Volume 3, Issue 1, January 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# AAA Mechanism for Visiting Mobile Node in Network Mobility Environment

**Arockiam L**
*Department of Computer Science, St. Joseph's College, Trichy, India*

**Isac Gnanaraj J**
*Department of Computer Science, St. Joseph's College, Trichy, India*

***Abstract— Due to the huge demand for mobile applications and devices, many new technologies and mechanisms are being invented. Network Mobility (NEMO) is a kind of deployment scenario where an entire network moves from one location to another location. While changing the point of attachment, there is possibility for the hacker to interrupt communication and to claim it as a genuine node. Authentication, Authorization and Accounting (AAA) become inevitable in security. Authentication is the key solution to protect from many security attacks because it authenticates the nodes before accessing the network. The Visiting Mobile Node (VMN) is to be authenticated because it belongs to another Foreign Network (FN). The loyalty of the VMN must be ensured before providing access to the Mobile Network (MN). The credentials of the VMN reside at the AAA (AAA-VMN) server of the VMN's Home Network (HN). The Mobile Router (MR) must verify the credentials submitted by the VMN, with the AAA-VMN. Here, an AAA mechanism for ensuring the loyalty of the VMN is proposed by considering the computational power of the VMN and the mechanism is simulated.***

***Keywords— NEMO, Security, Authentication, Authorization, digital certificate***

## I. INTRODUCTION

Each day mobile networks receive a large number of new users and devices. The service providers put in a lot of effort and perform research to accommodate the increasing number of users. When the number of users increases, the congestion and traffic jam problems arise. NEMO was proposed by the IETF in RFC 3963 [1] to overcome such difficulties. NEMO supports mobility of a whole network where as host mobility supports only mobility of single node. A set of nodes together form a network called MN that can move from one network to another network is led by a node called MR. On behalf of the all the nodes of MN, the MR connects with the Access Router (AR). Every communication to the Mobile Network Nodes (MNN) passes through the MR. MR along with its nodes can change its point of attachment at any time without disturbing the session continuity. When MR moves from HN to FN, MR obtains another address called Care-of-Address (CoA). MR requests HA to update its CoA. This process is called Binding Update (BU). After binding CoA with its original address, HA sends Binding Acknowledgement (BA) to MR. AR verifies the loyalty of MR, before providing access to the Internet.

VMN is a node which belongs to another FN. When the VMN tries to access the MR, the MR authenticates the VMN before providing service to the VMN. Existing mechanisms considered authentication process same as the Local Mobile Nodes (LMN). The VMN is different from the LMNs. For authenticating the LMNs, MR requests its AAA-Home server (AAA-H) to verify the loyalty of the LMNs. All the credentials of the LMN are available in the HN itself. But, for authenticating VMN, MR has to contact the AAA server of VMN's HN (AAA-V) and also the AAA-H. MR needs to be authorized by AAA-H to provide access to the VMN and authenticates the VMN by contacting the AAA-V. All the credentials of the VMN reside at the AAA-V.

## II. MOTIVATION AND OBJECTIVES

Many research works focus on providing a robust AAA mechanism to the NEMO environment which was standardized and documented by IETF [1]. de Laat et al. [2] proposed the Generic AAA architecture and it was documented by IETF in RFC 2903 which was developed based on the framework proposed by Vollbrecht J et al. [3]. It was developed to support multi-domain environment and multiple service providers. A network of cooperating generic AAA servers communicating via a standard protocol was included to develop this architecture. Julien Bournelle et al. [4] and few researchers revealed that the Generic AAA architecture lacks in providing effective AAA mechanisms to protect the NEMO environment.

A protocol for carrying authentication, authorization, and configuration information between a Network Access Server (NAS) which desires to authenticate its links and a shared Authentication Server is called Remote Authentication Dial In User Service (RADIUS) [5]. The Diameter base protocol [6] was developed to provide an AAA framework for applications like network access or IP mobility. Diameter was developed to work in both local and roaming situations. It is considered as an alternative for RADIUS. David Binet et al. [7] proposed an AAA architecture based on Protocol for Carrying Authentication Network Access (PANA), Diameter and EAP for a multi-operator environment. Ming-Chin

 

Chuang et al. [8] proposed a mechanism for mutual authentication by combining an AAA model with NEMO. The mechanism proposed by them aimed to lower computation and local authentication. The pre-shared secret values were used between AAA servers for authenticating the MNNs. This makes the network vulnerable to man-in-the-middle attacks and impersonation attacks. A framework based on AAA was proposed by Zhang Jie et al. [9] where a foreign network's AAA server cache mechanism was used to reduce the delay in authentication process. IDs and certificates were mentioned in their framework but, the details are insufficient and the cache mechanism causes delay in the authentication process because it maintains a timetable for the nodes coming from another network and it is decreased while the node moves away from the network. The entries into the table are restricted to 10. If more than 10 nodes come inside the network, the server may not work properly because of the limited space which is allocated to store the details of the nodes. The messages passed from AAA-Home (AAAH) to MNN and from MNN to MR give a chance to hackers to capture and use it for replay attacks. All the messages have to be passed through the AR, MR and HA. They did by-pass these nodes and passed the messages directly to the AAA server. Direct access to the AAAH or AAAF is vulnerable.

