8. Network Protocols and Mobile IP

Ad-hoc Networks, Routing
Micro-mobility: Cellular IP, HAWAI
Macro-mobility: DHCP, Mobile IP
Registration, Encapsulation, Tunneling, Security
IPv4 versus IPv6

Motivation for a Mobility-supported Network

- **Routing:**
  - Based on an IP destination address, the network prefix (e.g., 137.193.63) determines the physical subnet
  - Change of physical subnet implies change of IP address to obtain a topological correct address (standard IP) or needs special entries in routing tables

- **Specific routes to end-systems?**
  - Change of all routing table entries to forward packets to the right destination required
  - Does not scale with the number of mobile hosts and frequent changes in the location
  - Security problems

- **Changing the IP address?**
  - Adjust the host IP address depending on the current location
  - Almost impossible to find a mobile system, DNS updates take a too long time
  - TCP connections break, security problems

Mobile ad-hoc Networks

- Standard Mobile IP (cf. later) needs an infrastructure:
  - Home Agent/Foreign Agent in the fixed network
  - DNS, routing are not designed for mobility
- Sometimes there is no infrastructure!
  - Remote areas, ad-hoc meetings, disaster areas
  - Cost can also be an argument against an infrastructure
- Main topic is routing:
  - No default router available
  - Every node should be able to forward

Manet: Mobile Ad-hoc Networking

Routing Examples for an Ad-hoc Network

- **Distance Vector (IP example RIP):**
  - Periodic exchange of messages with all physical neighbors that contain information about who can be reached at what distance
  - Selection of the shortest path if several paths available

- **Link State (IP example OSPF):**
  - Periodic notification of all routers about the current state of all physical links
  - Routers get a complete picture of the network

Example:
- ARPA packet radio network (1973), DV-Routing
- Every 7.5 s exchange of routing tables including link quality
- Updating of tables also by reception of packets
- Routing problems solved with limited flooding
Problems of Traditional Routing Algorithms

- Dynamic of the topology:
  - Frequent changes of connections, connection quality, participants

- Limited performance of mobile systems:
  - Periodic updates of routing tables need energy without contributing to the transmission of user data, sleep modes difficult to implement
  - Limited bandwidth of the system is reduced even more due to the exchange of routing information
  - Links can be asymmetric, i.e., they can have a direction-dependent transmission quality

- Key problem:
  - Protocols have been designed for fixed networks with infrequent changes and typically assume symmetric links!

DSDV (Destination Sequenced Distance Vector)

- Early work:
  - On-demand version: AODV (Ad-hoc On-demand Distance Vector)

- Expansion of distance vector routing

- Sequence numbers for all routing update packets:
  - Assures in-order execution of all updates
  - Avoids loops and inconsistencies

- Decrease of update frequency:
  - Store time between first and best announcement of a path
  - Inhibit update, if it seems to be unstable (based on the stored time values)

Dynamic Source Routing (1)

- Split routing into discovering a path and maintaining a path

- Discover a path:
  - Only if path for packets to a certain destination is needed and no path available

- Maintaining a path:
  - Only while path is in use one has to make sure that it can be used continuously

- No periodic updates needed!

- Path discovery:
  - Broadcast a packet with destination address and unique ID
  - If a station receives a broadcast packet
    - If the station is the receiver (i.e., has the correct destination address) then return the packet to the sender (path was collected in the packet)
    - If the packet has already been received earlier (identified via ID) then discard the packet
    - Otherwise, append own address and broadcast packet
  - Sender receives packet with the current path (address list)

Dynamic Source Routing (2)

- Optimizations:
  - Limit broadcasting if maximum diameter of the network is known
  - Caching of address lists (i.e. paths) with help of passing packets:
    - Stations can use the cached information for path discovery (own paths or paths for other hosts)

- Maintaining paths:
  - After sending a packet:
    - Wait for a layer 2 acknowledgement (if applicable)
    - Listen into the medium to detect if other stations forward the packet (if possible)
    - Request an explicit acknowledgement
  - If a station encounters problems it can inform the sender of a packet or look-up a new path locally

