3G Cellular Systems: cdma 2000

David Tipper
Associate Professor

Graduate Telecommunications and Networking Program
University of Pittsburgh
2720 Slides 13

3G Development

- 1986 ITU began studies of 3G as:
  - Future Public Land Mobile Telecom. Systems (FPLMTS)
  - 1997 changed to IMT-2000 (International Mobile Telecom. in Year 2000)
  - ITU-R studying radio aspects, ITU-T studying network aspects (signaling, services, numbering, quality of service, security, operations)
- IMT-2000 vision of 3G
  - *1 global* standard in *1 global frequency band* to support wireless data service
  - Spectrum: 1885-2025 MHz and 2110-2200 MHz worldwide
  - Multiple radio environments (phone should switch seamlessly among cordless, cellular, satellite)
  - Support for packet switching and asymmetric data rates
- Target data rates for 3G
  - Vehicular: 144 kbps
  - Pedestrian: 384 kbps
  - Indoor office: 2.048 Mbps → roadmap to > 10Mbps later
- Suite of four standards approved after political fight

Third Generation Standards

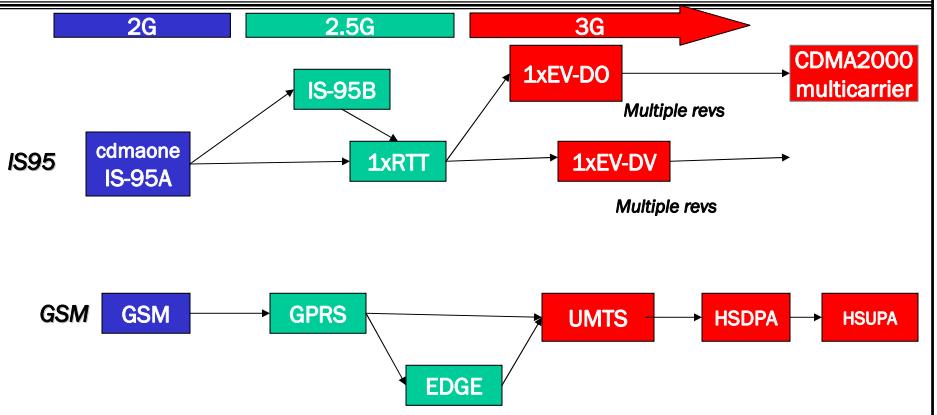
- ITU approved suite of four 3G standards
- EDGE (Enhanced Data rates for Global Evolution)
  - TDMA standard with advanced modulation and combined timeslots
  - Provides unification of NA-TDMA and GSM
  - Only meets some of the 3G requirements (2.75G!)
- UMTS (Universal Mobile Telephone Service) also called WCDMA (wideband CDMA)
  - Dominant standard outside of US and leading standard for 3G worldwide
  - Viewed as 3G migration path for GSM/TDMA systems
- CDMA 2000
  - Competes directly with UMTS/W-CDMA
  - Evolutionary path for IS-95 which is the dominant standard in the US
- TD-SCDMA : Stand alone standard developed in China

cdma2000

Major Characteristics

- Evolves to meet IMT 2000 data rate requirements for 3G
- Backward compatibility with IS-95B (cdmaone)
- Support for data services
  - High data rate (up to 2 Mbps)
  - Optimized for packet and circuit data services
- Support for multimedia services
  - Concurrent channels (support concurrent communication channels for related data streams)
  - QoS negotiation and control mechanisms
- Reuse/adoption of existing standards
  - Reuse IS-95 standards (Air Interface) and IS-41 standards (networking),
  - Mobile IP, RADIUS, etc.

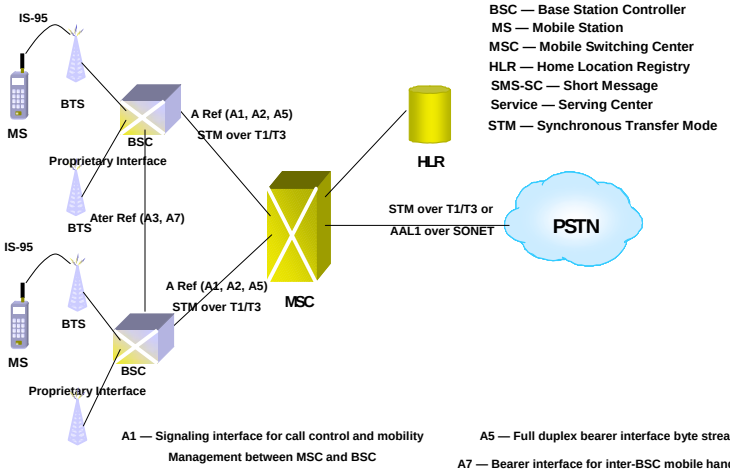
3G Evolution: major streams



Briefly review IS95 and cdma2000 1xRTT

2G cdmaOne (IS-95)

- cdmaOne
- Voice 14.Kbps or variable rate up to 9.6 Kbps
- Data 9.6kbps or 14.4 Kbps
- 1.25 MHz carrier
- 64 Walsh codes per carrier



BTS — Base Transceiver Station
BSC — Base Station Controller
MS — Mobile Station
MSC — Mobile Switching Center
HLR — Home Location Registry
SMS-SC — Short Message Service — Serving Center
STM — Synchronous Transfer Mode

A1 — Signaling interface for call control and mobility Management between MSC and BSC

A2 — 64 kbps bearer interface for PCM voice

A3 — Signaling interface for inter-BSC mobile handoff

A5 — Full duplex bearer interface byte stream

A7 — Bearer interface for inter-BSC mobile handoff

IS-95 CDMA - Radio Aspects

- IS-95 is an air interface standard only
- System use FDD/FDMA/CDMA
- FDD => Uplink and Downlink channels separated according to Cellular band or PCS band regulatory requirements
- Bandwidth after spreading is 1.23 MHz with guardband becomes 1.25 MHz
- IS-95a standard designed for AMPS cellular band
  - Channel operates at 1.228 Mchips/sec
  - A 64 bit spreading code is used (Walsh Code)
  - Modulation is QPSK and slight variations OffsetQPSK