Many research works focused on protecting the communication happening in the NEMO environment. Seong Yee Phang et al. [10] proposed a framework to provide an access control mechanism between the network nodes and service providers using firewalls and AAA server. They introduced a new entity called AAA Server to authenticate the MNNs. Introducing a new element in the existing architecture may force the service providers to modify the entire structure and the protocol. Panagiotis Georgopoulos et al. [11] proposed an architecture to secure the MN. They presented an overview of NEMO BS, IPSec, RADIUS AAA, Transport Layer Security (TLS) based authentication methods and wireless security techniques. Based on all these techniques, they proposed the architecture. Bournelle et al. [12] suggested three deployment scenarios on which the AAA mechanisms are being executed. The deployment scenarios are: MR-pan in the fixed infrastructure, MR-bus in the fixed infrastructure and MR-pan in the MR-bus. They proposed the architecture based on the two works done by Saber Zrelli et al. [13] and Ng C et al. [14]. In the first work, an authentication architecture based on the access control mechanisms was proposed to offer basic authentication in nested mobile environments. In the second work, a basic AAA model for NEMO and various usage scenarios were described. From the scenarios, a set of AAA requirements in NEMO was drawn. The architecture was developed to adopt the three deployment scenarios discussed above. Tat kin et al. [15] proposed a solution for authentication using random number coupled with PKI concept. The solution fully depends on Certification Authority (CA) which is maintained by third party. Authenticating MR is also an important task because, the nodes of the MN communicate with the external users and devices through the MR. An AAA mechanism for the MR was proposed in [16].

## III. AAA MECHANISM FOR VMN IN NEMO (AVM-NEMO)

Authenticating VMN is an important task in the NEMO environment because it does not have any previous relationship with the MR or MN. As VMN belongs to a FN, all the credentials of VMN are available at AAA-V. The MR contacts the AAA-V and receives the credentials to verify and allow the VMN in the MN. Providing authentication with less computation power mechanism is the goal of this research work. Whenever authentication process is started, the authorization and accounting processes become inevitable. VMN at any time is able to change its point of attachment. Whenever the VMN moves from its HN to FN and comes under MR, three different procedures are executed. The first procedure is executed, when the VMN tries to access the MR while the MR is roaming within the HN. The second procedure is executed when the VMN requests access to MR while the MR is roaming in the FN. The third procedure is executed when the VMN moves into the MN after its first visit. The messages passed between the nodes for authentication purpose are taken for generating the hash values. The hash values are added with the original message in order to maintain the integrity of the message. The timestamp and the serial numbers are used to avoid replay attacks. The random number is used along with the IP and MAC addresses to form the digital certificates. Periodically the random number is changed by the AAA-H to avoid the replay and eavesdropping attacks.

### *A. Authentication when MR in HN*

The first procedure is executed whenever the VMN requests access to the MR, while MR is in its HN. When VMN comes at the first time, it sends request message to access Internet via MR, along with the BU request message.

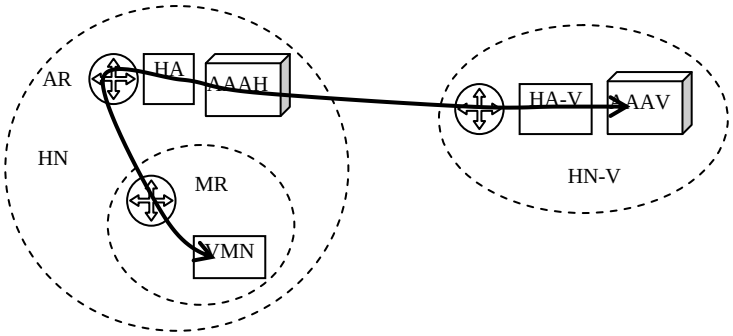


Fig.1. Authentication of VMN when MR in HN

Fig. 1 shows the diagrammatic representation of the authentication process which is executed when MR roams within its HN.

