Security enhancement for IPv6 mobility using Certificateless Public Key Encryption

S. Padma
Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu, India

ABSTRACT

Mobile IPv6, also known as MIPv6, is an IETF standard that has added the roaming capabilities of Mobile Nodes (MNs) in IPv6 network. It allows an MN to move from one network to another without any disruption in communication. The MN registers its current location to the Home Agent (HA) and the Correspondent Node (CN) with the help of a secure Binding Update (BU). Return Routability Protocol (RRP) is a mechanism used in MIPv6 to provide authentication and secure these BU messages. Though RRP has advantages, it has several security threats and issues. Hence, this paper proposes an improved RRP that overcomes security threats using certificate less public key cryptography. The security properties of our proposed protocol are verified using Automated Validation of Internet Security Protocols and Applications (AVISPA).

Keywords: Binding Update, Certificateless Public Key Encryption, Return Routability and Mutual Authentication.

I. INTRODUCTION

Internet protocol (IP) is an internet layer protocol that helps in delivering the packets from a source host to a destination host based on the IP address available in the packet header. Mobile IP (MIP) is a communication protocol that allows the mobile device users, associated with one network to stay connected even while moving to a different network with a different IP address.

The primary entities of Mobile IPv6 (MIPv6) includes Mobile Node (MN), Correspondent Node (CN), Home Agent (HA). MIPv6 allows the MN to remain connected to CN even when MN moves from home to a foreign network [1-3]. The basic mechanism of MIPv6 is as follows. MN obtains a Home address (HoA) from its original location and additionally acquires a temporary address known as Care-of-address (CoA) when it moves to a foreign network. The CoA is registered to HA by MN [4]. When a datagram is sent from CN to MN, it will be passed to the MN’s HA. The HA then checks if the MN is in the home or the foreign network. The HA forwards the datagram to HoA of MN when it is in home network and to CoA when it is in foreign network.

Over the years, a number of BU schemes [5-9] were proposed. Return Routability protocol (RRP) is a binding update protocol that allows a node to confirm the presence of another node to which the packet is sent [5]. In order to overcome the various security threats faced by RRP, Return Routability using Identity Based Encryption (RR-IBE) was proposed [10]. In RR-IBE which uses Public Key Cryptography, private key is obtained from a trusted third party called Private Key Generator (PKG). However, this introduces the inherent key escrow property. Also, lack of key revocation remains an issue.

To overcome the disadvantages of RR-IBE, the current paper proposes an improved RRP that uses Certificate Less Public Key Encryption (CL-PKE) [11]. Also, the proposed protocol mainly focuses on pairing based CL-PKE [12][13].

II. METHODS AND MATERIAL

2.1 Related works

A. Return Routability Protocol

The RRP mechanism is used for verifying the BU messages between the MN and the CN for successful
and secure Route Optimization (RO) communication as shown in Figure 1. It mainly consists of four messages: the Home Initiation message (HoTI), Care-of Test Initiation message (CoTI), Home Test message (HoT), and Care-of Test message (CoT). The RRP works as follows: it starts with the MN sending two initial messages (HoTI and CoTI) to the CN in two different ways, directly and through the HA. The path between the MN and HA is strongly secured by the IP security protocol. The MN sends the HoTI to the HA using the IPSec tunnel. The CN then receives the HoTI from the HA and the CoTI message from the MN. As a result, the CN creates secret cryptography messages (HoT and CoT) to send to the MN in two different ways, directly and through the HA. When the MN receives both the messages, it creates a shared key \( K_{bm} \) by hashing the tokens together and RRP is completed.

The RRP is faced with a number of security threats such as man-in-the-middle attack, replay, reflection, and amplification attacks. Therefore, the RRP must be enhanced to overcome these obstacles.

**2.2 Improved Return Routability Protocol**

CL-PKE is a security mechanism that requires a trusted third party known as Key Generating Centre (KGC). In contrast to the PKG in RR-IBE, the KGC does not have access to entities’ private key. Instead, the KGC supplies the entity with the partial private key. The proposed protocol is based on the following assumptions:

- The MN first registers with CN to obtain public key of CN.
- There exists a secure IPSec tunnel between MN and HA.
- The path between CN and KGC are secure because KGC authenticates each and every client.
- IPSec tunneling does not exist between HA and CN and also the path between MN and CN is not secure.

### A. Key Generation

The proposed protocol consists of five phases that helps in key generation. Here, let a security parameter \( k \) be given as an input to the Setup algorithm.

