T.C.
MARMARA UNIVERSITY
INSTITUTE FOR GRADUATE STUDIES IN
PURE AND APPLIED SCIENCES

PERFORMANCE EVALUATION OF MOBILE INTERNET PROTOCOL

Birol ÇELİK

(Computer Engineering)

THESIS

FOR THE DEGREE OF MASTER OF SCIENCE

IN

COMPUTER ENGINEERING PROGRAMME

SUPERVISOR
Asst. Prof. Dr. Demir ÖNER

ISTANBUL 2006

TEŞEKKÜR

Tez çalışmam süresince pozitif yaklaşım ve düşünceleriyle çalışma motivasyonumu artırarak beni bu noktaya taşıyan, yoğun çalışma ortamında bile bana zaman ayırarak, bilgi ve deneyimleri ile beni yönlendiren ve araşatırmaya yönelik katkı ve değerlendirmelerinden ötürü tez danışmanım sayın Asst. Prof. Dr. Demir ÖNER'e, sağladığı kaynaklarla çalışmalarıma katkı sağlayan Sayın Bahadır KORKUT'a, desteklerinden güç aldığım tüm dost ve çalışma arkadaşlarıma, ve her türlü desteğiyle, her zaman hep yanımda olan sevgili eşim Zehra ÇELİK'e çok teşekkür ederim.

MAYIS 2006 **Birol ÇELİK**

CONTENTS

ÖZET

MOBİL İNTERNET PROTOKOLU PERFORMANS DEĞERLENDİRMESİ

Son yıllarda mobil iletişim, İnternet ve IP tabanlı ağlar kadar büyük ilgi görmeğe başladı. Taşınabilir bilgisayarların gelişmesi ile mobil kullanım artarak hayatımızdaki yerini almaktadır. Kablosuz ağ arayüzlerindeki ve global ağ uygulamalarındaki son gelişmeler, mobilite konusunun sistemlerinin kablolu ve kablosuz ağların ilgi alanı içine girmesini sağlamıştır.

Mobil IP, mobil iletişimde günümüzde en ümit verici protokol olarak kabul görmektedir. Mobil IP IETF (Internet Engineering Task Force) tarafından IPv4 üzerine, İnternet üzerinde Mobil IP ihtiyacını karşılamak amacı ile geliştirilmiştir. Temel Mobil IP (Mobil İnternet Protokolü) de, paketler mobil kullanıcıya ev sahibi sunucu üzerinden geçerek giderler. Bununla beraber mobil kullanıcıdan, karşıdaki kablolu ağda bulunan kullanıcıya paketler direk gönderilirler. Bu asimetrik yönlendirme, özellikle karşı kullanıcının mobil kullanıcıya yakın olma durumunda, üçgen yönlendirme diye adlandırılmaktadır. Bu üçgen yönlendirme problemine çözüm getirmek ve karşı kullanıcı ile direk haberleşebilmek için optimize edilmiş Mobil IP yönlendirme methodu geliştirilmiştir. Üçgen yönlendirme problemini çözmek Mobil IP nin temel konularından biridir. IETF tarafından geliştirilen optimize edilmiş yönlendirme metodu bu sorunun çözümü için geliştirilmiştir. Bununla beraber günümüzde bu problemi çözmeye yönelik bir çok metod geliştirilmiş olsa da en çok kabul gören optimize edilmiş yönlendirme metodudur. Fakat Optimize edilmiş yönlendirme methodu da henüz yeterli etkinliğe erişmemiş olup üzerinde araştırma ve geliştirme çalışmaları devam etmektedir.

Bu tezde, Mobil IP ve Optimize edilmiş yönlendirmeli Mobil IP protokollerinin performans değerlendirmesi yapılmıştır. NS2 benzeticisi (Network Simulator 2)

kullanarak “Temel Mobil IP” ile “Optimize Edilmiş Mobil IP” protokollerinin başarımları, paket gecikmeleri ve paket kayıpları yönlerinden karşılaştırılmıştır. Simulasyon yapılırken, mevcut uygulmaya, gerekli düzenleme ve eklemeler yapılarak sonuca varılmıştır.

MAYIS 2006 **Birol ÇELİK**

ABSTRACT

PERFORMANCE EVALUATION OF MOBILE INTERNET PROTOCOL

Recent advances in wireless network interfaces and the implementation of the global networks make host mobility an issue of interest both in wireless and wired networks. The most promising protocol proposals for handling of host mobility in IP networks are Mobile IP. Mobile IP built on IPv4, was designed by (Internet Engineering Task Force) to serve the needs of supporting portable IP addresses on Internet. In the basic Mobile IP protocol, datagrams going to the mobile node have to travel through the home agent when the mobile node is away from home network. This asymmetric routing, called Triangle Routing, is generally far from optimal, especially when the destination node is close to the mobile node. Eliminating the Triangle Routing problem, in order to improve network efficiency, is one appealing topic in Mobile IP.

Route Optimization eliminates Triangle Routing problem but it does not solve packet loss problem during handoff periods. Smooth handoff and buffer supports are added Route Optimized Mobile IP to reduce packet loss during handoff periods and improve Mobile IP performance. Route optimization with smooth handoff extends the registration protocol to inform the mobile node's previous foreign agent about the mobile node movement to a new foreign network. But there is some packet loss before previous foreign agent extension is received. Agent buffering mechanism with smooth handoff packets eliminates this packet loss by buffering and re-tunneling the buffered packets to the mobile node's new foreign agent along with any future packets. Hence, packet loss during handoff can be completely eliminated.

In this thesis performances of Mobile IP and Route Optimization Mobile IP protocols are evaluated and compared. For this study, Network Simulator 2 (NS2) is used. In the simulation, Route Optimization with buffer and smooth handoff is implemented to increase performance. Packet loss, end-to-end delay, and throughput are considered as performance.

Index Terms—Mobile Internet Protocol, route optimization, smooth handoff, Mobile IP routing protocols

June 2006 **Birol ÇELİK**

CLAIM FOR ORIGINALITY

The standard Mobile IP has the triangle routing problem when a mobile user moves from the Home Agent to a Foreign Agent. This problem causes longer end-to-end average delay time, especially high packet loss and consequently low throughput.

The route optimization method is proposed to solve this problem. Smooth handoff method and buffer support are used to minimize the undesired effects encountered during handoff in Route Optimized Mobile IP. But to use Route Optimized Mobile IP method in IPv4, a binding cache needs to be implemented in each Mobile Node and Corresponding Node.

In this thesis, performance of Basic Mobile IP and Route Optimized Mobile IP (with smooth handoff and buffer support) are evaluated and compared by using the simulator NS2. Buffer and smooth handoff methods implemented in NS2 to analyze the end-to-end average delay, packet loss and throughput at Route Optimized Mobile IP and finally compared with Basic Mobile IP.

MAY 2006 **Asst. Prof. Dr. Demir ÖNER** **Birol ÇELİK**

ABBREVIATIONS

ARP : Address Resolution Protocol
AODV : Ad-Hoc on Demand Distance Vector Routing
BU : Binding Update
BW : Binding Warning
CBR : Constant Bit Rate
CN : Correspondent Node
DHCP : Dynamic Host Configuration Protocol
DSDV : Destination Sequenced Distance Vector Routing
DSR : Dynamic Source Routing
DVMRP : Distance Vector Multicast Routing Protocol
FA : Foreign Agent
FTP : File Transfer Protocol
GRE : Generic Routing Encapsulation
HA : Home Agent
HO : Handoff
IETF : Internet Engineering Task Force
IP : Internet Protocol
IPv4 : IP version 4
IPv6 : IP version 6
ISI/USC : Information Sciences Institute of University of Southern California
MAC : Media Access Control
MIP : Mobile Internet Protocol
MIPv4 : Mobile IP version 4
MIPv6 : Mobile IP version 6
MN : Mobile Node
NAM : Network Animator
NOAH : No Ad-Hoc Routing Protocol

NS2 : Network Simulator Second Series

OTCL : Object Tool Command Language Extensions

PARC : (Xerox) Palo Alto Research Center

PFA : Previous Foreign Agent

PIM : Protocol Independent Multicast

QOS : Quality of Service

RED : Random Early Detection

ROMIP : Route Optimized Mobile Internet Protocol

RTP : Real Time Transport Protocol

RTCP : Real Time Transport Control Protocol

SRM : Scalable Reliable Multicast

TCL : Tool Command Language

TCP : Transport Control Protocol

TORA : Temporally-Ordered Routing Algorithm

UDP : User Datagram Protocol

LIST OF FIGURES

TABLES

PART I

INTRODUCTION AND OBJECTIVES

I.1. INTRODUCTION

During the last several years, IP is becoming the dominant network protocol. With the popular use of mobile devices, the desire for mobile access to the Internet is increasing. An important area of IP research is the mobile wireless networking. There are currently two variations of mobile wireless networks. The first type of mobile wireless network is known as an infrastructure network that is a network with fixed and wired gateways. Typical applications of this type of network include wireless local area networks (WLANs). The second type of wireless network, which lacks an underlying infrastructure mobile network, is commonly known as a mobile ad-hoc network (MANET).

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 by indicating its IP address. On the other hand, a mobile node must be able to communicate even if it changes its point of attachment. The problem was resulted by assigning two IP addresses to mobile node, one of them is called the home address, and the other is the Care-of Address. The Internet Engineering Task Force (IETF) named this protocol as the "mobile IP" that is the proposed standard for IP mobility support.

The standard defines three entities: mobile node, home agent, and foreign agent (see Appendix A). Each mobile node has a permanent IP address assigned by its home network, which is called home address. Once the mobile node decides to move away from its home network, the new location of the mobile node is determined by the care-of-address, which is a temporary IP address assigned by the foreign network. In addition to the addressing procedures, the standard offers a mobility binding method used by the mobile node, the home and foreign agents. The way IP packets are routed from the correspondent node towards the mobile node is through tunneling of the packets by the home agent to the care-of-address, bound by the mobile node. Once the packet arrives to the destination, the foreign agent decapsulates information and forwards it to the mobile node. Routing the packets to the mobile node via its home agent known as "Triangle Routing", forces packets destined for the mobile node to route along non-optimized paths.

Internet applications such as browsing, e-mailing, and audio/video streaming, currently common in wired networks, will be demanded in this mobile environment. As a result, performance of mobile IP is becoming very important and needed more improvement. Average end-to-end delay, packet losses, and throughput are important criteria's to provide continuous connectivity, responsiveness, and steady throughput.

Route optimization is the most important research on solution for optimization of mobile IP. Route optimization enables the datagrams to be routed directly in both directions between MN (mobile node) and CN (Correspondent Node). Route optimization also provides support for smooth handoffs by letting the previous foreign agent tunnel datagrams to mobile node's current location. Despite the advantages provided by route optimization, route optimized mobile IP requires changes to existing Internet nodes and routers.

In Part II of this thesis, mobile IP and ROMIP (Route Optimized Mobile IP) were overviewed. In Part III, performance criteria of the Network Simulator (NS 2), and the implementation of the simulation were explained. In Part IV, evaluation of the simulation results were presented and in Part V, the conclusion is stated.

I.2. OBJECTIVES

The objective of this thesis is to evaluate and compare the performances of basic mobile IP and ROMIP by using the NS 2 simulator and making necessary additions and modifications on the NS 2.

I.3. LITERATURE SURVEY

Various research groups have studied the problems described above for the basic mobile IP.

The Transmission Control Protocol (TCP) is a predominant protocol in the Internet service. The TCP/IP protocol was originally designed for Internet without mobility in mind. With the increase of mobility demands, it is important to understand how TCP performance is affected by various existing mobility protocols, which can in turn help design new protocols or pursue improvements. Mobile IPv4 (Perkins) [4] is a popular mobility protocol used in the current IP4 networks.

Mobile IP has progressed for standardization within the Internet Engineering Task Force (IETF), and its specification is now available as Request for Comments (RFC) 2002 [4]. Related specifications are available as RFCs 2003–2006.

Mobile IP has been designed within the IETF to serve the needs of the growing population of mobile computer users who wish to connect to the Internet and maintain communications as they move from place to place. The basic protocol is described, with details given on the three major component protocols: Agent Advertisement, Registration, and Tunneling [3][4][5][6][24].

David B. Johnson [23] analyzed the mobile IP problem, reviewed the current state of Mobile IP, and discussed its scalability to very large numbers of mobile nodes in a large internetwork. Charles E. Perkins [24] analyzes further strategies of mobile IP, such as route optimization, smooth handoff, and security.

IETF proposed extension part of the basic mobile IP, called Route Optimization [18][20]. Charles E. Perkins [2] analyzed and simulated further strategies for improving route optimizing especially handoff system by using buffering at foreign agent and results show substantial performance improvements in terms of throughput, registration overhead, lost and duplicate packets during a handoff without restrictions on physical placement of foreign agents. Then Hao (Leo) Chen [20] analyzed the route optimization performance with simulation. He founds that the Route Optimization successfully eliminated the effect of Triangle routing and improved the network efficiency by lowering down the end-to-end packet delay.

A fast and efficient handoff scheme [9] was a good project to handle the movements of mobile nodes. Cheng Lin Tan, Stephen Pink and Kin Mun Lye adopted hierarchical mobility management architecture to restrict the handoff process overheads within the vicinity of the mobile node, and used multicast as the packet forwarding mechanism to deliver packets to multiple base stations within the vicinity of the mobile node to achieve fast handoff performance.

Hierarchical foreign agent (FA) management can reduce the registration overhead due to frequent local handoffs [8]. Route optimization has been proposed to eliminate the triangle routing problem. The major disadvantage of this scheme is that changes are required in all of the correspondent nodes.

Speed could have a negative effect on mobility, especially the performance of ad-hoc routing protocols. Holland [26] simulated several ad-hoc scenarios and showed that the average throughput decreases at higher speeds. The results corresponded to a simulation performed in NS network simulator [25] focusing only on the performance of ad-hoc networks. Fladenmuller [27] analyzed the effect of Mobile-IP handoffs on the TCP protocol. In the paper "The effect of mobile IP handoffs on the performance of TCP" [27] states that mobile IP may be appropriate for the current applications, however its long handoff periods make it unsuitable for the future.

PART II

MOBILE IP

II.1. OVERVIEW

Mobile IP is an extension of IPv4, developed by the mobile IP Working Group of the Internet Engineering Task Force (IETF), which was expanded to manage and maintain IP traffic for mobile devices. The key feature of the mobile IP [24] design is that all required functionalities for processing and managing mobility information are embedded in well-defined entities, the Home Agent (HA), Foreign Agent (FA), and mobile node (MN). The current mobile IPv4 protocol is completely transparent to the transport and higher layers and does not require any changes to existing Internet nodes and routers.

The mobile IP protocol allows the MNs to retain their IP address regardless of their point of attachment to the network. This can be fulfilled by allowing the MN to use two IP addresses. The first one, called the home address, which is static, and mainly used to identify higher layer connections. The second IP address is the Care-of Address, which is the MN's new point of attachment with respect to the network topology. While the mobile node is roaming among different networks, the Care-of Address changes. In mobile IPv4, a router called Foreign Agent achieves the Care-of Address management.

The Mobile node receives data over its home network by using its home address. When the mobile node moves into a foreign region, it will need to obtain a new Care-of Address via the Foreign Agent. All foreign agents may be busy in the foreign network. In this case, the mobile node can also obtain a new Care-of address by contacting the Dynamic Host Configuration Protocol (DHCP) [RFC1541] without the help of any FA. This new Care-of Address, which is called co-located care-of address, will be registered by its Home Agent. The Home Agent (see Figure II-1) forwards packets to the mobile node's Care-of Address which is delivered by Corresponding Node. The delivery can take place only if the packet is redirected or tunneled such that the Care-of Address appears as the destination IP address. The Home Agent tunnels the packet to the Foreign Agent. After receiving the packet, the Foreign Agent will have to apply the reverse transformation to decapsulates it, such that the packet will appear to have the mobile node's home address as the destination IP address. After decapsulating, the Foreign Agent sends the packet to the mobile node. The IP packets sent by the mobile node are delivered by standard IP routing procedures, each to its destination (Figure II.1). When the mobile IP packets follow a route similar to the one viewed in Figure II.1, this type of routing is typically called Triangle Routing. This indirect routing delays the delivery of the datagrams to mobile nodes, and places an unnecessary burden on the networks and routers along their paths through the Internet.

Route Optimization allow better routing for mobile IP protocol, so that datagrams can be routed from a correspondent node (CN) to a mobile node (MN) without going to the home agent except the first packet.

