Performance of Various Mobile IP Protocols and Security Considerations

K.V.Ramana Ph.D. *vamsivihar@gmail.com*
Jawaharlal Nehru Technological University
Kakinada, 533003,India
.

Raghu.B.Korrapati Ph.D. *raghu.korrapati@waldenu.edu*
Walden University

K.S.S. Praveen Kumar *praveen.kanakala@gmail.com*
Jawaharlal Nehru Technological University
Kakinada, 533003,India.

Bh.V. Naveen *naveen.bhimala@gmail.com*
Jawaharlal Nehru Technological University
Kakinada, 533003,India

Abstract

Mobile IP is the underlying technology for support of various mobile data and wireless networking applications. Mobile IP can be thought of as the cooperation of three major subsystems. First , there is a discovery mechanism defined so that mobile computers can determine their new attachment points (new IP addresses) as they move from place to place within the internet. Second , once the mobile computer knows the IP address at its new attachment point , it registers with an agent representing it at its home network. Lastly , Mobile IP defines simple mechanisms to deliver datagram's to the mobile node when its is away from its home network. This work focuses on parameters based comparison for different mobile IP protocols. Parameters include Bandwidth , Time Delay and file size. An analytic model is adopted to propose for evaluating the mean signaling delay and the mean bandwidth per call according to the type of MT mobility. In this analysis, the MHMIP outperforms the DHMIP and MIP strategies in almost all the studied cases. The main contribution of this paper is the analytic model that allows the mobility management performance evaluation and basic security implementations on Agents. In future, Maintaining most computers on a private network, visible to the public Internet necessitated with highly secured environment.

Keywords: Mobile IP, Agents , Band width , Time delay, Mobility Management.

1. INTRODUCTION

Mobile Computing is becoming increasingly important due to the rise in the number of portable computers and the desire to have continuous network connectivity to the Internet irrespective of the physical location of the node. The Internet infrastructure is built on top of a collection of protocols, called the TCP/IP protocol suite. **Transmission Control Protocol (TCP)** and **Internet Protocol (IP) [1],[2]** are the core protocols in this suite. IP requires the location of any host connected to the Internet to be uniquely identified by an assigned IP address. This raises one of the most important issues in mobility, because when a host moves to another physical location, it has to change its IP address. However, the higher level protocols require IP address of a host to be fixed for identifying connections. **The Mobile Internet Protocol (Mobile IP) [3]** is an extension to the Internet Protocol proposed by the **Internet Engineering Task Force (IETF)** that addresses this issue. It enables mobile computers to stay connected to the Internet regardless of their location and without changing their IP address. More precisely, Mobile IP is a standard protocol that builds on the Internet Protocol by making mobility transparent to applications and higher level protocols like TCP.

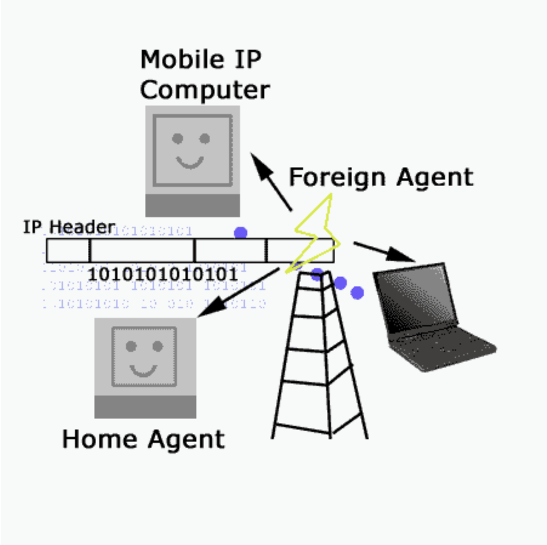
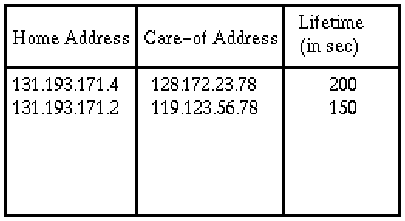


Figure 1: Mobile IP

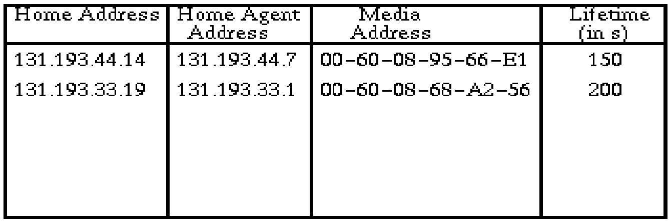
Mobile IP supports mobility by transparently binding the home address of the mobile node with its care-of address. This mobility binding is maintained by some specialized routers known as mobility agents. **Mobility agents** are of two types - **home agents and foreign agents**. The home agent, a designated router in the home network of the mobile node, maintains the mobility binding in a mobility binding table where each entry is identified by the tuple <permanent home address, temporary care-of address, association lifetime>. Table 1 shows a mobility binding table. The purpose of this table is to map a mobile node's home address with its care-of address and forward packets accordingly.



Home Address	Care-of Address	Lifetime (in sec)
131.193.171.4 131.193.171.2	128.172.23.78 119.123.56.78	200 150

TABLE 1: Mobility Binding Table

Foreign agents are specialized routers on the foreign network where the mobile node is currently visiting. The foreign agent maintains a visitor list which contains information about the mobile nodes currently visiting that network. Each entry in the visitor list is identified by the tuple: < permanent home address, home agent address, media address of the mobile node, association lifetime>. Table 2 shows an instance of a visitor list.



Home Address	Home Agent Address	Media Address	Lifetime (in s)
131.193.44.14	131.193.44.7	00-60-08-95-66-E1	150
131.193.33.19	131.193.33.1	00-60-08-68-A2-56	200

TABLE 2: Visitor List

In a typical scenario, the care-of address of a mobile node is the foreign agent's IP address. There can be another kind of care-of address, known as collocated care-of address, which is usually obtained by some external address assignment mechanism.