1. **Initial setup**: The setup phase is run by the KGC and the output is distributed to the MN, CN, HA. It consists of the following steps:
   - Run a Bilinear Diffie-Hellman parameter generator algorithm with input \( k \) and generate output \((G1, G2, e)\) where \( e \) is a bilinear map such that \( e: G1 \times G1 \rightarrow G2 \). Here, \( G1 \) denotes an additive group and \( G2 \) denote a multiplicative group of some prime order \( q \).
   - Select an arbitrary generator \( P \) of group \( G1 \).
   - Choose a master key \( s \) at random from \( Z_q^* \) and \( P_0 = sP \).
   - Choose four cryptographic hash functions namely \( H1: \{0, 1\}^n \rightarrow G1^*, \) \( H2: G2 \rightarrow \{0,1\}^b, \) \( H3: \{0, 1\}^n \times \{0, 1\}^n \rightarrow Z_q^* \) and \( H4: \{0,1\}^n \rightarrow \{0,1\}^9 \).
   - The output generated from the setup algorithm is \((G1, G2, e, n, P, P_0, H1, H2, H3, H4)\), called as params where \( n \) is the length of the plain text.
2. **Extraction of partial private key**: The KGC runs this algorithm to produce the partial private key of CN. This algorithm takes the identifier of CN (IDCN) as input and generates the partial private key $D_{CN} = \text{H1}(ID_{CN})$.

3. **Generation of secret value**: This algorithm is run by MN, CN and HA separately that takes params and their respective IDs (i.e., IDMN, IDCN, IDHA) as inputs. It selects a secret values at random and outputs $X_{MN}$, $X_{CN}$, $X_{HA}$ for MN, CN and HA respectively.

4. **Generation of private key**: The CN runs this algorithm and generates the private key $R_{CN}$ using the params, the secret value $X_{CN}$ and the partial private key $D_{CN}$ from the KGC as input as follows, $R_{CN} = X_{CN}D_{CN}$

5. **Generation of public key**: This algorithm is run by CN. The inputs are params and their respective secret value $X_{CN}$. It computes the public key of CN, $P_{CN} = (A_{CN}, B_{CN})$, where $A_{CN} = X_{CN}P$ and $B_{CN} = X_{CN}P_0$.

**B. Proposed Protocol**

The former RR-IBE protocol is extended to proposed protocol as shown in Figure 2.

<table>
<thead>
<tr>
<th>SYMBOL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A \rightarrow B : M$</td>
<td>A sends the message to B</td>
</tr>
<tr>
<td>${M}K$</td>
<td>Encryption of message $M$ using key $K$</td>
</tr>
<tr>
<td>$\text{Dreq}_{CN}$</td>
<td>Partial private key request</td>
</tr>
<tr>
<td>$\text{D}_{CN}$</td>
<td>Partial private key response</td>
</tr>
<tr>
<td>$\text{MN}<em>{COA}$ and $\text{MN}</em>{HOA}$</td>
<td>MN’s care-of-address and home-of-address</td>
</tr>
<tr>
<td>$\text{MN}_{SMCOA}$</td>
<td>MN’s old care-of-address</td>
</tr>
<tr>
<td>$\text{MN}_{HA}$</td>
<td>MN’s home agent address</td>
</tr>
<tr>
<td>$\text{CN}_{CNA}$</td>
<td>Address of the correspondent node</td>
</tr>
<tr>
<td>$N_0$, $N_1$</td>
<td>Nonces</td>
</tr>
<tr>
<td>$P_{CN}$</td>
<td>Public key of CN</td>
</tr>
</tbody>
</table>

Table I show the notations used in the proposed protocol. The contents of the messages are given below: The Home of Test Init message is sent from the MN to the CN through the HA using IPSec tunnel mode. Message M1 is composed of the source address of the MN ($\text{MN}_{COA}$ and $\text{MN}_{HOA}$) and the destination address of the HA ($\text{MN}_{HA}$).

**Home of Test Init**: 

(HOTI) $\text{MN} \rightarrow \text{HA}: M1$  
where $M1 = \text{MN}_{COA}$, $\text{MN}_{HOA}$, $\text{MN}_{HA}$, $\text{MN}_{CNA}$,  
$\text{MN}_{SMCOA}\{N_0, \text{MN}_{HOA}$, $\text{MN}_{COA}$, msglength, type\}CLPKE  

(HOTI’) $\text{HA} \rightarrow \text{CN}: M1’$  

This M1 contains data on the old address for the MN in the non home network ($\text{MN}_{SMCOA}$) to remind the HA or CN of the MN’s previous location before it switches to another network with $\text{MN}_{COA}$. Thus, if a message is switching from the CN to the previous $\text{MN}_{COA}$, the CN can send this message to the current $\text{MN}_{COA}$. Both M1 and M1’ contains a nonce or random number ($N_0$). The msglength shows the length of the message and the type informs the next protocol. On receiving both M1 and M1’, the CN compares both the messages. If $N_0$ is same in both then CN sends a partial private key request to the KGC. In the HOTI, HOTI’, COTI and BU messages of MN, the random numbers are encrypted using certificateless public key encryption. This encryption is done by using the public key of CN ($P_{CN}$) as mentioned in the previous section.
where $M_1' = MN_{HOA}, MN_{CNA}, MN_{OldCOA}, \{N_0, MN_{HOA}, MN_{COA}, msg\text{length}, type\} CLPKE$

