Enhanced Mobile IP Protocol

Baher Esmat, Mikhail N. Mikhail, Amr El Kadi

Department of Computer Science, The American University in Cairo,
Cairo, Egypt
{besmat, mikhail, elkadi}@aucegypt.edu

Abstract. One of the most recent Internet challenges is to support transparent movement of people along with their computers, data and most of all applications. Therefore, Mobile IP has been developed to provide Internet mobility services.

This paper aims at enhancing the IETF Mobile IP standard. The model developed in this paper suggests a new caching mechanism, which is based on the Mobile Information Server (MIS). Actually, the MIS is designed to be part of the border router of any network that supports mobility services. Moreover, the paper suggests a *peering technique* by which information about mobiles hosts could be shared among different MISs. All the design issues including model components as well as mechanisms for caching and peering are described in details.

The simulation results show that the proposed design provides improved performance and better bandwidth utilization. The suggested architecture provides other qualitative advantages such as scalability and transparency.

1 Introduction

Mobile computing has assumed an increasing importance in recent years, and will pervade future distributed computing system. Although network standards were not designed with the capability of supporting the demand of mobility, the need is that they should grant the users a continuous access to their data, irrespective of their point of attachment. Mobile computing is still restricted by many obstacles [1].

As a mater of fact, the current IP version 4 [2] makes an implicit assumption that the point at which a computer is attached to the Internet is fixed, and its IP address identifies the network to which it belongs. The challenge is to develop a protocol, which allows computers to roam freely around the Internet and communicate with other stationary or mobile nodes, without major changes in the existing TCP/IP stack.

The mobility problem within the Internet is mainly concerned with the IP layer, since this layer handles all aspects related to addressing as well as routing. To illustrate this point [3], if a computer moves to another network, and retains its original IP address, this address will not reflect its new location, and consequently, all routed packets to this host will be lost. In the other hand if the mobile host gets a new address when migrating to another network, the IP address changes, the transport layer (i.e. TCP) connection identifier changes too [4], and hence all connections with this mobile host through its old address are going to be lost. Therefore, if the mobile

C.G. Omidyar (Ed.): MWCN 2000, LNCS 1818, pp. 158-173, 2000.

host moves without changing its address, it will lose routing, and if it gets new address, it will lose connections.

This paper is organized as follows. The next section presents the Mobile IP standard protocol. Section 3 describes the contribution of this work. An overview for the proposed design is going to be illustrated in section 4. In section 5, all the model components will be identified and discussed in detail. Next, section 6 presents all the simulation details as well as the results. Finally, section 7 concludes the paper.

2 Mobile IP

During the last few years, many contributions have been offered by different entities and groups, towards designing a model for a mobility supports Internet. The proposed models are different in terms of their components and methodology, but they are all aiming at keeping the mobile hosts communicating transparently via the Internet. Proposals from Columbia University [5,6], Sony [7,8], the Loose Source Routing(LSR) Proposal [9] as well as the Internet Engineering Task Force (IETF) Mobile IP working group [10,11,12], are the most outstanding models,

Since this work is an extension to the IETF Mobile IP standard, it is worth to focus on the operation of this standard protocol. First of all, it should be mentioned that the Mobile IP working group has been in charge of standardizing Mobile IP. Recently, the Mobile IP has become a standard, after passing through two stages [13]. The first one in which the base protocol was developed, with the objective that mobile nodes can roam transparently around the Internet, with no modifications whatsoever to other stationary nodes. The second phase has answered many open questions regarding the best route that the packet may take to reach a mobile node. This has been known by the *route optimization* problem.

2.1 Mobile IP Operation

According to [12], the IETF Mobile IP architecture defines special entities called the Home Agent (HA) and the Foreign Agent (FA), both cooperate to allow a Mobile Host (MH) to move without changing its IP address. Each MH is associated with a unique *home network* as indicated by its permanent IP address. Normal IP routing always delivers packets meant for the MH to this network. When an MH moves to a *foreign network*, the HA is responsible for intercepting and forwarding packets destined to the MH to anew address which is called the *care-of address*. The MH uses a special registration protocol to keep its HA informed with its new location.

Whenever a MH moves from its home network to a foreign network, or from one foreign network to another, it looks for a FA on the new network in order to obtain its new care-of address. In order for the MH to be able to work with this new address, it must go through a registration procedure via both, the foreign agent and the home agent. After a successful registration, packets arriving for the MH on its home network are *encapsulated* by its HA and forwarded to its FA. Encapsulation refers to the process of enclosing the original datagram as data inside another datagram with new IP header [14]. The source and destination addresses in the new header correspond to the HA and FA respectively. Upon receiving the encapsulated datagram, the FA strips off the new header and forwards the original one to the MH. This process at the FA end is known as *decapsulation*. If on the other hand, the mobile node needs to send a packet to any destination, the packet will be routed to its destination with the normal fashion without using either the home agent or the foreign agent. The figure below illustrates the operation of the mobile IP routing.