Modulation and coding features

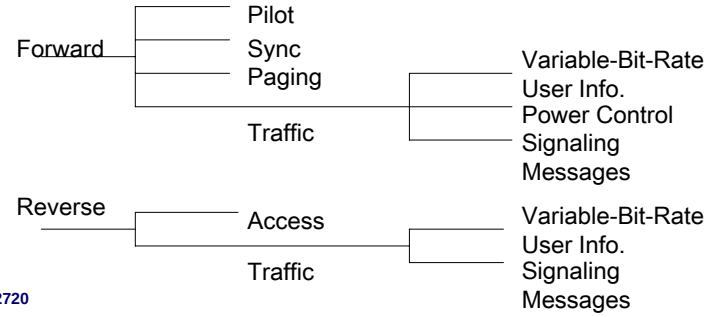
Modulation	Quadrature phase shift keying or variations
Chip rate	1.2288 Mcps
Nominal data rate (Rate Set 1)	9.6 kbps
Filtered bandwidth	1.23 MHz -> 1.25 MHz with guard band
Coding	Convolutional coding Constraint length = 9 Viterbi decoding
Interleaving	With 20 ms span

Codes used in IS-95 systems

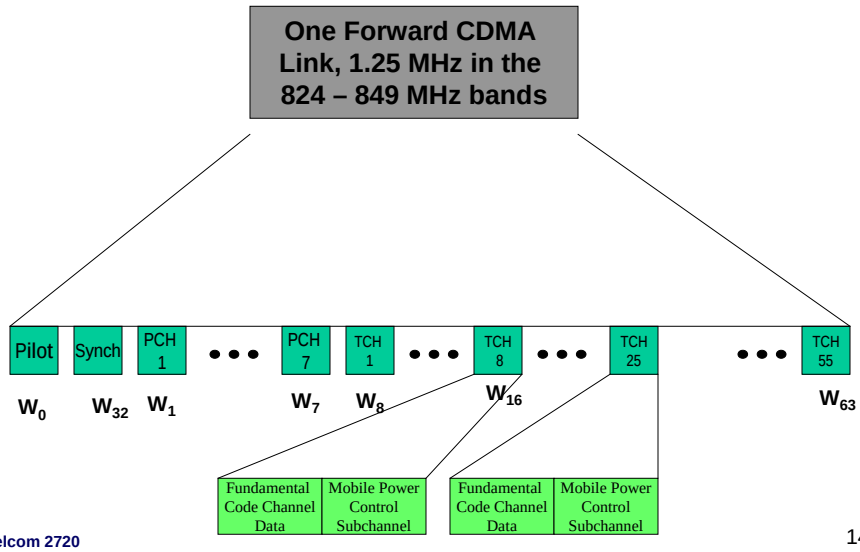
- Walsh codes
  - They are the “orthogonal codes” used to create “logical channels” on the up/downlink (at the same time and within the same frequency band)
- PN (pseudo-noise) codes
  - They are used to distinguish between transmissions from different cells and are generated using “linear feedback shift registers”
  - Basically a pseudo-random number generator
  - They have excellent autocorrelation properties
  - Two short PN codes and a long PN code are used in IS-95 that have periods of $2^{15} - 1$ and $2^{42} - 1$
- Convolutional codes for error correction
- Block codes with interleaving and error correction

IS-95 Logical Channels

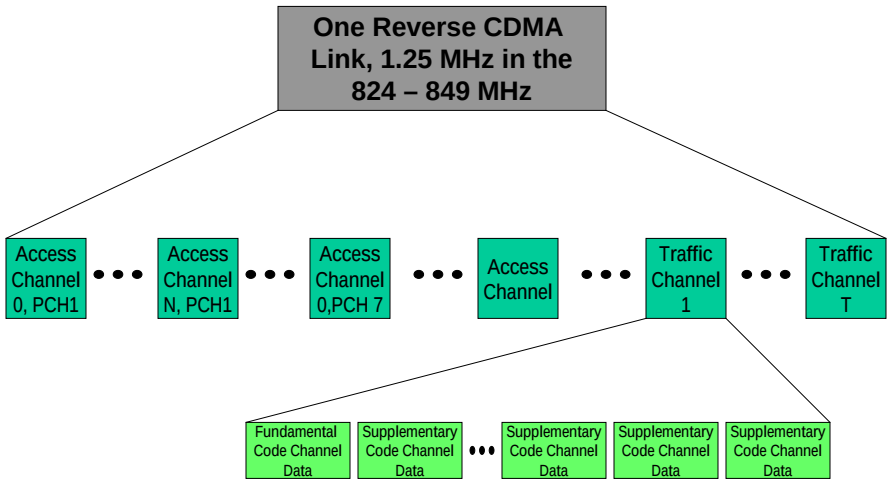
- CDMA systems define multiple channels *per frequency channel*
- Pilot channel
  - Provides a reference to all signals (beacon)
- Sync channel
  - Used for obtaining timing information
- Paging channel
  - Used to “page” the mobile terminal when there is an incoming call
- Traffic channel
  - Carries actual voice or data traffic : fundamental code channel
    - Up to seven supplemental code channels



IS-95 Forward (Downlink) Channel



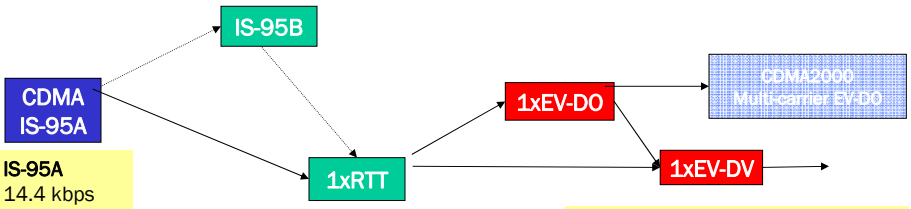
Reverse CDMA Channel



IS-95 evolution to 3G

IS-95B
Uses multiple code channels
Data rates up to 64kbps
Many operators went direct to 1xRTT

