Cellular Wireless Networks

Textbook Chapter 10

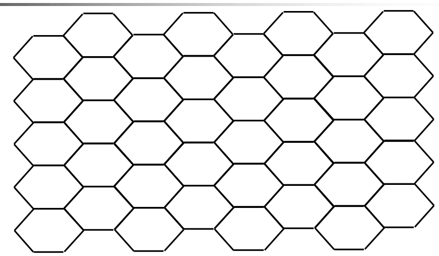
Cellular Network Organization

- Use multiple low-power transmitters (100 W or less)
- Areas divided into cells
  - Each served by its own antenna
  - Served by base station consisting of transmitter, receiver, and control unit
  - Band of frequencies allocated
  - Cells set up such that antennas of all neighbors are equidistant (hexagonal pattern)

Frequency Reuse

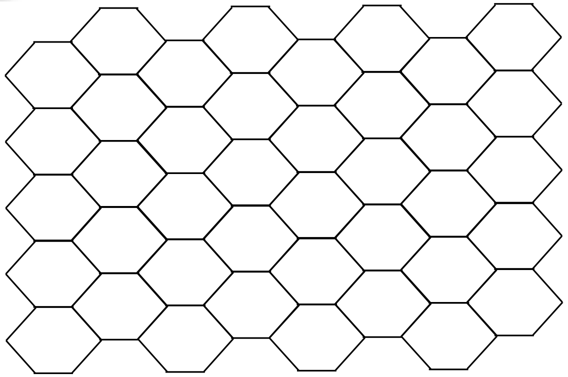
- Adjacent cells assigned different frequencies to avoid interference or crosstalk
- Objective is to reuse frequency in nearby cells
  - 10 to 50 frequencies assigned to each cell
  - Transmission power controlled to limit power at that frequency escaping to adjacent cells
  - The issue is to determine how many cells must intervene between two cells using the same frequency

Cellular Concept



- Several small cells instead of a single transmitter=> frequency reuse: better efficiency
- Fixed Channel Allocation:
- Cluster of size $N = i^2+ij+j^2$; and $D = \text{sqrt}(3N)R$
- R cell radius and
- D distance at which a frequency can be reused with acceptable interference

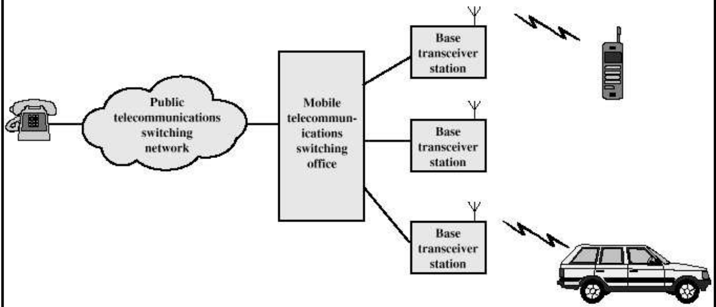
Examples



Approaches to Cope with Increasing Capacity

- Adding new channels
- Frequency borrowing – frequencies are taken from adjacent cells by congested cells
- Cell splitting – cells in areas of high usage can be split into smaller cells
- Cell sectoring – cells are divided into a number of wedge-shaped sectors, each with their own set of channels
- Microcells – antennas move to buildings, hills, and lamp posts

Cellular System Overview



Cellular Systems Terms

- Base Station (BS) – includes an antenna, a controller, and a number of receivers
- Mobile telecommunications switching office (MTSO) – connects calls between mobile units
- Two types of channels available between mobile unit and BS
  - Control channels – used to exchange information having to do with setting up and maintaining calls
  - Traffic channels – carry voice or data connection between users

Steps in an MTSO Controlled Call between Mobile Users

- Mobile unit initialization
- Mobile-originated call
- Paging
- Call accepted
- Ongoing call
- Handoff