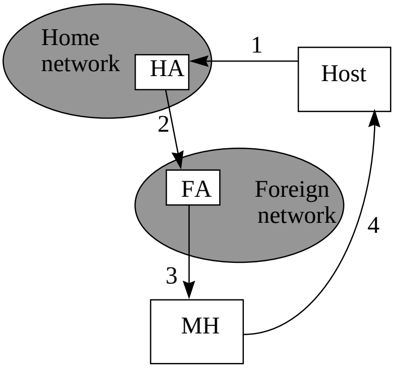

Fig. 1.

2.2 Route Optimization

As depicted in Figure 1, the IETF scheme has a major routing problem. Any packet which means to reach a mobile host, is directed first to the appropriate home agent, then to the foreign agent and finally received by the mobile host. This means that the above scheme does not allow the source host to reach the mobile host directly without passing by its home network. This problem is known as the *triangle routing problem*, and in order to solve it, a technique for route optimization is needed.

Route optimization [15] means solvingthe problem of triangle routing, by allowing for each host to maintain a binding cache for a mobile host wherever it is. When sending a packet to a mobile node, if the sender has a binding cache containing the care-of address of that mobile node, it will deliver the packet directly toward the mobile node, without the need to pass through the home network.

2.3 Mobile IP Problems

Although the IETF Mobile IP working group has enhanced its base protocol and provided a solution for route optimization, the protocol seems to have some deficiencies. From a performance point of view, the protocol intended to optimize the routing process, but realistically the routing has not been thoroughly optimized. For example, consider two computers connected to the same network, computer A and computer B. If the first one wants to reach a certain mobile host, it must go through the home network, at least for the first few packets, before reaching the mobile node.

Then, it caches the mobile node’s address, so that it could reach it directly for the rest of the packets. Afterwards, if computer B needs to access the same mobile host, it must go through the same procedure again, as it does not have any cached information regarding the mobile host. The same process applies for any host on this network when trying to contact this specific mobile host. This implies that the first few packets directed from any host on a certain network toward a mobile host, are inefficiently routed through the home agent.

Another problem exist that relate to the fact that current implementation of Internet Protocol version 4 (IPv4) [2], which is currently running on all the Internet hosts worldwide, do not allow for any such mobile information to be cached. This means that in order for such a routing optimization to be achieved, every single host on the Internet must have its IP software modified.

2.4 Mobility Support in IPv6

IPv6 [16] has been developed with some sophisticated features that have not been supported by the current Internet Protocol (IPv4). IPv6 sustains major requirements concerning addressing, routing, security and mobility.

Mobility support in IPv6 [17] follows the same methodology that has been developed for IPv4. The same terminology is still valid as for home agents, mobile hosts, home and foreign networks, as well as encapsulation or tunneling. However, the term foreign agent is not of any more use. The reason is that any IPv6 is able to configure its own IP address automatically, as well as to choose its default gateway. This is accomplished via the Stateless Address Autoconfiguration [18] and the Neighbor Discovery protocols [19]. Therefore, it is quite straightforward that whenever an IPv6 mobile host migrates to any foreign network, it could easily detect the change in network connectivity, and configure its IP address automatically. Moreover, mobility within IPv6 borrows heavily from the route optimization specified for IPv4, which was described earlier in a previous section. By default, all IPv6 hosts are able to cache mobility information, via authenticated binding update messages. It is only the mobile host that has the authority to send binding updates to any other correspondent nodes.

Although people have been waiting for IPv6 to become the Internet standard [20], and many vendors have implemented IPv6 in their products for testing purposes, IPv6 is still under development. It is quite conceivable that the Mobile IP deployment will coincide with the standardization and implementation of IPv6 [21].

3 The Proposed Scheme

This work is intended to enhance the Mobile IP standard that has been developed by the IETF Mobile IP working group. Most of the Mobile IP protocol specifications are used in the development of this work.

This paper suggests a method for caching mobile information, different from that developed by the IETF working group. The proposed model implies suggests a *central cache engine* within each network, or a cluster of networks, responsible for caching mobile information. Moreover, all the functions performed by the HA's and

FA's, regarding encapsulation, decapsulation, registration and authentication, could be part of this central cache engine.

In addition, it is recommended for any network, or class of networks, connected to the Internet, to use its boarder router as a Mobile Information Server (MIS) which handles all caching as well as mobility services. As a matter of fact, designing a central caching mechanism does not necessarily imply that this should be part of the network router. Instead, building such a cache server, along with other mobility functions, can take place in any workstation in the network. However, this design is recommended for more than one reason. First, the proposed model manipulates the cached mobile information as part of the routing information that already exists in the routers, so that any cache entries are considered part of the routing table. . This new model allows for MISs to work in a peering fashion, by which mobility information can be exchanged. In addition, the model developed here aims at being transparent for the IP version used, whether it is IPv4 or IPv6. Eventually, the paper delivers a new caching mechanism, as part of the Mobile IP protocol. A complete practical architecture, with a simulation of all components and their functionality is delivered. Efficiency, scalability and transparency are the main value-added features in this new scheme, taking into account all security policies which have been addressed through the base Mobile IP model.

