Introspection in Mobile IP

Mihai-Marius Criste, Vasile Dadarlat

***Abstract*— Mobility is important and undeniable currently having view new portable devices that have captured the market and the need connectivity further to the Internet.**
Mobility support in IP networks is a topic that has received considerable attention. Mobil IP is one of the dominating protocols which provides the support of mobility in the internet.
In this paper, we go will through the characteristics of Mobile IP, the protocol overview, then proceed to brief current developments namely (Mobile IPv4 and Mobile IPv6), the issues, and advantages with Mobile IP.
Discussed few of the challenges that are faced by the Mobile IP and solutions have been proposed for a successful deployment of Mobile IP in the future.

***Index Terms*— MIP, MIPv4, MIPv6**

I. INTRODUCTION

Today organizations are more dependent on the information, so you need employees to be connected not just to local organizations, but also from other locations as well as must work remotely and access to information own businesses by using these mobile devices with services adequate security.Mobile IP has been designed with the Internet Engineering Task Force(IETF) to serve the needs of growing population of mobile computer users who wish to connect to the internet and maintain communication as they move from place to place. Mobile IP enables a wireless network node to move freely from one point of connection to the Internet to another, without disrupting the end-to-end connectivity.The idea of Mobile IP is similar to postal service delivery: once you move to a new location, you ask your home post office to send your mail to your new location‟s address by the local post office there . Thus, a mobile device first leaves its home network and connects to a foreign network. The agent then sends packets locally to the mobile device visiting that network.[3]
Mobile IP are:

- Mobility Support, increased number of mobile
- users
- Standardization, uses the current IP Protocol
- Inter-Operability, can be used across different
- service providers
- Alternative Technologies, lack of proper alterna-
- tives other than Mobile IP

Manuscript received Nov 23, 2016
Mihai-Marius Criste, Ph.D. and Network Server Administrator
Vasile Dadarlat, professor of computer sciences within the Computer Science Department of the Automation and Computers Faculty,Technical University of Cluj-Napoca

- IPv4 Availability, limited availability of IPv4 ad-dress necessitates the need for Mobile IP
- Improved Security, while registering with the
- home agent

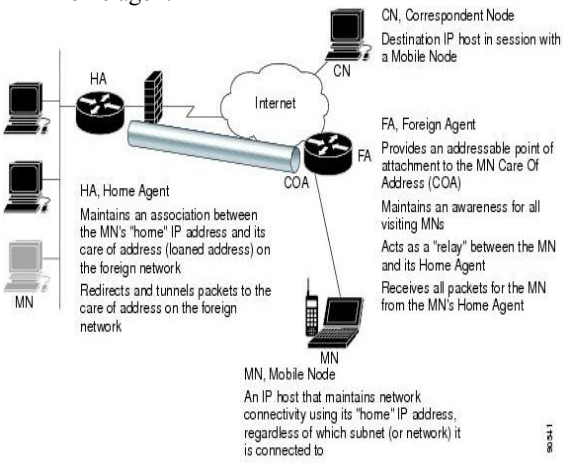

Fig 1- Mobile IP topology (Cisco)[14]

II. MOBILE IPV4(MIPV4)

A.Mobile IPV4 elements

MOBILE NODE (MN): is a moving internet connected device on which the location and point of attachment to the internet can be changed while keeping ongoing communication without interruption using its home fixed address. This kind of device is usually IP phone, laptop computer or router.
HOME ADDRESS: An IP address assigned to Mobile device within the network for extended period of time. It remains the same regardless of where the device is attached to the internet.
HOME AGENT (HA): is a router on the mobile devices home network. It tracks the mobile device location (care of address), intercept and tunnels packets to the mobile device when it is away from home, and maintains current location information for the mobile device.
HOME NETWORK: is the network within which a device identifies as its home IP address. The IP routing mechanism will deliver packets destined to mobile device's home address to the mobile device's Home Network.
FOREIGN AGENT (FA): is a router on the mobile device's visited network. It provides the care-of-address to the mobile device and routing service to the mobile device whilst registered and acts as a default router for datagram generated by the mobile device. The foreign agent de-capsulates and delivers datagram to the mobile device that are encapsulated by the mobile device's home agent
FOREIGN NETWORK: Any network other than the mobile device's home network, on which the mobile device can

