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 which is based on mobile internet protocol (IP) based technology. The mobile IP 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 its 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 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 key exchange scheme, which leads to a balanced effort to make secure and efficacious registration with minimal registration delay.

2. RELATED WORKS

The base registration protocol uses the secret keys

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
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 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, 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 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 to attain a better performance and to exclude the time consuming certificate based operations. In this approach, Authentication, Authorization and Accounting (AAA) protocol is combined with the ID based scheme for reduction in registration latency up to 63 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. 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>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>Hash function</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Message Authentication Code (MAC)</td>
</tr>
<tr>
<td>{}</td>
<td>Encryption</td>
</tr>
<tr>
<td>Auth_n</td>
<td>Authentication of a node</td>
</tr>
<tr>
<td>N_MN, N_HA, N_FA</td>
<td>Nonces produced by MN, HA and FA respectively</td>
</tr>
<tr>
<td>ID_MN, ID_HA, ID_FA</td>
<td>Identity of MN, HA and FA respectively</td>
</tr>
<tr>
<td>K_{MN-HA}</td>
<td>Shared secret key between MN and HA</td>
</tr>
</tbody>
</table>

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\(_1\)> where RReq\(_1\) = ID\(\_HA\), ID\(\_MN\), MN\(\_COA\), N\(\_HA\), and N\(\_MN\).

After the initial computation, KGC issues the private key to MN via a secure channel. The MN chooses an ephemeral private key \(a\) and computes the following,
\[ T\_MN = aS\_MN \]
\[ T\_MN^* = aP \] (a point on elliptic curve)
\[ \text{Auth}_{\_MN} = H\left(\text{ID}\_MN \| \text{ID}\_FA \| T\_MN \| T\_MN^*\right) \]

In the setup of IDA scheme, a key generation center (KGC) chooses a master secret key \(s\) and computes P\(_\text{MN}\) = H (ID\(_\text{MN}\)). Then it generates a private key of MN, S\(_\text{MN}\) = sP\(_\text{MN}\). 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 \(b\) and computes the following,
\[ T\_FA = bS\_FA \]
\[ T\_FA^* = bP \] (a point on elliptic curve)
\[ \text{Auth}_{\_FA} = H\left(\text{ID}\_FA \| \text{ID}\_FA \| T\_FA \| T\_FA^*\right) \]

Upon receipt of step 2 message from FA, MN verifies the authentication of MN through MAC value. Then, MN computes T\(_\text{MN}^* = s^{-1} T\_MN^*\) and checks if H (ID\(_\text{FA}\) \| ID\(_\text{FA}\) \| T\(_\text{FA}^*\)) equals Auth\(_\text{FA}\). If they are not equal, MN terminates the protocol. Otherwise, MN authenticates FA. MN also verifies the nonces and then updates its necessary fields in dynamic parameter database for the next registration.

**Step 3: Forwarding registration request from FA to HA**

FA → HA: RReq\(_1\), <RReq\(_1\)> where RReq\(_1\) = ID\(\_HA\), ID\(\_FA\), MN\(\_COA\), N\(\_FA\), and N\(\_MN\). After computing, MN sends RReq\(_1\) message, MAC of RReq\(_1\), T\(_\text{MN}\), and Auth\(_\text{MN}\) to FA.

**Step 4: Sending registration reply from HA to FA**

HA → FA: RRep\(_1\), <RRep\(_1\)> where RRep\(_1\) = ID\(\_HA\), ID\(\_FA\), N\(\_FA\), and Auth\(_\text{FA}\).

Upon receiving the message from FA, HA verifies the authentication of MN through MAC value by the shared key K\(_\text{MN-HA}\). HA computes T\(_\text{FA}^* = s^{-1} T\_FA^*\) and checks if H (ID\(_\text{FA}\) \| ID\(_\text{FA}\) \| T\(_\text{FA}^\ast\)) equals Auth\(_\text{FA}\). If they are not the same, HA rejects the registration request. Otherwise, HA authenticates FA. The KGC computes P\(_\text{HA} = H\left(\text{ID}\_HA\right)\). Then it generates a private key of HA, S\(_\text{HA}\) = sP\(_\text{HA}\). 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,
\[ T\_HA = cS\_HA \]
\[ T\_HA^* = cP \] (a point on elliptic curve)
\[ \text{Auth}_{\_HA} = H\left(\text{ID}\_HA \| \text{ID}\_FA \| T\_HA \| T\_HA^*\right) \]

HA also computes new nonce N\(_\text{HA}\) and enciphers it with the shared key K\(_\text{MN-HA}\). After computing, HA then sends RRep\(_1\) message where RRep\(_1\) = ID\(_\text{HA}\), N\(_\text{HA}\), and Auth\(_\text{HA}\) to FA.

