Requirement of Mobile IP, its issues and solutions

Milan Vachhani
Assistant Professor,
Department of MCA,
B. H. Gardi College of Engineering & Technology,
Rajkot

Priyanka Ramani
Student of MCA
B. H. Gardi College of Engineering & Technology,
Rajkot

ABSTRACT
In the most recent years, the area of mobile computing has developed enormously. Devices like PDAs, handhelds and digital mobile phones those ongoing gadgets of luxury have converted into a necessity in today's "always stay connected" routine. At this time Mobile IP came into picture to provide the portability without disconnecting. This allows the mobile node to use two IP addresses: a fixed home address and a care of address that change at every new point of connection. But with the advantages of Mobile IP also came the disadvantages, the biggest disadvantage that is security. When a device moves from its home network and enters a new network (foreign network), it has to change its IP address and re-establish a new TCP connection. If communication with this moving device occurs at that time, the communication has to be disconnected until a new IP address of a moving device is obtained. To solve this mobility issue, a working group within the Internet Engineering Task Force (IETF) proposed a solution, which is called Mobile IP Protocol. In this paper, we discuss a few of the common security threats that mobile IP networks are exposed to as well as some proposed solutions to deal with such threats.

Keywords
Mobile node (MN), Home Agent (HA), Corresponding agent (CN), Foreign Agent (FA), mobile host (MH), Communication Host (CH), Care of Address (CoA).

1. INTRODUCTION
The number of mobile devices, computers, mobile, (PDA), and personal digital assistants and mobile phones are increasing rapidly. 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.

Globally, mobile data and increase year after year until 2014, increasing 39 times between 2009 and 2014, to reach 3.6 Exabyte company Exabyte month or $ 40 annually in 2014 [8].

Mobile IP uses Ways plans TCP / IP standard to their destinations, according to the IP address. The following figure shows will sign the global mobile data traffic is growing at a 3.6 Exabyte monthly in 2014, more than 2.3, which is the result of mobile video traffic [8]. This is due to the increased use of laptops and mobile phones appropriate with high-speed broadband.

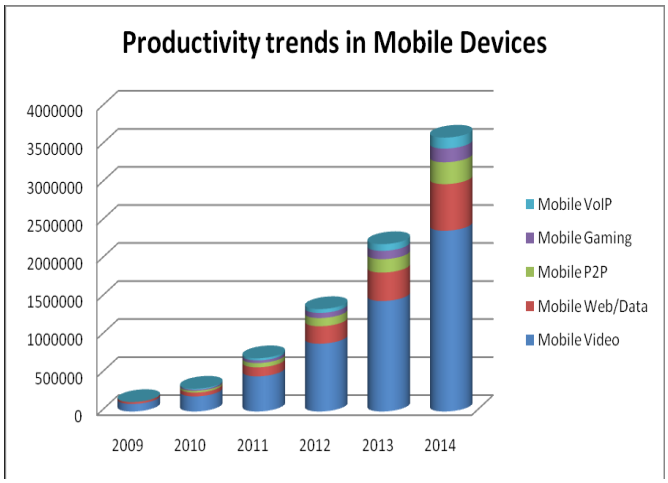

Fig. 1: Productivity trends in Mobile Devices

2. IMPORTANCE OF MOBILE IP
It is necessary to the requirement of Mobile IP because of the limitations, which are observed for the period of traditional research. In the traditional intellectual property system, a node always has an address that uniquely identifying. In addition, this address comprises two components, the network ID and host identifier.

The principle of network and host portion of an IP address would take us to the following issues:

1) if a node changes its point of attachment is a necessity to replace your IP address. This means that there are no places (nodes) over the Internet with the same host and network ID.

2) Whether a node changes address the rest of do not know your new address, unless it is informed for these reasons, a traditional IP node moves to a different network will not be able to communicate in the new network with the output additional IP configuration. There are situations, which demand highly communication node being disconnected from your network base. Moreover, reconfiguration may not be simple for the average user. Through all these reasons, it would be best for the users connecting to remote networks where work and play as if they were on your home network that can be done using Mobile IP.

