify integrity of messages between MR and MAG1 in this session.

Step 10: MAG1 ➔ MR; EAP-Success

(MAC = F1(Success field ||MSK))

Step 11: MAG1➔LMA: PBU; (SQN||(T-ID_{MR}||(Right(N_S)||Left(N_{MR})) $ShK_{LMA/HAAA}$|| 0] $ShK_{MAG1/LMA}$

When the MAG1 receives the DEA message, it keeps the MSK key then transmits the EAP-Success message with an MAC field using the MSK key.
At the same time, the MAG1 sends a PBU (Proxy Binding Update) message to the LMA. This message must include the field kept in the step 5 ({SQN||(T-ID_{MR} = F5(ID_{MR}||N_{MR})) ||(Right(N_S)||Left(N_{MR})} $ShK_{LMA/HAAA}$) with the ID of the last MAG1 witch the MR is attached. Since it is an initial authentication (first attachment of the MR to the network), and then this field must be set to zero.

Step 12: LMA ➔HAAA: AAR;

Upon receiving the PBU message, the LMA:

- ✓ Decrypts the field encrypted with the$ShK_{MAG1/LMA,}$
- ✓ Then, notes that this is the first attachment of MR to the network (If ID_{MAG} field equal to zero, then MR is not related to any node in the network)
- ✓ Afterward, decrypts the field encrypted with the $ShK_{LMA/AAA}$ to know the T-$ID_{MR.}$
- ✓ Finally, it sends an AA Request message to the server to fetch the relevant parts of the authorization information and subscriber policy profile related to this mobility service session. This message must contain the T-ID encrypted using shared key between the LMA and the server.

Step 13: HAAA➔LMA: AAA;

The diameter server has the role of a Proxy MIPv6 remote policy store.
So, the server sends an AA Answer (AAA) containing the authorization information and subscriber policy profile related to the MR (ID_{MR}, (Right (N_S)||Left(N_{MR})),Related MAG,…)

Step 14: LMA➔MAG1: PBA;

After verifying the equality between fields received from the MAG1 and the server, the LMA sends a proxy binding acknowledgment (PBA) to the MAG1.

Figure 3, presents the composition of the generated tokens of authentication.

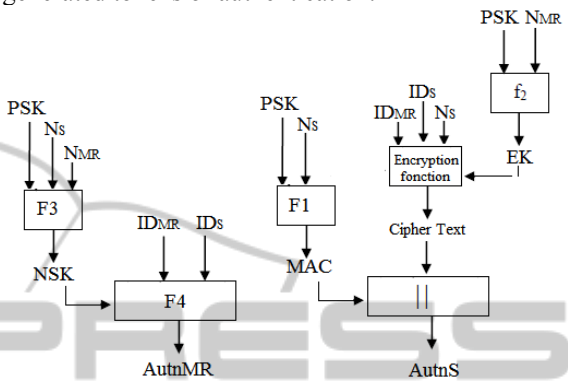

Figure 3: Compositions of the $Autn_{MR}$ and $Autn_{S.}$

3 ANALYSIS AND VERIFICATION OF THE PROPOSED SCHEME

Providing an efficient and secure strong authentication support is one of the critical challenges in new wireless networks generations. This is why our principal target in this paper is to overcome the limitation of the first authentication scheme between mobile router and PMIPv6 domain. In this section, we present the security analysis of the proposed scheme using the SPAN tool.

3.1 Security Analysis and Resistance against Attacks

Our scheme is carefully designed to not only achieve mentioned goal (strong authentication support) but also to prevent against some typical attacks such as reply attack and to guarantee confidentiality as well as integrity of fields exchanged between network nodes. In this subsection, we will enumerate the enclosed security requirements of our proposed scheme.

a. Authentication

In order to prevent spoofing attack, our proposed scheme guarantees strong authentication between HAAA and MR. When the MR enters in PMIPv6 domain, a mutual

authentication is performed through the $Autn_{MR}$ and $Autn_S$ fields.

b. Confidentiality

In our scheme, we attempted to ensure the confidentiality of critical fields:

✓ *Shared keys*

To ensure the secrecy of keys, we attempt to not exchange them in the network. However, if this is not possible, it is necessary to choose a secure manner to share them.

