ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

Issues in Mobile IP, Security, Challenges and Solutions

Mohammad Meraj Ud Din Mir

Research Scholar, Dept. of Computer Science and System Studies, Sri Venkateshwara University, Rajabpur Gajraula, Amroha, Uttar Pradesh, India

ABSTRACT:-Mobile IP is a standard that allows users to move from one network to another without loosing 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.

IP routing is based on the IP address, which uniquely identities a node's point of attachment to the internet. 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, I will through light that despite several challenges that Mobile IP faces, it would turn out to be the protocol for supporting mobility in the future. I will support my claim by analyzing the factors that would influence the widespread adoption of Mobile IP and to go further to discuss the counter claims in an effort to convince the reader that the advantages of Mobile IP.

KEYWORDS:- Mobile IP, IP routing, TCP/IP, Internet Engineering Task Force (IETF), IP datagrams, Care-of-address, collocated care-of-address, Mobile node, Home Agent, Home Address, Home Network, Foreign agent, Foreign Network, Correspondent Node, Dynamic Host Configuration Protocol, Point-to-point IP Control Protocol, IPv4, IPv6, Generic Routing Encapsulation or IP tunneling (IP encapsulation),

I. INTRODUCTION

Wireless communication has witnessed a growth number of users in the recent years; one of the main advantages of wireless technology is mobility, which allow mobile users to move from one network to another and maintaining their permanent IP address. This keeps transportation and high level connections while moving. Mobile IP is a standard protocol established by the Internet Engineering Task Force "IETF", to provide an efficient and scalable mechanism for mobile nodes within the internet. Mobile IP environments mostly exist in wireless networks where users need to carry their devices across several networks with different IP address.

Mobile IP is built on the IP protocol for internet infrastructure. As Mobile IP is a layer 3 solution for IP mobility, it will suffer from security problem in the same way as IP. As such the issue of securing Mobile IP has become the most significant point with increasing demand on Mobile IP. The main goal of network security is to provide confidentiality, availability and integrity for data communication. In general confidentiality protects data so that it is not disclosed from unauthorized persons. Availability protects data from any attempts to withhold information and integrity protects data from unauthorized modification.

The Mobile IP allows for location-independent routing of IP datagrams on the Internet. Each mobile node is identified by its home address disregarding its current location in the Internet. While away from its home network, a mobile node is associated with Care-of-address which identifies its current location and its home address is associated with the local end point of a tunnel to its *home agent*. Mobile IP specifies how a mobile node registers with its home agent and how the home agent routes datagrams to the mobile node through the *tunnel*.

DOI: 10.15680/IJIRCCE.2015. 0312123

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

II. BACKGROUND

Wireless communication has witnessed a growth number of users in the recent years, one of the main advantages of wireless technology is mobility, which allow mobile users to move from one network to another while maintaining their permanent IP address. This keeps transportation and high level connections while moving. Mobile IP is a standard protocol established by the Internet Engineering Task Force “IETF”, to provide an efficient and scalable mechanism for mobile nodes within the internet. Mobile IP environments mostly exist in wireless networks where users need to carry their devices across several networks with different IP address.

The goal of IP Mobility is to maintain the TCP connection between a mobile host and a static host while reducing the effects of location changes while the mobile host is moving around, without having to change the underlying TCP/IP. To solve the problem, the RFC allows for a kind of proxy agent to act as a *middle-man* between a mobile host and a correspondent host.

III. MOBILE IP TERMINOLOGY

Mobile IP has the following elements and entities that are required for optimum functionality .

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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

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.

A mobile device may have two addresses, a permanent home address and a care-of address (CoA). A care-of address is a temporary IP address that identifies a mobile device's current point of attachment to the internet and allows it to connect from different locations by keeping its home address. When a mobile device is leaving its home network and connects to any foreign network, it is assigned a care-of address. This may be a "foreign agent care-of address" which is a static address of a foreign agent with which the mobile device is registered, and a "co-located care-of address" which is a temporary IP address assigned to the mobile device. A co-located care-of address is assigned by Dynamic Host Configuration Protocol (DHCP), Point –to Point IP control protocol (PPP), or manual configuration.
Mobile IP Components

