Defence Science Journal, Vol. 63, No. 5, September 2013, pp. 502-507, DOI : 10.14429/dsj.63.4003

An Efficacious and Secure Registration for Internet Protocol Mobility

Mathi Senthil Kumar[*] and M.L.Valarmathi[#]

[*]*Amrita Vishwa Vidyapeetham University, Coimbatore, India*
[#]*Government College of Technology, Coimbatore, India*
[*]*E-mail: msenthil_cse@yahoo.co.in*

ABSTRACT

For the ample development of mobile internet protocol (IP) technology and the recurrent movement of a mobile device, it is necessary for the mobile device to inform their home network where initially registered through an efficient and secured procedure against any sort of attacks. The procedure of registration for IP mobility by the portable system must have a better performance by providing a certain level of security, such as authentication, integrity, replay attack protection, and location privacy. All at once, the extreme security in the registration of IP mobility may cause long registration time, principally for real-time systems. This paper mainly deals with a balanced effort for secure and efficient registration procedure which gives better security and efficiency in terms of registration delay. The proposed work provides an easy and fast registration procedure and lessens the registration delay through the usage of an identity based authenticated key exchange scheme that eliminates expensive pairing operations. The proposed protocol is verified by using AVISPA tool. The performance evaluation reveals that the proposed protocol significantly outperforms the existing protocols in terms of the registration delay.

Keywords: Ephemeral private key, anonymity, authenticated key exchange, authentication, IP mobility, replay attack

1. INTRODUCTION

The wireless network and Internet are two elementary systems of our current generation. Especially in recent years, there has been a tremendous growth in development of mobile networks and laptops connected to the Internet and the World Wide Web[1] which is based on mobile internet protocol (IP) based technology. The mobile IP[2] is a standard communication protocol that is designed to support seamless data transmission for mobile device users to move from their home networks to foreign networks.

In a mobile IP environment, a mobile node (MN) is initially attached with its home agent (HA) and the home address is assigned for MN by HA in the home network. While the MN moving from home to a visiting network, it is associated with a care-of address (COA). MN registers the COA at it's HA with a registration procedure for informing their current location to HA as it is required for further communication. When a correspondent node delivers a data packet to MN, then HA will redirect the data packet destined to MN's foreign agent (FA) at the visiting network. As a form of the packet exchanges between wired and wireless networks with mobility agents, the registration of IP mobility implies higher security risks than the static operations in the fixed networks. Due to the significant increase in vulnerabilities for wireless network, the registration procedure must be protected against any type of security threats. The overall mobile IP environment with MN's attachment is shown in Fig. 1.

A large number of studies have been investigated in[3] to describe the registration signaling messages with the protocol description for improvement on security and/or efficiency. Since an efficacious registration process is of the same significance as the secure registration and there is a direct proportionality between the security and the efficiency, the registration protocol should be addressed with the improvisation on both of them. Hence, our work focuses on a specific registration of IP mobility using an identity based authenticated (IDA) scheme, which leads to a balanced effort to make secure and efficacious registration with minimal registration delay.

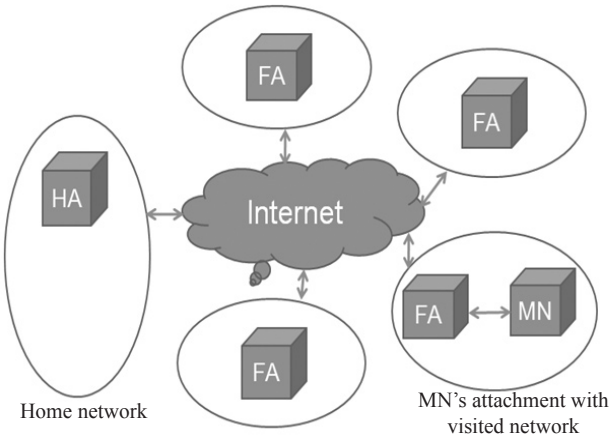

Figure 1. IP Mobility environment – MN's attachment with foreign network

2. RELATED WORKS

The base registration protocol[4,5] uses the secret keys

Received 1 March 2013, revised 19 August 2013, online published 25 September 2013

and distributes them with manual key delivery to each of the MNs for the authentications of its registration packets among the mobility agents and MN. It uses either a timestamp or a nonce version. The registration time is the lowest among other protocols, but this approach is not scalable. To acquire enhanced scalability and improvement in authentication, the certificate-based public key infrastructure (CA-PKI) is employed in the registration protocols[6-8] for the authentications among MN, FA, and HA. CA-PKI uses public key based certificates [PKC] and digital signatures. Due to MN's limited computing power and low bandwidth, it is not possible for MN to do complex public-key based and certificate retrieval operations.