The registration and authentication procedure is as follows:

 

1. VMN → MR: (Reg_Req$_{VMN}$, BU)
2. MR → AAA-H: (Reg_Req$_{VMN}$, Permit_Nodes$_{n+1}$)
   MR asks permission to add one more node in its MN.
3. MR → VMN: PUK$_{VMN}$(Req_MAC$_{VMN}$, Req_MNP$_{VMN}$, Req_IP$_{VMN}$, Req_DC$_{VMN}$, S$_{No}$, T$_{Stamp}$)
   Based on the permission from the AAA-H, MR replies to the VMN.
   MR requests VMN to send the credentials of the VMN for authentication purpose.
   It asks the Digital Certificate (DC) for ensuring the loyalty of the node.
4. VMN → MR: PUK$_{MR}$ (MAC$_{VMN}$, MNP$_{VMN}$, IP$_{VMN}$, DC$_{VMN}$, S$_{No}$, T$_{Stamp}$)
   VMN sends the credentials to MR to verify its loyalty.
5. MR → HA-V → AAA-V: PUK$_{HA-V}$ (DC$_{VMN}$, MNP$_{VMN}$, IP$_{VMN}$, Z$_{VMN}$, ACC$_{VMN}$)
   MR requests the AAA-V via HA-V to verify the credentials of the VMN.
   Authorization and Accounting details are also requested to know whether VMN has sufficient permission and account to be allowed for accessing the MN.
6. MR → VMN: PUK$_{VMN}$(BA, CoA$_{VMN}$)
   Based on the reply from the AAA-V, MR replies to VMN.
   VMN sets up its network configurations based on the received CoA.
   MR starts an account for the new VMN for billing purpose.

Computing and processing the whole PKI is not easy for the mobile nodes which have low computation power. The public and private keys are used to encrypt and decrypt the message respectively. The computation and distribution of the keys are carried out by the AAA servers, instead of going to the third party called, certificate authority (CA). VMN uses the keys and simply performs the encryption and decryption.

*B. Authentication when MR in FN*

The second procedure is executed while MR is roaming in the FN and VMN is trying to access the MR for the first time. The messages used to authenticate the VMN, pass through the AR of the FN.

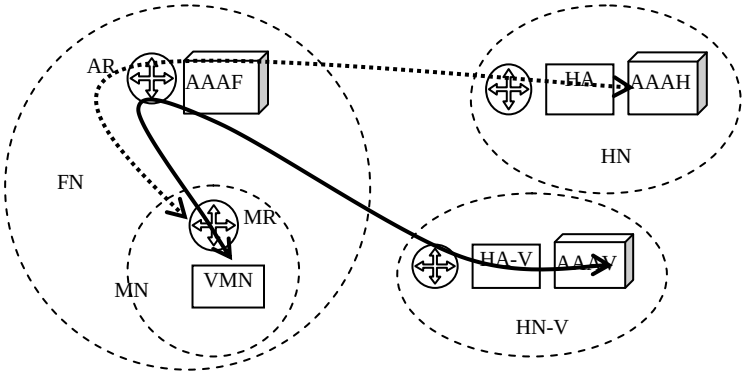


Fig. 2. Authentication of VMN when MR in FN

Figure 2 shows the diagrammatic representation of the authentication process which is executed when MR roams into another network. The dotted line shows the permission request of MR to AAA-H for adding one more node and the line without dots shows the authentication messages passed between the MR and AAA-V through the AR of the FN.

The registration procedure is as follows:

1. VMN → MR: (Reg_Req$_{VMN}$, BU)
2. MR → AR → AAA-F → HA → AAA-H: PUK$_{AR}$(Reg_Req$_{VMN}$, Permit_Nodes$_{n+1}$)
   Based on the permission from the AAA-H, AR replies to MR and MR replies to VMN
3. MR → VMN: PUK$_{VMN}$(Req_MAC$_{VMN}$, Req_MNP$_{VMN}$, Req_IP$_{VMN}$, Req_DC$_{VMN}$, S$_{No}$, T$_{Stamp}$)
4. VMN → MR: PUK$_{MR}$ (MAC$_{VMN}$, MNP$_{VMN}$, IP$_{VMN}$, DC$_{VMN}$, S$_{No}$, T$_{Stamp}$)
5. MR → HA-V → AAA-V: PUK$_{HA-V}$ (DC$_{VMN}$, MNP$_{VMN}$, IP$_{VMN}$, Z$_{VMN}$, ACC$_{VMN}$)
   Based on the reply from the AAA-V, MR replies to VMN.
6. MR → VMN: PUK$_{VMN}$(BA, CoA$_{VMN}$)
   VMN sets up its network configurations based on the received CoA
   MR starts account for the new VMN for billing purpose

*C. Re-Authentication*

The third procedure called Re-Authentication is executed when VMN comes back to MR after its first visit. During its first visit, MR stores all the credentials of VMN. When VMN comes back, MR receives the credentials from VMN and verifies against the entries already available in it. Periodically, the DC is changed. So, MR requests VMN to resend the DC and it verifies with the AAA-V.