- Using some elements exchanged, the MR and the server should be able to calculate the NSK using the flowing fields:
  -The PSK initially shared between the MR and the server
  -The nonce N_{MR} calculated by the MR, which must be sent encrypted
  -The nonce N_S calculated by the HAAA, which must be sent encrypted.
- To exchange the MSK between HAAA and MAG1, we use the shared key between HAAA and MAG1. Whereas, the MR must be able to compute this key using the previous exchanged fields.

✓ *Generated nonces*

To exchange the nonce NMR and NS between the MR and HAAA privately and therefore avoid being modified by an attacker, MR sends its generated nonce NMR encrypted with the HAAA's public key (KpubS) and the HAAA server sends its generated nonce NS encrypted with the computed key EK1.

c. Integrity

In order to verify the integrity of critical exchanged fields, MAC is used. It protects against falsification attack and validates the authenticity of the sender node. Any malicious node will not be able to modify the contents of the exchanged fields specifically nonces (NMR, NS) and response of the server in the end of the authentication transition (Success or Failure).

d. Anti Replay attack resistance

In order to prevent the malicious effect of the reply attack, sequence number (SQN) field is integrated. This SQN is generated by the MR node and it must be encrypted. So message is considered only if the sequence number is in the correct range.

e. Identity protection

In the first connection, unlike some EAP protocols (like EAP-AKA) we use an encrypted identity to be protected and not exposed to attackers. In the next authentication, we assume that the MR sends a Temporary identity computed based on the (IMSI or MAC) and the NS generated in this authentication. Besides, the server will receive an encrypted new T-IDMR in every re-authentication process. Therefore, our solution provides a strong user identity protection against identity related attack.

f. Man in the middle attack protection

In our protocol, the encryption key EK1, is randomly generated and no keys (MSK) are transmitted in clear. Also, the identity of the MR is encrypted. In addition, the critical fields are protected by an MAC. Therefore our protocol can resist against the man in middle attack.

g. Brute force attack resistance

In general, a key which is used for a long time can be under brute force attack.

For this reason, some items must be taken into consideration:

Assume that the length of keys is long enough.

✓ Assume that the PMIPV6 entities domain should change their shared keys (ShKHAAA/MAG1, ShKHAAA/LMA) periodically to reduce the probability of hacking due to brute force attacks.

✓ Use of a new computed EK key for each authentication.

✓ Refreshe the key PSK, in the next authentication, using the generated nonce NMR.

3.2 Security Screening of Proposed Protocol using the AVISPA and SPAN Software Tool

AVISPA (AVISPA, 2003; A. Armando, 2005) tool provides the High Level Protocol Specification Language (HLPSL) (2006) to specify concerned protocols and formally validate them. Many security protocols and systems are verified using AVISPA as given in (Collections of Security Protocols).

a. Authentication

Using the AVISPA/SPAN tools, we are able to check and verify the mutual authentication between MR and HAAA server. Based on HLPSL language; we use the *witness* and *request* events to verify the authentication goal between MR and the server.

In general, the request event defines the authenticator agent (A) and the authenticated agent

(B) as the first and second arguments. Moreover, the third argument (A_B) is used to associate the witness and request predicates with each other and to refer to them in the goal section. It should be declared as a constant of type protocol_id in the top-level role. Finally, the receiver (A) must make sure that the fourth value (K) was indeed created by the sender (B); it was created for it and that it was not replayed from a previous session. To achieve this, we must write a line like the following:

```
Request (A,B,A_B,K)
```

Every request event must be accompanied and preceded by an accompanying witness event. In addition, for our type of authentication (strong authentication), no agent should accept the same value more than once from the same partner of communication. This is the definition offered by Lowe's notion of agreement (G. Lowe, 1997):

```
witness (B,A,A_B,K)
```

- HAAA authenticates MR:

When we write our code based on HLPSL language we must add, in the role of the HAAA, the following line:

```
Role S %server
…
…
8. State=1
/\
RCV(der_eap_res(F4(F3(PsK.NS'.Nmr').I
Dmr.IDS)))
=|> State':=2
/\
Request
(S,MR,auth_1,F3(PsK.NS'.Nmr'))
```

The interpretation of this request is as follows. The server requires that MR exists and agrees on the value `F3(PsK.NS.Nmr)` and also intend it to be used for the protocol id auth_1.

