Mobility management in IP networks & Mobile IP

Lecture slides for S-38.3192
22.2.2007
Mika Ilvesmäki

Learning goals in Mobility Management & Mobile IP

- After this lecture you will know
  - Reasons why mobility and its management are not straightforward tasks in the Internet
  - What are the mobility problems, mobility design guidelines and mobility management tasks
  - How Mobile IP works and what enhancements have been proposed (and what additional functionality they introduce)
  - How different traffic types are forwarded in Mobile IP –environment

- After reading the article “An Evaluation of Current QoS solutions for Mobile IP networks” by Agarwal et al. you will be able to
  - List and briefly explain the challenges that QoS solutions face in the Mobile IP environment
  - List and briefly explain the shortcomings of using standard RSVP-protocol in Mobile IP environment
  - List and briefly explain the advantages and disadvantages of using advance resource reservation –solutions in Mobile IP –environment
General notes on mobility

- Mobility in communications consists of various technologies and aspects
  - Wireless transmission
    - Using the frequency space
      - Multiplexing, modulation, spread spectrum, cellular systems
  - Medium access control
    - SDMA, FDMA, TDMA, CDMA
  - Communication systems
    - GSM, DECT, TETRA, UMTS, Satellite systems, Broadcast systems
- Mobility may occur on 1) Access-level (OSI 2), 2) Network-level (OSI 3) 3) Transport-level (OSI 4)

What is mobility?

- A node moving from a location to another L2 location while preserving its original (IP) address
  - Horizontal handover in the IP level regardless that we (most probably) need vertical handover in layer 2.
    - Different layer 2 networks are (usually) separated by routers (or gateways)
  - The problem: IP address identifies 1) (to a large degree) the host identity and 2) the host location.
- On the border of different layer 2 networks the change of IP address has to be notified
  - For instance when moving from WLAN to GPRS
  - This would be YAP (Yet Another Protocol)
    - and most probably it would also break up TCP connection state
Types of mobility

- Global mobility
  - (interdomain) movement across different domains
- Macro mobility
  - (intradomain) movement across different subnets within domain
- Micro mobility
  - (intrasubnet) movement within subnet

Mobility challenges

1. Locating the mobile host or service
   - address discovery (location)
2. Preserving connectivity
   - although location may change (tracking)
3. Controlled disconnectivity
   - file systems can do this
4. Controlled stand-by
5. Quick resume of communications
   - without unnecessary data lost
What moves? Services or users

• Service mobility
  – User moves and connects to his home network with arbitrary devices
    • VPNs, secure connections, WWW-mail services, etc.

• User mobility
  – User and the device moves and connects to his home network
    • Use of all home network services
    • Appearing to be in the home network

Why mobility in IP?

• Need to change physical media without breaking (TCP) connections
• People want Wireless Network Access
  – Ease and economy of operation
• Continuous connectivity
• Home network addressable from the entire Internet
Host routes – the easy solution?!

• Spread knowledge on the movements to all Internet routers
  – Assign a new address to the mobile node as it moves
  – This solution does not scale, overload of networks with location information exchange

• We need to restrict the circulation of location and IP address information to a minimum!
  – Location independent identifier

Mobility design guidelines

• No modifications to (other) host operating systems
• Internet-wide mobility calls for a scalable solution
  – and preferably infrastructure independency
• Application transparency, seamless transitions
• No modifications to Internet routing
  – mobility solution needs to have location/mobility mgmt, host routes are not an option in the Internet
• Compatibility with Internet Addressing
• No additional vulnerabilities should be introduced
• Independence of layers (do not assume that L3 and L2 addresses are related).
• Handle disconnections properly
• Support mobility at the edge devices
  – Do not assume proxies exist
Mobility management

• Location management
  – registration and location updates
  – to enable a network to discover the current location of a mobile node (MN)
  – Location-independent identifier (IP address, hostname, some other host id)
• Handoff management
  – to enable a network to maintain a connection while MN moves its location in the network

Mobile IP standards

• Mobile IP is an IETF effort
  – dealt with in several workgroups
• Mobile IP is defined in IETF standards
  – See also, RFC 1701 (GRE) and RFC 1321.
• Standards define
  – Agent discovery
  – Registration procedure
  – Tunneling
• Mobile IP is not widely used because of DHCP and VPNs provide email and web-access and NAT and firewalls block the Mobile IP functionality
Movement detection

- MN detects Home/Foreign Agent-advertisements (modified RFC 1256)
  - or solicits for a H/FA presence (unmodified RFC 1256)
    - H/FA advertisement = extended ICMP
    - Sequence numbers used to detect need for re-registration
- If no advertisements/solicitations answered
  - send ICMP to home router (check TTL!)
  - assume foreign network and try to obtain an address using DHCP or configure IP address manually
  - then register with Home Agent

Mobile IP components

- Mobile and correspondent nodes
- Foreign Agents (IPv4 only)
- Home Agents
- Tunnels
- Care-of- addresses
Tunneling

- Tunnel is a path followed by packet that is encapsulated within another packet’s payload
  - Put (IP) packets inside IP packets
    - avoid standard unicast routing
    - use other protocols in the Internet
  - Tunnels are defined manually
  - Tunnels reduce the MTU
  - Tunnel faults are hard to detect
- Tunneling techniques are several
  - IPinIP (RFC 2003, default), MinIP (RFC 2004), GRE (RFC 1701 & 1702) etc.