4 Design Overview

The proposed design is based on a centralized caching architecture. For a specific network, there is a cache server responsible for any mobile information concerning any node belonging to that network, or even it could cache other information regarding any external mobile node. In addition to caching, this server can handle all the functions of the home agent as well as the foreign agent, such as registration, authentication and tunneling procedures.

5 Model Components and Description

Figure 2 depicts the main components of the new suggested design. The figure illustrates four different networks (any networks that are members o the Internet for demonstration purpose) in order to describe the various functions and scenarios of this model.

5.1 Mobile Information Server (MIS)

The new model defines a new term called MIS. The MIS is suggested to be implemented in the border router. Border routers are basically responsible for routing the traffic between a group of networks and the outside world of the Internet. Moreover, In addition, border routers are now made responsible for other mobile services that were part of the home agent and the foreign agent in the Mobile IP scheme. Also, the new caching mechanism is designed to take place on these routers.

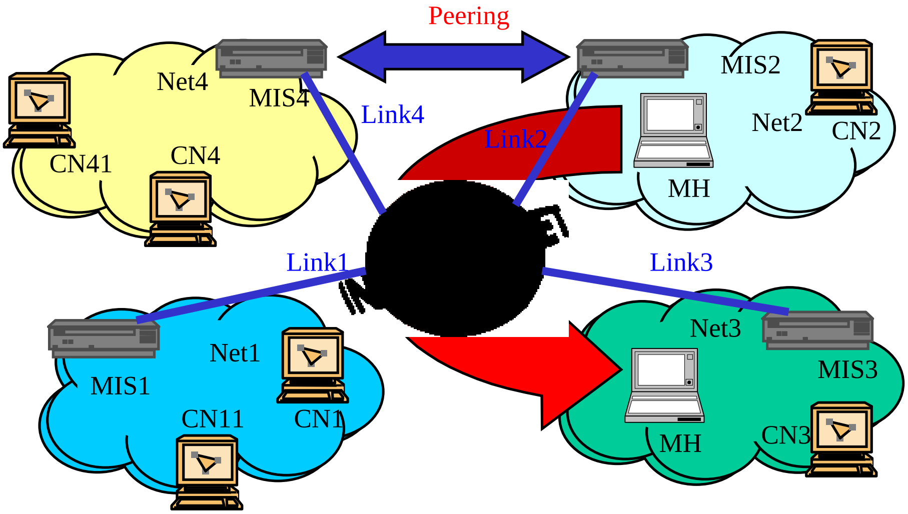

Fig. 2. New proposed model

Therefore, and because any of these routers handles a lot of other new services, it is going to be called in the context of this paper the MIS.

In addition to routing and caching functions, any MIS can be configured to work as a peer to another MIS. As a result of peering, MISs can exchange mobile information by the same concept of exchanging routing updates. Moreover, the MIS should include a table that encompasses all IP addresses of visiting mobile hosts, along with their Media Access Control (MAC) addresses, in order to deliver the packets to the proper destination after decapsulation. This table is called the *visitor list.*

5.2 Caching

It has been mentioned earlier that the MISs are responsible for caching mobile information. Actually, the cache entries are considered normal routing entries, with some extra fields for mobility.

Basically, the cache entry is suggested to include the following fields:

M O C P	*old IP address*	*next hop*	*new IP address*

In this entry, the first four fields are flags which indicate the type of this routing entry. The following table describes briefly each of those flags.

The next two fields are similar to any ordinary routing information, they represent a destination IP address, as well as the next router in the way to reach this destination. In this case, the destination IP address is the old IP address of the mobile host. Finally, there is another field that indicates the new location of the mobile node.

Flag	Routing Entry
M	Set to 1 for all mobile routing entries
O	Set to 1 for mobile hosts controlled by the MIS
C	Set to 1 for mobile entries cached at the MIS as a result of cache update messages
P	Set to 1 for mobile entries cached at the MIS as a result of peering

Table 1. Mobile routing entry

5.3 MIS Peering

The MIS methodology provides another value-added service that is not in the Mobile IP protocol. This model allows for different MISs to share mobility information. In this case, the MISs seem to be working as peers, and the process of exchanging mobility information is called peering. As a matter of fact, the MIS in order to export any information regarding certain mobile host to another MIS, it should be the owner of this mobile host. In other words, the routing entry for this specific mobile node must have its *O* flag set to 1. When this routing entry gets to the peer MIS, it will have the *P* flag set to 1, in order to indicate that this information has come as a result of peering. Moreover, each MIS has in its Mobile IP configuration a list in which other MIS peers are defined. This means that MISs work as peers to each other based on some pre-defined routing configuration.

