Virtual University of Pakistan

Federal Government University

# Wireless Networks

## Course Code – CS-718

**Course Instructor:**

**Dr. Ghalib A. Shah**
**Virtual University of Pakistan**

### Reference Books:

1. Wireless Communications: Principles and Practices by T. S. Rappaport
2. Wireless Communications and Networks by William Stallings
3. WCDMA for UMTS: Radio Access for Third Generation Mobile Communication by H. Holma and A. Toskala
4. CDMA2000 Evolution: System Concepts and Design Principles by K. Etemad
5. WLANs and WPANs towards 4G Wireless by R. Parsad and L. Munoz
6. 802.11 Wireless Networks: The Definitive Guide by Matthew Gast

**Video Links:** http://www.vumultan.com/CS718Video.aspx

**Published By:** www.vumultan.com

# CS718 – Wireless Communication

# Lecture 1
# Introduction to Wireless Communication

## Course Basics

- Instructor : Dr. Ghalib A. Shah
- Pre-requisite : Data Communication and Networks
- Text books
    1. Wireless Communication and Networks, 2nd Ed., W. Stalling.
    2. Wireless Communications: Principles and Practices, 2nd Ed., T. S. Rappaport.
    3. The Mobile Communications Handbook, J. D. Gibson

## Objectives of Course

- Introduce
    - ✓ Basics of wireless communication
    - ✓ Evolution of modern wireless communication systems
    - ✓ Wireless Networks
    - ✓ Research issues in emerging wireless networks
- Outcomes
    - ✓ Adequate knowledge of wireless networks
    - ✓ Able to carry research in different domains of wireless networks

## Course Syllabus

- Introduction to wireless communication
- Evolution of wireless communication systems
- Medium access techniques
- Propagation models
- Error control techniques
- Cellular systems
    - ✓ AMPS, IS-95, IS-136, GSM,
- Wireless networks
    - ✓ GPRS, EDGE, WCDMA, cdma2000, Mobile IP, WLL, WLAN and Bluetooth
- Emerging networks
    - ✓ WiMAX, MANET, WSN

## Introduction to Wireless Communication

I. The Wireless vision
II. Radio Waves
III. Channel Capacity
IV. Signal-to-Noise Ratio
V. EM Spectru

## The Wireless vision

- What is wireless communication?
- What are the driving factors?
    - ✓ An explosive increase in demand of tetherless connectivity.
    - ✓ Dramatic progress in VLSI technology
        - o Implementation of efficient signal processing algorithms.

- New Coding techniques

✓ Success of 2G wireless standards (GSM)

**What is wireless communication?**

WC is one of the most vibrant areas of communication field today. While it has been a topic of study since 1960s but the last decade has seen a surge of research activities in this area. This is due to influence of several factors

1. First there has been an explosive increase in demand of tetherless connectivity, mainly by cellular telephony but expected by wireless data applications.
2. Second the dramatic progress in VLSI technology has enabled implementation of efficient signal processing algorithms and coding techniques

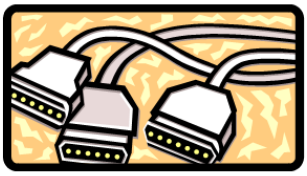
When two parties communicate without having any physical contact or medium of communication

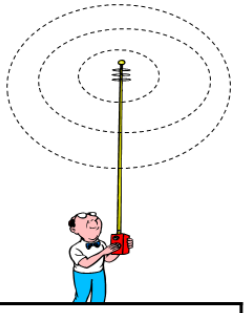
There are several driving factors of its popularity.

i. People want connectivity anywhere anytime for example, at airports, hotels, customers place, or group of people wants to share data at any location. Such requirements have made the wireless connectivity indispensable.

ii. Keep in mind that the course mainly focuses on wireless networks rather than communication techniques.

**Wired Vs. Wireless Communication**





| Wired | Wireless |
|---|---|
| Each cable is a different channel | One media (cable) shared by all |
| Signal attenuation is low | High signal attenuation |
| No interference | High interference<br>noise; co-channel interference; adjacent channel interference |

**Why go wireless?**

- Advantages
  - ✓ Sometimes it is impractical to lay cables
  - ✓ User mobility
  - ✓ Cost
- Limitations
  - ✓ Bandwidth
  - ✓ Fidelity
  - ✓ Power
  - ✓ (In) security

**Electromagnetic Signal**

- Function of time
- Can also be expressed as a function of frequency
  - ✓ Signal consists of components of different frequencies
- EM signal is used as a means to transmit information. EM is a function of time but it can also be expressed as a function of frequency
- That is the signal consists of components of frequencies. However, the frequency domain view of a signal is more important.

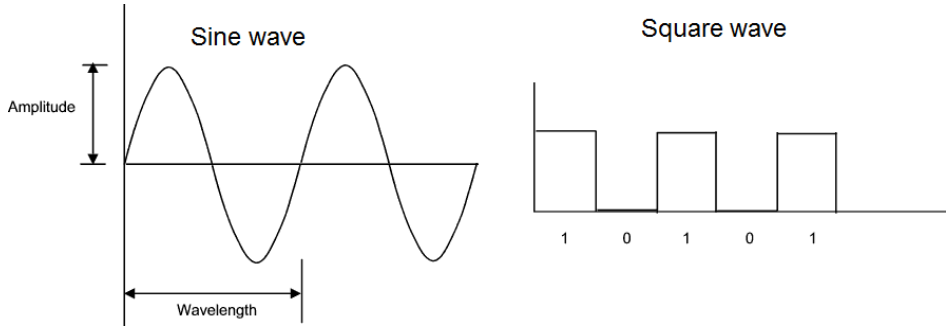
**Time-Domain Concepts**

In time domain, the signal can be either analog or digital.

- Analog signal - signal intensity varies in a smooth fashion over time.
  - ✓ For example in speech, voice changes its amplitude/intensity over time with continuous change.
  - ✓ No breaks or discontinuities in the signal
- Digital signal - signal intensity maintains a constant level for some period of time and then changes to another constant level
  - ✓ Digital signals are binary 0s, 1s or text
- Periodic signal - analog or digital signal pattern that repeats over time

  $s(t + T) = s(t)$ $-\infty < t < +\infty$

  where T is the period of the signal
- Aperiodic signal - analog or digital signal pattern that doesn't repeat over time
- Peak amplitude (A) - maximum value or strength of the signal over time; typically measured in volts
- Frequency (f )
  - ✓ Rate, in cycles per second, or Hertz (Hz) at which the signal repeats
- Period (T ) - amount of time it takes for one repetition of the signal
  - ✓ $T = 1/f$
- Phase ($\phi$) - measure of the relative position in time within a single period of a signal
- Wavelength ($\lambda$) - distance occupied by a single cycle of the signal
  - ✓ Or, the distance between two points of corresponding phase of two consecutive cycles
  - ✓ $\lambda = vT$



- ✓ General sine wave s(t ) = A sin(2πft + ϕ)
- ✓ Figure shows the effect of varying each of the three parameters
  - a) A = 1, f = 1 Hz, ϕ = 0; thus T = 1s
  - b) Reduced peak amplitude; A=0.5
  - c) Increased frequency; f = 2, thus T = ½
  - d) Phase shift; ϕ = π/4 radians (45 degrees)
- ✓ note: 2π radians = 360° = 1 period

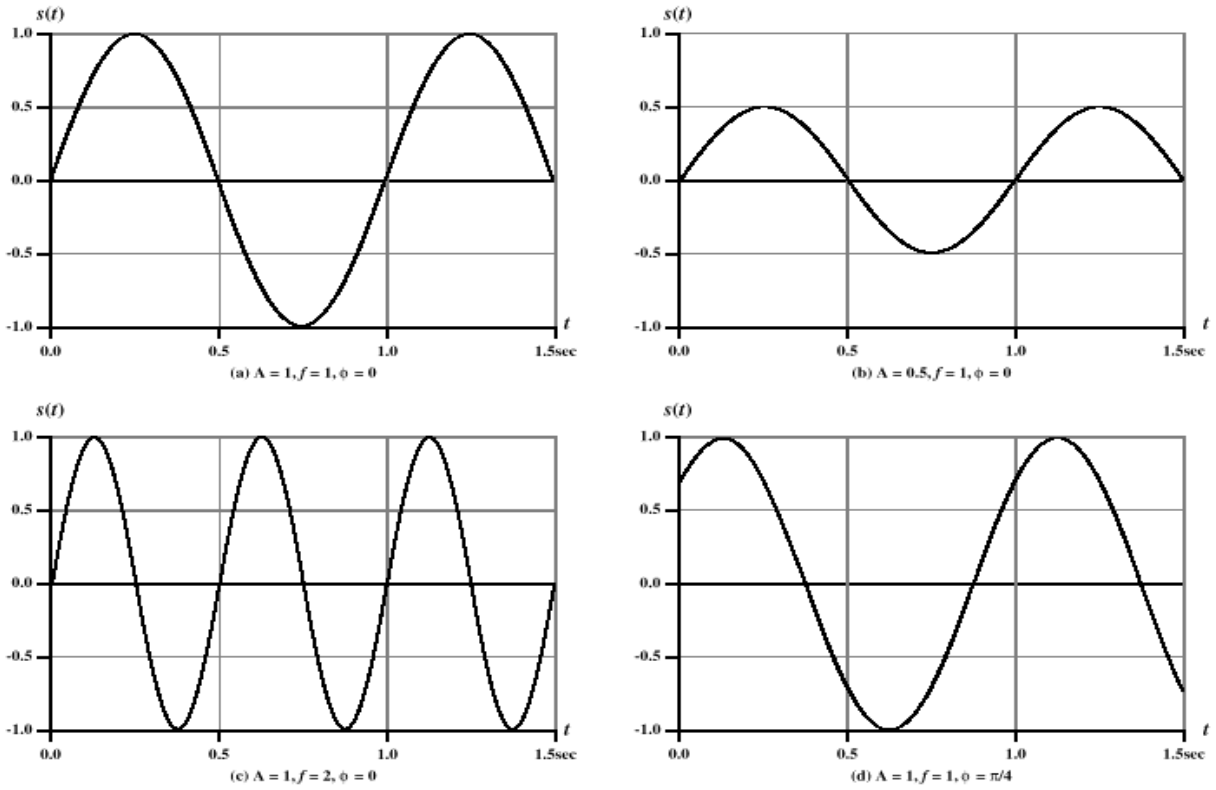



**Figure 2.3** $s(t) = A \sin(2\ ft + \phi)$

**Frequency-Domain Concepts**

- Fundamental frequency - when all frequency components of a signal are integer multiples of one frequency, it's referred to as the fundamental frequency
- Spectrum - range of frequencies that a signal contains
- Absolute bandwidth - width of the spectrum of a signal
- Effective bandwidth (or just bandwidth) - narrow band of frequencies that most of the signal's energy is contained in
- Any electromagnetic signal can be shown to consist of a collection of periodic analog signals (sine waves) at different amplitudes, frequencies, and phases
- The period of the total signal is equal to the period of the fundamental frequency

**Relationship between Data Rate and Bandwidth**

- The greater the bandwidth, the higher the information-carrying capacity
- Conclusions
  - ✓ Any digital waveform will have infinite bandwidth
  - ✓ BUT the transmission system will limit the bandwidth that can be transmitted
  - ✓ AND, for any given medium, the greater the bandwidth transmitted, the greater the cost
  - ✓ HOWEVER, limiting the bandwidth creates distortions

**About Channel Capacity**

- Impairments, such as noise, limit data rate that can be achieved
- For digital data, to what extent do impairments limit data rate?
- Channel Capacity – the maximum rate at which data can be transmitted over a given communication path, or channel, under given conditions

**Concepts Related to Channel Capacity**

- Data rate - rate at which data can be communicated (bps)
- Noise - average level of noise over the communications path
- Error rate - rate at which errors occur
- Error = transmit 1 and receive 0; transmit 0 and receive 1

**Nyquist Bandwidth**

- For binary signals (two voltage levels)
  - ✓ C = 2B
- With multilevel signaling
  - ✓ C = 2B $\log_2$ M
    M = number of discrete signal or voltage levels
- Give an example for M = 8 and B 3100 C = 18600
- So the data rate can be increased by increasing the number of different signal elements. This places an extra burden on receiver

**Signal-to-Noise Ratio**

- Ratio of the power in a signal to the power contained in the noise that's present at a particular point in the transmission
- Typically measured at a receiver
- Signal-to-noise ratio (SNR, or S/N)

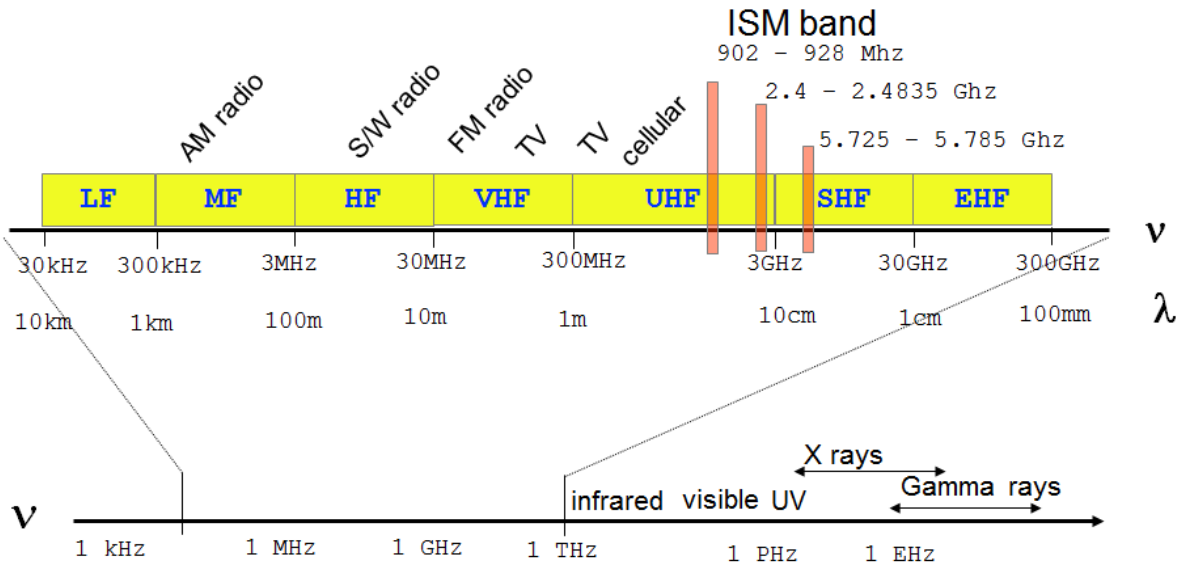
$$(SNR)_{\text{dB}} = 10\log_{10}\frac{\text{signal power}}{\text{noise power}}$$

- A high SNR means a high-quality signal, lower number of required intermediate repeaters
- SNR sets upper bound on achievable data rate
- SNR expresses the amount in decibels that the intended signal exceeds the noise level.

**Shannon Capacity Formula**

- Equation: $C = B\log_2(1+\text{SNR})$
- Represents theoretical maximum that can be achieved
- In practice, only much lower rates achieved
- Formula assumes white noise (thermal noise)
- Impulse noise is not accounted for
- Attenuation distortion or delay distortion not accounted for
- Nyquist formula indicates that all other things being equal, doubling the bandwidth doubles the data rate
- Shannon investigates relationship of data rate with bandwidth and noise.
- From the Eq., data rate can be increased either by increasing bandwidth or signal strength.
- LowerF = 3Mhz, UpperF = 4 MHz SNR = 24 then
  B = 4 – 3 = 1 MHz
  SNRdb = 10log10 (24) = 251
  C = 10^6 x log2(1 + 251)
  Approx. 10^6 x 8 bps = 8 Mbps
  For this data rate, the number of signal levels by Nyquist formula are M = 16

**EM Spectrum**




Propagation characteristics are different in each frequency band

- 20 Hz to ~14 kHz, acoustic — normal range of adult human hearing (most children and some animals perceive sounds outside this range, most teens and children can hear frequencies from 14 kHz up to ~16 kHz where most adults can't)
- 530 kHz to 1.710 MHz, electromagnetic — AM radio broadcasts
- 42 MHz to 260 MHz, electromagnetic — VHF terrestrial TV broadcast channels

- 88 MHz to 108 MHz, electromagnetic — FM radio broadcasts
- 902 MHz to 928 MHz, common cordless telephone frequency in the US
- 0.8 to 2.3 GHz, (electromagnetic) - mobile phone conversation channels.
- 2.4 GHz, (electromagnetic) - microwave ovens, Wireless LANs and cordless phones (starting in 1998).
- 5.8 GHz, cordless phone frequency introduced in 2003
- 428 THz to 750 THz, electromagnetic — visible light, from red to violet
- 30 Petahertz (PHz), electromagnetic — x-rays
- 300 Exahertz (EHz) and above - gamma rays

**Design Challenges**

- Two fundamental aspects of wireless communication
  - ✓ Channel fading
    - Multipath fading
    - Path loss via distance attenuation
    - Shadowing by obstacles
  - ✓ Interference
    - Multiple transmitters to a common receiver
    - Multiple transmitters to multiple receivers
- In wireless telecommunications, **multipath** is the propagation phenomenon that results in radio signals' reaching the receiving antenna by two or more paths. Causes of multipath include atmospheric ducting, ionospheric reflection and refraction, and reflection from terrestrial objects, such as mountains and buildings.
- The primary concern in wireless systems is to increase the reliability of air interface.
- This is achieved by controlling the channel fading and interference.
- Recently the focus has shifted to spectral efficiency.

**Summary**

- EM seen in domain of time and frequency
- Analog and digital signal
- Periodic and aperiodic signal
- Frequency, amplitude and wavelength of signal
- Fundamental frequency
- Channel capacity
  - ✓ Nyquist formula
  - ✓ Shannon formula
- EM Spectrum
- Design challenges in wireless communication

**Course Syllabus**

- Introduction to wireless communication (3 hrs)
- Evolution of wireless communication systems (3 hrs)
- Medium access techniques (3 hrs)
- Propagation models (3 hrs)

- Error control techniques (3 hrs)
- Cellular systems (9 hrs)
  - ✓ AMPS, IS-95, IS-136, GSM,
- Wireless networks (12 hrs)
  - ✓ GPRS, EDGE, WCDMA, cdma2000, Mobile IP, WLL, WLAN and Bluetooth
- Emerging networks (9 hrs)
  - ✓ WiMAX, MANET, WSN, etc

## Lecture 2
## Introduction to Wireless Communication

**Outlines**

- Review of previous lecture #1
- Wireless Transmission
- Encoding/Modulation
- Noises
- Losses/Gain
- Summary of today's lecture

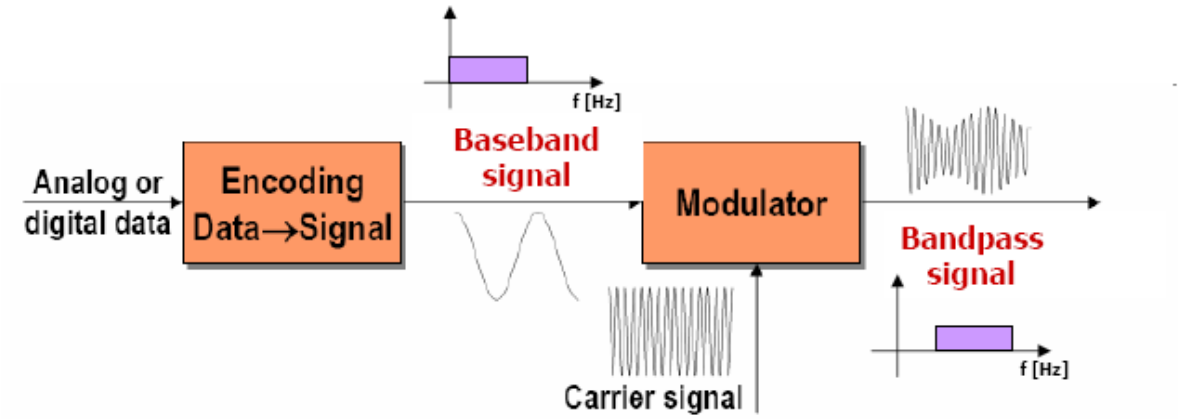
**Last Lecture Review**

- Objectives of course
- Course syllabus
- Wireless vision
  - ✓ Driving factors
    - Tetherless connectivity
    - VLSI technology
    - Success of 2G systems
  - ✓ Wireless Prons/Cons
  - ✓ EM Signal
    - Time domain concept: analog, digital, periodic, aperiodic, Amplitude, frequency, period, wavelength
    - Frequency domain concept: fundamental frequency, spectrum, absolute bandwidth, effective bandwidth
    - Channel capacity: Nyquist formulation, SNR, Shannon formula
  - ✓ EM Spectrum

- In the last lecture that was also the first lecture of this course, we discuss the objectives of the course. Our focus will be to introduce the current wireless networking technologies and recent developments in wireless networks.
- Thereafter, the course syllabus was presented. The course consists of different cellular systems like GSM, AMPS , wireless networks like GPRS, EDGE, WLAN and some emerging networking technologies like wireless sensor networks, personal area networks etc.

**Transmission in Wireless Domain**

- Baseband Signal
  - ✓ obtained by converting analog or digital data into analog or digital signal, bandwidth = [0, fmax)
- Bandpass Signal
  - ✓ band-limited signal whose minimum frequency is different from zero, bandwidth = [f1, f2)




**Wireless Transmission**

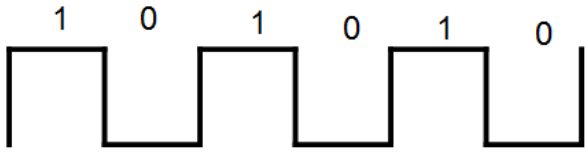
- Virtually impossible to transmit baseband signals in wireless domain.
- Single transmission medium (air) for all users and applications.
- In wired networks, new wiring can be added to accommodate new applications/users – one wire for telephone, one for cable, one for LAN, etc.
- Antenna size must correspond to signal's wavelength
  - ✓ 1 MHz signal → few 100 m-s high antenna;
  - ✓ 1 GHz signal → few cm-s high antenna
- Characteristics of wireless-signal propagation heavily depend on signal's frequency
- Low-frequency signals 'tilt downwards' and follow the Earth's surface
- Do not propagate very far

**Signal Encoding/Modulation**

- We are concerned with transmitting digital data.
- Some transmission media will only propagate analog signals e.g., optical fiber and unguided media
- Therefore, we will discuss transmitting digital data using analog signals.
- The most familiar use of this transformation is transmitting digital data through the public telephone network.
- In computer networks no matter if its wired or wireless, we are interested to transfer digital information from one end to other end. Therefore, we will discuss the techniques which are used to transmit digital data.

**Encoding**

- Each pulse in digital signal is a signal element.
- Binary data are transmitted by encoding each data bit into signal elements.




- There can be one-to-one correspondence between data elements and signal elements or one-to-multiple/multiple-to-one

- Data rate: the rate in bits/sec that data are transmitted
- Modulation rate: the rate at which signal element is changed and is expressed in baud i.e. signal elements/second.
- The duration or length of bit is the amount of time it takes for the transmitter to emit the bit. For data rate R, bit time is 1/R.
- At receiver
  - ✓ The bit time must be known i.e. start and end time of bit.
  - ✓ The encoding must be known i.e. high (1) and low (0)
  - ✓ These tasks are performed by sampling each bit position at middle of interval and comparing the value to threshold.

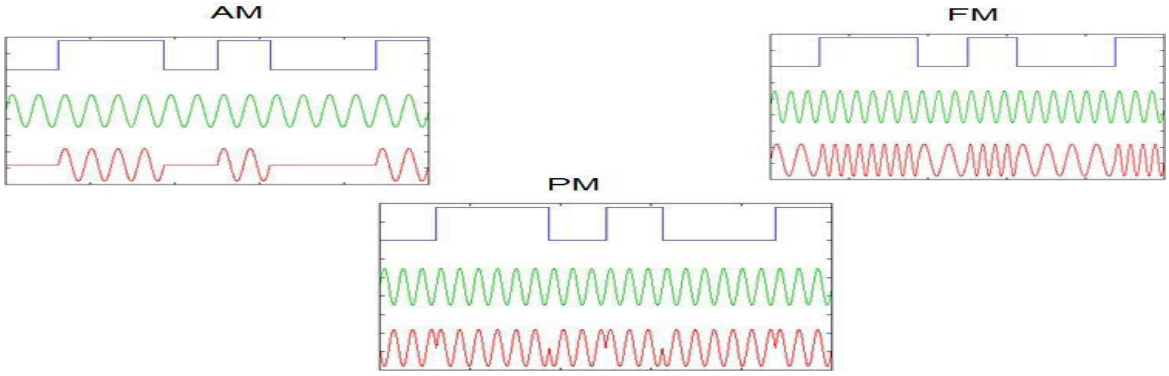
**Carrier and Information Signals**

- Carrier signal: In radio frequency systems an analog signal is always used as the main airborne signal
- Information Signal: On top of this signal another signal, analog or digital, is added that carries the information
- Modulation: This combination of signals is called the modulation

- Modulation is why a perfect sine wave is desired
- Modulators superimpose the information onto the sine wave by making tiny modifications to the sine wave
- If the sine wave is not perfect, these small changes may be lost by the time the signal gets to the other end of the link

**Modulation**

- Modulation is how an information signal is added to a carrier signal
- This is the superimposing of the information onto the carrier
- In an RF system a modulator generates this information signal
- Then it is passed to the transmitter and out the antenna
- Then at the other end the signal is demodulated
- The way to think of this is like a letter
  - ✓ The envelope is the carrier and the letter is the information
  - ✓ The envelope is only needed during transmission
- Three types: AM, FM, PM

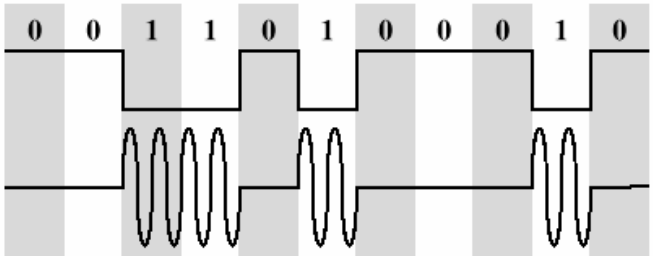


**Types of Encoding**

- There are three forms of Encoding
  - ✓ ASK – Amplitude-Shift Keying
  - ✓ FSK – Frequency-Shift Keying
  - ✓ PSK – Phase-Shift Keying

**Amplitude Shift-Keying (ASK)**

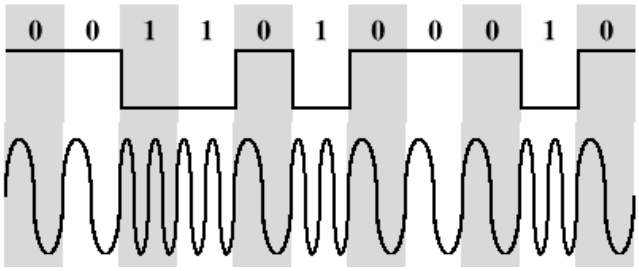
- ASK changes the height of the sine wave as time goes by
- The two binary values are represented by two different amplitudes of the carrier frequency.
- One binary digit represented by presence of carrier, at constant amplitude
- Other binary digit represented by absence of carrier




- Susceptible to sudden gain changes
- Inefficient modulation technique
- On voice-grade lines, used up to 1200 bps
- Used to transmit digital data over optical fiber

**Binary Frequency Shift-Keying (BFSK)**

- FSK changes the frequency of the sine wave as time goes by, without changing the height
- Two binary digits represented by two different frequencies near the carrier frequency




- Less susceptible to error than ASK
- On voice-grade lines, used up to 1200bps
- Used for high-frequency (3 to 30 MHz) radio transmission
- Can be used at higher frequencies on LANs that use coaxial cable

**Multiple Frequency-Shift Keying (MFSK)**

- More than two frequencies are used
- More bandwidth efficient and less susceptible to error
- To match data rate of input bit stream, each output signal element is held for:
  - ✓ $T_s$=LT seconds
    where T is the bit period (data rate = 1/T)
- $f_i = f_c + (2i - 1 - M)f_d$
  - ✓ $f_c$ = the carrier frequency
  - ✓ $f_d$ = the difference frequency
  - ✓ M = number of different signal elements = $2^L$
  - ✓ L = number of bits per signal element

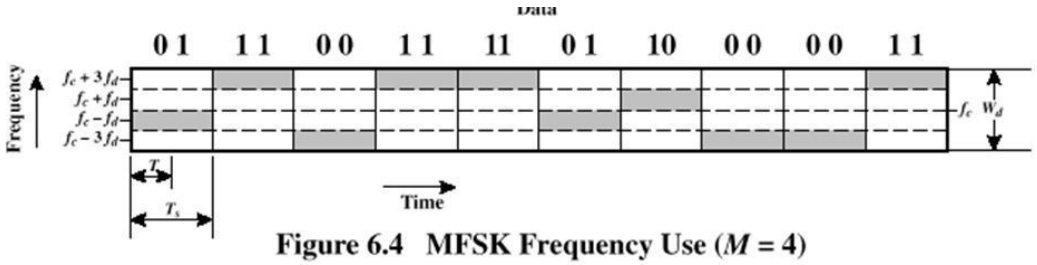


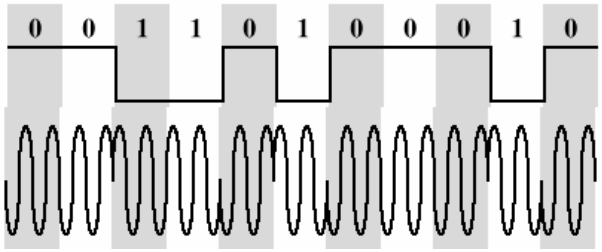

**Figure 6.4 MFSK Frequency Use ($M = 4$)**

**Phase Shift-Key (PSK)**

- PSK changes the phase of successive sine waves
- Two-level PSK (BPSK)
- Uses two phases to represent binary digits

$$s(t) = \begin{cases} A\cos(2\pi f_c t) & \text{binary } 1 \\ A\cos(2\pi f_c t + \pi) & \text{binary } 0 \end{cases}$$

$$= \begin{cases} A\cos(2\pi f_c t) & \text{binary } 1 \\ -A\cos(2\pi f_c t) & \text{binary } 0 \end{cases}$$




- In general when you see phase modulation schemes explained B stands for binary, which is only 2 points. Q stands for quadrature, which is 4 points and 16 and 64 represent the higher number of points in the modulation schemes
- Every time the number of points is increased the speed is increased, but interference tolerance is reduced
- This is one of the reasons for automatic speed reduction in the face of interference
- Going from binary - 2 to 64 requires a really clean signal

**Noise**

- Noise consists of all undesired radio signals, whether manmade or natural
- Noise makes the reception of useful information difficult
- The radio signal's strength is of little use, if the noise power is greater than the received signal power
- This is why the signal to noise ratio is important
- Categories of Noise
  - ✓ Thermal Noise
  - ✓ Intermodulation noise
  - ✓ Crosstalk
  - ✓ Impulse Noise

**Thermal Noise**

- Thermal noise due to agitation of electrons
- Present in all electronic devices and transmission media
- Cannot be eliminated
- Function of temperature
- Particularly significant for satellite communication
- Amount of thermal noise to be found in a bandwidth of 1Hz in any device or conductor is:
  $N_0 = \mathrm{k}T \ (\mathrm{W/Hz})$
  - ✓ $N_0$ = noise power density in watts per 1 Hz of bandwidth
  - ✓ k = Boltzmann's constant = 1.3803 ´ $10^{-23}$ J/K
  - ✓ T = temperature, in kelvins (absolute temperature)
- Noise is assumed to be independent of frequency
- Thermal noise present in a bandwidth of B Hertz (in watts):
  $N = \mathrm{k}TB$
  or, in decibel-watts
  $N = 10\log \mathrm{k} + 10\log T + 10\log B$
  $= -228.6\,\mathrm{dBW} + 10\log T + 10\log B$

**Noise Terminology**

- Intermodulation noise – occurs if signals with different frequencies share the same medium
  - ✓ Interference caused by a signal produced at a frequency that is the sum or difference of original frequencies
- Crosstalk – unwanted coupling between signal paths
  - ✓ Nearby twisted pairs, unwanted signals are picked by antennas
- Impulse noise – irregular pulses or noise spikes
  - ✓ Short duration and of relatively high amplitude
  - ✓ Caused by external electromagnetic disturbances, or faults and flaws in the communications system

**Manmade Noise**

- Manmade noise is part of modern life
- It is generated almost anywhere that there is electrical activity, such as automobile ignition systems, power lines, motors, arc welders, fluorescent lights, and so on
- Each occurrence is small, but there are so many that together they can completely hide a weak signal that would be above the natural noise in a less populated area

**Natural Noise**

- Naturally occurring noise has two main sources
  - ✓ Atmospheric noise, such as thunderstorms, from 0 to 5 MHz
  - ✓ Galactic noise, such as stars, at all higher frequencies
- Both of these sources generate sharp pulses of electromagnetic energy over all frequencies
- The pulses are propagated according to the same laws as the desirable signals being generated by the radio frequency equipment
- The receiving systems must accept them along with the desired signal

**Noise Remedy**

- Increasing receiver amplification cannot improve the signal to noise ratio since both signal and noise will be amplified equally and the ratio will remain the same

**Loss**

- All components exhibit one of two properties: Loss or Gain
- If the signal coming out is smaller than the signal going in, it is loss that appears as heat
- Attenuators produce loss

**Attenuation**

- Causes of loss or attenuation in RF systems and the environments through which they transmit include
  - ✓ Water, regardless of how it appears or where it is found including inside connections
  - ✓ When water is encountered in the air as the signal passes through, the form of the moisture matters
  - ✓ At frequencies above 10 GHz attenuation from rain becomes significant
  - ✓ When the raindrop's size matches the wavelength attenuation occurs

- Examples of the affect outside include
  - ✓ Rain causes about .08 dB of loss per mile for 2.4 GHz and 5.8 GHz
  - ✓ Fog causes about .03 dB per mile for 2.4 GHz for 5.8 GHz the loss is about .11 dB per mile
  - ✓ Ice changes the effective design of an antenna, therefore changing its performance

**Other Impairments**

- Atmospheric absorption – water vapor and oxygen contribute to attenuation
- Multipath – obstacles reflect signals so that multiple copies with varying delays are received
- Refraction – bending of radio waves as they propagate through the atmosphere

**Gain**

- If the signal gets larger before it exits the device, it is gain
- RF amplifiers produce gain
- Gain is an active process in most cases, in other words it requires a power source
- Gain can also be the combination of signals from different directions appearing together, such as the main signal and a reflected signal
- However, the total gain cannot exceed the original level transmitted from the antenna in such a case

**Summary**

- Wireless Transmission
  - ✓ Why baseband signal can not be transmitted?
  - ✓ Need bandpass signals whose minimum frequency is higher than 0
  - ✓ Modulator produces bandpass by superomposing basband signal over higher frequency signals
    - AM, FM, PM
- Digital data analog signals
  - ✓ Some transmission media like optical fibers and unguided propagate only analog signals
  - ✓ For example public telephone network
  - ✓ Requires data encoding
    - ASK, FSK, PSK
- Noises
  - ✓ Thermal/white noise
  - ✓ Intermodulation noise
  - ✓ Crosstalk
  - ✓ Impulse noise
  - ✓ Natural noise
    - Atmospheric noise like thunderstorms
    - Galatic noise such as stars
  - ✓ Manmade noise
    - Ignition systems, power lines, motors arc welders, flourscent lightd etc
- Attenuation and other impairments

## Lecture 3
## Introduction to Wireless Communication

**Outlines**

- Review of previous lecture #2
- Multiplexing
- Transmission Mediums
- Propagation modes
- Multi-path propagation
- Fading
- Summary of today's lecture

**Last Lecture Review**

- Wireless Transmission
  - ✓ Digital data analog signal
  - ✓ Baseband/bandpass signal
  - ✓ Encoding techniques/Modulation
  - ✓ Receiver synchronization / Demodulation
- Noises
  - ✓ Thermal noise
  - ✓ Intermodulation noise
  - ✓ Crosstalk
  - ✓ Impulse Noise
  - ✓ Manmade noise / Natural noise
- Losses / Gain

**Multiplexing**

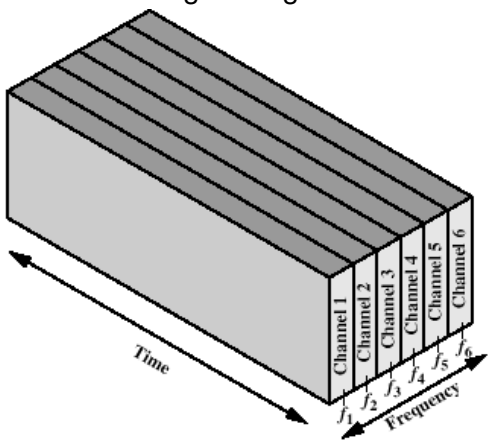
- Capacity of transmission medium usually exceeds capacity required for transmission of a single signal
- Multiplexing - carrying multiple signals on a single medium
  - ✓ More efficient use of transmission medium


**Reasons for Widespread Use of Multiplexing**

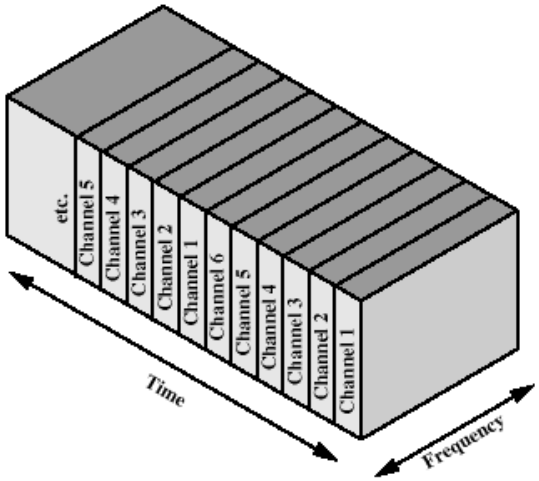
- Cost per kbps of transmission facility declines with an increase in the data rate
- Cost of transmission and receiving equipment declines with increased data rate
- Most individual data communicating devices require relatively modest data rate support
- For example You got an ADSL connection which has much higher bandwidth than a normal internet user requirements. If two or more friends share the same ADSL connection then the cost per bit rate will be reduced and similarly the cost of ADSL modem will be shared among them. As a result the internet facility will become more cheap.
- Similarly the cost of cellular installments will drop down if the number of users on the network are increased.

**Multiplexing Techniques**

- Frequency-division multiplexing (FDM)
  - ✓ Takes advantage of the fact that the useful bandwidth of the medium exceeds the required bandwidth of a given signal




- Time-division multiplexing (TDM)
  - ✓ Takes advantage of the fact that the achievable bit rate of the medium exceeds the required data rate of a digital signal




- For example multiplexing of voice signals. The useful spectrum is 300 to 3400 hz. A channel of bandwidth 4 khz is adequate as it keeps some frequency slots free.
- In Standard telemcom. Voice multiplexing scheme consists of 12 4khz channel voice channels from 60-108khz

**Classifications of Transmission Media**

- Transmission Medium
  - ✓ Physical path between transmitter and receiver

- Guided Media
  - ✓ Waves are guided along a solid medium
  - ✓ E.g., copper twisted pair, copper coaxial cable, optical fiber

- Unguided Media
  - ✓ Provides means of transmission but does not guide electromagnetic signals
  - ✓ Usually referred to as wireless transmission
  - ✓ E.g., atmosphere, outer space

**Unguided Media**

- Transmission and reception are achieved by means of an antenna
- Configurations for wireless transmission
  - ✓ Directional
  - ✓ Omnidirectional

**General Frequency Ranges**

- Microwave frequency range
  - ✓ 1 GHz to 40 GHz
  - ✓ Directional beams possible
    - o Suitable for point-to-point transmission
- Used for satellite communications
- Radio frequency range
  - ✓ 30 MHz to 1 GHz
  - ✓ Suitable for omnidirectional applications
- Infrared frequency range
  - ✓ Roughly, $3x10^{11}$ to $2x10^{14}$ Hz
  - ✓ Useful in local point-to-point multipoint applications within confined areas

**Terrestrial Microwave**

- Description of common microwave antenna
  - ✓ Parabolic "dish", 3 m in diameter
  - ✓ Fixed rigidly and focuses a narrow beam
  - ✓ Achieves line-of-sight transmission to receiving antenna
  - ✓ Located at substantial heights above ground level
  - ✓ Due to attenuation particularly rainfall, requires repeaters/amplifiers placed farther apart 10-100 km.
- Applications
  - ✓ Long haul telecommunications service
  - ✓ 4 – 6 GHz band is common
  - ✓ But due to increased congestion 11 GHz is coming into use now
  - ✓ Microwave links provide TV signals to local CATV and then distributed to subscribers via coaxial cable.
- Short point-to-point links between buildings
  - ✓ Enterprise offices, university campuses

**Satellite Microwave**

- Description of communication satellite
  - ✓ Communication satellite is Microwave relay station

- ✓ Used to link two or more ground-based microwave transmitter/receivers
- ✓ Receives transmissions on one frequency band (uplink), amplifies or repeats the signal, and transmits it on another frequency (downlink)
- ✓ Broadcast in nature

- Applications
  - ✓ Television distribution
  - ✓ Long-distance telephone transmission
    - Used for point-to-point trunks between telephone exchange offices.
  - ✓ Private business networks
- Transmission characteristics
  - ✓ Optimum range is 1-10 GHz
  - ✓ Below 1 GHz, significant natural noise (solar, galactic, atmospheric) and manmade
  - ✓ Above 10 GHz, higher attenuation due to atmospheric absorption
  - ✓ Mostly use 5.925-6.425 for uplink and 3.7-4.2 GHz for downlink referred as 4/6 GHz band
  - ✓ Due to saturation, 12/14 GHz band has been developed. Uplink: 14-14.5, downlink: 11.7-12.2 GHz
  - ✓ In Future, 20/30GHz. Uplink: 27.5-30.0, downlink: 17.7-20.2 GHz
  - ✓ Long propagation delay of about 250 ms, which is noticeabe in telephone conversation.
  - ✓ Broadcast in nature and suitable for TV broadcast service.

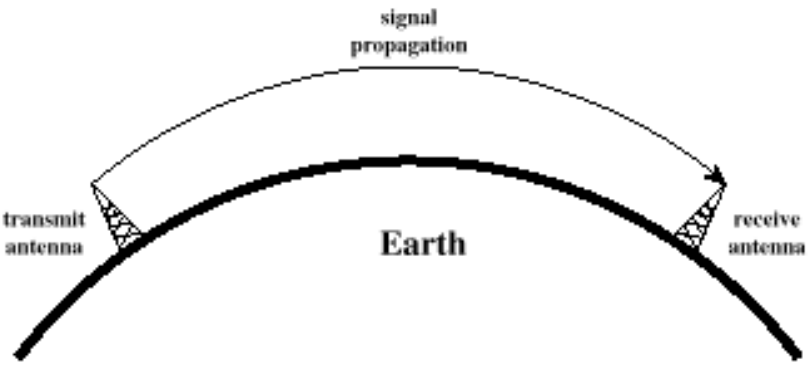
**Broadcast Radio**

- Description of broadcast radio antennas
  - ✓ Omnidirectional
  - ✓ Antennas not required to be dish-shaped
  - ✓ Antennas need not be rigidly mounted to a precise alignment
- Applications
  - ✓ Broadcast radio
  - ✓ VHF and part of the UHF band; 30 MHZ to 1GHz
  - ✓ Covers FM radio and UHF and VHF television
- Characteristics
  - ✓ Because of longer wavelength, radio waves relatively suffer less attenuation.
  - ✓ Prime source of impairments is multi-path interference. Reflection from land water and human made objects can create multiple paths.
  - ✓ Less sensitive to rainfall

**Propagation Modes**

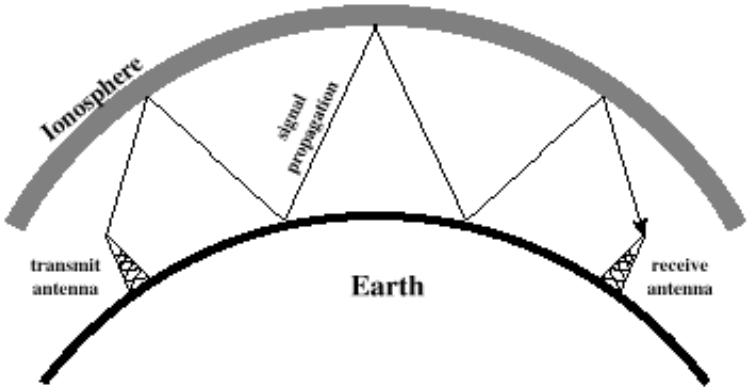
- Ground-wave propagation
- Sky-wave propagation
- Line-of-sight propagation

**Ground Wave Propagation**




- EM waves of low frequency induce current in the earth surface that slow down the wavefront near the earth causing the wavefront to tilt downward.
- Follows contour of the earth
- Can Propagate considerable distances
- Frequencies up to 2 MHz, which are low frequencies and have tendency to tilt downwards
- EM waves of low frequency are scattered by the atmosphere such that they do not penetrate the upper atmosphere.
- Example
  - ✓ AM radio

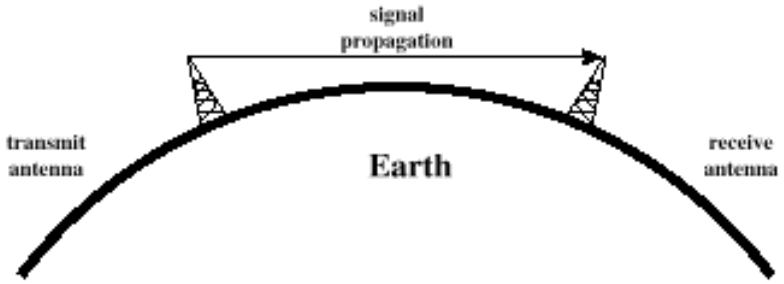
**Sky Wave Propagation**




- Signal reflected from ionized layer of atmosphere back down to earth
- Signal can travel a number of hops, back and forth between ionosphere and earth's surface
- Reflection effect caused by refraction
- Examples
  - ✓ Amateur radio
  - ✓ CB radio
- The troposphere is the first layer

- It starts at the Earth's surface and goes up to about 10 kilometers
- Air in this layer decreases in temperature at a rate of about 2.5° C for every 300 meters of altitude gained
- The second layer of the atmosphere is the stratosphere
- It extends from about 10 km to 50 km
- The air in this layer maintains a nearly constant temperature of about -65° C
- Above about 50 km and extending upward to more than 500 km is the ionosphere
- The ionosphere gets its name because the molecules in it are ionized
- Electrons have been stripped from the atoms by the bombardment of the Sun's rays and other high energy particles from the Sun
- These ionized particles with large quantities of free electrons act on any radio waves that pass through the ionosphere

**Line-of-Sight Propagation**




- Transmitting and receiving antennas must be within line of sight
  - ✓ Satellite communication – signal above 30 MHz not reflected by ionosphere
  - ✓ Ground communication – antennas within effective line of site due to refraction
- Refraction – bending of microwaves by the atmosphere
  - ✓ Velocity of electromagnetic wave is a function of the density of the medium
  - ✓ When wave changes medium, speed changes
  - ✓ Wave bends at the boundary between mediums

**Line-of-Sight Equations**

- Optical line of sight

$$d = 3.57\sqrt{h}$$

- Effective, or radio, line of sight

$$d = 3.57\sqrt{Kh}$$

  - ✓ d = distance between antenna and horizon (km)
  - ✓ h = antenna height (m)
  - ✓ K = adjustment factor to account for refraction, rule of thumb K = 4/3
- Maximum distance between two antennas for LOS propagation:

$$3.57\left(\sqrt{Kh_1} + \sqrt{Kh_2}\right)$$

  - ✓ $h_1$ = height of antenna one
  - ✓ $h_2$ = height of antenna two

**Example**

- Let h1 = 100 m, h2 = 0 or the second antenna is at ground level.
  D = 3.57 ( 4/3x100)^1/2 + 0 = 41 km.
- Now suppose that h2 = 10m. To achieve same distance, what must be h1?
  41 = 3.57(Kh1)^1/2+(13.3)^1/2
  h1 = 46.2m

**Propagation Factors**

- The transmitter's power output
- The frequency being transmitted
- The effect of the Earth's shape in between the points
- The conductivity of the Earth along the transmission path
- The microclimate through which the signal passes

**Multipath Propagation**

- Reflection - occurs when signal encounters a surface that is large relative to the wavelength of the signal
- Diffraction - occurs at the edge of an impenetrable body that is large compared to wavelength of radio wave
- Scattering – occurs when incoming signal hits an object whose size in the order of the wavelength of the signal or less

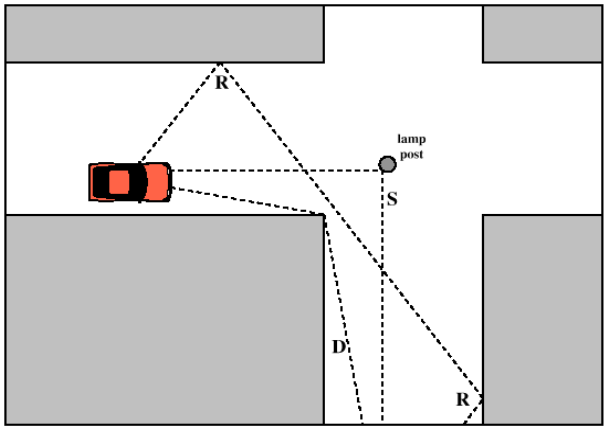



**Figure 5.10 Sketch of Three Important Propagation Mechanisms: Reflection (R), Scattering (S), Diffraction (D) [ANDE95]**

**The Effects of Multipath Propagation**

- Multiple copies of a signal may arrive at different phases
  - ✓ If phases add destructively, the signal level relative to noise declines, making detection more difficult
- Intersymbol interference (ISI)
  - ✓ One or more delayed copies of a pulse may arrive at the same time as the primary pulse for a subsequent bit

**Types of Fading**

- Fast fading
  - ✓ Rapid variation in signal strength occurs over distance about one-half of wavelength.
  - ✓ At 900 Mhz cellular badn, lambda is 0.33 m.
- Slow fading
  - ✓ Users cover distance well in excess of a wavelength as it passes buildings of different heights, vacant lots and so on
  - ✓ A slow variation in signal strength.
- Flat fading
- Selective fading

**Fading channel**

- Additive white Gaussian noise (AWGN) channel
  - ✓ Signal is degraded only by thermal noise
  - ✓ Accurate for space communication and some wire communication such as coaxial cable.
- Rayleigh fading
  - ✓ Fading occurs when there are multiple indirect paths but no direct LOS path
  - ✓ Suitable for Outdoor environment
- Rician fading
  - ✓ When there exist a direct LOS path in addition to multiple paths.
  - ✓ Suitable for smaller cells and indoor environment

**Summary of today's lecture**

- Multiplexing
  - ✓ FDM, TDM
- Transmission Mediums
  - ✓ Guided media
  - ✓ Unguided media
    - Microwave
    - Radio waves
    - Infra red
- Propagation modes
  - ✓ Ground wave propagation
  - ✓ Sky-wave propagation
  - ✓ LOS propagation
- Multi-path propagation
- Fading
- Next lecture
  - ✓ Error detecting and correcting techniques

## Lecture 4
## Error Detecting and Correcting Techniques

**Outlines**

- Review of previous lecture #3
- Transmission Errors
- Parity Check
- Cyclic Redundancy Check
- Block Error Code
- Summary of today's lecture

**Last Lecture Review**

- Multiplexing
  - ✓ FDM, TDM
- Transmission Mediums
  - ✓ Guided media
  - ✓ Unguided media
    - Microwave
    - Radio waves
    - Infra red
- Propagation modes
  - ✓ Ground wave propagation
  - ✓ Sky-wave propagation
  - ✓ LOS propagation
- Multi-path propagation
- Fading

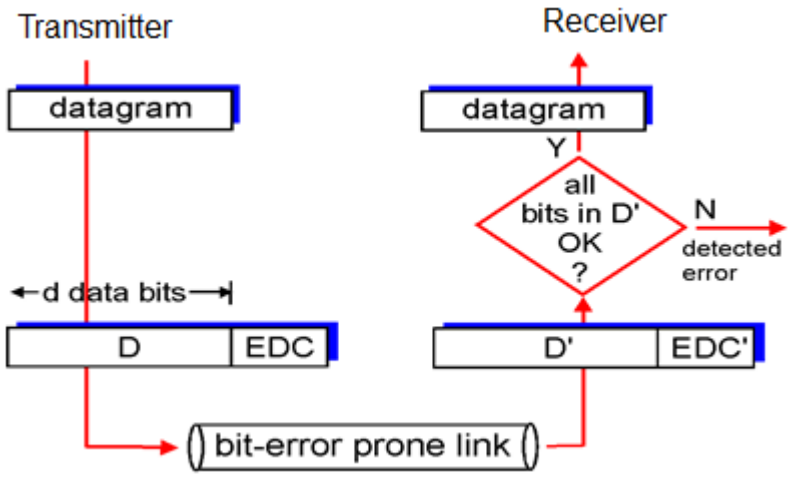
**Coping with Transmission Errors**

- Error detection codes
  - ✓ Detects the presence of an error
- Error correction codes, or forward correction codes (FEC)
  - ✓ Designed to detect and correct errors
  - ✓ Widely used in wireless networks
- Automatic repeat request (ARQ) protocols
  - ✓ Used in combination with error detection/correction
  - ✓ Block of data with error is discarded
  - ✓ Transmitter retransmits that block of data

**Error Detection Process**

- Transmitter
  - ✓ For a given frame, an error-detecting code (check bits) is calculated from data bits
  - ✓ Check bits are appended to data bits

- Receiver
  - ✓ Separates incoming frame into data bits and check bits
  - ✓ Calculates check bits from received data bits
  - ✓ Compares calculated check bits against received check bits
  - ✓ Detected error occurs if mismatch




- Error detection not 100% reliable!
- protocol may miss some errors, but rarely
- larger EDC field yields better detection and correction

**Parity Checks**

Single bit parity check

- Even or Odd parity
- Only single bit error detection
- What about multiple bit errors
- Use when probability of bit errors is small and independent
- Errors are usually clustered together
- The ability of receiver to both detect and correct errors is known as forward error correction (FEC)

- Examples of parity bit check
  - ✓ Adding parity bit

    1 1 0 0 0 1 0 1 1 Odd

    1 1 0 0 0 1 0 1 0 Even
  - ✓ Odd parity errors

    1 1 0 1 0 1 0 1 1 error detected

    1 1 0 1 0 0 0 1 1 error undetected

Two-dimensional parity checks

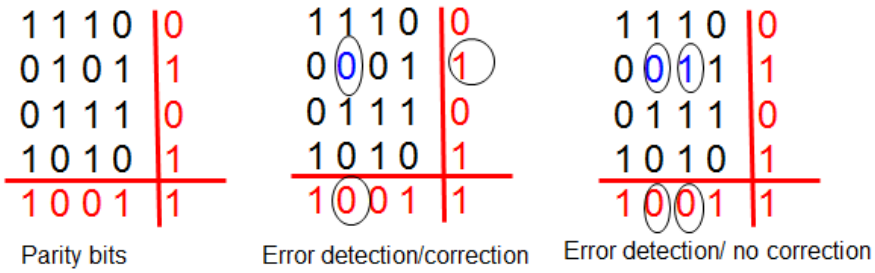
- Generalization of 1-bit
- D bits are divided into i rows and j columns.

| | | | | |
|---|---|---|---|---|
| $D_{1,1}$ | $D_{1,2}$ | … | $D_{1,j}$ | $D_{1,j+1}$ |
| $D_{2,1}$ | $D_{2,2}$ | … | $D_{2,j}$ | $D_{2,j+1}$ |
| . | . | … | . | . |
| . | . | … | . | . |
| . | . | … | . | . |
| $D_{i,1}$ | $D_{i,2}$ | … | $D_{i,j}$ | $D_{i,j+1}$ |
| $D_{i+1,1}$ | $D_{i+1,2}$ | … | $D_{i+1,j}$ | $D_{i+1,j+1}$ |

- Receiver can not only detect but correct as well using row, column indices

**Example:** 2D Odd parity check

- 1110010101111010
- Let i = 4, j = 4




**Cyclic Redundancy Check (CRC)**

- Transmitter
  - ✓ For a k-bit block, transmitter generates an (n-k)-bit frame check sequence (FCS)
  - ✓ Resulting frame of n bits is exactly divisible by predetermined number
- Receiver
  - ✓ Divides incoming frame by predetermined number
  - ✓ If no remainder, assumes no error
- Algorithm
  - ✓ Generator: Transmitter and receiver agree on an r + 1 bit pattern P.
  - ✓ Transmitter chooses r additional bits to append with k data bits.
  - ✓ Which is remainder of d / P.
  - ✓ Receiver: if remainder of D / P is 0 , success otherwise error

CRC using Modulo 2 Arithmetic

- Exclusive-OR (XOR) operation
- Parameters:
  - ✓ T = n-bit frame to be transmitted
  - ✓ D = k-bit block of data; the first k bits of T
  - ✓ F = (n – k)-bit FCS; the last (n – k) bits of T
  - ✓ P = pattern of n–k+1 bits; this is the predetermined divisor
  - ✓ Q = Quotient
  - ✓ R = Remainder
- For T/P to have no remainder, start with

$$T = 2^{n-k}D + F$$

- Divide $2^{n-k}D$ by P gives quotient and remainder

$$\frac{2^{n-k}D}{P} = Q + \frac{R}{P}$$

- Use remainder as FCS

$$T = 2^{n-k}D + R$$

- Does R cause T/P have no remainder?

$$\frac{T}{P} = \frac{2^{n-k}D + R}{P} = \frac{2^{n-k}D}{P} + \frac{R}{P}$$

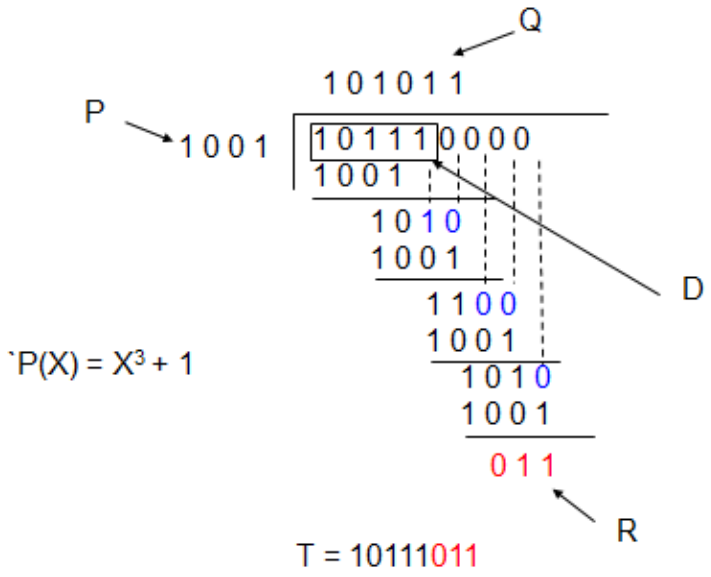
- Substituting,

$$\frac{T}{P} = Q + \frac{R}{P} + \frac{R}{P} = Q + \frac{R+R}{P} = Q$$

- No remainder, so T is exactly divisible by P
  - ✓ No remainder, so T is exactly divisible by P

CRC Example

- Let d = 10111, P=1001



CRC using Polynomials

- All values expressed as polynomials
  - ✓ Dummy variable X with binary coefficients

$$\frac{X^{n-k}D(X)}{P(X)} = Q(X) + \frac{R(X)}{P(X)}$$

$$T(X) = X^{n-k}D(X) + R(X)$$

- Widely used versions of P(X)
  - ✓ CRC–12
    - $X^{12} + X^{11} + X^3 + X^2 + X + 1$
  - ✓ CRC–16
    - $X^{16} + X^{15} + X^2 + 1$
  - ✓ CRC – CCITT
    - $X^{16} + X^{12} + X^5 + 1$
  - ✓ CRC – 32
    - $X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$

**Wireless Transmission Errors**

- Error detection requires retransmission
- Detection inadequate for wireless applications
  - ✓ Error rate on wireless link can be high, results in a large number of retransmissions
  - ✓ Long propagation delay compared to transmission time

**Block Error Correction Codes**

- Transmitter
  - ✓ Forward error correction (FEC) encoder maps each k-bit block into an n-bit block codeword
  - ✓ Codeword is transmitted; analog for wireless transmission

- Receiver
  - ✓ Incoming signal is demodulated
  - ✓ Block passed through an FEC decoder

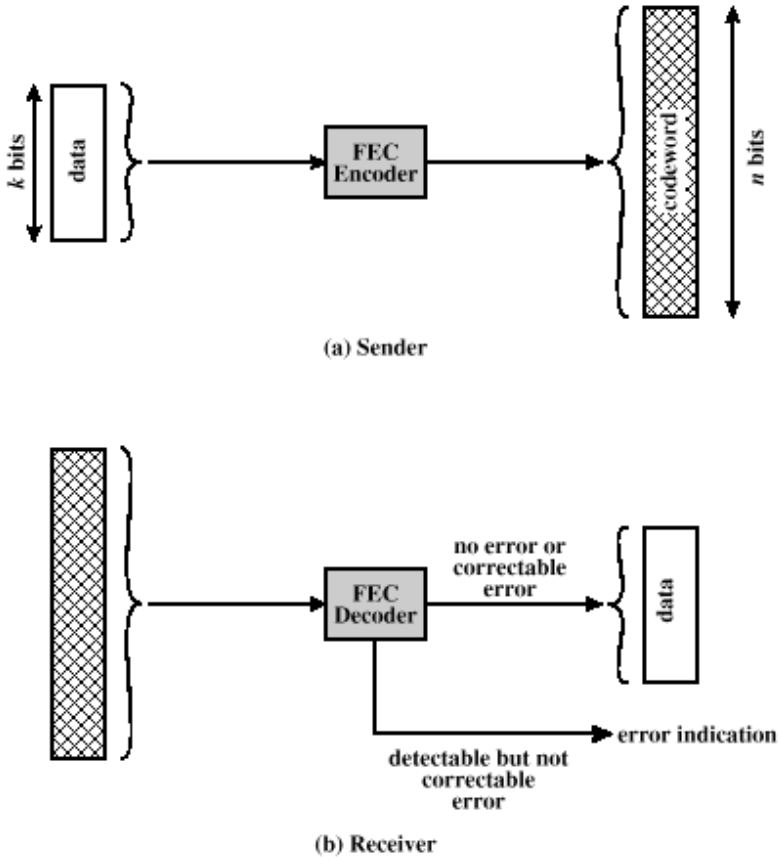



**Figure 8.5 Forward Error Correction Process**

**FEC Decoder Outcomes**

- No errors present
  - ✓ Codeword produced by decoder matches original codeword
- Decoder detects and corrects bit errors
- Decoder detects but cannot correct bit errors; reports uncorrectable error
- Decoder detects no bit errors, though errors are present

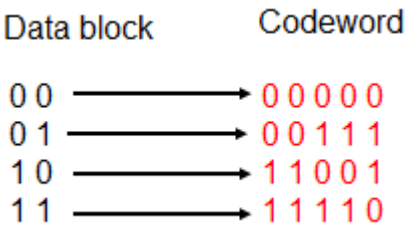
**Block Code Principles**

- Hamming distance – for 2 n-bit binary sequences, the number of different bits
  - ✓ E.g., $v_1$=011011; $v_2$=110001;
  - ✓ 011011 XOR 110001 = 101010
  - ✓ d(v1, $v_2$)=3
- Redundancy – ratio of redundant bits to data bits
- Code rate – ratio of data bits to total bits
- Coding gain – the reduction in the required $E_b/N_0$ to achieve a specified BER of an error-correcting coded system

**Block Codes**

- The Hamming distance d of a Block code is the minimum distance between two code words
- Error Detection:
  - ✓ Upto d-1 errors
- Error Correction:
  - ✓ Upto $\left\lfloor \frac{d-1}{2} \right\rfloor$

- Example of Block code
- Let k = 2, n = 5




- Suppose we receive 0 0 1 0 0 pattern
- Minimum distance is with codeword 0 0 0 0 0, so we deduct 0 0 as data bits.

## Lecture 5
## Error Detecting and Correcting Techniques (Part II)

**Outlines**

- Review of previous lecture #3
- Block Codes
  - ✓ Hamming
  - ✓ BCH
  - ✓ Reed Solmon
- ARQ
  - ✓ Sliding window
  - ✓ Go-back-N
- Summary of today's lecture

**Last Lecture Review**

- Transmission Errors
- Parity Check
  - ✓ Single-bit parity
  - ✓ 2D parity
- Cyclic Redundancy Check
- Block Error Code

**Hamming Code**

- Designed to correct single bit errors
- Family of (n, k) block error-correcting codes with parameters:
  - ✓ Block length: $n = 2^m - 1$
  - ✓ Number of data bits: $k = 2^m - m - 1$
  - ✓ Number of check bits: $n - k = m$
  - ✓ Minimum distance: $d_{min} = 3$
- Single-error-correcting (SEC) code
  - ✓ SEC double-error-detecting (SEC-DED) code

**Example of Error Detection/Correction**

| | | | | | |
|---|---|---|---|---|---|
| C1 | 1 | 1 | 0 | 1 | 1 |
| C2 | 0 | 0 | 0 | 0 | 1 |
| XOR | 1 | 1 | 0 | 1 | 0 |

Hamming distance = 3

Received Codeword (Cr) = 1 0 0 1 1

| | | | | | |
|---|---|---|---|---|---|
| C1 | 1 | 1 | 0 | 1 | 1 |
| Cr | 1 | 0 | 0 | 1 | 1 |
| XOR | 0 | 1 | 0 | 0 | 0 |

| | | | | | |
|---|---|---|---|---|---|
| C2 | 0 | 0 | 0 | 0 | 1 |
| Cr | 1 | 0 | 0 | 1 | 1 |
| XOR | 1 | 0 | 0 | 1 | 0 |

**Hamming Code Process**

- Encoding: k data bits + (n -k) check bits
- Decoding: compares received (n -k) bits with calculated (n -k) bits using XOR
  - ✓ Resulting (n -k) bits called syndrome word
  - ✓ Syndrome range is between 0 and $2^{(n-k)}$-1
  - ✓ Each bit of syndrome indicates a match (0) or conflict (1) in that bit position
- Example of Hamming Encode
- Data = 00111001

| Bit Position | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Pos. Number | 1100 | 1011 | 1010 | 1001 | 1000 | 0111 | 0110 | 0101 | 0100 | 0011 | 0010 | 0001 |
| Trans. Block | | | | | | | | | | | | |

| Bit Position | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Pos. Number | 1100 | 1011 | 1010 | 1001 | 1000 | 0111 | 0110 | 0101 | 0100 | 0011 | 0010 | 0001 |
| Trans. Block | 0 | 0 | 1 | 1 | x | 1 | 0 | 0 | x | 1 | x | X |

| Bit Position | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Pos. Number | 1100 | 1011 | 1010 | 1001 | 1000 | 0111 | 0110 | 0101 | 0100 | 0011 | 0010 | 0001 |
| Trans. Block | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 |

| Bit Position | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Pos. Number | 1100 | 1011 | 1010 | 1001 | 1000 | 0111 | 0110 | 0101 | 0100 | 0011 | 0010 | 0001 |
| Trans. Block | 0 | 0 | 1 | 1 | x | 1 | 0 | 0 | x | 1 | X | X |
| Check bits | | | | | 0 | | | | 1 | | 1 | 1 |

| Position | Code |
|---|---|
| 10 | 1010 |
| 9 | 1001 |
| 7 | 0111 |
| 3 | 0011 |
| XOR | 0111 |

**Decoding Hamming**

| Bit Position | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Pos. Number | 1100 | 1011 | 1010 | 1001 | 1000 | 0111 | 0110 | 0101 | 0100 | 0011 | 0010 | 0001 |
| Trans. Block | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 |

| Position | Code |
|---|---|
| 10 | 1010 |
| 9 | 1001 |
| 7 | 0111 |
| 6 | 0110 |
| 3 | 0011 |
| XOR | 0110 |

**BCH Codes**

- BCH → Discoverer: Bose, Chaudhuri and Hocquenghem.
- Multiple error correcting codes
- Generalization of Hamming Code.
- Flexibility in choice of parameters
  - ✓ Block length, code rate
- For positive pair of integers m and t, a (n, k) BCH code has parameters:
  - ✓ Block length: $n = 2^m - 1$
  - ✓ Number of check bits: $n - k <= mt$
  - ✓ Minimum distance:$d_{min} >= 2t + 1$
- Correct combinations of t or fewer errors
- The generator polynomial can be constructed from the factors of $(X^{2m-1} + 1)$

**Reed-Solomon Codes**

- Subclass of nonbinary BCH codes
- Data processed in chunks of m bits, called symbols
- An (n, k) RS code has parameters:
  - ✓ Symbol length: m bits per symbol
  - ✓ Block length: $n = 2^m - 1$ symbols = $m(2^m - 1)$ bits
  - ✓ Data length: k symbols
  - ✓ Size of check code: $n - k = 2t$ symbols = $m(2t)$ bits
  - ✓ Minimum distance: $d_{min} = 2t + 1$ symbols

**Automatic Repeat Request**

- Mechanism used in data link control and transport protocols
- Relies on use of an error detection code (such as CRC)
- Flow Control
- Error Control

**Flow Control**

- Assures that transmitting entity does not overwhelm a receiving entity with data
- Protocols with flow control mechanism allow multiple PDUs in transit at the same time
- PDUs arrive in same order they're sent
- Sliding-window flow control
  - ✓ Transmitter maintains list (window) of sequence numbers allowed to send
  - ✓ Receiver maintains list allowed to receive
- Reasons for breaking up a block of data before transmitting:
  - ✓ Limited buffer size of receiver
  - ✓ Retransmission of PDU due to error requires smaller amounts of data to be retransmitted
  - ✓ On shared medium, larger PDUs occupy medium for extended period, causing delays at other sending stations

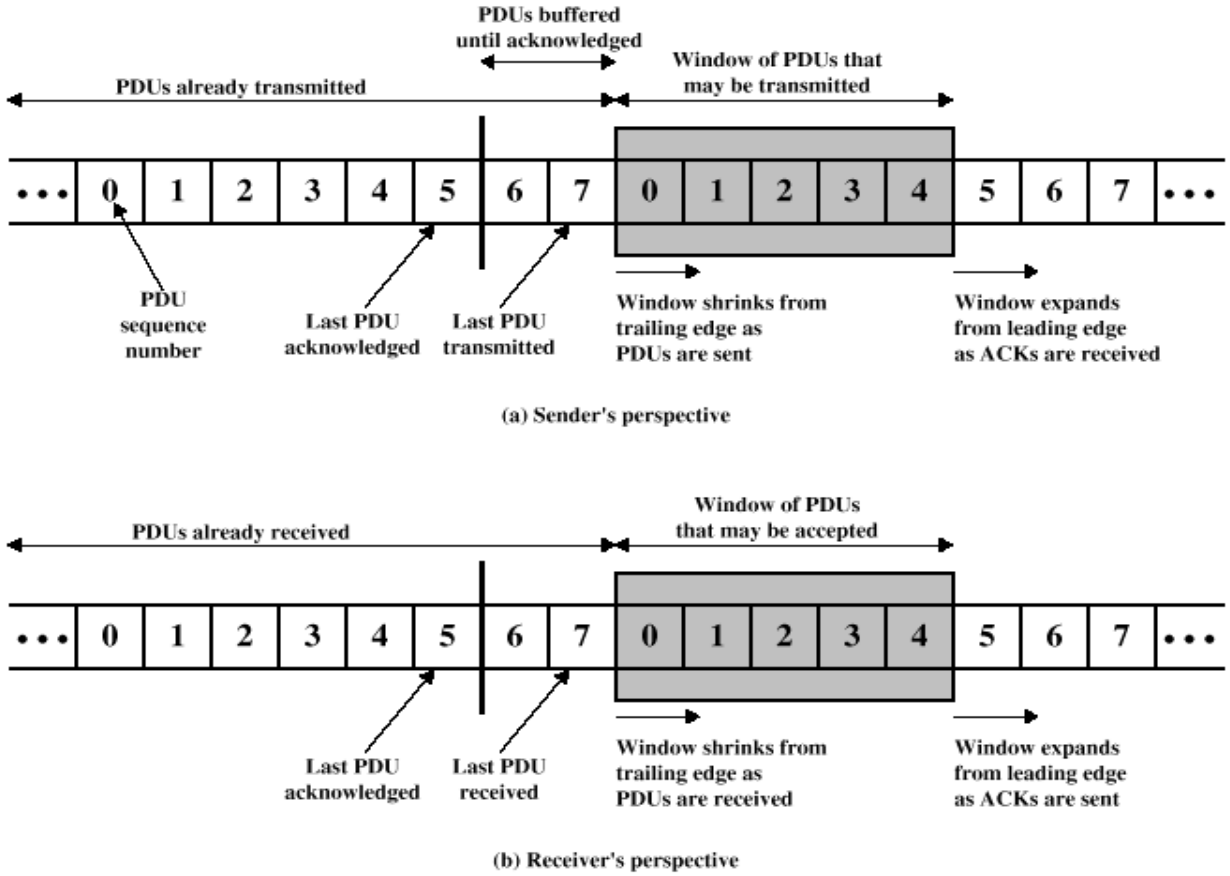



**Figure 8.17 Sliding-Window Depiction**

- Mechanisms to detect and correct transmission errors
- Types of errors:
  - ✓ Lost PDU : a PDU fails to arrive
  - ✓ Damaged PDU : PDU arrives with errors

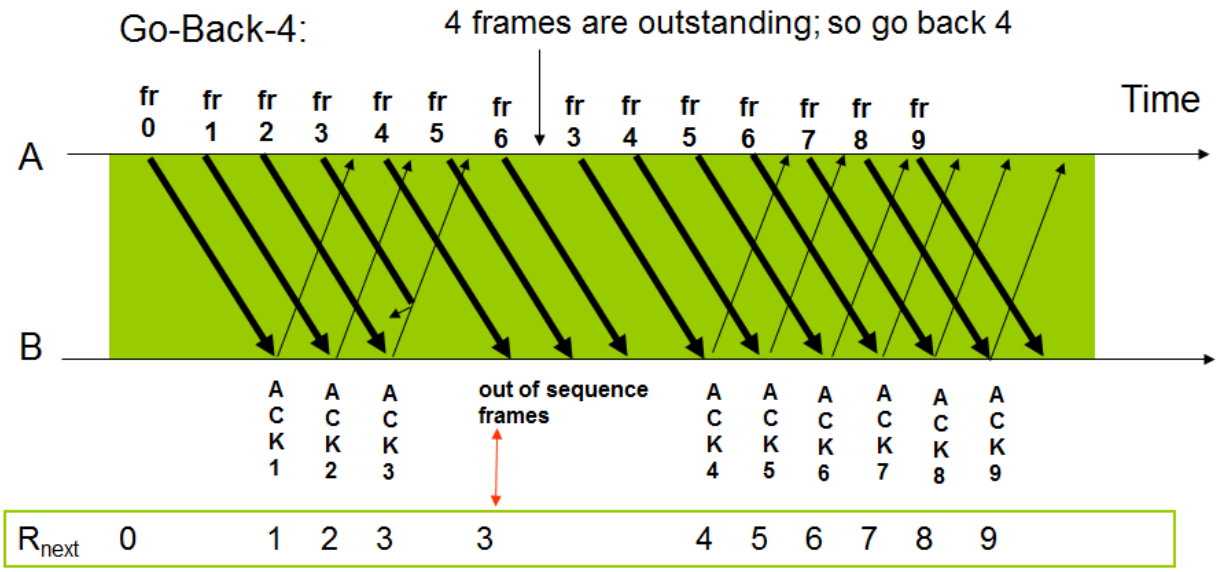
**Error Control Requirements**

- Error detection
  - ✓ Receiver detects errors and discards PDUs
- Positive acknowledgement
  - ✓ Destination returns acknowledgment of received, error-free PDUs
- Retransmission after timeout
  - ✓ Source retransmits unacknowledged PDU
- Negative acknowledgement and retransmission
  - ✓ Destination returns negative acknowledgment to PDUs in error

**Go-Back-N**

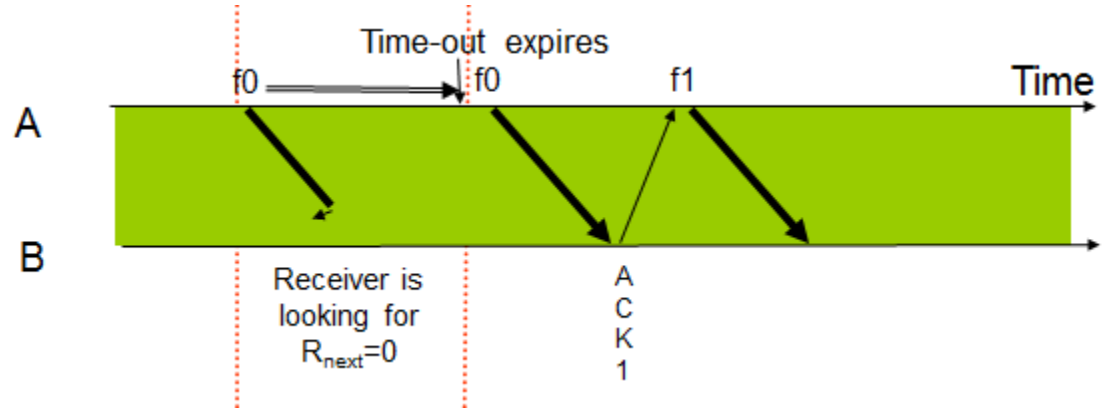
- Improve Stop-and-Wait by not waiting!
- Keep channel busy by continuing to send frames
- Allow a window of up to $W_s$ outstanding frames
- Use m-bit sequence numbering
- If ACK for oldest frame arrives before window is exhausted, we can continue transmitting
- If window is exhausted, pull back and retransmit all outstanding frames
- Alternative: Use timeout

**Go-Back-N ARQ**

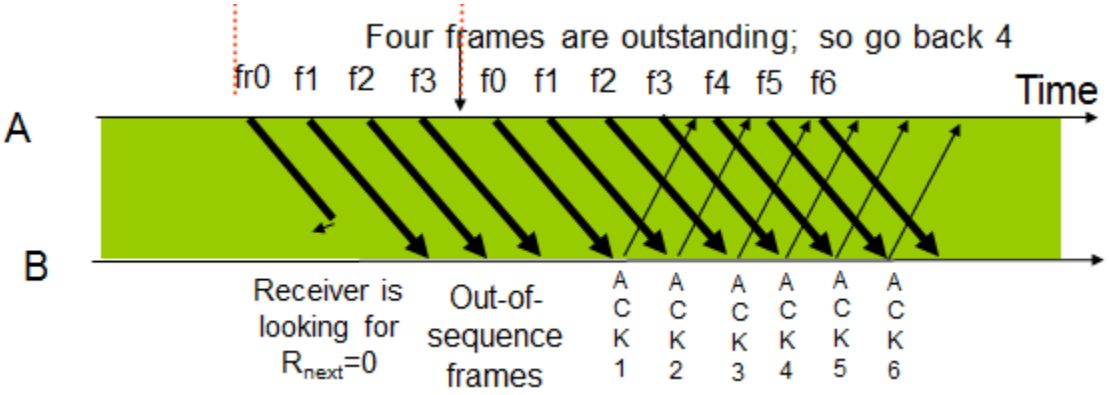



- Frame transmission are pipelined to keep the channel busy
- Frame with errors and subsequent out-of-sequence frames are ignored
- Transmitter is forced to go back when window of 4 is exhausted
- Window size long enough to cover round trip time

- Stop-and-Wait ARQ



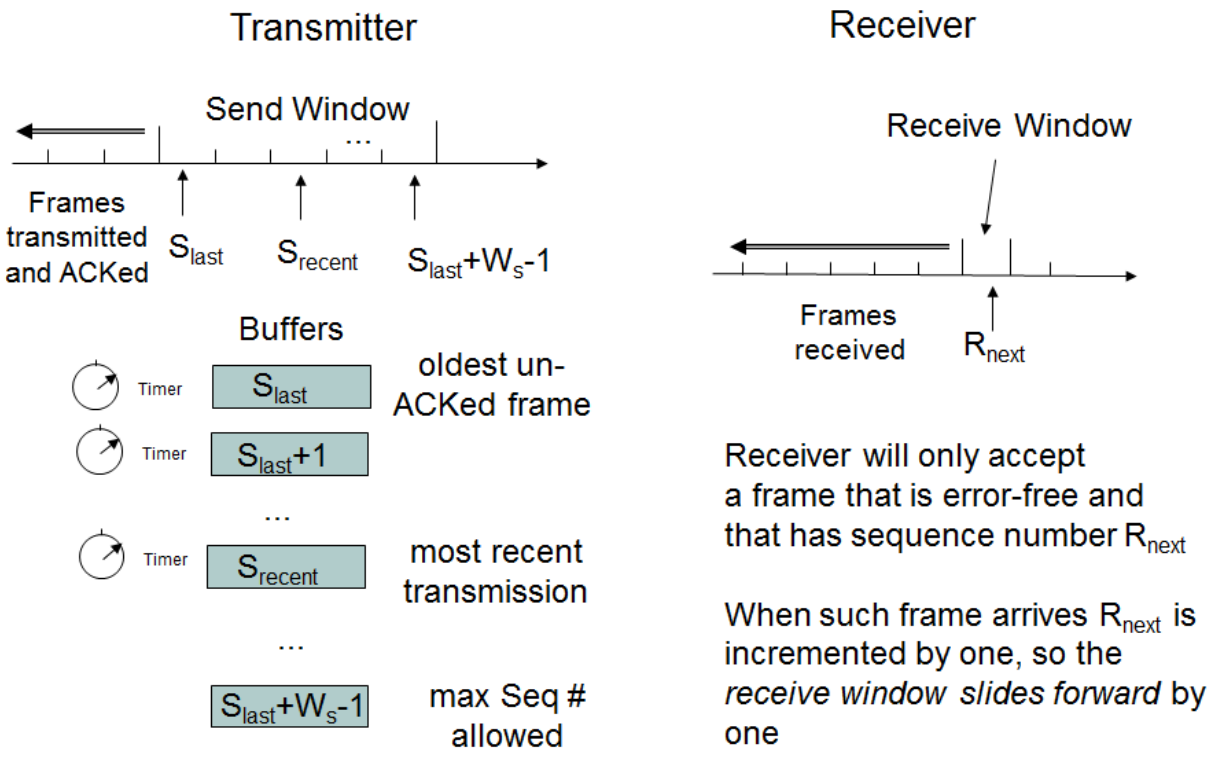

- Go-Back-N ARQ




**Go-Back-N with Timeout**

- Problem with Go-Back-N as presented:
  - ✓ If frame is lost and source does not have frame to send, then window will not be exhausted and recovery will not commence
- Use a timeout with each frame
  - ✓ When timeout expires, resend all outstanding frames

**Go-Back-N Transmitter & Receiver**




**Go-back-N ARQ**

- Acknowledgments
  - ✓ RR = receive ready (no errors occur)
  - ✓ REJ = reject (error detected)
- Contingencies
  - ✓ Damaged PDU
  - ✓ Damaged RR
  - ✓ Damaged REJ

## Lecture 6
## Multiple Access Techniques

**Outlines**

- Review of previous lecture #5
- FDMA
- TDMA
- Random Access
  - ✓ ALOHA
  - ✓ Slotted ALOHA
- Summary of today's lecture
- CDMA
  - ✓ Reservation-based ALOHA

**Last Lecture Review**

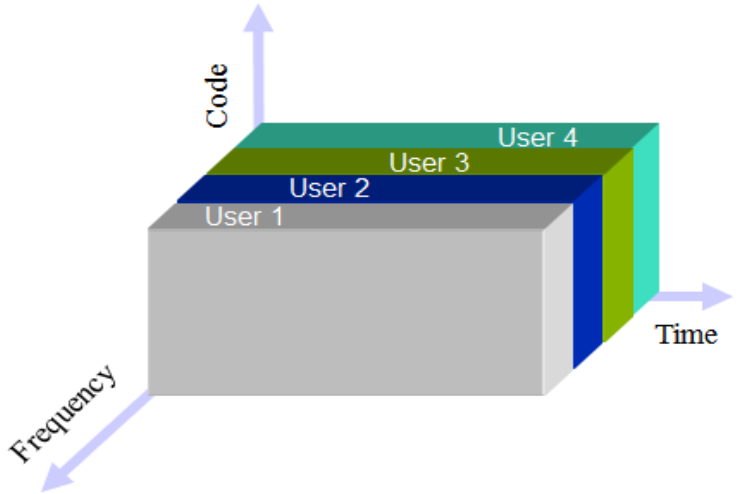
- Block Codes
  - ✓ Hamming
  - ✓ BCH
  - ✓ Reed Solmon
- ARQ
  - ✓ Sliding window
  - ✓ Go-back-N

**Multiple Access Techniques**

- Frequency Division Multiple Access (FDMA)
- Time Division Multiple Access (TDMA)
- Random Access
- Code Division Multiple Access (CDMA)

**FDMA**

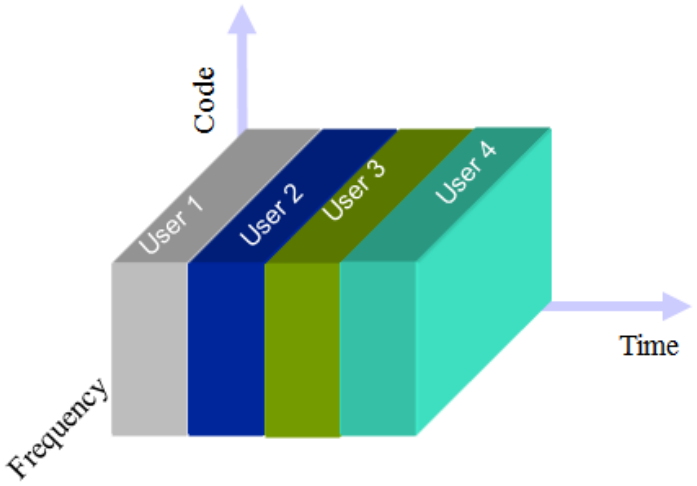
- FDMA was the initial multiple-access technique for cellular systems
- Separates large band into smaller channels.
- Each channel has the ability to support user.
- Guard bands are used to separate channel preventing co-channel interference
- Narrow bandwidth (30 khz).



- Advantages
  - ✓ Simple to implement in terms of hardware.
  - ✓ Fairly efficient with a small base population and with constant traffic.
- Disadvantages
  - ✓ Network and spectrum planning are intensive and time consuming.
  - ✓ Channels are dedicated for a single user, idle channels add spectrum inefficiency.

**TDMA**

- Entire bandwidth is available to the user for finite period of time.
- Users are allotted time slots for a channel allowing sharing of a single channel.
- Requires time synchronization.
- Each of the user takes turn in transmitting and receiving data in a round robin fashion.

