Efficient and Secure AAA for Mobile Router in Network Mobility Environment (A3MR-NEMO)

William Asiedu
Dept. of Info Tech. Edu, UEW-K

K.O. Boateng
Dept. of Computer Eng. KNUST

ABSTRACT
Mobile Networks play a vital role in the communication and networking fields. Usage of mobile devices and mobile applications are increasing because of its any-where any-time strategy. Many mobile applications, services, algorithms and protocols are developed to provide a better quality of service to the users. When the number of users increases, the mobile network operators search for new methodologies to adopt the vast number of users. The increasing number of users increases the signaling overhead and security issues. To offer a solution to these problems, we propose a mechanism base on Authentication, Authorization and Accounting system on NEMO. This mechanism provides efficient, reliable and secure communication among mobile network nodes. Experiment results shows consistency with theoretical analysis and exhibit better protection and low overhead compared to recent related studies through NS3.

Keywords
Access router, Algorithm, AAA, NEMO, Mobile Route

1. INTRODUCTION
The Mobile Router (MR) plays a vital role in the NEMO environment. The Mobile Network Nodes (MNNs) communicate with external devices and users through MR. MNNs are registered with MR. At any given time, MR can change its place of attachment. Before access is granted to MR, the Access Routers (AR) of the Home Network (HN) and the Foreign Network (FN) authenticate MR and verify the authorization provisions and accounting details to ensure that the MR has all the privileges to access the internet. Authentication, Authorization and Accounting (AAA) is an essential aspect of any security algorithms. This is because before granting access to any node, the service provider or the network operator must ensure that the requesting node is genuine and not malicious or security breach.

However, it is clear that a new mechanism which has less computational delay and protects the NEMO environment is needed. The objective of this mechanism is to develop procedures to perform AAA for MR. The procedures are developed taking into consideration the computational time and security of mobile devices. The Digital Signature (DC) is introduced in this mechanism to protect the NEMO environment from replay attacks. The existing mechanisms do not make use of the DC.

MR keep changing its point of attachment and a hacker can try to access HN by acting as a genuine node. The AR of the HN verifies the credentials of mobile nodes. Many researchers have tried to protect the communication which takes place between the MNNs of the NEMO environment [1] and [3], propose another authentication system. In its home registration procedure, MR sends its MAC address directly to the HA without hiding or encrypting it. This makes the NEMO more vulnerable to Denial-of-Service (DoS) and other security attacks. They suggest a system for low computation as well as local authentication procedures and they utilise the pre-shared values between the important nodes. This makes the network vulnerable to man-in the-middle attacks and impersonation attacks.

[4] utilise tickets and try to decrease the delay in the authentication process. However, the system suggested by them rises the computational cost for foreign AAA servers. On the other hand, a mechanism recommended by [5] and [8] leads to a problem as when the foreign network is located far from the home network, the authentication inactivity rises. Similarly, [6] and [2] propose a different AAA mechanism.

The cache mechanism proposed by them causes delay in the authentication process. The tables used in the cache take significant time to update and maintain the records. The entries into the table are restricted to 10. If more than 10 nodes are coming inside the network, then the server gets jammed. The messages passed from AAA-Home (AAA-H) to MNN and MNN to MR can be captured and used for replay attacks.

2. RELATED WORKS
AAA forms part of the security system. Several studies indicate that the authentication process should commence before any other activity is begun in the mobile system. That is to say that when an MNN or MR travels into a network, it should first be authenticated before further communications is initiated. The MR which leads communications in the stead of the mobile nodes should likewise be verified to determine if it is good or malicious. From available data, it is evidently acknowledged that the main explanations for the failure of the NEMO authentication process are the provision of insufficient security restrictions, extended delays in the authentication process and undependability of the algorithms utilised to run and to validate the security parameters.

Furthermore, [10][11] propose an AAA design built on PANA, Diameter and EAP for a multi-operator environment. They utilise two Wi-Fi egress interfaces in MR and a system to select the best at a specific period. An MR might not be limited to just two interfaces. It should support all the wireless technologies utilised by the MNNs. They indicate that prior to beginning the Binding Update (BU) process, the AAA procedure should begin and the AAA information should be swapped [13]. In this scenario, how the mobile node can recognise the routes and addresses of the HA and the AR (Access Router) of the Foreign Network (FN) before finishing the BU procedure is questionable. If not, the AAA procedure must convey the BU data. In addition, they do not indicate how the local nodes should be authenticated. On the other hand, another framework is suggested by [12] and [16], to offer an access control instrument between the network nodes and service providers by having firewalls as well as an AAA server. At this point, they present new elements to verify the MNNs. The introduction of new elements in the protocols and