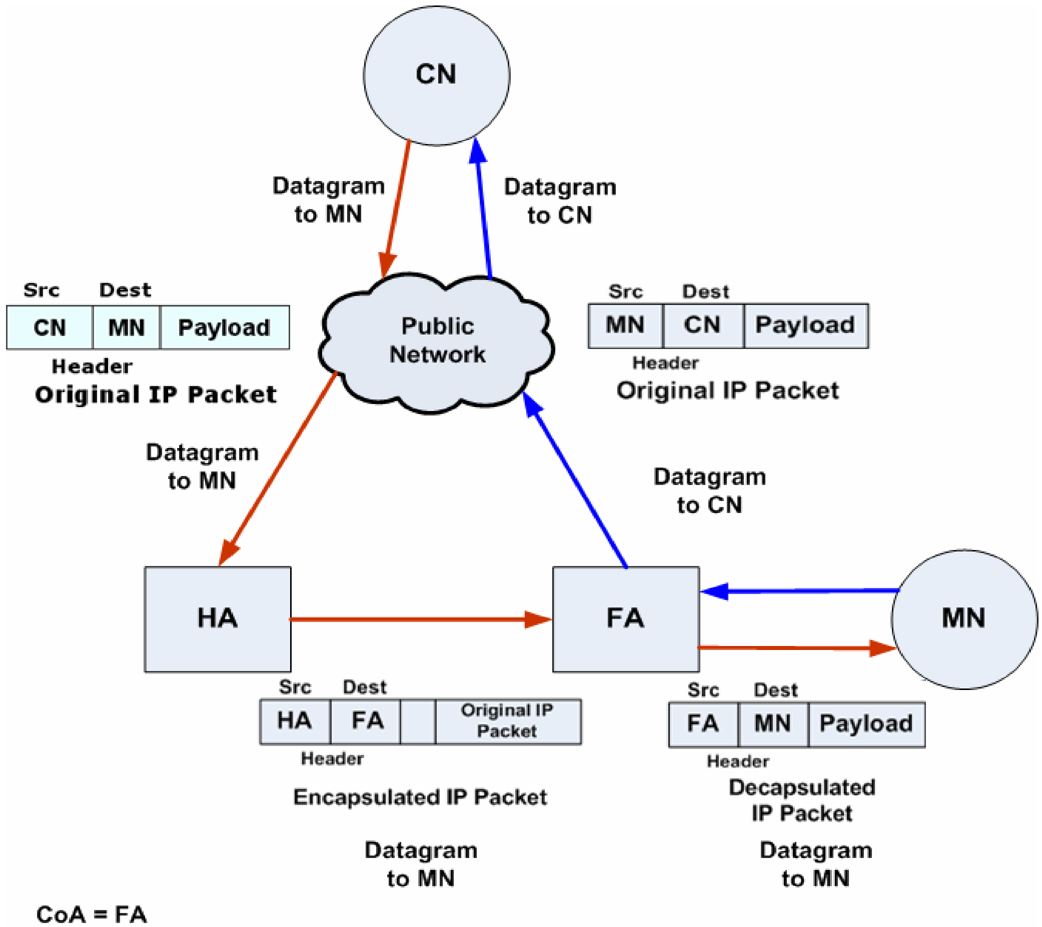


Figure II.1: Mobile IP packet flow

II.2. MOBILE IP PROTOCOL

Mobile IP includes these basic capabilities: discovery, registration, and tunneling.

II.2.1. Agent Discovery

A mobile node may move from one network to another due to the handoff performed by the physical layer, without the IP level being aware of it. This move is detected by the agent discovery process by using two methods; use of the lifetime method and network prefix. Agent Discovery process determines whether the mobile node it is currently connected to its home network or to a foreign network. Mobile IP agent discovery mechanism is based on the Internet Control Message Protocol (ICMP) router discovery mechanism described in RFC 1256 [14]. The mechanism uses two ICMP messages: Router Solicitation and Router Advertisement. The mobile IP extends ICMP router discovery mechanism. In the agent discovery [4] mechanism, mobility agent transmits agent advertisements to announce its services on a link. An agent advertisement is an ICMP router advertisement extended to carry a Mobility Agent Advertisement Extension [14] as shown Figure II.2 and in Appendix C.

Home agents and foreign agents periodically advertise their presence by multicasting agent advertisement messages on the network to which they are connected and for which they are configured to provide service. A Mobile node listens for the agent advertisement messages to determine which agent (home agent or foreign agent) it is connected to. If a mobile node receives an advertisement from its own home agent, it realizes that it has returned home and registers directly with its home agent. Otherwise, the mobile node chooses whether to retain its current registration or to register with a new foreign agent from among those it knows of. While at home or registered with a foreign agent, a mobile node expects to continue to receive periodic advertisements from its home agent or from its current foreign agent, respectively. When mobile node receives an agent advertisement from a foreign agent, it uses lifetime field and network prefix to detect movement. Mobile node uses lifetime field as a timer, if the time expires before the mobile node receives another agent advertisement message from the agent, then mobile node assumes that it has lost contact with that agent. Mobile node also checks agent advertisement message whether it is at home or at a foreign network by using network prefix. If the mobile node realizes movement, it attempts registration with that agent. If there are no advertisement messages, the mobile node may multicast an agent solicitation message onto its current network, which should be answered by an agent advertisement message from each home agent or foreign agent on this network that receives the solicitation message.

The agent advertisement extension as shown in Figure II.2 contains information about the service provided by the mobility agent. Mobile nodes use these advertisements to determine their current point of attachment to the Internet. Mobile nodes transmit agent solicitations when only in the absence of agent advertisement messages and a care-of address has not been determined through a link layer protocol [16]. An agent solicitation is an ICMP router solicitation. A mobile node can continue to send out solicitations until a suitable foreign agent is detected. The node may send three initial solicitations at a maximum rate of one per second and follow a binary exponential back-off mechanism afterwards in order to reduce the solicitation rate and limit the overhead on the local link.

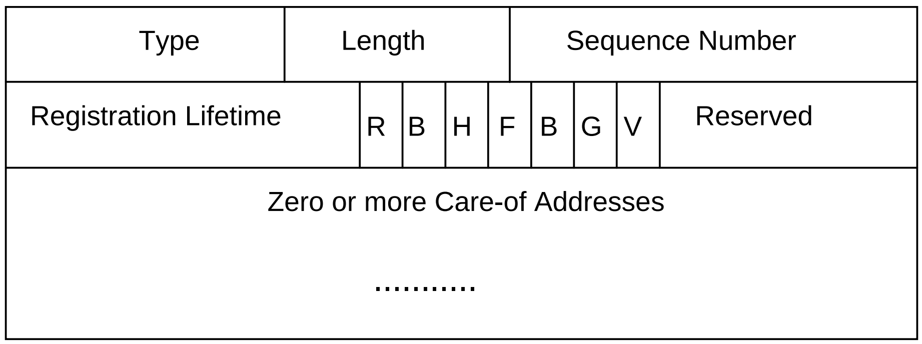


Figure II.2: Mobility Agent Advertisement Extension

A mobile node can distinguish an agent advertisement from other ICMP router advertisement messages by checking the IP total length field (in bytes) and the total number of advertised addresses. If the IP length field indicates that the message is actually longer than it should be, the rest of the bytes are considered as one or more extensions [16].

II.2.2. Registration

Mobile IP registration [4] provides a flexible mechanism for mobile nodes to communicate their current reachability information to their home agent. Registration messages exchange information among mobile nodes, a foreign agent, and the home agent. Registration creates or modifies a mobility binding table at the home agent seen in Table II.1 and at the foreign agent seen Table II.2, associating the mobile node's home address with its care-of address for the specified lifetime. A mobile node performs registration process in the following cases: (1) Upon visiting a foreign network, mobile node informs its home agent of its current care-of address. (2) Upon moving to a new foreign network, mobile node registers with the new care of address. (3) Upon returning to home, mobile node deregisters, that is informs its home network of its return to its home network.

Much of the basic IETF mobile IP protocol [4] deals with the issue of registration with a foreign agent and with a mobile node's home agent. Mobile IP defines a set of new control messages, sent with UDP [22]. Currently, the following two message types are defined: Registration Request, Registration Reply. The mobile node registration is shown in Figure II.3. When a mobile node visits a foreign agent to notify its care-of address to home agent, it sends a registration request message to the foreign agent (step 1 Figure II.3). The registration request includes the address of the mobile node and the address of its home agent which is listed in visitor list of foreign agent . The foreign agent forwards the request to the home agent (step 2 Figure II.3), which returns a registration reply message to the foreign agent (step 3 Figure II.3). Finally, the foreign agent forwards the registration reply message to the mobile node (step 4 Figure II.3). When a mobile node returns to home network, it makes registration request directly to its home agent.

Home Address	Care of Address	Life Time (sec.)
118.125.2.23	120.102.12.47	175
118.125.2.25	121.23.124.32	205

Table II.1 Mobility binding table at home agent

Home Address	Home Agent Address	Media Address	Life Time (sec.)
118.125.2.1	118.125.2.21	00-23-12-A2-FA-45	175
121.23.124.2	121.23.124.32	00-30-14-D0-B2-05	205

Table II.2 Mobility binding table (visitor) at foreign agent

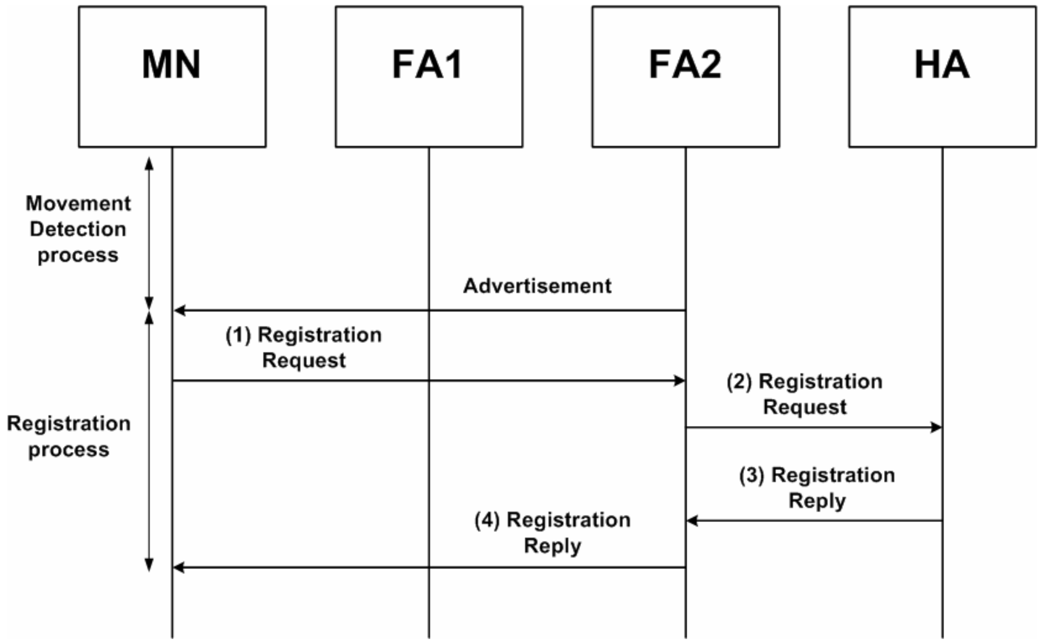


Figure II.3: Mobile IP registration phases

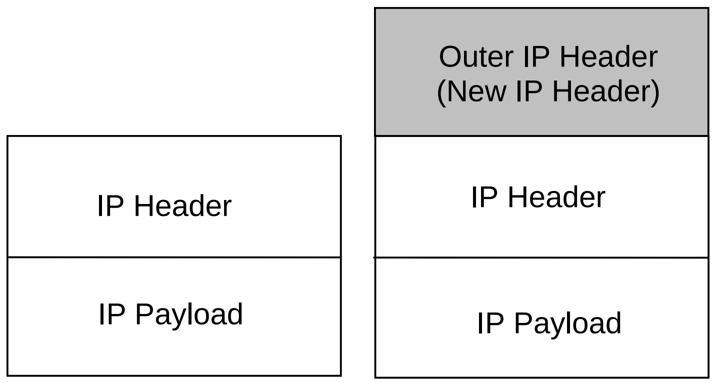
Each registration with a home agent or foreign agent has associated with it a lifetime period, negotiated during the registration. When this lifetime period expires, the mobile node's registration is deleted. In order to maintain continuous service from its home agent or foreign agent, the mobile node must re-register within this period. The lifetime period may be set to infinity, in which case no re-registration is necessary. When registering with its home agent on returning to its home network, a mobile node registers with a zero lifetime and deletes its current binding, since a mobile node needs no services of its home agent while at home.

All registrations with a mobile node's home agent must be authenticated in order to guard against fake registrations that could arbitrarily redirect future packets destined to a mobile node.

II.2.3. Tunneling

The home agent, after a successful registration, will begin to attract datagrams destined for the mobile node and tunnel each one to the mobile node's care-of address. One of several encapsulation algorithms can do the tunneling, but the default algorithm that must always be supported is simple IP-within-IP encapsulation, as described in RFC 2003 [3]. Other method is the minimal encapsulation method. Encapsulation is a very general technique used for many different reasons, including multicast, multi-protocol operations, authentication, privacy, defeating traffic analysis, and general policy routing.

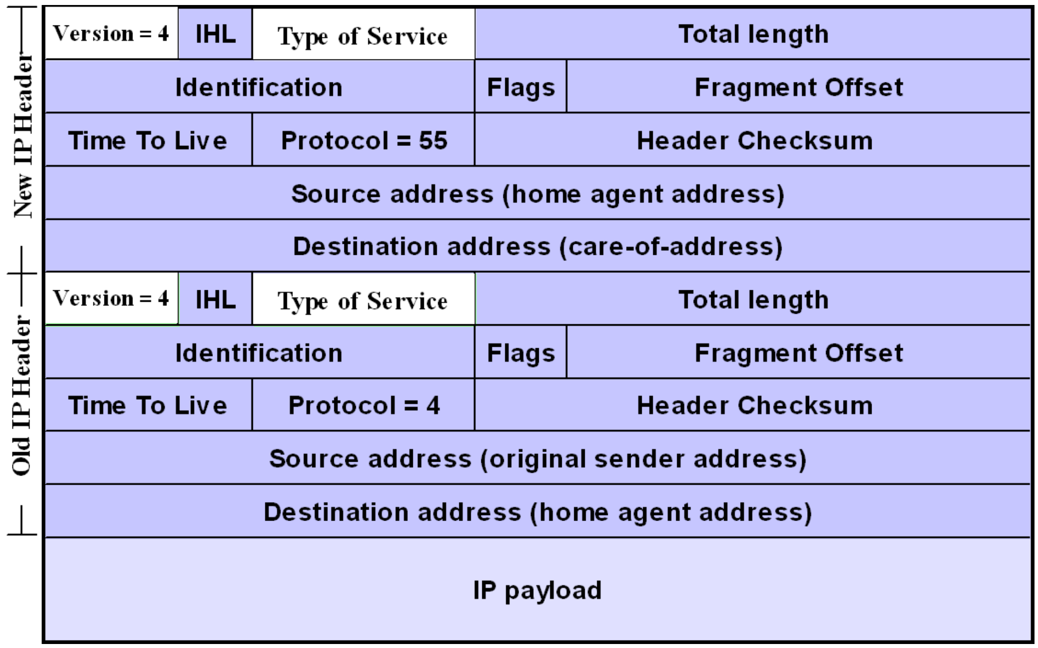
The protocol requires support for “IP within IP” encapsulation for tunneling is illustrated in Figure II.4. In this method, to tunnel an IP packet, a new IP header is wrapped around the existing packet; the source address in the new IP header is set to the address of the node tunneling the packet and the destination address is set to the mobile node’s care-of address. The new header added to the packet is shaded in gray in Figure II.4 [23].



(a) Original IP Packet (b) IP within IP encapsulated packet

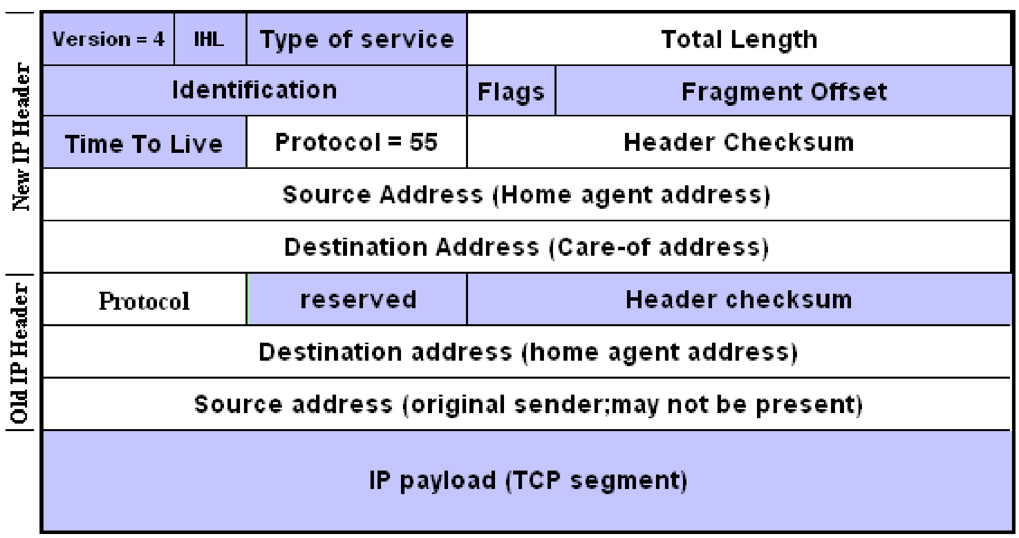
Figure II.4: Mobile IP Encapsulation

IP within IP encapsulation header and minimal encapsulation header are shown in figure II.5 a and b respectively. Minimal encapsulation method is only modifies the fields of the original IP header that are copied into a new forwarding header and adds to the packet between the original IP header and any transport-level header such as TCP or UDP. The fields in the original IP header are then replaced such that the source address is set to the address of the node tunneling the packet, and the destination address is set to the mobile node’s care-of address. This type of encapsulation adds less overhead to each packet, but it cannot be used with packets that have already been fragmented by IP, since the small forwarding header does not include the fields needed to represent that the original packet is a fragment rather than a whole IP packet.