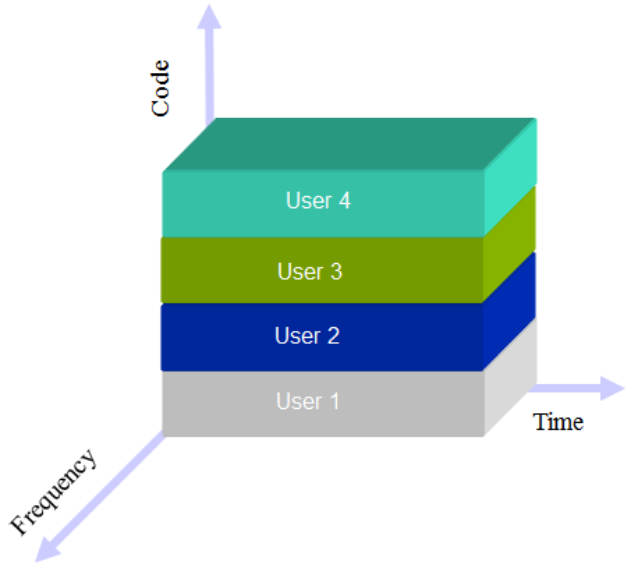



**How it works?**

- User presses Push-to-Talk (PTT) button
- A control channel registers the radio to the closest base station.
- The BS assigns an available pair of channels.
- Unlike FDMA, TDMA system also assigns an available time slot within the channel.
- Data transmission is not continuous rather sent and received in bursts.
- The bursts are reassembled and appear like continuous transmission.
- Advantages
  - ✓ Extended battery life and talk time
  - ✓ More efficient use of spectrum, compared to FDMA
  - ✓ Will accommodate more users in the same spectrum space than an FDMA system
- Disadvantages
  - ✓ Network and spectrum planning are intensive
  - ✓ Multipath interference affects call quality
  - ✓ Dropped calls are possible when users switch in and out of different cells.
  - ✓ Too few users result in idle channels (rural versus urban environment)
  - ✓ Higher costs due to greater equipment sophistication

**CDMA**

- CDMA is a spread spectrum technique used to increase spectrum efficiency.
- SS has been used in military applications due to anti-jamming and security.




- Basic Principles of CDMA
  - ✓ D = rate of data signal
  - ✓ Break each bit into k chips
    - Chips are a user-specific fixed pattern
  - ✓ Chip data rate of new channel = kD

**CDMA Example**

- If k=6 and code is a sequence of 1s and -1s
  - ✓ For a '1' bit, A sends code as chip pattern
    - <c1, c2, c3, c4, c5, c6>
  - ✓ For a '0' bit, A sends complement of code
    - <-c1, -c2, -c3, -c4, -c5, -c6>
- Receiver knows sender's code and performs electronic decode function
  - ✓ <d1, d2, d3, d4, d5, d6> = received chip pattern
  - ✓ <c1, c2, c3, c4, c5, c6> = sender's code
- $S_u(d) = d1 \times c1 + d2 \times c2 + d3 \times c3 + d4 \times c4 + d5 \times c5 + d6 \times c6$

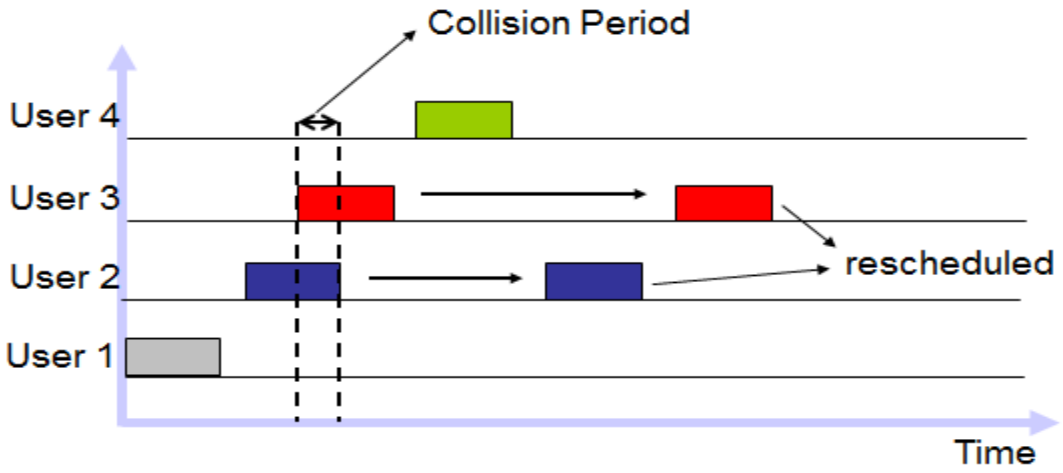
- User A code = <1, –1, –1, 1, –1, 1>
  - ✓ To send a 1 bit = <1, –1, –1, 1, –1, 1>
  - ✓ To send a 0 bit = <–1, 1, 1, –1, 1, –1>

- User B code = <1, 1, –1, – 1, 1, 1>
  - ✓ To send a 1 bit = <1, 1, –1, –1, 1, 1>

- Receiver receiving with A's code
  - ✓ (A's code) x (received chip pattern)
    - User A '1' bit: 6 -> 1
    - User A '0' bit: -6 -> 0
    - User B '1' bit: 0 -> unwanted signal ignored
- Advantages
  - ✓ Greatest spectrum efficiency:
  - ✓ CDMA improves call quality by filtering out background noise, cross-talk, and interference
  - ✓ Simplified frequency planning - all users on a CDMA system use the same radio frequency spectrum.
  - ✓ Random Walsh codes enhance user privacy; a spread-spectrum advantage
  - ✓ Precise power control increases talk time and battery size for mobile phones
- Disadvantages
  - ✓ Backwards compatibility techniques are costly
  - ✓ Currently, base station equipment is expensive
  - ✓ Low traffic areas lead to inefficient use of spectrum and equipment resources

**Random Access**

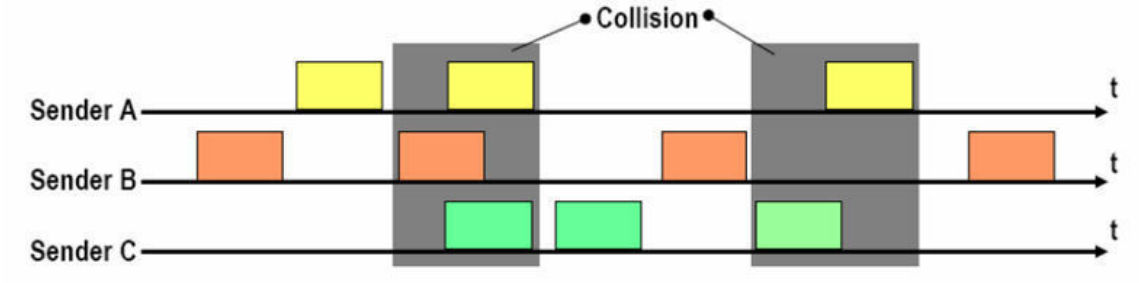
- Random Access Methods
  - ✓ more efficient way of managing medium access for communicating short bursty messages
    - in contrast to fixed-access schemes, each user gains access to medium only when needed -has some data to send
    - drawback: users must compete to access the medium ('random access')
    - collision of contending transmissions
- Random Access Methods in Wireless Networks
  - ✓ Can be divided into two groups:
    - ALOHA based-no coordination between users
    - carrier-sense based-indirect coordination -users sense availability of medium before transmitting



**ALOHA-based Random Access**

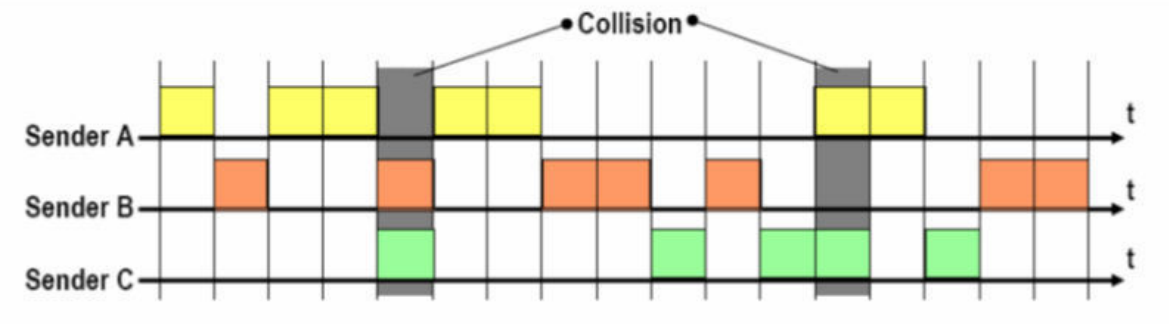
- User accesses medium as soon as it has a packet ready to transmit
  - ✓ after transmission, user waits a length of time > round-trip delay in the network, for an ACK from the receiver
  - ✓ if no ACK arrives, user waits a random interval of time (to avoid repeated collision) and retransmits
- Advantages:
  - ✓ simple, no synchronization among users required
- Disadvantages:
  - ✓ low throughput under heavy load conditions
  - ✓ probability of collision increases as number of users increases
- Max throughput = 18% of channel capacity

**Pure-ALOHA**




**Slotted ALOHA**

- Time is divided into equal time slots –when a user has a packet to transmit, the packet is buffered and transmitted at the start of the next time slot
  - ✓ BS transmits a beacon signal for timing, all users must synchronize their clocks
- advantages:
  - ✓ partial packet collision avoided
- Disadvantages
- throughput still quite low!
  - ✓ there is either no collision or a complete collision
- max throughput = 36% of channel capacity

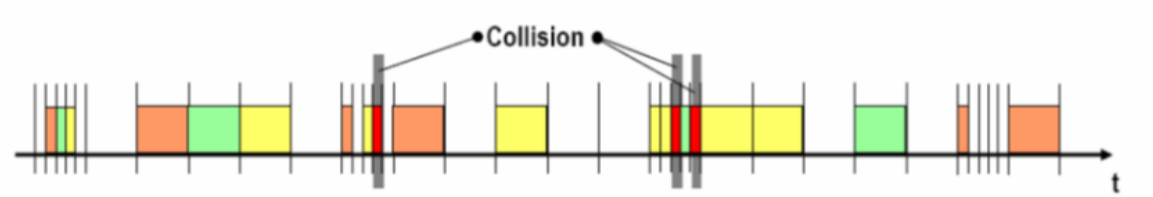


**Slotted ALOHA in GSM**

- Two types of channels in GSM:
  - ✓ Traffic channels (TCH): used for transmission of user data –based on FDMA/TDMA
    - Signalling channels, used for control and management of a cellular network
  - ✓ Random Access Channel (RACH): signalling channel for establishing access to the network (i.e. BS)
    - employs Slotted ALOHA
    - only channel in GSM where contention can occur

**Reservation ALOHA**

- Time slots are divided into reservation and transmission slots / periods
  - ✓ during reservation period, stations can reserve future slots in transmission period
  - ✓ reservation slot size << transmission slot size
  - ✓ collisions occur only in reservation slots
- Advantages:
  - ✓ higher throughput under heavy loads
  - ✓ max throughput up to 80% of channel capacity
- Disadvantages:
  - ✓ more demanding on users as they have to obtain / keep 'reservation list' up-to-date
- R-Aloha is most commonly used in satellite systems
- satellite collects requests, complies 'reservation list' and finally sends the list back to users




**Summary**

- FDMA
- TDMA
- CDMA
- Random Access
  - ✓ ALOHA
  - ✓ Slotted ALOHA
  - ✓ Reservation-based ALOHA
- Next Lecture
  - ✓ Carrier-sense based random access
  - ✓ Spread Spectrum

## Lecture 7
## CSMA and Spread Spectrum

**Last Lecture Review**

- FDMA
- TDMA
- CDMA
- Random Access
- ALOHA
- Slotted ALOHA
- Reservation-based ALOHA

**Carrier Sense Multiple Access (CSMA)**

- Disadvantages of ALOHA
  - ✓ users do not listen to the channel before (and while) transmitting
  - ✓ suitable for networks with long propagation delays
- Carrier Sense Multiple Access
  - ✓ polite version of ALOHA
  - ✓ Listen to the channel before transmitting
    - o if sensed channel busy, back-off (defer transmission), and sense channel again after a random amount of time
    - o if channel idle, transmit entire frame

**Versions of CSMA**

- Employs different node behaviour when channel found busy
  - ✓ Non-persistent CSMA
    - o after sensing busy channel, node waits entire back-off period before sensing again
  - ✓ Persistent CSMA
    - o after sensing busy channel, node continues sensing until the channel becomes free; then …
  - ✓ 1-persistent CSMA
    - o node transmits immediately with probability 1
  - ✓ p-persistent CSMA
    - o node transmits with probability p; or, it defers transmission with probability (1-p)

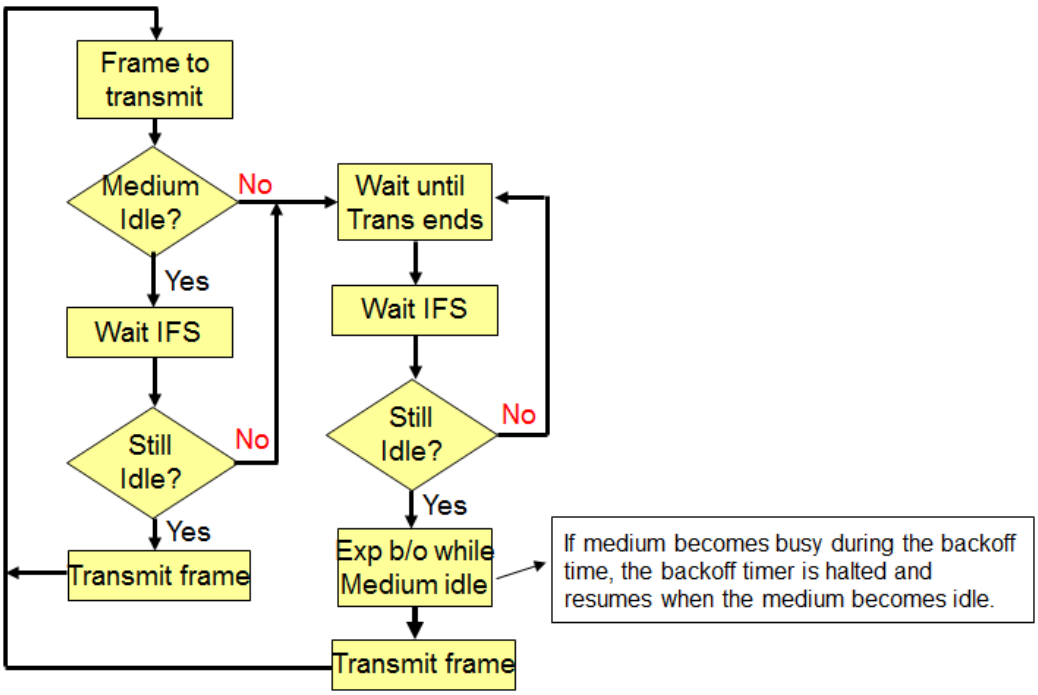
**CSMA / Collision Avoidance**

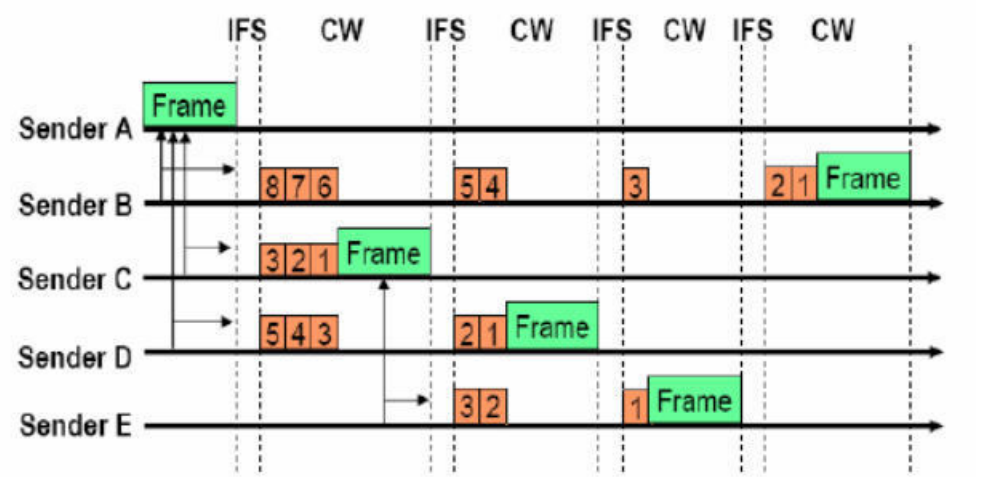
- Used where CSMA/CD cannot be used, e.g. in wireless medium collision cannot be easily detected as power of transmitting overwhelms receiving antenna
- CSMA/CA is designed to reduce collision probability at points where collisions would most likely occur
  - ✓ when medium has become idle after a busy state, as several users could have been waiting for medium to become available
- key elements of CSMA/CA:
  - ✓ IFS –interframe spacing –priority mechanism–the shorter the IFS the higher the priority for transmission
  - ✓ CW intervals –contention window –intervals used for contention and transmission

of packet frames

- ✓ Backoff counter–used only if two or more stations compete for transmission

**CSMA/CA Algorithm**




**Spread Spectrum**

- Problem of Radio Transmission
  - ✓ frequency dependent fading can wipe out narrowband signals for duration of interference
- Solution:
  - ✓ spread narrow band signal into a broad band signal using a special code

- ✓ initially developed for military in order to combat jamming and interception
- ✓ power of spread signal is the same as of narrow band signal, resulting in a lower power spectral density due to larger bandwidth

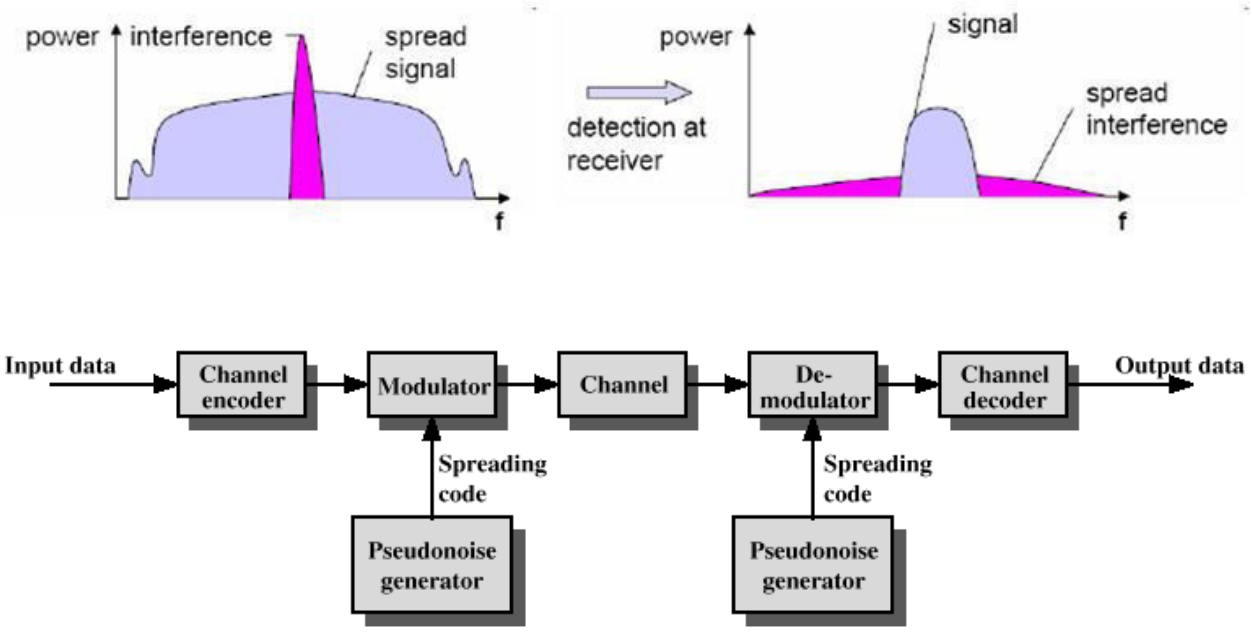



**Figure 7.1 General Model of Spread Spectrum Digital Communication System**

**Types of spreading:**

- Direct sequence spread spectrum (DSSS)
- Frequency hopping spread spectrum (FHSS)

**Frequency Hoping Spread Spectrum (FHSS)**

- Signal is broadcast over seemingly random series of radio frequencies
  - ✓ A number of channels allocated for the FH signal
  - ✓ Width of each channel corresponds to bandwidth of input signal
- Signal hops from frequency to frequency at fixed intervals
  - ✓ Transmitter operates in one channel at a time
  - ✓ Bits are transmitted using some encoding scheme
  - ✓ At each successive interval, a new carrier frequency is selected
- Channel sequence dictated by spreading code
- Receiver, hopping between frequencies in synchronization with transmitter, picks up message
- Advantages
  - ✓ Eavesdroppers hear only unintelligible blips
  - ✓ Attempts to jam signal on one frequency succeed only at knocking out a few bits

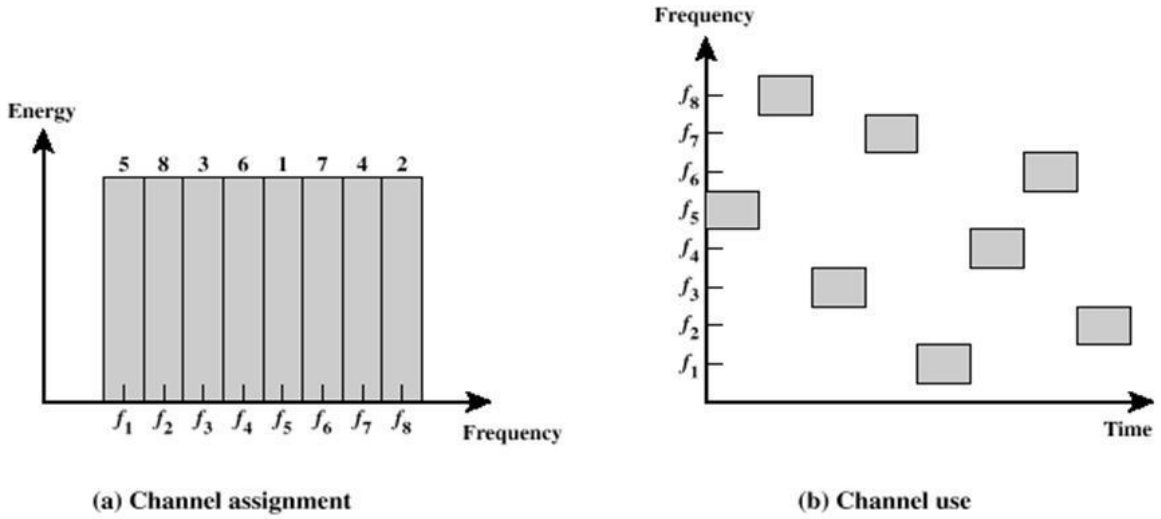
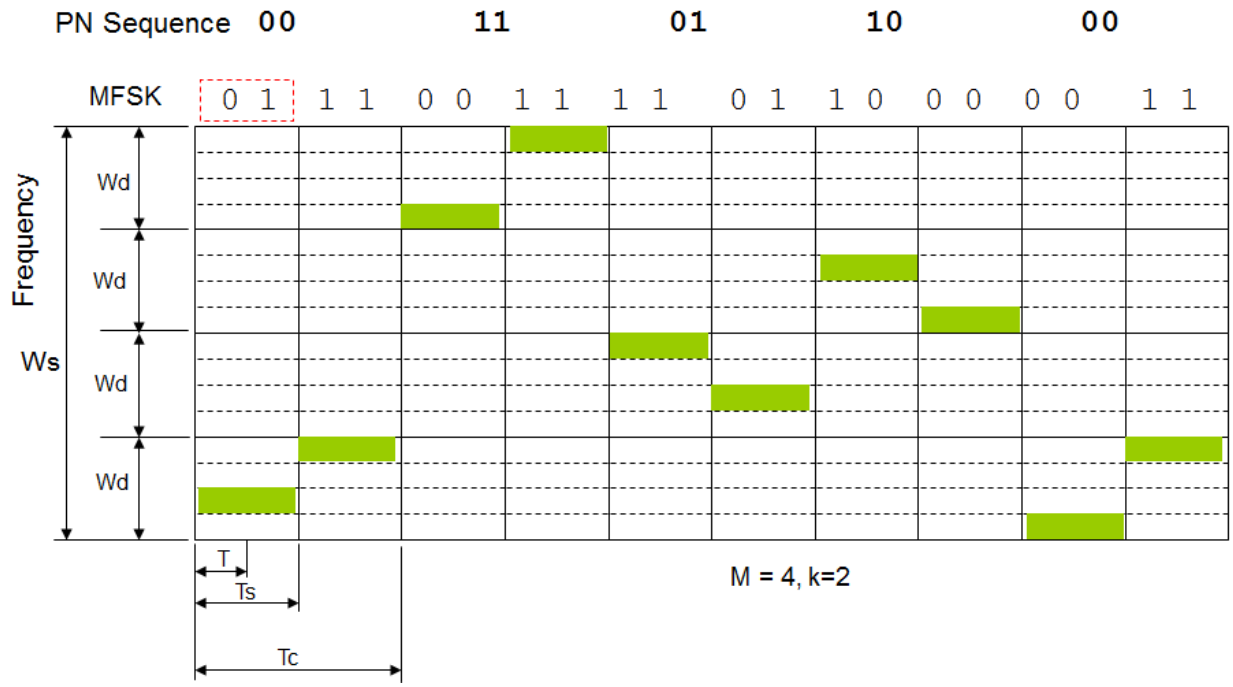



**Figure 7.2 Frequency Hopping Example**

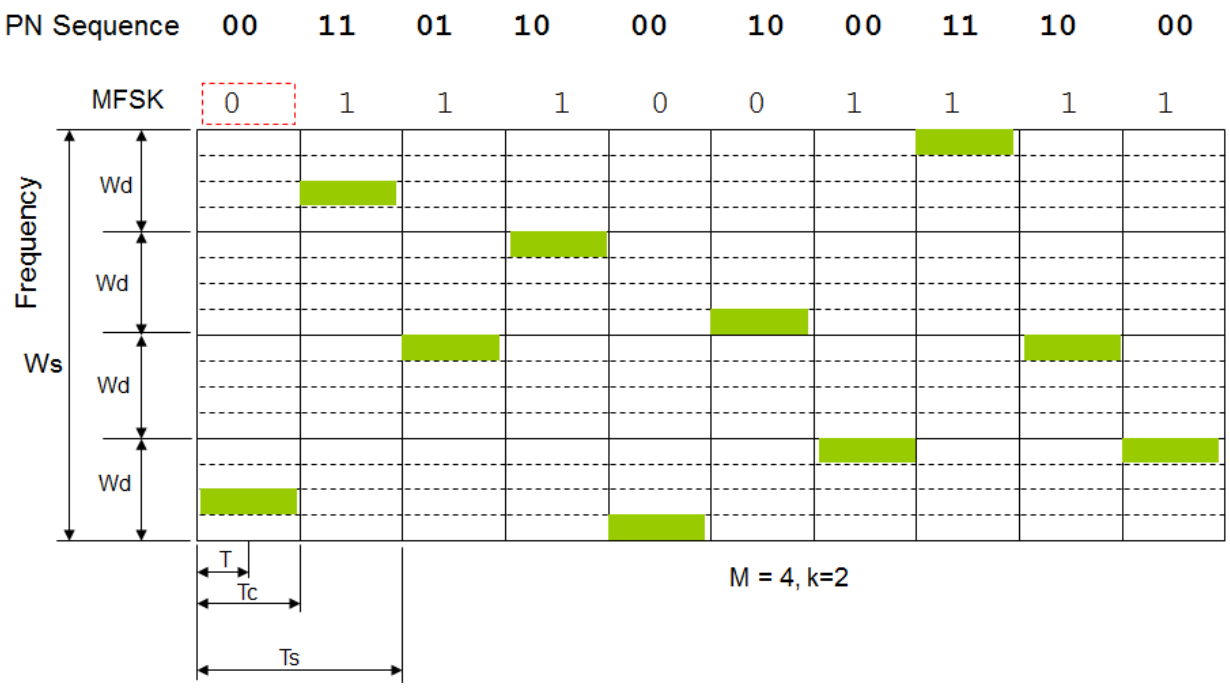
### FHSS Using MFSK

- MFSK signal is translated to a new frequency every $T_c$ seconds by modulating the MFSK signal with the FHSS carrier signal
- For data rate of R:
  - ✓ duration of a bit: T = 1/R seconds
  - ✓ duration of signal element: $T_s$ = LT seconds
- $T_c \geq T_s$ - slow-frequency-hop spread spectrum
- $T_c < T_s$ - fast-frequency-hop spread spectrum

### Slow-frequency Hop Spread Spectrum using MFSK



**Fast-frequency Hop Spread Spectrum using MFSK**




**FHSS Performance Considerations**

- Large number of frequencies used
- Results in a system that is quite resistant to jamming
  - ✓ Jammer must jam all frequencies
  - ✓ With fixed power, this reduces the jamming power in any one frequency band

**Direct Sequence Spread Spectrum (DSSS)**

- Each bit in original signal is represented by multiple bits in the transmitted signal
- Spreading code spreads signal across a wider frequency band
  - ✓ Spread is in direct proportion to number of bits used
- One technique combines digital information stream with the spreading code bit stream using exclusive-OR

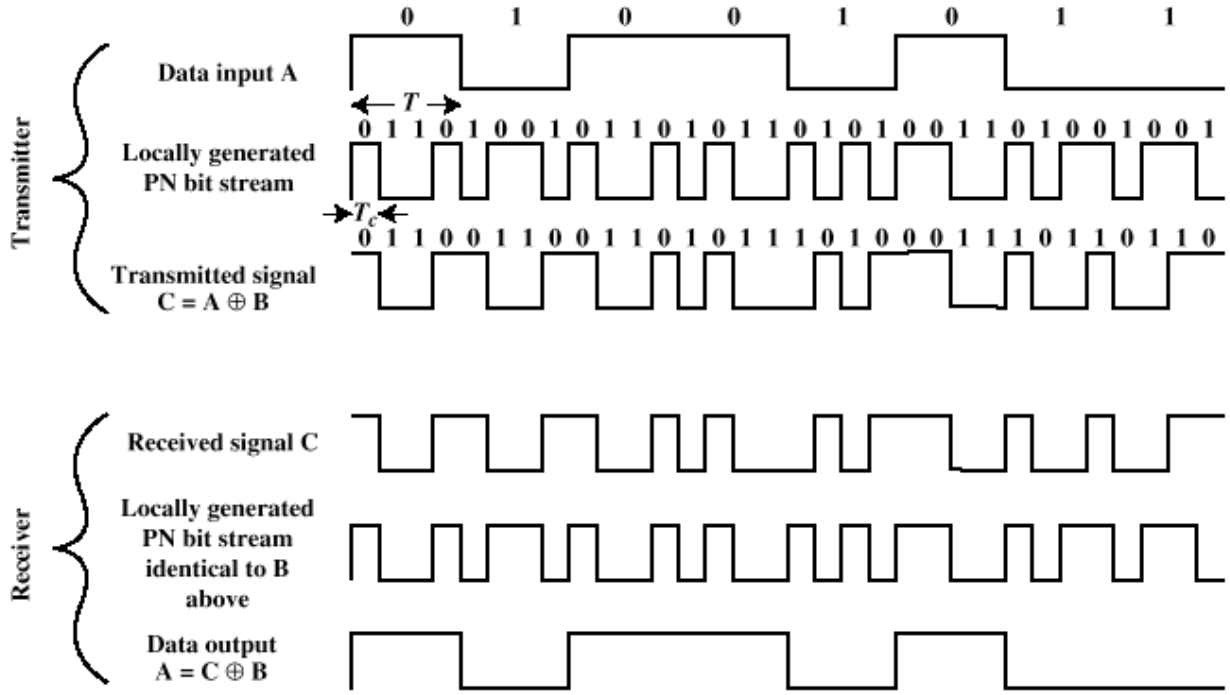



**Figure 7.6 Example of Direct Sequence Spread Spectrum**

**Summary**

- CSMA
  - ✓ Versions of CSMA
  - ✓ CSMA/CA
  - ✓ Example
- Spread Spectrum
  - ✓ Frequency Hoping
  - ✓ Direct Sequence
- Next Lecture
  - ✓ Evolution of wireless networks

## Lecture 8
## Evolution of Wireless Networks

**Today Goals**

- Review of previous lecture #7
- 1G wireless cellular networks
  - ✓ NMT
  - ✓ AMPS
  - ✓ TACS
- 2G cellular systems
  - ✓ GSM
  - ✓ IS-136
  - ✓ PDC
  - ✓ IS-95
- Summary of today's lecture

**Last Lecture Review**

- CSMA
  - ✓ Versions of CSMA
  - ✓ CSMA/CA
  - ✓ Example
- Spread Spectrum
  - ✓ Frequency Hoping
  - ✓ Direct Sequence

**Evolution of Wireless Systems**

- The worldwide success of cellular telephone has lead to the development of newer wireless systems and standards for other types of communications besides mobile voice.
- For example
  - ✓ Cellular networks to facilitate high speed data traffic
  - ✓ Replace fiber optics and copper lines between fixed points several kms apart.
  - ✓ Replacement of wires within homes, offices etc (evolution of Bluetooth)

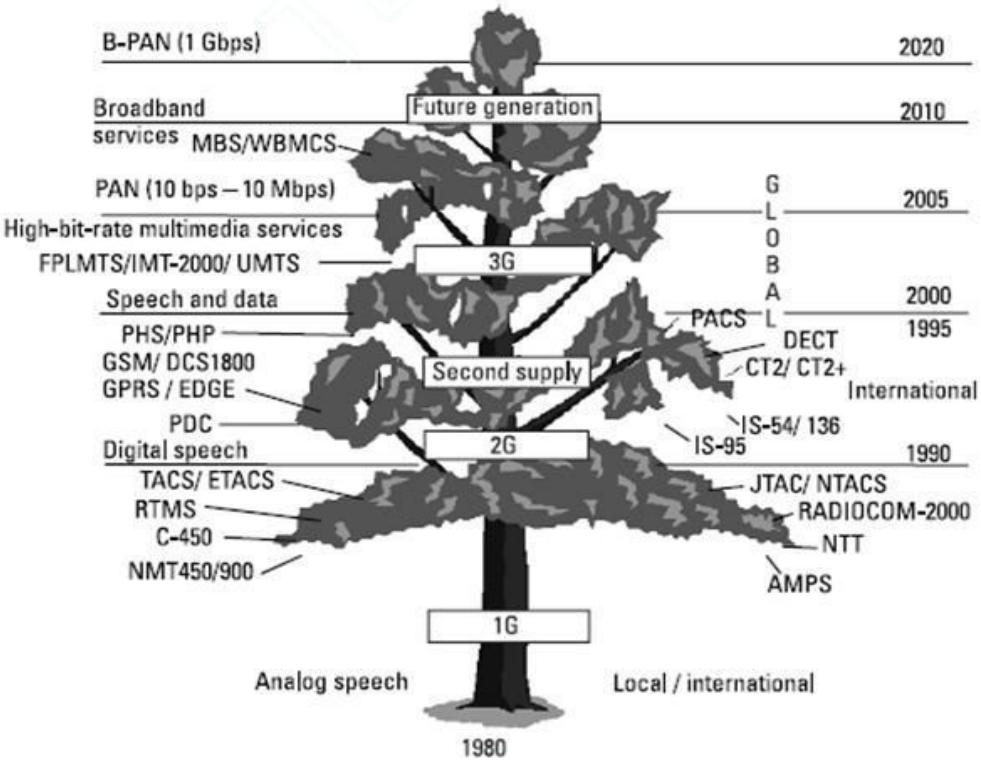
- Prior to the introduction of cellular phones, mobile telephone service was provided by a high power tx/rx.
- A typical system would support about 25 channels with an effective radius of about 80 km.
- The way to increase the capacity of the system is to use lower-power systems with shorter radius and to use numerous tx/rx. Cellular systems were evolved to provide organization of tx/rx and to further improve the capacity of systems.
- Explain little bit about cellular architecture….

**First-Generation Cellular Networks**

- Analog systems
- Standards
  - ✓ NMT (Nordic Mobile Telephone)
    - o used in Nordic countries, Switzerland, Netherlands, Eastern Europe and Russia.
  - ✓ AMPS (Advanced Mobile Phone System)
    - o used in the United States,
  - ✓ TACS (Total Access Communications System)
    - o used in the United Kingdom,

- ✓ C-450
  - in West Germany, Portugal and South Africa,
- ✓ Radiocom 2000 in France
- ✓ RTMI in Italy.
- ✓ In Japan there were multiple systems. Three standards, TZ-801, TZ-802, and TZ-803

**Evolution Tree of Wireless Systems**




**NMT**

- First fully-automatic cellular phone system
  - ✓ Started in 1970, in service 1981
- Two standards NMT-450 and NMT-900
  - ✓ Corresponds to frequency and the later has higher bands.
- Cell size range from 2 km to 30 km.
  - ✓ Use smaller size in urban areas for better quality and larger in less-populated areas.
- Handsets 1 watt and Car phone uses 6-15 watt
- Automatic switching (dialing) and handover.
- No spec. for voice traffic encryption
  - ✓ Buy a scanner, tune to the desired channel and intercept.
- NMT also supported a simple data transfer mode called DMS (Data and Messaging Service) or NMT-Text

- Using DMS, also text messaging was possible between two NMT handsets before SMS service started in GSM
- but this feature was never commercially available except in Russian and Polish NMT networks.
- NMT Suspended
  - ✓ In Finland TeliaSonera's NMT on December 31, 2002.
  - ✓ Norway's last NMT network on December 31, 2004.
  - ✓ Sweden's TeliaSonera NMT on December 31, 2007.

**AMPS**

- 1G cellular phone used in US, which uses FDMA
- Operates in 800 MHz band
  - ✓ Total of 832 channels;
    - o 416 in 824–849 MHz for transmissions from mobile to the base
    - o 416 in 869–894 MHz for transmissions from base to the mobile.
    - o Each channel is 30 KHz wide
- Require large bandwidth for large base population.
- No protection against eavesdropper
  - ✓ ESN (Electronic Serial Number) was cloned in 1990s to make free calls from different cells.
- Replaced with D-AMPS, GSM and CDMA for better security and capacity

**TACS**

- A variant of AMPS developed by Motorola.
- It has been used in some European countries (including the UK & Ireland), as well as Japan and Hong Kong.
- ETACS was an extended version of TACS with more channels.
- The last ETACS service operated by Vodafone was discontinued on 31 May 2001

**Second-Generation Cellular Networks**

- Digital system i.e. voice is digitized
- Unlike 1G that relies on FDMA/FDD, 2G use digital modulation formats and TDMA/FDD, CDMA/FDD multiple access techniques
- Can be divided into two standards; TDMA and CDMA
- The main 2G standards are
  - ✓ GSM (TDMA-based), originally from Europe but used worldwide
  - ✓ IS-136 aka D-AMPS, TDMA-based, used in the Americas
  - ✓ IS-95 aka cdmaOne, CDMA-based, used in the Americas and parts of Asia
  - ✓ PDC (TDMA-based), used exclusively in Japan
- Using digital signals between the handsets and the towers increases system capacity in two key ways:
  - ✓ Digital voice data can be compressed and multiplexed much more effectively than analog voice encodings through the use of various CODECs, allowing more calls to be packed into the same amount of radio bandwidth.

- ✓ The digital systems were designed to emit less radio power from the handsets. This meant that cells could be smaller, so more cells could be placed in the same amount of space. This was also made possible by cell towers and related equipment getting less expensive.

- 2G Advantages
  - ✓ The lower powered radio signals require less battery power, so phones last much longer between charges, and batteries can be smaller.
  - ✓ The digital voice encoding allowed digital error checking which could increase sound quality by reducing dynamic and lowering the noise floor.
  - ✓ Going all-digital allowed for the introduction of digital data services, such as SMS and email.
  - ✓ Better security, harder to be scanned

**GSM**

- 2.27 billion subscribers across more than 212 countries, 81% of the global mobile market
- Its ubiquity provides international roaming very common
- 8-slots TDMA with 200 KHz radio channel, with frame duration of 4.615 ms
- The channel data rate is 270.833 kbit/s
- Operates in four different bands
  - ✓ Mostly 900 MHz or 1800 MHz
  - ✓ US and Canada use 850 MHz and 1900 MHz
  - ✓ 25 MHz bandwidth of each subdivided into 124 channels
  - ✓ E.g. in 900 MHz, uplink 890-915 MHz, downlink 935-960 MHz

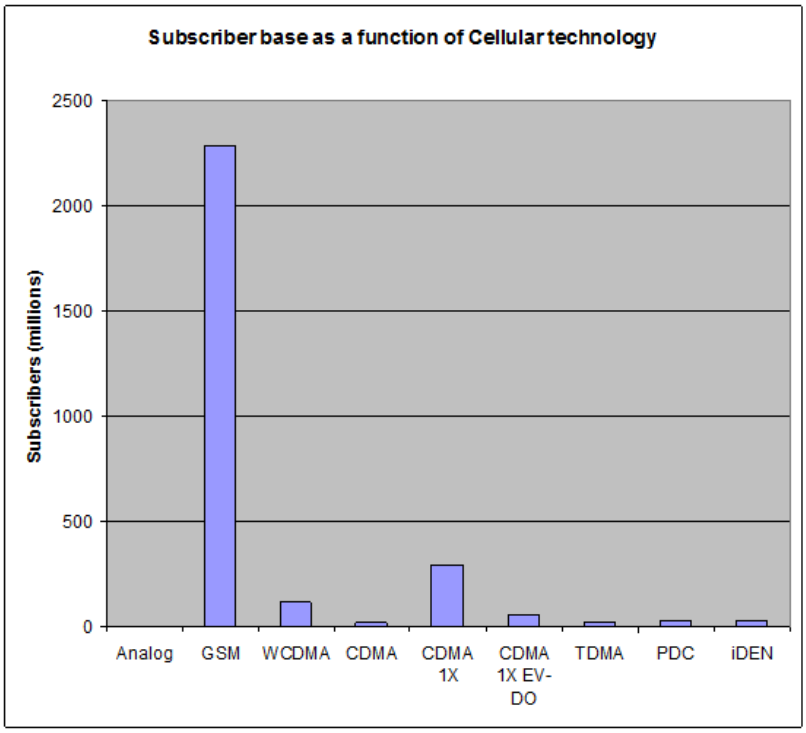
**Others Systems**

- IS-136 or D-AMPS
  - ✓ 3-Slot TDMA, used in North and South America, Australia
  - ✓ Channel bandwidth is 30 KHz.
  - ✓ Frequency bands (824-849MHz and 869-894 MHz)
- Pacific Digital Cellular (PDC)
  - ✓ Japanese standard similar to IS-136
  - ✓ 25 KHz channel
  - ✓ 11.2 kbps at 3-slot and 5.6 kbps at 6-slot
  - ✓ Operates in 800 MHz downlink 810-888 MHz, uplink 893-958 MHz)
  - ✓ In 1.5 GHz (downlink 1477-1501 MHz, uplink 1429-1453 MHz)
- IS-95 or cdmaOne
  - ✓ Supports up to 64 users that are orthogonally coded
  - ✓ Channel bandwidth is 1.25 MHz
  - ✓ Widely deployed in N. America, Korea, Japan, China, S. America, Australia
  - ✓ Channel data rate is 1.2288 Mchips/s (Mega Chips)

# Subscriber statistics end Q1 2007

| **World** | **2,831,345,390** | |
|---|---|---|
| GSM | 2,278,095,380 | 80.5% |
| 3GSM (WCDMA) | 114,664,827 | 4.0% |
| CDMA | 18,138,942 | 0.6% |
| CDMA 1X | 289,963,166 | 10.2% |
| CDMA 1X EV-DO | 57,376,347 | 2.0% |
| TDMA | 16,235,932 | 0.6% |
| PDC | 27,857,370 | 1.0% |
| iDEN | 26,494,743 | 0.9% |
| Analog | 2,518,683 | 0.1% |

| **Top 10 growth countries** | |
|---|---|
| **GSM net additions in Q1 2007:** | |
| China | 18,040,914 |
| India | 13,728,036 |
| Pakistan | 7,662,993 |
| Indonesia | 5,394,269 |
| Iran | 5,135,330 |
| Brazil | 3,877,141 |
| Argentina | 3,809,765 |
| Nigeria | 3,321,118 |
| Thailand | 3,255,817 |
| Russian Federation | 3,215,204 |




**Summary of today's lecture**

- 1G analog systems
  - ✓ NMT
  - ✓ AMPS
  - ✓ TACS
  - ✓ C-450
- 2G digital cellular systems
  - ✓ GSM
  - ✓ IS-136
  - ✓ IS-95
- Next Lecture
  - ✓ 3G and 4G

## Lecture 9
## Evolution of Wireless Networks (Part II)

**Outlines**

- Review of last lecture #8
- 2.5G
  - ✓ HSCSD
  - ✓ GPRS
  - ✓ EDGE
  - ✓ IS-95B
- 3G
  - ✓ UMTS/W-CDMA
  - ✓ CDMA2000
- Summary of today's lecture

**Review of last lecture #8**

- 1G wireless cellular networks
  - ✓ NMT
  - ✓ AMPS
  - ✓ TACS
- 2G cellular systems
  - ✓ GSM
  - ✓ IS-136
  - ✓ PDC
  - ✓ IS-95

**Key Specifications of 2G Technologies**

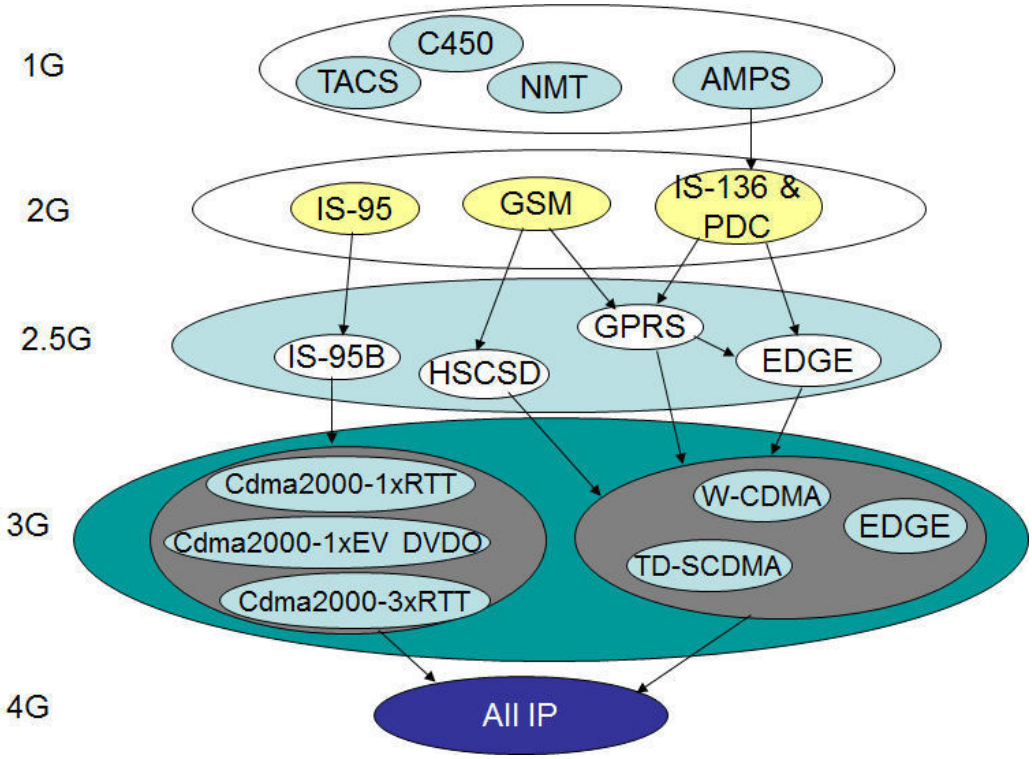
| | IS-95/cdmaOne | GSM, DCS-1900 | IS-54, IS-136, PDC |
|---|---|---|---|
| Uplink frequencies | 824-849 MHz (US)<br>1850-1910 MHz (US pcs) | 890-915 MHz (EU)<br>1850-1910 MHz (US) | 800 MHz, 1500 MHz (Japan)<br>1850-1910 MHz (US pcs) |
| Downlink frequencies | 869-894 MHz US<br>1930-1990 MHz US pcs | 935-960 MHz EU<br>1930-1990 MHz US pcs | 869-894 MHz US<br>800, 1500 MHz Japan |
| Duplexing | FDD | FDD | FDD |
| Multiple access tech. | CDMA | TDMA | TDMA |
| Modulation | BPSK with Quad. | GMSK with BT.3 | DQPSK |
| Carrier bandwidth | 1.25 MHz | 200 KHz | 30 KHz |
| Data rate | 1.2288 MChips/s | 270.833 kbps | 48.6 kbps |
| Channels / carrier | 64 | 8 | 3 |
| Speech Coding | CELP @ 13kbps<br>EVRC @ 8 kbps | RPE-LTP @ 13 kbps | VSELP @ 7.95 kbps |

**Evolution to 2.5G**

- 2.5G upgrade must be compatible with 2G technology
- Three different upgrade paths developed for GSM and two of these supports IS-136
  - ✓ High speed circuit switched data (HSCSD)
  - ✓ General packet radio service (GPRS)

- ✓ Enhanced Data rates for GSM Evolution (EDGE)
- GPRS and EDGE supports IS-136
- IS-95B upgrade for IS-95

**Wireless Networks Upgrade Paths**




**HSCSD**

- Works in circuit switch mode.
- Speed increased by allowing single user to use consecutive time slots in GSM standard
- Relaxes error control coding algorithms specified in GSM increasing data rate from 9.600 to 14.400 Kbps
- By using 4 slots, raw data rate of up to 57.6 kbps to individual user.
- Ideal for dedicated streaming or real-time interactive web sessions

**GPRS**

- Packet-based data networks.
- Well-suited for non real-time traffic like email, faxes, web browsing
- Unlike HSCSD, GPRS allows multi-user channel sharing of individual radio channel and time slots and supports many more users.
- GPRS units are automatically instructed to tune to dedicated GPRS channels and particular time slots for always-on access.
- When all 8 slots are dedicated, data rate reaches to 171.2 kbps (8 x 21.4 kbps of raw un-coded data)

**EDGE (2.75G)**

- More advanced upgrade to 2G that requires addition of new hardware and software
- Developed as a path to become eventual 3G high speed data access
- New modulation 8-PSK in addition to GSM standard GMSK.
- Allows nine different formats known as Multiple modulation and Coding Scheme (MCS)
- Each MCS state may either use GMSK (low rate) or 8-PSK (high rate).
- A family of MCS for each GSM slot and users can adaptively determine best MCS setting
- User start first with max error protection and max data rate until the link has unacceptable outage or delay
- By combining different channels (multi-carrier trans), EDGE provides upto several megabits per second data throughput.

**IS-95B or cdmaOne**

- IS-95/CDMA has a single upgrade path IS-95B for eventual 3G operation.
- Dedicate multiple orthogonal user channels for specific users.
- IS-95A support 64 users with data rate 14,400 Kbps
- Medium data rate service by allowing user to command up to 8 Walsh codes.
- The raw data rate reaches to 8x14,400 = 115.2 kbps
- Supports hard handoff procedure
    - ✓ Allow units to search different radio channels without instruction from switch. User can rapidly tune to different BS.

**Evolution to 3G**

- Third generation of mobile phone standards based on the International Telecommunication Union (ITU) family of standards under the International Mobile Telecommunications programme, "IMT-2000"
- 3G technologies enable network operators to offer users a wider range of more advanced services while achieving greater network capacity through improved spectral efficiency. Services include
    - ✓ Broadband wireless data, all in a mobile environment.
    - ✓ Typically, they provide service at 5-10 Mb per second.
- The most significant feature of 3G is that it supports
    - ✓ greater numbers of voice and data customers
    - ✓ at higher data rates at lower incremental cost than 2G

**3G Evolution**

- The community remain split into two camps
    - ✓ GSM/IS-136/PDC
        - The 3G evolution is wideband CDMA (W-CDMA)
        - Also known as UMTS
    - ✓ IS-95B or CDMA
        - Evolution path is cdma2000
        - Several variants exist but all based on IS-95B

- ITU-2000 standards are separated into two major organizations reflecting two 3G camps
  - ✓ 3GPP: 3G partnership project for W-CDMA
  - ✓ 3GPP2: 3G partnership project 2 for cdma2000

**3G W-CDMA (UMTS)**

- This standard has evolved under European Telecom. Standards Institute (ETSI).
- Backward compatible with 2G standards GSM, IS-136 and PDC technologies as well as 2.5G
- Bit level packaging of GSM data is retained, with additional capacity and bandwidth provided by new CDMA air interface
- Always-on packet-based service for computers, entertainment devices and telephone.
- Require expensive new BS equipments making installation slow and gradual
- Data rate supported up to 2.048 Mbps per user
  - ✓ Allowing high quality data, multimedia, streaming audio (for stationary user).
- Future version will support data rate in excess of 8 Mbps
- Minimum spectral allocation of 5 MHz
- Data rates from as low as 8 kbps to as high as 2 Mbps will be carried simultaneously on a single radio channel.
- Each channel can support between 100 and 350 voice calls simultaneously depending on propagation conditions

**3G CDMA 2000**

- Provides seamless and evolutionary upgrade path for 2G and 2.5G CDMA technology.
- Centers on original 1.25 MHz radio channel
- CDMA operators may seamlessly and selectively upgrade without changing entire BS equipment
- The first 3G CDMA standard cdma2000 1xRTT using single channel (1x => multi-carrier)
- Cdma2000 1x
  - ✓ supports data rate up to 307 kbps in packet mode
  - ✓ Can support up to twice as many users as 2G CDMA
  - ✓ No additional equipment needed, simply software and new channel cards at BS
- Cdma2000 1xEV Evolution by Qualcomm
  - ✓ Proprietary high data rate packet standard to be overlaid on existing
  - ✓ CDMA 1xEC-DO dedicates the channel strictly to data user and support 2.4 Mbps per channel.
- Cdma2000 3xRTT
  - ✓ The ultimate 3G solution relies upon multicarrier that gang adjacent channels together into 3.75 MHz.
  - ✓ Three non-adjacent channels may be operated simultaneously and in parallel.
  - ✓ Data rate in excess of 2 Mbps similar when compared to W-CDMA
- Advocates of cdma2000 claim their standard much more seamless and less expensive upgrade path when compared to W-CDMA.

**3G TD-SCDMA**

- In china, more than 8 millions GSM subscribers were added in just 1 month.
- china's desire to craft its own wireless vision.
- Chinese CATT and Siemens jointly submitted IMT-2000 3G standard based on Time Division Synchronous Code Division Multiple Access
- Relies on existing GSM infrastructure
- 1.6 MHz channel and smart antennas to yield more spectral efficiency.
- 5 ms frames divided into 7 slots allocated to single data only user or several slow users
- TD-SCDMA allows easy upgrade to GSM.

## Lecture 10
## Evolution of Wireless Networks (Part III)

- Review of previous lecture
- Limitation of 3G
- 4G
- Objectives
- Issues
- QoS
- Security
- Multimedia Service
- Applications
- Convergence of Cellular and WLAN
- Billing Issue
- Wireless Networks
- Summary of today

### Review of last lecture

- 2.5G
  - ✓ HSCSD
  - ✓ GPRS
  - ✓ EDGE
  - ✓ IS-95B
- 3G
  - ✓ UMTS/W-CDMA
  - ✓ CDMA2000

### Specifications of 2.5G and 3G standards

| Technology | Channel BW | Duplex | Infrastructure Changes | New Spectrum | New handsets |
|---|---|---|---|---|---|
| **HSCSD** | 200 KHz | FDD | Software upgrade at BS | No | Yes, New headsets provide 57.6 kbps on HSCSD and 9.6 kbps on GSM |
| **GPRS** | 200 KHz | FDD | New packet overlay at routers and gateways | No | Yes, new GPRS sets work at 171.2 kbps, 9.6 kbps on GSM, dual-mode. |
| **EDGE** | 200 KHz | FDD | New TX/Rx at BS, software upgrade at BS, controller | No | Yes, new set work at 384 kbps on EDGE, GPRS at 144 kbps and GSM at 9.6 kbps, tri-mode |
| **W-CDMA** | 5 MHz | FDD | Completely new BS | Yes | Yes, new handsets work at 2 Mbps in WCDMA and rest as above |
| **IS-95B** | 1.25 MHz | FDD | New software at BS | No | Yes, IS-95B at 64kbps, IS-95A at 14.4 kbps and IS-95 at 9.6 kbps |
| **Cdma2000 1xRTT** | 1.25 MHz | FDD | New software at backbone, new channel cards at BS, new packet service node | No | 1xRTT at 144 kbps and rest as above. Older sets will work. |
| **Cdma2000 1xEV(DO/DV)** | 1.25 MHz | FDD | New software and cards upgrade to 1xRTT | No | 1xEV at 2.4 Mbps and as above |
| **Cdma2000 3xRTT** | 3.75 MHz | FDD | Backbone modifications and channel cards at BS | May be | 3xRTT at 2 Mbps and rest as above |

**Limitations of 3G**

- Difficulty of CDMA to provide higher data rates
- Need for continuously increasing data rate and bandwidth to meet the multimedia requirements
- Limitation of spectrum and it's allocation
- Inability to roam between different services
- To provide a seamless transport end-to-end mechanism
- To introduce a better system with reduced cost

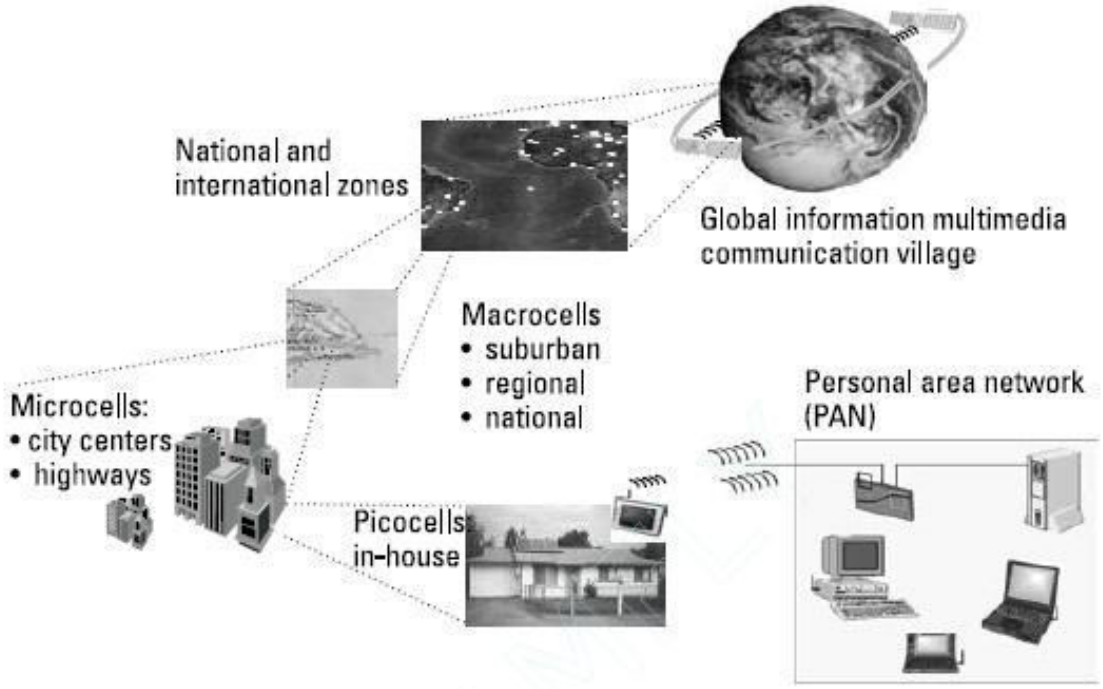
**4G**

- Provide a comprehensive IP solution where voice, data and streamed multimedia can be given to users on an "Anytime, Anywhere" basis, and at higher data rates than previous generations.
- No formal definition but certain objectives
  - ✓ Fully IP-based integrated system
  - ✓ Provides 100 Mbit/s and 1 Gbit/s speeds both indoors and outdoors, with premium quality and high security.

**4G Objectives**

- A spectrally efficient system (in bits/s/Hz and bit/s/Hz/site).
- A nominal data rate of 100 Mbit/s at higher relative speeds and 1 Gbit/s while client and station are in relatively fixed positions
- High network capacity: more simultaneous users per cell
- Smooth handoff across heterogeneous networks,
- Seamless connectivity and global roaming across multiple networks
- High quality of service for next generation multimedia support (real time audio, high speed data, HDTV video content, mobile TV, etc)
- Interoperability with existing wireless standards
- An all IP, packet switched network

**Global information multimedia communication village**



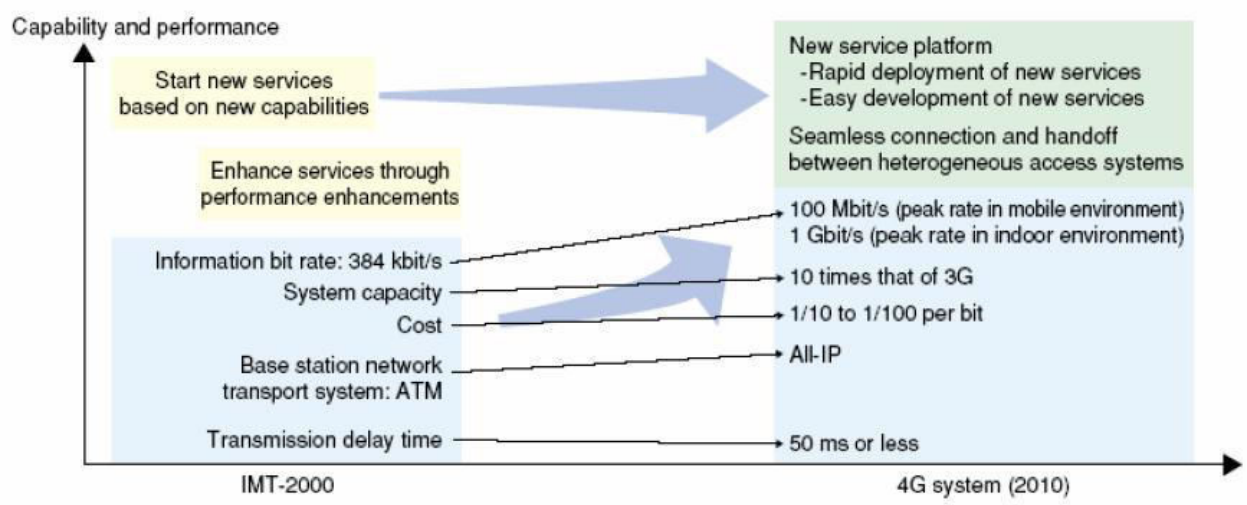

**Convergence of High Speed Internet & Mobility a Major Driver of Future Wireless**

- The Wireless Industry has grown at enormous pace over the past decade.
- Over 2.5 billion subscribers to cellular services are enjoying the benefits of staying connected while on the move.
- With the growth in Internet, a wide range of services are accessed by users through a wired infrastructure.
- The introduction of mobile Internet brought about by the convergence of Mobile & Internet technologies is the future objective.

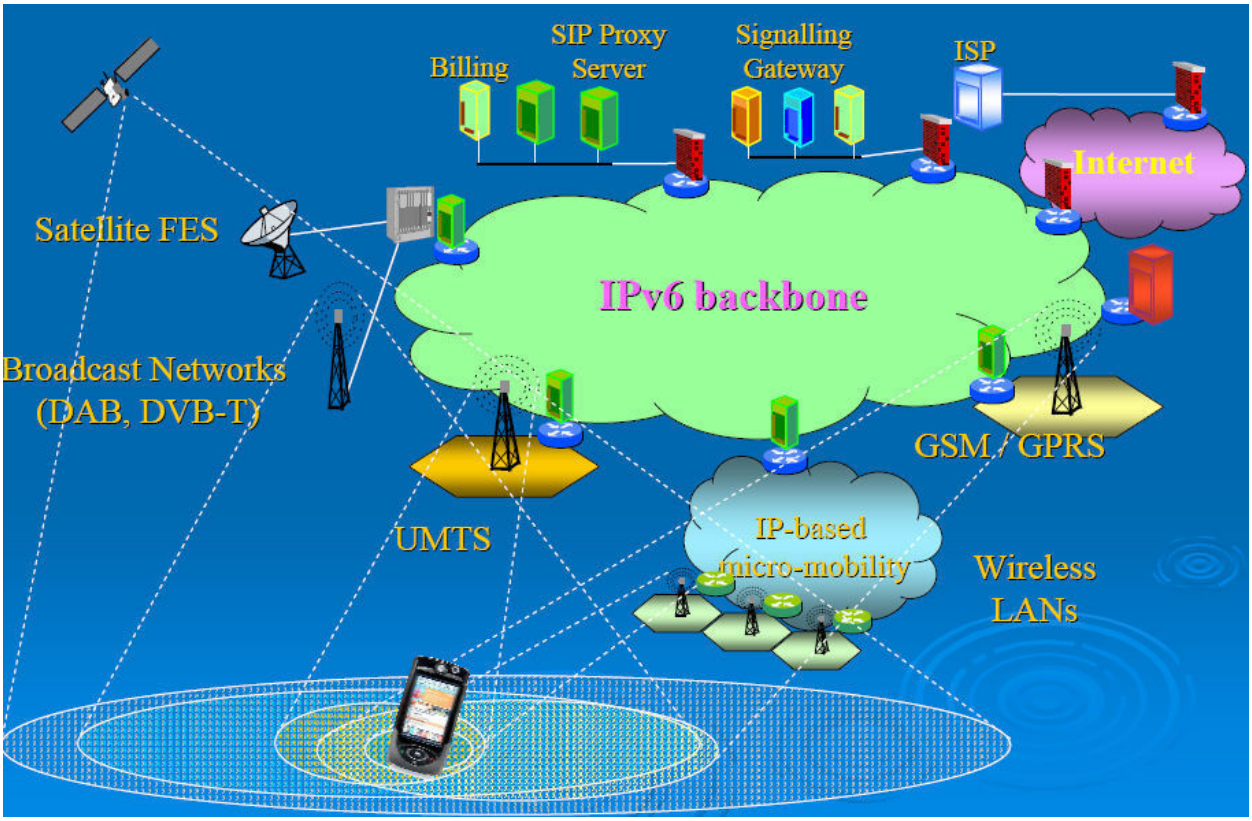
**4G Concept**

- "The user has freedom and flexibility to select any desired service with reasonable QoS and affordable price, anytime, anywhere."

## Design Objectives

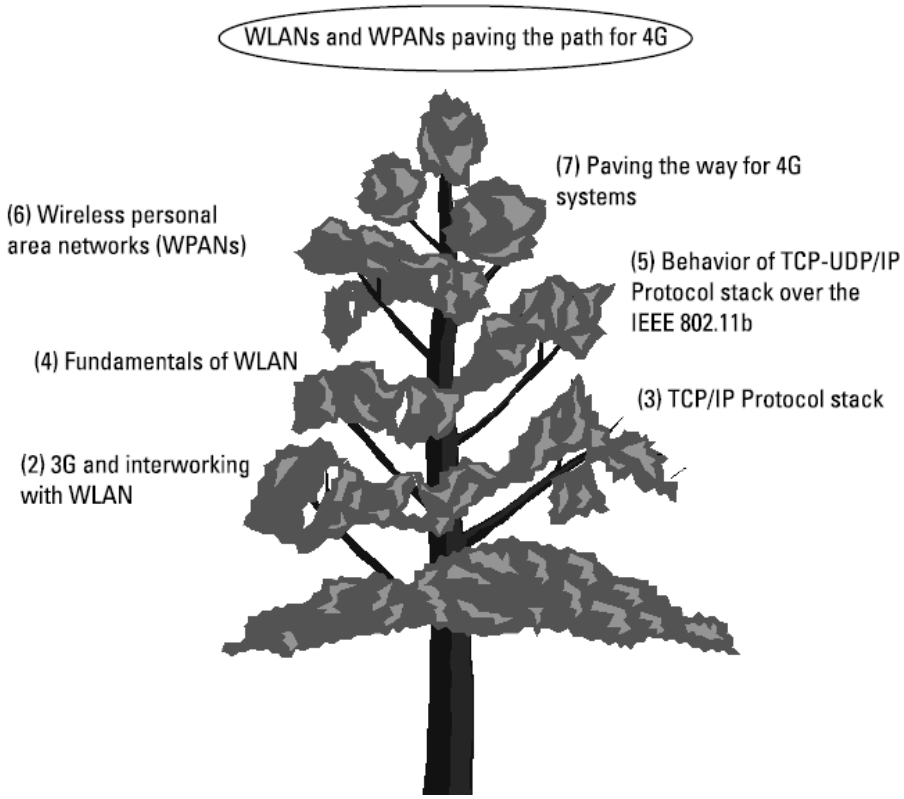



## Heterogeneous Networks



**Next Generation will also have specifically needs to resolve it's own multiple issues**

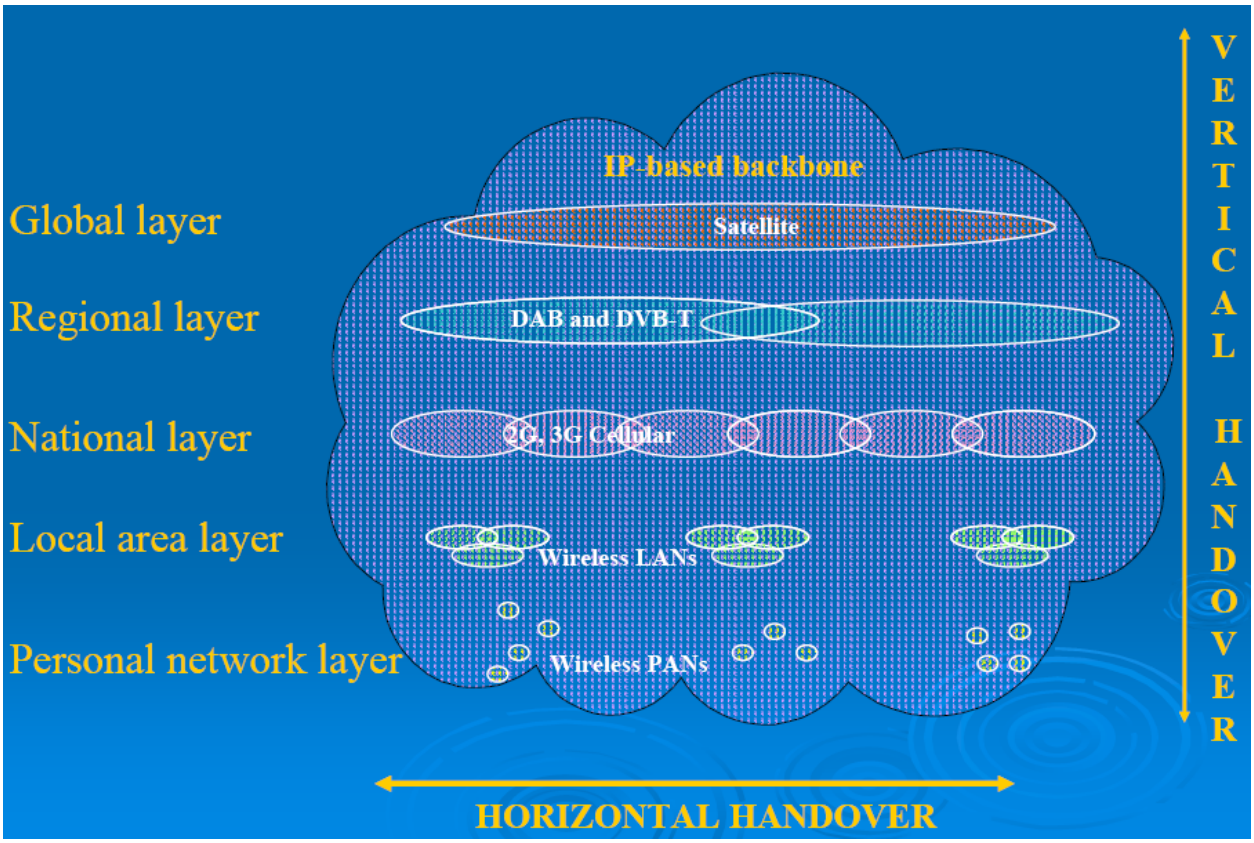
- Heterogeneous networks
- Access, handover
- Location coordination, resource coordination
- Adding new users
- QoS, wireless security and authentication
- Network failure backup
- Pricing and billing




**Quality of Service (QoS)**

- Traffic generated by the different services will not only increase traffic loads on the networks, but will also require different quality of service (QoS) requirements (e.g., cell loss rate, delay, and jitter) for different streams (e.g., video, voice, data).
- Providing QoS guarantees in 4G networks is a non-trivial issue where both QoS signalling across different networks and service differentiation between mobile flows will have to be addressed.
- One of the most difficult problems that are to be solved, when it comes to IP mobility, is how to insure the constant QoS level during the handover.
- Depending on whether the new access router is in the same or some other sub network, we recognize the horizontal and vertical handover.

**Hierarchical layer for 4G**




**Quality of Service**

- However, the mobile terminal can not receive IP packets while the process of handover is finished. This time is called the handover latency.
- Handover latency has a great influence on the flow of multimedia applications in real-time.
- Mobile IPv6 have been proposed to reduce the handover latency and the number of lost packets.
- The field “Traffic Class” and “Flow Label” in IPv6 header enables the routers to secure the special QoS for specific packet series with marked priority.

**MULTIMEDIA – Video Services**

- 4G wireless systems are expected to deliver efficient multimedia services at very high data rates.
- Basically there are two types of video services: bursting and streaming video services.
- **Streaming:** is performed when a user requires real-time video services, in which the server delivers data continuously at a playback rate.
- **Bursting:** is basically file downloading using a buffer and this is done at the highest data rate taking advantage of the whole available bandwidth.

**Security**

- Security in wireless networks mainly involves authentication, confidentiality, integrity, and authorization for the access of network connectivity and QoS resources for the mobile nodes flow.
- The heterogeneity of wireless networks complicates the security issue.
- Dynamic reconfigurable, adaptive, and lightweight security mechanisms should be developed.
- AAA (Authentication Authorization Auditing) protocols provide a framework for such suffered especially for control plane functions and installing security policies in the mobile node such as encryption, decryption and filtering.

**Convergence of Cellular Mobile Networks and WLANs**

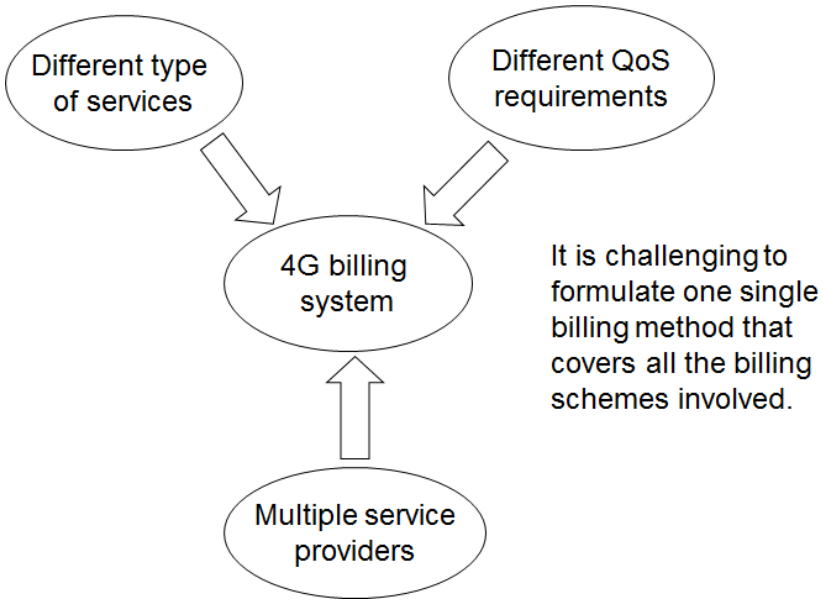
- Benefits for Operators
  - ✓ Higher bandwidths.
  - ✓ Lower cost of networks and equipment.
  - ✓ The use of licence-exempt spectrum.
  - ✓ Higher capacity and QoS enhancement.
  - ✓ Higher revenue.
- Benefits for Users
  - ✓ Access to broadband multimedia services with lower cost and where mostly needed.
  - ✓ Inter-network roaming.

**Applications**

- Virtual Presence: This means that 4G provides user services at all times, even if the user is off-site.
- Virtual navigation: 4G provides users with virtual navigation through which a user can access a database of the streets, buildings etc.
- Tele-geoprocessing applications: This is a combination of GIS (Geographical Information System) and GPS (Global Positioning System) in which a user can get the location by querying.
- Tele-Medicine and Education: 4G will support remote health monitoring of patients. For people who are interested in life long education, 4G provides a good opportunity.
- Crisis management: Natural disasters can cause break down in communication systems. In today's world it might take days or 7 weeks to restore the system. But in 4G it is expected to restore such crisis issues in a few hours.

**Multiple Operators and Billing System**

- In today's communication market, an operator usually charges customers with a simple billing and accounting scheme.
- A flat rate based on subscribed services, call durations, and transferred data volume is usually enough in many situations.
- With the increase of service varieties in 4G systems, more comprehensive billing and accounting systems are needed.




**WLANs**

- Use the unlicensed Industrial Scientific and Medical (ISM) band
- ISM bands in US
  - ✓ 900 MHz (902-928 MHz)
  - ✓ 2.4 GHz (2400-2483.5 MHz)
  - ✓ 5.7 GHz (5725-5850 MHz)
- The most widely adopted standard

**IEEE 802.11**

- A family of standards define Phy and MAC
- IEEE 802.11:
  - ✓ Infrared (IR)
  - ✓ 2.4Ghz ISM band with 1 or 2 Mbps
- IEEE 802.11b: 11 Mbps in 2.4 GHz
- IEEE 802.11a: 54 Mbps in 5.7 GHz
- IEEE 802.11g: 54 MHz in 2.4 GHz
- IEEE 802.11i: Security
- IEEE 802.11e: QoS
- IEEE 802.11f: Inter-access point protocol

**Worldwide Interoperability for Microwave Access**

- WiMAX
  - ✓ aimed at providing wireless data over long distances in a variety of ways,
    - o from point-to-point links
    - o full mobile cellular type access.
  - ✓ Based on IEEE 802.16, also called wireless MAN
  - ✓ last mile wireless broadband access as an alternative to cable and DSL

**Wireless PAN**

- IEEE802.15
  - ✓ IEEE 802.15.1 or Bluetooth
    - Moderate data range up to 720 kbps
    - Operates in ISM band
    - 10 m to 100 m range
  - ✓ IEEE 802.15.2
    - Co-existence issues of IEEE 802.11 and 802.15
  - ✓ IEEE 802.15.3 high rate
    - Low power high data rate up to 20 Mbps
    - Designed for multimedia applications over low power devices
  - ✓ IEEE 802.15.4 / ZigBee
    - Low power with range of 100m
    - Low rate about 20 kbps

**Summary**

- Next Lecture
  - ✓ Fundamental principles of Cellular networks

## Lecture 11
## Fundamentals of Cellular Networks (Part I)

**Outlines**

- Review of last lecture
- Cellular Concept
- Frequency Reuse
- Locating co-channel cells
- Example
- Summary of today's lecture

**Review of last lecture**

- Limitation of 3G
- 4G
  - ✓ Objectives
  - ✓ Issues
  - ✓ QoS
  - ✓ Security
  - ✓ Multimedia Service
  - ✓ Applications
- Convergence of Cellular and WLAN
- Billing Issue
- Wireless Networks

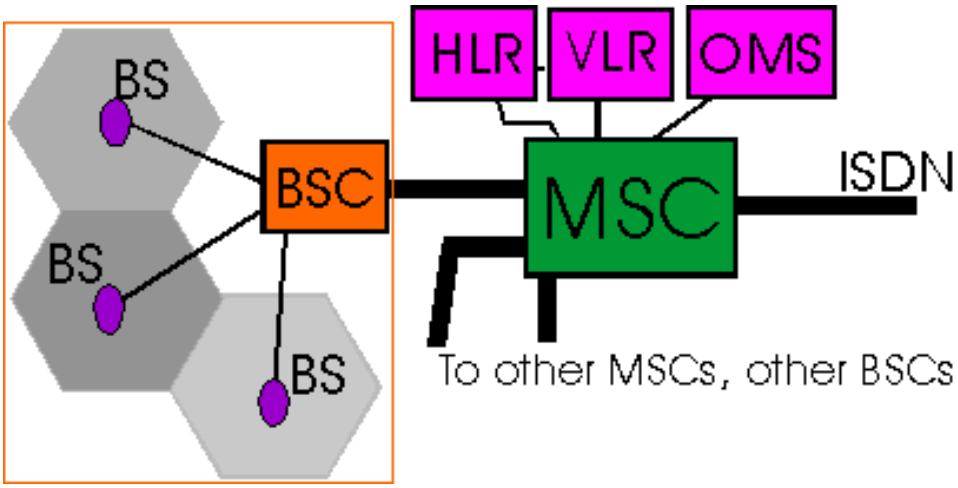
**Introduction**

- Early mobile system objective was to achieve a large coverage using single high power antenna
- Impossible to reuse the same frequencies in the same coverage area.
- For example, Bell mobile system in 1970 could support maximum of 12 simultaneous calls over a thousand square mile.
- The Govt regulatory could not make spectrum allocation proportion to the increasing demand
- Became imperative to restructure the telephone system to achieve high capacity with limited radio spectrum.

**Cellular Concept**

- Cellular concept was a major breakthrough in solving problem of spectrum congestion and user capacity
- Offers high capacity without any major change in technology
  - ✓ Replacing high-power transmitter (large cell) with many low-power transmitter (small cells) each providing service to small
  - ✓ Each BS is allocated a portion of the channels.
  - ✓ Nearby BS are assigned different group of channels
  - ✓ So that all the available channels are distributed among the nearby BS.
  - ✓ May be reused as many times as necessary as long as the BS using same channels are not in overlapping.
- As the demand for service increases, the number of BS can be increased with reduced transmission power.
- Thereby providing additional capacity with no addition to spectrum.
- This is the foundation of  for all modern wireless communication systems.

**AMPS Architecture**




**Frequency Reuse**

- Relies on intelligent allocation and reuse of channels.
- A small geographical area with allocation of a group of channels is called cell.
- BS antennas are designed to achieve the desired coverage within a cell avoiding co-channel interference.
- The design process of selecting and allocating channel groups for all the cellular BS is called frequency reuse or frequency planning.

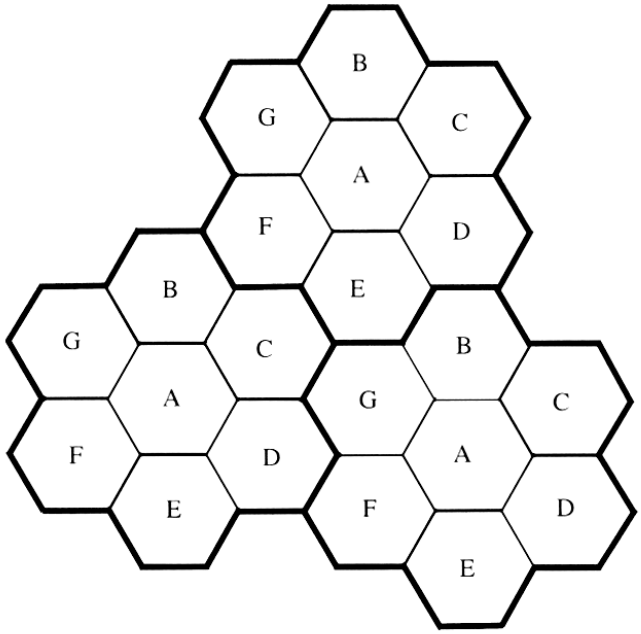
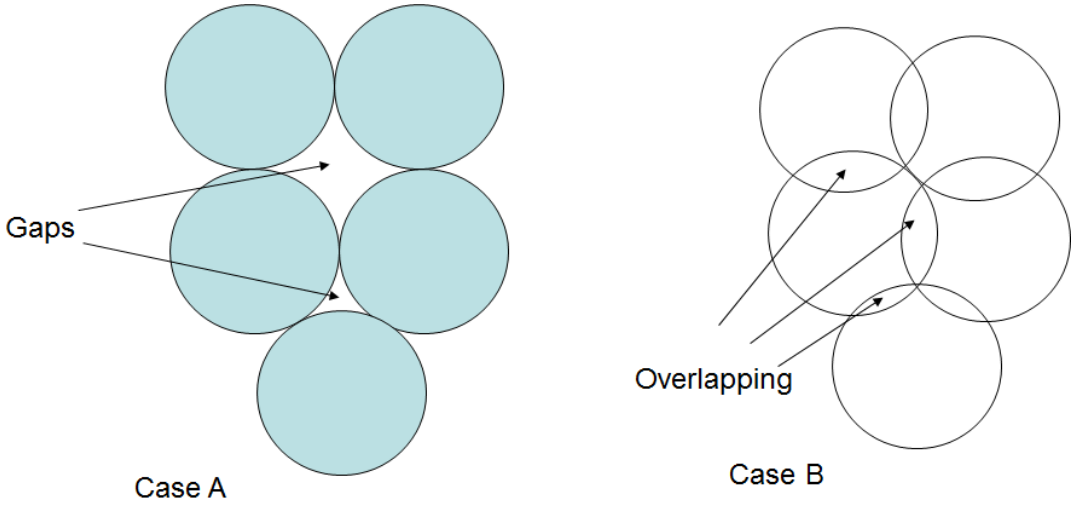
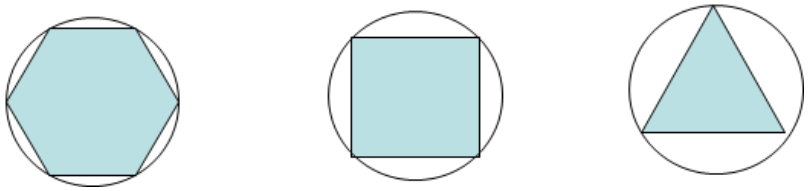



**Figure 3.1** Illustration of the cellular frequency reuse concept. Cells with the same letter use the same set of frequencies. A cell cluster is outlined in bold and replicated over the coverage area. In this example, the cluster size, *N*, is equal to seven, and the frequency reuse factor is 1/7 since each cell contains one-seventh of the total number of available channels.

- The hexagonal shape representing a cell is conceptual and simplistic model of coverage.
- The actual radio coverage is known as the footprint and is determined from field measurement, propagation prediction models
- However a regular shape is needed for systematic system design and adaptation to future growth.
- It might be natural to choose a circle to represent coverage but adjacent circles cannot be overlaid upon a map without leaving gaps or creating overlapping.




- Three possible choices of shapes: square, equilateral triangle and hexagon.
- For a give distance between the center of a polygon and its farthest perimeter points, the hexagon has the largest area of the three



- Thus by using hexagon geometry, the fewest number of cells can cover a geographic region and it closely approximates circle.