in the systems might force service providers to alter the whole system and the protocol. Consequently, it is perceived as difficult to add extra features as well as to streamline the available protocol. [16], propose a system for mutual validation by uniting an AAA model with NEMO. They recommend a system with little computation and local authentication. They indicate that there are secret values which are pre-shared between AAA servers for verifying MNNs. However, some specifics are not present such as how the AAA servers have to interact within themselves and what criteria should be taken into consideration. This exposes the network to man-in-the-middle attacks as well as impersonation attacks. For local authorization, [7][15], make use of tickets and they try to decrease the delays in the authentication process. The system they suggest rises the computational cost for foreign AAA servers. Also, they suggest a different system which is an ID-based ticket for client verification in a public environment [18]. They indicate that the overhead of the home authentication server decreases due to the fact that the ticket renewal is carried out by the foreign network. On the other hand, [9] propose a different authentication system. In this system, there is a bidirectional between the new access router and the former access router. The study of [17], and that of [14], both do not give adequate information on how the MNNs access the MR safely. One more challenge associated with the system suggested by [20], is that, when the foreign network is travels a long distance from its home network the authentication dormancy rises.

Furthermore, [20] and [21], opined that the usage of IPsec to secure NEMO systems was unsuccessful in providing a robust mechanism to limit spillage of saved confidential information. They recommend a handover method which is built on the leakage resilient-authenticated key establishment (LR-AKE) protocol to be conducted by MRs and MNNs. PKI is utilised to counter all forms of attacks with necessary changes. Nevertheless, mobile devices cannot perform cryptographic calculations of PKI due to their limits in memory, speed and other parameters.

3. AAA MECHANISM FOR MR

Authenticating the MR is a vital task in the NEMO environment. This is because while the MR is moving from one network to another, malicious nodes try to access the network by replaying previously captured messages [18] and [22]. Another important reason to authenticate MR is that if the MR's credentials are hacked, MNNs and MR face Denial of Service (DoS) and Session hijacking problems; as a result of mobility support for MR and its MN at any time the MR changes its location together with MNNs [23]. Macro and micro mobility are possible for the MR. When the MR roams within its HN, all communications related to authentication are addressed to the AAA server of HN (AAA-H). The credentials of MR are available at AAA-H and this AAA-H authenticates, authorizes and maintains the account details of the MR. Whenever the MR moves away from the HN, the AAA server of FN (AAA-F) contacts AAA-H to authenticate the MR. There are three different procedures executed based on the location of the MR to perform AAA. When the MR goes into the HN for the first time, the first process, which is called Home Registration procedure, is executed to register the MR in the HN. In this Home Registration procedure, the credentials of MR are created and saved in AAA-H. MAC address, the time of its registration and a random number that is generated by AAA-H are used to create a Digital Certificate (DC). The DC and other credentials are used to authenticate the MR. One of the major advantages of NEMO is the support it provides for mobility of the entire network. MR with its MN changes its point of attachment as it roams. When the MR leaves the HN to the FN, the remaining two authentication processes are executed. The second process which, is known as the Initial Authentication, occurs when the MR goes into the FN for the first time. In this procedure, the MR requests AR of FN to access the network and resources of FN. Before providing access permission, AR authenticates MR by contacting AAA-H.

Likewise, AAA-H verifies the loyalty of MR and responds to AAA-F. If the response indicates that MR is genuine and has sufficient authorization and accounting elements then AR allows MR to access the network. The AAA server of FN (AAA-F) caches all credentials and stores it for future AAA operations. The third procedure is known as re-Authentication. This occurs when MR goes into the FN after its first visit. This implies that MR initially leaves the FN and then latter returns to the FN. In the third procedure, AR authenticates MR although MR has already visited FN. The credentials of MR are stored in AAA-F during the first visit of MR. In this procedure, the loyalty of the MR is ensured by AR and AAA-F without communicating with AAA-H. However, to verify DC, AAA-F communicates with AAA-H to get new a DC for the MR because DC is occasionally modified by AAA-H. This proposed mechanism considers all these three methods and it has been designed based on multi-operator and multi-deployment views.

3.1 Home Registration

The Home Registration procedure is executed when MR moves into HN for the first time. Before accessing the resources and network of HN, the MR is to be authenticated and authorized. MR requests AR of FN to access the internet and also it requests on behalf of the nodes attached with MR in the MN. A typical network architecture and flow of the registration messages are graphically shown in Figure 1. The outer circle denotes HN and inner circle denotes MN. The PDA and Laptop are the two Mobile Network Nodes (MNNs) attached with MR of MN. The registration messages used for AAA purposes are passed among MR, AR and AAA-H which is shown by the arrow.

