Mobile IP: A Study Of Issus, Challenges, And Comparison Of Ipv4 & Ipv6

Khaled Mahmood Al-Adhal, Dr. S.S Tyagi
Department of Computer Science & Engg. Faculty of Engineering & Technology Manav Rachna International University
Professor & Head Department of Computer Science & Engg. Faculty of Engineering & Technology Manav Rachna International University

Abstract

Mobile IP [7] has been designed within the IETF to enable seamless connectivity for a new class of mobile Internet computers. The driving forces for Mobile IP include progress in wireless communications, the startling growth of the Internet, and it equally compelling growth of processing capabilities of laptops, PDAs, and other mobile computing devices.

In this paper, we are the stimulation for Mobile IP, the basics of the protocol, and the relationship of Mobile IP with other protocols, and we provide a survey of the handoff performance in Mobile IP [1].

After the protocol overview, we then proceed to brief current developments involving Mobile IP (including mobility for IP version4, 6) and the current state of standardization of Mobile IP.

Key words: Mobile IP, Issus, Handover, IP Protocol and mobility for IP version 4, 6.

Introduction

Mobile communication services are experienced remarkable growth and among these, services providing Internet access from mobile terminals are steadily increasing by tens of thousands of subscribers per day.

The greatest challenge for supporting mobility at IP layer is handling address changes **[6]** in other word, Mobile Internet Protocol, IP enables the transfer of information between mobile computers, and mobile computers include laptops and wireless communications.

The mobile computers change their locations to a foreign network, at the foreign network, the mobile computer also communicate through the home network of the mobile computer.
The increasing number of portable computers, combined with the growth of wireless services, makes supporting Internet mobility important. Many researchers came to a conclusion that IP is the correct layer to implement the basic mobility support.

When a mobile computer, or mobile node, moves to a new network while its IP address is unchanged, the mobile node address does not reflect the new point of attachment. Consequently, routing protocols that exist cannot route datagram's to the mobile node correctly. Mobile node must reconfigure with a different IP address that represents the new location **[1]**.

Assigning a different IP address is cumbersome. Thus, under the current Internet Protocol, if the mobile node moves without changing its address, it loses routing. If the mobile node does change its address, it loses connections.
Mobile IP solves this problem by allowing the mobile node to use two IP addresses, the first address is a fixed home address. And the second address is a care of address that changes at each new point of attachment, mobile IP enables a computer to roam freely on the Internet.

Mobile IP also enables a computer to roam freely on an organization's network while still maintaining the same home address. Consequently, communication activities are not disrupted when the user changes the computer's point of attachment **[1]**.
In this paper we provide a survey of the handoff performance in Mobile IP. , and evaluate the use of Link Layer Information to enhance Mobile IP handoff with the aim of reducing packet loss and handoff latency. Instead, the network is updated with the new location of the mobile node. The following figure illustrates the general Mobile IP topology.

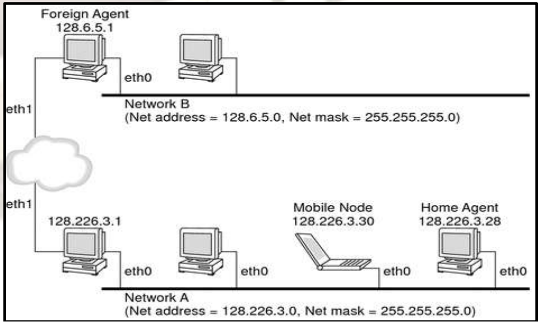

Figure 1. Mobile IP Topology

Features of Mobile IP [6]: Mobile IP was successful as it has several notable features like no geographical limitation, no physical connectivity required, supports security, no modifications for the current IP address. The main factors that influence the need for Mobile IP are:

- Mobility Support, increased number of mobile users.
- Standardization, uses the current IP Protocol
- Inter-Operability, can be used across different service providers
- Alternative Technologies, lack of proper alternatives other than Mobile IP
- IPv4 Availability, limited availability of IPv4 address necessitates the need for Mobile IP
- Improved Security, while registering with the home agent.