The basic Mobile IP protocol has four distinct stages. These are:

- **Agent Discovery:** Agent Discovery consists of the following steps:
  - Mobility agents advertise their presence by periodically broadcasting Agent Advertisement messages. An Agent Advertisement message lists one or more care-of addresses and a flag indicating whether it is a home agent or a foreign agent.
  - The mobile node receiving the Agent Advertisement message observes whether the message is from its own home agent and determines whether it is on the home network or a foreign network.
  - If a mobile node does not wish to wait for the periodic advertisement, it can send out Agent Solicitation messages that will be responded by a mobility agent.
- **Registration:** Registration consists of the following steps:
  - If a mobile node discovers that it is on the home network, it operates without any mobility services.
  - If the mobile node is on a new network, it registers with the foreign agent by sending a Registration Request message which includes the permanent IP address of the mobile host and the IP address of its home agent.
  - The foreign agent in turn performs the registration process on behalf of the mobile host by sending a Registration Request containing the permanent IP address of the mobile node and the IP address of the foreign agent to the home agent.
  - When the home agent receives the Registration Request, it updates the mobility binding by associating the care-of address of the mobile node with its home address.
  - The home agent then sends an acknowledgement to the foreign agent.
  - The foreign agent in turn updates its visitor list by inserting the entry for the mobile node and relays the reply to the mobile node.

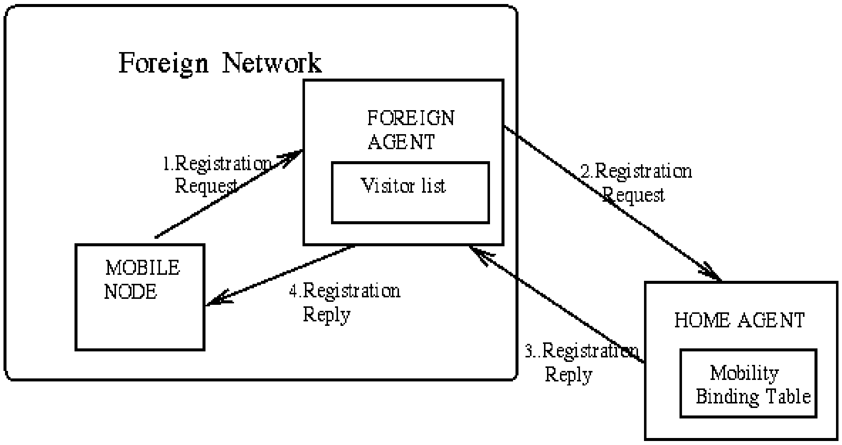


FIGURE 2: Registration process in Mobile IP

- **In Service:** This stage can be subdivided into the following steps:
  - When a correspondent node wants to communicate with the mobile node, it sends an IP packet addressed to the permanent IP address of the mobile node.
  - The home agent intercepts this packet and consults the mobility binding table to find out if the mobile node is currently visiting any other network.
  - The home agent finds out the mobile node's care-of address and constructs a new IP header that contains the mobile node's care-of address as the destination IP address. The original IP packet is put into the payload of this IP packet. It then sends the packet. This process of encapsulating one IP packet into the payload of another is known as IP-within-IP encapsulation, or tunneling.
  - When the encapsulated packet reaches the mobile node's current network, the foreign agent decapsulates the packet and finds out the node's home address. It then consults the visitor list to see if it has an entry for that mobile node.
  - If there is an entry for the mobile node on the visitor list, the foreign agent retrieves the corresponding media address and relays it to the mobile node.
  - When the mobile node wants to send a message to a correspondent node, it forwards the packet to the foreign agent, which in turn relays the packet to the correspondent node using normal IP routing.
  - The foreign agent continues serving the mobile node until the granted lifetime expires. If the mobile node wants to continue the service, it has to reissue the Registration Request.

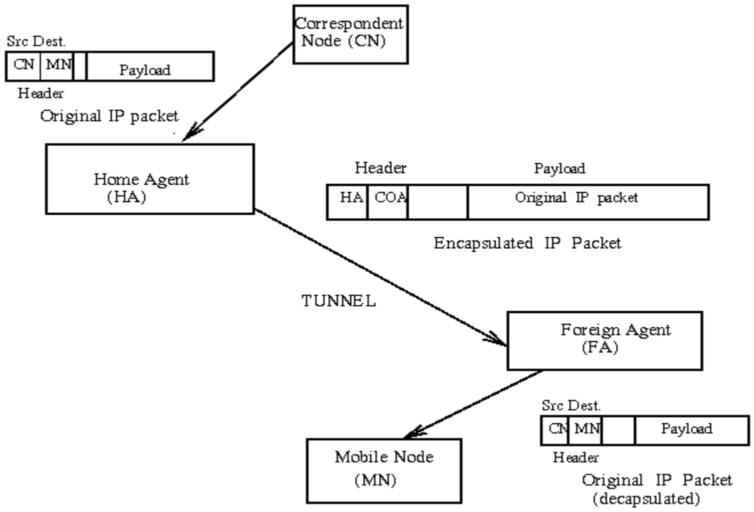


FIGURE 3: Tunneling operation in Mobile IP

- **Deregistration:** If a mobile node wants to drop its care-of address, it has to deregister with its home agent. It achieves this by sending a Registration Request with the lifetime set to zero. There is no need for deregistering with the foreign agent as registration automatically expires when lifetime becomes zero. However if the mobile node visits a new network, the old foreign network does not know the new care-of address of the mobile node. Thus datagram already forwarded by the home agent to the old foreign agent of the mobile node are lost.

The hierarchical mobile IP (HMIP) **[4]** protocol was proposed to employ the hierarchy of foreign agents (FAs) and the gateway FAs (GFAs) to reduce the number of registration operations and to reduce the signaling latency. However, since user mobility characteristics and network traffic load are always in changing, the centralized and pre-planned network topology of HMIP would become invalid or even lead more signaling cost if no adjustment to be adopted. This paper introduces a novel distributed and dynamic mobility management strategy for mobile IP where the signaling burden is evenly distributed and the regional network boundary is dynamically adjusted according to the real-time measurement of handover strength or traffic load in the networks.

The rest of the paper is organized as follows. In Section 2, demonstrates the related work which gives brief idea about existing system and proposed system. In Section 3, the core module of this work and the respective methodology is presented. In Section 4, Security issues are highlighted. In Section 5, the results and graphs of the proposed methodology are presented. Finally, Section 6 concludes the paper.

2. RELATED WORK

The mobile IP can provide continuous Internet access services for the mobile user and does provide a simple and scalable solution to user mobility. Yet, mobile IP is not a good solution for users with high mobility because it may cause excessive signaling traffic and long latency. The hierarchical mobile IP (HMIP) protocol was proposed to employ the hierarchy of foreign agents (FAs) and the gateway FAs (GFAs) to reduce the number of registration operations and to reduce the signaling latency.

However, since user mobility characteristics and network traffic load are always in changing, the centralized and pre-planned network topology of HMIP would become invalid or even lead more signaling cost if no adjustment to be adopted.

This paper introduces a novel distributed and dynamic mobility management strategy for mobile IP where the signaling burden is evenly distributed and the regional network boundary is dynamically adjusted according to the real-time measurement of handover strength or traffic load in the networks.

