International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-6, Issue-8)

Research Article | **August 2017**

A Framework to Enhance Security in Nemo Environment Using AAA Mechanisms

Isac Gnanaraj J
Department of Computer Science, Don Bosco College, Yelagiri Hills, Tamil Nadu, India

Sriram
Department of Computer Applications, Don Bosco College, Yelagiri Hills Tamil Nadu, India

Abstract—

One of emerging trends in the mobile network era is Network Mobility (NEMO). It was standardized by the Internet Engineering Task Force (IETF) and gained attention of the researchers because of research opportunities that it provides. Though it was developed based on MIPv6, there are few spots that must be analyzed and rectified, especially in the security aspects. According to the literatures, NEMO lacks in providing a robust Authentication, Authorization and Accounting (AAA) services to its users. AAA operations must be performed for all the players of the mobile network, because a hacker may reside at any place and try to access the mobile network by hiding behind valid or genuine nodes' addresses. This research work aims to provide an AAA framework for NEMO by comprising three different mechanisms which are developed for Local Mobile Node (LMN), Visiting Mobile Node (VMN) and Mobile Router (MR). Simulation and performance analysis are done.

Keywords— network mobility, authentication, security, framework, authorization

I. INTRODUCTION

As the demand for mobile device increase day by day, the number of devices for individual users is also increasing. Increasing number of mobile devices forces the service provider to go for alternate solutions for accommodating the increased number of signals. To overcome the signaling difficulties in mobile networks, IETF developed and standardized a protocol called, Network Mobility (NEMO) [1]. Another mobility scenario that is already being used by all service providers is Host Mobility in which each device is connected directly with the base station transceiver or access point. In NEMO as shown in Figure 1, group of nodes forms a network and one of the devices acts as a router, that is called as Mobile Router (MR). All the communications from the mobile network nodes to the outside nodes pass through the MR. Providing security is an important task for any service providers to ensure quality of service. Through literature review it is found that LMN, VMN and MR are the major players of NEMO. Authentication must be performed before granting access to these nodes in order to secure the NEMO environment.

A Mobile Network Node (MNN) has two different addresses, namely, Home Address (HoA) and Care of Address (CoA). HoA is the permanent address which is obtained from the Home Network (HN). CoA is called as temporary address which is obtained from Foreign Network (FN) in which the MNN is currently roaming. Whenever the MNN moves away from its HN, Home Agent (HA) forwards all the communication addressed to MNN, to its CoA that is the current location of MNN.

Securing the nodes of NEMO starts with authenticating the nodes. Many researchers expressed that NEMO doesn't provide robust Authentication, Authorization and Accounting (AAA) services. AAA is considered as an important part of any security protocols which must be executed at earlier stage of connection establishment or call setup. In order to provide better secured environment, already three mechanisms have been proposed, namely, AMR-NEMO [2], AVM-NEMO [3] and ALM-NEMO [4]. To perform AAA for MR, AMR-NEMO was proposed. To perform AAA for VMN and LMN, AVM-NEMO and ALM-NEMO was proposed respectively. These three mechanisms are to be integrated with NEMO BSP, so that the NEMO environment would become more secure. A framework is developed in this paper by integrating all these three mechanisms with the NEMO BSP.

II. BACKGROUND

Many researchers provided various mechanisms to protect the NEMO environment in the aspect of AAA. Vollbrecht J et al. [6] proposed a framework and based on this, de Laat et al. [5] proposed the Generic AAAarchitecture. Julien Bournelle et al. [7] expressed that Generic AAA architecture did not provide an effective AAA mechanism. Remote Authentication Dial In User Service (RADIUS) [8] was proposed to carry authentication, authorization, and configuration information between a Network Access Servers (NAS) which need to authenticate its links and a shared Authentication Server. Diameter [9][10] was proposed as an alternative for RADIUS. A Diameter based application was developed by Hakala et al. [11] for real-time credit-control over the end users' services such as network access, Session Initiation Protocol (SIP) services, messaging services, and download services.