operate successfully when away from its home network.
CARE-OF-ADDRESS: is a temporary IP address assigned to a mobile device while it is away from home network.
CORRESPONDENT NODE (CN): A device that sends or receives packets to or from the mobile device; the correspondent device may be another mobile device or a non mobile internet device[1].

B.The Mobile IPv4 process:

has three main phases:

1) Agent Discovery

A mobile node discovers its foreign agents and home agents during agent discovery.Agent Discovery is the method by which a mobile node determines whether it is currently connected to its home network or to a foreign network, and by which a mobile node can detect when it has moved from one network to another.When connected to a foreign network, the methods also allow the mobile node to determine the foreign agent care-of address being offered by each foreign agent on that network. Mobile IP extends ICMP Router Discovery as its primary mechanism for Agent Discovery.An Agent Advertisement is formed by including a Mobility Agent Advertisement Extension in an ICMP Router advertisement message

2) Registration Procedures

The mobile node registers its current location with the foreign agent and home agent during registration.There are two different procedures defined for registration, depending on the type of care-of address used by the mobile node and other specifics we will get into shortly. The first is the direct registration method, which has just two steps:

- Mobile node sends *Registration Request* to home agent.
- Home agent sends *Registration Reply* back to mobile node.

In some cases, however, a slightly more complex process is required, where the foreign agent conveys messages between the home agent and the mobile node. In this situation, the process has four steps:

- Mobile node sends *Registration Request* to foreign agent.
- Foreign agent processes *Registration Request* and forwards to home agent.
- Home agent sends *Registration Reply* to foreign agent.
- Foreign agent processes *Registration Reply* and sends back to mobile node.

The first, simpler method is normally used when a mobile node is using a co-located care-of address. In that situation, the node can easily communicate directly with the home agent, and the mobile node is also set up to directly receive information and datagrams from the home agent. When there is no foreign agent, this is obviously the method that *must* be used. It is also obviously the method used when a mobile node is de-registering with its home agent after it arrives back on the home network.

The second method is required when a mobile node is using a foreign care-of address. Recall that in this situation, the mobile node doesn't have its own unique IP address at all; it is using a shared address given it by the foreign agent, which precludes direct communication between the node and the home agent. Also, if a mobile node receives an *Agent Advertisement* with the "*R"* flag set, it also should go through the foreign agent, even if it has a co-located care-of address.

3) Tunneling:

A reciprocal tunnel is set up by the home agent to the care-of address (current location of the mobile node on the foreign network) to route packets to the mobile node as it roams.The process of encapsulating an IP packet within another IP packet in order to forward the packets to some other place other than the address that is specified in the original destination field [4].When a mobile node is away from its home network, the packets that are sent to the home agent have to be directed to the mobile node care of address, for this purpose it is necessary to encapsulate the IP packet with new source and the destination IP address. The path that is followed by this encapsulated IP packet is called tunnel.

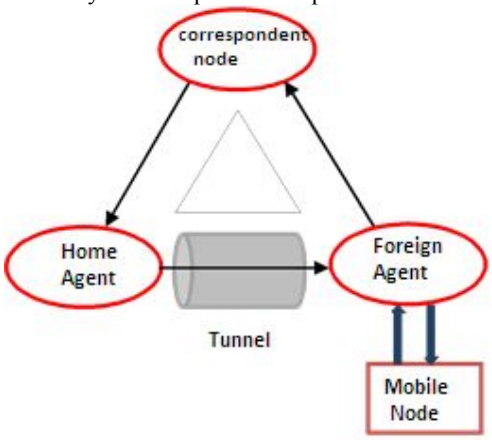

Fig.2 Tunneling and encapsulation

III. MOBILE IPV6 (RFC 6275)

Mobile IP was developed for IPv4, but IPv6 simplifies the protocols[2].