Thence, an analytic model is adopted to propose for evaluating the mean signaling delay **[5]** and the mean bandwidth per call according to the type of MT mobility. In this analysis, the MHMIP outperforms the DHMIP and MIP strategies**[6], [7]** in almost all the studied cases. The main contribution of this paper is the analytic model that allows the mobility management performance evaluation and basic security implementations on Agents.

2. METHODOLOGY

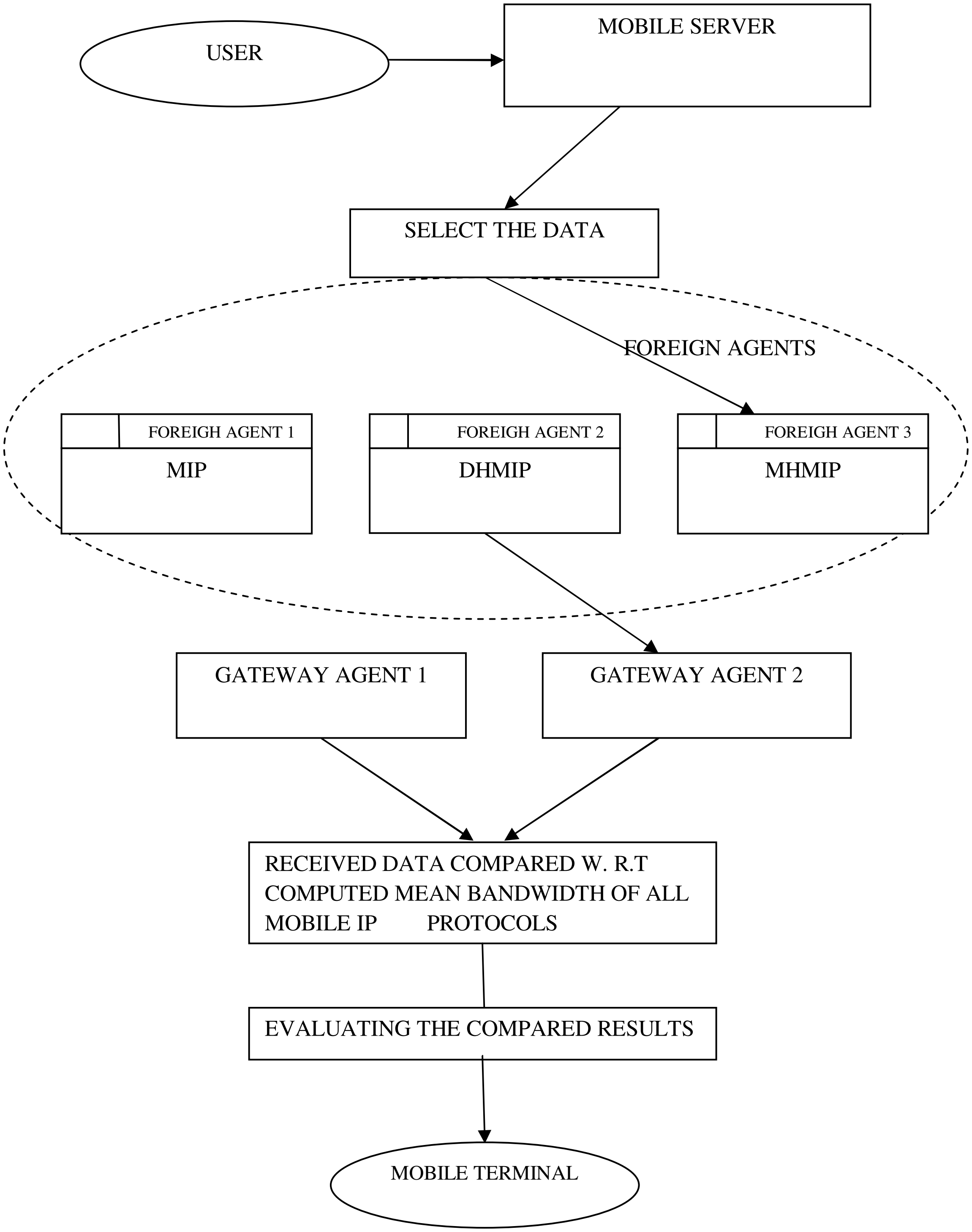
Working of Mobile IP

A mobile node can have two addresses - a permanent home address and a care of address (CoA), which is associated with the network, the mobile node is visiting. There are two kinds of entities in Mobile IP:

- A home agent stores information about mobile nodes whose permanent home address is in the home agent's network.
- A foreign agent stores information about mobile nodes visiting its network. Foreign agents also advertise care-of addresses, which are used by Mobile IP.

A node wanting to communicate with the mobile node uses the permanent home address of the mobile node as the destination address to send packets to. Because the home address logically belongs to the network associated with the home agent, normal IP routing mechanisms forward these packets to the home agent. Instead of forwarding these packets to a destination that is physically in the same network as the home agent, the home agent redirects these packets towards the foreign agent through an IP tunnel by encapsulating the datagram with a new IP header using the care of address of the mobile node.

Control Flow Sructure of Proposed Methodology


USER
MOBILE SERVER
SELECT THE DATA
FOREIGN AGENTS
FOREIGH AGENT 1
MIP
FOREIGH AGENT 2
DHMIP
FOREIGH AGENT 3
MHMIP
GATEWAY AGENT 1
GATEWAY AGENT 2
RECEIVED DATA COMPARED W. R.T
COMPUTED MEAN BANDWIDTH OF ALL
MOBILE IP PROTOCOLS
EVALUATING THE COMPARED RESULTS
MOBILE TERMINAL