*Unshaded fields are copied from the inner IP header.

(a). IP within IP header



*Unshaded fields in the inner IP header are copied from the original IP header.

*Unshaded fields in the outer IP header are modified from the original IP header.

(b). Minimal Encapsulation header

Figure II.5: Encapsulation headers

II.3. ROUTING

Mobile IP protocol employs asymmetric routing, where packets sent to a mobile node is routed via its Home Agent, and packets sent from a mobile node are directly routed through the Foreign Agent. This asymmetric routing or more generally known as “Triangle Routing”, forces packets destined for the mobile node to route along non-optimized paths.

Mobile IP protocol did provide transparent routing of IP datagrams for mobile devices; but the proposed routing algorithm was not optimized. IETF introduced an extension to the mobile IP protocol – Route Optimization [11]. Route Optimization solves the problem of “Triangle Routing” by maintaining binding caches in the nodes, so that packets can be routed directly to a mobile device.

II.3.1. Triangle Routing

Triangle routing is the basic routing scheme with mobile IPv4. In triangle, routing the mobile node sends its packets directly to the correspondent node. The correspondent node sends all datagrams to mobile node's home address. The home agent then tunnels them to mobile node's care-of address, as illustrated in Figure II.6. To preserve transport-layer connections mobile node uses its home address as the source address of all datagrams it sends.

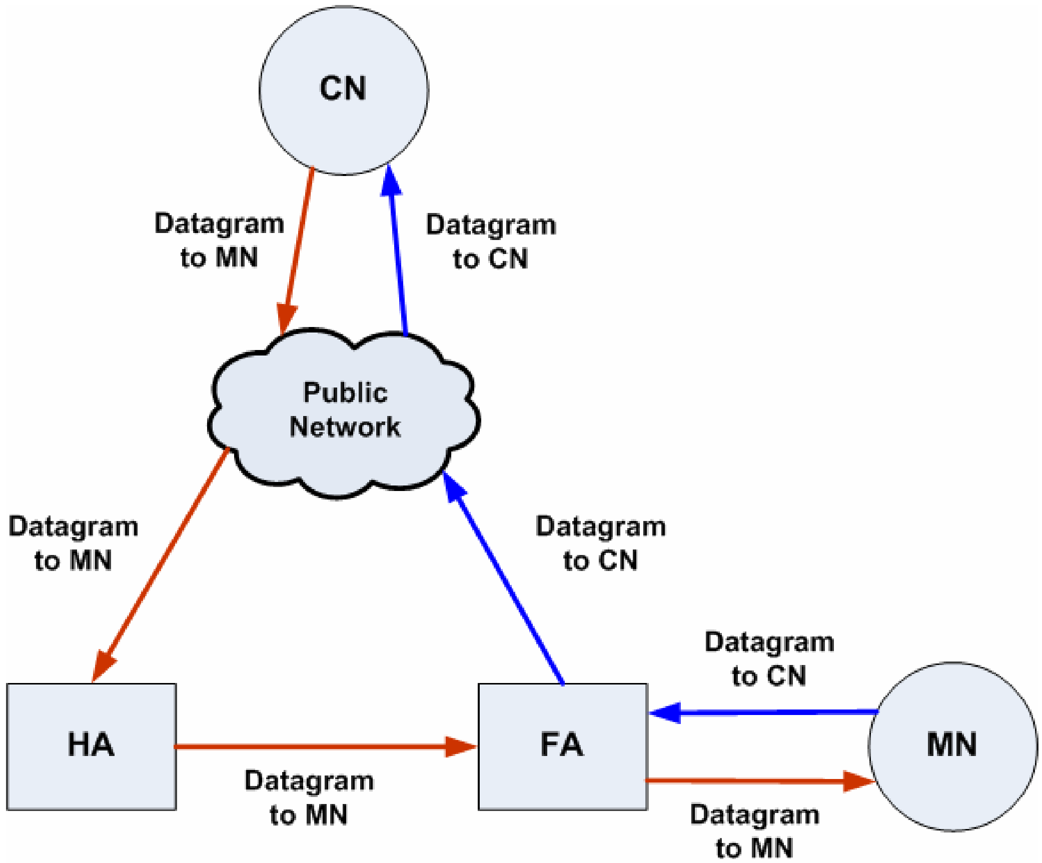


Figure II.6 Triangle Routing in mobile IP

II.3.2. Route Optimization

The basic IETF mobile IP [5] provides transparent packet routing to mobile nodes operating in the Internet. However, all packets for a mobile node away from home must be route optimization routed through the mobile node's home network and home agent (triangle routing). Triangle routing limits the performance of the protocol, creates a significant bottleneck, and does not account for handoff losses. Thus, in September 2001, the IETF introduced the Route Optimization extension to the mobile IP protocol. Route optimization developed to gain the ability for correspondent nodes to be able to cache the location of a mobile node and tunnel packets directly to the mobile node at its current location. A group consisting of Andrew Myles of Macquarie University, Charles Perkins of IBM has been working particularly to develop this functionality within the IETF [24].

Figure II.7 illustrates the operation of Route Optimization. The figure shows communication between CN and MN, when MN is in foreign network.

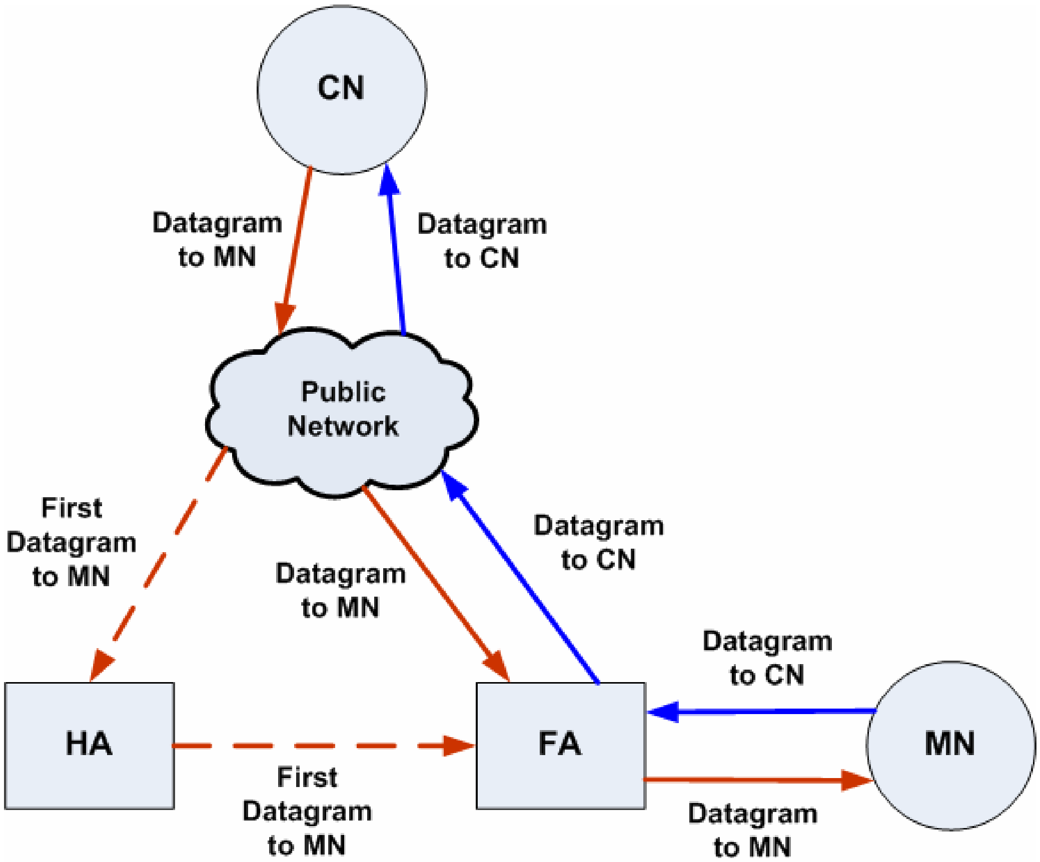


Figure II.7 Route optimization in Mobile IP

Route Optimization enables any node to maintain a binding cache containing the Care-Of Address (COA) of one or more mobile nodes. Binding cache is a cache of mobility bindings of mobile nodes, maintained by a node for use in tunneling datagrams to those mobile nodes. When a Corresponding Node is ready to send an IP datagram to an MN and has a binding cache entry for the destination MN, it can tunnel the datagram directly to the COA indicated in the cached mobility binding. When there is no binding cache entry, datagrams destined for an MN will be routed to the MN's home network and then tunneled to the MN's current COA by the MN's HA. This is the only routing mechanism supported by the basic mobile IP protocol. With Route Optimization, the original sender of the datagram will be informed of the MN's current mobility binding, giving the sender an opportunity to cache the binding. Any node may maintain a binding cache to optimize its own communication with MNs. CN can create a binding cache entry for an MN only when it receives the

MN's mobility binding update message. When a MN's HA intercepts a datagram from the CN and tunnels it to the MN, the HA decides that the CN has no binding cache entry for the destination MN. The HA then will send a Binding Update (mobile node's current mobility binding, and in particular it is Care-Of Address) message to the CN, informing it of the MN's current mobility binding. Upon receiving a Binding Update message from the HA of the MN, CN then can store a binding cache entry for the MN. Once CN has a binding cache entry for the MN, it will tunnel the datagram to the mobile node's Care-Of Address. A binding warning message informs the HA that the target node need a fresh binding for the mobile node as shown in Figure II.8. All binding update messages are sent by mobile node’s home agent, except the notification sent to a mobile node’s previous foreign agent.

When a mobile node moves to a new foreign network and registers with a new foreign agent, the basic mobile IP protocol does not notify the mobile node’s previous foreign agent that the node has left. After the mobile node registered with its home agent, IP packets intercepted by the home agent are tunneled to the mobile node’s new care-of address, but any packets in flight that had already been tunneled by the home agent to the old care-of address are lost and are assumed to be retransmitted by higher-level protocols if needed. The previous foreign agent eventually deletes the mobile node’s registration after the expiration of the lifetime period established when the mobile node registered with that foreign agent.

Route optimization extends the registration protocol to provide that mobile node’s previous foreign agent to be notified about the mobile node moved to a new foreign network and informs the mobile node’s new binding as illustrated in Figure II.9. When the mobile node moves to a foreign network and registers with a different care-of address, FA (FA2) notifies the previous foreign agent by sending a binding update message.

Hence packets in flight to this foreign agent, as well as packets tunneled from correspondent nodes with out-of-date binding cache entries for the mobile, are forwarded to the mobile node’s new care-of address.

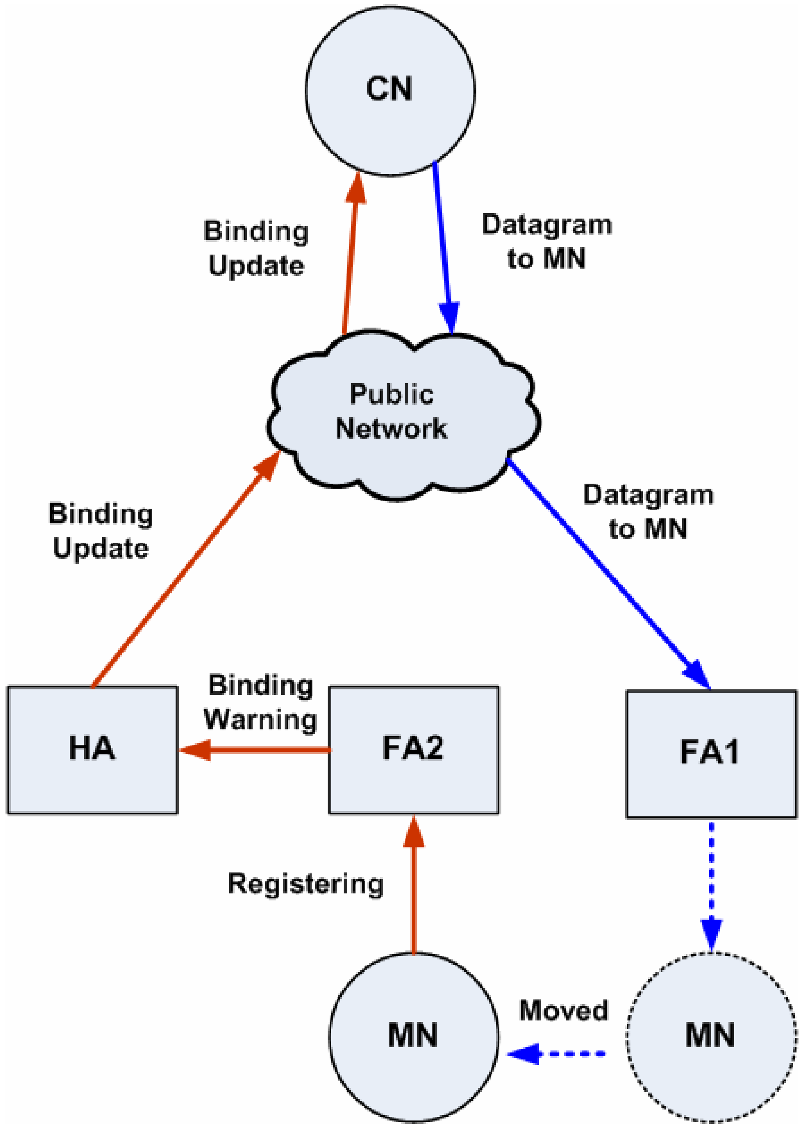


Figure II.8 Binding warning and Update.

After being notified of the mobile node's new binding, the previous foreign agent creates a binding cache entry for the mobile node, acting as a "forwarding pointer" to its new location. This notification also allows any datagrams buffered by the previous foreign agent to be released immediately. Such a "forwarding pointer" binding cache entry at a mobile node's previous foreign agent is treated in the same way as any other binding cache entry. When the previous foreign agent receives a packet that has been tunneled to this mobile node, but the previous foreign agent is unable to deliver the packet locally to the mobile node, the PFA buffers packets. After receiving binding update message, PFA tunnels these packets to the mobile node through new FA (FA2).