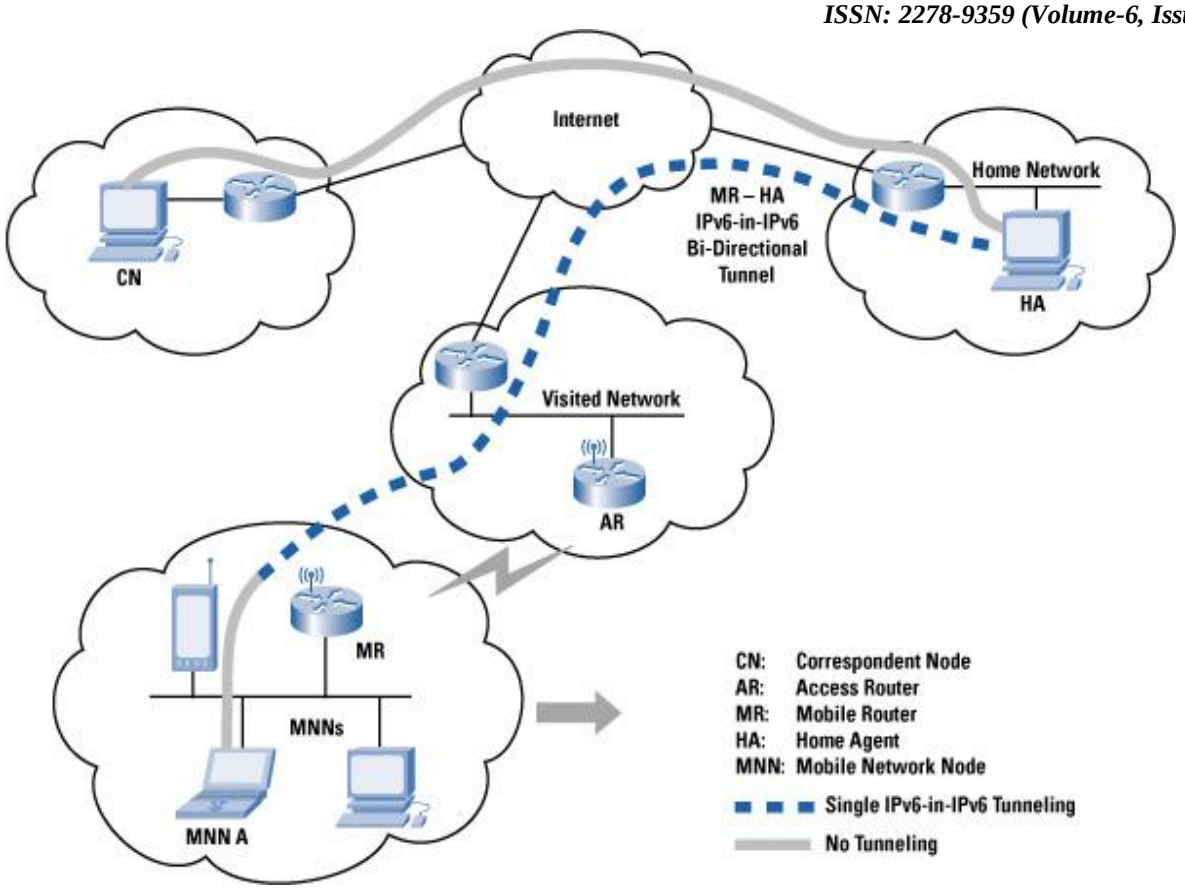

Fig. 1.Structure and Operations of NEMO Basic Support Protocol

Eronen et al. [12] developed an Extensible Authentication Protocol (EAP) as a standard mechanism for various authentication methods. Garcia-Martin et al. [13] proposed a Diameter SIP application for AAA in conjunction with SIP and it provided a Diameter client co-located with a SIP server, with the ability to request the authentication of users and authorization of SIP resources usage from a Diameter server.

