Mobile IP, Ad-Hoc networks
S38.188 lecture notes

Jouni Karvo

Apr 5th, 2004

1 Mobile IP

Mobile IP is being developed in IETF working groups *mip4* and *mip6*. For IPv4, Mobile IP is defined in RFC3344 [3] and reverse tunnelling in RFC3024 [2], and work is going on for VPN and AAA extensions. For IPv6, Mobile IP specifications are IETF internet drafts.

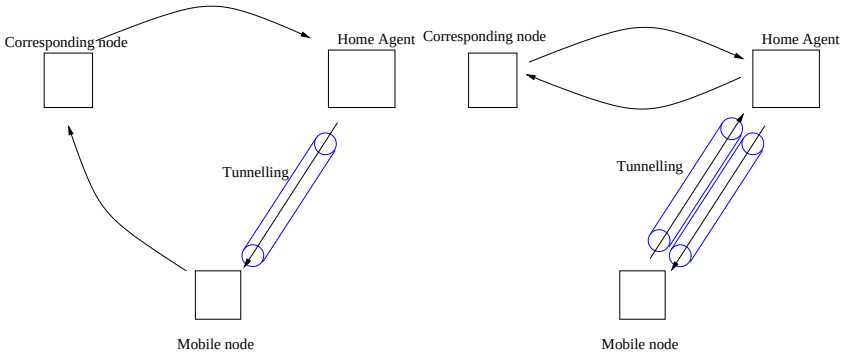
Mobile IP is an overlay over the normal IP network, intended for providing host mobility transparent for upper layer applications. Using Dynamic Host Configuration Protocol (DHCP) allows a traveller to access the Internet, but mobile IP is used for finding and reaching the mobile station.

The Internet Protocol (IP) routing is based on the IP addresses, that define where the destination node should be found. Moving the host with a specific IP address generates problems, since the routing algorithms rely on using network prefixes. This means that all hosts having the same first bits in the address are supposed to be found in the same part of the network. If the IP address of a host is changed when the host has active connections, it leads to breaking of established connections. Also, changing the IP address results in losing the binding in DNS. Thus, the dependence of the IP address and host location must be broken.

The hosts that support Mobile IP have *two* IP addresses. The *home address* is static, and is used by applications to identify the host. The *care-of address* is temporary and depends on the actual location of the host (mobile node). As for the HLR in GSM, mobile IP requires a static host in the home network. This host, the *home agent* has the information on the mobile node's current care-of address. The mobile node informs the home agent whenever its care-of address changes (due to mobility), by sending *binding updates*.

Whenever a host (corresponding node) tries to communicate with the mobile node, it sends the packets with the home address. The packets are routed to the home network. If the mobile node is not present in the home network, the home agent gets the packet, and *encapsulates* it within another IP packet containing the mobile node's care-of address, and sends the packets forward. This procedure is called *tunnelling*. In Mobile IPv4, the mobile node sends its packets directly to the corresponding node, and thus a triangular path is

established, where packets going in each direction follow different routes. See Figure 1. For Mobile IPv6, the tunnel between the Home Agent and the Mobile Node is bi-directional, and the packets to the Corresponding node are first tunnelled to the Home Agent, who then forwards them to the Corresponding Node.



(a) IPv4 (b) IPv6

Figure 1: Routing in mobile IP

There are three mechanisms in mobile IP [4]

- Discovering the care-of address,
- Registering the care-of address, and
- Tunnelling to the care-of address.

These mechanisms are treated in the next sections.

1.1 Discovery of the Care-of Address

When the mobile node moves to another network, it must first detect that it has moved to a new network, called *foreign* network. Then, it must obtain a new care-of address. For IPv6, this can be implemented using the *Stateless Autoconfiguration* procedure. For IPv4, this can be node in two ways. First, the routers in the foreign network, *foreign agents*, send messages called *agent advertisment* messages. When the mobile node receives such a message, it sets its care-of address as the IP address of the foreign agent. In this case, the foreign agent acts as the endpoint of the tunnel, and de-capsulates the messages for the mobile node. Second, the mobile node can acquire a care-of address by a different means, such as via DHCP, in which case the mobile node itself acts as the tunnel endpoint. The latter method allows the mobile IP to work in networks that do not have specific mobile IP functionality implemented, with

the expense of the need of free IP addresses in the foreign networks. Note that for Mobile IPv6, there are no foreign agents.

