Mobility Support in IPv6

Dilip Antony Joseph (CS00294)
Indian Institute of Technology, Madras
dilip@peacock.iitm.ernet.in

Abstract

Mobile computing has become ubiquitous today. Laptop computers, PDAs and mobile phones connect to the internet from different locations and access data. Original topological IP routing fails in the case of mobile nodes. Mobile IP extensions to IPv4 have been used for getting data correctly routed to roaming mobile users. However, these extensions suffer from problems like Triangular routing. The IPv6 is a new internet protocol which has been developed to replace IPv4. IPv6 has inbuilt support for node mobility and secure communication. One of the main advantages of IPv6 is that it avoids the Triangular Routing problem through Binding Updates and also does not need Foreign Agents as in IPv4. In this term paper, we shall describe the mobility support offered by IPv6 in detail and also compare it with the relevant parts of IPv4. We also analyze the security aspects of mobility with special reference to firewalls and authentication. In the last part of this paper, we have identified certain problems with mobile IPv6 which are yet to be solved and have given some preliminary solutions.

1 Introduction

Over the last few years, the number of mobile computing devices like laptop computers, Personal Digital Assistants (PDAs) and smart mobile phones have mushroomed. These devices are carried from place to place by the users, all the while expecting smooth and uninterrupted network connectivity.

The IPv4 protocol has been successfully used for the past two decades to provide network connectivity between the various fixed computers on the internet. However, the mobility of the devices between different homogeneous or heterogeneous networks, raises many issues which cannot be handled by IPv4. Thus, IPv4 was extended to include support for Mobile IP. These mobility extensions suffer from problems like *Triangular Routing* and do not naturally gel in with the IPv4 protocol as they were added at a later stage. IPv6 is a new internet protocol which is to replace IPv4. The development of a completely new protocol gave the opportunity to incorporate mobility support right into the protocol. IPv6 avoids the problem of Triangular routing which was a major cause of inefficiency in IPv4 mobility support.

The main contributions of this term paper are that it explains the Mobile IPv6 protocol in a step by step and clear fashion. At each step, it compares how it is different from the mobility support in IPv4 (As far as we know, such step by step comparison is not available in literature.). It identifies some of the persisting problems with Mobile IPv6. An attempt is also made to come up with solutions

to these problems.

The rest of the term paper is organized as follows. Firstly in Section 2, we explain why mobile IP is needed. Section 3 presents a general overview of the functioning of IPv6 mobility support. Various individual components of the protocol are described in detail in Sections 3.1 to 3.7. Comparisons to Mobile IPv4 are made at appropriate locations throughout the paper. The advantages of Mobile IPv6 over Mobile IPv4 are collected together in Section 6. The problems caused by firewalls in Mobile IP are explained in Section 4. Section 7 describe the problems which are left unsolved by mobile IPv6. Some solutions to these problems are also offered in this section. Section 8 concludes the paper.

2 The Need for Mobile IP

Let us first look at why the traditional IPv4 protocol, which works so well for fixed nodes, fails in the case of mobile nodes. IP based routing is dependent on the hierarchical structure of the IP address. At this point, we introduce an example, which will be used throughout the rest of the paper to explain the various concepts related to mobile IP. Let us consider that a computer at *MIT* wants to deliver a packet to the machine *kurunji* with IP address (144.16.245.5) in IIT Madras. The router at MIT knows that all domains with IP addresses beginning in 144. are located in India, and hence the packet is sent to the Bombay gateway. From the remaining part of the IP address, the Bombay gateway understands that the packet is meant for IIT Madras which is on the ERNET network. Thus this packet reaches the Computer Centre of IIT Madras. The router at the Computer Centre finally sends it to the machine *kurunji* on the basis of the last part of the IP address. This presents a simplified picture of how hierarchical routing takes place in IP. Here, we can see that each router on the internet looks at only a part of the IP address during forwarding. It is infeasible to maintain correct and up to date routing tables based on the full 32 bit IP address at every router on the internet.

