ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 10,December 2012

AAA Mechanism for Mobile Router in Network Mobility Environment

Isac Gnanaraj. J[1], Arockiam. L[2]

Research Scholar in Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, India [1]
Associate Professor in Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, India [2]

ABSTRACT: **Network mobility and host mobility are the two different mobility deployments in mobile networks. Network Mobility Basic Support (NEMO BS) protocol provides session continuity while the whole network changes its point of attachment. While there are many advantages which show the NEMO as a dominant deployment of the future, still few security issues retard the commercial deployment. Many researchers contributed several mechanisms and techniques to protect the communications in NEMO environment. Authentication, Authorization and Accounting (AAA) is a part of security and the entry level shield. NEMO lacks in providing robust AAA mechanisms. As it grows and receives plenty of new users every day, new security issues are raising. Here, a new AAA mechanism is proposed for Mobile Router (MR). When the MR moves into another network, before consuming services, it must be authenticated and authorized. The proposed AAA mechanism provides a better authentication procedure by considering the time and the capacity of the mobile devices for computing the security protocols.**

Keywords: **NEMO, AAA, Security, time**

I. INTRODUCTION

Each day mobile networks receives a big number of new users and new devices. Providing services to all the users without interruption and without compromising security has become an important work of the service providers. Many researchers found that the host mobility cannot tolerate such a growth and some new technology must be found. NEMO BS enables the whole network to move from one network to another without interrupting the session continuity. The MR is responsible for the entire transactions happen in the Mobile Network (MN) which is movable. Nodes that exist in the MN communicates with external devices or users through the MR. NEMO BS was standardized and documented by Internet Engineering Task Force (IETF) in RFC 3963 [1].

The MR has two addresses depending on the point of its attachment. First one is Home Address (HoA) that is obtained from its Home Network (HN) and the second one is Care-of-Address (CoA) that is obtained from the Foreign Network (FN). When the MN moves away from its HN to a FN, the MR which takes care of the communication gets a new CoA. As soon as the MR receives the CoA, it starts Binding Update (BU) process by sending the new CoA to HN and Home Agent (HA) to register its new location with the HN. The data to be sent to the MR are redirected to the new CoA by the HA. The BU must be safe and infeasible for modification and impersonation. While the MN changes its point of attachment, a malicious node or a hacker may claim it as a genuine by replaying the BU processes. When the MR or the MNN receives a data, then the sender of the data must be authenticated before accepting the data. Similarly, there are many security issues need to be considered in order to provide a secured environment for the NEMO users.

Many researchers expressed that, though the NEMO was developed based on IPv6, it lacks in providing a secured environment. Many research works are being carried to provide security to the NEMO environment and still many security issues remain unsolved. Many AAA based security mechanisms are being carried out to authenticate the sender node. Along with authentication, the mechanisms are developed to authorize the nodes by allowing to access the resources and to provide connectivity to an MNN, and to account the usage of the resources. AAA plays a vital role in providing security to the NEMO environment, because it eliminates many security issues like impersonation, denial of service (DoS), etc.

II. MOTIVATIONS AND OBJECTIVES

Many researchers have been concentrating on providing a robust AAA mechanism to the NEMO environment since the NEMO was standardized and documented by IETF [1]. Generic AAA architecture was proposed by de Laat et. al. [2] and it was documented by IETF in RFC 2903 and it was developed based on the

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 10,December 2012

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 were included to develop this architecture. 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 Server (NAS) which desires to authenticate its links and a shared Authentication Server. The Diameter base protocol [6] was developed to provide an AAA framework for applications like network access or IP mobility. Diameter was made to work in both local AAA and roaming situations. It is considered as an alternative for RADIUS. 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. [7].

A mechanism for mutual authentication by combining an AAA model with NEMO was proposed by Ming-Chin Chuang et al. [8]. They proposed the mechanism with low computation and local authentication. There were pre-shared secret values between AAA servers 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. [9] proposed a framework based on AAA where they used a foreign network's AAA server cache mechanism to reduce the delay in authentication process. IDs and certificates were mentioned in their framework but, the details are not enough. 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 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 may not work properly. 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 related works were carried out to provide a better secured environment. The related works are listed below. A framework was proposed by Seong Yee Phang et al. [10] to provide an access control mechanism between the network nodes and service providers by having firewalls and AAA server. Here, they introduced a new entity called AAA Server to authenticate the MNNs. Introducing a new element 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 gave 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. Julien Bournelle et al. [12] suggested to perform AAA based on the three deployment scenarios. 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 an 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 and protocols 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 and 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.

