Security Issues, Challenges and Solutions in Network Mobility: A Review

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

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

***Abstract*—Network Mobility (NEMO) gains lot of attention after standardized and documented by Internet Engineering Task Force (IETF). A group of nodes lead by a node called Mobile Router (MR) can change its point of attachment without disruption in the session continuity is called NEMO. Many researchers put a lot of efforts to provide a better secured environment for the NEMO users. Many security issues are solved and few remain untouched or not fully solved. All the researchers mentioned that still more effective mechanisms needed to strengthen the security of NEMO. Security issues and the proposed solutions by many researchers are reviewed in this paper. Also, security issues related to host mobility are reviewed for reference.**

Keywords- Network Mobility; NEMO; Security; Diameter; Radius

I. INTRODUCTION

In general, there are two types of deployment available in the mobile networks, namely, Host Mobility and Network Mobility. In the host mobility, each and every device will be connected with the Access Router (AR) or the base station. In NEMO, a group of devices form a network called Mobile Network (MN) which is movable as a whole and one of the devices called MR will be connected with the AR. All other devices will get connection via MR. NEMO Basic Support (NEMO BS) protocol is standardized and documented by IETF in RFC3963 [1]. At anytime the MN can change its point of attachment. While moving from one network to another, the session continuity should not be broken in order to get uninterrupted services. Literature reveals that NEMO BS documentation lacks in providing the information of how the communication must be protected. Many research works are being carried out to provide a better security mechanism to protect the communication. This paper reviews the security threats and the solutions provided by the researchers.

II. SECURITY THREATS AND RELATED WORKS

Some of the issues in NEMO BS have been solved and few issues are yet to be solved. NEMO BS did not provide much detail on security issues and protection. Binding Update (BU) spoofing is the one of the major issues in NEMO. One of the drawbacks of the traditional communication mechanism is the delay or hardness in sync up with security standards to be employed between the communicating nodes [2]. IP spoofing is a part of the Distributed Denial of Service (DDoS) attacks which is most difficult to defend. Mihui Kim et al. [3] proposed a mechanism to defend the IP spoofing attacks. Their work consists of five parts such as speed detection, attack packets filtering, attack agent identification, isolation of attack agent, and neighboring routers notification. Identifying attack agents and notifying the neighboring router are the two most important works. Here, all the MRs or a top level MR or the AR should perform detection and filtering. During detection, the configurable network address and the rate of change of IP addresses for a single MAC address were taken into consideration. Identification and isolation of attack nodes may restrict the attack for some time but it cannot be sustained for a longer period.

For better performance of the routing, the closer Home Agent was located by making the communication shorter. Angel Cuevas et al. [4] proposed a mechanism to secure the dynamic Home Agent (HA) discovery process and their mechanism was based on the research work proposed by Cuevas et al. [5]. The base work only proposed the routing solution but failed to provide security. They focused on adding security to the Peer-to-Peer Home Agent Network architecture that is used to discover HAs that are geographically distributed.

A. IPSec

In the Internet Protocol (IP) networks, to protect the communications the IPSec is used. IPSec is a protocol suite for securing the communications by authenticating and encrypting the IP packets. IPSec supports data origin authentication, network-level peer authentication, data integrity, replay protection and data confidentiality. IPSec uses the following protocols for various purposes related to security: Authentication Header (AH), Encapsulating Security Payloads (ESP) and Security Association (SA). AH is used for connectionless integrity and data origin authentication. By using sliding window technique it protects against replay attacks. ESP is used for authenticity, integrity and confidentiality. ESP considers protection for whole inner IP packet when the outer header remains unprotected. SA is a bundle of algorithms and parameters to protect the communications. Along with these protocols IPSec also uses the Internet Key Exchange (IKE) [6] [7]. There are two modes of operation available in the IPSec, namely, transport mode and tunnel mode. The transport mode of operation takes place between end-stations and the tunnel mode of operations takes place between gateways.

IPSec [1] [8] is generally used to secure all the communications between MR and HA. Many researchers (like Souhwan Jung et al. [9]) considered that IPSec is more secure for the NEMO environment but still some modifications are needed to make it more secure. Because, as the researchers expressed, the mechanisms or the techniques which are using the IPSec are not secured. Many researchers expressed that the IPSec implementation is not entirely error free [10]. Niels Ferguson et al. [11] criticized that the complexity of the IPSec had lead to a large number of ambiguities, contradictions, inefficiencies, and weaknesses. They have found serious security weaknesses in all major components of IPsec.