IP works fine as long as *kurunji* is a fixed computer. Now let us assume that *kurunji* is actually a laptop connected to the Computer Science Department network at IIT Madras. Suppose the laptop is disconnected from its home network and plugged into the Department of Computer Science network at Stanford University. Now, when the computer at MIT tries to transmit a packet to *kurunji*, how will the routers on the way know that *kurunji* is currently at Stanford, USA and not at IIT Madras, India? A quick-fix solution would be to assign a new IP address for *kurunji* in the Stanford University network. But then how will all the machines in the internet that wish to transmit to *kurunji* know about the new IP address? What about the packets already in transit on the internet while the node moved away? The Domain Name Services (DNS) may not be able to update its internal tables so that *kurunji* is mapped to its new IP address in a short time period. It will not scale up to support the simultaneous mobility of hundreds of thousands of computers.

Let us consider another situation in which the laptop *kurunji* is connected to the wireless LAN of the Dept. of Computer Science at IIT Madras. Now suppose that it is moved from the Computer Science Department WLAN to that of the Civil Engineering Department LAN (located at the bottom floor of the same building). All open TCP connections are to be maintained during the transit. Now since TCP connections are identified by the IP address of their endpoints, changing the IP addresses on entering the new WLAN will immediately terminate the

TCP connection.

Clearly, the issues mentioned above cannot be handled by pure IPv4. To provide support for mobility, Mobile IP was proposed as an extension to IPv4 and is in use today. However in IPv6, mobility support is directly built into the protocol. In the next section we describe in detail, how the mobility of nodes is handled in IPv6.

3 Mobile IPv6 Operations

In this section, we describe the functioning of the Mobile IPv6 protocol. The mobile entities like laptops, PDAs, mobile phones etc. are further referred to as *Mobile Nodes* (*MNs*)in this paper. Each MN has a unique home IP address corresponding to its *home network*, and can communicate with different networks whenever link level connectivity to the network is available – wired or wireless. The network to which an MN connects to after moving away from the home network is called the *Foreign Network*. The fixed or mobile nodes to which send packets to the MN are called *Correspondent Nodes* (*CNs*).

Let us continue with the example begun in the previous section. When the laptop *kurunji* moves to the new subnet at Stanford University, it acquires a global routable *Care of Address* (*CoA*) in the foreign network using the IPv6 auto-configuration mechanism. After acquiring a *CoA*, it sends a binding update to a machine or router on its Home Network called the *Home Agent* (*HA*). Any packets sent to *kurunji* at its home IP address by Correspondent Nodes (for example, the machine at MIT) is intercepted by the Home Agent (located in IIT Madras) and tunneled to the *kurunji* at its current Care of Address using IPv6 encapsulation. This packet reaches *kurunji* in its foreign network (Stanford University) via normal IP routing. On receiving the encapsulated packet from the HA, the node sends a Binding Update to the CN informing it about its current CoA – future packets can be routed directly to the CoA, thus avoiding the triangular routing problem (see Section 3.6). When *kurunji* wants to send a packet to the CN at MIT, it can directly send the packet using the router in the foreign network i.e. the packet does not have to go through the HA.

Although the overall protocol looks simple, there are various issues to be considered at each stage of the process. For example, how does the MN discover that it has entered a new foreign network, how does it acquire a *CoA*, how do binding updates work etc. There are also problems like Firewalls blocking packets of the mobile node and remote redirection attacks by hackers. All these issues and problems are discussed in detail in the following sections.

3.1 Entering a Foreign Network

In this section, we discuss how an MN realizes that it has moved into a new network. We then describe the process by which the MN locates routers and other resources needed for its operations in the foreign network.