Additional Functions in an MTSO Controlled Call

- Call blocking
- Call termination
- Call drop
- Calls to/from fixed and remote mobile subscriber

Mobile Radio Propagation Effects

- Signal strength
  - Must be strong enough between base station and mobile unit to maintain signal quality at the receiver
  - Must not be so strong as to create too much cochannel interference with channels in another cell using the same frequency band
- Fading
  - Signal propagation effects may disrupt the signal and cause errors

Handoff Performance Metrics

- Cell blocking probability – probability of a new call being blocked
- Call dropping probability – probability that a call is terminated due to a handoff
- Call completion probability – probability that an admitted call is not dropped before it terminates
- Probability of unsuccessful handoff – probability that a handoff is executed while the reception conditions are inadequate

Handoff Performance Metrics

- Handoff blocking probability – probability that a handoff cannot be successfully completed
- Handoff probability – probability that a handoff occurs before call termination
- Rate of handoff – number of handoffs per unit time
- Interruption duration – duration of time during a handoff in which a mobile is not connected to either base station
- Handoff delay – distance the mobile moves from the point at which the handoff should occur to the point at which it does occur

Handoff Strategies Used to Determine Instant of Handoff

- Relative signal strength
- Relative signal strength with threshold
- Relative signal strength with hysteresis
- Relative signal strength with hysteresis and threshold
- Prediction techniques

Power Control

- Design issues making it desirable to include dynamic power control in a cellular system
  - Received power must be sufficiently above the background noise for effective communication
  - Desirable to minimize power in the transmitted signal from the mobile
    - Reduce cochannel interference, alleviate health concerns, save battery power
  - In SS systems using CDMA, it's desirable to equalize the received power level from all mobile units at the BS

Types of Power Control

- Open-loop power control
  - Depends solely on mobile unit
  - No feedback from BS
  - Not as accurate as closed-loop, but can react quicker to fluctuations in signal strength
- Closed-loop power control
  - Adjusts signal strength in reverse channel based on metric of performance
  - BS makes power adjustment decision and communicates to mobile on control channel

Traffic Engineering

- Ideally, available channels would equal number of subscribers active at one time
- In practice, not feasible to have capacity handle all possible load
- For N simultaneous user capacity and L subscribers
  - $L < N$ – nonblocking system
  - $L > N$ – blocking system

Blocking System Performance Questions

- Probability that call request is blocked?
- What capacity is needed to achieve a certain upper bound on probability of blocking?
- What is the average delay?
- What capacity is needed to achieve a certain average delay?

Traffic Intensity

- Load presented to a system:

$$A = \lambda h$$

  - λ = mean rate of calls attempted per unit time
  - h = mean holding time per successful call
  - A = average number of calls arriving during average holding period

Capacity in Cellular Systems

- Blocking Probability (Grade Of Service): *Erlang B* formula

$$GOS = \frac{A^C / C!}{\sum_{n=0}^{C} A^n / n!}$$

- λ: calls arrival rate; T: calls average duration (service time: $1/\mu$)

Factors that Determine the Nature of the Traffic Model

- Manner in which blocked calls are handled
  - Lost calls delayed (LCD) – blocked calls put in a queue awaiting a free channel
  - Blocked calls rejected and dropped
    - Lost calls cleared (LCC) – user waits before another attempt
    - Lost calls held (LCH) – user repeatedly attempts calling
- Number of traffic sources
  - Whether number of users is assumed to be finite or infinite

First-Generation Analog

- Advanced Mobile Phone Service (AMPS)
  - In North America, two 25-MHz bands allocated to AMPS
    - One for transmission from base to mobile unit
    - One for transmission from mobile unit to base
  - Each band split in two to encourage competition (12.5MHz per operator)
  - Channels of 30 KHz: 21 CtrlCh (FSK), 395 TrafficChannels (FM voice) per operator
  - Frequency reuse exploited (R = 7)

