A New Security Mechanism for Binding Update in MIPv6 using Hybrid Cryptosystem

Vikram Raju R¹, Kumkum Garg (SMIEEE)² and Anil Kumar Dahiya (SM-IEEE)³
Manipal University Jaipur/CSE, Jaipur, India
¹Email: vikramraju.r@gmail.com
²Email: kumkum.garg@jaipur.manipal.edu
³Email: dahyaanil@yahoo.com

Abstract—A Mobile Node (MN) has to intimate to the Home Agent (HA) about its location to Correspondent Node (CN), using a Binding Update (BU) between HA and MN. During this exchange, an intruder may enter easily because of security lapses. Hence, a security mechanism is required to protect the BU. A new security system using hybrid cryptosystem is proposed for Binding Update (BU) in MIPv6.

Index Terms—MIPv6, BU, CN, MN (Mobile Node) and session key

I. INTRODUCTION

The growing use of IP devices in portable applications has created the demand for mobility support for entire networks of IP devices [1]. While mobile node is in foreign network, possibly untrusted networks, then security is very important aspect. A mobile node may tunnel its packets to HA, which in turn encapsulates and forward them to the CN. If route optimization were used then MN would send packets directly to the CN. If binding update is not managed carefully, then any malicious user pretending as a MN or CN is able divert the traffic. The binding update is used to redirect traffic from one address to another. Many attacks are possible on BU like, session hijacking attacks on BU [2-4], and Denial of Service attacks (DOS) [5-7] and Man-in-middle (MITM) attacks [8][9].

In this paper, new security architecture is proposed for providing confidentiality using hybrid technique to BU and a new key is generated for each and every session. Due to this new proposal, delay can reduce compared with existing RRP.

The rest of the paper is organized as follows. In section 2 problem statement given, the section 3 discusses the proposed technique. Section 4 contains simulation results and finally section 5 concludes the paper.

II. PROBLEM STATEMENT

In Return Routability (RRP) [10] the authentication is given to messages as shown in Fig.1.

1) MN sends the Home Test Init message (HoTi) to CN (through MN-HA tunnel) with its HoA as the source address.
2) CN maintains two arrays of secret numbers: Node Key array and Nonce array. The CN will generate nonces message for every two minutes. For HoTi, CN chooses a Random index number i, and calculates the
keygen token for HoTi, Then CN sends Home Test message (HoT) to MN, which contains the home keygen token and i, and sets HoA as the destination address.

\[ \text{Home-keygen-token} := \text{First}(64, \text{HMAC\_SHA1} (\text{Kcn}, (\text{HoA} \| \text{nonce} \| 0))) \]

Then, CN sends Home Test message (HoT) to MN, which contains the home keygen token and i, and sets HoA as the destination address.

3) The MN will send the CoTi message directly to CN.

4) CN respond with Care-of Test message (CoT) in a similar way, which contains the care of keygen token and the random index number j, and sets CoA as the destination address.

5) MN calculates the Binding Management Key as follow after receiving HoT and CoT:

\[ K_{bm} = \text{SHA1} (\text{HoT} \| \text{CoT}) \]

Where SHA1 is a 160 bit Secure Hash Algorithm. Then the CN sends the acknowledgement for that encrypted BU, and then bi-directional tunnel between MN and CN is established [5].

### III. Proposed Solution

A novel hybrid cryptography mechanism is proposed, using session key generation. Hybrid cryptography is a combination of more than one cryptography algorithm. Here, a combination of ECC (Elliptic Curve Cryptography) and DES (Data Encryption Standard) [11] is used. ECC is used for exchanging the keys between MN and CN. BU is exchanged between CN and MN using DES algorithm. The proposed solution has three stages.

A. Sharing information between MN and CN

B. Exchanging keys using ECC

C. Exchanging the BU using DES

#### A. Sharing information between MN and CN

Initially MN and CN share a base point \((Q(x, y))\) based on a Ecliptic Curve \(y^2 = x^3 + ax + b\) where \(4a^3 + 27b^2 \neq 0\) and one large prime \(p\). MN spends some time in each network. This duration is called session. MN moves from home network to foreign network (session-1 is the time it spends in home network and session-2 is the time it spends in foreign network).

