AAA Mechanism for Local Mobile Node in Network Mobility Environment

Arockiam L
Associate Professor in Computer Science,
St. Joseph's College (Autonomous)
Tiruchirappalli, India

Isac Gnanaraj J
Research Scholar in Computer Science,
St. Joseph's College (Autonomous)
Tiruchirappalli, India

***Abstract*— Network Mobility (NEMO) is a kind of mobility deployment scenario where a group of nodes form a network and moves from one network to another network that is led by a node called Mobile Router (MR). NEMO Basic Support (NEMO BS) protocol enables a whole network to move and to change its point of attachment. Providing security is an important task because of increasing number of users. Authentication, Authorization and Accounting (AAA) are the parts of security management. NEMO BS lacks in providing a robust AAA service to its mobile nodes. Existing mechanisms focused on providing AAA but they treated the Local Mobile Node (LMN), Local Fixed Node (LFN) and Visiting Mobile Node (VMN) as same. LMN belongs to same Mobile Network (MN) where its MR exists. VMN belongs to another network and new to the MN. A new AAA mechanism for LMN is proposed in this paper. The parameters and the calculations considered in this mechanism secures NEMO environment and take less time to complete the AAA processes. The simulation of the proposed mechanism shows better result.**

Keywords-NEMO; Security; Authentication; AAA;

I. INTRODUCTION

Every day, mobile network grow with a huge number of new users and devices. When the number of users increases, the service providers put in their efforts to accommodate all the users. Signaling and traffic jam problems also occur when the network adds more number of users. To overcome these problems, a new deployment called, NEMO was introduced. NEMO BS protocol was developed based on IPv6 it was standardized and documented by Inter Engineering Task Force (IETF) in RFC3963 [1]. Another deployment called host mobility is suffered by the traffic and signaling overhead problems. NEMO has many advantages like session continuity and support for moving a whole network, etc. In NEMO, a set of nodes move from one network to another network with session continuity and one of the nodes acts as a router called MR. The mobile nodes of MN communicate with external nodes through MR. MR supports NEMO BS and has an interface to connect all the nodes of MN as well as the external antenna or Access Router (AR). MR along with its mobile nodes can change its point of attachment at anytime. MR and its nodes are identified by Home Address (HoA) which is assigned by Home Network (HN). MR is assigned a new address called Care-of-Address (CoA), when MR moves into another network called Foreign Network (FN). MR sends Binding Update (BU) request to its Home Agent (HA) to update its new CoA. HA sends back Binding Acknowledgement (BA) message. The messages addressed to MR are redirected to its CoA by HA.

MN has four kinds of nodes, namely, MR, LMN, LFN and VMN. MR is a router which takes care of the entire communication of MN. LMN and LFN belong to MN where LMN can change its point of attachment and LFN is a fixed node. VMN belongs to another FN and now it accesses the Internet via MR. Though NEMO has a lot of benefits, it lacks in providing a secured environment to its users. Based on the literature review presented in the Section 2, it is found that NEMO BS does not provide a robust AAA service to its users and still many research works are going. An AAA mechanism called ALM-NEMO is proposed to secure the NEMO environment.

II. MOTIVATION AND RELATED WORKS

Many researchers contributed their mechanisms to secure NEMO environment. Based on a framework proposed by Vollbrecht J et al. [2], Generic AAA architecture was proposed by de Laat et al. [3] and it was documented by IETF in RFC 2903. It was aimed to create a generic framework which would allow complex authorizations to be executed through a network of AAA servers. Few researchers like Julien Bournelle et al. [4] criticized that the Generic AAA architecture lacks in providing an effective AAA mechanisms to protect the communications. Remote Authentication Dial In User Service (RADIUS) [5] is a protocol for carrying authentication, authorization, and configuration information between a Network Access Servers (NAS) which need to authenticate its links and a shared Authentication Server. RADIUS was developed as an access server authentication and accounting protocol.

