

Mobile IP: Enabling User Mobility

Bashir Hayat, Saila Alam
Department of Computer Science, University of Peshawar,
NWFP, Pakistan.

Phone: +92-91-9216732

Email: {bashir_hayat@yahoo.com, s_alam3812000@yahoo.com}

ABSTRACT

This review paper gives a brief insight about Mobile IP, its features and entities constituting Mobile IP environment. The paper explores the working and routing mechanism of Mobile IP with a deep insight about triangle routing in Mobile IP Version 4 (MIPv4) and route optimization in Mobile IP Version 6 (MIPv6). This paper discusses several security issues regarding Mobile IP implementation. This paper also highlights route optimization problems and focuses on the solution of those problems.

Keywords

Mobile IP, Correspondent Node, Mobile Node, Home Address, Home Network, Foreign Network, Care-of-Address, Collocated Care-of-Address, Home Agent, Foreign Agent, Correspondent Agent, Tunnel, Binding Cache, Binding Warning Message, Binding Request Message, Binding Update Message, Binding Acknowledge Message, Visitor list.

1. INTRODUCTION

Last decades have seen a substantial interest in mobile networks. To provide mobility between homogeneous or heterogeneous networks IETF devised an Internet protocol for Internet users, called Mobile IP [1].

Mobile Node (MN) identified by its home address can continue communication while away from its home network [2]. The Correspondent Node (CN) communicates with MN by its home address. Home Agent (HA) is responsible for the delivery of packets to the current location of MN. The mobility of MN thus remains hidden from CN. The communication remains secure but efficiency degrades due to longer path from CN to MN via HA. Route optimization mechanism was coined to solve the problem, which in turn introduced many security issues in packet delivery at MN.

A mobile network is characterized by the concepts of MN, Home Network (HN), CN, Foreign Network (FN), Home Agent (HA), Foreign Agent (FA), Care-of-Address (CoA),

Collocated Care-of-Address (CCoA), and tunnel, Correspondent Agent (CA), Binding Cache, Binding Warning Message, Binding Request Message, Binding Update (BU) Message, Binding Acknowledge Message, Visitor list.

Mobile node (MN) is a node that shows mobility without changing its IP i.e. it can change its point of attachment from one link to another but will be reachable through its home address.

Correspondent node (CN) is a node that is intended to communicate with a MN. It may be mobile or a stationary node [1].

Home address is a permanent IP address assigned to a MN in its home network.

Care-of-Address (CoA) is an IP address of the FN, which the MN visited.

The current CoA of the MN is known as its primary CoA [1]. One CoA may correspond to multiple mobile nodes.

Collocated Care-of-Address (CCoA) is a temporary IP address assigned to a particular MN on FN, which corresponds to only one MN at a time [3].

Home Network (HN) is the network on which mobile node's permanent IP address is defined.

Foreign Network (FN) is any network that is visited by MN while away from its HN.

Home Agent (HA) is a router on the HN that provides services to MN. HA intercepts the packets destined for MN within the HN, encapsulates them and tunnels them to the mobile node's current CoA [1].

Foreign Agent (FA) is a router on the FN that intercepts packets destined for MN within the FN, encapsulates them and finally delivers them to the MN.

Tunnel is a secure path from HA to FA that ensures the successful delivery of packets to the MN.

Correspondent Agent (CA) is a router in the CN that intercepts the packets destined for the MN and directly tunnels them to the MN without any encapsulation or decapsulation.

Binding Cache is an authenticated cache, maintained by any node, which performs route optimization, for direct delivery of packets to MN [2]. It contains sorted Care-of-Addresses of MNs.

Binding Warning Message warns the node to update its binding cache.

Binding Request Message is sent by any node to get the current location of MN.

Binding Update (BU) message is used to notify the respective node about current location (CoA) of the MN.

Binding Acknowledge Message is sent as an acknowledgement of BU message only when the acknowledgement bit in the BU message is set to 1.

The FA maintains visitor list, which contains the information of all the MNs visiting the FN.