The procedure is as follows:

1. VMN → MR: PUK$_{MR}$(Reg_Req, DC$_{VMN}$, MNP$_{VMN}$, IP$_{VMN}$, S$_{No}$, T$_{Stamp}$)
2. AR: DC$_{VMN}$ == DC$_{AAA-V}$
   If Not_Match
   MR→ HA-V → AAA-V: PUK$_{HA-V}$(Resend_DC$_{AAA-V}$, CoA$_{VMN}$, IP$_{VMN}$, MNP$_{VMN}$)

 

MR: Verifies the digital certificate with the previous certificates. If the certificate is not matched, then AR sends request to AAA-V to resend or send the new certificate. Due to security and to protect from replay attacks and passive eaves dropping the certificate is changed over the time.

3. MR → HA-V → AAA-V: $PUK_{HA\text{-}V}(Z_{VMN}, ACC_{VMN})$
   Before granting access MR checks the authorization and accounting details once again with the AAA-V.
4. MR → VMN: $PUK_{MR}(CoA_{MR}, S_{NO}, T_{Stamp})$
   If the CoA is available again for the MR, then the same CoA is used or else the new CoA is assigned. VMN sets up its network according to the new CoA.

Before granting access to the VMN, MR checks whether it is allowed to add VMN again. It checks the number of nodes already available in the MN. During the absence of VMN some other node may have entered into MN. If another VMN has entered into the MN, MR requests AAA-H to add one more node in the MN, MR → AR → AAA-F → HA → AAA-H: $PUK_{AR}$ ($Reg\_Req_{VMN}$, $Permit\_Nodes_{n+1}$).

## IV. RESULTS AND DISCUSSIONS

The proposed mechanism, AVM-NEMO uses the light weight parameters for securing NEMO environment by considering the computational ability of the mobile devices. Existing mechanisms considered both VMN and LMN as the same and executed the AAA procedures. VMN differs from LMN and LFN. In the proposed mechanism, the AAA procedures are executed only for the VMN. AVM-NEMO is proposed only for VMN and it does not consider the VMN and LMN as the same.

During the simulation of the proposed mechanism, the AAA procedures take less time and the mobile devices very easily convert the plain text into cipher text and vice versa. Existing mechanisms take much time and processing power for such procedures. The configuration of the mobile devices is fixed randomly with the processor below 50 MHz. When verifying the DC, the hash value is changed by AAA servers by changing the RNo periodically.

At the first time, the DC is sent as

`975b9ab014ed710343b658b3f52c822bf22b0f3af0769f0dffff8760cefe58a1.`

At the second time the DC is sent as

`af05c87702cade1206d44dbbc53846864f2edcd3e664ee0d47515217cfd384ad.`

This change restricts the replay attacks.

The proposed mechanism protects the NEMO environment from replay attacks, non-repudiation and violation against message integrity. Protecting from these attacks makes the NEMO environment safe from man-in-the-middle attack and denial of service attacks. The $R_{No}$, $S_{No}$, and $T_{Stamp}$ are used to avoid the replay attacks. The attacker cannot assume or calculate the $R_{No}$ because it is done by the AAA server. For generating $S_{No}$, the AAA server uses different calculations. The hash function is used to ensure the message integrity. The hash value is appended with the original message and sent to the receiver. The receiver generates the hash value by having the original message and verifies against the received hash value. The public and private keys are used to ensure that there is no possibility of non-repudiation.

## V. CONCLUSION

AVM-NEMO is proposed to perform AAA in the NEMO environment to secure communication by considering the computational power of mobile devices. VMN is authenticated at MN to gain access to the Internet via MR. When VMN tries to access the MN, three procedures are executed. The procedures are executed when MR roams in HN, in FN and when VMN moves back into the same MN. Simulation results show that the proposed mechanism, AVM-NEMO secures the NEMO environment and makes the processes easier for the mobile devices. VMN is treated as a separate node from the LMN and LFN, as it belongs to another network. The proposed mechanism considers device authentication and in future user authentication will be taken into consideration.

## ACKNOWLEDGMENT

This research work is supported by University Grants Commission, Government of India under the Minor Research Project scheme. Ref. No.: F. MRP-4044/11 (MRP/UDC-SERO).

## REFERENCES

[1] Devarapalli V, Wakikawa R, Petrescu A, Thubert P, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005
[2] de Laat C, Gross G, Gommans L, Vollbrecht J, Spence D, "Generic AAA Architecture", RFC 2903, August 2000
[3] 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
[4] 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
[5] Rigney C, Rubens A, Simpson W, Willens S, "Remote Authentication Dial In User Service", RFC 2865, June 2000
[6] Calhoun P, Loughney J, Guttman E, Zorn G, Arkko J, "Diameter Base Protocol", RFC 3588, September 2003
[7] 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

 

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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

[15] 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

[16] 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, pp. 832-636

 