5.4 Mobility Scenarios

Reference to Figure 2, this section describes a scenario in which a mobile host *MH* migrates from its home network *Net2* to a foreign network *Net3*. The scenario shows how other correspondent nodes can reach *MH* while it is away from *Net2*, and even when it gets back.

1. *MH* migrates to *Net3* and gets a care-of address, which is actually the IP address of *MIS3*. Then, it sends a registration request to *MIS3*, which will relay this request to *MIS2*.
2. *MIS2* accepts the registration after checking the authentication extension included in the request. Hence, a registration reply is sent to *MIS3*, which in turn will inform *MH* with its status.
3. From now on and since the registration request has been accepted, *MH* becomes reachable via *MIS3*.
4. *CN1* wants to reach *MH*. So, it will start sending packets toward *Net2*. The packets arrive at *MIS2*, which could realize that they are destined to *MH*. *MIS2* contains a cache entry for the new location of *MH*. Actually, the *O* flag for this cache entry must be set to 1 because *MH* is owned by *MIS2*.
5. Right after the encapsulation, *MIS2* recognizes that *CN1* does not perceive that *MH* had moved. Therefore, *MIS2* sends *CN1* a cache update message. This cache update will be intercepted by *MIS1*, which in turn will update its routing table. In

this case, the cache entry at *MIS1* will have its *C* flag set to 1 since it has been generated through a cache update message.

6. *MIS3* receives encapsulated packets, and decapsulates them to *MH*, after obtaining its MAC address from the visitor list.
7. All packets from *MH* in their way back to *CN1*, are always routed directly to *Net1*, without necessarily passing by *Net2*.
8. *MH* decides to return to *Net2*. Consequently, it will ask for registration at *MIS2*.
9. If *MIS2* accepts this registration request, *MH* starts acting normally without any The next two fields are similar to any ordinary routing information, they represent a destination IP address, as well as the next router in the way to reach this destination. In this case, the destination IP address is the old IP address of the mobile host. Finally, there is another field that indicates the new location of the mobile node. mobility services.
10. *MIS2* sends a cache delete message to *MIS3* in order to release any routing information regarding *MH*.
11. *CN1* may try again to contact *MH*.
12. Packets are going to be tunneled through *MIS1* and directed to *MIS3*. From decapsulation, *MIS3* will discover that the destination address is not any more in its mobile visitor list.
13. *MIS3* sends a cache delete message to *MIS1*, which consequently is going to route the packets without any kind of encapsulation, through the ordinary route to *MIS2*.

In addition, Figure 2 depicts another correspondent node *CN11* that may need to access *MH* *net3*. Unlike the standard Mobile IP, all the packets from *CN11* toward *MH* will be routed directly to *MIS3*, since *MIS1* has a cache entry for *MH*.

Another difference between this new architecture and the Mobile IP one is the peering mechanism. Again from Figure 2, *MIS2* and *MIS4* work as peers to each other. Hence, *MIS4* will be notified that *MH* had moved. Therefore, it is possible that *CN4* can contact *MH* directly through a tunnel from *MIS4* to *MIS3*.

6 Simulation

Throughout the development of this work, simulation has been used to compare the Mobile IP standard protocol and the new proposed model. The main prominent difference between the two models is the caching methodology, by which the route optimization is verified, and the whole routing performance is induced. Actually, the influence of the caching mechanism can be evident in the total amount of traffic through the whole network, as well as the delay associated with packets while carried from source to destination nodes.

Therefore, this simulation has focused on the traffic as a main point for discrimination. All the quantitative results shown out of the two comparable models are in terms of packet delay as well as bandwidth consumption.

6.1 COMNET III

COMNET III [22] is a performance analysis tool which simulates computer and communication networks. It can be used to model both circuit switching and packet switching networks. In addition, it can accommodate different topologies of WANs and LANs in which many standards and protocols are supported, such as Ethernet, Token Ring, PPP, X.25, Frame Relay and ATM.

Regarding this work, COMNET III version 1.2 for Windows has been used to implement a number of models which differentiate between the standard Mobile IP architecture proposed by the IETF, and the model suggested in this paper. The simulated model presents all the issues described previously, concerning registration, tunneling, caching, route optimization as well as border routers which are known here by MISs. The networks described in the simulation were represented by Ethernet connections for LANs, Point-to-Point (PPP) links for WANs and processing nodes to simulate computers and workstations. All the networks are inter-connected using routers, in which user-defined routing tables are used to simulate the model. In addition, sending and receiving messages among the various nodes simulates the traffic. Finally, the model is verified and executed, and the results can be shown in graphs, or presented through reports of text format.