**Step 5: Forwarding registration reply from FA to MN**

FA ↔ MN: RRep\(_1\), <RRep\(_1\)> where RRep\(_1\) = ID\(_\text{HA}\), N\(_\text{HA}\), and Auth\(_\text{HA}\) to MN.

Before forwarding registration reply to MN from FA, HA checks if H (ID\(_\text{HA}\) \| ID\(_\text{FA}\) \| T\(_\text{HA}^\ast\)) equals Auth\(_\text{HA}\). If they are not equivalent, then FA terminates the registration reply message. Otherwise, FA authenticates HA. Then FA forwards RRep\(_1\), <RRep\(_1\)> where RRep\(_1\) = ID\(_\text{HA}\), N\(_\text{HA}\), and Auth\(_\text{HA}\) with T\(_\text{FA}\) and Auth\(_\text{FA}\) (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\(_\text{FA}^* = s^{-1} T\_FA^*\) and checks if H (ID\(_\text{HA}\) \| ID\(_\text{FA}\) \| T\(_\text{FA}^\ast\)) equals Auth\(_\text{FA}\). If they are not the same, MN rejects the registration reply. Otherwise, MN authenticates HA. 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 AuthMN and registration request message. It sends them to FA.
4. The FA creates AuthFA and forwards the message to HA.
5. The HA verifies AuthHA and generates the reply message and AuthHA. Subsequently, it sends registration reply to FA.
6. Next, FA checks AuthHA and forwards the reply message to MN.
7. Finally, the MN verifies the claim made by FA with AuthHA.

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 AuthMN, AuthHA, and AuthFA 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>
<thead>
<tr>
<th>Protocol</th>
<th>MN-FA</th>
<th>FA-HA</th>
<th>MN-HA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base</td>
<td>None</td>
<td>None</td>
<td>MAC</td>
</tr>
<tr>
<td>Protocols in 6,7</td>
<td>Digital signature</td>
<td>Digital signature</td>
<td>Digital signature</td>
</tr>
<tr>
<td>Protocol in 8</td>
<td>None</td>
<td>PKC</td>
<td>PKI</td>
</tr>
<tr>
<td>Protocol in 9</td>
<td>PKI</td>
<td>Digital signature</td>
<td>Symmetric encryption</td>
</tr>
<tr>
<td>Protocol in 10</td>
<td>None</td>
<td>Digital signature</td>
<td>Symmetric encryption</td>
</tr>
<tr>
<td>ID based SSK 11</td>
<td>None</td>
<td>AAA</td>
<td>AAA</td>
</tr>
<tr>
<td>Protocol in 16</td>
<td>None</td>
<td>MAC</td>
<td>MAC</td>
</tr>
<tr>
<td>Certificateless PKI 17</td>
<td>None</td>
<td>Digital signature</td>
<td>MAC</td>
</tr>
<tr>
<td>Protocol in 18</td>
<td>None</td>
<td>ID based signature</td>
<td>MAC</td>
</tr>
<tr>
<td>Proposed</td>
<td>IDA</td>
<td>IDA</td>
<td>MAC</td>
</tr>
</tbody>
</table>

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 SauN 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 NHA 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 IDMN 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>
<thead>
<tr>
<th>Protocol</th>
<th>Rerun attack</th>
<th>Location privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Protocol in 7</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Protocol in 9</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Protocol in 10</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>ID based SSK 11</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Protocol in 16</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Certificateless PKI 17</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Protocol in 18</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Proposed</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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
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) = 2.81911 ms. 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.

### 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


**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 Vidyaapeetham 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.