Mobile Networking Concepts and Protocols

CNT 5517

Some slides are adapted from Dr. Dave Johnson Notes

Dr. Sumi Helal, Ph.D.

Professor

Computer & Information Science & Engineering Department

University of Florida, Gainesville, FL 32611

helal@cise.ufl.edu

Lecture Contents

- Evolution of Mobile Networks
- GSM
- GPRS
- Mobile IP
- Wireless IP
- QoS Issue

Mobile Networking Evolution

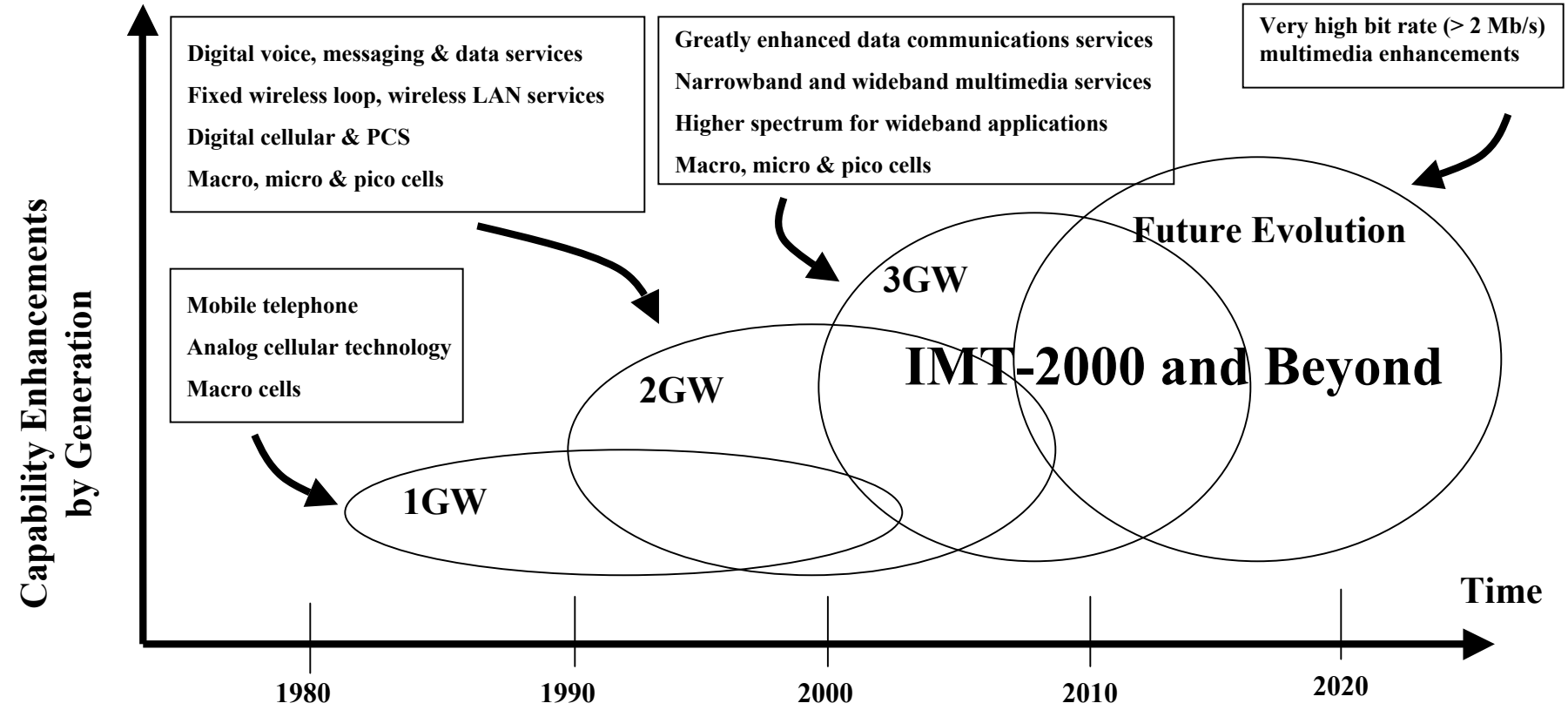
- 1st Generation Wireless (1970s)
  - Ex: **AMPS** (USA: 900Mhz); **C-Nets** (Germany: 450Mhz); **NMT** (Switzland: 450, 900Mhz), …
  - Analog technology
  - Poor spectral efficiency
  - Voice only
- 2nd Generation Wireless (1980s)
  - Ex: **GSM**: 900 and 1800Mhz, 9.6kbps, FDMA+TDMA; **CDMA(IS-95A/B)**, 900 and 1800Mhz, 14.4/64kbps, FDMA+CDMA
  - Digital or Analog + Digital technology
  - Higher spectral efficiency through Multiple Access Air interfaces: FDMA, TDMA, CDMA
  - Voice and limited data (circuit switch wireless data)

Mobile Network Evolution (Cont'd)