Diameter [6] [13] is an AAA protocol and it is considered as an alternative to RADIUS. Many research works were carried out based on the Diameter protocol. Calhoun et al. [7] developed an application which allows Diameter server to authenticate, authorize and collect accounting information for Mobile IPv4 services rendered to a mobile node. Combined with the Inter-Realm capability of the base protocol, it enabled mobile nodes to receive service offered by foreign service providers. Diameter Accounting messages were used by the foreign and home agents to transfer usage information to respective servers. Hakala et al. [8] developed a Diameter application that was used to implement real-time credit-control for a variety of end user services such as network access, Session Initiation Protocol (SIP) services, messaging services, and download services. Eronen et al. [9] proposed an Extensible Authentication Protocol (EAP) which provided a standard mechanism for support of various authentication methods. Garcia-Martin et al. [10] proposed a Diameter SIP application that enabled the Diameter client to request AAA information. It was designed to be used 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. Korhonen et al. [11] described MIPv6 bootstrapping using the Diameter NAS to home AAA server interface. They addressed the AAA functionality required for the MIPv6 bootstrapping solutions outlined in RFC4640 [12], and focused on the Diameter-based AAA functionality for the NAS-to-HAAA (home AAA) server communication.

An AAA architecture based on Protocol for Carrying Authentication Network Access (PANA), Diameter and EAP for a multi-operator environment was proposed by David Binet et al. [14]. Ming-Chin Chuang et al. [15] proposed an AAA mechanism to reduce the authentication delay and to perform a local authentication. Pre-shared secret values between AAA servers were used for authenticating the MNNs. Some details lack like, how the AAA servers should communicate within them and what are the parameters to be considered. This makes the network vulnerable to man-in-the-middle attacks and impersonation attacks. Zhang Jie et al. [16] proposed a framework based on AAA where they used a foreign network's AAA server cache mechanism to reduce the delay in authentication process. The cache mechanism used in their mechanism increases delay in the authentication process. Because, it maintains a timetable for the nodes coming from another network and it is decreased while the node move away from the network. The entries into the table are restricted to 10. If more than 10 nodes are coming inside the network, then the server struggles to handle the processes. 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. According the NEMO BS protocol, the messages pass 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.

Seong Yee Phang et al. [17] proposed a framework to provide an access control mechanism between the network nodes and service providers by introducing firewalls and AAA server. Introducing a new element forces the service providers to modify the entire structure and the protocol. Panagiotis Georgopoulos et al. [18] proposed an architecture to secure the MN based on IPSec, RADIUS AAA and Transport Layer Security (TLS). Julien Bournelle et al. [19] explored a three deployment scenarios, namely, MR-pan in the fixed infrastructure, MR-bus in the fixed infrastructure and MR-pan in the MR-bus. They proposed an architecture based on the two works done by Saber Zrelli et al. [20] and Ng C et al. [21]. Tat kin et al. [22] 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. AAA Mechanism for Mobile Router was proposed in our previous research works [23].

Literature reveals that NEMO needs robust AAA mechanisms to secure its communications. Existing mechanisms proposed for AAA have issues at some places. At few places, existing mechanisms leave a place for replay attacks and the computations are heavier for the mobile devices. Computations proposed in the existing mechanisms can be carried out only by the high-end mobile devices. Mobile nodes of MN are different and VMNs belong to foreign networks. Same mechanism cannot be executed for all the nodes. Hence, different AAA mechanisms are needed. This proposed mechanism, ALM-NEMO provides AAA procedures for performing AAA on LMNs.