**Capacity of System**

- When using hexagon to model coverage areas
  - ✓ Center-excited Cell: BS depicted as being either in the center of the cell
    - Omni-directional antenna is used
  - ✓ Edge-excited Cell: on three of the six cell vertices
    - Sectored direction antenna is used
- Consider a cellular system
  - ✓ which has S duplex channels available for reuse.
  - ✓ Each cell allocated group of k channels (k < S)
  - ✓ S channels divided among N cells (unique and disjoint) then

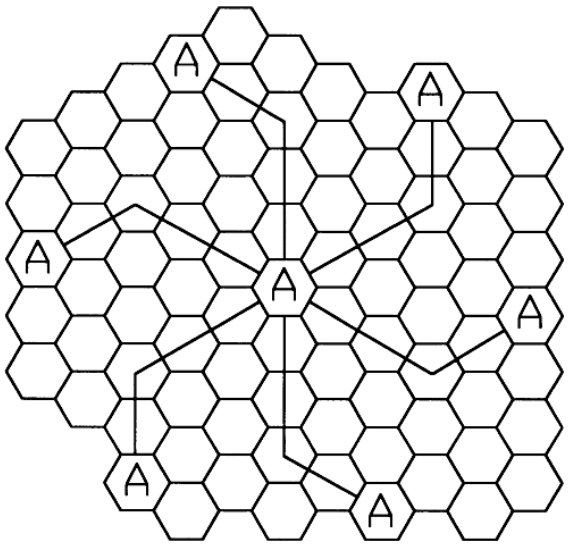
$$S = kN$$

- Cluster: N cells, which collectively use the complete set of available frequencies
- If a cluster is replicated M times in the system, the number of duplex channels C as a measure of capacity is

  $$C = MkN = MS$$
- So capacity is directly proportional to the replication factor in a fixed area.
- Factor N is called cluster size and is typically equal to 4, 7, 12.
- If cluster size N is reduced while cell size is kept constant
  - ✓ More clusters are required
  - ✓ More capacity is achieved
- Large cluster size indicates that co-channel cells are far from each other
- Conversely, small cluster size means co-channel cells are located much closer together
- The value of N is a function of how much interference a mobile or BS can tolerate
  - ✓ Clusters are inversely proportion to N
  - ✓ Capacity is directly proportional to Clusters
- Thus frequency reuse factor is given by 1/N.
- In last fig, each hexagon has exactly six equidistant neighbors and that the lines joining the centers of any cell and its neighbors are separated by multiple of 60 degrees.
  - ✓ There are only certain cluster sizes and layouts possible

**Locating co-channel neighbors**

- To connect hexagons without gaps,
  - ✓ The geometry of hexagon is such that the number of cells per cluster N can only have values $N = i^2 + ij + j^2$
    where i and j are non-negative integers.
- To find out the nearest co-channel neighbors of a particular cell, do the following
  - ✓ Move I cells along any chain of hexagon
  - ✓ Then turn 60 degree counter clockwise and move j cells
- Example




In this example N=19, i=3, j=2

**Example**

- BW = 33 MHz allocated to particular FDD cellular system, where two 25 KHz simplex channel to provide full-duplex for voice/data.
- Compute the number of channels per cell if a system uses
  - ✓ Four-cell reuse
  - ✓ Seven-cell reuse
  - ✓ Twelve-cell reuse.
- If 1 MHz is dedicated to control channels, determine equitable distribution of control and voice channels per cell for above three systems?

**Solution: Part I**

- TotalBW = 33 MHz,
- ChannelBW = 25 KHz x 2 = 50 KHz/duplex channel
- S = 33,000 / 50 = 660 channels
- For N = 4
  - k = 660 / 4 ≈ 165 channels
- For N = 7
  - k = 660 / 7 ≈ 95 channels
- For N = 12
  - k = 660 / 12 ≈ 55 channels

**Solution: Part II**

- Sc = 1000 / 50 = 20 channels
- Sv = S – Sc = 660 – 20 = 640 channels
- For N=4,
- 5 control channels + 160 voice channel.
- For N=7,
  - ✓ 4 cells with 3 control + 92 voice channels
  - ✓ 2 cells with 3 control + 90 voice channels
  - ✓ 1 cell with 2 control + 92 voice channels
  - ✓ In practice, 1 control/cell and 4x91 + 3x92 voice channels
- For N = 12,
  - ✓ 8 cells with 2 control + 53 voice channels
  - ✓ 4 cells with 1 control + 54 voice channels
  - ✓ In practice, 1 control and 8x53 + 4x54 voice channels

**Summary**

- Cellular Concept
- Frequency Reuse
- Locating co-channel cells
- Example
- Next Lecture
  - ✓ Handoff Strategies
  - ✓ Interference and System Capacity

## Lecture 12
## Fundamentals of Cellular Networks (Part II)

**Outlines**

- Channel Assignment Strategies
- Handoff Strategies
  - ✓ When to handoff
  - ✓ 1G, BS based
  - ✓ 2G or today's, Mobile-Assisted
- Prioritizing Handoff
  - ✓ Guard channels concept
  - ✓ Queuing handoff requests
- Practical handoff considerations
  - ✓ Umbrella cell
  - ✓ Cell dragging

**Last lecture**

- Cellular Concept
- Frequency Reuse
- Locating co-channel cells
- Example

**Channel Assignment Strategies**

- For efficient spectrum utilization, frequency reuse scheme should be consistent with objectives
  - ✓ Increasing system capacity
  - ✓ Minimizing interference
- Strategies can be classified as Fixed and Dynamic
- In Fixed Channel Assignment Strategy,
  - ✓ Each cell is allocated a predetermined set of voice channels.
  - ✓ A call attempt can only be served if unused channel in that particular cell is available
  - ✓ If all channels are occupied then the call is blocked
- Several variation exist like borrowing strategy
  - ✓ A cell is allowed to borrow a channel from neighboring cell if all of its channels are occupied
  - ✓ A mobile switching center (MSC) supervises such procedures and ensures that borrowing of channel does not disrupt the or interfere with any of the calls in progress in the donor cell
- Dynamic Channel Assignment Strategy
  - ✓ Voice channels are not allocated to cells permanently
  - ✓ On each call request, the BS requests a channel from MSC.
  - ✓ MSC allocates a channel by taking into account
  - ✓ The likelihood of future blocking within the cell
  - ✓ The frequency of use of the candidate channel, reuse distance
- Hence, MSC only allocates a channel if that is not presently in use in the cell which falls within minimum restricted distance of frequency reuse.
- It reduces the likelihood of the call blocking, increasing the trunking capacity of the system.
- It requires MSC to collect real-time data on channel occupancy, traffic distribution and RSSI of all channels
  - ✓ This increases storage and computational load on the system
  - ✓ But provides increased channel utilization and decreased call blocking

**Handoff Strategies**

- Handoff: a mobile user moves to a different cell while conversation is in progress, MSC transfers the call to a new BS.
  - ✓ Identifying new BS
  - ✓ New voice and control channels to be allocated
- Handoff must be performed
  - ✓ Successfully
  - ✓ Infrequently
  - ✓ Imperceptible
- To achieve this, designer must specify optimum signal level at which handoff initiates
- Once, a signal level is specified as min usable for acceptable voice quality
  - ✓ A slightly stronger signal level is used as threshold
  - ✓ Normally taken between -90dBm and -100 dBm.
- This margin Δ = Pr_handoff – Pr_min, can not be too large or too small
  - ✓ If Δ is too large, unnecessary handoffs, burden on MSC
  - ✓ If Δ is too small, insufficient time to complete a handoff before a call is lost due to weak signal
  - ✓ Δ should be chosen carefully to meet conflicting requirements

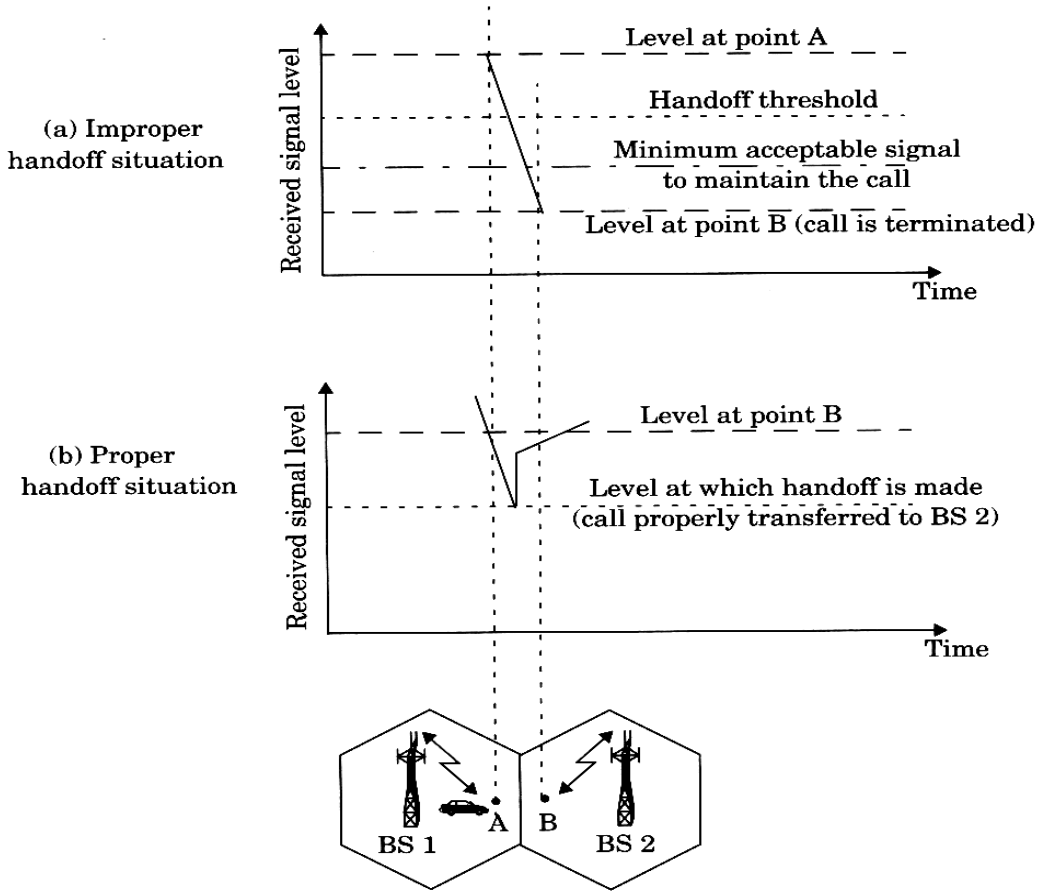



**Figure 3.3** Illustration of a handoff scenario at cell boundary.

- Call drops
  - ✓ Excessive delay by MSC due to high traffic load
  - ✓ $\Delta$ is set too small for handoff time
  - ✓ No channels are available on any of nearby BS
- When to handoff,
  - ✓ Drop in signal level is not due to momentary fading
  - ✓ Mobile is actually moving away from serving BS
  - ✓ To ensure this,
    - BS monitors the signal level for certain period of time
    - The period depends on the vehicle speed
  - ✓ If slope of average received signal level is steep, handoff is made quickly
- In 1G, signal level was measured by BS and supervised by MSC
  - ✓ Each BS constantly monitors the signal strength of all its reverse channels to determine relative location of each mobile user
  - ✓ In addition, the locator receiver (a spare receiver) is used to scan and measure RSSI of mobile users in neighboring cells and reports to MSC
  - ✓ Based on these measurements, MSC decides if handoff is necessary

**Mobile assisted handoff (MAHO)**

- In 2G, handoff decisions are mobile assisted
  - ✓ Each mobile measures RSSI of all surrounding BS
  - ✓ Reports to serving BS
  - ✓ Handoff is initiated if power of serving BS is lesser than nearby BS by a certain level or for a certain period of time
  - ✓ Enables calls to be handed over between Base Stations at much faster rate than in 1G
  - ✓ MSC no longer constantly monitors RSSI.
  - ✓ More suitable for microcellular where HO is frequent
- intersystem handoff
  - ✓ If a mobile moves from one cellular system to a different system controlled by a different MSC
  - ✓ Issues to be addressed
    - A local call becomes a long-distance call (roaming)
    - Compatibility between two MSC must be determined
    - Different systems have different policies and methods for managing handoff requests
- Prioritizing handoff
  - ✓ Call termination in middle of conversation is more annoying than being blocked on a new call attempt

**Prioritizing Handoffs**

- Two methods of handoff prioritizing
  - ✓ Guard channel concept
    - A fraction of available channels is reserved exclusively for handoff

requests
- Has disadvantage of reducing total carried traffic
- Offers efficient spectrum utilization when dynamic channel assignment strategies by minimizing number of required guard channels

✓ Queuing of handoff requests
- Possible due to time interval elapsed when the signal level drops below to threshold until minimum signal level
- Decrease probability of forced termination due to lack of available channels
- Tradeoff between decrease in probability of forced termination and total traffic
- The delay time and queue size is determined from traffic pattern
- Queuing does not guarantee zero probability of call termination since large delays will signal level to drop min

**Practical handoffs consideration**

- Several problems arise to design a system for wide range of mobile velocities
  - ✓ High speed vehicles pass through a cell in a matter of seconds
    - With micro cells addition, the MSC can quickly become burdened
  - ✓ Pedestrian users may never need a handoff during a call
  - ✓ Issues
    - Schemes to handle high speed and low speed users simultaneously
    - Ability to obtain new cell sites
- Additional capacity is provided through addition of new cell sites,
- Difficult to obtain new cell sites
- Install additional channels and BS at same location of an existing cell
- By using different antenna heights and power levels, possible to provide large and small cells, which are co-located at single location called umbrella cell
  - ✓ Provide large coverage area to high speed users minimizing number of handoffs
  - ✓ Small coverage to slow speed users
  - ✓ Speed can be estimated by BS or MSC by RSSI

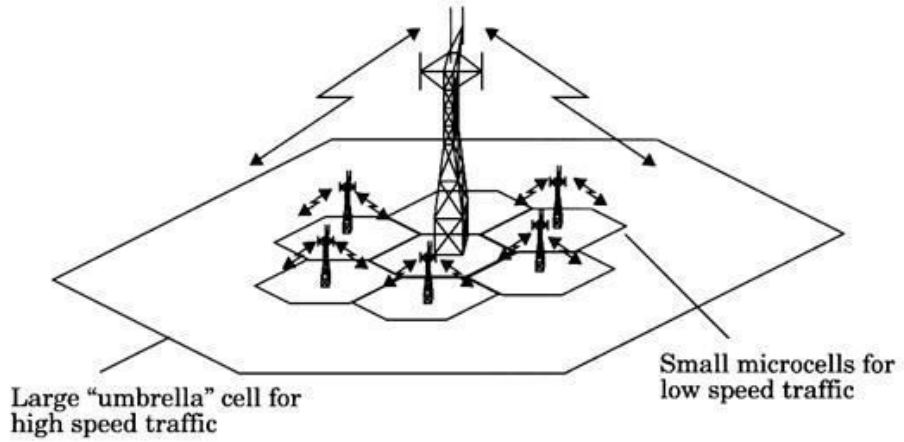



**Figure 3.4** The umbrella cell approach.

- Cell dragging
  - ✓ Problem in micro-cell due to high signal strength of pedestrian users.
  - ✓ Occurs in urban areas when there is a LOS path
  - ✓ Average signal strength does not decay rapidly even if a user travels well beyond the range of cell
  - ✓ The RSSI may be above the handoff threshold and thus handoff is not made
  - ✓ This creates potential interference since a user has traveled deep within a neighboring cell
  - ✓ Handoff parameters, threshold must be adjusted carefully
- In 1G,
  - ✓ Time to make handoff when signal drops below threshold is 10s.
  - ✓ This requires that the value of $\Delta$ be on the order of 6 dB to 12 dB.
- In 2G
  - ✓ Such as GSM, MAHO determines the best handoff candidates and requires only 1 or 2 seconds.
  - ✓ $\Delta$ is usually between 0 dB and 6 dB.
  - ✓ Provides MSC substantial time to rescue a call that is in need of handoff
- In IS-95 (CDMA) system
  - ✓ Provides unique handoff capability that can not be provided in with other wireless systems
  - ✓ Unlike channelized (hard handoff), SS mobiles share the same channel in every cell.
  - ✓ Thus handoff does not assign channel but a different BS handles a communication task
  - ✓ By simultaneously evaluating RSSI from single user, MSC decides which version of the signal is best
  - ✓ This ability selects between instantaneous received signals from a variety of BS is called soft handoff
- In IS-95 (CDMA) system
  - ✓ Provides unique handoff capability that cannot be provided in with other wireless systems
  - ✓ Unlike channelized (hard handoff), SS mobiles share the same channel in every cell.
  - ✓ Thus handoff does not assign channel but a different BS handles a communication task
  - ✓ By simultaneously evaluating RSSI from single user, MSC decides which version of the signal is best
  - ✓ This ability selects between instantaneous received signals from a variety of BS is called soft handoff

**Summary**

- Channel Assignment Strategies
- Handoff Strategies
- Prioritizing Handoff
- Practical handoff considerations

## Lecture 13
## Fundamentals of Cellular Networks (Part III)

**Outlines**

- Last lecture review
- Interference and system capacity
  - ✓ Co-channel interference and capacity
  - ✓ Adjacent channel interference and capacity
- Channel Planning for Wireless System

**Last lecture review**

- Channel Assignment Strategies
- Handoff Strategies
  - ✓ When to handoff
  - ✓ 1G, BS based
  - ✓ 2G or today's, Mobile-Assisted
- Prioritizing Handoff
  - ✓ Guard channels concept
  - ✓ Queuing handoff requests
- Practical handoff considerations
  - ✓ Umbrella cell
  - ✓ Cell dragging

**Interference and system capacity**

- Sources of interference
  - ✓ Another mobile in the same cell
  - ✓ Call in progress in a neighboring cell
  - ✓ Other BS operating in same frequency
  - ✓ Another non-cellular system leaks energy into cellular frequency band
- Interference on voice channels causes cross-talk
- On control channels, interference leads to missed and blocked calls
- A major bottleneck in increasing capacity
- Two major types
  - ✓ Co-channel and adjacent channel interference

**Co-channel interference and system capacity**

- Co-channel cells: cells that use the same set of frequencies and interference is called co-channel interference
- By increasing SNR, co-channel can not be combated
- To reduce it, co-channel cells must be separated by a min distance
- When size of each cell is approximately same and BS transmit at same power, co-channel interference ratio is independent of transmission power and is a function of radius of cell (R) and distance between centers of nearest co-channel cell (D)
- By increasing the ratio of D/R,
  - ✓ Separation between co-channel cells relative to coverage distance of a cell is increased.
  - ✓ Thus interference is reduced.
- The parameter Q (co-channel reuse ratio) is related to cluster size. Thus for a hexagonal geometry

$$(1) \qquad Q = \frac{D}{R} = \sqrt{3N}$$

- ✓ A small value of Q provides larger capacity since N is cluster size
- ✓ Large value of Q improves transmission quality due to smaller level of co-channel interference
- ✓ A trade-off must be made between these two objectives

- Let $i_0$ be the number of co-channel interfering cells, then the signal-to-interference ratio for a mobile receiver which monitors a forward channel is

$$(2) \qquad \frac{S}{I} = \frac{S}{\sum_{i=1}^{i_o}(I_i)}$$

- ✓ where S is the desired signal power from desired BS and $I_i$ is the interference power caused by $i_{th}$ interfering co-channel cell

- Average received signal strength at any point decays as a power law of the distance of separation between transmitter and receiver
- Average received power $P_r$ at a distance d from the transmitting antenna is approx

$$(3) \qquad P_r = P_o\left(\frac{d}{d_o}\right)^{-n}$$

- ✓ Where Po is the power received at a close-in reference point at a small distance $d_o$ from the transmitting antenna, n is path loss exponent ranging between 2 and 4

- Now consider co-channel cell interference
- If $D_i$ is the distance of $i^{th}$ interferer from the mobile, the received power will be proportional to $(D_i)^{-n}$
- When the transmit power of each BS is equal and the path loss exponent is same throughout coverage then S/I can be approximated as

$$(4) \qquad \frac{S}{I} = \frac{R^{-n}}{\sum_{i=1}^{i_o}(D_i)^{-n}}$$

- Considering only the first layer of interfering cells, which are equidistant D from the desired BS
- Eqn 4 implies to

$$(5) \qquad \frac{S}{I} = \frac{R^{-n}}{i_o D^{-n}} = \frac{(D/R)^n}{i_o} = \frac{(\sqrt{3N})^n}{i_o}$$

- ✓ It relates S/I to cluster size N, which in turn determines the overall capacity of the system

- For US AMPS system, tests indicate that for sufficient voice quality S/I should be greater or equal to 18 dB.
- By using Eqn 5, in order to meet this requirement, N should be at least 6.49 assuming n=4.
- Thus a minimum cluster size of 7 is required to meet S/I requirement of 18 dB
- It should be noted Eqn 5 is based on hexagonal cell geometry

- For 7-cell cluster, hexagonal cell geometry layout
- Mobile is at the boundary of the cell

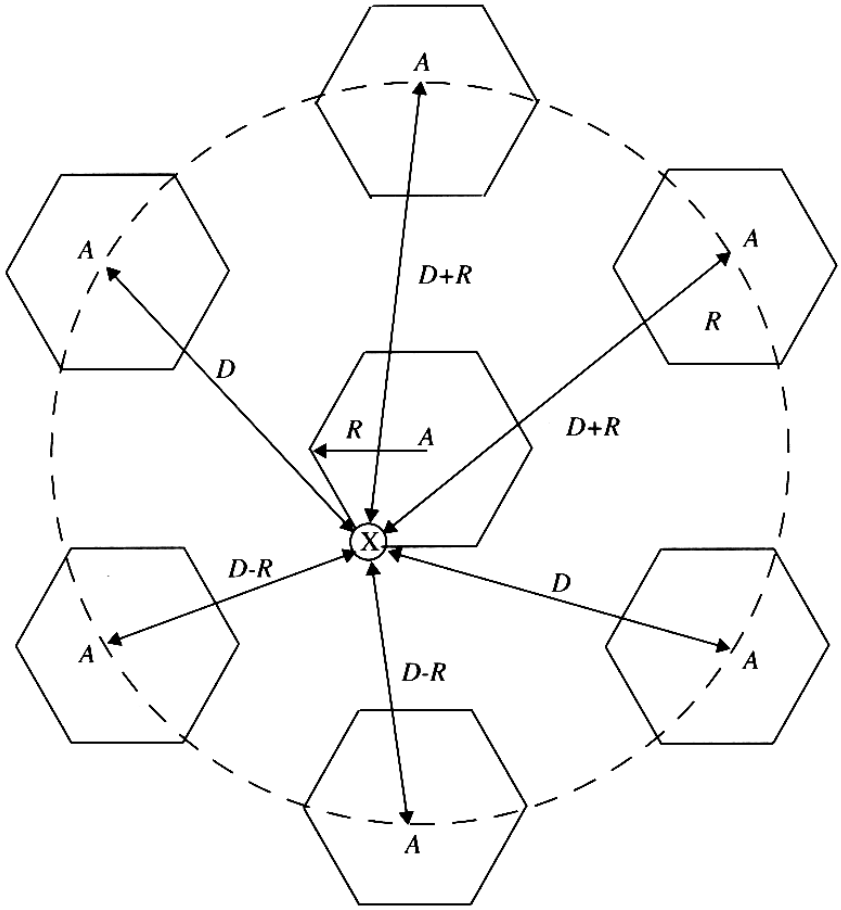



**Figure 3.5** Illustration of the first tier of co-channel cells for a cluster size of $N = 7$. An approximation of the exact geometry is shown here, whereas the exact geometry is given in [Lee86]. When the mobile is at the cell boundary (point $X$), it experiences worst case co-channel interference on the forward channel. The marked distances between the mobile and different co-channel cells are based on approximations made for easy analysis.

- The worst case S/I ratio can be approximated using Eqn 4

$$\frac{S}{I} = \frac{R^{-4}}{2(D-R)^{-4} + 2(D+R)^{-4} + 2D^{-4}} \quad (6)$$

- The above Eqn can be rewritten in terms of co-channel reuse ratio Q as

$$\frac{S}{I} = \frac{1}{2(Q-1)^{-4} + 2(Q+1)^{-4} + 2Q^{-4}} \quad (7)$$

- For N=7, the value of Q is 4.6
- The worst case S/I is approximated as 49.56 (17 dB) using Eqn 7, where exact solution using Eqn 4 is 17.8 dB.

**Example**

- If S/I is required 15 dB for satisfactory forward channel performance, what is the frequency reuse factor and cluster size that should be used for maximum capacity if path loss exponent n = 4 and n = 3? Assuming 6 co-channel cells in first tier at same distance from desired BS
  - ✓ n = 4, lets consider 7-cell reuse
    - Using Eqn. 1, reuse ratio is 4.583
    - Using 5, S/I = 1/6 x (4.583)^4 = 75.3 = 18.66 dB
    - Since this is greater than min required, N=7 can be used
  - ✓ n = 3, first consider 7-cell reuse
    - S/I = 1/6 x (4.583)^3 = 16.04 = 12.05 dB
    - Since this is less than min required,
    - Next possible value of N is 12-cell reuse (i = j = 2)
    - Using Eqn. 1, reuse ratio is 6.0
    - S/I = 1/6 x (6)^3 = 36 = 15.56 dB
    - Since this is greater than min required S/I, So N=12 is used

**Channel Planning for Wireless Systems**

- Generally available spectrum is divided into channels used throughout a country or continent
  - ✓ Control channels
    - 5% of total devoted for initiating, requesting or paging a call, data messages
  - ✓ Voice channels
    - 95% dedicated for revenue generating traffic
  - ✓ Channels may be assigned by wireless carrier in any manner depending on particular propagation conditions or services it wishes to offer
  - ✓ However, control channels are not allowed to be used as voice channels or vice versa
  - ✓ Control channels are vital for any successful launch of call, the frequency reuse strategy or S/I is more conservative than voice channels
  - ✓ While voice channels are assigned only 7-cell reuse, control channels are allocated using 21-cell reuse
- Key feature of CDMA systems is that cluster size N = 1, frequency reuse planning is not as difficult as for TDMA or 1G systems
- However, most practical CDMA use some sort of limited frequency reuse due to ill-behaved propagation conditions
- For example interfering channels on same channel can create interference overload that exceeds the dynamic range of CDMA power control capabilities, leading to dropped calls
- Most popular approach is to use f1/f2 cell planning, where nearest neighbor cells use channels that are different from its closest neighbor
- This would require mobiles to make hard handoff
- In CDMA a single 1.25 MHz channel carries 64 simultaneous voice channels
- CDMA system has dynamic time varying coverage region depending on instantaneous

number of users, known as breathing cell

- The wireless engineer has to carefully plan the coverage and signal levels for best and worst cases of serving cell as well as neighboring cell from both coverage and interference view.
- Breathing cell can lead to abrupt dropped calls
- Hence, the engineer must make difficult decision of power levels and thresholds

**Adjacent channel interference**

- Interference resulting from signals which are adjacent in frequency
- It results from imperfect receiver filters which allow nearby frequencies to leak into passband
- It is more serious if the transmitter is more close to the user's receiver listening to desired channel
- This is near-far effect
  - ✓ A nearby transmitter captures the receiver of subscriber.
  - ✓ Or mobile close to BS transmits on adjacent channel to one being used by a weak mobile
- Adjacent channel interference can be minimized by careful filtering and channel assignment
- A cell need not be assigned channels adjacent in frequency
- By keeping frequency separation in a given cell between channels as large as possible, interference can considerably minimized
- By sequentially assigning successive channels to different cells, channel allocation schemes are able to separate channels in a cell as many as N
- Some assigning strategies also avoid use of adjacent channels in neighboring cell sites.
- If reuse factor (1/N) is large i.e. N is small, the separation may not be sufficient to keep intf within tolerable limits.
- For example if a close-in mobile is 20 times as close to BS as another mobile and energy has leaked to passband, S/I at BS for weak mobile is approx
- $S/I = (20)^{-n}$
- For n-4, this is -52 dB
- If filter of BS receiver has a slope of 20 dB/octave then intf must be displaced 6 times the passband bandwidth from the center to achieve 52 dB attenuation
- This implies more than 6 channels separation are needed for an acceptable S/I level

## Lecture 14
## Fundamentals of Cellular Networks (Part IV)

**Outlines**

- Trunking and Grade of Service
  - ✓ Measuring Traffic Intensity
  - ✓ Trunked Systems
    - Blocked Calls Cleared
    - Blocked Calls Delayed
  - ✓ Erlang Charts
- Improving Coverage and Capacity
  - ✓ Cell Splitting
  - ✓ Sectoring
  - ✓ Repeaters for Range Extension
  - ✓ Microcell Zone Concept

**Last lecture review**

- Interference and system capacity
  - ✓ Co-channel interference and capacity
  - ✓ Adjacent channel interference and capacity
- Channel Planning for Wireless System

**Trunking**

- Allows a large number of users to share a small number of channels
- Channel allocated per call basis from a pool of available channels
- Relies on statistical behavior of users so that a fixed number of channels (circuits) may accommodate a large random user community
- Trunking theory is used to determine number of channels for particular area (users)
- Tradeoff between the number of available channels and likelihood of call blocking during peak calling hours

**Trunking Theory**

- Developed by Erlang, Danish Mathematician, how a large population can be accommodated by a limited number of servers, in late $19^{th}$ century
- Today, used to measure traffic intensity
- 1 Erlang represents the amount of traffic intensity carried by a completely occupied channel
  - ✓ i.e. one call-hour per hour or one call-minute per minute
  - ✓ 0.5 Erlang: Radio channel occupied 30 minutes during 1 hour

**Grade of Service**

- GOS is a benchmark used to define performance of a particular trunked system
  - ✓ Measure of the ability of a user to access trunked system during the busiest hour.
    - Busy hour is based on the demands in an hour during a week, month or year.
    - Typically occur during rush hours between 4 pm to 6 pm.
- GOS is typically given as likelihood of call blocking or delay experienced greater than certain queue time

**Traffic intensity**

- Traffic intensity is measured as call request rate multiplied by call holding time

  User traffic intensity of $A_u$ Erlang is

  (1) $A_u = \lambda H$

  Where H is average call duration or holding time and λ is average number of call requests.

  For system of U users and unspecified channels, the total offered traffic intensity A is

  (2) $A = UA_u$

  In a C channel trunked system, traffic equally distributed, traffic intensity per channel Ac

  (3) $A_c = UA_u/C$
- Note that traffic is not necessarily the carried traffic but offered to the trunked system
- If offered load increases the system capacity, the carried traffic becomes limited
- In Erlang, max possible carried traffic is the number of channels C
- AMPS is designed for a GOS of 2% blocking
  - ✓ i.e. 2 out of 100 calls will be blocked due to channel occupancy
- There are two types of commonly used trunked systems
  - ✓ Blocked Calls Cleared
  - ✓ Blocked Calls Delayed

**Block Calls Cleared**

- User is given immediate request if a channel is available.
- If no channel available, the requesting user is blocked and free to try later
- Assume call arrivals as Poisson Distribution
- the Erlang B formula determines the probability that call is blocked with no queuing, is a measure of GOS for trunked system

$$(4) \qquad Pr[blocking] = \frac{\frac{A^C}{C!}}{\sum_{k=0}^{C} \frac{A^k}{k!}} = GOS$$

**Erlang B Trunking GOS**

Capacity of an Erlang B System

| Number of Channels C | Capacity (Erlangs) For GOS | | | |
|---|---|---|---|---|
| | = 0.01 | = 0.005 | = 0.002 | = 0.001 |
| 2 | 0.153 | 0.105 | 0.065 | 0.046 |
| 4 | 0.869 | 0.701 | 0.535 | 0.439 |
| 5 | 1.36 | 1.13 | 0.900 | 0.762 |
| 10 | 4.46 | 3.96 | 3.43 | 3.09 |
| 20 | 12.0 | 11.1 | 10.1 | 9.41 |
| 24 | 15.3 | 14.2 | 13.0 | 12.2 |
| 40 | 29.0 | 27.3 | 25.7 | 24.5 |
| 70 | 56.1 | 53.7 | 51.0 | 49.2 |
| 100 | 84.1 | 80.9 | 77.4 | 75.2 |

## Erlang B

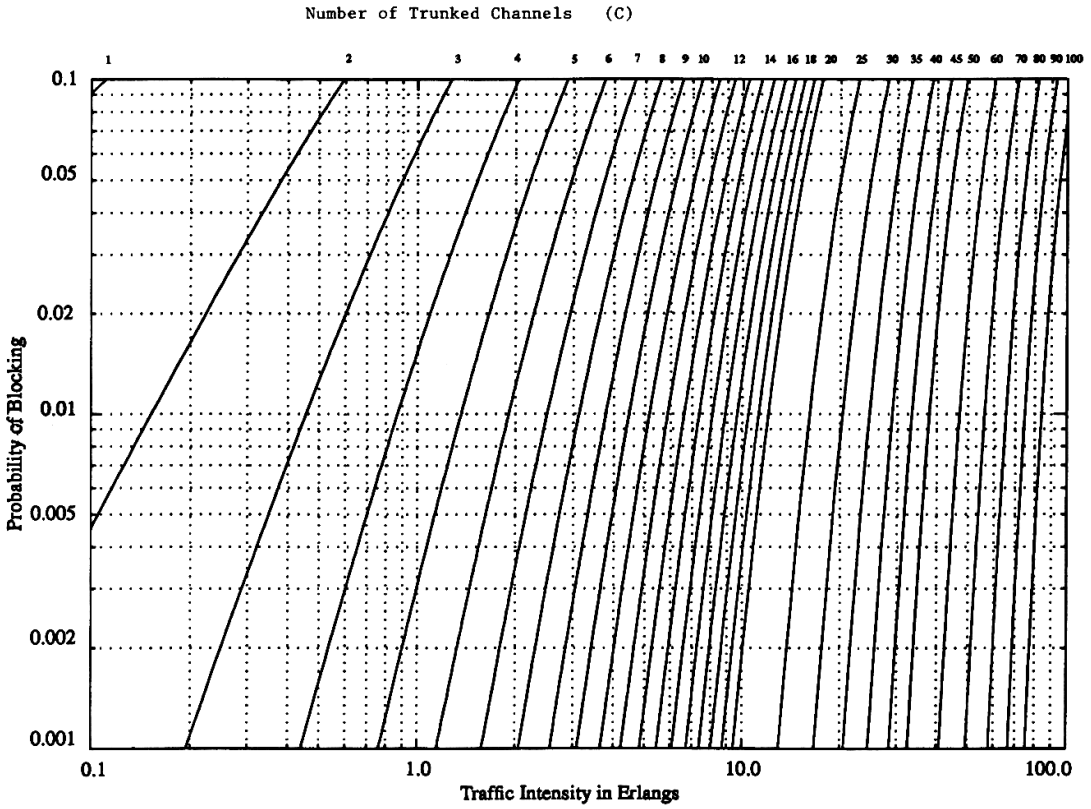



**Figure 3.6** The Erlang B chart showing the probability of blocking as functions of the number of channels and traffic intensity in Erlangs.

## Block Calls Delayed

- Queue is provided to hold blocked calls.
- Call request may be delayed until a channel becomes available
- Its measure of GOS is defined as the probability that a call is blocked after waiting specific length of time in the queue
- The likelihood of a call not having immediate access is determined by Erlang C formula

$$(5)\quad Pr[delay > 0] = \frac{A^C}{A^C + C!\left(1 - \frac{A}{C}\right)\sum_{k=0}^{C-1}\frac{A^k}{k!}}$$

## Erlang C

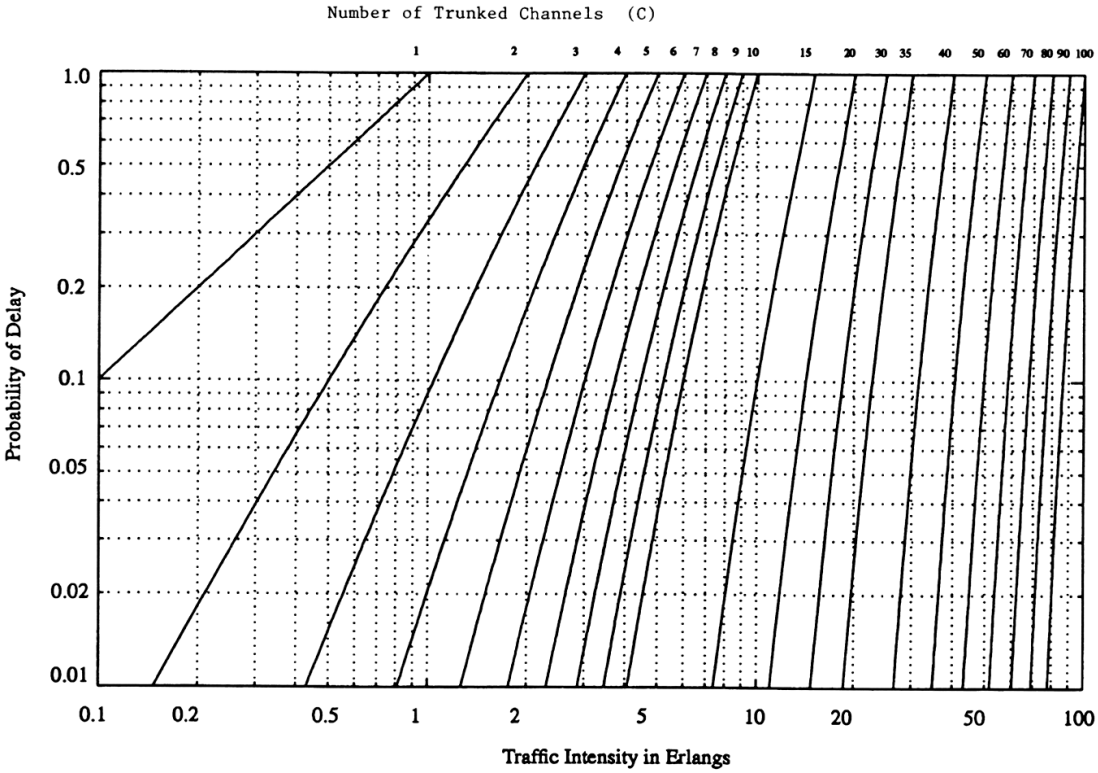



**Figure 3.7** The Erlang C chart showing the probability of a call being delayed as a function of the number of channels and traffic intensity in Erlangs.

- if no channels are available immediately, the call is delayed, probability that call is forced to wait more than **t** seconds is

$$\begin{aligned} Pr[delay > t] &= Pr[delay > 0]Pr[delay > t|delay > 0 \\ (6) \qquad &= Pr[delay > 0]exp(-(C-A)t/H) \end{aligned}$$

- Average delay D in all calls in queued system is

$$(7) \qquad D = Pr[delay > 0]\frac{H}{C-A}$$

Where the average delay of queued cell is given by H / (C – A)

## Trunking Efficiency

- A measure of the number of users which can be offered a particular GOS with particular configuration of channels
- The way channels are grouped can alter the number of users handled
- For example, From table
  - ✓ 10 trunked channels at GOS of 0.01 can support 4.46 Erlang of traffic
  - ✓ Whereas 2 groups of 5 channels can support 2x1.36=2.72 Erlangs of traffic, 60% lesser

**Improving Coverage and Capacity**

- As demand increases, number of channels per cell become insufficient
- Cellular design techniques needed to provide more channels per unit coverage area
- Various techniques developed to expand the capacity of system
  - ✓ Cell splitting
  - ✓ Sectoring
  - ✓ Micro cell zone concept

**Cell Splitting**

- Achieve capacity improvement by decreasing R and keeping D/R (cell reuse ratio) unchanged
- Divide the congested cells into smaller cells
  - ✓ Smaller cells are called micro cells
- If radius of cell is cut to half, approximately four cells would be required
  - ✓ Increased number of cells would increase the number of clusters, which in turn increase the capacity
- Allows a system to grow by replacing larger cells with smaller cells without upsetting the allocation scheme

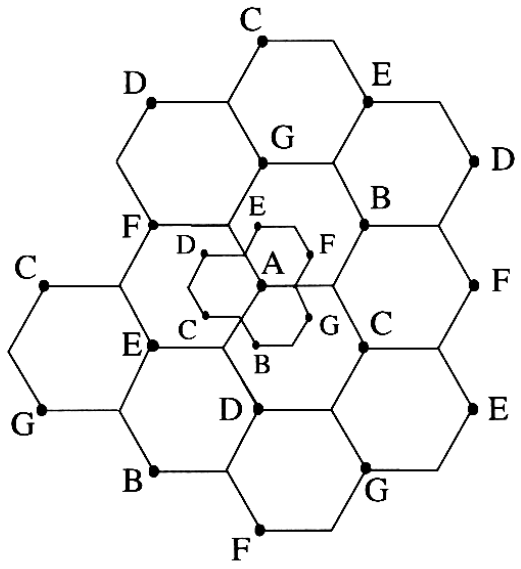



**Figure 3.8** Illustration of cell splitting.

- For new cells to be smaller in size, tx power must be reduced. By which factor?

$$P_r[at\ old\ cell\ boundary] \propto P_{t1}R^{-n} \quad (9)$$

$$P_r[at\ new\ cell\ boundary] \propto P_{t2}(R/2)^{-n} \quad (10)$$

- If n = 4 then the received powers equal to each other becomes

$$P_{t2} = \frac{P_{t1}}{16} \quad (11)$$

- Power must be reduced by 12 dB in order to maintain S/I requirements
- Thus low speed and high speed users can simultaneously handled
- Channels in old cell must be broken down into two groups corresponding to smaller and larger cells
- At beginning of cell splitting, fewer channels to smaller power groups.
- As demand grows, more channels will be required and thus more micro cells
- In the end, the whole system will be replaced with micro cells

**Sectoring**

- Keep cell radius unchanged and decrease D/R
- Increases SIR so that cluster size may be reduced
  - ✓ SIR is improved using directional antennas
  - ✓ Hence increasing frequency reuse without changing transmission power
- Cell is partitioned into 3 120o sectors or 6 60o sectors as shown in Fig

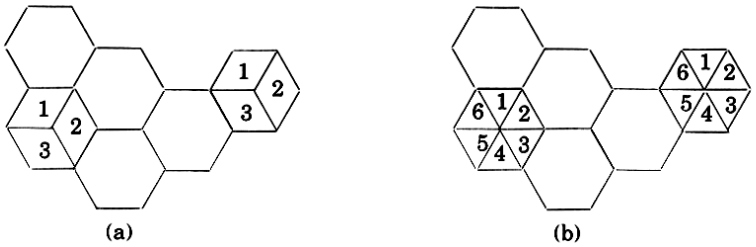



**Figure 3.10** (a) 120° sectoring; (b) 60° sectoring.

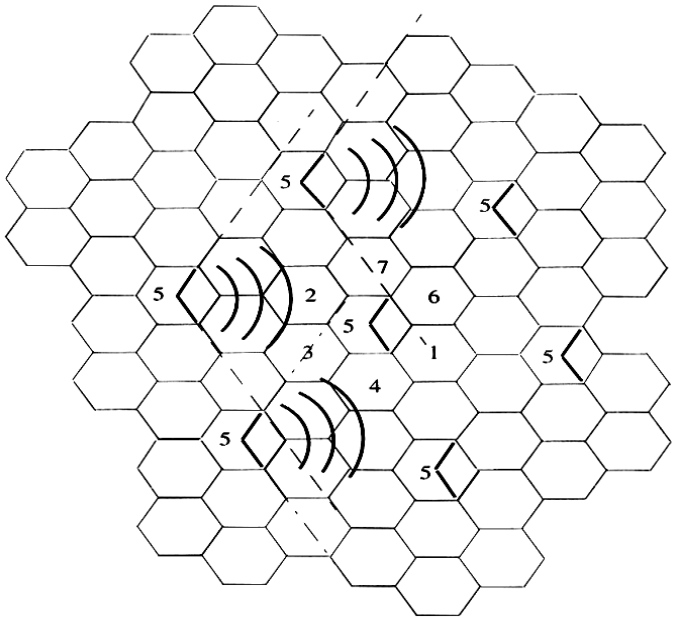



**Figure 3.11** Illustration of how 120° sectoring reduces interference from co-channel cells. Out of the 6 co-channel cells in the first tier, only two of them interfere with the center cell. If omnidirectional antennas were used at each base station, all six co-channel cells would interfere with the center cell.

- Instead of interference from 6 cells, only 2 sectors interfere
- thus S/I can be found to be 24.2 dB, where it is 17 dB in worst case presented before
- This S/I improvements allow designers to decrease cluster size N and hence enhances capacity
- Drawbacks
  - ✓ Increased number of handoffs

**Microcell Zone Concept**

- A cell is divided into zones with a single BS sharing the same radio equipment
- Zones are connected through coaxial cable, fiber optics or microwave links to the BS
- Superior to sectoring since antennas are placed at outer edges of the cells and any channel may be assigned to any zone by BS
- As mobile travels from one zone to other, it retains same channel, BS simply switches the channel to a different zone.
- Co-channel interference is minimized becuase
  - ✓ Large BS is replaced by several low powered tx
  - ✓ Improves S/I

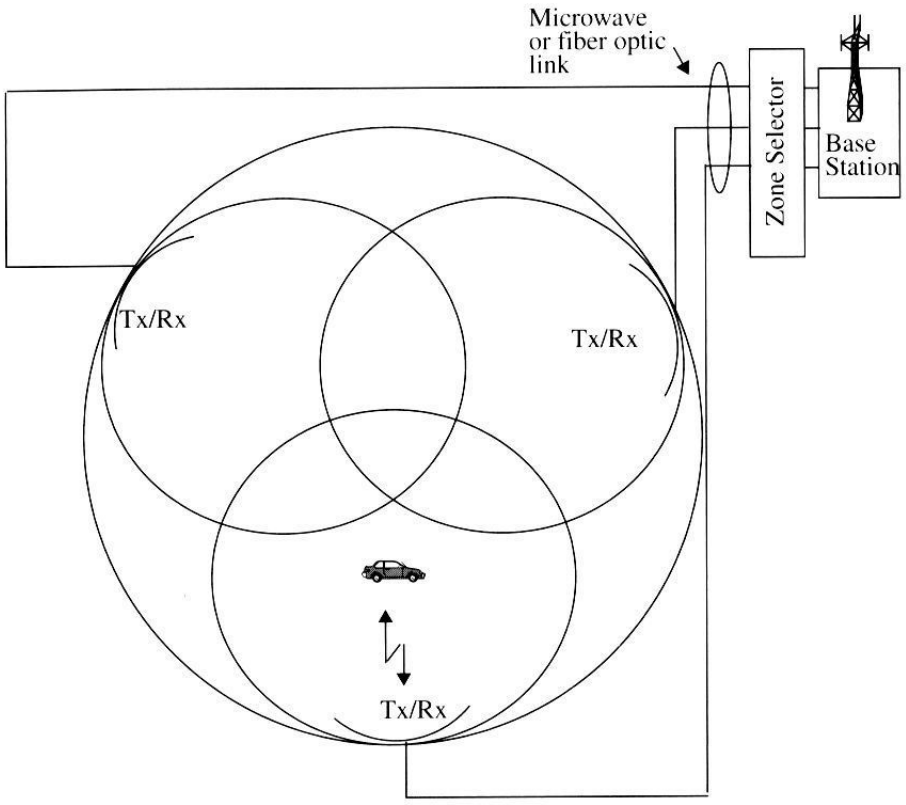



**Figure 3.13** The microcell concept [adapted from [Lee91b] © IEEE].

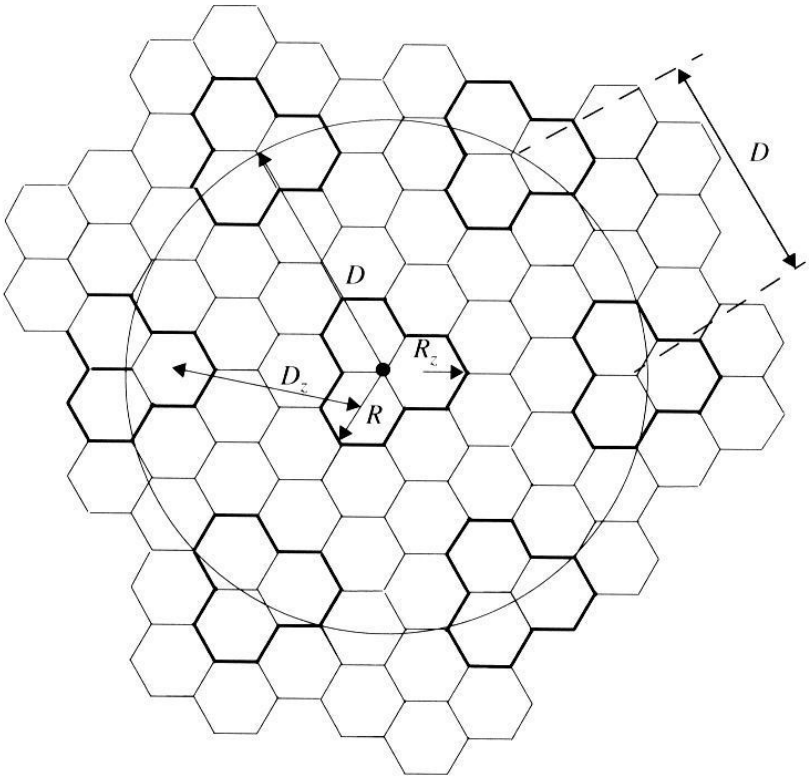



**Figure 3.14** Define $D$, $D_z$, $R$, and $R_z$ for a microcell architecture with $N = 7$. The smaller hexagons form zones and three hexagons (outlined in bold) together form a cell. Six nearest co-channel cells are shown.

# Lecture 15
# Analog Mobile Phone System

**Outlines**

- AMPS introduction
- System Overview
- Call handling
- Air interface
- Supervisory signals
- N-AMPS

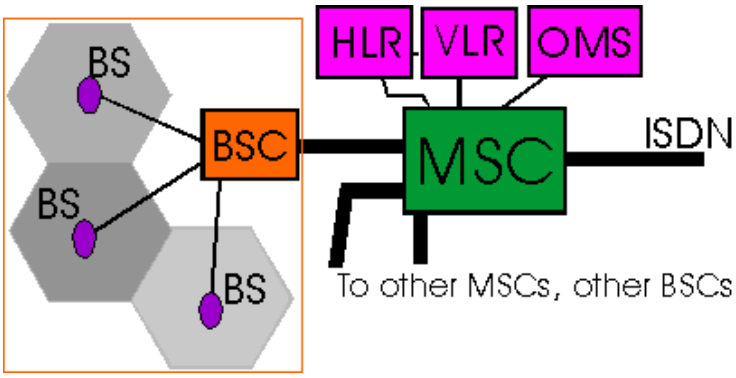
**Last Lecture review**

- Trunking and Grade of Service
  - ✓ Measuring Traffic Intensity
  - ✓ Trunked Systems
    - Blocked Calls Cleared
    - Blocked Calls Delayed
  - ✓ Erlang Charts
- Improving Coverage and Capacity
  - ✓ Cell Splitting
  - ✓ Sectoring
  - ✓ Repeaters for Range Extension
  - ✓ Microcell Zone Concept

**AMPS Introduction**

- First deployed in late 1983 in urban and suburban areas of Chicago.
- Total of 40 MHz in 800 MHz band allocated by FCC
- Later on, Additional 10 MHz allocated as user demand increased
- First AMPS systems used large cells and omni directional antennas to minimize initial equipment cost
- It covered approximately 2100 square miles
- AMPS system uses 7-cell reuse pattern with provision of sectoring and cell splitting to increase system capacity.
- After extensive tests, it was found that 30 KHz channel requires s SIR of 18 dB.
- The smallest reuse factor which satisfies this requirement using 120 degree directional antenna is N = 7
- ETACS: European Total Access Communication System
  - ✓ Identical to AMPS except scaled to 25 KHz as opposed to 30 KHz
  - ✓ Different format of mobile identification number (MIN) due to need of accommodating different country codes in Europe as opposed to area code in US

**AMPS Architecture**




**System Overview**

- AMPS and ETACS both use FM and FDD for radio transmission like other 1G systems
- In US,
  - ✓ Transmissions from mobiles to BS (reverse link) use frequencies between 824-849 MHz
  - ✓ While BS transmits to mobiles (forward link) using frequencies between 869-894 MHz
  - ✓ A separation of 45 MHz between forward and reverse channels is due to use of inexpensive and highly selective duplexers in mobile units.
- The control channel and blank-and-burst data streams are transmitted at 10kbps in AMPS and 8kbps in ETACS
- These wideband streams have max frequency deviation of ± 8KHz and ±6.4 KHz for AMPS and ETACS
- Each BS has
  - ✓ One control channel transmitter that transmits on forward control channel (FCC)
  - ✓ One control channel receiver that listen to reverse control channel (RCC) to set-up a call
  - ✓ 8 or more duplex voice channels
  - ✓ Commercial BS supports as many as 57 voice channels
- Forward Voice Channel (FVC) carry the conversation originating from landline caller to cellular subscriber
- Reverse Control Channel (RVC) in opposite
- The actual number of control and voice channels varies widely depending on the traffic, maturity of the system and location of other BSs.
- The number of BS in a service area varies widely as well from few towers in rural area to several hundred or more BS in a large city.
- Each BS continuously transmits digital FSK data on FCC at all times so that idle subscriber units can lock onto the strongest FCC.
- All users must be locked onto a FCC in order to originate or receive calls.
- The BS RCC receiver constantly monitors transmission from subscribers that are locked onto the matching FCC

- In US AMPS, there are 21 control channels and ETACS supports 42 control channels per provider
- Thus any cellular phone needs to scan limited number of control channels to find best serving BS
- It is upto the service providers to make sure adjacent FCC are not assigned to nearby BSs
- The nonwireline service provider ("A" provider) is assigned odd system identification number (SID) and wireline service provider ("B" provider) is assigned even SID.
- SID is transmitted once every 0.8 seconds on each FCC, along with other overhead data which reports the status of cellular system
- In ETACS area identification numbers (AID) are used instead of SID.

**Call handling**

- Call: landline user → cellular subscriber
  - ✓ From PSTN arrives at MSC.
  - ✓ A paging request is sent out with subscriber MIN simultaneously on every BS FCC.
  - ✓ If intended subscriber receives its page on FCC, it responds with ACK on RCC.
  - ✓ The MSC directs the BS to assign FVC and RVC pair to take place call
  - ✓ The BS also assigns supervisory audio tone (SAT) and a voice mobile attenuation code (VMAC) as it moves the call to the voice channels
- SAT
  - ✓ It allows user and BS to distinguish each other from co-channel users located in different cells
  - ✓ Transmitted continuously on the both FVC and RVC at three different frequencies 5070 Hz, 6000 Hz, 6030 Hz
- VMAC
  - ✓ Instructs the user to transmit at a specific power level
- Once on the voice channel, wideband FSK data is used by BS and subscriber in a blank-and-burst mode to initiate handoffs, change transmitter power as needed and provide other system data
- Blank-and-burst signaling allows the MSC to send bursty data on voice channels by temporarily omitting speech and SAT and replacing with data.
- Call: mobile user → landline user
  - ✓ Subscriber transmits request (MIN, electronic serial number, station class mark and destination number on RCC
  - ✓ If received correctly by BS, sent to MSC
  - ✓ MSC check if user is properly registered, connects to the PSTN
  - ✓ Assigns FVC and RVC with SAT and VMAC
- During a call, MSC issues numerous blank-and-burst commands which switch
  - ✓ Between different voice channels on different BS depending on where the user is traveling
- The MSC uses scanning receiver called locator in nearby BS to determine RSSI for handoff

- When a new call request arrives from PSTN or subscriber
  - ✓ Voice channels may be occupied
  - ✓ MSN holds line open while instructing current BS to issue directed retry to subscriber on FCC
  - ✓ It forces the subscriber to switch to different control channel or BS depending on radio propagation effects, current traffic, location of subscriber
  - ✓ However it may or may not succeed.

**AMPS and ETACS air interface**

| Parameter | AMPS | ETACS |
|---|---|---|
| Multiple Access | FDMA | FDMA |
| Duplexing | FDD | FDD |
| Channel BW | 30 KHz | 25 KHz |
| Traffic channels per RF channel | 1 | 1 |
| Reverse channel freq | 824-849 MHz | 890-915 MHz |
| Forward channel freq | 869-894 MHz | 935-960 MHZ |
| Voice modulation | FM | FM |
| Data rate on control/wideband channel | 10kbps | 8kbps |
| Spectral efficiency | 0.33 bps/Hz | 0.33 bps/Hz |
| Number of channels | 832 | 1000 |

**Supervisory signals (SAT and ST tones)**

- Allow each user and BS to confirm that they are connected during a call
- SAT always exists during use of any voice channel.
- AMPS and ETACS use three SAT signals at frequencies of 5970 Hz, 6000 Hz or 6030 Hz
- BS constantly transmits one of three SAT tones on each voice channels when in use
- SAT is superimposed on voice signal on both forward and reverse channels
- The particular frequency of SAT denotes location of BS and is assigned by MSC
- When a call is setup and a voice channel is issued
  - ✓ SAT is transmitted immediately on FVC
  - ✓ Subscriber unit begins monitoring FVC, it must detect, filter and demodulate SAT
  - ✓ Similarly it reproduces SAT on RVC
  - ✓ This is required to dedicate a voice channel
  - ✓ If SAT is not presented or improperly detected within a one second interval, Both BS and subscriber unit cease transmission
- Signaling Tone (ST)
  - ✓ It is a 10 kbps data burst which signals call termination by the subscriber
  - ✓ It is a special “end-of-call” message containing alternating 1s and 0s sent on RVC for 200 ms
  - ✓ Unlike blank-and-burst messages which briefly suspends SAT transmission, ST

tone must be sent simultaneously with SAT.

- ✓ Alerts the system that user has deliberately terminated the call as opposed to being dropped by the system

**Wideband Blank-and-burst Encoding**

- AMPS voice channels carry wideband (10 kbps) data streams for blank-and-burst signaling
- The wideband data stream is encoded using Manchester coding
- The advantage is that the energy of the Manchester coded signal is concentrated at the transmission rate frequency of 10 KHz and little energy leaks into audio band below 4 KHz

**Narrowband AMPS (N-AMPS)**

- 10 KHz channel: 3 times large number of users and bandwidth
- Uses same SAT, ST and blank-and-burst except signaling was done by using sub-audible data streams

**Lecture 16**
**GSM: Global System for Mobile Communication**

**Outlines**

- Review of Last Lecture
- GSM Introduction
- GSM System Architecture
- GSM Network Areas
- Specifications
- Subscriber Services
- Mobility
- Identifiers in GSM Network

**Last Lecture**

- AMPS introduction
- System Overview
- Call handling
- Air interface
- Supervisory signals
- N-AMPS

**GSM Introduction**

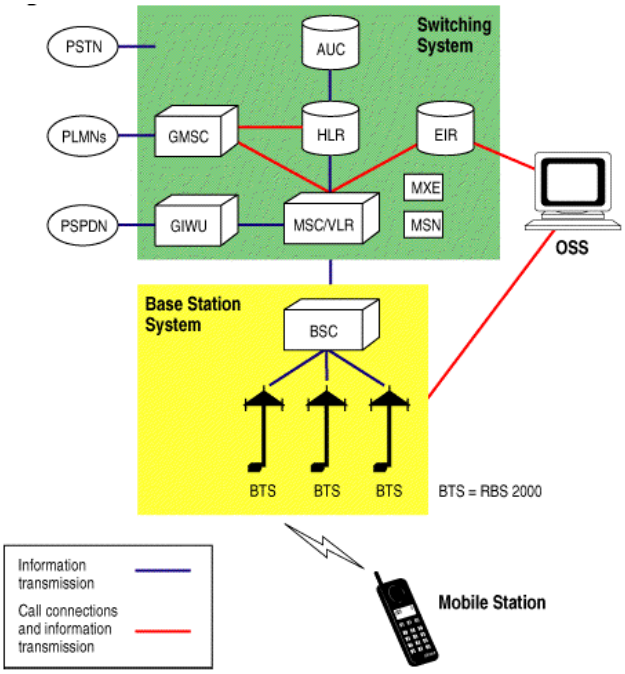
- Analog systems:
  - ✓ Inability to handle the growing capacity needs in a cost-efficient manner
- Various systems have been developed without the benefit of standardized specifications.
- Digital Systems:
  - ✓ Ease of signaling, lower levels of interference, integration of transmission and switching, and increased ability to meet capacity demands.
  - ✓ It addresses the specification issue particularly
  - ✓ GSM provides recommendations, not requirements.
  - ✓ The GSM specifications define the functions and interface requirements in detail but do not address the hardware to limit the designers as little as possible

**GSM Milestones**

| Year | Milestone |
|---|---|
| 1982 | GSM formed |
| 1986 | field test |
| 1987 | TDMA chosen as access method |
| 1988 | memorandum of understanding signed |

- The GSM network is divided into three major systems:
  - ✓ Switching System (SS)
    - Is responsible for performing call processing and subscriber-related functions.
  - ✓ Base Station System (BSS),
    - All radio-related functions are performed in the BSS, which consists of base station controllers (BSCs) and the base transceiver stations (BTSs).

- ✓ Operation and Support System (OSS).
  - The functional entity from which the network operator monitors and controls the system.
- ✓ To offer the customer cost-effective support for centralized, regional, and local operational and maintenance activities that are required for a GSM network.

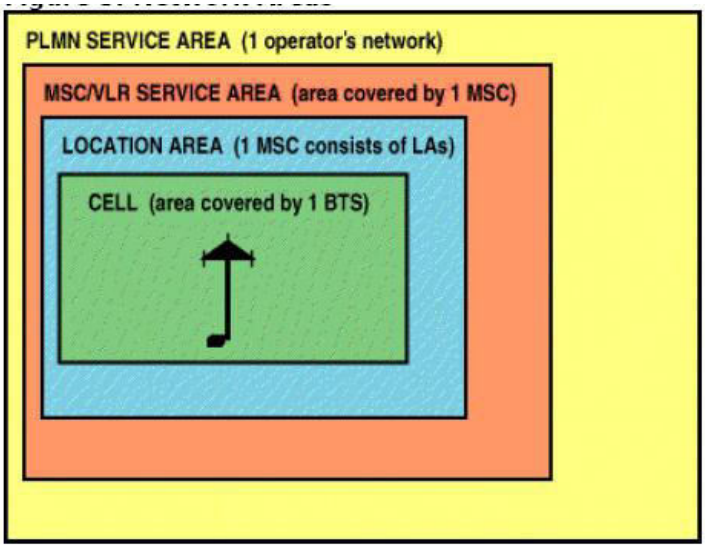



- Mobile Switching Centre MSC
  - ✓ The core switching entity in the network.
  - ✓ Is connected to the radio access network (RAN);
  - ✓ The RAN is formed by the BSCs and BTSs within the Public Land Mobile Network (PLMN).
  - ✓ All calls to and from the user are controlled by the MSC.
  - ✓ A GSM network has one or more MSCs, geographically distributed.
- Base Station Controller (BSC)
  - ✓ Provides all the control functions and physical links between the MSC and BTS.
  - ✓ It is a high-capacity switch that provides functions such as handover, cell configuration data, and control of radio frequency (RF) power levels in base transceiver stations.
  - ✓ A number of BSCs are served by an MSC.
- Base Transceiver Station (BTS)
  - ✓ Handles the radio interface to the mobile station.
  - ✓ The BTS is the radio equipment (transceivers and antennas) needed to service each cell in the network.
  - ✓ A group of BTSs are controlled by a BSC.

- Home Location Register (HLR)
  - ✓ A database used for storage and management of subscriptions.
  - ✓ Data about subscribers, including a subscriber's service profile, location information, and activity status.
  - ✓ When an individual buys a subscription, he or she is registered in the HLR of that operator.
- Visitor Location Register (VLR)
  - ✓ A database that contains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers.
  - ✓ The VLR is always integrated with the MSC.
  - ✓ For roaming user, VLR connected to that MSC will request data about the mobile station from the HLR through MSC.
- Authentication Centre (AUC)
  - ✓ Provides authentication and encryption parameters that verify the user's identity and ensure the confidentiality of each call.
  - ✓ The AUC protects network operators from different types of fraud found in today's cellular world.
- Equipment Identity Register (EIR)
  - ✓ A database that contains information about the identity of mobile equipment that prevents calls from stolen, unauthorized, or defective mobile stations.
  - ✓ The AUC and EIR are implemented as stand-alone nodes or as a combined AUC/EIR node.
- Message Centre (MXE)
  - ✓ Provides integrated voice, fax, and data messaging.
  - ✓ Specifically, the MXE handles short message service, cell broadcast, voice mail, fax mail, email, and notification.
- Gateway Mobile Services Switching Centre (GMSC)
  - ✓ A node used to interconnect two networks.
  - ✓ The gateway is often implemented in an MSC. The MSC is then referred to as the GMSC.
- GSM inter-working unit (GIWU)
  - ✓ Consists of both hardware and software that provides an interface to various networks for data communications.
  - ✓ Through the GIWU, users can alternate between speech and data during the same call.
  - ✓ The GIWU hardware equipment is physically located at the MSC/VLR.

**GSM Network Areas**

- Cell
  - ✓ Identified by cell global identity (CGI)
- Location Area (LA)
  - ✓ Group of Cells, identified by LAI
- MSC
- Public Land Mobile Network
  - ✓ Service area of one operator




**Specifications**

- Frequency band—1,850 to 1,990 MHz (mobile station to base station).
- Duplex distance—80 MHz.
- Channel bandwidth -- 200 kHz.
- Modulation—Gaussian minimum shift keying (GMSK).
- Transmission rate—over-the-air bit rate of 270 kbps.
- Access method—time division multiple access
- (TDMA)
- Speech coder—GSM uses linear predictive coding (LPC). Speech is encoded at 13 kbps

**GSM Subscriber Services**

- There are two basic types of services offered through GSM:
  - ✓ Telephony (also referred to as tele-services)
  - ✓ Data (also referred to as bearer services).
- Telephony services are mainly voice services that provide subscribers with the complete capability (including necessary terminal equipment) to communicate with other subscribers.
- Data services provide the capacity necessary to transmit appropriate data signals between two access points creating an interface to the network.
- In addition to normal telephony and emergency calling, the following subscriber services are supported by GSM:

- Dual-tone multi-frequency (DTMF)
  - ✓ DTMF is a tone signalling scheme often used for various control purposes via the telephone network, such as remote control of an answering machine.

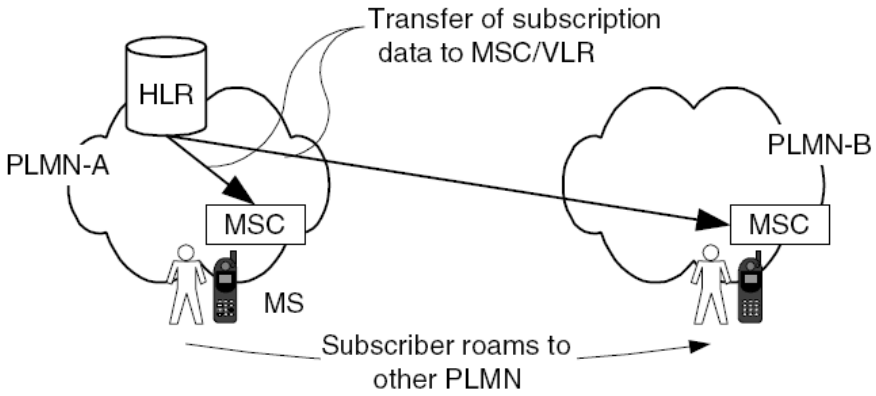
- Facsimile group III
  - ✓ GSM supports CCITT Group 3 facsimile.

- ✓ As standard fax machines are designed to be connected to a telephone using analog signals, a special fax converter connected to the exchange is used in the GSM system. This enables a GSM–connected fax to communicate with any analog fax in the network.

- Short message services
  - ✓ A message consisting of a maximum of 160 alphanumeric characters can be sent to or from a mobile station.
  - ✓ If the subscriber's mobile unit is powered off or has left the coverage area, the message is stored and offered back to the subscriber when the mobile is powered on or has re-entered the coverage area of the network.
- Cell broadcast
  - ✓ A variation of the short message service is the cell broadcast facility.
  - ✓ A message of a maximum of 93 characters can be broadcast to all mobile subscribers in a certain geographic area.
  - ✓ Typical applications include traffic congestion warnings and reports on accidents.
- Voice mail
  - ✓ This service is actually an answering machine within the network, which is controlled by the subscriber.
  - ✓ Calls can be forwarded to the subscriber's voice-mail box and the subscriber checks for messages via a personal security code.
- Fax mail
  - ✓ With this service, the subscriber can receive fax messages at any fax machine. The messages are stored in a service centre from which they can be retrieved by the subscriber via a personal security code to the desired fax number.

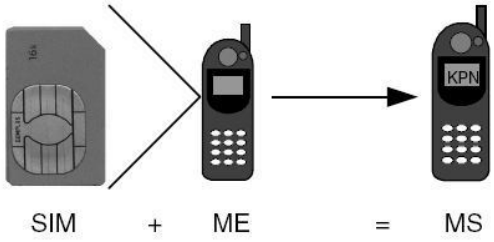
**GSM Mobility**

- Roaming with GSM is made possible through the separation of switching capability and subscription data.
- A GSM subscriber has her subscription data permanently registered in the HLR in his/her HPLMN.
- The GSM operator is responsible for provisioning this data in the HLR. The MSC and GMSC in a PLMN, on the other hand, are not specific for one subscriber group.



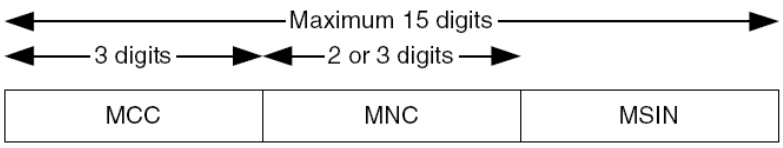
**Mobile Station**

- Mobile Equipment (ME)
- Subscriber Identification Module (SIM)
  - ✓ This is the chip embedded in the SIM card that identifies a subscriber of a GSM network;
  - ✓ When the SIM card is inserted in the ME, the subscriber may register with a GSM network.
  - ✓ The ME is now effectively personalized for this GSM subscriber;
  - ✓ The SIM card contains information such as IMSI, advice of charge parameters, operator-specific emergency number, etc.




**Identifiers in the GSM Network**

- GSM uses several identifiers for
  - ✓ The routing of calls,
  - ✓ Identifying subscribers (e.g. for charging),
  - ✓ Locating the HLR, identifying equipment, etc.
- International Mobile Subscriber Identity (IMSI)
  - ✓ It is embedded on the SIM card and is used to identify a subscriber.
  - ✓ The IMSI is also contained in the subscription data in the HLR.
  - ✓ Roaming charging – a VPLMN uses the IMSI to send billing records to the HPLMN of a subscriber.



## Lecture 17
## GPRS: General Packet Radio Service (Part I)

**Outlines**

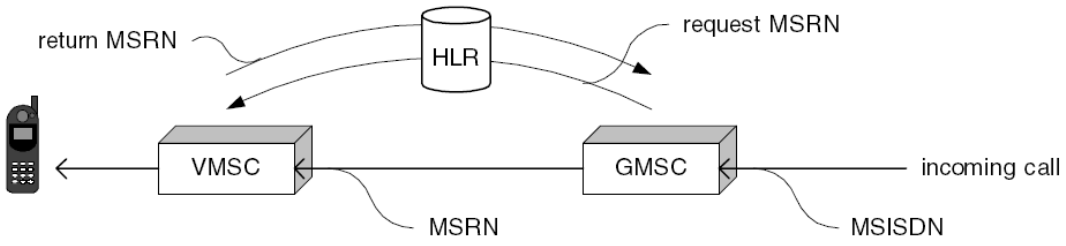
- Review of last lecture
- Identifiers in GSM Network and Call Routing
- Introduction to GPRS
- GPRS Architecture
- Registration and Session Management
- Routing Scenario in GPRS
- Channels Classification

**Last Lecture**

- GSM Introduction
- GSM System Architecture
- GSM Network Areas
- Specifications
- Subscriber Services
  - ✓ Dual-tone multifrequency (DTMF)
  - ✓ Facsimile group III
  - ✓ Short message services
  - ✓ Cell broadcast
  - ✓ Voice and fax mail
- Mobility
- Identifiers in GSM Network

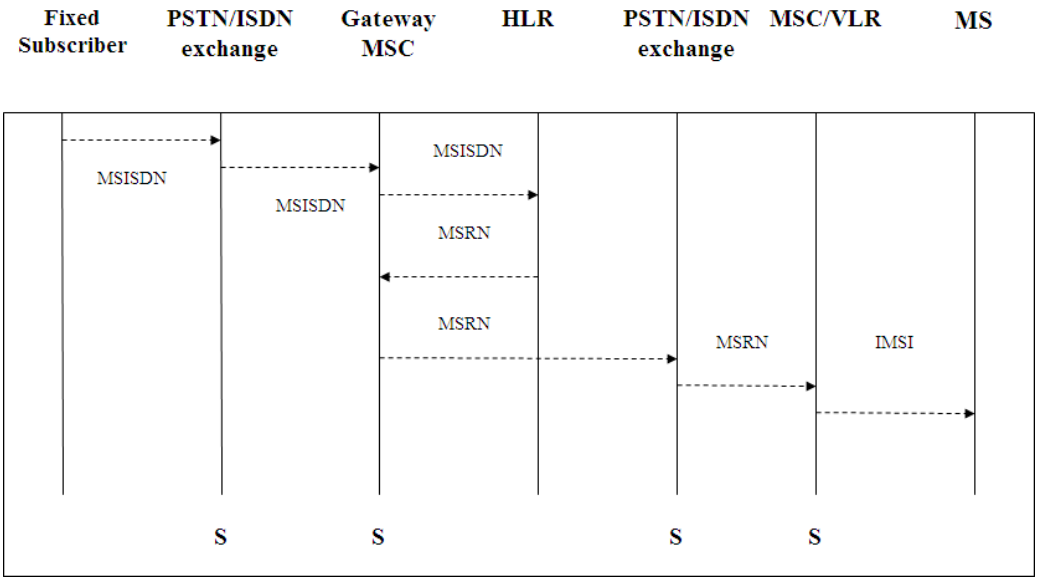
**Identifiers in the GSM Network**

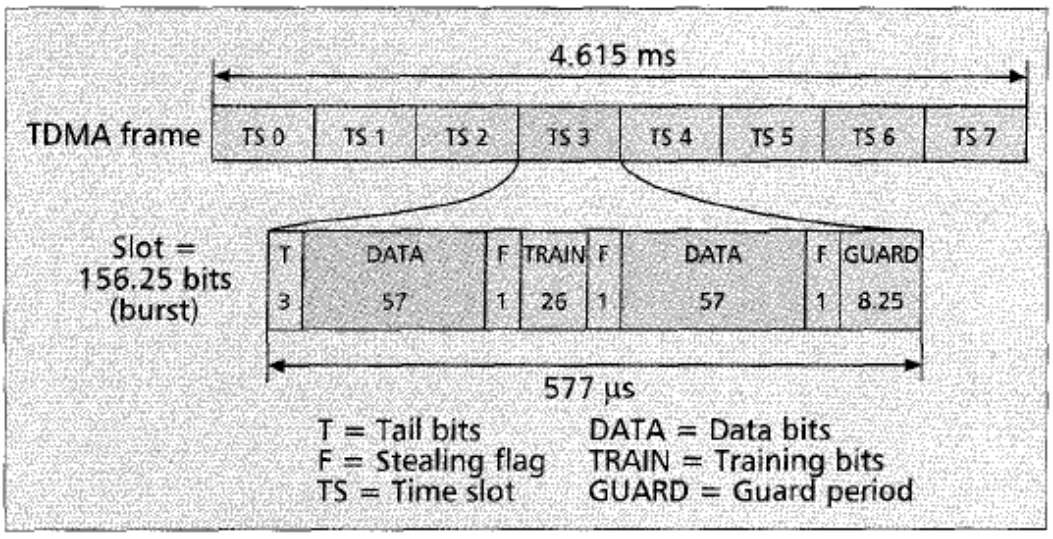
- GSM uses several identifiers for
  - ✓ The routing of calls,
  - ✓ Identifying subscribers (e.g. for charging),
  - ✓ Locating the HLR, identifying equipment, etc.
- International Mobile Subscriber Identity (IMSI)
  - ✓ It is embedded on the SIM card and is used to identify a subscriber.
  - ✓ The IMSI is also contained in the subscription data in the HLR.
- International Mobile Equipment Identifier
  - ✓ Each ME has a unique IMEI which is hard-coded in the ME and cannot be modified.
  - ✓ (IMEI) is used to identify the ME.
- Mobile Station Roaming Number
  - ✓ (MSRN) is used in the GSM network for routing a call to a MS.
  - ✓ The MSRN is allocated to a subscriber during MT call handling and is released when the call to that subscriber is established.
  - ✓ Each MSC in a PLMN has a (limited) range of MSRNs allocated to it.



- Mobile Station Integrated Services Digital Network Number (MSISDN Number)
  - ✓ The MSISDN is used to identify the subscriber when, among other things, establishing a call to that subscriber or sending an SMS to that subscriber.
  - ✓ The MSISDN is not stored on the subscriber's SIM card and is normally not available in the MS.
  - ✓ The MSISDN is provisioned in the HLR, as part of the subscriber's profile, and is sent to MSC during registration.

**Call Routing in GSM**




- General Packet Radio Service in GSM", Jian Cai and David J. Goodman, Rutgers University,
- IEEE Communications Magazine, Oct 1997

## GPRS

- GPRS is an enhancement over the GSM and adds some nodes in the network to provide the packet switched services. These network nodes are called GSNs (GPRS Support Nodes) and are responsible for the routing and delivery of the data packets to and from the MS and external packet data networks (PDN).

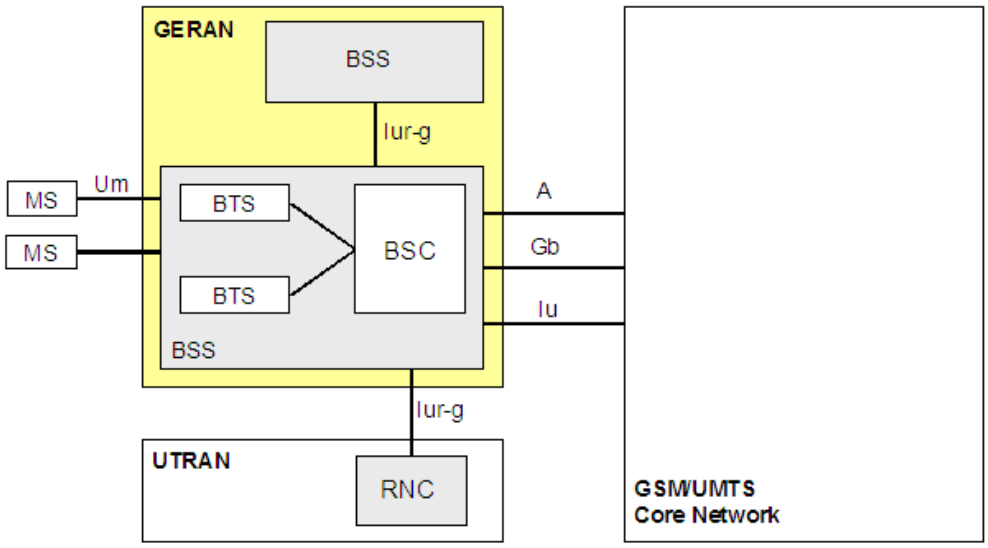
## Introduction to GPRS

- Goals of GPRS:
  - ✓ Efficient bandwidth usage for bursty data traffic (e.g. Internet)
  - ✓ Higher data rates
  - ✓ New charging models
- Initially specified by ETSI
- A lot of releases (R97, R98, R99, R4 etc.)
- Specifications handed over to 3GPP
- A lot of specifications considered in this overview:
  - ✓ Release 5 (Ganz) / 6 (most recent TS at 3GPP)

## GPRS Release 5/6

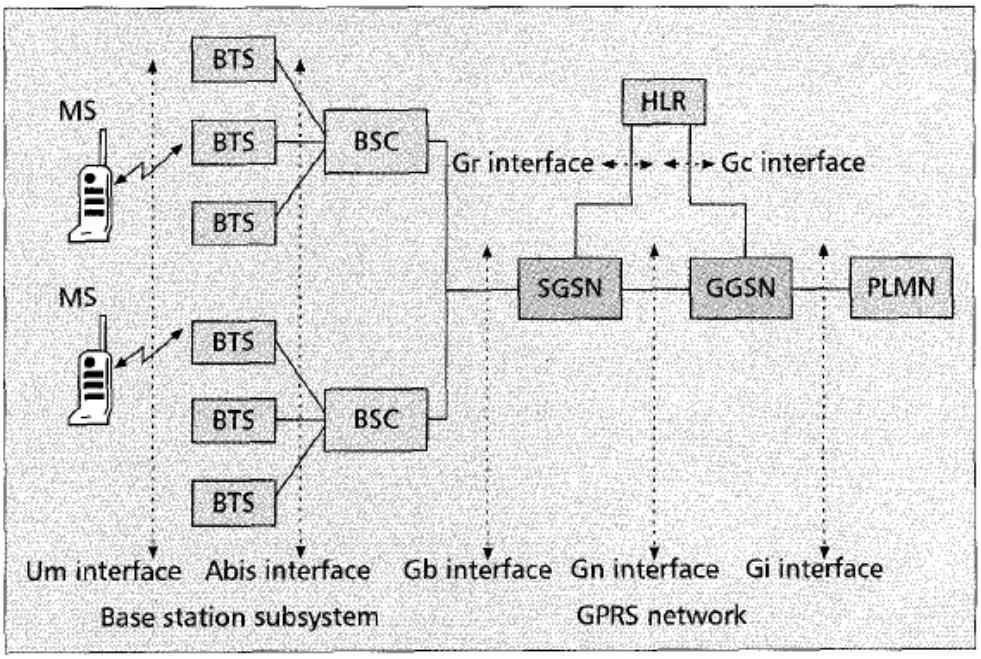
- Two modes determined by generation of core network:
  - ✓ 2G core => A/Gb
  - ✓ 3G core => Iu
- Iu interface added in rel. 5 to align with UMTS

## GERAN Reference Architecture




3GPP TS 43.051 (Release 6)

**GPRS Architecture**




- "General Packet Radio Service in GSM", Jian Cai and David J. Goodman, Rutgers University,
- IEEE Communications Magazine, Oct 1997

**A/Gb mode**

- Class A: MS can operate simultaneous packet switched and circuit switched services
- Class B: MS can operate either one at one time
  - ✓ Most common for handsets today
- Class C: MS can operate only packet switched services
  - ✓ E.g. expansion cards for laptops

**Iu mode**

- CS/PS mode: Same as Class A in A/Gb mode
- PS mode: MS can only operate packet switched services
- CS mode: MS can only operate circuit switched services

**Service Types**

- Point-to-Point
  - ✓ Internet access by user
- Point-to-Multipoint
  - ✓ Delivery of information (e.g. news) to multiple locations or interactive conference applications

**GPRS BSS**

- A software upgrade is required in the existing Base Transceiver Site (BTS).
- The Base Station Controller (BSC) also requires a software upgrade, and the installation of a new piece of hardware called a packet control unit (PCU).
- The PCU directs the data traffic to the GPRS network and can be a separate hardware element associated with BSC.
- The PCU provides a physical and logical data interface out of BSS for packet data traffic.

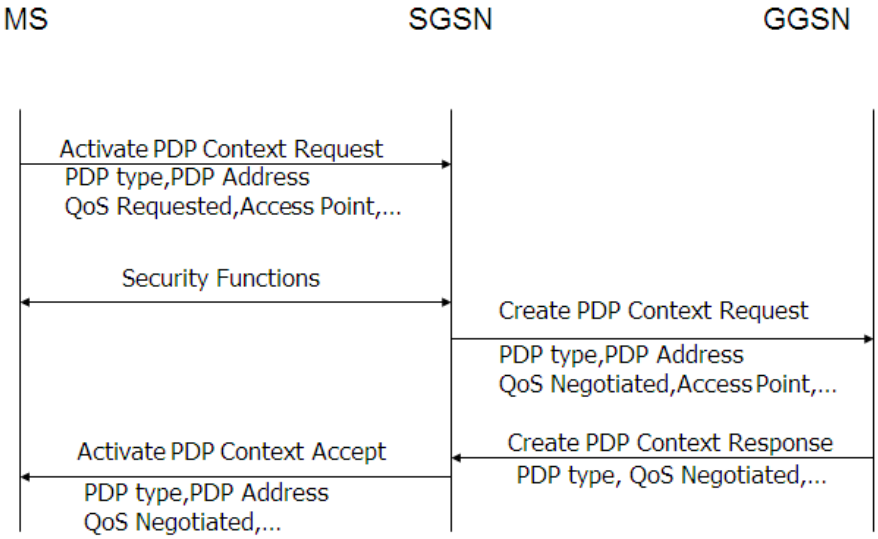
**Registration of a Mobile Node**

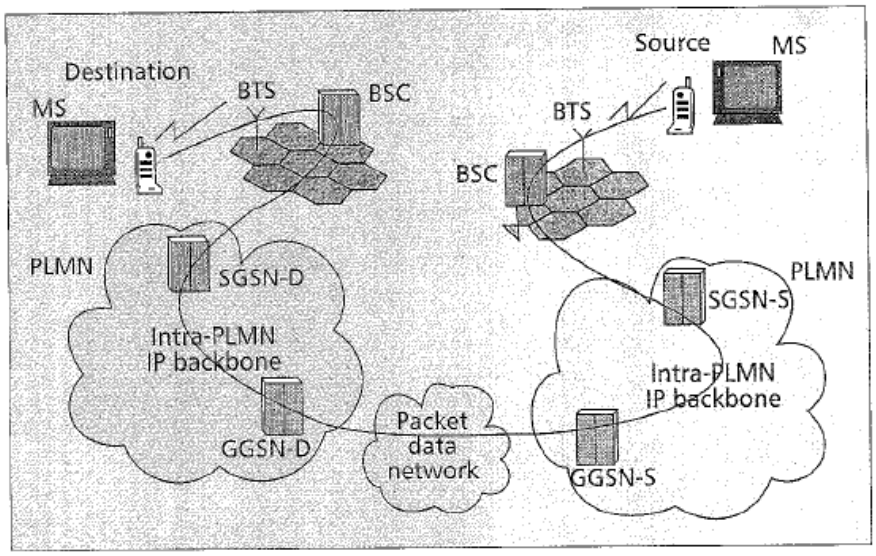
- A mobile station must register itself with GPRS network.
  - ✓ GPRS attach
    - The device sends message to the new SGSN containing the last assigned Temporary Mobile Subscriber Id (TMSI), location area information, etc.
    - The new SGSN queries the old SGSN for the identity of this mobile device.
    - Then the new SGSN requests more information from the mobile device to authenticate itself against the new SGSN
  - ✓ GPRS detach
    - GPRS detach can be initiated by the MS or the network.

**Session Management**

- After Successful attach, when it wishes to begin a packet data, it must activate Packet Data Protocol (PDP) address.This address is unique only for a particular session. It consists of,
  - ✓ PDP type
  - ✓ PDP address assigned to MS
  - ✓ Requested QoS
- Once PDP Context is activated, a two-way tunnel is established between the device current SGSN and the corresponding GGSN.
- GGSN hides the mobility from onward
- PDP-Address allocation:
  - ✓ Static:Assigned by network operator of User's home PLMN.
  - ✓ Dynamic:Assigned by Corresponding GGSN.

