Improvising Mobile IP Operation in Wireless Network Environments

[1]Nilofer SK, [2] S. Srivani
[1]Assistant Professor in Mallareddy Engineering College for women, JNTU, Hyderabad, India
[2]Associate Professor in Mallareddy Engineering College for women, JNTU, Hyderabad, India.

Abstract

Development of wireless and mobile networks is towards all-IP networks, where Mobile IP is seen as de-facto global standard for handling macro-mobility. One may assume that near soon in all-IP scenario all wireless networks will be using Mobile IP. However, this increases the importance of proper implementation of Mobile IP in NS-2 as the most-used simulation environment in the scientific community. Mobile IP protocol is a possible solution that makes Internet available to mobile devices. Mobile IP is located at network layer in OSI model, and is designed as upgrade to existing network layer used in regular IP communication. The goal of Mobile IP protocol is to enable the use of permanent IP addresses and change the location of Internet access at the same time and provides solutions to routing inefficiencies and to have security against attacks.

Keywords - *Mobile IP, NS-2 Simulator, Wireless Network.*

I. INTRODUCTION

An increasing amount of Inter-net users take advantage of wireless technology when accessing the Internet. This gives great benefits, but also has the drawback that connections are lost whenever a user moves to a new network. As we aware of mobile IP that provides seamless roaming across all wireless networks acts as internet standard provides vast applications like media streaming, internet telephony and vital services without interruption when a user moves from one network boundary to other.Inter peak's Mobile IP products are compliant with the WiMAX Forum standards for mobility in WiMAX net-works, and the 3GPP2/3GPP standards for current 3G cellular networks Moreover, the products implement seamless Fast Handover ("make-before-break") for the full support of Voice-over-IP and other real-time applications Internet. Every host in the Internet is identified by unique IP address that consists of a network and host identifier. The IP datagrams are routed to the network in which the host is located and afterwards to the host itself. The IP address is attached directly to the network where the host is located. What happens if the user with unique IP address in the (wireless) network wants to become mobile? The user will try to establish connection with the same address in the new environment and then a problem occurs, the connection can't be established unless the host enters in the range of different access point that is part of the same network. Mobile IP solves this problem by giving mobile hosts and routers the possibility to forward packets from one location to another. However, we have different transport protocols over the IP, where the most important ones are TCP and UDP. If the host is in the middle of UDP session (e.g. VoIP conversation, Online Gaming, Video session) and it moves in the range of a new access point, the blackout period occurs. In this period the Mobile Host (MH) is not able to receive packets. During this period the MH obtains a new IP address and informs the rest of the entities included in the communication process. In this paper we do detailed analysis of behavior of transport protocols in the Internet with implemented Mobile IP for macro-mobility management.

II. RELATED WORK

The basic foundation that led us to take up this idea for this project was based on the works by Babak Shahabi and Shaoyun Yang regarding "Analysis of Mobile IP in Wireless LANs" [5]. Their project compared results between STP and RSTP using NS-2 and OPNET, and we used their NS-2 portion as a reference. Furthermore, we used the NS-2 tutorial about "Creating Wired-cum-Wireless and Mobile IP simulations in NS" by Marc Greis [4]. The tutorial had provided the basic structure for our project to build upon for further research and simulations.

A. Mobile IP operation

Mobile IP is protocol that enables moving between subnets without changing IP address of device. There are three entities in Mobile IP terminology. Mobile node – device or router that has the ability to change its location without changing IP address, home agent – server or router that intercepts packets designated to mobile node, and tunnels them to mobile node's present location. The last is foreign agent – server or router that provides connection services to mobile nodes while they are in its network. In mobile IP the home address seems to be fixed and its job is to identify TCP connections of network whereas care-of address is alterable when it makes attachment to new point and treated to be mobile node network address. Similarly mobile node able to get data continuously on its home network on the other hand mobile IP requires existence of network node called to as home agent. The complete action of mobile IP was depicted in Fig.1

