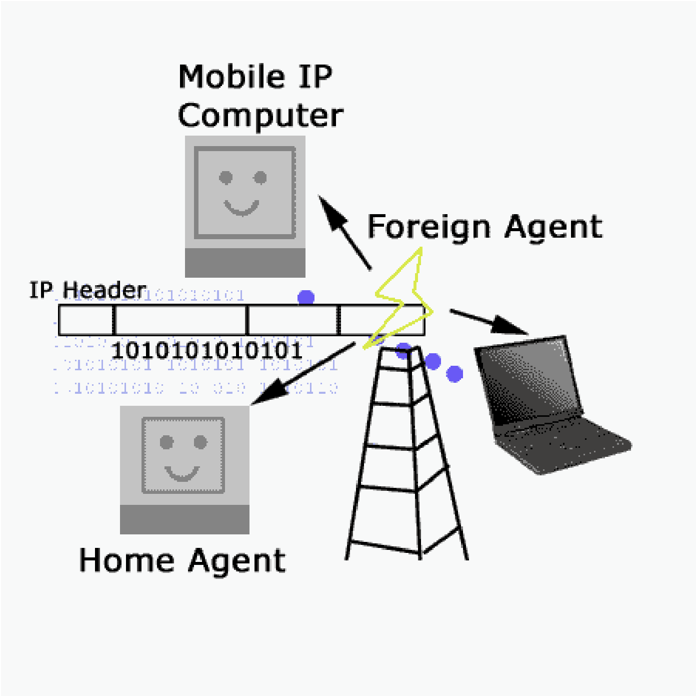
Mobile IP

by Debalina Ghosh



Introduction

Mobile Computing is becoming increasingly important due to the rise in the number of portable computers and the desire to have continuous network connectivity to the Internet irrespective of the physical location of the node. The Internet infrastructure is built on top of a collection of protocols, called the TCP/IP protocol suite. Transmission Control Protocol (TCP) and Internet Protocol (IP) are the core protocols in this suite. IP requires the location of any host connected to the Internet to be uniquely identified by an assigned IP address. This raises one of the most important issues in mobility, because when a host moves to another physical location, it has to change its IP address. However, the higher level protocols require IP address of a host to be fixed for identifying connections. The **Mobile Internet Protocol** (Mobile IP) is an extension to the Internet Protocol proposed by the Internet Engineering Task Force (IETF) that addresses this issue. It enables mobile computers to stay connected to the Internet regardless of their location and without changing their IP address. More precisely, Mobile IP is a standard protocol that builds on the Internet Protocol by making mobility transparent to applications and higher level protocols like TCP [6]. This article provides an introduction to Mobile IP and discusses its advantages and disadvantages.

The TCP/IP Protocol Suite

TCP/IP protocol suite, the cornerstone of Internet networking, is a four-layer system. Each layer is responsible for a specific task [18]. The four layers, from top to bottom, are application layer, transport layer, network layer, and link layer. The **application layer** handles the details of the particular application (e.g., FTP, TELNET, HTTP etc.). The **transport layer** provides a flow of data between two Internet nodes. There are two widely used transport layer protocols on the Internet: TCP (Transmission Control Protocol) [15] and UDP (User Datagram Protocol)[13]. TCP provides a reliable flow of data between two nodes by maintaining a connection-oriented environment. On the other hand, UDP provides an unreliable and connectionless datagram service. The **network layer** handles the movement of packets around the network by implementing efficient routing algorithms. IP (Internet Protocol) [14], the default network layer protocol on the Internet, is described in detail in the next section. The **link layer** provides interfaces to the network hardware devices in the form of device drivers. Examples include IEEE 802.2 (LANs), X.25, packet radio etc. The physical layer, which is often tightly-coupled with the datalink, is responsible for transmitting raw bits across the network through network interface cards and cables.

The overall protocol stack is also a tightly-coupled system. Each layer provides some services that the upper layers use. Thus, support for mobility is likely to affect all the layers. For example, the link layer needs to make provisions to accomodate the distinguishing characteristics of wireless media like low bandwidth and difference in power levels of end-to-end nodes. The network layer that routes data to a destination host based on its location, needs to be modified so that it can handle routing when the physical location of the host changes. Similarly, at the transport layer, it is neccessary to provide a better end-to-end delivery service, especially in the case of dropped packets; packets may be lost during mobility and need to be delivered immediately to the new location. Finally, the application layer requires additional support in terms of automatic configuration, service discovery, and link awareness [7]. As an example of an application layer change, if an FTP session is in progress during mobility, the FTP application needs to configure itself being aware of the location changes.

Mobile IP extends IP to support mobile computing. The next section gives an overview of IP, as a preamble to Mobile IP.