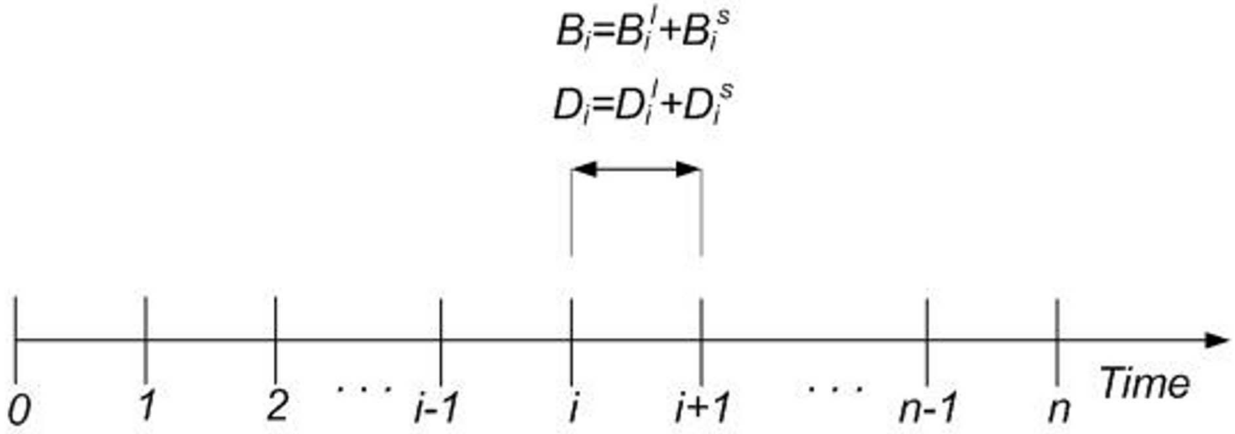
The above figure depicts the illustration of the contended methodology, the data entered by the mobile user is sent to the mobile terminal. The Mobile Terminals (MTs) registers with the Home Agents (HAs) When ever their Care-of-Addresses (CoAs) change. They use different Foreign Agents (FAs) and Gateway FAs (GFAs) hierarchy's to concentrate the registration processes. For high-mobility MTs, the Hierarchical MIP (HMIP) and Dynamic HMIP (DHMIP) strategies localize the registration in FAs and GFAs, yielding to high-mobility signaling. The Multicast HMIP strategy limits the registration Processes in the GFA's. We evaluate the mean signaling delay and the mean bandwidth per call according to the type of MT mobility at the mobile server.

When acting as transmitter, a mobile node sends packets directly to the other communicating node through the foreign agent, without sending the packets through the home agent, using its permanent home address as the source address for the IP packets. This is known as triangular routing. If needed, the foreign agent could employ reverse tunneling by tunneling the mobile node's packets to the home agent, which in turn forwards them to the communicating node. This is needed in networks whose gateway routers have ingress filtering enabled and hence the source IP address of the mobile host would need to belong to the subnet of the foreign network or else the packets will be discarded by the router.

The Mobile IP protocol defines the following:

- An authenticated registration procedure by which a mobile node informs its home agent(s) of its care-of-address.
- an extension to ICMP Router Discovery, which allows mobile nodes to discover prospective home agents and foreign agents; and
- The rules for routing packets to and from mobile nodes, including the specification of one mandatory tunneling mechanism and several optional tunneling mechanisms.

In order to understand the contended mechanism, an illustration is considered by taking as an example the mean bandwidth computation. In this figure, the holding time of ongoing call is divided into time intervals small enough that we may assume that in each time interval]i, i + 1], at most one handoff may occur.



In each interval, let

- n be the number of intervals for a call,
- B^l_i be the bandwidth used by a call during the time interval]i, i + 1],
- B^s_i be the signaling bandwidth used by a call during handoff that occurred in the time interval]i , i+1], and

- B^i be the total bandwidth used by a call during the time interval]i , i+1]

B^l_i and B^s_i are random variables with values that depend on the occurrence or not of a handoff during the interval]i, i+1] and on the possible path reestablishment once the handoff occurs.

The variable B^l_i can take two values. When a handoff occurs for a call in the interval]i; i + 1], B^l_i represents the sum of the allocated bandwidth over the original path and the one allocated over the links of the new established path.

Otherwise, it represents the bandwidth used on the link of the on-going connection. Bi represents the sum of the bandwidth used by the on-going call (B^l_i) and the bandwidth used for signalling (B^s_i). Otherwise, it represents the allocated bandwidth to the on-going call (B^l_i).

$$B_i = B^l_i + B^s_i \qquad (1)$$

$$B_i = B^l_i \qquad (2)$$

Equation (1), is applicable only if a handoff occurs in [i, i+1] and other Equation (2) is applicable.

The mean of B_i over the handoff events is given by the following equation,

$$E[B_i] = E[B^l_i] + E[B^s_i]$$

The computed mean bandwidth value is used as a parameter to evaluate the comparison among different Mobile IP protocols.

Motivation for The Mobile IP Design

The IP address of a host consists of two parts: 1) The higher order bits of the address determine the network on which the host resides; 2) The remaining low-order bits determine the host number.

IP decides the next-hop by determining the network information from the destination IP address of the packet. On the other hand, higher level layers like TCP maintain information about connections that are indexed by a quadruplet containing the IP addresses of both the endpoints and the port numbers. Thus, while trying to support mobility on the Internet under the existing protocol suite, we are faced with two mutually conflicting requirements: (1) a mobile node has to change its IP address whenever it changes its point of attachment, so that packets destined to the node are routed correctly, (2) to maintain existing TCP connections, the mobile node has to keep its IP address the same. Changing the IP address will cause the connection to be disrupted and lost.

Mobile IP, the standard proposed by IETF, is designed to solve the problem by allowing each mobile node to have two IP addresses and by transparently maintaining the binding between the two addresses. One of the IP addresses is the permanent home address that is assigned at the home network and is used to identify communication endpoints. The other is a temporary care-of address that represents the current location of the host. The main goals of Mobile IP are to make mobility transparent to the higher level protocols and to make minimum changes to the existing Internet infrastructure.

4. SECURITY ISSUES

To provide security for the network, it is essential to incorporate security mechanism in the communicating parties of the network. In this regard, Security modules configured for the router is much more vital. This section projects the demonstration of implementing security on Routers.

Implementing Security on Routers

The diagram below shows a simple network configuration.

