Implementing Mobile IP Scenario Using NS-2

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Software Engineering

By:

Jalandher Jajula

(800831003)

Under the supervision of:

Mr. Sumit Miglani

Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

June 2010

Certificate

I hereby certify that the work which is being presented in the thesis entitled, **"Implementing Mobile IP Scenario Using NS-2"**, in partial fulfillment of the requirements for the award of degree of Master of Engineering in Software Engineering submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Mr.Sumit Miglani and refers other researcher's works which are duly listed in the reference section.

The matter presented in this thesis has not been submitted for the award of any other degree of this or any other university.

(Jalandher Jajoria)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Mr.Sumit Miglani)

Assistant Professor

Computer Science and Engineering Department

Thapar University
Patiala

Countersigned by

(Dr.RAJESH BHATIA)

Head

Computer Science & Engineering, Department

Thapar University

Patiala

(Dr.R.K.SHARMA)

Dean (Academic Affairs)

Thapar University,

Patiala.

Acknowledgment

First and foremost, I would like to express my sincere gratitude to my advisor **Mr. Sumit Miglani, Assistant Professor,** Computer Science & Engineering Department for his immense help, guidance, stimulating suggestions and encouragement all the time. He always provide a motivating and enthusiastic atmosphere to work with. It was a great pleasure to do this thesis under his supervision.

I am also thankful to **Dr. Rajesh Bhatia,** Head of Department, Computer Science & Engineering Department and **Mrs. Inderveer Channa,** P.G. Coordinator, for the motivation and inspiration that triggered me for the thesis. I would also like to thank all the staff members who were always there at the need of the hour and provided with all the help and facilities, which I required for the completion of the thesis.

Last but not the least, I express my heartfelt thanks to my parents and all of my friends for encouraging me and providing me useful information during my work.

Finally, my special thanks goes to authors whose works I have consulted and quoted in this work.

Jalandher Jajula

(802831003)

Abstract

The number of wireless networks is increasing day by day as a result of it more number of users are opting for the wireless technology. The emergence of mobile devices or mobile nodes allows the users to access the network when they are on the move. As users move frequently from one network to another network a new IP address is assigned to the mobile node every time when it visits a new network. The mobile node has no way to inform the change in its IP address to the other nodes present in the network to which it belongs so the packets sent to the mobile node previous IP address are simply lost.

To deal with the change in the IP addresses of the mobile node every time it visits a new network can be handled by the Mobile IP.

Mobile IP is a protocol, developed by the Mobile IP Internet Engineering Task Force (IETF) working group that allows the delivery of the packets to mobile nodes when they moves to a new network based on its old IP address.

In this thesis work an attempt has been made to simulate the mobile IP scenario with the use of NS-2 network simulator.

List of Figures

AH ……..Authentication Header
BU ……..Binding Update
CN ……..Correspondent Agent
CoT ……Care of Test
CoTI ……...Care of Test Initialization
DHCP ……Dynamic Host Configurable Protocol
DoS ……Denial of Service
DNS…… Domain Name Server
ESP ……Encapsulation Security Header
FA ……...Foreign Agent
FMN ……...Fake Mobile Node
FTP……..File Transfer Protocol
FQDN…….. Fully Qualified Domain Names
HA ……..Home Agent
HMAC ……Hashed Message Authentication Code
HoT ……Home Test
HoTI ……Home Test Initialization
ICMP ……...Internet Control Message Protocol
IETF ……....Internet Engineering Task Force
IKE ……..Internet Key Exchange
IPSec ……....Internet Protocol Security
LSRR…….loose source and record route
MAC ……Message Authentication Code
MD ……...Message Digest
MIPv6 ……..Mobile IP Version 6
MN ……...Mobile Node
MH……Mobile Host

MIP……Mobile Internet Protocol

MA……Mobile Agent

NS2 ……..Network Simulator 2

SA …….Security Association

TCP……Transmission Control Protocol

CHAPTER 1

INTRODUCTION

1.1 Introduction

The Internet has come a long way since the 1960.It is made up many wide and local area networks joined by various network connecting devices. To make the communication possible between the various network devices TCP/IP Protocol suite is developed [1]. Within the TCP/IP Protocol suite, perhaps the most important protocol is the Internet Protocol (IP) which makes use of classful and classless addressing scheme that represents both the topological location and the identity of a node in the network. With the advent of wireless and mobile computing technology there is the rise in the usage and number of mobile devices by the users that wants to connect with the network i.e. Internet at any time irrespective of physical location but the existing IP protocol fails to handle the issue of mobility in the mobile devices also the growth of IP-based data and voice applications in the context of mobile devices (for example PDAs, laptops and 3rd and 4th generation mobile phones) and new access technologies are driving a desire to support mobility at the IP level. To deal with the issue of mobility there arises a need to develop a new protocol which is an extension to the existing Internet Protocol (IP) [6] infrastructure.

1.2 Mobile IP

The most widely employed network protocol IP is not designed to handle the issues of mobility. For this purpose Internet Engineering Task Force (IETF) develops a protocol called as Mobile IP that act as an enhancement to the existing Internet Protocol

Mobile IP addresses the problem by introducing two IP addresses for mobile hosts – a static 'home address' by which the host is known globally, across the network and a transient 'Care-of Address' by which the host is temporarily known when attached to different networks other than its home network. Any communication that occurs between

the mobile node and any other node will identify the mobile node with its home address when the mobile node is moves away from its home network it assigns the representative in its home network i.e. the router which will going to receive the packets meant for the mobile node coming from the another node based on its old IP address. Once the representative accepts the incoming packets it forwards the packets to the mobile node which is located in a new network.

1.3 Importance of Mobile IP

The importances of mobile IP are as follows:

a. Mobile IP addresses the issue of mobility which is not addressed by the traditional IP in which if a node changes its point of attach then it is must for it to change its IP address. If anode changes its address the other nodes will not know about its new IP address unless they are informed about it.
b. In response to the increasing popularity of palm-top and other mobile devices mobile IP is developed to enable the mobile nodes to maintain the internet connectivity while moving from one internet attachment point to another.
c. It supports network layer mobility in a manner that is transparent to all upper layers i.e. transport layer and application layer.
d. The applications designed around the assumptions of the traditional, non-mobile Internet will continue to function even in a mobile host environment.

For all the above reasons it would be better for users to be connected to remote networks on which they work and enjoy as if they are in their home network which can be done using mobile IP[3].

1.4 Organization of the Thesis

This thesis consists of six chapters which are organized as follows. In the first chapter an introduction of mobile IP is described under the sub topics of Mobile IP and importance of mobile. Chapter two gives a literature review of Mobile IP, it describes background, the architecture of mobile IP, mobile IP operations, those are agent discovery, registration

and tunneling. In Chapter three detailed description of problem statement and objectives of the mobile IP simulations are discussed. Chapter4 discusses the implementation details of the proposed approach. In chapter five the simulation set up for different scenarios are set and the results obtained are presented and discussion is made on the results. Finally, conclusion of the work and future recommendations are presented in chapter six.

CHAPTER 2

LITERATURE REVIEW

This chapter explains the reasons why the mobility cannot be supported in the existing IP protocol and represents the proposed approaches of the researcher's that can be used to overcome the weaknesses of IP addressing and routing scheme in supporting the mobile host.

2.1 Internet Addressing and Routing

The IP uses a hierarchical addressing scheme in which the 32 bit address is divided into two parts: net-id and host-id. The net-id identifies a network where as host-id identifies a host on the network. It facilitates routing generally in two steps:

a. Routers forward the datagram to the network using the network ID part.
b. Once the datagram reaches the destination network, Routers deliver the datagram to the host using the host ID part.

2.2 The Host Mobility Problem with IP

Despite the advantages, the addressing and routing scheme of IP makes mobile computing difficult.

Consider the scenario illustrated in Figure 2.1.

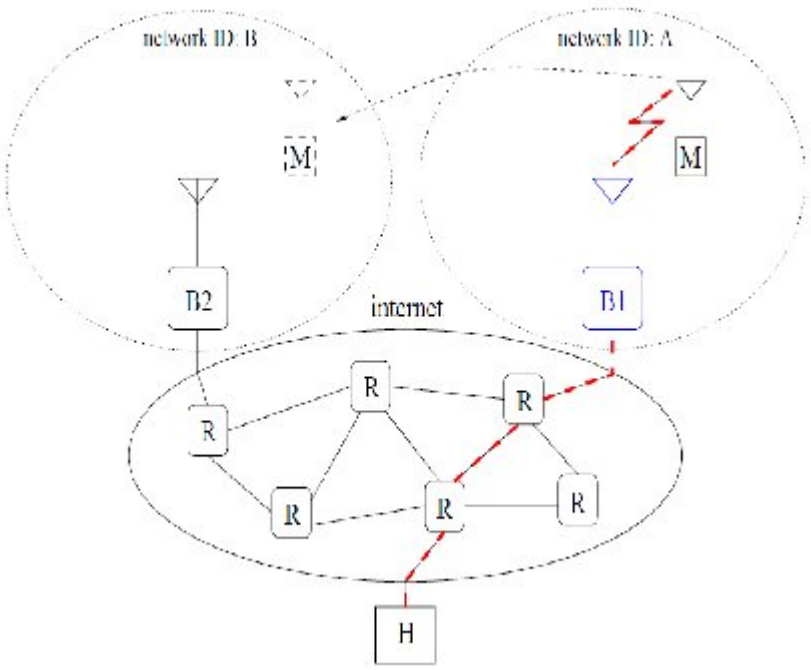


Figure: 2.1 Illustration of two base stations, B1 and B2, attached to an internet. A mobile host, M, is communicating with host H using base station B1 [4].