Brief Overview of IPv4

At the network layer, the Internet is viewed as a set of networks or autonomous systems connected together in a hierarchical manner. IP is the mechanism that connects these networks together. Its basic function is to deliver data from a source to a destination independent of the physical location of the two.

IP identifies each node uniquely, using an IP address that designates its physical attachment to the Internet. IP addresses are 32-bit long integers and are represented in a dotted decimal format (e.g., 128.55.44.1), for ease of use. Every IP packet consists of an IP header and an IP payload. The header contains the IP addresses of the sending node and the receiving node along with some other information.

To correctly deliver these packets, IP executes two major steps: packet routing and packet forwarding. Packet routing involves use of protocols like BGP, RIP, and OSPF to decide the route that each packet has to travel. The route is decided using a routing table of < destination address, next hop > pairs at each router. Destination addresses are paired with a pair contained in the routing table. Packet forwarding involves use of protocols like ARP, proxy ARP etc. to deliver the packet to the end node once it has arrived at the destination network. This is typically done by discovering the hardware address of the host corresponding to its IP address.

Motivation for the Mobile IP design

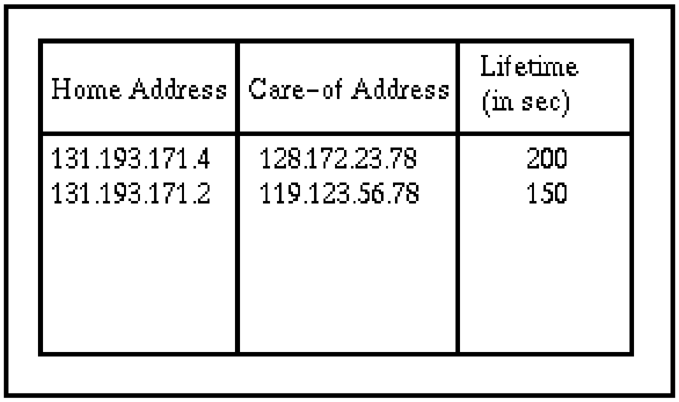
The IP address of a host consists of two parts [9]: 1) The higher order bits of the address determine the network on which the host resides; 2) The remaining low-order bits determine the host number.

IP decides the next-hop by determining the network information from the destination IP address of the packet. On the other hand, higher level layers like TCP maintain information about connections that are indexed by a quadruplet containing the IP addresses of both the endpoints and the port numbers. Thus, while trying to support mobility on the Internet under the existing protocol suite, we are faced with two mutually conflicting requirements: (1) a mobile node has to change its IP address whenever it changes its point of attachment, so that packets destined to the node are routed correctly, (2) to maintain existing TCP connections, the mobile node has to keep its IP address the same. Changing the IP address will cause the connection to be disrupted and lost.

Mobile IP, the standard proposed by IETF, is designed to solve the problem by allowing each mobile node to have two IP addresses and by transparently maintaining the binding between the two addresses [12]. One of the IP addresses is the permanent home address that is assigned at the home network and is used to identify communication endpoints. The other is a temporary care-of address that represents the current location of the host. The main goals of Mobile IP are to make mobility transparent to the higher level protocols and to make minimum changes to the existing Internet infrastructure.

Overview of the Protocol

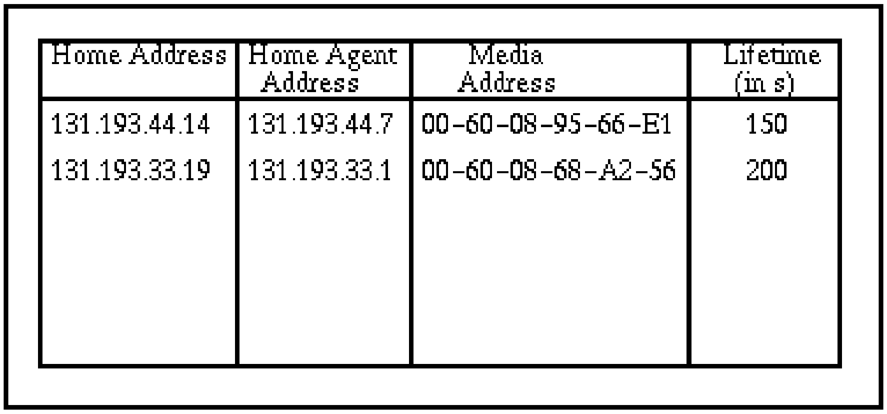
As discussed in the last section, Mobile IP supports mobility by transparently binding the home address of the mobile node with its care-of address. This mobility binding is maintained by some specialized routers known as mobility agents. Mobility agents are of two types - home agents and foreign agents. The home agent, a designated router in the home network of the mobile node, maintains the mobility binding in a **mobility binding table** where each entry is identified by the tuple <permanent home address, temporary care-of address, association lifetime>. Figure 1 shows a mobility binding table. The purpose of this table is to map a mobile node's home address with its care-of address and forward packets accordingly.



