ENSC 835-3: NETWORK PROTOCOLS AND PERFORMANCE

CMPT885-3: SPECIAL TOPICS: HIGH-PERFORMANCE NETWORKS

Route Optimization on Mobile IP over IPv4

Spring 2002

FINAL PROJECT

Hao (Leo) Chen
lcheu@sfu.ca

http://www.sfu.ca/~lcheu/885-project.htm

Contents

List of Figures

Abstract

The support of mobility in the modern communications networks is becoming essential and important with the booming development of mobile devices. Mobile IP[RFC3220], built on IPv4, was designed by IETF 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. On the other hand, the datagrams sent from the mobile node to other wired nodes can be routed directly. 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. IETF proposed extension part of the basic mobile IP, called ”Route Optimization”[ROMIP] to address this problem. Other approaches, like reverse routing [ZY99] are also proposed for this purpose. Actually, in the next generation of the Internet Protocol - IPv6, ”Route Optimization” is integrated as a fundamental part of the mobility support [MIPv6]. However, IPv4 has already been widely deployed and will continuously dominate the Internet for a long time. Therefore, the study of Route Optimization is still of interest to me. My project is to add the Route Optimization on Mobile IP to the *ns-2* . More specifically, I implemented two Route Optimization messages out of four. Simulations have already been done to justify the modification.

The first section of the report is a survey on the routing schema in mobile IP protocol, including the “Triangle Routing” problem and the Route Optimization extension in MIP. The second section focuses on the current implementation architecture of mobile IP in *ns-2* . Section 3 is the highlight, elaborating my implementation of Route Optimization on mobile IP in *ns-2* , from the system architecture modification to the implementation details. After extending Route Optimization on mobile IP, simulations should be carried out for validation. The simulation scenarios, scripts and results will be presented in the section 4. Then, the report is finalized with the summary and discussion in section 5.

1 Introduction

This section describes what the Mobile IP is and the Route Optimization approach for the Mobile IP in IPv4, and the project objectives as well. The following subsections are very descriptive in terms of helping the reader to understand the main ideas behind our project and get the feeling about the scope of this project.

1.1 What is Mobile IP?

The exponential growth of portable devices, including: laptop and palmtop computers, personal organizers, etc., and increasing number of wireless devices and services — dictate the need for mobility support in today’s network communications.

To simplify future references to the above devices we will name all the portable and wireless devices - mobile devices. In fact, the main reason to call these devices “mobile devices” lays in their very nature. These devices are not stationary to the network and frequently change their point of access to the network/Internet. All these make these devices considered as the mobile ones. For further clarification and purposes of our project we will call mobile devices - mobile nodes.

Let’s just say here that Mobile Node (MN) is a host or router that changes its point of access from one network or subnetwork to another. In the project itself we will be mainly concern with the Mobile Host (MH). In our project MH will be the main target and representative of the MN for the purpose of establishing and monitoring the network connection between the correspondent host (either mobile or stationary) and the target MH.

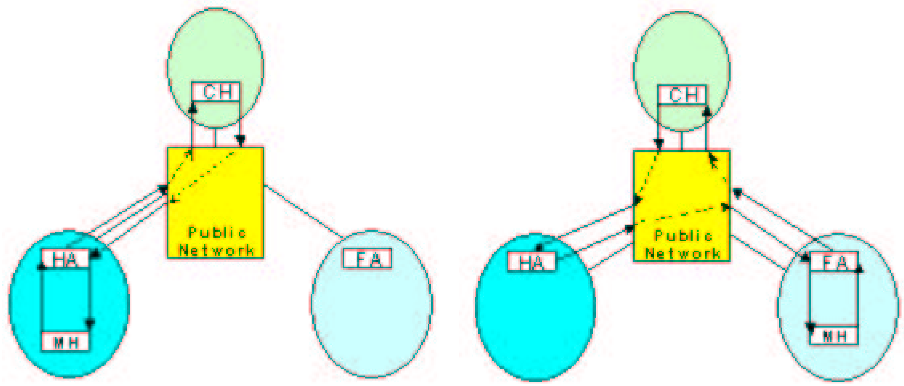
Now, after all the declarations above, we are ready to move on and explain what the Mobile IP actually is. Mobile IP (MIP) protocol was built on the top of the Internet Protocol (IP) to support the mobility. In that sense, MIP protocol for IPv4 provides continuous Internet connectivity to MH.

The IP layer was picked for implementing basic mobility support as the most appropriate one, compared with lower or higher layers. The problem with lower layers, such as the Link layer solutions, is that they are limited to a single medium. One of the most important and guiding principles of the Internet is to find general-purpose solutions that work for all network technologies, as opposed to special-purpose and hardware-specific solutions. Also, mobility solutions that require big changes at layers above IP tend to be highly impractical.

MHs have to switch between networks in different domains while they move around the network, they also need to switch between different types of network (Ethernet, packet radio, cellular telephone, etc.) to achieve the best possible connectivity regardless of where they are located.

MIP protocol allows MHs to send and receive datagrams addressed with their home network IP address, regardless of the IP address of their current point of access to the Internet. MIP protocol allows any MN to move about and to change its point of attachment to the Internet, while continuing to be identified by its home IP address. Home IP address of the MN refers to the node's IP address on its home network.

Correspondent Host (CH) sends IP datagrams to the MH at any destination, regardless of whether that MH is in its home or other (foreign) network, in the same manner as if the MH never leaves its home network. All the packets destined to the MH go through the Home Agent (HA): which tunnels them to the MH directly, if it is in the home network (see Figure 1 (a)), or through the Foreign Agent (FA), if the MH is in foreign network (see Figure 1 (b)). The MH on the other hand sends its IP datagrams directly to the CH, meaning that, when MH is located on foreign network, packets are not routed to the HA and therefore bypass going through the home network on their path to CH. The MIP protocol is simple and provides transparent routing of packets to MH. MIP protocol is compatible with existing applications and hosts, and doesn't place special burdens on IP routers and CHs in the Internet.



