Transparent user operation in Mobile IP environment

Davor Janković Krešimir Šikić
Faculty of Electrical Engineering and Computing
University of Zagreb
Unska 3, HR – 10000 Zagreb, Croatia
davor.jankovic@zg.t-com.hr

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.

This research covered the establishing of testing and developing environment which was used to simulate Mobile IP protocol. Mobile IP protocol was simulated on the base of existing Mobile IP distribution. Also, established network environment was used to develop distribution of Mobile IPv4 protocol, which was then tested in combination with existing distributions.

VMWare program was used as a virtual machine simulator, and Linux operating system was used as a platform for developing and testing procedures.

I. INTRODUCTION

Internet, apropos TCP/IP protocol as a communication standard, was not designed to enable user's mobility. Mobile IP protocol, designed and described by Charles E. Perkins, is one of possible answers to question how to make Internet accessible to mobile devices. The official document by which Mobile IP was introduces is Request for comment 2002. Mobile IP is situated on network layer according to OSI model, and is designed as an upgrade to existing IP communication protocol. Mobile IP is also transparent to protocols of higher layers according to OSI model, so there is no need for their modification in order to implement Mobile IP.

There are two basic parts in this Mobile IP protocol research. The first part is about making network infrastructure and implementing a RFC compatible distribution of Mobile IP in it. Network infrastructure needed to be optimal regarding the needed resources. Also it must enable full inquiry into protocol's work. One of available Mobile IP distributions must be implemented and its work must be explained and demonstrated.

The second part is about developing Mobile IP software. Software should be implemented using the infrastructure from the first part. Software must be fully compliant with RFC 2002 specification, and its operation must be presented in the proper way.

II. MOBILE IP OPERATION

Internet Protocol version 4 (IPv4) assumes that IP address uniquely defines the point of connection to the Internet. That is why, the device that connects to Internet must be located in network that has same prefix as its IP address. If not, packets designated for it would newer reach its destination.

Mobile IP is protocol that enables moving between subnets without changing IP address of device. It is implemented at network layer according to OSI model, and it is independent of other layers. It is independent of physical medium that transmits network data, and it does not affect higher layers protocols. There are three entities in Mobile IP terminology. Mobile node – device or router that has the ability to change it's 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.

Mobile node receives his IP address in his home network. This address is called home address. It is permanent and identifies mobile node as device attached to IP network. When mobile node is in foreign network, it also has temporary address, a care-of address. Network that has the same prefix as mobile node's home address is called home network. Network in which foreign agent is located and which is served by that foreign agent is called foreign network.

Device that communicates with mobile node while he's located in some foreign network uses mobile node's home address as destination address. Home agent then receives packets designated to mobile node, and tunnels them to the present location of mobile node, the foreign network. Foreign agent that serves that foreign network receives encapsulated packets from tunnel, decapsulates them and sends them to mobile node. Mobile node also responses through foreign agent. But packets send from mobile node, after passing through foreign agent, don't use tunnel to home agent but standard IP routing mechanism. That way of communication is under Mobile IP terminology known as triangular routing mechanism and is illustrated on the picture below.

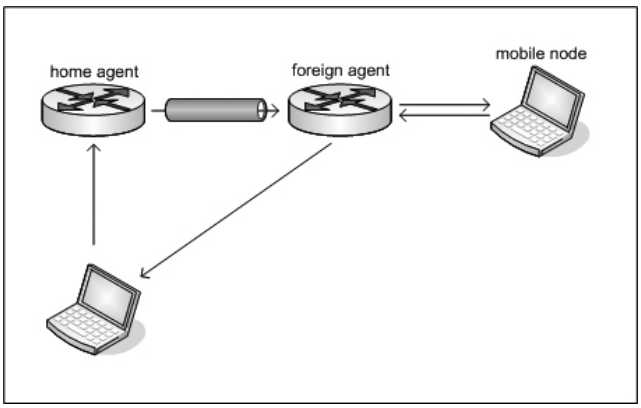

Figure 1 - Paths of data flow in Mobile IP

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.