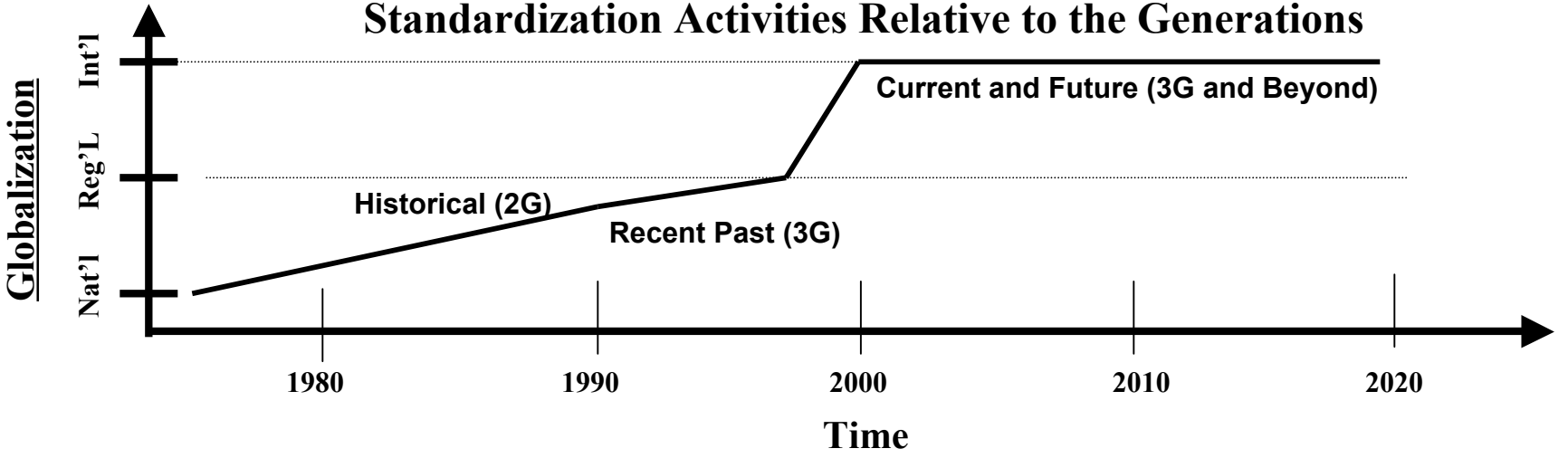
- 3rd Generation Wireless (2000's)
  - Ex: **UMTS** in Europe, 114Kbps-2Mbps; **CDMA2000** in the US, up to 2Mbps
  - Better support for wireless data
  - Mobile Internetworking, or wireless packet data (GPRS, EDGE, Mobile IP)

- 4th Generation Wireless (future)
  - Wireless and Mobile Multimedia
  - Smart Antenna, Spatial Division Multiple Access
  - Research stage: **ACTS**, …

Generations of Terrestrial Commercial Wireless Systems



Standardization Activities Relative to the Generations



Mobile Networking Evolution

	1st	2nd	3rd	4th
Name	Analog Cellular (1970s)	Digital Cellular, PCS (1980s~)	IMT-2000 (2000~)	(Beyond IMT-2000) (2005~)
Core Network	Circuit-based Analog (PSTN)	Circuit-based Digital (GSM,IS-95)	IP-based (GPRS, Mobile-IP)	All-IP-based
Air Network	FDMA	FDMA+TDMA, CDMA	WCDMA, cdma2000	Smart Antenna
Frequency (MHz)	900	900, 1800MHz	2000MHz	5~60GHz

Mobile Networking Evolution

	1st	2nd	3rd	4th
Main Services	Voice phone	Voice phone, Low bit rate data (short msg.)	Voice phone, High rate data (web surfing)	same services as fixed telecomm.
Data service Bandwidth	NA	< 10kbps	< 2Mbps < 384kbps < 144kbps	< 20Mbps < 2Mbps
Main Organizer	Nation-based	SDO (IETF,ETSI)	ITU-R (TG8/1), 3GPP/3GPP2	ITU-R (WP8F/ WP8D)

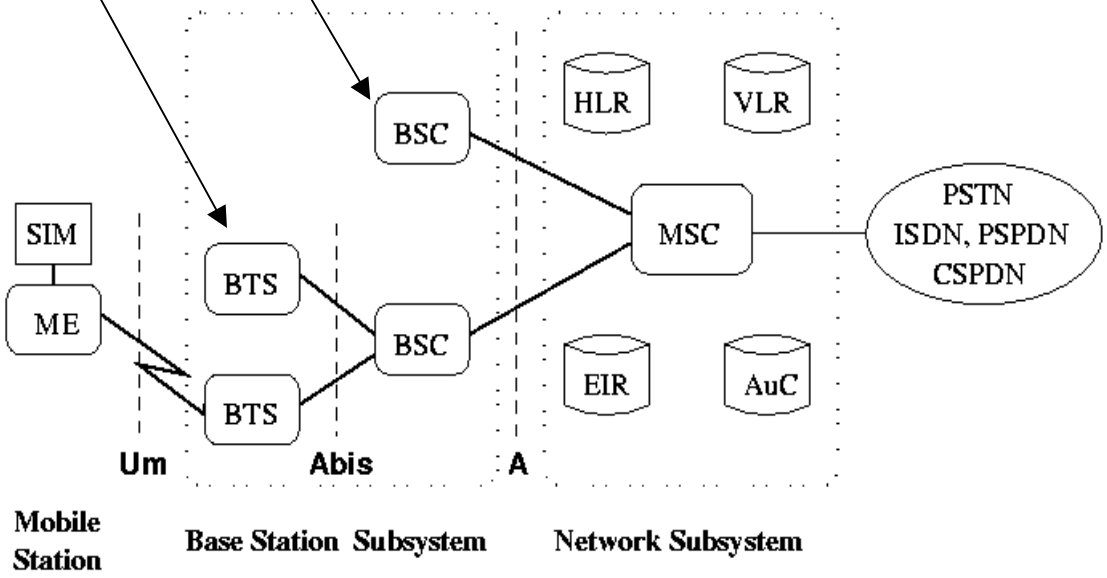
GSM : Global System for Mobile communication

- **Configuration**
  - MS : ME (IMEI-International Mobile Equipment Identity) + SIM (IMSI-International Mobile Subscriber entity)
  - BSS : BTS(Radio transceiving, Handling radio-link protocols) + BSC(Radio channel setup, frequency hoping, handover)
  - NS : Handling subscriber(user using SS7, registration, authentication, location updating, handover, call routing to a roaming) + Switching(connecting to fixed net.)
- **Air link**
  - Uplink(890~915MHz)/Downlink(935~960MHz)
  - FDMA(25MHz = 124carriers * 200kHz) + TDMA(burst period : 15/26ms)