Problems of Mobile IP:

Although growing rapidly, Mobile IP still has the following problems:

(1) "Triangle routing" Problem: The Communication Host (CH) has to send packets to the Mobile Host (MH) via the Home Agent (HA), while the MH sends packets directly to the CH. As the communication in the two directions follows different routes, the problem of "triangle routing" arises, which leads to low efficiency especially when the MH is far away from the HA and the CH is near to the MH.

(2) Handoff Problem: Handoff problem means that the HA sends the IP packets of the MH to the original foreign network via the tunnel because it doesn’t know the latest Care of Address (CoA) of the MH during the period starting when the MH leaves the original foreign network and ending when the HA receives the new registration address of the MH. As a result, these dropped IP packets have an influence on the communication between the MH and the CH especially when handoff occurs frequently or the MH is far away from the HA.

(3) Problem of Intra-Domain Movement: The frequent intra-domain movement of the MH within a small area will lead to frequent handoff. Consequently, great amounts of registered messages are generated in the network and the network performance is greatly affected.

(4) QoS Problem: In the mobile environment, it is hard to provide QoS over Mobile IP due to dynamically varying wireless network topologies, limited network resources, unpredictable effective bandwidth and high error rate.

Overview IP Mobile: Mobile IP, *Mobile Internet Protocol* has been proposed by IETF to support portable IP addresses for mobile devices that often change their network access points to the Internet. In the basic of mobile IP protocol, datagram's sent from wired or wireless hosts and destined for the mobile host that is away from home, it have to be routed through the home agent. Nevertheless, datagram's sent from mobile hosts to wired hosts can be routed directly **[4]**.

Terminology [2]: Before getting into more details, it is a good idea to frame the discussion by setting some terminology, adapted from the mobile IP specification. Mobile IP introduces the following new functional entities [1].

Mobile Node (MN): It is a host or router that changes its point of attachment from one network or sub network to another. A mobile node may change its location without changing its IP address, it may continue to communicate with other Internet nodes at any location using its (constant) IP address, assuming linklayer connectivity to a point of attachment is available.

Home Agent (HA): A router on a mobile node's home network, which tunnels datagram’s for delivery to the mobile node when it is away from home, and maintains current location information for the mobile node and tunnels packets for delivery to the MN when it moves away from its home network.

Foreign Agent (FA): A router on a mobile node's visited network, which provides routing services to the mobile node while, registered. The foreign agent detunnels and delivers datagram's to the mobile node that were tunneled by the mobile node's home agent. For datagram's sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes.

Correspondent Node: A peer with which a MN communicates is called a correspondent Node (CN). A CN may be either mobile or stationary. If the node is mobile, it transmits and receives the packet via the HA on the other hand if the node is stationary, it transmits and receives the packet via a traditional IP router that has no mobility management capabilities.

Mobile IP basic operation: Mobile IP is a way of performing three related function:

1. Agent Discovery: Mobility agents advertise their availability on each link for which they provide service.

2. Registration: When the mobile node is a way from home, it registers its care-of address with its home agent.

3. Tunneling: In order for datagram's to be delivered to the mobile node when it is away from home, the home agent has to tunnel the datagram's to the care-of address **[4]**.

The following figure shows a mobile node that resides on its home network, Network A, before the mobile node moves to a foreign network, Network B. Both networks support Mobile IP.

The mobile node is always associated with the home address of the mobile node, 128.226.3.30 **[1]**.

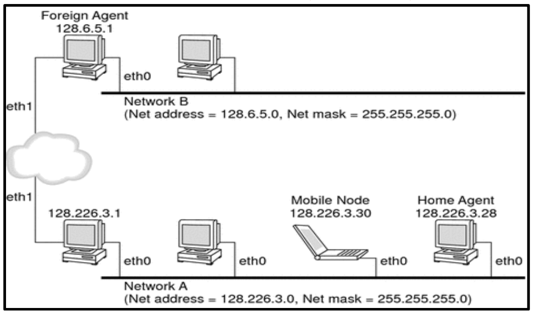

Figure 2. Mobile Node Residing On Home Network

The following figure shows a mobile node that has moved to a foreign network, Network B. Datagram's that are destined for the mobile node are intercepted by the home agent on the home network, Network A. The datagram's are encapsulated. Then, the datagram's are sent to the foreign agent on Network B. The foreign agent strips off the outer header. Then the foreign agent delivers the datagram to the mobile node that is located on Network B.