CDMA2000 1xEV-DO: Evolved Data Optimized
Classified as a "3G" system
2.4Mbps Down 153kbps Up
Use new or existing spectrum



IS-95A
14.4 kbps
data rate

CDMA2000 1xRTT:
First phase in CDMA2000 evolution
Easy co-existence with IS-95A air interface
Release 0: max 153 kbps Up/Down
Release A: max 307 kbps Down/153 kbps Up

CDMA2000 1x Evolved Data/Voice (EV-DV)
Integrate voice and data on a single channel . 3.1Mbps Downlink
1.2 Mbps Uplink
Future development on hold as EV-DV not widely adopted

IS-95/cdma2000 Protocol Revisions

IS95 (cdmaone standard) TIA standards http://www.tia.org

1. IS-95/J-STD-008 (cdmaone)
2. IS-95A
3. IS-95A+TSB-74
4. TIA/EIA-95B minimum required features
5. TIA/EIA-95B all required features

cdma2000 standards 3GPP2 http://www.3gpp2.or

1. CDMA2000 Release 0 (cdma2000 1x-RTT)
2. CDMA2000 Release A
   CDMA 2000 EVDO
   1) Release 0
   2) Revision A, B, C

Source: Qualcomm CDMA University Student Guide.

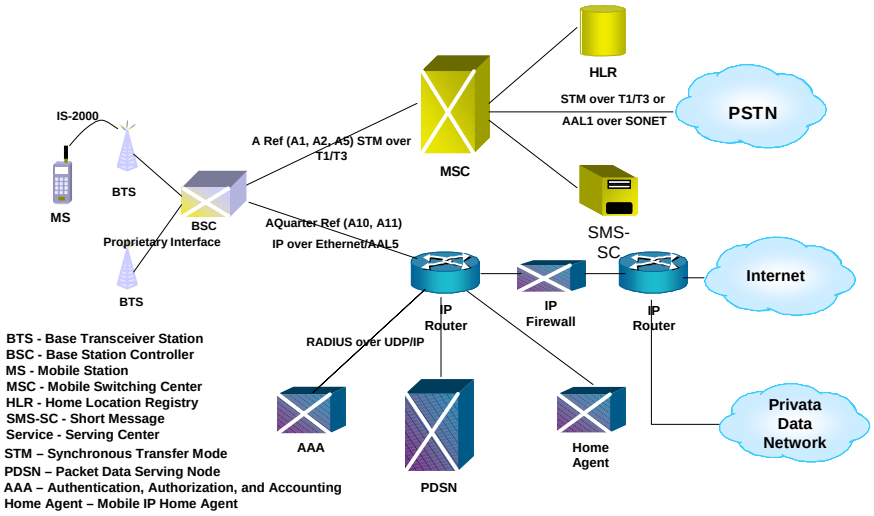
cdma2000

- cdma2000 1xRTT (Radio Transmission Technology)
  - 2.5G service over IS-95a, b, *cdmaone* systems
  - overlay like GPRS
  - Uses same 1.25MHz channels as IS-95
  - cdma2000 slight changes to IS-95 radio link
    - Extend number of Walsh codes on DownLink from 64 to 128
    - Reverse Link Pilot for coherent demodulation
      - Mobile broadcasts pilot (Walsh code 0) as well as traffic channels
    - Forward link Fast Power Control based on reverse link pilot
      - reduces interference to users on same frequency in cell and between cells

cdma2000

- cdma2000 1xRTT (Radio Transmission Technology)
  - One user can have Multiple Walsh codes (Supplemental Channels) to get greater data rate
  - Data rates 153Kbps Up/Down
  - Release A: provides higher downlink rate (307Kbps) adds
    - Turbo codes
    - SMV: *S*electable *M*ode codebook excited LPC *V*ocoder
      - » Defined by 3GPP2 for CDMA2000
      - » SMV 4 rates: 8.5, 4, 2 & 0.8kbps
      - » Lower bit rates allow more error correction
      - » Dynamically adjust to radio interference conditions
  - Substantial additions in the backhaul
    - In fashion similar to GPRS separates voice (circuit switched) and packet data at BSC
    - Based on IP protocols

CDMA2000 1x Network



BTS - Base Transceiver Station
BSC - Base Station Controller
MS - Mobile Station
MSC - Mobile Switching Center
HLR - Home Location Registry
SMS-SC - Short Message
Service - Serving Center
STM – Synchronous Transfer Mode
PDSN – Packet Data Serving Node
AAA – Authentication, Authorization, and Accounting
Home Agent – Mobile IP Home Agent

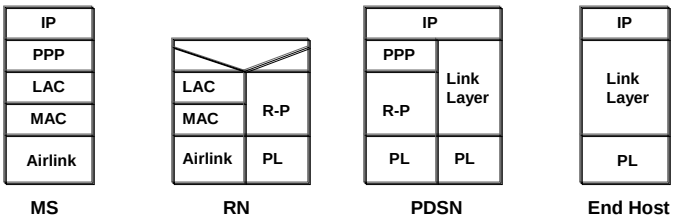
A10 – Bearer interface between BSC (PCF) and PDSN for packet data
A11 – Signaling interface between BSC (PCF) and PDSN for packet data

Packet Data Serving Node (PDSN)

- PDSN – similar to SGSN in GPRS
  - Establish, maintain, and terminate PPP sessions with mobile station
  - Support simple and mobile IP services
  - Route packets between mobile stations and external packet data networks
  - Collect usage data and forward to AAA server
- AAA (authentication, authorization, and accounting) server
  - Authentication: PPP and mobile IP connections
  - Authorization: service profile and security key distribution and management
  - Accounting: usage data for billing
  - uses RADIUS (Remote Authentication Dial in User Service) protocol

Simple IP Service (CDMA2000)

Simple IP: the user is assigned a dynamic IP address from the local PDSN and is provided IP routing service by a service provider network. The user retains its IP address as long as it is served by a radio network which has connectivity to it's address assigned by the PDSN. There is no IP mobility beyond this PDSN.