Mobile Nodes make use of the IPv6 *Neighbour Discovery* protocol to detect mobility. *Unreachability Detection* indicates when the MN has moved out of the coverage of its current router. For wireless networks, MNs can also detect that it has moved into a new network when the signal strength from the current base station falls below a threshold. *Router Discovery* is used to find a new router in the network. This is done by listening to the periodically broadcast *Router Advertisement* messages. On the basis of the information contained in the Router advertisementis, the MN configures its Care of Address and

sets it Default Router entry to be used to send packets while in the foreign network. In Mobile IPv4, the Router Advertisements are broadcast by the *Foreign Agents* and contain the CoA to be used. In IPv6, the explicit notion of Foreign Agents has been done away with and the MN configures its CoA as described in Section 3.2.

The minimum interval between two advertisements is 3 seconds. This lag of 3 seconds may work fine for wired networks. However for wireless networks, it will be a hindrance to smooth handoffs (explored later in Section 3.7). The MN need not always wait for a Router Advertisement – it may send *Router Solicitation* messages. We must keep in mind that mobile nodes are often constrained in processing capabilities and work on limited battery power. In such a case, continuously listening for Router Advertisements leads to the expenditure of scarce battery power. The MN should try to remain in doze mode for as long as possible. However, the MN should also constantly monitor for unreachability of its current default router - an indication that the MN has changed location. No clear solution exists for how the MN can optimally conserve resources while listening for Router Advertisements. We must also note that sending *Router Solicitations* is a very costly operation and may lead to network congestion if a large number of MNs attempt it simultaneously.

3.2 Acquiring a Care Of Address (CoA)

A Mobile Node on entering a new network must first acquire a *Care of Address* (*CoA*). Stateless autoconfiguration is used by the MN for this purpose. This does away with the need for Foreign Agents or DHCP servers, which were required in Mobile IPv4. In the following sub-section, we briefly describe the IPv6 autoconfiguration process, on the basis of the information contained in RFC 2462 [7].

3.2.1 IPv6 Stateless Address Autoconfiguration

The autoconfiguration process includes creating a link-level local address for the MN in its current network and also verifying its uniqueness on the link. It also determines the information to be autoconfigured like default router information and Care of Addresses. This can be done by a stateless or stateful manner. The stateful approach is taken in the DHCP v6 protocol, with which will not deal in this term paper. Stateless autoconfiguration requires no manual configuration of hosts or servers – the host generates its own address using a combination of locally available information and the information available in the router advertisements. The subnet prefixes are taken from the Router Advertisements while the MNs generate unique *interface identifiers*. These two are combined to get the Care of Address. Of course, the address generated should be verified to be unique using the *Duplicate Address Detection Algorithm*. The generated Care of Addresses are also associated with a lifetime.

We must also note here that IPv6 provides for a extremely large number of IP addresses (due to its 128 bit length). In IPv4, the luxury of assigning a unique Care of Address to every roaming MN was not possible due to IP address shortage.

3.3 Registering with the Home Agent

After acquiring a Care of Address in the foreign network, the MN should register this CoA with a machine or router in its home network known as the *Home Agent* (*HA*). In the case of Mobile IPv4, this registration process is handled with the support of the Foreign

Agent. In Mobile IPv6, there is no Foreign Agent and the MN directly sends a *Binding Update* to the Home Agent. The Home Agent creates an entry for the MNs CoA in its *Binding Cache* and sends a *Binding Acknowledgment* back to the MN. The HA also sends out IPv6 Neighbour Discovery messages for the MN in the home network. This is done so that all the packets received for the roaming MN are sent to the HA, to be in turn tunneled to the MN.

Before exploring the concept of *Binding Caches* and *Binding Updates* in Section 3.4, we look at how a Home Agent is located in the first place.

3.3.1 Dynamically Finding a Home Agent

The Home Agent of a network may change over a period of time - the machine may have been replaced by another one. In such a scenario, a currently roaming MN belonging to the particular home network will not be aware of this change of HA Address. IPv6 supports the dynamic discovery of Home Agents. The MN sends the registration Binding Update to the Home Agent IPv6 *any cast address*, which will be invariant. Exactly one Home Agent responds – it rejects this Binding Update but sends a list of Home Agent addresses in decreasing order of preference back to the MN. Now the MN tries to register with the HAs in the list one by one in decreasing order of priority, till the registration succeeds. Detailed information about anycast addresses can be found in [8].