2. PHASES IN MOBILE IP

2.1. Agent Discovery Phase

In agent discovery phase MN discovers whether it is in home network or foreign network [3]. HA and FA advertise their services using ICMP Router Discovery Protocol (IRDP), which carry mobile IP extensions. MNs determine their current point of attachment from these advertisements. If a MN is unable to receive these advertisements, it may solicit the agents to send their advertisements by sending a solicitation message. Due to these advertisements, a MN may know which types of services these agents provide.

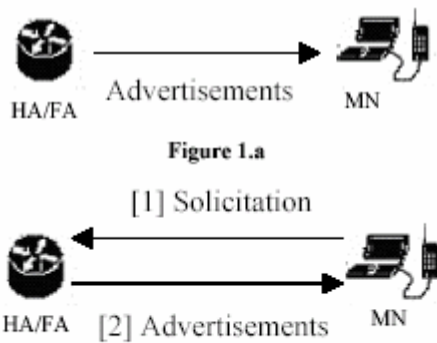


Figure 1.a

Figure 1.b

2.2. Registration Phase

In this phase MN registers its current CoA with HA by sending the registration request message to HA, either via FA or directly using mobile node's CCoA. In response to this registration request message, HA sends a registration reply message to MN again either via FA or directly to CCoA. This registration must be authenticated for the successful delivery of packets to and from the MN as it moves around. The MN must register its current location before registration time expires. After the authenticated registration of MN, HA and FA update their binding caches and visitor list entry respectively.



Figure 2.a. Registration Request via CCoA

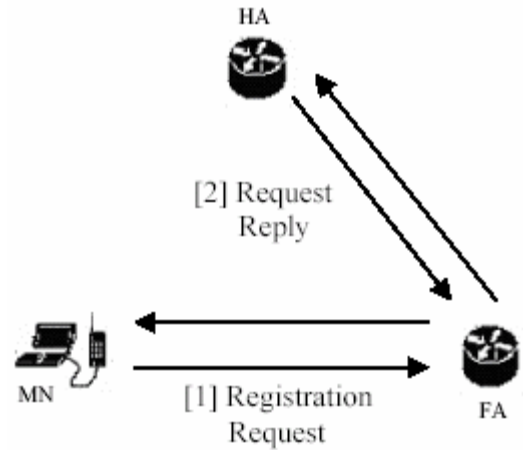


Figure 2.b. Registration Request via FA

2.3. Tunneling

During this phase, data packets are encapsulated at one end of the tunnel and decapsulated when packets reach at the other end [3].

In *packet forwarding*, CN sends packets destined for MN at home address. HA intercepts these packets, encapsulates them either using IP encapsulation within IP encapsulation, Generic Record Encapsulation (GRE) or minimal encapsulation, and tunnels them to FA. Upon receiving the packets, FA decapsulates them and delivers them to MN.

In *reverse tunneling*, MN delivers the packets to FA using source address as its home address [3]. FA encapsulates the datagrams and sends them to HA using reverse tunneling. HA delivers the packets to CN after decapsulating them.

MN may also perform the encapsulation and decapsulation if it is using its CCoA.