Then, we must add the accompanying witness predicate in role of MR, as part of the transition in which the value F3(PsK.NS'.Nmr') is sent to the server as follows.

```
Role MR
…
…
6. State=2
/\
RCV(eap_req({F1(PsK.NS').IDmr.IDS.NS'
}_F2(PsK.Nmr')))
=|> State':=3
/\
SND(eap_res(F4(F3(PsK.NS'.Nmr').IDmr.
IDS)))
/\ request(MR,S,auth_2,NS')
/\
witness(MR,S,auth_1,F3(PsK.NS'.Nm
r'))
```

The interpretation of this witness is as follows. Agent MR asserts that we want to be the peer of agent S(server), agreeing on the value `F3(PsK.NS'.Nmr')` in an authentication effort identified by the protocol_id auth_1.

Hence, in the goal section of the protocol, we add the following lines:

```
authentication_on auth_1
```

- MR authenticates HAAA server

The same thing for MR, and also the same explanations are repeated.

In the role of MR, we add the request event in the corresponding position:

```
Role MR
…
…
6. State=2
/\
RCV(eap_req({F1(PsK.NS').IDmr.IDS.NS'
}_F2(PsK.Nmr')))
=|> State':=3
/\
SND(eap_res(F4(F3(PsK.NS'.Nmr').IDmr.
IDS)))
/\
request(MR,S,auth_2, NS')
/\
witness
(MR,S,auth_1,F3(PsK.NS'.Nmr'))
```

In the role of HAAA, we add the matching witness event as follows.

```
Role S %sever
4. State=0
/\ RCV(der({SQN'.IDmr'.Nmr'}_KpubS))
=|> State':=1
/\ NS':=new()
/\ SND(
dea_eap_req({{F1(PsK.NS').IDmr'.IDS.N
S'}_F2(PsK.Nmr').{SQN'.F5(NS'.IDmr').
Right(Nmr').Left(NS')}_KlmaS}_KmagS))
/\
witness(S,MR,auth_2,NS')
```

Then, in the goal section of the protocol, we add the following line.

```
authentication on auth 2
```

a. Confidentiality and secrecy of keys

The secret event is the goal fact related to confidentiality. For security goal, we are able to check the secrecy of MSK key, generated nonces (N_S and N_{MR}) and the SQN number among MR and HAAA. We achieve this, generally, by placing such secret facts in the role that creates the value that should be secret.

```
Role MR
1. State=0
/\ RCV(start)
=|> State':=1
/\ SND(EAPpol)
2. State=1
/\ RCV(RequetID)
=|> State':=2
/\ Nmr':=new() /\ SQN':=new()
/\ secret(SQN',sec_1,{LMA,S,MR})
/\ secret(Nmr',sec_2,{S,MR})
…
…
```

```
Role S
…
…
4.State=0
/\  RCV(der({SQN'.IDmr'.Nmr'}_KpubS))
=|> State':=1
/\ NS':=new()
/\ secret(NS',sec_3, S,MR})
```

And, in the goal section of our protocol, we must add the following line.

```
secrecy ofsec 1,sec 2,sec 3
```

b. Results and discussion

AVISPA and SPAN tools assume that all transitions between nodes pass through an intruder. This intruder tries to exploit given information that was collected for constructing attacks against the simulated protocol. In general, if one of security goal is violated the used output tool shows that the protocol is found unsafe. Then, the back-ends display the violated goal, provide the attack trace and explain the sequence of events leading up to the violation. Else, if you show that the tool output has declared that your protocol is found safe under specific goals, these mean that no violation is found.

In our work, we validated our scheme using the On-the-fly Model-Checker (OFMC) (D. Basin et al., 2005), which performs the protocol analysis by exploring the transition system in a demand-driven way and the Constraint-Logic-based Attack Searcher (CL-AtSe) (M. Turuani, 2006), which applies constraint solving with powerful simplification heuristics and redundancy elimination techniques. The back-ends are called with the default options. The tool outputs shown in Figure 4 shows that our protocol has been found to be a safe scheme and that no attack has been found. This means that the stated security goals are successfully checked by the back-ends.

Figure 4: OFMC and ATSE performance analysis results.

4 CONCLUSIONS

While the number of attacks within the network increases, security has become an important a crucial issue these days. For this reason, we are concerned in this paper to propose a new method of authentication based on EAP protocol in order to provide trust between a mobile router and a PMIv6 domain. Our proposed protocol has been modeled and validated using the AVISPA software tool. After this verification, we can confirm that our protocol has achieved its main objectives. As a future work, we

detail the necessary steps for the re-authentication of MR within the same PMIPv6 domain when it removes between different MAGs and the re-authentication of MR between different PMIPv6 domains.