AMPS Operation

- Subscriber initiates call by keying in phone number and presses send key
- MTSO verifies number and authorizes user
- MTSO issues message to user's cell phone indicating send and receive traffic channels
- MTSO sends ringing signal to called party
- Party answers; MTSO establishes circuit and initiates billing information
- Either party hangs up; MTSO releases circuit, frees channels, completes billing

Differences Between First and Second Generation Systems

- Digital traffic channels – first-generation systems are almost purely analog; second-generation systems are digital
- Encryption – all second generation systems provide encryption to prevent eavesdropping
- Error detection and correction – second-generation digital traffic allows for detection and correction, giving clear voice reception
- Channel access – second-generation systems allow channels to be dynamically shared by a number of users

Mobile Wireless TDMA Design Considerations

- Number of logical channels (number of time slots in TDMA frame): 8
- Maximum cell radius (R): 35 km
- Frequency: region around 900 MHz
- Maximum vehicle speed (V_m):250 km/hr
- Maximum coding delay: approx. 20 ms
- Maximum delay spread (Δ_m): 10 µs
- Bandwidth: Not to exceed 200 kHz (25 kHz per channel)

Steps in Design of TDMA Timeslot

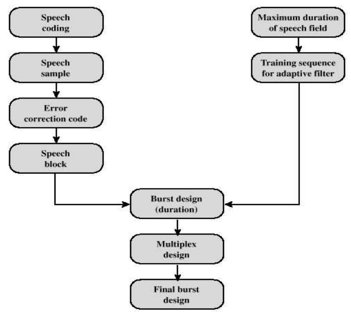


Figure 10.12 Steps in Design of TDMA Timeslot

GSM Network Architecture

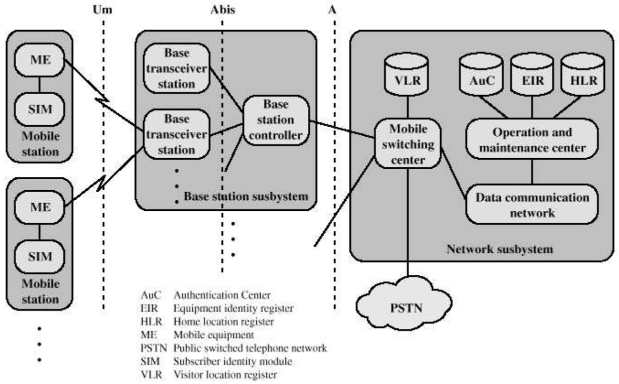
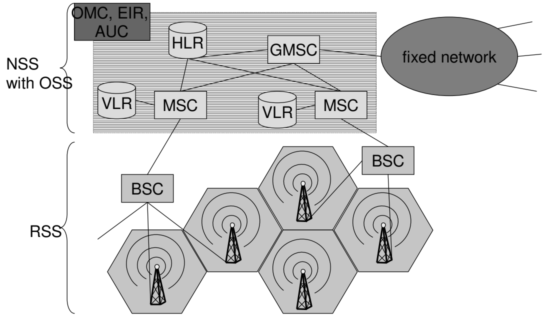


Figure 10.14 Overall GSM Architecture

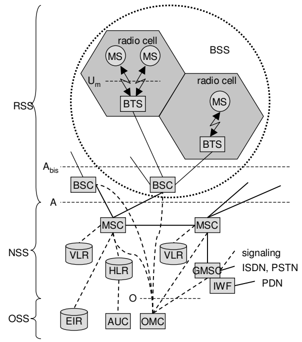
Architecture of the GSM system

- GSM is a PLMN (Public Land Mobile Network)
  - several providers setup mobile networks following the GSM standard within each country
  - components
    - MS (mobile station)
    - BS (base station)
    - MSC (mobile switching center)
    - LR (location register)
  - subsystems
    - RSS (radio subsystem): covers all radio aspects
    - NSS (network and switching subsystem): call forwarding, handover, switching
    - OSS (operation subsystem): management of the network

