



Scope and Challenges in Mobile IP

Kanij Fatema Aleya, Madhumita Santra, Supriya Maji, Asoke Nath
Department of Computer Science, St. Xavier's College (Autonomous)
Kolkata, India

Abstract—*The last couple of years there was a tremendous growth in the number of mobile internet users and the need for mobility support is indispensable for seamless internet connectivity. The area of mobile computing has grown tremendously. Devices like PDAs, handhelds and digital cellular phones etc are used by the users throughout the globe. In the present paper the authors have made a systematic study on mobile IP, how it works and the scope and challenges that Mobile IP faces and their solutions.*

Keywords—*foreign agent; home agent; tunnelling; smooth handoff; denial of service attack*

I. INTRODUCTION

We want to keep our IP addresses wherever we are, but a traditional IP design does not support mobility. So, whenever we change our location, we also need new IP addresses. Changing IP addresses is undesirable for several reasons. As we know, most Internet traffic is TCP, and changing the IP address forces TCP to establish a new connection. As a result, packets might get lost during this change. Moreover, a mobile node will be assigned a foreign IP address instead of a local IP address. Then, using the foreign IP address makes it difficult for users to gain access to their private or local networks, such as local printers. Mobile IP was designed to solve all these problems. Mobile IP is a standard that allows users to move from one network to another without losing connectivity. Mobile devices have IP addresses that are associated with one network and moving to another network means changing IP address. Using the mobile IP system will allow users to achieve this and at the same time make the underlying process transparent for a user. Cell phones allow users freedom of movement and Personal Digital Assistance “PDA” offers users to access email in any location. Global Positioning System (GPS) has the capability to pinpoint the location of the device anywhere in the world. Mobile IP is scalable for large number of users, and users can be confident that no one can read their messages or use their resources.

II. MOBILE IP ENTITIES

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.

Home Network (HN): This is the network to which the mobile node is permanently connected.

Home Agent (HA): The Home Agent forwards the packets to the mobile node when it away from its home network.

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 mobile node visited network. It receive and forward the packet for the mobile node.

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.

III. WHY MOBILE IP?

In IP networks, routing is based on stationary IP addresses. A device on a network is reachable through normal IP routing by the IP address it is assigned on the network. When a device roams away from its home network, it is no longer reachable by using normal IP routing. This results in the active sessions of the device being terminated. Mobile IP enables users to keep the same IP address while traveling to a different network, ensuring that a roaming individual can continue communication without sessions or connections being dropped. The basic idea behind Mobile IP is to let one host have two simultaneous addresses, one at the home network and one at the foreign network. The home network address is never changed. This address is used by applications and transport protocols. The address at the foreign network is temporary.

Mobile IP 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: We can see 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.

Standardization: Internet protocol 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. So any device that supports IP can also support Mobile IP.

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. 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.

IV. MECHANISM OF MOBILE IP

A. Agent Discovery

The agent discovery procedure used in Mobile IP is based on the Internet Control Message Protocol (ICMP) router advertisement standard protocol. It allows the mobile node to determine whether it is connected to the home network or foreign network. A special message called agent advertisement periodically broadcasted by the home agent or foreign agent to advertises their availability or services. The mobile node listen these advertisement and compare the network portion to its home address network portion. If it matches then it is home agent otherwise it is foreign agent. Then it acquires an care of address when the mobile agent does not receive any advertisement message it generate agent solicitation message when it is looking for a foreign agent.

B. Registration

When a mobile node is away from home its registers its care-of-address with its home agent. Registration process can perform directly from the mobile node when the care-of-address is dynamically generated or registration process can be perform by the foreign agent by the following steps:

Step1: The mobile node registers with the foreign agent giving its home address, current data link address and some security information.

Step2: The foreign agent contact the mobile host home agent.

Step3: the home agent examines the security information which contains a time stamp to prove that it is generated within the past few sec. if it is happy it tells the foreign agent to proceed.

Step4: When the foreign agent gets the acknowledge from home agent its makes an entry in its tables and inform the mobile host that it is registered.