**PDP Context Activation**




**Physical Channels**

- Defined by timeslot (0-7) and radio frequency channel
- Shared Basic Physical Sub Channel
  - ✓ Shared among several users (up to 8)
- Dedicated Basic Physical Sub Channel
  - ✓ One user
- Packet Data Channel (PDCH)
  - ✓ Dedicated to packet data traffic from logical channels (next slide)
    - Control
    - User data

**Lecture 18**
**GPRS: General Packet Radio Service (Part II)**

**Outlines**

- GPRS Protocol Architecture
  - ✓ MS – BSS
  - ✓ BSS – SGSN
  - ✓ SGSN – GGSN
  - ✓ GGSN – PDN
- GPRS Air Interface
- Data Routing and Mobility
- Uplink Data Transfer
- Downlink Data Transfer
- QoS in GPRS

**Last Lecture**

- Introduction to GPRS
- GPRS Architecture
- Registration and Session Management
- Routing Scenario in GPRS
- Channels Classification

**Logical Channels**

- Mapped by the MAC to physical channels
- Control channels for control, synchronization and signaling
  - ✓ Common
  - ✓ Broadcast
  - ✓ Dedicated
- Packet Traffic channels
  - ✓ Encoded speech
  - ✓ Encoded data

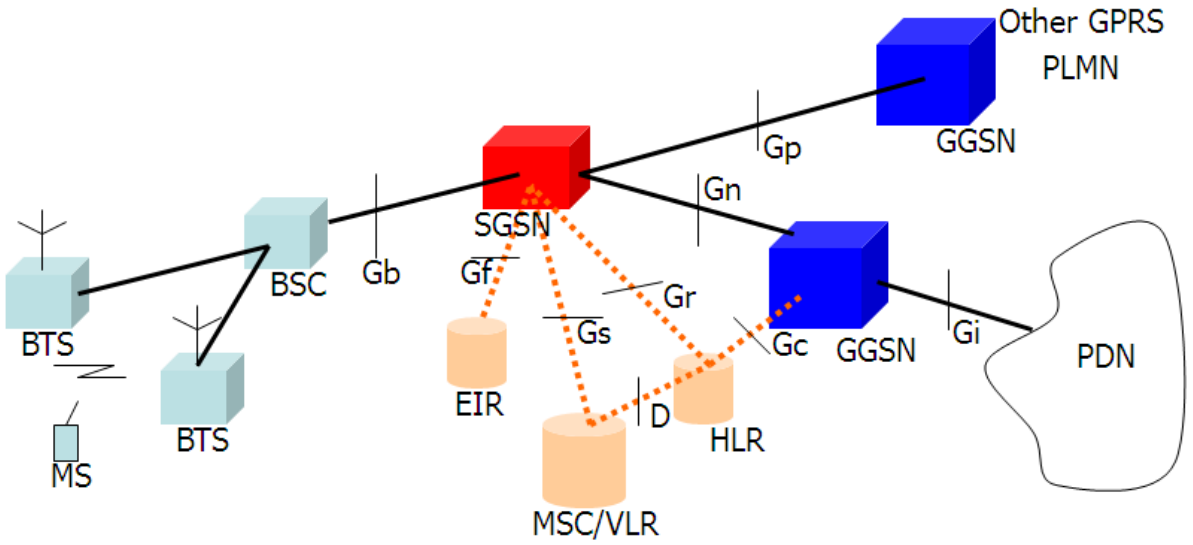
**Control Channels**

- Packet Common Control Channel (PCCCH)
  - ✓ When allocated in a cell, GPRS related mobiles camp on it
  - ✓ Divded into
    - Random Access (PRACH): MS initiate packet transfer or respond to paging messages
    - Paging (PPCH): to page an MS prior to packet transfer
    - Access Grant (PAGCH): send resource assignment to MS prior to packet transfer
    - Packet Notification (PNCH): used to send a PTM-Multicast notification to

group of MS

- Packet Dedicated Control Channel (PDCCH)
  - ✓ Slow Associated Control Channel (SACCH)
    - Radio measurements, power control and data
    - SMS transfer during calls
  - ✓ Fast Associated Control Channel (FACCH)
    - For one Traffic Channel (TCH)
    - Carry Ack
  - ✓ Stand-alone Dedicated Control Channel (SDCCH)
    - is used in the GSM system to provide a reliable connection for signalling and Short Message Service.
- Packet Broadcast Control Channel (PBCCH)
  - ✓ Frequency correction channels
    - Allows the MS to synchronize their Local Oscillator (LO) to the Base Station LO, using frequency offset estimation and correction.
  - ✓ Synchronization channel (MS freq. vs. BS)
  - ✓ Broadcast control channel for general information on the base station

**GPRS Architecture**

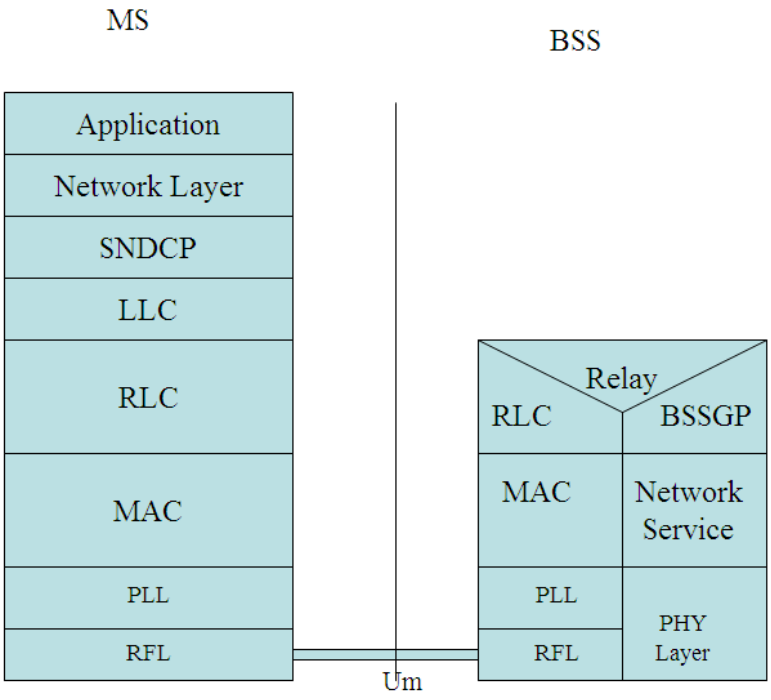



**Protocol Architecture**

- Transmission Plane
  - ✓ The protocols provide transmission of user data and its associated signaling
- Signaling Plane
  - ✓ Comprises protocols for the control and support of functions of the transmission plane

**Transmission Plane**

- GPRS Backbone:SGSN GGSN
  - ✓ GTP tunnels the user packets and related signaling information between the GPRS support nodes.
- Sub-network dependent convergence protocol
  - ✓ It is used to transfer packets between SGSN and MS
- Data link layer
  - ✓ LLC(MS-SGSN)
  - ✓ RLC/MAC(MS-BSS)
- Physical layer
  - ✓ PLL:channel coding,detection of errors, forward error correction, interleaving, detection of physical link congestion
  - ✓ RFL:modulation and demodulation




SNDCP : Sub-network dependent convergence protocol
LLC : Logical link control
RLC : Radio link control

**Radio Link Control**

- Can provide reliability for MAC transmissions
- Transparent mode
  - ✓ No functionality
- Acknowledged mode
  - ✓ Selective Repeat ARQ
  - ✓ Sender: Window

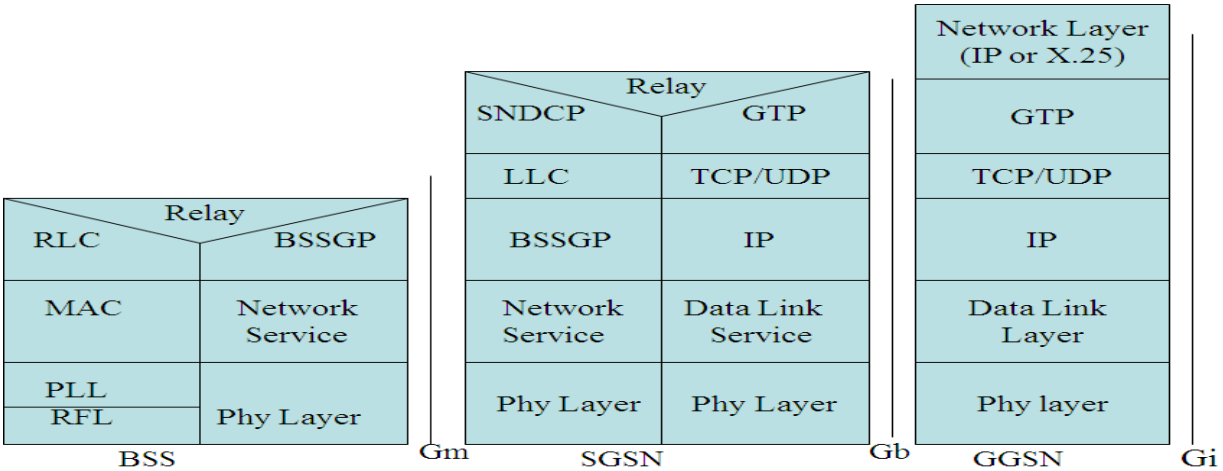
- ✓ Receiver: Uplink ACK/NACK or Downlink ACK/NACK
- Unacknowledged mode
  - ✓ Controlled by numbering within TBF
  - ✓ No retransmissions
  - ✓ Replaces missing packets with dummy information bits

**Media Access Control (MAC)**

- Performs contention resolution between channel access attempts
- Connection oriented
- Connections are called Temporary Block Flows (TBF)
  - ✓ Logical unidirectional connection between two MAC entities
  - ✓ Allocated resources on PDCH(s)
  - ✓ Temporary Flow Identity (TFI) is unique among concurrent TBFs in the same direction

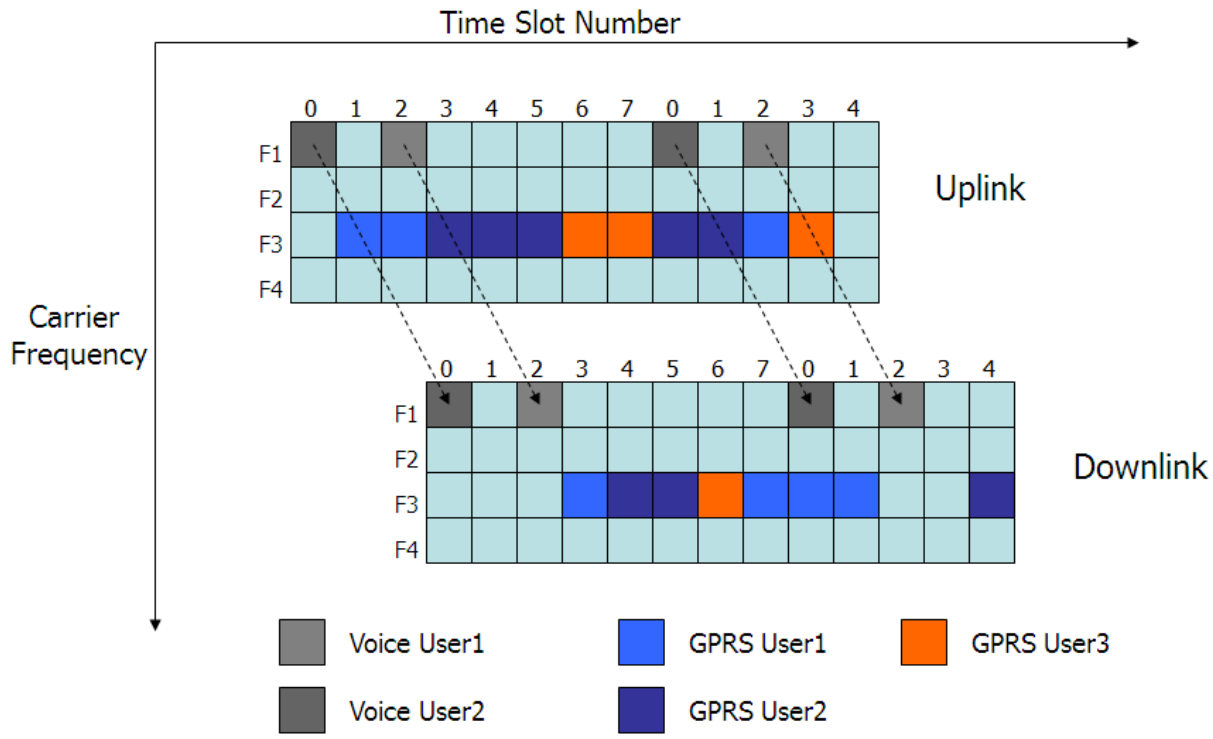
**MAC: Channel Access & Resource Allocation**

- Slotted Aloha
  - ✓ Used in PRACH
    - MSs send packets in uplink direction at the beginning of a slot
    - Collision: Back off -> timer (arbitrary) -> re-transmit
- Time Division Multiple Access (TDMA)
  - ✓ Predefined slots allocated by BSS
  - ✓ Contention-free channel access



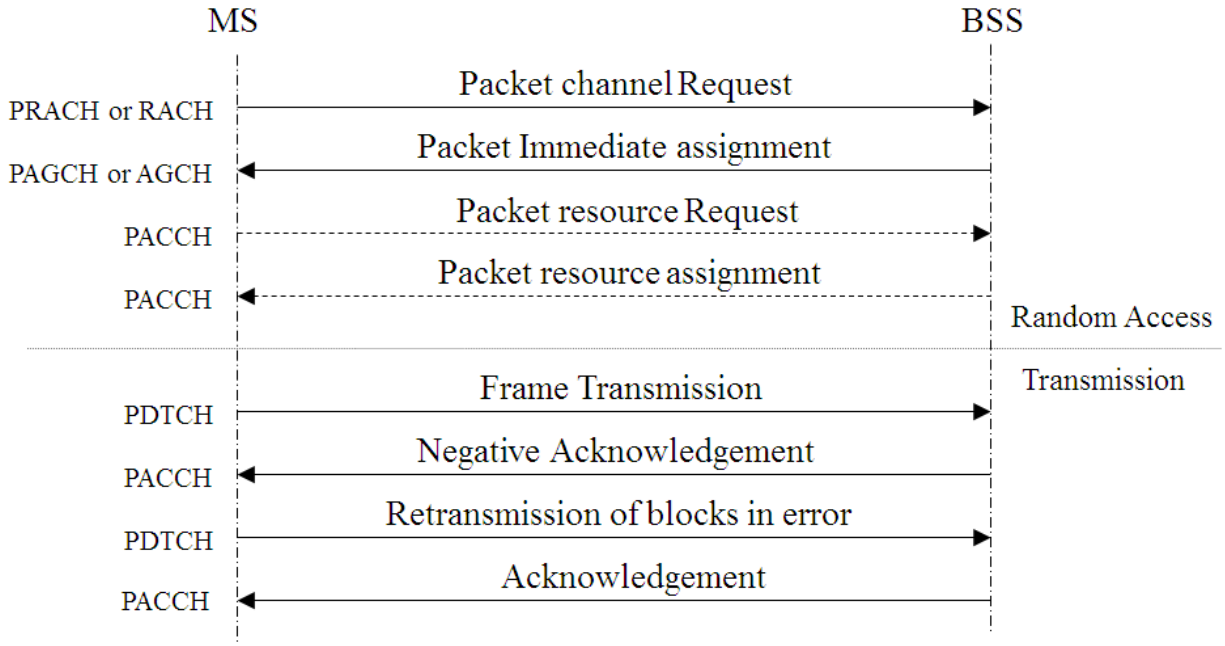

Transmission Plane

**GPRS Air Interface**

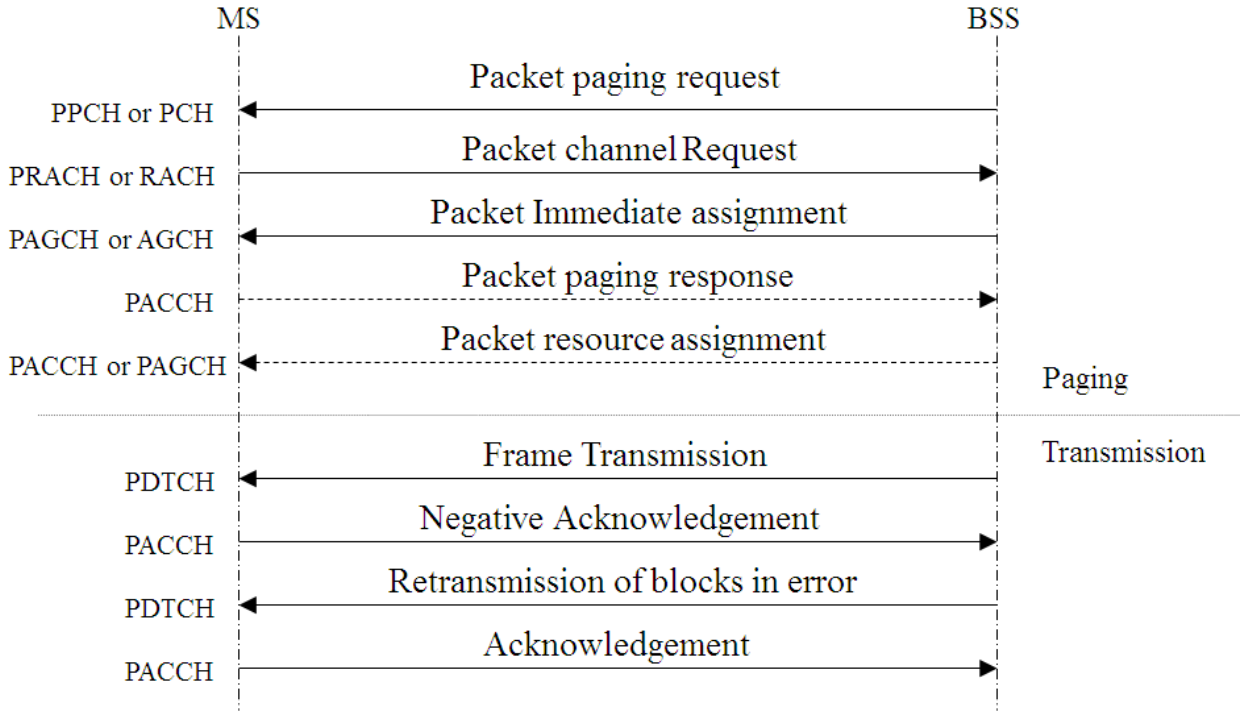



- Master slave concept
  - ✓ One PDCH acts as Master
  - ✓ Master holds all PCCCH channels
  - ✓ The rest of channels act as Slaves
- Capacity on demand
  - ✓ PDCH(s) are increased or decreased according to demand
  - ✓ Load supervision is done in MAC Layer

**Uplink Data Transfer**




**Downlink Data Transfer**



**Mobility**

- A mobile station has three states in GPRS system:
  - ✓ Idle
  - ✓ Standby
  - ✓ Active
- The operation of GPRS is partly independent of the GSM network. However, some procedures share the network elements with current GSM functions.
- Data is transmitted between a mobile station and the GPRS network only when the mobile station is in the active state.
- In the active state, the SGSN knows the cell location of the mobile station.
- In the standby state, the location of the station is known only as to which routing area it is in.
- In the idle state, the mobile station does not have a logical GPRS context activated or any Packet-Switched Public Data Network (PSPDZ) addresses allocated, The MS can receive only those multicast messages that can be received by any GPRS mobile station.

**QoS Support**

- Assumes that IP multimedia applications are able to
  - ✓ Define their requirements
  - ✓ Negotiate their capabilities
  - ✓ Identify and select available media components
- GPRS specifies signaling that enable support for various traffic streams
  - ✓ Constant/variable bit rate
  - ✓ Connection oriented/connection less
  - ✓ Etc.

**QoS Profile for GPRS Bearers**

- 4 parameters:
  - ✓ Service precedence
    - o 3 classes
  - ✓ Reliability parameter
    - o 3 classes
  - ✓ Delay parameters
    - o 4 classes
  - ✓ Throughput parameter
    - o Maximum and mean bit rates
- QoS profile is included in Packet Data Protocol (PDP) context
- Negotiation managed through PDP procedures (activation, modification and deactivation)

**Conclusions**

- Same GMSK modulation as GSM
- 4 channel coding modes
- Packet-mode supporting up to about 144 kbps

- Flexible time slot allocation (1-8)
- Radio resources shared dynamically between speech and data services
- Independent uplink and downlink resource allocation

**EDGE Airlink**

- Extends GPRS packet data with adaptive modulation/coding
- 2x spectral efficiency of GPRS for best effort data
- 8-PSK/GMSK at 271 ksps in 200 KHz RF channels supports 8.2 to 59.2 kbps per time slot
- Supports peak rates over 384 kbps

**Summary**

- GPRS Protocol Architecture
  - ✓ MS – BSS
  - ✓ BSS – SGSN
  - ✓ SGSN – GGSN
  - ✓ GGSN – PDN
- GPRS Air Interface
- Data Routing and Mobility
- Uplink Data Transfer
- Downlink Data Transfer
- QoS in GPRS

**Lecture 19**
**cdmaOne/IS-95**

**Outlines**

- Last Lecture
- IS-136
- CDMA/IS-95
- Advantages and drwabacks
- IS-95 Forward Channels
  - ✓ Pilot Channel
  - ✓ Sync Channel
  - ✓ Paging
  - ✓ Traffic
- IS-95 Reverse Channels
  - ✓ Access Channels
  - ✓ Traffic

## Last Lecture

- GPRS Protocol Architecture
  - ✓ MS – BSS
  - ✓ BSS – SGSN
  - ✓ SGSN – GGSN
  - ✓ GGSN – PDN
- GPRS Air Interface
- Data Routing and Mobility
- Uplink Data Transfer
- Downlink Data Transfer
- QoS in GPRS

## IS-136

- Evolution of AMPS
- Based on TDMA
- Operates in 800 / 1900 MHz band
- TDMA frames of 6 time slots, 40 ms in length
- Half rate in 1 slot and double rate in 4 slots

## IS-136 Channels

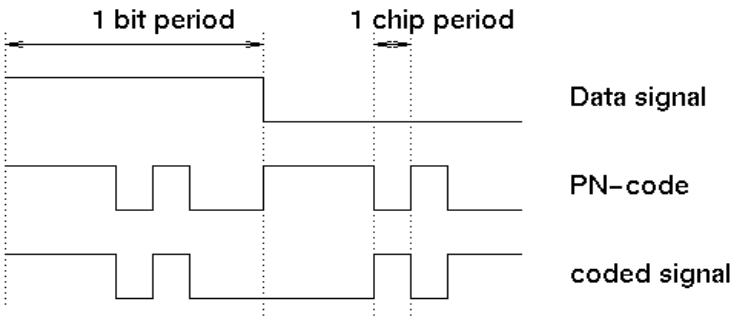
- Digital Control Channel (DCCH)
- Occupies full rate channel (2 time slots)
- Divided into logical channels
- SMS point-to-point, paging and access response channel (SPACH)
- Broadcast control channel (BCCH)
- Shared channel feedback (SCF)
- Random access control channel

**Specification summary**

| Parameter | IS-136 specification |
|---|---|
| Multiple access | TDMA/FDD |
| Modulation | p/4 DQPSK |
| Channel bandwidth | 30 kHz |
| Reverse channel frequency band | 824 – 849 MHz |
| Forward channel frequency band | 869 – 894 MHz |
| Forward and reverse channel data rate | 48.6 kb/s |
| Spectrum efficiency | 1.62 b/s/Hz |
| Equalizer | unspecified |
| Channel coding | 16-bit CRC and convolutional coding |
| Interleaver | Two-slot interleaver |
| Users per channel | 3 or 6 |

**What is CDMA**

- Both an access method and air-interface
  - ✓ Rest of the network is very similar
  - ✓ Radio resource management, mobility management, security are similar
- Power control and handoffs are different
- Uses DSSS
- Frequency reuse factor is 1
- 3 systems
  - ✓ IS-95 2G, W-CDMA, and CDMA2000



**Advantages of CDMA Cellular**

- Higher capacity
- Improves voice quality (new coder)
- Less power consumption (6-7 mW)
- Choice for 3G systems
- 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, Produce self-jamming
- 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
- Air-interface is the most complex

**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

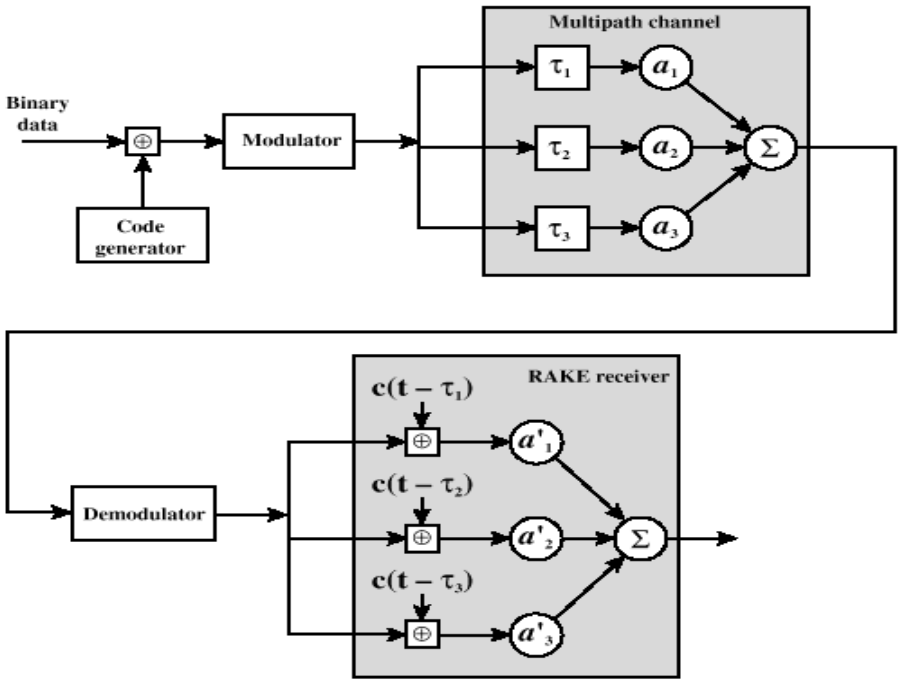
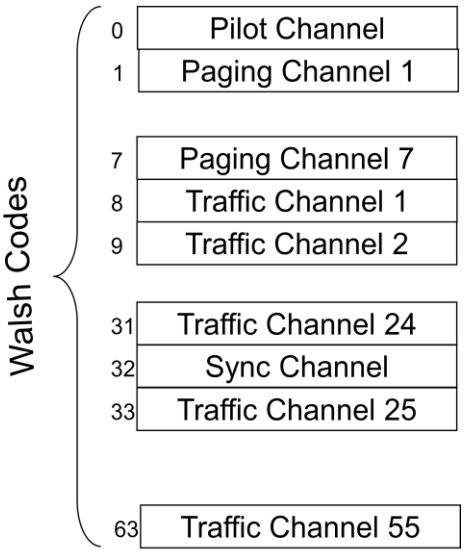



**Figure 10.18 Principle of RAKE Receiver [PRAS98]**

**IS-95 CDMA Forward Channel**

- The forward link uses the same frequency spectrum as AMPS (824-849 MHz)
- 4 types of logical channel:
  - ✓ A pilot,
  - ✓ A synchronization,
  - ✓ 7 paging and
  - ✓ 55 traffic channels
- QPSK is the modulation scheme
- Orthogonal Walsh codes are used (64 total)
- After orthogonal codes, they are further spread by short PN spreading codes

**Forward Channels**




**The pilot channel**

- Continuous signal on a single channel, allows MS to acquire timing info, provides a phase reference for demodulation process and means for signal strength comparison.
- 4-6 dB stronger than all other channels
- Obtained using all zero Walsh code; i.e., contains no information except the RF carrier
- No power control in the pilot channel

**Sync Channel**

- Used to acquire initial time synchronization
- Synch message includes system ID (SID), network ID (NID), the offset of the PN short code, the state of the PN-long code, and the paging channel data rate (4.8/9.6 Kbps)
- Uses W32 for spreading
- Operates at 1200 bps

**Paging Channel**

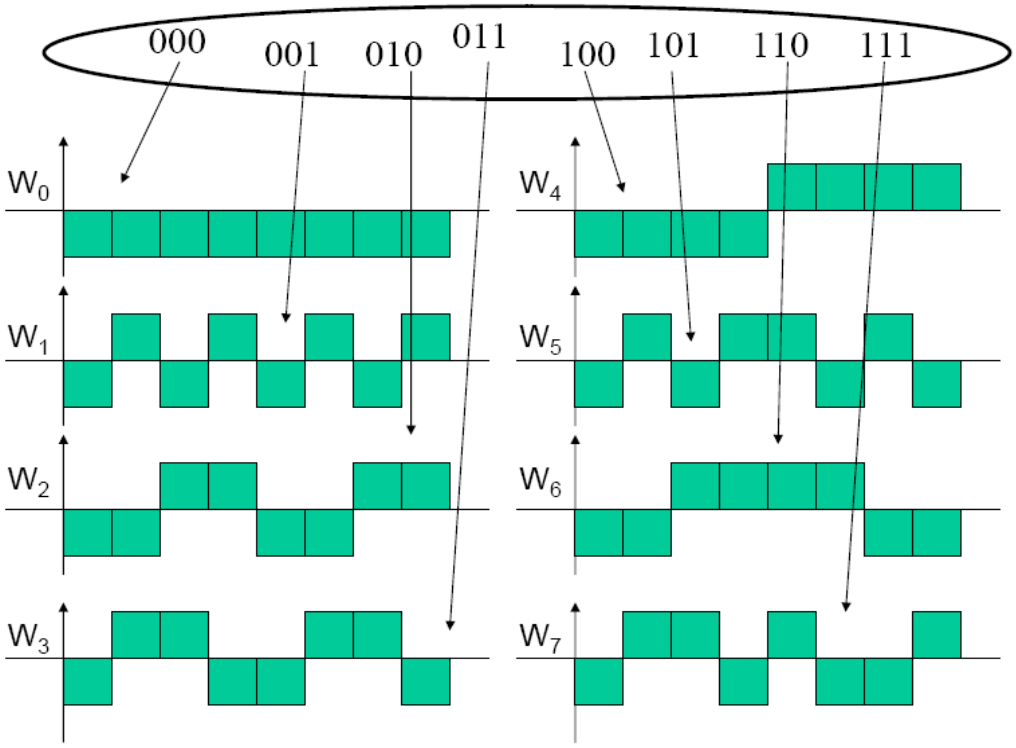
- Uses W1-W7
- There is no power control
- Additionally scrambled by PN long code, which is generated by LFSR of length 42
- The rate 4.8 Kbps or 9.6Kbps

**Traffic Channels**

- Carry user information
- Two possible date rates
  - ✓ RS1={9.6, 4.8, 2.4, 1.2 Kbps}
  - ✓ RS2={14.4, 7.2, 3.6, 1.8 Kbps}
- RS1 is mandatory for IS-95, but support for RS2 is optional
- Also carry power control bits for the reverse channel

**Forward Link Transmission**

- For voice traffic, the speech is encoded at a data rate of 8550 bps
- After additional bits added for error detection, it becomes 9600 bps.
- The full channel capacity is not used when user is not speaking,
  - ✓ During quiet periods, data rate is upto 1200 bps
  - ✓ 2400 bps is used to transmit transients in the background noise
  - ✓ 4800 bps is used to mix digitized speech and signaling data
- Digitized speech is transmitted in 20 ms blocks with FEC rate ½ thus making effective data rate to a max of 19.2 kbps
- The resulting stream is XORed with Walsh code generating data at 1.2288 Mbps.




**Summary**

- IS-136
- CDMA/IS-95
- Advantages and drwabacks
- IS-95 Forward Channels
  - ✓ Pilot Channel
  - ✓ Sync Channel
  - ✓ Paging
  - ✓ Traffic
- Next Lecture

# Lecture 20
# EDGE

## Outlines

- Last Lecture Review
- Walsh Codes
- IS-95 Reverse Link
- EDGE Introduction
- Modulation and Coding Schemes
- Link Adaptation and Incremental Redundancy
- Capacity Planning
- Dynamic Abis pool

## Last Lecture

- IS-136
- CDMA/IS-95
- Advantages
  - Frequency diversity, multipath resistance, privacy, graceful degradation
- Drwabacks
  - Self-jamming, near-far problem, soft handoff
- IS-95 Forward Channels
  - Pilot Channel
  - Sync Channel
  - Paging
  - Traffic
- IS-95 Reverse Channels
  - Access Channels
  - Traffic
- Next Lecture

## Forward Link Channel Parameters

| Channel | Sync | Paging | | Traffic rate Set 1 | | | | Traffic Rate Set 2 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Data rate (bps) | 1200 | 4800 | 9600 | 1200 | 2400 | 4800 | 9600 | 1800 | 3600 | 7200 | 14400 |
| Code repetition | 2 | 2 | 1 | 8 | 4 | 2 | 1 | 8 | 4 | 2 | 1 |
| Modulation symbol rate (sps) | 4800 | 19200 | 19200 | 19200 | 19200 | 19200 | 19200 | 19200 | 19200 | 19200 | 19200 |
| PN Chips / modulation symbol | 256 | 64 | 64 | 64 | 64 | 64 | 64 | 64 | 64 | 64 | 64 |
| PN Chips / bit | 1024 | 256 | 128 | 1024 | 512 | 256 | 128 | 682.67 | 341.33 | 170.67 | 85.33 |

**Walsh Codes**

- 2x2 Walsh Matrix

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- User 1 (1, 1) and user 2 (1, -1)
- 4 x 4 Walsh matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

**IS-95 Reverse Link**

- Consists of upto 94 logical channels each occupying same bandwidth of 1228 KHz.
- It supports 32 access channels and 62 traffic channels
- Access channel is used to initiate a call, to respond to paging channel and for location update
- In reverse, convolutional encoder has a rate of 1/3, thus trippling the effective rate to a max of 28.8 kbps

**IS-95 CDMA Reverse Channel**

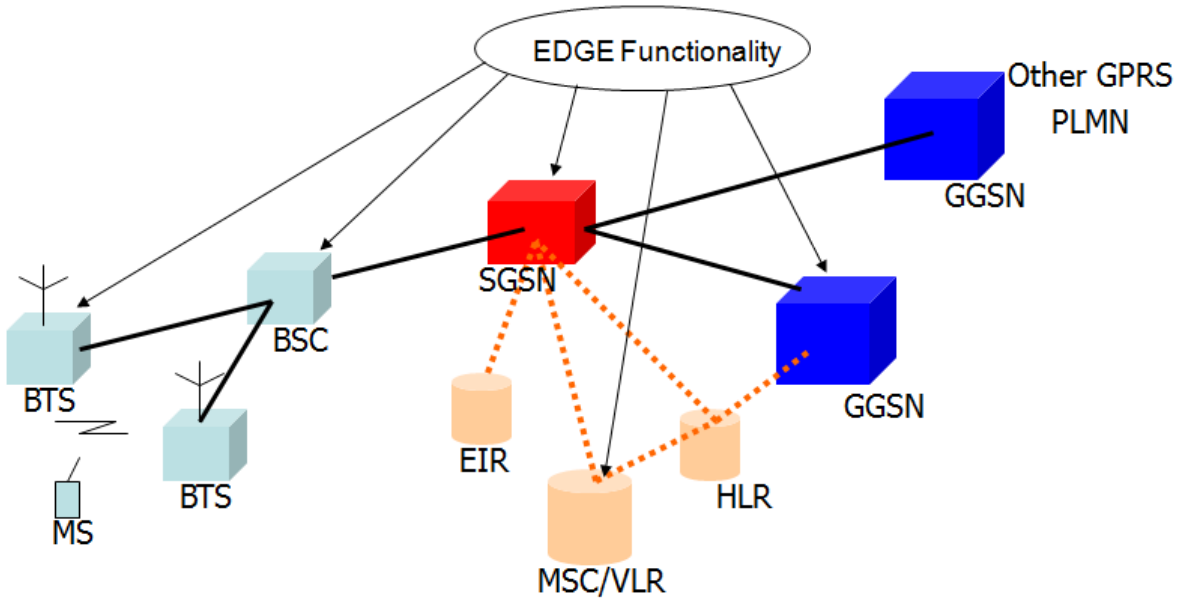
- Uses OQPSK for power efficiency and QPSK demodulation is easy
- 869-894 MHz range.
- No spreading of the data using orthogonal codes
    - Data coming out of the block interleaver are grouped in units of 6 bits that serves as an index to select a row of the 64x64 Walsh matrix and that row is substituted for the input
    - Thus data rate is expanded by a factor of 64/6 to 307.2 kbps

**Enhanced Data rates for GSM Evolution**

- GPRS data rates still fall short compared to that promised by 3G.
- The delay in deployment of 3G technology led to the emergence of EDGE
- Phase 1 (Release'99 & 2002 deployment) supports best effort packet data at speeds up to about 384 kbps
- Phase 2 (Release'2000 & 2003 deployment) will add Voice over IP capability

**GPRS Architecture**

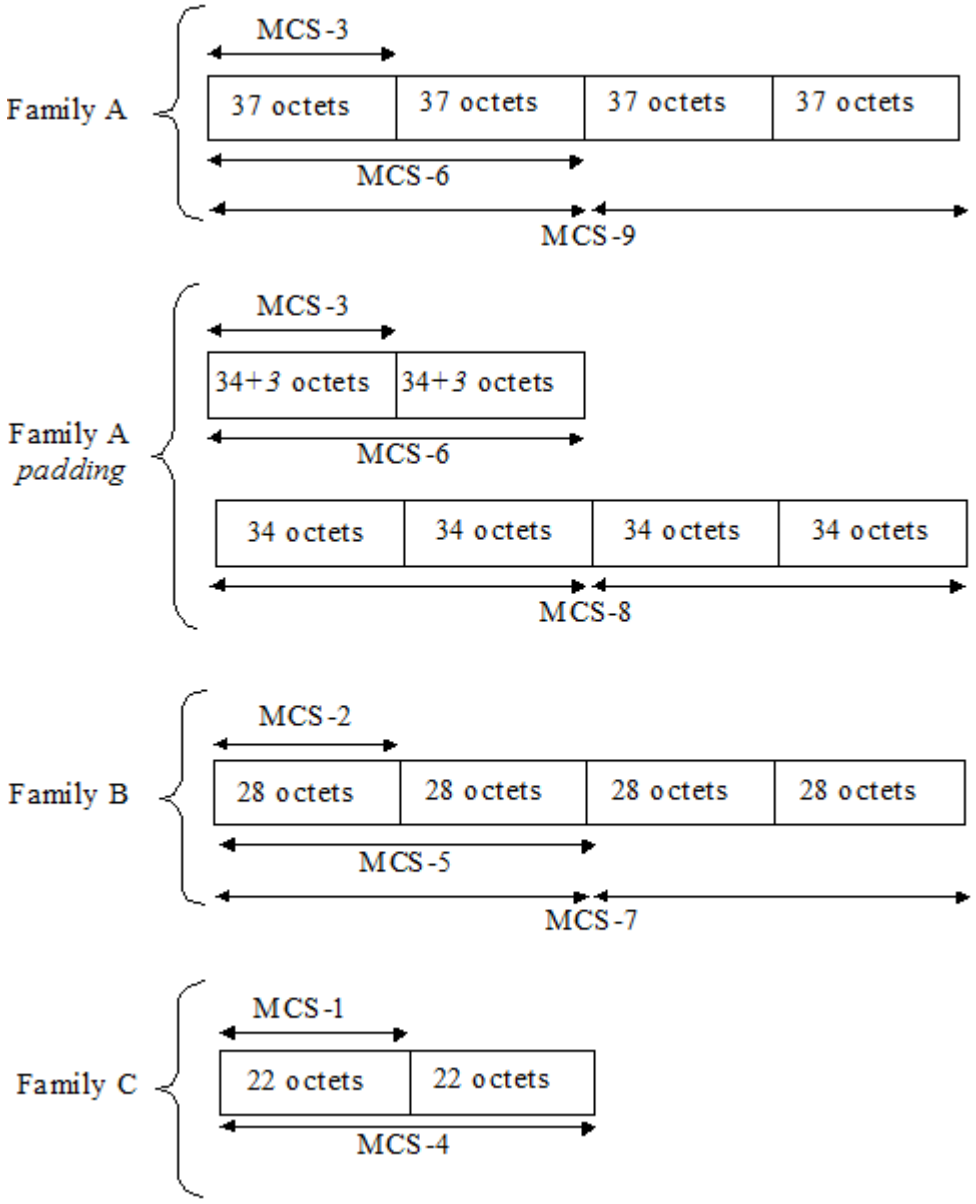
- Similar to GPRS but some changes for higher data rates. Important change is modulation scheme




- GMSK is used in GPRS, only one bit per symbol is used
- In EDGE, Octogonal PSK (8-PSK) is used which enables a threefold higher data rate of 59.2 kbps per radio time slot.
  - ✓ Achieved by transmitting 3 bits per symbol.
- GMSK has constant amplitude modulation while 8-PSK has variations in amplitude.
- This changes the radio frequency characteristics requiring changes in BS.
- minor changes in hardware and software in existing systems, leads to major changes in network performance.
- Radio network Planning
  - ✓ Coding Scheme: nine modulation and coding schemes (MCS) that provide different throughput as shown in table

| Scheme | Modulation | Maximum rate [kb/s] | Code Rate | Family |
|---|---|---|---|---|
| MCS-9 | 8PSK | 59.2 | 1.0 | A |
| MCS-8 | | 54.4 | 0.92 | A |
| MCS-7 | | 44.8 | 0.76 | B |
| MCS-6 | | 29.6 / 27.2 | 0.49 | A |
| MCS-5 | | 22.4 | 0.37 | B |
| MCS-4 | GMSK | 17.6 | 1.0 | C |
| MCS-3 | | 14.8 / 13.6 | 0.80 | A |
| MCS-2 | | 11.2 | 0.66 | B |
| MCS-1 | | 8.8 | 0.53 | C |

**Payload Format**



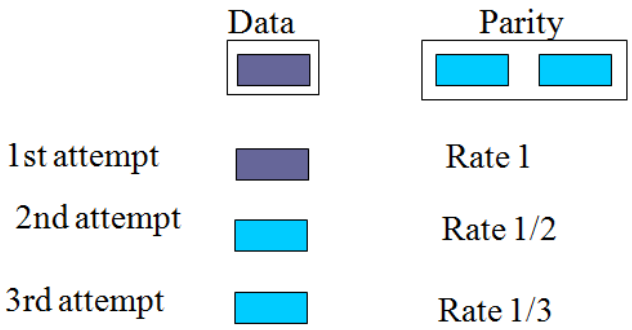

- Based on this coding, a data rate of 8 x 59.2 = 473kbps can be achieved
- Though GMSK is more robust but 8-PSK gives more throughput
- However increased data rate comes at the price of decreased sensitivity of the system. This has impact on coverage and in turn network planning
- Another advantage in EDGE is that switching between different coding schemes takes place easily i.e. data block can be sent with better protection on failure
- not possible in GPRS to switch to different coding scheme on reception failure, retransmission uses the same protection as for its initial transmission

**Link Adaptation and Incremental Redundancy**

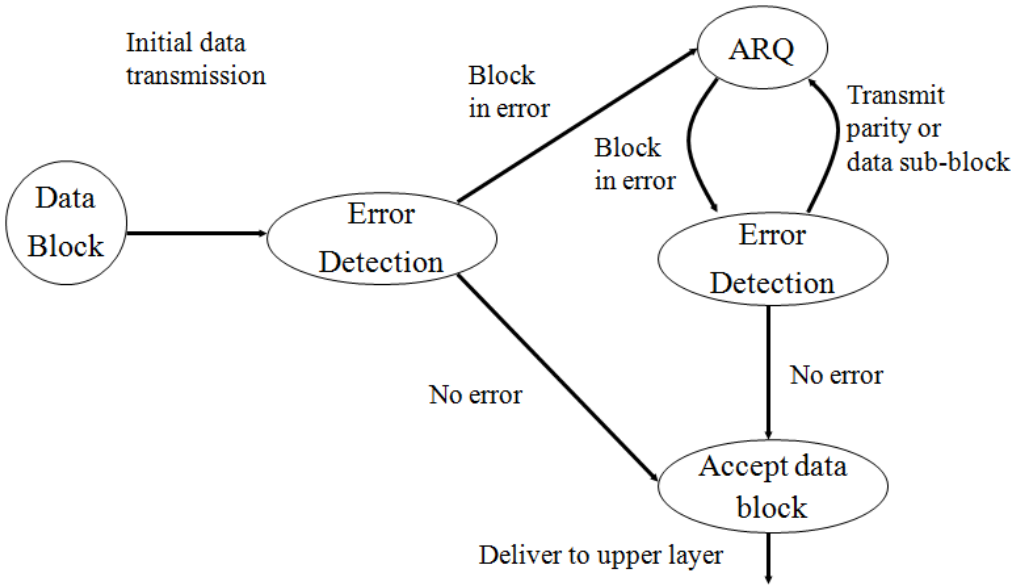
- Link Adaptation (LA)
  - ✓ As propagation condition changes, quality of signal changes → MCS changes all the time
  - ✓ LA is used for maximizing the throughput per channel by changing the coding scheme
  - ✓ LA algorithms are based on bit error probability (BEP) measurements
- Incremental redundancy
  - ✓ Improves the throughput and is done by automatically adapting the transmitted redundancy to the channel conditions
  - ✓ Achieved through ARQ and FEC

**Incremental Redundancy (IR)**

- Send redundancy *only if* necessary
- Generalized Type-II ARQ
- Finer granularity of code rate
- Example




**State Diagram for IR**

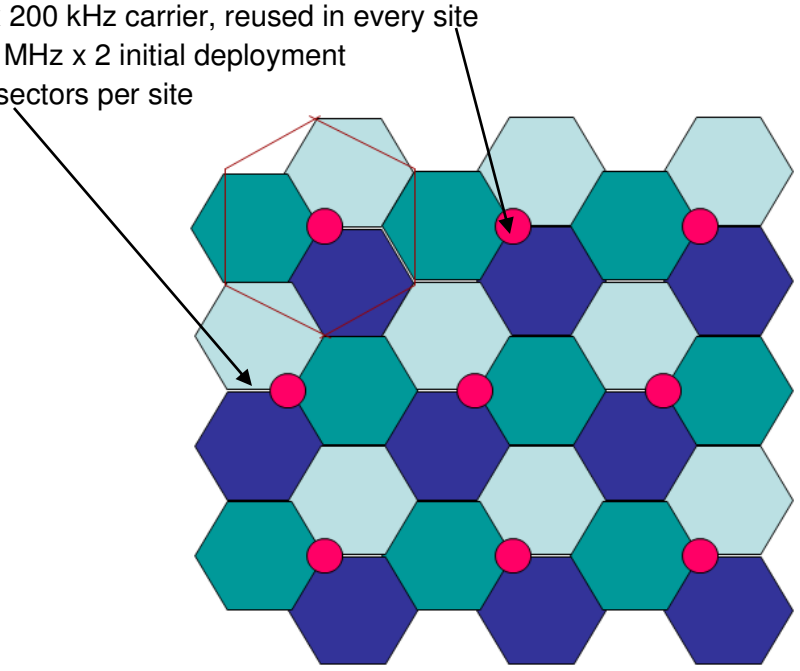


**Capacity Planning in EDGE**

- Similar to GPRS but high throughput per radio time slot changes some aspects of planning
- The reuse pattern defines the number of cells in a cluster using different frequencies.
- A frequency reuse of 3/9 means that each f is used only once in three sites/cluster, wherein each site is three sectored
- Reuse for control and reuse for traffic channels are independent of each other
- The actual reuse employed - for traffic or control - is operator controlled and limited only by the available spectrum
- Typically, 4/12 is used for control and 1/3 for traffic. However, other combinations are also possible subject to performance requirements, environment and spectrum availability.
- Higher the f reuse, higher the throughput and less delay
- Time slot capacities have dynamic range depending on users.

**1/3 Frequency Re-use (EDGE Compact)**

- 3 x 200 kHz carrier, reused in every site
- <1MHz x 2 initial deployment
- 3 sectors per site



- EDGE-capable and non-EDGE-capable TRX in a one sector can be configured to have only one BCCH
- TBF parameter setting makes it possible for TBFs of GPRS and EDGE radio network to be multiplexed dynamically on one time slot
- However this should be avoided as the performance suffers in both the uplink and downlink
  - ✓ In UL, GPRS suffers due to large amount of 8-PSK retransmissions.
  - ✓ In DL, it is due to GMSK modulation where 8-PSK can carry higher data rate for EDGE

**Dynamic Abis in EDGE**

- Interface between BS and BSC
- However voice signals are still carried in 16 kbps Abis channels and static for GSM/GPRS
- 8-PSK changes data rate from 8.8 kbps to 59.2 kbps, which is insufficient for data beyond MCS2
- This data rate is not always there and so dynamic Abis concept is used in EDGE
- BSC allocates Abis capacity from dynamic Abis pool (DAP) for data calls from EGPRS when needed

**Benefits**

- For Operators
  - ✓ Migration to wireless multimedia services
  - ✓ Improved customer satisfaction
  - ✓ Possibility of early market deployment of third generation type applications
- For Users
  - ✓ Improved quality of service
  - ✓ Personal multimedia services
  - ✓ Potentially lower price per bit

**Summary**

- Walsh Codes
- IS-95 Reverse Link
- EDGE Introduction
- Modulation and Coding Schemes
- Link Adaptation and Incremental Redundancy
- Capacity Planning
- Dynamic Abis pool
- Next Lecture
  - ✓ WCDMA

# Lecture 21
# WCDMA (Part I)

## Outlines

- Last Lecture review
- UMTS
- Service Classes in UMTS
- UTRAN Architecture
- Radio Interface protocol Architecture
- Protocol Models for UTRAN
- Logical Channels

## Last Lecture Review

- Walsh Codes
- IS-95 Reverse Link
- EDGE Introduction
- Modulation and Coding Schemes
- Link Adaptation and Incremental Redundancy
- Capacity Planning
- Dynamic Abis pool

## UMTS

- UMTS networks have predominance of data traffic unlike GSM networks.
- The data rate will be significantly higher than that offered by GSM / GPRS / EDGE
- 3G networks serve different purpose and thus the major changes from previous networks are
  - ✓ Max user data rate up to 384 kbps
  - ✓ Efficient handover between different operators and technologies e.g. GSM and UMTS
  - ✓ Ability to deliver at requested bandwidth
  - ✓ Ability to deliver different services with the required quality

## WCDMA Radio Fundamentals

- WCDMA has emerged as most preferred and adopted technology for 3G air interface
- The major differences between WCDMA and GSM are:
  - ✓ 5 MHz channel bandwidth as compared to 200 KHz in GSM
  - ✓ Packet data scheduling is load based unlike time slot based in GSM
  - ✓ Theoretically only one f channel, while GSM uses many channels
  - ✓ Quality control is done using RRM algorithm, while it was done by implementing frequency planning techniques in GSM.
  - ✓ Users/cell/channel are separated by codes unlike time or frequency in GSM

## Service classes in UMTS

- In 3G network, ME will be able to establish multiple connections simultaneously.
- Network allows efficient cooperation between application with diverse quality of service requirements.
- The quality can be defined by two main parameters
  - ✓ Guaranteed and max bit rate possible (kbps)
  - ✓ Permissible delay (ms)
- Based on the QoS criteria, multimedia services has been further classified
  - ✓ Conversational

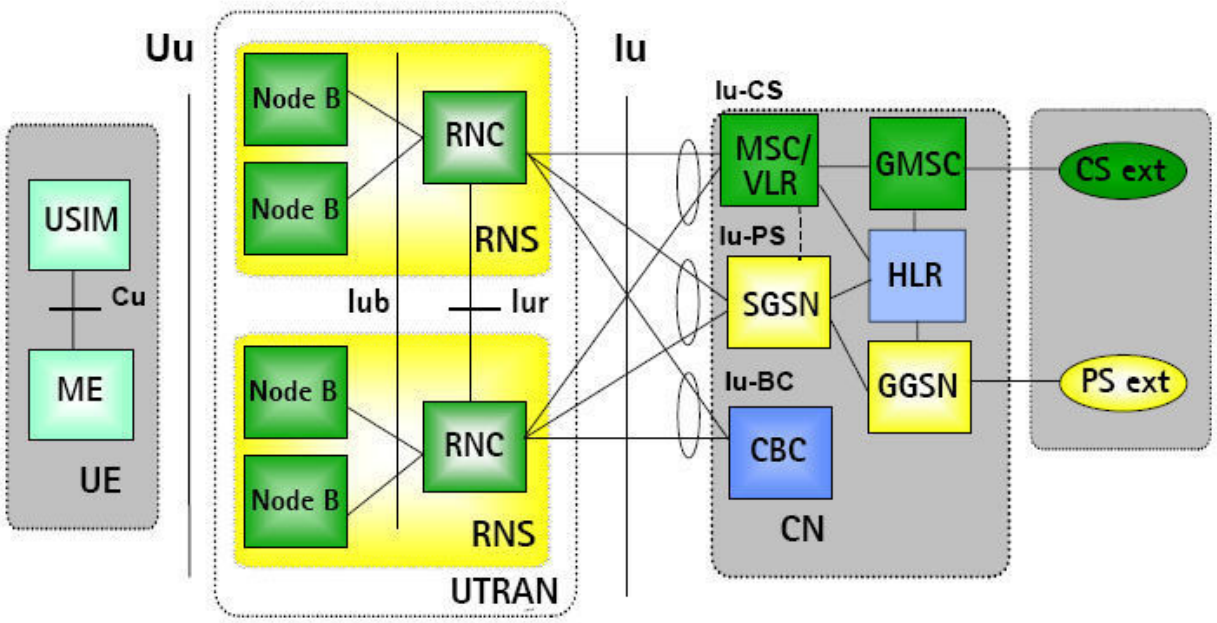
- The most delay sensitive, e.g. applications video telephony, VoIP

✓ Streaming
- Flow which is steady and continuous, it is server to user

✓ Interactive
- Web browsing is an example. A user may request timetables of buses, trains or flight schedule

✓ Background
- Short messages, file transfer, email that has least stringent requirements of QoS

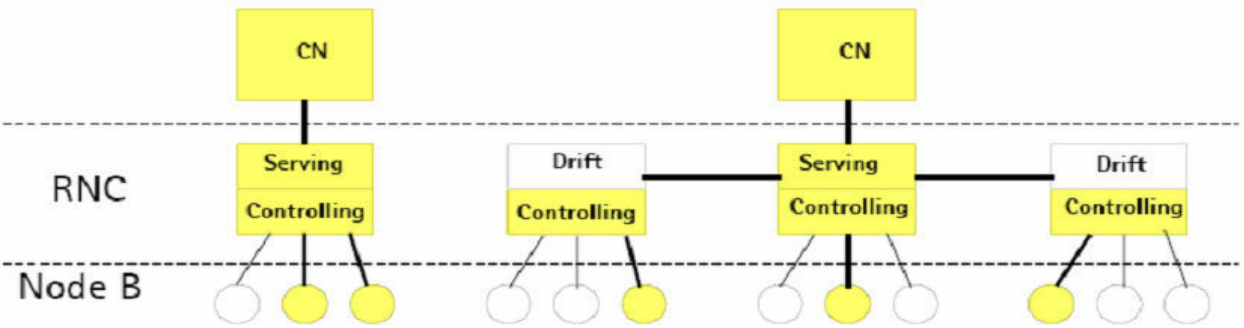
**UTRAN and System Architecture**



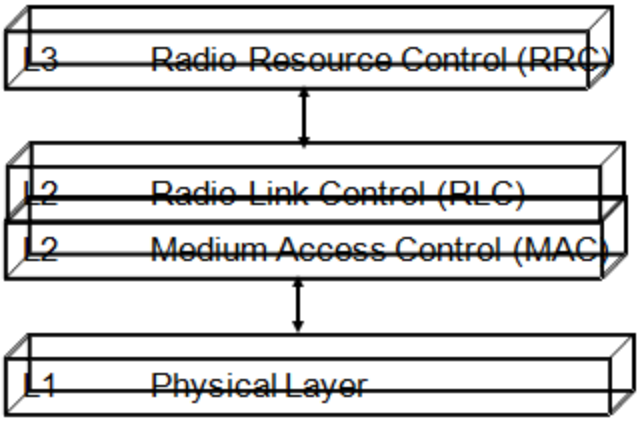

- USIM contains authentication information and associated algorithms, encryption and subscriber related information
- ME is user independent
- BS
  - ✓ Also known as node B in WCDMA and is more complex than BS in GSM
  - ✓ Its functions include handover channel management, baseband conversion, channel encoding and decoding, interfacing to other network elements

**Radio Network Controller**

- Concerning one connection between UTRAN and one UE, the following roles of RNCs exist:
  - ✓ Serving RNC that controls the connections to a UE
  - ✓ Drift RNC that lends its resources of Serving RNC for a particular UE
- Each RNC also has the controlling RNC role towards its Node Bs




**Radio Interface protocol architecture**




- Layer 1
  - ✓ The actual medium of transfer
  - ✓ The main functions of this layer include RF processing, modulation/demodulation, multiplexing / demultiplexing of physical channels
  - ✓ Error detection and correction, rate matching, power control, synchronization etc
- Layer 2
  - ✓ It has two main sub-layer
    - RLC
    - MAC
- MAC
  - ✓ Responsible for mapping logical channels to the transport channels
  - ✓ An interface between L1 & L3 and provides packet multiplexing / demultiplexing
  - ✓ Measurement related to traffic volume on logical channels and reporting to layer 3
- RLC
  - ✓ Segmentation reassembly of variable size data packets
  - ✓ Error correction by retransmission and ACKed data transfer mode
  - ✓ Controlling rate flow, concatenation, cyphering and preservation of higher-order PDUs
  - ✓ Operates in three mode as in GPRS

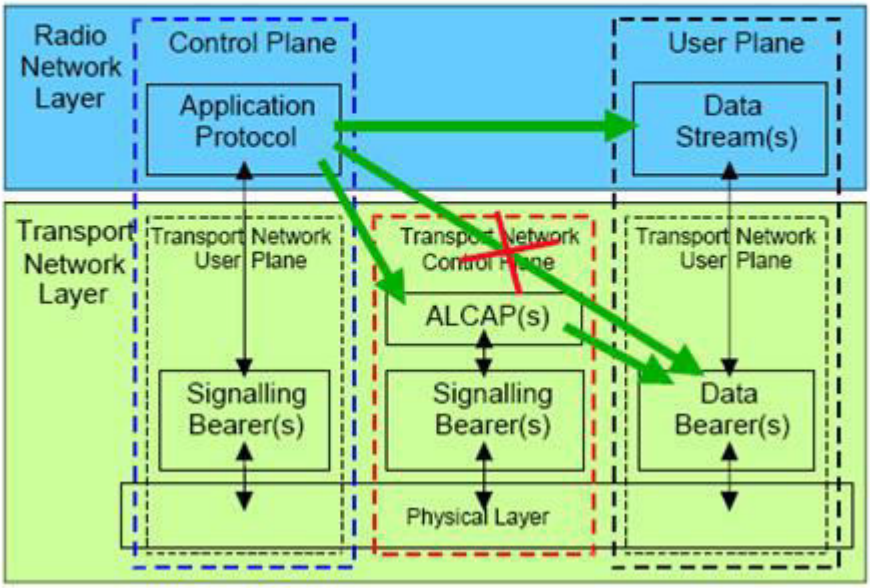
- Layer 3
  - ✓ Contains sub-layers but RRC is the one that interact with layer 2
  - ✓ Handles control plane signaling between UE and network in connected mode
  - ✓ Responsible for bearer functions like establishment, release, maintenance and reconfiguration in the user plane and of radio resources in control plane
  - ✓ Functions of RRC include radio resource management and mobility management, as well as power control, routing and paging
- Two other layers
  - ✓ Packet data convergence protocol (PDCP)
    - Major functions being compression of PDU at transmitting end and decompression at receiving end in all of three modes of RLC.
  - ✓ Broadcast – Multicast Control (BMC)
    - Functions only in transparent and unACKed modes providing broadcast/multicast scheduling and transmission of user data.

**Protocol Model for UTRAN**

- UTRAN protocol structure is based this model

For all signaling activities in the network, it includes RANAP, RNSAP, NBAP protocols

Trans. Of all user-specific data CS or PS through user plan



**Logical Channels in WCDMA**

| Channel | Abb. | Functionality |
|---|---|---|
| Broadcast Common Control channel (DL) | BCCH | Transmits the system control information |
| Common Control channel (UL/DL) | CCCH | Used (usually by UE) for transmitting info related to control between network and UE |
| Common Traffic Channel (DL) | CTCH | Used to transmit dedicated info to a group of UEs |
| Dedicated Control Channel (UL/DL) | DCCH | Dedicated channel for control related information between UEs and network |
| Dedicated Traffic Channel (UL/DL) | DTCH | Similar to DCCH except that it is used for user information |
| Paging Control channel (DL) | PCCH | Used to page info the UE |

**Summary**

- UMTS
- Service Classes in UMTS
- UTRAN Architecture
- Radio Interface protocol Architecture
- Protocol Models for UTRAN
- Logical Channels
- Next Lecture
  - ✓ WCDMA

**Lecture 22**
**WCDMA (Part II)**

**Outlines**

- Last Lecture Review
  - ✓ Spreading and Scrambling
  - ✓ Transport Channels
  - ✓ Physical Channels
    - UL Dedicated
- Signalling
- Physical Layer Procedures
  - ✓ RACH Operation
  - ✓ Cell Searching
  - ✓ Power Control
    - Open Fast loop
    - Closed Loop

**Last Lecture Review**

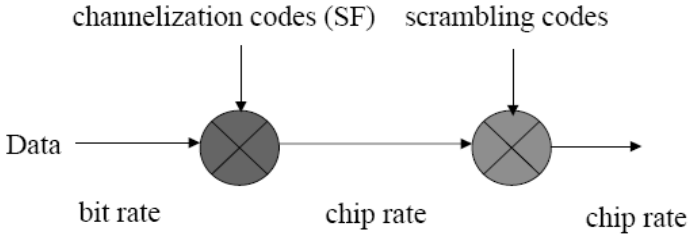
- Last Lecture review
- UMTS
- Service Classes in UMTS
- UTRAN Architecture
- Radio Interface protocol Architecture
- Protocol Models for UTRAN
- Logical Channels

**Air interface parameters**

| | |
|---|---|
| Carrier Spacing | 5 MHz (nominal) |
| Chip Rate | 3.84 Mcps |
| Frame Length | 10 ms (38400 chips) |
| No. of slots / frame | 15 |
| No. of chips / slot | 2560 chips (Max. 2560 bits) |
| Uplink SF | 4 to 256 |
| Downlink SF | 4 to 512 |
| Channel Rate | 7.5 Kbps to 960 Kbps |

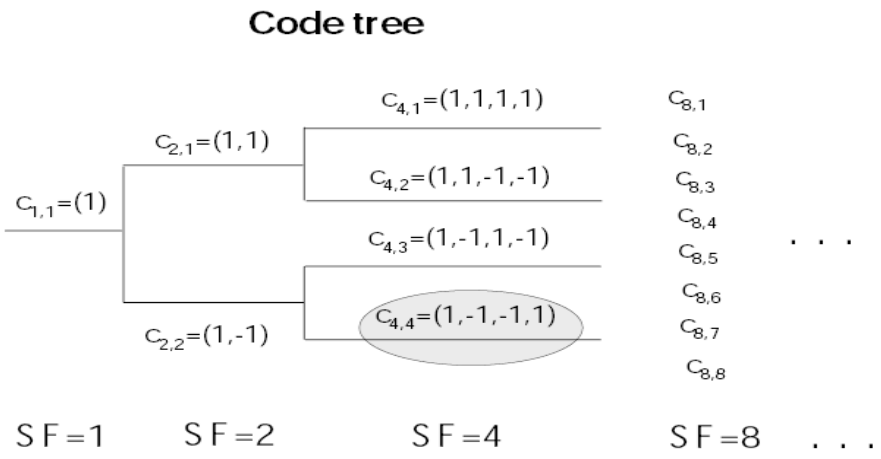
**Spreading and Scrambling**

- Spreading means increasing the signal bandwidth
- Strictly speaking, spreading includes two operations:
  - ✓ Channelization (increases signal bandwidth) - using orthogonal codes
  - ✓ Scrambling (does not affect the signal bandwidth) - using pseudo noise



**Channelization**

- Channelisation codes are orthogonal codes, based on Orthogonal Variable Spreading Factor (OVSF) technique
- The codes are fully orthogonal, i.e., they do not interfere with each other, only if the codes are time synchronized
- Thus, channelization codes can separate the transmissions from a single source
- In the downlink, it can separate different users within one cell/sector
- Limited orthogonal codes must be reused in every cell
  - ✓ Problem: Interference if two cells use the same code
  - ✓ Solution: Scrambling codes to reduce inter-base-station interference
- It is possible that two mobiles are using the same codes.
- In order to separate different users in the uplink, scrambling codes are used.
- One code tree is used with one scrambling code on top of the tree.
-

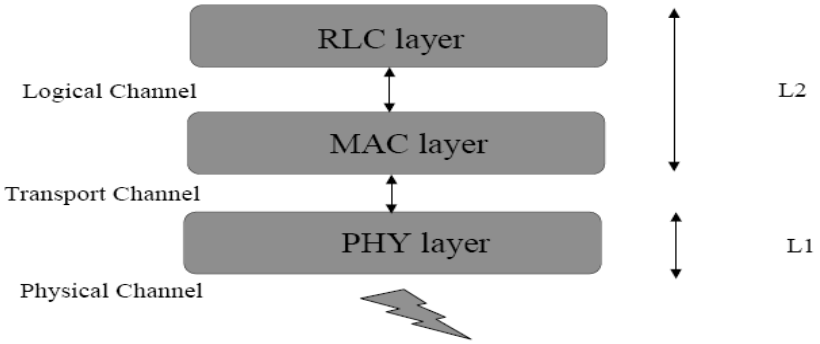



**Scrambling**

- In the scrambling process the code sequence is multiplied with a pseudorandom scrambling code.
- The scrambling code can be a long code (a Gold code with 10 ms period) or a short code (S(2) code).
- In the downlink scrambling codes are used to reduce the inter-basestation interference. Typically, each Node B has only one scrambling code for UEs to separate base stations. Since a code tree under one scrambling code is used by all users in its cell, proper code management is needed.

**Channel Concept**

- Three separate channels concepts in the UTRA: logical, transport, and physical channels.
  - ✓ Logical channels define what type of data is transferred.
  - ✓ Transport channels define how and with which type of characteristics the data is transferred by the physical layer.
  - ✓ Physical data define the exact physical characteristics of the radio channel.




**Transport Channels -> Physical Channels**

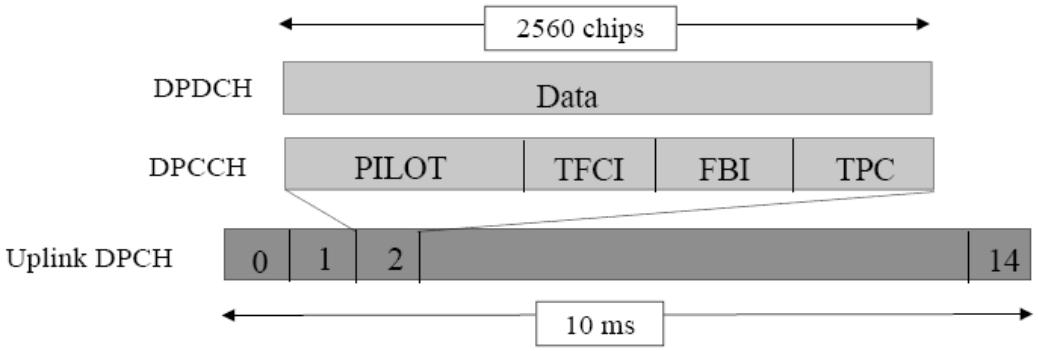
- Transport channels contain the data generated at the higher layers, which is carried over the air and are mapped in the physical layer to different physical channels.
- The data is sent by transport block from MAC layer to physical layer and generated by MAC layer every 10 ms.
- The transport format of each transport channel is identified by the Transport Format Indicator (TFI), which is used in the interlayer communication between the MAC layer and physical layer.
- Several transport channels can be multiplexed together by physical layer to form a single Coded Composite Transport Channel (CCTrCh).
- The physical layer combines several TFI information into the Transport Format Combination Indicator (TFCI), which indicate which transport channels are active for the current frame.
- Two types of transport channels: ***dedicated*** channels and ***common*** channels.
  - ✓ Dedicated channel –reserved for a single user only.
    - Support fast power control and soft handover.
  - ✓ Common channel – can be used by any user at any time.
    - Don't support soft handover but some support fast power control.
- In addition to the physical channels mapped from the transport channels, there exist physical channels for *signaling* purposes to carry only information between network and the terminals.

| **Transport Channel** | **Physical Channel** |
|---|---|
| (UL / DL) Dedicated channel **DCH** | Dedicated physical data channel **DPDCH**<br>Dedicated physical control channel **DPCCH** |
| (UL) Random access channel **RACH** | Physical random access channel **PRACH** |
| (UL) Common packet channel **CPCH** | Physical common packet channel **PCPCH** |
| (DL) Broadcast channel **BCH** | Primary common control physical channel **P-CCPCH** |
| (DL) Forward access channel **FACH**<br>(DL) Paging channel PCH | Secondary common control physical channel **S-CCPCH** |

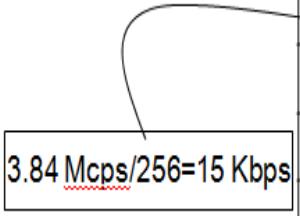
| | |
|---|---|
| (DL) Downlink shared channel **DSCH** | Physical downlink shared channel **PDSCH** |
| **Signaling physical channels** | Synchronization channel **SCH** |
| | Common pilot channel **CPICH** |
| | Acquisition indication channel **AICH** |
| | Paging indication channel **PICH** |
| | CPCH Status indication channel **CSICH** |
| | Collision detection / Channel assignment indicator channel **CD** / **CS-ICH** |

**UL Dedicated Channel DCH**

- Due to audible interference to the audio equipment caused from the discontinuous UL transmission, two dedicated physical channels are
  - ✓ Dedicated Physical Control Channel (DPCCH)
  - ✓ Dedicated Physical Data Channel (DPDCH)
- code multiplexing instead of time multiplexing to overcome discontinuous transmission (DTX) .
- Dedicated Physical Control Channel (DPCCH) has a fixed spreading factor of 256 and carries physical layer control information.
- DPCCH has four fields: Pilot, TFCI, FBI, TPC.
  - ✓ Pilot – channel estimation + SIR estimate for PC
  - ✓ TFCI – bit rate, channel decoding, interleaving parameters for every DPDCH frame
  - ✓ FBI (Feedback Information) – transmission diversity in the DL
  - ✓ TPC (Transmission Power Control) – power control command




- Dedicated Physical Data Channel (DPDCH) has a spreading factor from 4 to 256 and its data rate may vary on a frame-by-frame basis informed on DPCCH channel.
- Parallel channel codes can be used in order to provide 2 Mbps user data

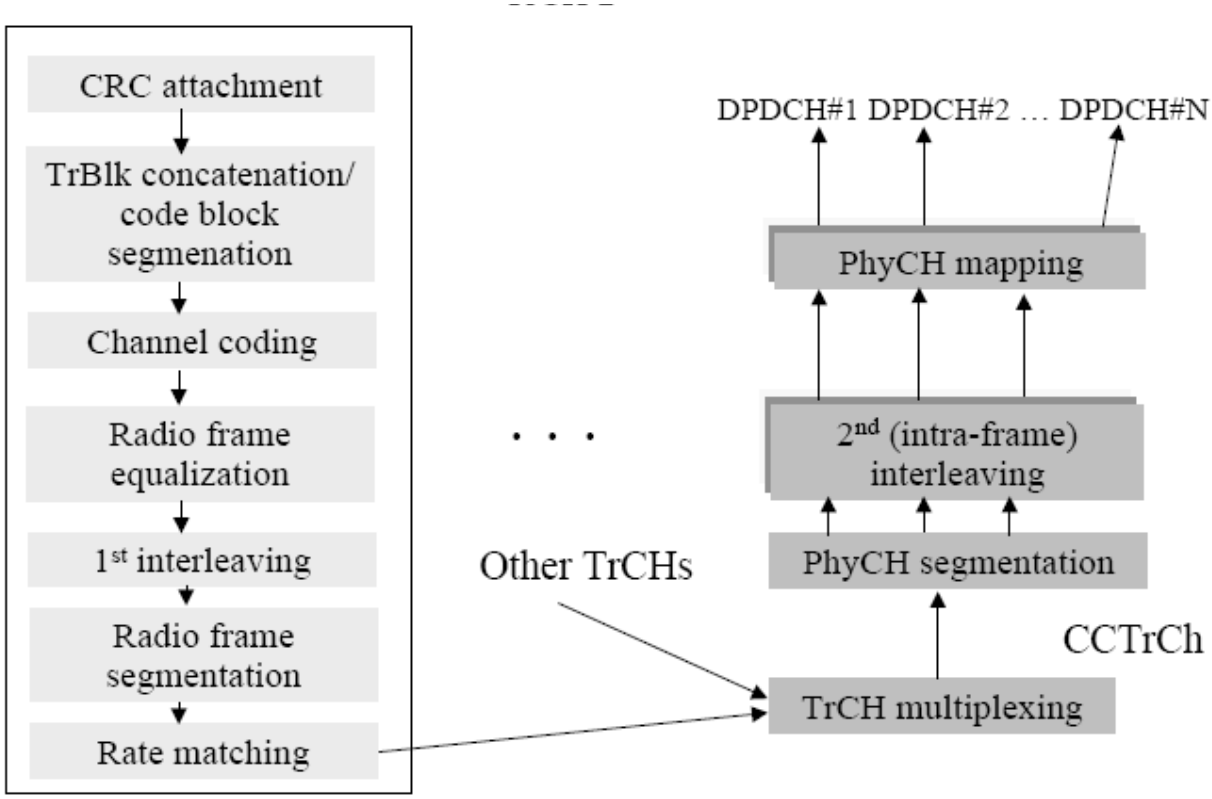



| DPDCH SF | DPDCH channel bit rate (Kbps) | Max. user data rate with ½ rate coding (approx.) |
|---|---|---|
| 256 | 15 | 7.5 Kbps |
| 128 | 30 | 15 Kbps |
| 64 | 60 | 30 Kbps |
| 32 | 120 | 60 Kbps |
| 16 | 240 | 120 Kbps |
| 8 | 480 | 240 Kbps |
| 4 | 960 | 480 Kbps |
| 4, with 6 parallel codes | 5740 | 2.3 Mbps |

**UL receiver in BS**

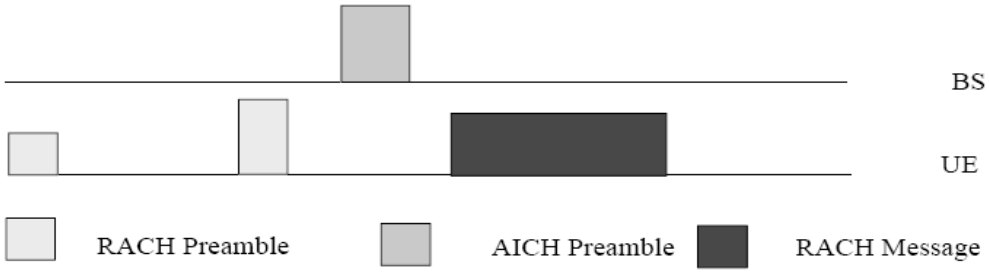
- It performs following
  - ✓ Start receiving the frame, de-spreading DPCCH and buffering the DPDCH according to max bit rate corresponding to the smallest spreading factor
  - ✓ For every slot
    - Obtain channel estimate using pilot bits and estimate SIR
    - Send TPC command in DL to UE to control UL tx power
    - Decode TPC bit in every slot and adjust DL power for that UE
  - ✓ For every 2nd or 4th slot
    - Decode FBI bits, if present in 2 or 4 slots and adjust antenna phases and amplitude for transmission diversity
  - ✓ For every 10 ms frame
    - Decode TFCI information from DPCCH frame to obtain bit rate
  - ✓ For transmission time interval (TTI) of 10, 20, 40 or 80 ms, decode DPDCH data

**UL Multiplexing and Channel Coding Chain**




**RACH Operation**

- First, UE sends a preamble.
- The SF of the preamble is 256 and contain a signature sequence of 16 symbols – a total length of 4096 chips.
- Wait for the acknowledged with the Acquisition (AICH) from the BS.
- In case no AICH received after a period of time, the UE sends another preamble with higher power.
- When AICH is received, UE sends 10 or 20 ms message part.
- The SF for the message is from 32 to 256.

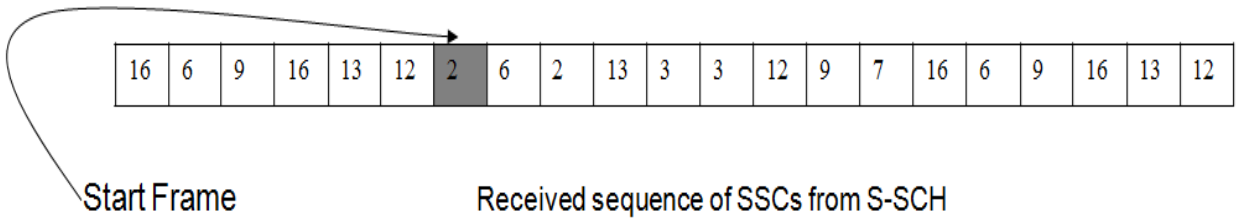


**Synchronisation Channel (SCH) – Cell Searching**

- Cell search using SCH has three basic steps:
  - ✓ The UE searches the 256-chip primary synchronisation code, which is common to all cells and is the same in every slot. Detect peaks in the output of the filter corresponds to the slot boundary (slot synchronisation).
  - ✓ The UE seeks the largest peak secondary synchronisation code (SSC). There are 64 unique SSC sequences. Each SSC sequence has 15 SSCs. The UE needs to know 15 successive SSCs from the S-SCH, then it can determine the code group in order to know the frame boundary (frame synchronisation).
  - ✓ Each code group has 8 primary scrambling. The correct one is found by each possible scrambling code in turn over the CPICH of that cell.

**SSC Sequence**

| Secondary Synchronization Code (SSC) and Code Group | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Code group | #0 | #1 | #2 | #3 | #4 | #5 | #6 | #7 | #8 | #9 | #10 | #11 | #12 | #13 | #14 |
| . . . | | | | | | | | | | | | | | | |
| 30 | 2 | 5 | 11 | 7 | 2 | 11 | 9 | 4 | 16 | 7 | 16 | 9 | 14 | 14 | 4 |
| 31 | 2 | 6 | 2 | 13 | 3 | 3 | 12 | 9 | 7 | 16 | 6 | 9 | 16 | 13 | 12 |
| 32 | 2 | 6 | 9 | 7 | 7 | 16 | 13 | 3 | 12 | 2 | 13 | 12 | 9 | 16 | 6 |
| . . . | | | | | | | | | | | | | | | |




**Power Control**

- Fast Closed Loop PC – Inner Loop PC
  - ✓ Feedback information.
  - ✓ Uplink PC is used for near-far problem. Downlink PC is to ensure that there is enough power for mobiles at the cell edge.
  - ✓ One PC command per slot – 1500 Hz
  - ✓ Two special cases for fast closed loop PC:

    - Soft handover: how to react to multiple power control commands from several sources. At the mobile, a “power down” command has higher priority over “power up” command.
    - Compressed mode: Large step size is used after a compressed frame to allow the power level to converge more quickly to the correct value after the break.
- Closed Loop PC - Outer Loop PC
    - ✓ Set the SIR target in order to maintain a certain frame error rate (FER). Operated at radio network controller (RNC).
- Open loop PC
    - ✓ No feedback information.

**Summary**

- Spreading and Scrambling
- Transport Channels
- Physical Channels
    - ✓ UL Dedicated
- Signalling
- Physical Layer Procedures
    - ✓ RACH Operation
    - ✓ Cell Searching
    - ✓ Power Control
        - Open Fast loop
        - Closed Loop

**Lecture 23**
**WCDMA (Part III)**

**Outlines**

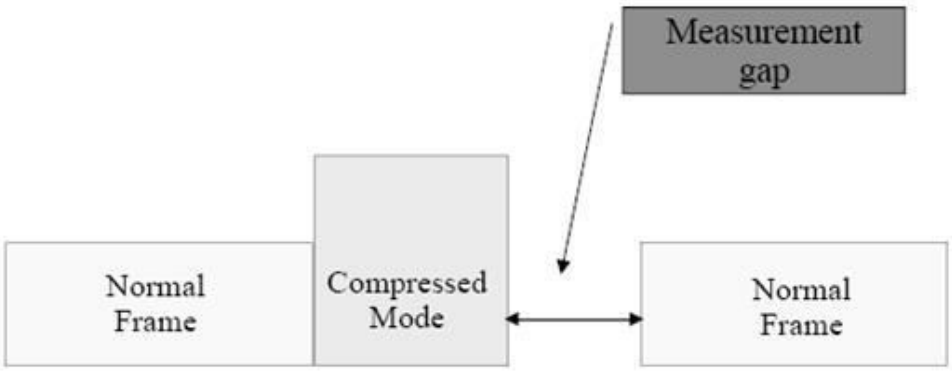
- Compressed mode measurements
- Handover measurements
  - ✓ -mode
  - ✓ Inter-mode
  - ✓ Inter-system
- WCDMA packet data access
- Transport channels for packet data
  - ✓ Common , dedicated, shared
- Packet scheduling algorithms
  - ✓ division scheduling
  - ✓ division scheduling
  - ✓ Transmission Power-based scheduling

**Last Lecture Review**

- Spreading and Scrambling
- Transport Channels
- Physical Channels
  - ✓ UL Dedicated
- Signalling
- Physical Layer Procedures
  - ✓ RACH Operation
  - ✓ Cell Searching
  - ✓ Power Control
    - Open Fast loop
    - Closed Loop

**Compressed Mode Measurements**

- The compressed mode is needed when making measurement from another frequency without full dual receiver terminal.
- The intention is not to loose data but to compress
- The transmission and reception are halted for a short time to perform measurements on the other frequencies.

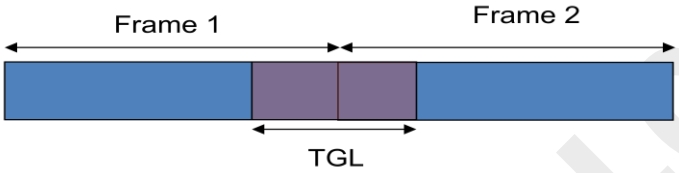



- Three methods for compressed mode:
  - ✓ Lowering the data rate from higher layers because they have knowledge of compressed mode schedule.
  - ✓ the data rate by changing the spreading factor.
  - ✓ Reducing the symbol rate by puncturing at the physical layer multiplexing chain but limited to rather short Transmission Gap Lengths (TGL).
- More power is needed during compressed mode.

- No power control during compressed mode. Large step size is used after a compressed frame to allow the power level to converge more quickly to the correct value after the break.

**Transmission Gap length (TGL)**

- The specified TGL are 3,4,7,10 and 14 slots
  - ✓ TGL lengths 3, 4 and 7 can be obtained with both single and double frame methods
  - ✓ TGL 10 or 14 only obtained with double frame method allowing minimizing the impact during a single frame.




  - ✓ Very short values of TGL (1 or 2) is excluded the hardware requires some time to switch to different frequency and not as much time for measurements
  - ✓ Link performance does not degrade much if the terminal is not at the cell edge since there is room to compensate with fast power control.

**Handover measurements**

- Intra-mode handover
  - ✓ Include soft handover, softer handover and hard handover.
- Inter-mode handover
  - ✓ Handover to the UTRA TDD mode.
- Inter-system handover
  - ✓ Handover to other system, such as GSM.

**Intra-Mode Handover**

- Rely on the Ec/No measurement performed from the CPICH.
- The quantities defined that can be measured by the terminal from CPICH are
  - ✓ Received Signal Code Power (RSCP): received power on one code after de-spreading
  - ✓ RSSI: wideband received power within channel b/w
  - ✓ Ec/No, representing RSCP/RSSI
- Additional information for soft handover purposes is the relative timing between the cells to allow coherent combining in the RAKE receiver, otherwise would be difficult to combine.
  - ✓ If cells are within 10ms window, the relative timing can be found from primary scrambling code phase
  - ✓ Otherwise terminals need to decode System Frame Number from primary CCPCH that takes time and may suffer errors.
  - ✓ The 10 ms window has no relevance when timing information provided in neighboring cells list.

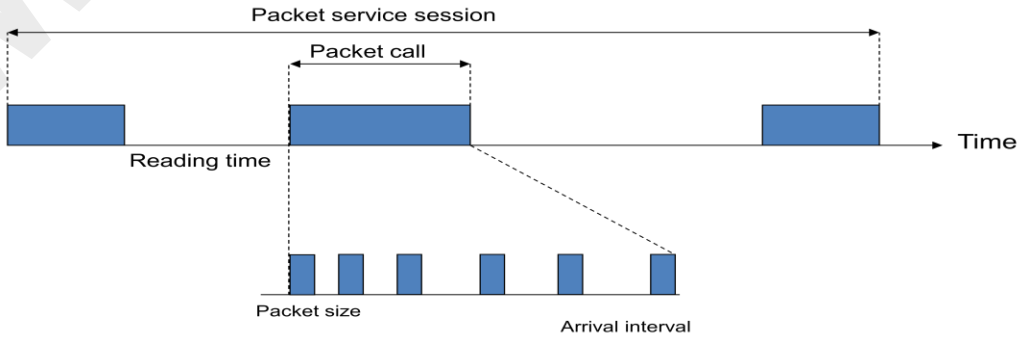
- For hard handover, timing info is not needed and different frequency measurements can be done with aid of compressed mode
- Dual mode FDD-TDD terminals operating in FDD measure power level from TDD cells available
- The TDD CCPCH bursts sent twice during 10ms frame can be used for measurement.
- Since TDD cells are synchronized, finding one slot means that other TDD cells have roughly same timing for their burst.
- Terminal receives GSM synch channel during compressed frames in UTRA FDD.
- GSM 1800 set special requirements for compressed model

**Packet Data Access**

- Four basic types of traffic classes
  - ✓ Conversational class -> real-time connection, performed between human users, really low delay, nearly symmetric, e.g., speech
  - ✓ Streaming class -> real-time connection, transferring data as a steady and continuous, low delay, asymmetric, e.g., video
  - ✓ Interactive class -> non-real-time packet data, response requested from other end-user, reasonable round-trip delay, e.g., Web browsing
  - ✓ Background class -> non-real-time packet data, no immediate action expected, less sensitive to delivery time, e.g. e-mail

**Types of Data Packet Traffic**

- Packet data traffic is a non-real-time packet services including Interactive and Background traffic classes. Their properties are
  - ✓ Packet data is bursty. Sometimes a large amount of data is transferred. At the other times no data is sent. Thus, the required bit rate can change rapidly.
  - ✓ Packet data tolerates longer delay than real-time services. It is controllable traffic from the RNC; thus, RNC can decide when and how to send the data.
  - ✓ Packets can be transmitted by the radio link control layer which provides retransmission and error correction services. Therefore, it allows high frame error rate with low transmission power.
- One example of packet data traffic is ETSI packet data model for web browsing.
- Characteristics of packet service session
  - ✓ Session arrival process, number of packet calls per session, reading time, number of packets within a call, inter-arrival time in a call, packet size



**WCDMA packet Access**

- In WCDMA packet allocations, e.g., time and bit rate, are controlled by the packet scheduler (PS) located in RNC. PS functions include:
  - ✓ Properly allocate the available resources (time, code or power) between the packet data users
  - ✓ Decide the allocated bit rates and the length of the allocation
  - ✓ Decide to use the transport channel
  - ✓ Monitor the packet allocations and the systems loads
- PS can allocate common, dedicated or shared channels to packet data users. It can also change the bit rate during active connection.
- PS can increase or decrease the network load by increasing or decreasing the bit rates of the packet bearers respectively.