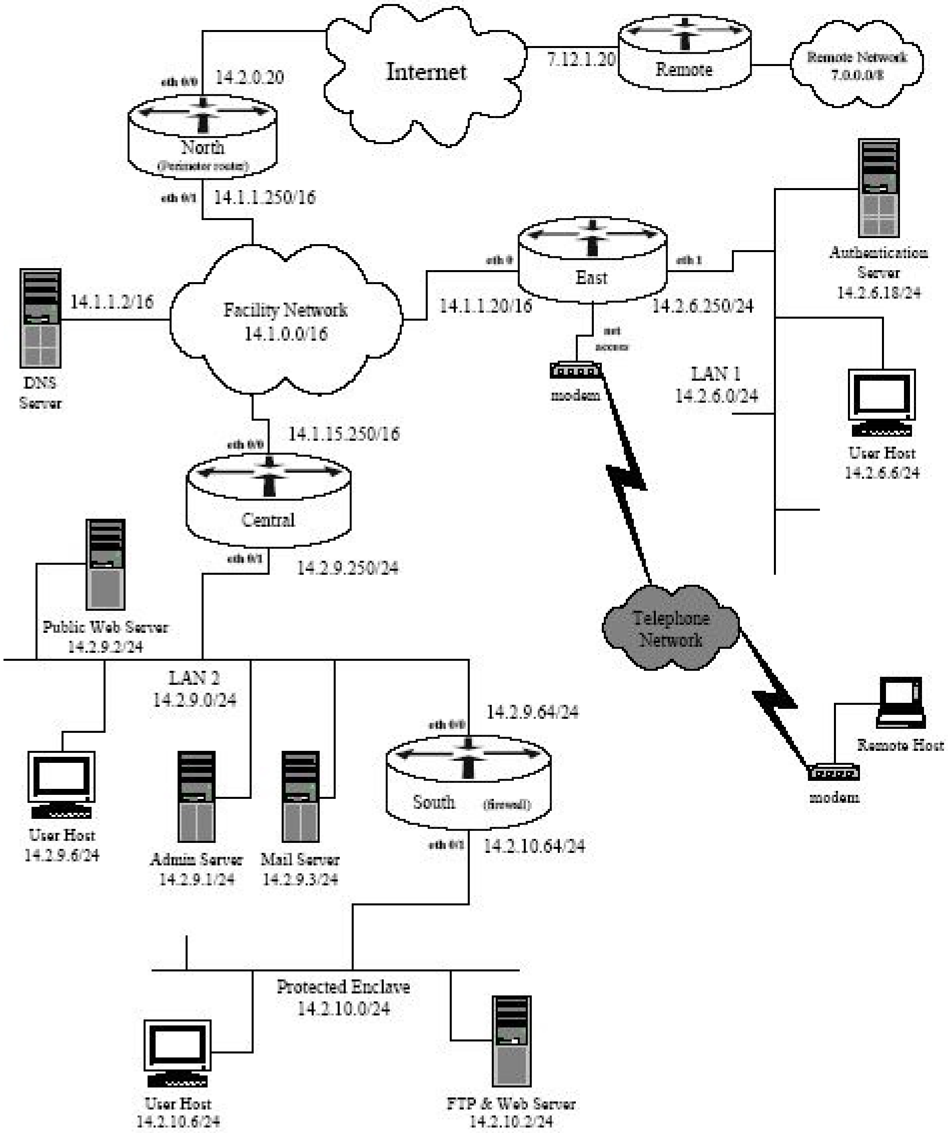


FIGURE 4: Example Network Architecture.

Above figure is simply a vehicle for presenting security guidance about routers, it is not a design for a secure network. However, this architecture reasonably reflects the kinds of networks found in many organizations.

Router Access Security

This includes various mechanisms used to protect the router itself. These include physical access, router network traffic and loopback interface, remote administration concerns, and configuration issues.

- **Physical Security**

  Network equipment, especially routers and switches, should be located in a limited access area. If possible, this area should only be accessible by personnel with administrative responsibilities for the router. In practice, physical security mechanisms and policies must not make access too difficult for authorized personnel, or they may find ways to circumvent the physical security precautions.

  To illustrate one reason why physical security is critical to overall router security, consider the password recovery procedure for routers. Using this procedure, an individual with physical access can gain full privileged (enable) access to a Router without using a password. The details of the procedure vary between router models, but always include the following basic steps. An administrator (or an attacker) can simply connect a terminal or computer to the console port and follow the procedure below

  Step 1 Configure the router to boot up without reading the configuration memory (NVRAM). This is sometimes called the test system mode.

  Step 2 Reboot the system.
  Step 3 Access enable mode (which can be done without a password if you are in test system mode).
  Step 4 View or change the password, or erase the configuration.
  Step 5 Reconfigure the router to boot up and read the NVRAM as it normally does.
  Step 6 Reboot the system."

- **Router Network Traffic and the Loopback Interface**

  The primary job of a router is forwarding traffic between networks, but routers also generate some network traffic. Routers and other network devices communicate using various management protocols, such as routing protocols, SNMP, NTP, and TFTP. When the router initiates a network connection, that connection must have some source address; typically a router will select a source address from one of the addresses bound to one of its network interfaces. This can be problematic in several ways, mainly because the source address for some services can vary.

  To create a loopback interface, simply assign it an IP address. For a border router, the loopback's address usually should be in the range of the internal or DMZ network, not the external network. Note that the loopback address cannot be the same as the address of any other interface, nor can it be part of the same network as any other interface.

  In general, router network services that can be bound to the loopback interface should be. Commands to set source interface bindings are given with the discussion of each service in the rest of the guide.

- **Remote Access**

  This document will discuss five connection schemes which can be used for router administration.

  1. No Remote – administration is performed on the console only.
  2. Remote Internal only with AAA – administration can be performed on the router from a trusted internal network only, and AAA is used for access control.
  3. Remote Internal only – administration can be performed on the router from the internal network only.
  4. Remote External with AAA – administration can be performed with both internal and external connections and uses AAA for access control.

5. Remote External – administration can be performed with both internal and external connections.

The five regimes listed above are listed in the order that best protects the router and allows for accounting of router activities.

- **Authentication, Authorization, and Accounting (AAA)**

  This is the router's access control facility for controlling access, privileges, and logging of user activities on a router. Authentication is the mechanism for identifying users before allowing access to a network component. Authorization is the method used to describe what a user has the right to do once he has authenticated to the router. Accounting is the component that allows for logging and tracking of user and traffic activities on the router which can be used later for resource tracking or trouble shooting. Section 4.6 contains details on configuring AAA in an example network.

Router Network Service Security

Routers support a large number of network services at layers 2, 3, 4, and 7. Some of these services can be restricted or disabled, improving security without degrading the operational use of the router. Some of these services are application layer protocols that allow users and host processes to connect to the router. Others are automatic processes and settings intended to support legacy or specialized configurations but which are detrimental to security. As stated in Section 3, general security practice for routers should be to support only traffic and protocols the network needs; most of the services listed below are not needed.

Turning off a network service on the router itself does not prevent it from supporting a network where that protocol is employed. For example, a router may support a network where the bootp protocol is employed, but some other host is acting as the bootp server. In this case, the router's bootp server should be disabled.

Access Control Lists, Filtering, and Rate Limiting

IOS uses access lists to separate data traffic into that which it will process (permitted packets) and that which it will not process (denied packets). Secure configuration of Routers makes very heavy use of access lists, for restricting access to services on the router itself, and for filtering traffic passing through the router, and for other packet identification tasks.

Access lists on routers provide packet selection and filtering capabilities. An access list consists of one or more rules. For IP traffic, there are two types of access lists available: standard and extended. Standard access lists only allow source IP address filtering.