Mobility on the Network Layer

- User mobility and device mobility

- Distance-driven mobility dimensions:
  - Micro mobility:
    - Mobile nodes move within a single domain (determined by a logical view of sub-networks managed by a single administration)
    - Support of fast and seamless hand-over between access points
    - Reduction of traffic load in backbone network
    - Examples: Cellular IP, HAWAII, Hierarchical Mobile IP, Fast Handoff, ...
  - Macro mobility:
    - Mobile nodes move between domains, where each domain is concatenated by an IP network
    - Examples: Dynamic Host Configuration Protocol (DHCP), Mobile IP (MIP)
    - Distinction not completely clear:
      - Two networks in which a node moves (macro mobility) may be concatenated to achieve a single logical network (micro mobility)

  - Important criteria: Security, Efficiency, Scalability, Transparency, Manageability

Cellular IP

- Operation:
  - "CIP Nodes" maintain routing entries (soft state) for Mobile Nodes (MN)
  - Multiple entries possible
  - Routing entries updated based on packets sent by MN

- CIP Gateway:
  - Mobile IP tunnel endpoint
  - Initial registration processing

- Security provisions:
  - All CIP Nodes share "network key"
  - MN key: MD5 (net key, IP address)
  - MN gets key upon registration
Cellular IP: Security

- Advantages:
  - Initial registration involves authentication of MNs and is processed centrally by CIP Gateway
  - All control messages by MNs are authenticated
  - Replay-protection (using timestamps)

- Potential problems:
  - MNs can directly influence routing entries
  - Network key known to many entities (increases risk of compromise)
  - No re-keying mechanisms for network key
  - No choice of algorithm (always MD5, prefix+suffix mode)
  - Proprietary mechanisms (not, e.g., IPSec AH)

Cellular IP: Other Issues

- Advantages:
  - Simple and elegant architecture
  - Mostly self-configuring (little management needed)
  - Integration with firewalls / private address support possible

- Potential problems:
  - Not transparent to MNs (additional control messages)
  - Public-key encryption of MN keys may be a problem for resource-constrained MNs
  - Multiple-path forwarding may cause inefficient use of available bandwidth

HAWAII

- Operation:
  - MN obtains co-located COA and registers with HA
  - Handover: MN keeps COA, new BS answers Reg. Request and updates routers
  - MN views BS as foreign agent

- Security provisions:
  - MN-FA authentication mandatory
  - Challenge/Response Extensions mandatory

HAWAII (Hand-off-aware Wireless Access Internet Infrastructure)

- Advantages:
  - Mutual authentication and C/R extensions mandatory

- Potential problems:
  - Co-located COA raises DHCP security issues (DHCP has no strong authentication)
  - Decentralized security-critical functionality (Mobile IP registration processing during handover) in base stations
  - Authentication of HAWAII protocol messages unspecified (potential attackers: stationary nodes in foreign network)
  - MN authentication requires PKI or AAA infrastructure

HAWAII: Other Issues

- Advantages:
  - Mostly transparent to MNs (MN sends/receives standard Mobile IP messages)

- Potential problems:
  - Mixture of co-located COA and FA concepts may not be supported by some MN implementations
  - No private address support possible because of co-located COA

Hierarchical Mobile IPv6 (HMIPv6)

- Operation:
  - Network contains mobility anchor point (MAP)
    - Mapping of regional COA (RCOA) to link COA (LCOA)
    - Upon handover, MN informs MAP only
    - Gets new LCOA, keeps RCOA
    - HA is only contacted if MAP changes

- Security provisions:
  - No HMIPv6-specific security provisions
  - Binding updates should be authenticated
Hierarchical Mobile IP: Security

- Advantages:
  - Local COAs can be hidden, which provides some location privacy
  - Direct routing between CNs sharing the same link is possible (but might be dangerous)