**Transport Channels for Data Packet Access**

- Common channels - RACH in the uplink and FACH in the downlink
  - ✓ One or few RACH or FACH per sector
  - ✓ Low setup time
  - ✓ No feedback channel -> no fast closed loop power control, no soft handover, use fixed power
  - ✓ Poor link-level radio performance and generated more interference
  - ✓ Suitable for small data amounts
- Dedicated Channel - DCH in the uplink and downlink
  - ✓ Use fast power control and soft handover
  - ✓ Longer setup time
  - ✓ Up to 2 Mbps
  - ✓ Suitable for large data amounts
  - ✓ Not suitable for bursty data
  - ✓ In case of changing bit rate in the downlink, the downlink orthogonal code is reserved according to maximum bit rate.
- Shared Channel - uplink and downlink
  - ✓ A single orthogonal code is shared with many packet user with established DCH in time division manner - code efficient
  - ✓ Fast allocation and rate modification (frame-by-frame basis)
  - ✓ Suitable for large data amounts and bursty data
  - ✓ Use fast power control, but no soft handover

**Packet Scheduling Algorithms**

- In WCDMA packet scheduling algorithms can be done in two ways, in a time or code division manner.
- Time division scheduling
  - ✓ One user is allocated a channel at a time (10 ms frame)
  - ✓ All available capacity can be allocated to that user
  - ✓ High data rate for a short period of time

- Code division scheduling
  - ✓ Many users are allocated the channels simultaneously
  - ✓ Low data rate for a long period of time
  - ✓ Increase more users, each user's bit rate is decreased

**Time Division Scheduling**

- Advantages
  - ✓ High bit rate required less energy per bit
  - ✓ Less interference
  - ✓ Shorter delay due to high bit rate

**Code Division Scheduling**

- Advantages
  - ✓ Resources are in full usage due to longer transmission time
  - ✓ Small variation in interference level

**Transmission Power-based Scheduling**

- Users close to the BS requires less transmission power and can get a higher bit rate, whereas users at the cell edge could get lower bit rate
- Advantages
  - ✓ Minimize the average power sent per bit
  - ✓ Less interference
  - ✓ Increase the throughput
- Disadvantages
  - ✓ Accurate power estimation
  - ✓ Unfair resource allocation

**Summary**

- Compressed mode measurements
- Handover measurements
  - ✓ Intra-mode
  - ✓ Inter-mode
  - ✓ Inter-system
- WCDMA packet data access
- Transport channels for packet data
  - ✓ Common, dedicated, shared
- Packet scheduling algorithms
  - ✓ Time division scheduling
  - ✓ Code division scheduling
  - ✓ Transmission Power-based scheduling
- Next Lecture
  - ✓ cdma2000

**Lecture 24**
**CDMA2000**

**Outlines**

- Last lecture review
- Cdma2000 introduction
- New MAC and Physical layer features
- Physical layer of cdma2000
- Reverse Physical channels
- New Network elements in cdma2000
  - ✓ Packet Control Function (PCF)
  - ✓ Packet Data Serving Node (PDSN)
- Mobility Management
- Handoff
  - ✓ Intra-PCF
  - ✓ Inter-PCF/Intra-PDSN
  - ✓ Inter-PDS

**Last Lecture review**

- Compressed mode measurements
- Handover measurements
  - ✓ Intra-mode
  - ✓ Inter-mode
  - ✓ Inter-system
- WCDMA packet data access
- Transport channels for packet data
  - ✓ Common, dedicated, shared
- Packet scheduling algorithms
  - ✓ Time division scheduling
  - ✓ Code division scheduling
  - ✓ Transmission Power-based scheduling

**CDMA2000 Introduction**

- Provides seamless and evolutionary upgrade path for 2G and 2.5G cdma technology.
- Centers on original 1.25 MHz radio channel
- CDMA operators may seamlessly and selectively upgrade without changing entire BS equipment
- The first 3G cdma standard cdma2000 1xRTT using single channel (1x => multi-carrier)
- Cdma2000 1x
  - ✓ Supports data rate up to 307 kbps in packet mode
  - ✓ Can support up to twice as many users as 2G cdma
  - ✓ Cdma 1xEV-DO dedicates the channel strictly to data user and support 2.4 Mbps per channel.

**cdma2000**

- Cdma2000 3xRTT
  - ✓ The ultimate 3G solution relies upon multicarrier that gang adjacent channels together into 3.75 MHz.
  - ✓ Three non-adjacent channels may be operated simultaneously and in parallel.
  - ✓ Data rate in excess of 2 Mbps similar when compared to W-CDMA
- Advocates of cdma2000 claim their standard much more seamless and less expensive upgrade path when compared to W-CDMA.

**WCDMA vs. CDMA2000**

| Parameter | W-CDMA | cdma2000 |
|---|---|---|
| Carrier spacing | 5 MHz | 3.75 MHz |
| Chip rate | 4.096 MHz | 3.6864 MHz |
| Data modulation | BPSK | FW – QPSK; RV - BPSK |
| Spreading | Complex (OQPSK) | Complex (OQPSK) |
| Power control frequency | 1500 Hz | 800 Hz |
| Variable data rate implement. | Variable SF; multi code | Repet., puncturing, multi code |
| Frame duration | 10 ms | 20 ms (also 5, 30, 40) |
| Coding | Turbo and convolutional | Turbo and convolutional |
| Base stations synchronized? | Asynchronous | Synchronous |
| Base station acquisition/detect | 3 step; slot, frame, code | Time shifted PN correlation |
| Forward link pilot | TDM dedicated pilot | CDM common pilot |
| Antenna beam forming | TDM dedicated pilot | Auxiliary pilot |

- The new physical and MAC layer features and techniques
  - ✓ Link adaptation based on adaptive modulation, coding and spreading
  - ✓ Physical layer fast hybrid ARQ
  - ✓ Enhanced channel coding and turbo codes
  - ✓ Space and antenna diversity
  - ✓ Fast forward link power control and coherent uplink demodulation

**Physical Layer**

- The cdma2000 air interface is designed to provide flexible framework for supporting voice and other circuit-switched data as well as bursty packet data bearer services with different QoS
- cdma2000 supports RF channel band width of SRx1.25 MHz. currently SR 1 and 3 are supported and can be extended to 6, 9 and 12.
- A number of fixed and variable rate physical channels are defined with new variable-length spreading codes and PN codes.
- The data rate, channel encoding and modulation parameters are specified by radio configurations (RCs)
  - ✓ For SR 1 and 3, there are 7 RCs for reverse link and 9 for forward link

| *SR* | *Forward RC* | *Data Rate (Base, Peak)* | *Reverse RC* | *Data Rate (Base, Peak)* |
|---|---|---|---|---|
| SR1 | RC1 | 9.6 | RC1 | 9.6 |
| | RC2 | 14.4 | RC2 | 14.4 |
| | RC3 | 9.6, 153.6 | RC3 | 9.6, 307.2 |
| | RC4 | 9.6, 307.2 | | |
| | RC5 | 14.4, 230.4 | RC4 | 14.4, 230.4 |
| SR3 | RC6 | 9.6, 307.2 | RC5 | 9.6, 614.4 |
| | RC7 | 9.6, 614.4 | | |
| | RC8 | 14.4, 460.8 | RC6 | 14.4, 1036.8 |
| | RC9 | 14.4, 1036.8 | | |

- RC1 and RC2 are similar to Rate Set 1 and 2 in IS-95
- RCs are chosen such that base rate for a forward and a reverse link match. If RC3 is used on reverse link, either RC3 or RC4 can be used on forward

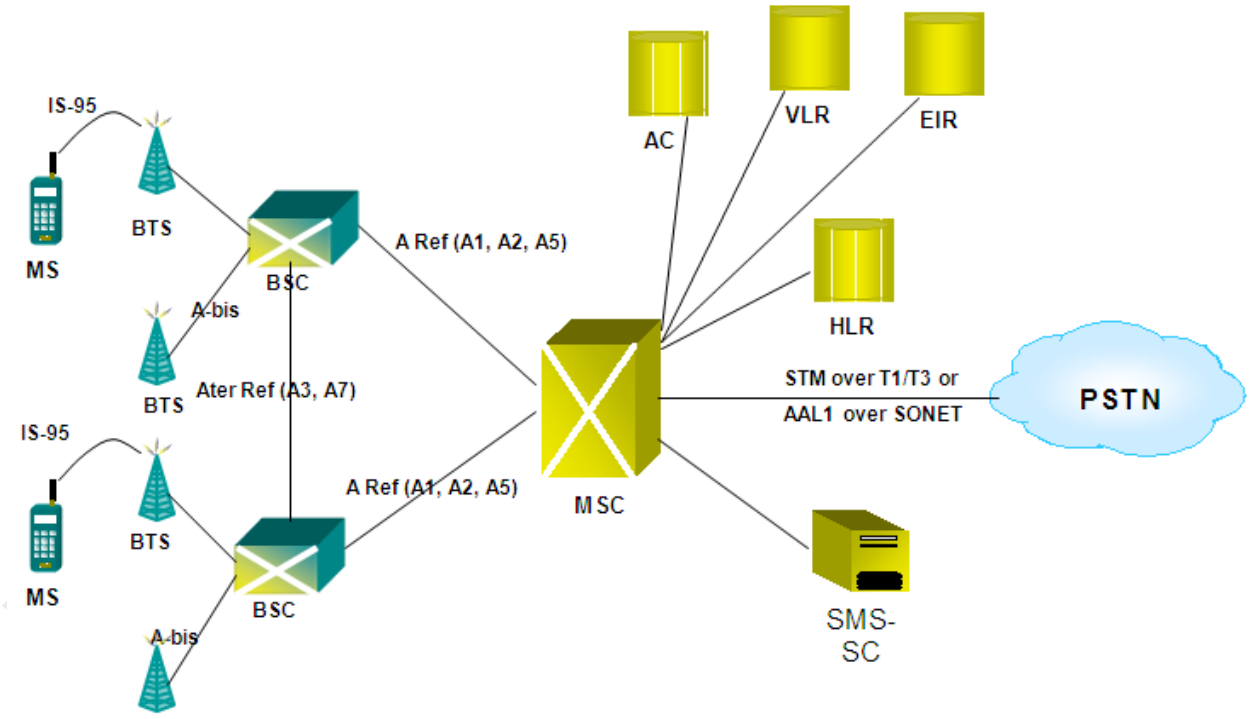
**Reverse Physical Channel**

| | Channel Type | Max SR1 | Max SR3 | |
|---|---|---|---|---|
| Common Channel | Reverse Pilot channel | 1 | 1 | Un-modulated SS signal by each MS, BS detect corresponding Uplink channel |
| | Reverse Access Channel | 1 | NA | For backward compatibility, used for uplink common control signaling |
| | Reverse Enhanced Access Channel | 1 | 1 | New channel used by MS to initiate communicate or respond to BS when no dedicated channel is assigned to user |

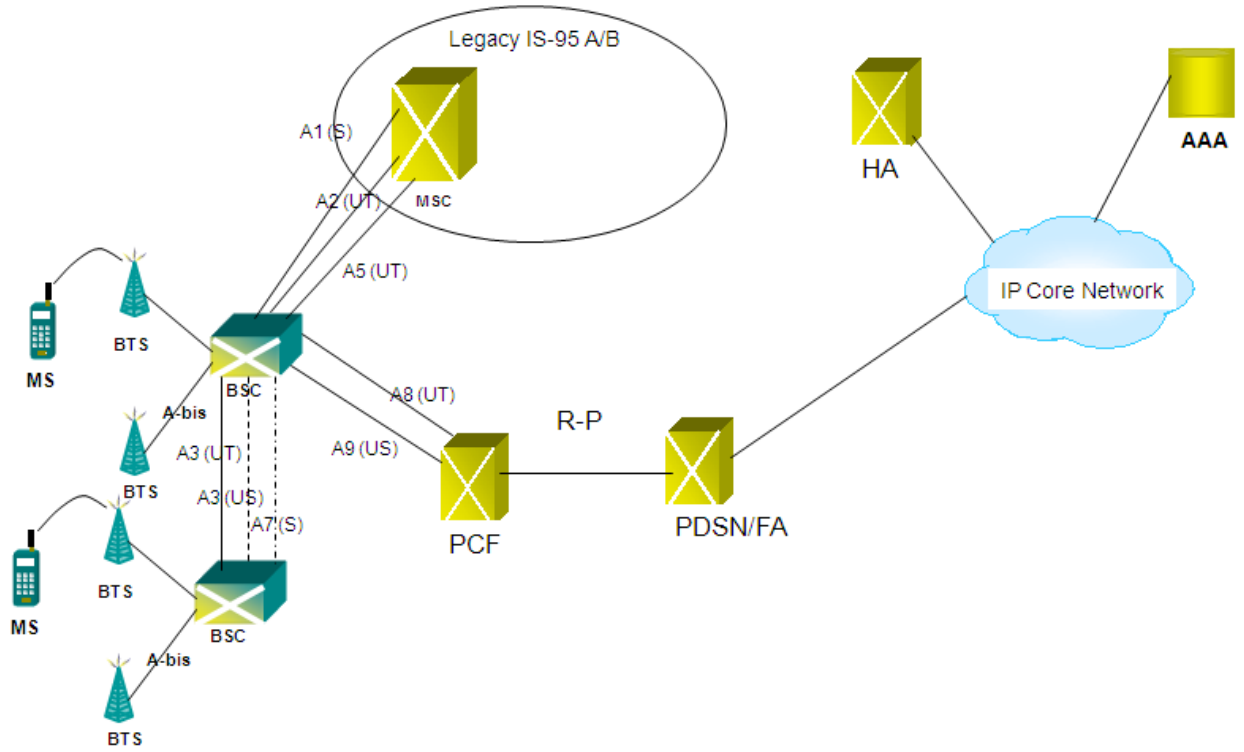
| | | | | |
|---|---|---|---|---|
| | Reverse Common Control Channel | 1 | 1 | Common channel used for short burst data and signaling messages when traffic channels are not in use |
| Dedicated Channel | Reverse Dedicated Control Channel | 1 | 1 | As before |
| | Reverse Fundamental Channel | 1 | 1 | Basic traffic channel that carries voice, low-rate data and associated signaling messages |
| | Reverse Supplemental Code Channel | 7 | NA | Fixed rate data only channel to provide higher transmission rate |
| | Reverse Supplemental Channel | 2 | 2 | Variable rate packet data channel carrying only high speed coded info |

**Legacy cdmaOne Network**

- Designed to support voice and low-rate circuit-switched traffic



**New Network elements in CDMA2000**




- MS: additional features to support data services and enhanced signaling messages to both circuit-switched and packet-switched
- BS (BTS & BSC): enhanced radio interface (significant hardware and software changes) to provide voice, data and multimedia traffic support
- Packet Control Function (PCF):
  - ✓ an entity that manages the buffering and relay the packets between BS and PDSN
  - ✓ Maintain radio resource status (e.g. active, dormant)
  - ✓ Collects radio link related accounting info to be used by AAA.
- Packet Data Serving Node (PDSN): new network entity
  - ✓ Acting as a FA by providing routing services (maintaining routing tables and route discovery) according to Mobile IP
  - ✓ Managing the radio-packet (R-P) interface and PPP sessions for MS
  - ✓ Initiating authentication, authorization and accounting for mobile user to the AAA server
  - ✓ When part of VPN, it can establish a tunnel through the public data network using layer 2 tunneling protocol (L2TP) to the VPN gateway.
  - ✓ PDSN may optionally use IPSec protocol to further protect the tunnel
- Home Agent
  - ✓ Network element within mobile's home network
  - ✓ Two major functions: mobile IP registration and packet forwarding

- ✓ HA interacts with AAA to receive mobile IP registration requests that have been authenticated and return registration response
- ✓ HA also forwards IP packets to and from current point of attachment through FA

- AAA
  - ✓ Authentication: verification of devices and subscribers for network access as well as user-based QoS requests
  - ✓ Authorization: whether a user or device is authorized for particular service with a specific QoS based on service profile. The requesting entity may cache the authorization info making further decision itself without going to AAA.
  - ✓ Accounting: involves collecting and storing billing-related data concerning the offered services. It includes session details (requested and offered QoS, duration of usage etc) and mobility records (dates and times of attach and detach etc)

**Mobility management for packet data services**

- When an MS originates a call
  - ✓ Messages are exchanged to establish and close an R-P connection between PCF/BSC and PDSN
  - ✓ Once serial connection established between MS and PDSN
    - MS and PDSN negotiate authentication protocol according to a challenge handshake authentication protocol (CHAP) or a password authentication protocol (PAP)
    - PDSN sends authentication response to AAA server, which decide to authenticate or not
    - PDSN constructs a network access identifier (NAI) of the form MSID@realm (realm of the home network)
    - The user is identified as a valid user and PDSN also knows which IP service template to apply to this subscriber
  - ✓ When PPP session is established, PDSN assigns the mobile an IP address from a pool of IP addresses
  - ✓ The routers in the packet network must be able to route any packet with this IP to the PDSN that provides service to the mobile

**Handoff**

- Intra-PCF
  - ✓ Supported by A8/A9 interfaces carrying user traffic and signaling between BS and PCF
- Inter-PCF and Intra-PDSN
  - ✓ On location change, must occur when causes to divert the packet data session from one R-P interface to another
  - ✓ New R-P connection between target PCF and serving PDSN is established and PPP session will be moved to this
  - ✓ Previous R-P session tear down
  - ✓ PCF-PCF handoff may occur while MS is in active or dormant state
  - ✓ Dormant handoff is supported to maintain PPP session, where a MS is dormant to minimize the use of air-link resources.

- ✓ During active session, PDSN supports low-latency handoff by bi-casting data to the target and previous PCF

- Inter-PDSN
  - ✓ A network based on simple IP does not support mobility beyond a PDSN coverage area because
    - New IP will be acquired from new PDSN and traffic on existing IP will be undeliverable.
    - Needs to support fast handoff i.e. Mobile IP
- Inter-PSDN Fast Handoff
  - ✓ The target PDSN initiates establishment of a P-P session with the serving PDSN.
  - ✓ P-P interface is used to keep PPP session anchored when PDSN to PDSN handoff is performed allowing existing PPP session to continue and reducing service interruption time and data loss

**Summary**

- Cdma2000 introduction
- New MAC and Physical layer features
- Physical layer of cdma2000
- Reverse Physical channels
- New Network elements in cdma2000
  - ✓ Packet Control Function (PCF)
  - ✓ Packet Data Serving Node (PDSN)
- Mobility Management
- Handoff
  - ✓ Intera-PCF
  - ✓ Inter-PCF/Intra-PDSN
  - ✓ Inter-PDSN

## Lecture 25
## 1st Review

**Last Lecture**

- Cdma2000 introduction
- New MAC and Physical layer features
- Physical layer of cdma2000
- Reverse Physical channels
- New Network elements in cdma2000
  - ✓ Packet Control Function (PCF)
  - ✓ Packet Data Serving Node (PDSN)
- Mobility Management
- Handoff
  - ✓ Intera-PCF
  - ✓ Inter-PCF/Intra-PDSN
  - ✓ Inter-PDSN

**Lecture 1 - Introduction Part I**

1. The Wireless vision
2. Radio Waves
3. Channel Capacity
4. Signal-to-Noise Ratio
5. EM Spectrum

**Lecture 1 - Introduction Part II**

- Wireless Transmission
  - ✓ Baseband signal, carrier frequency, fundamental frequency
  - ✓ antenna size must correspond to signal's wavelength
    - 1 MHz signal → few 100 m-s high antenna;
    - 1 GHz signal → few cm-s high antenna
- Encoding/Modulation
- Noises
  - ✓ Thermal, Intermodulation, Crosstalk, Impulse
- Losses/Gain

**Lecture 3 – Introduction Part III**

- Multiplexing
- Transmission Mediums
  - ✓ Guided, Unguided
- Propagation modes
  - ✓ Ground wave, Sky wave, LOS
- Multi-path propagation
  - ✓ Reflection, Diffraction, Scattering
- Fading

**Lecture 4 – Error part I**

- Transmission Errors
- Parity Check
- Cyclic Redundancy Check
- Block Error Code

**Lecture 5 – Error part II**

- Block Codes
  - ✓ Hamming
  - ✓ BCH (Generalization of Hamming)
  - ✓ Reed Solmon (Subclass of non-binary BCH)
- ARQ
  - ✓ Sliding window
  - ✓ Go-back-N

**Lecture 6 – Multiple Access (Part I)**

- FDMA
- TDMA
- CDMA
- Random Access
  - ✓ ALOHA
  - ✓ Slotted ALOHA
  - ✓ Reservation-based ALOHA

**Lecture 7 – Multiple Access (Part II)**

- CSMA
  - ✓ Versions of CSMA
  - ✓ CSMA/CA
  - ✓
- Spread Spectrum
  - ✓ Frequency Hoping
  - ✓ Direct Sequence

**Lecture 8 – Evolution Part I**

- 1G wireless cellular networks
  - ✓ NMT
  - ✓ AMPS
  - ✓ TACS
- 2G cellular systems
  - ✓ GSM
  - ✓ IS-136
  - ✓ PDC
  - ✓ IS-95

**Lecture 9 – Evolution Part II**

- 2.5G
  - ✓ HSCSD
  - ✓ GPRS
  - ✓ EDGE
  - ✓ IS-95B
- 3G
  - ✓ UMTS/W-CDMA
  - ✓ CDMA2000

**Specifications of 2.5G and 3G standards**

| Technology | Channel BW | Duplex | Infrastructure Changes | New Spectrum | New handsets |
|---|---|---|---|---|---|
| HSCSD | 200 KHz | FDD | Software upgrade at BS | No | Yes, New headsets provide 57.6 kbps on HSCSD and 9.6 kbps on GSM |
| GPRS | 200 KHz | FDD | New packet overlay at routers and gateways | No | Yes, new GPRS sets work at 171.2 kbps, 9.6 kbps on GSM, dual-mode. |
| EDGE | 200 KHz | FDD | New TX/Rx at BS, software upgrade at BS, controller | No | Yes, new set work at 384 kbps on EDGE, GPRS at 144 kbps and GSM at 9.6 kbps, tri-mode |
| W-CDMA | 5 MHz | FDD | Completely new BS | Yes | Yes, new handsets work at 2 Mbps in WCDMA and rest as above |
| IS-95B | 1.25 MHz | FDD | New software at BS | No | Yes, IS-95B at 64kbps, IS-95A at 14.4 kbps and IS-95 at 9.6 kbps |
| Cdma2000 1xRTT | 1.25 MHz | FDD | New software at backbone, new channel cards at BS, new packet service node | No | 1xRTT at 144 kbps and rest as above. Older sets will work. |
| Cdma2000 1xEV(DO/DV) | 1.25 MHz | FDD | New software and cards upgrade to 1xRTT | No | 1xEV at 2.4 Mbps and as above |
| Cdma2000 3xRTT | 3.75 MHz | FDD | Backbone modifications and channel cards at BS | May be | 3xRTT at 2 Mbps and rest as above |

**Lecture 10 Evolution III**

- Limitation of 3G
- 4G
  - ✓ Objectives
  - ✓ Issues
  - ✓ QoS
  - ✓ Security
  - ✓ Multimedia Service
  - ✓ Applications
- Convergence of Cellular and WLAN
- Billing Issue

**Quality of Service (QoS)**

- Traffic generated by the different services will not only increase traffic loads on the networks, but will also require different quality of service (QoS) requirements (e.g., cell loss rate, delay, and jitter) for different streams (e.g., video, voice, data).
- Providing QoS guarantees in 4G networks is a non-trivial issue where both QoS signaling across different networks and service differentiation between mobile flows will have to be addressed.

**Security**

- Security in wireless networks mainly involves authentication, confidentiality, integrity, and authorization for the access of network connectivity and QoS resources for the mobile nodes flow.
- The heterogeneity of wireless networks complicates the security issue.
- Dynamic reconfigurable, adaptive, and lightweight security mechanisms should be developed.
- AAA (Authentication Authorization Auditing) protocols provide a framework for such suffered especially for control plane functions and installing security policies in the mobile node such as encryption, decryption and filtering.

**Lecture 11 – Cell Conept part I**

- Cellular Concept
- Frequency Reuse
- Locating co-channel cells

**Lecture 12 – Cell Concept Part II**

- Channel Assignment Strategies
- Handoff Strategies
  - ✓ When to handoff
  - ✓ 1G, BS based
  - ✓ 2G or todays, Mobile-Assisted
- Prioritizing Handoff
  - ✓ Guard channels concept
  - ✓ Queuing handoff requests
- Practical handoff considerations
  - ✓ Umbrella cell
  - ✓ Cell dragging

**Lecture 13 – Cell Concept Part III**

- Interference and system capacity
  - ✓ Co-channel interference and capacity
  - ✓ Adjacent channel interference and capacity
- Channel Planning for Wireless System

**Lecture 14 – Cell Concept Part IV**

- Trunking and Grade of Service
  - ✓ Measuring Traffic Intensity
  - ✓ Trunked Systems
    - Blocked Calls Cleared
    - Blocked Calls Delayed
  - ✓ Erlang Charts
- Improving Coverage and Capacity
  - ✓ Cell Splitting
  - ✓ Sectoring
  - ✓ Repeaters for Range Extension
  - ✓ Microcell Zone Concept

**Lecture 15 - AMPS**

- AMPS introduction
- System Overview
- Call handling
- Air interface
- Supervisory signals
- N-AMPS

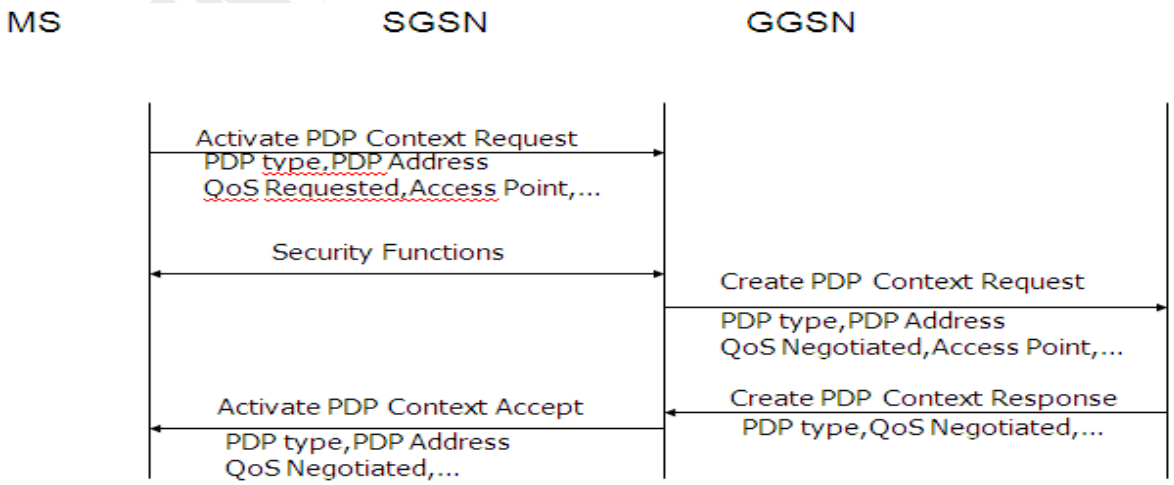
**Lecture 16 GSM**

- GSM Introduction
- GSM System Architecture
- GSM Network Areas
- Specifications
- Subscriber Services
- Mobility

**Lecture 17 – GPRS (part I)**

- Introduction to GPRS
- GPRS Architecture
- Registration and Session Management
- Routing Scenario in GPRS
- Channels Classificatio

**PDP Context Activation**



**Lecture 18 – GPRS part II**

- GPRS Protocol Architecture
  - ✓ MS – BSS
  - ✓ BSS – SGSN
  - ✓ SGSN – GGSN
  - ✓ GGSN – PDN
- GPRS Air Interface
- Data Routing and Mobility
- Uplink Data Transfer
- Downlink Data Transfer
- QoS in GPRS

**Lecture 19 - IS-95**

- IS-136
- CDMA/IS-95
- Advantages
  - ✓ Higher capacity, Improves voice quality (new coder),
  - ✓ Self-jamming, near-far problem,
  - ✓ IS-95 Forward Channels
  - ✓ Pilot Channel
- IS-95 Reverse Channels
  - ✓ Less power consumption (6-7 mW)
  - ✓ Privacy, graceful degradation
- Drawbacks
  - ✓ Sync Channel
  - ✓ Paging
  - ✓ Traffic

**Lecture 20 - EDGE**

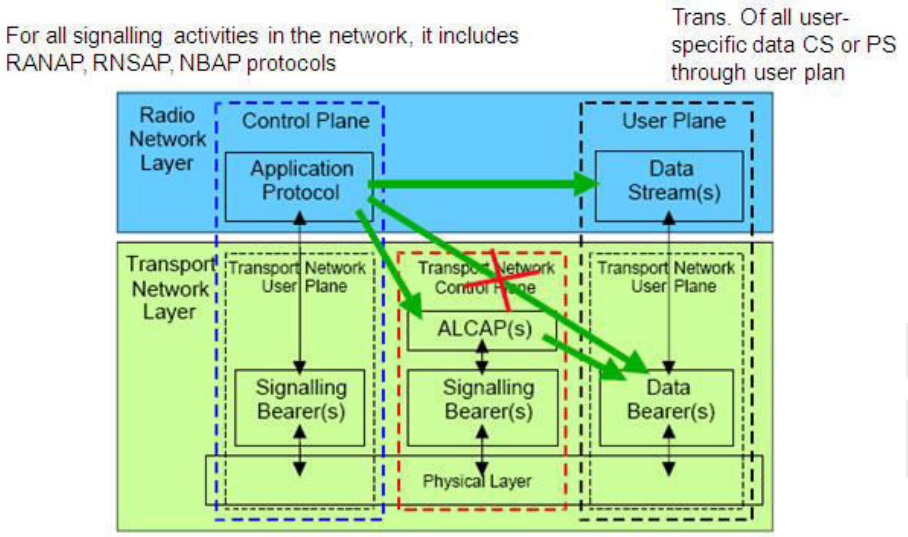
- EDGE Introduction
- Modulation and Coding Schemes
- Link Adaptation and Incremental Redundancy
- Capacity Planning

**Lecture 21 – UMTS / WCDMA part I**

- UMTS
- Service Classes in UMTS
  - ✓ Conversational, Streaming, Interactive, Background
- UTRAN Architecture
  - ✓ RNC (Serving, Drifting)
- Radio Interface protocol Architecture
- Protocol Models for UTRAN
- Logical Channels

**Protocol Model for UTRAN**

- UTRAN protocol structure is based this model




**Lecture 22 - WCDMA Part II**

- Spreading and Scrambling
- Channel Concept
  - ✓ Logical Channel (RLC) ->Transport Channels (MAC)->Physical Channels (PL)
- Physical Layer Procedures
  - ✓ RACH Operation (Preamble of 16 symbols and wait for ACK on AICH)
  - ✓ Cell Searching (256 chip primary Synch, 15 SSCs
  - ✓ Power Control
    - Fast Closed loop (1500 Hz TPC,
    - Closed Loop

**Lecture 23 - WCDMA Part III**

- Compressed mode measurements
- Handover measurements
  - ✓ Intra-mode
  - ✓ Inter-mode
  - ✓ Inter-system
- WCDMA packet data access
- Transport channels for packet data
  - ✓ Common, dedicated, shared
- Packet scheduling algorithms
  - ✓ Time division scheduling
  - ✓ Code division scheduling
  - ✓ Transmission Power-based scheduling

**Lecture 24 - CDMA2000**

- New MAC and Physical layer features
- Physical layer of cdma2000
- Reverse Physical channels
- New Network elements in cdma2000
  - ✓ Packet Control Function (PCF)
  - ✓ Packet Data Serving Node (PDSN)
- Mobility Management
- Handoff
  - ✓ Intra-PCF
  - ✓ Inter-PCF/Intra-PDSN
  - ✓ Inter-PDSN

**Lecture 26**

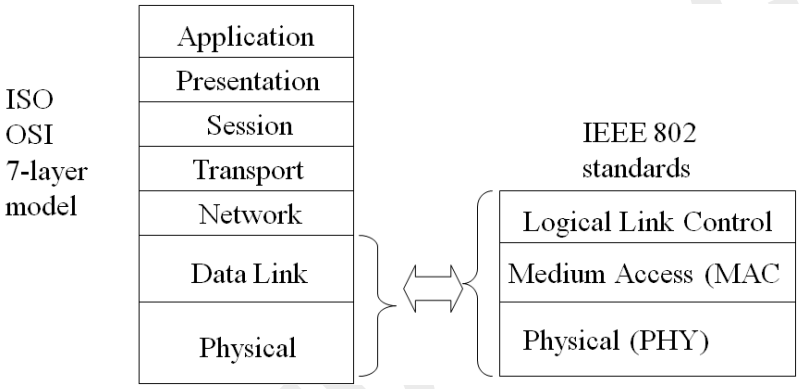
**Wireless LAN / IEEE 802.11**

**Outlines**

- Overview of IEEE 802.11
- IEEE 802.11 Protocols
- Architecture
- Services
- MAC Protocols
  - ✓ DCF
  - ✓ PCF

**Standardization of Wireless Networks**

- Wireless networks are standardized by IEEE.
- Under 802 LAN MAN standards committee.




**Overview, IEEE 802.11 Committee**

- Committee formed in 1990
  - ✓ Wide attendance
- Multiple Physical Layers
  - ✓ Frequency Hopping Spread Spectrum
  - ✓ Direct Sequence Spread Spectrum
  - ✓ Infrared
- 2.4GHz Industrial, Scientific & Medical shared unlicensed band
  - ✓ 2.4 to 2.4835GHz with FCC transmitted power limits
- 2Mb/s & 1Mb/s data transfer
- Draft 5.0 Letter Ballot passed and forwarded to Sponsor Ballot
  - ✓ Published Standard adopted in 1997

**IEEE 802.11 Overview**

- Goals
  - ✓ To deliver services in wired networks
  - ✓ To achieve high throughput
  - ✓ To achieve highly reliable data delivery
  - ✓ To achieve continuous network connection.

**WLAN Requirements**

- Throughput
- Number of Nodes/Scalability
- Connection to Backbone LAN
- Service Area: 100 to 300 m
- Power Consumption
- Transmission Robustness and Security
- Collocated network Operation
- License-free operation
- Handoff/Roaming
- Dynamic Configuration

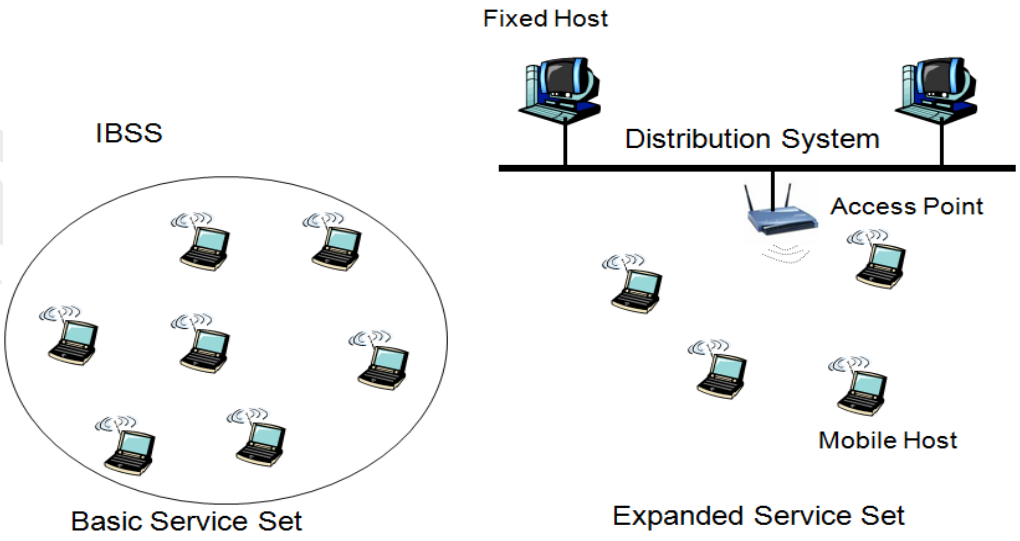
**IEEE 802.11 Protocols**

- IEEE 802.11a: PHY Standard : 8 channels : 54 Mbps : 5 GHz band: OFDM.
- IEEE 802.11b: PHY Standard : 3 channels : 11 Mbps : 2.4 GHz band: FHSS, DSSS.
- IEEE 802.11d: MAC Standard : operate in variable power levels :
- IEEE 802.11e: MAC Standard : QoS support : EDCF.
- IEEE 802.11f: Inter-Access Point Protocol : 2nd half 2002
- IEEE 802.11h: Supplementary MAC Standard: Enhanced version of 802.11a to support European Regulatory provides TPC and DFS.
- IEEE 802.11i: Supplementary MAC Standard: Alternative WEP
- IEEE 802.11n: 100 + Mbps : Enhancement to 802.11g using MIMO
- IEEE 802.11s: mesh networking extension

**IEEE 802.11 Architecture**

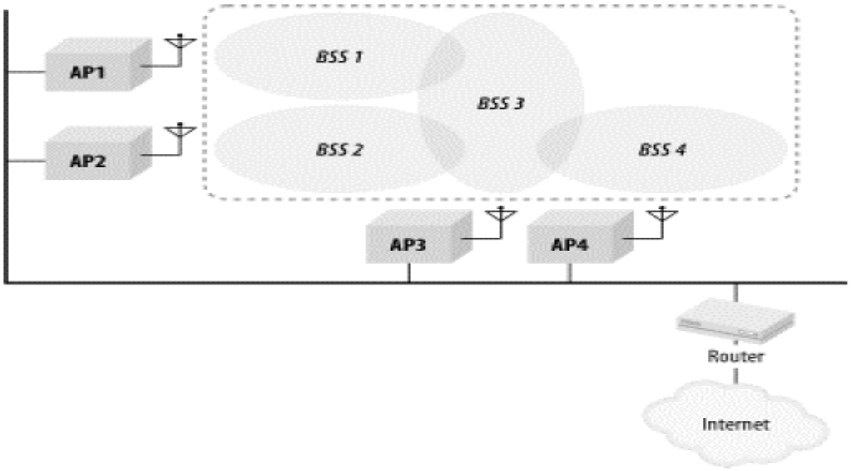
- WLAN is based on cellular architecture
- Each cell/Basic Service Set (BSS) is controlled by a base station/Access Point (AP).
- Access Points are connected with backbone called Distribution System (DS).
- The whole interconnected WLAN through DS form Extended Service Set (ESS) as a single layer in OSI model.
- Mobile Station (MS) in BSS with no connection to other BSSs form Independent BSS (IBSS).

**Wireless LAN / IEEE 802.11**



**ESS**

- Access Point functions as a bridge and a relay point.
- In BSS, MS communicate through Access Point
- IBSS is typically an ad hoc network, where station communicate directly.
- To integrate 802.11 with 802.2 (Wired LAN), a portal is used.
- Portal is a device such as bridge or router attached to DS.




**802.11 Services**

- IEEE 802.11 defines nice services.
- Three services for WLAN access and confidentiality.
- Six services used to support delivery of MAC Service Data Unit (MSDU) between stations.

**Messages Distribution in ESS**

- Two services involved in distribution of messages within DS.
- Distribution
  - ✓ Primary service used to exchange MAC frames between stations of two BSSs.
  - ✓ Source sends to AP of one BSS, which sends to DS. DS then sends to AP of the destination.
  - ✓ Message transport in DS is beyond the scope of IEEE 802.11 standard.
- Integration
  - ✓ Enables transfer of a data between a station on an IEEE 802.11 LAN and a station on an integrated IEEE 802.x LAN (Wired LAN).
  - ✓ It takes care of any address translation and media conversion logic

**Association-Related Services**

- Three services are implemented
  - ✓ Association:
    - Establishes an initial association between a station and an AP
    - AP can communicate its identity to other APs within ESS to facilitate routing and delivery of addressed frames.

- ✓ Re-association
  - Enables an established association to be transferred from one AP to another
- ✓ Disassociation
  - A notification from either a MS or AP that an existing association has terminated.

**Access and Privacy Services**

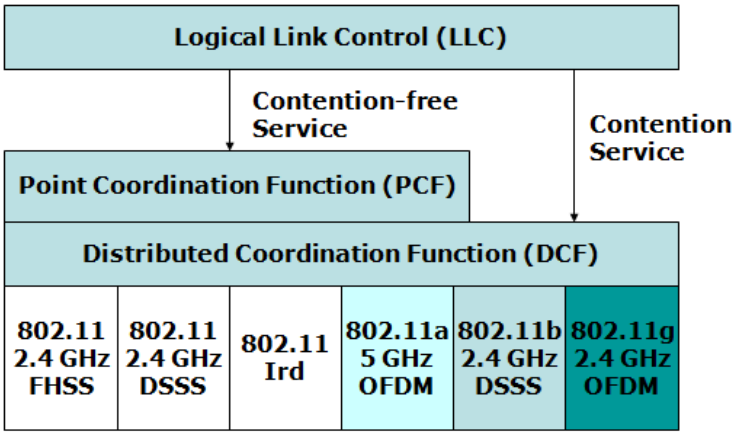
- Authentication
  - ✓ Establishes the identity of stations.
  - ✓ However, IEEE 802.11 requires mutually acceptable, successful authentication before association.
- De-authentication
  - ✓ Invoked to terminate existing authentication
- Privacy
  - ✓ Standard provides optional use of encryption to assure privacy

| Service | Station or distribution service? | Description |
|---|---|---|
| Distribution | Distribution | Service used in frame delivery to determine destination address in infrastructure networks |
| Integration | Distribution | Frame delivery to an IEEE 802 LAN outside the wireless network |
| Association | Distribution | Used to establish the AP which serves as the gateway to a particular mobile station |
| Reassociation | Distribution | Used to change the AP which serves as the gateway to a particular mobile station |
| Disassociation | Distribution | Removes the wireless station from the network |
| Authentication | Station | Establishes identity prior to establishing association |
| Deauthentication | Station | Used to terminate authentication, and by extension, association |
| Privacy | Station | Provides protection against eavesdropping |
| MSDU delivery | Station | Delivers data to the recipient |

**IEEE 802.11 Medium Access Control (MAC)**

- MAC Layer provides three functions
  - ✓ Reliable data delivery
  - ✓ Medium access control
  - ✓ security

**IEEE 802.11 Protocol Architecture**




**Reliable Data Delivery**

- Reliability at TCP level?
  - ✓ Significant delay due to wait timers
- Reliability at MAC
  - ✓ Quick fix
  - ✓ Hop by hop ACK at MAC as atomic operation.

**MAC Protocol**

- Two types of algorithms:
  - ✓ Distributed access protocol
    - Distribute the decision to transmit
  - ✓ Centralized control
    - Better in ESS, when AP connected to DS

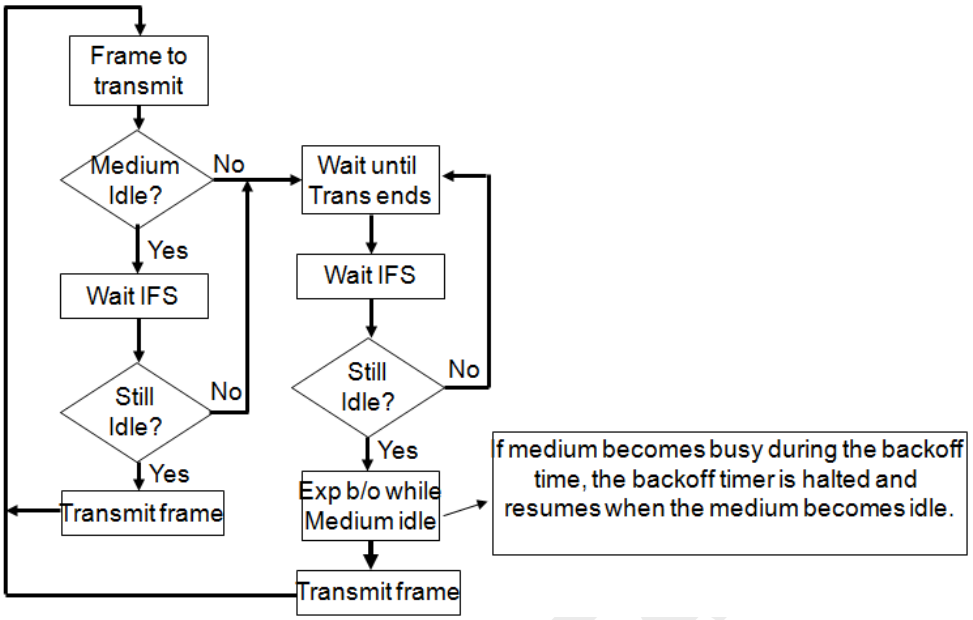
**Distributed Coordination Function (DCF)**

- DCF sub layer uses CSMA algorithm
- Collision detection as in Ethernet is not possible in wireless comm.
- It implements collision avoidance (CA) algorithm.
- It uses a set of delays of different periods called inter-frame space (IFS)

**CSMA/CA**

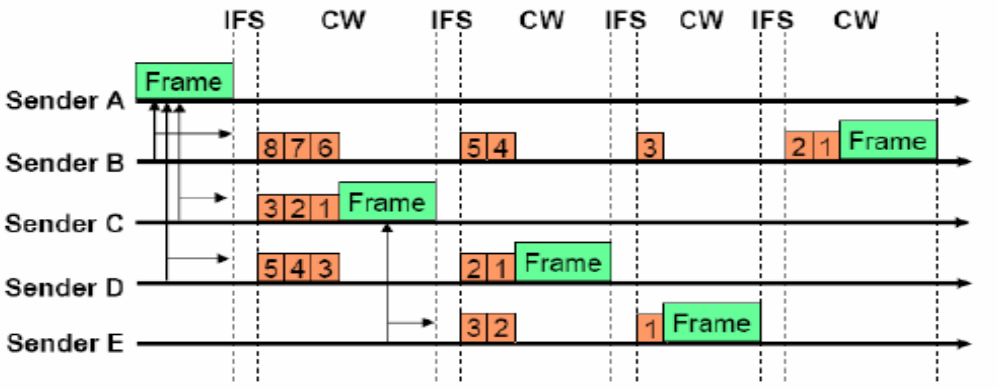
- A Station willing to transmit senses the medium.
- If the medium is busy, defers
- If idle, wait for Distributed Inter-Frame Space (DIFS) or Exponential back off.

**CSMA/CA Algorithm**




**Example**

- A is transmitting a frame when B, C and D sense the channel.
- B, C, and D run their random number generator to get a back off time
- Station C draws the smallest number followed by D and B.
- After completion of A:
  - ✓ B, C, D wait for the IFS period and start their counters.
  - ✓ C finishes first and starts transmission, after checking again whether the medium is idle.
  - ✓ B and D freeze their counters.
  - ✓ After completion of C: B and D wait for the IFS period and (re-) start their counters



**Lecture 27**
**WLAN Part II**

**Outlines**

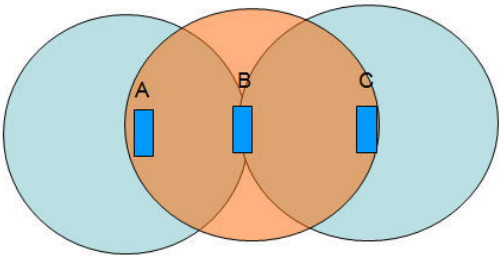
- Last Lecture Review
- Problems with DCF
- Virtual Carrier Sensing
- RTC/CTS Protocol
- Interframe Spacing
- PCF
- Fragmentation / Reassembly
- MAC Frame Format
- Frame Types
- Physical Media in Original IEEE 802.11

**Last Lecture**

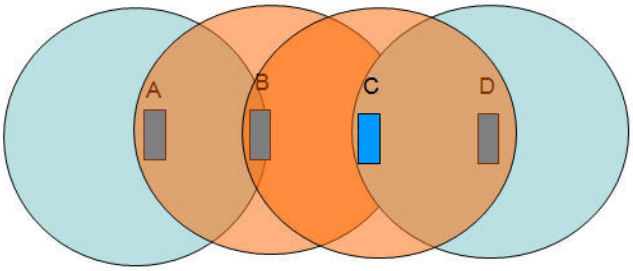
- Overview of IEEE 802.11
- IEEE 802.11 Protocols
- Architecture
- Services
- MAC Protocols
  - ✓ DCF
  - ✓ PCF

**Problems with DCF**

- Hidden Node

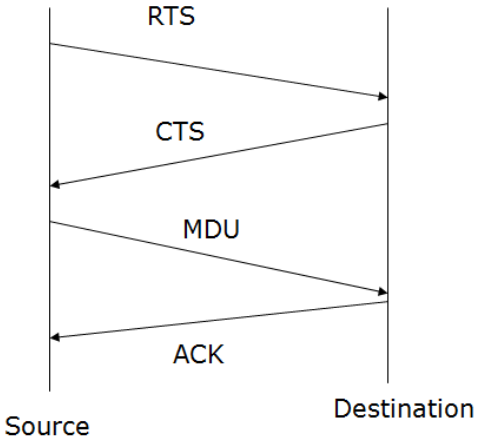



- Exposed Node problem




**RTS/CTS Protocol**

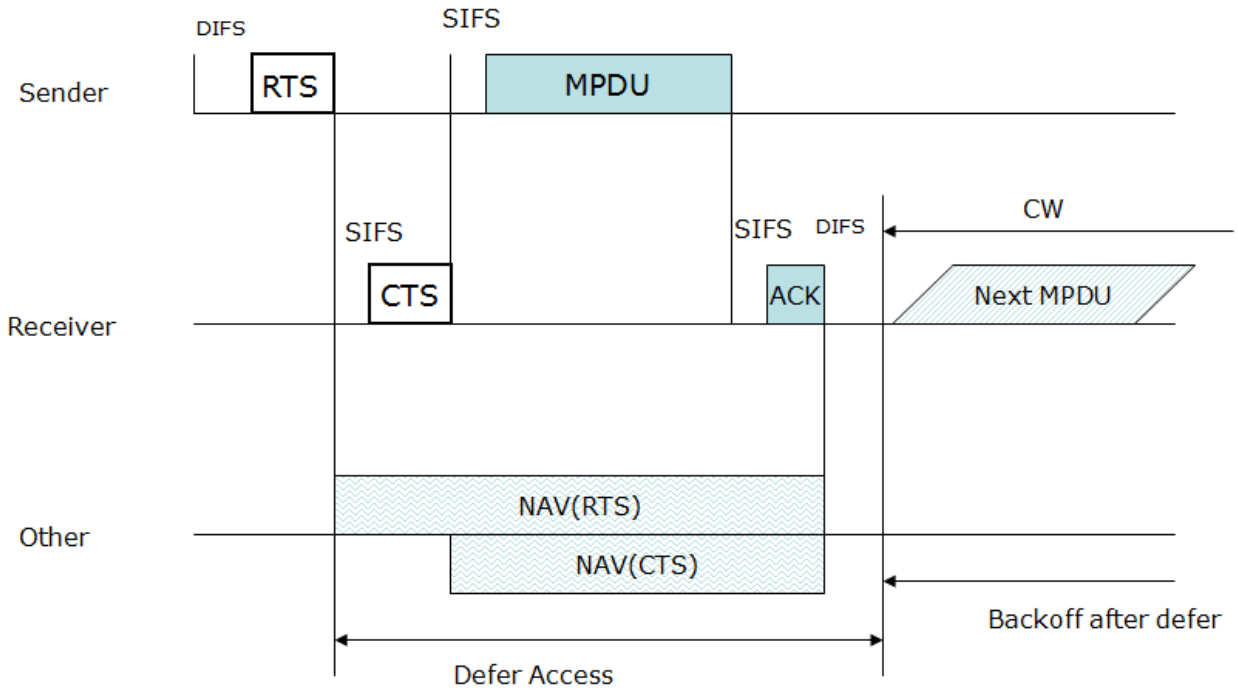
- Virtual Carrier Sense technique.
- Source sends Request-to-Send beacon
- Destination, if free, sends Clear-to-Send beacon.
- Source transmits data packet.
- Destination ACKs if receives successfully
- RTS includes source, destination ID and duration of following transaction.
- The duration info allows to protect the transmission from collision on the transmitter side.




- The destination response in CTS also includes the same duration amount.
- This helps in overcoming hidden terminal problem.
- All the stations hearing RTS/CTS set their Network Allocation Vector (NAV) to the given duration.
- Since RTS/CTS are shorter frames than MSDU, collision is detected fast.
- If MSDU is smaller than RTSThreshold, Standard allows to skip RTS/CTS.

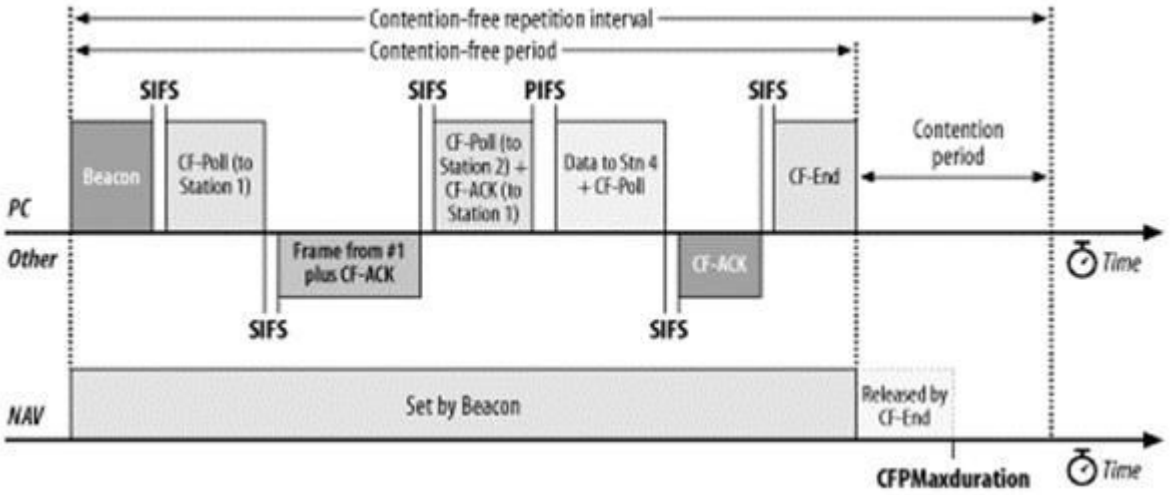
**Interframe Spacing**

- Short interframe space (SIFS)
  - ✓ The SIFS is used for the highest-priority transmissions, such as RTS/CTS frames and positive acknowledgments.
- PCF interframe space (PIFS)
  - ✓ The PIFS is used by the PCF during contention-free operation. Stations with data to transmit in the contention-free period can transmit after the PIFS has elapsed and pre-empt any contention-based traffic
- DCF interframe space (DIFS)
  - ✓ The DIFS is the minimum medium idle time for contention-based services. Stations may have immediate access to the medium if it has been free for a period longer than the DIFS.
- Extended interframe space (EIFS)
  - ✓ The EIFS is not a fixed interval. It is used only when there is an error in frame transmission.




**Point Coordination Function**

- Centralized access to medium.
- Implemented on top of DCF.
- AP issues polls to the MS on round robin fashion.
- PIFS is used between polling.




**Fragmentation and Reassembly**

- In Ethernet, MAC frame can be upto 1518 bytes long.
- Not possible to support such larger size of frame because of:
  - ✓ Higher bit error rate
  - ✓ If it is corrupted, large size would incur high overheads.
  - ✓ On FH, medium is interrupted periodically (20ms), smaller packet would result in smaller chance of postponing transmission.
- In IEEE 802.11 segmentation/reassembly is added to support Ethernet frames.
- Each MSDU is divided into several frames/segments.
- All the segments are transmitted after SIFS of ACK reception.
- Segments are reassembled to MSDU in the order as transmitted.


FC = Frame control
D/I = Duration/Connection ID
SC = Sequence control

**(a) MAC frame**


DS = Distribution system
MF = More fragments
RT = Retry
PM = Power management
MD = More data
W = Wired equivalent privacy bit
O = Order

**(b) Frame control field**

IEEE 802.11 MAC Frame Format

**MAC Frame Fields**

- Frame Control – frame type, control information
- Duration/connection ID – channel allocation time
- Addresses – context dependant, types include source and destination
- Sequence control – numbering and reassembly
- Frame body – MSDU or fragment of MSDU
- Frame check sequence – 32-bit CRC

**Addresses**

- Destination address
  - ✓ As in Ethernet, the destination address is the 48-bit IEEE MAC identifier that corresponds to the final recipient: the station that will hand the frame to higher protocol layers for processing.
- Source address
  - ✓ This is the 48-bit IEEE MAC identifier that identifies the source of the transmission. Only one station can be the source of a frame, so the Individual/Group bit is always 0 to indicate an individual station.
- Receiver address
  - ✓ This is a 48-bit IEEE MAC identifier that indicates which wireless station should process the frame. If it is a wireless station, the receiver address is the destination address.
- Transmitter address
  - ✓ This is a 48-bit IEEE MAC address to identify the wireless interface that transmitted the frame onto the wireless medium.

**Frame Control Fields**

- Protocol version – 802.11 version
- Type – control, management, or data
- Subtype – identifies function of frame
- To DS – 1 if destined for DS
- From DS – 1 if leaving DS
- More fragments – 1 if fragments follow
- Retry – 1 if retransmission of previous frame
- Power management – 1 if transmitting station is in sleep mode
- More data – Indicates that station has more data to send
- WEP – 1 if wired equivalent protocol is implemented
- Order – 1 if any data frame is sent using the Strictly Ordered service

**Control Frame Subtypes (Type 01)**

- Power save – poll (PS-Poll)
- Request to send (RTS)
- Clear to send (CTS)
- Acknowledgment
- Contention-free (CF)-end
- CF-end + CF-ack

**Data Frame Subtypes (Type 10)**

- Data-carrying frames
  - ✓ Data
  - ✓ Data + CF-Ack
  - ✓ Data + CF-Poll
  - ✓ Data + CF-Ack + CF-Poll
- Other subtypes (don't carry user data)
  - ✓ Null Function
  - ✓ CF-Ack
  - ✓ CF-Poll
  - ✓ CF-Ack + CF-Poll

**Management Frame Subtypes (Type 00)**

- Association request
- Association response
- Reassociation request
- Reassociation response
- Probe request
- Probe response
- Beacon
- Announcement traffic indication message
- Dissociation
- Authentication
- Deauthentication

**Physical Media Defined by Original 802.11 Standard**

- Direct-sequence spread spectrum
  - ✓ Operating in 2.4 GHz ISM band
  - ✓ Data rates of 1 and 2 Mbps
- Frequency-hopping spread spectrum
  - ✓ Operating in 2.4 GHz ISM band
  - ✓ Data rates of 1 and 2 Mbps
- Infrared
  - ✓ 1 and 2 Mbps
  - ✓ Wavelength between 850 and 950 nm

**IEEE 802.11a and IEEE 802.11b**

- IEEE 802.11a
  - ✓ Makes use of 5-GHz band
  - ✓ Provides rates of 6, 9 , 12, 18, 24, 36, 48, 54 Mbps
  - ✓ Uses orthogonal frequency division multiplexing (OFDM)
  - ✓ Subcarrier modulated using BPSK, QPSK, 16-QAM or 64-QAM
- IEEE 802.11b
  - ✓ Provides data rates of 5.5 and 11 Mbps
  - ✓ Complementary code keying (CCK) modulation scheme

**Summary**

- Problems with DCF
- Virtual Carrier Sensing
- RTC/CTS Protocol
- Interframe Spacing
- PCF
- Fragmentation / Reassembly
- MAC Frame Format
- Frame Types
- Physical Media in Original IEEE 802.11

**Lecture 28**

**Mobile Ad hoc Network**

**Outlines**

- Introduction
  - ✓ What is Ad hoc networks?
  - ✓ Characteristic
  - ✓ Ad hoc vs. cellular networks
  - ✓ Application
  - ✓ Challenges
- Routing Protocol
  - ✓ Expected Properties of Ad-hoc Routing Protocols
  - ✓ A taxonomy for routing protocols in Mobile ad
  - ✓ Some common protocols (DSDV, AODV, DSR, ZRP, TORA)

**Last Lecture Review**

- Problems with DCF
- Virtual Carrier Sensing
- RTC/CTS Protocol
- Interframe Spacing
- PCF
- Fragmentation / Reassembly
- MAC Frame Format
- Frame Types
- Physical Media in Original IEEE 802.11

**What is Ad hoc**

- Ad hoc
  - ✓ For a specific purpose of occasion
  - ✓ For this case alone
- IEEE802.11
  - ✓ a network composed solely of stations within mutual communication range of each other via the wireless media.
  - ✓ an independent basic service set
- Mobile distributed multi-hop wireless network (manet)
  - ✓ A group of mobile, wireless nodes which cooperatively and spontaneously form a network independent of any fixed infrastructure or centralized administration
  - ✓ A node communicates
    - o directly with nodes within wireless range
    - o indirectly with all other destinations using a dynamically determined multi-hop route though other nodes in the manet

**The characteristic of ad hoc networks**

- Heterogeneous nodes
- Self-creating
  - ✓ not rely on a pre-existing fixed infrastructure
- Self-organizing
  - ✓ no predetermined topology

- Self-administering
  - ✓ no central control
- creating a network “on the fly”
- Ad hoc networks
  - ✓ infrastructureless
  - ✓ multiple hop
    - Radio power limitation, channel utilization, and power-saving concerns
  - ✓ DCF(distributed coordination function)
- Cellular networks
  - ✓ infrastructure-based
  - ✓ one hop(uplink or downlink)
  - ✓ PCF(pointed coordination function)

**Challenges**

1. Spectrum allocation
2. Self-configuration
3. Medium access control (MAC)
4. Energy efficiency
5. TCP Performance
6. Mobility management
7. Security & privacy
8. Routing protocols
9. Multicasting
10. QoS
11. Service Location, Provision, Access

**Routing Protocols**

- Expected Properties of Ad-hoc Routing Protocols
- A taxonomy for routing protocols in Mobile ad hoc networks
  - ✓ Reactive or On-demand routing protocols
  - ✓ Proactive or Table-driven
  - ✓ Hybrid
  - ✓ Hierarchical
  - ✓ Geographical

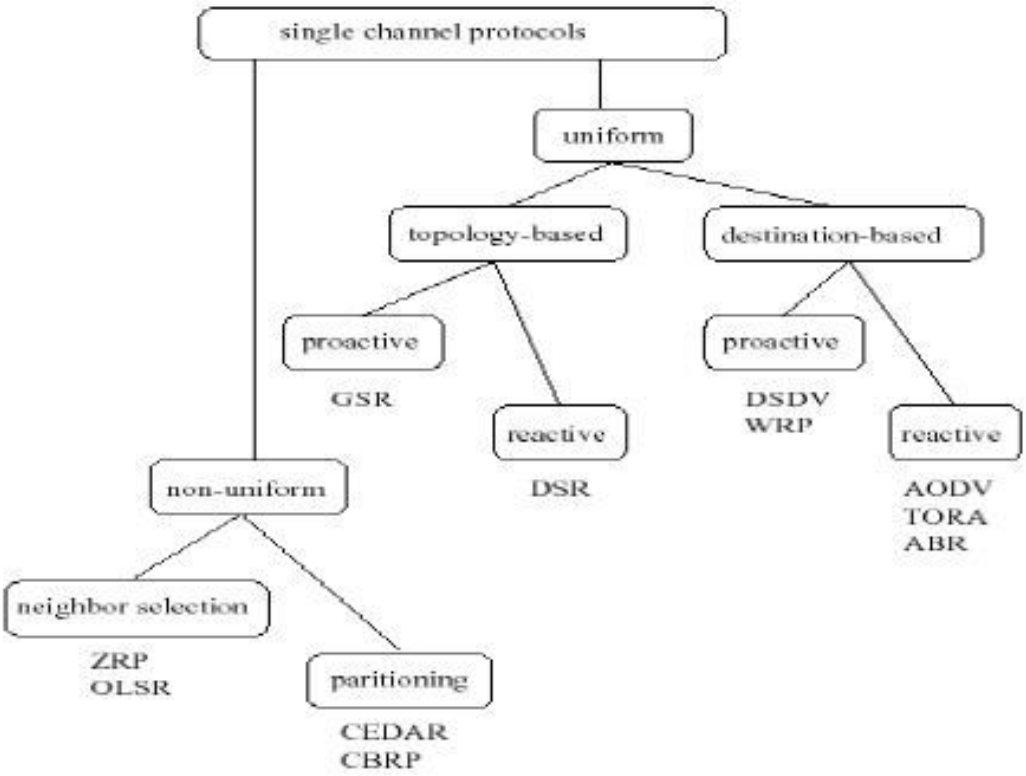
**Expected Properties of Routing**

- Ideally an ad hoc network routing protocol should
  - ✓ be distributed in order to increase reliability
  - ✓ assume routes as unidirectional links
  - ✓ be power efficient.
  - ✓ consider its security
  - ✓ be hybrid protocols
  - ✓ be aware of Quality of Service

**Taxonomy**

- Communication model
  - ✓ Multi-channel: Channel assignment using low-layer info
  - ✓ Single channel model
- Structure
  - ✓ Are all nodes treated uniformly?
  - ✓ How are distinguished nodes selected (neighbors or cluster-based)?

- State information
  - ✓ Is network-scale topology obtained at each node?
- Scheduling
  - ✓ Is route information continually maintained for each destination (proactive or reactive)?

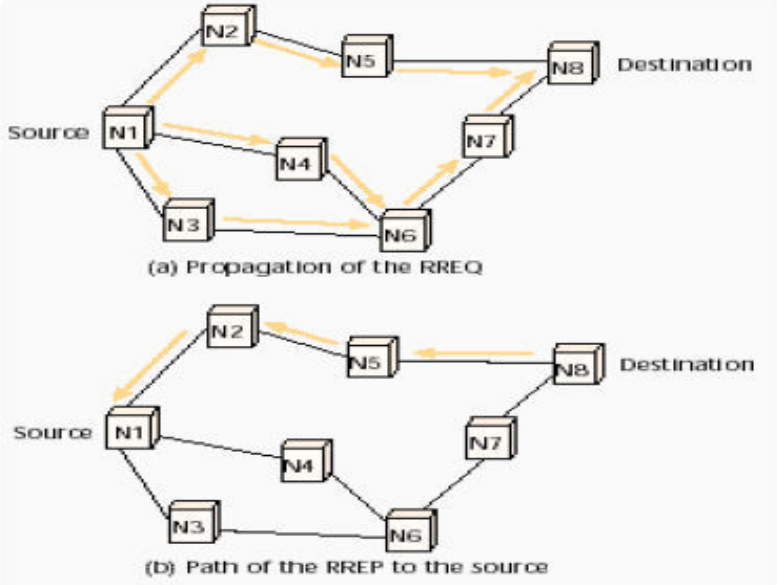



**DSDV**

- Is based on the idea of Ballman-Ford routing algorithm
- Every mobile station maintains a routing table that lists
  - ✓ all available destinations
  - ✓ the number of hops to reach the destination
  - ✓ the sequence number assigned by the destination node
- A station transmits its routing table
  - ✓ periodically
  - ✓ if a significant change has occurred in its table from the last update sent
- The routing table updates can be sent in two ways
  - ✓ full dump
  - ✓ incremental update
- Put figure with same illustration of DSR

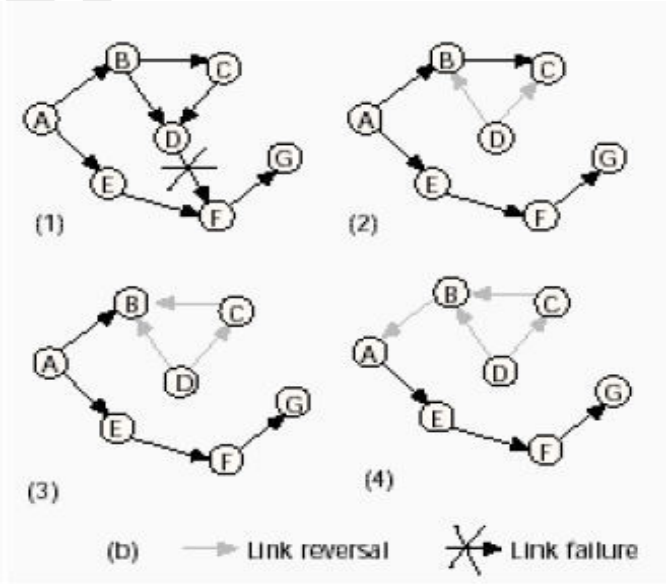
**AODV**

- It borrows
  - ✓ the basic on-demand mechanism of route discovery and route maintenance from DSR
  - ✓ the use of hop-by-hop routing, sequence numbers, and periodic beacons from DSDV
- A node periodic broadcasts *hello* information to maintain the local connectivity
- It only supports the use of symmetric links



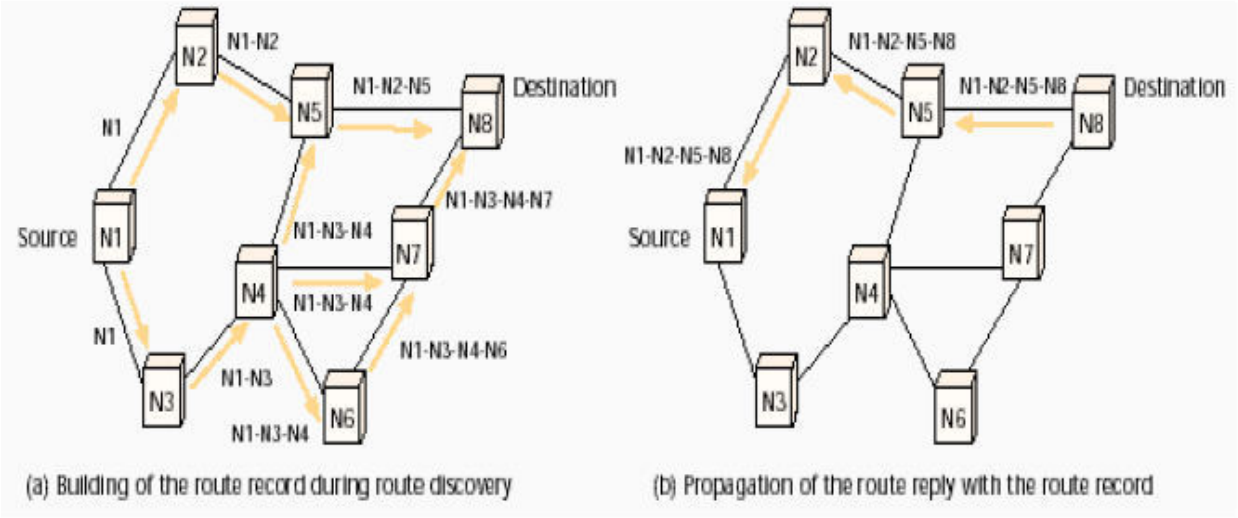

**TORA**

- Is based on the concept of link reversal
- Finds multiple routes from a source node to a destination node
- The control messages are localized to a very small set of nodes near the occurrence of a topological change



**DSR**

- A node maintains route caches containing the source routes that it is aware of
- The node updates entries in the route cache as and when it *learns* about new routes
- Route discovery
  - ✓ route request packet contains
    - the address of the source
    - the destination
    - a unique identification number
  - ✓ route reply is generated by
    - the destination
    - an intermediate node with current information about the destination
- Route maintenance
  - ✓ Route error packets are generated at a node when the data link layer encounters a fatal transmission problem
  - ✓ Acknowledgements, including passive acknowledgments




**OLSR (cont'd)**

- Only the *multipoint relays* nodes (MPRs) need to forward LS updates
- OLSR is particularly suited for dense networks
- In sparse networks, every neighbor becomes a multipoint relay, then OLSR reduces to pure LS protocol

**ZRP**

- A hybrid routing protocol that combines both proactive and on-demand routing strategies
- Each node has a predefined zone
- Inside zones: proactive routing
- Outside zones: on-demand routing
- ZRP provides more flexibility

**Outlines**

- Introduction
  - ✓ What is Ad hoc networks?
  - ✓ Characteristic
  - ✓ Ad hoc vs. cellular networks
  - ✓ Application
  - ✓ Challenges
- Routing Protocol
  - ✓ Expected Properties of Ad-hoc Routing Protocols
  - ✓ A taxonomy for routing protocols in Mobile ad
  - ✓ Some common protocols (DSDV, AODV, DSR, ZRP, TORA)

**Lecture 29**

**Security in IEEE 802.11**

**Outlines**

- Types of Attack
- Goals of 802.11 Security
- WEP Protocol
- WEP Authentication
- Security flaws in original 802.11
- 802.1x Security
  - ✓ AKM Operations with AS
  - ✓ AKM operations with PSK
- IBSS Security model

**Last Lecture**

- Introduction
  - ✓ What is Ad hoc networks?
  - ✓ Characteristic (Heterogeneous, Self-creating, self-organizing, self-adminstrating, on-the-fly)
  - ✓ Ad hoc vs. cellular networks
  - ✓ Challenges (Spectrum allocation, Self-configuration, Medium access control (MAC), Energy efficiency, TCP Performance, Mobility management, Security & privacy, Routing protocols, Multicasting, QoS, Service Location, Provision, Access)
- Routing Protocol
  - ✓ Expected Properties of Ad-hoc Routing Protocols
  - ✓ A taxonomy for routing protocols in Mobile ad
  - ✓ Some common protocols (DSDV, AODV, DSR, ZRP, TORA)

**Types of Attacks**

- Passive attacks
  - ✓ to decrypt traffic based on statistical analysis
- Active attacks
  - ✓ To inject new traffic from authorized mobile stations, based on known plaintext
- Active attacks
  - ✓ To decrypt traffic, based on tricking the access point
- Dictionary building attacks
  - ✓ Allows real-time automated decryption of all traffic

**802.11 Security**

- Goals of 802.11 security
  - ✓ Access Control
    - Ensure that your wireless infrastructure is not used.
  - ✓ Data Integrity
    - Ensure that your data packets are not modified in transit.
  - ✓ Confidentiality
    - Ensure that the contents of your wireless traffic is not learned

- 802.11 security consists of two subsystems
  - ✓ A data encapsulation technique called *W*ired *E*quivalent *P*rivacy (WEP)
  - ✓ An authentication algorithm called Shared Key Authentication

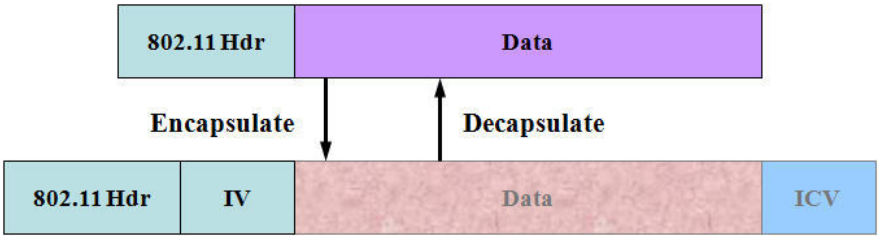
**WEP**

- Wireless connections has important security issues to keep the intruders from accessing, reading and modifying the network traffic.
- But mobile systems need to be connected.
- We need an algorithm which provides the same level of security that physical wire does.
- WEP is used to
  - ✓ Protect wireless communication from eavesdropping.
  - ✓ Prevent unauthorized access to wireless network (feature of WEP, but not an explicit goal in the 802.11 standard)
- WEP relies on a secret key which is shared between the sender and the receiver.
  - ✓ SENDER: Mobile station (e.g. Labtop with a wireless ethernet card)
  - ✓ RECEIVER: Access Point (eg. base station)
- Secret Key is used to encrypt packets before they are transmitted
- Integrity Check is used to ensure packets are not modified in transit.
  - ✓ The standard does not discuss how shared key is established
  - ✓ In practice, most installations use a single key which is shared between all mobile stations and access points.

**WEP Protocol**

- To send a message M:
  - ✓ Compute a checksum c(M) (is not depend on secret key k)
  - ✓ Pick an IV v and generate a keystream RC4(v,k)
  - ✓ XOR <M, c(M)> with the keystream to get the ciphertext
  - ✓ Transmit v and ciphertext over a radio link
- When received a message M
  - ✓ Use transmitted v and the shared key k to generate the keystream RC4(v,k)
  - ✓ XOR the ciphertext with RC4(v,k) to get <M',c'>
  - ✓ Check is c'=c (M')
  - ✓ If it is, accept M' as the message transmitted

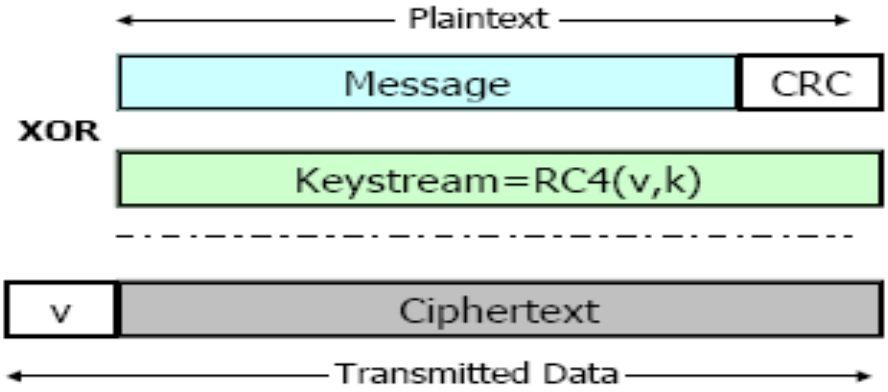
**WEP Encapsulation**



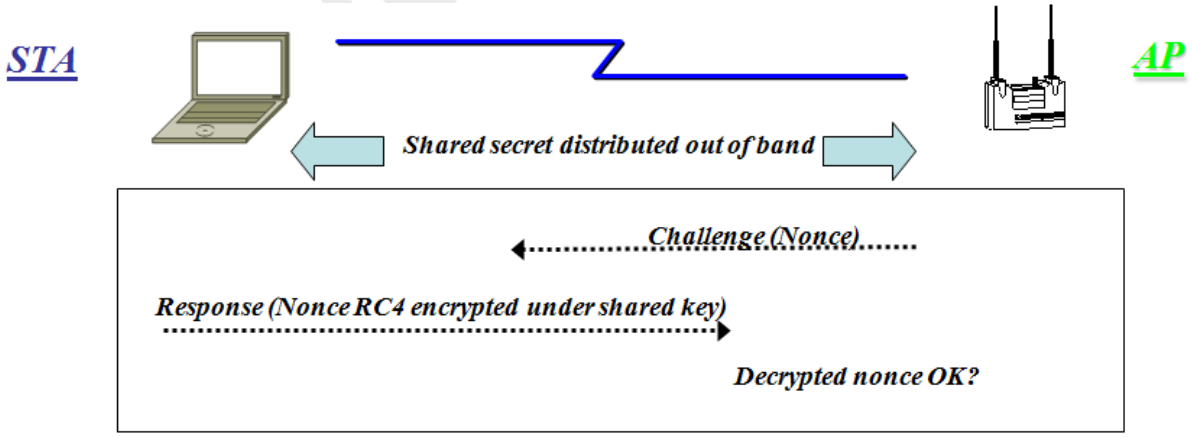
- WEP Encapsulation Summary:
  - ✓ Encryption Algorithm = RC4
  - ✓ Per-packet encryption key = 24-bit IV concatenated to a pre-shared key
  - ✓ WEP allows IV to be reused with any frame
  - ✓ Data integrity provided by CRC-32 of the plaintext data (the "ICV")
  - ✓ Data and ICV are encrypted under the per-packet encryption key

**Defense of WEP**

- Integrity Check(IC) field
  - ✓ Used to ensure that packet has not been modified in transit
- Initialization Vector(IV)
  - ✓ Used to avoid encrypting two ciphertexts with the same key stream
  - ✓ Used to argument the shared key and produce a different RC4 key for each packet to avoid statistical attacks




**WEP Authentication**




- 802.11 Authentication Summary:
  - ✓ Authentication key distributed out-of-band
  - ✓ Access Point generates a "randomly generated" challenge
  - ✓ Station encrypts challenge using pre-shared secret

**Security Flaws**

- Physical threat: user loses 802.11 NIC, doesn't report it
  - ✓ Attacker with physical possession of NIC may be capable of accessing the network
- Impersonation: User Identification
  - ✓ 802.11 does not identify users, only NICs
  - ✓ Problems
    - MAC may represent more than one user
    - Multi-user machines becoming common; which user is logged on with which MAC?
    - Users may move between machines
    - Machine may allow logins by other users within the domain
- Mutual Authentication
  - ✓ 802.11 shared authentication not mutual
    - Client authenticates to Access Point but Access Point does not authenticate to client
    - Enables rogue access points
    - Denial of service attacks possible
  - ✓ Solution
    - Mutual authentication: Require both sides to demonstrate knowledge of key
- Known Plaintext Attack
  - ✓ WEP supports per-packet encryption, integrity, but not per-packet authentication
  - ✓ Given a known packet (ARP, DHCP, TCP ACK, etc.), possible to recover RC4 stream
  - ✓ Enables spoofing of packets until IV changes
  - ✓ Can insert a packet, calculate ICV, encrypt with known RC4 stream
  - ✓ Solution
    - Add a keyed message integrity check
    - Change the IV every packet
- Denial of Service: Disassociation Attacks
  - ✓ 802.11 associate/disassociate messages unencrypted and unauthenticated
    - Enables forging of disassociation messages
    - Creates vulnerability to denial of service attacks
- Dictionary Attacks
  - ✓ WEP keys are derived from passwords that makes it much easier to break keys by brute force
  - ✓ Attacker uses a large list of words to try to guess a password and derive the key

**How to address these issues**

- Addition of new 802.11 authentication methods
  - ✓ Hardware changes needed for each new method
    - Creates incentive to limit number of authentication methods supported, make new methods optional

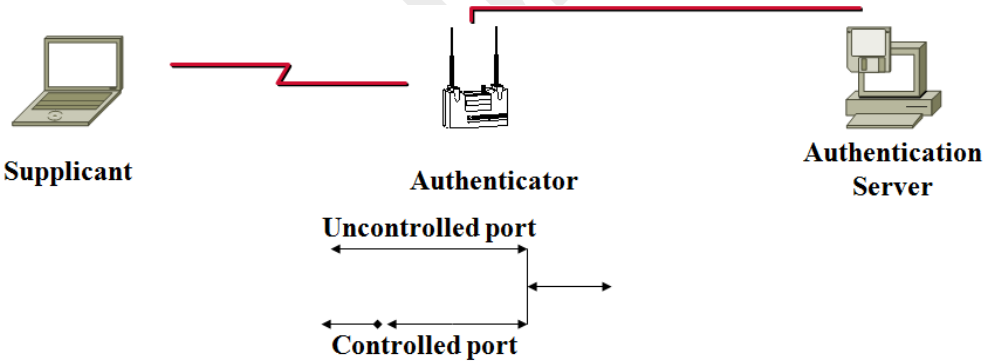
- ✓ Result: No upgrade path to extended authentication
- ✓ "Hard coding" authentication methods makes it difficult to respond to security vulnerabilities

- The solution: a flexible security framework
  - ✓ Implement security framework in upper layers
  - ✓ Enable plug-in of new authentication, key management methods without changing NIC or Access Point

**How 802.1x Address Security Issues of 802.11**

- EAP Framework
- User Identification & Strong authentication
- Dynamic key derivation
- Mutual authentication
- Per-packet authentication
- Dictionary attack precautions
- system setup and operation of an RSN, in two cases: when an IEEE 802.1X AS is used and when a PSK is used
- For an ESS, the AP includes an Authenticator, and each associated STA includes a Supplicant.

**IEEE 802.1X Terminology**



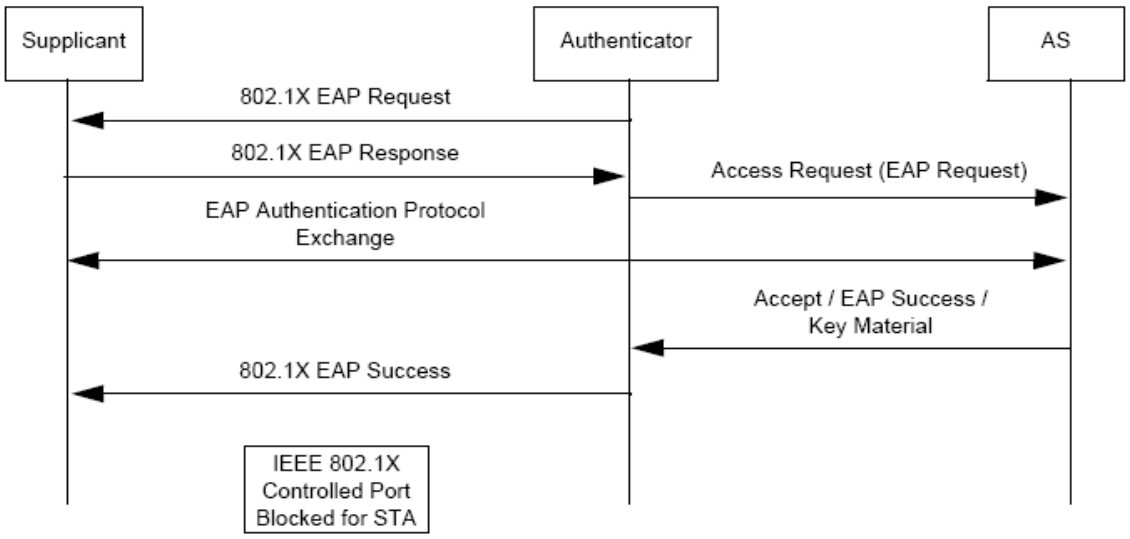

- 802.1X
  - ✓ created to control access to any 802 LAN
  - ✓ used as a transport for ***Extensible Authentication Protocol*** (EAP, RFC 2284)

**AKM Operation with AS**

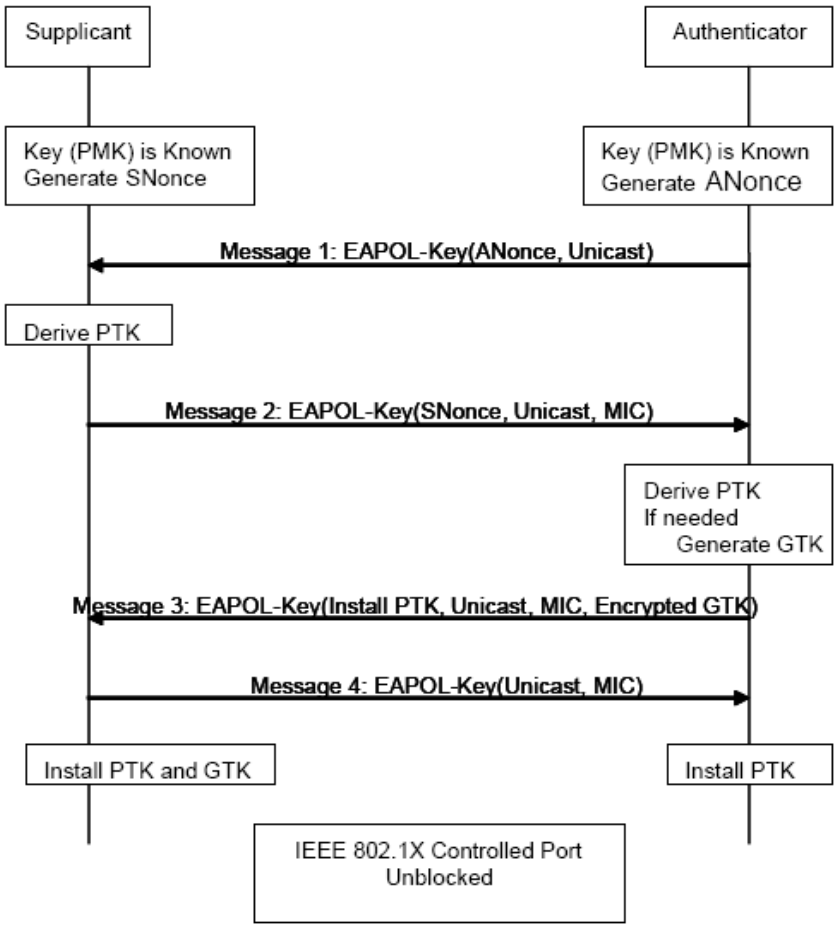
- Prior to any use of IEEE 802.1X, IEEE 802.11 assumes that the Authenticator and AS have established a secure channel.
- A STA discovers the AP's security policy through passively monitoring Beacon frames or through active probing
  - ✓ If IEEE 802.1X authentication is used, the EAP authentication process starts when the AP's Authenticator sends the EAP-Request or the STA's Supplicant sends the EAPOL-

Start message.