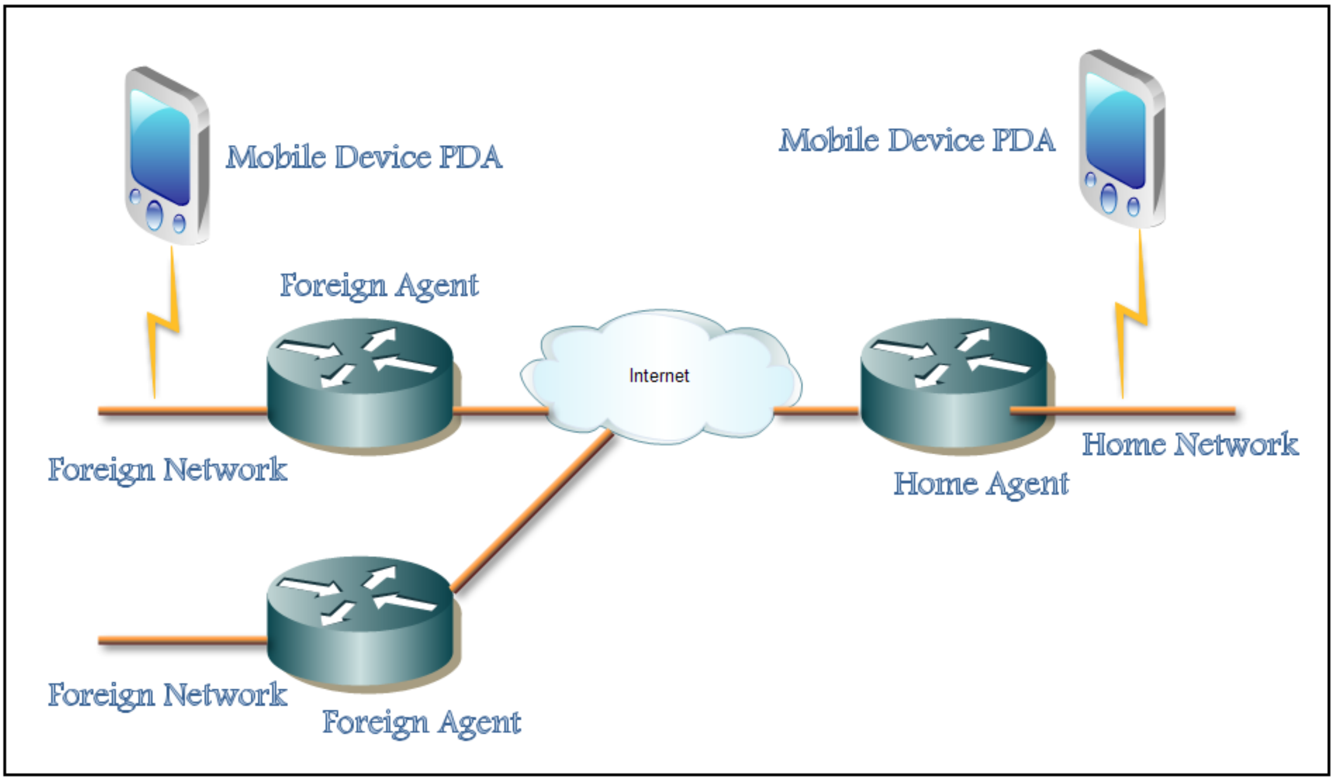


Fig. 1:- IP Tunneling (Generic Routing Encapsulation)

GRE (Generic Routing Encapsulation) or IP tunneling (IP encapsulation) is a technique that encapsulates IP datagrams within IP datagrams. GRE is a technique that allows datagrams to be encapsulated into IP packets and then redirected to an intermediate host. At this intermediate destination, the datagrams are decapsulated and then routed to the next leg. In doing so, the trip to the intermediate host appears to the inner datagrams as one hop. The general outline of GRE can be found in *RFC 1701*.