3.4 Binding Caches and Binding Updates

The *Binding Caches* and *Binding Updates* are very important to Mobile IPv6. Binding Updates are used by the mobile node to register with its Home Agent and also to inform Correspondent Nodes about its current location. This section explores the functioning of the Binding Caches and Binding Updates.

A *binding* is an association between the Home Address of the Mobile Node and its Care Of Address, along with the remaining period of association. This binding is stored in the *Binding Cache* of the node. Each IPv6 node has a *Destination Cache* into which the *Binding Cache* can be easily integrated. The binding is created on receiving a *Binding Update* message. The binding cache follows a cache replacement policy like LRU (Least Recently Used).

IPv6 defines several extension headers - Routing, Authentication, Destination Options and Hop-by-Hop Options. The *Binding Updates* are sent as part of the Destination Options Header of an IP packet. This implies that the binding update messages can be sent along with other data packets, thus saving network bandwidth. The current Care of Address of the MN is specified inside the message. The Home Address of the MN is obtained from the source address in the packet header. A life time field in the Binding Update message specifies the number of seconds for this binding is to be considered valid. The binding should be refreshed before it expires. Each Binding Update is also associated with an *Id* field, which ensures that the updates are applied in the correct order. The value of *Id* is incremented each time a node sends a Binding update. The setting of the *H bit* indicates a request to the node receiving the update to serve as a Home Agent for the MN. This bit is set during the Home Agent registration described in Section 3.3. A *Binding Acknowledgment* may be requested by setting the *A bit* of the Binding Update. If the acknowledgment is not received within a timeout period (starting at 1 second), the MN keeps retransmitting the update with an ex-

ponential backoff in the timeout period. The acknowledge option is used mainly in the case of Home Agent registrations and not with Correspondent Nodes.

The *Binding Update* feature of Mobile IPv6 is the target of hacker attacks like the *Remote Indirection attack*. The various security problems associated with Mobile IPv6 are described in Section 5.

3.5 Sending and Receiving Data

In this section, we shall describe how a node receives and sends packets while it is away from its home network. We have already seen the process of obtaining a Care of Address and registering with the Home Agent.

3.5.1 From CN to MN

When a Correspondent Node (CN) wishes to send a packet to the MN, it first looks in its Binding Cache for the MN's current Care of Address. If no CoA is found, the CN sends the packet to the MN's Home IP Address. When this packet reaches the Home Network, it is intercepted by the Home Agent (HA). It is the responsibility of the Home Agent to correctly forward the packet to the MN at its Current Care of Address, looked up from its Binding Cache. The HA encapsulates this packet in the payload field of another IP packet addressed to the MN's current CoA. The source field of this outer packet is set to the HA's IP address. This is called *IPv6 encapsulation*. This packet reaches the MN at its CoA where it is decapsulated and sent locally within the mobile node itself as packet from the CN. Thus, the higher layers of the networking protocol stack see the packet as having directly originated from the CN and process it appropriately.

Many fields of the original header are duplicated during IP-in-IP encapsulation. This waste of bandwidth due to redundancy may be decreased by using a form of encapsulation called *minimal* encapsulation.

When an MN receives an encapsulated packet from the CN via the HA, it immediately sends a Binding Update to the CN. Once the binding is created in the CN's binding cache, packets may be directly to the MN, without the help of the Home Agent. This avoids the problem of triangular routing described in Section 3.6. The packet is addressed to the Care of Address of the MN. However, the home address of the MN is indicated as the final destination using the IPv6 *Routing Headers*. When this packet reaches the mobile node, normal IPv6 processing of the Routing Header is done and the packet gets delivered to the higher layers of the protocol stack using the MN's home address. The binding is maintained by the MN by sending more update messages before the expiry time of the binding. When the MN moves into a new network, the MN sends the Binding Update messages with the new CoA to its HA and all currently corresponding nodes.