Figure 2.1 shows two base stations B1 and B2 attached to an internet interconnected using several routers, denoted using symbol R. Station B1 supports wireless LAN A (with network ID A), and B2 supports wireless LAN B (with network ID B). Host H is using TCP/IP [20] to communicate with mobile host M via station B1. The network ID part of M's IP address is A (i.e., M is a host in wireless LAN A). Suppose M migrates to wireless LAN B. Host H cannot communicate with M because IP routers continue to forward data grams destined for M to wireless LAN A.

Mobile M can acquire a new IP address from wireless LAN B and uses the new address to communicate with H. Host H sends subsequent data grams to M using the new address. IP routers will correctly forward the data grams to wireless LAN B. Thus, H and B reestablish communication. Unfortunately, changing an IP address breaks the TCP connections that already exist between M and H, because TCP uses the IP address of each

end of a connection to identify the connection. To summarize the difficulties in supporting host migration in an internet:

- Changing an address facilitates routing, but breaks existing TCP connections.
- Maintaining an address keeps existing TCP connections, but creates routing problems.

In theory, IP routers can treat mobile computers as a special case and maintain a host-specific route for each mobile. When a mobile migrates to a new network, routers propagate a route update for the mobile. In practice, propagating host-specific routes for mobiles does not work well for two reasons. First, routers need special protocols to propagate the routes in a timely fashion because current IP routing protocols are not designed to operate in a rapidly changing topology [5]. Second, routers need to propagate routes to every router in the internet because a mobile could be communicating with any host attached to the internet.

Researchers have proposed the following approaches in the existing IP in order to support mobility of the mobile hosts.

2.3 The IEN-135 Approach

In the early days of Internet, researchers had discovered the weakness of IP's addressing and routing scheme in supporting mobile hosts. In Internet Engineering Notes (IEN) 135 [8], Sunshine and Postel proposed using loose source routing to support mobile hosts. They also proposed reserving a single network ID for the mobiles. That is, all mobiles reside in a single virtual network. A mobile host uses the same address regardless of the physical network to which the host attaches. A global database maintains the bindings of mobile-to-forwarder. A new message format was designed to query and update the location of a mobile. When communicating with a mobile, a host is responsible for obtaining the address of the mobile's forwarder and acts as the address insertion agent for itself.

2.4 The IBM Approach

Researchers [3] at IBM Corporation also proposed using loose source routing to support mobile hosts. Unlike the IEN-135 approach, the IBM approach does not restrict all mobiles to use the same network ID. Each mobile has a home network. The network ID of a mobile's IP address identifies the home network of the mobile. Each home network has at least one mobile router (MR) that maintains the forwarder information and acts as the address insertion agent for the mobiles in the network.

To send a datagram to a mobile that is away from its home network, a sender transmits the datagram, without using the LSRR option. IP routers will forward the datagram to the home network of the mobile. When the datagram reaches the home network, an MR intercepts the datagram and forwards the datagram using the LSRR option to the current forwarder of the mobile. The forwarder then delivers the datagram to the mobile. When it replies, the mobile uses the LSRR option to carry the address of the forwarder to the sender. The IBM approach assumes that the sender will perform a route reversal procedure [38] when responding to the datagram from the mobile. Unfortunately, most IP implementations do not support the route reversal procedure [12].

2.5 The SONY Approach

Researchers [14] at SONY Corporation proposed an approach that incorporates the forwarder function into each mobile. Thus, each mobile has two IP addresses, one permanent address, called a virtual IP (VIP) address that is used to identify the mobile, and one temporary IP (TIP) address for the forwarder. Like the IBM approach, the SONY approach also uses routers, called primary resolvers [15], at home networks to intercept datagram and serve as address insertion agents for mobiles. When a mobile migrates to a foreign network, the mobile uses a mechanism (e.g., Dynamic Host Configuration Protocol (DHCP) to obtain a temporary address. The mobile then uses a control packet to carry the VIP-to-TIP binding back to its primary resolver. Routers along the path are allowed to snoop the control packet and cache the binding in a table called Address Translation Table (ATT) [15]. A non mobile host can also install an Address Translation Table to make communication with mobiles more efficient. Thus, besides the primary

resolvers, intermediate routers and hosts that have installed the ATT can serve as address insertion agents for mobiles.

The advantage of the SONY approach is self-sufficiency: a mobile need not rely on a forwarder to be able to communicate when visiting a foreign network. However, the mobile still needs to obtain a temporary address from the foreign network. The extra address requirement makes the scheme unappealing in an environment where IP addresses are a scarce resource. [13].

2.6 The Columbia Approach

At Columbia University, researchers [17] proposed an approach that uses packet forwarding and IP tunneling to support mobile hosts. The Columbia approach uses Mobile Support Routers (MSRs) to support a campus-sized wireless mobile internet. Each MSR supports wireless communication for a geographical area called a cell. MSRs use IP tunnels to turn the physically disjoint cells into a coherent virtual subnet of the campus internet. Each MSR serves as a forwarder for the mobiles in its cell, as an address insertion agent for the mobiles in other cells, and as a router to the virtual mobile subnet.

To send a datagram to a mobile, a sender sends the datagram to a nearest router of the mobile subnet (i.e., a nearest MSR). The router uses a location table and auxiliary protocols to learn the current location of the mobile. If the mobile is not in the local cell, the router forwards the datagram over an IP tunnel to the MSR that is handling the mobile. The MSR then forwards the datagram to the mobile. When a mobile visits a foreign campus, the mobile either uses the MSRs in the foreign campus or becomes a forwarder for itself. In the later case, the mobile is said to be in popup mode [17] and has two IP addresses.

2.7 The IETF Mobile IP Approach

The Internet Engineering Task Force (IETF) Mobile IP Working Group uses a forwarding scheme similar to the Packet Forwarding Method described in and the forwarding scheme of the Columbia approach. The IETF approach uses home agents,

foreign agents, and IP tunnels between the two types of agents to support mobile hosts [2]. Each mobile has at least one home agent. A home agent of a mobile resides in the home network of the mobile, maintains the location of the mobile, and serves as an address insertion agent for the mobile while the mobile is away from the home network.

2.8 Mobile IP Development

Mobile IP solves a problem introduced by the fact that traditional IP addresses simultaneously represent the host's identity and encode the host's topological location on the IP network [6]. Mobile IP provides IP level mobility to allow hosts to roam around different sub networks. Applications on a Mobile IP enabled host can survive physical disconnection and reconnection while changing their points of attachment to the Internet

2.8.1 Terminologies used in Mobile IP

The emergency of mobile IP introduced new architectural entities and terminologies [2]. Most important entities and terminologies in mobile IP are the following:

1. ***Mobile Node (MN):*** It is a node that can change a point of connection without changing its IP address.

2. ***Home Agent (HA):*** A system in the mobile node's home network which registers the location of the mobile node receives packets destined for the mobile node at the home network and tunnels the packets to the care of address of the mobile node.

3. ***Correspondent Agent (CN):*** any node that communicates with the mobile node.

4. ***Foreign Agent (FA):*** it is a router at the foreign network that assists a locally reachable mobile node in delivering packets between the mobile node and the home agent. It also assists the mobile node in getting the care of address.

5. ***Home address:*** the IP address of the mobile node at the home network. This address remains the same irrespective of the attachment place of the mobile node.

6. ***Care of Address:*** Care-of-address is an IP address that identifies the current location of a mobile node when the node is not attached to its home network. It will be obtained from the foreign network and will be registered to home agent.

7. ***Home Network:*** The network in which the mobile node exists for most of the time.

8. ***Foreign Network:*** a network which the mobile node visits.

9. ***Binding Update:*** The association of a home address with a care-of address, along with the remaining lifetime of that association.