David Binet et al. [14] gave an overview of the constraints and recommendations provided by various service providers and also they proposed a proactive authentication approach to increase the overall performance of IP handover. Ming-Chin Chuang et al. [15] proposed a mechanism for AAA to reduce the authentication delay. Jie et al. [16] proposed an AAA framework using a foreign network's AAA server cache mechanism to reduce the delay in authentication process. Seong Yee Phang et al. [17] proposed a framework with access control mechanism to be used between the network nodes and service providers by introducing firewalls and AAA server. Panagiotis Georgopoulos et al. [18] proposed architecture to secure the MN by having IPSec, RADIUS AAA and Transport Layer Security. Julien Bournelle et al. [19] explored a three deployment scenarios such as MR-pan in the fixed infrastructure, MR-bus in the fixed infrastructure and MR-pan in the MR-bus and also they proposed architecture based on the two works done by Saber Zrelli et al. [20] and Ng C et al. [21].

From the literatures, it is found that a robust AAA framework is needed to secure the NEMO communications in the aspect of authentication and authorization. Though existing frameworks suggest different AAA mechanisms, few issues were found during simulation and analysis. Low-configured mobile devices took more time to complete the security procedures and some devices couldn't complete due to the computation processes. The paths between mobile devices and mobile routers are still vulnerable to security attacks.

III. AAA FRAMEWORK FOR NETWORK MOBILITY ENVIRONMENT (AF-NEMO)

A robust AAA framework is the need of the hour to provide a secured environment to the NEMO users. Device authentication must be performed effectively before starting the user authentication, because, the automated hacking software must be restricted in order to mitigate the Denial-of-Service (DoS) attacks. The devices involving in the communication must be genuine so that the legitimate users will not be affected. The major players of NEMO, namely, Mobile Router (MR), Visiting Mobile Node (VMN), Local Mobile Node (LMN) and Local Fixed Node (LFN) are to be authenticated to provide a secured environment to the NEMO users.

The framework, AF-NEMO consists of three different mechanisms, namely, AMR-NEMO, AVM-NEMO and ALM-NEMO. Each mechanism has different set of procedures to executed based on the various scenarios. AMR-NEMO has HomeReg_MR(), InitAuth_MR() and ReAuth_MR() procedures. AVM-NEMO has AuthHN_VMN(), AuthFN_VMN() and ReAuth_VMN() procedures. ALM-NEMO has HomeReg_LMN(), AuthHN_LMN() and AuthFN_LMN() procedures. Figure 1 shows proposed mechanisms along with the procedures.

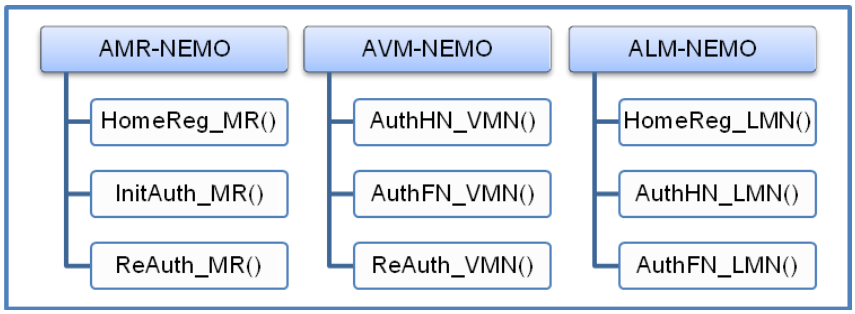

Fig. 2. AF-NEMO Framework

A. AMR-NEMO

AMR-NEMO is proposed to perform AAA operations on MR. Three different deployment scenarios are considered. The first scenario is that MR comes into a HN for the first time and registers itself in the network. During the registration process, MR may have MNNs attached. For performing AAA for those MNNs mechanisms are proposed in the following sections. The second scenario is that after the registration, MR is authenticated by having the credentials provided at the registration process. The third scenario is that MR is authenticated after the initial authentication. In the third scenario, routers of FN already holds all the credentials of MR. So, the number of control signals are reduced which are used for authentication purpose. By considering these three scenarios, three procedures are implemented, namely, HomeReg(), InitAuth() and ReAuth().