A. 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. Agents periodically send agent advertisements to the network which they serve. Broadcast of multicast is used as destination address.

Receiving agent advertisement from a new foreign agent is a signal that mobile node has changed his location and has to act according to it. Mobile node can send message by which he requests for potential foreign agent in new network. This message is called agent solicitation and is identical to router solicitation message which is part of router discovery protocol. Every Mobile IP agent that receives agent solicitation must respond to it with proper agent advertisement.

B. 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 canceled. Registration with care-of address lasts for a certain time period, so when it is close to termination, it must be refreshed. Also, when mobile node returns home from some foreign network, registration with past foreign agent must be canceled. Registration process is consisted from registration request packet and registration response packet which is sent as answer to request. Registration request and response are sent via foreign agent so that he could have insight into new registrations and could adapt to them. Sequence by which registration packets are sent is illustrated on the image below.

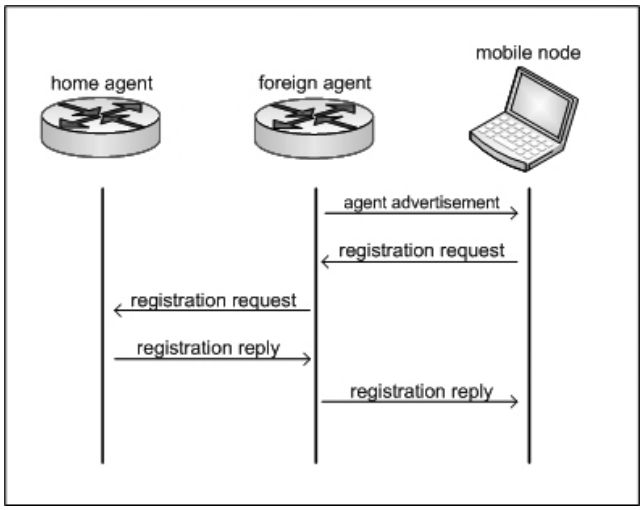

Figure 2 - Packets in Mobile IP registration process

Foreign agent, same as home agent, checks values inside of registration request and can deny registration in some cases. These cases are mostly about bad authentication parameters or poorly formed registration request.

Registration packets can contain various extensions. Most important extensions are linked to authentication process in Mobile IP. Each Mobile IP entity has its own list of other Mobile IP devices to which he shares security association. If there is a security association with another Mobile IP device, every registration packet designated do this device must contain authentication extension. Each mobile node must have security association with his home agent, and home agent must have security association with all mobile nodes he serves as home agent. Optionally, there can be security association between home and foreign agents, and foreign agents and mobile nodes. Two Mobile IP devices tar share security association must share 128 bit key that is used in digital signing of registration packets. RFC 2002 specification defines Message Digest 5 (MD5) algorithm as authentication algorithm. On the basis of registration packet and shared key, unique signature is calculated and it's carried with packet as a part of authentication extension. Mobile IP has defined protection against reply attacks, and has recommended two independent methods. First method is based on time frames in which other device must respond to registration packed, and second method is based on pseudorandom numbers. Method based on using time frames requires use of Network Time Protocol (NTP protocol) which himself can potentially be subject to attacks.

C. 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. BUILDING SIMULATION ENVIROMENT

Because of the large hardware requirements for making test network for implementation of Mobile IP, testing network was built using a virtual machine simulator. There are two basic demands that the used simulator must fulfill. The first is related to a level of simulation of entities in the network. Simulator must enable installation of independent operating system into virtual machine, and has to work on this operating system as on any other real computer. Simulator must be able to create virtual hardware that virtual machines use. This demand is particularly related to ability to use few network interfaces as Mobile IP agents will also be routers on the network. Simulator must enable creating virtual network interfaces that can be configurable directly from operating system. The other demand concerns connecting independent virtual machines. There is a need of connecting virtual machines into one network. Simulator must enable connecting virtual machines to network, and create different IP networks so that the virtual machines that work as routers could connect those networks.