Extended access lists can permit or deny packets based on their protocols, source or destination IP addresses, source or destination TCP/UDP ports, or ICMP or IGMP message types. Extended access lists also support selective logging. Both standard and extended IP access lists can be applied to router interfaces, vty lines (for remote access), IPSec, routing protocols, and many router features. Only standard IP access lists can be applied to SNMP.

- **Filtering Traffic Through the Router**

  The following examples illustrate methods to protect the router or the internal network from attacks.

  - **IP Address Spoof Protection**

    The filtering recommendations in this sub-section are applicable to border routers, and most interior routers. With backbone routers, it is not always feasible to define 'inbound' or 'outbound'.

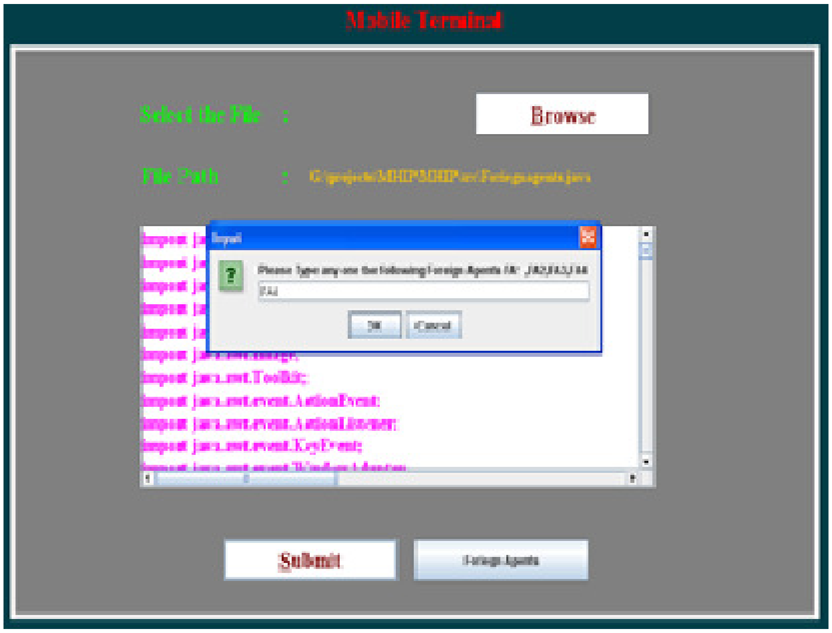
  - **Inbound Traffic**

Do not allow any inbound IP packet that contains an IP address from the internal network (e.g., 14.2.6.0), any local host address (127.0.0.0/8), the link-local DHCP default network (169.254.0.0/16), the documentation/test network (192.0.2.0/24), or any reserved private addresses (refer to RFC 1918) in the source field. Also, if your network does not need multicast traffic, then block the IP multicast address range (224.0.0.0/4).

- **Outbound Traffic**
  Do not allow any outbound IP packet that contains an IP address other than a valid internal one in the source field. Apply this access list to the internal interface of the router.

5. RESULTS AND DISCUSSIONS

An efficient analysis has been done on comparing various Mobile IP protocols and from the results of those analysis, it has been observed that MHMIP has taken minimum bandwidth, minimum time delay when compared with MIP and DHMIP.



Mobile Terminal

Select the File :

File Path : [illegible]

Input

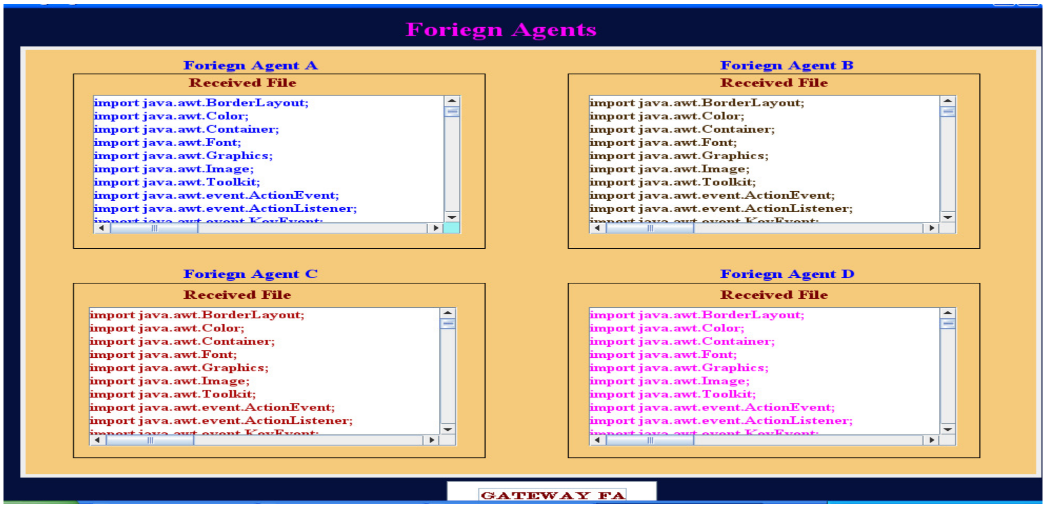
Please Type any one the following Foreign Agents FA1 ,FA2,FA3,FA4

FA1

```
import java.awt.Image;
import java.awt.Toolkit;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.event.KeyEvent;
```

FIGURE 5: Scenario of selecting a file for flooding to foreign agent from Home Agent.

Figure 5 illustrates the demonstration of browsing the file for transmitting to foreign agent.



Foriegn Agents

Foriegn Agent A

Received File

```
import java.awt.BorderLayout;
import java.awt.Color;
import java.awt.Container;
import java.awt.Font;
import java.awt.Graphics;
import java.awt.Image;
import java.awt.Toolkit;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.event.KeyEvent;
```

Foriegn Agent B

Received File

```
import java.awt.BorderLayout;
import java.awt.Color;
import java.awt.Container;
import java.awt.Font;
import java.awt.Graphics;
import java.awt.Image;
import java.awt.Toolkit;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.event.KeyEvent;
```

Foriegn Agent C

Received File

```
import java.awt.BorderLayout;
import java.awt.Color;
import java.awt.Container;
import java.awt.Font;
import java.awt.Graphics;
import java.awt.Image;
import java.awt.Toolkit;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.event.KeyEvent;
```

