Mobile IP

Mobile Computing

Introduction
- Amount of mobile/nomadic computing expected to increase dramatically in near future.
- By looking at the great acceptance of mobile telephony, one can foresee a similar acceptance of mobile computing.
- Today, tens of millions of people in the U.S alone carry a lightweight/inexpensive terminal giving them access to worldwide information network called PCN.
- As user's demand increase with offered services of mobile communications systems, the main expectation on such systems will be:
  - To provide access to any service anywhere at anytime.

Mobility versus Portability

There are two similar terms: Mobility and portability
- **Portability**: Computers can be operated at any set of points of attachment, but not during the time that the computer changes its point of attachment.
- **Mobility**: Involves continuous contact with network resources maintained. There is an uninterrupted connectivity between the application and the source.
Introduction to Mobile IP

**Background**: Problem with Traditional IP Scheme.
- Addressing: Routing based on IP hierarchical addressing structure.
- Address valid when host attaches itself to network.
- Routers use this association to route the packet to host.
  - Prefix used for packet delivery.
  - Change in network, address no longer valid.
- This scheme works well with stationary hosts.
- For mobile hosts addressing structure needs to be modified.

Supporting Mobility

- Several solutions proposed to solve addressing problem: **Changing the address**.
  - TCP related Problems
  - Loss of packets.
  - Access to Private networks.
- Mobile IP was designed to solve all these problems

Mobility of IP-based Wireless Networks

**Categories of Mobility**
- Host Mobility and Network Mobility.
- Macro-mobility and Micro-mobility
- IP Mobile Multicasting
Requirements of Mobility

- Efficient Handoff
- Location Management
- Efficient Routing
- Security
- Scalability
- Fault Tolerance
- Simultaneous Mobility
- Link Layer Independence
- Compatibility with IP Routing.
- Transparency
- Quality of Service.

Introduction to Mobile IP

- Mobile IP: an Internet Engineering Task Force (IETF) standard protocol which allows users to keep their own IP addresses even though they move from one network to the other.
- (RFC 2002): Charles Perkins
  - Nodes to continue to receive datagrams no matter where they happen to be attached to the Internet.
- Goals:
  - Host to stay connected to the Internet regardless of its location.
  - Track a host without needing to change the mobile host’s long-term IP address.
- Additional control messages for managing routing tables.

Mobile IP - Characteristics

- Mobile Host communicates with other nodes after changing its link-layer point of attachment yet without changing its IP address.
- Mobile host communicates with other nodes that do not implement mobile IP.
- All messages exchanged in this framework are authenticated.
- Number of administrative messages minimized.
  - Low Bandwidth factor.
Mobile IP - Characteristics

- No geographical limitation: A user can take a palmtop or laptop computer anywhere without losing connection to home network.

Impact
- Network access is assured at all times and from all locations. Home and local resources would be accessed continuously.
- There would no longer be an excuse for lack of productivity due to lack of connectivity.

IETF Mobile IP: Terminology

- Mobility Agent (MA)
  - Home agent (HA)
  - Foreign agent (FA)
- Mobile Node (MN)
- Correspondent Node (CN)
- Care-of Address (COA)
  - Foreign agent-based COA (FCOA)
  - Colocated COA (CCOA)
- Mobility Binding

Care-of Address

- Care-of-address (COA): An address which identifies mobile node’s current location
  - When Mobile Host acts as a foreign agent, care of address is called co-located care-of Address.
- Home address: A mobile node is always associated a home network where it belongs.
- Mobility Binding: The association of home address with COA, along with the remaining lifetime of that association.
Mobile IP Architecture

Mobile IP Protocol Overview

- Mobile IP is a way of doing three relatively separate functions:
  - Location Discovery/Registration
  - In service (Tunneling)
  - Deregistration

Location Discovery

- The MN is responsible for discovering whether the MN is in a home or foreign network.
  - Agent Advertisement: Internet Router Discovery Protocol (IRDP) message (RFC 1991)
  - Agent Solicitation
  - Time to Live (TTL) set to 1, multicast address, 224.0.0.1, broadcast address, 255.255.255.255
- In the absence of advertisement and solicitation failure, DHCP can be used.
Registration

• Registration is the process by which the mobile host:
  • Requests routing services from a foreign agent.
  • Informs its home agent of its current care of address.
  • Renews registration if it is due to expire (Service time).