To overcome the deficiency in CA-PKI based registration methods, a registration scheme is introduced by Lam[9], *et al.*, with minimal use of the certificate-based public keys. However, it suffers with the absence of integrity between MN-FA and FA-HA during the transmission of the packets and also the registration delay is still fairly long due to the certificate-based operations. The Yang's protocol[10] is proposed the registration scheme which combines both secure key and minimal public key in addition to produce the communication session key for providing integrity between all correspondent pairs of the registration protocol. But it increases the registration delay up to 36.66 milliseconds (ms) approximately, compared to other protocols. An identity based secure session key (ID based SSK) is proposed[11] to attain a better performance and to exclude the time consuming certificate based operations. In this approach, Authentication, Authorization and Accounting (AAA) protocol[12] is combined with the ID based scheme for reduction in registration latency up to about 63 per cent compared to the existing ID based protocols[13-15]. The two protocols time invariant and time variant[16] are proposed to the improvement of the IP mobility registration that uses a self certified key exchange to generate the secret key. However, these protocols are addressed the security and efficiency in terms of two different variants rather than providing a balanced effort on registration procedure.

To address the balancing of both security and the efficiency, a registration using certificateless PKI[17] is proposed to lessen the registration delay with the considerable amount of security. Nevertheless, the certificateless PKI was established with higher registration delay about 30.48 ms. The protocol[18] with user anonymity is proposed for IP based mobile networks. It reduces the registration delay through a minimal usage of the identity based signature scheme. On the other hand, the signature scheme introduces the extra complexity on signing and verifying the messages. An ID-based authentication protocol with hierarchical support[19] was proposed for the registration with the multihops between MN and HA. This approach provides an access authentication with ID-based signature operations. The proposal lessens the total latency about 50 per cent and 83 per cent, respectively, compared with the existing ID-based signature and RSA-based signature schemes. However, these signature schemes incur an additional cost for signing and verifying the messages.

To preserve the privacy of MN, the proposal[20] investigates the dynamic revocation of the MN with group signature. Here, the mobility agents and the MN attach the signature for authentication. The home registration of the protocol is designed to reduce the handover latency while providing the authentication between MN and HA. The research work[21] has been investigated with the balanced effort on security and efficiency. The protocol reduces the registration time up to ~ 41 per cent compared with Yang's protocol. Owing to the increase of deceitful activities in the mobile IP based network, the necessity of the improvement on security is also increased. Nevertheless, the usage of the security must be afforded to the registration protocol without compromising the efficiency.

Therefore, the registration protocol must be improved to overcome the trade-off between security and efficiency. Building and expanding the registration protocols of the above discussed related works, the current paper suggests the proposal using IDA scheme to enhance the security with the same significance of efficiency. In this paper, authors presented a registration protocol using IDA scheme[22-23]. There are four major contributions of this paper as follows:

(i) the proposed work introduces IDA scheme for reducing computational cost as compared to the previously proposed registration protocols;
(ii) the proposed protocol uses the nonces from MN, HA, and FA to prevent all possible replay attacks;
(iii) to optimize the proposed protocol, the private keys are generated by MN rather than distributed to MN over open links and thus eliminates the communication steps;
(iv) the proposed protocol is verified using widely accepted AVISPA tool.

3. PROPOSED PROTOCOL

In this section, we propose a new IP mobility registration protocol using IDA key exchange scheme without signature operations. The IDA scheme is introduced between the mobile agents and MN. It reduces the computational overload without extra message exchange time and can be applied to low-power devices such as mobile devices.

3.1 Notations

The notations used in the proposed protocol are shown in Table 1.

Table 1. Notations used in the proposed protocol

Symbol	Description
H	Hash function
||	Concatenation
< >	Message Authentication Code (MAC)
{}	Encryption
$Auth_N$	Authentication of a node
N_{MN}, N_{HA}, N_{FA}	Nonces produced by MN, HA and FA respectively
ID_{MN}, ID_{HA}, ID_{FA}	Identity of MN, HA and FA respectively
K_{MN-HA}	Shared secret key between MN and HA

3.2 Protocol Portrayal

The proposed protocol is consisting of the following steps.

