Advanced Computer Networks
263-3501-00

Mobility Support

Patrick Stuedi
Spring Semester 2013
Last Week

- **WLAN/802.11**
  - Architecture (Infrastructure / Ad Hoc)
  - Physical layer (OFDM, rate adaption)
  - MAC (CSMA/CA, Polling, Low-power mode)

- **Cellular networks**
  - Principles: capacity and interference vs. cell size
  - GSM architecture
NSS Databases

- **Home Location Register (HLR)**
  - Contains permanent and semi-dynamic data of all subscribers
    - Mobile subscriber ISDN number
    - International mobile subscriber identity (IMSI)
    - Current VLR and MSC
    - Mobile subscriber roaming number (MSRN)
  - This user-specific information exists once for each user in one HLR

- **Visitor Location Register (VLR)**
  - Local (dynamic) database for a subset of the user data
  - Includes data about all users currently in the domain of the VLR
  - When an MS enters into the area of the VLR, the VLR copies all relevant information from the HLR
    - Avoid frequent HLR updates and long-distance signaling with the HLR
  - VLR gets updated at MS startup and then periodically
    - If no update is received by VLR for some time it's considered detached (e.g., roaming, new VLR takes over)
Call Setup (Mobile terminated call)

1: calling a GSM subscriber
2: forwarding call to GMSC
3: signal call setup to HLR
4, 5: request MSRN from VLR
6: forward responsible MSC to GMSC
7: forward call to current MSC
8, 9: get current status of MS
10, 11: paging of MS
12, 13: MS answers
14, 15: security checks
16, 17: set up connection
Call Setup (Mobile originated call)

1, 2: connection request
3, 4: security check
5-8: check resources (free circuit)
9-10: set up call
Handover

- Based on MS and BTS's periodic measurements of downlink and uplink quality
  - Measurements reports sent by the MS every 480 ms
- BSC collects all values from BTS and MS, calculates average and compares it with the \textit{HO\_MARGIN} (handover margin) threshold
  - Helps avoid the ping-pong effect
- Handover coordinated by either BSC or MSC depending on whether MS moves between two cells belonging to different MSCs or not
UMTS – Universal Mobile Telecommunications System

- 3G System
- Released ~2000
- Increased data rates
  - Up to 384 kbit/s (compared to 9.6 kbit/s or 14.4 kbit/s of GSM)
  - Up to 14.4 Mbit/s (in theory) with HSDPA (enhanced UMTS)
    - Best commercially available devices today achieve ~2Mbit/s

- Main difference between UMTS and GSM
  - GSM: FDMA and TDMA
  - UMTS: Uses CDMA

- Similarities between UMTS and GSM
  - UMTS uses GSM infrastructure for user databases and call setup (VLR, HLR, MSC, GMSC)

- UMTS Extensions: HSPA, HSPA+ (higher data rates)
CDMA in UMTS

- **Channelization**
  - Spread signal with orthogonal codes (channelization codes)
  - Increases the bandwidth of the signal
  - Each MS has its own channelization code (CCx)

- **Scrambling**
  - XOR the signal with a orthogonal scrambling code
  - Does not increase the bandwidth
  - Each cell and MS has its own scrambling code (SCx)
CDMA in UMTS: Downlink

- Spread signal for each MS (TN in the figure) with target channelization code
  - Protect different MS from each other
- Add the signals of for different MS
- Multiply with cell specific scrambling code
  - Protect different cells from each other
CDMA in UMTS: Uplink

- Each station spreads its signal with its channelization code...
  - Protect the stations
- ...and additionally multiplies with its spreading code
  - Spreading code needed to produce orthogonal signals even if different stations are not properly synchronized
OVSF codes

- Can be used to generate a set of codes with varying size
- A valid set of codes has the following property:
  For any two codes, neither should be part of the other (orthogonal property)
- Example of a valid code set: (1,-1), (1,1,-1,-1), (1,1,1,1,1,1,1,1,1,1,1),...
- SF = Spreading Factor
**WiMAX and 4G**