R-P is RN to PDSN interface – depends on layer 2 connection (Ethernet, Sonet, ATM, etc.)

Simple IP Service (CDMA2000)

- PPP is Data Link Layer protocol between the MS and PDSN. PPP is established prior to IP datagram is being exchanged between MS and PDSN.
- RN opens R-P session for a mobile. Once the R-P session is established, PDSN sends LCP (Link Configuration Protocol) Configure-Request for a new PPP session to the MS.
- Authentication: In an initial LCP configuration-request, the PDSN includes CHAP for authentication. If MS does not use CHAP, but prefers to use PAP, it will sends an LCP configuration Nack with proposing PAP.

  CHAP (Challenge Handshake Authentication Protocol):

  1. After the Link Establishment phase is complete, the authenticator sends a "challenge" message to the peer.
  2. The peer responds with a value calculated using a "one-way hash" function. The authenticator checks the response against its own calculation of the expected hash value. If the value matches, the authentication is acknowledged.

Simple IP Service (CDMA2000)

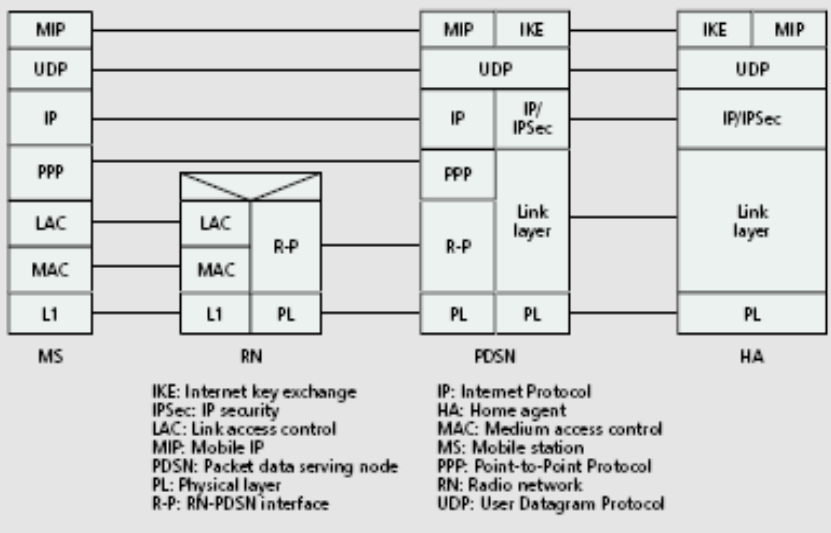
PAP (Password Authentication Protocol): It provides a simple method for the peer to establish its identify using a 2-way handshake. PAP is not a strong authentication method. Passwords are sent over the circuit "in the clear", and there is no protection from playback or repeated trial and error attacks.

- PDSN acts as a RADIUS client. PDSN communicate user CHAP or PAP authentication information to the local RADIUS server.
- PDSN also acts as a RADIUS client for accounting.
- Termination: PDSN clears the PPP state if there is no established underlying R-P session for the mobile station. The PDSN also clears the R-P session whenever the PPP session closed. PDSN also terminates PPP session if a PPP inactivity timer expires.

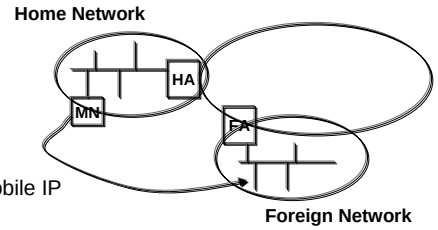
Mobile IP

- CDMA 2000 provides Simple IP Service & Mobile IP Service
- Mobile IP
  - IP routing
    - IP routes packets from a source endpoint to a destination by allowing routers to forward packets from incoming network interfaces to outbound interfaces according to routing tables based on IP address in packet header
  - Mobility issue
    - In TCP connections are indexed by a quadruplet that contains the IP addresses and port numbers of both connection endpoints
    - Changing any of these four numbers will cause the connection to be disrupted and lost
    - The correct delivery of packets to the mobile node's current point of attachment depends on the network number contained within the mobile node's IP address
    - To maintain the connection, as the mobile node moves from place to place, it must keep its IP address the same
  - Mobile IP is designed to solve mobility issues by allowing the mobile node to use two IP addresses, i.e., home address and care-of-address
    - Home address is static and is used to identify TCP connections
    - Care-of-address changes at each new point of attachment. It indicates the network number and thus identifies the mobile node's point of attachment with respect to the network topology
    - Used in cdma 2000 to support mobility beyond a PDSN with simple IP

Cdma2000 MIP Protocol Stack



Mobile IP (IETF RFC 3344)



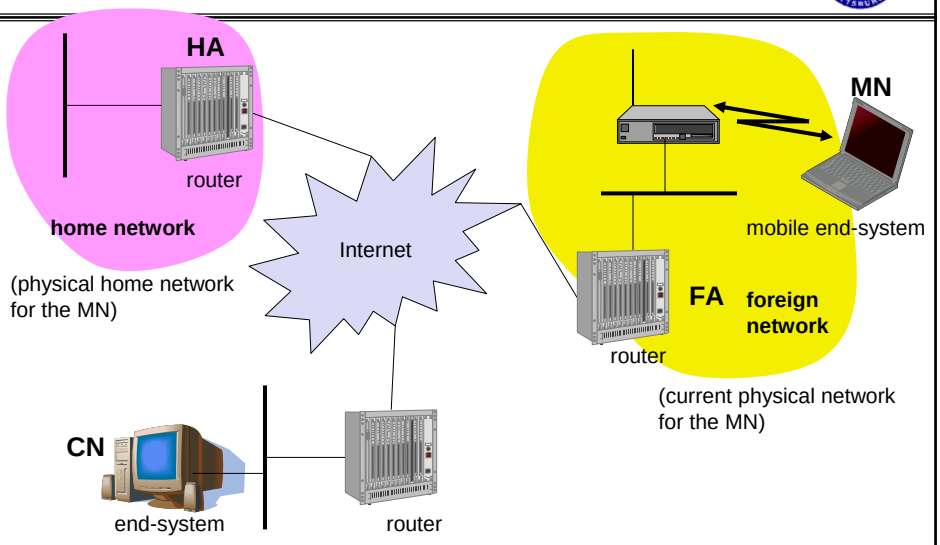
- Functional Entities in Mobile IP
  - Mobile node (MN)
  - Home agent (HA)
  - Foreign agent (FA)
- Mobile IP requires the existence of a network node known as the home agent. When the mobile node is not attached to its home network, the home agent gets all the packets destined for the mobile node and arranges to deliver them to the mobile node's current point of attachment.
- Whenever the mobile node moves, it registers its new care-of-address with its home network, the home agent delivers the packet from the home network to the care-of-address.
- In Mobile IP, the home agent redirects packets from the home network to the care-of-address as the destination IP address. The new header then encapsulates the original packet, causing the mobile node's home address to have no effect on the encapsulated packet's routing until it arrives at the care-of-address. → Tunneling