Step 1: Agent Advertisement

FA ⟶ MN: AA where AA = Advertisement, ID_{FA}, MN_{COA}, N_{FA}.

The agent advertises their presence by AA message where AA = Advertisement, ID_{FA}, MN_{COA}, N_{FA} to all MNs nearby through broadcasting.

Step 2: Sending registration request from MN to FA

MN ⟶ FA: RReq_1, <RReq_1> K_{MN-HA}, T_{MN} and $Auth_{MN}$ where RReq_1 = ID_{HA}, ID_{MN}, MN_{COA}, N_{HA}, and N_{MN}.

In the setup of IDA scheme, a key generation center (KGC) chooses a master secret key s and computes $P_{MN} = H(ID_{MN})$. Then it generates a private key of MN, $S_{MN} = sP_{MN}$. Note that s is maintained as master secret value to everyone except KGC. In addition to above setup, KGC performs the private key issuing process to MN via a secure channel. The MN chooses an ephemeral private key *a* and computes the following,

$T_{MN} = a\ S_{MN}$

$T_{MN}^{*} = a\ P$ (a point on elliptic curve)

$Auth_{MN} = H(ID_{MN} \| ID_{FA} \| T_{MN} \| T_{MN}^{*})$

MN also computes MAC of RReq_1 message with K_{MN-HA} where RReq_1 = ID_{HA}, ID_{MN}, MN_{COA}, N_{HA}, and N_{MN}. After computing, MN sends RReq_1 message, MAC of RReq_1, T_{MN} and $Auth_{MN}$ to FA.

Step 3: Forwarding registration request from FA to HA

FA ⟶ HA: RReq_1, <RReq_1> K_{MN-HA}, T_{FA} and $Auth_{FA}$

Upon receiving step 2 message, FA computes $T_{MN}^{*'} = s^{-1}T_{MN}$ and check if $H(ID_{MN} \| ID_{FA} \| T_{MN} \| T_{MN}^{*'})$ equals $Auth_{MN}$. If they are not equal, FA terminates the protocol. Otherwise FA authenticates MN. The KGC computes $P_{FA} = H(ID_{FA})$. Then it generates a private key of FA, $S_{FA} = sP_{FA}$. After the setup with initial computation, KGC issues the private key to FA via a secure channel. The FA chooses an ephemeral private key *b* and computes the following,

$T_{FA} = b\ S_{FA}$

$T_{FA}^{*} = b\ P$ (a point on elliptic curve)

$Auth_{FA} = H(ID_{HA} \| ID_{FA} \| T_{FA} \| T_{FA}^{*})$

After computing, FA forwards the registration request message, MAC of RReq_1 with T_{FA} and $Auth_{FA}$ to HA.

Step 4: Sending registration reply from HA to FA

HA ⟶ FA: RRep_1, <RRep_1> K_{MN-HA}, $\{N'_{HA}\}K_{MN-HA}$, T_{HA} and $Auth_{HA}$ where RRep_1 = ID_{HA}, N_{HA}, and N_{MN}.

Upon receiving the message from FA, HA verifies the authentication of MN through MAC value by the shared key K_{MN-HA}. HA computes $T_{FA}^{*'} = s^{-1}\ T_{FA}$ and check if $H(ID_{HA} \| ID_{FA} \| T_{FA} \| T_{FA}^{*'})$ equals $Auth_{FA}$. If they are not the same, HA rejects the registration request. Otherwise HA authenticates FA. The KGC computes $P_{HA} = H(ID_{HA})$. Then it generates a private key of HA, $S_{HA} = s\ P_{HA}$. After the computation, KGC issues the private key to HA through a secure channel. The HA chooses an ephemeral private key *c* and computes the following,

$T_{HA} = c\ S_{HA}$

$T_{HA}^{*} = c\ P$ (a point on elliptic curve)

$Auth_{HA} = H(ID_{HA} \| ID_{FA} \| T_{HA} \| T_{FA}^{*'})$

HA also computes new nonce N'_{HA} and enciphers it with the shared key K_{MN-HA}. After computing, HA then sends RRep_1 message where RRep_1 = ID_{HA}, N_{HA}, and N_{MN}, MAC of RRep_1, enciphered text of new nonce, T_{HA} and $Auth_{HA}$ to FA.