2.8.2 Architecture of Mobile IP

In Mobile IP, the network to which the Mobile Node is originally attached is called the Home Network, and the long-term IP address of Mobile Node on the Home Network is called the Home Address

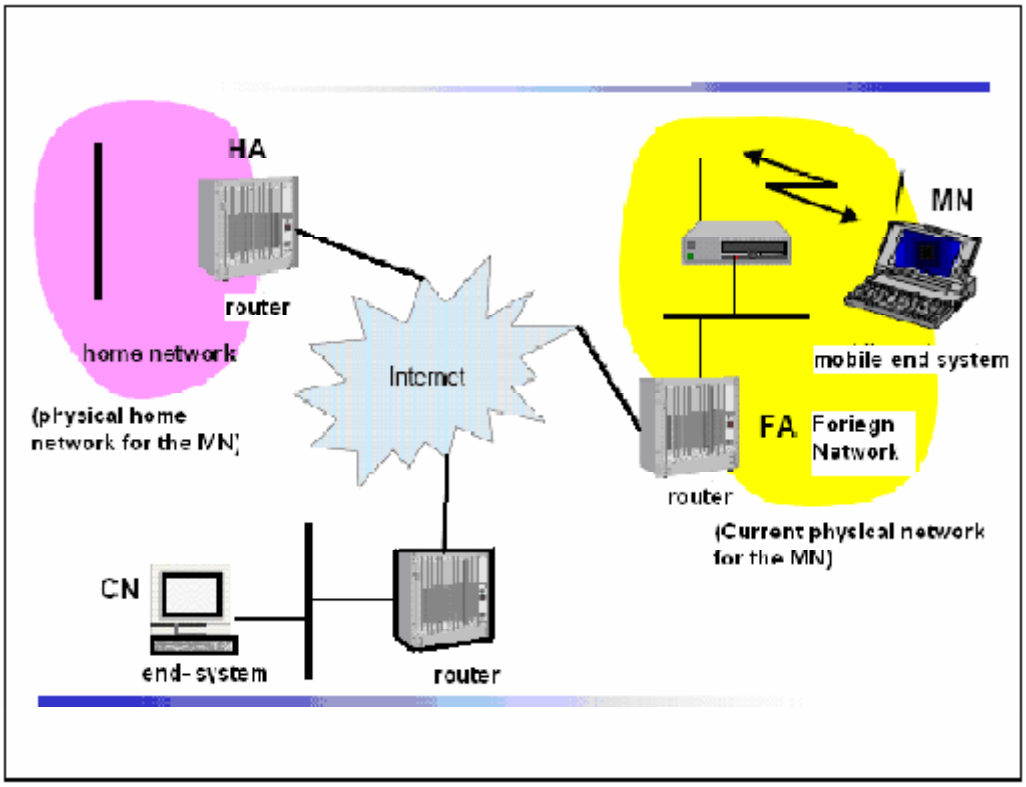


Fig 2.2 Architecture of Mobile IP Communication [10]

The default router of Mobile Node at the home network is called Home Agent. The network that is not the Mobile Node's Home Network is called Foreign Network.

Mobile IP supports the mobility issue related to the mobile nodes by maintaining two types of addresses- Home Address and Care-of Address (CoA).

When Mobile Node is at home network, it is assigned Home Address and only uses its Home Address. This Home Address is regarded as the "permanent" IP address provided to a stationary host, and is used for end-to-end communication. Mobile Node is always identified and addressable by its Home Address regardless of its current point of attachment to the Internet.

When Mobile Node moves away from its home network to a new network, it obtains a temporary, local care of address (COA) on the new network. After obtaining COA it registers with its Home Agent so that Home Agent can forward packets.

2.8.3 Mobile IP Operation

Mobile IP operation can be carried out in the following steps:

- **Agent Discovery:** the home agent and foreign agent advertise their presence and the mobile agent will discover them in this phase.

- **Registration:** The mobile node will register the care of address obtained from foreign network with home agent in this phase.

- **Tunneling:** A tunnel is set up to route packets from the home agent to the foreign agent and finally to the mobile node.

- **Binding Update:** The association between the current CoA and the Home Address of the MN is maintained by a mobility binding. Binding Update is used for renewing a registration which is due to expire, or deregistering when the MN returns home. Binding Update is also used to notify CNs about the current attachment point of the MN. There is a lifetime period associated with each binding in the cache. MNs are responsible for keeping the bindings alive by reregistering before the lifetime has expired or else the binding will be deleted from the cache. Maintaining a binding cache is a good way of optimizing the communication with an MN. Securing the Binding Update is also important - an authentication extension should accompany the Binding Update messages.

2.8.3.1 Agent Discovery

The foreign agent and the home agent periodically advertise their presence by sending a broadcast message. All advertisements are within a sub network and will not be routed

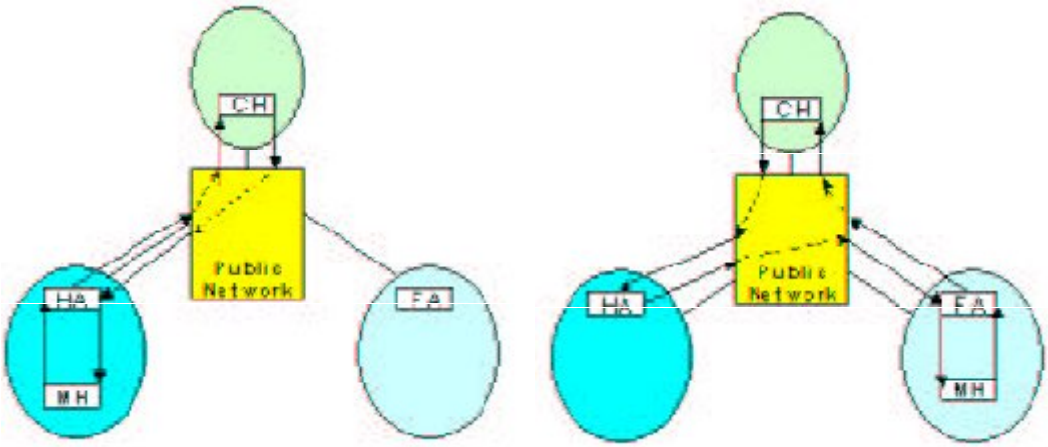
outside this network. This is achieved by sending a broadcast message with its TTL value set to one. A mobile node is also allowed to send ICMP Router Solicitation messages in order to elicit mobility agent advertisement [9].

A mobile node entering a new network listens to advertisements, checks the value of the network component of the source address of the advertised message. The mobile node will use this value to decide the network with which it is connected. If the value is the same as network identifier value of its IP address, it will know that it has connected to its home network; otherwise it will understand that it is connected to the foreign network.

If the mobile node understands that it is in its home network, it will deregister itself so that it will have only one IP address which is its home address. On the other hand, if the mobile node is connected to a foreign network, it will decide to ask for care of address. It will acquire the care of address in one of the following two forms:

1. Care of address obtained from foreign agent
2. Collocated care of address

A Foreign Agent care-of address is an IP address of a Foreign Agent that has an interface on the foreign network being visited by a Mobile Node. A Mobile Node that acquires this type of care of address can share the address with other Mobile Nodes. A collocated care-of address is an IP address temporarily assigned to the interface of the Mobile Node itself. A collocated care-of address represents the current position of the Mobile Node on the foreign network and can be used by only one Mobile Node at a time [7].



(a) MH in home network (b) MH in foreign network

Figure 2.3: MH in home/foreign network [25]

Communications between MH and CH are shown by arrows in this figure.

2.8.3.2 Registration

Once the mobile node obtains a care of address, it sends a registration message to its home agent. The registration process is almost the same whether the mobile node has obtained its care-of address from a foreign agent, or alternatively has acquired it from another independent service such as DHCP [9]. In the former case, the mobile node basically sends the request to the foreign agent which will send it to the home agent. In the latter case, the mobile node sends its request directly to the home agent, using its collocated care-of address as the source IP address of the request. The foreign agent inspects the validity of the registration request, adds the request to its pending list and forwards this request to the home agent to ascertain if the request is valid. The foreign agent responds with an appropriate error code if the request is invalid. A request may be invalid if the value specified in the registration lifetime field is too high.

The home agent authenticates the mobile node and checks the validity of the registration request. If the request is valid, the home agent associates the mobile node with its care-of-address and creates a tunnel in order to forward packets to the foreign agent. The home

agent may send a registration reply with appropriate error code if the registration request was found to be invalid.

The foreign agent then inspects the validity of the registration reply. If the reply is valid, the foreign agent adds the mobile node to its visitor list and creates a tunnel to the home agent. Finally this reply is forwarded to the mobile node. The mobile node checks the validity of the registration reply, and the presence of a valid registration specifies that the mobile agents are aware of its roaming.

The registration of the care of address will have the following procedure [7]:

When the registration is through the foreign agent

1. The mobile node sends the registration request to the foreign agent.
2. The Foreign agent processes the registration request, gets the address of the home agent from the registration request message and forwards it to the home agent.
3. The home agent sends the registration reply to the foreign agent accepting or denying the request.
4. The Foreign agent processes the registration reply and forwards it to the Mobile node.