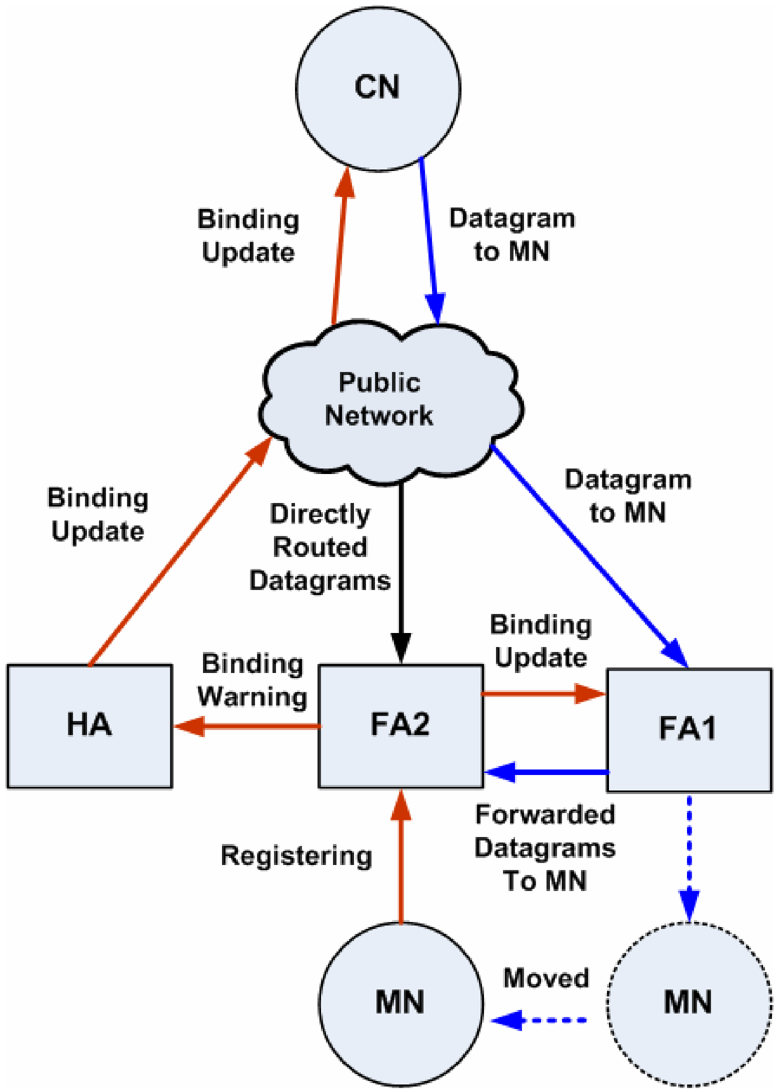


Figure II.9 Route optimization with smooth handoff

Mobile IP route optimization [18] extends the use of binding cache and binding update messages to provide smooth handoff. However, tunneled packets that arrive at the previous FA before it is notified of the new FA are lost. Such data loss may be increase if the MN looses contact with any FA for a relatively long period. Simulated smooth handoff scheme includes an additional foreign agent buffering mechanism. Besides decapsulating tunneled packets and delivering them directly to the MN, the FA buffers these packets. When it receives a previous foreign agent notification, it re-tunnels the buffered packets to the MN's new FA along with any future packets tunneled. Packet loss during a handoff can be completely eliminated, unless it takes too long time for MN to find a new FA after it loses contact with its previous FA. In that case, the buffer at the previous FA may overflow [2].

PART III

SIMULATION

III.1. PERFORMANCE CRITERIA FOR MOBILE IP

Major performance criteria's of mobile IP are packet delay, packet loss, and throughput. End-to-end throughput and delay are measures of data routing performance, and routing protocol effectiveness. Throughput is essentially a measure of the rate at which data is being transferred. However, throughput is affected directly from delay and packet loss. Basic mobile IP protocol performance problems are derived from triangle routing, and handoff.

Packet delay is defined as end-to-end delay for a packet sent from originating node (CN or MN) to arrive at the destination node (MN or CN) without error. But in triangle routing packets from the correspondent node travel to the home agent before being tunneled to the mobile node which affects end-to-end packet delay. This approach consumes many network resources, and degrades the performance of the mobile IP. The main components contributing to that delay normally include transmission delay, propagation delay between two end nodes, processing delay at each end node, and any queuing delays at intermediate routers. Average end-to-end packet delay is calculated by averaging all end-to-end packet delay samples over the total payload traffic exchange period.

Data is transmitted in packets, and packet loss is a measure of how many packets are lost during transportation. This includes packets, which are discarded, because they have arrived with transmission error.

Packets that are discarded or fail to arrive must be re-transmitted, and this quickly causes a "traffic jam" if the packet loss is severe.

III.2. THE NETWORK SIMULATOR NS 2

III.2.1. Overview

The NS Network Simulator is an event driven simulator for computer networks and network protocols. It was chosen as the simulation tool for this project because of its modular and open architecture. Since it is widely used in the research community, a large number of network components are available for NS. By reusing these components, the development of complex architectures can be considerably facilitated. Among others, NS supports the following technologies:

(1) Point-to-point connections, LANs, wireless links, satellite links

(2) Different queuing schemes (Drop Tail, Random Early-Detection etc.)

(3) IP, mobile IP

(4) Multicast (Distance Vector Multicast Routing Protocol, Protocol-Independent Multicast, etc.)

(5) TCP, UDP, and several experimental transport protocols

(6) Quality of Service (InterServ, DiffServ)

(7) Applications (Telnet, FTP, WWW-like traffic, etc.)

(8) Math support (random number generation, integrals, etc.)

(9) Network emulation

As shown in the simplified user's view of Figure III.1, NS is an Object-oriented Tcl (OTcl) script interpreter that has a simulation event scheduler and network component object libraries, and network set-up module libraries.

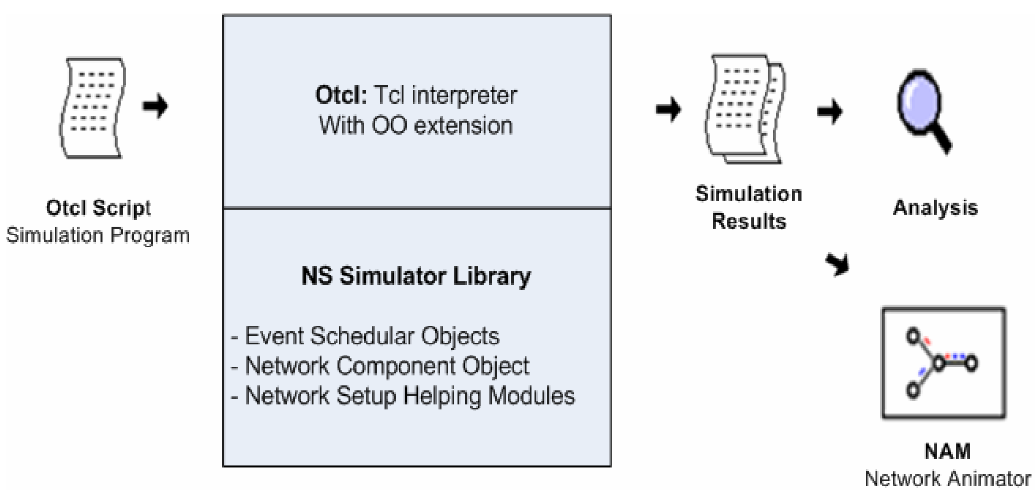


Figure III.1 Overview of Network Simulator

The current version of NS contains modules from several universities and research groups such as University Of California Berkeley, Sun, Xerox PARC, etc. The simulator framework uses a split-language programming approach. OTcl, an object oriented version of Tcl, is used for the control structure and the description of the simulation scenarios. Also the scheduling of events and the dynamic configuration of network components during the simulation is usually done in OTcl. The actual core of the simulator is written in C++ to allow for a fast simulation of large scenarios. While this approach is very flexible, it also adds complexity. To use the simulator it is necessary to have knowledge in OTcl as well as C++. Particularly debugging in both languages simultaneously can be a difficult task. Currently, no visual scenario generation tools exist for NS and scenarios are usually implemented by the user. However, simulation results can be visualized using the Network Animator NAM.

NS-2 has usages including:

(1). To evaluate the performance of existing network protocols.

(2). To evaluate new network protocols in design phase.

(3). To run large scale which are experiments not possible in real environment.

(4). To simulate a variety of IP networks

III.2.2. Support of Mobile IP and Wireless Communication

The original NS architecture only supported stationary nodes connected by wired links. Wireless nodes and channels were added at a later stage by a different research group which is contributed by both Carnegie Mellon University's Monarch group and SUN Microsystems Inc.. Monarch group extended the mobility support in NS-2 while SUN introduced the mobile IP into NS-2. These research groups focus on the simulation of wireless ad-hoc networks. However, since the original Carnegie Mellon University wireless model allows simulation of only wireless LANs and ad-hoc networks. The wired-cum-wireless feature was developed later in order to use the wireless model for simulations using both wired and wireless node. Also, SUN's mobile IP was integrated into the wireless model, although it was originally designed for wired nodes.

Their framework allows a very detailed modeling of wireless communication using Radio Propagation Models, Antennas, Link Layer, ARP, and MAC Layer protocols (e.g. IEEE 802.11), as well as ad-hoc routing protocols.

Special wireless nodes have to be used to compose wireless networks. These nodes have additional features in comparison to ordinary wired nodes. Nodes of a wireless network keep information about their location and they can move between locations with a specified speed. NS only supports linear movement of nodes. More complex movement patterns have to be constructed from linear segments. For wireless communication, the notion of links between nodes is no longer valid. To be able to send packets between mobile nodes, they have to be attached to the same channel in the NS. Packets sent over the channel are distributed to all nodes on the channel. Also, the internal structure of nodes was extended. While wired nodes hand packets directly to the corresponding agent which then processes the packets, packets at wireless nodes are passed through several additional layers.

A packet that is sent over a wireless channel is first handed to the Physical Layer (PHY). The Physical Layer uses a Radio Propagation Model (RPM) to determine the signal strength with which a packet is received. It then compares the signal strength with respect to a threshold to decide if the receiving node can detect the packet. If the signal is too weak, the packet is marked as “not received”. When the packet is detected, the signal strength is further compared to the receive threshold to determine whether the signal was strong enough to allow a correct interpretation or not. If the signal strength falls below that threshold, the packet is marked as “received with errors”. In any case, the packet is handed over to the Medium Access Control layer (MAC). The MAC layer discards packets when destination node could not be reached.

Since the wireless extension of NS was targeted at mobile ad-hoc networks, wireless nodes always have an ad-hoc routing agent attached. Currently, NS supports the following ad-hoc routing protocols:

(1) Destination Sequenced Distance Vector Routing (DSDV)

(2) Dynamic Source Routing (DSR)

(3) Ad-Hoc on Demand Distance Vector Routing (AODV)

(4) Temporally-Ordered Routing Algorithm (TORA)

III.2.3. Mobile IP Routing Protocols of NS

Ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. All nodes of Ad hoc networks behave as routers and take part in discovery and maintenance of routes to other nodes in the network. A number of routing protocols like Dynamic Source Routing (DSR), Ad Hoc On-Demand Distance Vector Routing (AODV), Destination-Sequenced Distance-Vector (DSDV) and Temporally Ordered Routing Algorithm (TORA) have been implemented for NS 2.

These ad-hoc routing protocols can be divided into two categories:

(1). Table-driven routing protocols

In table driven routing protocols, consistent and up-to-date routing information to all nodes is maintained at each node. DSDV is a table-driven routing protocol

(2). On-Demand routing protocols

In On-Demand routing protocols, the routes are created as and when required. When a source wants to send datagram to a destination, it invokes the route discovery mechanisms to find the path to the destination. TORA, DSR, AODV are the On-demand routing protocols.

The Destination-Sequenced Distance-Vector Routing Protocol was designed as an ad hoc protocol with a table-driven routing protocol. This is a hop by hop distance vector routing protocol requiring each node to periodically broadcast routing updates. The key advantage of DSDV is that it guarantees loop-freedom. If a node cannot access any base stations, the DSDV routing protocol allows a path along which data can be exchanged with all nodes. A sequence number is used with the basic Bellman–Ford algorithm to each routing table entry. When the network topology is modified less frequently less routing table data is exchanged.

TORA is a distributed routing protocol based on a “link reversal” algorithm. It is designed to discover routes on demand, provide multiple routes to a destination, establish routes quickly, and minimize communication overhead by localizing algorithmic reaction to topological changes when possible. Route optimality (shortest-path routing) is considered of secondary importance, and longer routes are often used to avoid the overhead of discovering newer routes.

Ad Hoc On-Demand Distance Vector Routing offers a pure distance-vector approach. It does not maintain a routing table. AODV is a purely ‘‘on demand’’ method that follows a route request and reply discovery cycle when the nodes communicate with other nodes. The AODV routing table will record a message with a destination sequence number (as with DSDV) to avoid a routing loop and produce the new routing topology.

The Dynamic Source Routing (DSR) protocol is an on-demand routing protocol based on the source routing concept. When mobile nodes request communications, the DSR protocol will search for a path. Mobile nodes are required to maintain routing table that contain the source routes of which the mobile node is aware. Entries in the route cache are continually updated as new routes are learned. The DSR protocol is similar to AODV and uses the source broadcast method as the DSR.

III.3. SIMULATION SCENERIO

III.3.1. Overview

To demonstrate the performance of Route Optimization protocol, all of the network simulator wireless protocols were analyzed that mentioned before, and then Dynamic Source Routing Protocol (DSR) ADHOC protocol was selected. Because DSR uses source routing and routes are stored in a route table (cache) which is suitable for implementing binding table and buffer support in NS 2. To use the network architecture of this thesis on the Network Simulator 2, new handoff mechanism and buffer support was added, Routing Agent, and mobile node modules were modified.

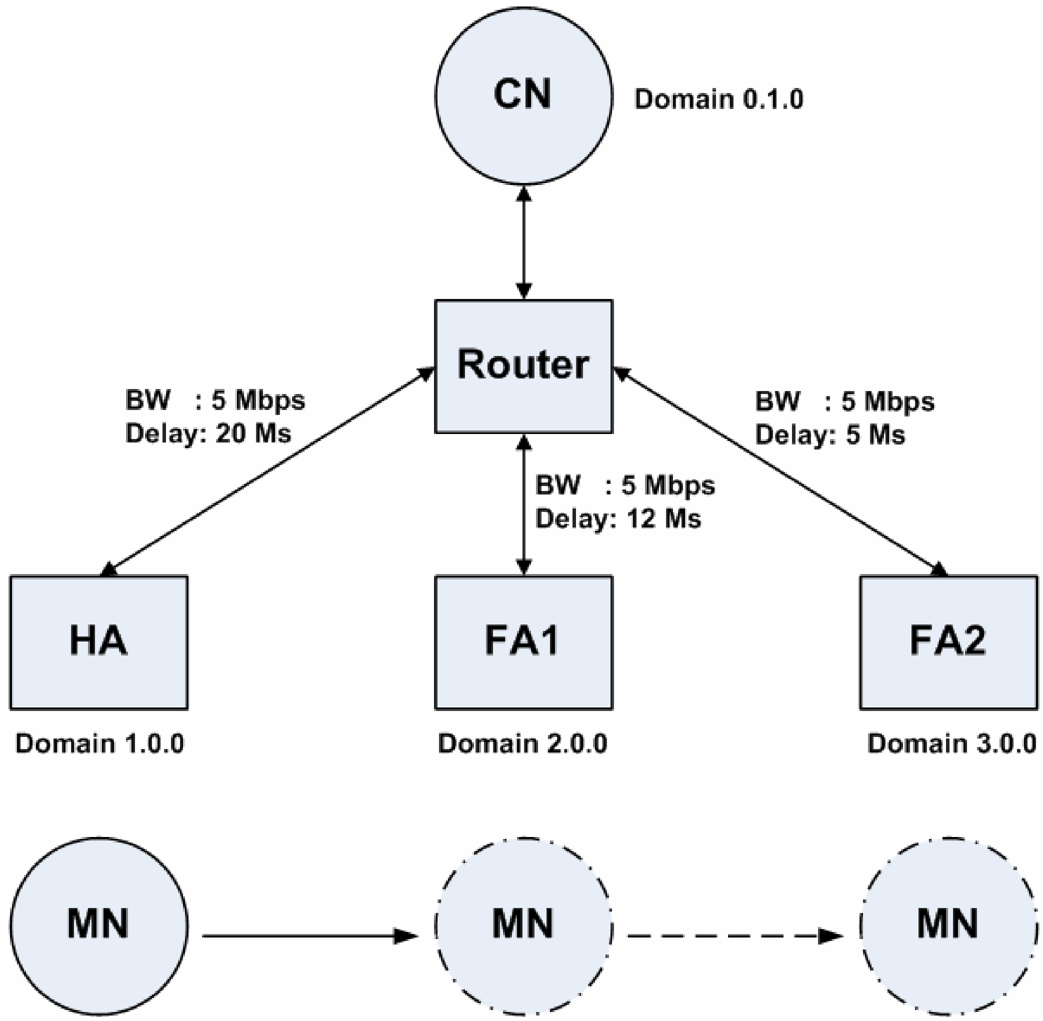


Figure III.2 Simulation Topology

The simulations were done both with route optimization and without route optimization in mobile IP for comparison.

Two scenarios are provided to illustrate performance of Route Optimization. The first scenario shows Basic mobile IP (without route optimization), and the second scenario shows the Route Optimization.

Two of the simulation scenarios as depicted in Figure III.2 consist of only one mobile node, one home agent, two foreign agents, one correspondent node, and one wired node. In the simulations, some important common simulation parameters are used as follows:

(1) Two Ray Ground Reflection Approximation Radio Propagation Model [appendix B] is used. This model uses free-space attenuation at near

distances and an approximation to Two Ray Ground at far distances [25]. The approximation assumes specular reflection off a flat ground plane.

(2) A unity gain omni-directional antenna, which is used in the simulation

(3) The network interface of the simulation implements a shared media model, which is subjected to collisions. The propagation model of each node can overhear packets transmitted by the others. The default parameters are taken to approximate the Lucent Wave LAN direct-sequence spread-spectrum (DSSS) radio interface.

(4) Data layer IEEE 802.11 is used which uses a "RTS/CTS/Data/ACK" pattern for unicast packets and a "Data" pattern for broadcast packets and uses both physical and virtual carrier sense.