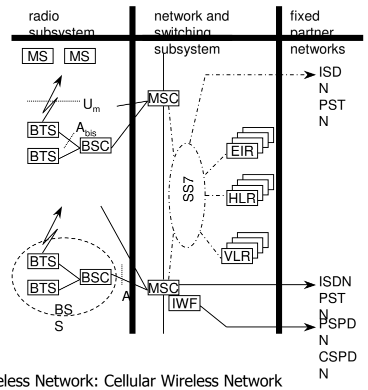
GSM: overview



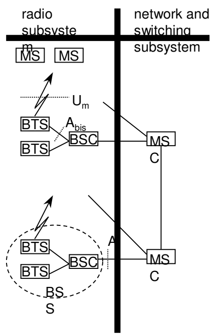
GSM: elements and interfaces



GSM: system architecture

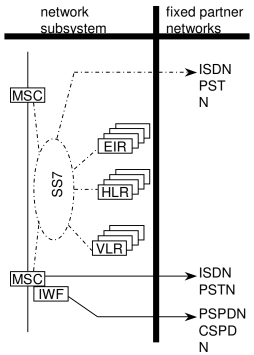


System architecture: radio subsystem



- Components
  - *MS* (Mobile Station)
  - *BSS* (Base Station Subsystem): consisting of
    - *BTS* (Base Transceiver Station): sender and receiver
    - *BSC* (Base Station Controller): controlling several transceivers
- Interfaces
  - U_m : radio interface
  - A_{bis} : standardized, open interface with 16 kbit/s user channels
  - *A*: standardized, open interface with 64 kbit/s user channels

System architecture: network and switching subsystem



Components
- *MSC* (Mobile Services Switching Center):
- *IWF* (Interworking Functions)

- *ISDN* (Integrated Services Digital Network)
- *PSTN* (Public Switched Telephone Network)
- *PSPDN* (Packet Switched Public Data Net.)
- *CSPDN* (Circuit Switched Public Data Net.)

Databases
- *HLR* (Home Location *R*egister)
- *VLR* (Visitor Location *R*egister)
- *EIR* (Equipment Identity Register)

Radio subsystem

- The Radio Subsystem (RSS) comprises the cellular mobile network up to the switching centers
- Components
  - Base Station Subsystem (BSS):
    - Base Transceiver Station (BTS): radio components including sender, receiver, antenna - if directed antennas are used one BTS can cover several cells
    - Base Station Controller (BSC): switching between BTSs, controlling BTSs, managing of network resources, mapping of radio channels (U_m) onto terrestrial channels (A interface)
    - BSS = BSC + sum(BTS) + interconnection
  - Mobile Stations (MS)

Mobile Station

- Mobile station communicates across Um interface (air interface) with base station transceiver in same cell as mobile unit
- Mobile equipment (ME) – physical terminal, such as a telephone or PCS
  - ME includes radio transceiver, digital signal processors and subscriber identity module (SIM)
- GSM subscriber units are generic until SIM is inserted
  - SIMs roam, not necessarily the subscriber devices

Base Station Subsystem (BSS)

- BSS consists of base station controller and one or more base transceiver stations (BTS)
- Each BTS defines a single cell
  - Includes radio antenna, radio transceiver and a link to a base station controller (BSC)
- BSC reserves radio frequencies, manages handoff of mobile unit from one cell to another within BSS, and controls paging

Network Subsystem (NS)

- NS provides link between cellular network and public switched telecommunications networks
  - Controls handoffs between cells in different BSSs
  - Authenticates users and validates accounts
  - Enables worldwide roaming of mobile users
- Central element of NS is the mobile switching center (MSC)

Mobile Switching Center (MSC) Databases

- Home location register (HLR) database – stores information about each subscriber that belongs to it
- Visitor location register (VLR) database – maintains information about subscribers currently physically in the region
- Authentication center database (AuC) – used for authentication activities, holds encryption keys
- Equipment identity register database (EIR) – keeps track of the type of equipment that exists at the mobile station