3. ARCHITECTURE OF MOBILE IP
The Emergency Mobile IP introduces new features and the most important architectural terminologies Mobile IP entities and terminologies are the following:

3.1 Mobile node (MN):
MN is a node, which can change one connection point with, changed its IP address

3.2 Home Agent (HA):
A system within the home network of the mobile node registers the location of the mobile node receives packets intended for the mobile node to the home and tunnels network packets to support of address of the mobile node.

3.3 Corresponding agent (CN):
A node that communicates with the mobile node.

3.4 Foreign Agent (FA):
It is a router on the foreign network that using a locally accessible the mobile node in providing of packets between the mobile node and the home the agent. It also helps the mobile node to obtain the care-of address.

3.5 Home address:
The IP address of the mobile node to the home network. The address remains the same whatever the mounting location of the mobile node.

3.6 Care Address:
Care of address is an IP address that identifies the current location of a mobile when the node is not tied to his home network node. it will be obtained from the foreign network and will be recorded for the home agent

3.7Home Network:
The network in which the MN is for the most part.

3.8Foreign network:
A network that visits of mobile nodes.

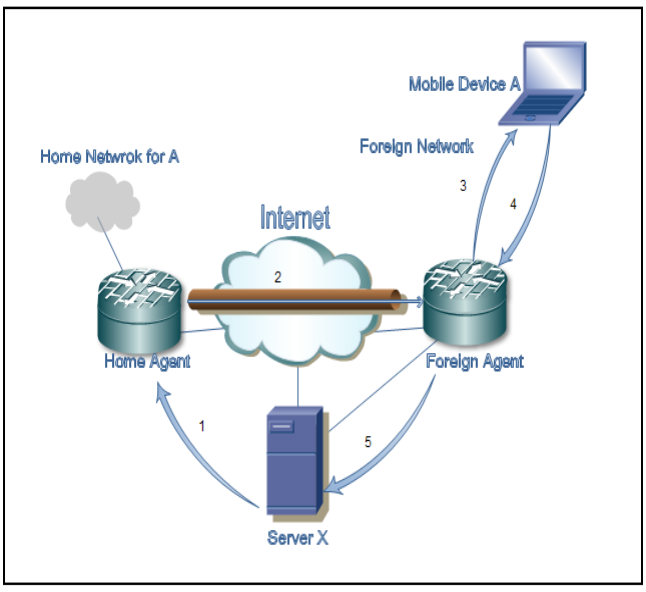

Fig. 2: Architecture of Mobile IP

4. THE ISSUES WITH MOBILE IP
There are some restrictions with mobile IP and hence it could be argued that the Mobile IP cannot be successful. This section explains, we propose the challenges faced by IP and mobile solutions for the same.

Major safety problems and corresponding solutions that deal with the mobile IP are presented below. Security attacks are as following [5], [1], and [10].

4.1 Denial of Service:
Attacks Denial of Service can be caused when an attacker sends many packets to a host (eg a Web server) that hosts CPU brings the knees. Meanwhile, no useful information can be exchanged with the host while annoying process all packages. It can also be caused when an intruder somehow interferes with packets flowing between two nodes in the network or when a malicious host generates a false registration request specify its own IP address as the care-of address of a mobile node. All packets sent by the corresponding nodes are tunneled by the home agent to host malicious nodes. The possible prevention method for this is to require cryptographically strong authentication on all log messages exchanged by a mobile node and its home agent. Default IP Mobile also supports MD5 Message-Digest algorithm that provides authentication and integrity checking password.

4.1.1 Information Theft:
Passive listening, an unauthorized person, inevitably, access to wired and wireless network infrastructure. The solution is either by the use of link layer encryption, which is supposed to key management for encryption is done without revealing the keys to any unauthorized party or the use of end-to-end encryption. Session Stealing, this type of attack is the transmission of packets of different lengths to avoid legitimate node to recognize that the session has been captured. The attack can prevent the above actions, end-to-end encrypted link layer.