GSM Architecture

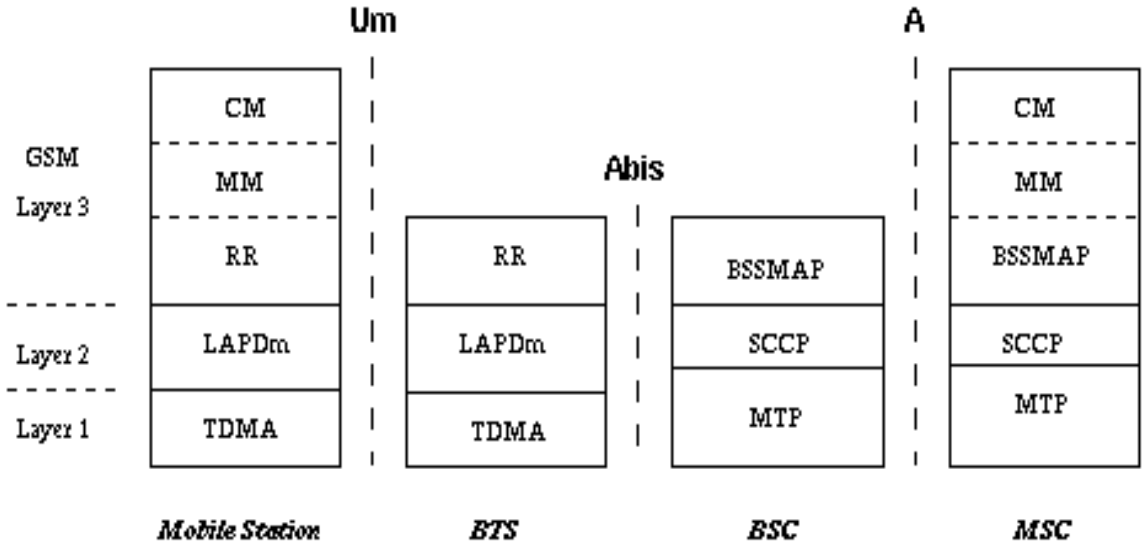
External H/O

Internal H/O



SIM Subscriber Identity Module BSC Base Station Controller MSC Mobile services Switching Center
ME Mobile Equipment HLR Home Location Register EIR Equipment Identity Register
BTS Base Transceiver Station VLR Visitor Location Register AuC Authentication Center

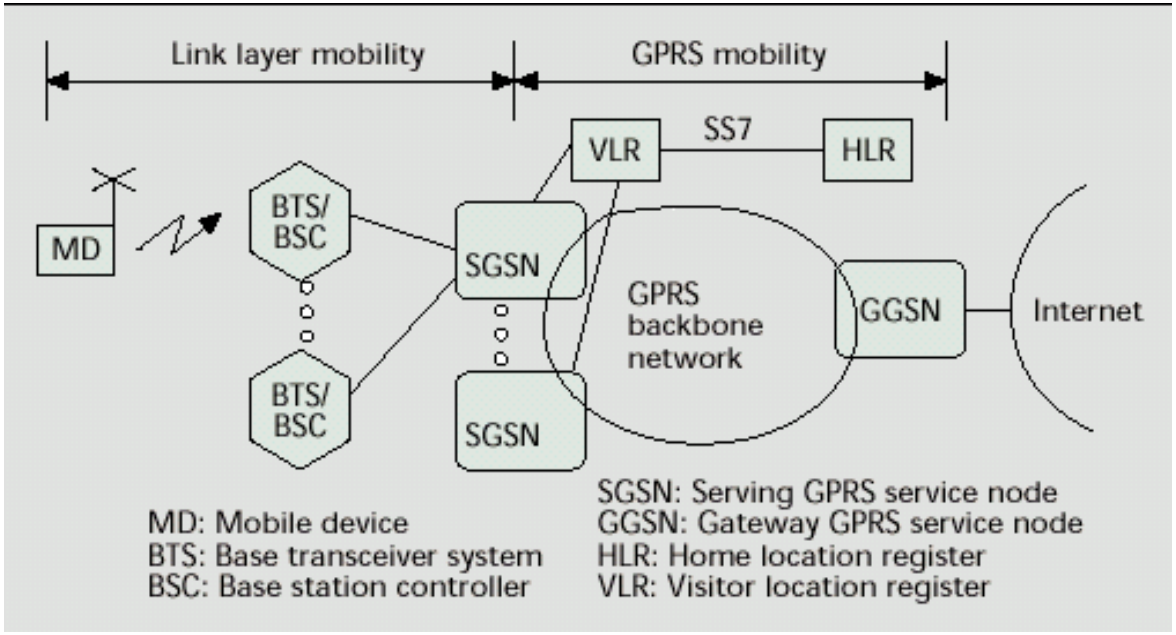
GSM Protocol



GPRS: General Packet Radio System for GSM

- Configuration
  - MS
  - BS
  - GSN/VLR/HLR
  - GSN: GPRS Support Node
  - SGSN: Serving GSN Node
  - GGSN: Gateway GSN Node
- Air Link interface
  - GMSK -> EDGE -> WCDMA
  - Paging: battery power reduced
  - Registration, authentication, handoff