Home agent

- Router for the home network
- Mobility service providing agent
  - access to the home address of the mobile node without mobile node’s presence.
- Advertise routing info on demand
  - to home network, and to other nodes
- Tunnels packets to mobile node (or foreign agent)
Mobile IP basic features

- Only the Home Agent knows where you are
  - This solution scales better
- With tunneling one is able
  - to forward packets from HomeAgent to MobileNode
    - And back, if necessary
  - to appear to be in one’s home network
- Security is required but not restricted
  - The four building blocks
    - Confidentiality, Authentication, Integrity, Non-repudiation

Mobile IP transforms the mobility problem into a routing problem!

Triangle routing and reverse tunneling

- CN sends to MN and traffic flows via HA (1., 2. and 3.)
- MN to CN
  - traffic may take the shortest path (4.)
  - If ingress filtering is in effect the traffic may be dropped
    - Solution: Reverse tunneling (5.)
      - Result: triangle routing with CN, HA and MN
New route advertisements

- Home agent knows the true location of the MN
  - HA sends redirects to correspondent nodes (avoid triangle routes)
  - HA sends newFAinfo to oldFA and make oldFA redirect packets

Traffic forwarding – home network

- Home Agent intercepts packets sent to the Mobile Node and sends the packets tunneled to the MN
- How about home network ARP requests?
  - What about cached ARP-replies?
    - Registration request & reply
Traffic forwarding – Internet

- Home Agent intercepts packets sent to the Mobile Node and sends the packets tunneled to the MN
- ARP requests outside of the home network are answered with HA L2 address
  - proxyARP aka Gratuitous ARP

Multicast

- Multicasts are sent to the
  - Multicast router
    - No encapsulation/tunneling needed
  - HA that should have multicast routing capability
    - encapsulated and tunneled to the HA
  - Multicast is received
    - normally as a group member (co-located address)
    - via HA as encapsulated/tunnelled packets
      - may require recursive encapsulation
Mobile IPv6

- MN creates its own CoA with automatic address configuration
  - Stateful: DHCPv6
  - Stateless: Local subnet prefix as in Neighbor Discovery (RFC 2461, IPv6 ARP) + own hardware address
- MN may notify its correspondents when it moves (no more triangular routing)
- Correspondents put CoA in routing headers
- HA encapsulates packets if it gets them
- Binding updates carried in Destination Option

IPv4 vs. IPv6 and mobility

IPv4
1. MN, HA
2. MN home address
3. Foreign Agent
4. FA CoA/CoCoA
5. Address from
   1. Agent discovery
   2. DHCP
   3. Manually
6. Agent discovery
7. Tunneling
8. Routes optimized by a separate protocol

IPv6
1. MN, HA
2. Global home address and link-local address
3. Plain IPv6 router
4. All colocated CoAs
5. Address from
   1. Auto-configuration
   2. DHCPv6
   3. Manually
6. Router discovery (ICMPv6)
7. Source routing (option) or tunneling
8. Integrated route optimization
### Mobility protocols in the Internet

<table>
<thead>
<tr>
<th>Mobility</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global mobility</td>
<td>Mobile IP (MIP)</td>
</tr>
<tr>
<td></td>
<td>TR45.6 (WIPNA)</td>
</tr>
<tr>
<td></td>
<td>Mobile IPv6</td>
</tr>
<tr>
<td>Global/macro mobility</td>
<td>HMIP</td>
</tr>
<tr>
<td></td>
<td>HMIPv6</td>
</tr>
<tr>
<td></td>
<td>TeleMIP</td>
</tr>
<tr>
<td></td>
<td>DMA</td>
</tr>
<tr>
<td>Macro</td>
<td>HAWAII</td>
</tr>
<tr>
<td>Micro</td>
<td>TIMIP</td>
</tr>
<tr>
<td></td>
<td>CIP</td>
</tr>
</tbody>
</table>

### Global/macro mobility

- Mobile IP, Mobile IPv6
  - more details earlier
- Hierarchical MIP, HMIPv6
  - introduces hierarchy in FAs, establishes a tunnel from the MN to a gateway FA. Packet to MN travel thru this tunnel
  - MAP (mobility anchor point) acts as a local HA for a certain domain
    - MAP receives packets for the MN and forwards them to the link CoA
    - As long as MN is within the MAP influence the global CoA stays the same
- HAWAII (Handoff-Aware Wireless Access Internet Infrastructure)
  - Mixes the concepts of co-located CoA and FA CoA, no private address support
  - Local handovers by sending registration to base stations (FA)
Macro/Micromobility

• Cellular IP, CIP
  – Local handovers without renewed registration with CIP gateway
    • Requires changes into Mobile IP protocols
    • Not transparent to existing systems
    • Easy to manage, self-configuring
    • Packets forwarded via multiple paths, routing tables changed by mobile nodes -> not secure

• TIMIP (Terminal Independent Mobile IP)
  – Combination of CIP, HAWAII and MIP

IP & Mobility summary

• True mobility is not built-in in the Internet
  – Mobile IP handles the task somehow, and other protocols support.

• Implicit solution: Applications have developed to a direction where true mobility is not needed.

• Waiting for the killer app…