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

Figure 1: MH in home/foreign network
Communications between MH and CH are shown by arrows in this figure

As you probably already noticed, the routing scheme of basic MIP protocol in IPv4 is far from perfect. The route used for packets from CH to the MH is not the most efficient. Packets from CH to MH have to go through three different (sub)networks: the CH's subnet, the HA's subnet, and the FA's subnet where the MH is currently located. This performance problem with MIP is known as "Triangle Routing".

"Triangle Routing" allows transparent inter-operation between MHs and their CHs, but forces all datagrams for an MH to be routed through its HA. Therefore, packets to the MH are often routed along paths that are significantly longer than optimal. For instance, if MH is visiting some subnet, even packets from CH on the same subnet must be routed through the Internet (Public Network) to the MH's HA (on its home network), only then to be routed back to the original subnet for final delivery. This indirect routing delays the delivery of the packets to MHs and places an unnecessary burden on the networks and routers along their paths through the Internet.

To avoid the "Triangle Routing", an extension to the basic MIP protocol called "Route Optimization" [ROMIP] was proposed.

1.2 Route Optimization

Route Optimization gives a way for any host to maintain a **Binding Cache** (a cache of mobility bindings of mobile nodes, maintained by a node for use in tunneling datagrams to those mobile nodes) containing the Care-Of Address (COA) of one or more MH(s). When sending an IP datagram to an MH, if the sender has a binding cache entry for the destination MH, 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 MH will be routed to the MH's home network and then tunneled to the MH's current COA by the MH's HA. This is the only routing mechanism supported by the base Mobile IP (MIP) protocol. With Route Optimization the original sender of the datagram will be informed of the MH'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. CH can create a binding cache entry for an MH only when it has received the MH's mobility binding.

When an MH's HA intercepts a datagram from CH and tunnels it to the MH, the HA decides that the CH has no binding cache entry for the destination MH. The HA then will send a **Binding Update** (a message indicating a mobile node's current mobility binding, and in particular its Care-Of Address) message to the CH, informing it of the MH's current mobility binding. Upon receiving a Binding Update message from the HA of the MH, CH then can store a binding cache entry for the MH. Once CH has a binding cache entry for the MH, it will tunnel the datagram to the Mobile Host's Care-Of Address.

The following Figure 2 are intended to help to understand how the Binding Update in Route Optimization works. The figure showing communications between CH and MH, when MH is in its home network, will be skipped, since in that case the communication pattern is the same to the operation of basic MIP protocol.

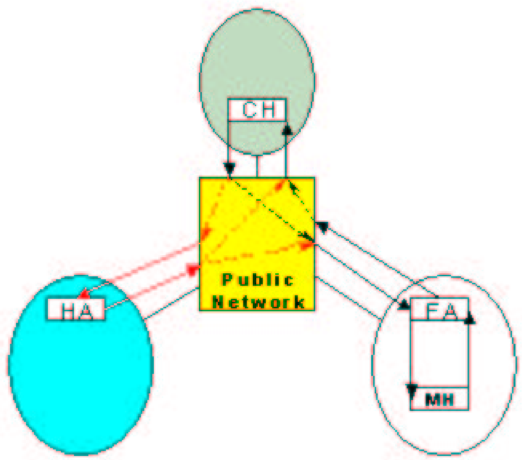


Figure 2: MH in foreign network
Communications between CH and MH are shown by arrows in this figure

The Figure 2 shows that when CH sends its initial datagram to the MH, HA tunnels the datagram to FA and sends **Binding Update** message to the CH (this initial stage of communication is shown by red arrows in the figure). FA forwards all the datagrams destined to the MH to it. After CH gets a Binding Update message from HA, it creates a binding cache entry and uses it for future communications with the MH. In that sense, future IP datagrams from the CH to the MH are routed directly through the FA, skipping going through the HA of the MH. IP datagrams from the MH to CH follow the same route as in the basic MIP protocol scenario.

The Binding Update message is used for notification of a mobile node's current mobility binding. It is sent by the Home Agent to the Correspondent Host. However, when the mobile node moves to another foreign network and has obtained a new Care-Of Address, the CH will still send the packets to the expired Care-Of Address of the MH until the entry in the Binding Caches expired, which will result in much loss of the packets. After the entry in Binding Caches expired, CH would tunnel the packets to the new COA of the MH only after received a new Binding Update message from the HA.

In order to reduce the packet loss in this situation, another Route Optimization message called **Binding Warning** is introduced to address this problem. The Binding Warning message is used to transmit warning that a Binding Update message is needed by one or more correspondent nodes. The mobile node can initiate a Binding Warning message to its home agent, requesting the home agent to send a Binding Update message to its correspondent host whenever it obtains a new Care-Of Address from a new FA. The following Figure 3 illustrates the situation when the MH moves from one foreign network to another foreign network, a Binding Warning message from MH to HA triggers a Binding Update message from HA to CH. Then, the CH will directly tunnel the packets to MH.