- Potential problems:
  - Decentralized security-critical functionality (handover processing) in mobility anchor points
  - MNs can (must!) directly influence routing entries via binding updates (authentication necessary)

Hierarchical Mobile IP: Other Issues

- Advantages:
  - Handover requires minimum number of overall changes to routing tables
  - Integration with firewalls/private address support possible

- Potential problems:
  - Not transparent to MNs
  - Handover efficiency in wireless mobile scenarios:
    - Complex MN operations
    - All routing reconfiguration messages sent over wireless link

DHCP: Dynamic Host Configuration Protocol

- Application:
  - Simplification of installation and maintenance of networked computers
  - Supplies systems with all necessary information, such as IP address, DNS server address, domain name, subnet mask, default router
  - Enables automatic integration of systems into an Intranet or the Internet, can be used to acquire a COA for Mobile IP

- Client/Server-Model:
  - The client sends via a MAC broadcast a request to the DHCP server (might be via a DHCP relay)

DHCP Protocol Mechanisms

- Server:
  - Several servers can be configured for DHCP, coordination not yet standardized (i.e., manual configuration)

- Renewal of configurations:
  - IP addresses have to be requested periodically, simplified protocol

- Options:
  - Available for routers, subnet mask, NTP (network time protocol) timeserver, SLP (service location protocol) directory, DNS (domain name system)

- Big security problems:
  - No authentication of DHCP information specified

DHCP Characteristics

- Server:
  - Several servers can be configured for DHCP, coordination not yet standardized (i.e., manual configuration)

- Renewal of configurations:
  - IP addresses have to be requested periodically, simplified protocol

- Options:
  - Available for routers, subnet mask, NTP (network time protocol) timeserver, SLP (service location protocol) directory, DNS (domain name system)

- Big security problems:
  - No authentication of DHCP information specified

Requirements to Mobile IP (RFC 3220, old 2002)

- Transparency:
  - Mobile end-systems keep their IP address
  - Continuation of communication after interruption of link possible
  - Point of connection to the fixed network can be changed

- Compatibility:
  - Support of the same layer 2 protocols as IP
  - No changes to current end-systems and routers required
  - Mobile end-systems can communicate with fixed systems

- Security:
  - Authentication of all registration messages

- Efficiency and scalability:
  - Only little additional messages to the mobile system required (connection typically via a low bandwidth radio link)
  - Worldwide support of a large number of mobile systems in the whole Internet
Terminology

- **Mobile Node (MN):**
  - System (node) that can change the point of connection to the network without changing its IP address
- **Home Agent (HA):**
  - System in the home network of the MN, typically a router
  - Registers the location of the MN, tunnels IP datagrams to the COA
- **Foreign Agent (FA):**
  - System in the current foreign network of the MN, typically a router
  - Forwards the tunneled datagrams to the MN, typically the default router for MN
- **Care-of Address (COA):**
  - Address of the current tunnel end-point for the MN (at FA or MN)
  - Actual location of the MN from an IP point of view
  - Can be chosen, e.g., via DHCP
- **Correspondent Node (CN):**
  - Communication partner

Example Network

Data Transfer to the Mobile System

1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

Data Transfer from the Mobile System

1. Sender sends to the IP address of the receiver as usual, FA works as default router

Overview

- **Agent Advertisement:**
  - HA and FA periodically send advertisement messages into their physical sub-nets
  - MN listens to these messages and detects, if it is in the home or a foreign network (standard case for home network)
  - MN reads a COA from the FA advertisement messages
- **Registration (always limited lifetime):**
  - MN signals COA to the HA via the FA, HA acknowledges via FA to MN
  - These actions have to be secured by authentication
- **Advertisement:**
  - HA advertises the IP address of the MN (as for fixed systems), i.e., standard routing information
  - Routers adjust their entries, these are stable for a longer time (HA responsible for a MN over a longer period of time)
  - Packets to the MN are sent to the HA,
  - Independent of changes in COA/FA