The GPRS System



GPRS Protocol Stack

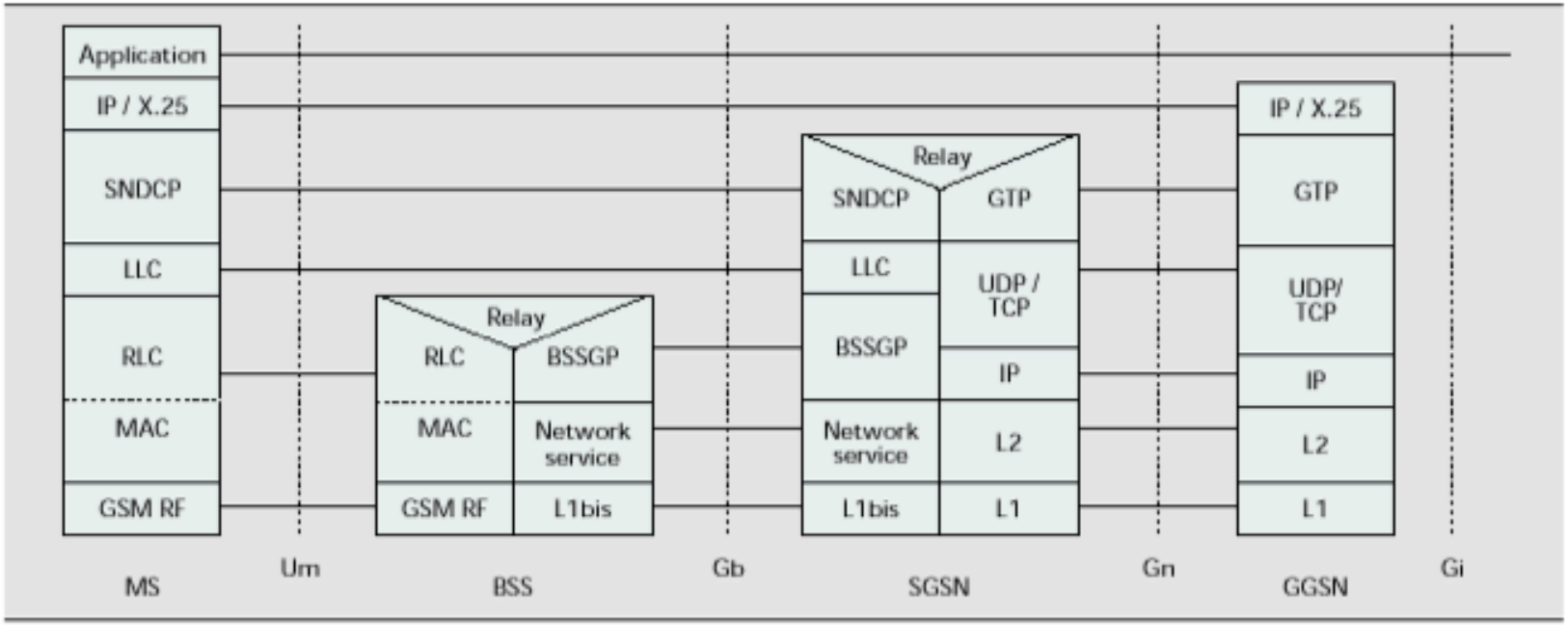
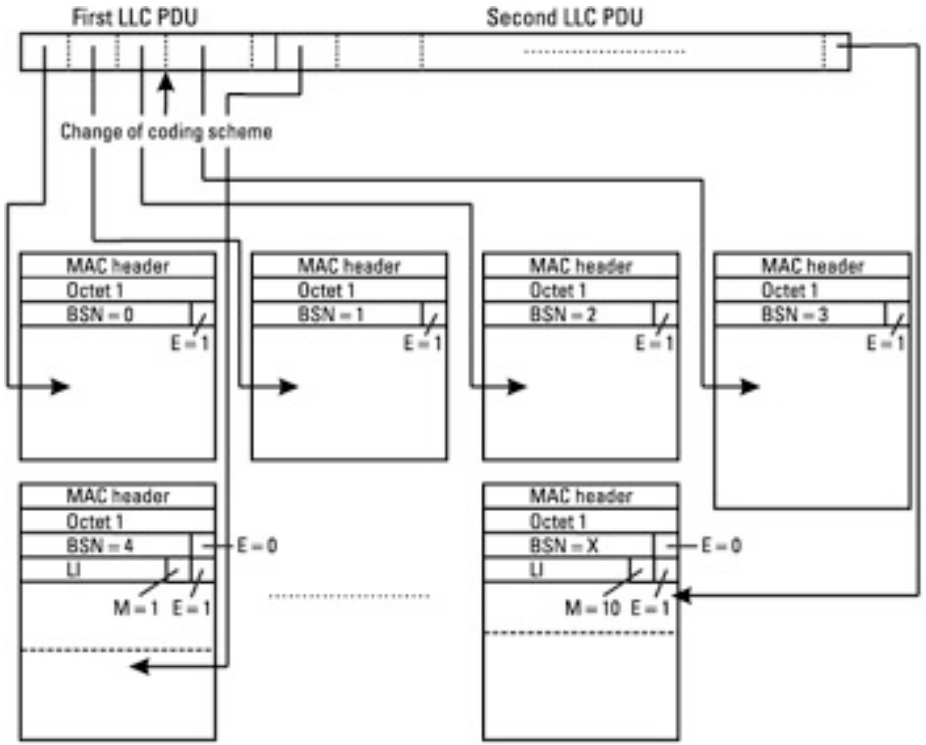


Figure 2. *The GPRS transmission plane [4].*

RLC: Reliable Link Controller, **SNDCP**: Sub-network Dependent Convergence Protocol
BSSGP: Base Station System GPRS Protocol, **GTP**: GPRS Tunneling Protocol,