Step 5: Forwarding registration reply from FA to MN

FA ⟶ MN: RRep_1, <RRep_1> K_{MN-HA}, $\{N'_{HA}\}K_{MN-HA}$, T_{FA} and $Auth_{FA}$

Before forwarding registration reply to MN from HA, FA checks if $H(ID_{HA} \| ID_{FA} \| T_{HA} \| T_{FA}^{*})$ equals $Auth_{HA}$. If they are not equivalent, then FA terminates the registration reply message. Otherwise FA authenticates HA. Then FA forwards RRep_1, <RRep_1> K_{MN-HA}, and $\{N'_{HA}\}K_{MN-HA}$, with T_{FA} and $Auth_{FA}$ (as computed in step 3) messages to MN.

Step: 6: Receiving registration reply from FA to MN

Upon receipt of step 5 message from FA, MN verifies the authentication of HA through MAC value. Then, MN computes $T_{FA}^{*'} = s^{-1}\ T_{FA}$ and checks if $H(ID_{HA} \| ID_{FA} \| T_{FA} \| T_{FA}^{*'})$ equals $Auth_{FA}$. If they are not the same, MN rejects the registration reply. Otherwise MN authenticates FA. MN also verifies the nonces and then updates its necessary fields in dynamic parameter database for the next registration.

4. SECURITY VERIFICATION AND ANALYSIS

4.1 Security Verification using AVISPA

The proposed protocol is simulated and verified using automated validation of internet security protocol and applications (AVISPA) tool[24-26]. The AVISPA tool has been used to analyze and verify the security properties of the protocols. AVISPA offers the following:

- A protocol designer can interact with the AVISPA tool by specifying a security scenario with high-level protocol specification language (HLPSL) which is an expressive and role based language.
- HLPSL specifications are translated into equivalent Intermediate Format (IF).
- IF specifications are put in to the back-ends of the AVISPA tool, which employ four analysis methods:

(1) On-the-fly model-checker (OFMC) is used for performing protocol falsification and bounded confirmation by the state transition model.

(2) Constraint-logic-based attack searcher (CL-AtSe) back-end is exploited for simplification heuristics and redundancy elimination techniques.

(3) SAT-based model-checker (SATMC) creates a propositional formula encoding with the transition relation for describing a violation of the security properties.

(4) Tree automata based on automatic approximations for the analysis of security protocols (TA4SP) is used to approximate the interloper information by means of regular tree languages and rewriting.

The scenario of a protocol simulation in AVISPA consists of three entities and five message exchanges, wherein MN, FA and HA are based on the IDA scheme. The simulation starts with the step 1 message, and follows with the messages step 2 to 5 for successful running of the entire protocol. The simulation of the protocol engrosses the following steps:

1. First, three entities, such as the MN, HA, and FA are defined in HLPSL specifications.

2. The FA sends an advertisement message AA to MN.
3. Then, the MN generates the authentication $Auth_{MN}$ and registration request message. It sends them to FA.
4. The FA creates $Auth_{FA}$ and forwards the message to HA.
5. The HA verifies $Auth_{FA}$ and generates the reply message and $Auth_{HA}$. Subsequently, it sends registration reply to FA.
6. Next, FA checks $Auth_{HA}$ and forwards the reply message to MN.
7. Finally, the MN verifies the claim made by FA with $Auth_{FA}$.

4.2 Authentication

The authentication of a communication entity plays an important role to endorse one another's individuality while sending the message between IP mobility based networks. Our proposed scheme provides better authentication among MN, HA and FA through $Auth_{MN}$, $Auth_{HA}$, and $Auth_{FA}$ with IDA scheme and MAC. From Table 2, it is analyzed that the proposed method gives the authentication between all correspondent entities of the IP mobility registration through light loaded security functions rather bilinear pairings and signature operations when compared to other methods.

Table 2. Authentication analysis

Protocol	MN-FA	FA-HA	MN-HA
Base[4,5]	None	None	MAC
Protocols in[6,7]	Digital signature	Digital signature	Digital signature
Protocol in[8]	None	PKC	PKI
Protocol in[9]	PKI	Digital signature	Symmetric encryption
Protocol in[10]	None	Digital signature	Symmetric encryption
ID based SSK[11]	None	AAA	AAA
Protocol in[16]	None	MAC	MAC
Certificateless PKI[17]	None	Digital signature	MAC
Protocol in[18]	None	ID based signature	MAC
Proposed	IDA	IDA	MAC

4.3 Certificateless PKI Communication

The proposed protocol with IDA scheme uses a certificateless PKI communication. The motivation for using IDA scheme instead of PKI is that the PKI uses the certificate which requires the cost effective process for certificate distribution and revocation that the IDA scheme does not require. Also, the PKI needs to verify each and every communication with the certificates. In the setup of the proposed protocol using IDA; the communication between sender and receiver needs to recognize the individuality of the receiver. It uses the KGC instead of the PKI that generates a partial private key S_{MN} using the master secret key that is known only by KGC and it is distributed to the MN via a secure channel.

