Performance Analysis of Mobile IPv4 and Mobile IPv6

Fayza Nada
Faculty of Computers and information, Suez Canal University, Egypt

Abstract: *The number of mobile computers is increasing at a phenomenal rate, and efficient support for mobility will make a decisive difference to the Internet's future performance. This, along with the growing importance of the Internet and the web indicates the need to pay attention to supporting mobility. Mobile IPv6 (MIPv6) is a protocol to deal with mobility for the next generation Internet (IPv6). However, the performance of MIPv6, especially in comparison with MIPv4, has not been extensively investigated yet. In this paper, we present an analysis of the Mobile IPv6 performance as the packets delay changes due to supporting mobility. We also introduce a comparison between Mobile IPv4 and Mobile IPv6 in supporting mobility.*

Keywords: *MIPv4, MIPv6, mobile networking, TCP performance, network simulation*.

Received November 18, 2005; accepted March 4, 2006

1. Introduction

Mobile communications services have experienced remarkable growth, and among these, services providing Internet access from mobile terminals are steadily increasing by tens of thousands of subscribers per day. In Japan, the third-generation mobile communications system, IMT-2000, was launched in 2001. The main goals of IMT-2000 services are to provide high quality multimedia services at speed up to 2 Mbit/s, to provide a global roaming service spanning mobile communications carriers worldwide, and to enable technologies to be examined by a coalition of telecommunications standards-setting bodies. Other wireless access technologies that are also under investigation include MMAC [12] and HIPERLAN/2 [11], which can provide even faster services at speeds on the order of 10 Mbit/s. Mobile communications seem to be entering an era of genuine high speed, wide area communications.

The increasing number of portable computers, combined with the growth of wireless services, makes supporting Internet mobility important. Many researchers have come to the conclusion that IP is the correct layer to implement the basic mobility support. The greatest challenge for supporting mobility at IP layer is handling address changes. In other words, it is required to keep uninterrupted connections among nodes when they change their IP addresses during the movement. Mobile IP has been designed within the IETF to serve the needs of the burgeoning population of mobile computer users who wish to connect to the Internet and maintain communications as they move from place to place. The Transmission Control Protocol (TCP) is a predominant protocol in the Internet service. The TCP/IP protocol was originally designed for fixed Internet without mobility in mind. With the increase of mobility demands, it is important to understand how TCP performance is affected over various existing mobility protocols, which can in turn help design new protocols or pursue improvements.

Mobile IPv4 (MIPv4) is a popular mobility protocol used in the current IPv4 networks. With the next generation Internet IPv6 emerging, the Mobile IPv6 protocol is designed to deal with mobility and to overcome some problems suffered by MIPv4. Although MIPv6 shares many features with MIPv4, there exist some differences. The difference in overall throughput of MIPv4 compared to MIPv6 is roughly proportional to the difference in packet size attributed to IPv6's increased header size. Mobile IP extends IP by allowing the mobile computer to have two addresses, one for identification, and the other for routing. We can outline the operation of the basic mobile IP protocol (MIPv4) as follows [7]: Mobility agents send agent advertisement messages. After receiving an agent advertisement, a mobile node can determine whether it is attached to the home network or to a foreign network. When a mobile node is attached to a foreign network, it obtains a care-of address on that foreign network. The mobile node registers its care-of address with its home agent, as shown in Figure 1. The home agent receives all datagrams distended to the mobile node's home address and tunnels them to the mobile node's care-of address. More details about MIPv4 can be found in [5]. Mobile IP still has many items that need to be worked on and enhanced such as the security issue and the routing issue. The IETF has been working on the problems

which had been found on MIPv4 protocol. IPv6 is derived from IPv4 and in many ways similar to it. As such, the IETF Mobile IP working group's current protocol design [8] for mobility of IPv4 nodes could be adapted for use in IPv6, with only the straightforward changes needed to accommodate differences between IPv4 and IPv6 such as the size of addresses. The most visible difference is that IPv6 addresses are all 128 bits long, instead of 32 bits long as in IPv4.