C. Tunneling

When the mobile device register itself the home agent will be able to intercept the IP packet that sends to the mobile node home address. Tunneling has two function encapsulating the packet to reach to the tunnel end point and decapsulates the packet when the packet reach to the tunnel end point. When a packet reach to the mobile node home address it encapsulates the original packet within a new packet placing the mobile node care of address as the destination address. When the foreign agent receive the packet It decapsulate the packet and forward it to the mobile node. Tunneling can be two types IP within IP and minimal encapsulation. In IP within IP the original packet becomes the payload and in the minimal encapsulation only the header part is added which is different from the original header.

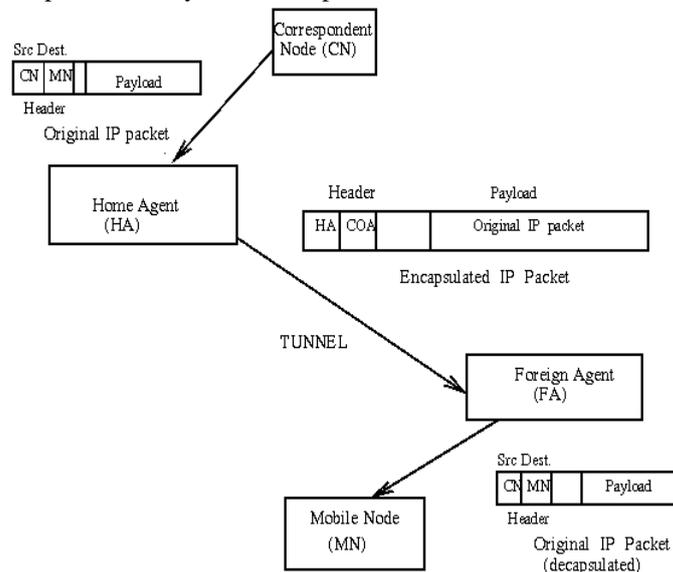


Fig 1

V. SECURITY ISSUES IN MOBILE IP

Security is always concern in any internetworking environment these days, but it is especially important in mobile ip. Because it has a number of risks due to it using a registration system and then forwarding datagrams across an unsecured network.

A. Denial Of Service Attack

In the case of a mobile IP network a denial of service attack occurs when a bad guy manages to do a bogus registration of a new care-of address for a particular mobile node. Such a bogus registration gives rise to two problems: The good guy's mobile node is no longer connected; the bad guy gets to see all traffic directed to the original mobile node. The Mobile IP specification prevents bad guys from being able to do bogus registrations by requiring strong authentication on all registration messages that are exchanged during the registration process. In this case, unless the shared key is exposed, this type of attack is rendered impossible.

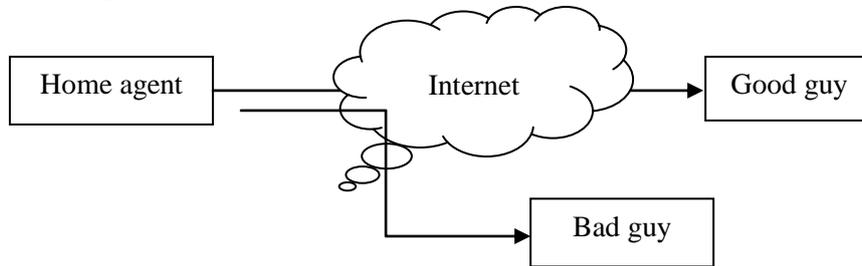


Fig-2

B. Passive Eavesdropping

Passive eavesdropping is one kind of information attack. When a mobile node and its home network is connected and transferred data the attacker analyses the traffic, determine the location and identify the communicating hosts. Passive attack is very difficult to detect because they do not involve any alteration of the data. when the messages are exchanged neither the sender nor the receiver is aware that a third party has read the messages. This can be prevented by encryption of data. So the attacker cannot decode or understand the cipher text and eavesdropping can no longer happen. If we use networking specific encryption then the traffic still might be a victim of eavesdropping. So the best solution is to use end to end encryption on all the traffic. This makes eavesdropping attack impossible.



Fig-3 Passive eavesdropping

C. Replay Attack

Using authentication we can protect the mobile devices from denial of service attack but we cannot protect the mobile devices from replay attack. Because the attacker can have a copy of registration request message, and the attacker use this message by registering a care of address for the mobile devices. To prevent this kind of attack, the mobile device has to generate a unique value for identification field when the registration process is happen. So the attacker registration request will be rejected because identification field that not match the expected value and this message will be ignored in the case of the mobile device.