A natural question now is why the HA uses encapsulated packets to create a tunnel to the MN rather than using Routing Headers which are more efficient. The HA does not alter the Routing Header because doing so will destroy the IPv6 authentication – i.e. the signature made by the CN will not be valid when the packet is authenticated at its destination MN. Hence, HAs use tunneling instead of Routing Headers.

In mobile IPv4, the CNs send the packets to the Home Agent which then tunnels the packet to the MN's foreign agent. Although extensions envisage the use of a Binding Cache, most nodes on the internet do not support it and hence it is not prevalent. So all communication from the CN to MN is only

through the HA. This is highly inefficient (see Section 3.6 and makes the HA a bottleneck.

3.5.2 From MN to CN

When the MN wants to send a packet to the CN, it does so directly through the foreign network router discovered when it first entered the network. The IP packet is addressed to the CN and carries the MN's home address as the source address. This communication with the CN does not involve the Home Agent of the MN neither in Mobile IPv6 nor in Mobile IPv4. However, this simple protocol may fail in the presence of firewalls, on which we shall elaborate in Section 4.

3.6 Solving the Triangular Routing problem

We have already mentioned about the Triangular Routing (also known as *Dogleg* routing) at multiple places in the paper. Here we shall describe this problem in detail with the help of our familiar example.

Suppose a computer belonging to the Stanford University network (the CN) wants to send a packet to the laptop *kurunji* (the MN), while it is at Stanford. The CN sends the packet to the home address of *kurunji* which in turn tunnels it back to Stanford. Thus we see that the packet has traveled half across the world and back, all the while when the two computers were at such close distance to each other. It is a big waste of network as well as a source of long latencies. This problem is known as the *triangular routing problem*. Figure 1 illustrates the problem.

The original mobile IPv4 functioned in this manner. *Route optimization* extensions were added to it, enabling CNs to obtain the Care of Address of the MN. However these extensions worked with only those machines on the internet which had these special enhancements in their protocol stack. Hence the solution was not very effective. However, in mobile IPv6, we have already seen that every IP node has a binding cache to store the CoA of the MN. The *Binding Updates* and *Binding Acknowledgment* messages help in maintaining the appropriate bindings in the binding cache. The triangular routing problem takes place only for a short initial period of the CN's communication with the MN. This is one of the major strengths of mobile IPv6.

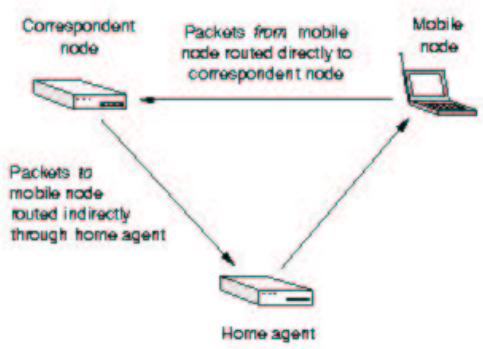

Figure 1: The Triangular Routing Problem (Source: [1])

3.7 Smooth Handoffs

Suppose *kurunji* moves from the Stanford University network to the University of California, Berkeley network and acquires a new Care of Address there. However, there will still exist packets on the internet which are addressed to the previous CoA. When these packets reach the Stanford network, *Host Unreachable ICMP* error messages are sent back. However, for smooth handoff and continuity in network connection, we require that the packets addressed to the MN at its previous CoA reach it even after it has acquired a new CoA. This becomes even more important in the case of MNs connected via wireless links, where the handoff between different networks is more frequent than in the case of wired con-

nections.