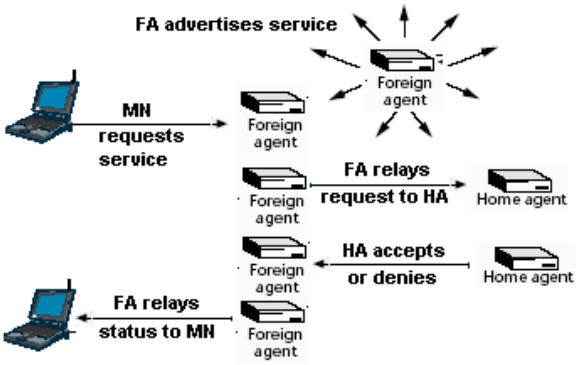

Figure 1. Registration overview.

Mobile IPv6 allows a mobile node to move from one link to another without changing the mobile node's IP address. A mobile node is always addressable by its "home address". Packets may be routed to the mobile node using this address regardless of the mobile node's current point of attachment to the Internet, and the mobile node may continue to communicate with other nodes (stationary or mobile) after moving to a new link. The movement of a mobile node away from its home link is thus transparent to transport and higher-layer protocols and applications. However, the performance of MIPv6, especially in comparison with MIPv4 has not yet been extensively investigated. In this paper, we introduce an analysis of Mobile IPv6 performance taken into consideration the additional load caused because of providing mobility as the internet delay is changed. A computer simulation model is used to simulate Mobile IPv6. The additional load are the time and work required to process the extra packets (binding update, binding request, tunneled packets etc.) generated in order to provide mobility.

The rest of this paper is organized as follows. Section 2 reviews the base Mobile IPv4, with its basic operations and the problems that have been found in it. Section 3 shows the mobility support in Mobile IPv6 and gives the analysis of its performance using a computer simulation model. In section 4, we outline the main differences between Mobile IPv4 and Mobile IPv6 in supporting mobility. Section 5 is for conclusions and future work.

2. Mobile IPv4 Overview

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 indicated by its IP address in order to receive datagrams destined to it; otherwise, datagrams 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 maintain transport and higher layer connections when the node changes location. The second has obvious and severe scaling problems, especially relevant considering the explosive growth in sales of notebook (mobile) computers. A new, scalable, mechanism is required for accommodating node mobility within the Internet.

2.1. Mobile IPv4 Basic Operations

Mobile IP is a way of performing three related functions:

- *Agent Discovery*: Mobility agents advertise their availability on each link for which they provide service.
- *Registration*: When the mobile node is away from home, it registers its care-of address with its home agent.
- *Tunneling*: In order for datagrams to be delivered to the mobile node when it is away from home, the home agent has to tunnel the datagrams to the care-of address. The following will give a rough outline of operation of the mobile IP protocol, making use of the above-mentioned operations. Figure 1 may be used to help envision the roles played by the entities.

Mobility agents make themselves known by sending agent advertisement messages. An impatient mobile node may optionally solicit an agent advertisement message. After receiving an agent advertisement, a mobile node determines whether it is on its home network or a foreign network. A mobile node basically works like any other node on its home network when it is at home. When a mobile node moves away from its home network, it obtains a care-of address on the foreign network, for instance, by soliciting or listening for agent advertisements, or contacting Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol (PPP).

While away from home, the mobile node registers each new care-of address with its home agent, possibly by way of a foreign agent. Datagrams sent to the mobile node's home address are intercepted by its home agent, tunneled by its home agent to the care-of

address, received at the tunnel endpoint (at either a foreign agent or the mobile node itself), and finally delivered to the mobile node.

In the reverse direction, datagrams sent by the mobile node are generally delivered to their destination using standard IP routing mechanisms, not necessarily passing through the home agent. When the home agent tunnels a datagram to the care-of address, the inner IP header destination (i. e., the mobile node's home address) is effectively shielded from intervening routers between its home network and its current location. At the care-of address, the original datagram exits from the tunnel and is delivered to the mobile node.