6.2 Network Components

This section provides a description for the network components simulated by COMNET III.

Processing node: All the simulated models use the processing node component to describe generic Internet hosts which are considered the endpoints of any Internet traffic.

Router node: Routers have been configured with *500 Mbps* bus rate, *50000 packet per second* as a processing rate, and the input and output delays are ignored. Moreover, all the models developed in this simulation have standardized on the static routing protocol, since using any dynamic protocols will make no difference to the results.

LAN connectivity: The IEEE 802.3 Ethernet standard is used.
WAN link: Point-to-Point Protocol (PPP) is used for all communication links with a bandwidth of *1.536 Mbps.*

Message source: Message sources are used to represent specific traffic based on the TCP/IP Protocol. A payload of *1460 bytes* and header of *40 bytes* is used for all the messages generated throughout the simulation. In addition, the message size may be changed based on the type of the message itself.

6.3 Simulated Models

This section describes a number of network architectures that have been simulated throughout this work. Generally, all the simulated models present the differences between the Mobile IP standard, and the new proposed scheme. The simulated models reflect the scenario that has been previously illustrated in Figure 2, in which a mobile host is migrating from one network to another whilst a correspondent node is trying to reach it. The models are simulated in simple as well as complicated structures. Simple models aim at presenting a preliminary overview for the Mobile IP operation, focusing on the main mechanisms and services for each architecture. On the other side, other more advanced designs are required in an attempt to simulate something close to reality. Such composite models include many nodes, routers and message sources that load the network with much more traffic.

6.3.1 Simple Models

This section illustrates the simplest cases for any Mobile IP architecture, where the simulated models consist of a single mobile node that migrates from its home network to another foreign one. Besides, there is a correspondent node belonging to another third network and it wants to get access to the mobile node. This scenario is shown for both the Mobile IP standard with route optimization support, and the new architecture developed within this paper. The most outstanding difference between the two schemes is the caching mechanism, as well as the fact that the border router within the new model is responsible for all mobile services.

Moreover, the simulation shows all the procedures defined by the Mobile IP standard. Such procedures include the registration request messages, registration acceptance, encapsulation as well as decapsulation. According to [3], the size of the registration message is *24 bytes* plus variable length extensions required for authentication. Likewise, the registration-reply is *16 bytes* beside those needed for authentication. As per our simulation, the registration messages are *48 bytes,* whereas the registration-reply messages are *40 bytes,* since extra bytes are used to indicate the variable length authentication extensions.

6.3.2 Composite Models

Similar to the simple models, in which the new proposed design has been compared to the Mobile IP standard, the composite models perform the same analogy accompanied by adding more components to the simulated models. In addition, the generated traffic is much more than that generated for the simple models.

Actually, the composite models contain five networks, two mobile hosts as well as many other correspondent nodes. Moreover, the new model simulates the peeing methodology that has been developed throughout this work.

6.4 Results

This section presents all the results that have been collected as an output from executing the simulated models. It will be noticed that all the models have been simulated over a simulation time of *60 seconds*.

As per the simple models, the point of discrimination between the two simulated schemes is the delay for the packets running from the source network to the foreign network where the mobile node is located. On the other hand, the evaluation of the composite models is based more the bandwidth consumption.

6.4.1 Simulation Results for Simple Models

As for the Mobile IP route optimization standard and as illustrated in Figure 2, when *CN1* talks to *MH*, the first few packets are going to be routed via *Net2*, then encapsulated toward *Net3*. The delay of the *CN1-Msg1* packets as well as that of the encapsulated packets *HA-Encap* are illustrated in Figure 3(a) and 3(b) respectively. The total average delay is *161.018 msec*.

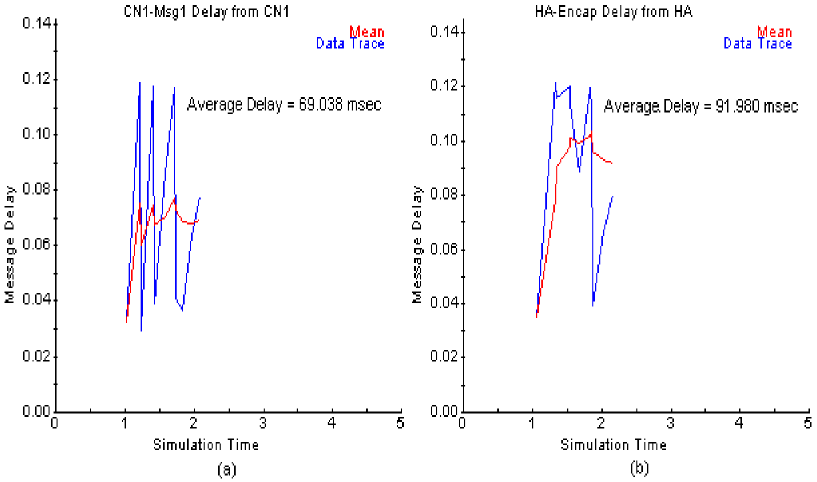

Fig. 3. Packet delay for *CN1-Msg1* and *HA-Encap*

But afterwards, *CN1* should get its cache updated and therefore packets are going to reach *MH* directly (CN1-Msg2) with an average packet delay of *94.544 msec*, as shown in Figure 4. The same scenario is applied for *CN11* when trying to access *MH*, causing almost the same results.