#### B. Exchanging the keys using ECC

The exchanging key procedure as follows and the whole operation is shown in fig.2

- MN and CN wants exchange the key.
- For each session, MN secretly picks a large number \(p_{ai}\) (where \(i = 1, 2, 3, \ldots n\) is the session number) randomly. CN secretly picks a large number \(p_{bi}\). MN computes \(Q_{ai} = p_{ai}B\). CN computes \(Q_{bi} = p_{bi}B\). They exchange the points \(Q_{ai}\) and \(Q_{bi}\).
- MN computes \(p_{ai}Q_{bi} = p_{ai}p_{bi}B\). CN computes \(p_{bi}Q_{ai} = p_{bi}p_{ai}B\). Both use the \(x\) value of \(p_{ai}p_{bi}B\) for the key \(key\).

\[ key_i = key \text{ XOR } key_{i-1} \quad (1) \]

**Note:** For session \(i=1\), the key key1 itself.
• For every new network one new large prime is picked randomly. Based on this new session, the key is generated.

![Diagram of key exchange using EC](image)

**Figure 2** key exchange using EC

**C. Exchanging the BU using DES**

**i. Home Network**

Once the key1 (i=1 for first session) is shared by MN and CN, the BU should be sent from MN to CN in a secure way by encrypting with DES. CN receives the encrypted BU from MN, decrypts it using shared key1 and sends the encrypted BA to MN. Once MN receives the BA, a bi-directional tunnel is established. The whole operation is shown in Fig 3 for the first session.

**ii. Foreign Network**

MN moves to foreign network from home network and gets the CoA from Foreign Link. key2 (i=2 for second session) is generated as per equation 1 and shared by MN and CN. The BU is sent from MN to CN in a secure way by encrypting with DES. CN receives the encrypted BU from MN, decrypts it using shared key2 and sends encrypted BA to MN. Once MN receives the BA, a bi-directional tunnel is established for data communication.

\[ key_2 = key_2 \ XOR \ key_1 \text{ (from (1))} \] (2)

![Diagram of BU exchange using DES](image)

**Figure 3** BU exchange using DES

**IV. SIMULATION RESULT AND DISCUSSION**

The proposed solution has been implemented in NS2 (ns2.28) simulator with mobiwan patch. The simulated area is set to 1600×800 sq.m. The proposed solution and RRP has been implemented in NS2 (ns2.28) simulator with mobiwan patch and explanation has given about simulation of proposed solution. The simulated area is set to 1600×800 sq.m having two Base stations (BS1 and BS2). Initially MN is in home network; at this stage MN shared the necessary information for ECC key exchange. Here MN is at (190,191, 194.002) and destination is at (210, 610). The time taken by RRP and proposed solution is the same but in security perspective proposed one is more secure.
• MN is at (190.191, 194.002) location under BS1, at 1.00262 seconds when it is home network, sent $E_{key1}$ (BU) to CN at 2 seconds.
• MN starts moving to foreign network reached at (202.632, 455.281) at the time of 66.4 seconds and lost connection with BS1.
• When MN moves under BS2 and gets the CoA from foreign link at 66.4027 seconds and sending $E_{key2}$ (BU) to CN at 67.4 seconds.

V. DISCUSSION

Here in the proposed solution, ECC has been used for exchanging keys and DES is used for encrypting the BU. For each session different key is used by generating different random number. The following disadvantages are there for the RRP

i. Attacker cannot guess the random number because for every session different random number is used. It is impossible to get key because different keys are maintained in different sessions, but in RRP only one key is used for each BU either new or old.
ii. If attacker come to know current key, Even though it is tough to find previous session key because new key is XOR of previous key.
iii. Proposed solution can avoid brute force attack by ECC and man-in-middle attack, IP spoofing by DES.

In RRP there is possibility for session hijacking attacks on BU. While exchanging HoT or CoT, if intruder will come to know these information intruder can calculate the Key and do the session hijacking at $CN\leftrightarrow HA$ or $MN \leftrightarrow HA$. Here in proposed solution, unlimited numbers of keys have been used session wise so the intruder cannot guess at all the keys, So hijacking attack is not possible.

VI. CONCLUSION

Several security techniques have been proposed for providing confidentiality and integrity to BU in MIPv6. We have simulated both RRP, proposed solution and observed the time taking for providing security to MIPv6 is almost same but proposed solution is secure than RRP. The proposed solution is providing more security in efficient way using hybrid cryptography against various attacks (IP spoofing attack, brute force attack, know plain text attack) because of combination of ECC and DES algorithms by using session key generation. ECC is having its own features and DES most secure symmetric cryptography algorithm.

REFERENCES