(5) Radio Coverage : 75m

(6) Positions : HA:(200,200), FA: (350,300), FA2: (500,300), CN: (800,800)

(7) Movement of MN : (150,275) _ (560,275)

(8) Traffic Type : Constant Bit Rate

(9) Routing Protocol : DSR (Dynamic Source Routing)

(10) Link delay : CN __HA: 25 ms, CN __FA: 20 ms, CN __FA2: 20 ms

(11) Application : FTP

(12) Addressing : Hierarchical

(13) Simulation Time : 90 second

(14) Protocol : TCP

The Network Simulator of version of NS-2 2.29 is used. This is the latest compatible version with all the required modules.

The first scenario is implemented for basic mobile IP. In this scenario, the current mobile IP architecture in NS-2 is used. As shown Figure III.2 before, typical mobile IP scenario consists of Home Agents (HA), Foreign Agents (FA) and Mobile-Nodes (MN). HA and FA are the same kind of node (Base-Station Node) in the current NS-2 system, and they use the same Agent to handle the packets. Since the HA and FA play the role to interconnect the wired and wireless nodes, they are implemented as Hybrid nodes of both wired nodes and wireless nodes..

III.3.2. Basic Mobile IP Scenario

Basic mobile IP scenario is shown in Figure III.3 and is explained step by step as follow.

(1) If the MN is within the domain of its own home network (HA), the MN communicates with the CN through home agent by using the usual TCP/IP protocol stack.

(2) If the MN moves to the foreign network domain (FA1), during the registration phase, MN sends a REG REQUEST message through FA1 to the HA register with the new Care-Of Address (COA).

(a) When the HA receives the REG REQUEST message from the FA1, it calls an OTcl function "encap-route" to add a route which specifies a MIPEncapsulator to handle all the future packets destined to the MN with MN's home IP address.

(b) If the REG REQUEST message received by the HA specifies a COA which is the IP address of the HA, this means the MN has returned home. In this case the HA calls an OTcl function (clear-reg) to clear the registration information for this MN. Later communication between the MN and the CN will go through the usual routing path, as long as the MN stays in the range of its HA.

(3) After the MN registers its COA to its HA, all the packets destined to the MN will be encapsulated by the MIPEncapsulator of the HA to its new COA. This encapsulation process is called Tunneling. MIPEncapsulator is the internal object to perform the IP-within-IP encapsulation for the HA.

(4) When the FA receives the encapsulated IP packets, a MIPDecapsulator decapsulates the IP packets and extracts the original IP packets, and then delivers to the MN using the mobility agent.

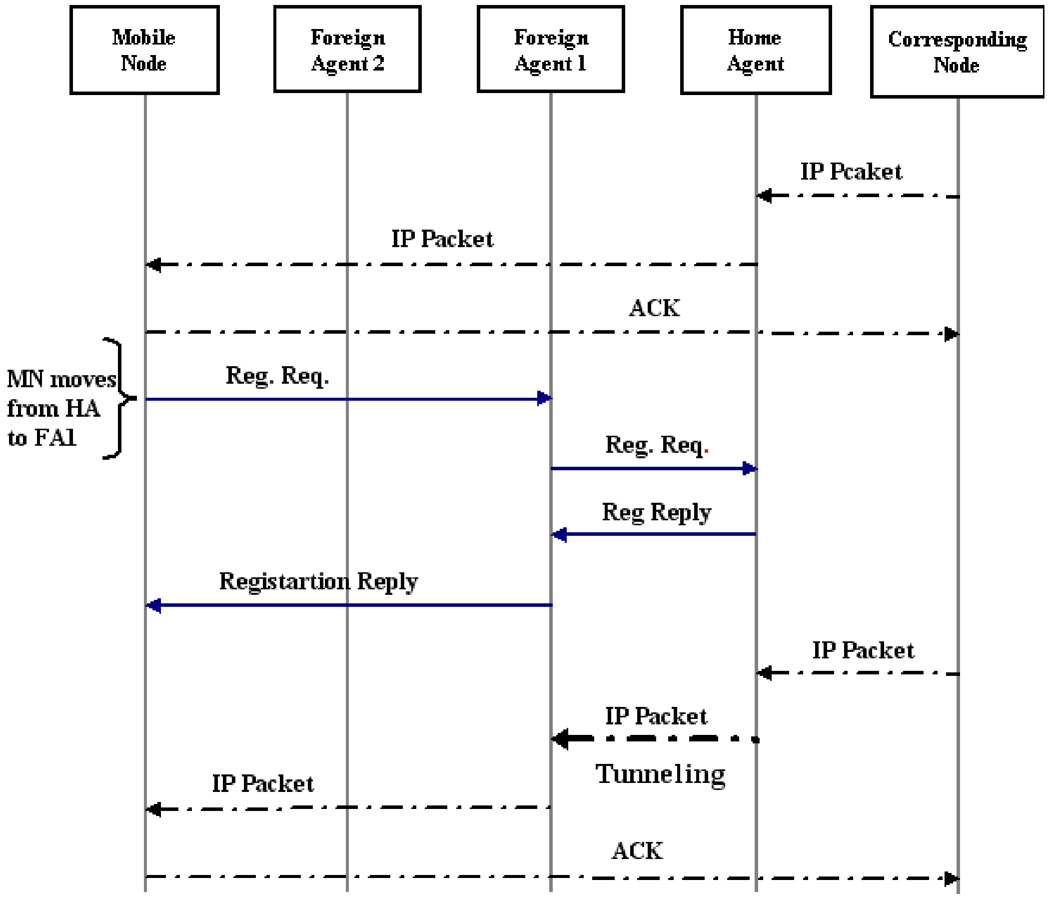


Figure III.3 Basic mobile IP Scenario diagram

III.3.3. Route Optimized Mobile IP Scenario

Binding Warning, Binding Update, and Smooth Handoff messages in route optimized mobile IP illustrated in Figure III.4.

In the first case, the MN is at FA1 and communicates with CN directly through FA1. When MN moves to another foreign network (FA2), MN sends registration request with previous foreign agent extension (PFA) to FA2. FA2 gets the address of the previous Foreign Agent (FA1) from the PFA extension of the registration request message sent by the MN. FA2 sends a binding update message to FA1. CN still sends packets to the old Care-Of Address of the MN that is to FA1, when FA1 update its binding table; it forwards these IP packets to MN. At the same time, FA2 sends a registration message to HA for MN. After receiving registration request, HA sends registration reply to MN through FA2. MN sends the Binding Warning message to HA requesting HA to send out Binding Update message to the CN. Then, the CN can correctly communicate with the MN directly through FA2 after receiving the Binding Update message.

In the second case, if handoff is occurred and if the previous FA (FA1) is not informed about the movement of MN to a new FA (FA2), then it will be impossible for the CN to communicate with the MN over the new FA (FA2) until the new COA is registered to HA. Meanwhile, the CN will try to communicate with old FA. Consequently, packet loss will occurred because all datagrams sent to the old FA will be discarded since they are not buffered. When the MN requests FA2 to notify the previous foreign agent that the mobile node has moved, this allows the packets in flight to this FA (FA1), as well as the packets tunneled from CN to be forwarded to the mobile node's new care-of address (FA2). So, this scenario illustrates Smooth Handoff method which includes the Binding Warning, Binding Update messages.

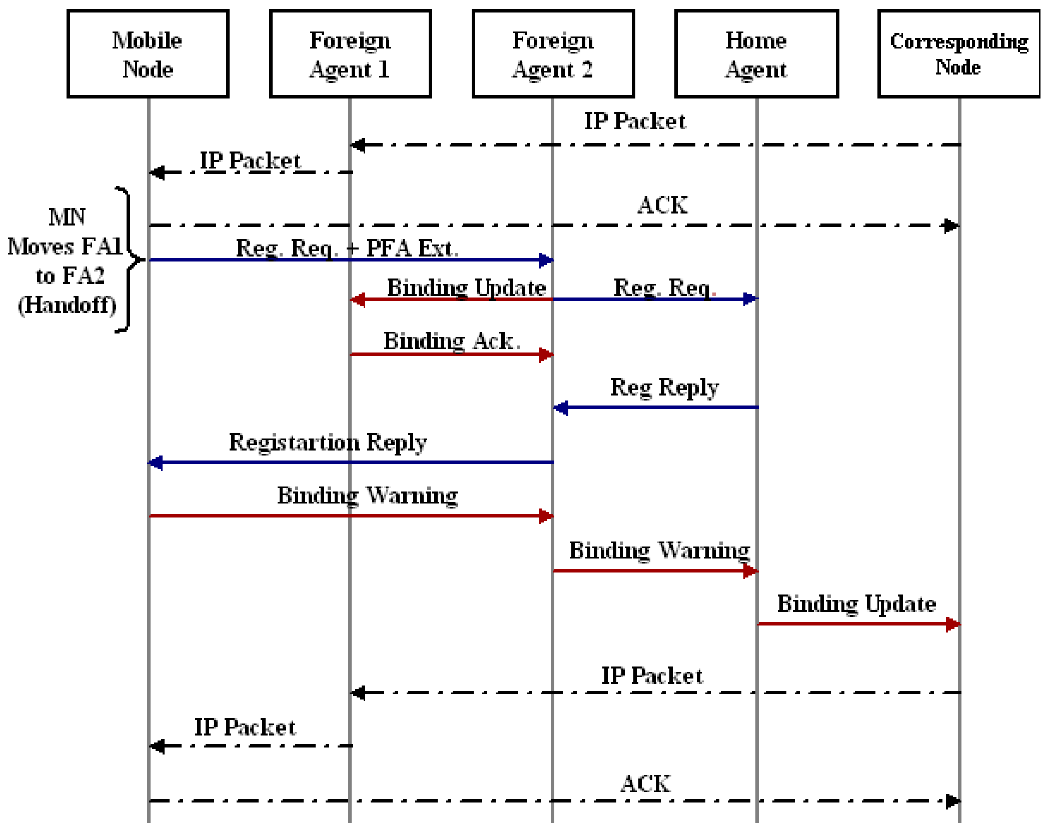


Figure III.4 Route Optimized Mobile IP scenario diagram

III.4. IMPLEMENTATION OF SIMULATION

To simulate the mobile network architecture of this project, two scenarios are generated and modifications are made on the NS2 Network Simulator. The following modules were modified: smooth handoff and buffer support was added to agent module, new analyzer implemented for post processing.

III.4.1. Contribution

Hao (Leo) Chen [20] "Route Optimization on mobile IP over IPv4" project and simulation in NS-2.1b8 is analyzed. In this simulation, and binding warning and binding update messages were implemented and average end-to-end delay were examined. This simulation was successfully implemented in NS-2.29 version, which has fewer bugs and is more stable compared to previous versions. Firstly, binding warning and binding update messages successfully adapted to NS-2.29 version and the new wireless trace feature is enabled to perform post-process data analysis on the trace file properly.

In this thesis, the Smooth Handoff feature was successfully implemented. Comparing the performance of the protocol with and without this feature, it is shown that Smooth Handoff does reduce packet loss when the mobile node moves from one foreign network to another. To reduce packet loss during handoff, a buffer mechanism is implemented at the mobility agents. The mobility agents (FA and HA) start to buffer the received packets when it detects weak signal on the link, and it forwards these buffered packets to the care of address. Smooth Handoff is not triggered if the previous mobility agent is the Home Agent.

III.4.2. Route Optimization

This section illustrates the Route Optimization when a mobile node moves away from its home network to a Foreign Agent network. To facilitate the design of Route Optimization, detailed flow charts are drawn to illustrate the high-level processing requirements of each message in the protocol (see Figures III.5 and III.6). The following section provides designs and overviews of the following messages: Binding Update, Binding Warning, and Previous Foreign Agent Extension.

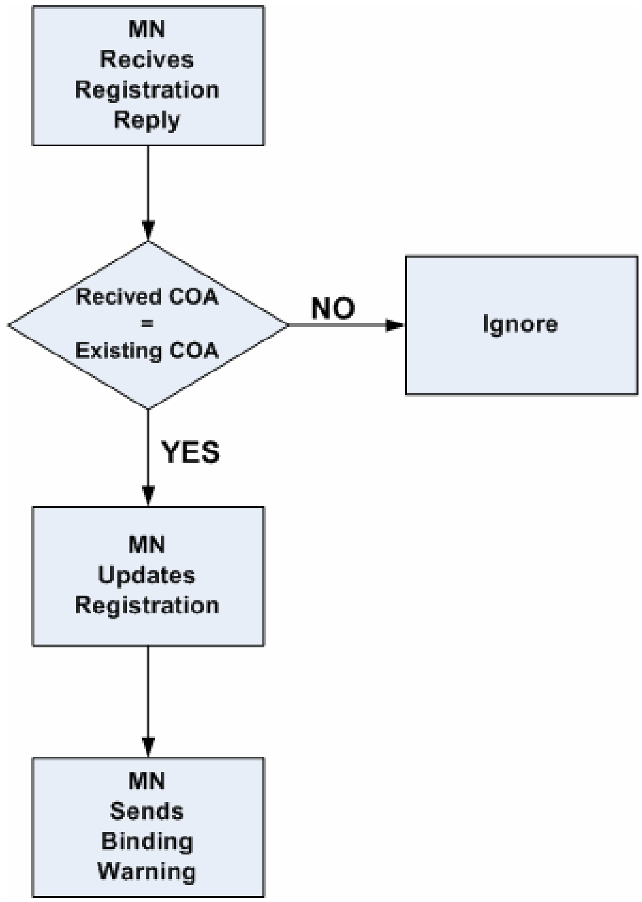


Figure III.5 Flowchart of sending Binding Warning Message by the MN

Upon receiving registration reply from HA, the mobile node generates a Binding Warning to the Home Agent as illustrated in the Figure III.4 and III.5. In response, the Home Agent sends a Binding Update to the CN to modify the binding cache for the mobile node.

If a new Care-of-Address is not received, a Binding Update is not required since the mobile node did not move to another foreign network.

The Home Agent or the Foreign Agent can generate the Binding Update message. The Home Agent generates the Binding Update message in response to a Binding Request or Binding Warning message. The Foreign Agent generates a Binding Update message to the previous Foreign Agent when a Previous Foreign Agent extension is received.

If the Correspondent Node receives the Binding Update, the Correspondent Node must store the new Care-of-Address in its binding cache.

If the Previous Foreign Agent receives the Binding Update, then this Binding Update is part of the Smooth Handoff process. Using the new Care-of-Address extracted from the message, the previous Foreign Agent updates its binding cache to redirect datagrams to the new Care-of-Address.

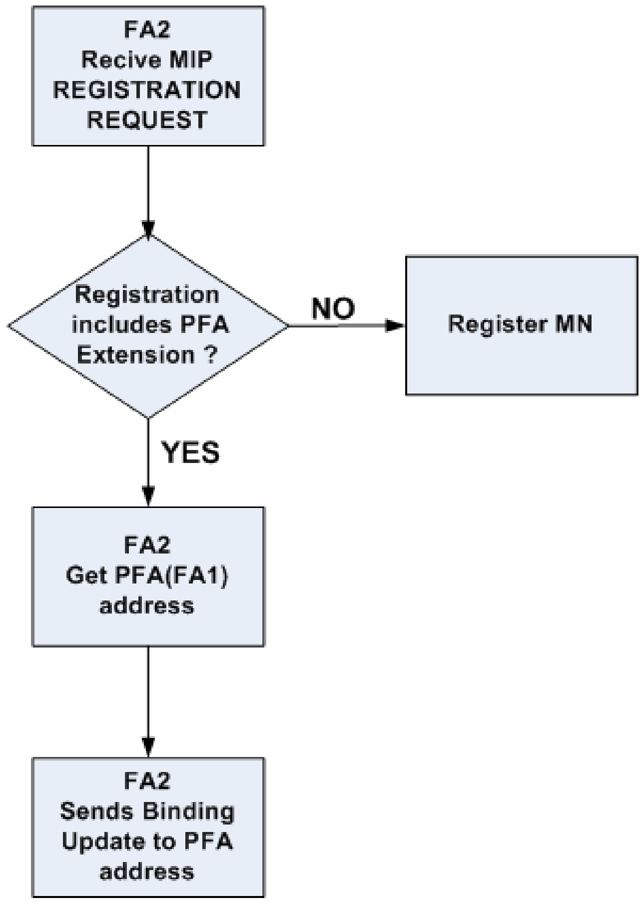


Figure III.6 Flowchart of sending Previous Agent Extension Message

Upon receiving a new Care-of-Address, the mobile node checks whether its previously visited network is the home network. If the previous network is the home network, then Smooth Handoff is not required since the Home Agent knows the new Care-of-Address for the mobile node. If, however, the previous network is a foreign network, then Smooth Handoff is triggered. Smooth handoff is initiated when the mobile node appends a previous Foreign Agent extension to the Registration Request. This extension contains the IP address of the previous Foreign Agent.