**Care of Test Init:**

(COTI) $MN \rightarrow CN$: $M_2$
where $M_2 = MN_{COA}, MN_{CNA}, MN_{OldCOA}, \{N_0, MN_{HOA}, MN_{COA}, msg\text{length}, type\} CLPKE$

**Partial private key request:**

(PPR) $CN \rightarrow KGC$: $M_3$
where $M_3 = CN_{CNA}, KGCA, Dreq_{CN}$

**Partial private key:**

(PPK) $KGC \rightarrow CN$: $M_4$
where $M_4 = CN_{CNA}, KGCA, D_{CN}$

**Authentication:**

(AU) $CN \rightarrow MN$: $M_5$
where $M_5 = CN_{CNA}, CN_{COA}, XOR(N_0, N_1)$

**Binding update:**

(BU) $MN \rightarrow CN$: $M_6$
where $M_6 = MN_{COA}, MN_{CNA}, \{N_1, BU\} CLPKE$

**Binding Acknowledgment:**

(BA) $CN \rightarrow MN$: $M_7$
where $M_7 = CN_{CNA}, CN_{COA}, BA.$

2.3 Security Analysis

In this section, the security features such as authentication, confidentiality, data integrity, inherent key escrow are discussed.

**A. Data Authentication**

In the proposed protocol, strong authentication is provided by sending a nonce $N_0$ encrypted using CLPKE in messages $M_1$, $M_1'$ and $M_2$. This nonce sent from MN to CN can be used for authentication from messages $M_5$ to $M_7$. The CN then authenticates MN by generating $N_1$ and subsequently performing an XOR with $N_0$ and sending it to MN. The MN further authenticates CN by sending $N_1$ to CN. In case of RR-IBE the PKG provides authentication for its client where as in our proposed protocol KGC provides authentication for its respective clients as shown in Table II.

**B. Data Confidentiality**

The public key $P_{CN}$ used for encrypting the data $M_1$, $M_2$, $M_6$ is generated using the generation of public key algorithm. The $P_{CN}$ is generated as follows: $P_{CN} = (A_{CN}, B_{CN})$, where $A_{CN} = X_{CN}P$ and $B_{CN} = X_{CN}P_0 = X_{CN} sP$. The secret value $X_{CN}$ used in $P_{CN}$ is generated using the ID$_{CN}$ and is known only by CN. $M_5$ is based on the nonce $N_0$ from the previous $M_1'$ and $M_2$, wherein $N_0$ is known by the MN and CN. $M_5$ uses XOR with two random numbers $N_0$ and $N_1$ and hence as a result, the initial message for the protocol goes through secure channels. All additional messages are mixed with random values and require a secure common key for decryption, making it very difficult for an intruder to extract any value from the exchanged messages. In RR-IBE when the PKG is compromised and the private key is known, the intruder can decrypt and view the messages where as in the proposed protocol when the partial private key is compromised the intruder is unable to decrypt the messages in this way the protocol provides confidentiality as shown in Table II.

**C. Data Integrity**

The MN sends two messages ($M_1$ and $M_2$) to the CN, each with the same content. Attacks can intercept the packets, but cannot correctly decrypt or change the data because the two packets are encrypted using the public key of CN ($P_{CN}$). The CN explores any change by comparing $M_1'$ with $M_2$. If the intruder generates a false $M_1$, $M_2$, $M_5$, $M_6$ or $M_7$ with the same content, then the CN cannot decrypt the message because the intruder knows the CN address, but not the correct secret value $X_{CN}$ which is generated using a secure algorithm (Generation of secret value). Thus, any modification to the exchanged data would be quite impossible, unless an adversary knows the secret value of CN. The security analysis of the proposed protocol is compared with existing protocols as shown in Table II.

**D. Prevents inherent key escrow**

In the RR-IBE protocol, the use of PKG to generate the private key introduces the inherent key escrow property. The PKG can decrypt any ciphertext using the private key. Also, the PKG can distribute the private key to an intruder. Unlike RR-IBE, in this propose protocol the KGC is used to generate the partial private key. The KGC then distribute the partial
private key to CN where the CN can generate the private key as discussed earlier. This prevents the KGC from knowing the private key.

F. Replay Attack prevention

The intruder can replay messages after intercepting one or both of them.

Case 1: The intruder intercepts $M_1'$ from HA and replays it to CN without changing its contents. The CN waits for $M_2$ to compare it with $M_1'$. If $M_1'$ and $M_2$ have the same contents, then the CN asks the KGC for the partial private key to generate the private key $R_{CN}$ to decrypt the message, which it then sends to the MN, but not to the intruder.