Agent Advertisement

Message Format

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Sequence Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration Lifetime</td>
<td>R B H F M G V</td>
<td>Reserved</td>
</tr>
<tr>
<td>Zero or more care of addresses</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Registration Overview

• Registration Request

<table>
<thead>
<tr>
<th>Type</th>
<th>S R D M G N rsv</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Home Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Home Agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Care-of-Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identification</td>
</tr>
</tbody>
</table>
In-Service

• HA accepts datagram on behalf of MN.
• Performs encapsulation, tunnels the datagram to MN’s current location.
• FA/MN decapsulates datagram, and delivers it to the mobile node.
• The home agent will iterate the procedure until the service time expires for the mobile node.
• Proxy ARP: For HA to intercept packets destined to a mobile host.

Delivering Datagrams

• Several methods of encapsulation (tunneling) are available
  – IP-in-IP encapsulation.
  – Minimal Encapsulation.
  – Generic record Encapsulation

IP in IP Encapsulation

• Simply encapsulates the original IP packet within the new IP header
  – decrements TTL by 1, and
  – sets the outer protocol field to 4 (IP-in-IP)
  – no support for IP fragmentation (path MTU discovery)
  – doubles IP packet sizes
Minimal Encapsulation

- Used to avoid the repetition of the IP fields.
- The original IP header is modified as shown in Figure. The protocol field is set to 55 (min. encaps)

Deregistration

- Deregistration involves MN dropping its COA after returning back to its home network.
- Request sent to HA.
- There is no need to deregister with the foreign agent because the service expires automatically when the service time expires.
Mobile IP Setup

- CN-MN Packet: Intercepted by HA (Proxy ARP) (Steps 1&2)
- Tunneling: Outer header: HA-FA, Inner Header: CN-MN (Step 3)
- Decapsulation at FA, Original Packet delivered to MN. (Step 4)
- Response from MN sent to CN using normal routing procedures. (5, 6 & 7)

Problems with Base Mobile IP

1. Dogleg Routing
   - Worst Case: When MN moves to the same Subnetwork as its CN
   - Fix: Route Optimization
     - Provides Binding Cache keeping track of MN
     - Supports Previous FA's Notification of MN's New Location

2. Wasteful Duplication in "IP in IP"
   - Encapsulation Overhead: Final Datagram = IPH + IPH + Payload
   - Fix: Minimal Encapsulation Scheme
Problems with Base Mobile IP

3. **Single Home Agent Model**: The dependence in Mobile IP on a fixed HA reduces fault tolerance.
   - Even though Simple and Easy, it is fragile
   - Fix: Supports Multiple Home Agents

4. **Unbearable Frequent Report to HA if MN moves frequently**
   - Fix: Supports FA Clustering: Only Inter-Cluster Moves are notified

Route Optimization

- With HA authorization, the CN can keep the binding cache of the MN home address and the COA.
- Within its lifetime, the CN can send messages directly to the COA rather than the HA.
- MN movement.
- Binding update.

Reverse Tunneling

- Used to address the firewall traversal problem.
- Typically, a firewall does not allow an outgoing packet whose source address is different from its network addresses.
- It is unusual to have outgoing and incoming packets in different paths.
- Solution is reverse tunneling: Instead of sending the packets directly to the CN, the MN sends the packets back to the HA, and then the HA forwards them to the CN
Reverse Tunneling

Tunnel Management

- Tunnel management involves maintaining Tunnel Soft State Information about a tunnel to enable more timely use of the tunnel, especially, including management of transient tunnel error conditions.
  - Idea: To return accurate ICMP messages to the sender.
- ICMP messages:
  - Datagram too big.
  - Time exceeded.
  - Destination Unreachable.
  - Source Quench.