Home Address	Care-of Address	Lifetime (in sec)
131.193.171.4	128.172.23.78	200
131.193.171.2	119.123.56.78	150

Figure 1: Mobility Binding Table

Foreign agents are specialized routers on the foreign network where the mobile node is currently visiting. The foreign agent maintains a **visitor list** which contains information about the mobile nodes currently visiting that network. Each entry in the visitor list is identified by the tuple: < permanent home address, home agent address, media address of the mobile node, association lifetime>. Figure 2 shows an instance of a visitor list.



Home Address	Home Agent Address	Media Address	Lifetime (in s)
131.193.44.14	131.193.44.7	00-60-08-95-66-E1	150
131.193.33.19	131.193.33.1	00-60-08-68-A2-56	200

Figure 2: Visitor List

In a typical scenario, the care-of address of a mobile node is the foreign agent's IP address. There can be another kind of care-of address, known as colocated care-of address, which is usually obtained by some external address assignment mechanism.

The basic Mobile IP protocol has four distinct stages [2]. These are:

1. **Agent Discovery:** Agent Discovery consists of the following steps:
    1. Mobility agents advertise their presence by periodically broadcasting Agent Advertisement messages. An Agent Advertisement message lists one or more care-of addresses and a flag indicating whether it is a

home agent or a foreign agent.

   2. The mobile node receiving the Agent Advertisement message observes whether the message is from its own home agent and determines whether it is on the home network or a foreign network.

   3. If a mobile node does not wish to wait for the periodic advertisement, it can send out Agent Solicitation messages that will be responded by a mobility agent.

2. **Registration:** Registration consists of the following steps:
   1. If a mobile node discovers that it is on the home network, it operates without any mobility services.

   2. If the mobile node is on a new network, it registers with the foreign agent by sending a Registration Request message which includes the permanent IP address of the mobile host and the IP address of its home agent.

   3. The foreign agent in turn performs the registration process on behalf of the mobile host by sending a Registration Request containing the permanent IP address of the mobile node and the IP address of the foreign agent to the home agent.

   4. When the home agent receives the Registration Request, it updates the mobility binding by associating the care-of address of the mobile node with its home address.

   5. The home agent then sends an acknowledgement to the foreign agent.

   6. The foreign agent in turn updates its visitor list by inserting the entry for the mobile node and relays the reply to the mobile node.

Figure 3 illustrates the registration process.