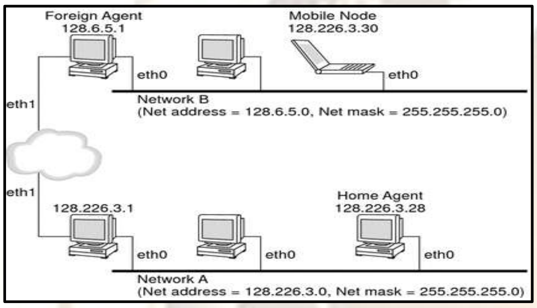

Figure 3. Mobile Nodes Moving to a Foreign Network

Protocol overview: Now, we will go into more detail about the various parts of the protocols.

Mobile Agent Discovery: The agent discovery procedure used in Mobile IP is based on the Internet Control Message Protocol (ICMP) router advertisement standard protocol. Agent advertisements are typically broadcast at regular intervals (e.g., once a second, or once every few seconds) and in a random fashion, by HA and FA.
When a MN is away from home, it wants to find agents so that it does not lose access to the Internet. There are two ways of finding agents **[7]**.
Firstly; selecting an agent from those periodically advertised.
Secondly; sending out a periodic solicitation until it receives a response from a mobility agent. MN thus gets its COA, which may be dynamically assigned or associated with its FA.

A mobility agent advertising its services on a link transmits agent advertisements **[1]**. MNs use these advertisements to determine their current point of attachment to the Interne.

Registration: A MN registers whenever it detects that its point-of attachment to the network has changed from one link to another. MN registers its COA with it's HA in order to obtain service, the registration process can be performed directly from the MN, or relayed by the FA to the HA, depending on whether the COA was dynamically assigned or associated with its FA **[8]**.

Tunneling: Tunneling is the method used to forward the message as described in Fig3, from HA to FA and finally to the MN.

After a MN returns home, it deregisters with it's HA to drop its registered COA. In other words, it sets its COA back to its home address. The MN achieves this by sending a registration request directly to it's HA with a lifetime set to Zero. There it has no need to deregister with the FA because the service expires automatically when the service time expires **[8]**.

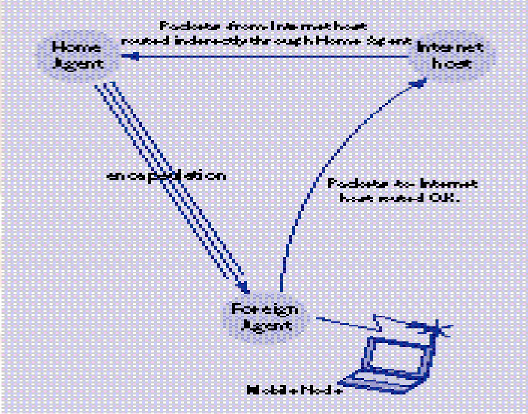
Packets from Internet host
routed indirectly through Home Agent
Home Agent
Internet host
encapsulation
Packets to Internet host routed OK.
Foreign Agent
Mobile Node

Figure 4. Tunneling Operation in Mobile IP

The source, encapsulator, decapsulator, and destination are separate nodes. The encapsulator node is considered as the entry point of the tunnel, and the decapsulator node is considered as the exit point of the tunnel.

Encapsulation is the mechanism of taking a packet consisting of packet header and data, putting it into the data part of a new packet. Encapsulation is a very general technique, used for many different reasons including multicast, multiprotocol operations, authentication, privacy, traffic analysis, and general policy routing.

Decapsulation is the reverse process of encapsulation. During service time (after the registration process and before the service time expiration), MN gets forwarded packets from FA, which were originally sent from the MN's HA.

Rout optimization of Mobile IP: We first provide an overview of the mobile Internet Protocol (MIP) **[2]**, including the "triangle routing" problem and the route optimization in mobile IP.
Mobile IP, the mobility support for IP, enables a mobile host (MH) to send datagram's to the correspondent host (CH) directly, routed by its home agent (HA) and foreign agent (FA)

However, packets from CH to MH have to be routed through three different (sub) networks: the CH's subnet, the HA's subnet, and the FA's subnet where the MH is currently located.