1.2 Registering the Care-of Address

As noted in the previous section, there are two modes for a mobile node in a foreign network — the node either communicates via a foreign agent or directly with the home agent. In both cases, the care-of address of the mobile node needs to be registered in the home agent. In the simplest case, the mobile node sends a registration message over UDP to the home agent, and the home agent replies either granting or denying the request. The registration messages contain a lifetime field that defines the period for which the registration is in effect. If the mobile node does not renew its registration, the registration expires after this period, and no further tunnelling to the mobile node will be done.

The registration procedure is supplemented with authentication features that are meant to prohibit malicious nodes to redirect packets addressed to the mobile node to somewhere else. In cases where there are no foreign agents involved, the authentication is easy, since it can be assumed that the MN can have a security association with the home agent. The IPv4 case with foreign agents is more troublesome, since the key management becomes a problem.

1.3 Tunnelling to the Care-of Address

When the mobile node is in a foreign network (and has its care-of address registered in the home agent), it is the task of the home agent to intercept the packets destined to the mobile node's home address. This can be done by exploiting Address Resolution Protocol (ARP) mechanisms, where the home agent advertises its own MAC address as the MAC address of the mobile node, and replies to the queries addressed with the mobile node's home address.

After the home agent has intercepted the packet for the mobile node, it uses an IP-in-IP tunnelling, where the IP datagram as a whole, and without alterations, is inserted to (encapsulated into) the payload of another IP datagram. The outer IP header uses the care-of IP address, and is routed normally to the mobile node (or to the foreign agent), where the encapsulation is taken off and the original IP datagram is found intact[1].

For Mobile IPv6, a two way IP6-IP6 tunnel is always established between HA and MN after the binding update.

When MN is not in the home network, the HA must take care of keeping the MN's home address reserved, so that stateless autoconfiguration will not reassign it to other nodes.

Whenever the mobile node returns to its home network, it has to de-register its care-of address from its home agent, set on its ARP processing and advertice its own MAC address as the MAC for its home address.

[1] Message integrity is not guaranteed, however, by any means; IP-in-IP tunnelling does not use cryptographic elements. Also, the messages are vulnerable to eavesdropping. IP-in-IP tunnelling can be substituted with another tunnelling protocol.

1.4 Route Optimisation

Route optimisation is used to enable the mobile node to communicate directly with the corresponding node, instead of sending all traffic via the home agent. Route optimisation in Mobile IPv6 is as follows: The MN sends a binding update to the CN. Route optimisation requires the binding cache functionality in the CN. If the CN has a binding cache, it will register the MN:s CoA to the binding cache. CN sends the packets to the MN using IPv6 routing header 2, which is actually a source routing functionality where the CoA is given as an address through which the packet must be routed on the way to the home address. When MN sends its packets to CN, it needs to include both addresses (Home and Care-of Address). The Home Address is needed so that CN knows with whom it is communicating, and the CoA is needed so that the routers on the way have topologically correct addresses. The MN takes care of this by using the Home Address extension option in each IPv6 packet. In the CN, the source address found in the packet is changed to the home address before processing the IPsec or upper layer protocols.

Between HA and MN there is a security association (which is natural), so they can trust each other and use IPSEC ESP for communications. IKE daemon can also be used. Between MN and CN, there is not (necessarily) any security association, so no IPsec authentication is used. Instead, *return routability* protocol is used for securing the origin of the binding updates.

1.4.1 Route Optimisation for Mobile IPv4 (obsolete)

As noted in Section 1, mobile IPv4 forms triangular routes. A route optimisation mechanism can be used to optimise routing, i.e. to allow the corresponding node to directly send messages to the mobile node. To use the protocol, the corresponding node needs to be able to support the mobile IP, at least to some extent. The idea is that when the home agent receivers a packet for a mobile node, it tunnels the packet to the mobile node but in addition sends the corresponding node a message called *binding update* that contains the necessary information (mainly the care-of address) for the corresponding node to send further packets directly to the care-of address.

Another route optimisation procedure is the establishment of a forwarding tunnel from the previous foreign agent to the current foreign agent when a hand-over is processed, providing for a smoother hand-over.

Naturally, these route optimisation mechanisms incur new security problems that need to be solved. Work stalled, and not included in the specifications.

1.4.2 Reverse tunnelling

Another approach for counterattacking the triangular routing problem in IPv4 is the *reverse tunnelling* approach, which actually corresponds to the Mobile IPv6 bidirectional tunnel approach.