III.4.3. Additions and Modifications Made on the Network Simulator (NS-2)

After examining the mobile IP and Route Optimization in NS-2 in detail, following modification and new methods, message formats and buffering mechanism added to the simulator. Both the C++ and the Tcl source code are modified to support the full Route Optimization protocol. The following is a summary of the source code modification.

MIP.H FILE

(1) A new function is added to generate previous Foreign Agent extension.

(2) A new function is added to generate previous Foreign Agent extension control messages.

(3) A new method is added to MIPT_PFA_REGUEST, MIPT_PFA_OK requests to send previous agent extension during handoff.

(4) Instance variable PFA_ TO MIPMHAGENT is added to decide previous foreign extension will be sent.

(5) A new logging interface is added to effectively print debug messages.

MIP-REG.CC FILE

(1) MIPBSAgent::recv function is modified to handle MIPT_PFA_REGUEST request.

(2) MIPMHAgent::recv function is modified to handle MIPT_PFA_OK request.

(3) A new method regPfa() is added to send previous foreign agent message.

DSDV.CC FILE

(1) DSDV_Agent::lost_link method is modified not to drop packets during handoff.

(2) DSDV_Agent::forwardPacket method is modified to buffer dropped packets during handoff.

(3) DSDV_Agent::routeUpdate method is modified to send buffered packets after handoff.

PART IV

EVALUATIONS OF THE RESULTS

The simulation result of the end-to-end packet delay is shown in Figure IV-1. X-axis is the time axis, Y-axis is the end-to-end packet delay, units of the both X and Y-axis are second. Figure IV.1 gives the comparison of the performance of Basic mobile IP protocol against the completed Route Optimization protocol.

In Figure IV.1 red line represents the end-to-end delay with Basic mobile IP protocol, green graph represents the end-to-end delay with Route Optimization, blue line represents the average end-to-end delay with Basic mobile IP protocol, and yellow line represents the average end-to-end delay with Route Optimization. The average end-to-end delay curve for Route Optimization is mostly lower than Basic mobile IP protocol. In order to reduce data loss during a handoff, added a buffering mechanism is added to the mobile agents. FAs buffer data packets when the link between mobile agent and MN lost and then forwards these packets to MN. This increases packet delay since data is kept in buffer until the link is established to the current FA. Also in the handoff phase, the MN includes a registration request with previous extension to the new FA. The new FA (FA2) sends binding update message to the previous FA (FA1) to forward packets to the new location. Packets waiting in buffer queue, increases delay but decreases the packet loss. Therefore, ROMIP without buffer has a low delay than buffered Route Optimized scheme and this introduces an additional delay but prevents packet loss due to handoff.

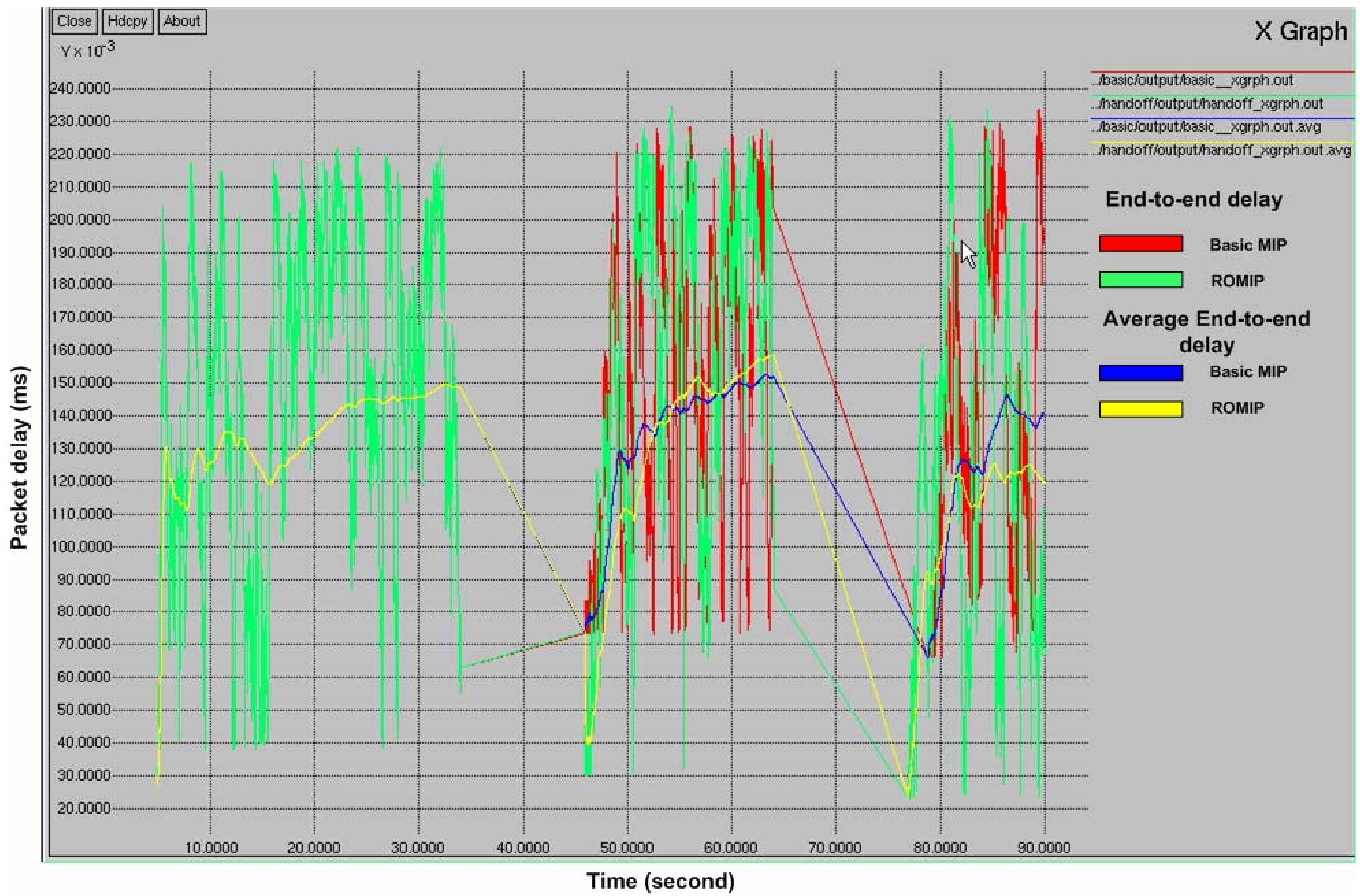


Figure IV.1 Average end-to-end packet delay for basic Mobile IP protocol and for buffered Route Optimization protocol.

In the same scenario as above packet loss of Route Optimization and Simple mobile IP illustrated in Figure IV.2. which shows the comparison of packet loss in case of basic mobile IP and ROMIP with smooth handoff and buffer. Red line represents the packet loss of Basic mobile IP protocol, and green line represents the packet loss with Route Optimization. On the Y-axis represents packet loss in bytes while X-axis represents the time in seconds. The packet loss is calculated based on the accumulated packet loss for a 1-second window.

In Figure IV.2, green lines show that ROMIP has only very small amount of loss packets. The red lines show that Basic mobile IP has a constant average of loss packets, out of handoff period and has a large amount of loss packets at handoff periods. It is seen from Figure IV.2 that MN has been at HA between 0 to 36 seconds and has a constant loss in Basic mobile IP but no loss at ROMIP scenario. When MN moves from HA to FA1 (first handoff) between 36 to 42 seconds and Basic mobile IP has a big amount of packet loss but ROMIP has not any loss. It is the same at FA1 between 42 to 72 seconds. However, at the second handoff between 66 to 72 seconds ROMIP has a very small loss compared to Basic mobile IP.

If increasing loss packets are examined on the graph it is seen that packet loss increases at handoff periods. But Basic mobile IP has some lost packets out of handoff periods. Where as in buffered ROMIP method packet loss is prevented.

As a result of the improvement in packet loss in smooth handoff simulation, also the throughput is improved compared to basic mobile IP. Figure IV.3 clearly shows that especially during the first handoff period between 34 and 46 seconds, and second handoff period that occurs between 64 and 76 seconds, throughput is clearly better and handoff period is shorter.

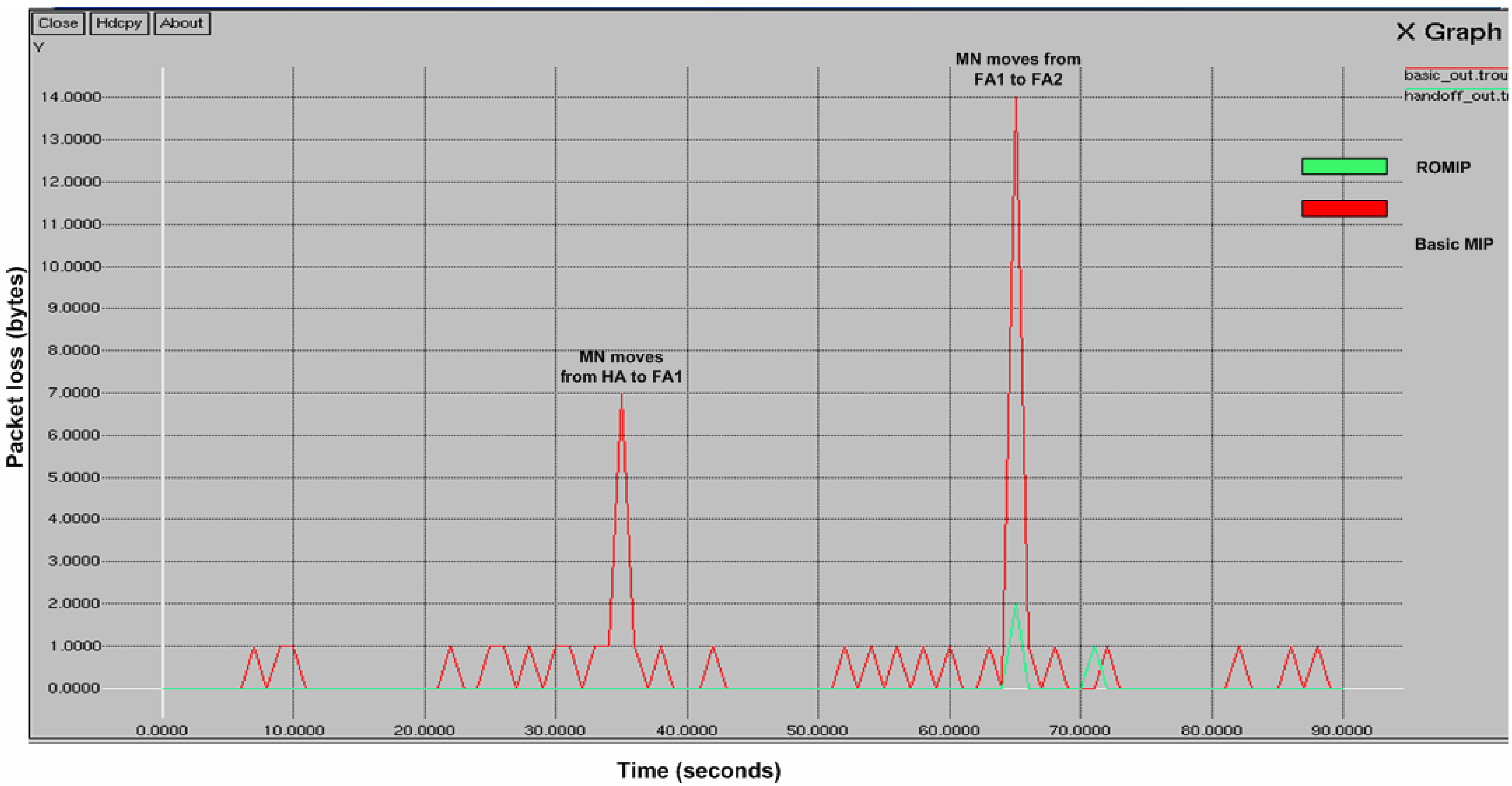


Figure IV.2 Comparison for packet loss of the basic Mobile IP protocol and that for buffered Route Optimization protocol during handoff.

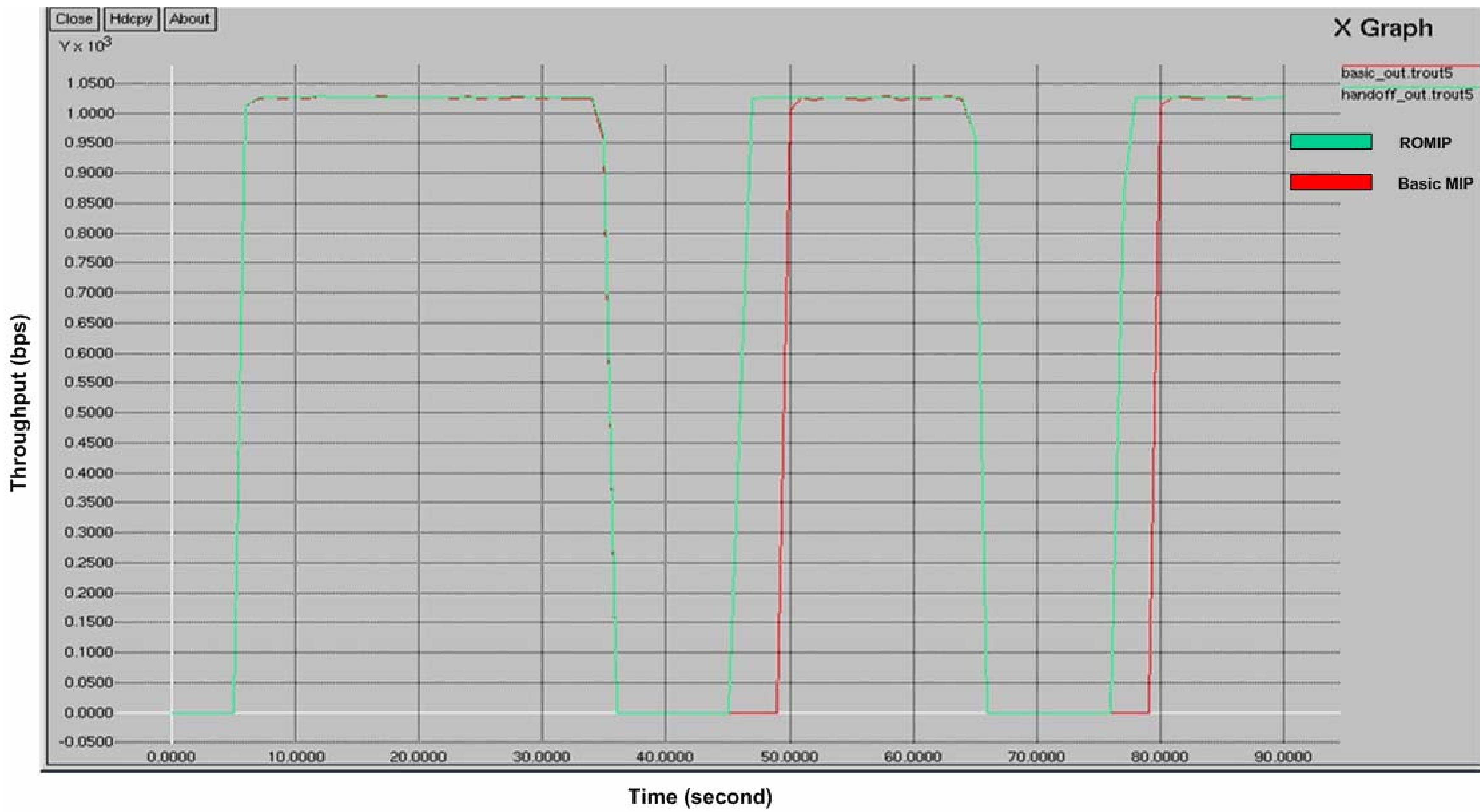


Figure IV.3 Throughput for the basic Mobile IP protocol with the buffered Route Optimization protocol.

PART V

CONCLUSIONS

In Triangle routing, home agent is a forwarding point for every IP packet, even if a shorter routing path is available between source and destination. This causes unnecessarily long end-to-end packet delay, more packets lost and less throughput. Route optimization eliminates delay, but does not solve packet loss during handoff period. Smooth handoff and buffer support eliminates this disadvantage of Route Optimization.

In this thesis, an overview and a comparison of basic mobile IP and Route optimized mobile IP (ROMIP) is presented and simulations for the two protocols were successfully implemented.

Accomplishments:

Literature survey has been made about simulations for performance analysis of mobile IP examined. Leo CHEN "Route Optimization on Mobile IP over IPv4" [20] simulated mobile IP and analyzed only the end-to-end delay. But smooth handoff and buffer support for ROMIP was not implemented.