Three types of keys are used in IPSec such as a pair of keys for public-key encryption, a pre-shared symmetric key and keys for digital signature. The nodes involved in communication should store these keys locally. Leakage of these keys would result in security problem [12]. If the keys are weak then there will be a possibility of offline dictionary attacks. Tat Kin Tan et al. [13] expressed that the implementation of IPSec caused heavy processing overheads because it needed both Mobile Network Node (MNN) and Correspondent Node (CN) to be agreed on Security Association (SA) that is a set of encryption standard. So, they proposed a method to eliminate the processing overhead by introducing Certificate Authority (CA) and Public Key Infrastructure (PKI) concept. Many research works are being carried out in Authentication, Authorization and Accounting (AAA).

B. *Generic AAA architecture*

Generic AAA architecture is standardized and documented by the IETF in RFC 2903. de Laat et al. [14] proposed this Generic AAA architecture which is built on the framework proposed by Vollbrecht J et al. [15]. The AAA infrastructure included a network of cooperating generic AAA servers communicating via a standard protocol. This architecture was developed to support multi-domain environment and multiple service providers.

A generic AAA architecture consists of a generic AAA server, Application Specific Module (ASM), Application Specific Information (ASI), Authorization Rule Evaluation (ARE), Authorization Event Log (AEL) and Policy Repository (PR). A generic AAA server is capable of authenticating users, handling authorization requests and collecting accounting data. The information available in an AAA protocol message that is specific to a particular application is called ASI. ASM is a software module that implements a program interface to a generic AAA server which handles application specific functionality for an AAA protocol message.

Many researchers found security issues in the Generic AAA architecture. Julien Bournelle et al. [16] stated that a protocol might be used between the client and the NAS like PANA or 802.11i. A protocol might be used among the NAS, local and home AAA servers. It is generally called AAA protocol like RADIUS [17] or Diameter [18]. An authentication method was needed between the client and the AAA server. The EAP framework would be used which allows using a wide variety of methods.

C. *Host Identity Protocol (HIP)*

HIP [19] [20] is also considered as a security protocol which separates the IP address and its name. The internet uses two spaces namely, IP addresses and Domain Name System (DNS). The HIP separates these two in order to support dynamic changes to be authenticated directly between nodes. The public cryptographic keys are used as host identifiers instead of IP address. HIP defined a packet format and procedures for updating the active HIP association. Szabolcs Nováczki et al. [21] proposed a technique called HIP-NEMO which is based on signaling delegation, hierarchical and connection tracking procedures. Their method is not transparent to the MNNs and if the MN changes its point of attachment, updation must be in all the CNs. Jukka Ylitalo et al. [22] presented and evaluated a network mobility scheme based on HIP. Without the solution for re-direction attacks, the MRs were authorized to send location updates directly to peer hosts on behalf of the mobile hosts.

The HIP has been used for host mobility also. Petri Jokela et al. [23] compared the handover performances of MIPv6 and HIP based mobility management in a heterogeneous IPv6 environment. They stated that even with an optimal implementation the standard MIPv6 protocol involves more signaling packets than HIP. Joseph Yick et al. [24] proposed a HIP based UMTS/WLAN architecture. They stated that the vertical handover delay was reduced to almost zero because of HIP's multi-homing support and Make-Before-Break handover scheme.

D. *RADIUS and Diameter*

Remote Authentication Dial In User Service (RADIUS) [17] 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 [18] 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. Saber Zrelli et al. [25] proposed an AAA architecture based on Diameter and Protocol for Carrying Authentication Network Access (PANA) for access control. They expressed that though their work solved some of the security issues, some open issues were also available like loss of connectivity, multiple login and credential abuse, dynamic service authorization and distinction between IP NEMO and IP classic hosts. David Binet et al. [26] also proposed an AAA architecture based on PANA, Diameter and EAP which is discussed in the next section.

III. Authentication, Authorization and Accounting (AAA) Issues

AAA is a part of security mechanisms. Many researchers stated that the authentication process must be started before starting any other actions in the mobile network. In other words, when an MNN or MR moves into a network, first it must be authenticated before starting further communications. MR, which is leading the communications on behalf of the mobile nodes, must also be verified whether it is a genuine or a malicious node. From the literatures, it is clearly identified that the major reasons for failure of NEMO authentication process are providing inadequate security parameters, longer delay in the authentication process and unreliability of the algorithms used to process and to verify the security parameters.

