Mobile IP: Issues, Challenges and Solutions

Janani Chandrasekaran
Department of Electrical and Computer Engineering
Rutgers University
jananic@eden.rutgers.edu

***Abstract*—The recent years have witnessed a tremendous growth in the number of mobile internet users and the need for mobility support is indispensable for seamless internet connectivity. Mobile IP is a mobility support protocol that supports roaming across multiple Access Points without having to re-establish the end to end connection.**

In this paper, we take the position that despite several challenges that Mobile IP faces, it would turn out to be the protocol for supporting mobility in the future. We support our claim by analyzing the factors that would influence the widespread adoption of Mobile IP and we go further to discuss the counter claims in an effort to convince the reader that the advantages of Mobile IP outweights its disadvantages.

I. Introduction

With the increase in popularity of the Vehicular Networking research and the resistance in the internet community to developing a radically different networking stack, there is a need for supporting highly mobile clients using the existing TCP/IP protocol stack [2], [5]. In the current implementation of wireless networks, when a node moves from one access point to another access point, it re-establishes the connection every time with a different IP address. This increases the Latency of the network and also provides an interrupted service.

The necessity for uninterrupted communication when the mobile device moves from one location to another calls for the a new technology. This kind of communication can be efficiently implemented using Mobile IP. Mobile IP, which is an extension to standard Internet Protocol proposed by the Internet Engineering Task Force(IETF). It maintains the same IP address even when the host node moves from one network to the other. Hence with the implementation of Mobile IP it is possible to have a continuous connectivity with the network irrespective of the location of the host node.

In my opinion, Mobile IP will be successful in the future as it has several notable features like no geographical limitation, no physical connectivity required, supports security, no modifications for the current IP address. The main factors that influence the need for 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 alternatives other than Mobile IP
- IPv4 Availability, limited availability of IPv4 address necessitates the need for Mobile IP
- Improved Security, while registering with the home agent

Mobile IP could be extended to encompass all the technologies for seamless mobility if the following issues are resolved. These are

- Security Issues
- Triangulation Problems
- Reliability Issues
- Latency Issues

This paper describes the working of Mobile IP in section II, addresses the factors that influence the need for Mobile IP in section III and the issues to be resolved for successfully implementing Mobile IP in section IV and the section V of the paper has the conclusion

II. Background

The Mobile IP uses the existing IP protocol to implement the communication effectively for the mobile hosts [3], [7], [9], [10], [12], [16]. It is necessary to be familiar with few terminologies before understanding the working of Mobile IP.

Mobile Node (MN): This corresponds to the node which moves from the home network to the foreign network. This node is assigned a permanent IP address to which the packets are always sent. The packets that are sent from other nodes to the mobile node will always be destined to its home IP address.

Home Network (HN): This is the network to which the mobile node is permanently connected. This subnet corresponds to the home address of the mobile node as well as home agent.

Home Agent (HA): The Home Agent forwards the packets to the mobile node that are destined for it. When the mobile node is in foreign network then it is the responsibility of the home agent to forward the packets that are destined to the mobile node to the foreign agent

Foreign Network (FN): This is the network to which the mobile node attaches itself after moving from the home network.

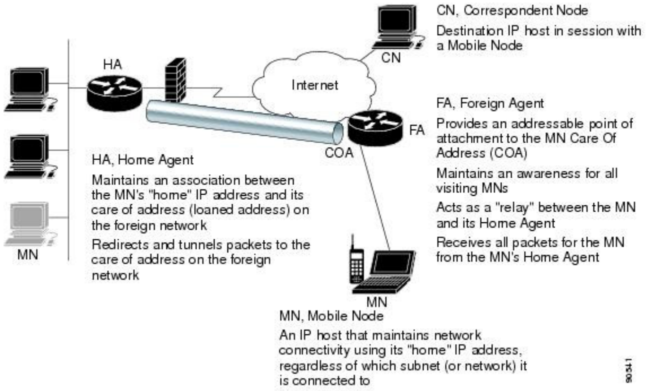
Foreign Agent (FA): Foreign Agent is a router located in the foreign network to which the mobile node is attached. It is configured to receive and forward the packets that are destined to the mobile node when the mobile node has a foreign agent care of address. While using collocated care of address, this foreign agent is used as a default router or for registering with the foreign network.