Terminology

- Mobile Node (MN)
  - system (node) that can change the point of connection to the network without changing its IP address

- Correspondent Node (CN)
  - communication partner (can be fixed or mobile)
- Home Network (HN)
  - particular network where mobile node's *home IP address* resides
- Foreign Network (FN)
  - Network where mobile node is visiting
- Home Agent (HA)
  - system in the home network of the MN, typically a router, that manages IP layer mobility.
- Foreign Agent (FA)
  - system in the current foreign network of the MN, typically a router that manages the network mobility

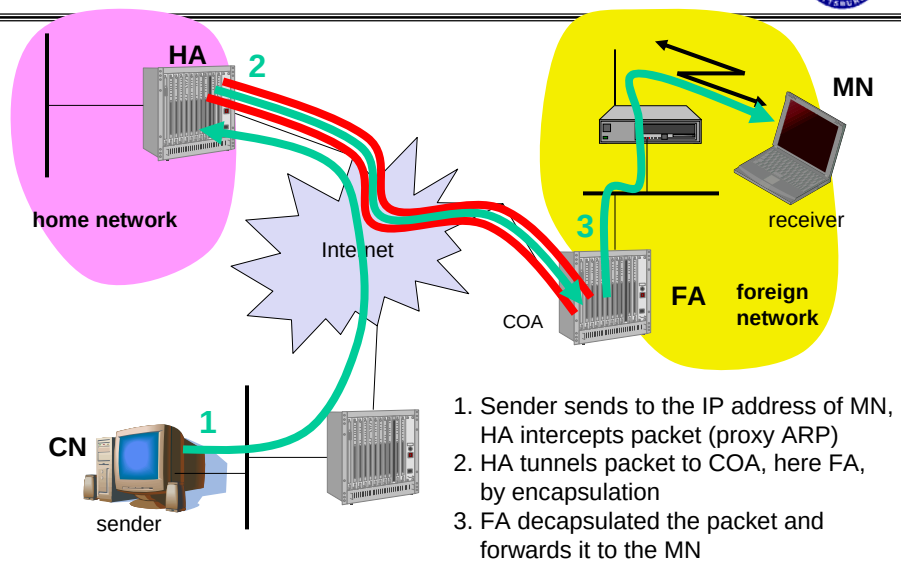
Example Scenario



Mobile IP Structure

- Home address
  - Long term IP address assigned to MN in the Home Network
  - remains unchanged regardless MN location,
  - used by DNS to locate MN
- Care-of Address (COA)
  - IP address in the Foreign Network that is the reference pointer to the MN when it is visiting the FN
  - Usually IP address of Foreign Agent
  - Option for MN to act as it's own FA in which case it is a co-located COA
- How Does Mobile IP deliver the data??
  - Home Agent
    - registers the location of the MN, reroutes IP packets sent to the MNs home address to the COA using a encapsulation/tunneling procedure
  - Foreign Agent (FA)
    - forwards the tunneled packets to the MN within the FN

Data transfer to the mobile system



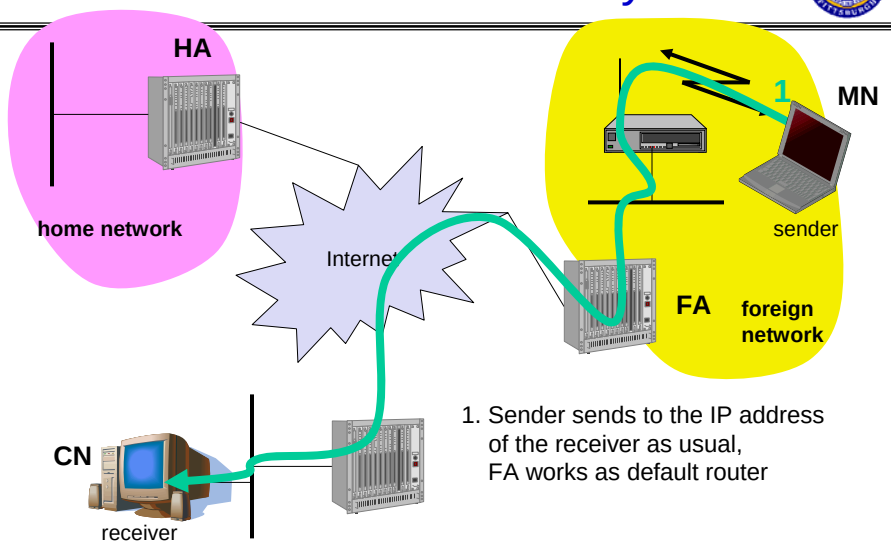
1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA decapsulated the packet and forwards it to the MN