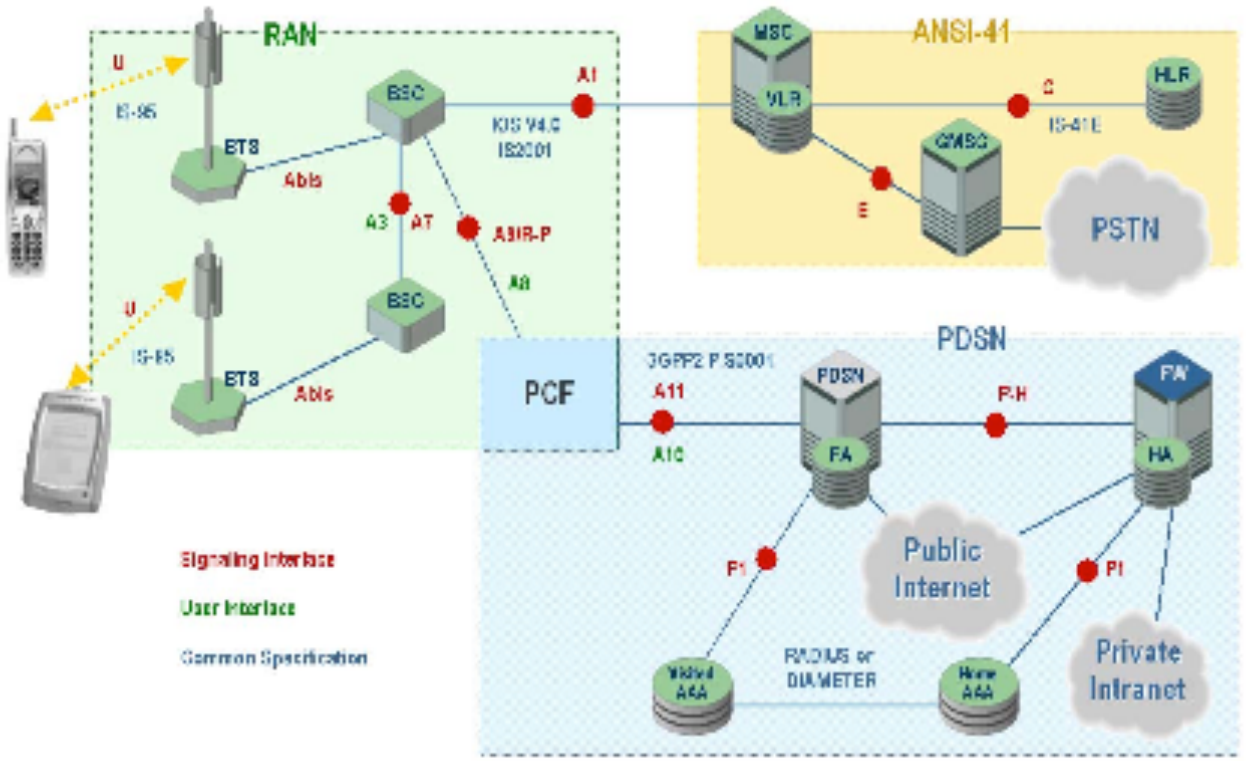
Reliable Link Controller



The I-95 CDMA Mobile Network

- IS-95 : TIA Interim standard for digital cellular communication system
- TDMA + CDMA
  - 800(cellular), 1.7~1.8MHz(PCS)
- CDMA
  - High capacity
  - Small cell radius
  - Spread spectrum technology
  - Special coding scheme

CDMA Network Architecture



RAN: Radio Access Network, **PCF**: Packet Control Function
PDSN: Packet Data Serving Node

Mobile-IP

- Internet Protocol (IP)
  - Connectionless packet delivery
  - Unreliable delivery
  - IP host addresses consist of two parts
    - *network id*
    - *host id*
  - By design, host address is tied to its network

Internet Protocol (IP)

- Intermediate routers need only look at the network id
- destination network responsible for getting packet to right host
- When a host moves to a new network, its IP address would have to change - packets to old address are lost

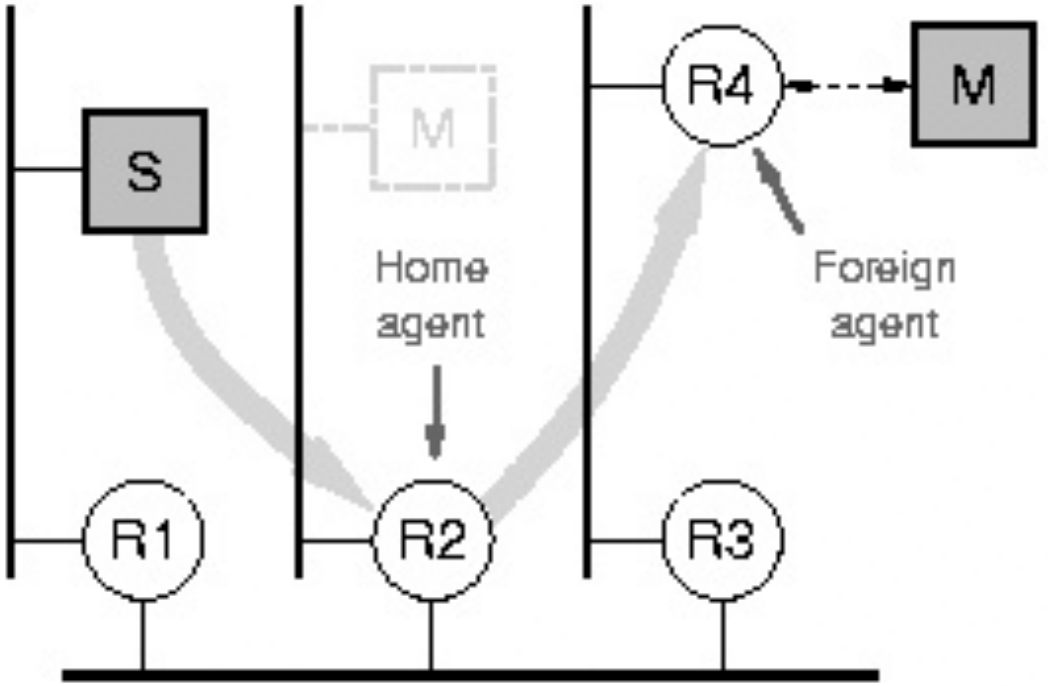
IETF Mobile IP Protocol

- IETF = Internet Engineering Task Force: Standards development body for the Internet
- Mobile IP allows a host to have a unique (location-independent) IP address.
- Each host has a *home agent* on its home network.
  - The home agent forwards IP packets when mobile host away from home.