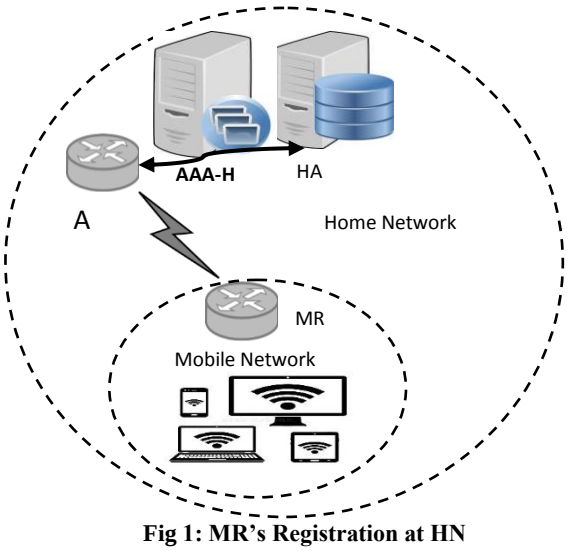

Fig 1: MR's Registration at HN

In this Home Registration procedure, MR, AR and AAA-H play important roles and the messages passed within these nodes must be protected. The Home Agent is an important part of HN which deals with communication whenever the

MR moves away from HN. The HA acts as an agent and forwards the messages to the Care-of-Address (CoA) whenever MR is absent in its HN. CoA is acquired by MR from AR of FN. Whenever MR is in the HN, AR and HA are considered as the same. This is because when MR is in HN, NEMO does not need an agent to forward the messages to MR.

The procedure for registering MR in HN is given below:

1. MR → AR: (NEMO_Req)

   AR forwards the message to the AAA-H and receives an answer from AAA-H.

2. AR → MR: (PUK_{AR}, S_{No}, Req_MAC_{MR}, R_{No}, T_{Reg}, h(m))

   PUK_{AR} – public key of the AR to encode the message

   Req_MAC_{MR} – AR asks the MR to send back the MAC address of MR

   T_{Reg} – MR's registration timestamp

   S_{No} – Serial number to be increased for every communication to prevent replays

3. MR→AR→AAA-H: PUK_{AR} (MAC_{MR}, S_{No}, T_{Reg} , h(m))

   MR utilises the public key of AR to encrypt the parameters like MAC_{MR}, S_{No} and T_{Reg} and sends it to AAA-H through AR.

   MR Configures the network adapter settings based on the details received from the AAA-H.

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

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

   The Hash function is utilised to generate the Digital Certificate with the parameters of MAC_{MR}, R_{NO} created by AAA-H and T_{Reg}.

5. AAA-H→AR→MR: PUK_{MR} (DC_{MR}, IP, S_{No} ,h(m))

   MR obtains the network configuration settings and executes setup operations.

6. MR→AR→AAA-H: PUK_{AR} ($Nodes_n$, $List\_Nodes_i$, 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

$Z_i \in (G)_i \times (R)_i \times (A)_i \times (C)_i \times (D)_i$

$$Z \in (G)_i x\ (R)_i\ x\ (A)_i\ x\ (C)_i\ x\ (D)_i$$

where

$$G_i = \sum_{j=0}^{p_i} (GZ)_j$$

$$R_i = \sum_{j=0}^{q_i} (RZ)_j$$

$$A_i = \sum_{j=0}^{r_i} (AZ)_j$$

$$C_i = \sum_{j=0}^{s_i} (CZ)_j$$

$$D_i = \sum_{j=0}^{t_i} (DZ)_j$$

p_i, q_i, r_i, s_i and t_i are the maximum number of access rights.

Authorization approvals are authorized based on these five factors. These are Group/MN based (GZ), Role based (RZ), Account based (AZ), Attribute or Configuration based (CZ) and Request/Demand based (DZ). When MR is moving under AR of HN for the first time, it sends a NEMO_Req message to AR requesting to access the network and resources.

NEMO_Req denotes that the requesting node is MR and some other nodes are fastened to it. The existing mechanisms directly send all the parameters which are used for authentication purpose without knowing whether the accessing AR has NEMO support or not. It takes considerable time to process and reject the requests if there is no support for NEMO. Then MR informs other nodes about the failure status. The proposed mechanism first verifies whether NEMO support is provided by AR. The NEMO_Req informs the need for NEMO at the first step without loading all the parameters. It saves the time of MR to inform other nodes about the failure or success of the process.

Each message that is used to register and authenticate the MR carries a set of parameters and a hash value. The hash value is produced by using all parameters. The recipient creates a hash value utilising the same set of parameters and verifies them against the hash value received from the sender. This process is executed to guarantee the truthfulness of the message. If a hacker changes any part of the message, the entire hash value gets changed. Therefore, the receiver is able to know whether the message has been modified or not. Computing and processing the complete PKI is impossible in mobile nodes that have low computational capacity. The public key of the recipient is utilised to encrypt the message when it is sent and while the encrypted message is decoded by the private key of recipient. The computation and allocation of the keys are handled by the AAA-H rather than a third certificate authority (CA). The MNNs utilises the keys and basically carry out the encryption and decryption. Each message includes a serial number to avoid replay attacks. Serial numbers are generated by the nodes and the servers. The serial numbers are generated in such a way that a hacker cannot find the next serial number. Generation of serial numbers and the mathematical formula to generate it are decided by the service providers and changed from time to time.