III. AAA Mechanism for LMN in NEMO (ALM-NEMO)

ALM-NEMO is an AAA mechanism proposed to perform AAA procedures to secure the NEMO environment by considering the computational time. While developing the mechanisms, the processor and the configuration of the mobile devices are considered. The proposed mechanism ALM-NEMO consists of three procedures. The first procedure is called Home Registration which is executed when LMN attempts to register with MN for the first time. The second procedure is executed when LMN tries to access MN while MR is roaming in HN. After the Home Registration procedure, LMN moves from HN to another FN. Later it comes back to MN. Whenever LMN moves away from HN, there is a possibility for a hacker to attack the network by replaying the previous messages. So, it is important to verify the loyalty of LMN, whenever it comes back to access MN. The third procedure is executed when MR roams in FN and LMN requests to access MN. All these procedures are simulated and the results are compared with the existing mechanisms.

A. Home Registration

Whenever LMN moves into the MN for the first time, it has to be registered and authenticated before getting access. During the registration, the credentials of LMN are stored in the AAA-H. MR stores some of the information for future authentication but due to the limited computation power and storage medium, few details are stored in the MR and rest of the details are available only at AAA-H. Generation of the keys is executed by the AAA-H because of the limited computation power of mobile devices.

The registration procedure is as follows:

1. LMN → MR: (Reg_Req_{LMN})

   LMN requests MR to register with the MN and HN.

2. MR → AAA-H: $PUK_{AAA\text{-}H}(Reg\_Req_{LMN}, Nodes_n, Permit\_Node_{n+1})$

MR forwards the request message to the AAA-H and requests to add one more node.

3. AAA-H → MR: $PUK_{MR}(S_{No}, R_{No\text{-}LMN}, T_{Reg\text{-}LMN})$

   Public and private keys of the LMN are generated by AAA-H and sent to MR

   $T_{Reg\text{-}LMN}$ – time of registration of the MR at HN

   S_{No} – Serial number to be incremented at each communication for avoiding replays

   $R_{No\text{-}LMN}$ – random is used to generate the DC

4. MR → LMN: $PUK_{LMN}(Req\_MAC_{LMN}, S_{No}, {}_{RNo\text{-}LMN}, T_{Reg\text{-}LMN})$

   MR asks the MAC address of LMN and sends the random number and registration time of LMN which is used to create DC.

5. LMN → MR: PUK_{MR} (MAC_{LMN}, S_{No})

   MR forwards the MAC address of LMN to AAA-H to form the DC.

6. AAA-H: $DC_{AAA\text{-}H}$ :: $H(MAC_{LMN}, R_{No}, T_{Reg})$

   MR: DC_{LMN} :: $H(MAC_{LMN}, R_{No}, T_{Reg})$

Hash function is used to create the Digital Certificate with the parameters of MAC address of LMN, a random number generated by AAA-H and registration time of LMN at HN.

Authorization (Z_{LMN}) information is sent to MR and LMN by AAA-H. The permission based on the request and account of the LMN.

Zi – authorization permissions for each node

Zi = { GZ_i, RZ_i, AZ_i, CZ_i, DZ_i }

LMN first sends request message to the MR during Router Solicitation (RS) and Router Advertisements (RA). Computing and processing the whole PKI are hard for the mobile nodes which have limited computation power. While sending a message, the public key of the receiver is used to encrypt the message and while receiving an encrypted message the private key of the receiver is used to decrypt the message. The computation and distribution of the keys are processed by the AAA-H instead of going to the third party called certificate authority (CA). The mobile nodes use the keys and simply perform the encryption and decryption operation. Authorization permissions are sanctioned based on the five categories, namely, Group/MN based (GZ_i), Role based (RZ_i), Account based (AZ_i), Attribute or Configuration based (CZ_i) and Request/Demand based (DZ_i).

B. Authentication when MR in HN

The second procedure is executed whenever the LMN requests access to the MR, while MR is in its HN. When LMN comes in to MN, it sends request message to access Internet via MR.