- **WiMAX**
  - 802.x compatible
  - Implementation of 802.16 standards
    - 802.16: Fixed Broadband Wireless Access
    - 802.16e: Mobile support (e.g. handover)
  - Increased data rates (compared to UMTS/3G)
  - Supports mobility (mobile WiMAX)
  - Physical layer: Uses OFDM
  - MAC layer: TDM-based, slot assignment based on MS profile, schedule provide to MS by base station
  - Uses 2GHz – 6GHz for mobile WiMAX, 2-66GHz for fixed WiMAX
  - Considered to be 4G

- **LTE**
  - Long Term Evolution
  - Successor of UMTS
  - New radio interface (not like HSDPA which was extending UMTS)
  - Fully packet switched (in contrast to GSM and UMTS which are circuit switched)
  - Uses OFDM
  - Goal: 300 Mbit/s for Download und 75 Mbit/s for Upload
  - Launched by Swisscom 2012
IP Layer in Wireless Systems
Wireless IP Networking
IP in Wireless

- All major wireless technologies run IP
  - 802.11 and WiMAX support IP naturally as they 802.x compatible
  - GSM has GPRS
    - Mobile station attached to IP network through GPSN (Gateway GPRS Support Node)
  - 3G
    - Mobile station attached to IP network through PDSN (Packet Data Serving Node)
  - Even Bluetooth runs IP
    - Bluetooth Network encapsulation protocol (BNEP)
IP/wireless Challenges: Addressing

- Number of mobile devices still grow rapidly
  - More than 6 billion devices (more than three times as many phones as personal computers!)
  - Problem: pressure on the IPv4 address space

http://www.bbc.co.uk/news/technology-19925506

Number of free '/8' networks
Solving the address problem

- Today: Network Address Translation (NAT)
  - Allows to assign private address to mobile phone
  - Problems with NAT: Many applications (e.g., Skype) require nodes behind NAT to be accessible by TCP
  - Solutions:
    - Relay traffic over node with public IP address (used by Skype)
    - NAT traversal (STUN, UDP hole punching, TCP hole punching, etc.)
  - Problems with NAT traversal:
    - There exists a plethora of different NAT types, and not all NAT traversal techniques work for all NAT types
Solving the address problem: NAT

- NAT device does address translation, stores mappings in NAT table
  - Entry per active TCP/UDP port
- Allows assigning private addresses to (mobile) devices but still enable Internet access
- Devices in the local network are not explicitly addressable
IP address changes in 3G networks

- IP of the phone as seen by a server in the Internet
  (locally the devices reported non-routable addresses that did not change)
- Operators have a pool of NAT addresses, bindings change over time

Figure 2: IPs sampled at 1-minute intervals on an HTC Touch Cruise (Left) and an Apple iPhone (Right) on the AT&T network, with radio resets every 30 minutes: all IPs were in the 32.152/13 range. The 16-bit prefix stays constant between resets and the 13-bit prefix across resets.
Problem with NAT Traversal

- Many applications (e.g., Skype, P2P) require nodes behind NAT to be accessible by TCP/UDP

- Solutions:
  - Relay traffic over node with public IP address
  - NAT traversal (STUN, UDP hole punching, TCP hole punching, etc.)

- “Peer-to-Peer Communication Across Network Address Translators”, Bryan Ford, 2005
Relaying in Skype

- Skype had to deal with NAT ever since
  - Now very useful in wireless networks
- One of several options in Skype: relay voice traffic over supernodes (nodes with good data rates and public IP addresses)
Solving the address problem (2)

- Near future: IPv6
  - Many websites have IPv6 enabled (e.g., Facebook, Google)
  - Mobile OS is IPv6 ready (Android, iPhone)
  - Transition to IPv6 for mobile operators is a long winding process
    - IPv4 the thin waist
    - Outdated equipment at provider not supporting IPv6
    - Tunneling (IPv4 over IPv6, IPv6 over IPv4)

- 4G is pushing IPv6 deployment
  - LTE requires IPv6 support for all devices
IP/wireless: Mobility

- IP address changes as the mobile device moves and changes its point of attachment

Problem:
- Active TCP connections break
- DNS too slow: new IP address might be unknown to clients that want to access the mobile node
- Security issues