Care-of-Address (COA): This is the address that the mobile node uses for communication when it is not present in its home network. This can either be foreign agent care-of-address or a collocated care-of-address.

- *Foreign Agent Care-of-Address (FA COA):* The mobile node uses foreign agent's IP address as its care-of-address
- *Collocated Care-of-Address (CO COA):* The network interface of the mobile node is temporarily assigned an IP number on the foreign network.

Correspondent Node (CN): The node which communicates with the mobile node. This node can be located in any network and routes the packets to the home network of the mobile node.

Tunneling: 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*



CN, Correspondent Node
Destination IP host in session with a Mobile Node

HA, Home Agent
Maintains an association between the MN's "home" IP address and its care of address (loaned address) on the foreign network
Redirects and tunnels packets to the care of address on the foreign network

FA, Foreign Agent
Provides an addressable point of attachment to the MN Care Of Address (COA)
Maintains an awareness for all visiting MNs
Acts as a "relay" between the MN and its Home Agent
Receives all packets for the MN from the MN's Home Agent

MN, Mobile Node
An IP host that maintains network connectivity using its "home" IP address, regardless of which subnet (or network) it is connected to

Fig. 1. Architecture of Mobile IP

For the Mobile IP to work effectively the three important entities that are to be altered are mobile node, home agent and foreign agent when the mobile node uses foreign agent care-of-address. If collocated care-of-address is used, then home agent is alone modified. It is preferred to have Foreign Agent type of care-of-address in IPv4 because of its limited address space.

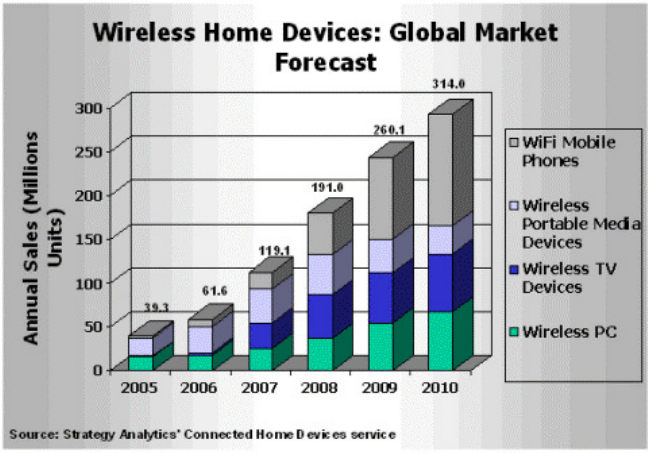
As shown in the figure 1 when the mobile node moves from its Home Network, it has to get connected to a Foreign network. There are two ways of finding agents when the mobile node is away from the home network. The first is by selecting an agent from among those periodically advertised, and the second is by sending out a periodic solicitation until it receives a response from a mobility agent. The mobile node thus gets its care-of-address which may be dynamically assigned or associated with its foreign agent. After receiving the care-of-address, the mobile node has to register this address with the home agent. As the correspondent node sends packets to the mobile node, the packets are will be forwarded to the home network. On the reception of the packets, the Home Agent encapsulates these packets within another packet with the source IP address as Home Agent address and the destination IP address as Foreign Agent care-of-address and forwards it to the Foreign Agent. Using collocated care-of-address, the Foreign Agent is responsible for unmarshalling the tunneled packets and sending it to the mobile node. Also it is responsible for sending the packets from the mobile node to correspondent node and to the home agent. On the other hand, with foreign agent care-of-address, the mobile node is directly connected to the foreign network and hence communicates directly with the home agent.

III. The Need for Mobile IP

Though the growth of Mobile IP was slow compared to the Wireless LAN, the need for Mobile IP is increasing rapidly. The various factors that influence the implementation of mobile IP which are discussed in this section [4], [6].