When the registration is directly from mobile node to home agent

1. The Mobile node sends a registration request to the home agent.
2. The home agent sends the registration reply to the mobile node accepting or denying the request.

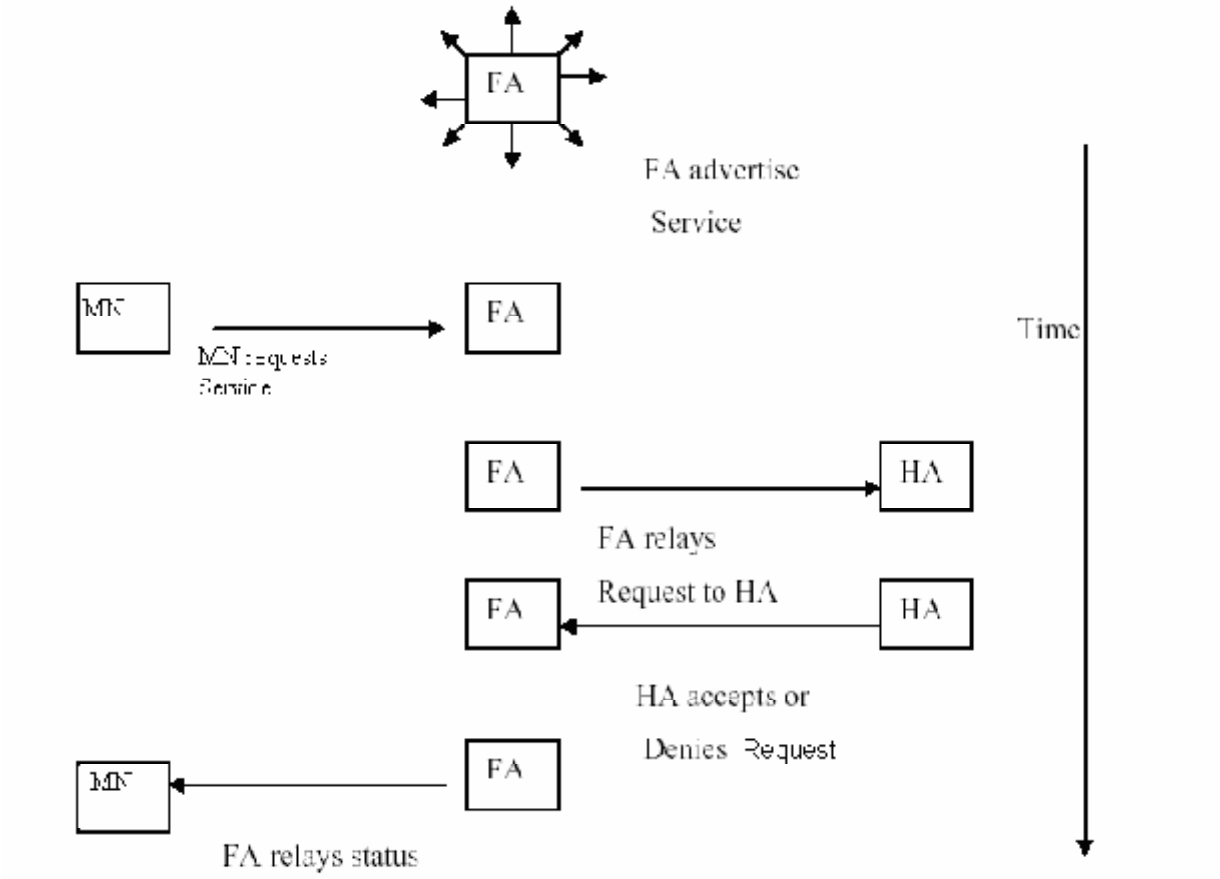


Fig. 2.4 Agent Discovery and Registration Process [7]

2.8.3.3 Tunneling

Once the process of registration is completed, the mobile node can establish a seamless communication irrespective of changing its point of attachment across the internet. The home agent, after a successful registration, will begin to attract datagram destined for the mobile node and tunnel each one to the mobile node at its care-of address. This tunneling is done by the IP-in-IP encapsulation [11].

With IP-in-IP encapsulation, an outer header is inserted before the datagram's existing IP header. There are spaces between the outer header and inner header for including other headers when security is required to protect the original payload during tunneling. In the

case of Mobile IP, the values of the fields in the new header are selected naturally, with the care-of address used as the destination IP address in the tunnel header. The encapsulating IP header indicates the presence of the encapsulated IP datagram by using the value in the outer protocol field. The inner header is not modified except to decrement the TTL by 1.

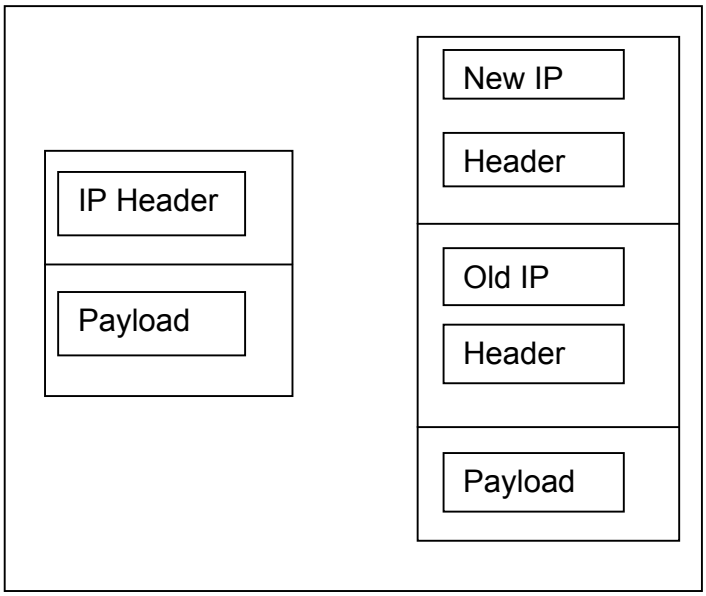


Fig. 2.5 IP-in-IP Encapsulation [11]

CHAPTER 3
PROBLEM STATEMENT

Problem Statement – When the mobility is added to the device it moves from one network to another network and each network is having a unique Net ID. In order to get fit into the new network its old IP address is replaced by new IP address, as a result of it would not be able to inform the other network devices that its IP address is changed and other devices would not been able to communicate with that particular mobile node.

To solve the problem we are going to use the concept of Mobile IP in our thesis work that allows the mobile node to retain its old IP address along with the new IP address when it moves to the new network from the old network.

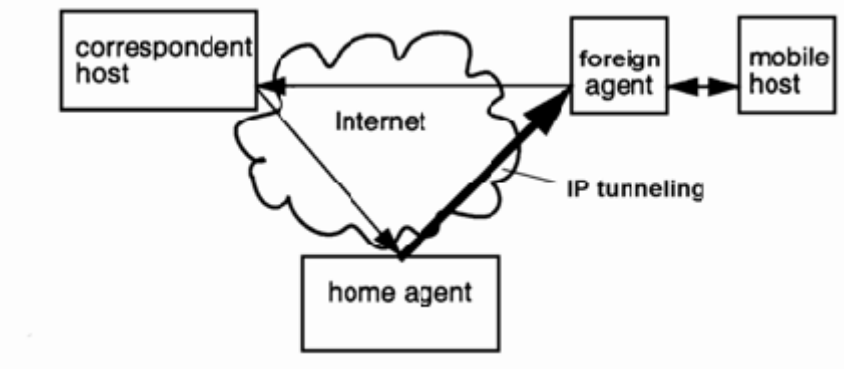


Figure 3.1Mobile IP routing.[22]

Objectives:

The purpose of this thesis is to implement the concept of Mobile IP with the use of NS-2 simulator. The various tasks carried out in achieving the objective can be outlined as follows:

1. Understand the Terminologies used in Mobile IP.
   (a) Home Agent , Foreign Agent, Home Network, Foreign Network, Care Of Address, Address Binding, IP Tunneling, Correspondent Node,etc., 2. Understand the Mobile IP architecture.
3. Understanding the Operations of Mobile IP
4. Learning of the OTCL script and its use in NS-2
5. Implementing and analyzing the Mobile IP concept in NS-2 by creating the necessary mobile nodes by the use of OTCL script.

CHAPTER 4
IMPLEMENTATION OF THE SYSTEM

The effectiveness of any protocol can be appreciated only when statistical data about the performance of the protocol is available. In order to collect the required statistical data, a simulation of the proposed protocol was performed and various scenarios of operation were analyzed. Simulation provides for repeatable, controlled experimentation with only a modest overhead required to construct and carry out simulations. This chapter provides an explanation of the implementation tool. In order to carry out some tests on the designed system, we have to implement it on a suitable language and platform. So we make a choice of the implementation language and implement it in a way that is convenient for simulation.