Leo's project was initially developed using NS 2.1b8. In this thesis Leo's project was successfully adopted to the latest stable NS release – NS 2.29.

The Smooth Handoff feature was successfully implemented. Comparing the performance with Smooth Handoff and without Smooth Handoff support, it was shown that smooth handoff reduced packet loss, and end-to-end average delay, and increased throughput during handoff periods. Smooth Handoff was not activated if the previous agent is the Home Agent.

Basic mobile IP and Route Optimization scenarios have been simulated to compare the performances of the two protocols. Advantages and drawbacks of each protocol have been examined.

Buffer support has been implemented in order to reduce the packet loss during handoff,. Previous foreign agent buffers the incoming packets and forwards these packets to the new foreign agent after the new FA sends binding update to the PFA. Hence, packet loss is significantly reduced.

New trace format of NS2 is used for analyzing to get more detailed results and an analyzer software was developed to analyze the results and to plot the graphs. The analyzer software is explained in appendix D. The source codes of the analyzer software and the NS2 simulator are presented in a CD, which is appended to this thesis.

The simulation results were evaluated from the aspect of mobile IP optimization. By comparing basic mobile IP and Route Optimized Mobile IP, it is seen that buffer support introduces an additional delay to route optimization but reduce packet loss during handoff periods. Hence, the throughput is significantly increased. Buffer management has also great importance on increasing throughput and decreasing packet loss.

In this thesis, it is shown that buffer and smooth handoff supported Route Optimized Mobile IP clearly and successfully eliminates the undesired effect of Triangle Routing, that is consequently decreases packet loss and increases the throughput.

REFERENCES

[1] Abdel-Hamid and H. Abdel-Wahab, "Local-area Mobility Support through Cooperating Hierarchies of Mobile IP Foreign Agents," in Proceedings of the 6th IEEE International Symposium on Computers and Communications (ISCC 2001), pp. 479-484, Hammamet, Tunisia, July 2001.

[2] C.E. Perkins and K-Y Wang, "Optimized Smooth Handoffs in Mobile IP," in Proceedings of the 4th IEEE Symposium on Computers and Communications (ISCC), pp.340-346, Red Sea, Egypt, July 6-8, 1999.

[3] C.E. Perkins, "IP Encapsulation within IP", IETF RFC 2003, October 1996.

[4] C.E. Perkins, "IP Mobility Support for IPv4", IETF RFC 3220, January 2002.

[5] C.E. Perkins, "IP Mobility Support", IETF RFC 2002, October 1996.

[6] C.E. Perkins, "Minimal Encapsulation within IP", IETF RFC 2004**,** October 1996.

[7] C.E. Perkins, "Mobile IP: Design principles and Practices, First Printing," Addision-Wesley, MA, 1997.

[8] C.E. Perkins, "Mobile-IP Local Registration with Hierarchical Foreign Agents," Internet Draft (Work in Progress), February 1996.

[9] Cheng Lin Tan, Stephen Pink and Kin Mun Lye, "A Fast Handoff Scheme for Wireless Networks," in Proceedings of the 2nd ACM international Workshop on Wireless Mobile Multimedia (WoWMoM), pp.83-90, Seattle WA USA, August 1999.

[10] D. Tandjaoui, N. Badache, H. Bettahar, A. Bouabdallah and H. Seda, "Performance Enchancement of Smooth Handoff in Mobile IP by Reducing Packets Disorder," Proceedings of 8th IEEE International Symposium on Computers and Communication (ISCC 03) , pp. 149-154, Kemer-Antalya, Turkey, June 30-July 3, 2003

[11] D.B. Johnson and C.E. Perkins, "Route Optimization in Mobile IP", Internet Draft (Work in Progress), draft-ietf-mobileip-optim-ll, September 2001.

[12] Erdal Cayirci, LAN F. Akyildiz and Fellow, "User Mobility Pattern Scheme for Location Update and Paging in Wireless System", IEEE Transactions on Mobile Computing, Vol. 1, No.3, July-September 2002.

[13] Network Research Group, Lawrence Berkeley National Laboratory. "NS-LBNL Network Simulator". URL: http://www-nrg.ee.lbl.gov/ns/.

[14] S. Deering, "ICMP Router Discovery Messages", IETF RFC 1256, September 1991.

[15] Ada Pang, Edlic Yiu, Edwood Yiu, "Comparison of Route Optimization and Reverse Routing ", Fall 2003, http://www.sfu.ca/~eyiu/

[16] Wilmer Caripe, "Mobile IP Extensions for Multi-Hop Wireless Networks", Thesis, Thayer School of Engineering

[17] J. Solomon, "Applicability Statement for IP Mobility Support," IETF RFC 2005, October 1996.

[18] C.E. Perkins, David B. Johnson, " Route Optimization in Mobile IP", draft-ietf-mobileip-optim-11.txt, September 2001.

[19] K. Daniel Wong, Hung-Yu Wei, Ashutosh Dutta, Kenneth Young "Performance of IP Micro Mobility Management Schemes using Host Based Routing ", Telcordia Technologies Inc. http://www.argreenhouse.com/bIos/dwong, ColumbIa UnIversIty, New York, NY 10027, USA

[20] Hao (Leo) Chen "Route Optimization on Mobile IP over IPv4"**,** Spring 2002, http://www.sfu.ca/.lcheu/885-project.htm

[21] Jiannong Cao, Liang Zhang, Henry Chan "Design and Performance Evaluation of an Improved Mobile IP Protocol" Department of ComputIng of Hong Kong PolytechnIc UnIversIty

[22] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[23] David B. Johnson, " Scalable Support for Transparent Mobile node Internetworking", Carnegie Mellon University Computer Science Department dbj@cs.cmu.edu

[24] Charles E. Perkins, "Mobile IP", Sun Microsystems

[25] Kevin Fall, Kannan Varadhan, "The NS Manual", *http://www.isi.edu/nsnam/ns/doc/index.html*

[26] Gavin Holland, "Analysis of TCP Performance over Mobile Ad Hoc Networks",Department of Computer Science, Texas A&M University

[27] Anne Fladenmuller, Ranil De Silva, "The effect of Mobile IP handoffs on the performance of TCP", Alcatel CIT, Software Department.

[28] S. McCanne and S. Floyd, "Ns-Network Simulator", http://www-mash.cs.berkeley.edu/ns/.

[29] Debalina Ghosh, "Mobile IP", University of Illinois at Chicago, http://www.acm.org/crossroads/xrds7-2/mobileip.html

[30] William Stallings, "Wireless Communications and Networks", Chapter 6 (pages 385 – 432)

Appendix A

TERMINOLOGY

Mobile IP introduces the following new functional entities:

Mobile node — A host or router that changes its point of attachment from one network or subnetwork to another, without changing its IP address. A mobile node can continue to communicate with other Internet nodes at any location using its (constant) IP address.

Home agent — A router on a mobile node's home network which delivers datagrams to departed mobile nodes, and maintains current location information for each.

Foreign agent — A router on a mobile node's visited network which cooperates with the home agent to complete the delivery of datagrams to the mobile node while it is away from home. A mobile node has a home address, which is a long-term IP address on its home network. When away from its home network, a care-of address is associated with the mobile node and reflects the mobile node's current point of attachment. The mobile node uses its home address as the source address of all IP datagrams it sends, except where otherwise required for certain registration request.

The following terms are frequently used in connection with mobile IP:

Agent advertisement — Foreign agents advertise their presence by using a special message, which is constructed by attaching a special extension to a router advertisement, as described in the next section.

Care-of address — The termination point of a tunnel toward a mobile node, for datagrams forwarded to the mobile node while it is away from home. There are two different types of care-of address: a foreign agent care-of address is an address of a foreign agent with which the mobile node is registered; a collocated care-of address is an externally obtained local address which the mobile node has associated with one of its own network interfaces.

Correspondent node — A peer with which a mobile node is communicating. A correspondent node may be either mobile or stationary.

Foreign network — Any network other than the mobile node's home network.

Home address — An IP address that is assigned for an extended period of time to a mobile node. It remains unchanged regardless of where the node is attached to the Internet.

Home network — A network, possibly virtual, having a network prefix matching that of a mobile node's home address. Note that standard IP routing mechanisms will deliver datagrams destined to a mobile node's home address to the mobile node's home network.

Mobility agent — Either a home agent or a foreign agent.

Mobility binding — The association of a home address with a care-of address, along with the remaining lifetime of that association.

Node — A host or a router.

Tunnel — The path followed by a datagram while it is encapsulated. The model is that, while it is encapsulated, a datagram is routed to a knowledgeable decapsulating agent, which decapsulates the datagram and then correctly delivers it to its ultimate destination [30].

Appendix B

Free Space Propagation and the Two Ray Model

In the absence of any reflections or multipath, radio wave propagation can be modeled using the free space propagation model, which says:

$$S_r = S_t G_t G_r \left(\frac{\lambda}{4\pi d} \right)^2 \qquad \text{(B.1)}$$

where:

- S_r : Signal power at the receiver antenna
- S_t : Signal power at the transmitter antenna
- G_t : Gain of the transmitting antenna (relative to isotropic antenna)
- Gr : Gain of the receiving antenna (relative to isotropic antenna)
- λ : Wavelength
- d : Propagation distance between antenna (the same unit as wavelength)

Alternatively, we can express Equation B.1 in dB units by taking **10 log$_{10}$** of both sides to obtain:

$$S_r(dBW) = S_t(dBW) + G_t(dBi) + G_r(dBi) + 20\log_{10}\left(\frac{\lambda}{4\pi}\right) - 20\log_{10}(d) \qquad \text{(B.2)}$$

The last two terms of Equation B.2 represents are called **Path Loss (PL)** for free space propagation free space loss. This is the channel's loss in going from the transmitter to the receiver expressed in dB. The first two right hand terms combined is called **Effective Isotropic Radiated Power** or **EIRP**. **EIRP** is the equivalent transmitter power required if an isotropic **(0 dBi)** antenna were used. Using these definitions, we obtain Equation B.3, where for free space propagation; Where free space loss is **PL (dB) = -20 log$_{10}$ (λ / 4πd)**

$$S_r(dBW) = EIRP(dBW) + Gr(dBi) - PL(dB) \tag{B.3}$$

For non-free space propagation conditions, **PL** might be described by **PL=A+B log $_{10}$ (R)** as discussed in Statistical Propagation Modeling for Cellular Systems. To understand why free space propagation usually does not apply at extended ranges in the ground mobile environment, let us consider the two-ray propagation model.

In a mobile radio channel, a single direct path (LOS : Line of sight) between the base station and a mobile node is rarely the only path for propagation. Hence, the free space propagation model of equation (B.1) is in most cases inaccurate when used alone. The 2-ray ground reflection model shown in Figure B.1 is a useful propagation model that is based on geometric optics, and considers both the direct path and a ground reflected propagation path between transmitter and receiver. This model has been found to be reasonably accurate for predicting the large-scale signal strength over distances of several kilometers for mobile radio systems that use tall towers (heights which exceed 50 m), as well as for line-of-sight micro cell channels in urban environments.

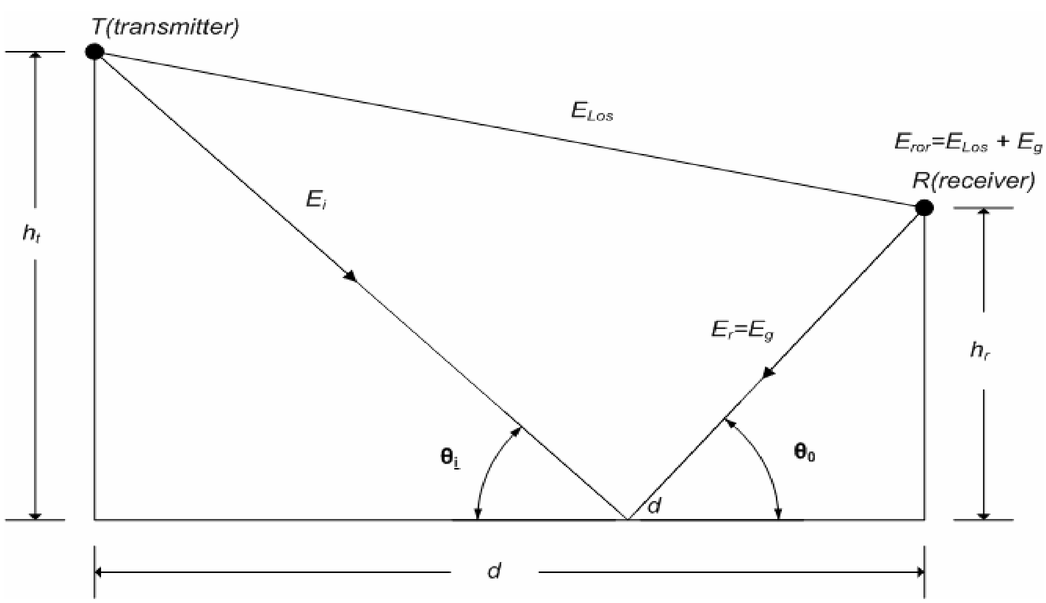


Figure B.1 Two-ray ground reflection model.

$$E(d.t) = \frac{E_0 d_0}{d} \cos\left(\omega_0\left(t - \frac{d}{c}\right)\right) \qquad (d > d_0) \tag{B.4}$$

E_0 : LOS component of the received signal

D_0 : Length of reflected path

$\frac{E_0 d_0}{d}$: Reflected component of the received signal

Specular reflection much like light from a mirror is assumed and to a very close approximation, the specular reflection arrives with strength equal to that of the direct path signal. The reflected signal shows up with a delay relative to the direct path signal and as a consequence, may add constructively (in phase) or destructively (out of phase) to the direct path signal. Received power is a function of range.

Appendix C

Mobile IP Message Formats

Mobility Agent Advertisement Extension

The Mobility Agent Advertisement Extension follows the ICMP Router Advertisement fields. It is used to indicate that an ICMP Router Advertisement message is also an Agent Advertisement being sent by a mobility agent. The Mobility Agent Advertisement Extension is defined as follows:

```
    0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Type      |    Length     |        Sequence Number        |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |    Registration Lifetime      |R|B|H|F|M|G|r|T|   reserved    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                  zero or more Care-of Addresses               |
 |                              ...                              |
```

Type : 16

Length : (6 + 4N), where 6 accounts for the number of bytes in the Sequence Number, Registration Lifetime, flags, and reserved fields, and N is the number of care-of addresses advertised.

Sequence Number : The count of Agent Advertisement messages sent since the agent was initialized.

Registration Lifetime : The longest lifetime (measured in seconds) that this agent is willing to accept in any Registration Request. A value of 0xffff indicates infinity. This field has no relation to the Lifetime" field within the ICMP Router Advertisement portion of the Agent Advertisement.

R : Registration required. Registration with this foreign agent (or another foreign agent on this link) is required even when using a co-located care-of address.
B : Busy. The foreign agent will not accept registrations from additional mobile nodes.

H : Home agent. This agent offers service as a home agent on the link on which this Agent Advertisement message is sent.

F : Foreign agent. This agent offers service as a foreign agent on the link on which this Agent Advertisement message is sent.

M : Minimal encapsulation. This agent implements receiving tunneled datagrams that use minimal encapsulation.

G : GRE encapsulation. This agent implements receiving tunneled datagrams that use GRE encapsulation.

r : Sent as zero; ignored on reception and should not be allocated for any other uses.

T : Foreign agent supports reverse tunneling.

reserved : Sent as zero; ignored on reception.

Care-of Address(es) : The advertised foreign agent care-of address(es) provided by this foreign agent. An Agent Advertisement must include at least one care-of address if the 'F' bit is set. The number of care-of addresses present is determined by the Length field in the Extension.

Registration Request

A mobile node registers with its home agent using a Registration Request message so that its home agent can create or modify a mobility binding for that mobile node (e.g., with a new lifetime). The Request may be relayed to the home agent by the foreign agent through which the mobile node is registering, or it may be sent directly to the home agent in the case in which the mobile node is registering a co-located care-of address.

IP fields;

Source Address: Typically, the interface address from which the message is sent.

Destination Address: Typically that of the foreign agent or the home agent.

The UDP header is followed by the Mobile IP fields shown below:

```
    0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Type      |S|B|D|M|G|r|T|x|          Lifetime             |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                          Home Address                         |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                           Home Agent                          |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                         Care-of Address                       |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 +                         Identification                        +
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                         | Extensions ...
                         +-+-+-+-+-+-+-+-
```

Type : 1 (Registration Request)

S : Simultaneous bindings. If the **'S'** bit is set, the mobile node is requesting that the home agent retain its prior mobility bindings.

B : Broadcast datagrams. If the **'B'** bit is set, the mobile node requests that the home agent tunnel to it any broadcast datagrams that it receives on the home network.

D : Decapsulation by mobile node. If the **'D'** bit is set, the mobile node will itself decapsulate the datagrams which are sent to the care-of address. That is, the mobile node is using a co-located care-of address.