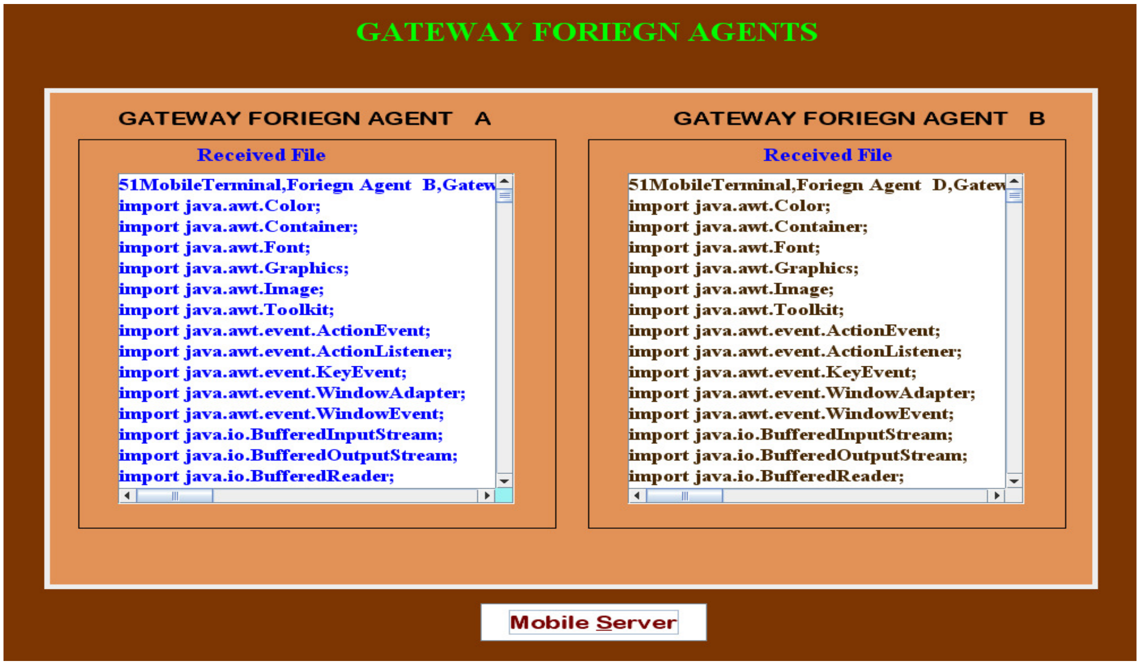
Foriegn Agent D

Received File

```
import java.awt.BorderLayout;
import java.awt.Color;
import java.awt.Container;
import java.awt.Font;
import java.awt.Graphics;
import java.awt.Image;
import java.awt.Toolkit;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.event.KeyEvent;
```

FIGURE 6: Data received by different foreign agents.

Figure 6 illustrates the phenomena of Information Dissemination to various Foreign Agents.

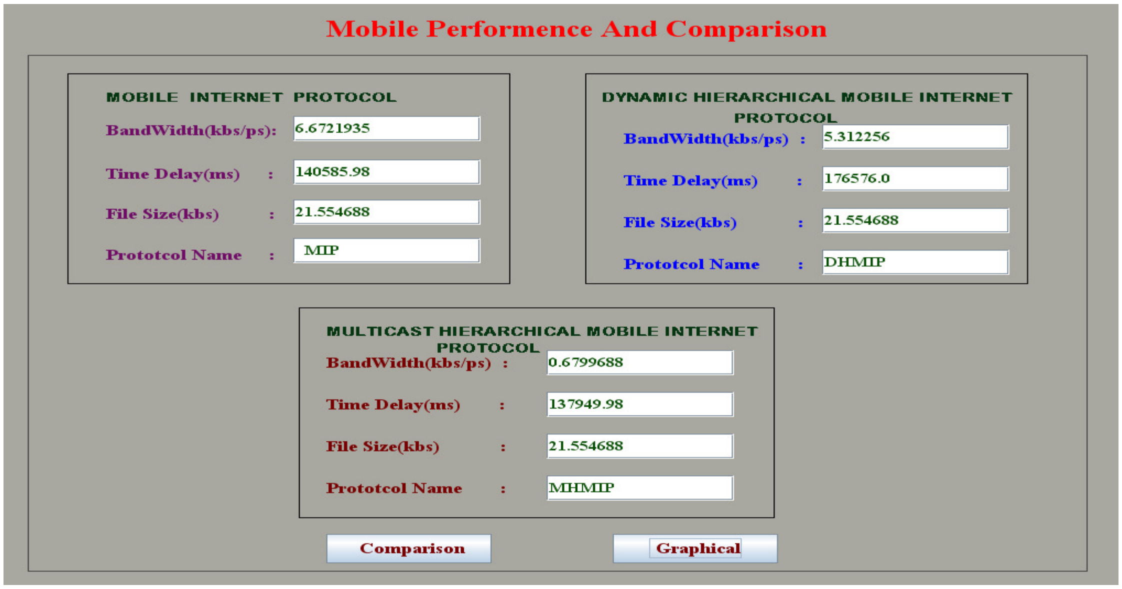


```
51MobileTerminal,Foriegn Agent  B,Gatew
import java.awt.Color;
import java.awt.Container;
import java.awt.Font;
import java.awt.Graphics;
import java.awt.Image;
import java.awt.Toolkit;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.event.KeyEvent;
import java.awt.event.WindowAdapter;
import java.awt.event.WindowEvent;
import java.io.BufferedInputStream;
import java.io.BufferedOutputStream;
import java.io.BufferedReader;
```

```
51MobileTerminal,Foriegn Agent  D,Gatew
import java.awt.Color;
import java.awt.Container;
import java.awt.Font;
import java.awt.Graphics;
import java.awt.Image;
import java.awt.Toolkit;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.event.KeyEvent;
import java.awt.event.WindowAdapter;
import java.awt.event.WindowEvent;
import java.io.BufferedInputStream;
import java.io.BufferedOutputStream;
import java.io.BufferedReader;
```

FIGURE 7: Scenario describing the data reception by two distinct Gateway Foreign Agents.

Figure 7 demonstrates the efffective reception of different Gateway Foreign Agents.



MOBILE INTERNET PROTOCOL

BandWidth(kbs/ps):	6.6721935
Time Delay(ms) :	140585.98
File Size(kbs) :	21.554688
Prototcol Name :	MIP

DYNAMIC HIERARCHICAL MOBILE INTERNET PROTOCOL

BandWidth(kbs/ps) :	5.312256
Time Delay(ms) :	176576.0
File Size(kbs) :	21.554688
Prototcol Name :	DHMIP

MULTICAST HIERARCHICAL MOBILE INTERNET PROTOCOL

BandWidth(kbs/ps) :	0.6799688
Time Delay(ms) :	137949.98
File Size(kbs) :	21.554688
Prototcol Name :	MHMIP

FIGURE 8: Comaprison of various Mobile IP protocols.