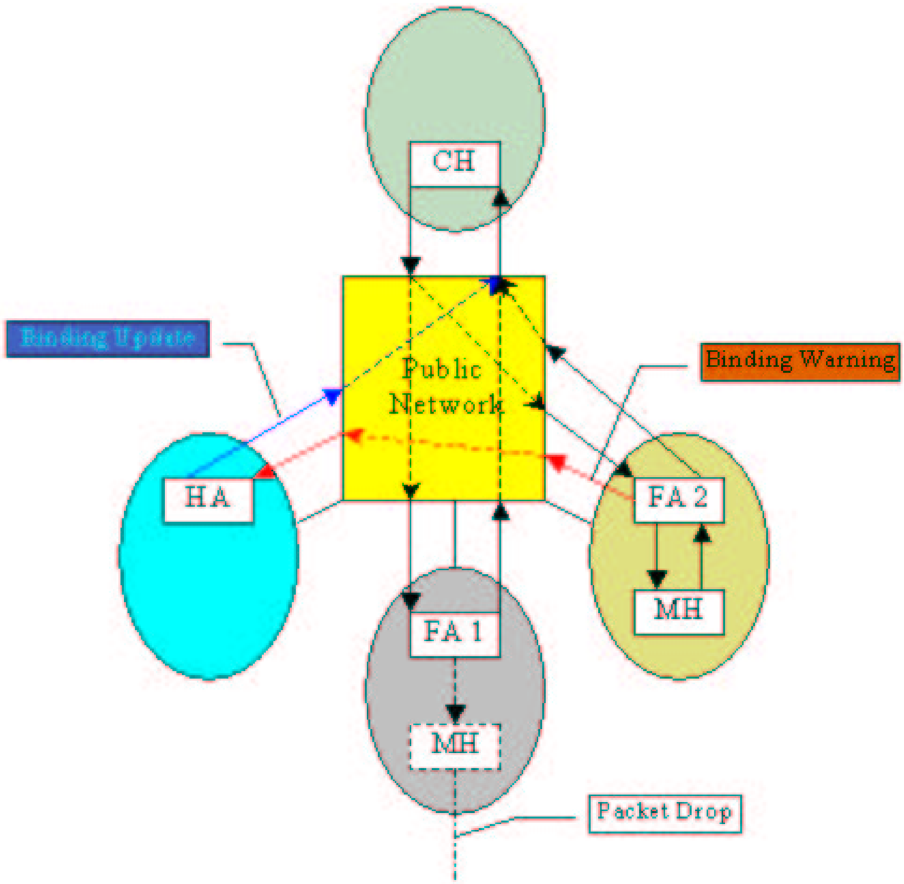


Figure 3: MH in foreign network 2
Communications between CH and MH are shown by arrows in this figure

The complete Route Optimization extension specified by [ROMIP] includes other two kind of messages: Binding Request Message and Binding Acknowledge Message. Binding Request message is used by a node to request a mobile node's current mobility binding from a mobile node or the mobile node's home agent. Binding Acknowledge message is used to acknowledge receipt of a Binding Update message.

1.3 Project Objectives

In the project, I will implement the Route Optimization extension of mobile IP over IPv4 in *ns-2* , since the basic mobile IP has already been implemented by Sun Microsystem Inc. and the mobile network support has been implemented by the Monarch project of CMU in *ns-2* . Also, the basic mobile IP over IPv6 in *ns-2* has been completed by MobiWan project of MOTOROLA Labs and INRIA Phone-Alpes PLANETE[NSDoc].

My implementation includes 2 of the 4 Route Optimization messages:

- **Binding Update** Message
- **Binding Warning** Message

We need to modify and extend the current modules of Mobile IP in ns-2. After the extension, we will compare the usual routing scheme in Mobile IP without optimization to the routing with optimization in terms of the end-to-end packet delay. We will show that Mobile IP with the Route Optimization extension conducts a better performance than basic Mobile IP with smaller end-to-end packet delay. Due to the time limitation, my implementation won't cover the timer part in the route optimization messages, which is used to keep the messages updated.

The objectives of the project are listed as follows:

1. Understand the mobile IP (*MIP*) protocol in IPv4.
2. Understand the Route Optimization in mobile IP.
3. Figure out the current mobile IP architecture in *ns-2*.
4. Implement the Route Optimization of mobile IP (*ROMIP*, part) in *ns-2*.
5. Simulate the MIP scenarios with and without Route Optimization.
6. Analyze and evaluate the simulation results of MIP with and without Route Optimization.

2 MIP in current *ns-2*

To figure out the current architecture of Mobile IP implementation in *ns-2* is the first and mandatory step of the project.

Regarding the current MIP architecture in *ns-2* , it is contributed by both CMU's Monarch group and SUN Microsystem Inc.. Monarch group extended the mobility support in *ns-2* while SUN introduced the mobile IP into *ns-2* . But, since the original CMU wireless model only allows simulation of wireless LANs and ad-hoc networks, the wired-cum-wireless feature was then developed 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.

As we introduced before, typical Mobile IP scenario consists of Home-Agents(HA), Foreign-Agents(FA) and Mobile-Hosts(MH). In the current *ns-2* system, HA and FA are basically the same kind of node - **Base-Station Node** in the *ns-2* system and they use the same Agent - **MIPBSAgent** 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.

Through the source analysis, I summarize the current routing schema in the mobile IP architecture of *ns-2* as follows:

1. If the MH is within the domain of its own HA, i.e., in the home network, the MH communicates with the CH through route_agent in usual routing manner.

2. If the MH moves to the domain of a FA, i.e., in the foreign network, during the registration phase, FA sends a REG_REQUEST message to the HA with the new Care-Of Address(COA) of the MH. One point should be noticed here that during the registration phase, the packets sent to the MH will be lost.

   - When the HA receives the REG_REQUEST message from the FA, it calls an OTcl function - "encap-route" to add a route which specifies a MIPEncapsulator to handle all the future packets destined to the MH with MH's home IP address.
   - If the REG_REQUEST message receives by the HA specified the same COA as the IP address of HA, which means the MH has returned home, the HA will call an OTcl function - "clear-reg" to clear the registration information for this MH. And, the later communication between the MH and the CH will go through the usual routing path.

3. After the MH registers its COA to its HA, all the packets afterward destined to the MH 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 IPinIP 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 deliver to the MH using the wireless route agent.

3 Implementation of Route Optimization of MIP in *ns-2*

In this section, we discuss the implementation details of Route Optimization of MIP using both text descriptions and flowcharts. We first discuss the main challenges encountered in the project, then the design of implementation of both **Binding Update** message and **Binding Warning** message. Finally, we summarize the implementation details in the source code level.

The following Figure 4 is a vivid overview of the basic concept of Route Optimization in MIP in the perspective of packet delivery.

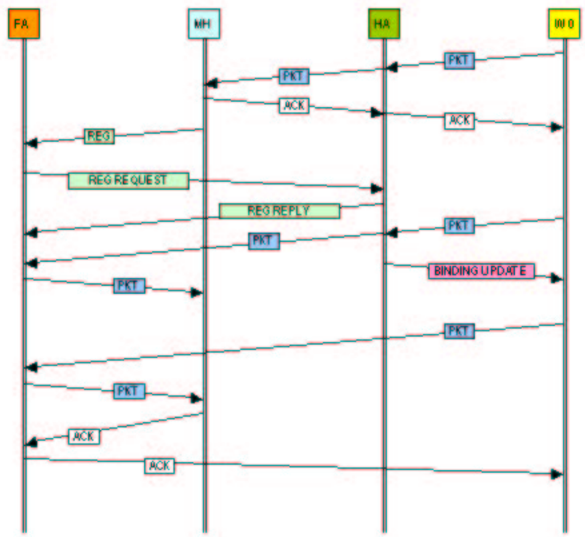


Figure 4: Overview of Route Optimization in MIP

3.1 Three Challenges

Among the many challenges I encountered in the project implementation, the following three are the key points.