TDMA Format – Time Slot Fields

- Trail bits – allow synchronization of transmissions from mobile units
- Encrypted bits – encrypted data
- Stealing bit - indicates whether block contains data or is "stolen"
- Training sequence – used to adapt parameters of receiver to the current path propagation characteristics
  - Strongest signal selected in case of multipath propagation
- Guard bits – used to avoid overlapping with other bursts

GSM Speech Signal Processing

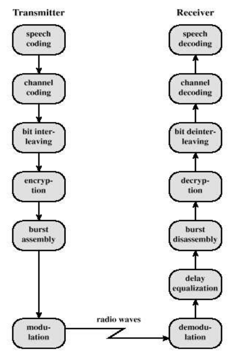
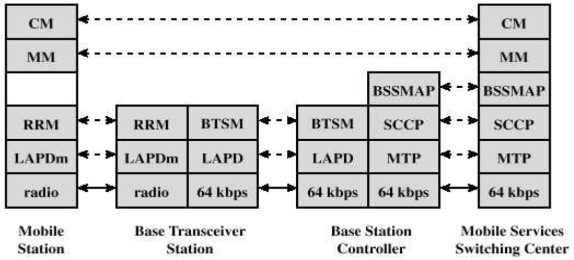


Figure 10.16 GSM Speech Signal Processing

GSM Signaling Protocol Architecture



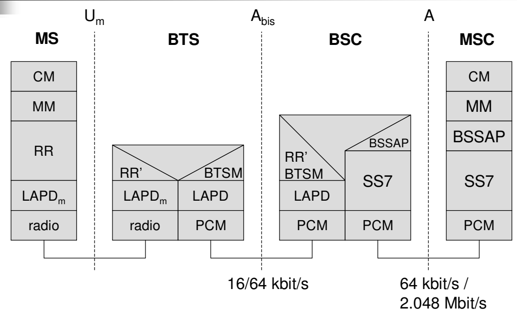
BSSMAP = BSS mobile application part
BTSM = BTS management
CM = connection management
LAPD = link access protocol, D channel
MM = mobility management
MTP = message transfer part
RRM = radio resources management
SCCP = signal connection control part

Figure 10.17 GSM Signaling Protocol Architecture

Functions Provided by Protocols

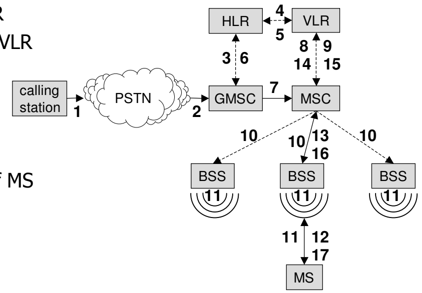
- Protocols above the link layer of the GSM signaling protocol architecture provide specific functions:
  - Radio resource management
  - Mobility management
  - Connection management
  - Mobile application part (MAP)
  - BTS management