It is the job of every home agent to attract and intercept datagrams that are destined to the home address of any of its registered mobile nodes. The home agent basically does this by using a minor variation on proxy Address Resolution Protocol (ARP), and to do so in the natural model it has to have a network interface on the link indicated by the mobile node's home address. However, the latter requirement is not part of the mobile IP specification. When foreign agents are in use, similarly, the natural model of operation suggests that the mobile node be able to establish a link with its foreign agent.

Notice that, if the home agent is the only router advertising reachability to the home network, but there is no physical link instantiating the home network, then all datagrams transmitted to mobile nodes addressed on that home network will naturally reach the home agent without any special link operations. Figure 2 illustrates the routing of datagrams to and from a mobile node away from home, once the mobile node has registered with its home agent. The mobile node is presumed to be using a care-of address provided by the foreign agent.

A datagram to the mobile node arrives on the home network via standard IP routing. The datagram is intercepted by the home agent and is tunneled to the care-of address, as depicted by the arrow going through the tube. The datagram is detunneled and delivered to the mobile node.

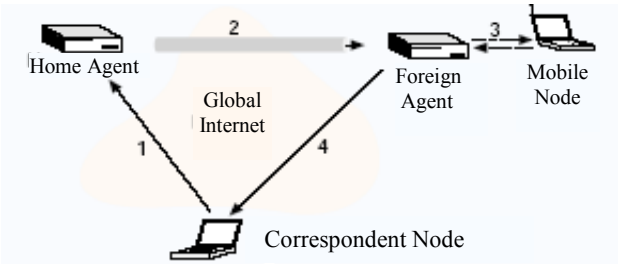

Figure 2. Mobile IP overview.

For datagrams sent by the mobile node, standard IP routing delivers each to its destination. In the figure, the foreign agent is the mobile node's default router.

2.2. Problems of Mobile IPv4

Mobile IP still has many items that need to be worked on and enhanced such as the security issue and the routing issue. The IETF has been working on the problems which had been found on the base Mobile IP protocol.

1. *Triangle Routing*: As noted above, datagrams going to the mobile node have to travel through the home agent when the mobile node is away from home, but datagrams from the mobile node to other stationary Internet nodes can be routed directly to their destinations. This additional routing, called triangle routing, is generally far from optimal, especially in cases when the correspondent node is very close to the mobile node (see Figure 3) Route Optimization is the protocol suggested to eliminate the triangle routing problem and is described in the next section.
2. *Duplicating Fields in "IP Within IP"*: To encapsulate the datagram, we put the original datagram inside another IP envelope, then the whole packet consists of the outer IP header plus the original datagram. The fields in the outer IP header add too much overhead to the final datagram -- several fields are duplicated from the inner IP header. This waste of unnecessary space is uneconomical. Minimal encapsulation scheme is defined to overcome this problem and becomes another option to encapsulate the datagram. Instead of inserting a new header, the original header is modified to reflect the care-of address, and in between the modified IP header and unmodified IP payload, a minimal forwarding header is inserted to store the original source address and original destination address. When the foreign agent tries to decapsulate, it will simply restore the fields in the forwarding header to the IP header, and remove the minimal forwarding header. There is a restriction to the use of this encapsulation method. If the original datagram is already fragmented, then minimal encapsulation must not be used since there is no room left to store fragmentation information.
3. *Fragility*: Although single home agent model is simple and easy to configure, it has the disadvantage of fragility. The mobile node becomes unreachable once the home agent breaks down. One possible solution is to support multiple home agents. If one conventional home agent fails, there are still other home agents who can take over the duty and route the datagram to the mobile node.
4. *Dogleg Routing*: If a mobile node happens to move to the same subnetwork as its correspondent node that wants to send it datagrams, this is what will happen in order for the datagram to be received by the mobile node, based on the base Mobile IP protocol: the correspondent node will send the datagram all the way to the mobile node's home agent, which may be a half globe away; its home

agent will then forward the datagram to its care-of address, which might just take a half second to reach if the datagram is sent directly from the correspondent node. This kind of "indirect routing" is inefficient and undesirable. The effort to define extensions to the operation of the base Mobile IP to allow for the optimization of datagram routing from a correspondent node to a mobile node has been made by the Mobile IP working group of the Internet Engineering Task Force (IETF). The key approach to route optimization is as follows: Binding cache containing the mobility binding of mobile node(s) is provided for the node that looks for optimizing its own communication with mobile nodes. In this way, the correspondent node has a way to keep track of where the mobile node(s) is. So when the time comes that the correspondent node wishes to send a datagram to the mobile node, it can send the datagram directly to the destination address, eliminating the "zig-zag" routing. The means for the mobile node's previous foreign agent to be notified of the mobile node's new location is provided. This mechanism allows datagrams in flight to the mobile node's previous foreign agent to be redirected to its current address [1].