III. AAA MECHANISM FOR MR IN NEMO (AMR-NEMO)

Authentication mechanism is the ultimate goal of this research work. Whenever authentication process is started, the authorization and accounting processes become inevitable. So, the authentication process cannot be separated from the authorization and accounting. Authenticating MR is an important task in the AAA, because, MR communicates with the external nodes on behalf of the internal members, called MNNs. In general, MR has to undergo different procedures to authenticate and to be authenticated. If MR moves into the HN at the first time as a new comer, it has to undergo the Home Registration procedure. When MR moves from HN to a FN, two authentication procedures take place. The first procedure is called Initial Authentication that happens when MR moves into the FN at the very first time. The second procedure is called re-Authentication that happens when MR moves into the FN again. This means MR first moves away from the FN and latter it comes into the same FN. This proposed mechanism considers

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 10,December 2012

all these three procedures and developed based on the multi-operator and multi-deployment perspectives.

A. *Home Registration*

When the MR along with the MNNs moves into the HN, the MR must be registered with AAA-H and HA. The AAA-H is the server located in the HN to perform the AAA for all the nodes accessing the HN. This server holds the credentials of all the nodes. The HA acts as an agent but AAA operations are carried out by the AAA-H. Whenever the messages are passed between two nodes, all the parameters are converted into hash value and added with the original plain text. This helps in maintain the message integrity. The serial number and the time stamp are used to avoid the replay attacks. The digital certificate is also changed to avoid the replay attacks.

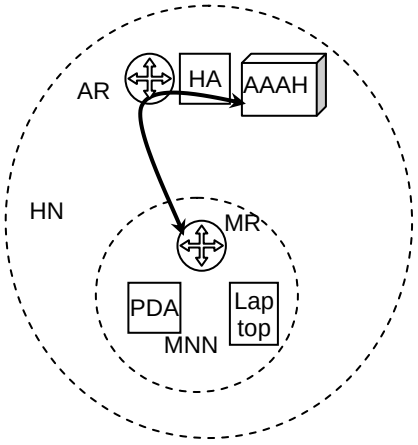

Figure 1. MR's Registration at HN

Figure 1 shows the deployment diagram of the MR. MR is in the HN and requests the AAA-H for registration. MR moves into the HN along with its MNNs such as PDA and Laptop.

The registration procedure is as follows:

1. MR → HA: (NEMO_Req)
   HA forwards the message to the AAA-H and gets the response from AAA-H.
2. HA → MR: (PUK_{HA}, S_{No}, Req_MAC_{MR}, R_{No}, T_{Reg}, h(m))
   PUK_{HA} – public key of the HA to encrypt the message
   Req_MAC_{MR} – HA asks the MR to send back the MAC address of MR
   T_{Reg} – time of registration of the MR at HN
   S_{No} – Serial number to be incremented at each communication for avoiding replays
3. MR→HA→AAA-H: PUK_{HA}(MAC_{MR}, S_{No}, T_{Reg} , h(m))
   MR uses the public key of HA to encrypt the parameters such as MAC_{MR}, S_{No} and T_{Reg} and sends it to AAA-H via HA.
   MR Configures the network adapter settings according to the parameters received from the AAA-H.
4. AAA-H: DC_{AAA-H} :: H(MAC_{MR}, R_{No}, T_{Reg})
   MR: DC_{MR} :: H(MAC_{MR}, R_{No}, T_{Reg})
   Hash function is used to create the Digital Certificate with the parameters of MAC_{MR}, R_{NO} generated by AAA-H and T_{Reg}.
5. AAA-H→HA→MR: PUK_{MR} (DC_{MR}, IP, S_{No} ,h(m))
   MR receives the network configuration settings and performs setup operations.
6. MR→HA→AAA-H:PUK_{HA}($Nodes_n$, $List\_Nodes_i$, Z_i, h(m))
   $Nodes_n$ – number of nodes attached
   $List\_Nodes_i$=1…n - list of nodes from i=1 to n
   Z_i – authorization permissions for each node
   Z_i = { GZ_i, RZ_i, AZ_i, CZ_i, DZ_i }

At first, MR sends the registration request message, NEMO_Req to the HA during Router Solicitation (RS) and Router Advertisements (RA). The AR of the HN supports both host mobility and NEMO. If the NEMO_Req is received, then the HN decides that the requesting node is MR and some other nodes are attached with the MR. When the HA receives NEMO_Req, then it forwards the request to AAA-H. Computing and processing the whole PKI is not possible with the mobile nodes which have low 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 certificate authority (CA). The MNNs uses the keys and simply perform the encryption and decryption. 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. *Initial Authentication*

When the MR changes its point of attachment, it requests the AR of the FN. The FN receives the credentials and sends it to the AAA-H to verify the loyalty of the MR.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 10,December 2012

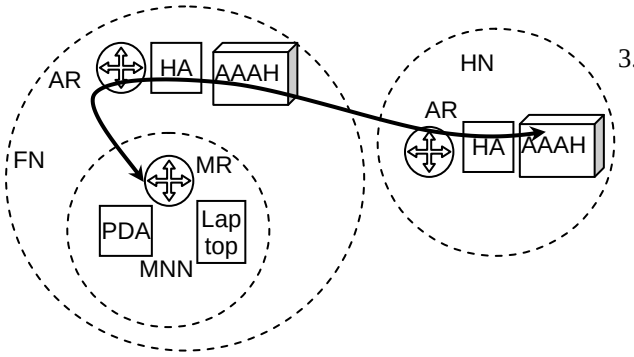

Figure 2. MR's Authentication at FN

Figure 2 shows the diagram of MR's authentication in the FN.