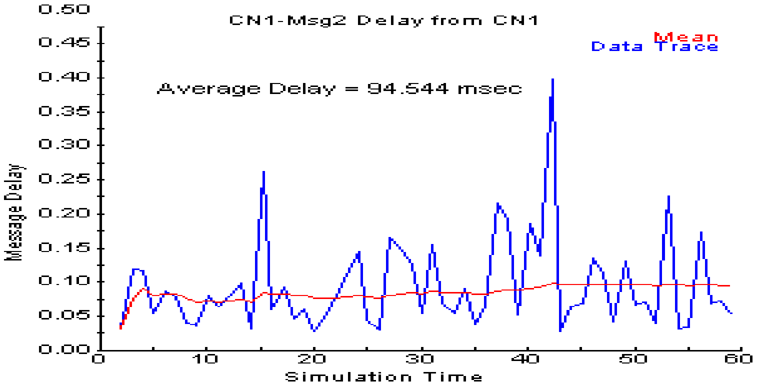

Fig. 4. Packet delay for *CN1-Msg1*

As formerly shown in Figure 2, *MIS1* is considered a central cache engine for *Net1*, responsible for any mobile information. Unlike the route optimization model, *CN11* may reach *MH* directly since the *MH* new care-of address is cached within *MIS1*. Therefore, the overall delay will be less than that of the last illustrated model. Figure 5 shows that in the new model, the average packet delay from *CN11* to *MH* is *79.681 msec*.

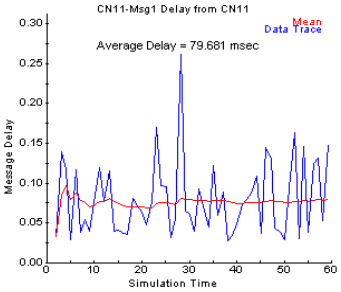

Fig. 5. Delay from *CN11* to *MH* in the new model

Although the difference in packet delays may be significant in such simple architectures, this might not be the case in real networks that carry millions of transferred packets per second. However, those models were basically simulated in order to prove that the proposed model has a quantitative advantage over the other models, even if this advantage is a minor issue in real applications. More importantly, this difference could be more significant from another perspective. For instance, if there is a certain application which ought the mobile node to stay in contact with a number of remote nodes at some other network, so that there are many nodes like *CN1* and *CN11* belong to the same network, and try to reach the same mobile host. In this case, it is better from a scalability point of view to have a central caching rather than storing the same information on many different machines.

6.4.2 Simulation Results for Composite Models

It has been stated before that for the composite models, the evaluation criteria is according to the bandwidth utilization. In fact, both composite models have been simulated with two networks working as home networks for two different mobile hosts, and each network has a single link to the Internet. The bandwidth utilization of each link is illustrated in this section.

Before presenting the results, it should be mentioned that COMNET III deals with any communication connection as a full-duplex link, in which the input bandwidth is independent of the output bandwidth. Therefore, it will be noticed that each link is represented by two graphs (a) and (b).

Assuming that the Internet link for the first home network is *Link A*, and for the other network is *Link B*. Figures 6 and 7 depict the channel utilization of *link A* in case the standard IP model and in the case of our new model respectively. Furthermore, Table 2 summarizes the results indicating that the new model is better than the standard one in bandwidth consumption.