5. *Security Issues*: The most pressing outstanding problem facing Mobile IP is that of security. A great deal of attention is being focused on making Mobile IP coexist with the security features coming into use within the Internet. Firewalls, [2] in particular cause difficulty for Mobile IP because they block all classes of incoming packets that do not meet specified criteria. Enterprise firewalls are typically configured to block packets from entering via the Internet that appear to emanate from internal computers. Although this permits management of internal Internet nodes without great attention to security, it presents difficulties for mobile nodes wishing to communicate with other nodes within their home enterprise networks. Such communications, originating from the mobile node, carry the mobile node's home address and would thus be blocked by the firewall [6].
6. *Routing Inefficiencies*: The base Mobile IP specification has the effect of introducing a tunnel into the routing path followed by packets sent bythe correspondent node to the mobile node. Packets from the mobile node, on the other hand, can go directly to the correspondent node with no tunneling required. This asymmetry is captured by the term triangle routing, where a single leg of the triangle goes from the mobile node to the correspondent node, and the home agent forms the third vertex controlling the path taken by data from the correspondent node to the mobile node. Triangle routing is alleviated by use of route optimization, but doing so requires changes in the correspondent nodes that will take a long time to deploy for IPv4. It is hoped that triangle routing will not be a factor for IPv6 mobility.

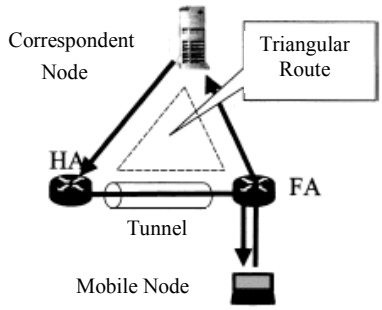

Figure 3. Triangle routing.

3. Mobile IPv6 Overview

Mobile IPv6 is the next generation protocol and in the near future, routers are going to become more faster and new technologies are going to reduce 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.

3.1. Mobile IPv6 Basic Operations

In Mobile IPv6, mobile node should assign three IPv6 addresses to their network interface(s) at least whenever they are roaming away from their home subnet. One is its home address, which is permanently assigned to the mobile node in the same way as any IP node. The second address is the mobile node's current link-local address. The third address, known as the mobile node's care-of address, which is associated with the mobile node only while visiting a particular foreign subnet. The association between a mobile node's home address and its care-of address, along with the remaining lifetime of that association, is known as a binding. The central data structure used in Mobile IPv6 is a cache of mobile node bindings, maintained by each IPv6 node, known as a binding cache. While away from home, a mobile node registers with a router in its home subnet, requesting this router to function as the home agent for the mobile node. While it has a home registration entry in its binding cache, the home agent uses proxy neighbor discovery to intercept any IPv6 packets addressed to the mobile node's home address on the home subnet, and tunnels each intercepted packet to the mobile node's primary care-of address indicated in this binding cache entry. To tunnel the

packet, the home agent encapsulates it using IPv6 encapsulation [3].