VI. IMPROVEMENTS OF MOBILE IP

A. Route Optimization

When a mobile device is communicating with a correspondent node from a foreign network, all its packets must be forwarded through its home agent, this is called triangle routing which can results in significant degrading of performance. Route optimization to mobile IP has been recently proposed, allowing the home agent to inform the correspondent node with the mobile devices care of address, thus correspondent node can communicate directly with mobile device without passing the home agent, which results in less delay and resource consumption. When a correspondent node sends packet to the home agent the home agent think that this node is unaware of the mobile node current care of address. The mobile sends an authenticated binding update to update its binding cache. Binding cache contain mapping from home address to the temporary address. Once the correspondent node update its binding cache it can directly sends packet to the mobile node.

B. Agent Smooth Handoff

When a mobile node moves and registers with a new foreign agent, IP datagrams intercepted by the home agent after the new registration are tunnelled to the mobile node's new care-of address, but datagrams in flight that had already been intercepted by the home agent and tunnelled to the old care-of address when the mobile node moved are likely to be lost. The old foreign agent eventually deletes its visitor list entry for the mobile node after the expiration of the registration lifetime. Route optimization provides a means for the mobile node's previous foreign agent to be reliably notified of the

mobile node's new mobility binding, allowing datagrams in flight to the mobile node's previous foreign agent to be forwarded to its new care-of address. This notification also allows any datagrams tunneled to the mobile node's previous foreign agent, from correspondent nodes with out-of-date binding cache entries for the mobile node, to be forwarded to its new care-of address. Finally, this notification allows any resources consumed by the mobile node at the previous foreign agent to be released immediately, rather than waiting for its registration lifetime.

VII. COMPAISON OF MOBILE IPV4 AND IPV6

Table-1

Mobile IPV4	Mobile IPV6
Triangular routing, Correspondent Node cannot understand the Binding update message.	Routing Optimization, RRP provide protection for Binding Update messages between Mobile Node and Correspondent Node.
When use Ingress Filtering to defeat Denial of Service attack, Reverse Tunnelling should be deployed to make sure the packets sent by Correspondent Node can reach the Mobile Node.	When use Ingress Filtering to defeat Denial of Service attack, no need for Reverse Tunnelling Better coexistence with the Ingress Filtering policy.
Address Resolution Protocol, easily to be attacked.	Using Neighbour Discovery Protocol, better robustness and security
Foreign agent a potential threat.	There is no foreign agent.

VIII. CONCLUSION AND FUTURE SCOPE

Mobile IP provides network mobility solution over the internet. This paper's study focus on the security aspect in mobile IP and provides a lot of suggestions and methods to improve security in mobile IP. It seems certain that Mobile IP will play an increasingly important part in the deployment of future Internet mobile networking, and current events related to the specification and production of standard billing procedures seem likely to accelerate the penetration of Mobile IP into the marketplace

ACKNOWLEDGMENT

I am very grateful to Prof. Shalabh Agarwal and Dr Asoke Nath of the Department of Computer Science, St. Xavier's College (Autonomous), Kolkata, India, for their help and guidance in while preparing the write up of this seminar. I am also very grateful to all the professors for helping us to their utmost. The write up of this seminar wouldn't have been possible without their guidance.

REFERENCES

- [1] Charles E. Perkins, "Mobile IP" (publisher: Prentice Hall] (Feb.2008)
- [2] Khaled Mahmood Al-Adhal, Dr. S.S Tyagi / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com 616-621Vol. 2, Issue 6, November - December 2012.
- [3] Chapter 8 MOBILE IP AND TCP Mobile Computing Summer 2002
- [4] Security Issues In Mobile IP Zhang ChaoTsinghua University Electronic Engineering
- [5] Mobile IP – Security Issues and Solutions Sameer Chandragiri Dept of Computer Science University of Texas at Arlington CSE 6345 Term Paper
- [6] Security in Mobile and Wireless Networks APRICOT Tutorial Perth Australia 27 February, 2006 Ray Hunt, Associate Professor Dept. of Computer Science and Software Engineering University of Canterbury, New Zealand
- [7] Mobile IP: A Solution for Transparent, Seamless Mobile Computer Communications J. Redi a, P. Bahlb a Dept.of Electrical and Computer Engineering, Boston University, redi@acm.org b Microsoft Research, Redmond, WA, bahl@microsoft.com