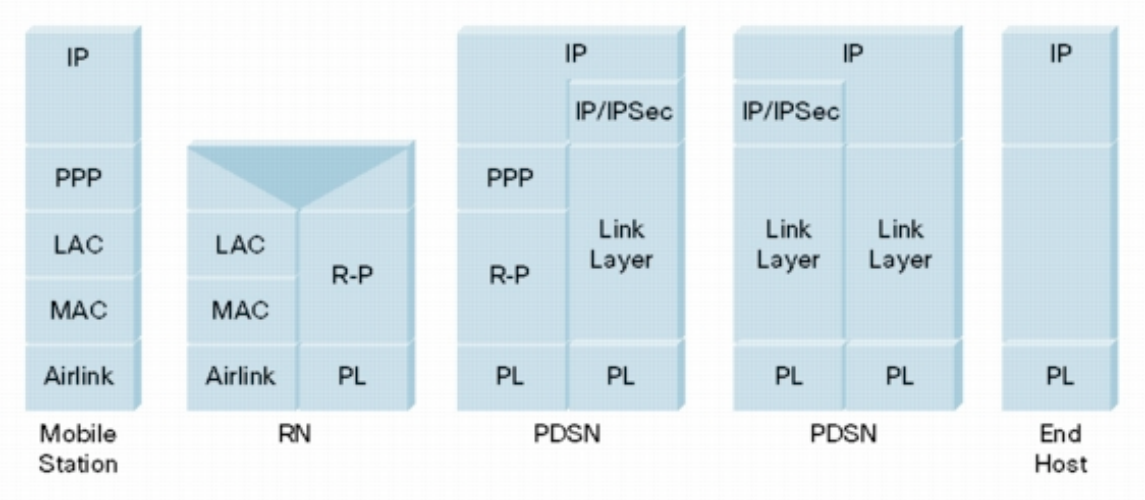
IETF Mobile IP Protocol

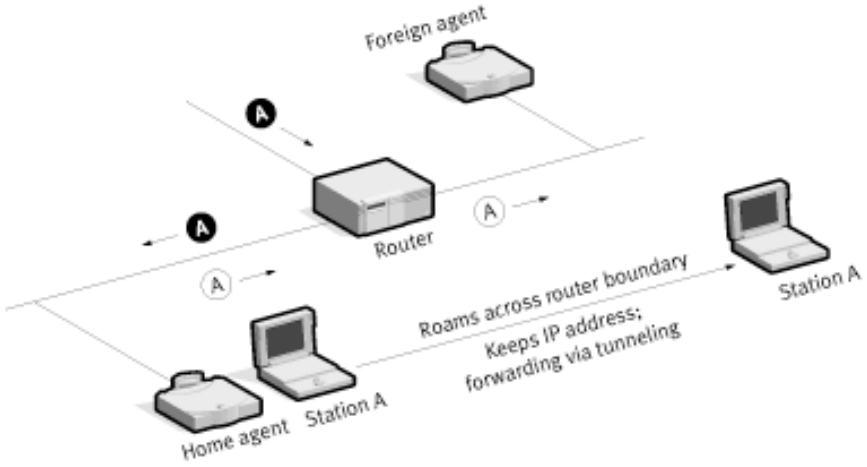
- When away from home, mobile host has a *care-of-address*
  - care-of-address = address of *foreign agent* within the foreign subnet - the foreign agent delivers forwarded packets to mobile host
  - care-of-address may also be a temporary IP address on the foreign network

Basic Architecture



Mobile IP Architecture





IETF Mobile IP

- When moving, the host registers with home agent - home agent always knows the host's current care-of-address.
- *Correspondent host* = Host that wants to send packets to the mobile host
- Correspondent host sends packets to the host's Mobile IP address, which are routed to the host's home network.

IETF Mobile IP

- Correspondent host need not know that the destination is mobile.
- Home agent *encapsulates* and *tunnels* packets to the mobile host's care-of-address.

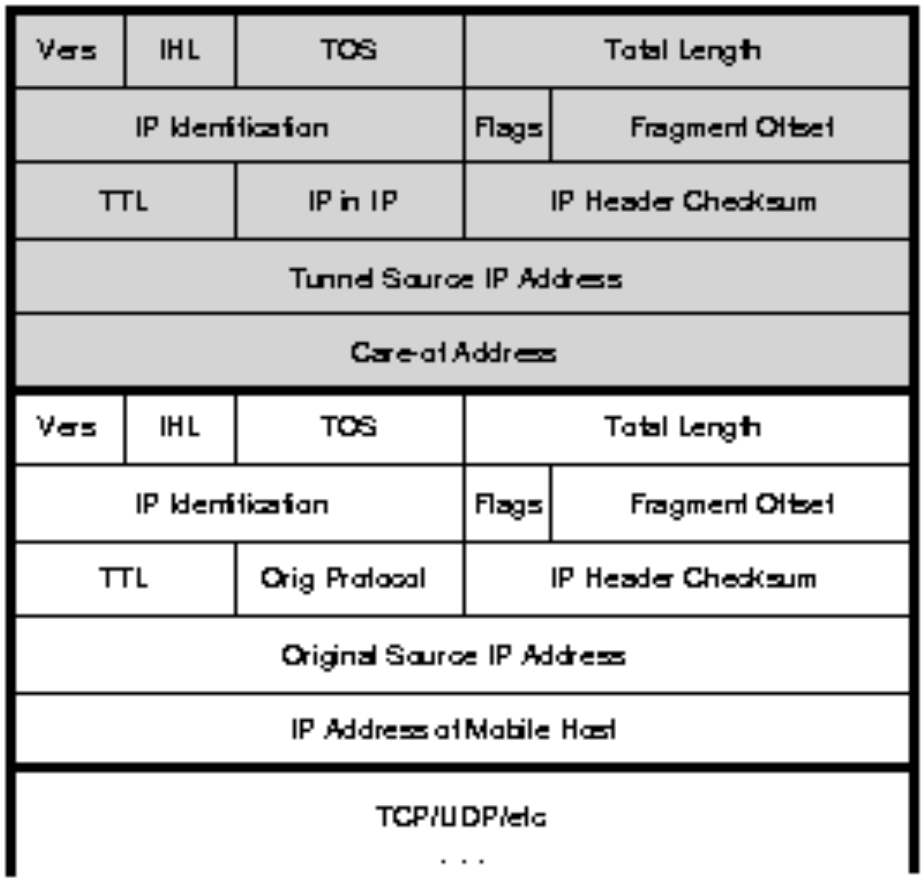
Encapsulation and Tunneling

- IP-in-IP encapsulation
- Received IP packet is encapsulated in a new IP packet with a new header. In the new header:
  - Destination = care-of-address
  - Source = address of home agent
  - Protocol number = IP-in-IP

Encapsulation and Tunneling

- Decapsulation protocol at foreign agent removes added header, and transmits the packet to the mobile host over the local network interface (be it wire-line or wireless).

IP-in-IP Encapsulation



Minimal Encapsulation

- Reduces the additional bytes added to header when encapsulating: 8 or 12 bytes are added.
  - Original source address need not be included in the tunnel header, if the original source is also the tunneling node

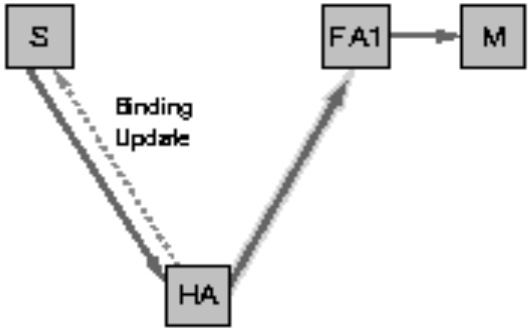
Authentication

- As host B can send “moving to new location” registration messages to host A’s home server, host B can pretend to be host A, and receive packets destined for host A.
- To avoid this, all registration messages must be “authenticated”.
- Protection against “replay” attacks must be provided.