Tunnel Soft State

- Soft state information:
  - MTU of tunnel
  - TTL (path length) of tunnel.
  - Ability to reach end of tunnel.
- ICMP messages received from the interior of tunnel updates the soft state of the tunnel at the encapsulator.
- Encapsulator might send ICMP for subsequent datagrams.
  - Example: TTL case.
Tunnel Soft State

- Tunnel MTU Discovery: ICMP datagram too big message.
  - Don’t Fragment (DF) option.
- Case 1: Source of the unencapsulated datagram is doing MTU discovery.
- Case 2: Source of the unencapsulated datagram is not doing MTU discovery.

Location Management

- Location Management is to identify the current location of a mobile node and keep track of its changes as it moves on.
  - For call setup process.

  **Key Questions**
  - How does network know where intended recipient of a message is currently located?
  - Where should information about current location of a mobile node be stored?
  - Who should be responsible for determining mobile node’s location?

Location Management

- Solutions based on Push or Pull based strategies.
- In Mobile IPv4, Home Agent (HA) and Foreign Agent (FA) are employed for location management.
  - HA address.
  - FA address.
- The HA maintains the Mobility binding.
- It’s a push based strategy.
Location Management

- Location management involves Handover Management.
- Handover Management: To provide mobile nodes for seamless handover, whenever they move into different IP network regions during a session.
  - Service disruption issues
  - Was not supported in the initial base Mobile IP specification.

Foreign Agent Smooth Handoff

- Handover management provides a means for MN’s previous FA to be reliably notified of MN’s current location (New mobility binding).
  - Datagram recovery.
  - Resource release.

Concerns about Mobile IP

- **Quality of Service (QOS)**
  - Encapsulation Issues.
- **Multicast support**
  - Bi directional Tunneling
  - Remote subscription.
- **Security**: Use of IPSec. (Use of AH and ESP headers)
  - Denial of service attack
  - Replay attack
  - Passive eavesdropping.
Concerns about Mobile IP

- **Voice over Mobile IP**: End-to-end delay, delay jitter, and packet loss.
  - Handoff delay performance.

Mobile IP Availability

- **Solaris Mobile IP**
  - Linux OS.
- **MosquitoNet Research Group (Stanford University)**
  - Linux OS.
- **Monarch Research Project (CMU)**
  - Free Mobile IP implementation.
- **Portland State Secure Mobile Networking Project**
  - Use if IPSec for Mobile IP.
- **Hierarchical Mobile IP**

Mobile IP Availability

- Most commercial vendors support Mobile IP.
  - Cisco, Nokia, Siemens, HP.
- Mobile IP client services, providers
  - Birdstep Intelligent Mobile IP Client v2.0, Universal Edition
  - Internet Mobility Management with Secco Mobile IP
  - ipUnplugged
Other Mobile IP Schemes

- Several schemes have been proposed:
  - Columbia Proposal (Ioannidis and Maguire from Columbia University)
  - IBM Proposal
  - Sony’s virtual IP Proposal
  - Cellular IP
  - Hierarchical Mobile IP.

Columbia Mobile IP Scheme

- Mobile Host (MH): A host or router that changes its point of attachment from one network or subnetwork to another.
- Campus (Mobile subnet): A collection of physical networks called cells under an administrative domain (e.g., a business network or a university campus).
- Hosts move within campus without changing their logical IP address based on subnet address.
- Supports micro mobility.

Columbia Mobile IP Scheme

- The campus consists of several Mobility Support Routers (MSRs) exchanging information about which mobiles are where, tunnel datagrams between them for host-to-host communication and so on.
- Two addresses associated with a mobile host: A logical address and a physical location address.
  - Logical: Permanent
  - Physical: Current location. (MSR’s address)
  - Binding maintained at current MSR.
Columbia Mobile IP Scheme

- Intra-Campus moves: Logical identifier of mobile host remains the same, only the binding changes.
- Inter-campus moves: Logical identifier of mobile host changes and it needs to acquire a temporary address.

Search
- Send a message to all MSRs to check if MH is registered. (WHOHAS message). MSR with which MH is registered responds. (IHAVE message).

Columbia Mobile IP Scheme

- When MH moves and registers with new MSR, it is its responsibility to inform the new MSR about its previous MSR. Forward Pointer Message (FWDPTR).
- Inter campus moves: Similar to IETF Mobile IP scheme