Therefore, packets destined to the MH are often routed along paths that are significantly longer than optimal. This redundant routing in mobile IP is known as "triangle routing **[3]**.

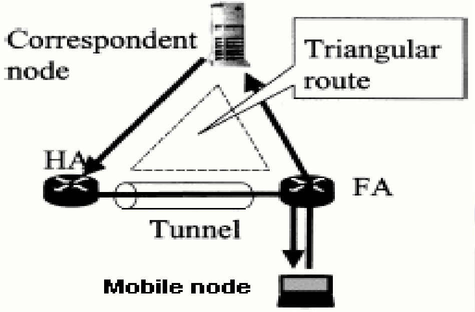

Figure 5. Triangle routing

This represents a routing asymmetry which is potentially noticeable and annoying to mobile users. It also sets up the home agent to be a single point of failure in the path to all the mobile nodes on the home network, and substantially increases the vulnerability of network operation on the mobile node to random congestion and traffic outages in the Internet **[1]**

Route optimization addresses this problem by requiring all hosts to maintain a binding cache containing the care-of address of MHs. The binding cache is a cache of mobility bindings of mobile nodes, maintained by a node to be used in tunneling datagram's to mobile nodes. Route optimization extension to mobile IP includes four messages: binding update, binding warning, binding request, and binding acknowledgment.

A binding update message is used to inform the CH of the MH's current mobility binding. The binding warning message is used to transmit warnings that a binding update message is needed by one or more correspondent hosts **[2]**.

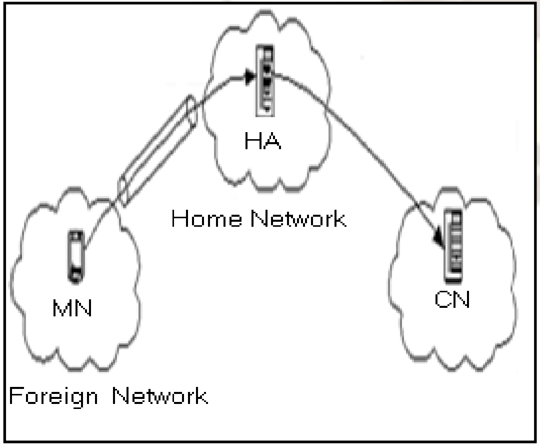

Fig 6.A. MN to CN in Basic Operation

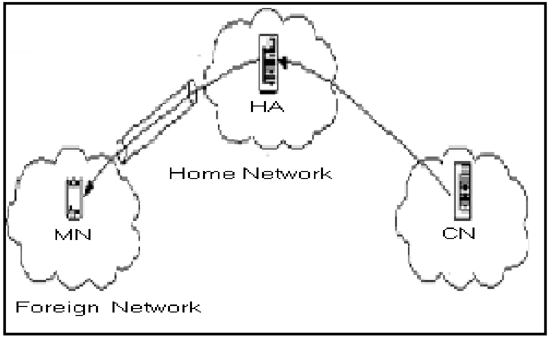

Fig 6.B. CN to MN in Basic Operation

Route optimization can be described in four parts:

- binding cache maintenance,
- smooth Handoffs,
- registration Key management,
- Special Tunnels.

The first three of these topics will form the topics of the next brief subsections.

Binding cache maintenance: In order to deliver bindings to correspondent nodes, route optimization defines four new messages sent to the same port (via UDP) as the base Mobile IP protocol:

- binding Warning (informs correspondent node that it should get a new binding),
- binding Request (correspondent node asks for a new binding),
- binding Update (correspondent node receives a new binding),
- Binding Acknowledgement (correspondent node acknowledges receipt).

The handling of these messages is fairly straight forward, with the following observations:

- the home agent typically delivers Binding Updates to the correspondent node, if the correspondent node sends a packet to the mobile node at its home address,
- thus, delivery of Binding Updates has to be drastically rate limited, since most correspondent nodes will not implement support for Binding Updates in the near future,
- the mobile node typically does not deliver the Binding Updates,

A correspondent node with a stale binding will tunnel packets to the wrong care-of address. The foreign agent at the stale care-of address should send a binding warning to either the correspondent node, or to the home agent.