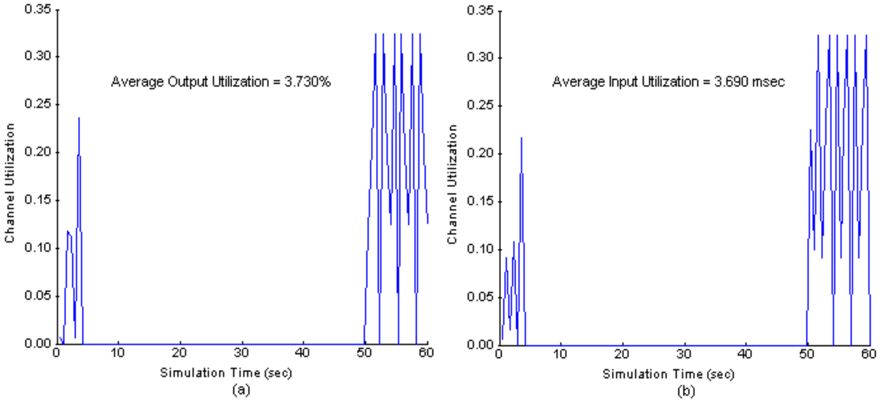

Fig. 6. Bandwidth utilization for *Link A* in the Mobile IP standard

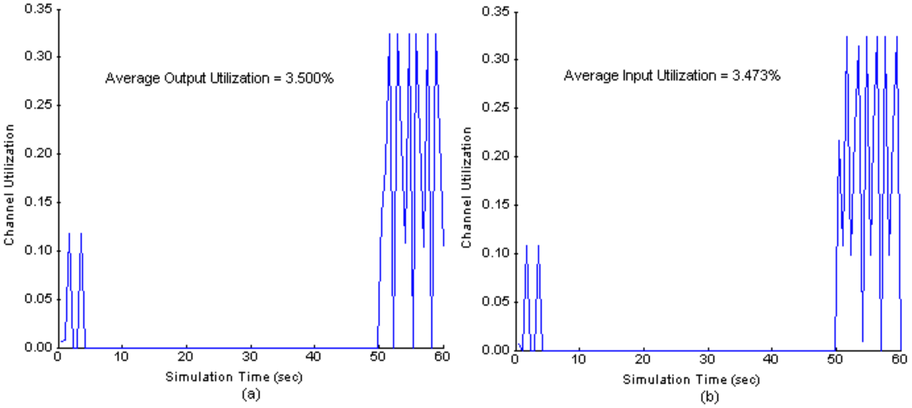

Fig. 7. Bandwidth utilization for *Link A* in the new model

Model	Link A		Total	Improvement
	In	**Out**		
Standard	3.690%	3.730%	7.420%	6.025%
New	3.473%	3.500%	6.973%	

Table 2. Improvement in bandwidth utilization for *link A*

As for the other home network connected via *Link B*, similar results are obtained and are represented in Figures 8 and 9 and summarized in Table 3.

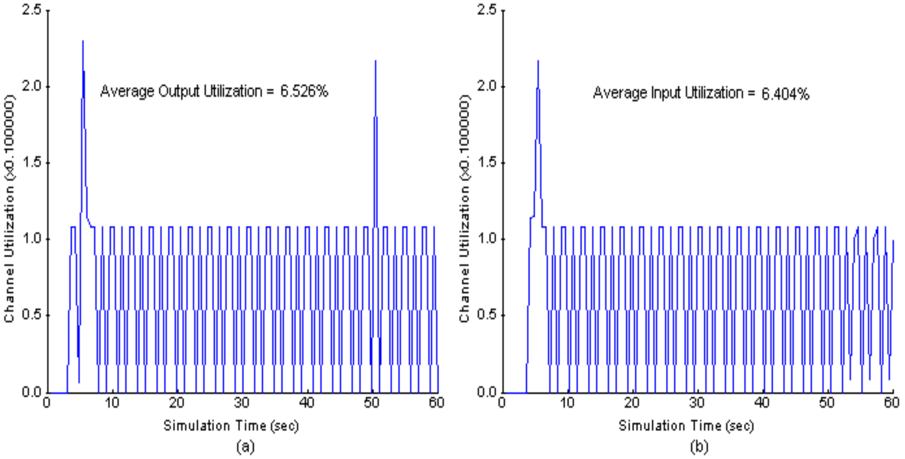

Fig. 8. Bandwidth utilization for *LinkB* in the Mobile IP standard

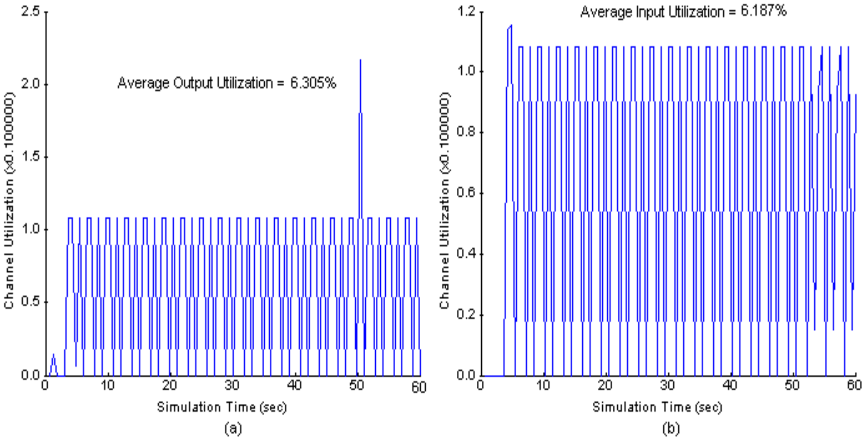

Fig. 9. Bandwidth utilization for *LinkB* in the new model

Model	LinkB		Total	Improvement
	In	**Out**		
Standard	6.404%	6.526%	12.930 %	3.387 %
New	6.187%	6.305%	12.492%	

Table 3. Improvement in bandwidth utilization for *link B*

Anyhow, such numbers prove the fact that the new model surpasses the standard one. Indeed the improvement ratio could be large or small depending on the number of the mobile hosts and the way they communicate with other nodes. But, the results prove that there is a quantitative improvement. Moreover, it should be mentioned that all the parameters that have been applied throughout the simulation are taken as an assumption, with the fact that changing such parameters will definitely change the output numerical results. However, any modification in the simulation parameters does not contradict with the fact that the new proposed model is quantitatively better than the Mobile IP standard.