3.2 Initial Authentication

When an MR changes its location of connection and moves into another network called FN for the first time, the initial authentication procedure is performed. MR sends a request message to the AR of the FN to access FN and its resources. The AR of FN obtains the credentials of MR and verifies with AAA-H.

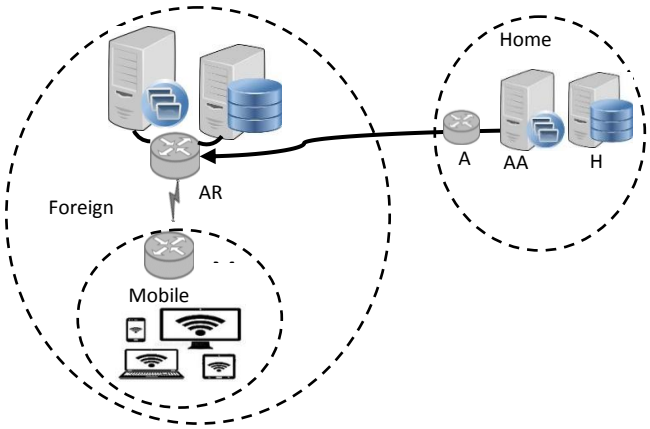

Fig 2: MR's Authentication at FN

The Initial Authentication procedure and the typical network framework are graphically shown in Figure 2. It shows MN roaming in FN. The AR of FN contacts AAA-H to authenticate MR.

The procedure to perform AAA in FN is as listed below:

1. MR→AR: (NEMO_Req, BU_Req, S_{No}, T_{Stamp}, h(m))
   MR delivers NEMO_Req and Binding Update requests 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 delivers the public and private keys together 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))
   MR sends the credentials used to authenticate.
4. AR→HA→AAA-H: PUK_{HA} (DC_{MR}, MNP_{MR}, IP_{MR}, S_{No}, S_{MR_No}, h(m))
   AAA-H authenticates the digital certificate and if it corresponds then, it sends the signals as valid.
5. AAA-H→HA→AR: PUK_{AR} (Flag_Veri, $Nodes_n$, S_{No}, Z_{MR}, h(m))
   AAA-H sends an authenticated flag if the MR is genuine and has sanctioned it to serve as an MR.
   AR permits the MR to utilise its resources together with its nodes.
6. AR → MR: PUKMR (BA, CoA, S_{No}, T_{Stamp}, h(m))
   AR gives the new CoA to the MR and notifies the HA.

When MR requests for access, AR informs MR to send all the credentials to authenticate MR. AR receives all the credentials of MR and forwards them to AAA-H to confirm the loyalty of MR. AR starts a new account for MR in AAA-F and periodically informs AAA-H about the network usage and billing status. The messages received by MR are encrypted by the sender using the public key of MR and MR decrypts the message by its private key. The calculation and allocation of the keys are performed by AAA servers.

3.3 Re-Authentication

The mobility support for the entire network enables MR to move from one network to another network. MR moves from one FN to another FN. When the MR moves back to the FN which it previously visited, the MR is authenticated again by the AR of the FN. During the second time, the AAA procedure takes a lesser time to be executed. All the credentials of MR are already available at AAA-F because of the previous authentication procedures executed for MR. During the second time, AR gives importance to the verification of the DC. Over a period of time, the DC is changed by AAA-H. AR receives DC from MR and matches against the DC which was obtained earlier. If the DC is not matched successfully, AR asks AAA-H to send a new DC. The new DC is then verified. Many studies recommend the Dynamic Host Configuration Protocol (DHCP) (Komori & Saito, 2002) (Rooney, 2010) for allotting IP addresses for mobile nodes.

The Re-Authentication procedure is listed below:

1. MR→AR: PUK_{AR} (NEMO_Req, DC_{MR}, MNP_{MR}, IP_{MR}, S_{No}, T_{Stamp}, h(m))

   MR requests AR of FN to regain access by sending all the credentials.

2. AR: IF $DC_{MR} \neq DC_{AAA\text{-}H}$ AR→AAA-H: PUK_{HA} (Resend_$DC_{AAA\text{-}H}$, $CoA3_{MR}$, IP_{MR}, MNP_{MR}, h(m)

   AR: Authenticates the digital certificate using the former certificate. If the certificates do not match, then AR requests AAA-H to deliver a new certificate. Because of security and in order to prevent replay attacks and passive eavesdropping the certificate is altered periodically.