- security is integrated and not an add-on, authentication of registration is included
- COA can be assigned via auto-configuration (DHCPv6 is one candidate), every node has address autoconfiguration
- no need for a separate FA,all routers perform router advertisement which can be used instead of the special agent advertisement; addresses are always co-located
- MN can signal a sender directly the COA, sending via HA not needed in this case (automatic route optimization)
- „soft" hand-over, i.e. without packet loss, between two subnets is supported MN sends the new COA to its old router
- the old router encapsulates all incoming packets for

the MN and forwards them to the new COA authentication is always granted

Mobile IPv6 extensions :

- Hierarchical Mobile IPv6
- Fast Handover for Mobile IPv6
- Proxy Mobile IPv6

There are two versions of Mobile IP: Mobile IP for IPv4 and IPv6. The major differences are summarised as follows[7][8]:

Key Features	Mobile Ipv4	Mobile IPv6
Special router as foreing agent	Yes	No
Support for route optimization	Part of the protocol	In Extensions
Ensure symmetric reachability between mobile nodes and its router at current location	No	Yes
Routing bandwidth overhead	More	Less
Decouple from Link Layer	No	Yes
Need to manage Tunnel soft state	Yes	No
Dynamic home agent address discovery	No	Yes

TABLE 1.Comparison between Mobile Ipv6 and Mobile Ipv4

IV. THE ISSUES WITH MOBILE IP

A.Security:

Security is the most outstanding problem with Mobile IP. A great de al of attention is being focused on making Mobile IPv4 coexist with the security features coming into use within the internet.

Firewalls, especially cause problem for Mobile IPv4 because they prevent all types of incoming packets that do not meet identified criteria. Enterprise firewalls are specifically configured to prevent packets from entering through the Internet that seem to come out from internal computers. Although this allows management of internal Internet nodes without great attention to security, it causes problems for mobile nodes within their home enterprise networks. Such communications carry the mobile node's home address and would therefore be prevented by firewall

B. Triangle routing" Problem"

The Communication Host (CH) has to forward packets to themobile host (MH) through the home agent (HA) while the MH sends packets straight to the CH. As communication in each direction is different ways, the problem of "triangle routing" emerges , which leads to low efficiency of MH, especially when you are away from the HA and the CH is near the MH.

Solution:

Mobile IP, routing optimization is required because all packets sent to the MH must pass through HA but the route might not be the best. After having received the packets sent by the CH to the MH, the HA notifies the CH information for linking the MH, i.e., the address of the relay agent MH current (FA) of , and CH wraps the packet and establishes the tunnel to the FA transparent transmission.The link information is transferred through via a certain port number. Whether the MH still moves, the new FA will be transferring the link information maintained to the old FA to secure that packets are transferred to the new FA. In addition, during this time the HA receives the link information updated so that the following stable packages will be transferred straight from the CH with the new FA. The mobile IP with route optimization sets high requirements on the CH. The CH must have the ability to obtain the link information, encapsulate the packets and establishing the tunnel. Consequently, the protocol stack CH needs many modifications

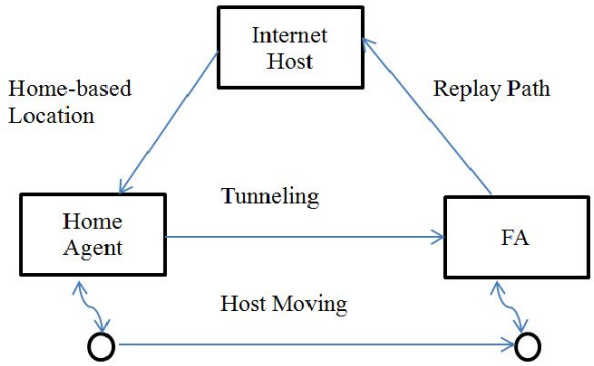

Figure. 3 Triungle routing

C. Handoff Problem

Handover issue means that the HA sends IP packets to the network MS original foreign across the tunnel, and you do notknow the final Care of Address (CoA) of the MH during the period that begins when the MH leaving the network original exterior and ends when the HA receives the new direction of the MH registration. As a result, these IP packets are dropp ed have an influence on the communication between the MS and the CH especially when transfer frequently occurs or the MSis away from the HA.