GSM protocol layers for signaling



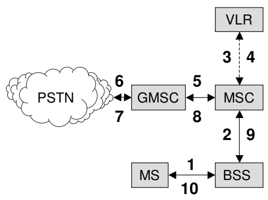
Mobile Terminated Call

- 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

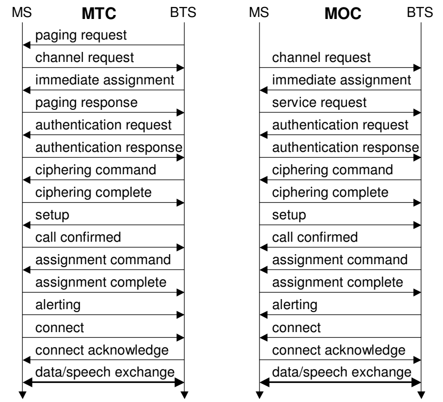


Mobile Originated Call

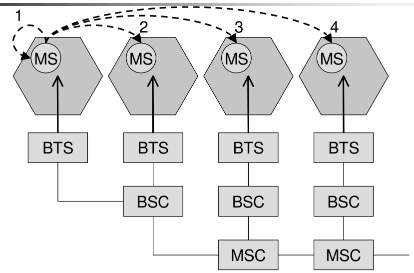
- 1, 2: connection request
- 3, 4: security check
- 5-8: check resources (free circuit)
- 9-10: set up call



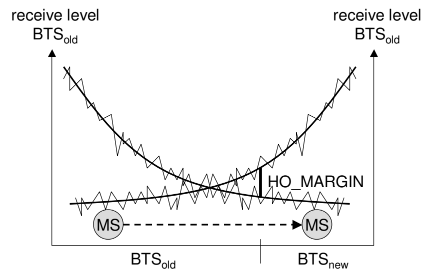
MTC/MOC



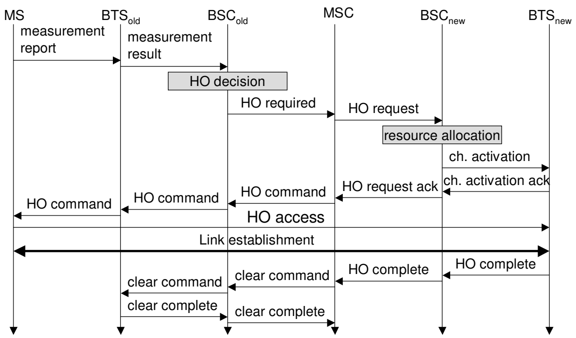
4 types of handover



Handover decision



Handover procedure

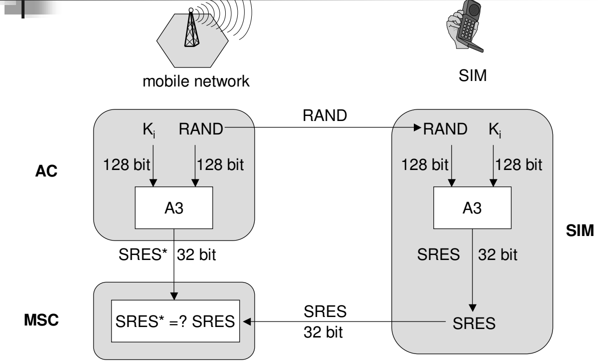


Security in GSM

- Security services
  - access control/authentication
    - user ⌫ SIM (Subscriber Identity Module): secret PIN (personal identification number)
    - SIM ⌫ network: challenge response method
  - confidentiality
    - voice and signaling encrypted on the wireless link (after successful authentication)
  - anonymity
    - temporary identity TMSI (Temporary Mobile Subscriber Identity)
    - newly assigned at each new location update (LUP)
    - encrypted transmission
- 3 algorithms specified in GSM
  - A3 for authentication ("secret", open interface)
  - A5 for encryption (standardized)
  - A8 for key generation ("secret", open interface)

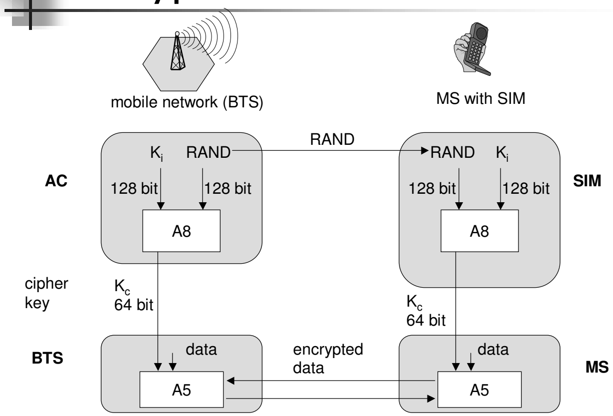
"secret":
• A3 and A8 available via the Internet
• network providers can use stronger mechanisms