Case 2: The intruder sends both $M_1'$ and $M_2$ to the CN. The CN asks for the partial private key from the KGC and obtains an $N_0$ which is only known by the correct MN and CN. The CN sends to the intruder a message $M_5$ that contains an XOR value of $N_0$ with a new random number $N_1$. The intruder is stopped because it does not know $N_0$.

G. Amplification Attack prevention

An amplification attack can generate more than one message from an initial message. This amplification attack works by sending a message from CN to MN through HA to asking MN to send more messages to a victim node. This type of attack is prevented in the proposed protocol because no messages or data are sent from CN to the HA in the proposed protocol.

### TABLE III: SECURITY ANALYSIS

<table>
<thead>
<tr>
<th></th>
<th>MN-HA</th>
<th>MN-CN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RR</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>RR-IBE</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Proposed</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Data confidentiality</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RR</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>RR-IBE</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Proposed</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Data integrity</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RR</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>RR-IBE</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Proposed</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
III. RESULTS AND DISCUSSION

3.1 Performance Analysis

In this section, the performance of the proposed scheme with the other related works are compared in terms of communication payload and latency of the BU.

A. Communication payload costs

The total bytes for all messages of RRP, RR-IBEP and our proposed protocol are 396, 1572 and 896 bytes respectively. Consider the size of ciphertext encrypted using CLPKE is 1024 bits. The size of a message can be calculated as follows.

For example length of HOTI = 128+128+128+128+128+1024 = 1664 bits.
Total no of bytes requires = HOTI+ HOTI’+COTI+PPR+PPK+AU+BU+BA = 1664+1408+1408+320+512+320+1280+256 = 7936 bits = 992 bytes.

By observing the above computations as shown, the communication payload of our proposed protocol is less than that of RR-IBEP and is greater than RRP. This is because the RRP provides less security when compared to our proposed protocol.

B. BU Latency

Latency is the measure of the time taken for a message to move from a source to a destination. The BU latency of a protocol can be calculated using the system parameters shown in Table III. The processing time, propagation time and bit rate are obtained from [14][15] and the operating time of SHA on MN used in RRP and RR-IBE are from [16]. The transmission time of a message can be calculated as follows.

Data transmission time = Size of data / Bit rate.

The BU latency for our proposed protocol can be given by:

Total Binding Update latency = Time required at source for sending messages + Time required at intermediate nodes + Time required at destination for processing the messages.

The latency of messages between MN and HA= 3.332+ 2.768 + 0.5 = 6.664ms
MN and CN = 7.34 + 9.628 + 6.288 = 23.256ms

<table>
<thead>
<tr>
<th>Table III : SYSTEM PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing time in HA,CN and MN</td>
</tr>
<tr>
<td>Propogation time in wireless links</td>
</tr>
<tr>
<td>Bit rate in wireless links</td>
</tr>
<tr>
<td>Propogation time in wired links</td>
</tr>
<tr>
<td>Bit rate in wired links</td>
</tr>
<tr>
<td>SHA operation on MN</td>
</tr>
</tbody>
</table>
C. Comparison of proposed protocol with existing protocols

Figure 5 and Figure 6 show the comparison of the proposed protocol with the existing protocols in terms of BU communication payload between MN and CN through HA and directly between MN and CN respectively.

![Comparison of proposed protocol with existing protocols](image)

**Figure 5**: Communication payload (in bytes) between MN and CN through HA vs. protocols.

![Communication payload between MN and CN vs. protocols](image)

**Figure 6**: Communication payload (in bytes) between MN and CN vs. protocols.

Firstly, in both the cases, when compared to the RR-IBEP [10], the proposed protocol has comparatively less cost. This is due to the following reasons:

1) In the proposed protocol the need for one pair key in RR IBE [10] to obtain the private key of CN is eliminated as the CN receives only the partial private key from the KGC and not the full private key.

2) The contents of the messages of the proposed protocol are refined.

3) In the proposed protocol encryption is done using CLPKE. Secondly, the proposed protocol has a little more cost than the RRP [5] in case of communication payload between MN and CN because it provides stronger security.

IV. CONCLUSION

The MIPv6 allows a mobile node to remain connected with a correspondent node even while moving from a home network to a foreign network without any disruption in communication. This paper introduces a protocol that enhances the signal security in mobility of IPv6. This is done by integrating the Return Routability Protocol with pairing based CL-PKC scheme. Also, a security analysis for our proposed protocol is performed indicating that our protocol enhances the security of the MIPv6 signals and is also free from various attacks like man-in-the-middle attack, replay attack etc. The performance analysis presented shows that the performance of the proposed protocol is better than the previously defined protocols ([5], [10]).

V. REFERENCES