In the current stack, GRE is performed via GRE pseudo interfaces which simulate point-to-point connections. GRE interfaces are created with the ifconfig utility:

```
# ifconfig gre0 create
```

Each GRE interface supports the following modes of operation:

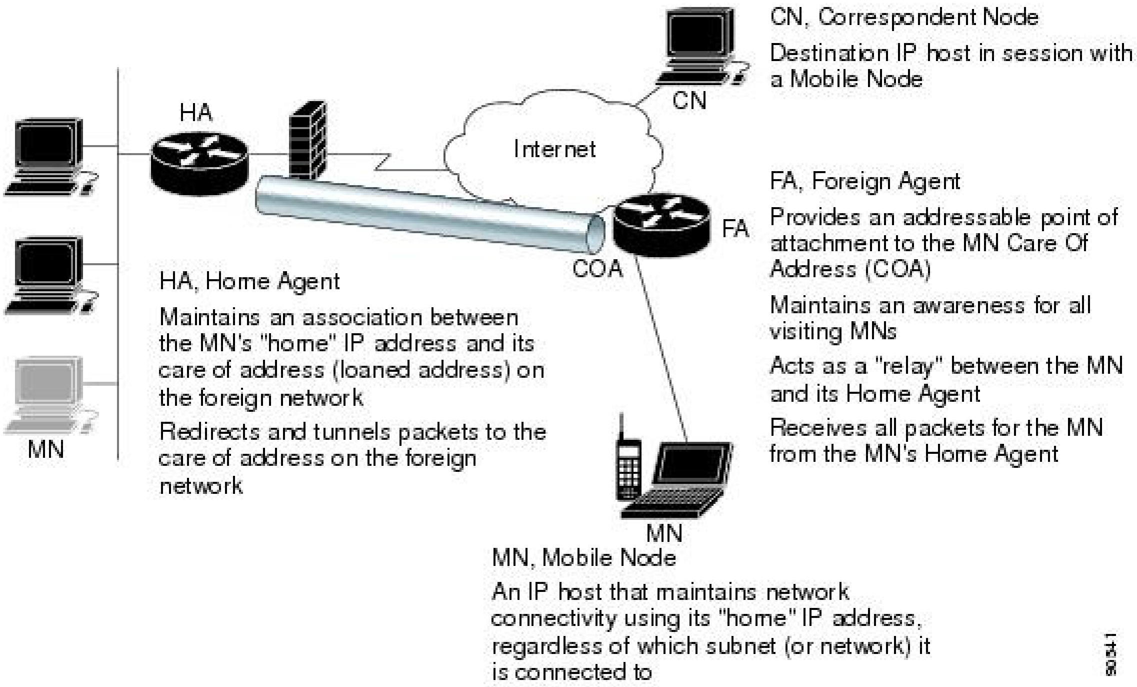
GRE encapsulation (default)

Outgoing datagrams are encapsulated by an IP header of protocol type 47, and a GRE header specifying the type of the encapsulated datagram (currently only IP). This mode is described in *RFC 1702*. It's also the default mode on Cisco routers.

MOBILE encapsulation (IP protocol number 55) Applicable for IP encapsulation only. Otgoing IP datagrams are encapsulated by a smaller header, and the original IP header is modified. This mode is described in *RFC 2004*.

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.