4.1.2 Insider Attack:
This typically involves a disgruntled employee access to sensitive data and transmits it to a competitor. The solution for this is to apply a strict control of who can access what data, to use a strong authentication of users and computers and to encrypt all data transfers between end-to-end final destination machines to prevent eavesdropping home and end.

4.1.3 Replay Attack:
A malicious host can get a copy of a valid registration, store, and then play it later, thus recording the false attention direction of the mobile node.

In order to prevent, generates the identification field is such a shape that allows the home agent to determine what the next value should be. In this way, the malicious host was frustrated because the ID field in your registration request is recognized as out of date by the agent.

5. ANOTHER PROBLEM WITH MOBILE IP
Although growing rapidly, Mobile IP still has the following problems:

5.1 "Triangle routing" Problem
The Communication Host (CH) has to forward packets to the mobile 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.

5.2 Handoff Problem

Handover issue means that the HA sends IP packets to the network MS original foreign across the tunnel, and you do not know 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 dropped have an influence on the communication between the MS and the CH especially when transfer frequently occurs or the MS is away from the HA.

Solution:

The transfer process divides into two stages:

1) **Mobile testing Phase:** In this stage a test mobile is performed to determining whether the MH has been changed to the sub-network access.

2) **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 the request, 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 [5].

5.3 Problem of Intra-Domain Movement

The frequent intra-domain movement of the MH within a small area will lead to frequent handoff. Consequently, a great amount of registered messages are generated in the network and the network performance is greatly affected [5].

Solution:

For intra-domain micro-motion, such as enhancing of Mobile IP protocols, Hawaii and TeleMIP available for adoption to resolve the problem of frequent transfers, and to reduce the transfer delay, the ratio of the packet loss, and registration information to the HA. [9].

5.4 QoS 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 [6].

6. CONCLUSION

Mobile IP has great potential. 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. There are works that are underway in this area in order to overcome the limitations that are currently present in Mobile IP. This paper also discussed some of the challenges faced by the Mobile IP and solutions have been proposed for the successful deployment of Mobile IP in the future.

The increasing numbers of office workers in the movement number, increasing dependence on the calculation of the network and the Internet, and more convenience and numeracy that support laptops are all the engine growth of the Mobile IP technology.

Since the introduction of Mobile IP in 1996, a number of free applications Mobile IP support and business have emerged. However, there are still some difficulties in large commercial applications of Mobile IP and some problems that cannot be satisfactorily resolved, such as security issues, encryption and authentication, input filtering, transfer node, intra-domain QoS and movement. While these problems are solved gradually, the Mobile IP technology will play an important role in mobile communications, providing unprecedented opportunity and convenience in the free communication of people and offering new opportunities to develop new applications in the future.

7. REFERENCES

[1] A. Fasbender and D. Kesdogan. and olaf kubitz. Analysis of Security and Privacy in Mobile IP, 4th International Conference on Telecommunication Systems, Modelling and Analysis, März 21 - 24, 1996, Nashville, TN, USA

[2] Lei Zhenzhou. Development and Market Trend of Mobile IP Technology[J]. China Radio Management, 2001

[3] Ye Minhua, Liu Yu, Zhang Huimin. Handover Technology in Mobile IP[J]. Telecommunication Technology, 2003

[4] Gloria Tuquerres, Marcos Rogerio Salvador and Ron Sprenkels, Mobile IP: Security & Application, 1999

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

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

[7] Yang Xin, Chen Junliang. Mobility Support of the Network and Its Research[J]. China Data Communications, 2004(5).

[8] 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.

[9] Feng Yong, Li Fangwei. QoS Guarantee over Mobile IP[J]. Telecommunications Science, 2002.

[10] Charles E. Perkins, Mobile Networking through Mobile IP