1. The first challenge in the implementation is how to implement the mobile IP on the correspondent node. The CH should be able to handle mobile IP messages, otherwise the Route Optimization can't be implemented. The straightforward approach is to employ the current HA/FA implementation and use it as the base of the correspondent node, which is the way I exploited.

2. The second technical challenge is to determine where I can insert my **Binding Update** and **Binding Warning** message code into the original architecture. This obstacles was overcome by tracing the execution of the *ns-2* .

3. Another technical challenge is how to split the code into C++ and OTcl in the *ns-2* . I address this problem by emulating the existing codes.

3.2 Binding Update Message

For the **Binding Update** message, the design consists of two parts.

1. The first part is the HA part. It is the Binding Update message sending of HA.

   The current MIP implementation in HA is to enable the MIPEncapsulator, and the MIPEncapsulator will handle every packet destined to the MH after registration. Therefore, we insert the code of sending Binding Update message into the MIPEncapsulator's packet handler.

   In order to avoid mis-sending binding update message, we check the IP address of the HA and the destination IP address of the packet. If the network address of the HA and the destination IP address of the packet are the same, which means that this node is actually the HA of the destinate MH, the Binding Update message will be sent out. Otherwise, the MIPBSAgent just forwards the packet in the usual routing manner.

   The Figure 5 could illustrate the process logic as follows.

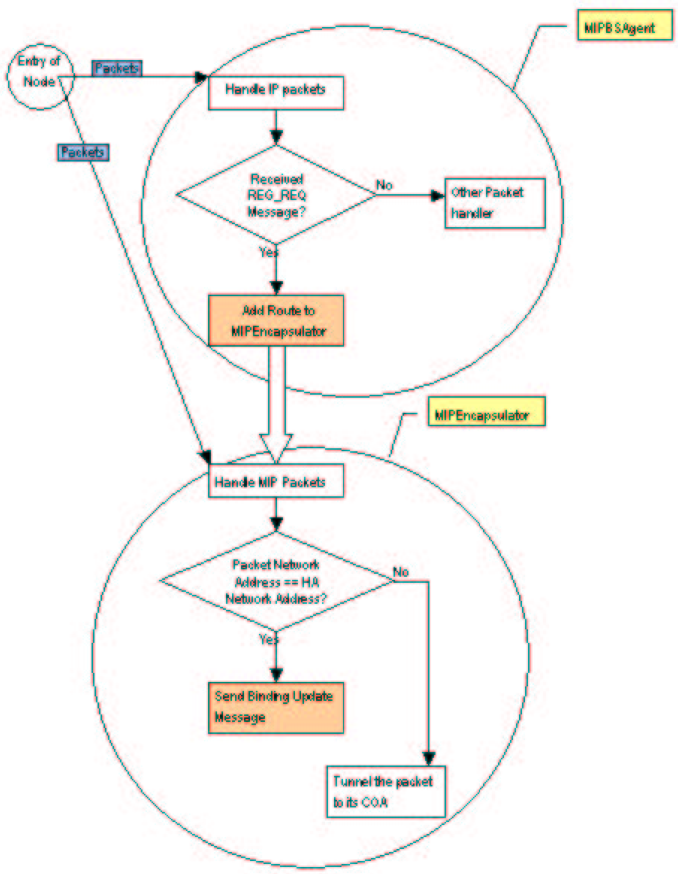


Figure 5: Flowchart of Sending Binding Update Message

2. The second part is the correspondent node part. It is to handle the Binding Update message.

   The correspondent node should follow the specification of MIP[RFC3220] to handle the MIP packets and store the Care-Of Address for the corresponding MH in Binding Caches. Since it is neither possible nor necessary to implement new Agent for every kind of node to handle both MIP and Binding Caches, I decide to modify the current implementation of MIPB-SAgent and use it as the Correspondent Host communicating with the MH.

   By adding the Binding Update message handler in its packet handle function, the modified MIPBSAgent is now able to extract the Care-Of Address from the Binding Update message and re-route the future packets to the COA directly by using the MIPEncapsulator. Now, the CH performs the similar function as the HA when tunneling the packets to the Care-Of Address of the MH.

   The Figure 6 could better illustrate the process logic as follows.

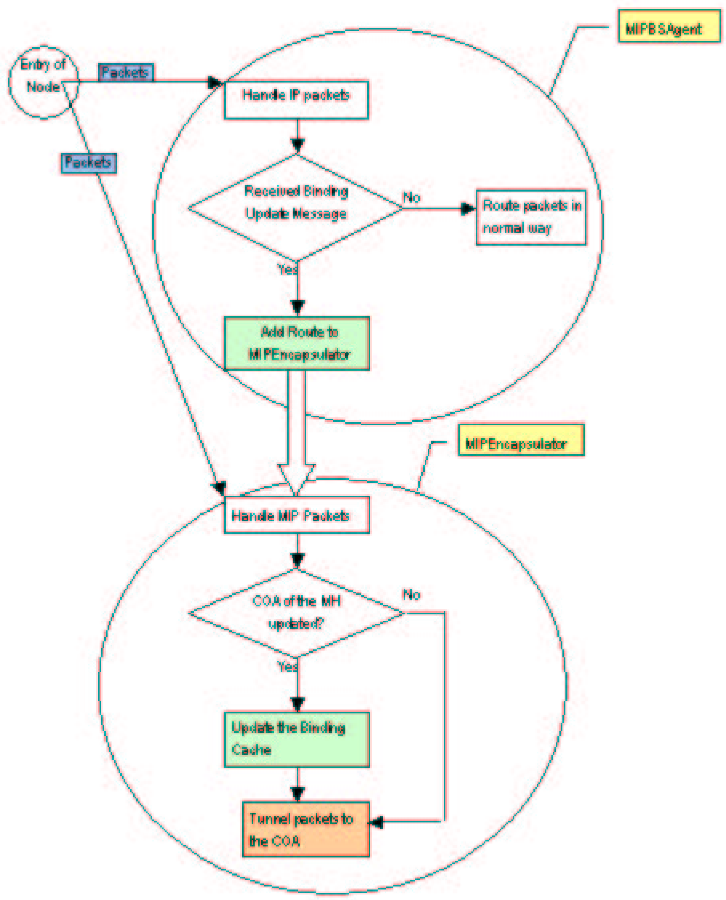


Figure 6: Flowchart of Receiving Binding Update Message

3.3 Binding Warning Message

For the **Binding Warning** message, it still consists of two parts:

1. The first part is the Mobile Node. It is to send out the Binding Warning message.

   When the mobile node moves from one foreign network to another foreign network, after it registers in the new network, it should notify the HA its new COA and send out the **Binding Warning** message requesting the HA to send **Binding Update** to the correspondent node(s).

   So, in the modification, whenever the mobile node receives the REG_REPLY message from the FA, which means it has already successfully registered in the foreign network, it determines whether a new Care-Of Address is obtained and send out the Binding Warning message if yes. To check whether a new Care-Of Address is obtained is to avoid repeated sending Binding Warning message, which is unexpected.

   The following Figure 7 could ease the understanding of the process flow in this part.

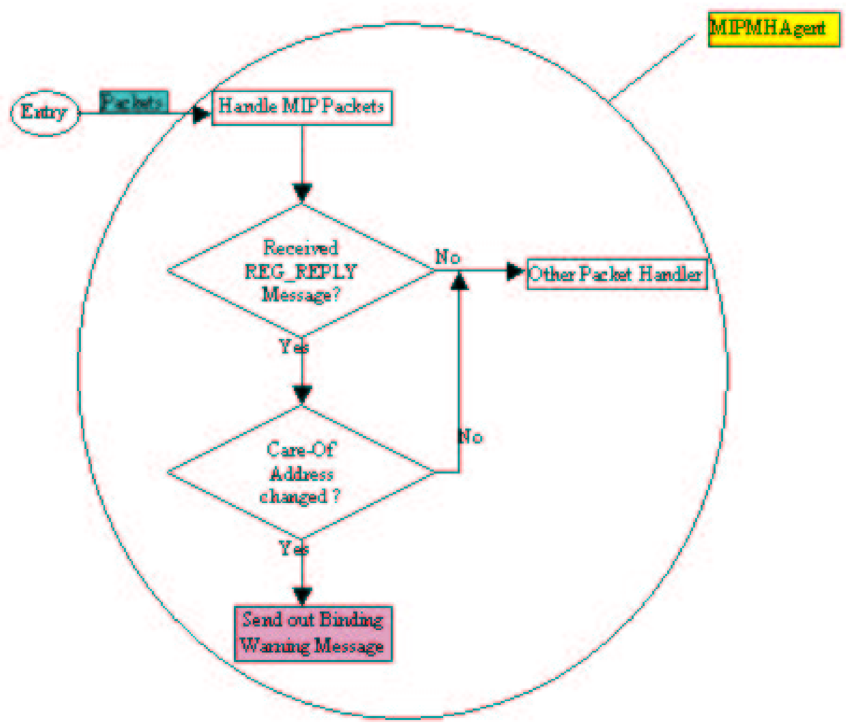


Figure 7: Flowchart of Sending Binding Warning Message

2. The second part is the HA. It is to handle the receiving of Binding Warning message.

   When the a MIP enabled router (HA/FA) receives the Binding Warning message sent by a mobile node, it first checks whether itself is the Home Agent of the mobile node.

   If yes, then, it retrieves the new COA address from the Binding Warning message and retrieves the address of the correspondent host from its registration table, and send out the Binding Update message to the correspondent host. How to send out the Binding Update message and what will happen after the delivery of Binding Update message can check the previous sections for details.

   If no, then, the router forwards the message through normal routes to the Home Agent of the mobile node.

   The following Figure 8 illustrates the process of receiving Binding Warning message.

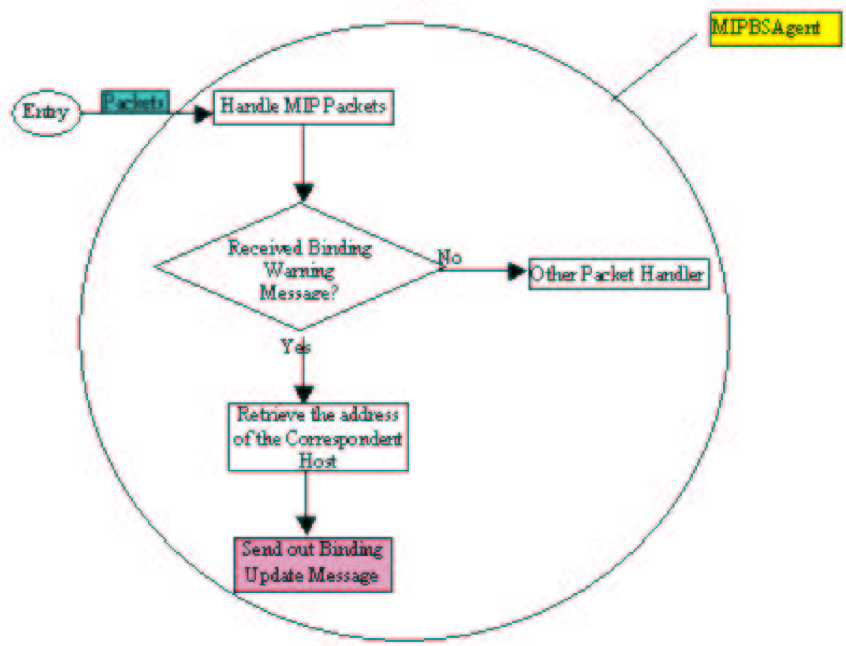


Figure 8: Flowchart of Receiving Binding Warning Message

3.4 Source Code Modification Review

After analyze the source code of the current Mobile IP implementation in *ns-2*, I modify the source codes of the Mobile IP for the Route Optimization extension. Following is a summary of the source code modification.