4.1 Network Simulator-2

The simulation of the protocol is done with Network Simulator 2 (NS2). NS2 supports wireless and standard MIP protocol, provided by the CMU Monarch's model [16]. In this model mobile nodes are independent; each one has one or more interface to the wireless channel. The main function of the channel is to distribute the packets to all the network interfaces, which is using the radio propagation model to know if they are able to receive the packets. There are also gateways between the wired and wireless nodes named a base station (BS) node to facilitate packets routing between wired and wireless networks [16]. NS2 is very useful for developing and investigating variety of protocols. These mainly include protocols regarding TCP behavior, router queuing policies, multicasting, multimedia, wireless networking and application-level protocols. Since NS2 is easily available, and suitable for our work and we choose it to use for our work. The work on NS2 consists of two major parts. The first is an enhancement of the protocol i.e. implementation of a new agent and the second is simulating the protocol.

NS2 uses an object oriented language that is used to simulate different network protocols. Its backend is written in C++ and its front end is OTcl. With OTcl it is possible to configure different network parameters for a system. In order to add our protocol on NS2, we first explore some theoretical concepts of the NS simulator itself. Then specific concepts related to our system which includes adding new protocol and agent and how to integrate the work with NS2 were studied. For each work done we have seen different resources helpful for our work.

NS software promotes extensions by users. It provides a rich infrastructure for developing new protocols. Also, instead of using a single programming language that defines a monolithic simulation, NS uses the split-programming model in which the implementation of the model is distributed between two languages [26]. The goal is to provide adequate flexibility without losing performance. In particular, tasks such as low-level event processing or packet forwarding through simulated router require high performance and are not modified frequently once put into place. Hence, they can be best implemented in compiled language like C++. On the other hand, tasks such as the dynamic configuration of protocol objects and exploring a number of different scenarios undergo frequent changes as the simulation proceeds. Hence, they can be best implemented in a flexible and interactive scripting language like OTcl. Thus, C++ implements the core set of high performance primitives and the OTcl scripting language express the definition, configuration and control of the simulation.

4.1.1 C++ - OTcl Linkage

NS supports a compiled class hierarchy in C++ and also similar interpreted class hierarchy in OTcl. From the user's perspective, there is a one-to-one correspondence (see Figure 4.1) between a class in the interpreted hierarchy and a class in the compiled hierarchy. The root of this class hierarchy is the class TclObject. Users create new simulator objects through the interpreter. These objects are instantiated within the interpreter and are closely mirrored by a corresponding object in the compiled hierarchy. The interpreted class hierarchy is automatically established through methods defined in

class TclClass while user instantiated objects are mirrored through methods defined in class TclObject.

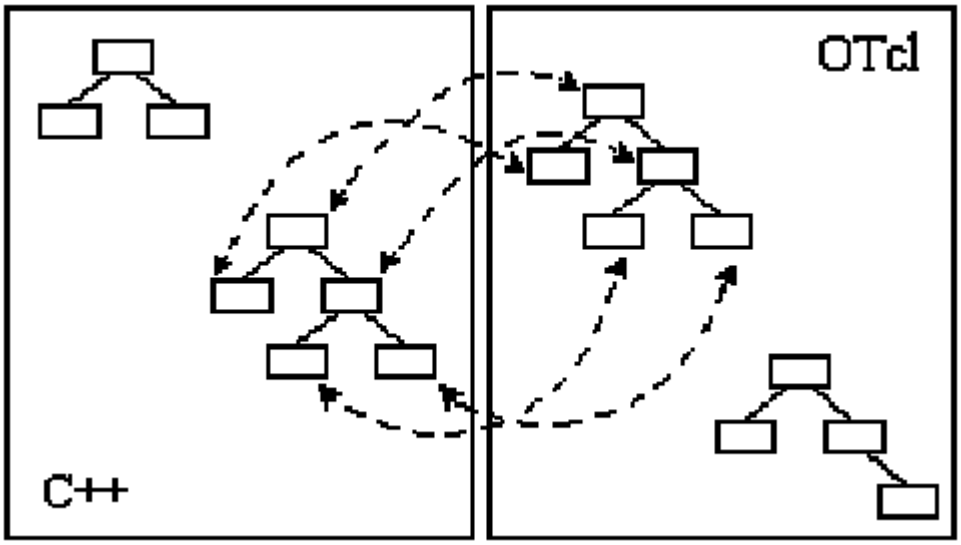


Figure 4.1 C++ -- OTcl linkage.[21]

The following classes are mainly responsible for maintaining C++ and OTcl linkage.

- Class Tcl: This class encapsulates the actual instance of the OTcl interpreter, and provides methods to access and communicate with that interpreter. It provides methods for obtaining a reference to Tcl instance, invoking OTcl procedures through the interpreter, getting or passing the results to the interpreter, storing and looking up "TclObjects" *etc*.

- Class TclObject: It is the base class for most of the other classes in the interpreted and compiled hierarchies. Every object in the class TclObject is created by the user from within the interpreter and an equivalent shadow object is created in the compiled hierarchy. The class TclClass performs this shadowing.

- Class TclClass: This is a pure virtual compiled class. Classes that are derived from this base class provide two functions: constructing the interpreted class hierarchy to mirror the compiled class hierarchy- and providing methods to instantiate new TclObjects.

- Class EmbeddedTcl: The objects in this class are responsible for loading and evaluating some NS scripts that are required at initialization.

- Class InstVar: This class defines the methods and mechanisms to bind a C++ member variable in the compiled shadow object to a specified OTcl instance variable in the equivalent interpreted object. This binding allows setting or accessing the variable from within the interpreter or compiled code at all times.

4.1.2 Major Components

Figure 4.2 [19] shows some major network components model in NS along with their place in the class hierarchy. The root of the hierarchy is the TclObject class that is the super class of all OTcl library objects. NSObject, the direct descendent of the TclObject, is the super class of all basic network component objects that handle packets, which may compose compound network objects such as nodes and links. The basic network components are further divided into two subclasses, Connector and Classifier, based on the number of the possible output data paths. The basic network objects that have only one output data path are under the Connector class, and switching objects that have possible multiple output data paths are under the Classifier class.

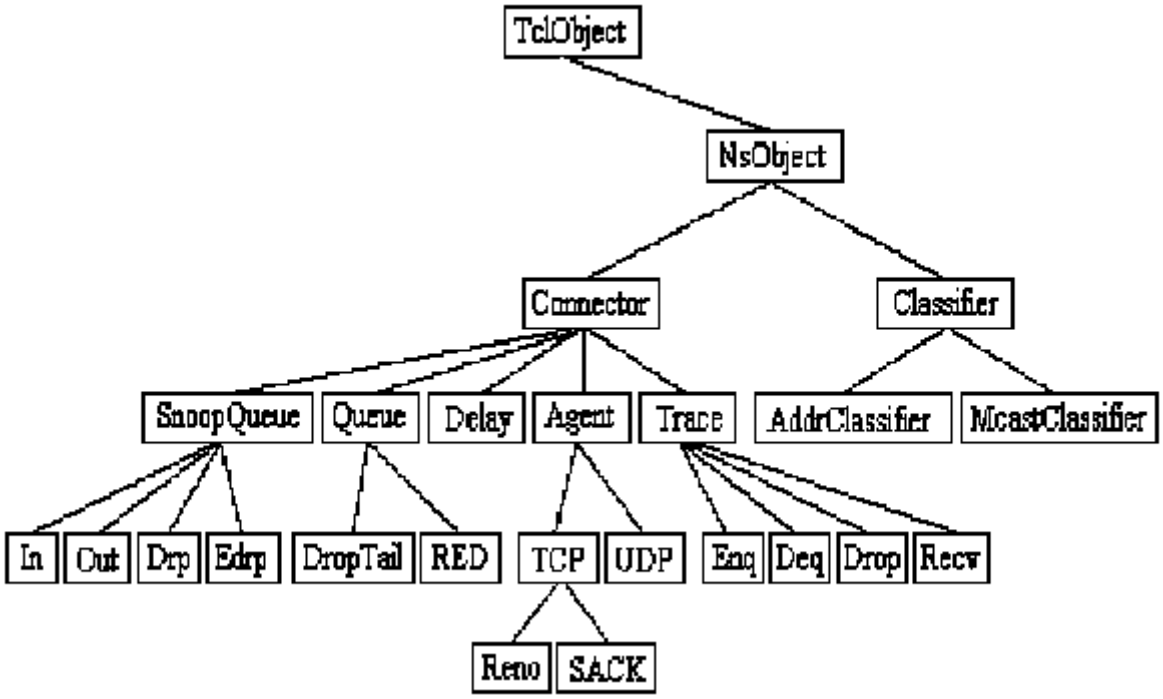


Figure 4.2 Major components in NS [19].