In addition, Mobile IPv6 provides a mechanism for IPv6 correspondent nodes communicating with a mobile node to dynamically learn the mobile node's binding. The correspondent node adds this binding to its binding cache. When sending a packet to any IPv6 destination, a node checks its binding cache for an entry for the packet's destination address, and if a cached binding for this address is found, the node routes the packet directly to the mobile node at the care-of address indicated in this binding; this routing uses an IPv6 routing header [4] instead of IPv6 encapsulation (The home agent can not use a routing header, since adding one to the packet at the home agent would invalidate the authentication in any IPv6 authentication header included in the packet by the correspondent node). If no binding cache entry is found, the correspondent node instead sends the packet normally (with no routing header), and the packet is then intercepted and tunneled by the mobile node's home agent as described above. Mobile IPv6 introduces four new IPv6 destination options to allow a mobile node's home agent and correspondent nodes learn and cache the mobile node's binding as follows:

- *Binding Update*: A binding update option is used by a mobile node to notify a correspondent node or the mobile node's home agent of its current binding. The binding update sent to the mobile node's home agent to register its primary care-of address is marked as a "home registration" as shown in Figure 4.
- *Binding Acknowledgement*: A binding acknowledgement option is used to acknowledge receipt of a binding update, if an acknowledgement was requested in the binding update, as shown in Figure 5.
- *Binding Request*: A binding request option is used to request a mobile node to send to the requesting node a binding update containing the mobile node's current binding. This option is typically used by a correspondent node to refresh a cached binding for a mobile node, when the cached binding is in active use but the binding's lifetime is close to expiration.
- *Home Address*: A home address option is used in a packet sent by a mobile node to inform the recipient of that packet of the mobile node's home address. When a mobile node sends a packet while away from home, it will set the source address in the packet's IPv6 header to one of its current care-of addresses, and will also include a "home address" destination option in the packet, giving the mobile node's home address. including the home address option in each packet, the sending mobile node can communicate its home address to the correspondent node receiving this packet, allowing the use of the care-of address to be transparent above the Mobile IPv6 support level (e. g., at the transport layer). The inclusion of a home address option in a packet affects only the correspondent node's receipt of this single packet; no state is created or modified in the correspondent node as a result of receiving a home address option in a packet. If the care-of address for the binding is equal to the home address of the mobile node, the binding update option indicates that any existing binding for the mobile node must be deleted.

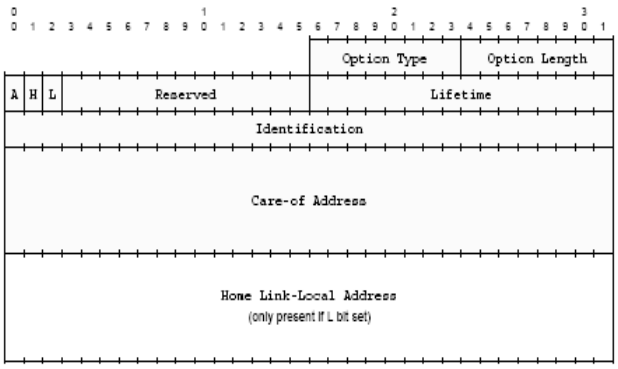

Figure 4. Binding update destination option format.

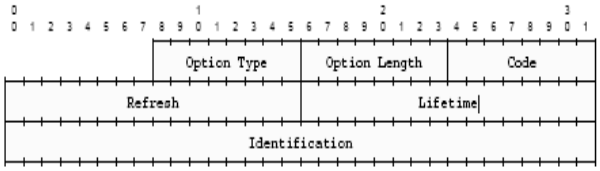

Figure 5. Binding acknowledgment destination option format.

3.2. Simulation of Mobile IPv6

In this simulation, the performance of Mobile IPv6 is analyzed in terms of the overhead time incurred to support mobility (in transmitting control messages (binding updates, binding requests, binding acknowledges, router advertisements) and tunneled packets from source to destination. To simulate Mobile IPv6, a hypothetical Internet, consisting of five networks is considered. Each network, in turn consists of three hosts and one router. We have considered all of the networks to be using star topology. An IP address format, consisting of a network number followed by a host offset id is used. Figure 6 shows the interconnections of the networks.

The Internet is initialized by assigning addresses to the routers and hosts and setting up routing tables. The process queue is initialized to contain two basic events, host movement and transmission request. As events are processed, they schedule other events, which are again put into the queue. This popping and pushing of events continues for the time of simulation. The mobile node, the foreign network, and the requesting node are randomly selected. The number of packets to be sent is also randomly selected. Exponential distribution is used to calculate the different delays, such as Internet delays (packets delay between two networks), Intranet delays (packet delay between a router and its host).