The problem of triangular routing is that the mobile node uses its home address as source addresses for messages sent to the corresponding nodes. Nat-

urally, when not in the home network, the home address and the care-of-address are different. For security reasons, most routers only accept to forward packets that have topologically correct addresses, i.e. the source address is the address from a network where the node resides.

The RFC 3024 [2] defines a work-around for this problem, called *reverse tunnelling*. The idea is that a tunnel is established from the mobile node's care-of address to the home agent, in addition to the forward tunnel from the home agent to the mobile node. Reverse tunnelling has some additional benefits in addition to fixing the topological problem:

- The TTL field of the packets does decrease due to the mobile node being away from the home network.
- It allows the mobile nodes to join multicast groups in the home network.

Reverse tunnelling does not itself help in firewall traversal, the firewalls need to have security associations separately.

In practice, reverse tunnelling is implemented so that the mobile node selects a foreign agent that supports reverse tunnelling. After registering, the mobile node sends its packets to the foreign agent, which encapsulates them and sends them to the home agent.

1.5 Mobile IPv6 spices

Dynamic Home Agent Address Discovery gives the possibility for the MN to find HA:s automatically. There is also a mechanism for redefining the home address of a MN in case of address prefix changes; Mobile Prefix Discovery. For an active MN, the HA can give the new address prefix directly.

2 Ad-Hoc Networks

Ad hoc networks are networks that do not require fixed infrastructure (base stations etc), but communicate directly with each other. The term ad-hoc refers to the way in which the nodes notice that there are other nodes that can be communicated with, i.e. in a non-planned, non-engineered way. When nodes having these ad-hoc connections start relaying other nodes' traffic, a network is formed, and this network is called an ad-hoc network. See Figure 2. When the nodes in the ad-hoc network are able to move, the network topology can change when the time goes on, and the network is called a mobile ad-hoc network (also referred to as MANET). Note that as such, the term mobile ad-hoc network does not refer to any specific link or network layer protocols. It is often used, though, to refer to an IETF work that considers IP based mobile ad-hoc networks.

The ad-hoc networks have been a research issue for several decades, and as yet no commercial applications have emerged. Even after the long research period, there are lots of open questions, waiting to be solved.

IETF MANET group, [1]

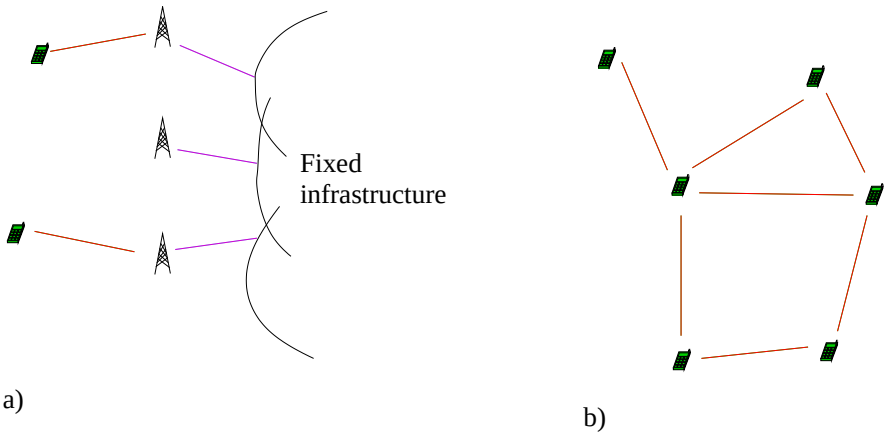


Figure 2: a) A mobile network with a fixed infrastructure vs.b) an ad-hoc mobile network

- The topology of an ad-hoc network is dynamic.
- The shared wireless medium has very constrained capacity.
- The devices are energy constrained. Mobile nodes typically use battery power as their energy source, and relaying messages consumes additional power.
- There is no implied security. Since the network is constructed in an ad-hoc manner, also hostile nodes might join the network.

References

[1] Corson, S., and Macker, J. *Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations*, Jan. 1999. RFC 2501.

[2] Montenegro, G. *Reverse Tunneling for Mobile IP, revised*, Jan. 2001. RFC 3024.

[3] Perkins, C. *IP Mobility Support for IPv4*, Aug. 2002. RFC 3344.

[4] Perkins, C. E. *Mobile IP Designe Principles and Practices.* Addison-Wesley, 1998.