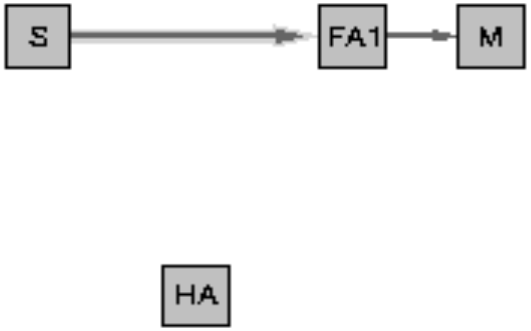
Route Optimizations

- Binding updates : When a home agent receives a packet from a correspondent host, the former: (1) sends a *binding update* informing the latter of the mobile host's current care-of-address; and (2) forwards the packet to the mobile host's care-of-address
- Correspondent host can cache the binding, and future packets can be *tunneled* directly to the care-of-address (without going via home agent)
- Cache consistency: A cached binding becomes stale when the mobile host moves
- How does a correspondent host know when the mobile host moves?

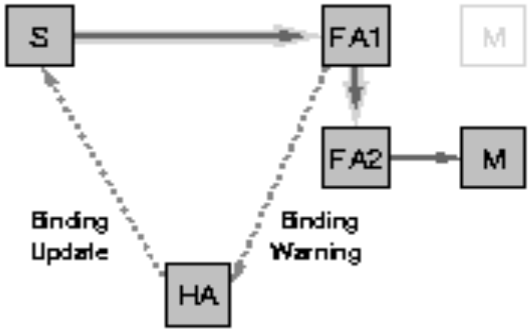
Route Optimization



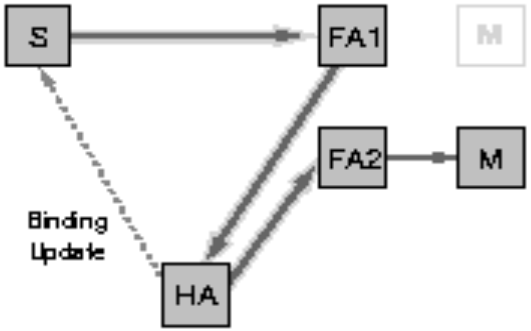
(a) Sending the first packet to a mobile host



(b) Sending subsequent packets to a mobile host



(c) Sending the first packet after a mobile host moves



(d) Tunneling the packet in case the the cache entry has been dropped

Route Optimizations

- Binding warning: Used by old foreign agent, to request the home agent to send current binding to a correspondent host.
- When a host moves:
  - Old foreign agent may cache a forwarding pointer to the new foreign agent
  - Packets re-tunneled along the forwarding path + binding warning sent to home agent to update the correspondent with the new binding

Route Optimization

- Old foreign agent may not cache (or may purge) the forwarding pointer:
  - Packets are forwarded to home agent (foreign agents know how to do that).
  - Home agent tunnels it to current care-of-address + sends binding update to correspondent

MosquitoNet

- No *foreign agent*
- Visiting mobile host is assigned a temporary IP address corresponding to the foreign subnet.
- Packets are tunneled directly to the mobile host (without having to go through a foreign agent)

MosquitoNet -- Advantages

- Mobile hosts can visit networks that do not have foreign agents
- Foreign agent is no more a single point of failure
- Scalability: foreign agent not needed on every network that a mobile may visit. Home agents only needed on networks with mobile clients
- Simpler protocol: Only part of foreign agent functionality is needed

MosquitoNet -- Disadvantages

- Mobile host needs to acquire a temporary IP on foreign subnet
- Security: If a temporary IP address is re-assigned to another mobile host a little too soon, the new mobile host may receive packets intended for the previous IP owner
- Packet loss: Foreign agents can forward packets destined for a mobile host that has moved to another foreign subnet. Without foreign agents, the packets will simply be dropped (lost)
- Mobile host is more complex in MosqNet, as it must incorporate some of the functionality of a foreign agent.