Fig. 2 Architecture of Mobile IP

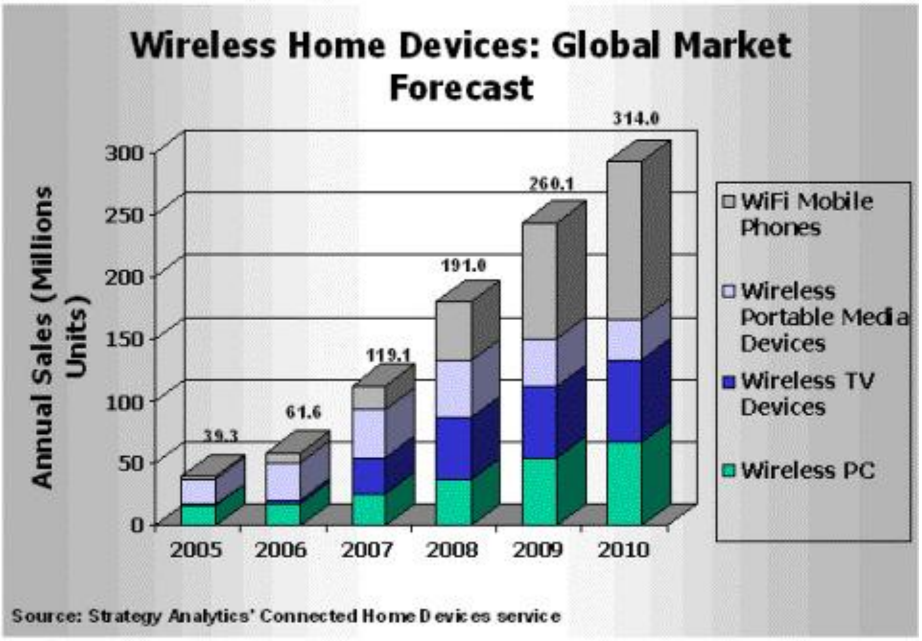

CN, Correspondent Node
Destination IP host in session with a Mobile Node
CN
HA
Internet
FA, Foreign Agent
Provides an addressable point of attachment to the MN Care Of Address (COA)
Maintains an awareness for all visiting MNs
Acts as a "relay" between the MN and its Home Agent
Receives all packets for the MN from the MN's Home Agent
FA
COA
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
MN
MN
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
90341

As shown in the figure 2 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 un-marshalling the tunneled packets and sending it to 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.

IV. 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 as under :-

A. MOBILITY SUPPORT:-Figure 3 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 in turn 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. 3. 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. 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 sub-network, 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. These are:-

1. The node must change its IP address whenever it changes its point of attachment, and
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 permanent IP address.

F. IMPROVED SECURITY :-Security problems are considered when registering to the home agent. 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 pre-shared 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 (HMACMD5).

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.

G. NATURAL SOLUTION:- The natural solution to overcome some of the limitations of the original IP addressing scheme is called Mobile IP. 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 (primary address) is never changed. This address is always used by applications and transport protocols. The address at the foreign network (secondary address) is temporary; it changes as the computer moves and is only valid at the specific foreign network.

V. SECURITY ISSUES WITH MOBILE IP

Security is one of the most challenging tasks in mobile IP network. Mobile IP allows mobile users to change their network attachment frequently without losing their connection, which gives many advantages to users. However, the mobility of communication devices and characteristics of the wireless channel introduce many security issues.

Security issues for Mobile IP are considered when the mobile device registers its care-of address to the home agent, this registration messages requires an authentication. The common security threats that face mobile IP networks as well as the method and suggestion to improve the security performance of mobile IP are discussed as under:-

A. A DENIAL-OF-SERVICE ATTACK:- A Denial-of-service attack (DoS) is raised up once the attackers prevent the authorized users from getting their work done. This kind of attack usually takes the following steps:
1. By sending a large number of requests over the internet. These many requests make the target device to run below the optimum speeds till it become unavailable.
2. The other way is to intercept the communication between two devices on the network directly. For example, attacker can use the techniques of redirection to make the data not reach the authorized user.

In the case of Mobile IP, the denial of service attack happens once the attacker starts to manipulate the registration of a care of address for particular mobile device, figure 4 illustrated Denial of Service’s manipulated registrations. Such a manipulation of registration leads to two issues:

- The Mobile device is no longer connected
- The attacker gets all the traffic directed to the original mobile device.