- *MIP.H*
  1. Add two type of MIP packets in the MIPRegType enumeration: MIPT_BU, MIPT_BW
     MIPT_BU is the type indicator of Binding Update message; MIPT_BW is the type indicator of Binding Warning message.
  2. Add two function headers in the header file
     - void MIPBSAgent::send_bu(int dest, int haddr, int ha, int coa);
       This function is used in MIPBSAgent to send out Binding Update message
     - void MIPMHAgent::send_bw(int dest, int haddr, int ha, int coa);
       This function is used in MIPMHAgent to send out Binding Warning message
- *MIP.CC*
  1. Modify the MIPEncapsulator::recv(Packet* p, Handler *h) function.
     - Enable the MIPEncapsulator to send out Binding Update message when the Home Agent receives packets destined to the mobile node away from home.
     - Save the address of the correspondent node and the current care-of address of the mobile node for later usage.
     - Send out the Binding Update message in MIPEncapsulator is to call a TCL function, which eventually invokes the send_bu method of MIPBSAgent.
- *MIP-REG.CC*
  1. Modify the MIPBSAgent::recv(Packet* p, Handler *) function.
     Modify this function, enable the MIPBSAgent to handle Binding Update message and Binding Warning message.
     - Handling Binding Update message:
       When the MIPBSAgent receives the Binding Update message, it stores the care-of address and then enables a MIPEncapsulator to tunnel the packets directly to the care-of address bypassing the home agent.
     - Handling Binding Warning message:
       When the MIPBSAgent receives the Binding Warning message, if it is the Home Agent of the Mobile node, then it retrieves the address of the correspondent node and sends a Binding Update message to it. If it is not the Home Agent, it just forwards the Binding Warning message to the Home Agent of the mobile node.
  2. Modify the MIPBSAgent::command(int argc, const char*const* argv) function.
     Provide the interface to OTcl modules, to send out the Binding Update message
  3. Add the MIPBSAgent::send_bu(int daddr, int haddr, int ha, int coa) function.
     Function to send the Binding Update message.

4. Modify the MIPMHAgent::recv(Packet* p, Handler *) function.
   Modify this function to send out the Binding Warning message when the Mobile node receives the registration reply message from FA/HA
5. Add the MIPMHAgent::send_bw(int daddr, int haddr, int coa) function.
   Function to send the Binding Warning message.

- *NS-MIP.TCL*

1. Add the MIPEncapsulator instproc setCH { mhaddr chaddr } function.
   This OTcl function is to store the address of the correspondent host in a hash table, indexed by the home address of the mobile node.
2. Add the MIPEncapsulator instproc setCOA { mhaddr coa } function.
   This OTcl function is to store the care-of address of the mobile node in a hash table, indexed by the home address of the mobile node.
3. Add the MIPEncapsulator instproc send-bu { daddr haddr coa } function.
   This OTcl function is to send out the Binding Update message by calling the MIPBSAgent::send_bu function.
   Before sending out the Binding Update message, it should check whether the same Binding Update message has already been sent out or not.
4. Add the MIPEncapsulator instproc nodeptr {} function.
   This OTcl function is to return the hierarchical address of the node where the MIPEncapsulator locates.
5. Add the Agent/MIPBS instproc getCOA { mhaddr } function.
   This OTcl function is to return the care-of address, indexed by the home address of the mobile node.
6. Add the Agent/MIPBS instproc getCH { mhaddr } function.
   This OTcl function is to return the address of the correspondent node, indexed by the home address of the mobile node.
7. Modify the Agent/MIPBS instproc encap-route { mhaddr coa lifetime } function.
   This is the main OTcl function to enable the MIPEncapsulator to encapsulate the packets.
   When adding the encapsulation route, it should first check whether the same route has been added or not,so to avoid redundant route.

4 Simulations

In order to verify the correctness the Route Optimization modification, simulations are mandatory for this purpose. The simulations should be done both with route optimization and without route optimization in mobile IP for comparison.

In addition, I set up two simulation scenarios: one is simply, another one is relatively complex.

4.1 Simulation Scenario

- Scenario One:

  This is a basic simulation scenario. It consists of only one mobile host, one home agent, one foreign agent, one correspondent host and one wired node, just refer to the following NAM screen shot, Figure 9.

  In the simulation, some important simulation parameters are listed as following:

  - Radio Coverage: 75m
  - Position of HA: (200,300), FA: (330, 300)
  - Movement of MH: (150, 275) $\rightarrow$ (410, 275)
  - Traffic Type: CBR
  - Link delay: CH $\rightarrow$ HA : 25ms, CH $\rightarrow$ FA : 10ms

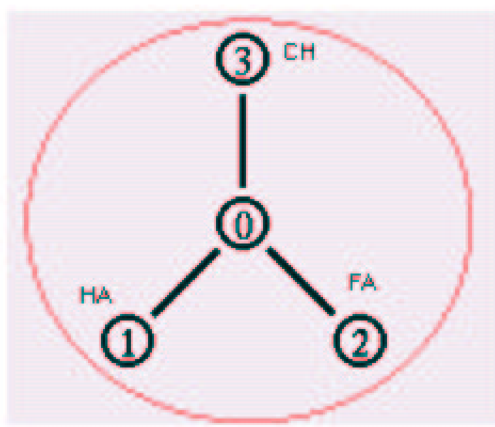


Figure 9: Simulation Scenario One

- Scenario Two:

  This scenario introduces another foreign agent. So, there are two foreign agents, instead of one in scenario one. The scenario is illustrated in the following Figure 10.

  Why the scenario two is necessary? It is because of the Binding Warning message.

  In this scenario, if there is no Binding Warning message enabled, since the home agent won't send out Binding Update message unless it receives packets destined to mobile host away from home, so, when the MH moves to another foreign network, the CH still sends packets to the old Care-Of Address of the MH and all packets will lost. The correspondent host won't receive the Binding Update message from the HA when the mobile host move to the second foreign agent's network.