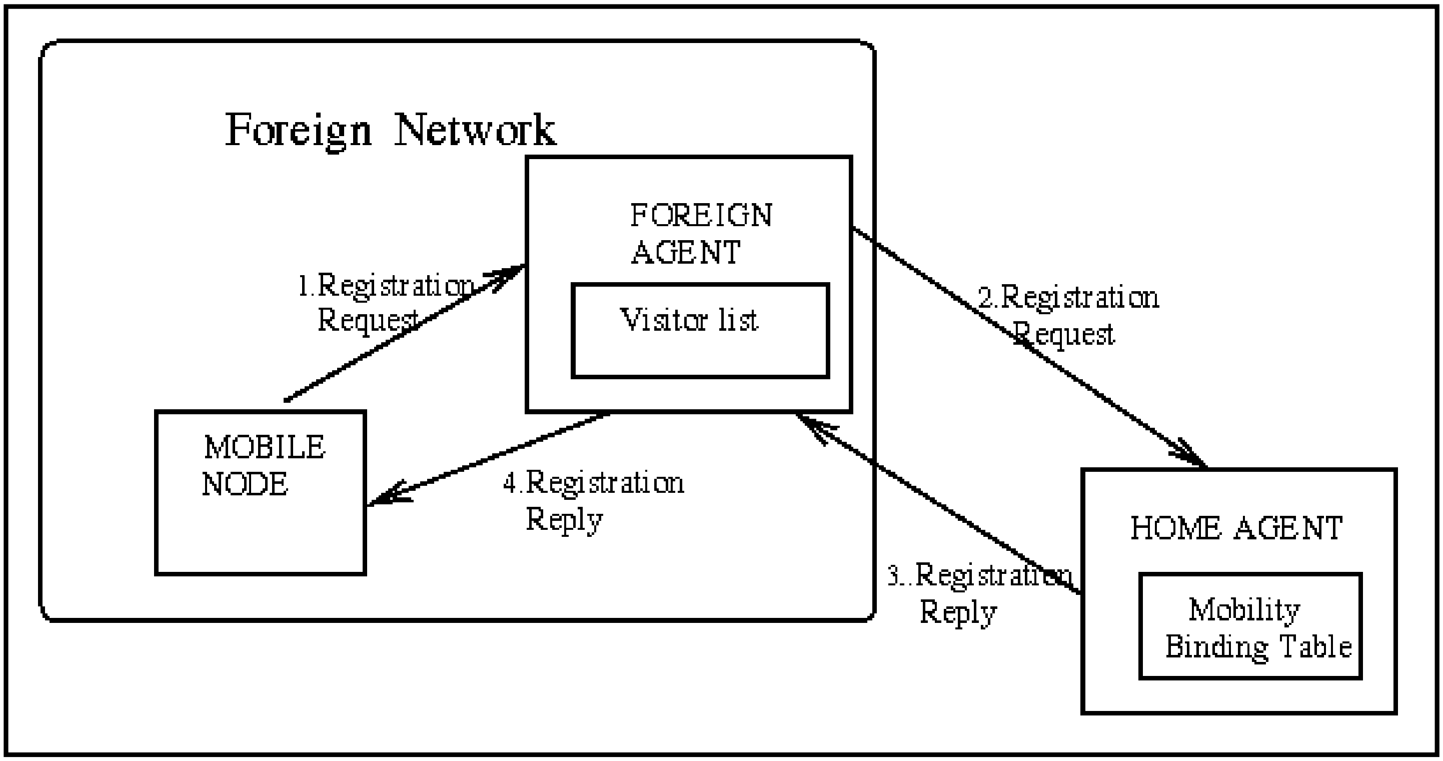


Figure 3: Registration process in Mobile IP

3. **In Service:** This stage can be subdivided into the following steps:

    1. When a correspondent node wants to communicate with the mobile node, it sends an IP packet addressed to the permanent IP address of the mobile node.

    2. The home agent intercepts this packet and consults the mobility binding table to find out if the mobile node is currently visiting any other network.

    3. The home agent finds out the mobile node's care-of address and constructs a new IP header that contains the mobile node's care-of address as the destination IP address. The original IP packet is put into the payload of this IP packet. It then sends the packet. This process of encapsulating one IP packet into the payload of another is known as **IP-within-IP** encapsulation [11], or **tunneling**.

    4. When the encapsulated packet reaches the mobile node's current network, the foreign agent decapsulates the packet and finds out the mobile node's home address. It then consults the visitor list to see if it has an entry for that mobile node.

    5. If there is an entry for the mobile node on the visitor list, the foreign agent retrieves the corresponding media address and relays it to the mobile node.

    6. When the mobile node wants to send a message to a correspondent node, it forwards the packet to the foreign agent, which in turn relays the packet to the correspondent node using normal IP routing.

    7. The foreign agent continues serving the mobile node until the granted lifetime expires. If the mobile node wants to continue the service, it has to reissue the Registration Request.

    Figure 4 illustrates the tunneling operation.