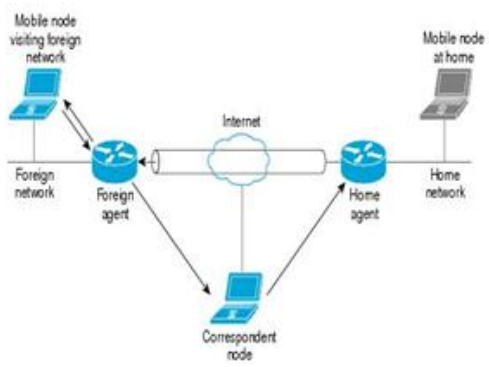

Fig.1 Mobile IP Routing

Whenever the mobile node is not attached to its home network (and is therefore attached to what is termed a foreign network), the home agent gets all the packets destined for the mobile node and arranges to deliver them to the mobile node's current point of attachment. Mobile IP support requires a Mobile Node in each mobile device and a Mobile IP provides an efficient and scalable mechanism for mobility within the Internet as discussed below in two scenarios:

- Mobile IP datagram flow in a network without a Foreign Agent. This requires the Mobile Node to have a public IP address in the visited network.
- In a visited network that contains a Foreign Agent, the Mobile Node does not require any IP address. Furthermore, the Foreign Agent only requires one public IP address for all Mobile Nodes.

The Mobile IP Protocol Home Agent in each such device's home network. Optionally, a Foreign Agent may be present in the network the device is visiting. Both Home Agents and Foreign Agents normally reside within routers in their network. When a mobile device visits another network, IP datagrams destined for the device are intercepted by its Home Agent and tunneled to the visited net-work using a temporary IP address. If there is a Foreign Agent on the visited network, it receives the tunneled packets, unpacks them and forwards them to the Mobile Node; otherwise, the Mo-bile Node itself receives the tunneled packets and unpacks them. Finally, the Mobile Node reinserts the original datagrams into the stack, resulting in a transparent operation using only the original IP addresses. Replies to the originating host can either be sent directly from the Mobile Node to the host, or tunneled back to the Home Agent, which in turn un-packs and forwards the replies to the host. That way of communication is under Mobile IP terminology known as triangular routing mechanism and is illustrated on the Fig.2

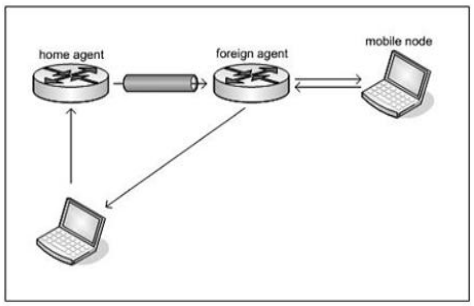

Fig.2 - Paths of Dataflow in Mobile IP

There are three basic processes that make Mobile IP work. They are Mobile IP agent discovery process, agent registration and packet tunneling process through care-of address.

Agent Discovery: Process of discovering Mobile IP agent uses existing router discovery protocol described in RFC 1256 specification. Mobile IP agents for its advertising use existing ICMP router adverts, with special extension contained of Mobile IP data. Within the agent advertisement are information weather the agent is home or foreign, what is his care-of address, his lifetime, and some other features.

Registration: After receiving agent advertisement from a new agent, mobile node realizes that it has changed network location and it has to register with his home agent. Registration mechanism within Mobile IP protocol enables mobile node to inform his home agent about new location and new care-of address. Registration process is also used when registration needs to be refreshed or cancelled.

Tunneling: Mobile IP protocol uses mechanism of IP within IP encapsulation of packets for packets that are intercepted by home agent and sent to care-of address. Also there is a possibility to use minimal encapsulation within IP which reduces overhead but increases time needed for processing tunneled packets.