3. AR → MR: PUK_{MR} (CoA_{MR}, S_{NO}, T_{Stamp}, h(m))

   If the CoA is accessible for a second time for the MR, then the same CoA is utilised but if not then the new CoA is given.

4. SIMULATION RESULTS

A3NeMo-Sim is a system designed for the NEMO environment. The proposed mechanism, A3MR-NEMO is simulated using A3NeMo-Sim and NS3. The configurations of MNNs are dynamically fixed. At each step of the procedure the time (in milliseconds) is tabulated and compared with the existing mechanisms. Each procedure is executed for several times and 10 simulations are taken randomly, and the average time is calculated to find the time taken to complete a procedure.

4.1 Simulation of Home Registration Procedure

During the registration process, MR sends a registration request to the AR and additional processes are executed.

Table 1: Time Taken by Home Registration Procedure for MR

No. Sim	*a* (ms)	*b* (ms)	*c* (ms)	*d* (ms)	*e* (ms)	*f* (ms)
1	4	42	13	13	13	10
2	1	37	7	9	5	5
3	2	20	4	7	5	9
4	1	47	9	7	6	36
5	2	32	4	7	6	3
6	1	36	4	5	5	6
7	2	41	4	5	9	4
8	1	23	5	5	5	4
9	1	28	5	5	8	4
10	3	76	3	4	5	4

The simulation of the Home Registration procedure calculates the duration it takes to process each parameter. Table 3.1 shows the duration taken to process each step involved in the transfer of parameters to the next node. The time it takes between the nodes, AR and MR, is more because the keys are generated by AR.

The time difference between the proposed and exiting mechanisms is computed mathematically as follows:

$$t_{A3MR} = \left(\sum_{i=1}^{n}(a_i + b_i + c_i + d_i + e_i + f_i)\right)/n$$

$$t_{LMAM} = \left(\sum_{i=1}^{n}(a_i + c_i + e_i)\right)/n$$

$$t_{Zhang} = \left(\sum_{i=1}^{n}(c_i + e_i)\right)/n$$

$$t_{LR-AKE} = \left(\sum_{i=1}^{n}(c_i + d_i + e_i)\right)/n$$

where

a is the time taken for MR-AR,

b is the time taken for AR-MR,

c is the time taken for MR-AR-AAAH,

d is the time taken for DC,

e is the time taken for AAAH-AR-MR,

f is the time taken for MR-AR-AAAH, and *n* is the number of iterations with different configurations.

From the equations, the average time for each mechanism is computed. The average time taken for the Home Registration procedure (*tA3MR*) is 67.7 ms. The average time taken by the existing mechanism LMAM (*tLMAM*) is 84.5 ms and Zhang's mechanism has the average time (*tZhang*) of 126.6 ms and LR-AKE (*tLR-AKE*'s) also the average time is 142.2 ms. Figure 3 shows the average time difference between the proposed A3MR and the existing mechanisms LMAM, Zhang and *tLR-AKE*'s mechanism. When the parameters are directly placed by the mechanism, it takes lesser time. When the parameters are generated and placed in the messages, they take more time. Based on the parameters taken, the time differs from message to message.

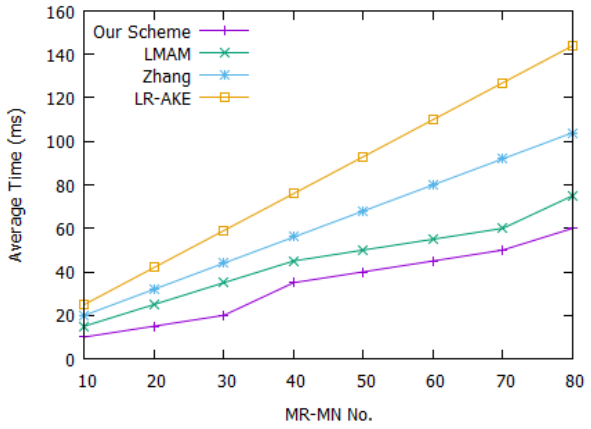

Fig 3: Average time difference for the Home Registration of MR between Proposed and Existing Mechanisms

4.2 Simulation of Initial Authentication Procedure

The MR together with the MN moves away from HN and gets access in FN. The AR of FN authenticates MR by verifying the credentials stored in AAA-H.