If the MN is able to receive packets at two CoAs simultaneously (for example, listen over two wireless interfaces), the problem is solved. However when this is not possible, the help of the routers in the foreign network is needed. The MN which has moved into the new network sends a binding update to the router in its previous foreign network. This binding update also requests the router to serve as a temporary Home Agent for the MN by setting the *H bit*. Whenever a packet arrives at the previous CoA, it is intercepted by the router and tunneled to the MN at its new Care of Address, as in the case of normal Home Agent operations. The life time of these bindings is set to a sufficiently small value by the MN.

4 Stopped by the Firewall

Most companies and institutions set up firewalls to secure their internal networks which are connected to the internet. These firewalls block out traffic to and from the internet on the basis of the rules configured by the network administrator. Many of these rules hinder the operations of the mobile node in a foreign network.

As mentioned earlier, when a mobile node in a foreign network wants to transmit data to a CN or wants to send a *Binding Update*, it directly uses the router in its foreign network. The destination address of the packet that of the CN while the source address is the MN's fixed home address, which is not topologically correct within the foreign network. Most firewalls are configured to block such packets with topologically incorrect source addresses. So these packets can never get out of the foreign network! This is called *ingress filtering*.

Now suppose we encapsulate the packet to the CN within an IP packet with the CoA as the source address and the destination that of the CN. Now this packet will pass through the firewall. But sometimes, firewalls are configured to even look for internal addresses. Let us consider the case where the packets manage to leave the foreign network. But now, there is another problem – the firewall at the CN's network may accept packets with source addresses belonging to the MN's home network; but not those belonging to its current foreign network! These packets are thus again prevented from reaching the CN.

Consider another situation in which the currently roaming MN wishes to send a packet to a CN in its home network. The MN puts its Home IP address as source and sends the packet to its home network. Assume the foreign network firewall allowed it to pass. But this packet will now be stopped by the firewall of the Home Network which will filters out all packets from outside containing a source address of an internal node. So the node cannot now even communicate with a node in its home network! Is it totally cut off from the rest of the world? Reverse tunneling presents a solution.

In *Reverse tunneling*, all packets to a CN from the MN go through the Home Agent of the MN. Although this solution works, it is inefficient because it now causes triangular routing in the reverse direction. Reverse tunneling is also associated with the security problems discussed in Section 5.

No satisfactory solution to this problem exists. One possible solution will be to set up separate rules for mobile nodes within the firewall. Another solution is to set up a separate machine in the foreign network to handle MN to CN communication. CN to MN communication takes places directly as described earlier. All MN to CN communication is first sent to this agent. All the traffic filtering rules are applied at this machine. The firewall gives special privileges for this machine to transmit messages to the CNs on behalf

of the MNs, using the MN's home address as the source. This machine may even be placed outside the regular network to enhance security – i.e. it is solely used by visiting MNs to transmit data to the CNs. However, the impact of this solution on the authentication between the MN and the CN is to be studied.

5 Issues in Security

Security is a highly essential requirement in Mobile IP. This section discusses the various aspects of security related to the mobile nodes, their home networks and the foreign networks.

First of all *Binding Updates* sent by the MN have to be authenticated. Without foolproof authentication, a malicious node will be able to fool the Home Agent or CN into setting an erroneous binding for the MN and make it unreachable to all further communication from the internet or the particular CN respectively. The foreign routers should also be authenticated – else a bogus router may 'offer' its services to the visiting MN and not forward any of the packets sent by the MN. The *Binding Updates* sent by the MN may also give away the MN's current location to an adversary, thus violating privacy.

In mobile IPv4, authentication was supported by digitally signing the registration messages using the Message Digest 5 protocol (RFC 1321) with 128 bit keys. Each registration message also included some unique data to ensure that two different registrations will never have the same signature. This prevents replay attacks in which the malicious nodes record valid MN to HA registration messages and replay them at a later stage, thus disrupting traffic to the MN from the HA. The uniqueness of the registration messages can be achieved by including a timestamp or a random number with registration messages. The random number method is more stable as it is not affected by hacker attacks on the NTP protocol to throw the MN and HA out of synchronization. Replay attacks can also be prevented by the Challenge Response protocols to Mobile IP.