A. Simulator

VMWare Workstation version 4.5 was chosen as a simulation system between few technologies and program packages. VMWare is a simulation program that enables physical hardware of one personal computer to be used between few virtual machines that are completely independent. Each virtual machine is separate unit and is almost completely independent of physical computer and can be used to install any operating system desired. Computers that VMWare simulates are called virtual machines, and operating system they run is called guest operating system. VMWare also gives excellent possibilities of connecting virtual machines to network via nine offered virtual switches. VMWare also enables connecting physical interface of host computer with virtual network and some additional services like NAT and DHCP.

As a platform that was used for testing and developing Mobile IP software Linux operating system was choused. Reasons are few. The first reason is fact that Linux operating system provides greater flexibility in configuring settings of network interfaces, ARP and routing table. The second reason is authors experience in developing network oriented software for Linux platform. Third reason is number of free or open source distributions of Mobile IP that could help in testing its own software. Finally, the last reason is related to resources needed for running simulation. Linux operating system can run without graphical interface where virtual machine uses much more of RAM memory, which is bottleneck of the whole system. Red Hat Linux version 9 was picked as a Linux distribution.

B. Testing network

Testing network was designed so that it can fully simulate operation of Mobile IP protocol. Also, network is scalable and can be extended according to demands and hardware limitations. Within the testing network there is sub network which simulates home network. Router that connects home network with rest of system is also home agent. There are also several foreign networks connected to system by foreign agents. Agents are all connected to central router that interconnects the whole network. Figure 3 shows a scheme of testing network.

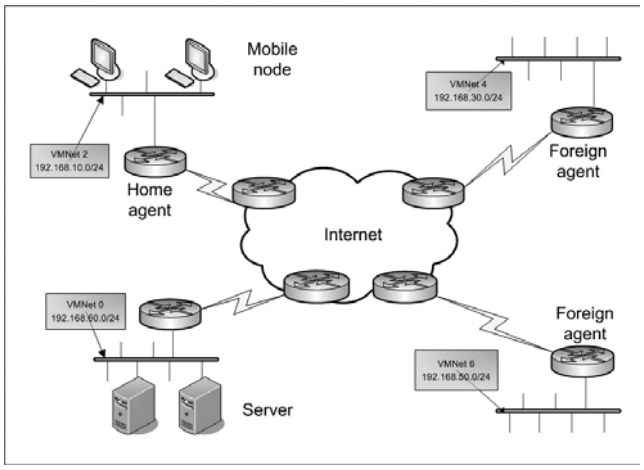

Figure 3 - Model of testing network

IV. DEVELOPED MOBILE IP DISTRIBUCION

As a part of the research, on the basis of built testing network, own software version of Mobile IP protocol was developed. Programs were designed according to RFC 2002 specification in program language C. Program language C was selected because of its portability and fact that most of API's used in development were also written in C language. Mobile IP distribution consists of three independent programs: home agent, foreign agent and mobile node. Programs are installed and run on user space, so there is no need for any kernel modifications in order to run the software. Each program is split into five parts. Main part of the program implements all necessary operations assigned to Mobile IP operations. There are also four sets of functions for handling network connections, timers, security and system configuration. Program diagram is illustrated on the image below.

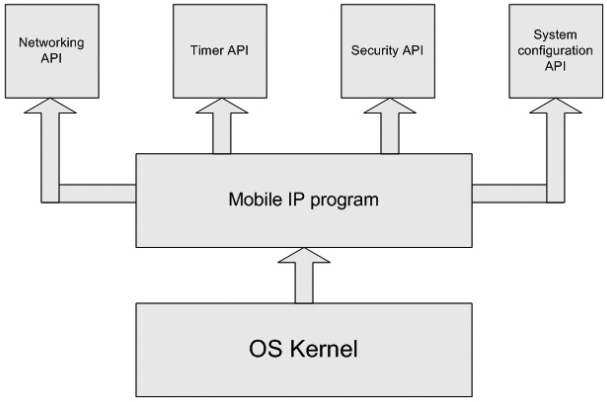

Figure 4 - Diagram of Mobile IP program

Mobile IP agents are implemented in routers that connect home and foreign networks with public network. Foreign agents as care-of address advertise IP address of their private interface. In order to realize influence of Mobile IP protocol to data paths on the network, traceroute program was used. Program was started on independent node on network, and destination address was home address of mobile node. Result is shown below for two separate cases: when the mobile node is situated in home network, and when it is on one of foreign networks.