Table 2: Time Taken by Initial Authentication Procedure for MR

No. Sim	*a* (ms)	*b* (ms)	*c* (ms)	*d* (ms)	*e* (ms)	*f* (ms)
1	55	142	54	96	93	112
2	49	122	41	89	88	154
3	68	110	60	91	93	124
4	122	132	49	83	84	135
5	126	152	48	95	96	145
6	45	148	43	97	96	187
7	73	162	47	87	88	125
8	90	142	50	81	80	178
9	40	120	50	80	81	195
10	45	123	39	97	96	185

The time difference between the proposed and exiting mechanisms is computed mathematically as follows:

$$t_{AMR-NEMO} = \left(\sum_{i=1}^{n}(a_i + b_i + c_i + d_i + e_i + f_i)\right)/n$$

$$t_{LMAM} = \left(\sum_{i=1}^{n}(a_i + b_i)\right)/n$$

$$t_{Zhang} = \left(\sum_{i=1}^{n}(a_i + d_i + e_i + f_i + g_i)\right)/n$$

$$t_{LR-AKE} = \left(\sum_{i=1}^{n}(c_i + d_i + e_i)\right)/n$$

Table 3.2 shows the time taken to process each security parameter that is used for AAA. From the equations, the average time for each mechanism is computed. The average time it takes for the Initial Authentication procedure (*tA3MR*) is 587.7 ms. The existing mechanisms LMAM have an average time (*tLMAM*) of 591.9 ms and Zhang's mechanism has an average time (*tZhang*) of 1285 ms and LR-AKE also have an average time (*tLR-AKE*) of 1675 ms.. Figure 3.8 shows the average time difference between the proposed, A3MR and the existing mechanisms, LMAM, Zhang and LR-AKE's mechanisms. The time it takes to generate the keys is more than the time it takes to place the parameters directly. Very often a hacker node tries to capture messages in order to replay them. But, the proposed mechanism rejects all these messages so that communication proceeds smoothly without interruptions.

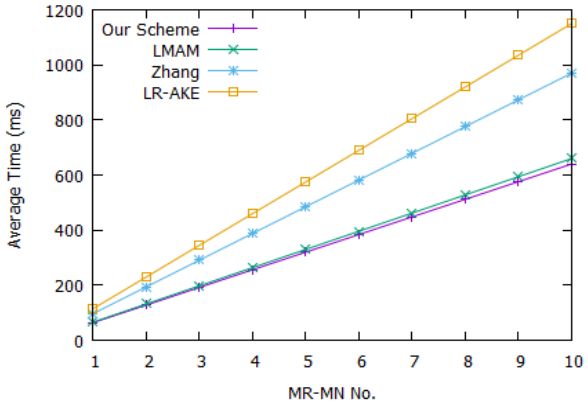

Fig 4: The average time difference for Initial Authentication of MR between the proposed and existing mechanisms

4.3 Simulation of Re-Authentication Procedure

Table 3: Time Taken for Re-Authentication of MR

No. Sim	α (ms)	β (ms)	γ(ms)
1	65	73	68
2	81	138	87
3	34	35	49
4	67	41	57
5	147	42	69
6	37	160	59
7	110	174	47
8	39	53	61
9	143	78	12
10	106	50	11

The duration it takes for the Re-Authentication procedure is shown in Figure 4 MR together with its MNNs revisiting the FN. The AR receives the credentials and verifies against the parameters stored earlier. For DC verification, the AR contacts AAA-H to resend the DC. The new DC received from AAA-H and the DC received from the MR are matched to ensure the loyalty of the MR. Table 3 shows the time it takes to process the steps involved in the Re-Authentication procedure.The time difference between the proposed and exiting mechanisms is computed mathematically as follows:

$$t_{AMR-NEMO} = \left(\sum_{i=1}^{n}(a_i + b_i + c_i)\right)/n$$

$$t_{LMAM} = \left(\sum_{i=1}^{n}(a_i + c_i)\right)/n$$

$$t_{Zhang} = \left(\sum_{i=1}^{n}(a_i + c_i)\right)/n$$

$$t_{LR-AKE} = \left(\sum_{i=1}^{n}(a_i + c_i)\right)/n$$

where
a is the time taken for MR-AR,
b is the time taken for AR-AAA-H,
c is the time taken for AR-MR, and n is the number of iterations with different configurations.

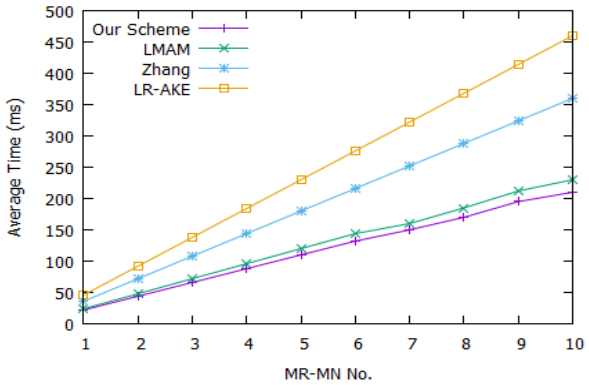

Fig 5: The average time difference for Re-Authentication of the MR between the proposed and existing mechanisms

From the equations, it is calculated that the average time taken for the Re-Authentication procedure (*tA3MR*) is 219.3 ms while the existing mechanisms, LMAM (*tLMAM*), Zhang (*tZhang*) and LR-AKE's (*tLR-AKE*) mechanisms have the average time of 240.7 ms, 353.6 ms and 395.2ms, respectively. Figure 5 shows the average time difference between the proposed A3MR-NEMO and the existing mechanisms, LMAM, Zhang and LR-AKE's mechanism.