When one phase of transmission is completed, the mobile node returns to its home network and the whole process of randomly selecting the mobile and requesting nodes, and the foreign network is repeated again. All the networks in the simulation are considered to be identical and equidistant and the hosts are identical. Congestion, collisions, error checking, and security issues will not be taken into consideration because it is seen that they are not going to play a direct role in our computations. The following parameters are used in the analysis:

- *Percentage of Encapsulated Packets*: The number of the encapsulated packets divided by the total number of transmitted packets and multiplied by 100.
- *Packet Delay*: The time taken by a packet to reach from one network to the other.
- *Percentage of the Additional Routing Time*: The time consumed in transmitting the mobility messages (binding update, binding requests ...) divided by the total transmission time and multiplied by 100.

In Figure 7, the mean packet delay is plotted vs. the percentage of the encapsulated packets. Note from the figure that, as the packet delay decreases the percentage of the encapsulated packets also decreases, this is because when the packet delay time decreases, packets will reach the home agent faster, the binding update will reach the correspondent node earlier, and transmission to the care-of address will begin earlier, decreasing the number of the encapsulated packets.

The number of encapsulated packets vs. total number of transmitted packets for constant packet delay is plotted in Figure 8. It can be seen that, increasing or decreasing the number of transmitted packets has no effect on the number of encapsulated packets. This follows from the fact that, packets is encapsulated only from the home agent to the mobile node when the correspondent node does not have the mobile node's care-of address and this happens only in the beginning of the transmission from the correspondent node to the mobile node, once the correspondent node gets the care-of address of the mobile node, it will use it for next transmission and no packets will be encapsulated. Then, the number of the encapsulated packets does not depend on the number of transmitted packets.

Figure 9 plots the packet delay vs. the additional routing time for routing mobility messages. It shows that, increasing the packet delay leads to increasing in the additional routing time. This comes from the fact that, increasing the packet delay means that the mobility messages (binding update, binding acknowledgement...) will reach late, causing increase in the additional routing time needed to route mobility messages.

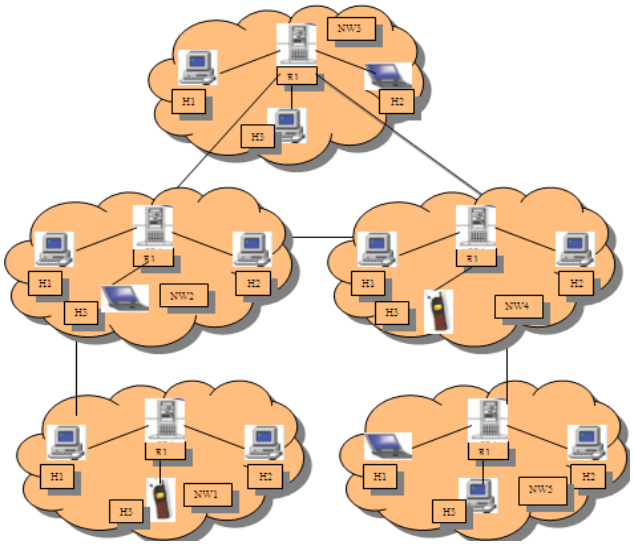

Figure 6. A hypothetical Internet with 5 networks (NW).

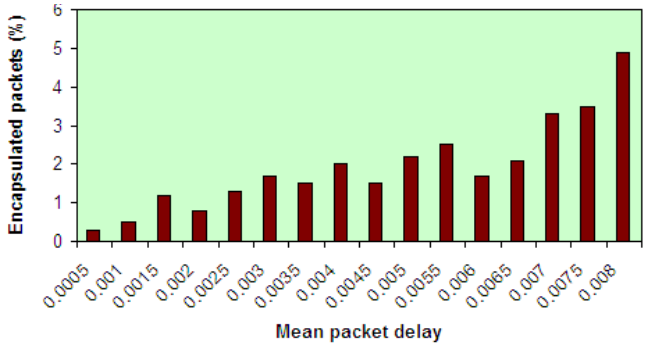

Figure 7. Mean packet delay vs. encaps. packets (%).