III. PROPOSED MODEL

A. Building Simulation Environment in NS2

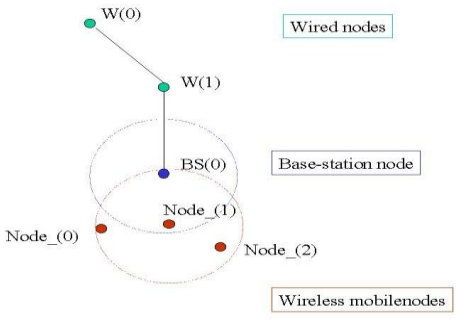

Fig.3Topology of Wireless Cum Wired Simulation in NS2 Environment

For simulation purpose we treated wireless as well as wired domain in which data can be exchanged between non-mobile and mobile nodes. AS shown in above Fig.3 as W (0) and W (1), are connected to wireless domain that consists of 3 mobile nodes namely node0, node1 and node 2 via a base-station node, BS.Thus we can conclude base-stations are acting like gateways between wireless and wired domains that allows packets could be exchanged between two types of nodes.

B. Running Mobile IP in a Simple wired-cum-Wireless Topology

Truly speaking we discussed as far creation of wired-cum-wireless topology that exchanges packets between wired and wireless domain through basestation BS.

So now we discuss how mobile node roam outside the domain of its basestation BS and could able to receive packets that are destined to it, where we still have similar wired domain consisting of 2 wired nodes, W0 and W1 and 2 base stations termed to Home Agent (HA) and Foreign Agent (FA) respectively, where wired node W1 is connected to HA and FA as shown in the Fig.4 below.

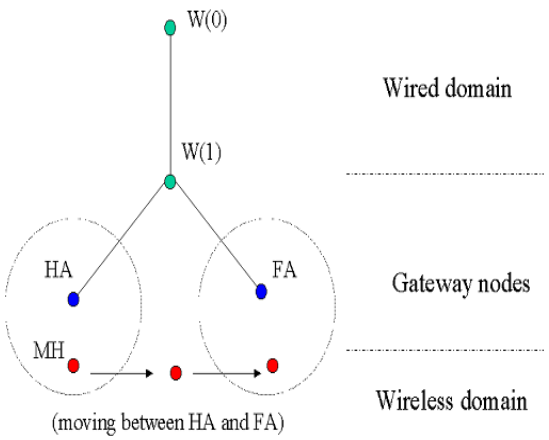

Fig.4 Topology for Mobile IP Simulation

Also a roaming mobile node termed to Mobile Host (MH) that had journey between its home agent and foreign agents. As we would set up a TCP flow between W0 and MH, then Mobile Host (MH) moves out from the domain of its home agent(HA) , into the domain of FA.So we therefore observe how packets are destined for MH is redirected by its HA to the FA as aforementioned mobile IP protocol

Problems Facing Mobile IP: As more serious outstanding problem facing today by Mobile IP is that of security, and other one is Routing inefficiencies. So in turn Mobile IP specification has the effect of introducing a tunnel into the routing path that is followed by the packets sent by the correspondent node (CN) to the mobile node. In the same way packets from the mobile node, on the other hand, destined directly to the correspondent node without need of tunneling phenomenon. So this part of asymmetry is captured well by the term triangle routing, in which a single leg of the triangle travels from the mobile node to the correspondent node, and the home agent forms the third vertex that control the path taken by data from the correspondent node (CN) to the mobile node. Finally Triangle routing is concluded by use of techniques in the route optimization draft, [2] but doing so requires altering in the correspondent nodes that will take a long time to deploy for IPv4 which leads to that triangle routing will not be a factor for IPv6 mobility.

C. Implementation Details

The main objective of the simulation was to discover which base station was forwarding packets to the MN at which time in the two cases as shown in Fig.5.

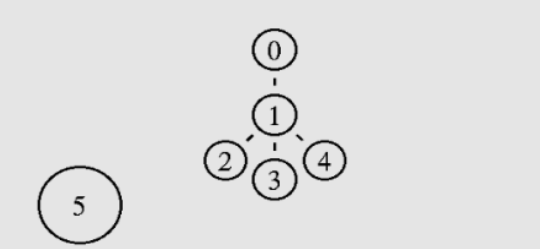

Fig.5: Basic Implementation Model.