  If Binding Warning message is enabled, MH will send the Binding Warning message to HA requesting HA to send out Binding Update message to the CH. Then, the CH can correctly communicate with the MH after receiving the Binding Update message.

  So, this scenario is used to justify the Binding Warning message.

  In the simulation, some important simulation parameters are listed as following:

  - Radio Coverage: 75m
  - Position of HA: (200,300), FA: (350, 300), FA2: (500, 300)
  - Movement of MH: (150, 275) $\rightarrow$ (560, 275)
  - Traffic Type: CBR
  - Link delay: CH $\rightarrow$ HA : 25ms, CH $\rightarrow$ FA : 17ms, CH $\rightarrow$ FA2 : 10ms

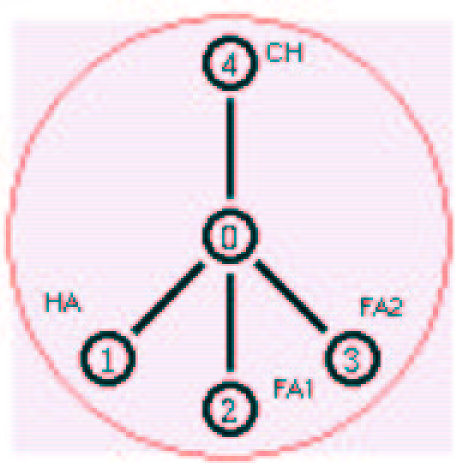


Figure 10: Simulation Scenario Two

4.2 Simulation Script

The simulation scripts for the two simulations are attached as appendix. Some key points should be explained here.

- set opt(threshold) 3.41828e-08
  Phy/WirelessPhy set RXThresh_ $opt(threshold)
  This is to set the Radio coverage, the number is calculated by an utility "threshold" included in *ns-2*

- set HAaddress [AddrParams addr2id [$HA node-addr]]
  [$MH set regagent_] set home_agent_ $HAaddress
  This is to set the home agent for the mobile host.

- $ns_ at 10.0 "$MH setdest 410.0 275.0 8.0"
  This is to set the track of the movement of the mobile node.

4.3 Post Process

- Script for end-to-end delay in XGraph

  The end-to-end packet delay is concerned in the project, because the packet delay is impacted by the "Triangle routing". So, in order to extract the end-to-end packet delay info from the ns trace file, I write a Perl script to extract the information.

  Another script to calculate the average end-to-end packet delay is also written in Perl for analysis usage.

- Script for NAM

  A script is used to trim out the redundant space at the end of each in the NAM file.

4.4 Result Analysis

- Scenario One

  The simulation result of the scenario one is as following:
  X axis is the time axis, Y axis is the end-to-end packet delay, unit of both X and Y axis is second.

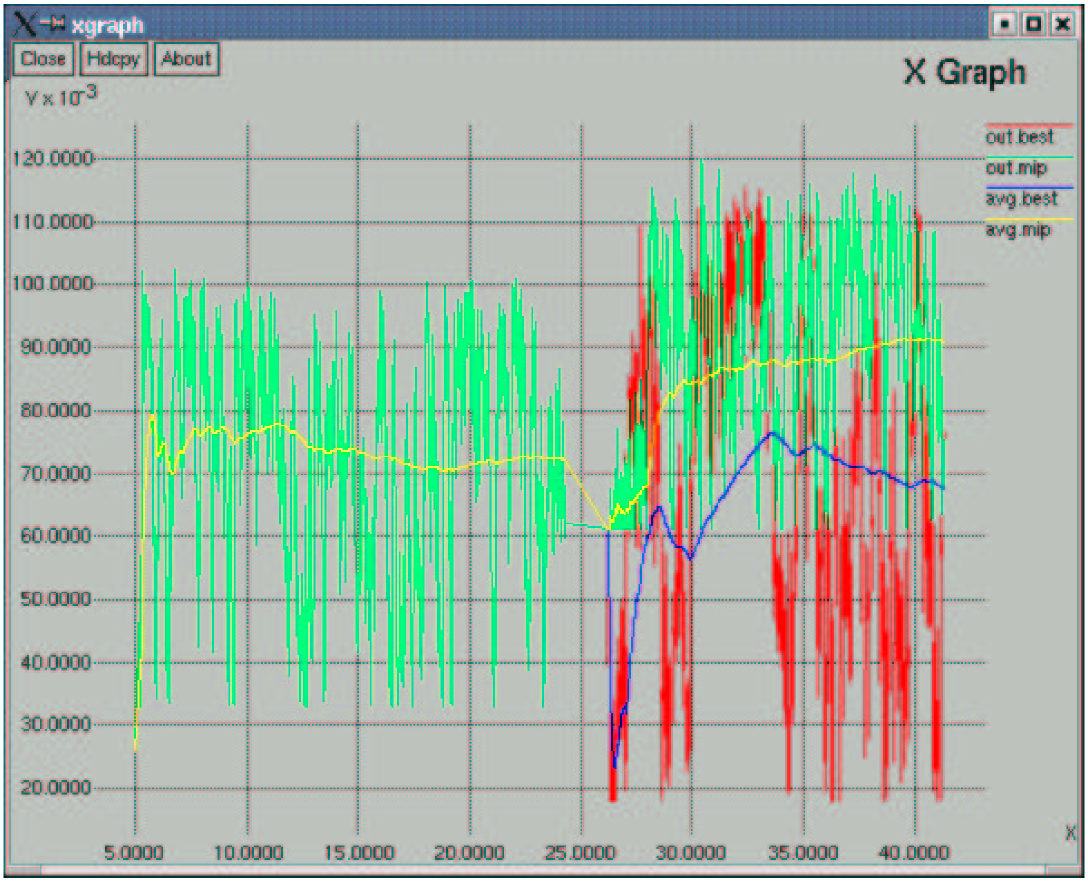


Figure 11: Simulation Result One

The green curve is the packet end-to-end delay of simulation without route optimization in mobile IP, while the red is the result of simulation with route optimization. Also, there are two curves illustrating average end-to-end packet delay: the yellow one is the average delay without route optimization, the blue one is that with route optimization.