REFERENCES

V. Devarapalli, R. Wakikawa, A. Petrescu and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", IETF, RFC 3963, January 2005.

D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", IETF, RFC 6275, July 2011.

I. El Bouabidi, S. Ben Ameur, S. Smaoui, F. Zarai and M. S. Obaidat, L. Kamoun, "Secure macro mobility protocol for new generation access network", International Wireless Communications and Mobile Computing Conference (IWCMC), Nicosia, pp. 518–523, 4-8 August 2014.

S. Smaoui, S. Ben Ameur, I. El Bouabidi, F. Zarai and M.S. Obaidat, "Secure micro mobility protocol for new generation wireless network", International Wireless Communications and Mobile Computing Conference (IWCMC), Nicosia, pp. 895–900, 4-8 August 2014.

A. H. A. Hashim, W. H. Hassan, S. Islam, R. A. Saeed, 1M.K. Hasan, J I. Daoud and O. O. Khalifa", An Enhanced Macro Mobility Management Scheme in NEMO Environment to Achieve Seamless Handoff", World Applied Sciences Journal (Mathematical Applications in Engineering), Vol. 21, pp. 35-39, 2013.

J. Kempf, "Goals for Network-Based Localized Mobility Management (NETLMM)", IETF, RFC 4831, April 2007.

H. Soliman, C. Castelluccia, K. El Malki and L. Bellier 'Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", Network Working Group RFC 5380, Standards Track, October 2008.

S. Gundavelli, V. Devarapalli, K. Chowdhury, B. Patil and K. Leung, "Proxy Mobile IPv6", IETF, RFC 5213, August 2008.

C. Vogt and J. Kempf, "Security Threats to Network-Based Localized Mobility Management (NETLMM)", IETF, RFC 4832, April 2007.

J. Korhonen, J. Bournelle, K. Chowdhury, A. Muhanna, U. Meyer, "Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor Interaction with Diameter Server", IETF, RFC 5213, August 2008.

B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz, "Extensible Authentication Protocol (EAP)", IETF, RFC 3748, June 2008.

W. Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", IETF, RFC 1994, August 1996.

D. Simon, B. Aboba and R. Hurst, "The EAP-TLS Authentication Protocol,'' IETF, RFC 5216, Mach 2008.

Y.E.H.E. Idrissi, N. Zahid, M. Jedra, "Security Analysis of 3GPP (LTE) – WLAN Interworking and A New Local Authentication Method based on EAP-AKA", Future Generation Communication Technology (FGCT), pp. 137 – 142, 12-14 December 2012.

A. H. Hassanein, A. A. Abdel Hafez, A. E. H. A. Gaafar, "New Authentication and Key Agreement Protocol for LTE-WLAN Interworking", International Journal of Computer Applications,Vol. 61, No.19, pp. 20-24, January 2013.

B. Yu, J. Zhang, Z. Wu, "Improved EAP-AKA Protocol Based on Redirection Defense", P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference, pp. 543 – 547, 8-10 November 2014.

H. Mun, K. Han, k. Kim, "3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement based on EAP-AKA", Wireless Telecommunications Symposium, pp. 1-8, April 2009.

AVISPA: Automated validation of internet security protocols and applications (2003) FET Open Project IST-2001-39252. http://www.avispa-project.org/

A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.-C Heam., O. Kouchnarenko, J. Mantovani , S. Modersheim , D. von Oheimb, M. Rusinowitch, J. Santos Santiago, M. Turuani, L. Vigano, and L. Vigneron, "The AVISPA Tool for the automated validation of internet security protocols and applications", In K. Etessami and S. Rajamani, editors, 17th International Conference on Computer Aided Verification, CAV2005, Lecture Notes in Computer Science, 3576, 281285, Edinburgh, Scotland, 2005.

HLPSL Tutorial available at http://www.avispa-project.org/package /tutorial.pdf/ June 30, 2006.

Collections of Security Protocols, available at http://www.avispa-project.org.

G. Lowe. "A hierarchy of authentication specifications", Proceedings of the 10th IEEE Computer Security Foundations Workshop (CSFW'97), pp. 31–43, 1997.

D. Basin, S. Mödersheim, and L. Vigano, "OFMC: A Symbolic Model-Checker for Security Protocols", International Journal of Information Security, Vol. 4, No. 3, pp. 181-208, June 2005.

M. Turuani, "The cl-atse protocol analyser", 17th international Conference, on Term Rewriting and Applications (RTA), USA, pp. 277-286 August 2006.