- ✓ EAP authentication frames pass between the Supplicant and AS via the Authenticator and Supplicant's Uncontrolled Ports.
- ✓ The Supplicant and AS authenticate each other and generate a PMK. The PMK is sent from the AS to the Authenticator over the secure channel.




- A 4-Way Handshake utilizing EAPOL-Key frames is initiated by the Authenticator to do the following:
  - ✓ Confirm that a live peer holds the PMK.
  - ✓ Confirm that the PMK is current.
  - ✓ Derive a fresh pairwise transient key (PTK) from the PMK.
  - ✓ Install the pairwise encryption and integrity keys into IEEE 802.11.
  - ✓ Transport the group temporal key (GTK) and GTK sequence number from Authenticator to Supplicant and install the GTK and GTK sequence number in the STA and, if not already installed, in the AP.
  - ✓ Confirm the cipher suite selection.
- Upon successful completion of the 4-Way Handshake, the Authenticator and Supplicant have authenticated each other; and the IEEE 802.1X Controlled Ports are unblocked to permit general data traffic.




**Operation of AKM with PSM**

- The following AKM operations are carried out when the PMK is a PSK:
  - ✓ A STA discovers the AP's security policy through passively monitoring Beacon frames or through active probing A STA associates with an AP and negotiates a security policy.
  - ✓ The PMK is the PSK.
  - ✓ The 4-Way Handshake using EAPOL-Key frames is used just as with IEEE 802.1X authentication, when an AS is present.
  - ✓ The GTK and GTK sequence number are sent from the Authenticator to the Supplicant just as in the AS case.

**IBSS Key usage Model**

- In an IBSS, the unicast data frames between two STAs are protected with a pairwise key. The key is part of the PTK, which is derived during a 4-Way Handshake.
- In an IBSS, the broadcast/multicast data frames are protected by a key, e.g., named B1, that is generated by the STA transmitting the broadcast/multicast frame.
- To allow other STAs to decrypt broadcast/multicast frames, B1 must be sent to all the other STAs in the IBSS.

- ✓ B1 is sent in an EAPOL-Key frame, encrypted under the EAPOL-Key encryption key (KEK) portion of the PTK,
- ✓ and protected from modification by the EAPOL-Key confirmation key (KCK) portion of the PTK.

- In an IBSS, a STA's SME responds to Deauthentication frames from a STA by deleting the PTK SA associated with that STA.

**Summary**

- Types of Attack
- Goals of 802.11 Security
- WEP Protocol
- WEP Authentication
- Security flaws in original 802.11
- 802.1x Security
  - ✓ AKM Operations with AS
  - ✓ AKM operations with PSK
- IBSS Security model
- Next Lecture
  - ✓ QoS in WLAN and Mobile IP

**Lecture 30**

**QoS in WLAN / Mobile IP**

**Outlines**

- Last lecture
- Limitations of QoS in IEEE 802.11
- Overview of 802.11e
- Traffic Categories
- EDCF
- HCF
- Mobile IP
  - ✓ Care-of-address,
  - ✓ MIP Protocol (Discovery, Registration, Tunneling)
  - ✓ Routing
  - ✓ Inefficiencies
  - ✓ MIPv6

**Last Lecture**

- Types of Attack
- Goals of 802.11 Security
  - ✓ Access control, data integrity, confidentality
- WEP Protocol
- WEP Authentication
- Security flaws in original 802.11
  - ✓ Physical threat, impersonation, mutual authentication, dictionary attacks, DOS
- 802.1x Security
  - ✓ AKM Operations with AS
  - ✓ AKM operations with PSK
- IBSS Security model

**QoS Limitations of 802.11**

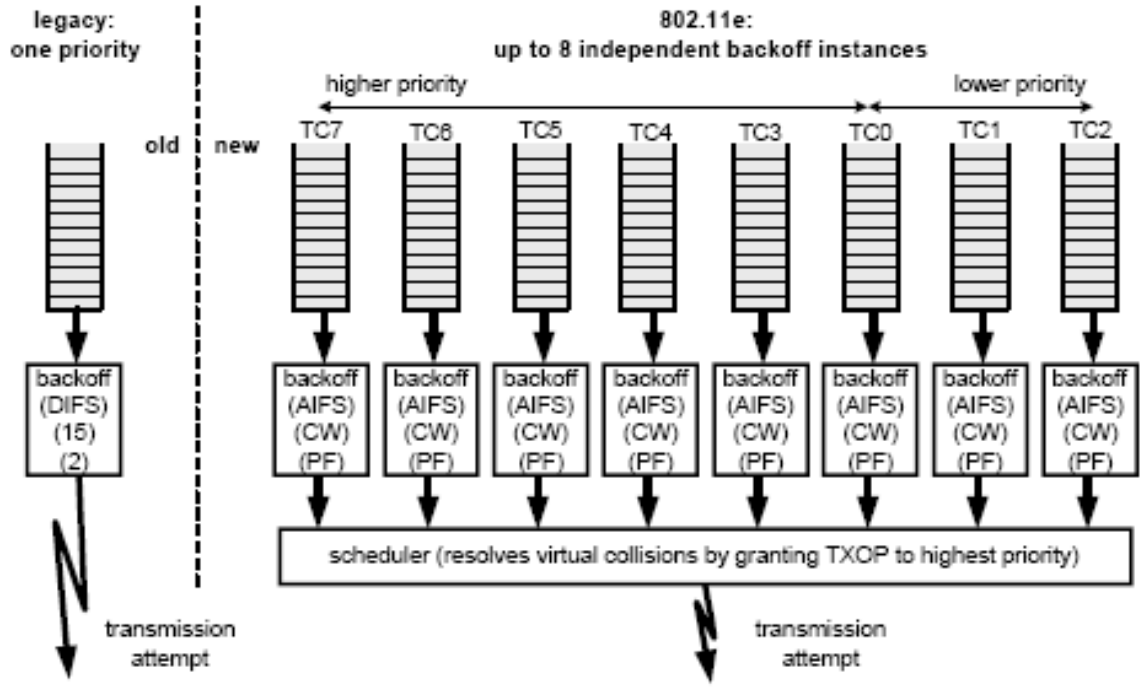
- DCF (Distributed Coordination Function)
  - ✓ Only support best-effort services
  - ✓ No guarantee in bandwidth, packet delay and jitter
  - ✓ Throughput degradation in the heavy load
- PCF (Point Coordination Function)
  - ✓ Inefficient central polling scheme
  - ✓ Unpredictable beacon frame delay due to incompatible cooperation between CP and CFP modes
  - ✓ 0Transmission time of the polled stations is unknown

**Overview of 802.11e**

- Formed in Sep. 1999. TheQoSbaseline document was approved in November 2000. The first draft was available in late 2001.
- Aim to support both IntServ and DiffServ
- New QoS mechanisms
  - ✓ EDCF (Enhanced DCF)
  - ✓ HCF (Hybrid Coordination Function)

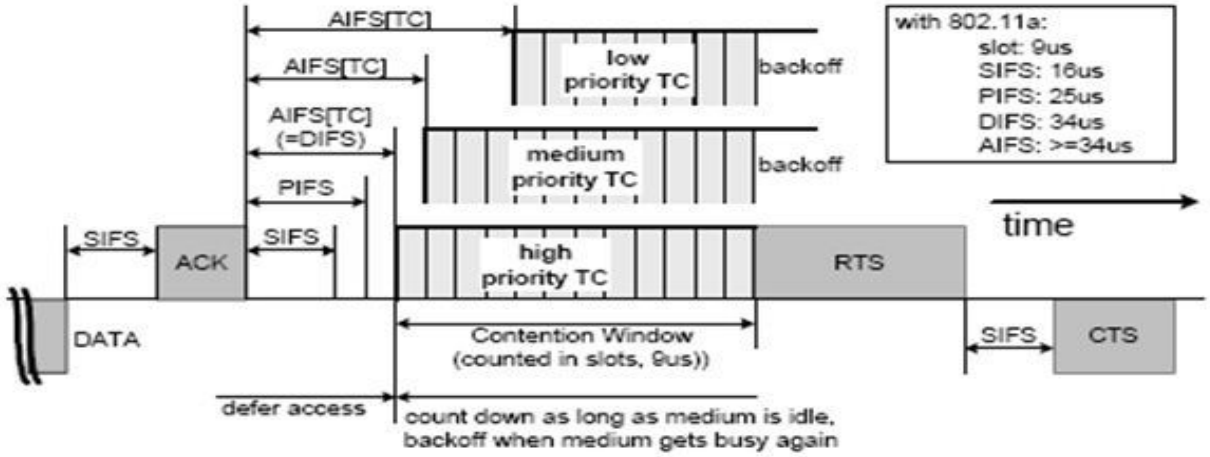
- Backwardly compatible with the DCF and PCF
- QoS is realized by introducing traffic categories (TCs)
- MSDUs are delivered through multiple backoff instances running as virtual stations
  - ✓ Each instance is parameterized with TC specific parameters
    - AIFS, CWmin, CWmax, Persistance factor (PF)
  - ✓ For legacy DCF, AIFS=DIFS, PF=2, CWmin < 15
  - ✓ CWnew[TC] = (CWold[TC]+1) x PF -1
- 0 <= I <= j <= 3  I, j are AC [0,1,2,3]
- CWmin[i] >= CWmin[j], CWmax[i] >= CWmax[j], AFIS[i] >= AFIS[j]
- QoS level in 802.11e

| Priority | Access Gateway | Designation |
|---|---|---|
| 1 | 0 | Best Effort |
| 2 | 0 | Best Effort |
| 0 | 0 | Best Effort |
| 3 | 1 | Video Probe |
| 4 | 2 | Video |
| 5 | 2 | Video |
| 6 | 3 | Voice |
| 7 | 3 | Voice |



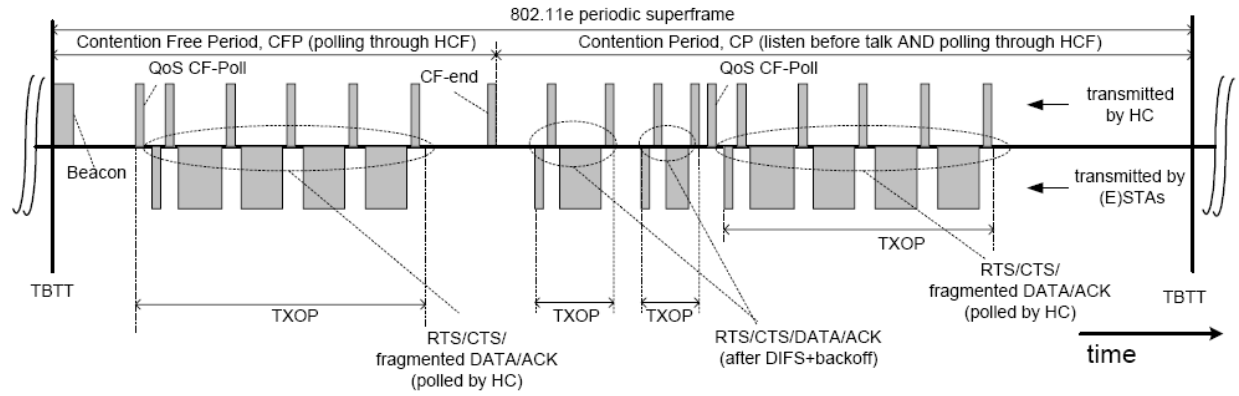
**EDCF (Enhanced DCF)**

- Enhanced DCF
- Also support bursting
- Different parameters for different TC/AC
- Replace DIFS with AIFS (AIFS>DIFS) which is shorter for audio and video traffic.
  - ✓ Audio = Video < Data
- CWmin and CWmax
  - ✓ Audio < Video < Data
- Different Persistence Factor (PF)
- For EDCF, AIFS>=DIFS, PF=1-16, CWmin=0-255




**HCF (Hybrid CF)**

- Provides policing and deterministic channel access by controlling the channel through the HC (Hybrid Coordinator)
- Operate in CFP and CP

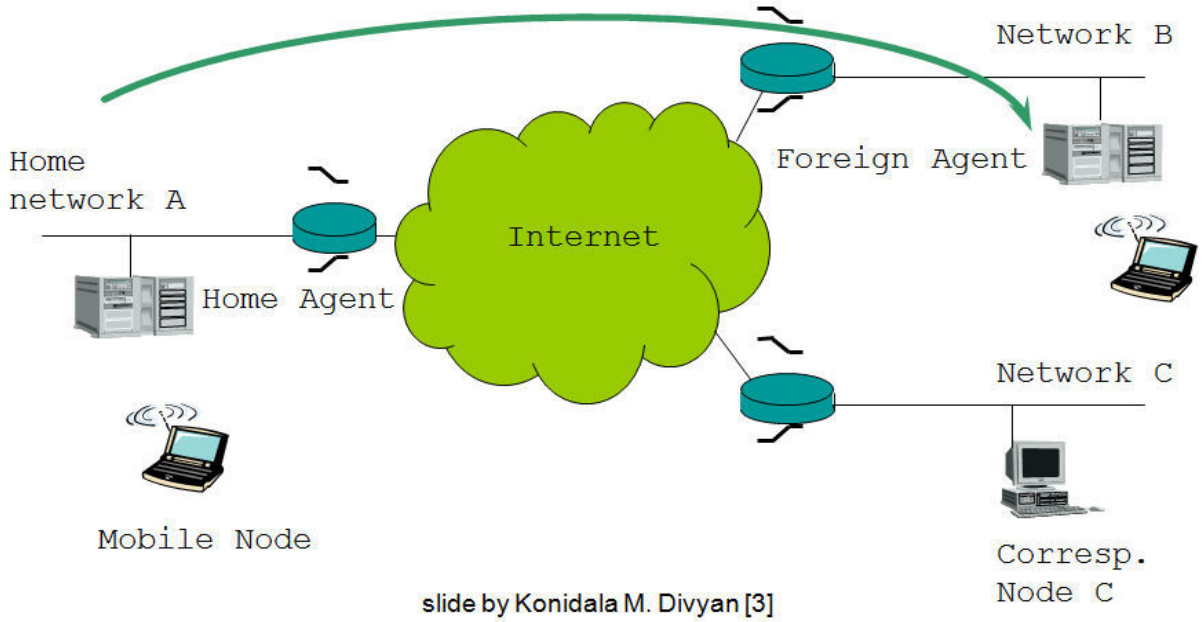



- Detecting the channel as being idle for PIFS, shorter than DIFS, gives the HC high priority over EDCF
- HCF model can provide Guaranteed Services with a much higher probability than pure EDCF
- A signaling protocol can be used to facilitate admission control and specify service rate requirement

**Mobile IP: Basics**

- Proposed by IETF (Internet Engineering Task Force)
  - ✓ Standards development body for the Internet
- Mobile IP allows a mobile host to move about without changing its *permanent* IP address
- Each mobile host has a *home agent* on its *home network*
- Mobile host establishes a *care-of* address when it's away from home

**Example**




slide by Konidala M. Divyan [3]

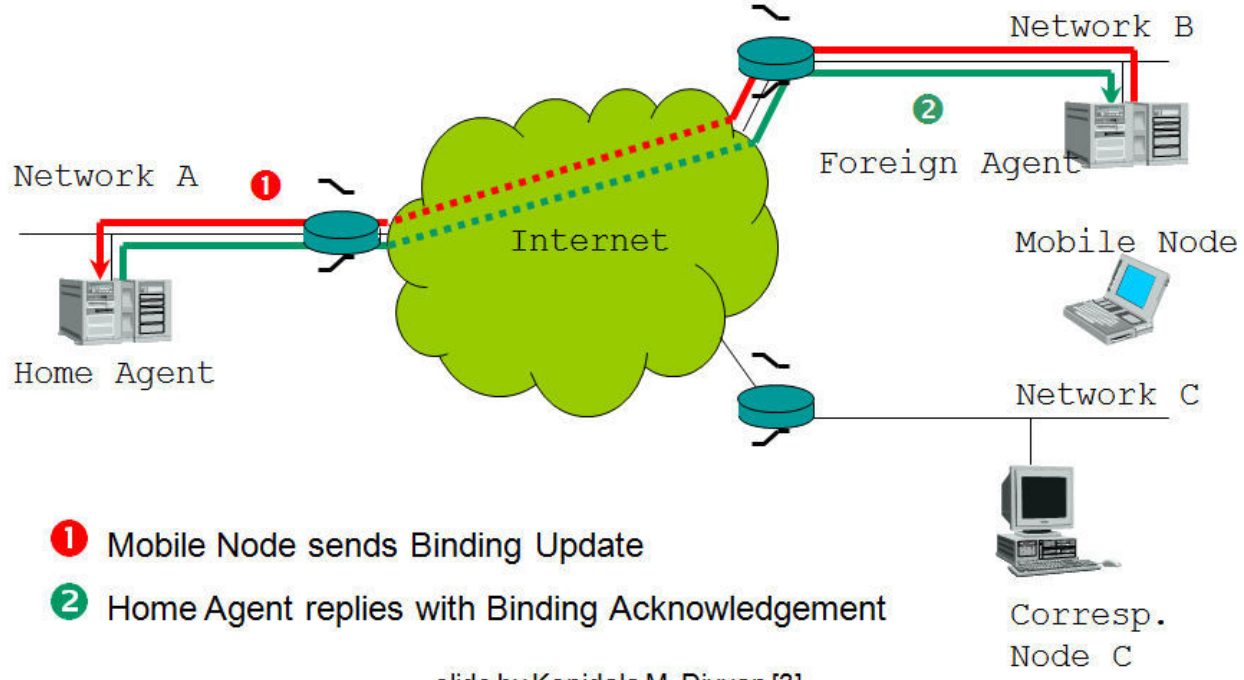
**Mobile IP: Basics, Cont.**

- Correspondent host is a host that wants to send packets to the mobile host
- Correspondent host sends packets to the mobile host's IP permanent address
- These packets are routed to the mobile host's home network
- Home agent forwards IP packets for mobile host to current care-of address
- Mobile host sends packets directly to correspondent, using permanent home IP as source IP

**Mobile IP: Care-of Addresses**

- Whenever a mobile host connects to a remote network, two choices:
  - ✓ care-of can be the address of a foreign agent on the remote network
    - o foreign agent delivers packets forwarded from home agent to mobile host
  - ✓ care-of can be a temporary, foreign IP address obtained through, e.g., DHCP
    - o home agent tunnels packets directly to the temporary IP address
- Regardless, care-of address must be registered with home agent

**Mobile Node registers at its Home Agent**




slide by Konidala M. Divyan [3]

**Protocol**

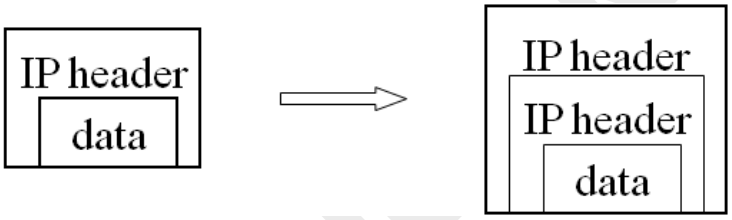
- In order to support mobility, Mobile IP includes three capabilities:
    1. Discovery
        - Mobile Agents send ICMP router advertisements with mobility agent advertisement extension periodically informing mobile nodes of its presence.
        - Mobile node is responsible for the discovery process.
        - In order to receive an advertisement, the mobile node may optionally request one from an agent or simply wait for the next advertisement.
    2. Registration
        - Mobile node recognizes that it is on a foreign network, acquires a Care-of-Address and requests its home agent to forward its data packets to the foreign agent.
        - The process of registration requires 4 steps:
            i. Mobile node request forwarding service by sending registration request to the foreign agent.
            ii. Foreign agent relays this request to the home agent.
            iii. Home agent accepts or denies the request and sends registration reply to the foreign agent.
            iv. Foreign agent relays this reply to Mobile node.
    3. Tunneling
        - After registration, an IP tunnel is set up between the home agent and care-of-address of the mobile node.
        - Home agent broadcasts gratuitous ARP request which causes all nodes in the

subnet to update their ARP caches to map the mobile nodes IP address to the home agents link level address.

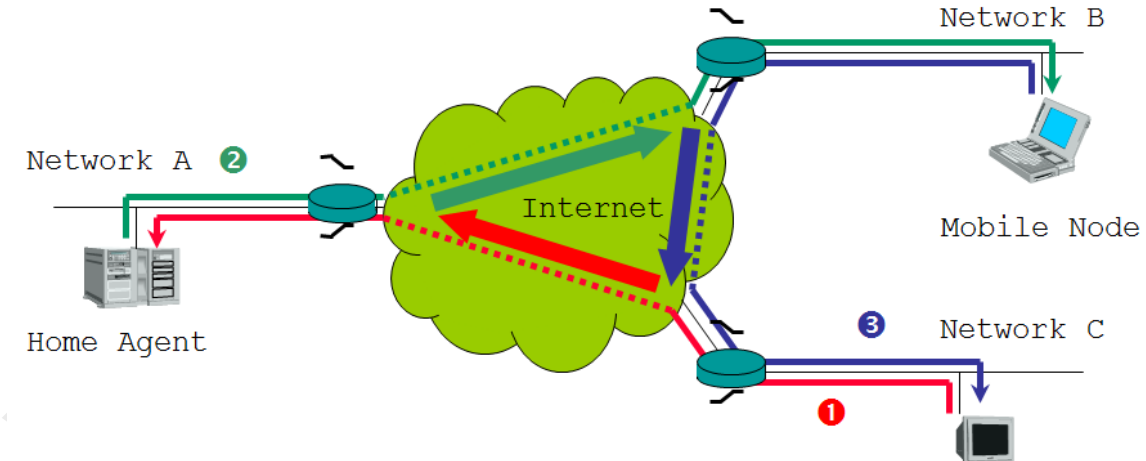
- Thus home agent receives packets destined to the mobile node, and forwards the packets to the foreign agent through the IP tunnel.
- In the foreign network, decapsulation is done by the foreign agent or by the mobile node itself.
- A correspondent node assumes that the reply from the mobile node is coming from its home network and continues to send the packet to the home agent.

**IP-in-IP Tunneling**

- Packet to be forwarded is encapsulated in a new IP packet
- In the new header:
  - ✓ Destination = care-of-address
  - ✓ Source = address of home agent
  - ✓ Protocol number = IP-in-IP

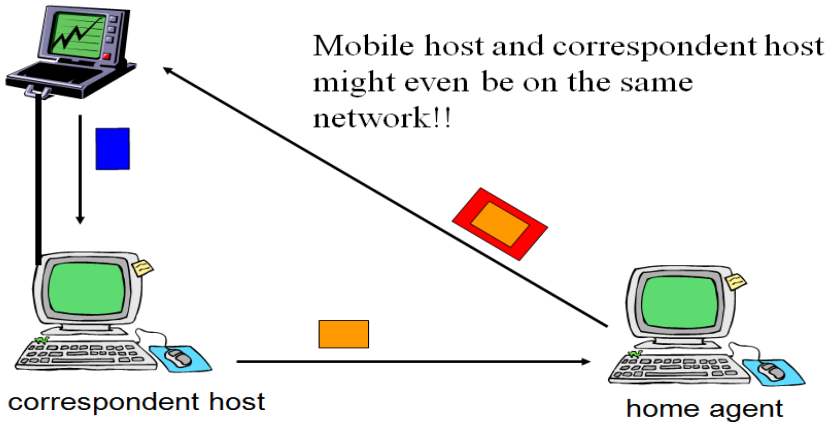



**Triangle Routing (Mobile IPv4)**




1. Corresp. Node C initiates communication with Mobile Node and sends packets to MN's home address
2. Home Agent intercepts packets and forward them to the Mobile Node (proxy functionality)
3. Mobile Node replies directly to Corresp. Node C

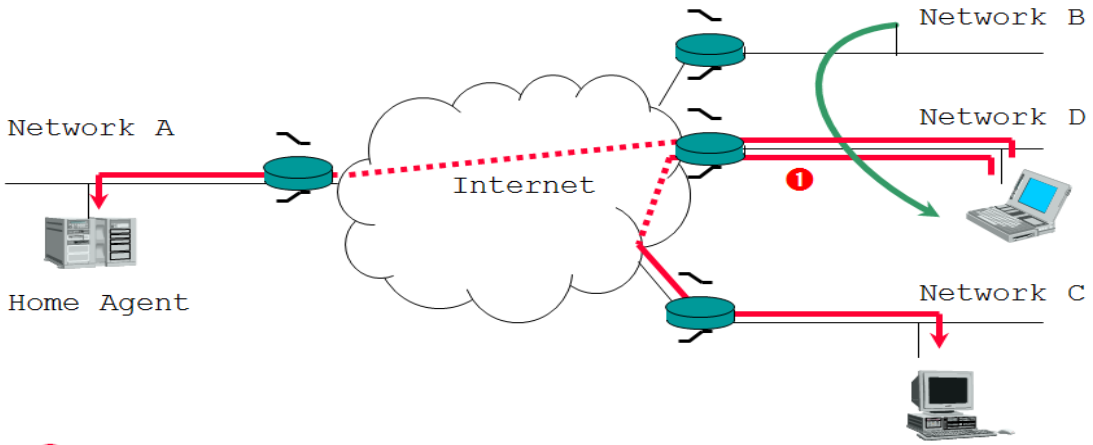
**Routing Inefficiency**




**Route Optimizations**

- Possible Solution:
  - ✓ Home agent sends current care-of address to correspondent host
  - ✓ Correspondent host caches care-of address
  - ✓ Future packets tunneled directly to care-of address
- But!
  - ✓ An instance of the cache consistency problem arises...
  - ✓ Cached care-of address becomes stale when the mobile host moves
  - ✓ Potential security issues with providing care-of address to correspondent

**Mobile IPv6 Roaming**




1 Mobile Node sends Binding Updates to Home Agent and all Corresp. Nodes, which already received a previous Binding Update from this Mobile Node

slide by Konidala M. Divyan [3]

**Summary**

- Last lecture
- Limitations of QoS in IEEE 802.11
- Overview of 802.11e
- Traffic Categories
- EDCF
- HCF
- Mobile IP
    - ✓ Care-of-address,
    - ✓ MIP Protocol (Discovery, Registration, Tunneling)
    - ✓ Routing
    - ✓ Inefficiencies
    - ✓ MIPv6

**Lecture 31**

**Wireless Mesh Networks**

**Outlines**

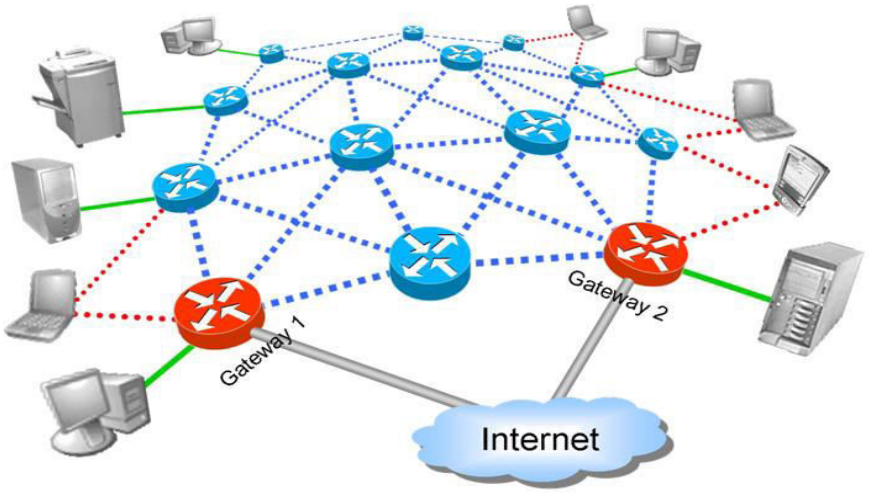
- Introduction to WMN
- Characteristics
- WMN vs MANET
- Architecture
- Applications
- Critical factors influencing performance
- Radio techniques, scalability, QoS, security, Ease of Use, Mesh connectivity

**Last Lecture**

- Limitations of QoS in IEEE 802.11
- Overview of 802.11e
- Traffic Categories
- EDCF
- HCF
- Mobile IP
  - ✓ Care-of-address,
  - ✓ MIP Protocol (Discovery, Registration, Tunneling)
  - ✓ Routing
  - ✓ Inefficiencies
  - ✓ MIPv6

**Introduction**

- Wireless mesh networks (WMNs) comprised of mesh routers and clients
- Mesh clients not only work as host but also perform routing for multi-hop destinations
- Mesh routers support bridge/gateway functionalities enabling integration of WMNs with existing wireless networks such as cellular, WSN, WiMAX etc
- WMN is dynamically self-organized and self-configured
- Conventional nodes e.g. PC, PDA, PocketPC, phones , equipped with wireless NIC can connect directly to mesh routers.
- Without Wireless NIC, Ethernet connection is also possible
- Thus WMN will allow always-on-line anywhere anytime.
- Gaining interest as a possible way of ISPs
- Can be deployed incrementally as needed




Source: NC State university, dept. of computer engineering

- Deploying WMN is not difficult because most of the components/protocols are readily available to some extent e.g. IEEE 802.11, WEP etc.
- However scalability in existing protocol is a great concern.

**Characteristics**

- Multi-hop
  - ✓ To extend the coverage range of wireless networks without sacrificing the channel capacity and non line-of-sight.
- Support for ad hoc networking
  - ✓ Due to flexible architecture, easy deployment and configuration, fault tolerance and mesh connectivity is possible.
  - ✓ Low up-front investment requirements
- Mobility dependence on type of mesh nodes
  - ✓ Mesh routers usually have minimal mobility
  - ✓ Mesh clients can be stationary or mobile
- Multiple type of network access
  - ✓ Both backhaul access to internet and P2P communication are supported
  - ✓ Integration of WMN with other wireless networks allow end-users access to WMN
- Dependence of power-consumption constraints on the type of mesh nodes.
- Compatibility and interoperability with existing wireless networks.
  - ✓ WMN based on IEEE 802.11 should support both mesh clients as well as Wi-Fi clients.
  - ✓ It should also be interoperable with other networks.

**WMNs vs MANET**

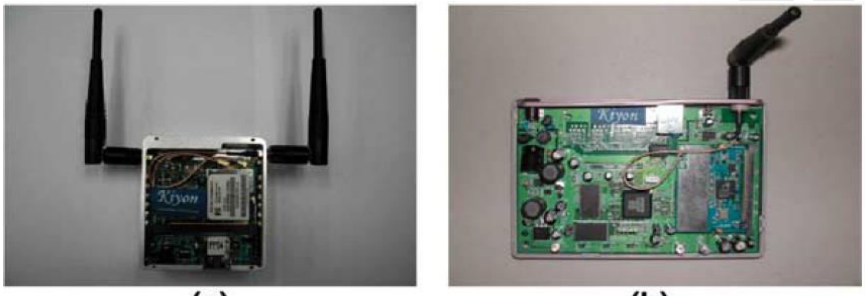
- WMNs are considered ad hoc due to lack of infrastructure (AP/BS).
  - ✓ Although ad hoc techniques like MANET are required but
    - WMNs require more sophisticated algorithms and design principles
    - WMN diversifies the capabilities of ad hoc that makes MANET subset of WMNs
  - ✓ Following differences will illustrate it more

| | |
|---|---|
| Wireless Backbone | Mesh routers as wireless backbone providing more coverage, connectivity and robustness. Individual nodes are routers in MANET making unreliable. |
| Integration | Supports client that use the same radio technology. Which is accomplished through host-routing function available in mesh router<br>Users of one network can enjoy services of other network |
| Dedicated routing and configuration | In MANET, each host perform routing and configurations which is done by mesh routers in WMNs. Hence decreasing load on end-user |
| Multiple radios | Two radios; one for routing and configuration functionalities between mesh routers. Second radio for network access by end users. These are performed on same channel in MANET. This significantly improves the performance |
| Mobility | Hosts also working as router in MANET make it more challenging, where the mobility of mesh routers is very limited |

**Architecture**

- Mesh router
  - ✓ Support routing functions for mesh networking in addition to conventional gateway/repeater functions.
  - ✓ Furthermore, equipped with multiple interfaces built on either same or different wireless access technologies.
  - ✓ Achieves the same coverage as the other wireless routers with less energy consumption through multi-hop routing.
  - ✓ MAC protocols are enhanced with better scalability in multi-hop mesh environment.

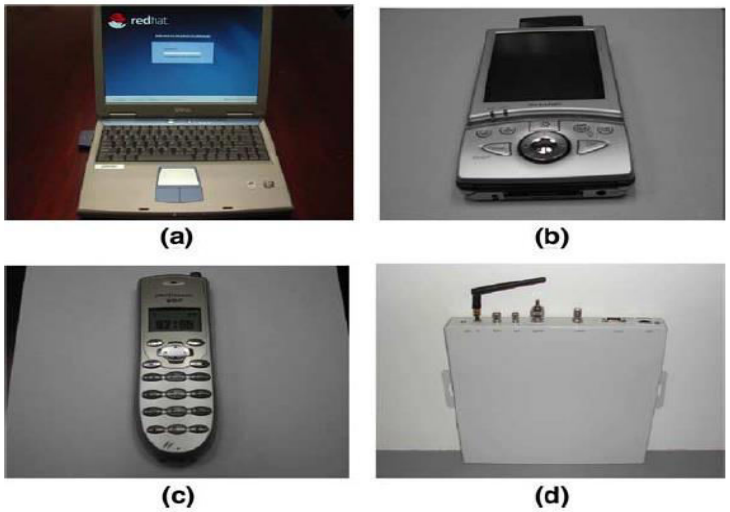
**WMN Routers**



(a) (b)

- Examples of mesh routers based on different embedded systems:
  - ✓ (a) PowerPC and (b) Advanced Risc Machines (ARM)
- Mesh clients
  - ✓ Also have necessary functions for routing in mesh networking.
  - ✓ However gateway or bridge functions do not exist.
  - ✓ Usually single interface

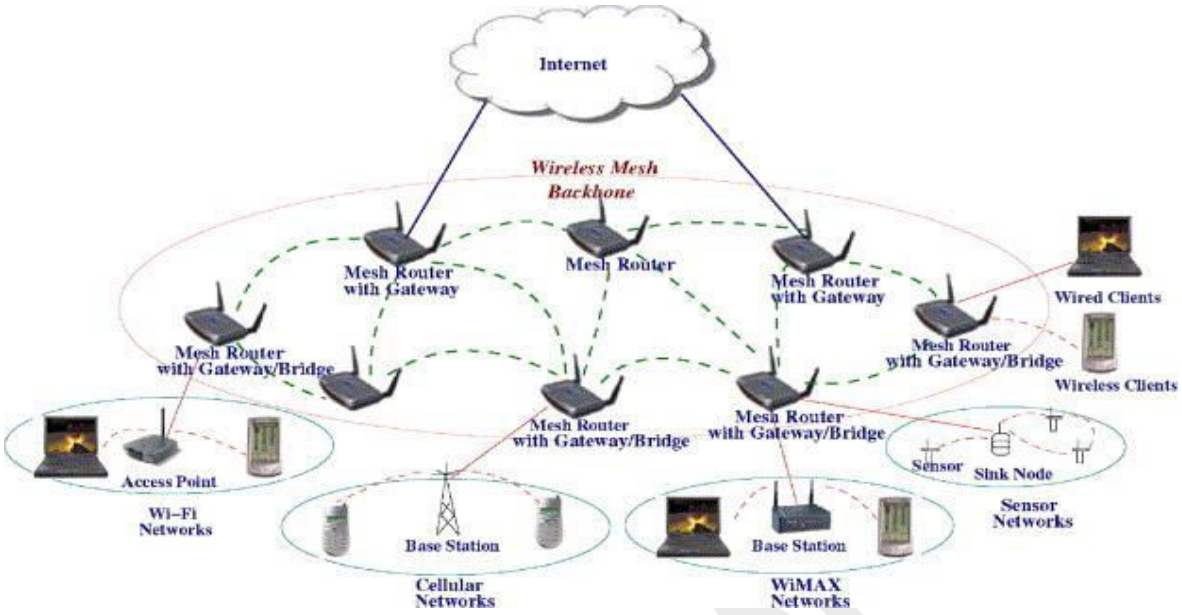
**WMN Clients**



(a) (b) (c) (d)

- Examples of mesh clients: (a) Laptop, (b) PDA, (c) Wi-Fi IP Phone and (d) Wi-Fi RFID Reader.

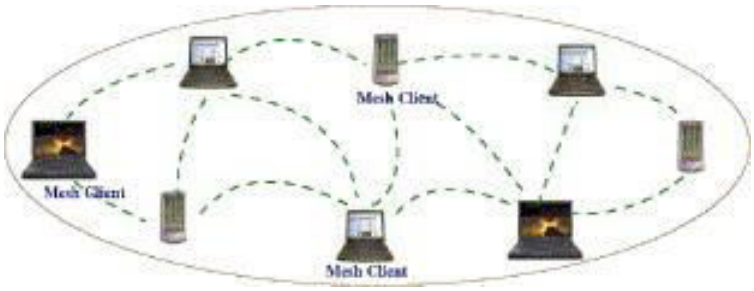
**Infrastructure/backbone WMNs**




- Built using various wireless technologies in addition 802.11
- With gateway functions, mesh router can connect to internet
- Infrastructure meshing allowing integration of different networks.
- If client has different technology then it can connect through BS and BS through Ethernet.
- The most common type. For example, community and neighborhood networks can be built.
  - ✓ Mesh routers can be placed on the roof of houses
  - ✓ Serve as access point for users inside the house and along the roads.
  - ✓ Two types of radio; one for backbone and other for users
  - ✓ Backbone communication can be established using long range and end-user using short range

**Clients WMNs**

- Client meshing provides P2P network among client devices
- No mesh router required.
- Clients in this arch. require more functionalities for configuration and routing
- Formed using single radio.



**Hybrid WMNs**

- Combination of infrastructure and client meshing
- Most applicable/practical scenario

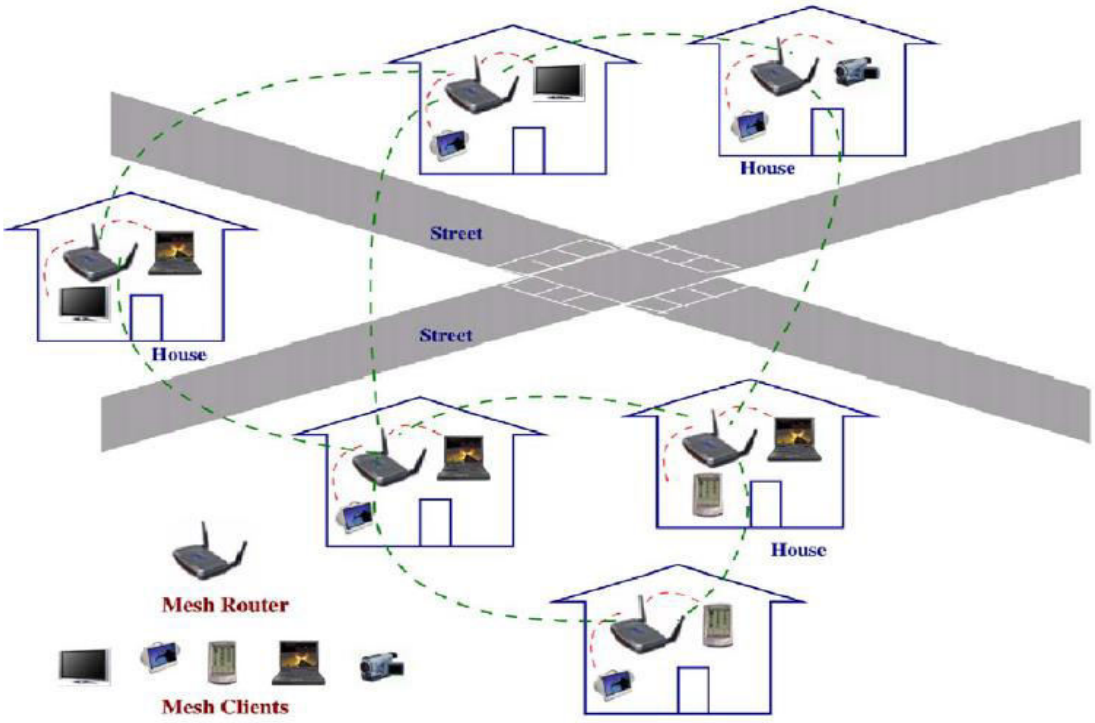

**Application scenario**

- Research and development in WMNs is motivated by several applications which can be supported on cellular, WiMAX etc.

**Broadband home networking**

- WLAN is not practical because AP leave dead zones and multiple APs require backbone network or access hub.
- Dead zones can be eliminated with multiple routers and adjusting their transmission power.

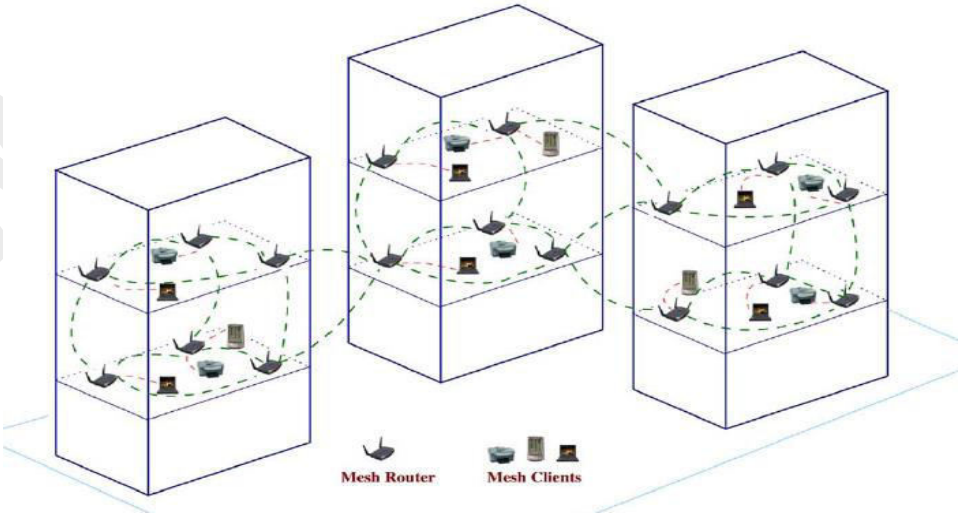
**Community and neighborhood networking**




- The common architecture is to use cable or DSL through internet.
- It has drawbacks
  - ✓ All traffic must flow through internet
  - ✓ Dead zones
  - ✓ Services between end-users can not be shared.
  - ✓ Single path for internet and neighborhood user

**Enterprise networking**

- Scalable with enterprise growth



**Other applications**

- Transportation system
- Instead of limiting access to stations, WMNs can extend access into buses, trains, ferries.
- Remote monitoring of in-vehicle security video and passenger information system
- Building automation
- Health and medical system
- Security surveillance system

**Critical factors influencing network performance**

- Radio techniques
  - ✓ Directional and smart antennas
  - ✓ MIMO systems
  - ✓ Multi-radio chipsets
  - ✓ More advanced techniques such as reconfigurable radios, cognitive radios
  - ✓ These require revolutionary design changes in higher layers
- Scalability
  - ✓ Multihop routing is common in WMN, which degrades performance.
  - ✓ IEEE 802.11 MAC is not scalable and throughput significantly reduces as number of hops increases to 4 or higher
- Mesh connectivity
  - ✓ Network self-organization and topology control algorithms are needed
- Broadband and QoS
  - ✓ Different from ad hoc networks, most applications of WMN are broadband services with various QoS requirements.
- Compatibility and inter-operability
  - ✓ Network access to both conventional and mesh clients
- Security
  - ✓ No centralized control
- Ease of use

**Summary**

- Introduction to WMN
- Characteristics
- WMN vs MANET
- Architecture
- Applications
- Critical factors influencing performance
  - ✓ Radio techniques, scalability, QoS, security, Ease of Use, Mesh connectivity

**Lecture 32**

**Wireless Mesh Networks Part II**

**Outlines**

- MAC Layer
  - ✓ Scalability
  - ✓ Single Channel
  - ✓ Multi-Channel
  - ✓ Some Ideas
  - ✓ Research Issues
- Network Layer
  - ✓ Routing
  - ✓ Wish List
  - ✓ Route Optimization Criteria
  - ✓ Routing fairness
  - ✓ Routing – Cross-layer design
- QoS Support at each layer
- WMN Standards

**Last Lecture**

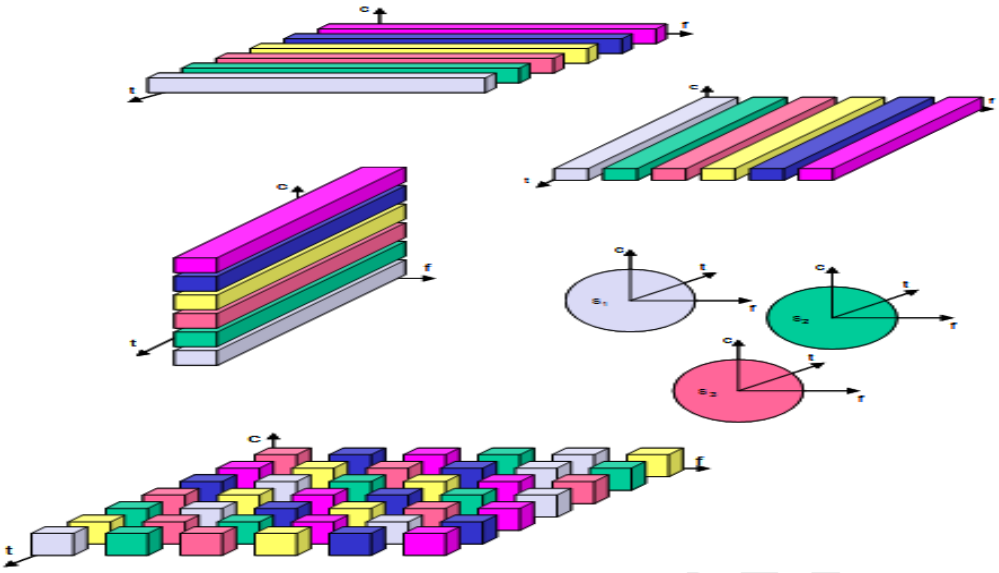
- Introduction to WMN
- Characteristics
- WMN vs MANET
- Architecture
- Applications
- Critical factors influencing performance
  - ✓ Radio techniques, scalability, QoS, security, Ease of Use, Mesh connectivity

**MAC Layer**

- MAC for WMNs is concerned with more than one hop communication.
- MAC is distributed and cooperative and works for multipoint-to-multipoint communication.
- Network self-organization is needed for the MAC.
- Mobility affects the performance of MAC
- The scalability of MAC can be addressed in two ways.
  - ✓ Enhance the existing or propose new for single channel to increase E2E throughput
  - ✓ Allow transmission on multiple channels of each network node

**Basic Techniques**

- Scheduled
  - ✓ Fix scheduled TDMA
  - ✓ Polling
  - ✓ Impractical due to lack of:
    - o Central coordination point
    - o Reasonable time synchronization
- Random Access
  - ✓ CSMA – simple and popular
  - ✓ RTS/CTS – protects the receiver
- Channels can be implemented by:
  - ✓ FDMA
  - ✓ CDMA (code assignment is an issue)
  - ✓ SDMA (with directional antennas)
  - ✓ Combinations of the above

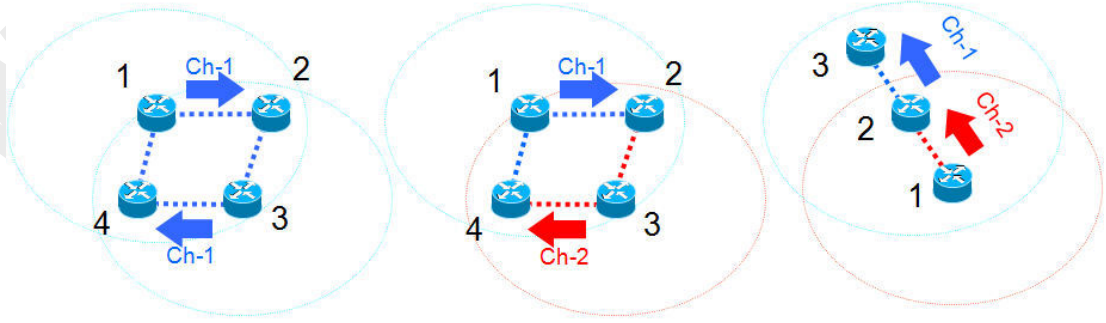


**Single channel MAC**

- Improving existing MAC protocol
  - ✓ By changing parameters of CSMA/CA based MACs like contention window size and backoff procedures for multi-hop.
  - ✓ Contention based approaches are not scalable and throughput degrades with increase in contention.
- Cross-layer design with advanced physical layer.
  - ✓ MAC based on directional antenna and power control
- Innovative solutions
  - ✓ Need new ideas to overcome low end-end throughput for multi-hop ad hoc environment.
  - ✓ TDMA or CDMA based MAC needs to be explored.
  - ✓ Compatibility, cost and complexity are the important factors in designing new protocols

**MAC – Multichannel Why?**

- Increases network capacity

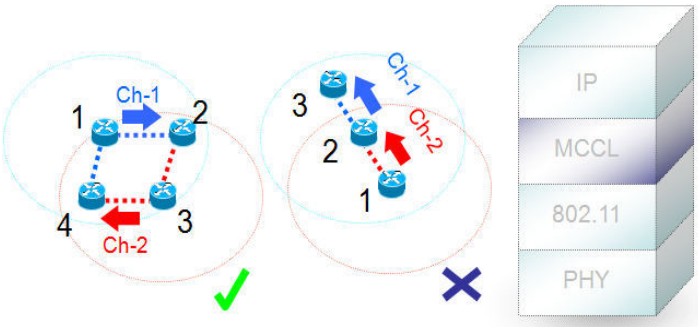



User bandwidth = B/2 User bandwidth = B Chain bandwidth = B

- B = bandwidth of a channel

**MAC – Multichannel**

- Perhaps, if a new Multi-Channel Coordination Layer (MCCL) is introduced b/w MAC and Network
- Must work within the constraints of 802.11
- May increase the capacity of the network




**Multi-channel MAC (MMAC)**

- Multi-channel single transceiver
  - ✓ One channel active at a time
  - ✓ Different nodes may operate on different times.
  - ✓ Hence, coordination is required
- Multi-channel multi-transceiver
  - ✓ A radio includes multiple parallel RF chips and baseband processing modules to support several simultaneous channels.
  - ✓ On top of multiple channel in physical layer, only single MAC to coordinate operations.
- Multi-radios MAC
  - ✓ A node has multiple radios each with its own MAC and physical.
  - ✓ A virtual MAC protocol such as a multi-radio unified MAC protocol is required to coordinate communication among all.

**MMAC Functions**

- Maintaining data structure of all channels in each node.
  - ✓ Classified into three types depending on its status of allocation.
- Negotiating channels during ad hoc traffic indication message (ATIM) window.
  - ✓ Negotiations are done through a pre-defined channel known to all nodes.
- Selecting a channel.
  - ✓ The criterion is to use a channel with the lowest count of source–destination pairs that have selected the channel.

**Multi-radio Unification Protocol**

- Discovering neighbours.
  - ✓ After the discovering procedures, neighbours are classified into MUP enabled and legacy nodes.
- Selecting a NIC
  - ✓ Based on one-hop round trip time (RTT) measurements. MUP selects the NIC with the

shortest RTT between a node and its neighbors.

- Utilizing the selected NIC for a long period.
  - ✓ This period is determined by a random process and in the order of 10–20 s.
- Switching channels.
  - ✓ After the random time period, all NICs are measured again through one-hop probe messages. If an NIC has a certain amount of quality improvement than the existing NIC, then it is selected for sending packets.

**Open research issues**

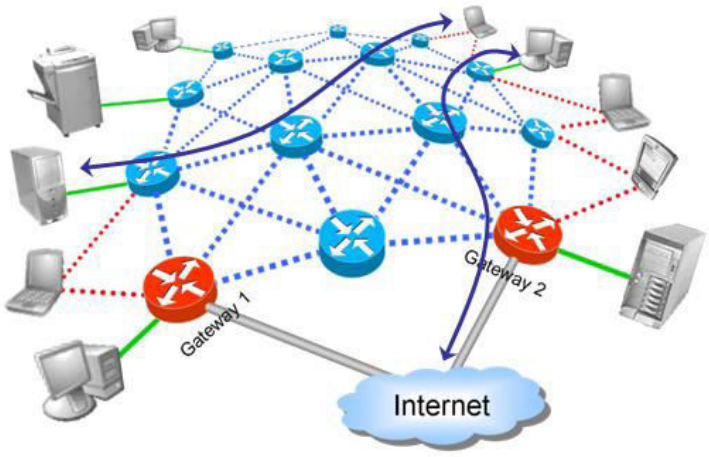
- Scalability issue in multi-hop ad hoc network has not been solved yet.
- CSMA/CA based MAC protocols solve partial problems
- A distributed TDMA or CDMA MAC can be the solution.
- Mesh routers and clients hold different characteristics like mobility, power consumption etc.
- A single solution may not be applicable for both.
- Some Mesh routers integrate various wireless networking technologies and require advance bridging functions
- Existing research focuses on capacity, throughput and fairness. But many applications may require broadband multimedia communication in WMNs.
- MAC developed with QoS metrics

**Network Layer**

- WMN will be tightly coupled with internet and IP has been widely accepted in different wireless networks.
- However routing differs from IP and cellular.

**Routing**

- Finds and maintains routes for data flows
- The entire performance of the WMN depends on the routing protocol
- May be the main product of a mesh company
- May be missing

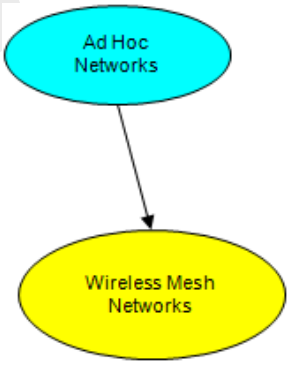


**Routing – Wish List**

- Scalability
  - ✓ Overhead is an issue in mobile WMNs.
- Fast route discovery and rediscovery
  - ✓ Essential for reliability.
- Mobile user support
  - ✓ Seamless and efficient handover
- Flexibility
  - ✓ Work with/without gateways, different topologies
- QoS Support
  - ✓ Consider routes satisfying specified criteria
- Multicast
  - ✓ Important for some applications (e.g., emergency response)

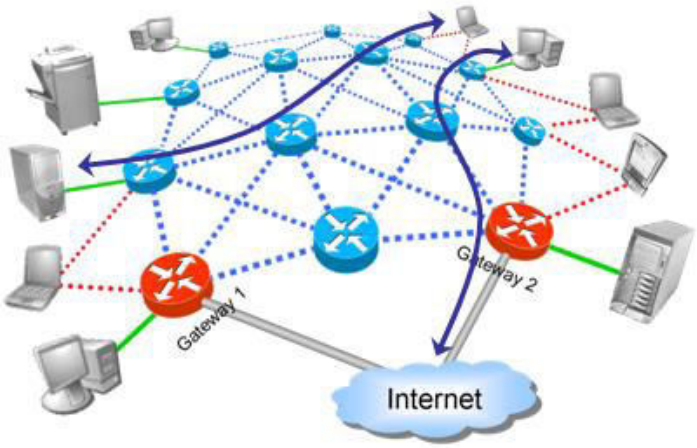
**Existing Routing Protocols**

- Internet routing protocols (e.g., OSPF, BGP, RIPv2)
  - ✓ Well known and trusted
  - ✓ Designed on the assumption of seldom link changes
  - ✓ Without significant modifications are unsuitable for WMNs in particular or for ad hoc networks in general.
- Ad-hoc routing protocols (e.g., DSR, AODV, OLSR, CBR, TORA)
  - ✓ Newcomers by comparison with the Internet protocols
  - ✓ Designed for high rates of link changes; hence perform well on WMNs
  - ✓ May be further optimized to account for WMNs' particularities




**Routing - Optimization Criteria**

- Minimum Hops
- Minimum Delays
- Maximum Data Rates
- Minimum Error Rates
- Maximum Route Stability
- Power Consumption
- Combinations of the above
- Use of multiple routes to the same gateway
- Use of multiple gateways

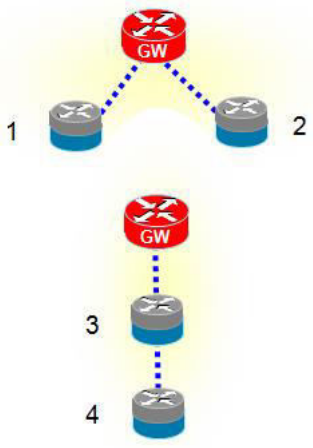



**Routing – Cross-Layer Design**

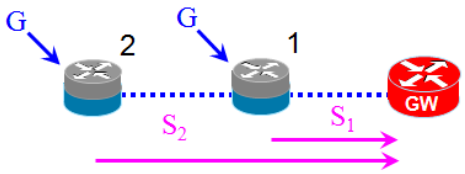
- Routing – Physical
  - ✓ Link quality feedback is shown often to help in selecting stable, high bandwidth, low error rate routes.
  - ✓ Fading signal strength can signal a link about to fail → preemptive route requests.
  - ✓ Cross-layer design essential for systems with smart antennas.
- Routing – MAC
  - ✓ Feedback on link loads can avoid congested links → enables load balancing.
  - ✓ Channel assignment and routing depend on each other.
  - ✓ MAC detection of new neighbors and failed routes may significantly improve performance at routing layer.
- Routing – Transport
  - ✓ Choosing routes with low error rates may improve TCP's throughput.
  - ✓ Especially important when multiple routes are used
  - ✓ Freezing TCP when a route fails.
- Routing – Application
  - ✓ Especially with respect of satisfying QoS constraints

**Network Layer - Fairness**

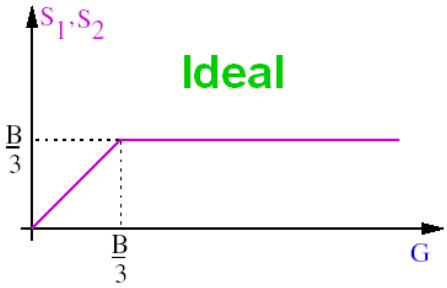
- Fairness
  - ✓ Equal share of resources to all participants.
  - ✓ Special case of priority based QoS.
- Horizontal – nodes 1, 2
  - ✓ The MAC layer's fairness ensures horizontal fairness.
- Vertical – nodes 3, 4
  - ✓ MAC layer is no longer sufficient

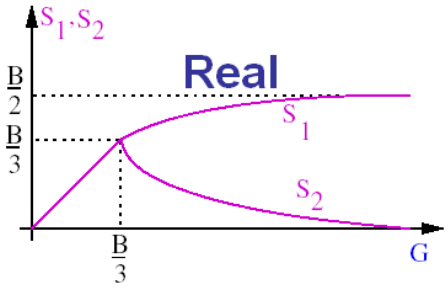


**Fairness Problem**




- Unfair
- Inefficient



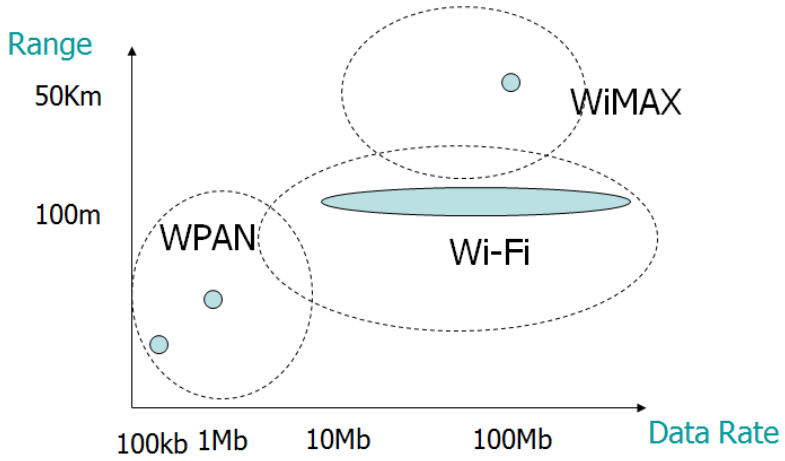




**QoS Support required at every layer**

- Physical Layer
  - ✓ Robust modulation
  - ✓ Link adaptation
- MAC Layer
  - ✓ Offer priorities
  - ✓ Offer guarantees (bandwidth, delay)
- Network Layer
  - ✓ Select "good" routes
  - ✓ Offer priorities
  - ✓ Reserve resources (for guarantees)
- Transport
  - ✓ Attempt end-to-end recovery when possible
- Application
  - ✓ Negotiate end-to-end and with lower layers
  - ✓ Adapt to changes in QoS

**WMNs Standards**

- WPAN: Bluetooth, Zigbee
- WiFi: 802.11a, b, g, n
- WiMAX: 802.16




- IEEE 802.16a WMAN Mesh
  - ✓ "mesh mode" in addition to the point-to-multipoint(PMP) mode defined in IEEE 802.16.
  - ✓ Operating in the licensed and unlicensed lower frequencies of 2–11 GHz, allowing non-line-of-sight (NLO) communications, spanning up to a 50 km range.
  - ✓ Supporting multihop communications.

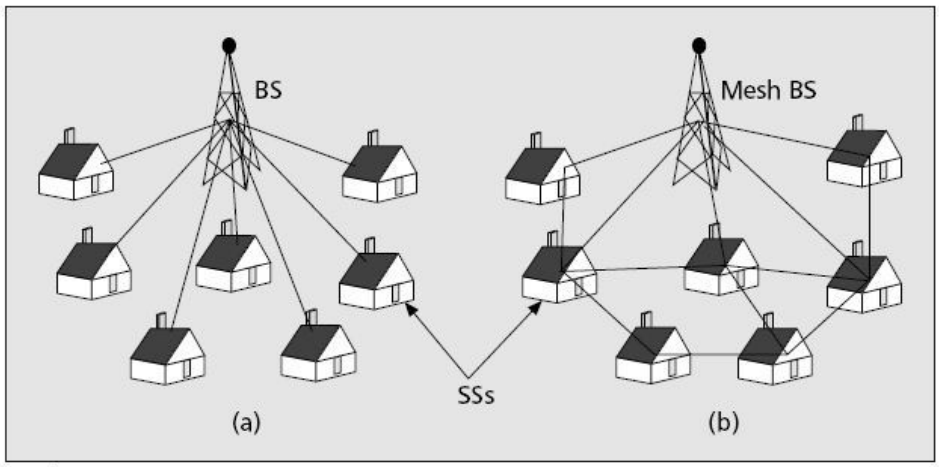
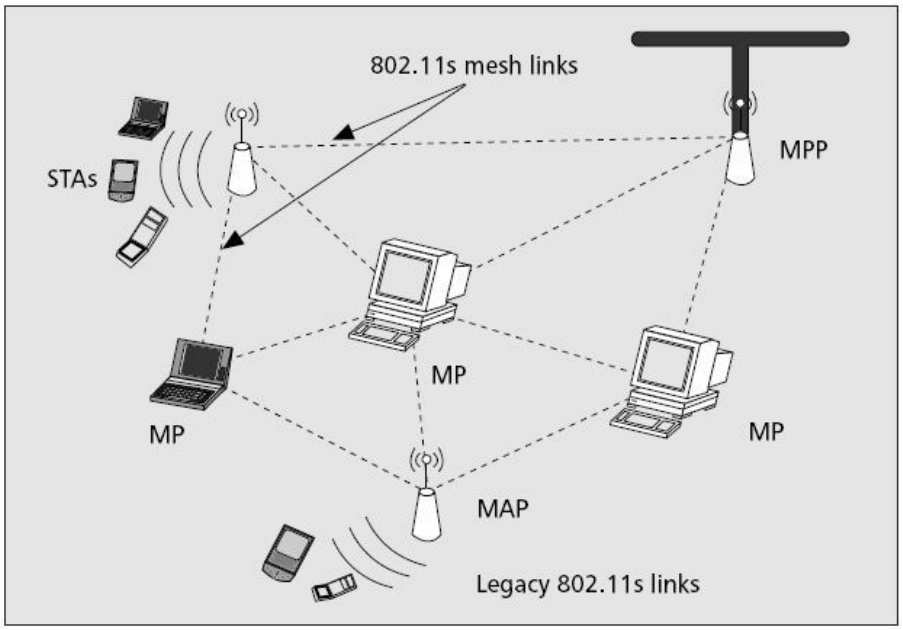
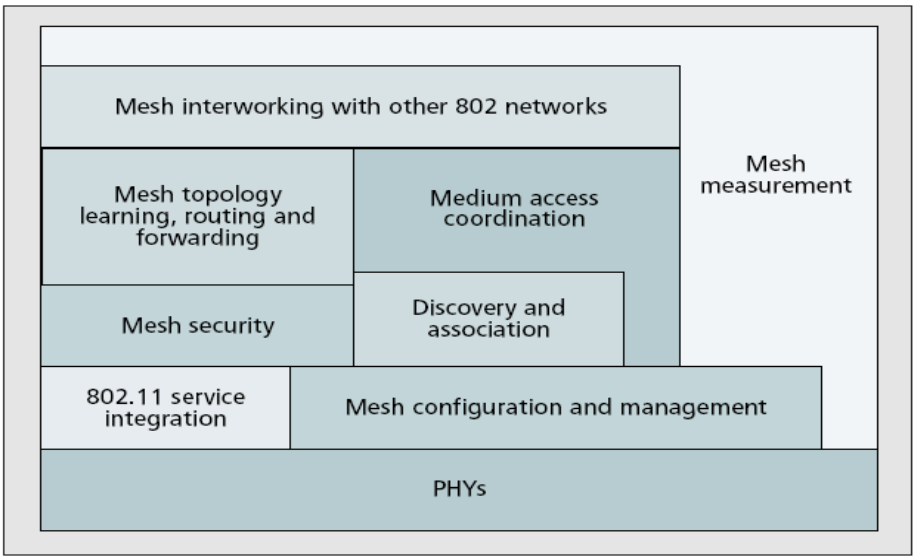



**Figure 1.** *Illustration for the IEEE 802.16a standards: a) point-to-multipoint mode; b) mesh mode.*

- 802.11s WLAN Mesh
  - ✓ MAC layer needs to be extended to a wireless DS to support broadcast/multicast
  - ✓ Multi-hop capability added to 802.11g/a/b
  - ✓ Auto configure on power up
  - ✓ Multi-channel multi-radio operation
  - ✓ Topology discovery
  - ✓ MAC Path selection protocol
  - ✓ Modified forwarding for QOS and mesh control




- 802.11s MCF Sublayer




**Summary**

- MAC Layer
  - ✓ Scalability
  - ✓ Single Channel
  - ✓ Multi-Channel
  - ✓ Some Ideaa
  - ✓ Research Issues
- Network Layer
  - ✓ Routing
  - ✓ Wish List
  - ✓ Route Optimization Criteria
  - ✓ Routing fairness
  - ✓ Routing – Cross-layer design
- QoS Support at each layer
- WMN Standards

**Lecture 33**

**TCP over Wireless Networks**

**Outlines**

- Motivation
- TCP Variants
  - ✓ Slow start
  - ✓ Fast Retransmit/Recovery (TCP Reno)
- Issues in Heterogeneous Wireless Networks
- TCP Schemes for Wireless
  - ✓ Pure Link-level Approaches
  - ✓ Soft-state Transport Layer Caching Approaches
  - ✓ Soft-state Cross Layer Signalling Approaches
  - ✓ Hard-state Transport Layer Approache

**Last Lecture**

- MAC Layer
  - ✓ Scalability
  - ✓ Single Channel
  - ✓ Multi-Channel
  - ✓ Some Ideas
  - ✓ Research Issues
- Network Layer
  - ✓ Routing
  - ✓ Wish List (Scalability, fast route discovery/repair, mobility, flexibility, QoS, Multicast)
  - ✓ Route Optimization Criteria
  - ✓ Routing fairness
  - ✓ Routing – Cross-layer design
- QoS Support at each layer
- WMN Standards

**Motivation**

- Characteristics of wireless networks
  - ✓ Lack of infrastructure in ad hoc networks
  - ✓ Mobility
  - ✓ Shared channel
  - ✓ Limited bandwidth
- Transport protocols typically designed for
  - ✓ Fixed end-systems
  - ✓ Fixed, wired networks
  - ✓ Characteristics of TCP
    - Window-based: not possible to maintain fine-grained timers on a per-flow basis
    - Slow –start
    - Loss-based congestion indication
    - Dependence on ACKs

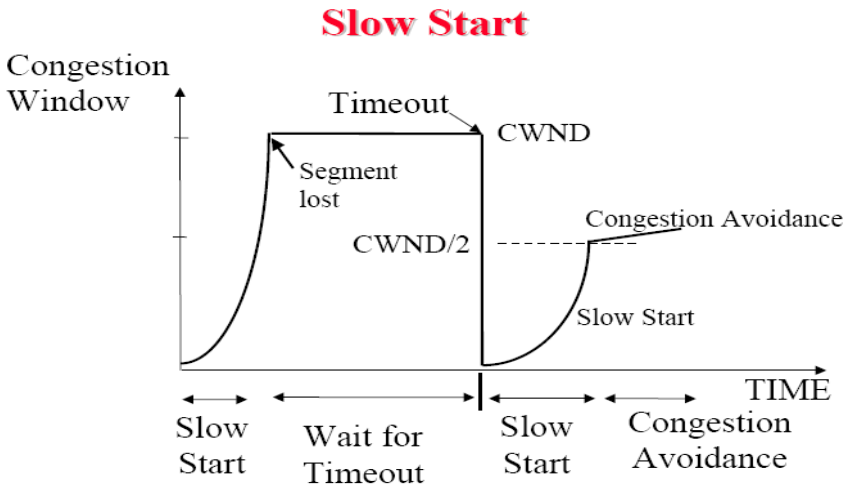
**TCP congestion control**

- Packet loss in fixed networks typically due to overload and is detected as
  1. Retransmission timeout (RTO) at source.
  2. Arrival of three duplicate ACKs at source.
  3. Receipt of ICMP source quench message.

- Routers discard packets as soon as the buffers are full
- TCP recognizes congestion only indirectly via missing acknowledgements
- Retransmissions unwise, they would only contribute to the congestion and make it even worse
- Slow-start algorithm as reaction which slowly converges to optimal bandwidth.

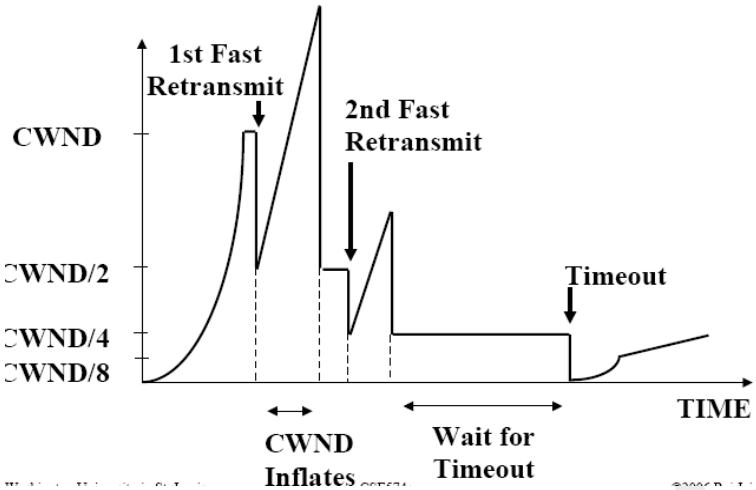
**TCP Slow Start**

- Sender calculates a congestion window for a receiver
- Start with a congestion window size equal to one segment
- Exponential increase of the congestion window up to the congestion threshold, then linear increase
- Missing acknowledgement causes the reduction of the congestion threshold to one half of the current congestion window
- Congestion window starts again with one segment




**TCP Fast Retransmit/Recovery (TCP Reno)**

- TCP sends an acknowledgement only after receiving a packet
- If a sender receives several acknowledgements for the same packet, this is due to a gap in received packets at the receiver
- However, the receiver got all packets up to the gap and is actually receiving packets
- Therefore, packet loss is not due to congestion, continue with current congestion window (do not use slow-start)
- When packet loss occurs, congestion window size is reduced
  - ✓ Due to timeout: cwnd = 1 and enter slow start
  - ✓ Due to duplicate ACKs: cwnd = cwnd/2 + 3×segment_size
- Congestion window size is increased when data is successfully acknowledged




**Issues in Heterogeneous Wireless Networks**

- Bit Error Rate (BER):
  - ✓ 10 or worse are possible upon change in wireless environment
- Bandwidth
  - ✓ Very less as compared to wired networks
  - ✓ TCP underestimated bandwidth in wireless networks
- Round Trip Time (RTT):
  - ✓ The wireless media exhibits longer latencies due to long distances or NLOS path.
  - ✓ Large variation in RTT in wireless networks
- Mobility:
  - ✓ Addition of mobile devices introduces huge amount of indeterminate delay in rather a stationary network.
- Power consumption

**Influences of BER/mobility on TCP**

- TCP assumes congestion if packets are dropped
  - ✓ typically wrong in wireless networks, here we often have packet loss due to *transmission errors*
  - ✓ furthermore, *mobility* itself can cause packet loss, if e.g. a mobile node roams from one access point (e.g. foreign agent in Mobile IP) to another while there are still packets in transit to the wrong access point and forwarding is not possible
  - ✓ The performance of an unchanged TCP degrades severely
- however, TCP cannot be changed fundamentally due to the large base of installation in the fixed network, TCP for mobility has to remain compatible
- the basic TCP mechanisms keep the whole Internet together

**Schemes**

- The various approaches revolve around distinguishing between the following:
  - ✓ Congestion loss
  - ✓ Error loss
  - ✓ Delay beyond the retransmission timer threshold
  - ✓ Out of order delivery beyond the three DUPAK threshold

**Classification**

- Pure Link-level Approaches:
  - ✓ These approaches aim at hiding the unwanted characteristics of the wireless links from the higher layers.
  - ✓ but a critical factor is the determination of the link-level timeout value.
- Soft-state Transport Layer Caching Approaches:
  - ✓ not crucial for the end-to-end connection and use caching as a technique to save the sender from unnecessary invocation of the congestion control mechanism.
  - ✓ but they require changes at the intermediate node (base station) and optionally at the mobile host and fail in the presence of encryption due to the intermediate node's dependence
- Soft-state Cross Layer Signaling Approaches:
  - ✓ These approaches make the transport layer sender aware of the wireless link and separate the congestion losses from the error losses
  - ✓ But involve changes at some or all of the intermediate nodes and at the transport layer of the sender's protocol.
- Hard-state Transport Layer Approaches:
  - ✓ These solutions encompass all forms of splitting and the end-to-end semantics may be sacrificed.
  - ✓ The advantage of these approaches is that the wireless link is completely shielded from damage loss.

**Pure Link-level Approaches**

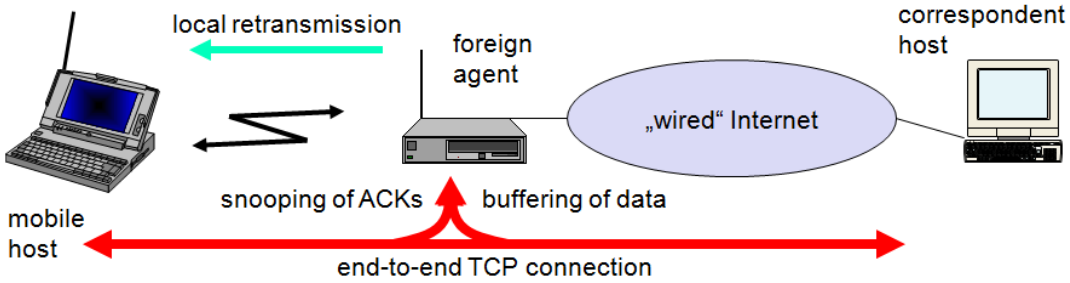
- Reliable link-level protocols are implemented on the wireless link which perform local retransmissions to improve the reliability of communication independent of the higher-level protocols.
  - ✓ These protocols employ techniques such as forward error correction (FEC) for error control
  - ✓ and automatic repeat request (ARQ) for retransmission of lost packets.
- The timeout value for local (link level) retransmissions is of major concern.
  - ✓ Interaction between the link-level retransmission timeouts and the transport-level timeouts for TCP can lead to degraded performance if care is not taken while selecting the timeout values.

**Soft-state Transport Layer Caching Approaches**

- Snoop

**Snooping TCP I**

- it involves modification of the network layer (IP) software at the base station (BS) by adding a module called snoop.
- Transparent extension of TCP within the BS/FA
- buffering of packets sent to the mobile host
- lost packets on the wireless link (both directions!) will be retransmitted immediately by the mobile host or foreign agent, respectively (so called "local" retransmission)
- the foreign agent therefore "snoops" the packet flow and recognizes acknowledgements in both directions, it also filters ACKs
- changes of TCP only within the foreign agent (+min. MH change)




**Snooping TCP II**

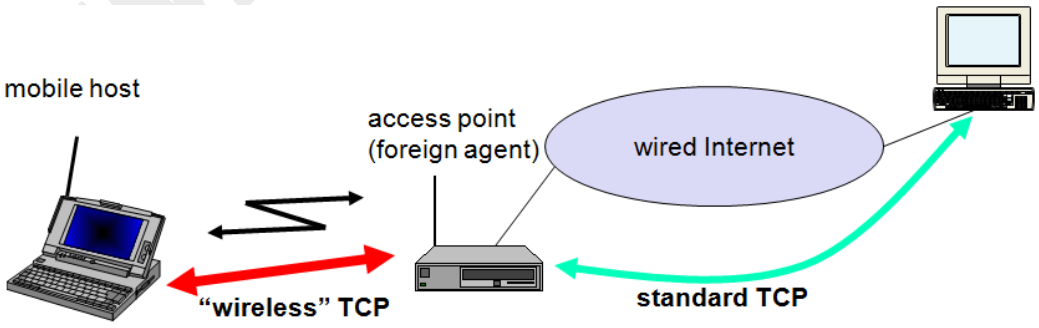
- Data transfer to the mobile host
  - ✓ FA buffers data until it receives ACK of the MH, FA detects packet loss via duplicated ACKs or time-out
  - ✓ fast retransmission possible, transparent for the fixed network
- Data transfer from the mobile host
  - ✓ FA detects packet loss on the wireless link via sequence numbers, FA answers directly with a NACK to the MH
  - ✓ MH can now retransmit data with only a very short delay
- Advantages:
  - ✓ Maintain end-to-end semantics
  - ✓ No change to correspondent node
  - ✓ No major state transfer during handover
- Problems
  - ✓ Snooping TCP does not isolate the wireless link well
  - ✓ Snooping might be useless depending on encryption schemes

**Soft-state Cross Layer Signaling Approaches**

- Explicit Congestion Notification (ECN)
  - ✓ is an extension proposed to Random Early Detection (RED).
  - ✓ marks a packet instead of dropping in when the average queue size is between minth and maxth.
  - ✓ Upon receipt of congestion marked packet, the TCP receiver informs the sender about incipient congestion,
  - ✓ which in turn will trigger the congestion avoidance algorithm at the sender.
- Explicit Bad State Notification (EBSN)
  - ✓ proposes a mechanism to update the TCP timer at the source to prevent source form decreasing its congestion window
  - ✓ EBSN's are sent to the source after every unsuccessful attempt by the base station to transmit packets over the wireless link.
  - ✓ EBSN would cause the previous timeouts to be cancelled and new timeouts put in place, based on existing estimate of round trip time and variance.
- Explicit Loss Notification (ELN)
  - ✓ Add ELN option to TCP acks. When a packet is dropped on the wireless networks,
  - ✓ future cumulative acknowledgements corresponding to the lost packet are marked to identify that a non-congestion related loss has occurred.

**Hard-state Transport Layer Approaches**

- Indirect TCP or I-TCP segments the connection
  - ✓ no changes to the TCP protocol for hosts connected to the wired Internet, millions of computers use (variants of) this protocol
  - ✓ optimized TCP protocol for mobile hosts
  - ✓ splitting of the TCP connection at, e.g., the foreign agent into 2 TCP connections, no real end-to-end connection any longer
  - ✓ hosts in the fixed part of the net do not notice the characteristics of the wireless part.



**Indirect TCP II**

- Advantages
  - ✓ no changes in the fixed network necessary, no changes for the hosts (TCP protocol) necessary, all current optimizations to TCP still work
  - ✓ transmission errors on the wireless link do not propagate into the fixed network
  - ✓ simple to control, mobile TCP is used only for one hop between, e.g., a foreign agent and mobile host
  - ✓ therefore, a very fast retransmission of packets is possible, the short delay on the mobile hop is known
- Disadvantages
  - ✓ loss of end-to-end semantics, an acknowledgement to a sender does not any longer mean that a receiver really got a packet, foreign agents might crash
  - ✓ higher latency possible due to buffering of data within the foreign agent and forwarding to a new foreign agent

**Wireless TCP**

- Preserve the end-to-end semantics.
- This Protocol tries to distinguish Random losses from Congestion losses by measuring the packet inter arrival time with the packet inter departure time.
- WTCP uses rate-based rather than window-based transmission control. Hence it shapes its data traffic,
- Never allows a burst of packet transmissions, and is fair when competing connections have different round-trip times.

**Mobile TCP**

- Special handling of lengthy and/or frequent disconnections with low BER links
- M-TCP splits as I-TCP does
  - ✓ unmodified TCP fixed network to supervisory host (SH)
  - ✓ optimized TCP SH to MH
- Supervisory host
  - ✓ no caching, no retransmission
  - ✓ monitors all packets, if disconnection detected
    - o set sender window size to 0
    - o sender automatically goes into persistent mode
- old or new SH reopen the window
- Advantages
  - ✓ maintains semantics, supports disconnection, no buffer forwarding
- Disadvantages
  - ✓ loss on wireless link propagated into fixed network
  - ✓ adapted TCP on wireless link.

**Ad Hoc Transport Protocol (ATP)**

- Layer coordination
  - ✓ Uses feedback from network nodes for congestion detection, avoidance, and control
- Rate based transmissions
  - ✓ Avoids impact of bursty traffic
- Decoupling of congestion control and reliability
  - ✓ Congestion control uses feedback from the network; Reliability is ensured through receiver feedback and selective ACK
- Assisted congestion control
  - ✓ Adapts sending rate based on feedback from intermediate nodes
- TCP friendliness and fairness
  - ✓ Achieved through feedback from intermediate nodes
  - ✓ But fairness yet an issue

**ATCP Approach**

- ATCP utilizes network layer feedback (from the intermediate nodes) to take appropriate actions
- Network feedback is:
  - ✓ ICMP: The Destination Unreachable ICMP message indicates route disruption
  - ✓ ECN: Indicates network congestion With ECN enabled, time out and 3 dup ACKs are assumed to no longer be due to congestion

**Transport Layer Challenges**

- New transport layer protocols need to be developed that avoids the shortcomings of TCP while being compatible with it
- Transport layer protocols for supporting real-time traffic in wireless meshes are desirable
- Integration of transport layer with other layers; or inferring and reacting with respect to the observations at other layers
- Impact of mobility on transport layer

**Summary**

- Motivation
- TCP Variants
  - ✓ Slow start
  - ✓ Fast Retransmit/Recovery (TCP Reno)
- Issues in Heterogeneous Wireless Networks
- TCP Schemes for Wireless
  - ✓ Pure Link-level Approaches
  - ✓ Soft-state Transport Layer Caching Approaches
  - ✓ Soft-state Cross Layer Signaling Approaches
  - ✓ Hard-state Transport Layer Approaches

**Lecture 34**

**Wireless Sensor Networks Part I**

**Outline**

- Introduction to WSN
- Applications of WSN
- Factors Influencing Performance of WSN
  - ✓ Power consumption, fault tolerance, scalability, topology, cost
- Architecture and Communication Protocols
- Challenges in WSNs.

**Last Lecture Review**

- Motivation
  - ✓ Fixed-end systems, fixed wired network, window-based, slow-start, loss-based congestion control
- TCP Variants
  - ✓ Slow start
  - ✓ Fast Retransmit/Recovery (TCP Reno)
- Issues in Heterogeneous Wireless Networks
  - ✓ BER, Bandwidth, variable RTT, Mobility, Power
- TCP Schemes for Wireless
  - ✓ Revolve around distinguishing congestion loss, error loss, delay bounds, dup Acks
  - ✓ Pure Link-level Approaches (FEC/ARQ)
  - ✓ Soft-state Transport Layer Caching Approaches (SNOOP)
  - ✓ Soft-state Cross Layer Signalling Approaches (ECN, EBSN, ELN, ATCP)
  - ✓ Hard-state Transport Layer Approaches (I-TCP, Mobile TCP)

**Introduction to WSNs**

- A sensor network is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it.
- Features:
  - ✓ Random deployment
  - ✓ Self-organizing
  - ✓ Cooperative capabilities
  - ✓ Local computation

**What is a Sensor?**

- Sensor is a small sized, low power, low cost, Micro-Electro-Mechanical Systems (MEMS)
- Which is capable of sensing, computing and communicating.

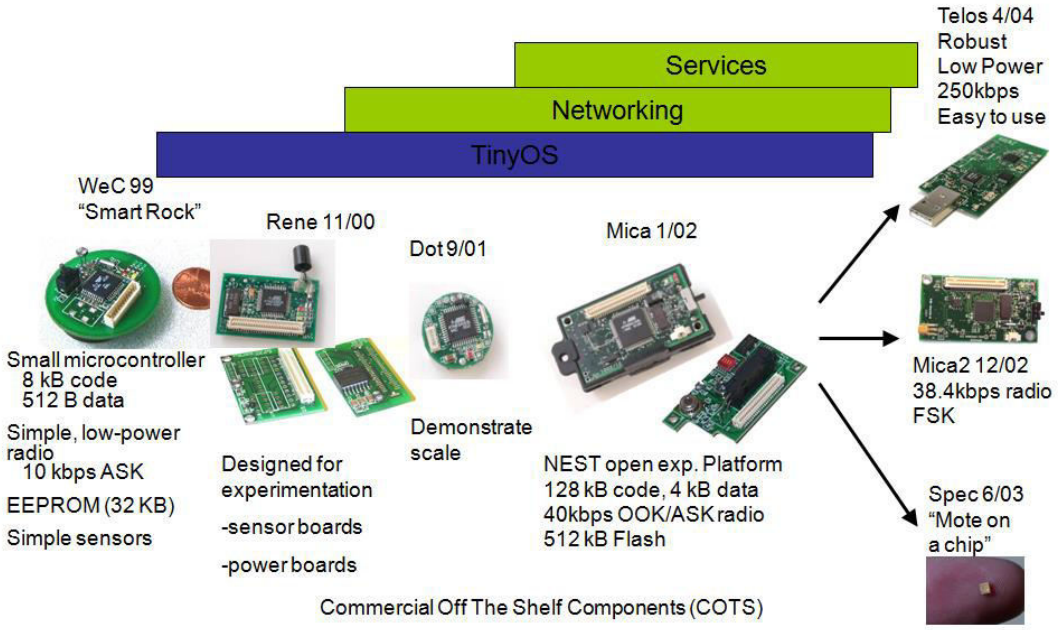
UC Berkeley Motes

MicroStrain X-Link


UC Berkeley: Smart Dust

| | |
|---|---|
| Processor Speed | 8 MHz |
| Flash | 512K bytes |
| SRAM | 8k bytes |
| Radio Frequency | 916 MHz/ 2.4 GHz (ISM) |
| Data Rate | 40 Kbits/Sec (Max) |
| Radio Range | 100 feet |
| Power | 2 x AA batteries |

**Open Experimental Platform**




**Introduction**

Sensor networks VS ad hoc networks:

- Scalability
  - ✓ The number of nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
- Deployment
  - ✓ Sensor nodes are densely deployed.
- Failure Rate
  - ✓ Sensor nodes are prone to failures.
- Highly Dynamic topology
  - ✓ The topology of a sensor network changes very frequently?
- Communication Paradigm
  - ✓ Sensor nodes mainly use broadcast, most ad hoc networks are based on p2p.
- Power Limitation
  - ✓ Sensor nodes are limited in power, computational capacities and memory.
- Unique IDs
  - ✓ Sensor nodes may not have global ID.