4.2 Further directions

A complete description of the implementation and architecture of NS2 is beyond the scope of this thesis. But there are many good sources available for detailed study of NS2 architecture [21]. Also there are some tutorials that may help start running simulations using NS.

4.2.1The NS Manual

The NS Manual is the full document for the ns2 [23]. It comprises of 46 chapters grouped in different categories. In the beginning chapters it describes the ns2 structure. It describes how ns2 works, interpretation of C++ the configurations done with OTcl. It also describes the importance of each of programming components in ns2.

The second part of this document comprises a wide variety subjects titled basics of simulator. It describes from the simple node configuration to the implementation of new protocol. It also describes some specific network types and their simulation in ns2. Third

part of the document consists of a support for using ns2. The support includes debugging ns, mathematical support, tracing and monitors, ns code styles and others. There are other additional documentations included in it like routing methods, different applications, emulation services, network animations.

4.2.2 Implementing New MANET Protocol in NS2

This is another resource for ns2 that is written in order to develop new protocol in ns2. It is specifically written for people who need developing their own routing protocol in ns2 [24]. In the beginning of the document, it describes the basics of ns2 and it begins on how to write a new protocol. It describes the steps in creating new agent giving a specific example throughout the explanation. It gives the important changes that are needed to be made on different files in ns2.

4.3 Why NS2?

NS2 is a publicly available common simulator with support for simulations of large number of protocols. It provides a very rich infrastructure for developing new protocols. It also provides the opportunity to study large-scale protocol interaction in a controlled environment. Moreover, NS software really promotes extension by users. The fundamental abstraction the software architecture provides is "programmable composition". This model expresses simulation configuration as a program rather than as a static configuration. NS also has certain disadvantages. It is a large system with a relatively steep learning curve [26]. NS's dual language implementation is proving to be a barrier to some developers. But increasing awareness among the researchers along with the other tools like tutorials, manuals and mailing lists have improved the situation.

4.3.1 Mobile IP extension

The NS2 MIP extension consists of a mobile host MH, a home agent HA and a foreign agent FA. The MH is a mobile node, the HA and FA are BS nodes, the NS2 model for the mobile IP node is shown in figure 7. The HA and FA have registration agent, which sends beacons to the mobile nodes, performs encapsulation and decapsulation, and reply

to solicitations from mobile nodes. The MH also have a registration agent, which responds to the beacons and sends solicitations to the HA and FA [16].

The base station nodes broadcast beacons or advertisement messages to the mobile node. The mobile node generates a solicitation message to the BS, which responds with address message send to the MH. Then the MH uses the address of the BS as a care of address. When the mobile node moves from one network to another it changes the care of address. All the packets which destined to the mobile node will be tunneled by the HA to the mobile node's CoA.

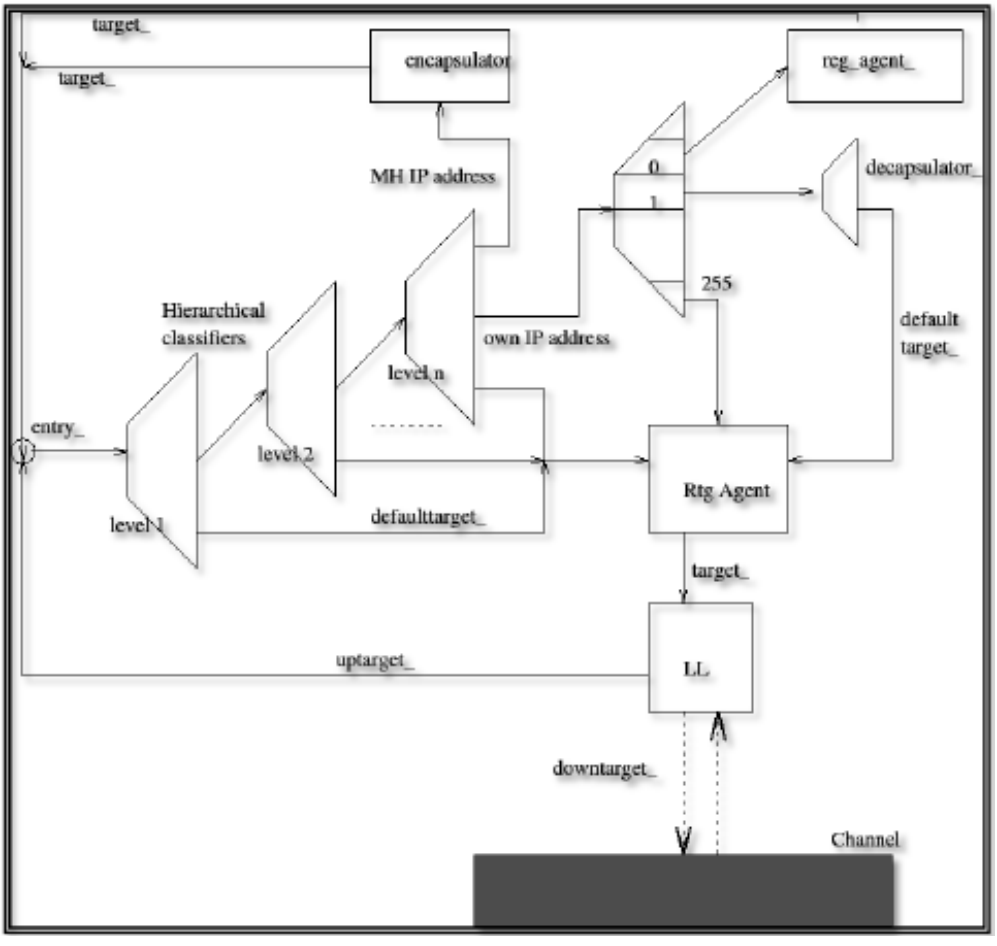


Figure 4.3 NS2 Model of Mobile IP Node [16]

CHAPTER 5
EXPERIMENTAL RESULTS

5.1 Simulation Details and Scenarios

To analyze the performance of the proposed Mobile IP, different scenarios have been considered. They are:

5.1.1 Mobile Host at its Home Network

Figure 5.1 shows that the mobile node is present in its home network and continuously listening the advertisement coming from its home agent.

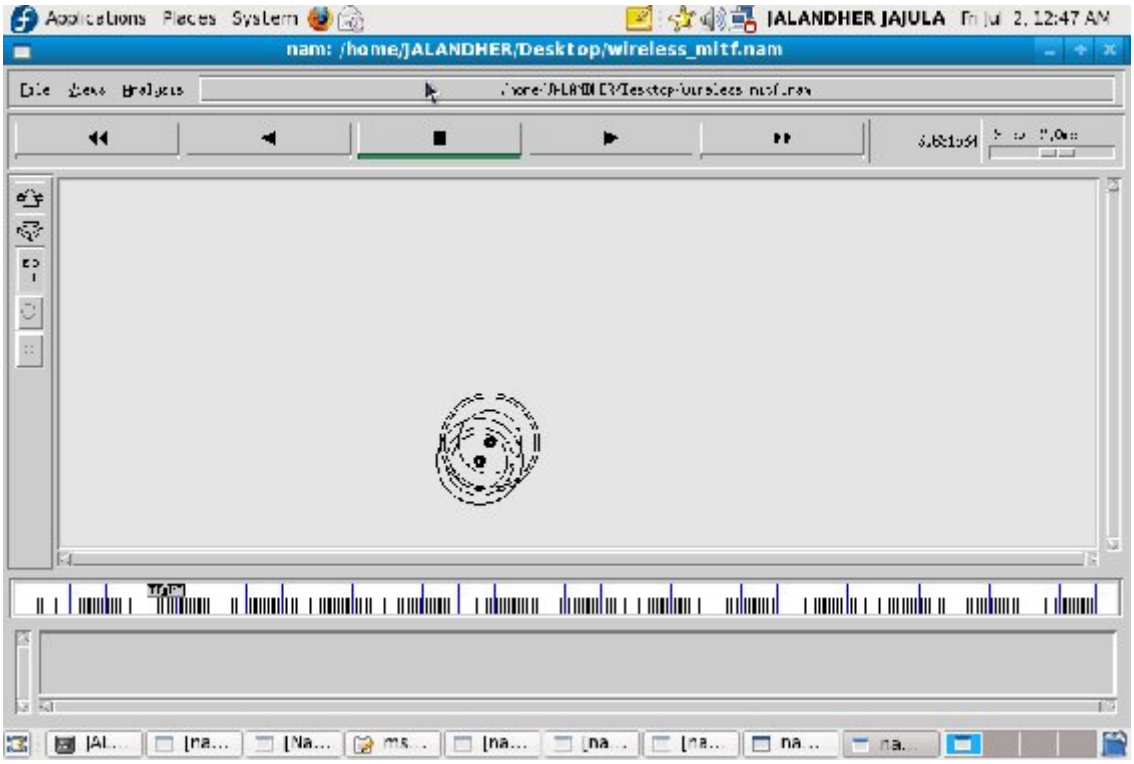


Figure 5.1: Simulation Scenario 1 - MH at Home Network Being Served by HA

5.1.2 Mobile Host leaving from home network

Figure 5.2 shows the mobile host leaving its home network and moving to foreign network.