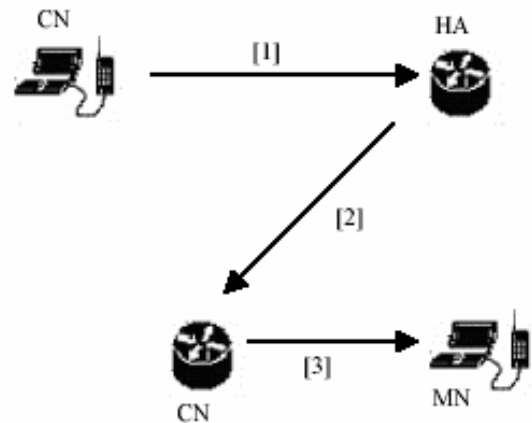


Figure 3.a Packet Forwarding

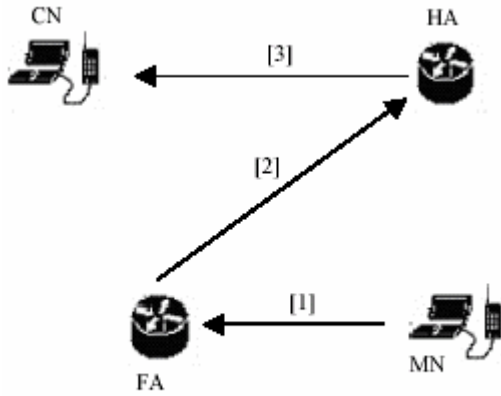


Figure 3.b Reverse Tunneling

3. TRIANGLE ROUTING

In triangle routing CN communicates with MN via HA. Packets are successfully routed to and from the MN as it roams, but this is inefficient because packets destined for MN will have to travel a longer path than the optimal path in order to reach the MN.

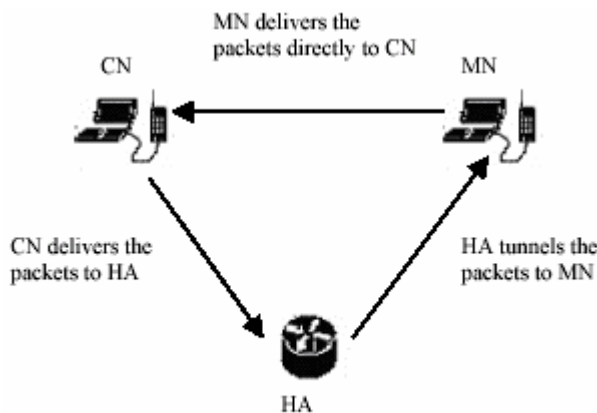


Figure 4. Triangular Routing

4. ROUTE OPTIMIZATION

To overcome the shortcomings of triangle routing, route optimization technique was introduced to directly tunnel the datagrams from CN to MN when it is away from HN.

4.2. Operation of Route Optimization

Route optimization operation can be divided into two main parts:

4.2.1. Updating Binding Caches

Before sending packets to a MN, CN checks its binding cache. If it finds the binding cache entry then packets are delivered directly to MN at its CoA. Otherwise, CN sends the datagrams to HA which tunnels them to MN [2]. For direct delivery of rest of the packets, HA sends an authenticated BU message to CN containing current CoA of the MN. Acknowledgement of BU message is not needed in this case since the reception of another packet at HA will result in delivery of another BU message. After receiving the BU message, CN maintains the

binding for MN in the binding cache to directly deliver the datagrams to MN. Each binding has an associated lifetime, which is specified in the BU message [2].

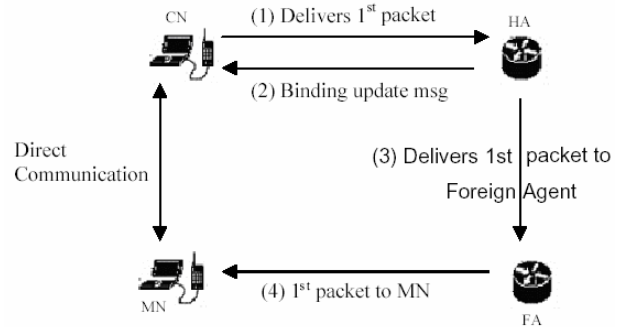


Figure 5

Consider a situation in which MN changes its location while packets detained for it are still in flight. These packets will reach MN's previous CoA. To deliver these packets to the MN's new location, smooth handoff takes place between its previous FA and new FA.

4.2.2. Foreign Agent Smooth Handoff

When MN moves from one link to another and registers there, it notifies the previous FA that maintains a mobility binding for it. This notification maybe included in registration request message sent to the new FA. The new FA builds an authenticated BU message with acknowledgement bit set to 1, and sends it to the previous FA, which upon receiving the BU message, maintains the binding in its binding cache for that MN and removes its entry from the Visitor list. The previous FA may also release the resources consumed by the MN before its registration lifetime expires. Acknowledgement of this BU message is required before the registration lifetime expires. In this way a bidirectional tunnel is established between the previous FA and new FA [4].