From the above figure, it is easy to see that the minimum end-to-end delay of simulation with route optimization is quite smaller than that of the simulation without route optimization, when the mobile host moves to the foreign network. Compare the average delay curves, they justify our claim again that the end-to-end packet delay decreases drastically when MIP with Route Optimization enabled.

- Scenario Two

  The simulation result of the scenario two is as following:
  X axis is the time axis, Y axis is the end-to-end packet delay, unit of both X and Y axis is second.

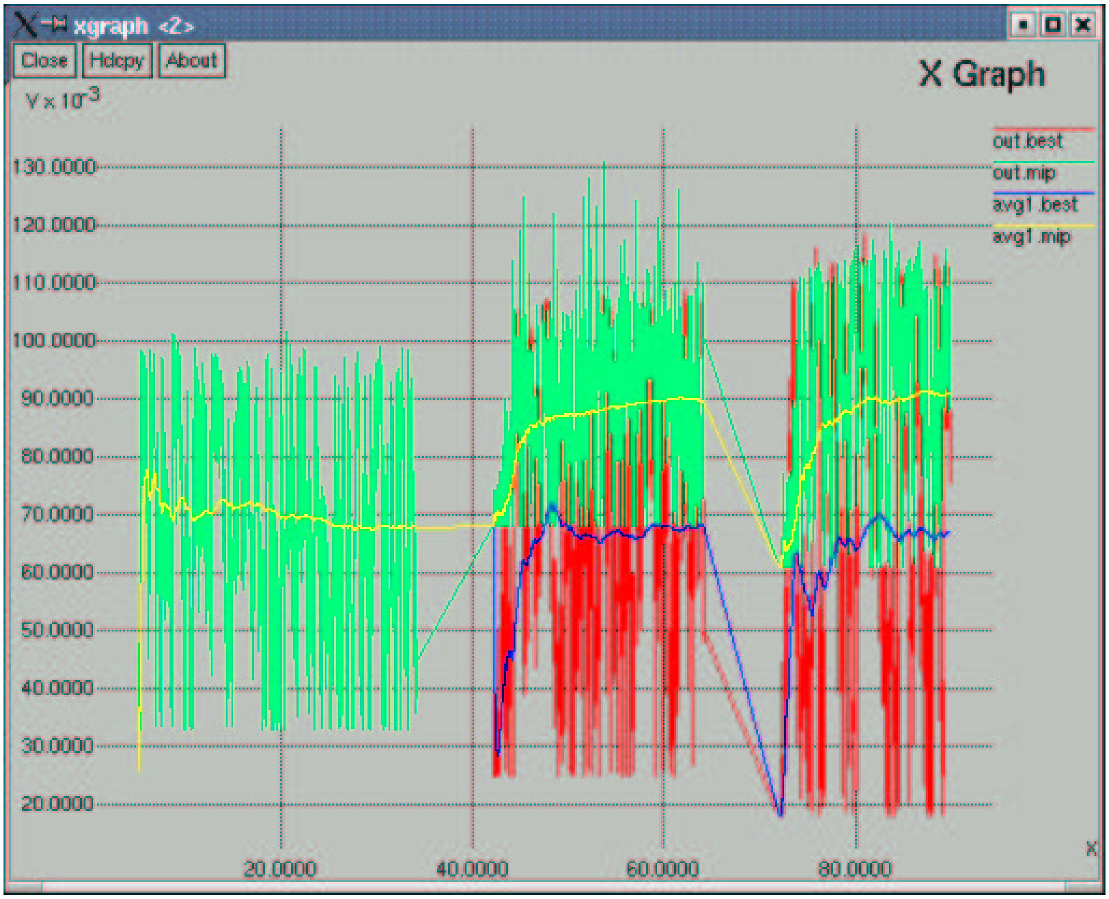


Figure 12: Simulation Result Two

The green curve is the packet end-to-end delay of simulation without route optimization in mobile IP, while the red curve is the result of simulation with route optimization. The blue curve is the average end-to-end packet delay with the route optimization, and the yellow one is the average delay without route optimization.

By comparing the average end-to-end delay curves and the minimum delay, we can say that the Route Optimization successfully eliminates the effect of "Triangle routing" and improves the network efficiency by lowering down the end-to-end packet delay.

5 Conclusion & Future Work

After studying the Mobile IP protocol and Route Optimization in Mobile IP, I modify and extend the mobile IP in *ns-2* to enable the Route Optimization. Simulations have been done and justified my extensioin. All my initial project goals have been fulfilled. Although my implementation is only part of the whole Route Optimization scheme, it is effective and sufficient to demonstrate the significance of Route Optimization in mobile IP. Through the simulations, the results are already self-explained.

The future work could be done to implement all the 4 Route Optimization messages in *ns-2* and compare them with other Route Optimization proposals, such as [ZY99][JR99].

References

[RFC3220] "IP Mobility Support for IPv4", C. Perkins, January 2002.
http://www.ietf.cnri.reston.va.us/rfc/rfc3220.txt?number=3220

[ROMIP] Internet Draft: "Route Optimization in Mobile IP", C. Perkins, D. Johnson, 09/06/2001. (66597 bytes)
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-optim-11.txt (work in progress)

[MIPv6] Internet Draft: "Mobility Support in IPv6", C. Perkins, D. Johnson, 11/21/2001. (310561 bytes)
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-15.txt (work in progress)

[NSDoc] The ns Manual, Edited by Kevin Fall & Kannan Varadhan.
http://www.isi.edu/nsnam/ns/doc/index.html

[CB96] S. Cheshire and M. Baker, "Internet Mobility 4x4",
ACM SIGCOMM Computer Communication Review, Conference proceedings on Applications, technologies, architectures, and protocols for computer communications. Volume 26 Issue 4, August 1996, pp. 318 - 329.

[ZY99] P. Zhou and O. Yang, "Reverse Routing: An Alternative to MIP and ROMIP Protocols",
Proceedings of 1999 IEEE Canadian Conference on Electrical and Computer Engineering, Volume 1, pp. 150 - 155.

[JR99] R. Jain, T. Raleigh, et al. "Enhancing Survivability of Mobile Internet Access Using Mobile IP with Location Registers",
INFOCOM '99. Proceedings of Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Volume: 1 pp. 3 - 11.