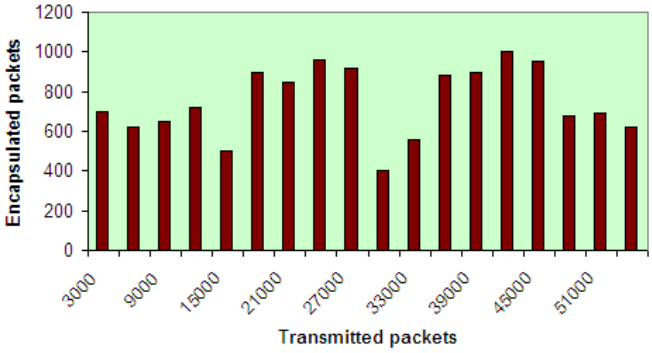

Figure 8. No. of transmitted packets vs. no. of encaps. packets.

4. Comparison of Mobile IPv4 and Mobile IPv6

- Packets sent to a mobile node while away from home in Mobile IPv6 are tunneled using an IPv6 routing header rather than IP encapsulation, whereas Mobile IPv4 must use encapsulation for all packets. The use of a routing header requires less additional header bytes to be added to the packet, reducing the overhead of Mobile IP packet delivery.
- No need to deploy special routers as "foreign agents" as are used in Mobile IPv4. Mobile IPv6, mobile nodes make use of the enhanced features of IPv6, such as neighbor discovery and address auto

configuration.

- "Route Optimization" procedure is built in as a fundamental part of Mobile IPv6, rather than being added on as an optional set of extensions that may not be supported by all nodes as in Mobile IPv4. This allows direct routing from any correspondent node to any mobile node, without needing to pass through the mobile node's home network and be forwarded by its home agent, and thus eliminates the problem of "triangle routing" present in the base Mobile IPv4 protocol.
- While a mobile node is away from home, its home agent intercepts any packets for the mobile node that arrive at the home network, using IPv6 neighbor discovery rather than ARP as is used in Mobile IPv4.
- Mobile IPv6 uses destination options which allow all Mobile IPv6 control traffic to be piggybacked on any existing IPv6 packets, whereas Mobile IPv4 and its route optimization extensions needs separate UDP packets for each control message.
- Mobile IPv6 allows mobile nodes and Mobile IP to coexist efficiently with routers that perform "ingress filtering". A mobile node now uses its care-of address as the source address in the IP header of packets it sends, allowing the packets to pass normally through ingress filtering routers. The mobile node carries its home address in a home address destination option, allowing the use of the care-of address in the packet to be transparent above the IP layer.
- Mobile IPv6 utilizes IP Security (IPsec) for all security requirements (sender authentication, data integrity protection, and replay protection) for binding updates (which serve the role of both registration and route optimization in Mobile IPv4), whereas Mobile IPv4 relies on its own security mechanisms for these functions, based on statically configured "mobility security associations".
- Although Mobile IPv6 enables wide-area mobility to be implemented at the IP level, it does not have functions characteristic of wireless access networks such as high-speed handover or paging functions.
- A key design point of Mobile IPv4 [9] was to support host mobility in networks without mandating changes to every existing IPv4 node, while Mobile IPv6 includes explicit support for host mobility.
- Mobile IPv6 and Mobile IPv4 with routing optimization [10] could in theory support mobile networks similarly as in Mobile IPv4. However, although mentioned in the Mobile IPv4 specification, the current specifications of Mobile IPv4 with routing optimization and Mobile IPv6 don't mention them anymore. Mobile IPv6 can not be used without major changes if we want to provide optimal mobility support to networks. Particularly, Mobile IPv6 doesn't scale to the size of the mobile network.
- Mobile IP still acts as an "open-door" for hackers of all kinds, there is no strong authentication of the visiting user, no data privacy and no data integrity protection between the MN and its home network.