During the simulation of A3MR, in all these procedures, a node called the hacker is placed intentionally. In each transaction, the hacker tries to capture the messages and later replay the messages to hack the communication. The hacker node captures the messages which are passed among the nodes. While authenticating the DC, it is altered after some time by the AAA-H so as to secure the replay attacks.
In the simulation, during the first time the DC is transmitted as
`d145a76e8dd6a88d1772be027efcda9f0a679e84a`
`ab773887b4cc`
`953557c800b.`
During the second time, the DC is sent as
`d2d28bf5c8568c8cf28cf422b19a49a1c8839af2c`
`d2224dea3fc8`
`387fb8e1aa4.`

This alteration in the DC prevents the hacker from finding the actual content of the message and likewise limits the replaying the DC.

5. RESEARCH FINDINGS AND INTERPRETATIONS

The figure 6 indicates the authentication delays of Mobile Router(MR) when it moves from one AAAF to another. It clear shows that as the number of hops between AAAH and AAAF increases, the time delay in proposed scheme is smaller than that in the LMAM scheme [8] and Zhang scheme [6]. The point here is that, the proposed scheme new AAAF will authenticate the MR from the last AAAF which is always

one hop away. The LMAM scheme on the other hand uses the local AAA authorisation without any help from any other AAA servers. Also as shown in the figure 3.11 the ticket computation in AAAF and MR will take some extra time, so the time delay of MR authentication in LMAM is almost the same with ours. These three procedures are developed using light weight parameters. Light weight parameters take lesser time to be produced and to be circulated over wireless links. In comparison to existing mechanisms, the proposed mechanism, A3MR, takes lesser time to be executed because of lesser computational time for processing parameters required by the mechanisms.Existent systems directly send parameters such as MNP, ID, etc., at the Home Registration process. The MNP and the ID could be given solely after registration with the HN. Therefore, in the proposed system, to begin with the NEMO request is delivered and then the other criteria are utilised. In the existing mechanism LMAM begins by directly transmitting the MAC address of the MR to the HA devoid of encryption which weakens the MR and makes it exposed to attacks. In the proposed system, delicate parameters are encrypted utilising the public key of the recipient before sending.

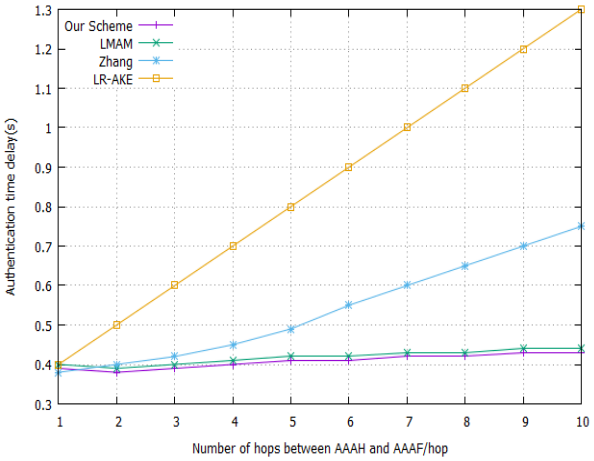

Fig 6: Authentication latency comparison with MR

The proposed mechanism, A3MR shields the NEMO system from replay attacks, non-repudiation and violation of a message's integrity. Protection against these attacks ensures that the NEMO environment is secured from man-in the-middle attacks as well as denial of service attacks. For protection against replay attack, the serial number and the time stamp are utilised. In the DC, the random number is altered occasionally by the AAAH. If an intruder attempts to intercept the DC, from time to time a distinct DC is generated. The hash function is utilised to guarantee the message's integrity. The hash value of all the parameters is attached to the original content. The recipient produces the hash value by utilising the same group of parameters. The received hash value and the produced hash value are compared to guarantee the message's integrity. Utilising public and private keys, the non-repudiation challenge is controlled.

6. CONCLUSION

A mechanism known as A3MR has been proposed to carry out AAA for the MR in the NEMO environment. This mechanism consists of three different procedures. The Home Registration procedure is executed for registering the MR with the HN. The Initial Authentication procedure deals with performing AAA operations when MR travels into FN for the first time. Re-Authentication process is executed when MR reenters into FN. A3MR utilises light weight parameters to verify the nodes. Existent systems utilise heavy parameters and computation methods that renders them more difficult to be processed by mobile devices. The proposed system makes it simpler to compute and also enhances security. Existent systems have security problems; however, these problems are addressed by the proposed mechanism. The hash functions and random numbers are used to ensure the message integrity and to protect the NEMO environment from replay attacks while DC is used to authenticate the mobile device which ensures the restriction of cryptanalytic and replay attacks. The proposed mechanism reduces the time delay during the authentication process. This paper proposed the A3MR mechanism to perform AAA operation for MR.