**Sensor networks**

- temperature
- humidity
- vehicular movement
- lightning condition
- pressure
- soil makeup
- noise levels
- the presence or absence of certain kinds of objects

**Applications of sensor networks**

- Military applications
  - ✓ Monitoring friendly forces, equipment and ammunition
  - ✓ Battlefield surveillance
  - ✓ Reconnaissance of opposing forces and terrain
  - ✓ Battle damage assessment
  - ✓ Nuclear, biological and chemical attack detection and reconnaissance
- Environmental applications
  - ✓ Forest fire detection
  - ✓ Biocomplexity mapping of the environment
  - ✓ Flood detection
  - ✓ Precision agriculture
- Health applications
  - ✓ Telemonitoring of human physiological data
  - ✓ Tracking and monitoring patients and doctors inside a hospital
  - ✓ Drug administration in hospitals
- Home applications
  - ✓ Home automation
  - ✓ Smart environment
- Other commercial applications
  - ✓ Environmental control in office buildings
  - ✓ Interactive museums
  - ✓ Managing inventory control
  - ✓ Vehicle tracking and detection
  - ✓ Detecting and monitoring car thefts

**Factors influencing sensor network design**

- Fault tolerance
  - ✓ Fault tolerance is the ability to sustain sensor network functionalities without any interruption due to sensor node failures.
  - ✓ The fault tolerance level depends on the application of the sensor networks.
- Scalability
  - ✓ Scalability measures the density of the sensor nodes.
  - ✓ Density = $\mu$ (R) = (N $\pi$ $R^2$)/A

- Production costs
  - ✓ The cost of a single node is very important to justify the overall cost of the networks.
  - ✓ The cost of a sensor node is a very challenging issue given the amount of functionalities with a price of much less than a dollar.
- Hardware constraints

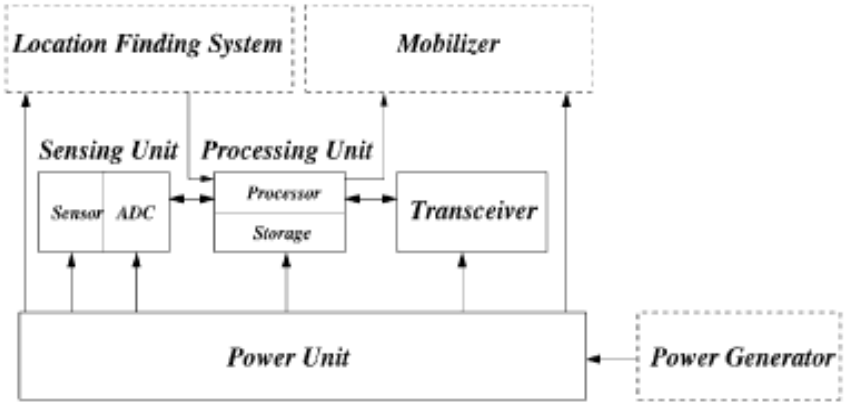
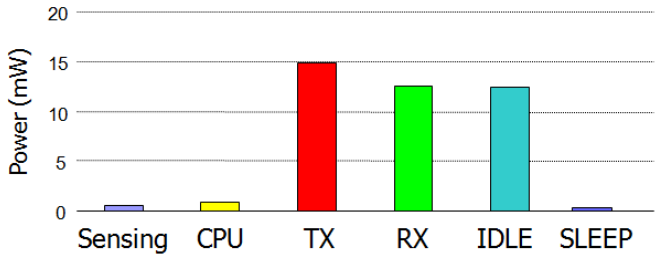



Fig. 1. The components of a sensor node.

- Sensor network topology
  - ✓ Pre-deployment and deployment phase
  - ✓ Post-deployment phase
  - ✓ Re-deployment of additional nodes phase
- Power consumption
  - ✓ Sensing
  - ✓ Communication
    - 3000 instructions can be executed for the same energy cost of sending a bit 100m by radio.
- Data processing

**Energy Consumption**

- Sensor node has limited energy supply
- Nodes may not be rechargeable
- 3000 instructions can be executed for the same energy cost of sending a bit 100m by radio.




Power consumption of a typical senor node

**Factors influencing sensor network design**

- Environment
  - ✓ Busy intersections
  - ✓ Interior of a large machinery
  - ✓ Bottom of an ocean
  - ✓ Inside a twister
  - ✓ Biologically or chemically contaminated field
  - ✓ Battlefield beyond the enemy lines
  - ✓ Home or a large building
  - ✓ Large warehouse
  - ✓ Fast moving vehicles
  - ✓ Drain or river moving with current.

**Communication architecture of sensor networks**

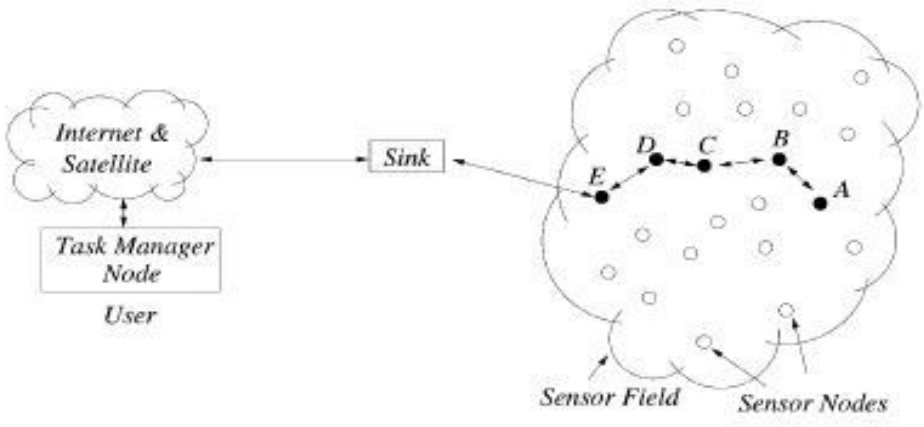



Fig. 2. Sensor nodes scattered in a sensor field.

**Communication architecture of sensor networks**

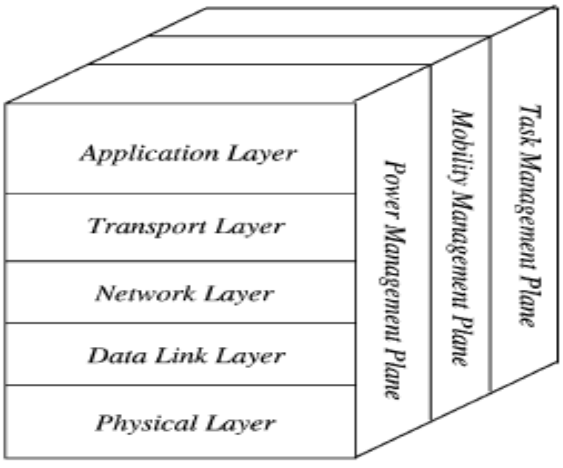


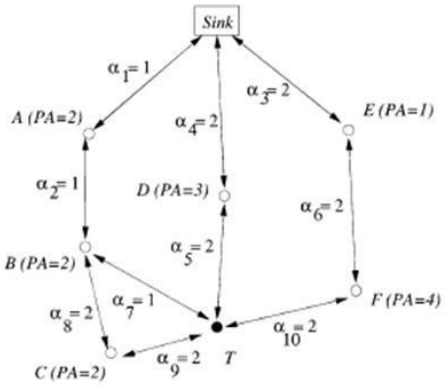

Fig. 3. The sensor networks protocol stack.

**Protocol Stack**

- Power Management Plan
  - ✓ Turning off the receiver after a msg is received from neighbor in order to avoid getting duplicate msg and conserving energy.
  - ✓ Informing neighbor nodes during low battery power.
- Mobility Management Plan
  - ✓ The mobility management plane detects and registers the movement of sensor nodes, so a route back to the user is always maintained, and the sensor nodes can keep track of who are their neighbor sensor nodes.
- Task Management Plan
  - ✓ The task management plane balances and schedules the sensing tasks given to a specific region. Not all sensor nodes in that region are required to perform the sensing task at the same time. As a result, some sensor nodes perform the task more than the others depending on their power level.

**Communication architecture of sensor networks**

- Application layer
  - ✓ An application layer management protocol makes the hardware and software of the lower layers transparent to the sensor network management applications.
  - ✓ Sensor management protocol (SMP)
  - ✓ Task assignment and data advertisement protocol (TADAP)
  - ✓ Sensor query and data dissemination protocol (SQDDP)
- Transport layer
  - ✓ This layer is especially needed when the system is planned to be accessed through Internet or other external networks.
  - ✓ No attempt thus far to propose a scheme or to discuss the issues related to the transport layer of a sensor network in literature.
- Network layer
  - ✓ Power efficiency is always an important consideration.
  - ✓ Sensor networks are mostly data centric.
  - ✓ Data aggregation is useful only when it does not hinder the collaborative effort of the sensor nodes.
  - ✓ An ideal sensor network has attribute-based addressing and location awareness.
- Maximum available power (PA) route: Route 2
- Minimum energy (ME) route: Route 1
- Minimum hop (MH) route: Route 3
- Maximum minimum PA node route: Route 3
- Minimum longest edge route: Route 1




- *Route 1*: Sink-A-B-T, total PA = 4, total $\alpha = 3$,
- *Route 2*: Sink-A-B-C-T, total PA = 6, total $\alpha = 6$,
- *Route 3*: Sink-D-T, total PA = 3, total $\alpha = 4$,
- *Route 4*: Sink-E-F-T, total PA = 5, total $\alpha = 6$,

**Communication architecture of sensor networks**

- Data aggregation

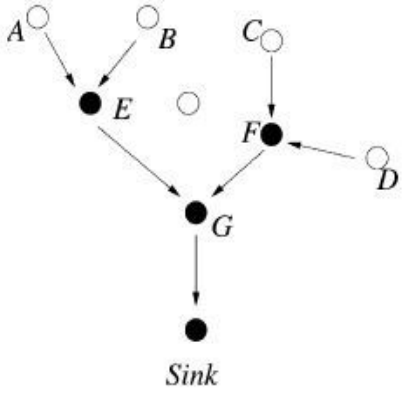


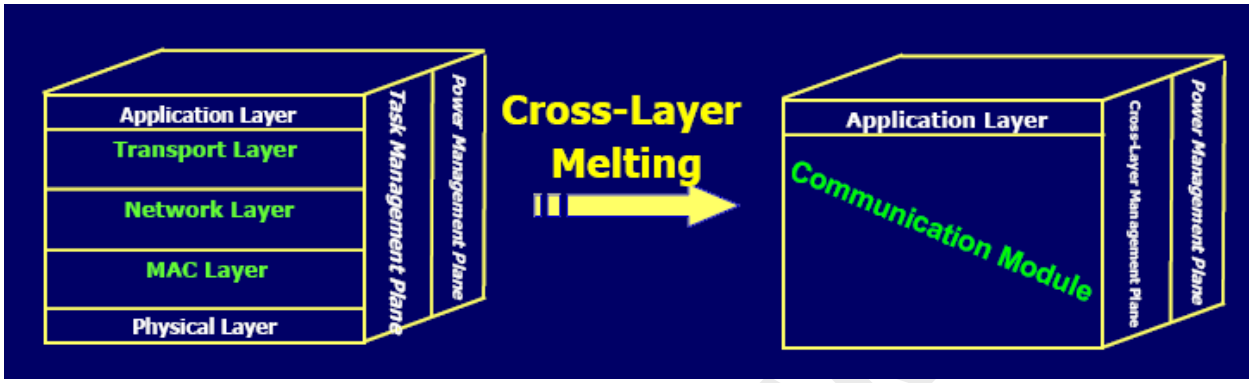

Fig. 5. Example of data aggregation.

**Communication architecture of sensor networks**

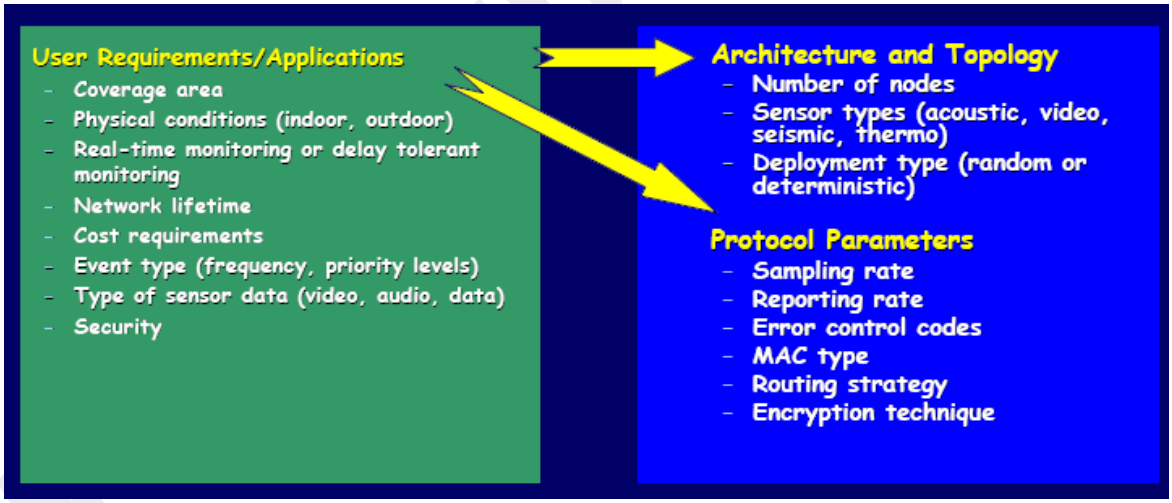
- Data link layer
  - ✓ The data link layer is responsible for the medium access and error control. It ensures reliable point-to-point and point-to-multipoint connections in a communication network.
- Medium access control
  - ✓ Creation of the network infrastructure
  - ✓ Fairly and efficiently share communication resources between sensor nodes
- Power saving modes of operation
  - ✓ Operation in a power saving mode is energy efficient only if the time spent in that mode is greater than a certain threshold.
- Error control
  - ✓ Forward Error Correction (FEC)
  - ✓ Automatic Repeat Request (ARQ).
  - ✓ Simple error control codes with low-complexity encoding and decoding might present the best solutions for sensor networks.

**Challenges in WSN**

- Cross-layer approach: A Grand Challenge
  - ✓ Traditional layered approach is not suitable for WSNs
  - ✓ Good for design, abstraction & debugging
  - ✓ Bad for energy efficiency, overhead & performance




- How to realize mapping?
- User/Applications Requirements →
  - ✓ Arch. & Topology or Communication Protocols
  - ✓ E.g. reliability ?




**Research Directions**

- Topology Control
- Coverage
- Data Aggregation
- Temporal/Spatial Correlation
- Localization / Synchronization
- Energy Efficient Data Dissemination
- QoS Framework
- Network Monitoring and Management
- How to integrate WSNs into NGWI ?

**Simulation for Sensor Networks**

- Simulation provides :
  - ✓ Controlled , Reproducible testing environment
  - ✓ Cost – effective alternative
  - ✓ Means to explore and improve design space

**TinyOS**

- The role of any operating system (OS) is to promote development of reliable application software by providing a convenient and safe abstraction of hardware resources.
- Wireless sensor networks (WSNs) are embedded but general-purpose, supporting a variety of applications, incorporating heterogeneous components, and capable of rapid deployment in new environments
- An open-source development environment
  - ✓ A programming language and model (NesC)
- TOSSIM for simulating TinyOS
- TinyDB for Sensor DB in TinyOS

**Summary**

- Introduction to WSN
- Applications of WSN
- Factors Influencing Performance of WSN
- Architecture and Communication Protocols
- Challenges in WSNs.

**Lecture 35**

**MAC Protocols for WSN Part II**

**Outlines**

- Challenges in WSNs.
- Attributes of MAC Protocol
- Overview of MAC protocols
- Energy Efficiency in MAC
- Proposed Routing Protocol
  - ✓ S-MAC
  - ✓ T-MAC
  - ✓ DS-MAC
  - ✓ Traffic Adaptive MAC
  - ✓ DMAC
  - ✓ Contention-Free MAC

**Last Lecture**

- Introduction to WSN
- Applications of WSN
- Factors Influencing Performance of WSN
  - ✓ Power consumption, fault tolerance, scalability, topology, cost
- Architecture and Communication Protocols

**Research Directions**

- Topology Control
- Coverage
- Data Aggregation
- Temporal/Spatial Correlation
- Localization / Synchronization
- Energy Efficient Data Dissemination
- QoS Framework
- Network Monitoring and Management
- How to integrate WSNs into NGWI ?

**Simulation for Sensor Networks**

- Simulation provides :
  - ✓ Controlled , Reproducible testing environment
  - ✓ Cost – effective alternative
  - ✓ Means to explore and improve design space

**TinyOS**

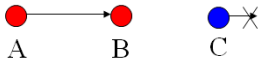
- The role of any operating system (OS) is to promote development of reliable application software by providing a convenient and safe abstraction of hardware resources.
- Wireless sensor networks (WSNs) are embedded but general-purpose, supporting a variety of applications, incorporating heterogeneous components, and capable of rapid deployment in new environments
- An open-source development environment
  - ✓ A programming language and model (NesC)
- TOSSIM for simulating TinyOS
- TinyDB for Sensor DB in TinyOS

**Introduction**

- Important attributes of MAC protocols
- Collision avoidance
  - ✓ Basic task — medium access control
- Energy efficiency
- Scalability and adaptivity
  - ✓ Number of nodes changes overtime
- Latency
- Fairness
- Throughput
- Bandwidth utilization

**Overview of MAC protocols**

- Contention-based protocols
  - ✓ CSMA — Carrier Sense Multiple Access
    - Ethernet
    - Not enough for wireless (collision at receiver)




Hidden terminal: A is hidden from C's CS

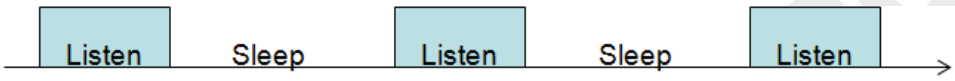
MACA — Multiple Access w/ Collision Avoidance
  - ✓ RTS/CTS for hidden terminal problem
  - ✓ RTS/CTS/DATA
- MACAW — improved over MACA
  - ✓ RTS/CTS/DATA/ACK
    - Fast error recovery at link layer
  - ✓ IEEE 802.11 Distributed Coordination Function
    - Largely based on MACAW
- Protocols from voice communication area
  - ✓ TDMA — low duty cycle, energy efficient
  - ✓ FDMA — each channel has different frequency
  - ✓ CDMA — frequency hopping or direct sequence

**Energy Efficiency in MAC Design**

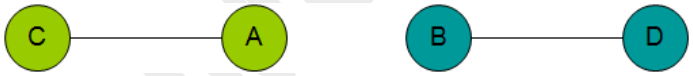
- Energy is primary concern in sensor networks
- What causes energy waste?
  - ✓ Collisions
  - ✓ Control packet overhead
  - ✓ Overhearing unnecessary traffic
  - ✓ Overemitting
  - ✓ Long idle time ⟵ Dominant in sensor nets
    - bursty traffic in sensor-net apps
    - Idle listening consumes 50—100% of the power for receiving (Stemm97, Kasten)

- TDMA vs. contention-based protocols
  - ✓ TDMA can easily avoid or reduce energy waste from all above sources
  - ✓ Contention protocols needs to work hard in all directions
  - ✓ TDMA has limited scalability and adaptivity
    - Hard to dynamically change frame size or slot assignment when new nodes join
    - Restrict direct communication within a cluster
  - ✓ Contention protocols easily accommodate node changes and support multi-hop communications

**S-MAC: Periodic Listen & Sleep**




- Frame
- Duty cycle
  - ✓ (Listen Interval / Frame Length)
- Frame schedule
  - ✓ Nodes are free to choose their listen/sleep schedule
  - ✓ Requirement: neighboring nodes synchronize together
  - ✓ Exchange schedules periodically (SYNC packet)
    - Synchronization period (SP)



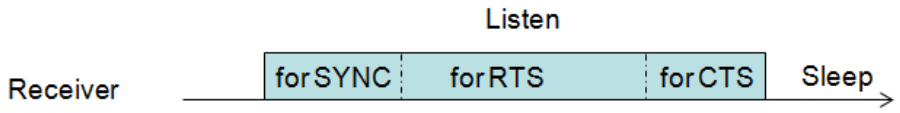

- Nodes communicate in receivers scheduled listen times

**S-MAC: Coordinated Sleeping**

- **Frame Schedule Maintenance**

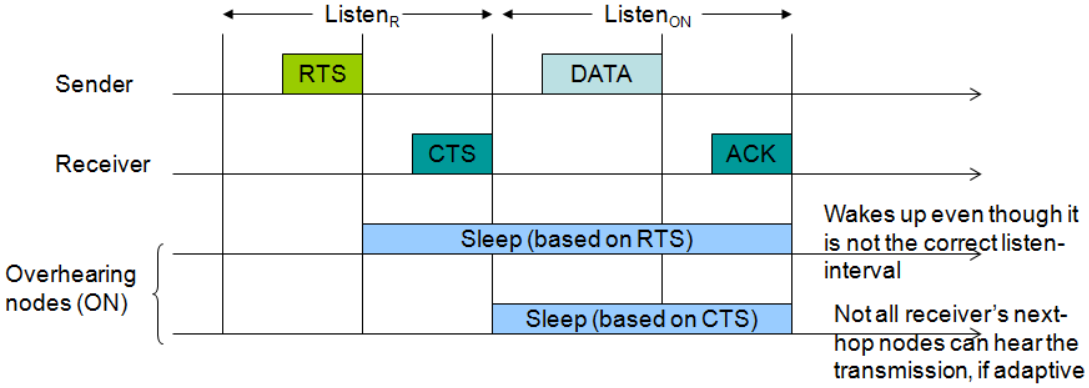
1. Choosing a schedule
   - Listen to the medium for at least SP
   - Nothing heard, choose a schedule
   - Broadcast a SYNC packet (should contend for medium)
2. Following a schedule
   - Receives a schedule before choosing/announcing
   - Follows the schedule
   - Broadcast a SYNC packet
3. Adopting multiple schedules
   - Receives a schedule after choosing/announcing
   - Can discard the new schedule; or
   - Follow both the schedules – suffer more energy loss

- **Maintaining Synchronization**
  - ✓ Clock drifts – not a major concern (listen time = 0.5s – $10^5$ times longer than typical drift rates)
  - ✓ Need to mitigate long term drifts – schedule updating using SYNC packet (sender ID, its next scheduled sleep time – relative);
  - ✓ Listen is split into 2 parts – for SYNC and RTS/CTS



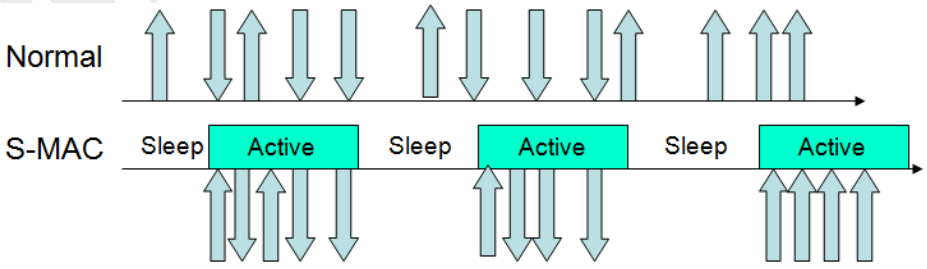

  - ✓ Once RTS/CTS is established, data sent in sleep interval

- **Adaptive Listening – Low-duty cycle to active mode**
  - ✓ Overhearing nodes – wakeup at the end of the current transmission (duration field in RTS/CTS)



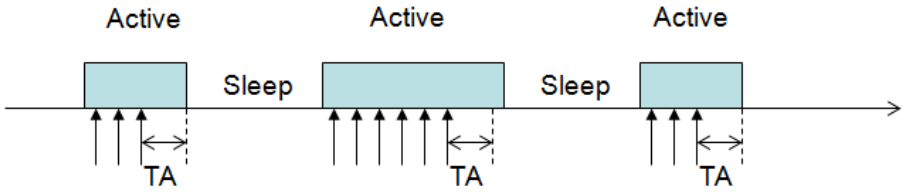

**Drawbacks of S-MAC**

- Active (Listen) interval – long enough to handle to highest expected load
  - ✓ If message rate is less – energy is still wasted in idle-listening
- S-MAC fixed duty cycle – is NOT OPTIMAL
- High Latency



**T-MAC: Preliminaries**

- Adaptive duty cycle:




- A node is in active mode until no activation event occurs for time TA
  - ✓ Periodic frame timer event, receive, carrier sense, send-done, knowledge of other transmissions being ended
- Communication ~= S-MAC/802.11
- Frame schedule maintenance ~= S-MAC

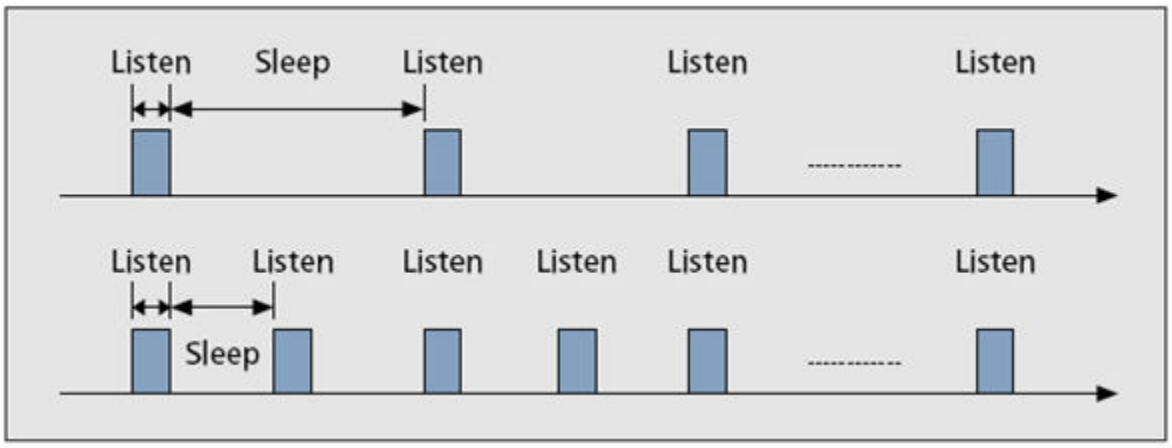
**T-MAC: Choosing TA**

- Requirement: a node should not sleep while its neighbors are communicating, potential next receiver
- TA > C+R+T
  - ✓ C – contention interval length;
  - ✓ R – RTS packet length;
  - ✓ T – turn-around time, time bet. end of RTS and start of CTS;
- TA = 1.5 * (C+R+T);
- Pros
  - ✓ Performs better under variable traffic load
- Cons
  - ✓ Higher overheads than SMAC to maintain variable wakeup schedule.
  - ✓ Unfairness and unpredictable delay.

**Dynamic Sensor-MAC (DSMAC)**

- TMAC improves the latency in SMAC at cost of complexity.
- DSMAC provides simple solution to static duty cycle.
- All nodes start with same duty cycle.
- If one-hop latency is observed higher by receiver, it doubles its duty cycle
- Nodes share their one-hop latency values with neighbors during SYNC period.
- The transmitter also doubles its duty cycle if the destination reported higher one-hop latency.
- This change will not affect the schedule of other neighbors.

**DSMAC Schduling**

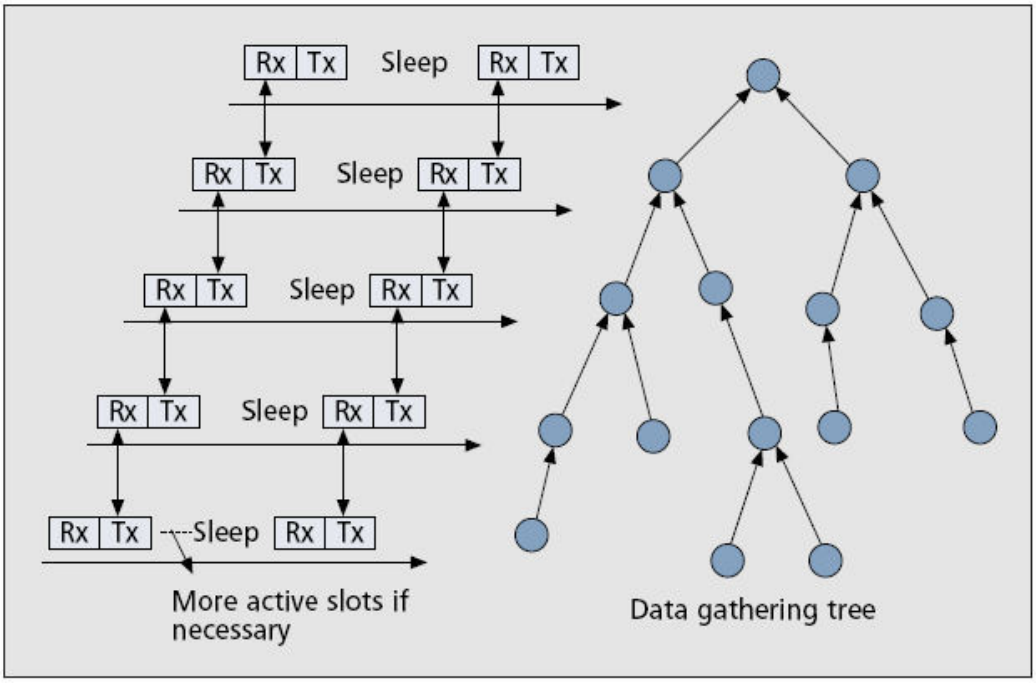



**Traffic-Adaptive MAC (TRAMA)**

- Time is divided into random-access and scheduled-access (transmission) periods.
- The random-access period is used to establish two-hop topology information
- MAC layer can calculate the transmission duration needed, which is denoted as *SCHEDULE_INTERVAL*
- the node calculates the number of slots for which it will have the highest priority among two-hop neighbors
- The node announces the slots it will use as well as the intended receivers for these slots with a *schedule packet*.
- the node announces the slots for which it has the highest priority but it will not use
- The schedule packet indicates the intended receivers using a bitmap whose length is equal to the number of its neighbors
- Advantages
  - ✓ Higher percentage of sleep time and less collision probability are achieved, as compared to CSMA-based protocols.
  - ✓ Since the intended receivers are indicated by a bitmap, less communication is performed for the multicast and broadcast types of communication patterns, compared to other protocols.
- Disadvantages
  - ✓ Transmission slots are set to be seven times longer than the random-access period. This means that without considering the transmissions and receptions, the duty cycle is at least 12.5 percent (idle time),

**DMAC**

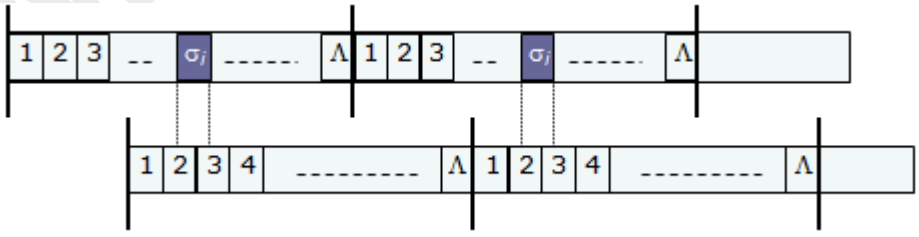
- Supports convergecast communication model,
- Data-aggregation tree is formed from sources to sink node.
- It is an improved slotted ALOHA algorithm.
- Slots are allotted according to the level of tree from leaf to root.
- It incurs low latency but no collision avoidance for nodes at same level



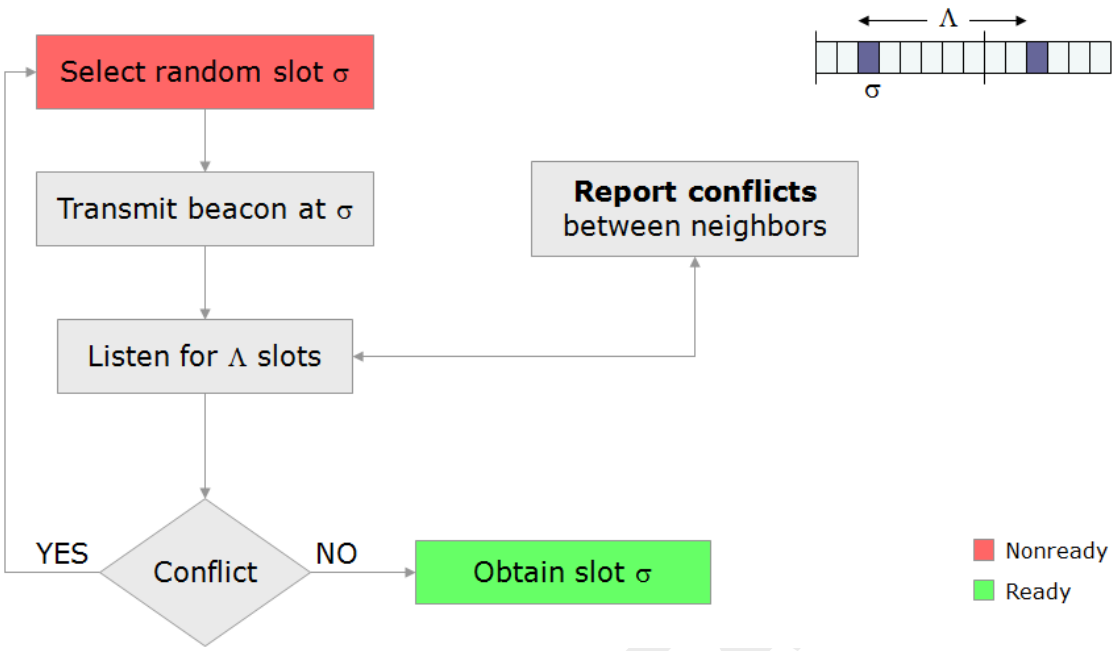

- A minimum period u consists of one packet tx and rx.
- Wakeup period in three is skewed depending on depth d. so du is the wakeup time
- Node at higher layer will be in rx state when lower layer nodes are in tx state
- Nodes on path wakeup sequentially to forward packet to next hop: low latency with efficient energy consumption

**Contention-Free MAC protocols for Wireless Sensor Networks**

- Asynchronous Slot Assignment
  - ✓ Each node locally *discretizes* its local time.
  - ✓ The number of slots in a time frame, called the *frame size* and denoted by $\Lambda$, is set to $2\delta_2$.
  - ✓ Having the same frame size at all nodes ensures that overlapping time slots remain the same.

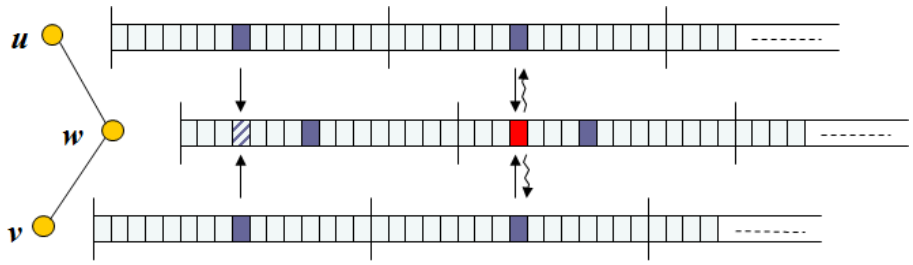


**ASAND – Basic Approach**




- *The basic idea behind ASAND protocol is demonstrated in the figure. A node first discretizes its local time into equal sized frames, each consisting of Λ slots. The main task for node i is to select a conflict-free time slot in its frame. When this occurs we say that the node is ready.*
- *Initially, node i is nonready and it selects randomly and uniformly a slot σi in its frame. In slot σi, node i broadcasts a "beacon" message mi to its neighborhood. In all other slots in the current frame, it listens to the channel and marks each slot in which a garbled signal is received. Then in the next frame, i transmits in all slots that were marked in the previous frame. We call this technique conflict reporting, and it effectively forces hidden terminals to refrain from obtaining overlapping time slots.*
- *If node i's initial broadcast in slot σi was collision-free, then i concludes that none of its neighbors has selected an overlapping time slot. Then, i broadcasts a second time in slot σi in the next frame. If this is also collision-free, then i concludes that none of its 2-hop neighbors selected a time slot conflicting with σi. Hence, the random slot selected by node i is conflict-free in its 2-neighborhood and i becomes ready. Otherwise, when i detects a collision in either its first or second broadcast, it goes back to the initial state and tries a new random slot.*

**ASAND – Conflict Reporting**



- The 2-hop neighbors *u* and *v* are unaware that they have selected conflicting time slots (their transmissions collide on w).
- Having observed a collision in its local time *t*, node *w* transmits at time $t+\Lambda$, creating a *spurious conflict* with both *u* and *v*.
- This is called *conflict reporting* – essentially reduces a conflict between hidden terminals to a conflict between neighbor nodes.
- After $t+\Lambda$, *u* and *v* will be forced to select new slots

- *i reports each collision exactly $\Lambda$ slots after it happened.*
- *This basic approach is a very high level description of the operation of ASAND, which makes it easy to introduce the protocol, but also brings up some fundamental issues that need to be addressed before an actual implementation.*
- *First, it is usually not possible to detect collisions for a wireless device during its own transmission. In Section 6, we propose a novel collision detection scheme based on a special modulation scheme utilizing unique ids of nodes.*

**Summary**

- Challenges in WSNs.
- Attributes of MAC Protocol
- Overview of MAC protocols
- Energy Efficiency in MAC
- Proposed Routing Protocol
  - ✓ S-MAC
  - ✓ T-MAC
  - ✓ DS-MAC
  - ✓ Traffic Adaptive MAC
  - ✓ DMAC
  - ✓ Contention-Free MAC

**Lecture 36**

**Routing in WSN Part III**

**Outlines**

- Routing Challenges and Design Issues
  - ✓ Deployment, Routing method, heterogeneity, fault tolerance, power, mobility etc
- Routing Protocols
  - ✓ SPIN
  - ✓ Directed Diffusion
  - ✓ ACQUIRE
  - ✓ LEACH
  - ✓ TEEN/APTEEN
  - ✓ GAF
  - ✓ GEAR
  - ✓ SPEED

**Last Lecture**

- Challenges in WSNs.
- Attributes of MAC Protocol
- Overview of MAC protocols
- Energy Efficiency in MAC
- Proposed Routing Protocol
  - ✓ S-MAC
  - ✓ T-MAC
  - ✓ DS-MAC
  - ✓ Traffic Adaptive MAC
  - ✓ DMAC
  - ✓ Contention-Free MAC

**Routing challenges and design issues**

- Node deployment
  - ✓ Manual deployment
    - Sensors are manually deployed
    - Data is routed through predetermined path
  - ✓ Random deployment
    - Optimal clustering is necessary to allow connectivity & energy-efficiency
    - Multi-hop routing
- Data routing methods
  - ✓ Application-specific
  - ✓ Time-driven: Periodic monitoring
  - ✓ Event-driven: Respond to sudden changes
  - ✓ Query-driven: Respond to queries
  - ✓ Hybrid
- Node/link heterogeneity
  - ✓ Homogeneous sensors
  - ✓ Heterogeneous nodes with different roles & capabilities
    - Diverse modalities
    - If cluster heads may have more energy & computational capability, they take care of transmissions to the base station (BS)
- Fault tolerance
  - ✓ Some sensors may fail due to lack of power, physical damage, or environmental interference

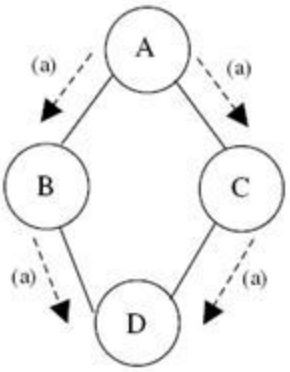
- ✓ Adjust transmission power, change sensing rate, reroute packets through regions with more power

- Network dynamics
  - ✓ Mobile nodes
  - ✓ Mobile events, e.g., target tracking
  - ✓ If WSN is to sense a fixed event, networks can work in a reactive manner
    - o A lot of applications require periodic reporting
- Transmission media
  - ✓ Wireless channel
  - ✓ Limited bandwidth: 1 – 100Kbps
  - ✓ MAC
    - o Contention-free, e.g., TDMA or CDMA
    - o Contention-based, e.g., CSMA, MACA, or 802.11
- Connectivity
  - ✓ High density → high connectivity
  - ✓ Some sensors may die after consuming their battery power
  - ✓ Connectivity depends on possibly random deployment
- Coverage
  - ✓ An individual sensor's view is limited
  - ✓ Area coverage is an important design factor
- Data aggregation
- Quality of Service
  - ✓ Bounded delay
  - ✓ Energy efficiency for longer network lifetime

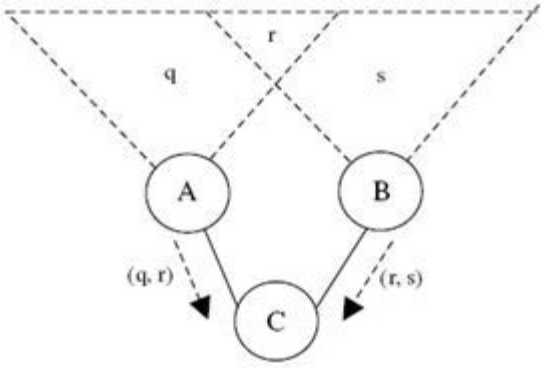
**Routing Protocols in WSNs**

I. Flat
II. Hierarchical
III. Location-based
IV. QoS-based

- Flooding
  - ✓ Too much waste
  - ✓ Implosion & Overlap
  - ✓ Use in a limited scope, if necessary
- Data-centric routing
  - ✓ No globally unique ID
  - ✓ Naming based on data attributes
  - ✓ SPIN, Directed diffusion, ...




- The implosion problem: Node A starts by flooding its data to all of its neighbors. D gets two same copies of data eventually, which is not necessary.




- The overlap problem: Twp sensors cover an overlapping geographic region and C gets same copy of data from these

**SPIN (Sensor Protocols for Information via Negotiation)**

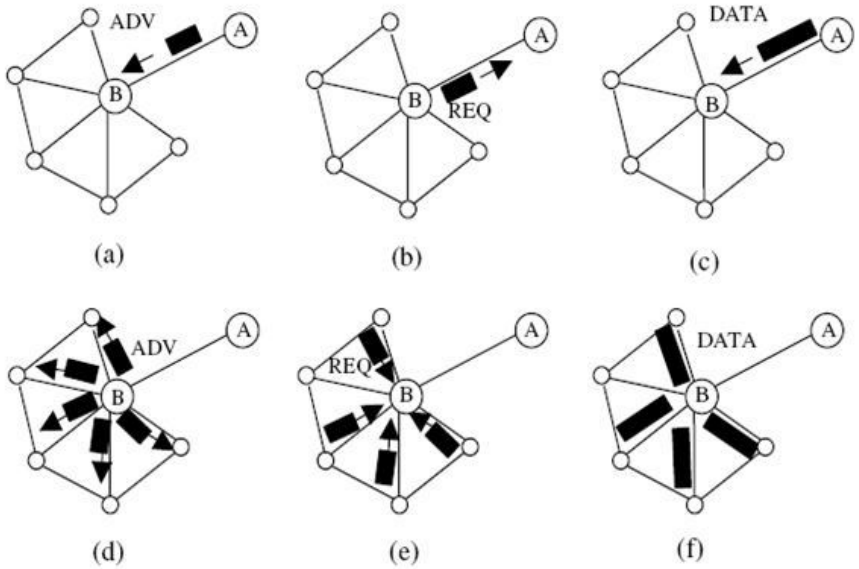



Fig. 3. SPIN protocol. Node A starts by advertising its data to node B (a). Node B responds by sending a request to node A (b). After receiving the requested data (c), node B then sends out advertisements to its neighbors (d), who in turn send requests back to B (e–f).

**SPIN**

- Pros
  - ✓ Each node only needs to know its one-hop neighbors
  - ✓ Significantly reduce energy consumption compared to flooding
- Cons
  - ✓ Data advertisement cannot guarantee the delivery of data
  - ✓ If the node interested in the data are far from the source, data will not be delivered
  - ✓ Not good for applications requiring reliable data delivery, e.g., intrusion detection

**Direct Diffusion: Motivation**

- Properties of Sensor Networks
  - ✓ Data centric
  - ✓ No central authority
  - ✓ Resource constrained
  - ✓ Nodes are tied to physical locations
  - ✓ Nodes may not know the topology
  - ✓ Nodes are generally stationary
- How can we get data from the sensors?

**Elements of Directed Diffusion**

- Naming
  - ✓ Data is named using attribute-value pairs
- Interests
  - ✓ A node requests data by sending interests for named data
- Gradients
  - ✓ Gradients is set up within the network designed to "draw" events, i.e. data matching the interest.
- Reinforcement
  - ✓ Sink reinforces particular neighbors to draw higher quality ( higher data rate) events

**Naming**

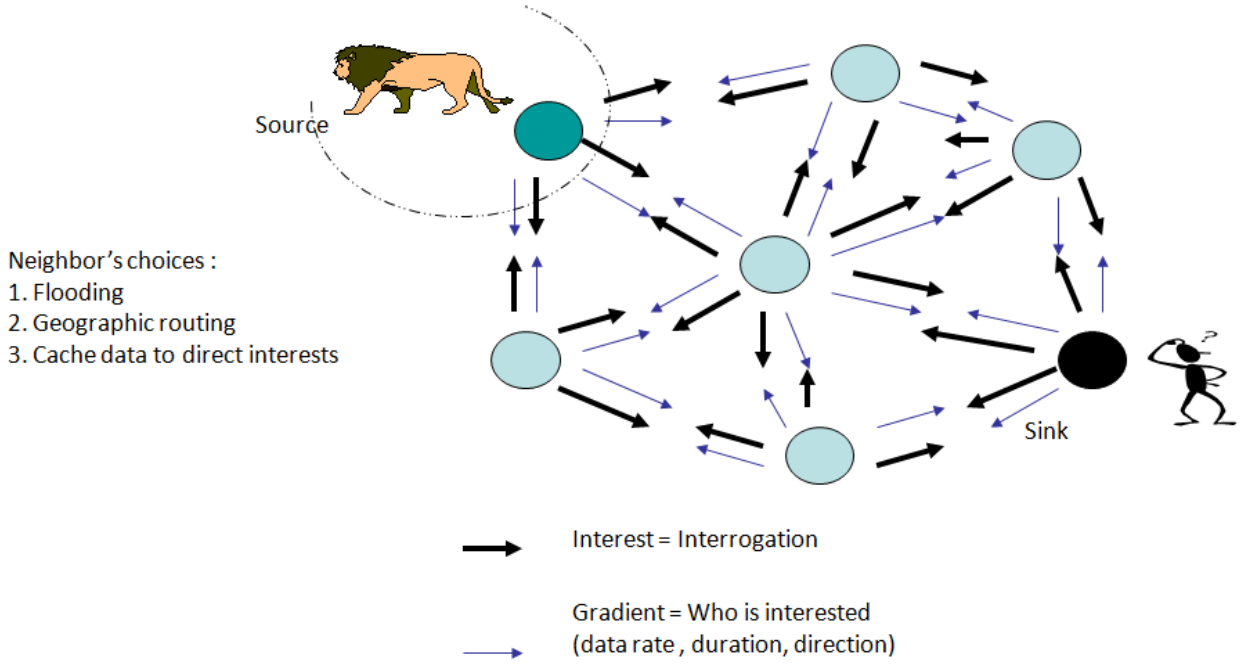
- Content based naming
  - ✓ Tasks are named by a list of attribute – value pairs
  - ✓ Task description specifies an *interest* for data matching the attributes
  - ✓ Animal tracking:

| **Request** | **Reply** |
|---|---|
| Interest ( Task ) Description | Node data |
| Type = four-legged animal | Type =four-legged animal |
| Interval = 20 ms | Instance = elephant |
| Duration = 1 minute | Location = [125, 220] |
| Location = [-100, -100; 200, 400] | Confidence = 0.85 |
| | Time = 02:10:35 |

**Interest**

- The sink *periodically broadcasts* interest messages to each of its neighbors
- Every node maintains an interest cache
  - ✓ Each item corresponds to a distinct interest
  - ✓ No information about the sink
  - ✓ Interest aggregation : identical type, completely overlap rectangle attributes
- Each entry in the cache has several fields
  - ✓ Timestamp: last received matching interest
  - ✓ Several gradients: data rate, duration, direction

**Setting up Gradient**

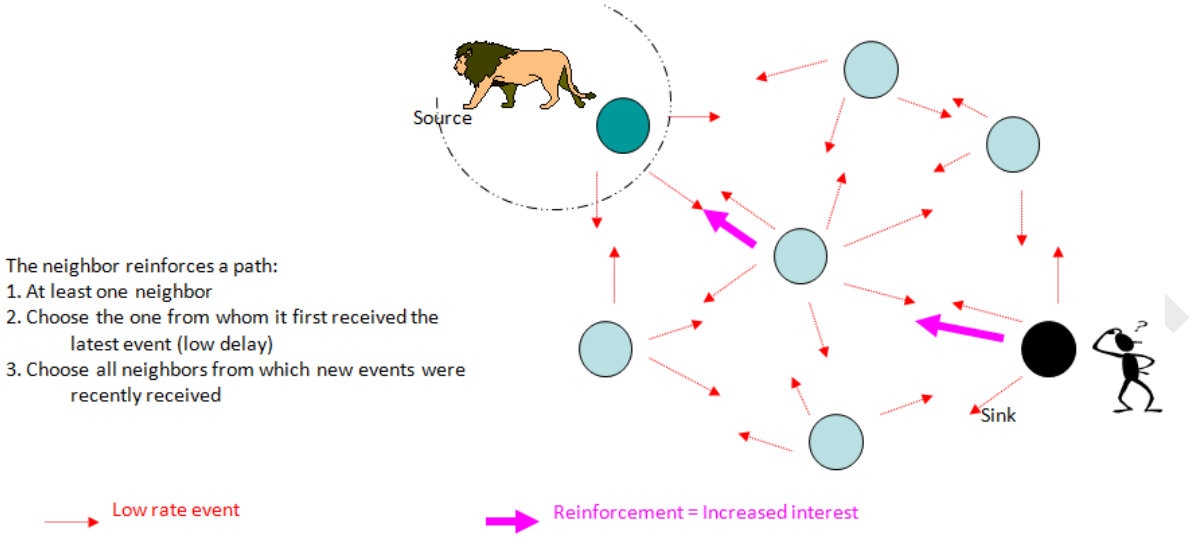



- Introduce sink and source
- The user requests for low-data-rate events
- Interest is sent and propagated. (the black arrow)
- Gradients are set up. (the blue arrow)
- Events are sent along the gradients. (the red arrow)
- The thin red arrow show a low data rate.
- The user reinforces the best path in terms of delay (the green arrow)
- The thick red arrow shows a high data rate.
- Suppose the middle node fail.
- There is no high-data-rate events received.
- The sink reinforces a low-data-rate path to recover from the node failure.

**Data Propagation**

- Sensor node computes the highest requested event rate among all its outgoing gradients
- When a node receives a data:
  - ✓ Find a matching interest entry in its cache
    - Examine the gradient list, send out data by rate
  - ✓ Cache keeps track of recent seen data items (loop prevention)
  - ✓ Data message is unicast individually to the relevant neighbors

**Reinforcing the Best Path**




- Introduce sink and source
- The user requests for low-data-rate events
- Interest is sent and propagated. (the black arrow)
- Gradients are set up. (the blue arrow)
- Events are sent along the gradients. (the red arrow)
- The thin red arrow show a low data rate.
- The user reinforces the best path in terms of delay (the green arrow)
- The thick red arrow shows a high data rate.
- Suppose the middle node fail.
- There is no high-data-rate events received.
- The sink reinforces a low-data-rate path to recover from the node failure.

**Directed Diffusion: Pros & Cons**

- Different from SPIN in terms of on-demand data querying mechanism
  - ✓ Sink floods interests only if necessary
    - A lot of energy savings
  - ✓ In SPIN, sensors advertise the availability of data
- Pros
  - ✓ Data centric: All communications are neighbor to neighbor with no need for a node addressing mechanism
  - ✓ Each node can do aggregation & caching
- Cons
  - ✓ On-demand, query-driven: Inappropriate for applications requiring continuous data delivery, e.g., environmental monitoring
  - ✓ Attribute-based naming scheme is application dependent
    - For each application it should be defined a priori
    - Extra processing overhead at sensor nodes

**ACQUIRE**

- View a WSN as a distributed DB
- Complex queries can be divided into subqueries
- BS sends a query
- Each node tries to answer the query by using precached info and forwards the query to another node
- If the cached info is not fresh, the nodes gather info from their neighbors within a lookahead of d hops
- Once the query is resolved completely, it is sent back to BS via the reverse path or shortest path
- ACQUIRE can deal with complex queries by allowing many nodes send to send responses
    - ✓ Directed diffusion cannot handle complex queries due to too much flooding
    - ✓ ACQUIRE can adjust d for efficient query processing
    - ✓ If d = network diameter, ACQUIRE becomes similar to flooding
    - ✓ In contrast, a query has to travel more if d is too small
    - ✓ Provides mathematical modeling to find an optimal value of d for a grid of sensors, but no experiments performed

**LEACH (Low Energy Clustering Hierarchy)**

- Cluster-based protocol
- Each node randomly decides to become a cluster heads (CH)
- CH chooses the code to be used in its cluster
    - ✓ CDMA between clusters
- CH broadcasts Adv; Each node decides to which cluster it belongs based on the received signal strength of Adv
- CH creates a txmission schedule for TDMA in the cluster
- Nodes can sleep when its not their turn to txmit
- CH compresses data received from the nodes in the cluster and sends the aggregated data to BS
- CH is rotated randomly

**LEACH**

- Pros
    - ✓ Distributed, no global knowledge required
    - ✓ Energy saving due to aggregation by CHs
- Shortcomings
    - ✓ LEACH assumes all nodes can transmit with enough power to reach BS if necessary (e.g., elected as CHs)
    - ✓ Each node should support both TDMA & CDMA
- Extension of LEACH [5]
    - ✓ High level negotiation, similar to SPIN
    - ✓ Only data providing new info is transmitted to BS

**TEEN (Threshold sensitive Energy Efficient Network protocol)**

- Reactive, event-driven protocol for time-critical applications
  - ✓ A node senses the environment continuously, but turns radio on and xmit only if the sensor value changes drastically
  - ✓ No periodic xmission
    - Don't wait until the next period to xmit critical data
    - Save energy if data is not critical
- CH sends its members a hard & a soft threshold
  - ✓ Hard threshold: A member only sends data to CH only if data values are in the range of interest
  - ✓ Soft threshold: A member only sends data if its value changes by at least the soft threshold
  - ✓ Every node in a cluster takes turns to become the CH for a time interval called cluster period
  - ✓ Hierarchical clustering

**Multi-level hierarchical clustering in TEEN & APTEEN**

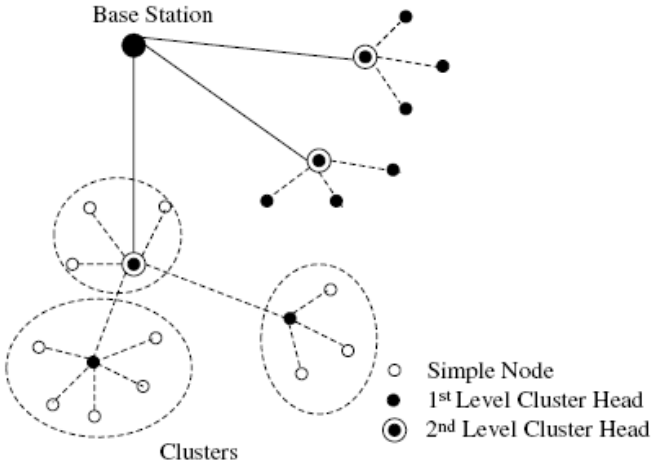



Fig. 8. Hierarchical clustering in TEEN and APTEEN.

**TEEN**

- Good for time-critical applications ☺
- Energy saving ☺
  - ✓ Less energy than proactive approaches
  - ✓ Soft threshold can be adapted
  - ✓ Hard threshold could also be adapted depending on applications
- Inappropriate for periodic monitoring, e.g., habitat monitoring ☹
- Ambiguity between packet loss and unimportant data (indicating no drastic change) ☹

**APTEEN (Adaptive Threshold sensitive Energy Efficient Network protocol)**

- Extends TEEN to support both periodic sensing & reacting to time critical events
- Unlike TEEN, a node must sample & transmit a data if it has not sent data for a time period equal to CT (count time) specified by CH
- Compared to LEACH, TEEN & APTEEN consumes less energy (TEEN consumes the least)
  - ✓ Network lifetime: TEEN ≥ APTEEN ≥ LEACH
- Drawbacks of TEEN & APTEEN
  - ✓ Overhead & complexity of forming clusters in multiple levels and implementing threshold-based functions

**GAF (Geographic Adaptive Fidelity)**

- Energy-aware location-based protocol mainly designed for MANET
- Each node knows its location via GPS
  - ✓ Associate itself with a point in the virtual grid
  - ✓ Nodes associated with the same point on the grid are considered equivalent in terms of the cost of packet routing
  - ✓ Node 1 can reach any of nodes 2, 3 & 4 → 2,3, 4 are equivalent; Any of the two can sleep without affecting routing fidelity

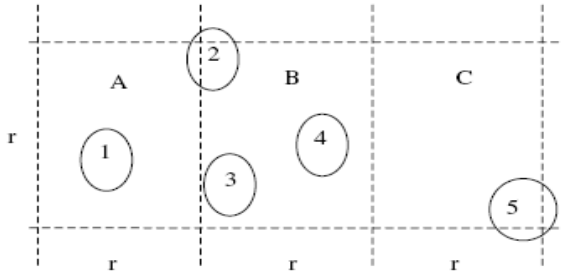



Fig. 11. Example of virtual grid in GAF.

**GAF**

- Three states
  - ✓ Discovery: Determine neighbors in a grid
  - ✓ Active
  - ✓ Sleep
- Each node in the grid estimates its time of leaving the grid and sends it to its neighbors
  - ✓ The sleeping neighbors adjust their sleeping time to keep the routing fidelity

**GEAR (Geographic and Energy Aware Routing)**

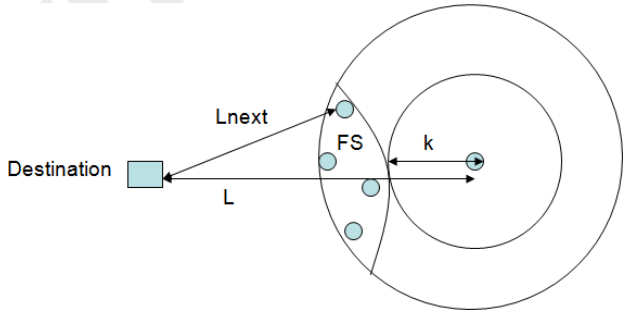
- Restrict the number of interest floods in directed diffusion
  - ✓ Consider only a certain region of the network rather than flooding the entire network
- Each node keeps an estimated cost & a learning cost of reaching the sink through its neighbors
- Estimated cost = f(residual energy, distance to the destination)
- Learned cost is propagated one hop back every time a packet reaches the sink
  - ✓ Route setup for the next packet can be adjusted

**GEAR**

- Phase 1: Forwarding packets towards the region
  - ✓ Forward a packet to the neighbor minimizing the cost function *f*
    - *Forward data to the neighbor which is closest to the sink and has the highest level of remaining energy*
  - ✓ If all neighbors are further than itself, there is a hole → Pick one of the neighbors based on the learned cost
- Phase 2: Forwarding the packet within the target region
  - ✓ Apply either recursive forwarding
    - Divide the region into four subareas and send four copies of the packet
    - Repeat this until regions with only one node are left
  - ✓ Alternatively apply restricted flooding
    - Apply when the node density is low
  - ✓ GEAR successfully delivers significantly more packets than GPSR (Greedy Perimeter Stateless Routing)
    - GPSR will be covered in detail in another class

**SPEED: A real-time routing protocol for WSN**

- Real-time Routing in WSNs
  - ✓ Ensures single hop delay D guarantee
  - ✓ E2E Deadline is D x (L/K+1)
- Cons.
  - ✓ No Energy consideration in FS?
  - ✓ Per hop delay differs greatly?
  - ✓ Coordination?




**Summary**

- Routing Challenges and Design Issues
  - ✓ Deployment, Routing method, heterogeneity, fault tolerance, power, mobility etc
- Routing Protocols
  - ✓ SPIN
  - ✓ Directed Diffusion
  - ✓ ACQUIRE
  - ✓ LEACH
  - ✓ TEEN/APTEEN
  - ✓ GAF, GEAR, SPEED
- Next Lecture
  - ✓ Transport Protocols for WSN / Security Issues

**Lecture 37**

**Transport Protocols/Security in WSN Part IV**

**Outlines**

- Transport Protocols for WSN
- TCP/UDP for WSN
- Protocols
  - ✓ PSFQ
  - ✓ ESRT
  - ✓ CODA
- Security Threats in WSN
- TinySec
- Motivations of Link Layer security
- TinySec Design goals
- Semantic Secure Encryption in TinySec

**Last Lecture**

- Routing Challenges and Design Issues
  - ✓ Deployment, Routing method, heterogeneity, fault tolerance, power, mobility etc
- Routing Protocols
  - ✓ SPIN
  - ✓ Directed Diffusion
  - ✓ ACQUIRE
  - ✓ LEACH
  - ✓
  - ✓ TEEN/APTEEN
  - ✓ GAF
  - ✓ GEAR
  - ✓ SPEED

**Reliable Transport Protocols for Wireless Sensor Networks**

- Sink-to-Node(s) Transport
  - ✓ Pump Slow Fetch Quickly (PSFQ)
  - ✓ Reliable Multi-Segment Transport (RMST)
  - ✓ Garuda
- Nodes-to-Sink Transport
  - ✓ Event-to-Sink Reliable Transport (ESRT)
  - ✓ End-to-End Reliable Event Transfer in WSNs
- Congestion Control
  - ✓ Congestion Detection and Avoidance (CODA)
  - ✓ Mitigating Congestion in WSNs

**Why not TCP or its variants for WSN?**

- Higher overheads for short data transmissions.
- Flow and congestion control cause unfair bandwidth for farther nodes.
- Throughput degrades under wireless due to higher packet losses.
- End-to-end congestion needs longer time to mitigate congestion, causing more congestion to occur.
- End-to-end reliability consumes more energy and bandwidth than hop-by-hop.
- Packet-based reliability, which is not required for event-driven applications

**Why not UDP?**

- Lower over overheads but
  - ✓ No congestion control
  - ✓ No flow control
  - ✓ No reliability

**Pump Slowly, Fetch Quickly (PSFQ)**

- Nodes broadcast fragments, in-sequence to next hop, which stores and forwards. If a node detects gap it broadcasts a NACK. Hop-by-hop store and forward

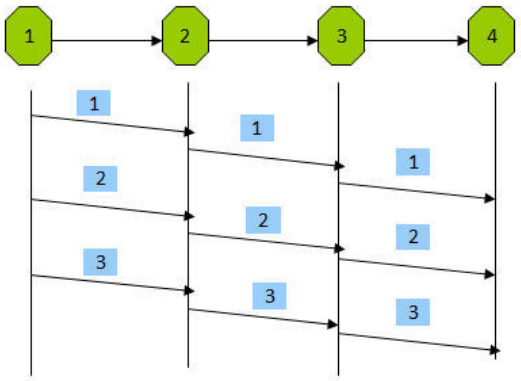
| | |
|---|---|
| Application | Reprogramming or re-tasking of sensor networks |
| Features | NACK, In sequence caching, Loss due to transmission drops not congestion, Hop-by-hop error recovery |
| Goals | Operate under high error rates, minimum support from underlying layers, low latency, minimize no of transmissions for lost detection and recovery |
| Description | Pump, Fetch, Report Msgs |

- C.Y. Wan, A.T. Campbell, and L. Krishnamurthy, "PSFQ: A Reliable Transport Protocol for Wireless Sensor Networks," *WSNA'02,* Atlanta, Georgia, USA, September 28, 2002.

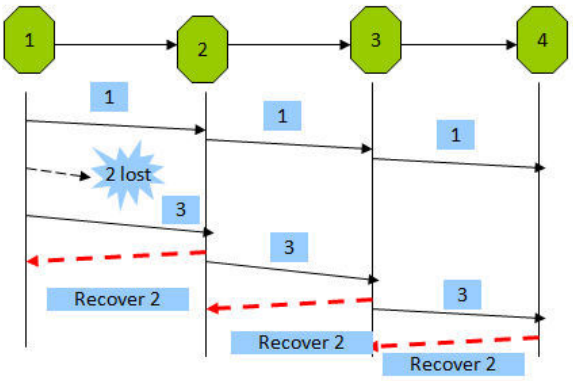
**PSFQ Operations**

- Pump Operation
  - ✓ User Node broadcasts a packet to its neighbors every Tmin
  - ✓ Decrements TTL and schedules a transmission
    - Tmin < Ttransmit < Tmax
    - If a node hears same transmission four times before Ttransmit it would cancel its transmission
- Fetch Operation
  - ✓ Sequence number gap is detected
    - Node will send a NACK message upstream, NACK scope is 1 hop
    - NACKs are generated every Tr; (Tr << Tmax)
    - NACKs can be cancelled if neighbors have sent similar NACKs
  - ✓ Node enters 'proactive fetch' mode if last segment hasn't been received and no packet has been delivered after Tpro = a * (Smax - Smin) * Tmax
- Report Operation
  - ✓ Used as a feedback/monitoring mechanism

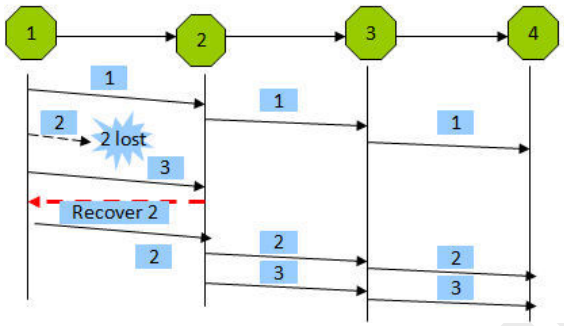
When No Link Loss – Multi-Hop Forwarding takes place



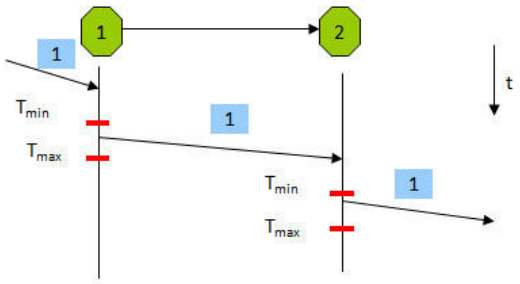

Error Recovery Control Messages are wasted



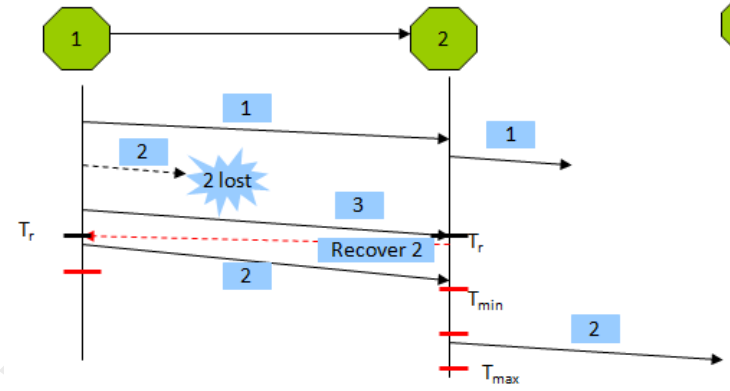

Error recovery – Store and Forward.



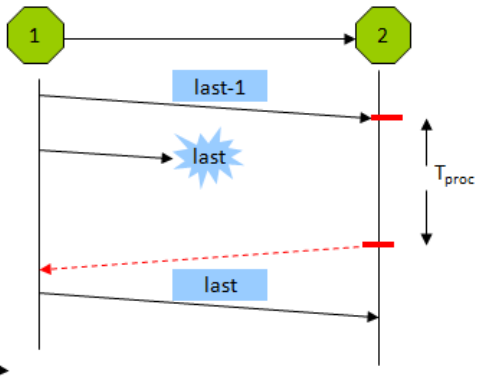

PSFQ Pump Operation. If not duplicate and in-order and TTL not 0 Cache and Schedule for Forwarding at time t ($T_{min}$<t<$T_{max}$)




**PSFQ**



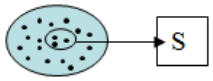

*PSFQ Fetch Operation.*




*PSFQ Proactive Fetch Operation.*

- Problems with PSFQ
  - ✓ Uniformly distributed channel error model
  - ✓ Need fine tuning of timers for good results (Tmin, Tmax, Tr)
  - ✓ First Packet Delivery
  - ✓ Cache size limitation

**Event-to-Sink Reliable Transport (ESRT) for Wireless Sensor Networks**

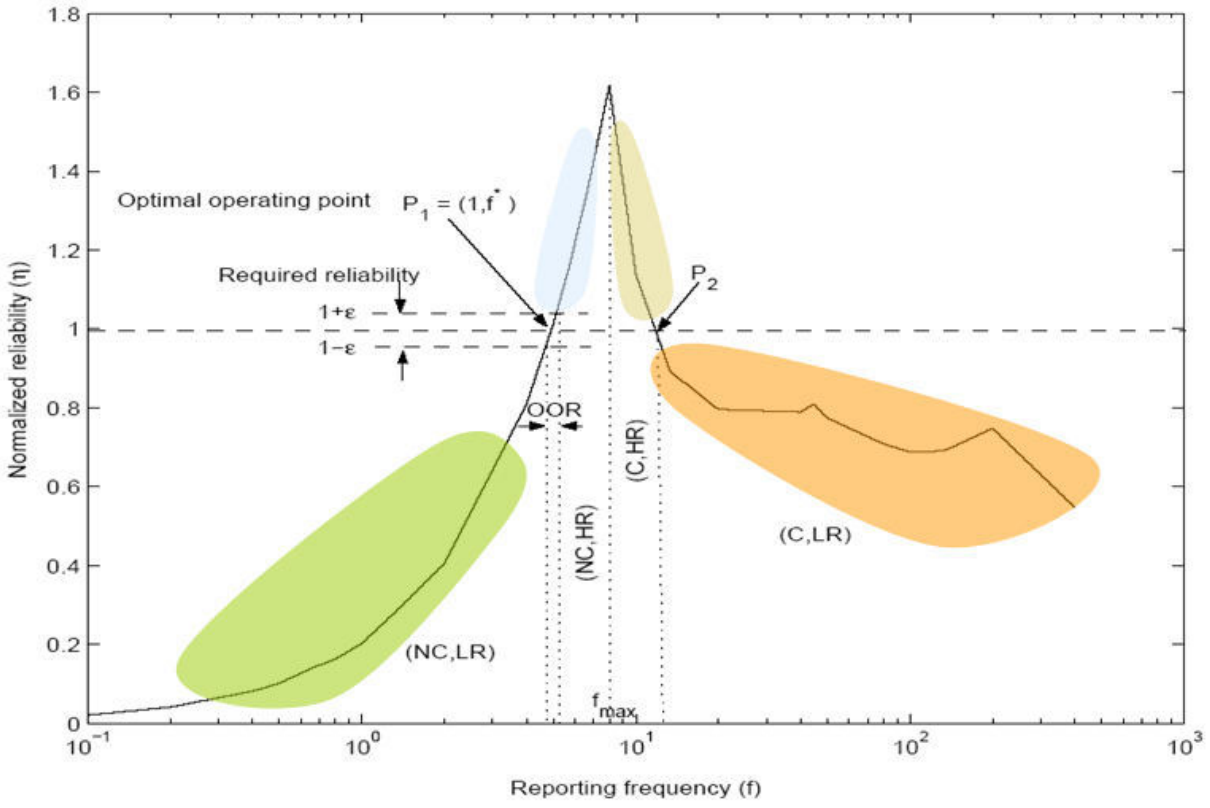



- Event-to-sink reliability
- Self-configuration
- Energy awareness [low power consumption requirement!]
- Congestion Control
- Variation in complexity at source and sink. [computation complexity]

**ESRT's Definition of Reliability**

- Reliability is measured in terms of the number of packets received. Or reporting frequency i.e., number of packets/decision interval.
- Observed reliability: number of received data packets in decision interval at the sink.
- Desired reliability: number of packets required for reliable event detection.
- Normalized reliability = observed/desired.
- Reliability is measured in terms of the number of packets received. Or reporting frequency i.e., number of packets/decision interval.
- Observed reliability: number of received data packets in decision interval at the sink.
- Desired reliability: number of packets required for reliable event detection.
- Normalized reliability = observed/desired.

**ESRT**




ESRT Operations

**Algorithm for ESRT**

- If congestion and low reliability: decrease reporting frequency aggressively. (exponential decrease)
- If congestion and high reliability: decrease reporting to relieve congestion. No compromise on reliability (multiplicative increase)
- If no congestion and low reliability: increase reporting frequency aggressively (multiplicative increase)
- If no congestion and high reliability: decrease reporting slowing (half the slope)
- Drawbacks: Event-based reporting frequency not good for all the nodes

**CODA: Congestion Detection and Avoidance**

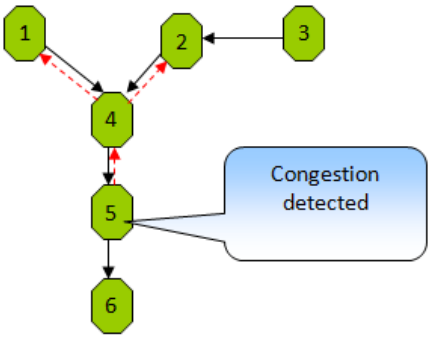
- The transport of event impulses is likely to lead to varying degrees of congestion in the network.
- CODA using channel sampling detects congestion and broadcasts this information to upstream nodes

| Application | General Purpose (event-to-sink) |
|---|---|
| Features | Uses buffer occupancy and channel sampling to detect congestion, assumes event occurrence as source of congestion not wireless links or interference |
| Goals | minimize congestion both transient and persistent |
| Description | Open-loop hop-by-hop backpressure, Closed-loop multi-source regulation |

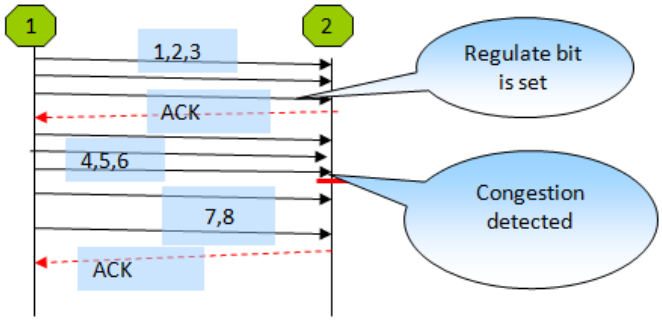
- C.Y. Wan, S.B. Eisenman, and A.T. Campbell, "CODA: Congestion Detection and Avoidance in Sensor Networks," The First ACM Conference on Embedded Networked Sensor Systems (Sensys03), Los Angeles, CA, USA. November, 2003.

**CODA**

- Congestion Detection
  - ✓ Accurate and efficient congestion detection is important
    - Buffer queue length or Buffer occupancy – not a good measure of the congestion.
    - Channel loading – sample channel at appropriate time to detect congestion.
- Open loop, hop-by-hop backpressure
  - ✓ A node broadcasts backpressure msgs to upstream nodes as long as it detects congestion
  - ✓ An upstream node decides whether to further propagate the msg or not, depending on its own local network condition
- Closed-loop, multi-source regulation
  - ✓ When a source event rate is greater than some max. theoretical throughput, it is more likely to contribute to congestion, so it enter into sink regulation
  - ✓ The sink sends ACKs at some predefined rate or certain no. of ACKs over a predefined period. If source does not gets necessary ACKs it decreases its rate.




Open loop, hop-by-hop backpressure




Closed loop, multi-source regulation

**Security threats in Sensor Networks**

- Use of wireless communications -In a broadcast medium, adversaries can easily eavesdrop on, intercept, inject and alter transmitted data.
- Adversaries can Interact with networks from a distance by inexpensive radio transceivers and powerful workstations.
- Resource consumption attacks. Adversaries can repeatedly send packets to drain nodes battery and waste network bandwidth, can steal nodes.
- However , these threats are not addressed. Focus is on guaranteeing message authenticity, integrity and confidentiality

**TINYSEC**

- Light weight and efficient link layer security package
- A research platform that is easily extensible and has been incorporated into higher level protocols.
- Developers can easily integrate into sensor network applications.

**Motivation for Link layer security in Sensor Networks**

- End-End security Mechanisms :
  - ✓ Suitable only for conventional networks using end-end communications where intermediate routers only need to view the message headers.
- Why end-end security mechanisms not suitable for sensor networks?
  - ✓ If message integrity checked only at the destination, the networks may route packets injected by an adversary many hops before they are detected. This will waste precious energy.
- BUT, in Sensor networks
  - ✓ In-network processing is done to avoid redundant messages-Requires intermediate nodes to have access to whole message packets and just not the headers as in conventional networks.
- A link layer security mechanism can detect unauthorized packets when they are first injected onto the network.

**Design Goals-Security Goals**

- A link layer security protocol should satisfy three basic security properties:
- Access control and Message integrity
  - ✓ prevent unauthorized parties from participating
- Confidentiality
  - ✓ keeping information secret form unauthorized parties
- Explicit omission: Replay protection
  - ✓ an adversary eavesdropping a legitimate message sent b/w 2 authorized parties replays it at a some time later

**Design goals –Performance goals**

- A system using cryptography will incur increased overhead in length of the message .
- Overhead limitations-REQUIRED
- Increased message length results
  - ✓ decreased message throughput
  - ✓ increased latency
  - ✓ Increased power consumption ( Sensor Networks)
  - ✓ Carefully tune the strength of security mechanisms for reasonable security while limiting overheads

**Design Goals-Ease of Use**

- Security Platform-
  - ✓ Higher level security protocols can use Tinysec to create secure pair wise communication between neighboring nodes.
- Transparency
  - ✓ Application programmers are unsure of security parameters and can disable if standardized APIs are not provided
  - ✓ Should be transparent to the user
- Portability
  - ✓ Should fit into the radio stack so that porting the radio stack from one platform to another (ATmel, Intel, X86 etc) is a simple job.

**Summary**

- Transport Protocols for WSN
- TCP/UDP for WSN
- Protocols
  - ✓ PSFQ
  - ✓ ESRT
  - ✓ CODA
- Security Threats in WSN
- TinySec
- Motivations of Link Layer security
- TinySec Design goals
- Semantic Secure Encryption in TinySec

**Lecture 38**

**Security/Extensions of WSN Part V**

**Outlines**

- Security primitives in TinySec
- Encryption Schemes
- Keying mechanism
- WMSN
  - ✓ Architecture
  - ✓ Applications
  - ✓ Advantages
  - ✓ Design Considerations
  - ✓ Protocols
- WSAN
  - ✓ Motivation
  - ✓ WSN vs WSAN
  - ✓ Architecture
  - ✓ Issues

**Last Lecture**

- Transport Protocols for WSN
- TCP/UDP for WSN
- Protocols
  - ✓ PSFQ, ESRT, CODA
- Security Threats in WSN
- TinySec
- Motivations of Link Layer security

**Security Primitives**

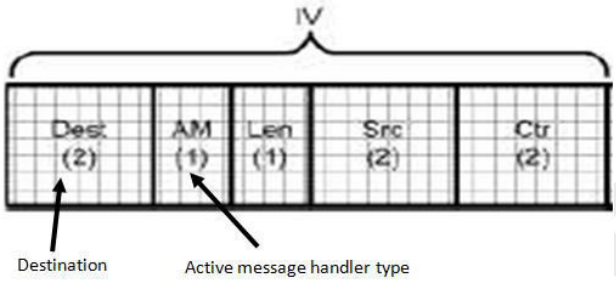
- Message Authentication code
  - ✓ A cryptographic secure checksum for checking the message integrity
  - ✓ Computing a MAC requires authorized senders and receivers to share a secret key, and this key is part of the input to a MAC computation
  - ✓ if an adversary alters a valid message or injects a bogus message, she cannot compute the corresponding MAC value
- Initialization vector (IV)
  - ✓ Encrypting the same plaintext two times should give two different ciphertexts (semantic security).
  - ✓ A common technique for achieving semantic security is to use a unique initialization vector (IV) for each invocation of algorithm
  - ✓ A side input to the encryption algorithm.

**TINYSEC-DESIGN**

- 2 Security Options-
  - ✓ Authentication Encryption ( Tinysec-AE)
    - o TinySec encrypts the data payload and authenticates the packet with a MAC.
    - o The MAC is computed over the encrypted data and the packet header.
  - ✓ Authentication only (Tinysec-Au)
    - o TinySec authenticates the entire packet with a MAC, but the data payload is not encrypted.
- Encryption : semantically secure encryption typically requires two design decisions
  - ✓ Specifying the IV format
  - ✓ Selecting an encryption Scheme

**Tinysec IV format**

- IV too long- add unnecessary bits to the packet
- Too short – Risk of repetition
- How long should be the IV? N bit IV repeat after 2^n +1.
  - ✓ If we use a n bit counter repetitions will not happen before that point.
  - ✓ Pseudorandom would repeat with probability of 2^(n/2)




**Encryption schemes**

- Symmetric key encryption schemes fall into two classes
  - ✓ Stream ciphers
    - A stream cipher (typically) uses a key K and IV as a seed and stretches it into a large pseudorandom keystream GK(IV ).
    - The keystream is then xored against the message
    - Stream ciphers have a devastating failure mode: if the same IV is ever used to encrypt two different packets, then it is often possible to recover both plaintexts
- Modes of operation using block ciphers.
  - ✓ block cipher is a keyed pseudorandom permutation over small bit strings, typically 8 or 16 bytes
  - ✓ CBC is the most appropriate scheme for sensor networks –why?
  - ✓ Works better with repeated IVs.

**CBC**

- IV is XOR'ed with the first data block before it is encrypted.
- Feed the result of encryption back into the encryption of the next block.
- The plain-text is XOR'ed with the previous cipher-text block before it is encrypted.
- The encryption of each block depends on all the previous blocks.
- This requires that the decryption side processes all encrypted blocks sequentially
- An error in an encrypted block
  - ✓ Causes the block with the error to be completely garbled.
  - ✓ The subsequent block will have bit errors at the same positions as the original erroneous block.
  - ✓ The blocks following the second block will not be affected by the error. Hence, CBC is self-recovering

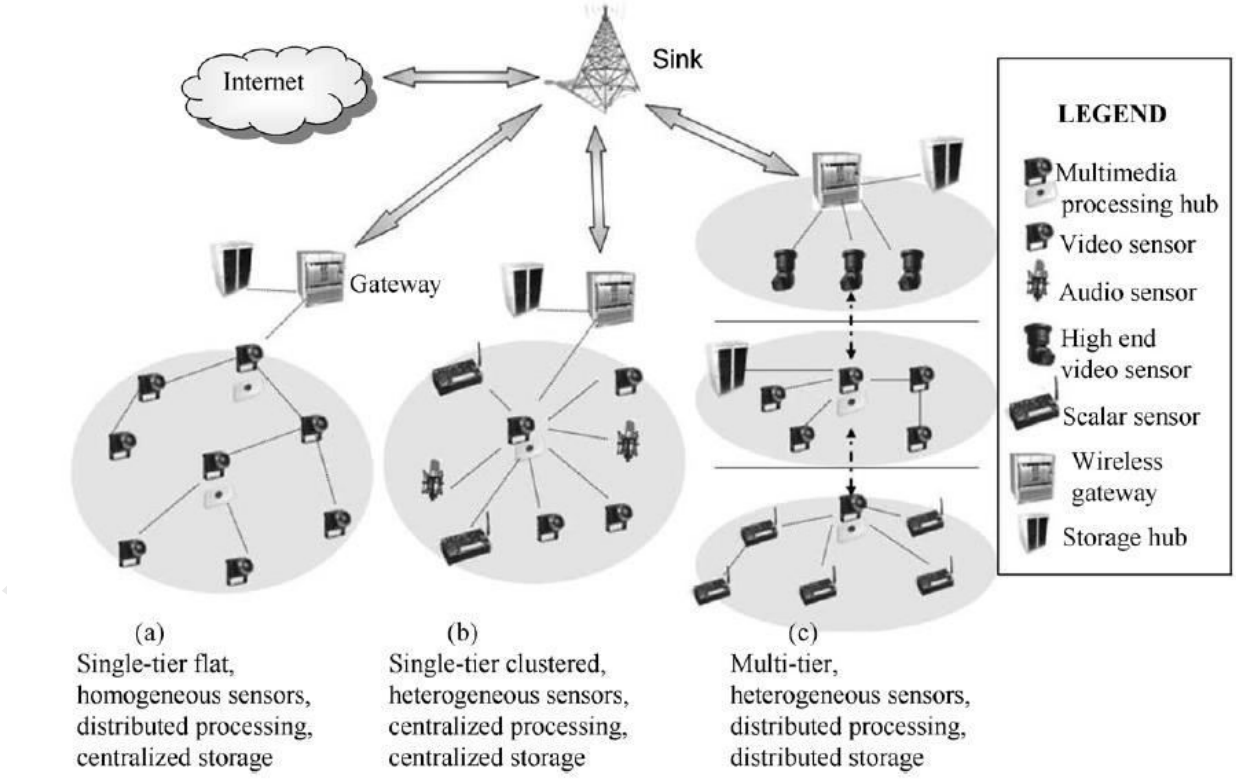
**Keying mechanism**

- Use per-link keying,
  - ✓ separate Tinysec key for each pair of node wishing to communicate.
  - ✓ Drawback: Key distribution becomes a challenge.
- Allow a group of nodes to share a TinySec key rather than each pairs.
  - ✓ Group keying provides an intermediate level of resilience.
- Appropriate keying mechanism for a particular network depends on several factors.
- Tinysec key- A pair of skipjack key-one for authentication, one or encryption.
- Simplest keying mechanism:
  - ✓ Use a single key for the entire network, Preload the key before deployment.-Adversary can compromise on node and get the key.

**Wireless Multimedia Sensor Networks**

- Networks of wirelessly interconnected devices that allow retrieving video and audio streams, still images, and scalar sensor data.
- Be able to store, process in real-time, correlate and fuse multimedia data originated from heterogeneous sources.

**Reference Architecture of WMSN**



**New Applications**

- Storage and Retrieval of Interesting Activities- e.g., IrisNet[93]. (2004)
- Traffic congestion avoidance, traffic. enforcement and control systems.
- Smart parking advice system. (2005)
- Automated Assistance for the elderly and family monitors. (2005)
- Manufacturing process control for semiconductor chip, food or pharmaceutical products.