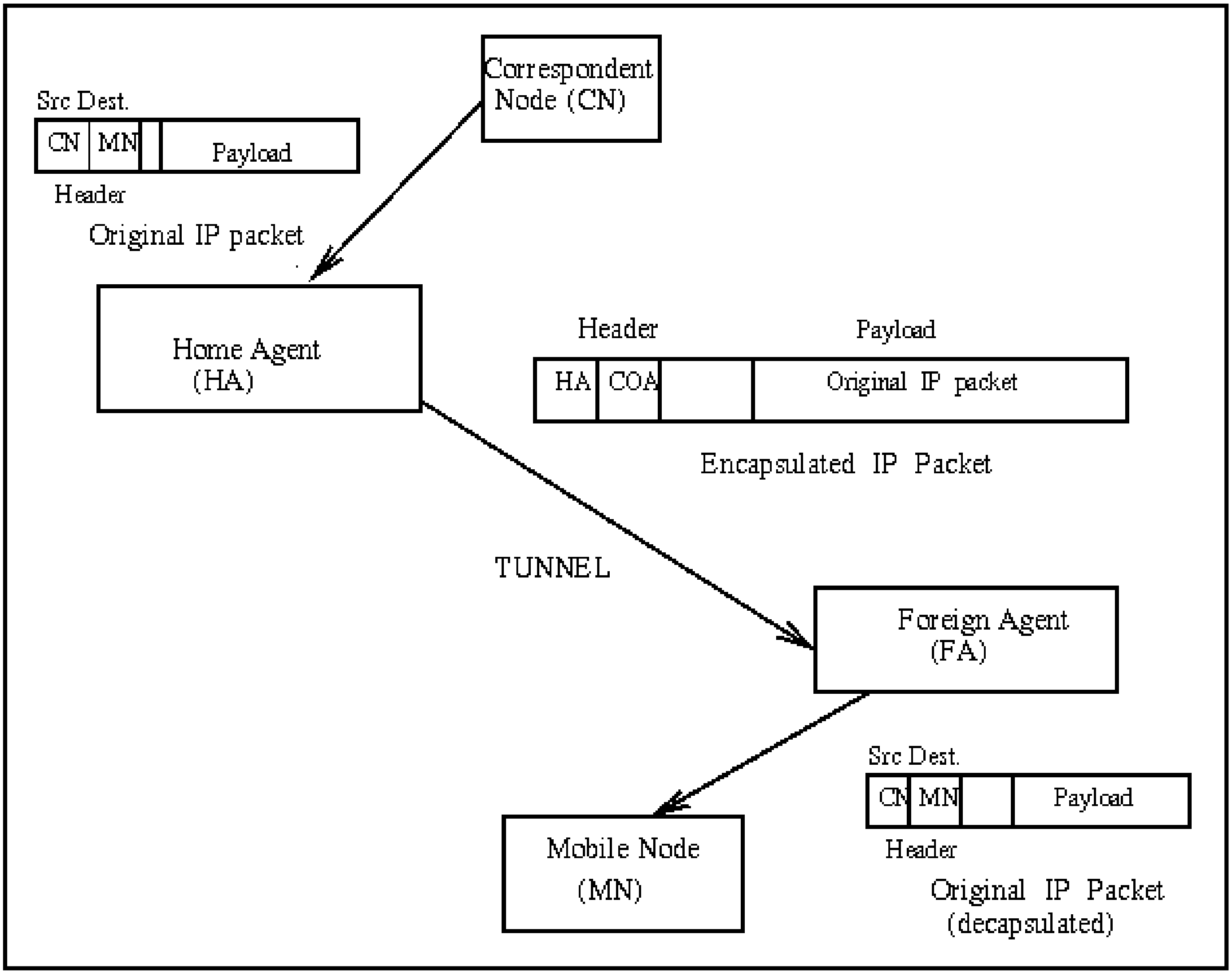


Figure 4: Tunneling operation in Mobile IP

4. **Deregistration:** If a mobile node wants to drop its care-of address, it has to deregister with its home agent. It achieves this by sending a Registration Request with the lifetime set to zero. There is no need for deregistering with the foreign agent as registration automatically expires when lifetime becomes zero. However if the mobile node visits a new network, the old foreign network does not know the new care-of address of the mobile node. Thus datagrams already forwarded by the home agent to the old foreign agent of the mobile node are lost.

Security Considerations

Security is very important in Mobile IP as mobile nodes are often connected to the Internet via wireless links which are very vulnerable to security attacks. For example, during registration procedure the home agent should be convinced that it is getting authentic Registration Request from a mobile node and not receiving information from a bogus node. Mobile IP solves this problem by specifying a security association between the home agent and the mobile node. This security association is at present manually configured. Every registration message should contain a mobile node-home agent aunthentication extension which contain an Security Parameters Index(SPI) followed by an authenticator [5]. The SPI is an index into the mobility security association and it defines the security context (i.e., the algorithm and the secret) used to compute and check the authenticator. The default algorithm is keyed MD5 [16] with a key size of 128 bits. Also each registration contains unique data to avoid valid registration recording by malicious nodes. Two methods are used to generate the unique data:

- *timestamps* - The node generating the message inserts the time-of-day, and the node receiving the message checks whether it is sufficiently close to its time-of-day.
- *nonces* - Node A generates a new random number in every message to node B, and checks whether node B returns the same number in its next message to node A. Both messages use an authentication code to protect against alteration by an outsider. Node B can also generate random numbers and use them in its messages.

Route Optimization

In the basic Mobile IP protocol, IP packets destined to a mobile node that is outside its home network are routed through the home agent. However packets from the mobile node to the correspondent nodes are routed directly. This is known as **triangle routing**. Figure 5 illustrates triangle routing.