7. REFERENCES

[1] Wee Hock Desmond Ng, Zhili Sun, Haitham Cruickshank, "Group Key Management with Network Mobility", 13th IEEE International Conference on Networks jointly held with the 7th IEEE Malaysia International Conference on Communications, Proceedings 1 and 2, 2005, pp. 716 – 721.

[2] Wenjing Ma, Song Mei, Zhang Yong, Lin Xin, Zhang Huan, "An Optimization Method to Develop AAA Architectures with MIPv6 Mobility Support", Proceedings of the IEEE Asia- Pacific Services Computing Conference, 2008, pp. 948 – 952.

[3] William Stallings, "Mobile IP", The Internet Protocol Journal, Volume 4, Number 2, 2001, pp. 2-14.

[4] Wilkes J. E., "Privacy and Authentication Needs for PCS", IEEE Personal Communications, Volume 2, 1995, pp. 11–15.

[5] Yinxin Jiang, Chuang Lin, Minghui Shi, Xuemin Shen, "Multiple Key Sharing and Distribution Scheme With (n, t) Threshold for NEMO Group Communications", IEEE Journal on Selected Areas In Communications, Volume 24, Number 9, 2006, pp. 1738-1747.

[6] 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, Volume 19, Issue 2, 2012, pp. 81-86.

[7] Abu Zafar M. Shahriar, Mohammed Atiquzzaman and William Ivancic, "Route Optimization in Network Mobility: Solutions, Classification, Comparison, and Future Research Directions", IEEE Communications Surveys & Tutorials, Volume 12,Number 1, 2010, pp. 24-38.

[8] Ming-Chin, C., & Jeng, F. L. (2008). LMAM: A Lightweight Mutual Authentication Mechanism for Network Mobility in Vehicular Networks. Proceedings of the IEEE Asia-Pacific Services Computing Conference, (pp. 1611-1616).

[9] Adeyinka O, "Internet Attack Methods and Internet Security Technology", Proceedings of the Second Asia International Conference on Modeling & Simulation, 2008, pp. 77-82.

[10] Alexandru Petrescu, Alexis Olivereau, "Mobile VPN and V2V NEMO for Public Transportation", Proceedings of the 9th International Conference on Intelligent Transport Systems Telecommunications, 2009, pp. 63-68.

[11] Angel Cuevas, Ruben Cuevas, Manuel Uruena, Carmen

Guerrero, "A Novel Overlay Network for a Secure Global Home Agent Dynamic Discovery", Springer LNCS 4806, 2007, pp. 921-930.

[12] Arkko J, Kempf J, Zill B, Nikander P, "SEcure Neighbor Discovery (SEND)", RFC 3971, 2005.

[13] Aziz A, Diffie W, "Privacy and Authentication for Wireless Local Area Networks, IEEE Personal Communications, Volume 2, 1994, pp. 25-31.

[14] Brown D, "Techniques for Privacy and Authentication in Personal Communication System", IEEE Personal Communications, Volume 2, 1995, pp. 6-10.

[15] Calhoun P, Loughney J, Guttman E, Zorn G, Arkko J, "Diameter Base Protocol", RFC 3588, 2003.

[16] Calhoun P, Johansson T, Perkins C, Hiller T, McCann P, "Diameter Mobile IPv4 Application", RFC 4004, 2005.

[17] Carlos J. Bernarods, Ignacio Soto and Maria Calderon, "IPv6 Network Mobility", The Internet Protocol Journal, Volume. 10, Number. 2, 2007, pp. 16-27.

[18] Christian Bauer, "NEMO Route Optimization with Strong Authentication for Aeronautical Communications", Proceedings of the IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications, Toronto, 2011, pp.788-793.

[19] Cuevas R, Guerrero C, Cuevas A, Caldern M, Bernardos CJ, "P2P Based Architecture for Global Home Agent Dynamic Discovery in IP Mobility", Proceedings of the IEEE 65th Vehicular Technology Conference, 2007, pp. 899-903.

[20] 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, 2007, pp. 53-58.

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

[22] Devarapalli V, Wakikawa R, Petrescu A, Thubert P, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, 2005.

[23] Donghai Shi, Chaojing Tang, "A Fast Handoff Scheme Based on Local Authentication in Mobile Network", Proceedings of the 6th International Conference on ITS Telecommunications, 2006, pp. 1025-1028.