In mobile IPv6, all the security related features are handled by IPv6 itself. All IPv6 nodes have inbuilt support for IPSEC. Authentication of *Binding Updates* is done by using the *Authentication Headers* feature of IPv6, while *Data Encapsulation Payload (ESP)* mechanisms (both Tunnel and Transport modes) may be used to support data integrity and secrecy. The key, algorithms and other security parameters are specified through the *Security Associations* set up for each connection. More details about the various features of IPSEC can be found in [6].

Authentication and encryption require keys to be known to the both the HA and the mobile nodes. Establishing secret keys between the MNs and the HAs is easier than between the MN and foreign routers, as the MN and the HAs belong to the same administrative domain. In any case, key distribution can be done through Key Distribution Centers (KDCs) or through a Public Key Infrastructure (PKI). Establishing secret keys between every pair of foreign routers, MNs and HAs is highly inefficient and error prone in large networks. HAs themselves can function as Key Distribution Centers and can have security associations with each MN in its domain as well as with routers in the domains in which the MNs are allowed to roam.

Tunneling between the HA and roaming node can be exploited to gain unauthorized access into the foreign network. Reverse tunnels from the internal foreign network to the internet can also be hijacked by hackers and can be used for sending sensitive packets through the firewall. Hence network administrators are not likely to accept any tunnels through the firewalls. Firewalls also hamper

the functioning of legal MNs. (refer Section 4). To solve this problem, firewalls must be made aware of the visiting mobile nodes and grant special access privileges to them. The information about the visiting nodes must be obtained from the foreign routers, leading to an increased load on the system. This is system is still not secure. Another approach mentioned in [4] is to integrate the mobility supporting architecture into the gateway system located inside the firewall from where it can be centrally administered.

[5] gives an overview to the security aspects of mobile IP and compares the various approaches taken.

6 Advantages of Mobile IPv6

In this section, we have collected together the various advantages of Mobile IPv6, some of which have already been mentioned earlier.

1. One of the main problems faced by IPv4 was the shortage of IP addresses. In such a situation, it was not possible to assign separate Care of Addresses (or co-lated IP addresses) for each mobile node in a foreign network. Mobile IPv6, with 128 bit IP addresses, makes it possible to even assign multiple CoAs to roaming mobile nodes.

2. The MNs acquire Care of Address using the IPv6 stateless address autoconfiguration methods (Section 3.2 and neighbour discovery mechanisms. There is no need for a Foreign Agent as in the case of Mobile IPv4.

3. Triangular routing (Section 3.6 was a major problem in Mobile IPv4. However the Binding Cache present in all IPv6 nodes mitigate this problem to a large extent. Also, the Binding protocol is uniformly handled by all nodes – correspondent nodes, home agents and foreign routers.

4. Security is an integral part of IPv6 and IPSEC features are built into each IPv6 node. As against in mobile IPv4, security features like authentication of registration messages, data integrity etc, do not have to be handled separately.

5. Mobile IPv6 offers an elegant solution for dynamically discovering Home Agents through IPv6 anycast addresses (Section 3.3.1. Such a feature was not available in Mobile IPv4.

6. [2] claims that Mobile IPv6 allows nodes to surpass *ingress filtering* by using the CoA of the MN as the source address of the packet to be sent to the CN. The Home Address of the MN is specified in the Home Address destination option. However this solution fails if the firewall is configured to detect internal addresses also.

7 Problems with Mobile IPv6

This section identifies a few problems associated with Mobile IPv6. First of all the hindrances to mobile IP caused by packet filtering at firewalls has not been completely solved.