Encapsulation

- Mandatory basic implementation (mandatory, RFC 2003)
- The outer header uses IP-in-IP as the protocol type
- The whole tunnel is equivalent to one hop from the original packet's point of view IP-in-IP-encapsulation tunnel between HA and COA

ver.	IHL	DS (TOS)	length	
IP identification			flags	fragment offset
TTL		*IP-in-IP*	IP checksum	
IP address of HA				
Care-of address COA				
ver.	IHL	DS (TOS)	length	
IP identification			flags	fragment offset
TTL		lay. 4 prot.	IP checksum	
IP address of CN				
IP address of MN				
TCP/UDP/ ... payload				

Data from the mobile system



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

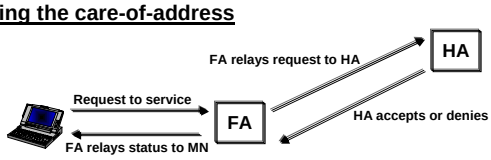
Mobile IP

Discovering the care-of-address

- The discovery process is built on top of existing standard protocol, Router Advertisement (RFC 1256).
- Home Agent and Foreign Agent broadcast agent advertisements that contain one or more care-of-address at regular intervals.
- Mobile node listens the advertisement and discovers care-of-address.
- If a mobile node needs to get a care-of-address and does not wish to wait for the periodic advertisement, the mobile node can broadcast or multicast a solicitation & it will be answered by any foreign agent or home agent that receives it.
- Home agent use agent advertisement to make themselves know, even if they do not offer any care-of-addresses.

Mobile IP

Registering the care-of-address



- Once a mobile node has a care-of-address, its home agent must find out about it.
- Mobile node sends a registration request with the care-of-address information.
- When HA receives the request, it adds the necessary information to its routing table, approves the request, and sends a registration reply back to mobile node.
- Binding: HA maintains the association of mobile node's home address and the care-of-address until registration lifetime expires. The triplet that contains home address, care-of-address, and registration lifetime is called a binding for the mobile node.

CDMA2000 Network

- **Packet Data Session**: describes an instance of continuous use of packet data service by the user. A packet data session begins when the user invokes packet data service. A packet data session ends when the user or the network terminates packet data service. During a particular packet data session, the user may change locations but the same IP address is maintained.
- **PPP Section**: A PPP session describes the time during which a particular PPP connection instance is maintained in the open state in both the mobile station and PDSN. If a user hands off from one RN to another RN but still connected to the same PDSN, the PPP session remains. If a user changes PDSN, a new session is created at the new PDSN.
- **R-P Session**: It is a logical connection established over the R-P interface for a particular PPP session. If a user changes RNs during packet data service, the R-P session between the previous RN and PDSN is released and a new R-P session is established.

Mobile IP Service (CDMA2000)

- The PPP, R-P session establishment and terminations are similar to Simple IP service except instead of CHAP and PAP, Mobile IP service is using MN-AAA Challenge Extension procedures.
- MIP – Agent Advertisements
  PDSN begins to transmission of an Agent Advertisement immediately following establishment of PPP or upon reception of an Agent Solicitation message from the mobile station.
- The mobile IP registration lifetime field in Agent Advertisement must be smaller than the PPP inactivity timer.
- Upon receiving Agent Advertisements, the mobile station sends a Mobile IP RR (Registration request)

Cdma2000 Packet Service

- PDSN keeps track of mobile state for active data session
- Mobility management by packet data location areas called PCF area
- Mobile registers with PDSN after detecting new PCF area

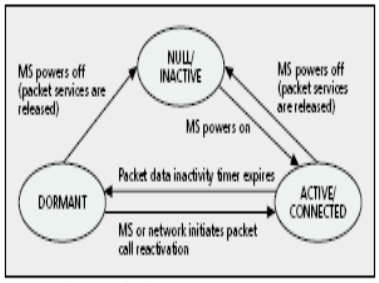


Figure 8. *cdma2000 packet data service state transitions.*

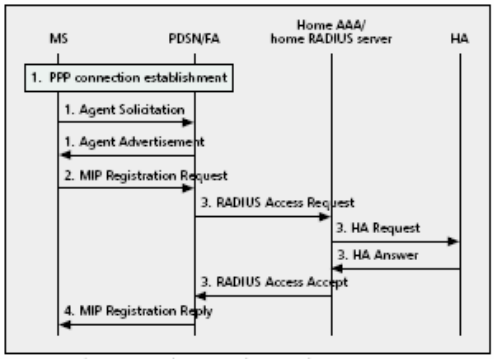


Figure 9. *cdma2000 MIP location update procedure.*

Mobility Management

PCF to PCF Handoff

- The link layer mobility management function is used to manage the change of the R-P session point of attachment while maintaining the PPP session and IP address(es). The R-P session point of attachment is the PCF. When a MS moves from one PCF to another PCF, a new R-P session is required to be setup for every packet data session.
  - The new PCF triggers a new R-P session setup.
  - If the selected PDSN is the same PDSN, then the PDSN triggers a release of the previous R-P session.
  - If a different PDSN is selected, then old R-P session will expire, unless the mobile station returns to the previous PDSN before the R-P session expires.
  - If a different PDSN is selected, then a new PPP session must be established.

PDSN to PDSN Handoff

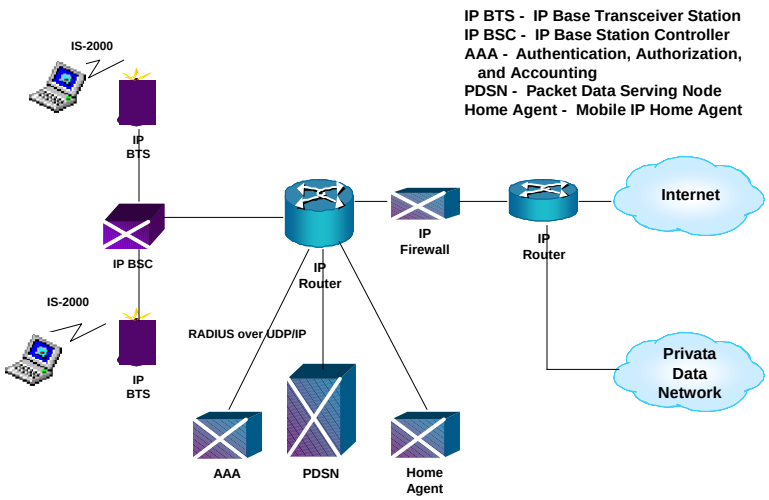
- Mobile IP provides the IP layer mobility management function that maintains persistent IP addresses across PDSNs. There is no similar IP layer mobility management function support between PDSNs for Simple IP service. For Mobile IP mobile stations, in order to maintain persistent IP addresses, the mobile station will effect a PDSN to PDSN handoff by registering with its Home Agent.
  - Establishment of new PPP session
  - Detection of new Foreign Agent via the Agent Advertisement Message
  - Authentication by RADIUS infrastructure
  - Registration with the Home Agent