Case 1: Downloading to Mobile Node

1) In the initial scenario MN starts travelling to the right at a speed of 10m/s ,during this time the MN is attached to its HA.
2) During 20s the correspondent node (CN) begins sending a file to the MN, as these packets are originally sent directly to the MN via the HA, but as the MN moves out of range in the network, they must be rerouted through the Foreign Agents(FA's) only.
3) Similarly during 80s the MN will turn around and make a back journey towards to its starting position at an increased rate of 20m/s. Thus speed is increased to limit the amount of time that the MN will be out of range of any of the FA's.
4) After completion of successful simulation, a trace file with the new API was generated that helps us to get the data regarding the transmission process during simulation.

Case 2: Uploading from Mobile Node

Here in this case scenario was the opposite of the first case. Thus MN was to upload a file to the CN making its journey through the various networks. To make comparison with first case, the same path was taken by the MN with the same kind of speeds. Moreover in this situation the trace file was also used

to retrieve data regarding when packets were sent and received. It also tracked which base station was transferring the packets to the CN.

For finding the complete details of the trace file and exactly extract only the information that was required we used a scripting language called AWK. The main purpose of AWK is to find through a data file and search each row for certain desired parameters. Also our AWK files found the trace files that determines if the event was a send or receive, where the packet was sent from and which node received it, the packet type, packet ID, and packet size.

So therefore after AWK had finished creating the data file, then MATLAB was used to plot the data in each file separately. We wrote a MATLAB script that would read all the data from the file and find it in the most correct way for well detailed plots. We believed this was the most effective and polished way to present our observations during the simulations process.

IV. SIMULATION RESULTS

This section presents all of the results that were obtained from our separate NS-2 simulations for each scenario. The data presented consists mostly of MATLAB plots that were generated from the trace files after they were filtered by our AWK script.

The actual time of each simulation was under ten seconds for each the simulation, AWK file, and MATLAB plot development. Fig.6 shows the MATLAB plot from the first scenario of downloading to the MN. It is color coded to show which base station receives each packet as the MN moves across the networks.

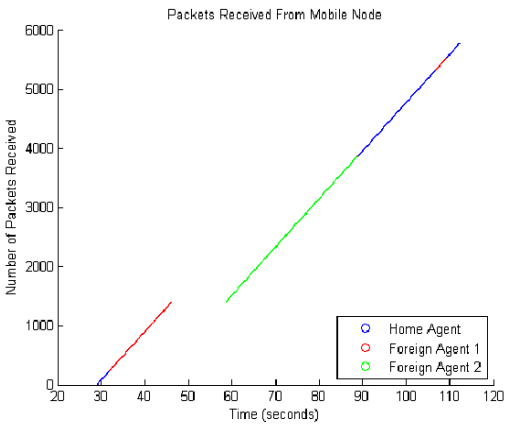

Fig.6: Scenario One No. of Packets Received vs. Time.

In each of the plots; blue represents the HA, red the first Foreign Agent (FA), and green the second Foreign Agent (FA).

Fig.7 shows the position versus packets received graph to demonstrate where the MN's X position is when each packet is received. This gives a better visual representation of the area covered by each base station.

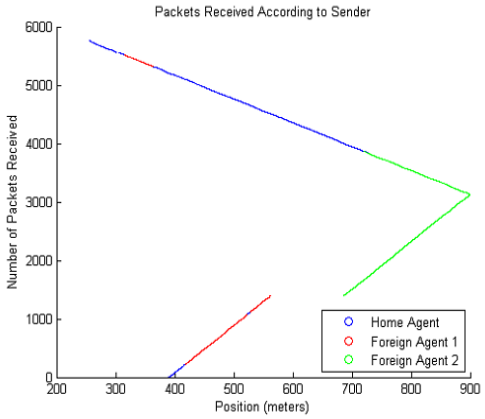

Fig.7: Scenario One No. of Packets Received vs. Position.

Fig.8 depicts the scenario in which a MN is uploading data to a CN as it traverses each network. We therefore had hoped to detect which base station each packet was sent to but found it seems to be complex to detect this in the trace file because each event showed that the packet was destined for the CN and does not indicate which base station the packet was expected to receive each packet.