For the first scenario that is the registration process, HomeReg() is implemented. InitAuth() is implemented for the second scenario and ReAuth() is implemented for the third scenario. NEMO BS protocol takes care of the decision making on the procedures to be called for the different scenarios.

The following procedure is running in the NEMO BSP to perform AAA on MR.

```
Procedure AMR-NEMO
begin
Listen-Signals
 if Signals[‘fresh’] = = 1
  call HomeReg()
 else if Signals[‘fresh’] = = 0 AND Signals[‘auth-done’] = = 0
  call InitAuth()
 else if Signals[‘fresh’] = = 0 AND Signals[‘auth-done’] >=1
  call ReAuth()
endif
end
```

B. AVM-NEMO

VMNs are from different network where MR and the routers of FN have no pre-relationship. Existing mechanisms proposed a single procedure to be used for VMN and LMN. But, in reality, there are two different procedures needed for VMN and LMN. The proposed mechanism, AVM-NEMO performs AAA for VMN. The credentials are available at the AAA server of FN and for performing AAA, MR communicates with AAA-F. The VMN is to authenticated in three different scenarios. The first scenario is that VMN tries to access the MN via MR while MR is roaming within its HN. MR has to be authorized to add one more node that is VMN in its MN and AR has to authorize in this way. MR communicates with MR of VMN through its HN’s MR. The communication paths are different from each other. The second scenario is that VMN tries to access MN while MR is roaming in FN. In this scenario, MR requests ARs (AAAH and AAAF) of both FN and HN. The third scenario is that VMN requests MR for the second time or at the next time. Authenticating VMN takes less time because MR already holds the credentials of VMN. Due to security concern the DC is changed often. MR requests AAA server of VMN to provide a new DC to authenticate VMN. Based on these scenarios, three different procedures, namely, AuthHN_VMN(), AuthFN_VMN() and ReAuth_VMN() have been implemented accordingly.

The following procedure is running in the NEMO BSP to perform AAA on VMN.

```
Procedure AVM-NEMO
begin
Liten-Signals
 if Signals[‘fresh’] = = 1 AND Roam = = HN
  call AuthHN_VMN ()
 else if Signals[‘fresh’] = = 1 AND Roam = = FN
  call AuthFN_VMN()
 else if Signals[‘fresh’] = = 0 AND Signals[‘auth-done’] >=1
  call ReAuth_VMN()
 endif
end
```


C. ALM-NEMO

LMNs are different from VMNs. The mechanism used for VMN cannot be used for LMN, because, the credentials are to be verified at different places and the network to which they belong are completely different. Many researchers proposed a single mechanism to be used for both LMN and VMN. ALM-NEMO is proposed here for performing AAA for LMNs based on three different scenarios. Before accessing the network, LMN is registered with its home network. When MR is in HN and the LMN is trying to access the network which is considered as a second scenario. In the third scenario, MR is roaming in FN and LMN is trying to access the network. The first scenario is mandatory and the LMN cannot omit this process. The second and third scenarios are depending on the location of LMN.