An AAA architecture based on PANA, Diameter and EAP for a multi-operator environment was proposed by David Binet et al. [26]. They used two WiFi egress interfaces in MR and a mechanism to choose the best at a given time. An MR may not be restricted to two interfaces only. It must support all the wireless technologies used by the MNNs. They stated that before starting the Binding Update (BU) process, the AAA process must start and the AAA data must be exchanged. In this case, it is questionable how the routes or addresses of the HA and the AR of the Foreign Network (FN) are found. Otherwise, the AAA process must carry the BU information. They didn't mention how the local nodes must be authenticated.

A framework was proposed by Seong Yee Phang et al. [27] 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. So, it is considered a tough one to include an additional burden and to restructure the existing protocol.

Ming-Chin Chuang et al. [28] proposed a mechanism for mutual authentication by combining an AAA model with NEMO. They proposed the mechanism with low computation and local authentication. They stated that there were pre-shared secret values between AAA servers for authenticating the MNNs. Some details are absent 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.

For local authorization, Jon Sik Moon et al. [29] used the tickets and they tried to reduce the delay in authentication process. The mechanism proposed by them increases the computational cost for the foreign AAA servers. They proposed another mechanism that is an ID-based ticket for user authentication in a ubiquitous environment [30]. They stated that the overhead of the home authentication server gets reduced because the ticket renewal is done in foreign network itself. Donghai Shi et al. [31] proposed an authentication scheme. In their scheme, they established a bidirectional tunnel between the new access router and old access router. These two research works lack in providing details of how the MNNs access the MR securely. Another problem in the procedure proposed by Donghai Shi et al., is if the foreign network is far away from the home network, then the authentication latency is increased.

Hanane Fathi et al. [12] expressed that the use of IPSec to secure NEMO procedures failed to provide a sturdy mechanism to restrict leakage of stored secrets. They proposed a handover procedure that is based on Leakage Resilient-Authenticated Key Establishment (LR-AKE) protocol to be performed by MRs and MNNs. PKI is used against all types of attacks with required modifications. But, the mobile devices are not capable of doing the cryptographic calculation of PKI because of their limitations in memory, speed and other parameters.

Zhang Jie et al. [32] proposed a framework based on AAA. They used a foreign network's AAA server cache mechanism to reduce the delay in authentication process. They used public keys, symmetric keys and hash functions to authenticate the MNNs. IDs and certificates were mentioned in their framework but, the authors failed to give details. 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 tables used in the cache take 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 may be jammed. The messages passed from AAA-Home (AAAH) to MNN and MNN to MR can be captured and used for replay attacks. There was no procedure to prevent the replay attack between these nodes. 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.

A. Mutual Authentication and Key Distribution

A system for distributing secret shares among a group of nodes is called secret sharing scheme in which, only the group members can modify and share their secrets [33]. Based on the concept of threshold secret sharing scheme, a mutual authentication and key distribution mechanism was proposed by Mihui Kim et al. [34] without having the Trusted Third Party (TTP). The local nodes, Local Fixed Node (LFN) and Local Mobile Nodes (LMN) must be authenticated before getting further services from the MR. They proposed an authentication scheme for MR and Visiting Mobile Node (VMN). This scheme treated the VMN and MR as same. Separate schemes are needed for MR and VMN because, the VMN can be authenticated by MR and the MR can be authenticated by its home agent. If VMN is also treated as MR then there is unnecessary additional load in the authentication process.

Tat kin et al. [13] 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. If the secret keys are to be obtained from CA or sent to CA, then the trust worthiness is questionable. They stated that the MR could decrypt the message using CA's public key which is openly available. If the key that is used to decrypt the message is available openly, then any hacker or malicious node can open the message and read the key also.

B. AAA for Different Deployment Scenarios

From an operator's perspective, there are three types of NEMO deployment that covers most of the deployment scenarios. Julien Bournelle et al. [16] suggested to perform

AAA based on these 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. In the first scenario, the user may have a mobile network which consists of Laptops or PDAs. This personal network can move into another fixed infrastructure based AR. In the second scenario, a bus or train can have a MR which communicates with the nearest ARs and provide services to the customers via its own MR. This MR may be operated by the administrators of bus or train or the service providers. All the passengers inside the bus or train can access the internet through the MR of the bus or train. In the third scenario, a mobile network of any user can come under the MR of the bus or train and can access the internet via the MR of the bus or train. Here, a nested mobile network is formed.