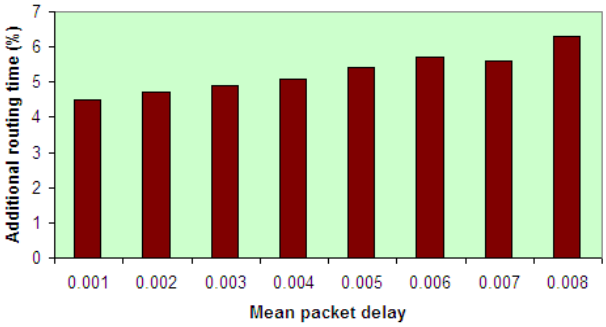

Figure 9. Mean packet delay vs. additional routing time (%).

5. Conclusions and Future Work

Mobility support in the IP protocol has been developed by the IETF leading to the Mobile IP protocol. Mobile IP has gained attention as a technology that can provide mobility to universal users independently of the access network. Currently, two versions of Mobile IP are available, versions 4 (MIPv4) and 6 (MIPv6). Mobile IPv6 is a protocol to deal with the next generation Internet. IP mobility protocols are used to adapt IP address changes and make the changes transparent to the transport layers and higher layer protocols. In this paper, we study the performance of MIPv6 taken into account the additional work done due to supporting mobility (work and time needed for routing mobility messages such as binding update, binding request ...). A simulation model has been used to simulate MIPv6. The results show that, increasing the packet delay time leads to increasing in the number of encapsulated packets, and results also in increasing the additional load on the network. Whereas, increasing the number of transmitted packets has no effect on the number of the encapsulated packets. The simulation model was conducted with a single communication session and for a limited period.

Further work will include into the simulation, competing traffic, collisions, transmission errors, and the impact of fast handover and hierarchical Mobile IPv6. Further work may also include an advanced simulation environment, to be used in validating, examining the performance of protocols for IP mobility support.

References

[1] Chen Y., "A Survey Paper on Mobile IP," available at: http://www.cis.ohio-state.edu/~jain /cis788-95/mobile_ip, 1996.

[2] Cheswick W. R. and Bellovin S., *Firewalls and Internet Security*, Addison Wesley, Reading,

Mass., 1994.
[3] Conta A. and Deering S., "Generic Packet Tunneling in IPv6," available at: ftp://ftp.ietf.org/internet-drafts/draft-ietf-ipngwg-ipv6-tunnel-07.txt, July 1996.
[4] Deering S. and Hinden R., "Internet Protocol, Version 6 (IPv6) Specification," *Internet Request for Comments (RFC1883)*, available at: ftp://ds.internic.net/rfc/rfc1883.txt, 1995.
[5] Nada F. A., "On Using Mobile IP Protocols," *Journal of Computer Science*, vol. 2, no. 2, pp. 211-217, 2005.
[6] Perkins C., "Mobile Networking Through Mobile IP," *IEEE Internet Computing Journal*, 1998.
[7] Perkins C., *Mobile IP Design Principles and Practices*, Addison Wesley Wireless Communications Series, 1997.
[8] Perkins C., "IPv4 Mobility Support," available at: http://ietf-draft-mobileip-protocol-17.txt, May 1996.
[9] Perkins C., "IP Mobility Support for IPv4," *Internet Request for Comments (RFC3220)*, available at: http://rfc.sunsite.dk/rfc/rfc3344.html, January 2002.
[10] Perkins C. and Johnson D. B., "Route Optimization in Mobile IP," available at: http://draft-ietf-mobileip-optim-11.txt, September 2001.
[11] Takagi Y., Ihara T., and Ohnishi H., "Mobile IP Route Optimization Method for Next-Generation Mobile Networks," *Electronics and Communications in Japan*, Part 1, vol. 86, no. 2, pp. , 2003.
[12] Umehira M., Aikawa S., Matsumoto Y., Nakura M., and Kobayashi T., "Multimedia Mobile Access Trends," *in Proceedings of the 2000 IEICE General Conference*, TB-2-2, pp. 698-699, 1999.

Fayza Nada received her BSc and MSc in computer science, both from College of Science, Suez Canal University, Egypt in 1991 and 2002, respectively. Currently, she is pursing her PhD in computer science, in the same college. Her research interests include performance analysis, mathematical modeling of computer and communications systems, queuing theory, and using mobile IP protocols in multimedia traffic.