M : Minimal encapsulation. If the **'M'** bit is set, the mobile node requests that its home agent use minimal encapsulation for datagrams tunneled to the mobile node.

G : GRE encapsulation. If the **'G'** bit is set, the mobile node requests that its home agent use GRE encapsulation for datagrams tunneled to the mobile node.

r : Sent as zero; ignored on reception and should not be allocated for any other uses.

T : Reverse Tunneling requested.

x : Sent as zero; ignored on reception.

Lifetime : The number of seconds remaining before the registration is considered expired. A value of zero indicates a request for deregistration. A value of 0xffff indicates infinity.

Home Address : The home IP address of the mobile node.

Home Agent : The home IP address of the mobile node's home agent.

Care-of Address : The home IP address for the end of the tunnel.

Identification : A 64-bit number, generated by the mobile node, used for matching Registration Requests with Registration Replies, and for protecting against replay attacks of registration messages.

Extensions : The fixed portion of the Registration Request is followed by one or more of the Extensions. An authorization-enabling extension must be included in all Registration Requests [5].

Route Optimization Message Formats

Route Optimization defines four message types used for management of binding cache entries. Each of these messages begins with a one-octet field indicating the type of the message.

The following Type codes are defined in this document:

16 = Binding Warning message

17 = Binding Request message

18 = Binding Update message

19 = Binding Acknowledge message

Binding Warning Message

A Binding Warning message is used to advise a node that it appears to have either no binding cache entry or an out-of-date binding cache entry for some mobile node. When any node receives a datagram tunneled to itself, if it is not the current foreign agent for the destination mobile node, it MAY send a Binding Warning message to the node that originated the tunneled datagram.

```
  0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |                   Reserved                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Mobile Node Home Address                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type : 16

Reserved : Sent as 0; ignored on reception.

Mobile Node Home Address : The home address of the mobile node to which the Binding Warning message refers.

Binding Update Message

The Binding Update message is used to notify another node of a mobile node's current mobility binding. It may be sent by the mobile node's home agent in response to a Binding Request message. It may also be sent by a mobile node, or by the foreign agent with which the mobile node is registering, when notifying the mobile node's previous foreign agent that the mobile node has moved.

```
    0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Type      |A|I|M|G|  Rsvd |            Lifetime           |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                    Mobile Node Home Address                   |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                        Care-of Address                        |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 +                         Identification                        +
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                         | Extensions ...
                         +-+-+-+-+-+-+-+-
```

Type : 18

Acknowledge (A) : The Acknowledge (A) bit is set by the node sending the Binding Update message to request a Binding Acknowledge message be returned acknowledging its receipt.

Identification Present (I) : The Identification Present (I) bit is set by the node sending the Binding Update message to indicate that the Identification field is present in the message.

Minimal Encapsulation (M) : If the Minimal Encapsulation (M) bit is set, datagrams may be tunneled to the mobile node using the minimal encapsulation protocol used in the base Mobile IP protocol.

GRE Encapsulation (G) : If the GRE Encapsulation (G) bit is set, datagrams may be tunneled to the mobile node using the GRE encapsulation protocol .

Reserved (Rsvd) : Sent as 0; ignored on reception.

Lifetime : The number of seconds remaining before the binding cache entry must be considered expired. A value of all ones indicates infinity. A value of zero indicates that no binding cache entry for the mobile node should be created and that any existing binding cache entry (and visitor list entry, in the case of a mobile node's previous foreign agent) for the mobile node should be deleted. The lifetime is typically equal to the remaining lifetime of the mobile node's registration.

Mobile Node Home Address : The home address of the mobile node to which the Binding Update message refers.

Care-of Address : The current care-of address of the mobile node. When set equal to the home address of the mobile node, the Binding Update message indicates that no binding cache entry for the mobile node should be created, and any existing binding cache entry (and visitor list entry, in the case of a mobile node's previous foreign agent) for the mobile node should be deleted.

Identification : If present, a 64-bit number is assigned by the node sending the Binding Request message for matching requests with replies to protect against replay attacks.

Binding Acknowledge Message

A Binding Acknowledge message is used to acknowledge receipt of a Binding Update message. A node receiving the Binding Update message if the Acknowledge (A) bit is set in the Binding Update message should send it.

```
    0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Type      |N|               Reserved                      |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                    Mobile Node Home Address                   |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 +                         Identification                        +
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type : 19

Negative Acknowledge (N) : If the Negative Acknowledge (N) bit is set, this acknowledgement is negative. For instance, if the binding update was not accepted, but the incoming datagram has the Acknowledge flag set, then the Negative Acknowledge (N) bit should be set in this Binding Acknowledge message.

Reserved : Sent as 0; ignored on reception.

Mobile Node Home Address: Copied from the Binding Update message being acknowledged.

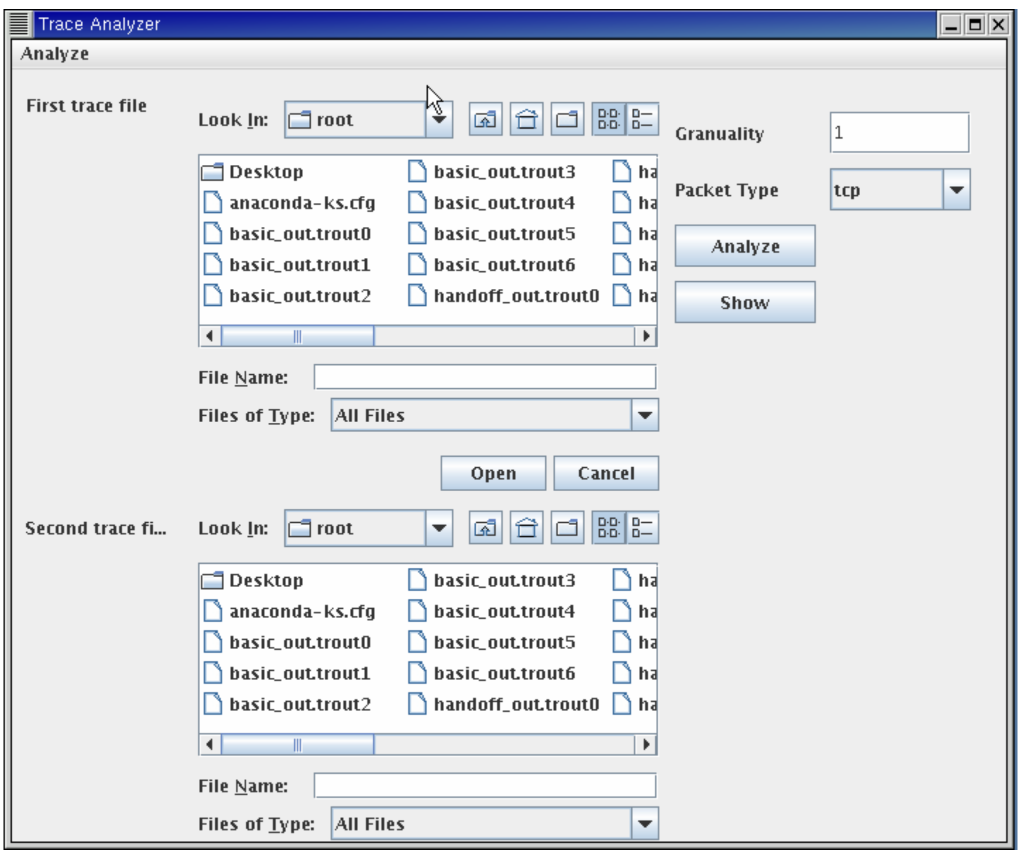
Identification : Copied from the Binding Update message being acknowledged, if present there [18].

Appendix D

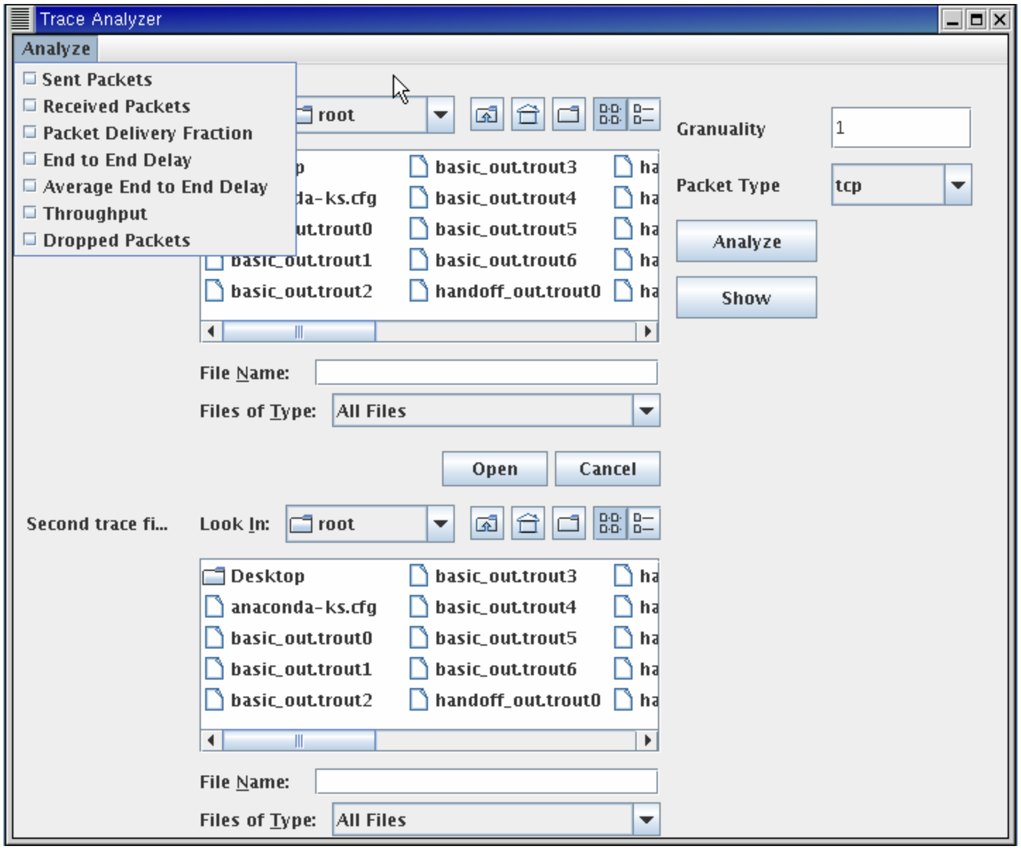
Trace Analyzer

Trace Analyzer is a NS2 trace files analyzer, which is a part of this thesis simulation.

Trace Analyzer runs under Windows, Linux, and UNIX as NS 2 simulator. The main problem is that NS2 does not provide any visualization options for simulation results (trace files) analysis. Because of this reason, trace analyzer was implemented in java language. Since the application is an open source it can be used for any project by adding needed functions.



(a) Trace analyzer main window



(b) Trace analyzer functions

Figure C.1 Trace Analyzer screen views

Figure C.2 shows the NS2 system architecture and trace analyzer on a simple block diagram. NS2 includes Network Animator, which is a visualization tool for packet flow. It only shows movement of generated packets as an animation, so this is not enough to analyze the simulation results. The simulator users have to create their own programs to process the results trace files. The NS2 output data contains a lot of complicated information about simulation. There are a few trace file formats and each of them can have various versions, so it can be difficult to find out how to extract the necessary data. This is the reason why Trace analyzer is so useful. It makes trace file processing very simple.

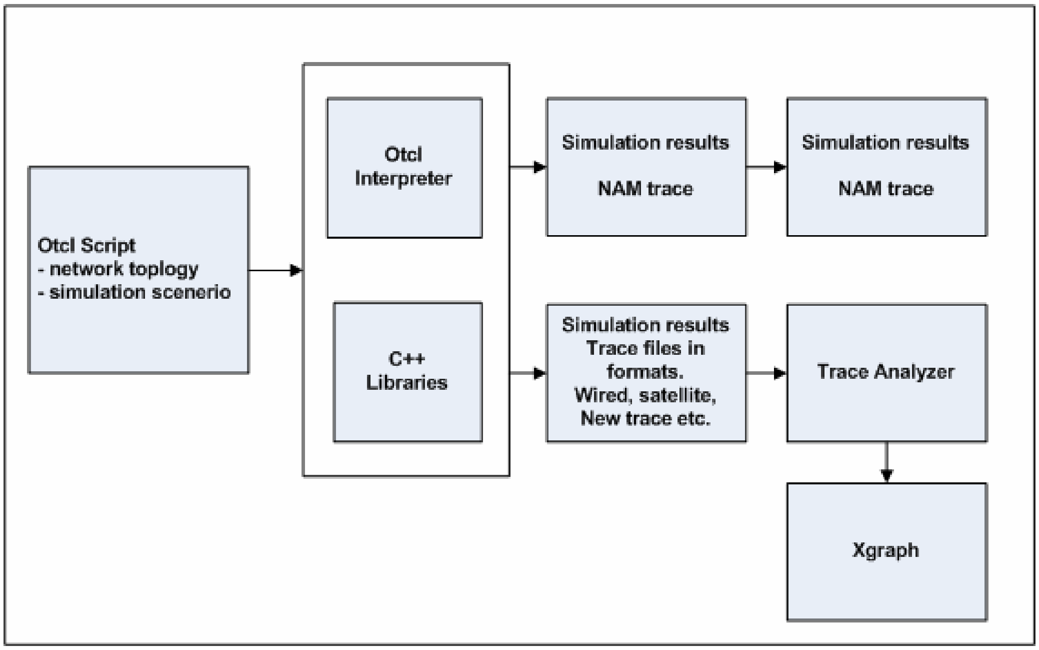


Figure C.2 NS2 system architecture with Trace Analyzer

For simulation results analysis the following quality determinants are used in Trace Analyzer system:

(1) Delay = packet receive time at destination node – packet send time at source node.

(2) End to end delay = total packet duration of all packets which are present in the trace file.

(3) Average end to end delay = calculated by division of end to end delay by total number of received packets.

(4) Throughput = number of generated/sent/received/forwarded/dropped packets or bits in a certain time interval.

(5) Packet duration = time interval between the packet start time and end time.

(6) Packet delivery fraction = the ratio between total number of received packets to send packets. This ratio is calculated by dividing the total number of received packets by the total number of sent packets and multiplexing the result by hundred.

(7) Dropped packets = total number of dropped packets.

Trace file loading stage is divided into 5 stages as shown Figure C.1 a and b:

(1) Loading of the first trace file from the upper file selection dialog.
(2) Loading of the second trace file from the bottom file selection dialog.
(3) Selecting the packet type (tcp, cbr, ubr).
(4) Analyzing the selected trace files. Trace file analyzing contains the analyzing of all the packets which is indicated by rows in trace file.

RESUME

Name Surname : Birol ÇELİK

Date of Birth : 08.07.1969

Contact Info : 1 nci Ordu Komutanlığı

Bilgi Sistem Yönetim Şube

Sistem İşletim Subayı

Phone : (0216) 556 84 21

E-mail : bcelik@kkk.tsk.mil.tr

Educational Degree:

1983-1987 Kuleli Military School

1987-1991 Turkish Military Academy

1999-2000 Ege University, Department of Computer Science Engineering

(Automatic Information Process Education)

Master Header and Instructor:

Master Header : Performance Evaluation of Mobile Internet Protocol

Master Instructor : Asst. Prof. Dr. Demir ÖNER

T.C.
MARMARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KABUL VE ONAY BELGESİ

PERFORMANCE EVALUATION OF MOBILE INTERNET PROTOCOL

Birol ÇELİK.'in PERFORMANCE EVALUATION OF MOBILE INTERNET PROTOCOL isimli Lisansüstü tez çalışması, M.Ü. Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 29 MAYIS 2006 tarih ve 1621 sayılı kararı ile oluşturulan jüri tarafından Bilgisayar Mühendisliği Anabilim Dalı Bilgisayar Mühendisliği (Eng.) Programında YÜKSEK LİSANS Tezi olarak Kabul edilmiştir.

Danışman	: Doç.Dr. Demir ÖNER	Marmara Üniversitesi
Üye	: Prof.Dr. Fuat İNCE	Marmara Üniversitesi
Üye	: Prof.Dr. Yılmaz ÇAMURCU	Marmara Üniversitesi

Tezin Savunulduğu Tarih : 26 HAZİRAN 2006

ONAY

M.Ü. Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 04.07.2006 tarih ve 2006/17-61.. sayılı kararı ile ...–...... tarihinde .Birol......ÇELİK..................'ın Bilgisayar....Mühendisliği... Anabilim Dalı ....–.................... Programında Y.Lisans (MSc.) derecesi alması onanmıştır.

Marmara Üniversitesi
Fen Bilimleri Enstitüsü Müdürü

Prof. Dr. Adnan AYDIN
MÜDÜR