They proposed an architecture based on the two works done by Saber Zrelli et al. [25] and Ng C et al. [35]. 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. One of the issues in this architecture is that only the egress interface of the MR could be authenticated. Hence, MNNs from the MN could access the Internet but, effective authorization could not be possible. Another issue is that, the MNN from the MN will not be allowed to use the local services because of the restriction to authorized users directly connected to the MR.

NEMO BS lacks a trouble-free, secure and robust AAA service. Panagiotis Georgopoulos et al. [36] 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. They stated some SLAs must be there between the nodes and the home networks. But, there is no detailed report on how the SLA should be formed. Similarly, few more details are missing like format and parameters of the control messages passed between the nodes and the networks.

IV. Security for Route Optimization (RO)

RO is another emerging trend which is a part of Quality of Service. Many research works are going on RO and many drawbacks are also there because of lacking security. KwangChul Jeong et al. [37] stated that the nested MNs were affected by the bi-directional pinball routing with hierarchical multiple MRs. They combined a RO scheme and AAA architecture and proposed an accounting system. They introduced a new option field in the header of Diameter. The bits were used to find out whether the VMN supports NEMO. The proposed system only gives solution to accounting and slightly to authorization. They studied some other research works also. RBU+ is an end-to-end route optimization scheme for nested mobile networks that was proposed by Hosik Cho et al. [38]. Three distinct solutions were proposed for the end-to-end routing in mobile networks using the method of obtaining the route from the Top Level Mobile Router (TLMR) to the destination MNN. Thubert et al. [39] stated that nested mobile networks have the overhead of nested tunnels between the MRs and the HAs and also causes number of security issues. They proposed a solution to overcome this problem by introducing a new routing header called reverse routing header. KwangChul Jeong et al. [40] proposed a route optimization mechanism by allowing the intermediate routers to maintain a routing table. It replaces the source address of the packet for reverse routing. As stated by them all these route optimization solutions concentrated only on providing a better route optimization and there were security issues because of the new routes and mechanisms.

Marıa Calderon et al. [41] proposed some approaches for route optimization. The triangle routing is the major problem in the nested mobile networks. In MIPv6, this triangle routing problem was solved by allowing the mobile node to update the current location in the CNs and further communication could bypass the HA. They stated that delegation of signaling rights from the MNN to the MR was necessary. The delegation of signal approaches were done in three ways like, delegation based on PKI certificates, delegation based on self-signed certificates and implicit delegation. Their approaches need changes in the software used by the CNs. It is not feasible for a mobile device to process such a PKI within the stipulated time and it needs a third party certification. Hence, it causes higher computational cost.

A mechanism was proposed by Manhee Jo et al. [42] for securing the RO. In their mechanism, the MR sends the BU directly to the CN. The CN receives the Care-of-Address (CoA) of the MNN from the MR and verify the address to find whether the MNN is authorized to use such address. The MNN authorize the MR to act on behalf of the MNN using Multi-key Cryptographically Generated Address (MCGA) [43] [44]. The MCGA could be generated using MNP, public key of the MNN and public key of the MR. MR and CN exchange a session key to reduce the handoff delay during BU process. Computing MCGA could be heavy for the mobile devices which are having low computing power.

V. AAA in MIPv6

NEMO BS protocol was developed from the MIPv6. MIPv6 supports host mobility while the NEMO supports network mobility. Many research works were made to provide better AAA mechanisms for MIPv6 networks. Wenjing Ma et al. [45] presented an optimization method to enhance the handover performance. They created a hierarchical AAA architecture and stored the AAA credentials temporarily in the local AAA server to avoid sending request to the AAAH each time. Then they encapsulated the BU and Home-Test (HoT) into authentication/authorization request information and tried to save time needed for the BU to travel from MN to HA. Also, they attempted to improve security association to solve the network access problem.