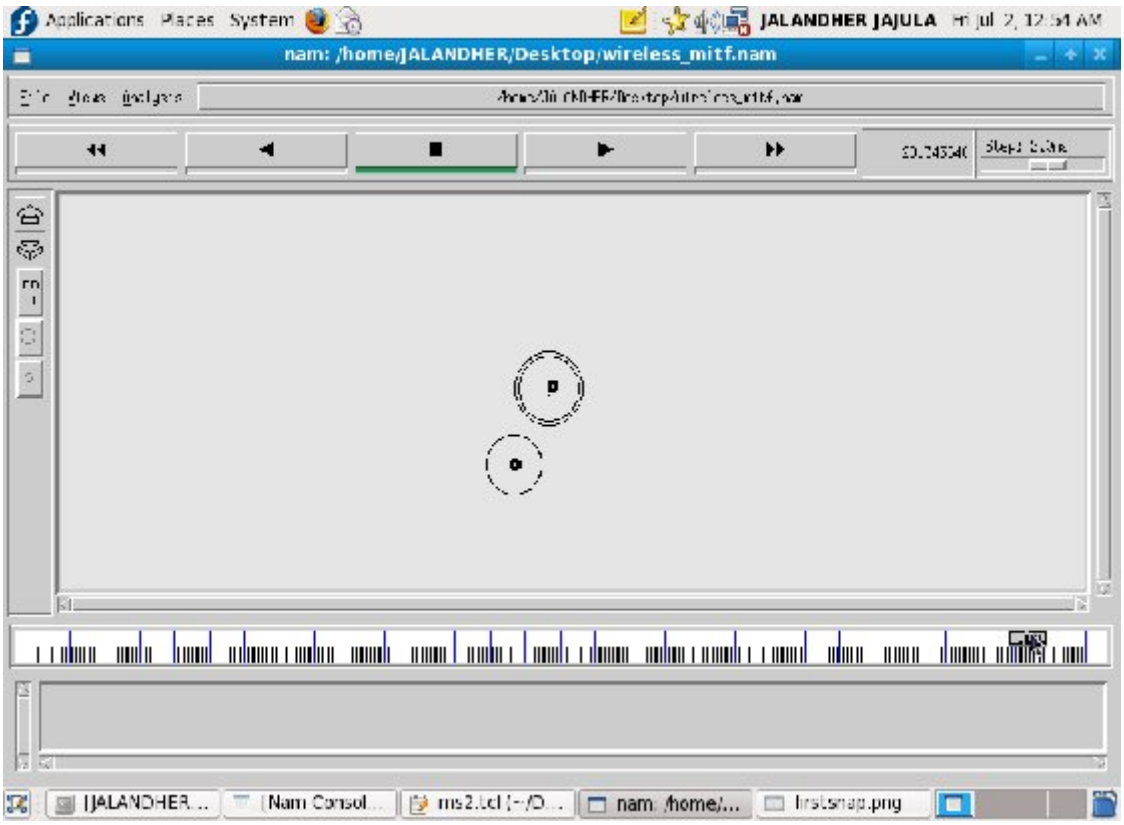


Figure 5.2: Simulation Scenario 2 – Mobile host leaving its Home Network

5.1.3 Mobile Host approaching towards Foreign Network

Figure 5.3 shows the mobile host 4 is approaching towards the foreign network.

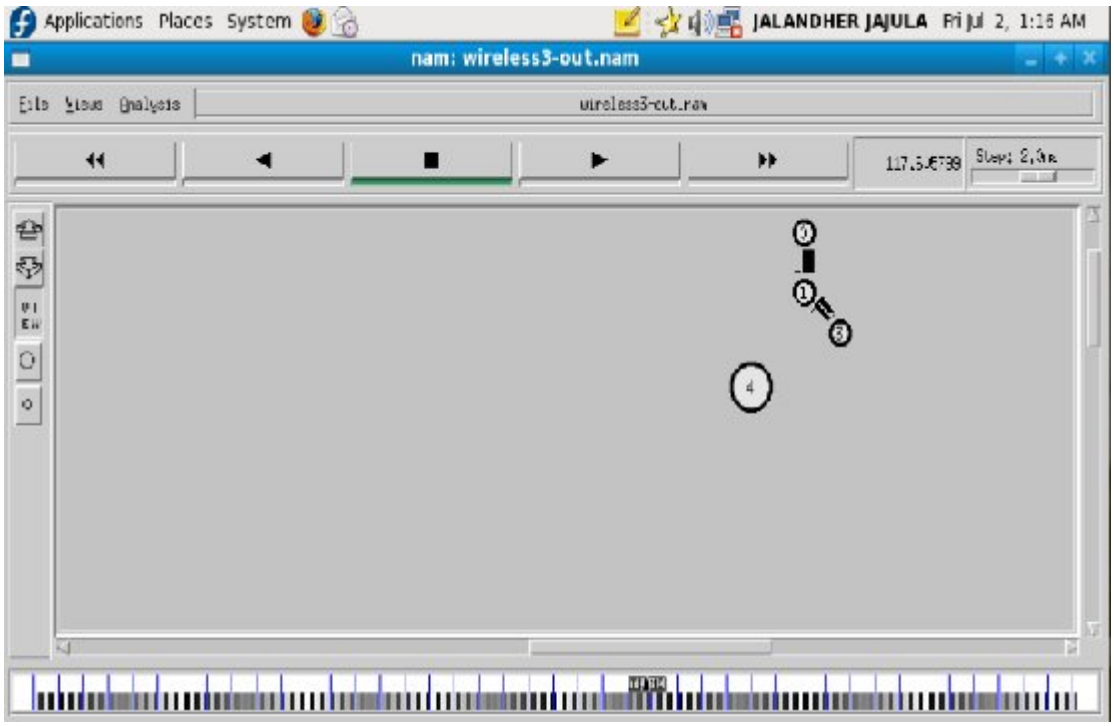


Figure 5.3 Mobile Host approaching the Foreign Network.

5.1.4 Mobile Host listening to advertisements coming from Foreign Agent

Figure 5.4 shows the mobile host reaches to the foreign network and continuously listening to the advertisements send by the Foreign Agent 1 and registered with it and obtain a COA.

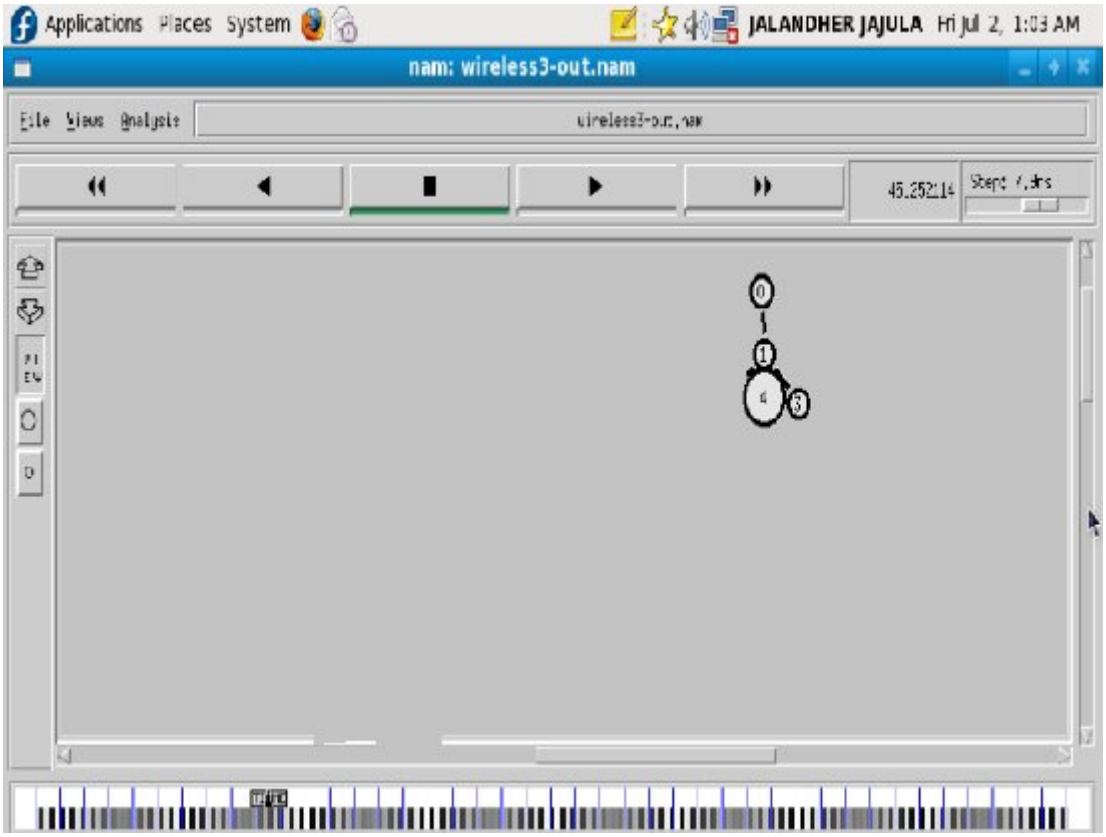


Figure 5.4: Mobile host reaches to the foreign network

5.1.5 Mobile Host receiving the incoming packets via Foreign Agent

Figure 5.5 shows the mobile node 4 receiving the packets from its home agent 2 via foreign agent 1.