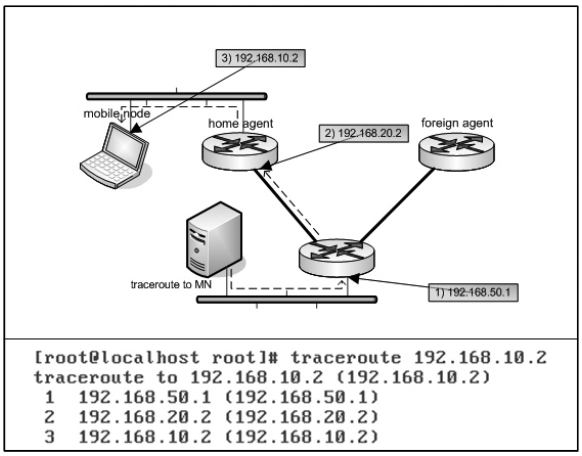

Figure 5 - traceroute to mobile node in home network

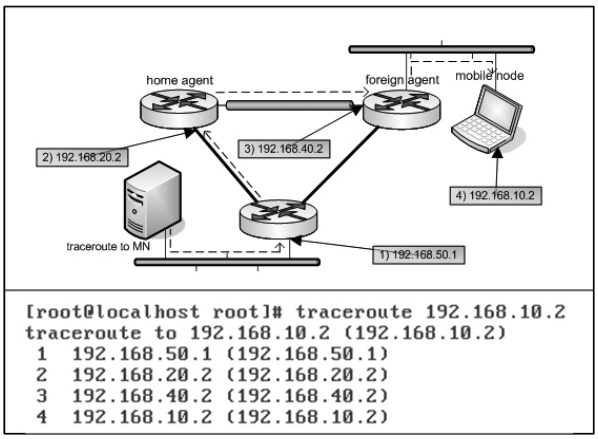

Figure 6 - Traceroute to mobile node in foreign network

According to demands in RFC 2002 specification MD5 was implemented as authentication algorithm. There is also algorithm based on pseudorandom numbers as reply attack protection.

A. Compatibility with RFC 2002

Software was tested within the simulated network environment in pair with other independent Mobile IP distribution. In our case, it was Dynamics Mobile IP distribution. In order to show compatibility with RFC 2002 specification, scenarios were designed by which all features of software were investigated. All tests were made with various combinations of own distribution and Dynamics distribution. All test showed full compatibility and interoperability in all segments of Mobile IP operation. Following tests were preformed:

- Agent advertisements processing
- Processing of agent solicitations and responding according to them
- Mobile node in home network registration
- Mobile node in foreign network registration
- Discovering of new network based on agent advertisements
- Granting registration from home agent
- Denying registration from home agent
- Denying registration from foreign agent
- Insensitivity for higher layer protocols

B. Insensitivity for higher layer protocols

Additional tests were done to demonstrate insensitivity of Mobile IP operation to work under higher layer protocols. The test was designed according to following scenario: a higher layer protocol File Transfer Protocol (FTP) was used. FTP protocol is based on connection oriented TCP protocol. Mobile IP software operation must not have any influence on FTP protocol operation. FTP client software was implemented on mobile node and FTP server was implemented on some independent node on network. FTP client requested file download. During file transmission, mobile node changed his point of connection several times. Timeline with bandwidth usage during transfer is shown on the image below. Three brakes in transmission that lasted about one second can be seen. At that moment mobile node changed its point of connection, discovered another agent and registered new location with its home agent. Communication then continued with ease.