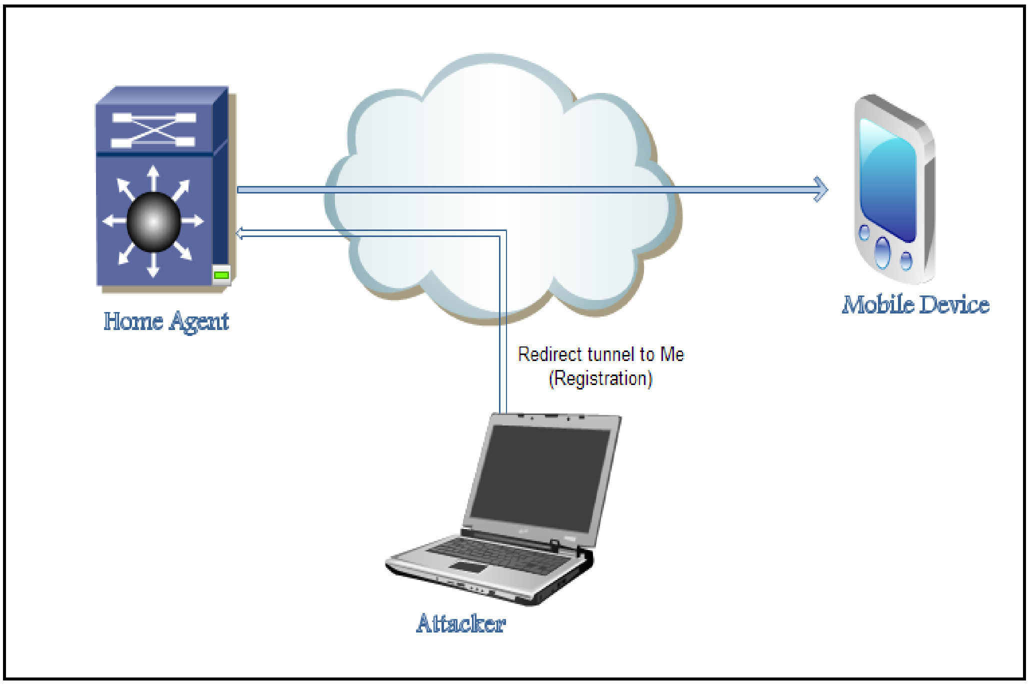


Figure 4:- Denial of Service attack to a Mobile IP network

In this kind of attack, the attacker generally needs to be in the middle between the two corresponding hosts in order to cut off their traffic. With a Mobile IP network, the attacker can attack the network from anywhere, if a mobile device is connected on the foreign network, it is mandatory to use the registration method to inform its home agent of its current care-of address to which home agent will intercept and tunnel all the traffic destined to the mobile device’s home address. So the attacker can generate a manipulated register request message declaring with its own IP address as the care-of address for a mobile device to the home agent. So all traffic transmitted to the Mobile device goes to the attacker instead. In order to protect the Mobile network from this kind of attacks, strong authentications are required in all registration traffic exchange by a mobile device and its home IP agent.

Authentication mechanism insures that that traffic is going to the mobile device that should receive it, not anybody else. Mobile IP allows a mobile device and home agent to use and agree with any authentication algorithms they agreed. However, all implementation of mobile IP supports the default algorithm MD5 which can provide the strong authentication that is needed.

B. PASSIVE EAVESDROPPING:-Passive Eavesdropping is type of a theft of information attack. A passive eavesdropping attack happens when an attacker start to listen to the traffic that is transferred between mobile device and its home agent.

The attacker in passive eavesdropping needs to access to the traffic in order this to happen; this can happen in different ways. An attacker can get access to a network and connect a host to the network. In case of a shared Ethernet, all traffic on the same segment may be a victim of eavesdropping. Sometimes a thief is able to receive packets transmitted by radio signals if he is close enough to the wireless network.

In order to prevent eavesdropping in mobile IP it is required to use encryption method to encrypt all ongoing traffic information. This can be done in several ways. Traffic should be encrypted on the foreign link, so the attacker can't decode and understand the cipher text and eavesdropping can no longer happen on the foreign link. Although, the traffic still might be a victim of eavesdropping on the rest of end to end connection.

The best solution would be to use the end to end encryption method on all traffic, this makes eavesdropping attacks impossible.

C. REPLY ATTACK:-Using Authentication, a mobile device can prevent the denial of service attack as mentioned in previous section. However it cannot protect mobile devices from a reply attack, because the attacker can have a copy of the valid registration request message, buffer it, and then reply it later on by registering a manipulated care-of address for the mobile device.

To prevent this kind of attack, the mobile device has to generate a unique value for identification field of each successful attempt of registration. As such, the stored registration request message by the attacker will be defined as out of date from the respective home agent. Mobile IP defines two ways to set identification field. The first one uses timestamp, where the mobile device uses an estimate date and time of day in the identification field. The second method uses a random number. In this method, the mobile device and home agent declare the value which is entered in the identification field accordingly. A message will be rejected if either device receives a registration message with identification field that not match the expected value and this message will be ignored in the case of the mobile device.