A. Mobility Support

Figure 2 plots the forecasted number of mobile devices in the year 2010. We can see that the forecasted number of mobile devices is predicted to go up by 314% for the year 2010. This increase inturn translates to increased number of mobile devices and thus increased need for mobility support. This would be one of the most compelling reasons for the deployment of Mobile IP.



Source: Strategy Analytics' Connected Home Devices service

Fig. 2. Productivity trends in Mobile Devices

B. Standardization

The way the Internet Protocol, the protocol that connects the networks of today's Internet, routes packets to their destinations according to IP addresses. All the devices like Desktops, Laptop's, PDAs, iPhones are all assigned an IP address. Mobile IP also uses the standard TCP/IP protocol suite [11] [15] [16]. So any device that supports IP can also support Mobile IP. Mobile IP does not drop the network prefix of the IP address of the node, which is critical to the proper routing of packets throughout the Internet. There are several advantages of using TCP/IP stack in Mobile IP

- **Failure recovery:** If there is a failure in a particular subnetwork, then it is still possible to establish the connection with the remaining networks.
- **Adding Networks:** It is possible to add more access points without changing the existing design.
- **Platform independent:** The standard TCP/IP protocol is platform independent and hence this makes it possible for Mobile IP to be implemented in different devices like cellular phones, iPhones, Laptops with Macintosh, Windows, Linux etc.
- **Reduced Cost :** There is a great reduction in cost because maintenance becomes simpler and any error handling can be performed easily. Also modifications in the existing network can be implemented without much overhead in cost.

C. Inter-Operability

There are various service providers available and with different network connections. With a heterogeneous network there is need for a standard protocol to be used with all these providers for an effective communication. This scenario can be explained better with the mobile phone services. For mobile phones there are various service providers available and also there is a need for connecting the call from one service to another service. For instance a node from a PSTN network to a mobile node of an ATnT network or an ATnT mobile node to a Verizon mobile node. Mobile IP allows this kind of interoperability to provide a good communication between all the nodes that are connected to different networks across the world.

D. Alternative Technologies

In order to support mobile communication without disconnecting from the network there are only two possible solutions that are available apart from Mobile IP which is cited in [11]. These are

1) the node must change its IP address whenever it changes its point of attachment,
2) host-specific routes must be propagated throughout much of the Internet routing fabric.

These alternatives are not widely accepted because in the first method it is not possible to maintain the connection in transport layer and higher layers of the protocol suite and in the second method there will be scalability problems with increase in the number of wireless devices. Therefore Mobile IP would turn out to be the quick fix at least in the next decade for providing seamless mobility support for the end-users.

E. IPv4 Availability

Just as IPv4 has become the de facto standard for networked communication, the cost of embedding substantial computing power into handheld devices has plummeted. As a result, the using a temporary IP for mobile communication uses exhaustive number of IPv4 addresses. The number of IPv4 address can be efficiently used by using Mobile IP, in which each host is assigned a permenant IP address.

F. Improved Security

Security problems are considered when registering to the home agent [10], [12]. All registration messages between a Mobile Node and Home Agent are required to contain the Mobile-Home Authentication Extension (MHAE). The integrity of the registration messages is protected by a preshared 128-bit key between a Mobile Node and Home Agent. The keyed message digest algorithm 5 (MD5) in ”prefix+suffix” mode is used to compute the authenticator value in the appended MHAE, which is mandatory. Mobile IP also supports the hash-based message authentication code (HMAC-MD5). The receiver compares the authenticator value it computes over the message with the value in the extension to verify the authenticity. Optionally, the Mobile-Foreign Authentication Extension and Foreign-Home Authentication Extension are appended to protect message exchanges between a Mobile Node and Foreign Agent and between a Foreign Agent and Home Agent, respectively. Replay protection uses the identification field in the registration messages as a timestamp and sequence number. The Home Agent returns its time stamp to synchronize the Mobile Node for registration.