Solution:

The transfer process divides into two stages:

- Mobile testing Phase:

In this stage a test mobile is performed to determining whether the MH has been changed to the sub-network access.

- Re-registration stage:

The re-registration phase refers to the period that begins when the MH sends a request for registration to the HA and terminating when the HA receives therequest, after the MH confirms movement. The duration depends upon the distance from the MH to the HA.After the above two steps are completed, the MH continues to communicate with the CH. But any lost packets caused in this period may interact with higher layer protocols, and hence degrade performance of communication. The interaction with the TCP is a typical example. In the Mobile IP environment, the packet loss caused by the transfer will cause the interruption time for the TCP connection longer, and therefore degrade the performance of TCP. More severe disruption of approximately up to 12 s, and meanwhile there are several exceptional broadcasting. In short, the performance of communication during handover MH depends on three factors: the test mobile, the new record and the interaction

with the high layer protocol

D. Intra-Domain Movement Problem:

If the MN frequently moves whthin the intra-domain,large number of handoffs occurs.This leads to the accumulation of the large amount of registration messages and the performance of the system is reduced.

E. Quality of Service Problem:

In the mobile environment, it is hard to provide QoS over Mobile IP due to dynamically varying wireless network topologies, limited network resources, unpredictable effective bandwidth and high error rate.

Solution:

The Resource Reservation Protocol (RSVP) and the Service

Differentiation (DiffServ) have their respective strengths and weaknesses in the provision of IP QoS via mobile but may be combined to solve the end-to-end quality of service problem. The Diffserv router used in the spine, and RSVP in the access part, When the host requests RSVP originates in the border router backbone access point, the border router will be divided

in certain applications and assign QoS levels in the DS field based on the contents, such as bandwidth and delay time taken by the RSVP requests for and preliminary definition of. In the backbone DiffServ domain, the DS field quality can be guaranteed of service transmission, and like border router, output spine restores original RSVP requests and sends them to the destination .

V. ADVANTAGES OF MOBILE IP

Some important advantages of Mobile IP have been discussed below:

A. Any device for user Convience

The Mobile IP Call Module can be deployed on any suitable device – smartphone, tablet, PC or Mac, providing flexibility of choice for the user and recreating their office experience. They can handover calls from one device to another and access the same functionality that they enjoy in their home country, irrespective of location.

B. Scalability

Mobile IP allos a device to change from any network to any other ,and support this for an arbitrary number of devices.The scope of the connection change can be global;You could detach a notebook from an office in Cluj and move it to London, for exemple ,and it will work the same as if you took it to the office next door.

C. Standardized

Since Mobile IP's inception, it has been adopted as a standard and is included with many advanced networking tools. Companies, such as Cisco, provide Mobile IP solutions with a number of their products, making the setup and expansion of a network using Mobile IP even easier.

D. Uniqueness

A Mobile IP address allows users to connect to the Internet Without a normal static or dynamic IP address lets the use of a unique mobil IP address.This unique address lets the computer connect through a network to a home IP address but still utilize and communicate with the network's protocol.

Having a unique IP is important for routing information to the correct computer.In short, if it were not for Mobile IPs,information would continue to be routed to the last known IP address at which that computer was located, and a seamless connection wold be impossible.