The following procedure is followed in NEMO BSP for LMN:

```
Procedure ALM-NEMO
begin
Liten-Signals
 if Signals[‘fresh’] = = 1 AND Roam = = HN
  call HomeReg()
 else if Signals[‘fresh’] = = 0 AND Signals[‘auth-done’] = = 0   AND Roam = = HN
  call AuthHN_VMN()
 else if Signals[‘fresh’] = = 0 AND Signals[‘auth-done’] >=1 AND Roam = = FN
  call AuthHN_VMN()
endif
end
```

IV. SIMULATION

The configuration of the MNNs is setup dynamically from lower-end to higher-end. The processors are configured from 100 MHz to 1.2 GHz and both single and dual core are used. The RAM is fixed dynamically from 64 MB to 512 MB. For the application development, Android 2.3 (Gingerbread), Android 4.0 (Ice Cream Sandwich) and Android 4.1 (Jelly Bean) are used. The IP addresses are allotted with various prefixes. The prefixes, fc00::/7 used as Unique Local Addresses (ULA) and 2000::/3 used for public access are used for the simulation. A^{3}NeMo-Sim is a tool developed for simulating the AF-NEMO framework and the individual scenarios are simulated using NS2.

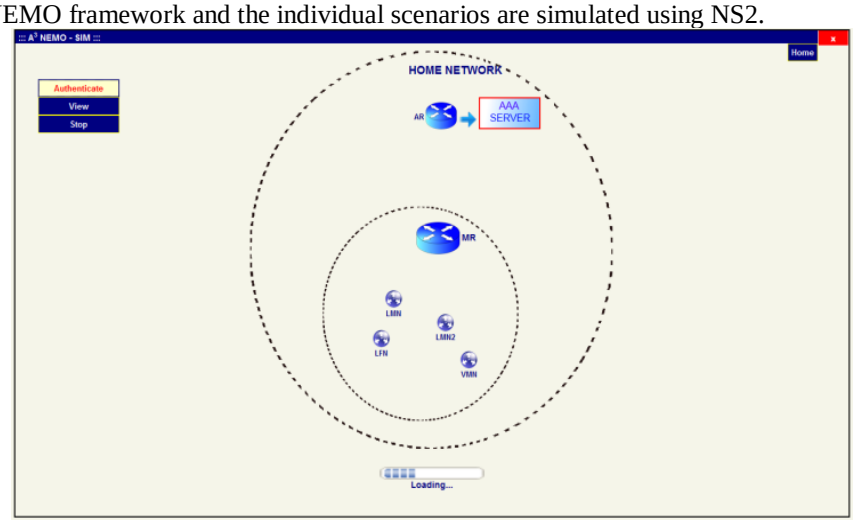

Fig. 3. Home Registration Procedure for MR

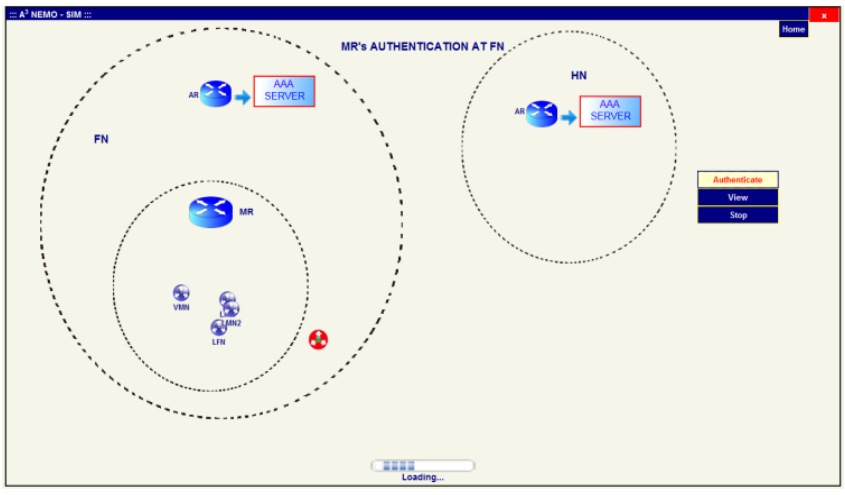

Fig. 4. Simulation of Initial Authentication Procedure for MR

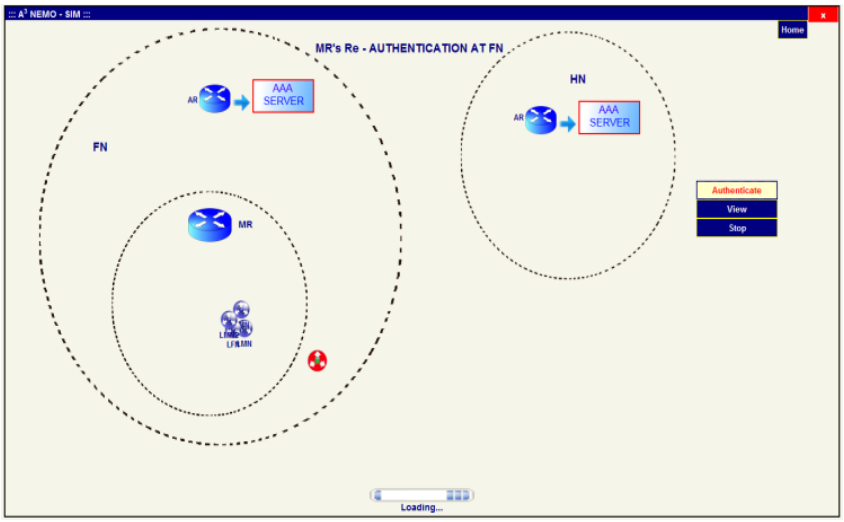

Fig. 5.Simulation of Re-Authentication of MR

Figure 3, 4 and 5 show the samples of simulations executed at various stages. The aim of the research, enhancing the security with less delay in authentication is achieved and it is verified using the simulation. The proposed mechanisms are integrated and a framework is developed. The proposed mechanisms are working well as an integrated system and also as an individual component. Based on the request and location of the MNNs, different mechanisms are invoked and the appropriate procedures are executed.