Note: RN and PCF are used interchangeably here.

cdma2000 1x-EVDO

- cdma2000 1x-EVDO (Evolution to Data Only/Optimized)
  - 3G data services over IS-95a, b, cdmaone systems
    - A 1.25 MHz radio carrier is dedicated to data only (DO)
    - New radio link interface modified to better handle data - will not support voice call
      - Higher data rates – 2.4Mbps downlink/153Kbps uplink
      - Time Division Multiplexing of users (only 1 user at a time on channel) 1.6ms time slot
      - Adaptive modulation and Coding 16-QAM
      - Hybrid ARQ
      - Support for Receiver Diversity (2 EV-DO channels tied up)

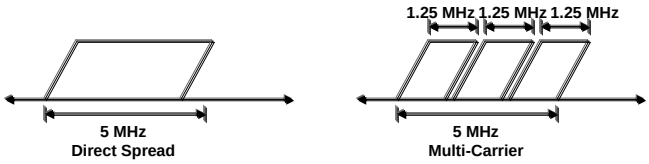
1xEVDO



cdma2000 EVDO - Multicarrier

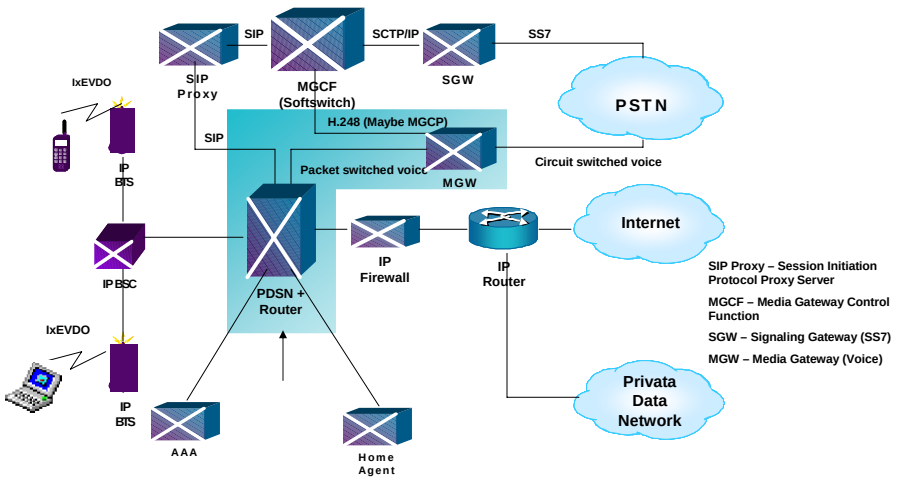
- cdma2000 1x-EVDO (Evolution to Data Only/Optimized)
  - Rev A
    - Combine multiple 1x-EVDO carriers to get higher data rates (3x is the norm)
    - Peak rates 3.1 Mbps Down, 1.8Mbps Up
    - QoS Mac layer
    - Multicast support
    - VoIP support for phone calls
      - » need additional equipment in the backhaul
      - » uses SIP for signalling

Multi-Carrier EVDO



- Multi-Carrier
  - Coded information symbols are transmitted on multiple carriers
    - e.g., Three 1.25 MHz carriers in 5 MHz Band, Six Carriers in 10 MHz Band
  - Equivalent to spreading signal over entire bandwidth allocation
  - RAKE receiver captures signal energy from all bands
  - Each forward link channel may be allocated an identical Walsh code on all carriers
  - Based on requirements for backwards compatibility, the multi-carrier approach is preferred over direct spread

1XEVDO – Rev A -- IP Data and Voice



CDMA2000 Design

- Meet IMT-2000 requirements
- Offer additional capacity and service enhancement as an evolution of IS-95 Based CDMA
- Integrated Voice and Data System
- Smooth backwards compatible evolution from existing IS-95 systems
- Nx1.25 MHz (N = 1, 3, 6, 9, 12) channel bandwidth
  - Permits deployments compatible with IS-95
  - Can be deployed in existing or newly allocated frequency bands
- Data rates from 1.2 kbps to greater than 2 Mbps are supported using
  - Variable spreading
  - Code aggregation
  - Different channel bandwidths
- Support both FDD and TDD configurations

CDMA2000 Parameters

Channel bandwidth	1.25 MHz or N x 1.25MHz
Channel structure	Direct spread spectrum or multicarrier spread spectrum
Chip rate	n x 1.2288 Mcps (n = 1, 2, …, 20) for multicarrier
Frame length	20ms for data and control, 5 ms for control information on the fundamental and dedicated control channel 1.6ms for EV-DO
Handover	Soft handover and interfrequency handover

Systems Comparison

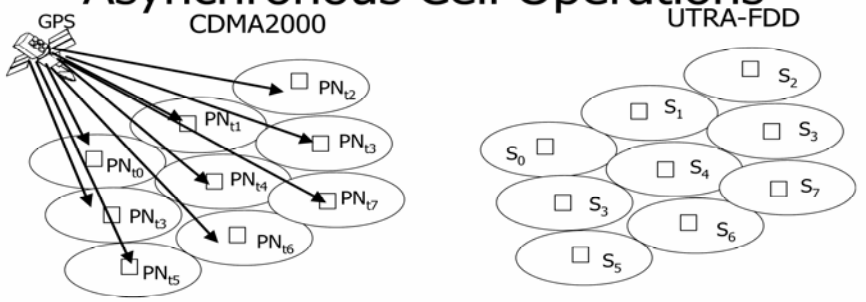
	CDMA 2000	WCDMA	GSM	IS-95
Physical Channel	1 to N x 1.25 MHz channels	5 MHz	200 kHz	1.23 MHz
Modulation	QPSK, QAM	QPSK	GMSK	OQPSK
Channel rate	N x 1.288 Mcps	3.84 Mcps	270.833kbs	1,228.8kcps
Modulation Efficiency (b/s/Hz)	1	.768	1.4	1.0