Figure 8 shows comparison of various mobile IP protocols by considering multiple parameters like Bandwidth, Time Delay.

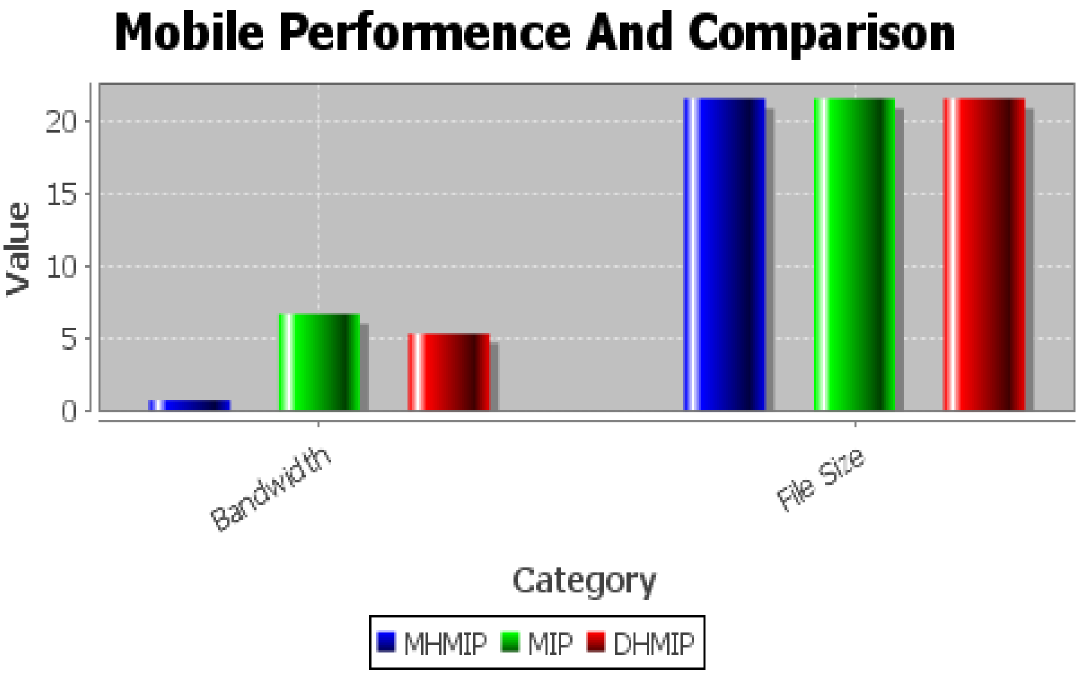


FIGURE 10: Histogram for Mobile IP comparisons.

Figure 10 compares the Mobile IP protocols In two categories. One w.r.t Bandwidth and other w.r.t.File Size.

6. CONCLUSION

In this work, an analytical model is proposed, which evaluates the mean handoff delay per call and the mean bandwidth per call of three mobility management approaches: MIP, DHMIP, and MHMIP. Numerical results show that the MHMIP mobility approach[8],[9],[10] ,[11] compares very favorably with the previously considered mobility approaches.

More specifically, our analysis gives in almost all cases a lower mean handoff delay per call and a mean bandwidth per call than those offered by the DHMIP and MIP approaches. It also shows the robustness of the MHMIP approach in the sense that for critical scenario corresponding to the extreme situation where all handoff events are localized at the multicast group borders, this approach essentially yields to-

1) A lower mean bandwidth per call than the DHMIP and MIP approaches;
2) A lower mean handoff delay per call than that offered by the MIP approach;
3) A lower mean handoff delay than that offered by the DHMIP except in case of frequent inter-GFAs handoffs with a network configuration having a high number of links involved in MHMIP path reestablishment.

Since we expect a diversity of multimedia applications for future IP mobile networks, we recommend using the MHMIP approach in networks parts carrying delay sensitive and/or low mean bandwidth consumption type of applications and this according to the mobility type

Future Enhancement

- It entails more configuration and administration to maintain usability.
- Not being fully visible on the Internet can cause some difficulty in connecting to certain services, such as streaming audio/video, chat/instant messaging programs, or some secure Web sites.

- Maintaining most computers on a private network, visible to the public Internet helps maintain a highly secure environment. While at the same time keeping them connected to the public Internet is the challenge.

7. REFERENCES

[1] C.E. Perkins, “IP Mobility Support for IPv4,” *IETF RFC 3344, Aug.2002.*

[2] D. Johnson, C. Perkins, and J. Arkko, “Mobility Support in IPv6,” *IETF RFC 3775, June 2004.*

[3] R. Cancers and V.N. Padmanabhan, “Fast and Scalable Handoffs for Wireless Internetworks*,” Proc. ACM MobiCom, pp. 56-66, 1996.*

[4] C. Castelluccia, “Extending Mobile IP with Adaptative Individual Paging: A Performance Analysis,” *Proc. Fifth IEEE Symp. Computers and Comm., pp. 113-118, July 2000.*

[5] H. Soliman, C. Castelluccia, K. El-Malki, and L. Bellier, “Hierarchical Mobile IPv6 Mobility Management HMIPv6,” *IETF RFC 4140, Aug. 2005.*

[6] E. Fogelstroem, A. Jonsson, and C. Perkins, “Mobile IPv4 Regional Registration,” *IETF RFC 4857, June 2007.*

[7] H. Omar, T. Saadawi, and M. Lee, “Supporting Reduced Location Management Overhead and Fault Tolerance in Mobile IP Systems,” *Proc. IEEE Symp. Computers and Comm., pp. 347-353, 1999.*

[8] S. Pack, T. You, and Y. Choi, “Performance Analysis of Robust Hierarchical Mobile IPv6 for Fault-Tolerance Mobile Services,” *IEICE Trans. Comm., vol. E87-B, no. 5, pp. 1158-1165, May 2004.*

[9] J. Xie and I.F. Akyildiz, “A Novel Distributed Dynamic Location Management Scheme for Minimizing Signaling Costs in Mobile IP,” *IEEE Trans. Mobile Computing, vol. 1, no. 3, pp. 163-175, July 2002*.

[10] Song, J. Huang, R. Feng, and J. Song, “A Distributed Dynamic Mobility Management Strategy for Mobile IP Networks*,” Proc Sixth Int’l Conf. ITS Telecomm. 2006.*

[11] Nadjia kara , “Mobility Management Approaches for Mobile IP Networks : Performance Comparison and Use Recommendations,” *IEEE Transactions On Mobile Computing , VOL 8 , NO ,10,OCTOBER 2009.*