D. SESSION STEALING:-Session Stealing is a type of theft of information attacks the same as passive eavesdropping, but in different steps:

- The attacker waits for the mobile device to authenticate and register with its home agent and starts application sessions.
- The attacker eavesdrops on the mobile device to see if any interesting conversation traffic comes through.
- The attacker then floods the mobile device with malicious packets.
- The attacker steals the session by intercepting the packet that is going to the mobile device then the attacker send their own packets that appear to have come from the mobile device.

The user of the mobile device might not notice that the session has been stolen because there is no sign that something like this has happened. The protection against session stealing is the same as passive eavesdropping by providing end to end encryption with authentication.

E. TUNNEL SPOOFING:-The tunnel to the home network or foreign network may be used to hide malicious packets and get them to pass through the firewall.

As registration method is a key role of Mobile IP, Mobile IP has some basic security solutions. Mobile IP requires authentication for registration methods between the mobile device and the home agent. Moreover, Mobile IP uses identification fields and timestamp to protect registration from any attacks.

VI. SECURITY MODELS

In order to secure the protocol, two approaches can be used.

WEAK SECURITY APPROACH:-Weak levels of security may be used between users in environment such as "campus", since these services are not high added value or not primarily of commercial nature. A protection against manipulated attempts could be:

- Home Agent assures the care-of address of mobile device is correct, because the allowed care-of address relates to a well known IP address.

- The mobile device in the foreign network has to authenticate bindings.
- When a mobile device attaches to the foreign network, it sends a registration request with password to the home agent.

STRONG SECURITY APPROACH :-The weak security approach that was discussed in the previous section is not suitable any more. Both now have to agree on a stronger level of security policy where mobile IP authenticates any binding message or authenticates information received about a mobile device. Trusted servers and private and public keys are used, but they slow down the operation.

SECURITY IMPROVEMENTS OF MOBILE IP

USING TUNNELING INSTEAD OF SOURCE ROUTING:-The main purpose of using tunneling techniques instead of source routing is that tunneling relates to fewer security threats. Attacker can use a manipulated care-of address as a destination in a loose source route. This will make the correspondent node reverse the source route and send the message to the manipulated care of address. So the mobile device is disconnected from communicating with his correspondent node. This issue can be solved by proper use of authentication.

AVOIDING 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 device's 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. However the main issue with route optimization is security. A network administrator configures a secret key to authenticate between the mobile device and its correspondent node, but with a large numbers of mobile devices, it is not practical to configure keys between a mobile device and every other correspondent node. In the case of triangle routing, it's conceivable to configure a key between mobile device and its home agent.

USING FIREWALL:A firewall is used to prevent unwanted access to network services. The firewall monitors the traffic going through the network and decides on the basis of defined rules whether certain packets are allowed through or not. In this way it tries to prevent unauthorized access. Typically, a firewall can't prevent the exploitation of vulnerability in the network service if the communication partner can access it. There are several kinds of firewall, mainly in the following three categories:

PACKET FILTERING: It is the oldest network filtering device, introduced on routers. The simple filtering data packet uses the network addresses as basic function of the firewall. It looks at each packet independently and compares it to a list of preconfigured rules. The issue with packet filtering is that it is hard to configure correctly and they cannot keep private IP address invisible to public IP addresses.

- **STATE-FULL INSPECTION:** This state-full filtering is an advanced form of packet filtering. It has two main improvements over packet filtering, session table to track all connections and recognition of dynamic application. This make state-full inspection better in protect the internal network from unwanted external access.
- **PROXY FILTER:** A proxy firewall is a firewall which is based dedicated proxy and circuit level proxy recourse as filter modules. These filter modules implement rules by deciding what data is transferred to the actual communication party. In this way it tries to proxy firewall its own network (segment) to protect against unauthorized access, but can also make a conversion of the data cache of certain content, and exercise all other functions that are particular to a proxy.

In summary, we can say that firewalls provide good security and flexibility for mobile IP by using the firewall categories described above.

IMPLEMENTING IPSEC AS A SOLUTION TO SECURITY ISSUES IN MOBILE IP:-IPSec (Internet Security protocol) is defined by IETF as a framework of open standards for ensuring private communications over IP networks protected by the use of cryptographic security services.