Just as with a Registration Request to a home agent, a Binding Update could create the opportunity for mischief if accepted from an unauthorized agent.

To protect against this, a correspondent node should not process any Binding Update unless it can be certain that the update was sent either by the mobile node or on behalf of the mobile node by an authorized agent such as the mobile node's home agent. An authentication extension to the Binding Update message is provided for this purpose.

Smooth handoffs: One interesting case is the delivery of a Binding Update to the mobile node's previous foreign agent whenever the mobile node moves to a new care-of address.

If this action is performed, the previous foreign agent can then deliver packets to the mobile node at its new care-of address. In doing this, the opportunity for dropping packets is drastically reduced, especially if the mobile node notifies its foreign agent immediately upon arrival at its new care-of address – even before the new registration process has completed.

To affect this smooth handoff, a *Previous Foreign Agent Notification* message has been defined. In this message, the mobile node creates all the information needed by its new foreign agent to deliver an authenticated Binding Update to the previous foreign agent.

The previous foreign agent is *required* to send a Binding Acknowledgement to the mobile node at its new care-of address.

As it happens, a foreign agent is modeled as a cheap and largely passive device in Mobile IP. It's not necessarily the type of network appliance that would keep a long list of clients and their respective security associations.

Thus, route optimization offers a variety of protocol messages enabling the establishment of a *registration key*, which can then be used to authenticate future Binding Update messages from the mobile node after it moves to another point of attachment. These messages are the subject of the next section.

Registration key establishment: To enable smooth handoffs, the mobile node needs a security association with its foreign agents.

This can be provided by using the appropriate messages piggybacked onto the base Mobile IP Registration Request message. At the conclusion of the registration process when the mobile node receives the Registration Reply, these key establishment messages allow the distribution of the registration key to both the mobile node and the foreign agent.

Typically, an appropriate key request message is appended to the Request message, and the corresponding key reply messages are appended to the reply.

There are a number of specific messages defined, in order to allow a great deal of exibility in the still-emerging area of key management. Among the possible scenarios, there are the following:

- The foreign agent could have a public key,
- the mobile node could have a public key,
- the foreign agent and mobile node could carry out a Diffie-Hellman key exchange,
- the foreign agent could share a security association with the home agent,
- The foreign agent could share a security association with the mobile node.

In any of these cases, a registration key can be securely established. In all but the last case, the registration key messages are authenticated to the mobile node by the home agent, which has the effect of eliminated most common *man-in-the-middle* attacks. Such attacks are particularly worrisome in a wireless environment with access mediated by an anonymous foreign agent.

Mobile IPv4 Overview [4]:

IP version 4 assumes that a node's IP address uniquely identifies the node's point of attachment to the Internet.

Therefore, a node must be located on the network as indicated by its IP address in order to receive datagram's destined to it; otherwise, datagram's destined to the node would be undeliverable. For a node to change its point of attachment without losing its ability to communicate, currently one of the two following mechanisms must typically be employed:

1. The node must change its IP address whenever it changes its point of attachment.
2. Host-specific routes must be propagated throughout much of the internet routing fabric.

Both of these alternatives are often unacceptable. The first makes it impossible for a node to mention transport and higher layer connections when the node changes location. The second has obvious and server scaling problems, especially relevant conceding the explosives growth in sales of notebook (mobile) computers.

A new scalable mechanism required for accommodating node mobility within the Internet **[6]**.

Mobile IPv6 Overview: Mobile IPv6 is the current protocol and in the present, routers are more faster and new technologies are reduced the Internet delay (delay incurred in transmitting packets from one network to another). Mobility support in IPv6 is particularly important, as mobile computers are likely to account for a majority or at least a substantial fraction of the population of the Internet during the lifetime of IPv6. The Mobile IPv6 protocol is just as suitable for mobility across homogeneous media as for mobility across heterogeneous media. For example, Mobile IPv6 facilitates node movement from one Ethernet segment to another as well as it facilitates node movement from an Ethernet segment to a wireless

LAN cell, with the mobile node's IP address remaining unchanged in spite of such movement **[13]**.