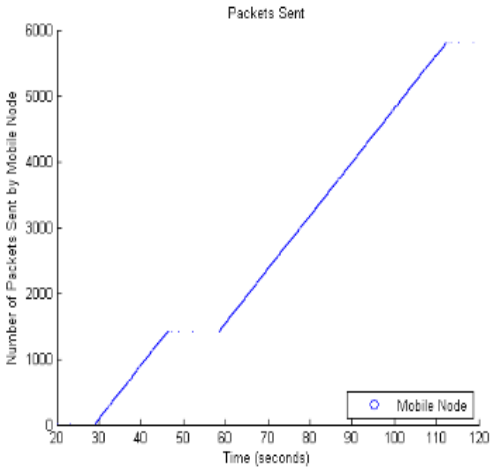

Fig.8 Packets Sent by Mobile Node

Fig.9 shows how the packets received by the CN as well as the base station node that forwarded each packet from the MN. This plot shows identical gaps in transmission just as the previous plots have shown.

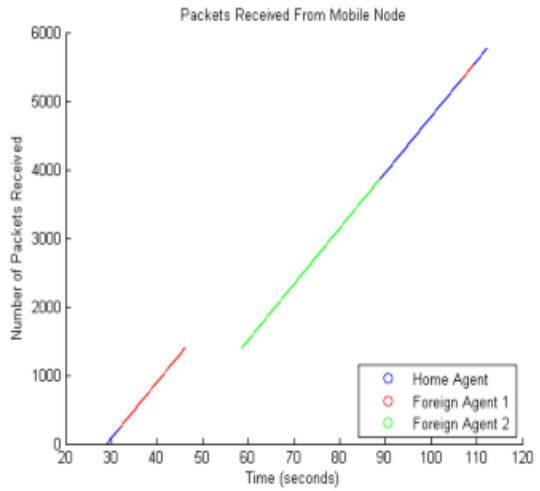

Fig.9 Packets Received from Mobile Node

Finally from above results however has an unexpected switch to the HA from FA2. We would thought that its position at the time would lead it to switch first to FA1 and then immediately back to the HA. We trust this behavior is a great example of the poor handover procedure used by the current MIP models in NS-2. We also noticed that dropping of packets while switching networks from HA to FA1 that is due to reason of MN being out of range of both agents.

V. CONCLUSION

We found that the research done in this project was very beneficial by giving us an in depth understanding of MIP, NS-2, and other tools. We learned that we use MIP constantly in everyday life and it will continue to be a very important protocol as mobility becomes of increasing importance in networks. It was also interesting to learn how the handoffs between networks are resolved by the MN to allow consistent data transfer between the MN and CN. It also lets us to extend out previous knowledge of C, MATLAB, and Linux to become much more proficient users of each tool.

REFERENCES

[1] J. Geier, Wireless LANs, Second Edition. United States of America. Sams Publishing. pp. 189 July 2001.

[2] "NS-2: User Information" [Internet] Avaiblable:http://nsnam.isi.edu/nsnam/index.php/User_Information, [April 2012].

[3] Mobile Networking – Research Areas Avail: http://monet.postech.ac.kr/research.html

[4] M. Greis. "Marc Greis Tutorial for the UCB/LBNL/VINT Network Simulator "ns"." Avai:http://www.isi.edu/nsnam/ns/tutorial/, [April 2012].

[5] B. Shahabi and S. Yang, .Analysis of Mobile IP in Wireless LANs, [Online] Avail: http://www2.ensc.sfu.ca/~ljilja/ENSC835/Projects/khan_sarai/Group6Final_report_ensc835. Pdf. Simon Fraser University, Burnaby, BC, 2011 [April 2012].

[6] G. Goebel. "An Awk Primer." [Online] Avail:http://www.vectorsite.net/tsawk.html [April 012]

[7] C. Palazzi, B. Chin, P. Ray, G. Pau, M. Gerla, M. Rochetti. "High Mobility in a Realistic Wireless Environment: a Mobile IP Handoff Model for NS-2." [Internet] Avail: http://www.math.unipd.it/~cpalazzi/papers/Palazzi-MobileIP.pdf. [April 2012].