Now whenever FA receives datagrams destined for MN, for which it has a binding cache entry but no visiting entry, it searches the current location of MN in the binding cache and directs the datagrams to MN at that location. In the meanwhile it sends a binding warning message to HA of MN, (as shown in figure 5.a) for the delivery of BU message to the CN [2].

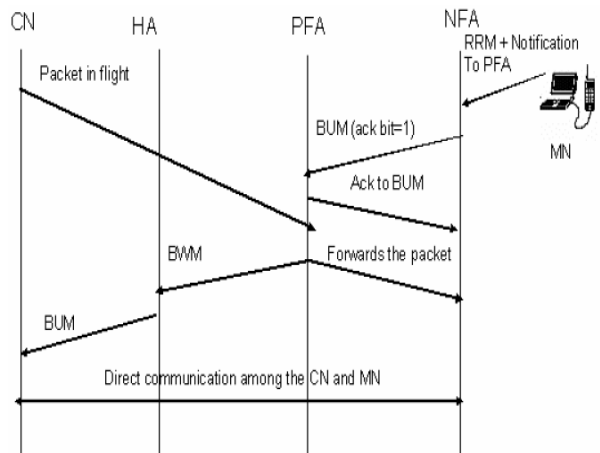


Figure 5.a

In case, if previous FA has no information about HA, it can send binding warning message directly to CN [2] (as shown in figure 5.b). CN then sends a binding request message to HA to find MN's current mobility [2]. The HA sends a BU message to CN, in response to either warning message from previous FA or binding request message from CN. This BU must be authenticated for successful delivery of datagrams to and from the MN. From this BU, CN updates its binding for MN and then starts its direct communication with the MN at its new (current) CoA.

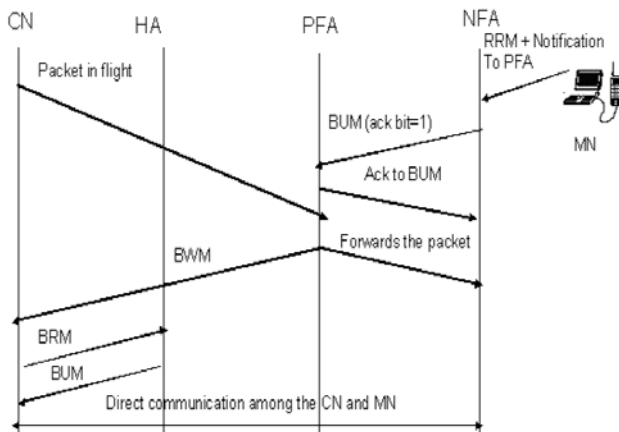


Figure 5.b

RRM: Registration Request Message
 BUM: Binding Update Message
 BWM: Binding Warning Message
 BRM: Binding Request Message

5. MOBILE IP THREATS

Route optimization provides an efficient mechanism for delivery of packets between CN and MN. On the other hand, it introduces many security issues regarding the delivery of packets from CN to MN or from MN to CN as they are directly communicating and having no security association in between them [5].

If BUs are not authenticated, then many new security problems will be introduced. Some of the attacks and possible solutions regarding these security problems are explained below.

5.1. Corrupting the Routing Table

In route optimization mechanism, CN maintains a routing table for each MN it wants to communicate with. If this table is corrupted, MN will no longer be available to CN for continuing the conversation [6]. Some possible attacks on the routing tables are:

5.1.1. Spoofing Binding Updates

If attacker is on the path between MN and CN, it can spoof the BU messages from MN to CN. It can capture these messages; make changes to them and then delivers them to the CN. If no authentication of these binding updates is to be done, then CN, believing that the message is delivered from the MN, will update its binding cache. As an example consider the following scenario:

A node **A** is sending packets to MN **B**. If an attacker is at address **C** (on the path between the MN and the CN), it could

spoof the data packets from **B**, insert false home address/CoA in them and delivers them to the CN **A**. The result of this attack will be to prevent the two parties to communicate with each other and may cause the transmission of unwanted packets to some other target node.