Jun Li et al. [46] stated that the handover performance was affected because of inserting several message round trips before mobile registration. The problem was AAA and MIPv6 were separately designed from their own viewpoints without mutual reinforcement. In their research work, all connected AAA participators constructed an overlay network which was naturally topology-aware. The Topologically-Aware AAA Overlay Network (TA4ON) was used for compatibly combining together resources and capacities. Jinsuk Baek et al. [49] proposed a dynamic AAA resolution for Hierarchical Mobile IPv6 Network. They stated that they proposed this scheme because there was a need to minimize the disruption time including AAA cost needed to process a handoff of an ongoing session. Jia Zong-pu et al. [47] proposed a handoff method based on AAA for MIPv6. They tried to eliminate the handoff delay and to increase the security. Jun-Won Lee et al. [48] proposed an authentication procedure for fast handoff IPv6 networks.

VI. Conclusion

A review has been conducted to analyze the issues, challenges and solutions provided related to NEMO security. Many research works were conducted to solve the security issues. Especially, many have aimed at solving the AAA issues. From the review, it is clear that many novel research works are needed to strengthen the AAA processes in NEMO environment. If the AAA mechanisms are stronger and well established then it will prevent many security threats like, DDoS attacks, man-in-the-middle attacks, etc. The security mechanisms should be fast and light weighted, at the same time security should not be compromised. In order to effectively secure the NEMO environment, all the nodes must be authenticated.

References

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

[2] Tat Kin Tan, Azman Samsudin, "Fast and simple NEMO authentication via random number", Proceedings of IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, Malaysia, May 2007, pp. 266-271

[3] Mihui Kim, Kijoon Chae, “A Fast Defense Mechanism Against IP Spoofing Traffic in a NEMO Environment”, Springer LNCS 3391, 2005, pp. 843-852

[4] 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

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

[6] Harkins D, Carrel D, "The Internet Key Exchange (IKE)", RFC 2409, 1998

[7] Kaufman C Ed., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, 2005

[8] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998

[9] Souhwan Jung, Fan Zhao, S. Felix Wu, and HyunGon Kim, "Threat Analysis on NEtwork MObility (NEMO)", Springer LNCS 3269, 2004, pp. 331-342

[10] Tat Kin Tan, Azman Samsudin, "Fast and simple NEMO authentication via random number", Proceedings of IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, Malaysia, May 2007, pp. 266-271

[11] Niels Ferguson, Bruce Schneier, "A Cryptographic Evaluation of IPsec", Counterpane Internet Security, Inc., 2000

[12] Hanane Fathi, SeongHan Shin, Kazukuni Kobara, Shyam S. Chakraborty, Hideki Imai, Ramjee Prasad, “LR-AKE-Based AAA for Network Mobility (NEMO) Over Wireless Links”, IEEE Journal on Selected Areas in Communications, Volume 24, Issue 9, September 2006, pp. 1725-1737

[13] 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

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

[15] 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

[16] 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

[17] Rigney C, Rubens A, Simpson W, Willens S, "Remote Authentication Dial In User Service", RFC 2865, June 2000

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

[19] Moskowitz R, Nikander P, "Host Identity Protocol (HIP) Architecture", RFC 4423, May 2006

[20] Moskowitz R, Nikander P, P. Jokela, Ed., T. Henderson, "Host Identity Protocol", RFC 5201, April 2008

[21] Szabolcs Nováczki, László Bokor, Sándor Imre, "A HIP based Network Mobility Protocol", Proceedings of the International Symposium on Applications and the Internet Workshops, January 2007, pp. 48-51

[22] Jukka Ylitalo, Jan Melén, Patrik Salmela, Henrik Petander, "An Experimental Evaluation of a HIP Based Network Mobility Scheme", Springer LNCS 5031, 2008, pp. 139-151

[23] Petri Jokela, Teemu Rinta-aho, Tony Jokikyyny, Jorma Wall, Martti Kuparinen, Heikki Mahkonen, Jan Melén, Tero Kauppinen, Jouni Korhonen, "Handover Performance with HIP and MIPv6", Proceedings of 1st International Symposium on Wireless Communication Systems, September 2004, pp. 324 – 328

[24] Joseph Yick Hon So, Jidong Wang, "HIP Based Mobility Management for UMTS/WLAN Integrated Networks", Australian Telecommunication Networks and Applications Conference, 2006