Solutions:
- In network mobility support in GPRS, UMTS or LTE (GPSN, PDSN, etc.)
- Mobile IP, Mobile IPv6, Hierarchical Mobile IP, etc
- SIP for multimedia applications
Mobile IP: Terminology

- Mobile Node (MN)
  - node changing its point of attachment
- Home Agent (HA)
  - system in the home network of the MN, typically a router
- Foreign Agent (FA)
  - system in the current foreign network of the MN, typically a router
- Correspondent Node (CN)
  - communication partner of MN
- Care-of Address (COA)
  - actual location of the MN from an IP point of view, often equal to the IP address of the FA
Mobile IP: How It Works (1)

Step 1: MN moves from its home network to a new foreign network

Step 1: MN moves from its home network to a new foreign network.
Mobile IP: How It Works (2)

Step 2:
- Rather than adopting a new IP address the MN stays with its old fixed
- MN searches for a foreign agent in the new network and queries the IP address of the foreign agent (COA)

Alternative:
- MN temporarily acquires an additional IP address (e.g., through DHCP) which acts as COA (the topologically correct address)
- MN = FA
Step 3: MN registers the COA with its home agent
Step 4: Any IP packet with destination address set to the old IP address of the MN will be tunneled by the HA to the FA and then forwarded to the MN.
Mobile IP: How It Works (5)

- Step 5: MN sends to the IP of the CN as usual, FA works as default as router
Reverse Tunneling

- **Problem:**
  - The IP address of the MN is topologically incorrect inside the foreign network (remember MN keeps fixed IP)
  - Firewall in foreign network may prevent packets from being transmitted with topologically incorrect source address

- **Solution: Reverse tunneling**
  - Establish a topologically correct reverse tunnel from CoA to HA
  - Outgoing packets tunneled to the HN and then routed to the CN
Mobile IP: Reverse Routing

- Outgoing packets are tunneled back to home agent from where they get forwarded to CN
Enhancements – Efficient Routing and Smooth Handover

Efficient Routing: Problem: Triangular Routing in Mobile IPv4
- Problem: Sender sends all packets via HA to MN
  - high latency and increased network load
- Solution:
  - HA informs the CN about the location of MN
  - CN caches the current COA of the MN for some time
  - CN directly tunnels packets to COA, instead of using HA
  - Problem: Security issues

Smooth handover:
- Problem: MN moves from one FA to another
  - Cached COA (at CN or HA) is outdated
- Solution:
  - the new FA sends a binding update to the old FA
  - the old FA forwards remaining packets to new FA and releases resources for the MN
  - if the old FA receives packets for an MN, but it is not its current FA, it can send a binding warning to the sender of the packet
Example: Efficient Routing and Smooth Handover

- CN
  - Data
  - Binding update
  - Binding ACK
  - Binding warning
  - Binding request
  - Binding update
  - Binding ACK

- HA
  - Data

- FA\text{old}
  - Data
  - Binding update
  - Binding ACK
  - Registration

- FA\text{new}
  - Data
  - Binding update
  - Binding ACK
  - Registration

- MN
  - Data
  - Smooth handover
  - MN changes location

$t$
Mobile IPv6

- No FA needed
  - IPv6 has autoconfiguration (a node can assign itself a topologically valid IPv6 address composed from the network address and its MAC address)
  - Use autoconfiguration to get a topologically correct COA
  - Packets are sent with COA as source address
    - COA is the current source address of the MN in the foreign network
    - No firewall problems
Mobile IP and NAT

- NAT traversal based on port information

Problem:
- MobileIP uses IP-in-IP tunneling between HA and FA
- Not enough information to allows packets to traverse NAT (no port information)

Solution: Extending the registration and tunnel procedure
- Registration message sent using UDP
- HA detects presence of NAT by comparing source IP with CoA
- MN indicates UDP tunneling capability by including the UDP tunneling extension in the registration request (includes the NAT tunnel port number)
- HA sets up UDP tunnel using the NAT tunnel port: packets correctly forwarded to MN
Mobile IP in practice

- First RFC 1996
- For 802.11 or WiMAX IP roaming
- Currently discussed in the context of LTE
- 3G and UMTS essentially have Mobile IP implemented internally
  - Part of PDSN in CDMA2000/3G
  - Part of GGSN in UMTS
- As a mechanism to perform IP handover across different wireless technologies (LTE->UMTS)
Mobility support in VoIP with SIP

- Remember: Mobility support
  - Support transport stack in the presence of changing points of attachment (e.g., changing IP address)

- SIP = Session Initiation Protocol

- Mainly used in VoIP and realtime traffic applications
  - SIP-based VoIP clients: Kphone, Twinkle, Gizmo, etc..