The procedure is as follows:

1. MR→AR: (NEMO_Req, BU_Req, S_{No}, T_{Stamp}, h(m))
   MR sends NEMO_Req and Binding Update request to the AR of the FN and the AR forwards it to AAA-F.
2. AAA-F→AR→MR: (PUK_{AR}, Req_MNP_{MR}, Req_IP_{MR}, DC_{MR}, S_{No}, T_{Stamp} ,h(m))
   AR sends the public and private keys along with the request to send the MNP, IP and digital certificate of the MR
3. MR→AR: PUK_{AR}(MNP_{MR}, IP_{MR}, DC_{MR}, S_{No}, S_{MR_NO}, T_{Stamp} ,h(m))
4. AR→HA→AAA-H: PUK_{HA}(DC_{MR}, MNP_{MR}, IP_{MR}, S_{MR_No}, h(m))
   AAA-H verifies the digital certificate and if it matches then it send the signals as verified.
5. AAA-H→HA→AR: PUK_{AR}(Flag_Veri, $Nodes_n$, Z_{MR}, h(m))
   AAA-H sends verified flag if the MR is genuine and has authorized to act as a MR.
   AR allows the MR to use its resources along with its nodes.
6. AR → MR: PUK_{MR}(BA, CoA, S_{No}, T_{Stamp}, h(m))
   AR assigns the new CoA to the MR and informs the HA.

C. *Re-Authentication*

When the MR along with its nodes moves away from the FN and come again into the FN, the Re-Authentication procedure is executed.

The procedure is as follows:

1. MR→AR: PUK_{AR}(NEMO_Req, DC_{MR}, MNP_{MR}, IP_{MR}, S_{No}, T_{Stamp}, h(m))
2. AR: IF $DC_{MR} \neq DC_{AAA\text{-}H}$
   AR→AAA-H: PUK_{HA}(Resend_$DC_{AAA\text{-}H}$, CoA_{MR}, IP_{MR}, MNP_{MR}, h(m))
   AR: Verifies the digital certificate with the previous certificates. If the certificate is not matched, then AR sends request to AAA-H to 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. AR → MR: PUK_{MR}(CoA_{MR}, S_{NO}, T_{Stamp}, h(m))
   If the CoA is available again for the MR, then the same CoA is used or else the new CoA is assigned.

IV. RESULTS AND DISCUSSIONS

The proposed mechanism, AMR-NEMO uses the light weight parameters by considering the ability of the mobile devices. In other words, AMR-NEMO ensures security with less computing cost compared to existing mechanism.

Existing mechanisms directly send the parameters like MNP, ID, etc., at the Home Registration process [9]. The MNP and the ID can be provided only after registering with the HN. Hence, in the proposed mechanism, first the NEMO request is sent and then other parameters are used. In the LMAM [8] mechanism, in the first step, the MAC address of the MR is directly sent to the HA without encrypting which makes the MR more vulnerable. In the proposed mechanism, sensitive parameters are encrypted using public key of the receiver and sent.

At each step of the authentication process, the parameters used in the proposed mechanism are lighter than the parameters used in the existing mechanisms. During simulation, the proposed mechanism takes less time than the existing mechanism [9] to process each step of the mechanism.

While verifying the DC, it is changed over a period of time by the AAA-H in order to protect the replay attacks. During the simulation, at first time the DC is

```
d145a76e8dd6a88d1772be027efcda9f0a679e
84aab773887b4cc953557c800b
```

At the second time, the DC is

```
d2d28bf5c8568c8cf28cf422b19a49a1c8839a
f2cd2224dea3fc8387fb8e1aa4
```

This change in the DC restricts the hacker to find the original content of the message and also restricts from replaying the DC.

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. For protecting from replay attack, the serial number and the time stamp are used. In the DC, the random number is changed periodically by the AAA-H. If the hacker tries to capture the DC, periodically different DC is received. The hash function is used to ensure the message integrity. The hash value of all the parameters is appended with the original content. The receiver generates the hash value by using the same set of

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 10,December 2012

parameters. The received hash value and the generated hash value are matched to ensure the message integrity. Using public and private keys, the non-repudiation problem is restricted.

V. CONCLUSION

A mechanism called AMR-NEMO, to perform AAA for MR in the NEMO environment is proposed. AMR-NEMO uses lighter parameters to authenticate the nodes. Existing mechanisms use heavy parameters and calculation processes which make it harder to be processed by the mobile devices. The proposed mechanism makes it easier to calculate and also security is enhanced. The existing mechanisms have some security issues and they are solved by the proposed mechanism. The proposed mechanism considers only device authentication. In the future, the 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] 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

Biography

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.