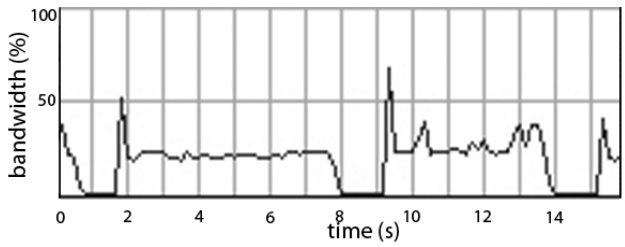

Figure 7 - Communication breakdowns caused by changing of mobile node's location

C. Convergence and overhead issues in Mobile IP protocol

When implementing Mobile IP protocol, time of convergence is great factor whenever mobile node changes its point of attachment. Mobile node cannot communicate from the moment he disconnects from one network until the moment he receives registration reply from his home agent. The effort is to keep this time window as small as possible.

The main factor that determinates time of convergence is duration between two agent advertisements. As the rate of sending agent advertisements increases, time of convergence gets smaller. But agent advertisements are broadcast packets so they increase bandwidth usage. That's why it is very important to find good relation between time of convergence and increased bandwidth usage by Mobile IP.

In own software version of Mobile IP protocol, time between two agent advertisements was set to 1 second, keeping time of convergence always smaller than 1,5 second and mostly around 0,8 second.

D. Real-time operation of Mobile IP protocol

Final tests were made to show real-time operation of Mobile IP protocol. The test was made with live video streaming and Voice over IP software. Tests were designed to show influence of network change to brake of communication using mentioned software. Transmission brake lasts from the moment mobile node changes location until the moment all devices became aware of change and do necessary action so that communication could continue. Tests have shown that the time needed for convergence of the whole system was about one second. In streaming application, with buffer set for time of little over one second, changing the network could not be noticed. In VoIP application changing of network was notable, although not to long for god communication. It can be concluded that Mobile IP developed Mobile IP software can be also used with real-time applications such as live streaming or Voice over IP.

E. Mobility support for IP version 6 protocol

Logical continuation in the evolution of Mobile IP protocol relates to adjustment of Mobile IP to IPv6 protocol which was described in RFC 3775 document.

Like in IPv4 protocol, the idea by which mobile node is accessible through it's home address is also present in Mobile IPv6. Also, there is still need for encapsulation of packets when they travel from home agent to care-of address.

In IPv6 protocol, mobile node has the ability of retaining care-of address by the aid of Neighbor Discovery and Stateless Address Autoconfiguration protocol. These two protocols form good protocol basis for Mobile IP operation. With help of two above mentioned procolos, there is no more need for foreign agents, so they have been eliminated form Mobile IP operation in IPv6 protocol.

CONCLUSION AND FURTHER WORK

The testing of developed Mobile IP software gave further insight into the protocol operation. With wired medium like Ethernet, for witch software was designed, the most important working parameter came out to be time between two agent advertisements. Two important factors depend on that parameter: network overhead caused by Mobile IP administrative packets and convergence speed of Mobile IP protocol on the other side. This work completed one chapter in researching and developing program support for mobility on Internet. Next steps are related to optimization of current software for wireless network environments. Special focus will be on process of agent selection by mobile node. Working on Mobile IP for IPv6 protocol is also another guideline in researching Internet mobility.

LITERATURE

[1.] Perkins C.: *Request for Comments: 3344, IP Mobility Support*, August 2002

[2.] Norris M.: *mobile IP Technology for M-Business*, October 2001

[3.] Johnson D., Perkins C., Arkko J.: *Request for Comments: 3775, Mobility support in Ipv6*, June 2004

[4.] Solomon J.: *Mobile IP the Internet Unplugged*, 1998

[5.] Perkins C.: *Mobile networking through Mobile IP, Tutorial*, February 1998

[6.] Perkins C.: *Mobile IP Design Principles and Practices*, 1997