Network Integration
Agent Advertisement

<table>
<thead>
<tr>
<th>0</th>
<th>7</th>
<th>8</th>
<th>15</th>
<th>16</th>
<th>23</th>
<th>24</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>code</td>
<td>code</td>
<td>checksum</td>
<td>registration lifetime</td>
<td>address 1</td>
<td>preference level 1</td>
<td>reserved</td>
</tr>
<tr>
<td>type = 16</td>
<td>length = 6 + 4 * #COAs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R: registration required</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B: busy, no more registrations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H: home agent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F: foreign agent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M: minimal encapsulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G: GRW encapsulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>r: =0, ignored (former Van Jacobson compression)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T: FA supports reverse tunneling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>reserved: =0, ignored</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Mobile IP Registration Request

<table>
<thead>
<tr>
<th>0</th>
<th>7</th>
<th>8</th>
<th>15</th>
<th>16</th>
<th>23</th>
<th>24</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>code</td>
<td>home address</td>
<td>COA</td>
<td>identification</td>
<td>extensions . . .</td>
<td></td>
<td></td>
</tr>
<tr>
<td>type = 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S: Simultaneous bindings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B: Broadcast datagrams</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D: De-capsulation by MN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M: Minimal encapsulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G: GRE encapsulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>r: =0, ignored</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T: reverse tunneling requested</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>x: =0, ignored</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Mobile IP Registration Reply

<table>
<thead>
<tr>
<th>0</th>
<th>7</th>
<th>8</th>
<th>15</th>
<th>16</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>code</td>
<td>home address</td>
<td>lifetime</td>
<td>extensions . . .</td>
<td></td>
</tr>
<tr>
<td>type = 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example codes:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>registration successful</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 registration accepted</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 registration accepted, but simultaneous mobility bindings unsupported</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>registration denied by FA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>65 administratively prohibited</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>66 insufficient resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>67 mobile node failed authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>68 home agent failed authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>69 requested Lifetime too long</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>registration denied by HA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>129 administratively prohibited</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>131 mobile node failed authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>133 registration identification mismatch</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>135 too many simultaneous mobility bindings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Encapsulation Principle

- Encapsulation of one packet into another as payload:
  - E.g., IPv6 in IPv4 (6Bone), Multicast in Unicast (Mbone)
  - Here: e.g., IP-in-IP-encapsulation, minimal encapsulation or GRE (Generic Record Encapsulation)
- IP-in-IP-encapsulation (mandatory, RFC 2003):
  - Tunnel between HA and COA

Encapsulation (1)

<table>
<thead>
<tr>
<th>0</th>
<th>15</th>
<th>16</th>
<th>23</th>
<th>24</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>source address</td>
<td>destination address</td>
<td>total length</td>
<td>identification</td>
<td>flags</td>
<td>fragment offset</td>
</tr>
<tr>
<td>TTL</td>
<td>protocol</td>
<td>IP checksum</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Encapsulation (2)

- Minimal encapsulation (optional, RFC 2004):
  - Avoids repetition of identical fields
  - E.g., TTL, IHL, version, DS (RFC 2474, old: TOS)
  - Only applicable for not fragmented packets, no space left for fragment identification

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address of MN</td>
</tr>
<tr>
<td>TTL</td>
<td>IP address of FA</td>
</tr>
<tr>
<td>IP ID</td>
<td>TCP/UDP/IP header</td>
</tr>
<tr>
<td>Flags</td>
<td></td>
</tr>
<tr>
<td>Fragment Off</td>
<td>TCP/UDP/IP header</td>
</tr>
<tr>
<td>Length</td>
<td>TCP/UDP/IP header</td>
</tr>
<tr>
<td>DS</td>
<td>TCP/UDP/IP header</td>
</tr>
<tr>
<td>Ver</td>
<td>TCP/UDP/IP header</td>
</tr>
<tr>
<td>IHL</td>
<td>TCP/UDP/IP header</td>
</tr>
</tbody>
</table>

Generic Routing Encapsulation

Optimization of Packet Forwarding

- Triangular Routing:
  - Sender sends all packets via HA to MN
  - Higher latency and network load

- Solutions:
  - Sender learns the current location of MN
  - Direct tunneling to this location
  - HA informs a sender about the location of MN
  - Big security problems!