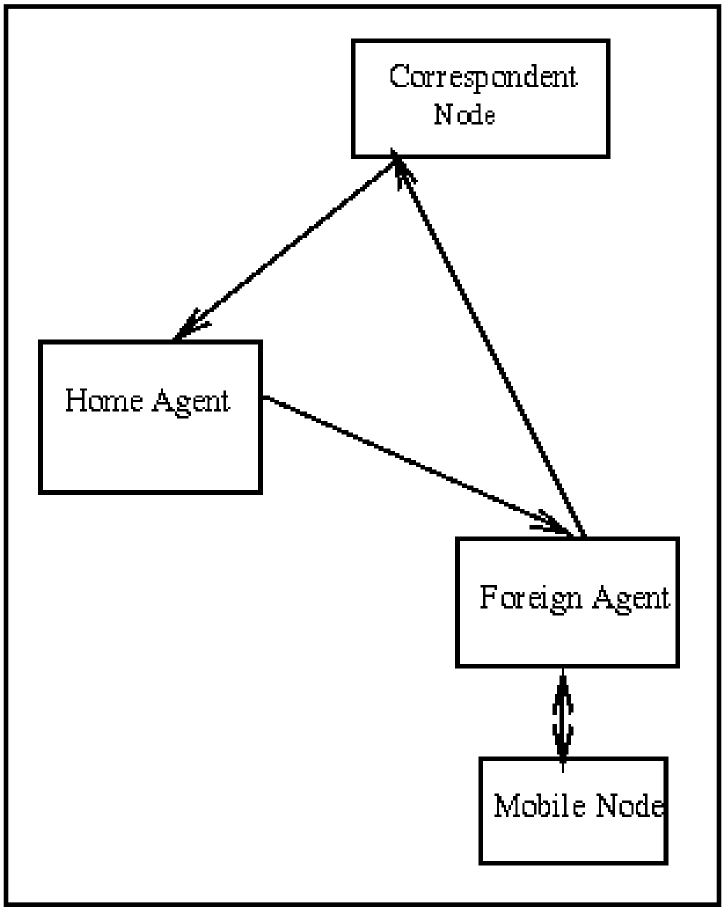


Figure 5: Triangle Routing

This method may be inefficient in many cases. Consider the case when the correspondent host and the mobile host are in the same network, but not in the home network of the mobile host. In this case the messages will experience unnecessary delay since they have to be first routed to the home agent that resides in the home network. One way to improve this is *Route Optimization*.

Route Optimization is an extension proposed to the basic Mobile IP protocol [4]. Here messages from the correspondent node are routed directly to the mobile node's care-of address without having to go through the home agent. Route Optimization provides four main operations. These are:

1. Updating binding caches,

2. Managing smooth handoffs between foreign agents,
3. Acquiring registration keys for smooth handoffs,
4. Using special tunnels.

1. Updating binding caches: Binding caches are maintained by correspondent nodes for associating the home address of a mobile node with its care-of address. A binding cache entry also has an associated lifetime after which the entry has to be deleted from the cache. If the correspondent node has no binding cache entry for a mobile node, it sends the message addressed to the mobile node's home address. When the home agent intercepts this message, it encapsulates it and sends it to the mobile node's care-of address. It then sends a Binding Update message to the correspondent node informing it of the current mobility binding.

2. Managing smooth handoffs between foreign agents: When a mobile node registers with a new foreign agent, the basic Mobile IP does not specify a method to inform the previous foreign agent. Thus the datagrams in flight which had already tunneled to the old care-of address of the mobile node are lost. This problem is solved in Route Optimization by introducing smooth handoffs. Smooth handoff provides a way to notify the previous foreign agent of the mobile node's new mobility binding.

If a foreign agent supports smooth handoffs, it indicates this in its Agent Advertisement message. When the mobile node moves to a new location, it requests the new foreign agent to inform its previous foreign agent about the new location as part of the registration procedure. The new foreign agent then constructs a Binding Update message and sends it to the previous foreign agent of the mobile node. Thus if the previous foreign agent receives packets from a correspondent node having an out-of-date binding, it forwards the packet to the mobile node's care-of address. It then sends a Binding Warning message to the mobile node's home agent. The home agent in turn sends a Binding Update message to the correspondent node. This notification also allows datagrams sent by correspondent nodes having out-of-date binding cache entries to be forwarded to the current care-of address. Finally this notification allows any resources consumed by the mobile node at the previous foreign agent to be released immediately, instead of waiting for the registration lifetime to expire.

3. Acquiring registration keys for smooth handoffs: For managing smooth handoffs, mobile nodes need to communicate with the previous foreign agent. This communication needs to be done securely as any careful foreign agent should require assurance that it is getting authentic handoff information and not arranging to forward in-flight datagrams to a bogus destination. For this purpose a registration key is established between a foreign agent and a mobile node during the registration process. The following methods for establishing registration keys have been proposed in the order of declining preference:

- If the home agent and the foreign agent share a security association, the home agent can choose the registration key.
- If the foreign agent has a public key, it can again use the home agent to supply the registration key.
- If the mobile node includes its public key in its Registration Request, the foreign agent can choose the new registration key.
- The mobile node and its foreign agent can execute the Diffie-Hellman key exchange protocol as part of the registration protocol.

This registration key is used to form a security association between the mobile node and the foreign agent.

4. Using special tunnels: When a foreign agent receives a tunneled datagram for which it has no visitor list entry, it concludes that the node sending the tunneled datagram has an out-of-date binding cache entry for the mobile node. If the foreign agent has a binding cache entry for the mobile node, it should re-tunnel the datagram to the care-of address indicated in its binding cache entry. On the other hand, when a foreign agent receives a datagram for a mobile node for which it has no visitor list or binding cache entry, it constructs a special tunnel datagram [8]. The special tunnel datagram is constructed by encapsulating the datagram and making the outer destination address equal to the inner destination address. This allows the home agent to see the address of the node that tunneled the datagram and prevent sending it to the same node. This avoids a possible routing loop that might have occured if the foreign agent crashed and lost its state information.