4.4 Rerun Attack Prevention and Location Privacy

The rerun attack prevention ensures that no message is processed more than once. In the proposed scheme, it is provided through the nonces between MN and the mobility agents. When an impostor reruns step 2 messages that is previously received by HA, HA will verify the N_{HA} from the received message. Because HA's superseded nonce in the request does not equal HA's new nonce stored on HA, HA will discard the request. Therefore, the replay attack fails. And also the paper deals with user anonymity by an attribute called location privacy through temporary identity ID_{MN} of the MN. Table 3 shows replay attack prevention and location privacy analysis of the existing IP Mobility registration protocols with the proposed protocol.

Table 3. Replay attack prevention and location privacy analysis

Protocol	Rerun attack	Location privacy
Base[4,5]	None	None
Protocol in[7]	None	None
Protocol in [9]	None	None
Protocol in[10]	Yes	None
ID based SSK[11]	Yes	None
Protocol in[16]	Yes	Yes
Certificateless PKI[17]	Yes	Yes
Protocol in[18]	Yes	Yes
Proposed	Yes	Yes

5. PERFORMANCE EVALUATION

For the performance evaluation, we used the following requirements on hardware platform for FA, HA and MN to set-up a model for Mobile IP registration environment. Basically, MN is a low power device than mobility agents. Thus, the hardware platform on FA and HA is a Core 2 Duo with 2.33 GHz processor under Windows XP SP 3; the one on MN is the HP (Compaq) iPAQ H3670 with a 206 MHz Strong ARM processor and 64 MB RAM, running the windows CE 2.11 pocket PC operating system.

5.1 Message Size

In the proposed method, the computed message size of the registration request and reply between MN and FA is 75 bytes; FA and HA is 155 bytes; HA and FA is 130 bytes; FA and MN is 43 bytes. Table 4 lists the message size of the various registration protocols in bytes among MN, FA and HA and they are compared with proposed method. The proposed protocol lessens the message size between MN and mobility agents when compared with Yang's protocol, time variant and time invariant. Certainly, the smallest amount of messages is exchanged in the base protocol while its security is the feeblest. Thus, it is examined that the proposed protocol offers less registration signaling traffic while providing better security.

5.2 Registration Delay Comparisons

The registration of IP mobility is depending on the signaling traffic in terms of message size among the participating entities of mobile IP environment. Here, the

Table 4. Message size of registration request and reply packets (in bytes)

Protocol	MN-FA	FA-HA	HA-FA	FA-MN	Total Size
Base[4,5]	50	49	46	42	187
Protocol in[7]	224	288	64	128	704
Protocol in[10]	66	578	582	66	1292
Time invariant[16]	206	364	108	54	732
Time variant[16]	226	404	124	70	824
Certificateless PKI	78	92	92	54	316
Protocol in[18]	82	176	146	48	452
Proposed	75	155	130	43	403

operation time for secure hash algorithm (SHA) to create hash value, and advanced encryption standard (AES) with encryption and decryption on FA and HA are obtained from[27-30]. The registration delay of the proposed scheme is estimated from the message size among MN, HA and FA and the system parameters[31]. The message transmission time is calculated by dividing the message size by the bit rate in wired or wireless links. For instance, the registration time for step 2 is computed based on the following estimation: 0.5 ms (MN processing time) + 2 ms (propagation time in wireless links) + 0.3 ms (message transmission time in wireless links = 75 bytes / 2 Mbps) + 0.019111 ms (SHA operation) = 2.8191ms. Accordingly, the registration time is estimated with each of the steps of our proposed protocol as follows: step 2 + step 3 + step 4 + step 5 = 2.819111 + 1.124 + 1.012196 + 7.461111 = 12.31 ms.