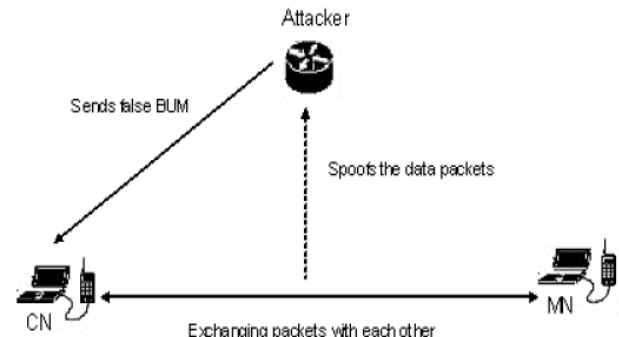


Figure 6

5.1.2. Attacks against secrecy and integrity

By sending the false BU messages to the CN, an attacker will be able to see and modify the data packets for the MN. This can be done by inserting the attacker's address in the CoA field of the spoofed BU message. When this message is delivered to the CN it will update its binding cache and starts delivering the packets to the attacker destined for the MN. Similarly an attacker could redirect the packets (for the CN) from the MN to itself. In this way an attacker (acting as the middle man) could break the integrity and secrecy between the two hosts.

5.1.3. Basic Denial of Service Attacks

By sending the false BU message to the CN, the MN and the CN will no longer be able to communicate with each other. In other words we can say that the attacker causes the basic denial of service for the two nodes as they can't be able to continue their conversation and are no longer using the resources for that communication.

5.1.4. Replaying and Blocking Binding Updates

In this attack the attacker reserves the mobile nodes previous location by capturing the BU message for that location. When the MN moves to a new location, the attacker could send (replay) the previous BU message to the CN. In this way the attacker will be able to redirect the packets for the MN to its previous location. An attacker could block the binding updates for that MN at the new location if it behaves as the MN until the correspondent cache entry for that MN expires.

5.1.5. Bombing CoA with Unwanted Data

If an attacker inserts false CoA in the BU message, it could redirect the packets to some other target node. The purpose is to bomb the target nodes with unwanted packets. This could be done if the attacker knows that there is a heavy data stream between the two nodes. This attack is serious because in this attack the target node could never know about the attacker and hence could not do anything to prevent this attack.

5.1.6. Bombing HoA with Unwanted Data

In this attack the attacker sends false BU message to the CN by inserting the target address as the home address of the MN.

After that it sends the binding cancellation message for that MN to the CN. This can be done by sending another BU message to the CN. In this BU message the attacker specifies the CoA as the home address (target nodes address) and lifetime set to zero [2]. The CN in response to such an update message will delete all its cache entries for that MN and start sending packets from the MN at its home address (in this case the target nodes address).

Thus the only solution is to authenticate the BU, each time the CN receives the BU message. Some possible solutions to these attacks are explained below:

5.2. Possible Solutions

5.2.1. Use of PKI (Public Key Infrastructure)

One way to authenticate the Binding updates is to use the typical authentication mechanisms like PKI (Public Key Infrastructure). But since the mobile IPv6 is designed at the global level, therefore it will be difficult to use a single PKI throughout the entire internet [7]. Hence some alternative solution must be considered which should be at least as much secure as for the current non-mobile IPv4 Internet.

5.2.2. Use of Cryptographically Generated Addresses

Another technique is to use the cryptographically generated addresses. The basic idea is to hash the MN's public key in the second half of the home address. This key may be from 62-64 bits of the IP address. This makes it difficult for an attacker to find the key that matches the given address. However, since only 62-64 bits of the IP address are used to hash the public key, the attacker may be able to find the match through error and trial mechanisms [6]. Also this technique could not prevent the bombing attacks.