MOBILE IPV6 SECURITY THREATS:-Mobile IPv6 has been developed to provide mobility and security for IPv6 with the same features as MIPv4. MIPv6 introduces different security threats as following:-

1. Threats against binding updates sent to home agents: an attacker might advise that a certain mobile device is currently at a different location than it really is. Then the home agent accepts the information sent to it as is. The mobile device may not get the message directed to it, and other nodes might get messages they did not want.
2. Threats against route optimization with corresponding nodes.
3. Threats where MIPv6 correspondent node functionality is used to launch reflection attacks against other parties. The response traffic against a node, whose IP address appears in the option, will be directed using the home address option without giving a possibility for ingress filtering to catch the forged.
4. Threats where the tunnels between the mobile device and the home agent are attacked to make it appear that the mobile node is sending traffic when it is not.
5. Threats where IPv6 Routing Header which is employed in MIPv6 is used to circumvent IP-address based rules in firewalls or to reflect traffic from other nodes. The generality of the Routing Header allows the kind of usage that opens vulnerabilities, even if the usage that MIPv6 needs is safe.
6. The security mechanisms of MIPv6 may also be attacked them, e.g. in order to force the participants to execute expensive cryptographic operations or allocate memory for the purpose of keeping state.

SECURING THE BINDING UPDATE:-MIPv6 is a host routing protocol, developed to modify the normal routing for a specific host, as it changes the way of sending packets to the host. The binding update tells a correspondent node of the new care-of address, a correspondent node authenticate the binding update and verifies that it does not come from the manipulated node . In order to successfully authenticate the update the mobile device and the correspondent node need to establish security association and share a secret key.

IPSec in transport mode is used between home agent and its mobile device in order to secure the MIPv6 message such as binding update.

VII. CONCLUSION AND SUGGESTIONS TO FUTURE WORK

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. In this paper we firstly described wireless network security threats and security technology, we also investigated mobile security threats and different security solutions that can be applied to Mobile IP with emphasis on IPSec to provide the security solution for Mobile IP. Mobility feature and IPSec were not built on IPv4 protocol; they were designed as an extension to IPv4 standard. Mobile IP was an extension of the IPv4 standard under the name “Mobile IPv4” to support mobility.

IPSec manages connections and can guarantee both encryption and data integrity through protocols of Authentication Header (AH), Encapsulated Security Payload (ESP) and Internet Key Exchange (IKE). The powerful way to secure mobile IP is by combining it with IPSec protocol; even though there are some limitations such as, IPSec does not stop traffic analysis and it use strong authentication for machines, not users. These limitations can be studied in future work.

IPSec is not the only protocol that deal with securing mobile IP, there are several security protocols such as AAA protocol (Authentication, Authorization and Accounting) and Public Key Infrastructure protocol that provide strong management. With a combination of these protocols with IPSec, we get more security and protection for mobile IP.

IPv6 was developed because the number of possible address entries in IPv4 is limited. In mobile IPv6, IPSec is a mandatory feature that is required to provide data security and services for communication in IPv6 network. The main difference between Mobile IPv4 and Mobile IPv6 is that Mobile IPv6 is not an add-on feature of IPv6, it is built into the base of IPv6 which makes it more efficient and easier to implement. Mobile IPv6 introduces different security threats that continue to get attention and should be studied in future work.

VIII. SUMMARY

Mobile IP is used to maintain communications while the IP address is changing. Mobile IPv6 is much more optimized and deployable than Mobile IPv4, such as direct communication between the correspondent node and mobile device, even though Mobile IPv6 is still incomplete; the issues have been with the security of the protocol.