Figure 2 illustrates the comparison result of registration protocols in terms of the registration delay in milliseconds. The registration time of base protocol is very low but maintains the lowest level of security. It is clear that the efficiency of CA-PKI and Lam proposal is limited by heavy certificate-based operations on MN. Yang's protocol requires highest registration time comparatively with other registration protocols. The time variant and invariant based protocols have more traffic with longer registration delay than the proposed protocol because of the witness operations. Certainly, the most messages are exchanged in ID based protocol for performing signature based operations with its higher registration time. Thus, the proposed protocol has less registration time and signaling traffic while providing better security.

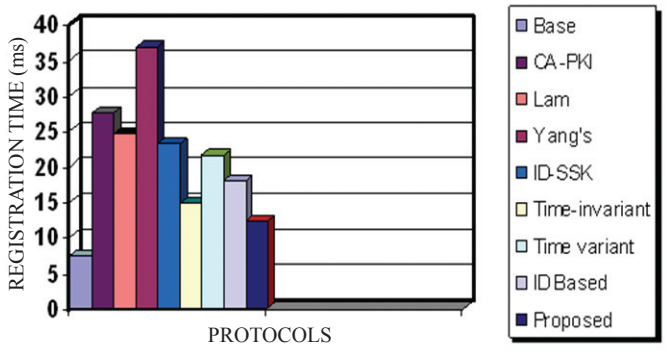

Figure 2. Registration delay comparisons.

6. CONCLUSIONS AND FUTURE WORK

The paper proposes the registration of IP mobility using IDA scheme to provide better security and to minimize the registration delay. The IDA key exchange protocol is used to provide authentication. The nonces from MN, HA, and FA prevents the possible replay attacks. The security attributes of the registration protocol are provided with authentication, rerun attack prevention and location privacy. The proposed work is verified for security using AVISPA tool. The performance evaluation demonstrates that the proposed protocol outperforms the existing protocols. For future work, it can be extended to Mobile IPv6 based networks and can be applied to variety of wireless networks, such as WLAN, Bluetooth, and beyond 3G mobile networks.

REFERENCES

1. Perkins, C. IP mobility support for IPv4. RFC 3344, August 2002.
2. Akyildiz, I.F.; Jiang, Xie & Mohanty, S. A survey of mobility management in next-generation all-IP-based wireless systems. *IEEE Wireless Comm.,* 2004, **11**(4), 16-28.
3. Senthil Kumar, Mathi & Valarmathi, M.L. Mobile IP registration protocols: A Survey. *Int. J. Comp. Appl.,* 2012, **51**(17), 24-34.
4. Perkins, C. IP Mobility Support. RFC 2002, October 1996.
5. Perkins, C.E. Mobile IP. *IEEE Comm. Mag.*, 1997, **35**(5), 84-99.
6. Jianzhu, Zhang & Jon, W.M. A secured registration protocol for mobile IP. 1999.
7. Jacobs, S. Mobile IP Public key based authentication. http://search/ietf.org/internet drafts/draftjacobs-mobileip-pkiauth-01.txt [Accessed on 17 May 2010].
8. Zao, J.; Kent, S.; Gahm, J.; Troxel, G.; Condell, M.; Helinek, P. & Castineyra, I. A public-key based secure mobile IP. *Wireless Networks,* 1999, **5**(5), 373-390.
9. Sufatrio, S. & Kwok, Y.L. Mobile-IP Registration Protocol: a security attack and new secure minimal public-key based authentication. *In* Proceedings of Fourth International symposium on Parallel Architectures, Algorithms and Networks, 1999, pp. 364-369.
10. Yang, C.Y. & Shiu, C.Y. A Secure Mobile IP Registration