5.2.3. Return Routability Tests

Another mechanism used to authenticate the BU is called *return routability test for the home address* [8]. In this test the CN, on receiving the initial BU message, sends a secret key to the HA which then forwards it to the MN through a secure tunnel. The MN uses that key and send the second BU message to the CN. The CN checks the key, it sends to the home address, and in this way verifies the home address of the MN.

However the only verification of home address is not sufficient as the MN acting as an attacker may send false CoA, targeting some other node, in its BU message to the CN. To solve this problem another test called *return routability test for the CoA* is required [8]. The CN sends another packet with a second key directly at the CoA. The MN uses the two keys (one from the HA and other from the CoA) to compute the BU. The correspondent on receiving the BU message checks both the keys. If any one is wrong, it will not update the binding for that MN.

These tests verify the home address and the CoA successfully, but results in many other attacks. e.g. If an attacker sends false home address and CoA to the CN, the CN triggers the BU protocol by generating two secret keys which it has to remember until it receives an authenticated BU [6]. If the attacker repeats this attack for multiple times, the CN will have to store a large number of keys. This may result in the

dropping of some initial messages of the MNs communicating with CN.

The above problem could be solved by designing some algorithm at the CN, which re-computes the keys on receiving the BU instead of remembering them [7].

5.3. Other Attacks

5.3.1. Reflection and Amplification Attack.

However another problem may be the reflection and amplification attack [6]. In the reflection attack the MN (an attacker) may send false home address to the CN, resulting in the transmission of the data packets to some other target node, which could not even know about the address of the attacker. This problem could be solved using return routability test for home address. But causing the CN to generate two messages in response to one message will amplify the packet flooding attack against the MN by a factor of two [6]. This is called amplification attack. Again the target node could never know the address of an attacker node.

These two problems could be solved by ensuring that the MN sends the initial BU message twice, one via the HA and other from its CoA, and CN responds only to that address from which it received the messages. In this way the attacker will have to send as many messages as it expects from the target node. Also it will be easier to trace the attacker by responding to the same address from which receiving the packets.

5.3.2. Unnecessary Authentication

In response to false home address or CoA, still the CN needs to do unnecessary authentication. This may result in the consumption of resources of both the MN and the CN due to the execution of BU protocol every time [6].

However unnecessary authentication can be reduced by limiting the resources like processor time, memory and communication capacity for Bindingupdate[6]. When this limit reaches, the node will stop its BU authentication and expires all its BU cache entries. Hence at worst, this attack could prevent the route optimization at all.

6. CONCLUSION

This report explains different mechanisms for optimizing the route in mobile IPv6. It also explains possible attacks and their solutions regarding the mechanisms used for optimization. However no proper solution for these security issues has been proposed yet. A lot of work is needed on this area. The actual problem exists in authenticating the binding updates between the CN and the MN. The path between the MN and the HA is much more secure as compared to the path between the MN and the CN. Hence the current task is to propose some mechanism through which the packets should be successfully delivered directly from the CN to the MN and vice versa.

7. REFERENCES

- [1] C. Perkins, D. Johnson, and J. Arkko. *Mobility Support in IPv6*. Internet Draft, IETF, February 26, 2003
- [2] Charles Perkins and David B. Johnson. *Route Optimization in Mobile IP*. Internet Draft, IETF, 6 September 2001
- [3] Introduction to Mobile IP. Version Number 1, Released 10/08/2001

[4] Rajeev Koodli. *Fast Handovers for Mobile IPv6*. Internet Draft, IETF, 1 March 2003

[5] Ericsson, and Jari Arkko. *Security Framework for Mobile IPv6 Route Optimization*. Internet Draft, November 2001

[6] J. Arkko and T.Aura. *MIPv6 BU Attacks and Defenses*. Internet Draft, February 2002

[7] Tuomas Aura. *Mobile IPv6 Security*. Microsoft Research Ltd. Roger Needham Building, 7 JJ Thomson Avenue, Cambridge, CB3 0FB, UK

[8] Ericsson, J. Arkko, and V. Devarapalli. *Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents*. Internet Draft, IETF, February 18, 2003.

Source:-

<<http://www.acm.org/ubiquity>>