The proposed framework, AF-NEMO secures the NEMO environment by having three different mechanisms. During simulation of the framework, a hacker node is placed intentionally to check the security of the environment. The hacker node is capturing all the messages and trying to replay the messages. The proposed mechanism protects this replay attacks, because, DC is changed often by the AAA servers. The mechanisms use hash functions (SHA-256) to ensure the integrity of the message. Whenever a message sent to another node for authentication, all parts of the messages are used to create a hash value and the hash value is appended with the original message. On the receiving end, the same hash function is used and the hash value is created. The newly created hash value matched against the hash value received from the sender. If these two hashes are equal, the sender confirms that the message is not modified. While protecting from the replay attacks, the framework also protects from man-in-the middle and non-repudiation issues.

The proposed framework reduces the delay in authentication process while comparing with the existing mechanisms. The parameters used to authenticate MNNs take lesser time to be generated and to be distributed over the mobile network.

V. CONCLUSION

The proposed framework, AF-NEMO is developed to secure the NEMO environment. AF-NEMO consists of three different mechanisms, namely, AMR-NEMO, AVM-NEMO and ALM-NEMO. All these three mechanisms have three different procedures each. AF-NEMO secures the NEMO environment from replay attacks, man-in-the middle problem and non-repudiation issues. AF-NEMO reduces the delay in authentication process using light weight parameters. Simulation results show that the proposed framework achieves its aim by having the proposed mechanisms. In future the framework will be enhanced to adopt the user authentication mechanisms.

REFERENCES

[1] Devarapalli V, Wakikawa R, Petrescu A, Thubert P, “Network Mobility (NEMO) Basic Support Protocol”, RFC 3963, January 2005

[2] Isac Gnanaraj J, Arockiam L, “AAA Mechanism for Mobile Router in Network Mobility Environment”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 10, December 2012, ISSN: 2278–1021, pp.832-836

[3] Arockiam L, Isac Gnanaraj J, “AAA Mechanism for Visiting Mobile Node in Network Mobility Environment”, International Journal of Advanced Research in Computer Science and Software Engineering, January 2013, ISSN: 2277-128X, pp. 195-199