GSM - authentication



K_i: individual subscriber authentication key SRES: signed response

GSM - key generation and encryption



Data services in GSM I

- Data transmission standardized with only 9.6 kbit/s
  - advanced coding allows 14,4 kbit/s
  - not enough for Internet and multimedia applications
- HSCSD (High-Speed Circuit Switched Data)
  - already standardized
  - bundling of several time-slots to get higher AIUR (Air Interface User Rate) (e.g., 57.6 kbit/s using 4 slots, 14.4 each)
  - advantage: ready to use, constant quality, simple
  - disadvantage: channels blocked for voice transmission

AIUR [kbit/s]	TCH/F4.8	TCH/F9.6	TCH/F14.4
4.8	1		
9.6	2	1	
14.4	3		1
19.2	4	2	
28.8		3	2
38.4		4	
43.2			3
57.6			4

Data services in GSM II

- GPRS (General Packet Radio Service)
  - packet switching
  - using free slots only if data packets ready to send (e.g., 115 kbit/s using 8 slots temporarily)
  - standardization 1998, introduced 2000
  - advantage: one step towards 3G, more flexible
  - disadvantage: more investment needed
- GPRS network elements
  - GSN (GPRS Support Nodes): GGSN and SGSN
  - GGSN (Gateway GSN)
    - interworking unit between GPRS and PDN (Packet Data Network)
  - SGSN (Serving GSN)
    - supports the MS (location, billing, security)
  - GR (GPRS Register)
    - user addresses

GPRS quality of service

Reliability class	Lost SDU probability	Duplicate SDU probability	Out of sequence SDU probability	Corrupt SDU probability
1	10^{-9}	10^{-9}	10^{-9}	10^{-9}
2	10^{-4}	10^{-5}	10^{-5}	10^{-6}
3	10^{-2}	10^{-5}	10^{-5}	10^{-2}

Delay class	SDU size 128 byte		SDU size 1024 byte	
	mean	95 percentile	mean	95 percentile
1	< 0.5 s	< 1.5 s	< 2 s	< 7 s
2	< 5 s	< 25 s	< 15 s	< 75 s
3	< 50 s	< 250 s	< 75 s	< 375 s
4	unspecified			

IS-95 (CdmaOne): [TIA/EIA IS-95]

- IS-95: standard for the radio interface
- IS-41: standard for the network part
- Operates of 800MHz and 1900MHz bands
- Uses DS-CDMA technology (1.2288 Mchips/s)
- Forward link (downlink): ½ convolutional code, interleaved, 64 chips spreading sequence (Walsh-Hadamard functions)
- pilot channel (code 0), synchronization channel (code 32), 7 paging channels, upto 63 traffic channels
- Reverse link (uplink): 1/3 convolutional code, interleaved, 6 bits are mapped into a Walsh-Hadamard sequence, spreading using a User-BaseStation specific code (with period 2^{42}-$1/2^{15}$)
- Tight power control (open-loop, fast closed loop)

Advantages of CDMA Cellular

- Frequency diversity – frequency-dependent transmission impairments have less effect on signal
- Multipath resistance – chipping codes used for CDMA exhibit low cross correlation and low autocorrelation
- Privacy – privacy is inherent since spread spectrum is obtained by use of noise-like signals
- Graceful degradation – system only gradually degrades as more users access the system

Drawbacks of CDMA Cellular

- Self-jamming – arriving transmissions from multiple users not aligned on chip boundaries unless users are perfectly synchronized
- Near-far problem – signals closer to the receiver are received with less attenuation than signals farther away
- Soft handoff – requires that the mobile acquires the new cell before it relinquishes the old; this is more complex than hard handoff used in FDMA and TDMA schemes