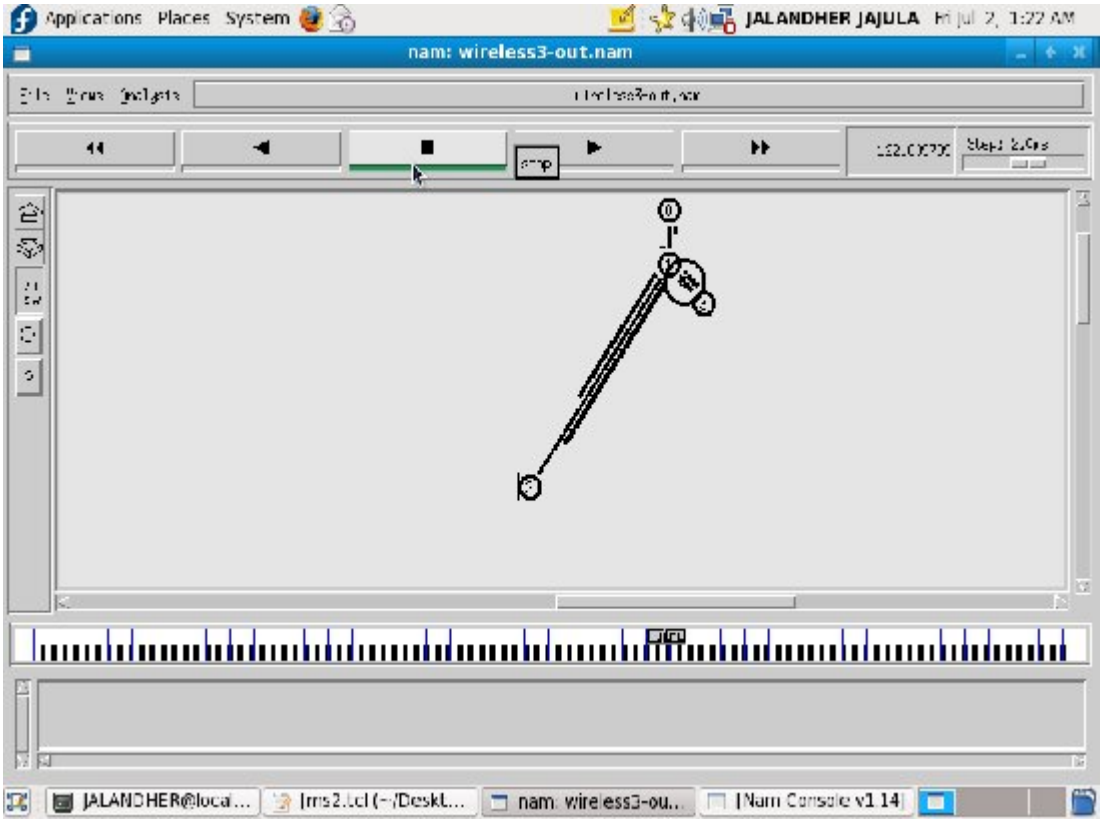


Figure 5.5: mobile node 4 receiving the packets from its home agent 2 via foreign agent 1.

CONCLUSIONS AND FUTURE WORK

Conclusions:

- We have simulated and analyzed the working of the mobile IP by considering different scenarios in which first of all the mobile node is in its home network and Continuously listening the massages from its home agent.
- The next scenario occurs in which the mobile Node leaves the home network and approaching towards the foreign network.
- The last scenario discusses the mobile host is present at the foreign network and receiving the packets from its home agent via foreign agent.

Future Scope:

- In the future, the work can be extended by considering the problem of triangular routing in which it can be seeing that when the communication happens between CN and MN present at the foreign network, the packets meant for MN has to go from CN to HA and from HA to MN as there is no direct communication between CN and MN, thus increases the latency in the delivery of packets.
- It can be extended for further by considering the issues of handoff that may cause jitter, delay and packet losses.
- The work can be extended by implementing the concept of quality of service in the mobile IP.

REFERENCES

[1] Charles E. Perkins, "Mobile IP Design Principles and Practices", Addison- Wesley Wireless Communications Series, Reading, MA, Oct 1997.

[2] Charles E. Perkins, "IP Mobility Support", Internet Engineering Task Force RFC 2002, Oct 1996.

[3] C.Perkins and P.Bhagwat,"A Mobile Networking System Based on Internet Protocol", IEEE Personnel Communications, First Quarter 1994.

[4] C. Hedrick, "Routing Information Protocol", Internet Network Information Center, RFC 1058, Aug. 1988.

[5] M. Borden, E. Crawley, B. Davie, and S. Batsell, "Integration of Real-time Services in IP-ATM Network Architecture", Internet Network Information Center, RFC 1821, August 1995.

[6] J. B. Postel, "Internet Protocol", Internet Engineering Task Force RFC 791, Sep 1981.

[7] S. Deering and R.Hinden, "Internet Protocol, Version 6 (IPv6) Specification", IETF RFC 2460, December 1998, http://www.ietf.org/rfc/rfc2460.txt.

[8] C. Sunshine and J.Postel, "Addressing Mobile Hosts in the ARPA Internet Environment", Internet Engineering Notes, IEN 135, March 1980.

[9] C.Kaufman, Ed., "The Internet Key Exchange (IKE)", RFC 4306, Microsoft, December 2005.

[10] Jochen H. Schiller, "Mobile Communication", University of Karlsruhe Institute of Telematics, 1999.

[11] John Zao, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra, Stephen Kent, " A public- key based secure mobile IP", Wireless Networks, Volume 5, Issue 5, October 1999.

[12] A. Myles and D.Skellern,"Comparison of Mobile Host Protocols for IP", Journal of Internetworking, Research and Experience, 4(4):175,194, Dec.1993.

[13] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[14] F.Teraoka, Y.Yokote, and M. Tokoro,"A Network Architecture Providing Host Migration Transparency", In Proceedings of ACM SIGCOMM '91, pages 209,220, Sept. 1991.

[15] F. Teraoka, K. Uehara, H. Sunahara, and J. Murai, "A Protocol Providing Host Mobility", Communications of the ACM, (8):67, 75, Aug.1994.

[16] "The NS Manual", http://www.isi.edu/nsnam/ns/ns-documentation.html

[17] J. Ioannidis and G. Q. Maguire Jr. "The Design and Implementation of a Mobile Internetworking Architecture", In Proceedings of USENIX Winter '93 Conference, pages 491,502, Jan. 1993.

[18] Chung, Jae, and Mark Claypool. 2000. "NS by Example", Worcester Polytechnic Institute [accessed 1 Feb 2003], Available from http://nile.wpi.edu/NS/.

[19] Breslau, Lee, Deborah Estrin, and Kevin Fall. 2000. "Advances in network simulation". *IEEE Computer*, vol. 33, no. 5:59-67.

[20] J. B. Postel, ed., "Transmission Control Protocol", RFC 793, Sept. 1981. http://www.ietf.org/rfc/rfc791.txt

[21] C. Perkins, D. Johnson, Internet Draft, "Route Optimization in Mobile IP" 09/06/2001. *http://www.ietf.org/internet-drafts/draft-ietf-mobileip-optim-11.txt*

[22] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", IETF RFC 2827, May 2000,http://www.ietf.org/rfc/rfc2827

[23] J. Solomon, “Applicability Statement for IP Mobility Support.“ 1996. RFC 1005.Available at: http://www.cis.ohio-state.edu/htbin/rfc/rfc2005.html

[24] Kevin Fall and Kannan Varadhan (Editors), "The NS Manual", UC Berkeley, LBL, USC/ISI, and Xerox PARC, January 2007.

[25] Francisco J. Ros and Pedro M. Ruiz, "Implementing a New Manet Unicast Routing Protocol in NS2", Dept. of Information and Communications Engineering University of Murcia, Report, December 2004.

[26] “NS2” The Network Simulator ns-2 Documentation, 1 December 2002,Available from http://www.isi.edu/nsnam/ns/ns-documentation.html.