REFERENCES

1. A survey on mobile ip.
2. A. Diab and A. Mitschele-Thiel. Minimizing mobile ip handoff latency.
3. Applicability statement for ip mobility support. http://www.rfc-editor.org/rfc/rfc2005.txt.
4. Charles Perkins, Andrew Myles, *Mobile IP*, SBT/IEEE International Telecommunications Symposium , Rio De Janeiro, Brazil, 22-25 August 1994.
5. Charles Perkins, The Internet Mobile Host Protocol (IMHP),Internet Draft, 6 July 1995. This draft specifies protocol enhancements that allow transparent routing of IP datagrams to mobile nodes in the Internet.
6. Charles Perkins, IP Encapsulation within IP,Internet Draft, 6 July 1995.
   This draft specifies a way by which an IP datagram may be encapsulated within an IP datagram.
7. Charles Perkins, Minimal Encapsulation within IP Internet Draft, 6 July 1995.
8. C. So-In, Mobile IP Survey, 2006
9. C. Perkins, "Mobile Networking through Mobile IP", online tutorial, October 2002.
10. Christian Huitema, *ROUTING IN THE INTERNET*, Prentice Hall, 1995, 315 pp.
11. ios ip configurationguide, release12.2 – configuring mobile ip [cisco ios software releases 12.2 mainline] – cisco systems. http://tinyurl.com/5mpj6w.
12. C. Perkins. Mobile networking through mobile ip. *Internet Computing, IEEE*, 2(1):58–69, 1998.
13. David Johnson and Charles Perkins, Route Optimisation in Mobile IP,Internet Draft, 6 July 1995.This draft specifies extensions to the operations of the base Mobile IP protocol to allow for optimal routing of datagrams from a correspondent node to a mobile node.
14. Fred Simonds, "Network security: data and voice communications" New York, McGraw-Hill, 1996
15. G. Montenegro and V. Gupta, "Sun's SKIP firewall traversal for Mobile IP," RFC 2356, June 1998.
16. Habib, A., Hafeeda, M.H, and Bhargava, B.,"Detecting Service Violation and DoS Attacks", In Proc. of Network and Distributed System Security Symposium (NDSS), 2003.
17. H. Hansen, "IPSec and Mobile IP in Mobile Ad Hoc Networking ", Helsinki University of Technology, April 2000.
18. Introduction to mobile ip. http://www.hpl.hp.com/personal/Jean Tourrilhes/MobileIP/ppal.html.
19. Introduction to mobile ip [ip tunneling] - cisco systems. http://tinyurl.com/5z9xpk.
20. 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*.
21. Jim Binkley, John Richardson: Security Considerations for Mobility and Firewalls, Internet Draft, November 1998.
22. Jian Hui Wang. "Security in Mobile IP" Concordia University, Canada.
23. John K. Zao, Matt Condell: Use of IPSec in Mobile IP, Internet Draft, November
24. John *K. Zao,* Matt Condell *"Use of IPSec in Mobile IP", November 1997*.
25. Johnson, D., Perkins, C. Mobility Support in IPv6. Internet Engineering Task Force, draftietf- mobileip-ipv6-16, March 2002. 152 pages
26. Jim Binkley, John Richardson: Security Considerations for Mobility and Firewalls, Internet Draft, November 1998
27. Jon Postel, Internet Protocol, RFC 791,September 1981.
28. Matthias Hollick, "The Evolution of Mobile IP Towards Security", German National Research Center for Information Technology Institute IPSI, 2000.
29. Mobile ip - wikipedia, the free encyclopedia.
30. Rfc 3344 - ip mobility support for ipv4.http://tools.ietf.org/html/rfc3344.
31. Rfc 4721 - mobile ipv4 challenge/response extensions (revised). http://tools.ietf.org/html/rfc4721.
32. Rfc ip mobility support. http://www.ietf.org/rfc/rfc2002.txt.
33. S. Sharma, N. Zhu, and T. cker Chiueh. Low-latency mobile ip hando for infrastructure-mode wireless lans.
34. Security Aspects of Mobile IP. SANS Institute 2001, as part of the Information Security Reading Room.
35. S. Kent, Atkinson, "*Security Architecture for the Internet Protocol*", RFC 2401, November 1998. [36] "The TCP IP Guide" Version 3.0, September 20 2005.
36. 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.
37. Terry Escamilla, "Intrusion Detection: Network Security beyond the firewall ", New York, John Wiley, 1998.
38. T. Braun and M. Danzeisen, "Secure Mobile IP Communication", on Proceedings of the 26th Annual IEEE Conference on Local Computer Networks, IEEE Computer Society, November 14-16, pp.586, 2001
39. V. Gupta, G. Montenegro, Secure and mobile Networking, Mobile Networks and Applications 3 (381-390), Baltzer Science Publisher BV, 1998.
40. V. Gupta, G. Montenegro, Secure and mobile Networking, Mobile Networks and Applications 3 (381-390), BaltzerScience Publisher BV, 1998.
41. William Stalling, "Wireless Communication and Networking", Pearson Education Asia, 2002