Differences between Mobile IPv6 and Mobile IPv4 [10]: There is no need to deploy special routers as "Foreign Agents", as in Mobile IPv4. Mobile IPv6 operates in any location without any special support required from the local router.

Support for route optimization is a fundamental part of the protocol, rather than a nonstandard set of extensions as IPv4.

Mobile IPv6 route optimization can operate securely even without pre-arranged security associations.

It is expected that route optimization can be deployed on a global scale between all mobile nodes and correspondent nodes.

Support is also integrated into Mobile IPv6 for allowing route optimization to coexist efficiently with routers that perform "ingress filtering".

The IPv6 Neighbor Unreachability Detection assures symmetric reach ability between the mobile node and its default router in the current location.

Most packets sent to a mobile node while away from home in Mobile IPv6 are sent using an IPv6 routing header rather than IP encapsulation, reducing the amount of resulting overhead compared to Mobile IPv4.

Mobile IPv6 is decoupled from any particular link layer, as it uses IPv6 Neighbor Discovery instead of ARP. This also improves the robustness of the protocol.

The use of IPv6 encapsulation (and the routing header) removes the need in Mobile IPv6 to manage "tunnel soft state".

The dynamic home agent address discovery mechanism in Mobile IPv6 returns a single reply to the mobile node. The directed broadcast approach used in IPv4 returns separate replies from each home agent.

Conclusion

Mobile IP is the genesis and continuing motivation for a worldwide effort to bring wireless data communications into common use. This report has given the review technical protocol details, status of the standardization process.

The main goal of the Mobile IP is to develop routing support to permit IP Nodes using either IPv4 or IPv6 to seamlessly roam among IP subnetworks and media types.

It seems certain that Mobile IP will play an increasingly important part in the deployment of future Internet mobile networking, and current events related to the specification and production of standard billing procedures seem likely to accelerate the penetration of Mobile IP into the marketplace.

And also in this paper we had mention the differences between kinds of protocols used in mobile IP, in next paper we are going to discuss the details of each protocol, and the basic operation, development, handover performance, and their problems in the current state.

Reference

1. Charles E. Perkins, "Mobile IP" (publisher: prentic hall] (Feb.2008)
2. Charles E. Perkins, Sun Microsystems (Mobile IP) 2009
3. Deguang Le, Jinyi Chang "Tunnelling-Based Route Optimization for Mobile IPv6" (20 1 0 IEEE)
4. Fayza nada "performance analysis of Mobile IPv4 and Mobile IPv6" The international Arab journal of information technology, vol 4, No 2, April 2007.
5. Jinfang Zhou and Ni Sun "A Seamless Handoff Scheme for Mobile IP" 2006 IEEE
6. Harri Forsgren, Kaj Grahn, Jonny Karlsson, Timo Karvi, and G○ran Pulkkis, 2009 IEEE "Securing Control Signaling Mobile IPV6 In Route Optimization With Identitybasedencryption
7. Janani Chandrasekaran " Mobile IP: Issues, Challenges and Solutions"
8. Mohammed Alnas, Irfan Awan and R Holton."A Survey of Handoff Performance in Mobile IP" Third UKSim European Symposium on Computer Modeling and Simulation 2009.
9. Mohamed Alnas, Irfan Awan, D.R Holton "Handoff Mechanism in Mobile IP" 2009 IEEE
10. Nguyen Ngoc Chan, Tran Cong Hung " Mechanisms of Mobile IP in delivering packets and its trends for changing from IPv4 to IPv6" Feb.2007
11. Reza Malekian "Mobile IP Network Mobility" 2008 International Conference on Advanced Computer Theory and Engineering
12. Reza Malekian "The Study of Handover in Mobile IP Networks" 2008 IEEE
13. Tsunehiko Chiba, Hidetoshi Yokota, Ashutosh Dutta, Dana Chee, Henning Schulzrinne "Route Optimization for Proxy Mobile IPv6 in IMS Network " 2008 IEEE
14. Qazi Bouland Mussabbir, Wenbing Yao, Zeyun Niu, and Xiaoming Fu “Optimized FMIPv6 Using IEEE 802.21 MIH Services in Vehicular Networks” 2007 IEEE.