E. Portability

IP creation on the go is the only way that users can access the Internet while away from a traditional modem/router setup.Mobil IP address create a tunnel to host server,which allows an access point to the Internet from any location where a signal can be received.Mobile IPs create connection protocols to connect to the Internet through multiple servers and networks.A Mobile Ip address allows users to roam through multiple networks and maintain an IP address.This option is useful for employees who travel throughout a building and cross into multiple wireless zones[13].

CONCLUSION

Typical mobile devices change networks several times throughout the day. When the original set of Internet protocols was designed, mobility was not an issue that was taken into account.It has been shown in this paper that, even with the limitations that exist in the implementation of Mobile IP, there is a higher need for Mobile IP in the future. Security needs receive active attention and benefit from the efforts of current deployment.Mobile IP provides network mobility solution over the internet. This paper has also discussed few of the challenges that are faced by the Mobile IP and solutions have been proposed for a successful deployment of Mobile IP in the future.

I hope that brief introduction to Mobile IP will engender interest in the solution to the remaining problems which continue to challenge deployment of the protocol.

Future work is addressing new mechanisms to provide quality of service support while maintaining the same simple lightweight protocol approach to host mobility and wireless access to the internet.

REFERENCES

[1] Geert Heijenk " Mobile & Wireless Networking"D. Johnson and C.Perkins, "Mobility support in IPv6," 2009

[2] D. Johnson and C.Perkins, "Route optimization in Mobile IP," IETF , November 1997

[3] Courtesy pf Youn-Hen Han , "Mipv4 &Mipv6 ", 2012

[4] Fayza Nada, "Performance analysis of Mobile IPv4 and Mobile IPv6," IETF, March 2006

[5] Marcelo Bagmulo,Phil Eardley,Alan Ford" Boosting mobility performance whith Multi-Path Tcp"2010

[6] X. Jiang and U. Narayanan,"Performance Analysis of Mobility Support in IPv4/IPv6 Mixed Wireless Networks," Vehicular Tec hnology, IEEE Transactions on, vol. 59, pp. 962-973, 2010.

[7] R. Gunasundari and S. Shanmugavel, "Performance Comparison of Mobile IPv4 and Mobile IPv6 protocols in

[8] wireless systems," in Communication Systems and Networks and Workshops, 2009. COMSNETS 2009. First International, 2009, pp. 1-8.

[9] S. William and M. Gerla, "IPv6 flow handoff in ad hoc wireless networks using mobility prediction," in Global Telecommunications Conference, 1999. GLOBECOM '99, 1999, pp. 271-275 vol.1a.

[10] Jie Li, Hui Jing and Guojun Wang, Authentication protocols for Mobile IP networks, IEEE Computer Society, ICICIC'08, 2008. http://www.tcpipguide.com/free/"MOBILE IP"

[11] Oracle, "System Administration Guide" Charles E. Perkins, Mobile Networking through Mobile IP

[12] The Cisco® Visual Networking Index (VNI) Global Mobile Data Traffic Forecast Update February 9, 2010.

Mihai-Marius Criste(B.April 24,1989) received his M.Sc in Computer Siences(2013) from the Technical University of Cluj-Napoca. Now he is stady Ph.D. and Network Server Administrator.
Responsible for IT maintenance and computer network administration Installation and maintenance of switching and routing equipment (CISCO). He is keen interest in Mobile IP and Networking.

Vasile-Teodor Dadârlat (b. January 13, 1955) received his M.Sc. in Computer Science(1980) from „Politehnica" University Bucharest and PhD in Computer Science (1995) from the Technical University of Cluj-Napoca. Now he is full professor of computer sciences within the Computer Science Department of the Automation and Computers Faculty,Technical University of Cluj-Napoca, Romania and director of associated „Computer Networks" Research Lab. His current research interests include different aspects of communications networks and protocols, digital circuits and e-learning systems. He has (co)authored 15 books and more than 60 papers, has more than 40 conferences participation, and has served on the TPCs of major conferences in networking and e-learning. Prof. Dadarlat has received a number of awards from the Romanian academic and technical bodies.