7 Conclusion

In this work, we have suggested possible enhancement to the Mobile IP protocol that has been developed and standardized by the IETF. The IETF Mobile IP working group has proposed a technique for route optimization. Based on this concept, this paper has provided a new methodology for caching mobile information. Also, a new vital component called the MIS has been added to the mobile architecture.

Simulation results supports the logical expectation of improved efficiency when the new architecture is used over the standard one.

In addition to the quantitative gain, the new model has achieved other substantial qualitative advantages. From a scalability point of view, and after describing the details of the two mobile architectures, it is quite clear that in order to deploy such a wide area caching mechanism; some sort of centralized management is required, which is implemented in the MIS. Moreover, our new design is transparent not only to the Internet hosts, but also to the protocol used whether it is IPv4 or IPv6.

References

1. George H. Forman and John Zahorjan.: The Challenges of Mobile Computing., Computer Science & Engineering, University of Washington, 1993.
2. Postel J.B., Editor.: Internet Protocol. IETF RFC 791, September 1981b.
3. P. Bhagwat, C. Perkins, and S. K. Tripathi.: Network Layer Mobility: an Architecture and Survey. *IEEE Personal Comm.,* Vol.3, No.3, June 1996, pp. 54-64.
4. Postel J.B., Editor.: Transmission Control Protocol. IETF RFC 793, September 1981c.
5. J. Ioannidis and G. Maguire Jr.:The Design and Implementation of a Mobile Internetworking Architecture. *In Proceedings of Winter USENIX,* San Diego, CA, January 1993, pp. 491-502.
6. John Ioannidis, Dan Duchamp, and Gerald Q. Maguire Jr. : IP-based Protocols for Mobile Internetworking. Department of Computer Science, Columbia University.
7. F. Teraoka, Kim Claffy, and M. Tokoro.: Design, Implementation and Evaluation of Virtual Internet Protocol. *In Proceedings of the 12th International Conference on Distributed Computing Systems,* June 1992, pp. 170-177.
8. F. Teraoka and M. Tokoro.: Host Migration Transparency in IP Networks. *Computer Communication Review,* January 1993, pp. 45-65.
9. Y. Rekhter and C. Perkins.: Loose Source Routing for Mobile Hosts. Internet draft, July 1992.

10. Charles Perkins, Andrew Myles, and David B. Johnson.: IMHP: A Mobile Host Protocol for the Internet. *Computer Networks and ISDN Systems 27*, December 1994, pp. 479-491.
11. Charles Perkins and Andrew Myles.: Mobile IP. *SBT/IEEE International Telecommunications Symposium*, Rio De Janeiro, August 1994.
12. Charles Perkins.: IPv4 Mobility Support. IETF RFC 2002, October 1996.
13. Charles Perkins. Mobile IP: Design Principles and Practices. Addison-Wesley, 1997.
14. Douglas E. Comer.: Internetworking with TCP/IP Volume I: Principles, Protocols and Architecture. Prentice-Hall, 1995.
15. Charles Perkins and David B. Johnson.: Route Optimization in Mobile IP. Internet draft, ftp://ftp.ietf.org/internet-drafts/draft-ietf-mobileip-optim-07.txt, November 1997.
16. S. Deering and R. Hinden.: Internet Protocol, Version 6 (IPv6) Specification. IETF RFC (1883), December 1995.
17. Charles Perkins and David B. Johnson.: Mobility Support in IPv6. Internet draft, ftp://ftp.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-07.txt, November 1998.
18. S. Thomson and T. Narten.: IPv6 Stateless Address Autoconfiguration. IETF RFC 1971, August 1996.
19. T. Narten, E. Nordmark, and W. Simpson.: Neighbor Discovery for IP Version 6 (IPv6). IETF RFC 1970, August 1996.
20. Scott O. Bradner and Allison Mankin.: IPng Internet Protocol Next Generation. Addison-Wesley Publishing Company, 1995.
21. Charles Perkins.: Mobile Networking Through Mobile IP. *IEEE Internet Computing*, February 1998, pp. 58-69
22. COMNET III User's Mannual, Planning for Network Managers Release 1.2, 1996.

23 Mockapetris P.: Domain Names-Concepts and Facilities. IETF RFC 1034, November 1987.