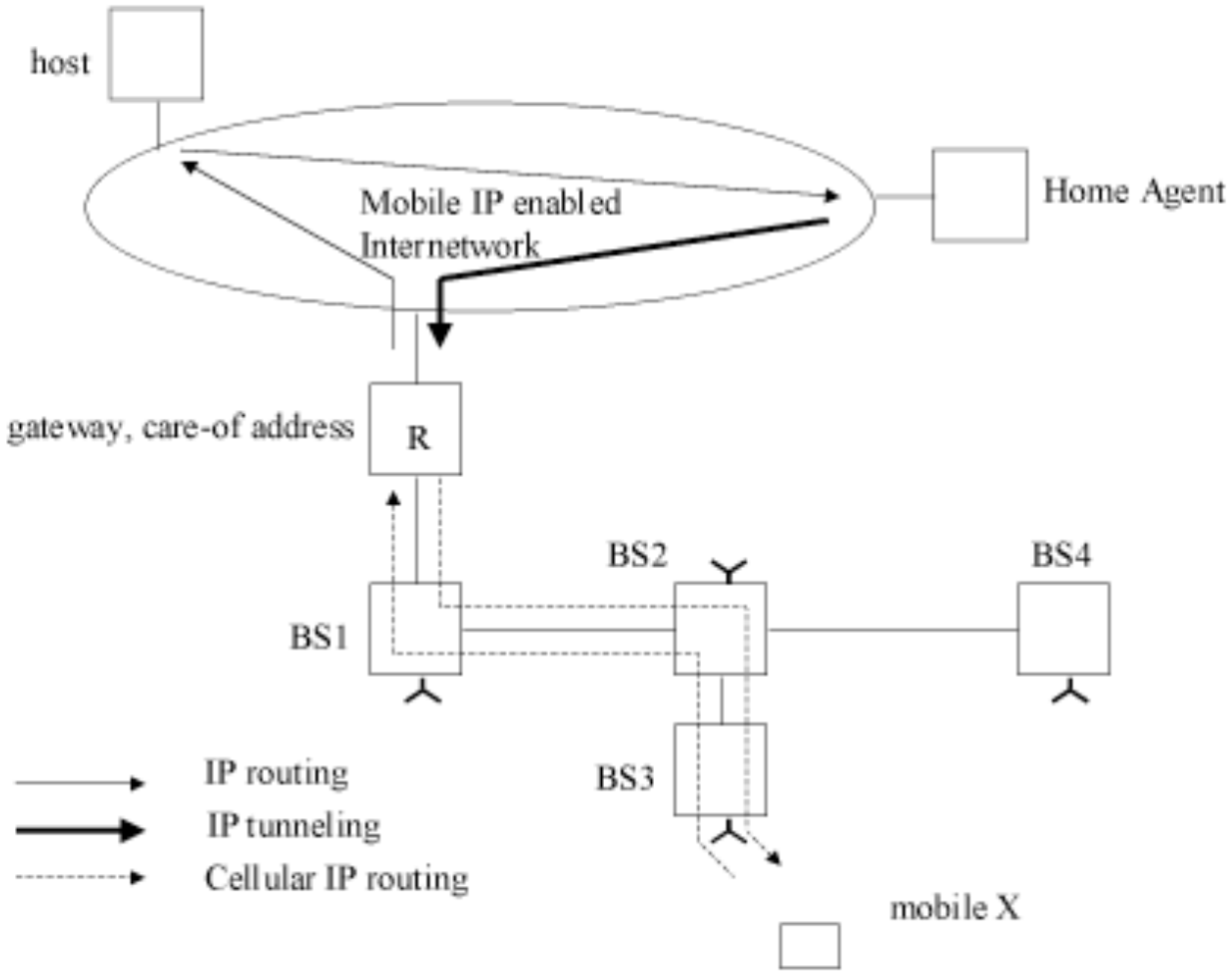
Cellular IP

- Mobile IP is not suitable for rapid mobility
  - With each handoff, a new IP address needs to be obtained and communicated to the home agent
  - Results in delays and possible TCP ill reaction during handoff
  - Cellular IP is one protocol that addresses issues of rapid mobility

Cellular IP Scalability

- Is IP based
- Uses “scalable” ideas from cellular mobile telephony
  - fast and smooth handoff within a restricted geographical area (Wireless IP Access Network) – no global mobility support
  - Passive Connectivity
    - Only active mobile nodes register with the system upon handoff
    - Location of idle mobile nodes is only approximately known

Cellular IP “Access Network”



Cellular IP Routing Protocol

- Mobile IP across “wireless IP access networks”
- Uplink packets are routed hop-by-hop to the gateway. Downlink packets are routed through the reverse path
- To maintain downlink route, *receiver* nodes periodically send empty IP packets to the gateway (route update packets)
- As a node becomes idle, its downlink route is removed from the base stations

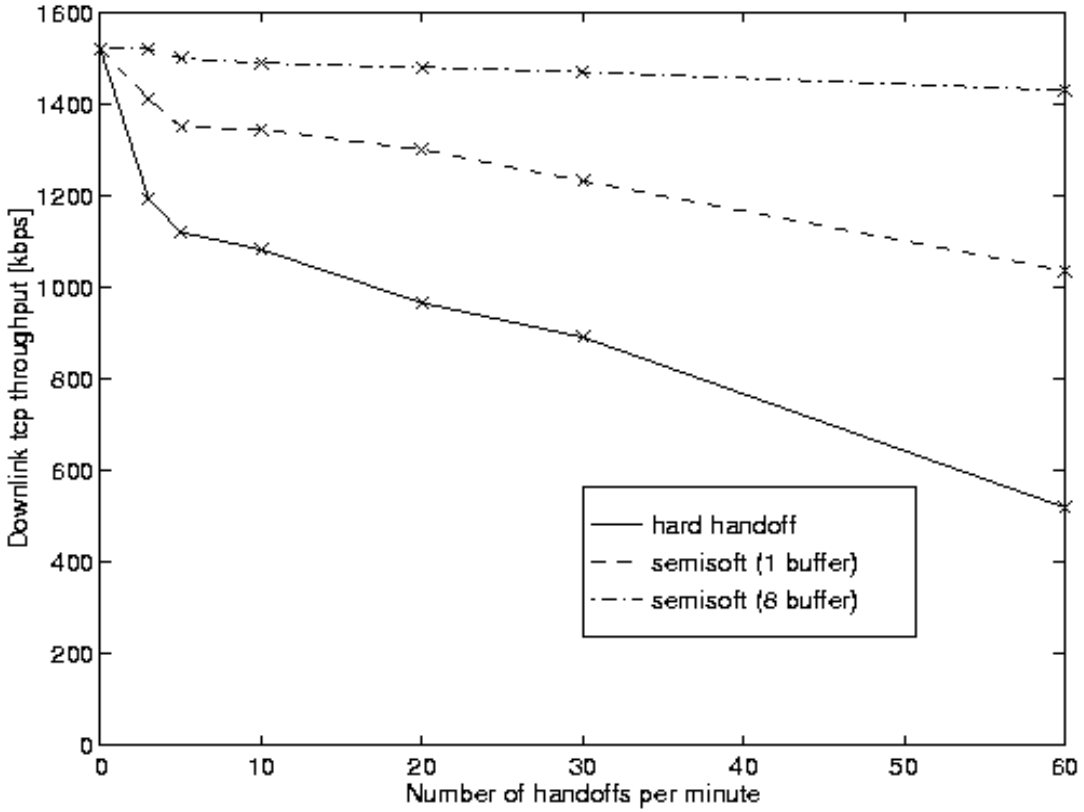
Cellular IP Handoff

- Simple and fast at the price of potential packet loss
- Mobile node initiated
- Tune to stronger signal and send “route update cache” packet to new base station
  - New downlink is configured to the new base station
  - Handoff latency is time from handoff to receipt of first packet through new BS
- During latency, downlink packets are lost

Cellular IP Handoff

- During handoff, route cache at old base station is not cleared. Rather it expires after a Timeout period
- There is a window of time where downlink packets are delivered to both old and new BS
  - This is exploited as follows: mobile node initiates handoff with new BS and immediately returns to listen to the old BS (Semi-Soft Handoff)

Cellular IP Handoff Performance



Downlink TCP Performance