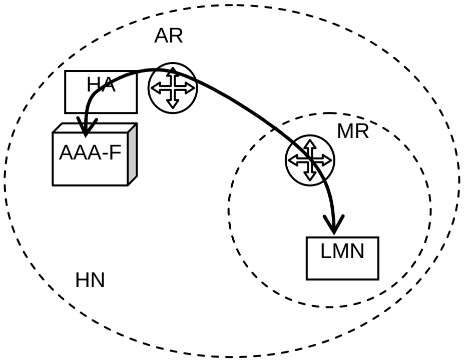

Fig. 1. Authentication of LMN when MR in HN

Figure 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. LMN → MR: $PUK_{LMN}(A\_Req_{LMN}, IP_{LMN}, DC_{LMN}, S_{No}, T_{Stamp})$

   LMN sends Access Request message to MR along with the parameters like IP and DC of LMN.

2. MR → AAA-H: $PUK_{AAA\text{-}H}(A\_Req_{LMN}, IP_{LMN}, DC_{LMN}, Req\_Z_{LMN}, Acc_{LMN}, S_{No}, T_{Stamp})$

   MR forwards the Request Message to AAA-H and requests the AAA-H to send the authorization and accounting details.

   While roaming into another network, authorization and accounting of LMN is changed based on the service utilized. So, it is important to get the details of LMN though it is registered with MR.

3. AAA-H → MR: $PUK_{MR}(Z_{LMN}, Acc_{LMN}, DC_{LMN}, S_{No}, T_{Stamp})$

   AAA-H responds MR with the details of authorization and accounting details along with the new DC of LMN. Periodically the DC is changed by having the new random number generated by AAA-H. During the absence of LMN, the DC of the LMN is changed by AAA-H.

4. MR → LMN: $PUK_{LMN}(Grant\_AAA, S_{No}, T_{Stamp})$

   Based on the permission from the AAA-H, MR replies to the LMN.

   Grant_AAA holds all information regarding authorization and accounting.

C. Authentication when MR in FN

The third procedure is executed while MR is roaming in the FN and LMN is trying to access the MR. The messages used to authenticate the LMN, passes through the AR of the FN.

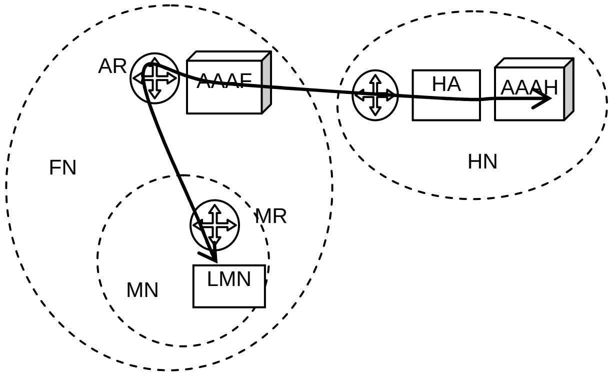

Fig. 2. Authentication of LMN when MR in FN

Figure 2 shows the diagrammatic representation of the authentication process which is executed when MR roams into another network.

The registration procedure is as follows:

1. LMN → MR: $PUK_{MR}(A\_Req_{LMN}, IP_{LMN}, DC_{LMN}, S_{No}, T_{Stamp})$

   LMN requests MR to access Internet via MR.

   MR receives the IP address and DC to verify the loyalty of LMN.

2. MR → AR : $PUK_{AR}(Req\_Nodes_{n+1}, IP_{LMN}, S_{No}, T_{Stamp})$

   MR requests AR of the FN to add LMN which belongs to MN.

   AR stores IPLMN under MR.