IV. The Issues with Mobile IP

There are some limitations with the Mobile IP and hence one could argue that the Mobile IP cannot be successful. This section explains the challenges faced by Mobile IP and solutions are proposed for the same

A. Security Issues

The major security issues and their corresponding solutions that are concerned with the Mobile IP are presented below. Security attacks [1], [14], [18].

- Denial Of Service Attacks The Denial of Service Attacks can be caused when an attacker sends a tremendous number of packets to a host (e.g., a Web server) that brings the hosts CPU to its knees. In the meantime, no useful information can be exchanged with the host while it is processing all of nuisance packets. It can also be caused when an intruder somehow interferes with the packets that are flowing between two nodes on the network or when a malicious host generates a bogus Registration Request specifying his own IP address as the care-of address for a mobile node. All packets sent by correspondent nodes would be tunneled by the nodes home agent to the malicious host. The possible prevention method for this is to require cryptographically strong authentication in all registration messages exchanged by a mobile node and its home agent. Also Mobile IP by default supports MD5 Message-Digest Algorithm that provides secret-key authentication and integrity checking.
- Theft of Information Passive Eavesdropping, an unauthorized person will inevitably gain wired or wireless access to the network infrastructure. The solution is either by the use of Link-Layer Encryption where it is assumed that key management for the encryption is performed without disclosing the keys to any unauthorized parties or the use of End-to-End Encryption. Session-Stealing, this type of attack involves transmitting various nuisance packets to prevent the legitimate node from recognizing that the session has been captured. The attack can be prevented from the above actions, end-to-end and link layer encryptions.
- Insider Attack This usually involve a disgruntled employee gaining access to sensitive data and forwarding it to a competitor. The solution for this is to enforce strict control for who can access what data, to use a strong authentication of users and computers and to encrypt all data transfer on an end-to-end basis between the ultimate source and ultimate destination machines to prevent eavesdropping.

- Replay Attack A malicious host could obtain a copy of a valid Registration Request, store it, and then replay it at a later time, thereby registering a bogus care-of address for the mobile node. In order to prevent, the Identification field is generated is a such a way that it allows the home agent to determine what the next value should be. In this way, the malicious host is thwarted because the Identification field in his stored Registration Request will be recognized as being out of date by the home agent.
- Other Attacks The malicious host can connect to the network jack and figure out the IP address to use, and finally tries to break to the other hosts on the network. He can find out the network-prefix that has been assigned to the link on which the network jack is connected. Also an intruder can guess a host number to use, which combined with the network-prefix gives him an IP address to use on the current link or else proceeds by trying to break into the hosts on the network guessing user-name/password pairs. To prevent such attacks all publicly accessible network jacks must connect to foreign agent that demands any nodes on the link to be registered. Otherwise, remove all non-mobile nodes from the link and require all legitimate mobile nodes to use link-layer encryption.

B. *Triangulation Problem*

The basic idea behind triangle routing [10], [15] is that a mobile node wants to send packets to another node that is on the same network. The receiver node happens to be far away from the mobile nodes home network. Then the sending node addresses all the packets to the home network. They pass through the Internet to reach the home agent and then tunnels them back across the Internet to reach the foreign agent. Triangle routing problem delays the delivery of the datagrams to mobile nodes and places an unnecessary burden on networks and routers along their paths through the Internet. This all can be improved by techniques in the route optimization, delivery of packets directly to care-of address from a correspondent node without having to detour through the home network. The sending node should be told the care-of address of the mobile node. The sending node makes its own tunnel to the foreign agent, an optimization of the process that was aforementioned. In the case where the sender contains the required software to learn the care-of address and is able to create its own tunnel, then the route is optimized. If not, another route must obviously be taken. A home agent finds out that a packet is being sent from one of the mobile nodes that it supports. From here, the home agent is aware that the sender is not using the optimal route. It then sends a binding update message back to the source as well as forwarding the packet back to the foreign agent. The source then uses this information, if proficient, to construct an entry in the binding cache. This binding cache is a book of mappings from mobile node addresses and care-of addresses. The next time this source has a packet to send to that mobile node, it will find the section in the cache and will tunnel the packet directly to the foreign agent.