[25] 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

[26] 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

[27] 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

[28] 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

[29] Jong Sik Moon, Sun Ho Lee, Im-Yeong Lee, Sang-Gu Byeon, "Authentication Protocol Using Authorization Ticket in Mobile Network Service Environment", Proceedings of 3rd International Conference on Human-Centric Computing, August 2010, pp. 1-6

[30] Jong Sik Moon, Im-Yeong Lee, Kang Bin Yim, Sang-Gu Byeon, "An Authentication and Authorization Protocol Using Ticket in Pervasive Environment", Proceedings of the IEEE 24th International Conference on Advanced Information Networking and Applications Workshops, April 2010, pp.822-826

[31] Donghai Shi, Chaojing Tang, "A Fast Handoff Scheme Based on Local Authentication In Mobile Network", Proceedings of 6th International Conference on ITS Telecommunications, June 2006, pp. 1025 – 1028

[32] 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

[33] Mida Guillermo, Keith M. Martin, Christine M. O'keefe, "Providing Anonymity in Unconditionally Secure Secret Sharing Schemes", Journal of Designs, Codes, and Cryptography, Volume 28, Issue 3, April 2003, pp. 227-245

[34] Mihui Kim, Eunah Kim, Kijoon Chae, "A Scalable Mutual Authentication and Key Distribution Mechanism in a NEMO Environment", Springer - LNCS 3480, 2005, pp. 591-600

[35] 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

[36] 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

[37] KwangChul Jeong, Tae-Jin Lee, Sungchang Lee, Hyunseung Choo, "Route Optimization with AAA in Network Mobility", Springer LNCS 3981, 2006, pp. 923-933

[38] Hosik Cho, Eun Kyoung Paik, Yanghee Choi,"RBU+: Recursive Binding Update for End-to-End Route Optimization in Nested Mobile Networks", Springer LNCS 3079, 2004, pp. 468-478

[39] Thubert P, Molteni M, "IPv6 Reverse Routing Header and its application to Mobile Networks", February 14, 2007, IETF, draft-thubert-nemo-reverse-routing-header-07

[40] KwangChul Jeong, Tae-Jin Lee, Hyunseung Choo, "Dual Binding Update with Additional Care of Address in Network Mobility", Springer LNCS 3794, 2005, pp. 783-793

[41] Marıa Calderon, Carlos J. Bernardos, Marcelo Bagnulo, Ignacio Soto, "Securing route optimisation in NEMO", Proceedings of the Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, April 2005, pp. 248-254

[42] Manhee Jo, James Kempf, "Secure Route Optimization for Network Mobility Using Secure Address Proxying", Proceedings of the Third International Conference on Mobile Computing and Ubiquitous Networking, October 2006, pp. 84-90

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

[44] Aura T, "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005

[45] 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, Beijing, December 2008, pp. 948 – 952

[46] Jun Li, Xin-ming Ye, Ye Tian, "Topologically-Aware AAA Overlay Network in Mobile IPv6 Environment", Springer LNCS 3976, 2006, pp. 293-306

[47] Jia Zong-pu, Zhang Jing, "A Handoff Method Based on AAA for MIPv6", Proceedings of the Third International Symposium on Computer Science and Computational Technology, August 2010, pp. 405-408

[48] Jun-Won Lee, SangWon Min, Byung K. Choi, "An Efficient Authentication Procedure for Fast Handoff in Mobile IPv6 Networks", Springer - Book of Information Networking - Towards Ubiquitous Networking and Services, 2008, pp. 639-648

[49] Jinsuk Baek, Eunjung Lee, "A Dynamic Authentication, Authorization, and Accounting (AAA) Resolution for Hierarchical Mobile IPv6 Network", International Journal of Computer Science and Network Security, VOL.6 No.7B, July 2006, pp. 170-179

AUTHORS PROFILE

Mr. J. Isac Gnanaraj, a research scholar, doing his research in the Department of Computer Science, St. Joseph's College (Autonmous), Tiruchirappalli, India. He has published many research articles in international conferences and journals. His research area is Network Mobility.

Email: ajisac@gmail.com

Dr. L. Arockiam is working as an Associate Professor in the Department of Computer Science, St. Joseph's College (Autonmous), Tiruchirappalli, India. He has published more than 120 research articles in the national/international journals and conferfences. He has 23 years of teaching experience and 15 years of research experience. He has been the resource persons for many international conferences and workshops.

Email: larockiam@yahoo.co.in