[4] Arockiam L, Isac Gnanaraj J, “AAA Mechanism for Local Mobile Node in Network Mobility Environment”, International Journal of Computer Networks and Wireless Communications, January 2013, ISSN: 2250-3501, pp. 8-12

[5] de Laat C, Gross G, Gommans L, Vollbrecht J, Spence D, "Generic AAA Architecture", RFC 2903, August 2000

[6] Vollbrecht J, Calhoun P, Farrell S, Gommans L, Gross G, de Bruijn B, de Laat D, Holdrege M, D Spence, "AAA Authorization Framework", RFC 2904, August 2000

[7] Julien Bournelle, Guillaume Valadon, David Binet, Saber Zrelli, Maryline Laurent-Maknavicius, Jean-Michel Combes, "AAA considerations within several NEMO deployment scenarios", Proceedings of the International Workshop on Network Mobility, Japan, January 2006
[8] Rigney C, Rubens A, Simpson W, Willens S, "Remote Authentication Dial In User Service", RFC 2865, June 2000
[9] Calhoun P, Loughney J, Guttman E, Zorn G, Arkko J, "Diameter Base Protocol", RFC 3588, September 2003
[10] V. Fajardo, J. Arkko, J. Loughney, G. Zorn, "Diameter Base Protocol", RFC 6733, October 2012
[11] Garcia-Martin M, Belinchon M, Pallares-Lopez M, C. Canales-Valenzuela, K. Tammi, "Diameter Session Initiation Protocol (SIP) Application", RFC 4740, November 2006
[12] Korhonen J, Bournelle J, H. Tschofenig, C. Perkins, K. Chowdhury, "Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction", RFC 5447, February 2009
[13] A. Patel, G. Giaretta, "Problem Statement for Bootstrapping Mobile IPv6 (MIPv6)", RFC 4640, September 2006
[14] David Binet, Antony Martin, Brahim Gaabab, "A Proactive Authentication Integration for the Network Mobility", Proceedings of the IEEE International Conference on Wireless and Mobile Communications, France, March 2007, pp. 53-58
[15] Ming-Chin Chuang, Jeng Farn Lee, "LMAM: A Lightweight Mutual Authentication Mechanism for Network Mobility in Vehicular Networks", Proceedings of IEEE Asia-Pacific Services Computing Conference, December 2008, pp. 1611-1616
[16] Zhang Jie, LIU Yuan-an, MA Xiao-lei, JIA Jin-tao, "AAA authentication for network mobility", Journal of China Universities of Posts and Telecommunications - ScienceDirect, April 2012, Volume 19, Issue 2, pp. 81-86
[17] Seong Yee Phang, HoonJae Lee , Hyotaek Lim, "A Secure Deployment Framework of NEMO (Network Mobility) with Firewall Traversal and AAA Server", Proceedings of International Conference on Convergence Information Technology, November 2007, pp. 352-357
[18] Panagiotis Georgopoulos, Ben McCarthy, Christopher Edwards, "A Collaborative AAA Architecture to Enable Secure Real-World Network Mobility", Springer LNCS 6640, Part I, 2011, pp. 212-226
[19] Julien Bournelle, Guillaume Valadon, David Binet, Saber Zrelli, Maryline Laurent-Maknavicius, Jean-Michel Combes, "AAA considerations within several NEMO deployment scenarios", Proceedings of the International Workshop on Network Mobility, Japan, January 2006
[20] Saber Zrelli, Thierry Ernst, Julien Bournelle, Guillaume Valadon, David Binet,"Access Control Architecture for Nested Mobile Environments in IPv6", Proceedings of the 4th Conference on Security and Network Architecture, France, June 2005
[21] Ng C, Tanaka T, "Usage Scenario and Requirements for AAA in Network Mobility Support", October 2002, IETF's draft-ng-nemo-aaa-use-00.txt
[22] Tat Kin Tan, Azman Samsudin, "Efficient NEMO Security Management via CAPKI", Proceedings of IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, Malaysia, May 2007, pp. 140-144.