- Change of FA:
  - Packets on-the-fly during the change can be lost
  - New FA informs old FA to avoid packet loss, old FA now forwards remaining packets to new FA
  - This information also enables the old FA to release resources for the MN

Change of Foreign Agent

Mobile IP with Reverse Tunneling

- Router accept often only "topological correct" addresses (firewall!):
  - A packet from the MN encapsulated by the FA is now topological correct
  - Furthermore multicast and TTL problems solved (TTL in the home network correct, but MN is too far away from the receiver)

- Reverse tunneling does not solve:
  - Problems with firewalls, the reverse tunnel can be abused to circumvent security mechanisms (tunnel hijacking)
  - Optimization of data paths, i.e. packets will be forwarded through the tunnel via the HA to a sender (double triangular routing)

- The standard is backwards compatible:
  - Those extensions can be implemented easily and cooperate with current implementations without these extensions
  - Agent Advertisements can carry requests for reverse tunneling
Mobile IP and IPv6

- Mobile IP was developed for IPv4, but IPv6 simplifies the protocols:
  - Security is integrated and not an add-on, authentication of registration is included
  - COA can be assigned via auto-configuration (DHCPv6 is one candidate), every router performs router advertisement which can be used instead of the special agent advertisement; addresses are always co-located
  - MN can signal a sender directly the COA, sending via HA not needed in this case (automatic path optimization)
  - "Soft" hand-over, i.e. without packet loss, between two subnets is supported:
    - MN sends the new COA to its old router
    - The old router encapsulates all incoming packets for the MN and forwards them to the new COA
  - Authentication is always granted

Problems with Mobile IP

- Security:
  - Authentication with FA problematic, for the FA typically belongs to another organization
  - No protocol for key management and key distribution has been standardized in the Internet
  - Patent and export restrictions
- Firewalls:
  - Typically mobile IP cannot be used together with firewalls, special set-ups are needed (such as reverse tunneling)
  - Tunneling makes it hard to give a flow of packets a special treatment needed for QoS
- QoS:
  - Many new reservations in case of RSVP
  - Tunneling makes it hard to give a flow of packets a special treatment needed for QoS

Security in Mobile IP

- Security requirements (Security Architecture for the Internet Protocol, RFC 1825):
  - Integrity: any changes to data between sender and receiver can be detected by the receiver
  - Authentication: sender address is really the address of the sender and all data received is really data sent by this sender
  - Confidentiality: only sender and receiver can read the data
  - Non-Repudiation: sender cannot deny sending of data
  - Traffic Analysis: creation of traffic and user profiles should not be possible
  - Replay Protection: receivers can detect replay of messages

IP Security Architecture (1)

- Two or more partners have to negotiate security mechanisms to setup a security association:
  - Typically, all partners choose the same parameters and mechanisms
  - Two headers have been defined for securing IP packets:
    - Authentication-Header:
      - Guarantees integrity and authenticity of IP packets
      - If asymmetric encryption schemes are used, non-repudiation can also be guaranteed
    - Encapsulation Security Payload
      - Protects confidentiality between communication partners

    IP Security Architecture (2)

- Mobile Security Association for registrations:
  - Parameters for the mobile host (MH), home agent (HA), and foreign agent (FA)
- Extensions of the IP security architecture:
  - Extended authentication of registration
    - MH-FA Authentication
    - HA-FA Authentication
    - MH-RA Authentication
    - HA-RA Authentication
  - Prevention of replays of registrations:
    - Time stamps: 32 bit time stamps + 32 bit random number
    - Nonces: 32 bit random number (MH) + 32 bit random number (HA)

Key Distribution

- Home agent distributes session keys
  - Foreign agent has a security association with the home agent
  - Mobile host registers a new binding at the home agent
  - Home agent answers with a new session key for foreign agent and mobile node