- SIP functionality
  - Call setup, termination, maintenance (e.g. after mobility)

- Standardized (RFCs 3261, 3853, 4320)

- SIP providers
  - Similar like traditional telecommunications provider
  - Have their own telephone number range
  - Provide signaling infrastructure
  - Examples: Sipcall, NetVoIP
SIP Basics

- End users (e.g., phone) identified through
  - SIP URI ('SIP:alice@sipcall.ch'), or through
  - Phone numbers

- SIP works with ENUM which provides a mapping a service for phone numbers to URIs

- SIP methods (or messages)
  - INVITE: Invites a user to join a call
  - ACK: Confirms that a client has received a final response to an INVITE
  - BYE: Terminates a call
  - REGISTER: Let's the system know about the current location of a user
SIP Architecture

- Main components: SIP proxies and location server
- Each end host has its own outbound proxy (provider specific)
  - Gateway for all SIP messages originating from a user
SIP Registration

- Happens periodically (when phone starts or moves)
- SIP user tells SIP server its current location
SIP call setup (SIP INVITE)

- SIP INVITE message has two main tasks
  - Locate the destination device
  - Exchange session parameters (TCP/IP endpoints, protocols, etc.)
SIP INVITE message

- SIP is text based
- Example of an INVITE message (basic part):

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com:5060;branch=z9hG4bK776asdhds
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
```

- Optional part can hold information about the data protocol to be used (e.g., protocol type, code type, etc..)
SIP Mobility

- SIP can handle four cases of mobility
  - Terminal mobility: terminal moves between different subnets
    - Mobile IP supports this as well
  - Personal mobility: the person moves between terminals
  - Service mobility: the person has access to the same services despite their movement between terminals and/or networks
  - Session mobility: the same session is maintained despite the user changing from one device to another
Pre-call mobility

- Captures both terminal and personal mobility
- Support natively by SIP
  - SIP registrar server in knows about the current location of the user
  - Call setup is routed over 'home' proxy of mobile host
  - Data traffic is transmitted directly between CN and MH
Mid-call mobility

- User sends another INVITE request to the CN, without going through any intermediate proxies
- INVITE message contains new location of the mobile host
- Can be used to provide session mobility
SIP mobility vs Mobile IP

- Native mobility support for SIP based applications
  - No need to use Mobile IP
- No tunneling needed (same as Mobile IPv6)
- Resides at the application layer, easier to be installed
- SIP mobility treats personal mobility and terminal mobility the same
- SIP can support changes in location as well as changes in transport specific properties (e.g., change from TCP to UDP) through optional parameters in SIP INVITE
- Not an option for non-SIP based applications
SIP and NAT

- Problem: SIP carries contact endpoints (e.g. IP/Port) in their SIP INVITE message
  - If those endpoints are behind a NAT the data connection cannot be established

- SIP/NAT Solutions
  - STUN
    - Figure out how a device is seen from the Internet
    - SIP Registration with STUN returned IP/port
  - TURN relay
    - Requires to trust a third party
  - Static IP and port forwarding
References

- RFCs 3261, 3853, 4320
- Peer-to-Peer Communication Across Network Address Translators, Bryan Ford, Usenix 2005
- Where’s that Phone?: Geolocating IP Addresses on 3G Networks, Mahesh Balakrishnan, Mohomed, Venugopalan Ramasubramanian, IMC'09
- An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol, Infocom 2006, Henning Schulzrinne
- Application-Layer Mobility Using SIP, Henning Schulzrinne
- Good course about SIP/VoIP from Prof. Gerald Q. "Chip" Maguire at KTH
  - http://www.ict.kth.se/courses/IK2554/VoIP-Coursepage-Fall-2010.html