Systems Comparison

	CDMA 2000	WCDMA	GSM	IS-95
Power Control	800 Hz up and down link	1500 Hz up and down link	2Hz	800 Hz uplink
Base Station Synch	Yes using GPS	No	No	Yes, using GPS
Load Based Scheduling	Somewhat with coding and multiple carriers	Yes variable Spreading and coding, TDD mode	Voice only	Voice only
System standard	Air only at this time	Complete System	Complete System	Air only
Security	Spread Spectrum + AAA IP sec (eventually)	F1-F9 algorithms + USIM card	A3, A5, A8 algorithm + SIM card	Spread Spectrum + optional CAVE

UMTS vs. CDMA 2000

Asynchronous Cell Operations



PN_{t0-n} - Time offset scrambling code
- Cell sites transmission and reception are synchronized through GPS timing
- Adjacent cell sites use different time offsets of same scrambling code for spreading

S_{1-n} - Scrambling codes
- Cell sites are not synchronized
- Each cell site uses a different scrambling code for spreading

UMTS Terrestrial Radio Access (**UTRA**) Frequency Division Duplex (**FDD**)

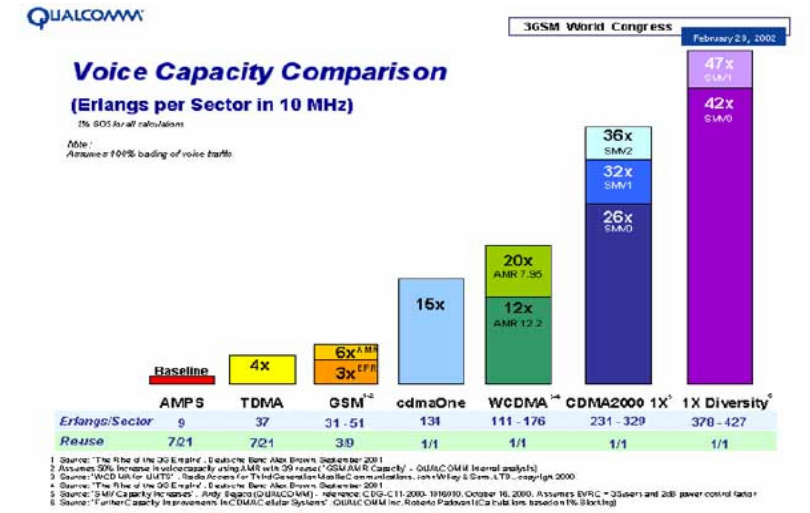
CDMA2000 Pros and Cons

- Evolution from original cdmaOne (IS-95a)
- Better migration story from 2G to 3G
  - ``In-band migration''
    - cdmaOne operators don't need additional spectrum
    - IP based
    - Higher data rates projected with multi-carrier version
- Better spectral efficiency than W-CDMA(?)
  - arguable
- CDMA2000 core network less mature
  - *cmdaone* interfaces were vendor-specific
  - *cdma2000* are as well
  - Weaker security than UMTS

UMTS Pros and Cons

- Universal Mobile Telephone Service (UMTS)
- Committed standard for Europe and likely migration path for other GSM operators
  - Legally mandated in parts of Europe
  - leverages GSM's dominant position → cheaper equipment and larger geographic roaming support
  - Standardized interfaces
  - Reuse 2.5 G equipment in backhaul
- Requires substantial new spectrum or re-engineering existing spectrum
  - 5 MHz each way
  - Slower to converge to all IP backhaul

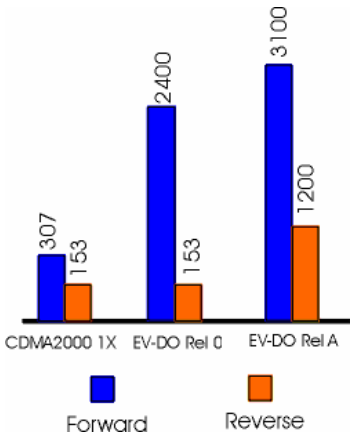
Wireless Capacity



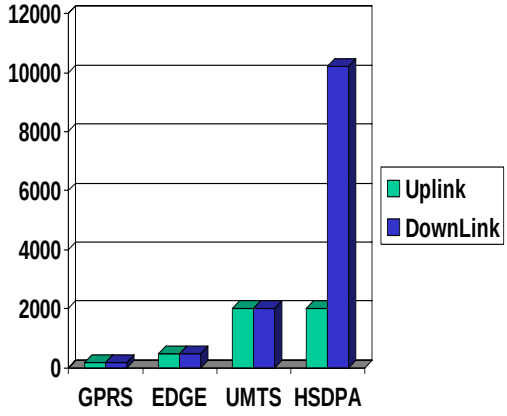
Source: Qualcomm

Wireless Capacity

Peak Data Rates in Kbps



cdma 2000



UMTS

Trends

- 2.5 -2.75G
  - More data services and usage than ever before
  - GPRS, HSCSD, EDGE, *cdma 2000 1xRTT*
  - High speed WLANs adjunct to cellular in public hotspots – several cellular providers deploying
- 3G
  - UMTS (WCDMA), *CDMA* 2000 1x EV-DO
  - Evolving to higher data rates with HSPDA,HSUPA Revs of cdma2000
- B3G/4G (Long Term Evolution – LTE)
  - All traffic IP, QoS among users/classes
  - Hybrid wireless data networks, cellular +WLAN
  - Demand?