3. AR → MR: PUKMR(Grant_Node$_{n+1}$, S_{No}, T_{Stamp})

4. MR → AR → AAA-H: $PUK_{AAA-H}(Req\_Node_{n+1}, IP_{LMN}, DC_{LMN}, Req\_Z_{LMN}, Req\_ACC_{LMN}, S_{No}, T_{Stamp})$

5. AAA-H → AR → MR: $PUK_{MR}(Grant\_Node_{n+1}, new\_DC_{LMN}, Z_{LMN}, ACC_{LMN})$

6. MR → LMN: $PUK_{LMN}(Grant\_Access, Msg_{LMN})$

IV. Results and Discussions

ALM-NEMO is proposed to perform AAA for LMNs which belong to MN led by MR. Existing AAA mechanisms for mobile nodes are executed by considering all mobile nodes as same. VMN and LMN are from different MNs and a single mechanism cannot be executed for both of the nodes. The proposed mechanism is simulated and the results are analyzed. During simulation, the processor for each mobile device is setup upto 50MHz randomly. The time taken to execute each step is observed and found that mobile devices take less time to execute the operation when compared with the existing mechanisms. In the existing mechanisms, procedures that perform authentication operations take more time because of the way of execution and the parameters take time to be generated. While concentrating on reducing delay in execution, security is also ensured. Security issues of the existing mechanisms are eliminated in the proposed mechanism. ALM-NEMO considers both local authentication and HN authentication to ensure security of NEMO environment.

Random number, time stamp and serial number are used to avoid the replay attacks. DC is changed periodically. While simulating the proposed mechanism, an attacker node is purposely placed between the communicating nodes and tried to intrude communication. But, none of the attempt is succeeded.

First time the DC is generated like

```
cf00e82a41fb32addcbf5c56bca6d93de234ccf571
48ba66c80355edaff7fd75
```

Second time the DC is changed to

```
47fa2c3647e0e692f93aa5f396dce584a4c5b6581a
88396118f0cfeab0297dd4
```

The random number is changed periodically by the AAA servers. Changing the DC protects replay attacks. In order maintain the integrity of the message, hash value is generated by having all the parameters sent to the receiver and attached with the original message. A small modification in the message will change the entire value of the hash. While receiving the message, the receiver will generate the hash value using the same set of parameters sent from the sender. The newly generated hash value and the received hash value are verified to ensure the integrity of the message.

V. Conclusion

An AAA mechanism called, ALM-NEMO is proposed to secure NEMO environment. Literature survey reveals that new mechanisms are needed to secure NEMO environment especially in the area of AAA. The parameters and the computations used by existing mechanisms consume much time and processing power. ALM-NEMO secures NEMO environment using different procedures which consumes less time and uses parameters which takes less time to get generated. While existing mechanisms uses same mechanism for all types of nodes, ALM-NEMO executed separate procedures for LMNs. Simulation results shows better results. ALM-NEMO deals with device authentication and in the future user authentication will be considered.

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] 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

[3] de Laat C, Gross G, Gommans L, Vollbrecht J, Spence D, "Generic AAA Architecture", RFC 2903, 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] Calhoun P, Johansson T, Perkins C, Hiller T, McCann P, "Diameter Mobile IPv4 Application", RFC 4004, August 2005

[8] Hakala H, Mattila L, Stura M, Loughney J, "Diameter Credit-Control Application", RFC 4006, August 2005

[9] Eronen P, T. Hiller, G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005

[10] Garcia-Martin M, Belinchon M, Pallares-Lopez M, C. Canales-Valenzuela, K. Tammi, "Diameter Session Initiation Protocol (SIP) Application", RFC 4740, November 2006

[11] 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

[12] A. Patel, G. Giaretta, "Problem Statement for Bootstrapping Mobile IPv6 (MIPv6)", RFC 4640, September 2006

[13] V. Fajardo, J. Arkko, J. Loughney, G. Zorn, "Diameter Base Protocol", RFC 6733, October 2012

[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

[23] 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

AUTHORS PROFILE

J. Isac Gnanaraj is doing his Ph.D in Computer Science at St. Joseph’s College (Autonomous), Trichy, India. He completed his MCA at Bishop Heber College,Trichy. His area of research is network mobility. He has published research articles in many international journals and conferences.

Dr. L. Arockiam is working as an Associate Professor in Computer Science at St. Joseph’s College, Trichy. He has 24 years of teaching experience and 15 years of research experience. He has published more than 100 research articles in the international journals and conferences. His research interest is on mobile & cloud computing, software metrics and web services.