C. *Reliability Issues*

The design of Mobile IP is founded on the premise that connections based on TCP should survive cell changes. However, opinion is not unanimous on the need for this feature. Many people believe that computer communications to laptop computers are sufficiently bursty that there is no need to increase the reliability of the connections supporting the communications. The analogy is made to fetching Web pages by selecting the appropriate URLs. If a transfer fails, people are used to trying again. This is tantamount to making the user responsible for the retransmission protocol and depends for its acceptability on a widespread perception that computers and the Internet cannot be trusted to do things right the first time. Naturally, such assumptions are strongly distasteful to many Internet protocol engineers. Nevertheless, the fact that products exhibiting this model are currently economically viable cannot be denied. Hopefully in the near future better engineering will counter this perception and increase the demand for Internet reliability.

D. *Latency Issues*

With Mobile IP, the handoff latency depends on the distance between Home Agent (HA) and Foreign Agent (FA). There are solutions proposed for this latency issues in the papers [8], [13], [17], [19].

V. CONCLUSION

Mobile IP which has a slow growth compared to the Wireless LAN seems to be a failure technology but Mobile IP has great potential. The increased user convenience and the reduced need for application awareness of mobility can be a major driving force for its adoption. It has been shown in this paper that even with the limitations that are present in the implementation of Mobile IP, there will be a higher need for Mobile IP in the future. Security needs are getting active attention and will benefit from the deployment efforts underway. There are works that are going on in this field to overcome the limitations that are currently present in Mobile IP. 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.

REFERENCES

[1] Applicability statement for ip mobility support. http://www.rfc-editor.org/rfc/rfc2005.txt.

[2] Cisco ios ip configurationguide, release12.2 - configuring mobile ip [cisco ios software releases 12.2 mainline] - cisco systems. http://tinyurl.com/5mpj6w.

[3] Introduction to mobile ip. http://www.hpl.hp.com/personal/Jean_Tourrilhes/MobileIP/ppal.html.

[4] Introduction to mobile ip [ip tunneling] - cisco systems. http://tinyurl.com/5z9xpk.

[5] Mobicom ’95 tutorial: Mobile - ip.

[6] Mobile ip - wikipedia, the free encyclopedia.

[7] Mobile-ip: Transparent host migration on the internet. http://www.linuxjournal.com/article/1271.

[8] A new prioritized fast handoff protocol for mobile ip, from napier university - white papers, webcasts and case studies - techrepublic. http://whitepapers.techrepublic.com.com/abstract.aspx?docid=334523.

[9] Rfc 3344 - ip mobility support for ipv4. http://tools.ietf.org/html/rfc3344.

[10] Rfc 4721 - mobile ipv4 challenge/response extensions (revised). http://tools.ietf.org/html/rfc4721.

[11] Rfc ip mobility support. http://www.ietf.org/rfc/rfc2002.txt.

[12] A survey on mobile ip.

[13] A. Diab and A. Mitschele-Thiel. Minimizing mobile ip handoff latency.

[14] A. Fasbender and D. Kesdogan. and olaf kubitz.

[15] C. Perkins. Mobile networking through mobile ip. *Internet Computing, IEEE*, 2(1):58–69, 1998.

[16] J. Redi and P. Bahl. Mobile ip:a solution for transparent seamless mobile computer communications. In *Report on Upcoming Trends in Mobile Computing and Communications*.

[17] S. Sharma, N. Zhu, and T. cker Chiueh. Low-latency mobile ip hando for infrastructure-mode wireless lans.

[18] T. Taleb, H. Nishiyama, N. Kato, and Y. Nemoto. securing hybrid wired/mobile ip networks from tcp-flooding based denial-of-service attacks. In *Global Telecommunications Conference, 2005. GLOBECOM ’05. IEEE*, volume 5, page 5 pp., 2005.

[19] D. Tandjaoui, N. Badache, and I. R. Diab. A new prioritized fast handoff protocol for mobile ip.