Protocol. *International Journal of Network Security,* July 2005, **1**(1), 38-45.
11. Jeong, K.C.; Choo, H. & Ha, S.Y. ID-based Secure Session Key Exchange Scheme to Reduce Registration Delay with AAA in Mobile IP Networks. *LNCS, Springer-Verlag,* 2005, **3515,** pp. 510-518.
12. Hyun-Sun, Kang & Chang-Seop, Park. A Key Management Scheme for Secure Mobile IP Registration Based on AAA Protocol. *IEICE Transaction on Fundamentals,* 2006, **E89–A** (6), 1842-1846.
13. Yang, C.C.; Li, J.W. & Chang, T.Y. A Novel Mobile IP Registration Scheme for Hierarchical Mobility Management. *In* International Conference on Parallel Processing Workshops, 2003, pp. 373–390.
14. Yoo, J. P.; Kim, K.; Choo, H.; Lee, J. I. & Song, J. S. Secure and scalable mobile IP registration scheme using PKI. *LNCS,* Springer-Verlag, 2003, **2668**, pp. 220-229.
15. Yang, C.C.; Hwang, M.S.; Li, J.W. & Chang, T.Y. A solution to mobile IP registration for AAA. *LNCS,* Springer-Verlag, 2003, **2524**, pp.329-337.
16. Dang, L.; Kou, W.; Zhang, J.; Cao, X. & Liu, J. Improvement of mobile IP registration protocols using self-certified public keys. *IEEE Trans. Mobile Computing,* 2007.
17. Dang, L.; Kou, W.; Dang, N.; Li, H.; Zhao, B. & Fan, K. Mobile IP registration in certificateless public key infrastructure. *IET Inf. Security.,* 2007, **1**(4), 167-173.
18. Dang, L.; Kou, W.; Li, H.; Zhang, J.; Cao, X.; Zhao, B. & Fan, K. Efficient ID-based registration protocol featured with user anonymity in mobile IP networks. *IEEE Tran. Wireless Comm.*, 2010, **9**(2), 594-604.
19. He, Liu & Mangui, Liang. Efficient identity-based hierarchical access authentication protocol for mobile network. *Security Comm.Networks*, 2012.
20. He, Liu & Mangui, Liang. Privacy-preserving registration protocol for mobile network. *Int.J. Comm. Syst.*, 2012.
21. Mathi, Senthil Kumar; Valarmathi, M.L. & Ramprasath, G. A secure and efficient registration for IP Mobility. *In* the Proceedings of the 1st International Conference on Security of Internet of Things, 2012, pp. 210-215.
22. Li, Xiaoyong & Zhang, Hui. Identity-based authenticated key exchange protocols. *In* International Conference on Educational and Information Technology, 2010.
23. Zhu, R.W.; Yang, G. & Wong, D.S. An efficient identity-based key exchange protocol with KGS forward security for low-power devices. *LNCS,* Springer-Verlag, 2007, **3828,** pp. 500-509.
24. Armando, A.; Basin, D.; Cuellar, J.; Rusinowitch, M. & Vigano, L. AVISPA: Automated Validation of Internet Security Protocols and Applications. *ERCIM News*, January 2006, **64**. Online Edition.
25. AVISPA v1.1 User Manual. http://www.avispa-project.org [Accessed on 13 July 2013].
26. AVISPA Tool Documentation. http://www.avispaproject.org/publication.html [Accessed on 14 July 2013].
27. Dai, W. Crypto++ 5.6.0 Benchmarks. http://www.cryptopp.com/benchmarks.html. [Accessed on 25 January 2012].
28. Orman, H. & Hoffman, P. Determining strengths for public keys used for exchanging symmetric keys. RFC 3766, April 2004.
29. Hess, A. & Shafer, G. Performance Evaluation of AAA/Mobile IP Authentication. *In* Proceedings of second Polish-German Teletraffic Symposium, Poland, 2002.
30. McNair, J.; Akyildiz, I.F. & Bender, M.D. An inter-system handoff technique for the IMT–2000 System. *In* Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies, 2000, **1**, 208-216.
31. Jeon, H.; Choo, H. & Oh, J.H. Identification Key based AAA Mechanism in Mobile IP Networks. *LNCS,* Springer-Verlag, 2004, **3043,** pp. 765-775.

CONTRIBUTORS

Mr Mathi Senthil Kumar received his ME (Computer Science and Engineering) from Government College of Technology, Coimbatore. Currently, he is pursuing his PhD (Computer Science and Engineering) from Anna University, Chennai. He is working as an Assistant Professor (Senior Grade) in the Department of Computer Science and Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham University, Coimbatore, Tamilnadu, India. He is an associate member of IETE. His research interest includes : Cryptography, mobile IP, and formal languages and automata.

Dr M.L. Valarmathi received her ME (Computer Science and Engineering) from Government College of Technology, Coimbatore and PhD (Computer Science and Engineering) from Bharathiar University, Coimbatore. She is working as an Associate Professor in the Department of Computer Science and Engineering, Government College of Technology, Coimbatore, Tamilnadu, India. Her research encompasses optimization techniques, image processing, algorithm design, compilers and network security. She is a member of ISTE. She has published more than 70 technical papers in National, International conferences and International Journals.