Minimal Encapsulation Scheme

Encapsulation in Mobile IP is carried out by putting the original datagram (=IP header+payload) inside another IP envelope. The fields in the outer IP header add too much overhead to the final datagram - several fields are duplicated from the inner IP header. To prevent this waste of space a Minimal Encapsulation Scheme [10] has been defined where instead of inserting a new header, the original header is modified to reflect the care-of address and a minimal forwarding header is inserted to store the original source and destination address. Thus the care-of address of the mobile node becomes the destination address of the IP packet and the home agent's address becomes the source address. The minimal forwarding header stores the original source and destination addresses. When the foreign agent tries to decapsulate, it simply restores the fields in the forwarding header to the IP header and removes the forwarding header. Figure 6 illustrates the Minimal Encapsulation scheme.

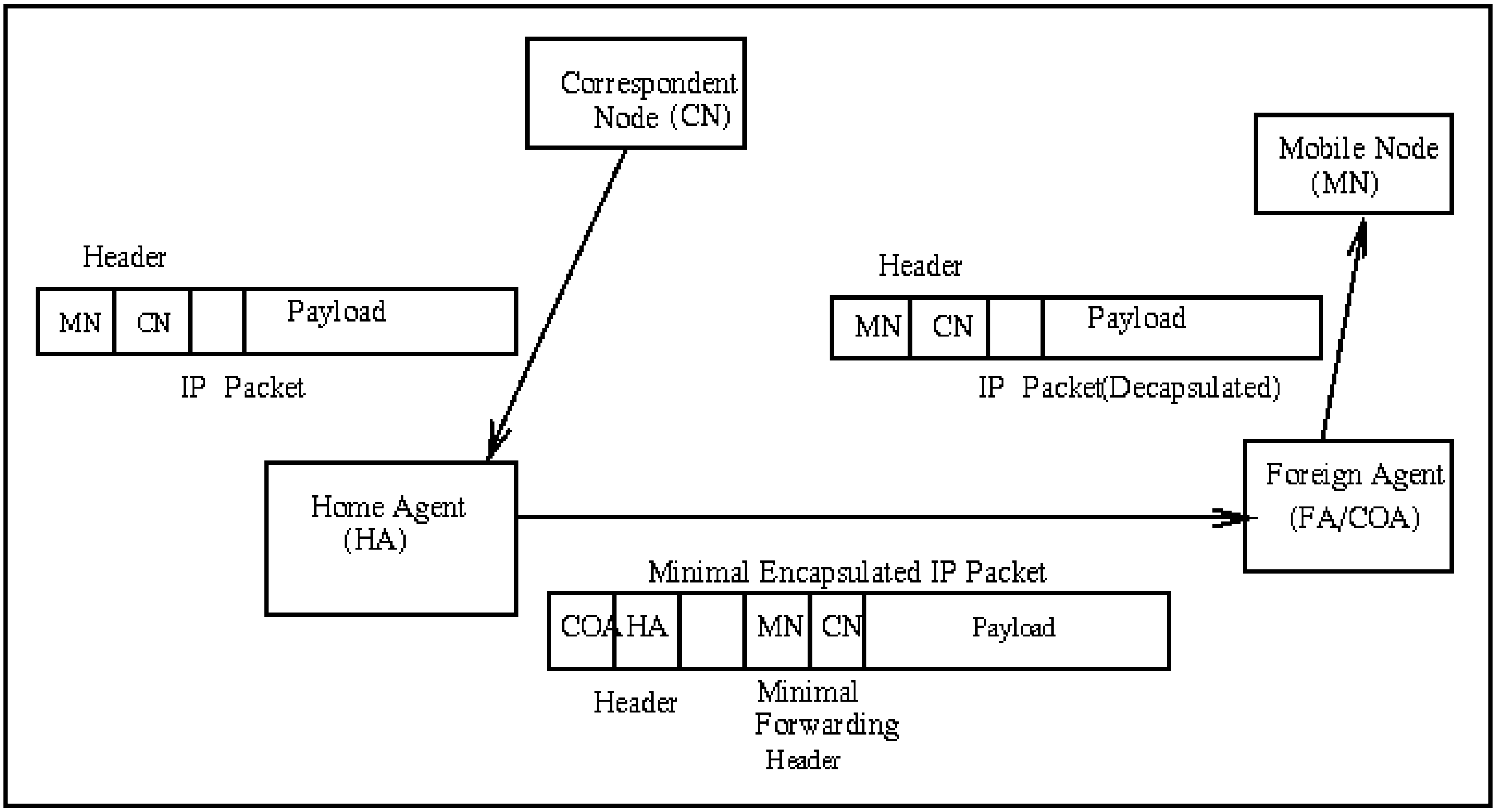


Figure 6: Minimal Encapsulation

Mobile IPv6

The next version of IP, IPv6 is designed to be an evolutionary step from IPv4. IPv6 addresses are 128 bits long. Mobility support in IPv6 solves many of the problems of basic Mobile IP [3]. Some advantages of Mobile IPv6 over Mobile IPv4 are:

- Route Optimization is built as a fundamental part of Mobile IPv6 unlike Mobile IPv4 where it is an optional set of extensions that may not be supported by all nodes.
- Foreign Agents are not needed in Mobile IPv6. The enhanced features of IPv6 like Neighbour Discovery and Address Autoconfiguration enable mobile nodes to function in any location without the services of any special router in that location.
- In Mobile IPv4, when a mobile node communicates with a correspondent node, it puts its home address as the source address of the packet. Thus " ingress filtering routers " used to filter out the packets as the source address of the packet is different from the network from which the packet originated. This problem is tackled in Mobile IPv6 by putting the care-of address as the source address and having a Home Address Destination option, allowing the use of the care-of address to be transparent over the IP layer.

Conclusion

It is evident that Mobile IP has great potential and it is being studied in a number of research projects like Stanford University's Mosquitonet project [17] and the CMU Monarch project [1]. Extensions have also been proposed to allow mobility management for the interface between a radio network and a packet data network in the third generation cdma2000 network.

Glossary

Care-of Address - The IP address of the mobile node's current point of attachment to the Internet.

Correspondent Node - A node that communicates with the mobile node. This node may be mobile or nonmobile.

Foreign Agent - A mobility agent on the foreign network of the mobile node that provides services to the mobile node.

Foreign Network - A network which the mobile node is currently visiting.

Home Address - A permanent fixed address of the mobile node which is used by TCP and higher level layers.

Home Agent - A mobility agent on the home network of the mobile node that maintains a mobility binding table.

Home Network - The network which is identified by the home address of the mobile node.

Mobile Node - A node that changes its point of attachment to the Internet.

Mobility Agent - A node that offers some services to a mobile node.

References

1

Carnegie Mellon University, *Monarch Project*. *http://www.monarch.cs.cmu.edu/*.

2

Chen Yi-an. *A Survey Paper on Mobile IP*. http://www.cis.ohio-state.edu/~jain/cis788-95/mobile_ip

3
Johnson,D. and Perkins,C. *Internet Draft - Mobility Support in IPv6*. http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-12.txt. March 2000, work in progress.

4
Perkins,C. and Johnson,D. *Internet Draft - Route Optimization in Mobile IP*. http://www.ietf.org/internet-drafts/draft-ietf-mobileip-optim-09.txt. February 2000, work in progress.

5
---. *Mobile IP*. http://www.srvloc.org/charliep/txt/commag97/paper.ps

6
---. *Mobile Networking Through Mobile IP*. http://computer.org/internet/v2n1/perkins.htm.

7
---. *Nomadicity: How Mobility Will Affect the Protocol Stack*. http://computer.org/internet/v2n1/nomad.htm.

8
---. and Johnson,D. *Special Tunnels for Mobile IP*. http://monarch.cs.cmu.edu/internet-drafts/draft-ietf-mobileip-spectun-00.txt.

9
---. *Mobile IP: Design Principles and Practice*. Addison-Wesley Longman, Reading, Mass., 1998.

10
---. *RFC 2004 - Minimal Encapsulation within IP*. http://www.ietf.org/rfc/rfc2004.txt. October 1996.

11
---. *RFC 2003 - IP Encapsulation within IP*. http://www.ietf.org/rfc/rfc2003.txt. October 1996.

12
---. *RFC 2002 - IP Mobility Support*. http://www.ietf.org/rfc/rfc2002.txt. October 1996.

13
RFC 768- User Datagram Protocol. *ftp://ftp.isi.edu/in-notes/rfc768.txt*. August 1980.

14
RFC 791 - Internet Protocol. *ftp://ftp.isi.edu/in-notes/rfc791.txt*. September 1981.

15
RFC 793 - Transmission Control Protocol. *ftp://ftp.isi.edu/in-notes/rfc793.txt*. September 1981.

16
Rivest R., *RFC 1321 - The MD5 Message-Digest Algorithm*. http://www.toc.lcs.mit.edu/~rivest/rfc1321.txtApri l1992.

17
Stanford University, *Mosquitonet Project*. http://mosquitonet.stanford.edu/.

18
Tanenbaum, Andrew S. *Computer Networks - Third Edition.* Prentice Hall, Inc., Upper Sadle River, New Jersey.

Biography

Debalina Ghosh is a graduate student in Computer Science at the University of Illinois at Chicago. She completed her Bachelors in Computer Science and Engineering from Jadavpur University, Calcutta, India. Her research interests are in Computer Networking and Computer Architecture. She can be reached at dghosh@eecs.uic.edu.