Mobile IPv6 does not also deal with home agent failures, although it does allow dynamic home agent discovery. We propose a solution in which the multiple home agent capable machines present in the network balance the load of roaming MNs among themselves. They also monitor whether the other HAs are

functioning correctly. If one of the HAs is noticed to be down, then another HA can automatically take over the roaming MNs currently being served by the dead HA. A message is sent to the MN informing it about the change. The bindings from the dead HA should be salvaged from periodic backups to a highly reliable central storage or to all the HAs. If the roaming MN by itself detects that its HA has gone down (for example, by long periods of silence from the HA), it can send a *distress signal* to the HA anycast address. Then another HA will take over. This is just a preliminary proposal. More work is to be done in developing the detailed protocol and its functioning is to be analyzed.

As briefly mentioned in the section on security (Section 5), preserving the location privacy of the MN is of concern. Authentication of the the node before sending a binding update to it and encryption of the update message can solve the problem to an extent. But suppose the MN wishes to communicate with a CN without revealing its current location. Of course, triangular routing through the HA is a solution – but it is highly inefficient. The problem remains unsolved.

Mobile nodes connected to the network via wireless links may change their locations at a very fast pace. This leads to a very large number of Binding Update messageis being sent to the HA and the CNs, which in turn causes network congestion. In the case of Mobile IPv4, solutions to avoid this problem by clustering Foreign Agents and sending location updates to the HA only on changing clusters, have been proposed. A similar solution can be adapted for Mobile IPv6, keeping in mind the absence of foreign agents.

8 Conclusion

In this term paper, we discussed the Mobile IPv6 protocol step by step with the help of a running example. We also compared each step with the corresponding procedures in Mobile IPv4. A list of advantages of Mobile IPv6 over Mobile IPv4 has also been drawn up. As against IPv4, mobility support is built into IPv6. Through binding caches, IPv6 mitigates the problem of triangular routing. The later sections of the term paper discussed the various aspects related to security in mobile IPv6 - authentication, data integrity and secrecy, firewalls etc. There do exist some problems with mobile IPv6 like firewall blocking, home agent failures, loss of privacy and update explosion. Some preliminary solutions have been proposed for these problems.

With the large scale use of IPv6 in the future, network connectivity for mobile nodes is sure to become seamless and efficient. A very large number of mobile devices of all types and sizes will use this support to access the internet and to communicate with each other. There are already many implementations of Mobile IPv6 existing[10], both in the industry and academia. With widespread use and active research, the protocol is sure to evolve to support newer and newer requirements and will achieve greater efficiency and efficacy in mobile communications.

References

[1] D. Johnson and C. Perkins, "Mobility Support in IPv6," ACM Mobicom 96, ACM, Nov. 1996, pp. 2737.

[2] Wolfgang Fritsche, Florian Heissenhuber, "Mobile IPv6 - Mobility Support for the Next Generation Internet" (White Paper), www.ipv6forum.com/navbar/papers/MobileIPv6_Whitepaper.pdf

[3] Charles E Perkins, "Mobile Networking Through Mobile IP, Tutorial", http://www.computer.org/internet/v2n1/perkins.htm

[4] S. Mink, F. Phlke, G. Schfer, J. Schiller. FATIMA: A Firewall-Aware Transparent Internet Mobility Architecture. Proceedings of ISCC

[5] S. Mink, F. Phlke, G. Schfer, and J. Schiller. Towards Secure Mobility Support for IP Networks. In Proceedings of the IFIP International Conference on Communication Technologies

[6] RFC 2401 - Security Architecture for the Internet Protocol, http://www.ietf.org/rfc/rfc2401.txt

[7] RFC 2462 - IPv6 Stateless Address Autoconfiguration, http://www.faqs.org/rfcs/rfc2462.html

[8] RFC 2526 - Reserved IPv6 Subnet Anycast Addresses, http://www.faqs.org/rfcs/rfc2526.html

[9] RFC 1688 - IPng Mobility Considerations, http://www.faqs.org/rfcs/rfc1688.html

[10] Mobile IP Implementations, http://mosquitonet.stanford.edu/mip/resource.html