Mobile Wireless CDMA Design Considerations

- RAKE receiver – when multiple versions of a signal arrive more than one chip interval apart, RAKE receiver attempts to recover signals from multiple paths and combine them
  - This method achieves better performance than simply recovering dominant signal and treating remaining signals as noise
- Soft Handoff – mobile station temporarily connected to more than one base station simultaneously

Principle of RAKE Receiver

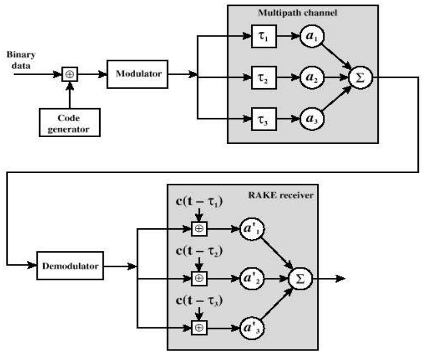


Figure 10.18 Principle of RAKE Receiver [PRAS98]

Types of Channels Supported by Forward Link

- Pilot (channel 0) - allows the mobile unit to acquire timing information, provides phase reference and provides means for signal strength comparison
- Synchronization (channel 32) - used by mobile station to obtain identification information about cellular system
- Paging (channels 1 to 7) - contain messages for one or more mobile stations
- Traffic (channels 8 to 31 and 33 to 63) – the forward channel supports 55 traffic channels

Forward Traffic Channel Processing Steps

- Speech is encoded at a rate of 8550 bps
- Additional bits added for error detection
- Data transmitted in 2-ms blocks with forward error correction provided by a convolutional encoder
- Data interleaved in blocks to reduce effects of errors
- Data bits are scrambled, serving as a privacy mask

Forward Traffic Channel Processing Steps (cont.)

- Power control information inserted into traffic channel
- DS-SS function spreads the 19.2 kbps to a rate of 1.2288 Mbps using one row of 64 x 64 Walsh matrix
- Digital bit stream modulated onto the carrier using QPSK modulation scheme

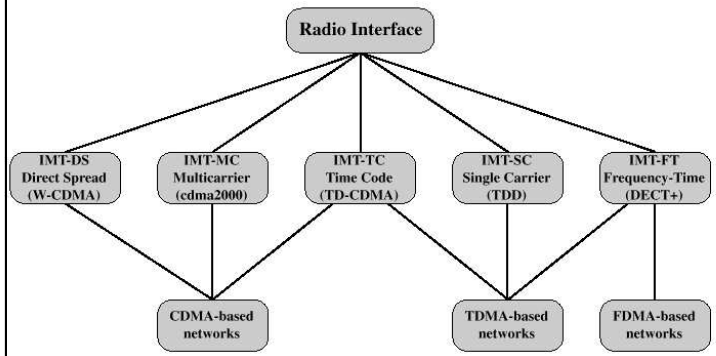
ITU's View of Third-Generation Capabilities

- Voice quality comparable to the public switched telephone network
- 144 kbps data rate available to users in high-speed motor vehicles over large areas
- 384 kbps available to pedestrians standing or moving slowly over small areas
- Support for 2.048 Mbps for office use
- Symmetrical / asymmetrical data transmission rates
- Support for both packet switched and circuit switched data services

ITU's View of Third-Generation Capabilities

- An adaptive interface to the Internet to reflect efficiently the common asymmetry between inbound and outbound traffic
- More efficient use of the available spectrum in general
- Support for a wide variety of mobile equipment
- Flexibility to allow the introduction of new services and technologies

Alternative Interfaces



CDMA Design Considerations

- Bandwidth – limit channel usage to 5 MHz
- Chip rate – depends on desired data rate, need for error control, and bandwidth limitations; 3 Mcps or more is reasonable
- Multirate – advantage is that the system can flexibly support multiple simultaneous applications from a given user and can efficiently use available capacity by only providing the capacity required for each service