**Advantages**

- Enlarging the Views
  - ✓ Provide multiple disparate viewpoints to overcome occlusion effects
- Enhancing the Views
  - ✓ Redundancy provides enhanced quality
- Enabling Multi-resolution Views
  - ✓ Heterogeneous media streams with different granularity can be acquired from the same point of view

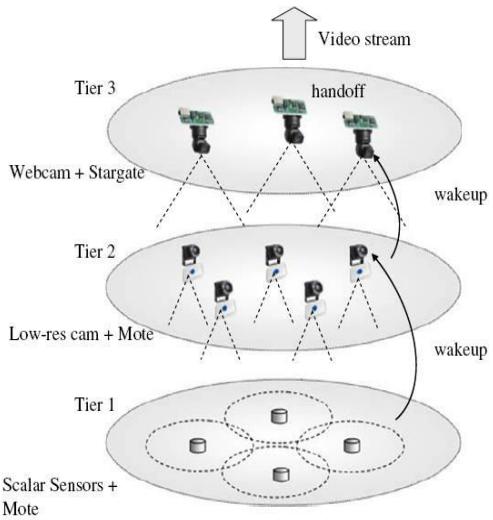
**Design Considerations**

- Application-specific QoS requirements
  - ✓ Snapshot and Streaming multimedia
  - ✓ Flexible architecture to support heterogeneous applications
- Multimedia source coding
  - ✓ intra-frame/inter-frame
  - ✓ distributed source coding
- Multimedia in-network processing
- Multimedia coverage model development
- Power consumption

**Examples of Deployed WMSN**

SensEye

- Three tasks:
  - ✓ object detection, recognition and tracking.
- Objective:
  - ✓ Demonstrate a camera sensor network containing heterogeneous elements provides numerous benefits over traditional homogeneous sensor networks.



**Application Layer**

- The services offered by the application layer include:
  - ✓ Providing traffic management and admission control functionalities
  - ✓ Performing source coding according to application requirements and hardware constraints, by using advanced multimedia encoding techniques
  - ✓ Developing flexible OS and Middleware to make functional abstractions and information gathered by the scalar and multimedia sensors available to higher layer applications

**Traffic Management and Admission Control**

- Tasks:
  - ✓ Prevent applications from establishing data flows when the network resources needed are not available
  - ✓ Traffic classes - provide differentiated service between real-time and delay-tolerant applications, and loss-tolerant and loss-intolerant applications.
- Related work:
  - ✓ An application admission control algorithm is proposed whose objective is to maximize the network lifetime subject to bandwidth and reliability constraints.(2003)
  - ✓ An application admission control method is proposed to determine admissions based on the added energy load and application rewards. (2003)

**Transport Layer**

- TCP or UDP?
  - ✓ For real-time applications like streaming media, UDP seems preferred over TCP
  - ✓ Effect of dropping packets in UDP
  - ✓ Support for traffic heterogeneity
- TCP with appropriate modifications is preferable over UDP for WMSNs, if standardized protocols are to be used.

**Non-Standard Protocols**

Focusing on reliability

- Reliable Multi-Segment Transport (RMST) (2004) or the Pump Slowly Fetch Quickly(PSFQ) protocol (2005)
  - ✓ Loss intolerant packets are separated and ensured to be successfully transmitted
  - ✓ Loss intolerant packets are buffered at intermediate nodes, allowing for faster retransmission in case of packet loss.
  - ✓ other packets are transmitted in UDP manner
  - ✓ No congestion avoidance
- Event-to-Sink Reliable Transport (ESRT) protocol (2005)
  - ✓ Not best effort but reliable requirement based rate control
  - ✓ Congestion detection and avoidance

**Using Multiple Paths**

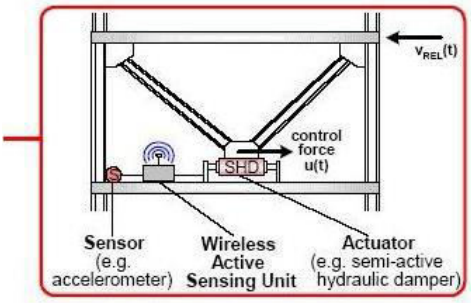
- Regulating streaming through multiple TCP connections. (2005)
  - ✓ Sender sends the desired streaming rate and allows throughput reduction to the receiver.
  - ✓ Receiver measures the actual throughput, controls the rate within the allowed bounds by using multiple TCP connections and dynamically changing its TCP window size for each connection.
- Spliting a large burst of data into several smaller bursts
  - ✓ Multi-flow Real-time Transport Protocol (MRTP). (2006)
- Allows the sink to regulate multiple sources associated with a single event
  - ✓ Congestion Detection and Avoidance (CODA) protocol. (2003)

**WSAN: I. Motivations**

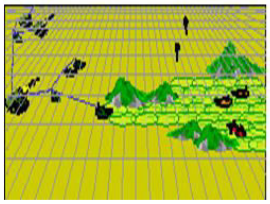
- Environmental Applications
  - ✓ Detecting and extinguishing forest fire

- Distributed Robotics & Sensor Networks
  - ✓ Mobile robots dispersed throughout the field in sensor networks, e.g. mines detection and destruction.

- Structure health monitoring and control
  - ✓ Sensors to observe seismic excitation in bridges/buildings
  - ✓ Actors to reduce deflections
- Surveillance/Emergency handling
  - ✓ Immediate alerts of changes in patient status
  - ✓ Relay data to hospital, correlate with patient records



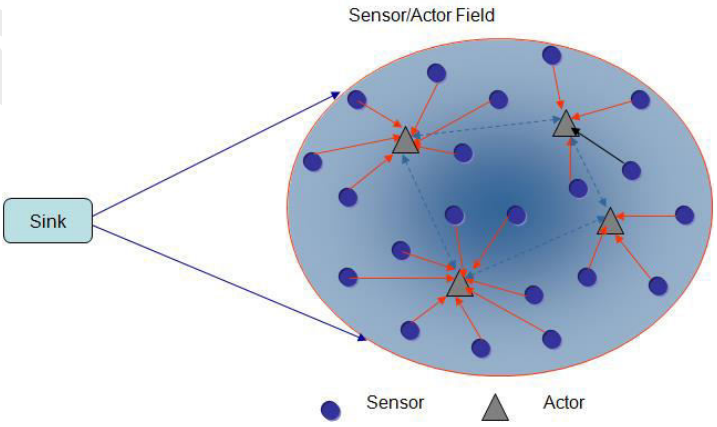

- Battlefield applications
- Sensors detect explosive materials or weapons (objects)
- Actors annihilate them or function as tank
- Microclimate controls in smart buildings
- In case of very low or high temperature/gas leakages, trigger the alarms or corresponding controller





**WSAN: II. Wireless Sensor Actor Networks**

- Sensors:
  - ✓ Passive nodes sensing from the environment
  - ✓ Limited energy, processing and communication capabilities.
- Actors:
  - ✓ Active nodes acting on the environment.
  - ✓ Higher processing and communication capabilities.
  - ✓ Less-constrained energy resources mobile.
- WSN + Actors ⟶ WSANs

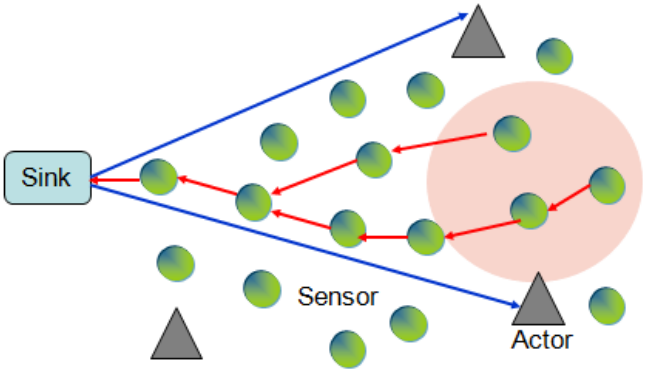

- [1] I. F. Akyildiz and I. H. Kasimoglu, "Wireless Sensor and Actor Networks: Research Challenges," Ad Hoc Networks, Vol. 2, Issue 4, pp. 351-367, October 2004.

**WSANs vs. Wireless Sensor Networks**

- Real-time requirements for timely actions
  - ✓ Rapidly respond to sensor input e.g. in battlefield
  - ✓ To perform right action, sensor data must be valid at the time of action.
- Heterogeneous Nodes
  - ✓ Sensors (densely deployed)
    - Heterogeneity e.g. multiple events detection or multi-level energy sources.
  - ✓ Actors (loosely deployed)
    - Different actions capabilities.
- Distributed local coordination requirements
  - ✓ Sensor-Actor coordination
  - ✓ Actor-Actor coordination
- Nodes mobility
  - ✓ Specially actor nodes e.g. robots, ambulance, tank etc.

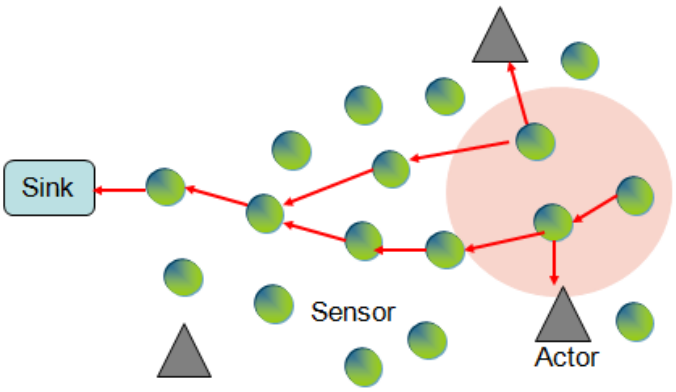
**WSAN Architecture**

- Semi-automated




▶ Sensors-sink, sink-actor comm.

- Automated




▶ Sensors-actors, sensors-sink comm.

**WSAN: III. Issues**

- Self-configuration of sensor nodes.
- Energy conservation is the primary concern as in WSNs.
- Localization of sensor nodes relative to actors.
- Real-time routing
  - ✓ Is it possible with highly dynamic topology?
- Aggregation?
  - ✓ It might affect the in-time data delivery
- Coordination
- Redundancy
  - ✓ Exploit spatial or temporal correlation.

**Summary**

- Security primitives in TinySec
- Encryption Schemes
- Keying mechanism
- WMSN
  - ✓ Architecture
  - ✓ Applications
  - ✓ Advantages
  - ✓ Design Considerations
  - ✓ Protocols
- WSAN
  - ✓ Motivation
  - ✓ WSN vs WSAN
  - ✓ Architecture
  - ✓ Issues

**Lecture 39**

**Bluetooth/Wireless Personal Area Networks (WPAN)**

**Outlines**

- Bluetooth introduction
- Technical features
- Access technique
- Bluetooth topology/scenario
- Specifications
- Architecture
- Core Protocols
- Packet format
- Link connections

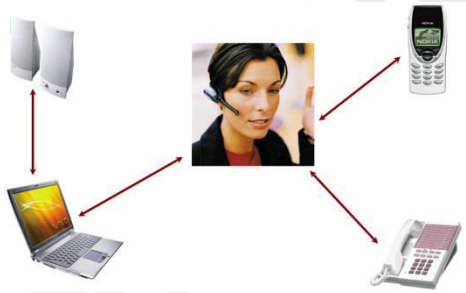
**Last Lecture**

- Security primitives in TinySec
- Encryption Schemes
- Keying mechanism
- WMSN
  - ✓ Architecture
  - ✓ Applications
  - ✓ Advantages
  - ✓ Design Considerations
  - ✓ Protocols
- WSAN
  - ✓ Motivation
  - ✓ WSN vs WSAN
  - ✓ Architecture
  - ✓ Issues

**What is Bluetooth?**

- "Bluetooth wireless technology is
  - ✓ An open specification for a
  - ✓ Low-cost, low-power, short-range radio technology
  - ✓ For ad-hoc wireless communication of
  - ✓ Voice and data anywhere in the world."

**Ultimate Headset**



**Cordless Computer**

**Bluetooth Application Areas**

- Data and voice access points
  - ✓ Real-time voice and data transmissions
- Cable replacement
  - ✓ Eliminates need for numerous cable attachments for connection
- Ad hoc networking
  - ✓ Device with Bluetooth radio can establish connection with another when in range

**Overview of Bluetooth History**

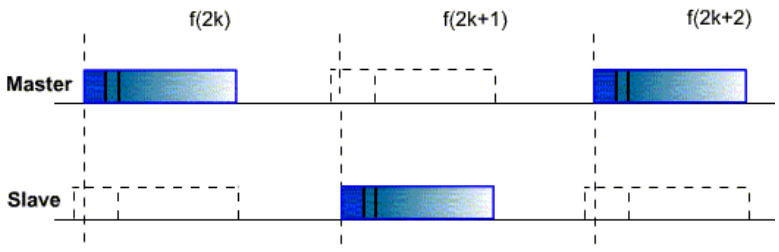
- What is Bluetooth?
  - ✓ Bluetooth is a short-range wireless communications technology.
- Why this name?
  - ✓ It was taken from the 10th century Danish King Harald Blatand who unified Denmark and Norway.
- When does it appear?
  - ✓ 1994 – Ericsson study on a wireless technology to link mobile phones & accessories.
  - ✓ 5 companies joined to form the Bluetooth Special Interest Group (SIG) in 1998.
  - ✓ First specification released in July 1999.

**Technical features**

| | |
|---|---|
| Connection Type | Spread Spectrum (Frequency Hopping) & Time Division Duplex (1600 hops/sec) |
| Spectrum | 2.4 GHz ISM Open Band (79 MHz of spectrum = 79 channels) |
| Modulation | Gaussian Frequency Shift Keying |
| Transmission Power | 1 mw – 100 mw |
| Data Rate | 1 Mbps |
| Range | 30 ft |
| Supported Stations | 8 devices |
| Data Security –Authentication Key | 128 bit key |
| Data Security –Encryption Key | 8-128 bits (configurable) |
| Module size | 9 x 9 mm |

**Time-Division Duplex Scheme**

- Channel is divided into consecutive slots (each 625 μs)
- One packet can be transmitted per slot
- Subsequent slots are alternatively used for transmitting and receiving
  - ✓ Strict alternation of slots between the master and the slaves
  - ✓ Master can send packets to a slave only in EVEN slots
  - ✓ Slave can send packets to the master only in the ODD slots

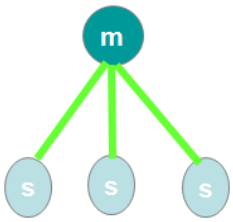


**Radio Specification**

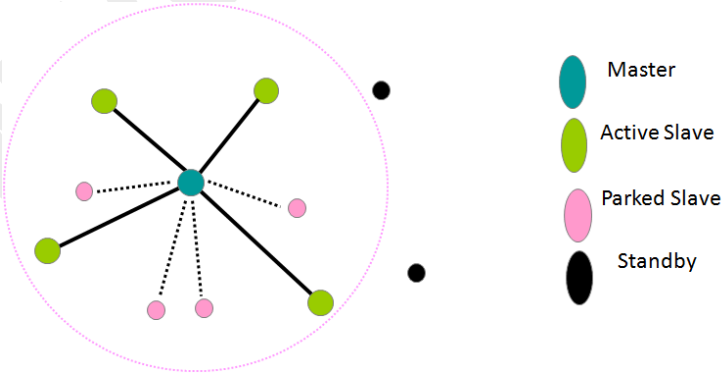
- Classes of transmitters
  - ✓ Class 1: Outputs 100 mW for maximum range
    - Power control mandatory
    - Provides greatest distance
  - ✓ Class 2: Outputs 2.4 mW at maximum
    - Power control optional
  - ✓ Class 3: Nominal output is 1 mW
    - Lowest power

**Typical Bluetooth Scenario**

- Bluetooth will support wireless point-to-point and point-to-multipoint (broadcast) between devices in a piconet.
- Point to Point Link
  - ✓ Master - slave relationship
  - ✓ Bluetooth devices can function as masters or slaves
- Piconet
  - ✓ It is the network formed by a Master and one or more slaves (max 7)
  - ✓ Each piconet is defined by a different hopping channel to which users synchronize to
  - ✓ Each piconet has max capacity (1 Mbps)

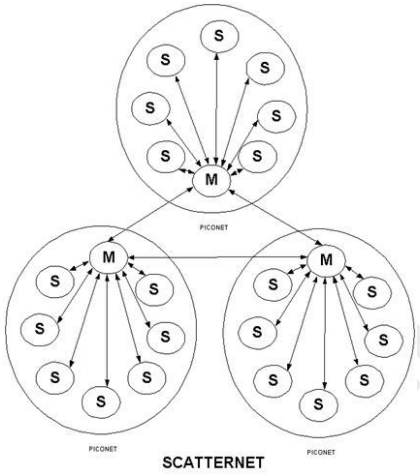

**Piconet Structure**




- All devices in piconet hop together.
- Master's ID and master's clock determines frequency hopping sequence & phase.
- Hopping sequence shared with all devices on piconet
- Bluetooth devices use time division duplex (TDD)
- Access technique is TDMA
- FH-TDD-TDMA

**Ad-hoc Network – the Scatternet**

- Inter-piconet communication
- Up to 10 piconets in a scatternet
- Multiple piconets can operate within same physical space
- This is an ad-hoc, peer to peer (P2P) network




**Bluetooth Standards Documents**

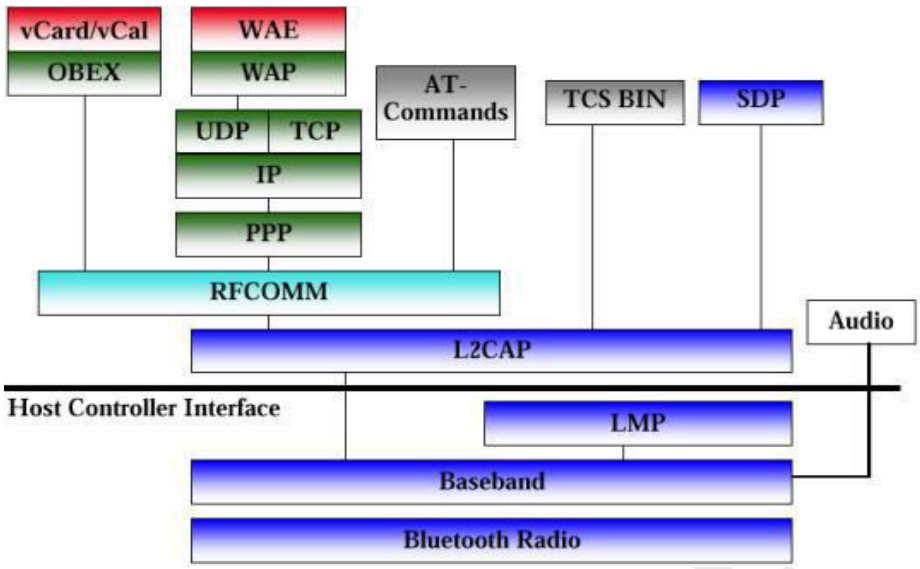
- Core specifications
  - ✓ Details of various layers of Bluetooth protocol architecture
  - ✓ Bluetooth is a layered protocol architecture
    - Core protocols
    - Cable replacement and telephony control protocols
    - Adopted protocols
- Profile specifications
  - ✓ Use of Bluetooth technology to support various applications

**Profiles**

- Generic Access Profile
- Service Discovery Application Profile
- Cordless Telephony Profile
- Intercom Profile
- Serial Port Profile
- Headset Profile
- Dial-up Networking Profile
- Fax Profile
- LAN Access Profile
- Generic Object Exchange Profile
- Object Push Profile
- File Transfer Profile
- Synchronization Profile

**Architecture**

- Core protocols
  - ✓ Radio
  - ✓ Baseband
  - ✓ Link manager protocol (LMP)
  - ✓ Logical link control and adaptation protocol (L2CAP)
  - ✓ Service discovery protocol (SDP)
- Cable replacement protocol
  - ✓ RFCOMM
- Telephony control protocol
  - ✓ Telephony control specification – binary (TCS BIN)
- Adopted protocols
  - ✓ PPP
  - ✓ TCP/UDP/IP
  - ✓ OBEX
  - ✓ WAE/WAP




**Core Protocols**

- Radio:
  - ✓ Defines technical characteristics of BT radios.
  - ✓ For example licence-free ISM band 2.4 GHz, FHSS at 1600 Hops/sec, 1 MHz channel bandwidth, GMSK modulation, tx power from 100 mw to 1 mw, raw transmission rate of 1 Mbps and so on.
- Baseband:
  - ✓ Defines procedure to communicate with other BT devices like formation of piconets, links in a piconet (ACL or SCO), and access of transmit resources in a piconet etc.
- Link Manager protocol (LMP):
  - ✓ It is transactional protocol between two link management entities used to setup properties of BT link. For example a device may authenticate each other, may learn each others features (SCO/ACL links, size of packet, power consumption mode).
- Host Controller Interface (HCI):
  - ✓ It is not a protocol rather an interface through which BT devices access the lower layers of BT protocol stack. A device may pass and receive data destined to or coming from another BT device, execute inquiries, request authentication and so on.
- Logical Link Control and Adaptation protocol (L2CAP):
  - ✓ Shields the specifics of BT lower layers and provides a packet interface to higher layers.

**Bluetooth protocols**

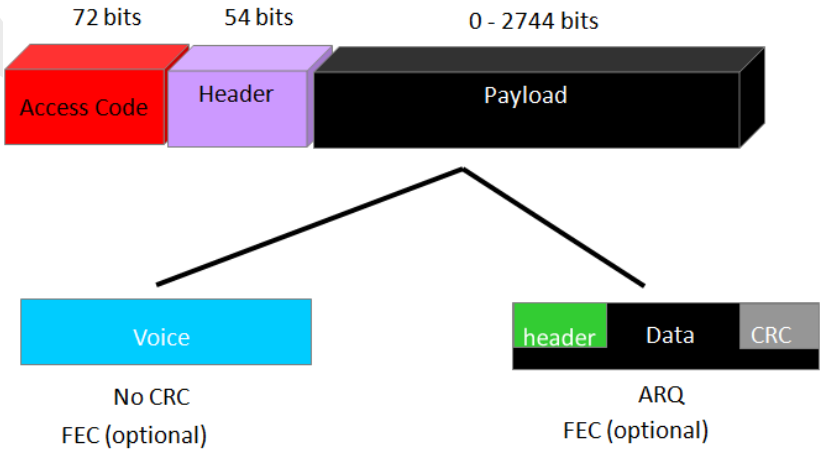
- Service Discovery Protocol (SDP)
  - ✓ Defines a service record format
    - Information about services provided by *attributes*
    - Attributes composed of an ID (name) and a value
    - IDs may be universally unique identifiers (UUIDs)

- Defines an inquiry/response protocol for discovering services
  - ✓ Searching for and browsing services
- RFCOMM (based on GSM TS07.10)
  - ✓ Emulates a serial-port to support a large base of legacy (serial-port-based) applications
  - ✓ Allows multiple "ports" over a single physical channel between two devices
- Telephony Control Protocol Spec (TCS)
  - ✓ Call control (setup & release)
  - ✓ Group management for gateway serving multiple devices
- Legacy protocol reuse
  - ✓ Reuse existing protocols, e.g., IrDA's OBEX, or WAP for interacting with applications on phones

**Baseband**

- Addressing
  - ✓ Bluetooth device address (BD_ADDR)
    - 48 bit IEEE MAC address
  - ✓ Active Member address (AM_ADDR)
    - 3 bits active slave address
    - all zero broadcast address
  - ✓ Parked Member address (PM_ADDR)
    - 8 bit parked slave address
- This MAC address is split into three parts
  - ✓ The Non-significant Address Part (NAP)
    - Used for encryption seed
  - ✓ The Upper Address part (UAP)
    - Used for error correction seed initialization & FH sequence generation
  - ✓ The Lower Address Part (LAP)
    - Used for FH sequence generation

**Packet Structure**



**Types of Access Codes**

- Channel access code (CAC) – identifies a piconet
- Device access code (DAC) – used for paging and subsequent responses
- Inquiry access code (IAC) – used for inquiry purposes

**Inquiry Procedure**

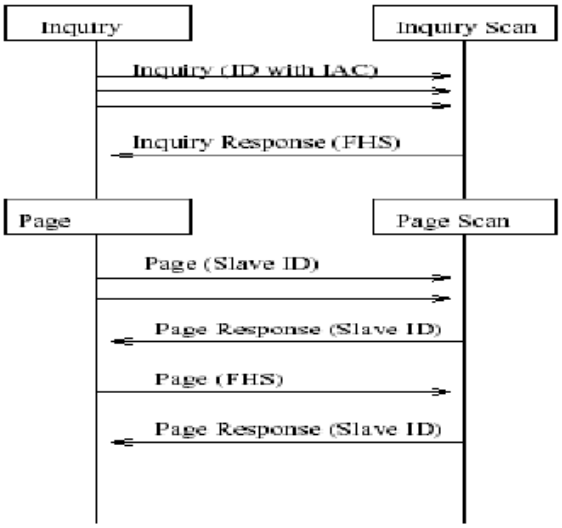
- Potential master identifies devices in range that wish to participate
  - ✓ Transmits ID packet with inquiry access code (IAC)
  - ✓ Occurs in Inquiry state
- Device receives inquiry
  - ✓ Enter Inquiry Response state
  - ✓ Returns FHS packet with address and timing information
  - ✓ Moves to page scan state

**Page Procedure**

- Master uses devices address to calculate a page frequency-hopping sequence
- Master pages with ID packet and device access code (DAC) of specific slave
- Slave responds with DAC ID packet
- Master responds with its FHS packet
- Slave confirms receipt with DAC ID
- Slaves moves to Connection state

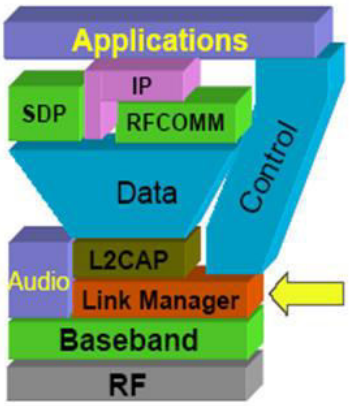
**Channel Establishment**

- Seven sub-states
  - ✓ Inquiry
  - ✓ Inquiry scan
  - ✓ Inquiry response
  - ✓ Page
  - ✓ Page scan
  - ✓ Master response
  - ✓ Slave response



**Link Manager Protocol**

- Pinconet Management
  - ✓ Channel control
  - ✓ Master-slave switch
- Link Configuration
  - ✓ Low power mode
  - ✓ QoS
  - ✓ Packet type selection
- Security
- Authentication
- Encryption




- The Link Manager carries out link setup, authentication & link configuration.
- Channel Control
  - ✓ All the work related to the channel control is managed by the master
    - The master uses *polling* process for this
  - ✓ The master is the first device which starts the connection
    - This roles can change (master-slave role switch)

**Connection State**

- Active Mode
  - ✓ Device participates actively on the transmission channel. The master regularly sends a packet to the slaves (polling) to enable the slaves to be able to send a packet to the master and re-synchronise themselves
- Sniff Mode
  - ✓ This is a low consumption mode. A Bluetooth module in the Sniff mode stays synchronised in the piconet. It listens to the piconet at regular intervals (Tsniff) for a short instant on specified slots for its message.
- Hold Mode
  - ✓ The module remains synchronised. This is lower consumption mode than the Sniff mode. Only the counter on the Bluetooth chip in hold mode is active. At the end of the Hold period, the Bluetooth module returns to the active mode.
- Park Mode
  - ✓ A Bluetooth module in this mode is no longer an active member of the piconet. However, it remains synchronised with the master and can listen to a broadcast channel (Beacon Channel).

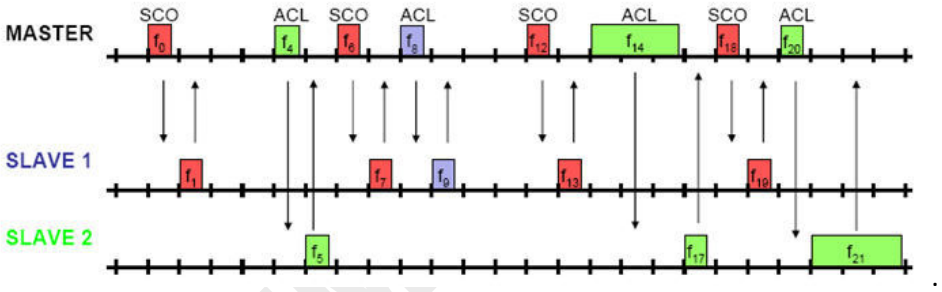
**L2CAP**

- Service provided to the higher layer:
  - ✓ L2CAP provides connection-oriented and connectionless data services to upper layer protocols
  - ✓ Protocol multiplexing and demultiplexing capabilities

- ✓ Segmentation & reassembly of large packets
- ✓ L2CAP permits higher level protocols and applications to transmit and receive L2CAP data packets up to 64 kilobytes in length.

**Links between Master and Slave**

- Synchronous connection oriented (SCO)
  - ✓ Allocates fixed bandwidth between point-to-point connection of master and slave
  - ✓ Master maintains link using reserved slots
  - ✓ Master can support three simultaneous links
  - ✓ Bandwidth reservation/QoS
  - ✓ No retransmissions required or done in this mode
- Asynchronous connectionless (ACL)
  - ✓ Point-to-multipoint link between master and all slaves
  - ✓ Only single ACL link can exist
  - ✓ 1, 3 or 5 slot packets are defined




**Flow Specification Parameters**

- QoS parameter in L2CAP defines traffic flow specification indicating the performance level that the sender will attempt to achieve
  - ✓ Service type
  - ✓ Token rate (bytes/second)
  - ✓ Token bucket size (bytes)
  - ✓ Peak bandwidth (bytes/second)
  - ✓ Latency (microseconds)
  - ✓ Delay variation (microseconds)

**Summary**

- Bluetooth introduction
- Technical features
- Access technique
- Bluetooth topology/scenario
- Specifications
- Architecture
- Core Protocols
- Packet format
- Link connections
- Next Lecture
  - ✓ High Speed WPAN

**Lecture 40**

**High Rate Wireless Personal Area Networks (WPAN)**

**Outlines**

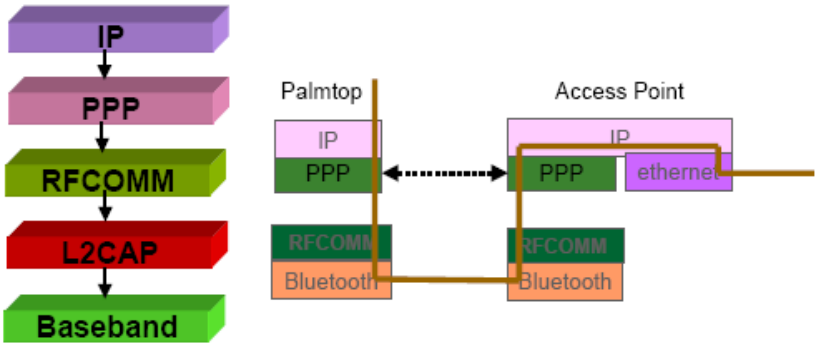
- IP Over Bluetooth
- Bluetooth Security
- WPAN Standards
- IEEE 802.15.3 Overview
- 802.15.3
  - ✓ Topology
  - ✓ Coordination
    - Starting a Piconet
    - Handing over control of piconet
    - Creating child piconet
    - Ending a Piconent
    - Association/Disassociation
  - ✓ Medium Access (Superframe)
  - ✓ Channel Time Management
  - ✓ Power management
  - ✓ MAC Frame format

**Last Lecture**

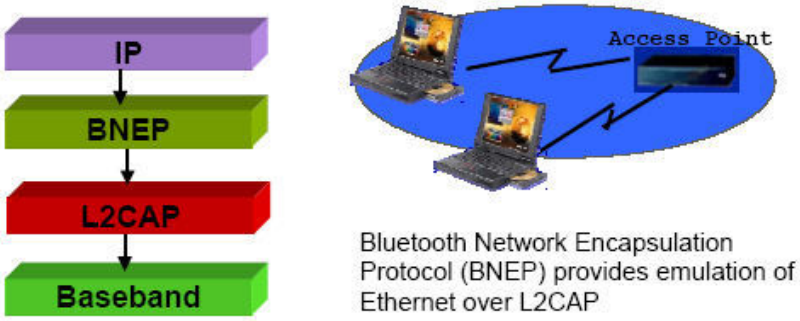
- Bluetooth introduction
- Technical features
- Access technique
- Bluetooth topology/scenario
- Specifications
- Architecture
- Core Protocols
- Packet format
- Link connections

**IP over Bluetooth**

- IP over Bluetooth v 1.0

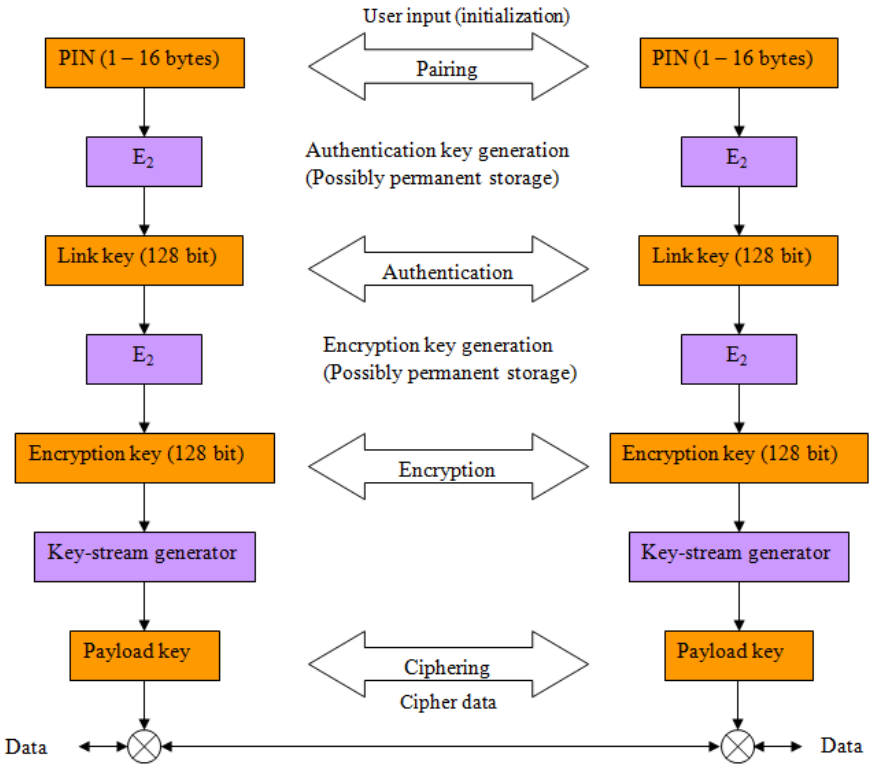



- IP over Bluetooth v 1.1




Bluetooth Network Encapsulation Protocol (BNEP) provides emulation of Ethernet over L2CAP

**Security**



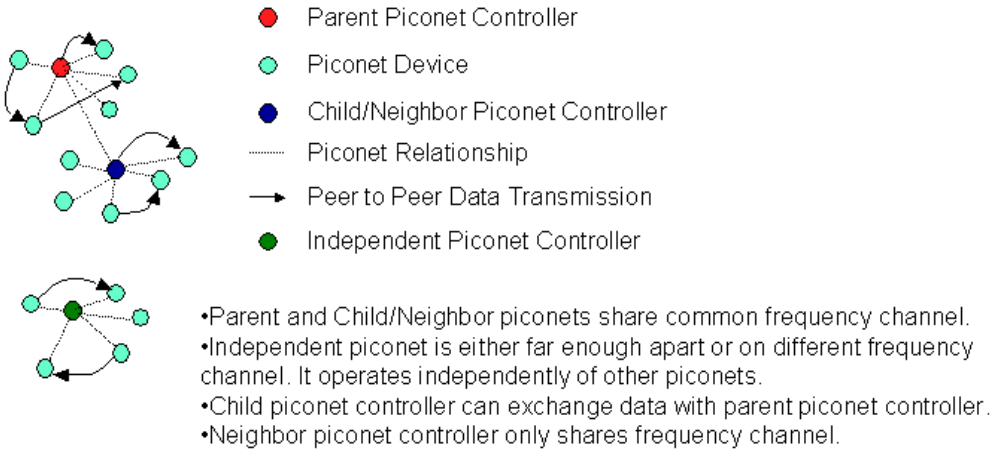

**WPAN Standards**

| IEEE standard | Topic | Data throughput | Suitable applications | QoS needs |
|---|---|---|---|---|
| 802.15.1 | Bluetooth | 1 Mbps | Cell phones, Computers, Personal Digital Assistants (PDAs)/ Handheld Personal Computers (HPCs), Printers, Microphones, Speakers, Handsets, Bar Code Readers, Sensors, Displays, Pagers and Cellular & Personal Communications Service (PCS) phones | QoS suitable for Voice applications |
| 802.15.2 | Coexistence of Bluetooth and 802.11b | N/A | N/A | N/A |
| 802.15.3 | High-rate WPAN | > 20 Mbps | Low power, Low cost solutions for portable consumers of digital imaging and multimedia Applications | Very high QoS |
| 802.15.4 | Low-rate WPAN | < 0.25 Mbps | Industrial, Agricultural, vehicular, Residential, Medical applications, Sensors and actuators with very low power consumption and low cost | Relaxed needs for data rate and QoS |

**IEEE 802.15.3 - Overview**

- High data rate WPAN
- Potential future standard
- Motivation: Data, High quality TV, Home cinema
- Dynamic topology
  - ✓ Mobile devices often join and leave the piconet
  - ✓ Short connection times
- Multiple Power Management modes
- Secure Network
- 2.4 GHz PHY
  - ✓ 4 channels (high density) or 3 channels (with 802.11b) modes are available
- Supports 5 data rates
  - ✓ 11Mbps(QPSK)
  - ✓ 22Mbps(DQPSK without coding)
  - ✓ 33Mbps(16QAM)
  - ✓ 44Mbps(32QAM), 55Mbps(64QAM)
- Based on piconets in a person space analogous to LAN in larger area
- Data Devices (DEV) establish peer-to-peer communication
- Includes also a Piconet Coordinator (PNC)
  - ✓ PNC manages the quality of service (QoS) requirements, power save modes and access control to the piconet.
- A new piconet created with same channel as of the existing PNC is called child/neighbor piconet
  - ✓ If channel access is also controlled by the parent PNC then it is called dependent piconet

**IEEE 802.15.3 – Topology**




- Parent Piconet Controller
- Piconet Device
- Child / Neighbor Piconet Controller
- Piconet Relationship
- Peer to Peer Data Transmission
- Independent Piconet Controller

**802.15.3**

- IEEE 803.15.3 MAC is designed to support the following goals:
  - ✓ Fast connection time
  - ✓ Ad hoc networks
  - ✓ Data transport with quality of service (QoS)
  - ✓ Security
  - ✓ Dynamic membership
  - ✓ Efficient data transfer

**Coordination in IEEE 802.15.3**

- Starting a piconet
  - ✓ DEV scans for the best channel and sends out beacons -> the DEV becomes PNC
  - ✓ If no channels available: Establishes a child or neighbor piconet instead
  - ✓ While the process of starting a piconet does not ensure that the "most capable" PNC is initially selected
- Handing over control of the piconet
  - ✓ When a DEV associates, PNC checks the capabilities of the new DEV to see if it is more capable to be the PNC of the piconet
  - ✓ In handover process, it maintains all existing time allocations so that there is no interruption in the delivery
- Creating a child piconet
  - ✓ A child piconet is one that is formed under an established piconet. The established piconet then becomes the parent piconet.
  - ✓ The child piconet functionality is useful for either extending the area of coverage of the piconet or shifting some computational or memory requirements to another PNC capable DEV.
  - ✓ The child piconet uses a distinct piconet ID (PNID) and acts as an autonomous piconet except that it is dependent on a private CTA from the parent piconet.
- Ending a piconet
  - ✓ If the PNC is going to stop operation and there are no other PNC capable DEVs in the piconet, the PNC places the PNC Shutdown information element (IE) into the beacon to notify the members of the piconet.
  - ✓ In the case that the PNC abruptly leaves the piconet without handing over control to another PNC capable DEV in the piconet, the piconet stops operation.
  - ✓ After the association timeout period (ATP) expires, a PNC capable DEV from the old piconet will be able to start a new piconet using the normal process,
  - ✓ In the case of dependent piconets, the parent PNC is able to end the dependent piconet via the Disassociation Request command,
- Association and disassociation
  - ✓ Associating with the piconet provides the DEV with a unique identifier, the DEVID, for that piconet

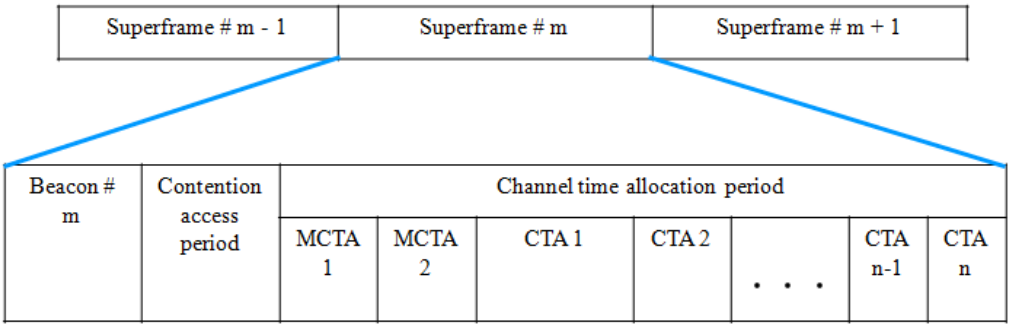
- ✓ The DEVID, one octet in length, is used instead of the DEV's address, 8 octets in length, to save overhead in the system.
- ✓ The association process optionally provides information about the services available in the piconet as well as the services provided or PNC capabilities
- ✓ PNC broadcasts the information about all of the DEVs in the piconet, and places information in the beacon about the new DEV.
- ✓ When a DEV wants to leave the piconet or if the PNC wants to remove a DEV from the piconet, the disassociation process is used.
- ✓ The DEVID of the disassociated DEV is no longer valid, until reissued by the PNC.
- ✓ However, the PNC is not allowed to reissue the DEVID until a waiting period hasexpired

**Security**

- Security for the piconet is one of two modes
  - ✓ Mode 0 Open:
    - Security membership is not required and payload protection (either data integrity or data encryption) is not used by the MAC. The PNC is allowed to use a list of DEV addresses to admit or deny entry to the piconet.
  - ✓ Mode 1—Secure membership and payload protection:

**IEEE 802.15.3 – Superframe**

- The super-frame is composed of three parts:
  - ✓ The beacon
    - Which is used to set the timing allocations and to communicate management information for the piconet.
  - ✓ The contention access period (CAP)
    - Which is used to communicate commands and/or asynchronous data if it is present in the superframe.
  - ✓ The channel time allocation period (CTAP)
    - Which is composed of channel time allocations (CTAs), including management CTAs (MCTAs).




- The MCTAs are shown first, but the PNC is allowed to place any number of them at any position in the superframe.

- Channel time is divided into superframe with
  - ✓ Beacon
    - Contains piconet synchronization parameter and IE (Information Element)s
  - ✓ CAP (Contention Access Period)
    - Optional. For command frames and non-stream data. Using CSMA/CA with backoff scheme
  - ✓ CFP (Contention Free Period)
    - For data stream. PNC assigns to DEV with each CTA (Channel Time Allocation)

**IEEE 802.15.3 – CAP**

- CAP
  - ✓ Allows contention via CSMA/CD
- CTA
  - ✓ The CTAP, uses a standard TDMA protocol where the DEVs have specified time windows,
- Contention Free Access
  - ✓ To enable power saving and QoS
  - ✓ CTA
    - Private CTA – for dependent piconet
    - Dynamic CTA – scheduled on a superframe by superframe basis
    - Pseudo-Static CTA – only for isochronous stream. Allowed to transmit during CTA as long as the number of consecutive lost beacon is less then mMaxLostBeacons

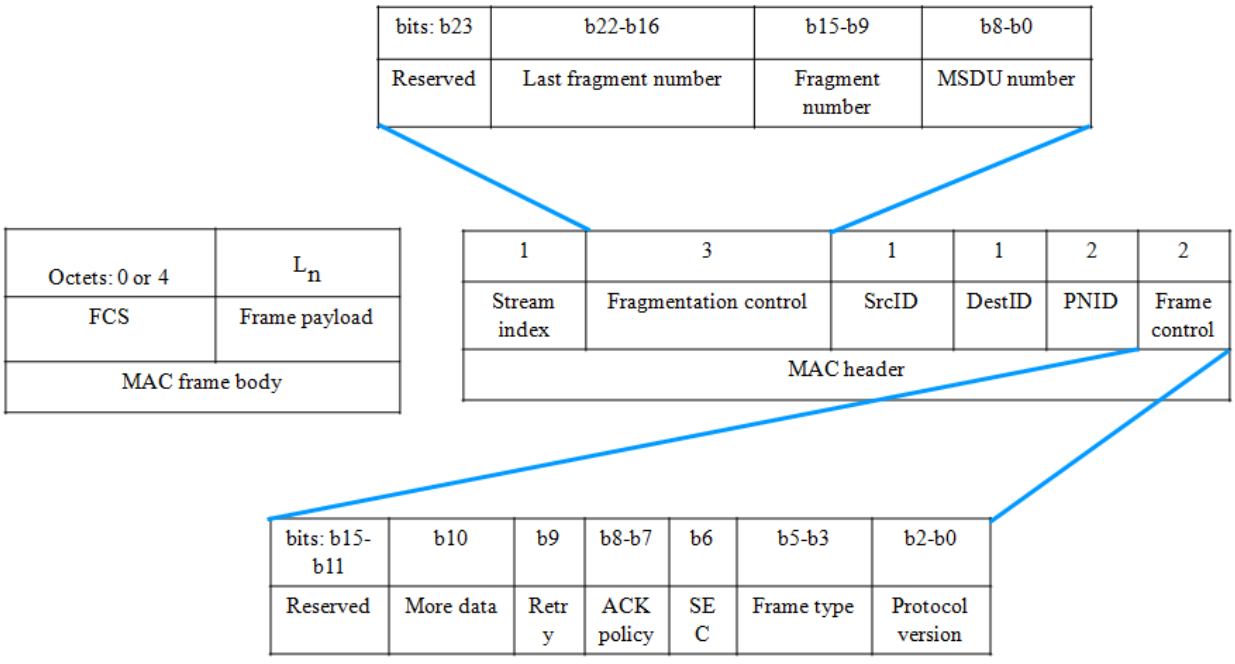
**Channel time management**

- There are three methods for communicating data between DEVs in the piconet:
  - ✓ Sending asynchronous data in the CAP, if present.
  - ✓ Allocating channel time for isochronous streams in the CTAP.
  - ✓ Allocating asynchronous channel time in the CTAP.
- Dynamic channel selection
  - ✓ Due to ISM bands, piconet is subject to interference from unlicensed users or other 802.15.3 piconets
  - ✓ PNC has the capability to dynamically change the channel that the piconet is using without requiring either user intervention or the disruption of services in the piconet.
  - ✓ To evaluate the status of the current channel as well as other channels, the PNC is able to use many methods including:
    - Gathering information about the current channel from other DEVs in the piconet using the Channel Status Request command.
    - Performing a passive scan of the channels.
    - Requesting other DEVs to perform a channel scan using the Remote Scan Request command,

**Power Management**

- Standard provides three techniques to enable DEVs to turn off for one or more superframes:
  - ✓ device synchronized power save (DSPS) mode
  - ✓ Piconet-synchronized power save (PSPS) mode
  - ✓ Asynchronous power save (APS) mode.
- PSPS
  - ✓ PSPS mode allows DEVs to sleep at intervals defined by the PNC.
  - ✓ The DEV sends a request to the PNC when it wants to enter the PSPS mode.
- DSPS
  - ✓ Besides allowing the DEVs to wake up and exchange traffic at the same time, the use of DSPS sets makes it easy for other DEVs in the piconet to determine exactly when a DSPS DEV will be available to receive traffic.
- APS
  - ✓ The only responsibility of a DEV in APS mode is to communicate with the PNC before the end of its ATP in order to preserve its membership in the piconet.

**MAC Frame format**




**ACK Policy**

- If the source DEV wishes to verify the delivery of a frame, then one of the acknowledgement (ACK) policies
  - ✓ NO ACK
    - The no-ACK policy, is appropriate for frames that do not require guaranteed delivery, where the retransmitted frame would arrive too late or where an

upper layer protocol is handling the ACK and retransmission protocol.

- ✓ The immediate-ACK (Imm-ACK) policy,
  - It provides an ACK process in which each frame is individually ACKed following the reception of the frame.
- ✓ The delayed-ACK (Dly-ACK) policy,
  - It lets the source send multiple frames without the intervening ACKs. Instead, the ACKs of the individual frames are grouped into a single response frame that is sent when requested by the source DEV.
  - The Dly-ACK process decreases the overhead in the Imm-ACK process while allowing the source DEV to verify the delivery of frames to the destination.

**Lecture 41**

**IEEE 802.15.4/ZigBee**

**Outlines**

- Overview of ZigBee
  - ✓ Whats is ZigBee, Zigbee in Wireless World, Architecture, Characteristics
- IEEE 802.15.4
  - ✓ Basics, Type of Devices
  - ✓ Topology, Addressing
  - ✓ Phy Layer
  - ✓ Channel Access Mechanisms
    - Slotted/Unslotted CSMA/CA
  - ✓ Data Transfer Model
  - ✓ Superframe Structure

**Last Lecture**

- IP Over Bluetooth
- Bluetooth Security
- WPAN Standards
- IEEE 802.15.3 Overview
- 802.15.3
  - ✓ Topology
  - ✓ Coordination
    - Starting a Piconet
    - Handing over control of piconet
    - Creating child piconet
    - Ending a Piconent
    - Association/Disassociation
  - ✓ Medium Access (Superframe)
  - ✓ Channel Time Management
  - ✓ Power management
  - ✓ MAC Frame forma

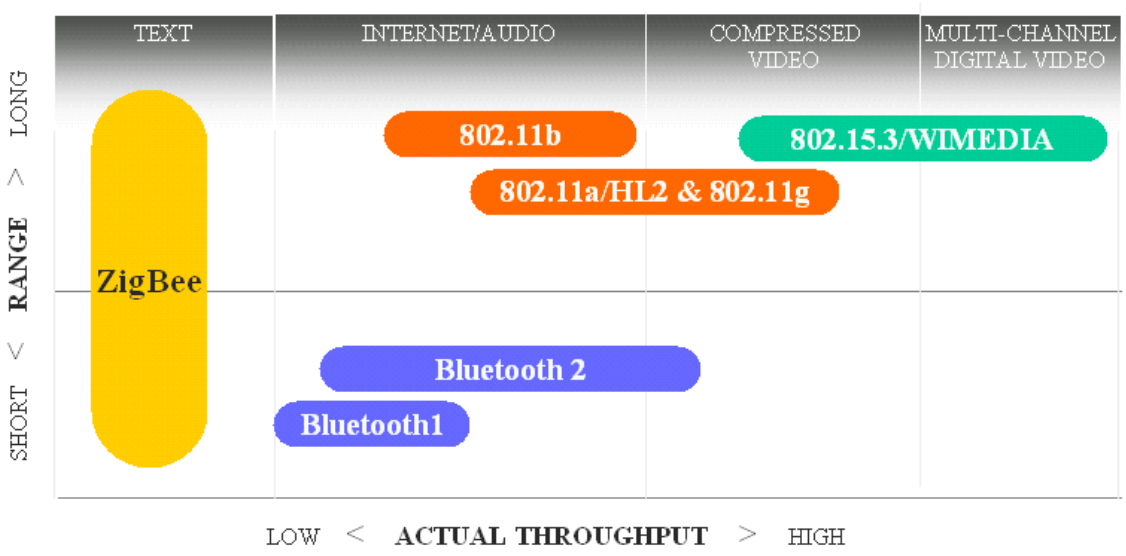
**What is ZigBee Alliance?**

- An organization with a mission to define reliable, cost effective, low-power, wirelessly networked, monitoring and control products based on an open global standard
- The alliance provides interoperability, certification testing, and branding.

**IEEE 802.15.4: What is ZigBee?**

- A standard for mesh networking
  - ✓ Reliability through meshed connectivity
- Designed for low power applications
  - ✓ Very long battery life
- Low data rate
  - ✓ 20-250Kb/sec (depending on band)
- Very Secure
  - ✓ AES-128 encryption available
- Self configuring
  - ✓ Allows ad hoc networks
  - ✓ Ease of installation and configuration

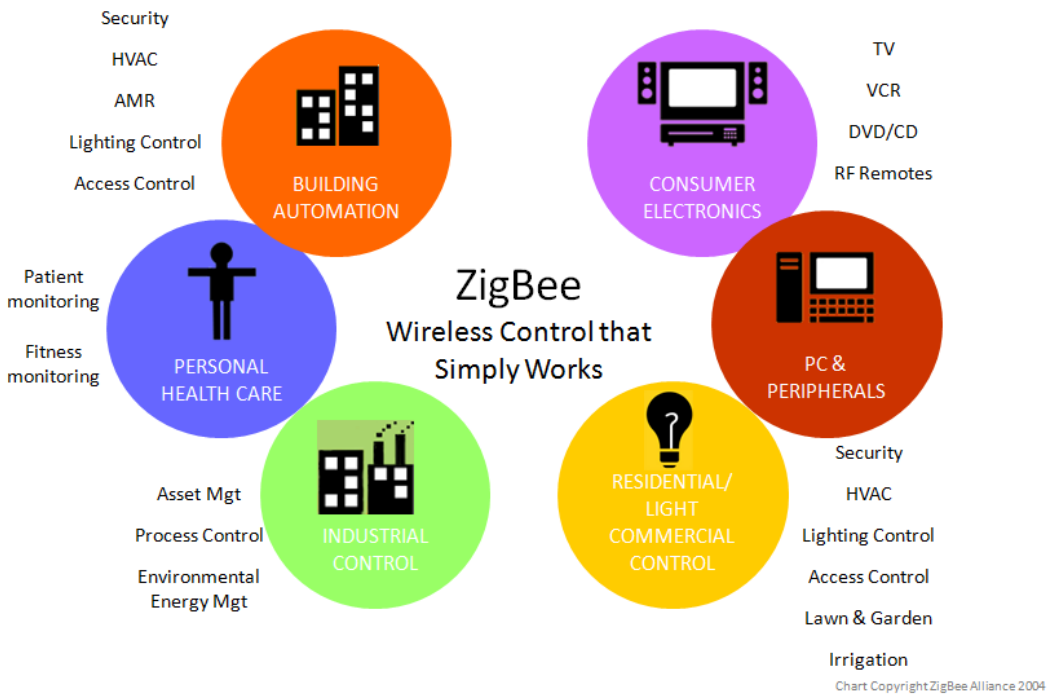
**ZigBee in the wireless world**



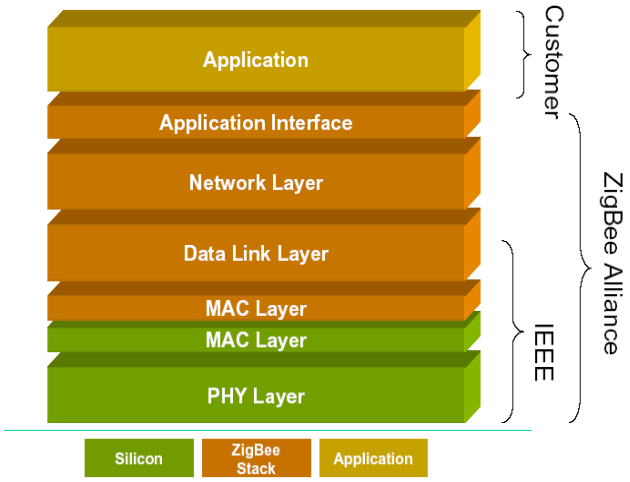

**ZigBee/IEEE 802.15.4 Market Feature**

- Low power consumption
- Low cost
- Low offered message throughput
- Supports large network orders (<= 65k nodes)
- Low to no QoS guarantees
- Flexible protocol design suitable for many applications

**ZigBee Target Markets**



**ZigBee/802.15.4 Architecture**




**ZigBee/802.15.4 Technology: General Characteristics**

- Data rates of 250 kbps , 20 kbps and 40kpbs.
- Star or Peer-to-Peer operation.
- Support for low latency devices.
- CSMA-CA channel access.
- Dynamic device addressing.
- 16 channels in the 2.4GHz ISM band, 10 channels in the 915MHz ISM band and one channel in the European 868MHz band.

**IEEE 802.15.4 Basics**

- 802.15.4 is a simple packet data protocol for lightweight wireless networks
  - ✓ Channel Access is via Carrier Sense Multiple Access with collision avoidance and optional time slotting

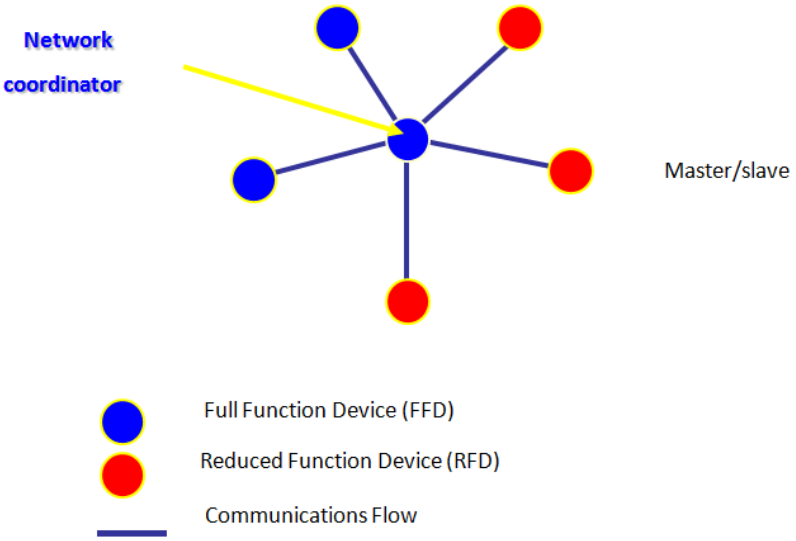
**IEEE 802.15.4 Device Types**

- There are two different device types :
  - ✓ A full function device (FFD)
  - ✓ A reduced function device (RFD)
- The FFD can operate in three modes serving
  - ✓ Device
  - ✓ Coordinator
  - ✓ PAN coordinator
- The RFD can only operate in a mode serving:
  - ✓ Device

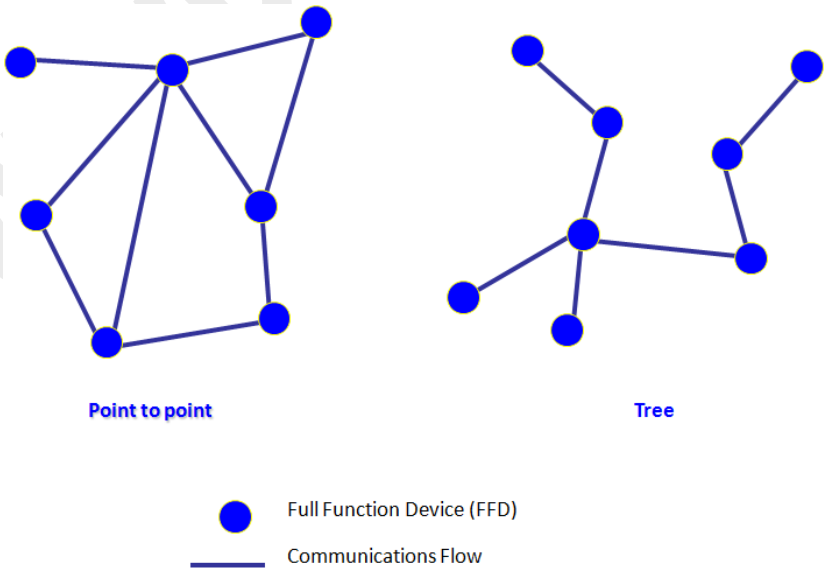
**FFD vs RFD**

- Full function device (FFD)
  - ✓ Any topology
  - ✓ Network coordinator capable
  - ✓ Talks to any other device
- Reduced function device (RFD)

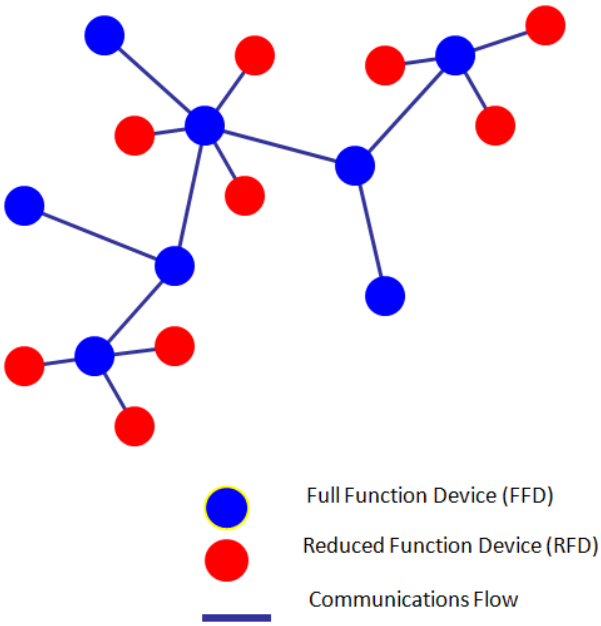
**Star Topology**




**Peer-Peer Topology**

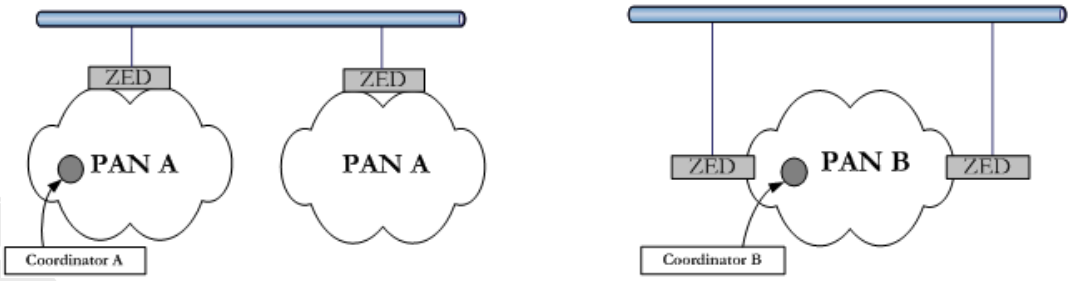


**Combined Topology**




**Extending ZigBee Networks**

- ZED (ZigBee Extension Device)
  - ✓ A ZigBee router with a wire interface
- Joins two or more radio disjoint PANs
- Provides a "wormhole" within a single PAN
  - ✓ A low cost, high reliability link within the radio network
- "Extends" the ZigBee network layer

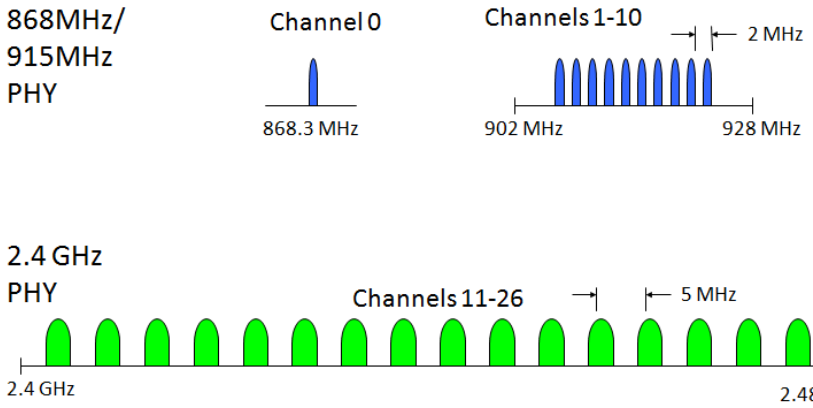



**Device Addressing**

- Each independent PAN will select a unique PAN identifier
- Addressing modes:
  - ✓ star: Network (64 bits) + device identifier (16 bits)
  - ✓ peer-to-peer: Source/destination identifier (64 bits)

**IEEE 802.15.4 PHY Overview**

- PHY functionalities:
  - ✓ Activation and deactivation of the radio transceiver
  - ✓ Energy detection within the current channel
  - ✓ Link quality indication for received packets
  - ✓ Clear channel assessment for CSMA-CA
  - ✓ Channel frequency selection
  - ✓ Data transmission and reception
- Operating Frequency Bands




**Frequency Bands and Data Rates**

- The standard specifies two PHYs :
  - ✓ 868 MHz/915 MHz direct sequence spread spectrum (DSSS) PHY (11 channels)
    - 1 channel (20Kb/s) in European 868MHz band
    - 10 channels (40Kb/s) in 915 (902-928)MHz ISM band
  - ✓ 2450 MHz direct sequence spread spectrum (DSSS) PHY (16 channels)
    - 16 channels (250Kb/s) in 2.4GHz band

**General Radio Specifications**

- Transmit Power
  - ✓ Capable of at least –3dBm
- Receiver Sensitivity
  - ✓ -85 dBm (2.4GHz) / -91dBm (868/915MHz)
- Link quality indication
  - ✓ The measurement may be implemented using
    - Signal to noise ratio estimation
    - Receiver energy detection

**Channel Access Mechanism**

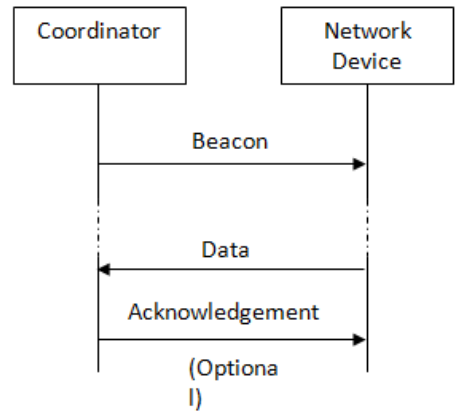
- Two type channel access mechanism, based on the network configuration:
  - ✓ In non-beacon-enabled networks → unslotted CSMA/CA channel access mechanism
  - ✓ In beacon-enabled networks → slotted CSMA/CA channel access mechanism
    - The super frame structure will be used.

**CSMA/CA Algorithm**

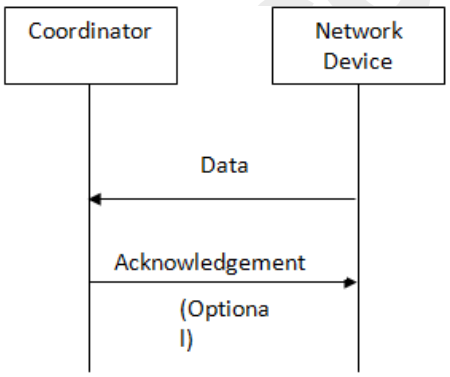
- Each device shall maintain three variables for each transmission attempt
  - ✓ NB: number of slots the CSMA/CA algorithm is required to backoff while attempting the current transmission.
  - ✓ BE: the backoff exponent which is related to how many backoff periods a device shall wait before attempting to assess a channel
- CW: (a special design)

**Data Transfer Model**

- Data transferred from device to coordinator

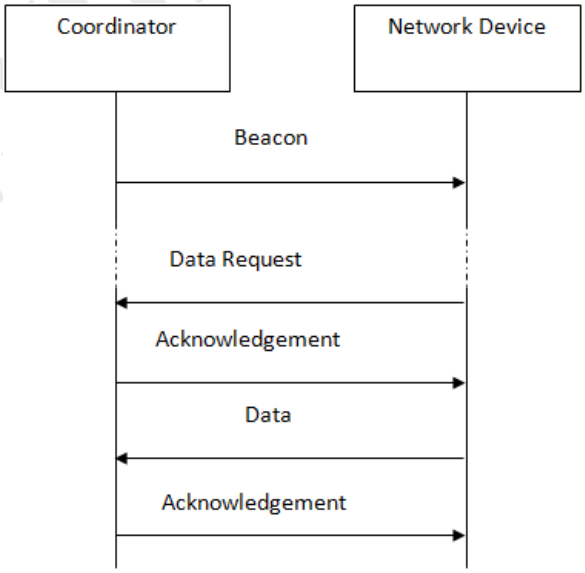



Communication to a coordinator
In a beacon-enabled network



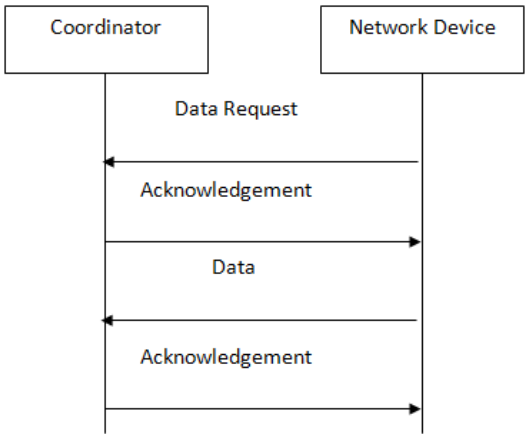

Communication to a coordinator
In a non beacon-enabled network

- Data transferred from coordinator to device.



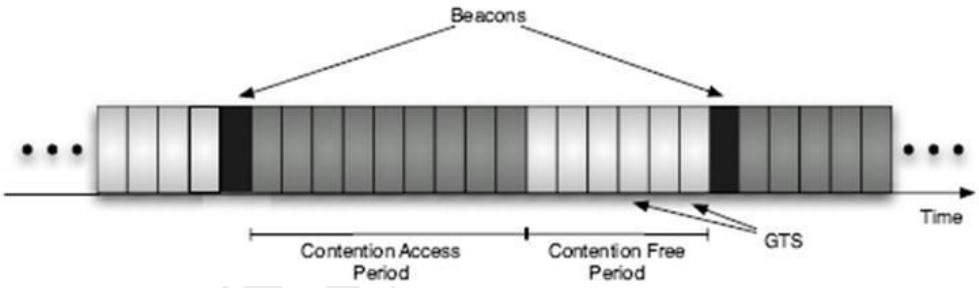

Communication from a coordinator
In a beacon-enabled network

- Data transferred from coordinator to device




Communication from a coordinator in a non beacon-enabled network

**Superframe**




- In CFP, a GTS may consist of multiple slots, all of which are assigned to a single device, for either transmission (t-GTS) or reception (r-GTS).
  - ✓ GTS = guaranteed time slots
- In CAP, the concept of slots is not used.
  - ✓ Each "contention slot" is of 20 symbols long.

**Lecture 42**

**IEEE 802.16**

**WiMAX Basics**

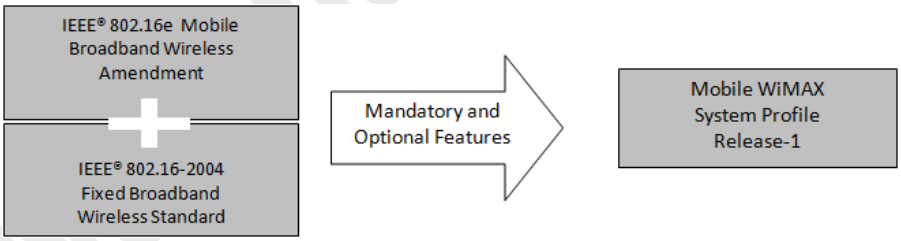
- WiMAX or 802.16 is an effort by the IEEE to develop a standards based air interfaces for the licensed and unlicensed radio frequencies from 2 to 66 GHz
- The approach they have taken is to develop a common MAC – Media Access Control sub layer of the data link layer
- Then to offer differing physical layers to accommodate the needs of the different frequencies and regulatory environments
- The IEEE believes that the existing approaches to delivering wireless data services do have the potential for long term growth when used outside of the local area network

**IEEE 802.16 Overview**

- Family of standards for wireless metropolitan area networks (WMAN)
- Provide broadband (i.e., voice, data, video) connectivity
- Specifies the air interface, including the medium access control (MAC) layer and multiple physical layer specifications
- 802.16e is an amendment to 802.16d (fixed or nomadic wireless broadband) to support mobility
  - ✓ Vehicular speeds up to 75 mph

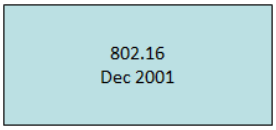
**WiMAX Forum**

- Formed in June 2001 to promote conformance and interoperability of the 802.16 standard
- Develops "system profiles" that define mandatory and optional features of standard

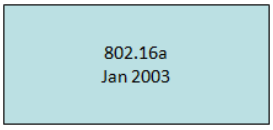



**802.16 Evolution**

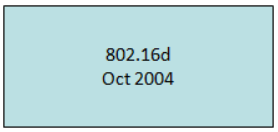
- Original fixed wireless broadband air Interface for 10 – 66 GHz
- Line-of-sight only
- Point-to-Multi-Point applications



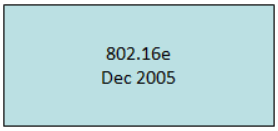

- Extension for 2-11 GHz
- Non-line-of-sight
- Point-to-Multi-Point applications



- Revised and replaced previous versions
- WiMAX System Profiles




- MAC/Physical layer enhancements to support subscribers moving at vehicular speeds




**Characteristics of 802.16 Frequency Ranges**

- 10 - 66 GHz
  - ✓ Short wavelength
  - ✓ Line-of-sight (LOS) required
  - ✓ Negligible multipath
  - ✓ The commonly used frequencies in this range are 10.5, 25, 26, 31, 38, and 39 GHz
- 2 – 11 GHz
  - ✓ Longer wavelength
  - ✓ LOS not required
  - ✓ Improved range and in-building penetration
  - ✓ Multipath effects may be significant

**IEEE 802.16 Standards**

| | **802.16** | **802.16d/HiperMAN** | **802.16e** |
|---|---|---|---|
| **Completed** | December 2001 | June 2004 (802.16d) | Estimate 2005 |
| **Spectrum** | 10 - 66 GHz | < 11 GHz | < 6 GHz |
| **Channel Conditions** | Line of Sight Only | Non Line of Sight | Non Line of Sight |
| **Bit Rate** | 32 – 134 Mbps in 28MHz channel bandwidth | Up to 75 Mbps in 20MHz channel bandwidth | Up to 15 Mbps in 5MHz channel bandwidth |
| **Modulation** | QPSK, 16QAM and 64QAM | OFDM 256 FFT<br>QPSK, 16QAM, 64QAM | Scalable OFDMA<br>128 to 2048 FFT |
| **Mobility** | Fixed | Fixed | Portable |
| **Channel Bandwidths** | 20, 25 and 28 MHz | 1.75 to 20 MHz | 1.75 to 20 MHz |

**Why do we need broadband wireless access?**

- Fill the gap between high data rate wireless LAN and very mobile cellular networks.
- Wireless alternative to cable and DSL for last-mile broadband access
  - ✓ Developing countries
  - ✓ Rural areas
- Provide high-speed mobile data and telecommunications services

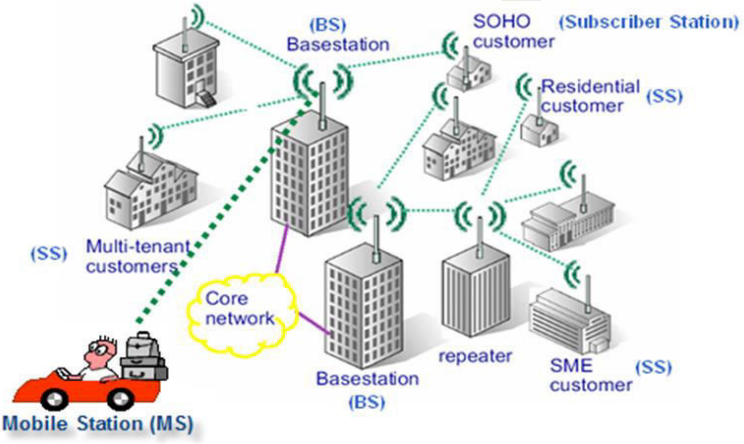
**802.11 v 802.16**

- 802.11's media access control protocol is optimized for shorter-range topologies
- It also was not designed to serve a large number of users
- Wireless MAN, on the other hand, was designed to solve the problems of delivering wireless broadband networks over longer distances and through more difficult environments, such as heavily wooded areas

**Comparison 802.11 and 802.16**

| Technology | 802.11 | 802.16 |
|---|---|---|
| **Range** | < 300 feet | < 30 Mile ( typical 3~4) |
| **Coverage** | Optimized for indoor short range | Outdoor LOS & NLOS |
| **Data rate** | 2.7 bps/Hz peak. <= 54Mbps in 20MHz | 5bps/Hz peak, <100Mbps in 20 MHz |
| **Scalability** | 1-10 CPE CSMA/CA | 1- hundreds CPE TDMA |
| **QOS** | No QOS | On demand BW ➔ voice Video, data |

**Network Architecture**




- Source: WiMAX Nuts and Bolts – Steve Hilton [3]

**Physical Layer**

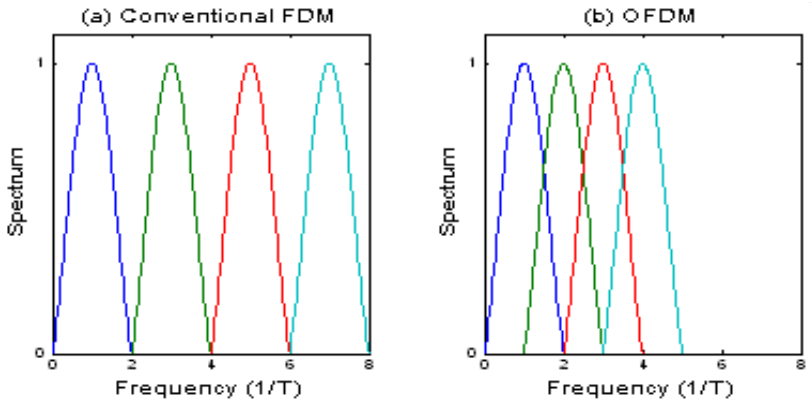
- Five physical layer modes

| | Designation | Applicability |
|---|---|---|
| | WirelessMAN-SC | 10 -66 GHz |
| | WirelessMAN-SCa | Below 11GHz – Licensed bands |
| 802.16d → | WirelessMAN-OFDM | Below 11GHz – Licensed bands |
| 802.16e → | WirelessMAN-OFDMA | Below 11GHz – Licensed bands |
| | WirelessHUMAN | Below 11GHz – Licensed-exempt bands |

**Orthogonal Frequency Division Multiplexing (OFDM)**

- Multiplexing technique that divides the channel into multiple orthogonal sub channels
- Input data stream is divided into several substreams of a lower data rate (increased symbol duration) and each substream is modulated and simultaneously transmitted on a separate sub channel
- High spectral efficiency, resilient to interference, and low multi-path distortion

**Conventional FDM and OFDM**




- Source: Broadband Wireless Access (W-PAN, W-LAN, WiMAX, Wi-Mob) (including OFDM concepts) - A. K. Seth [4]

**Orthogonal Frequency Division Multiple Access (OFDMA)**

- Multiple-access/multiplexing scheme
  - ✓ A multiple-access/multiplexing scheme that provides multiplexing operation of data streams from multiple users onto the downlink sub-channels and uplink multiple access by means of uplink sub-channels.
  - ✓ Dynamically assign a subset of subchannels to individual users
- WirelessMAN-OFDMA based on scalable OFDMA (SOFDMA)
  - ✓ Support scalable channel bandwidths from 1.25 to 20 MHz

**Other Physical Layer Features**

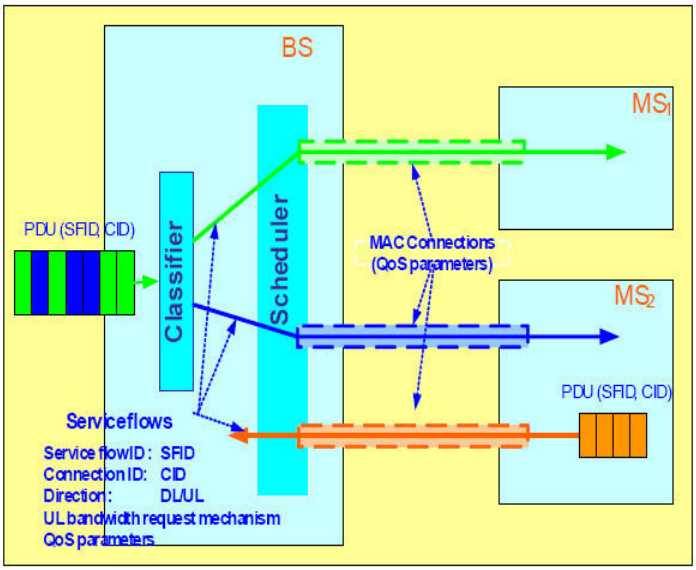
- Hybrid automatic repeat request (HARQ)
  - ✓ Adjusts automatically to channel conditions
  - ✓ Receiver saves failed transmission attempts to help future decoding
    - Every transmission helps increase probability of success
- Multiple-in Multiple-out (MIMO)
  - ✓ Multiple antennas on sender and receivers
  - ✓ Takes advantage of multi-path
  - ✓ Increased spectral efficiency

**TDD**

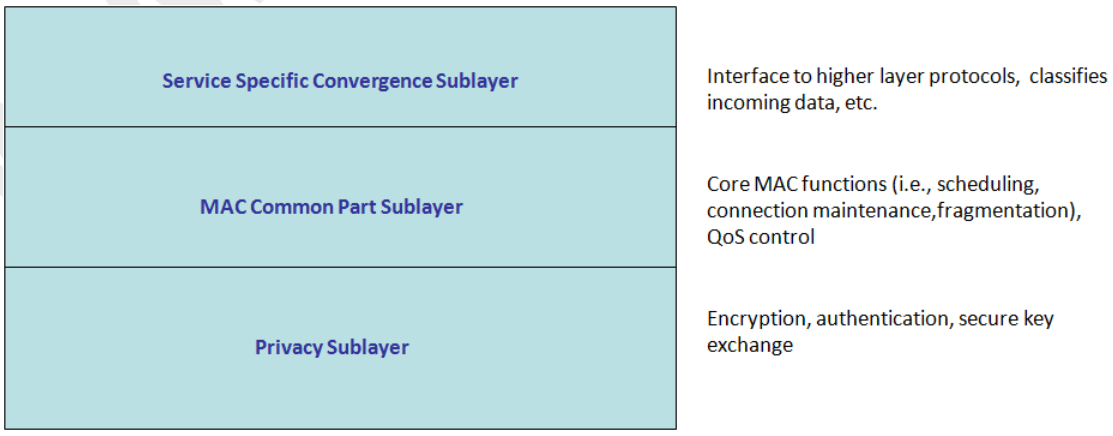
- The 802.16e PHY supports TDD and Full and Half-Duplex FDD operation;
- To counter interference issues, TDD does require system-wide synchronization;
- TDD is the preferred duplexing mode for the following reasons:
  - ✓ TDD enables adjustment of the downlink/uplink ratio to efficiently support asymmetric downlink/uplink traffic,
  - ✓ Unlike FDD, which requires a pair of channels, TDD only requires a single channel for both downlink and uplink providing greater flexibility
  - ✓ Transceiver designs for TDD implementations are less complex and therefore less expensive.

**MAC Layer**

- Connection-oriented
- A fundamental premise of the MAC architecture is quality of service (QoS)
- QoS provided via service flows




**MAC Layer**



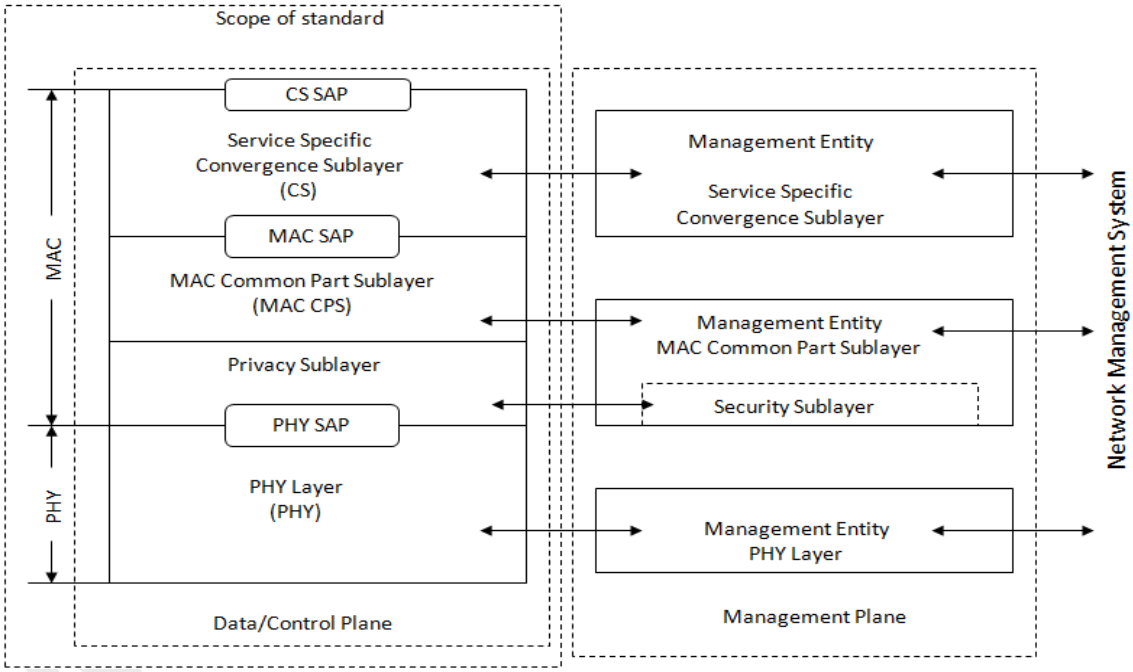
**Lecture 43**

**IEEE 802.16 MAC/QoS**

**Outlines**

- Reference Model
- Burst profiles
- Convergence sublayers
- MAC PDU format
- MAC PDU Transmission
- Fragmentation / Packing
- Request/Grant Scheme
- Classes of Uplink service
- Power management/Handoff
- WiMAX Basics
- 802.16 Evolution
- Characteristics of 802.16
- Why not 802.11 / 802.11 vs 802.16
- Network Architecture
- Phy Layer
  - ✓ Multiple Access technique
  - ✓ HARQ
  - ✓ MIMO
- MAC Layer
  - ✓ QoS
  - ✓ Power Management
  - ✓ Handoff

**Reference Model**




**Adaptive Burst Profiles**

- Burst profile
  - ✓ Modulation and FEC
- Dynamically assigned according to link conditions
  - ✓ Burst by burst, per subscriber station
  - ✓ Trade-off capacity vs. robustness in real time
- Roughly doubled capacity for the same cell area
- Burst profile for downlink broadcast channel is well-known

**ATM Convergence Sublayer**

- Support for:
  - ✓ VP (Virtual Path) switched connections
  - ✓ VC (Virtual Channel) switched connections
- Support for end-to-end signaling of dynamically created connections:
  - ✓ SVCs
  - ✓ soft PVCs
- ATM header suppression
- Full QoS support

**Packet Convergence Sublayer**

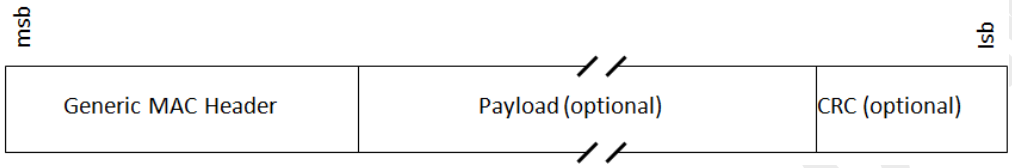
- Initial support for Ethernet, IPv4, and IPv6
- Payload header suppression
- Full QoS support
- Possible future support for:
  - ✓ PPP
  - ✓ MPLS
- Upon entering the network, the SS is assigned three management connections in each direction. These three connections reflect the three different QoS requirements used by different management levels.
  - ✓ Basic connection, which is used for the transfer of short, time-critical MAC and radio link control (RLC) messages.
  - ✓ The primary management connection is used to transfer longer, more delay-tolerant messages such as those used for authentication and connection setup.
  - ✓ The secondary management connection is used for the transfer of standards-based management messages such as DHCP, Trivial FTP, and SNMP.
- In addition to these management connections, SSs are allocated transport connections for the contracted services.
- Transport connections are unidirectional to facilitate different uplink and downlink QoS and traffic parameters;

**Definitions**

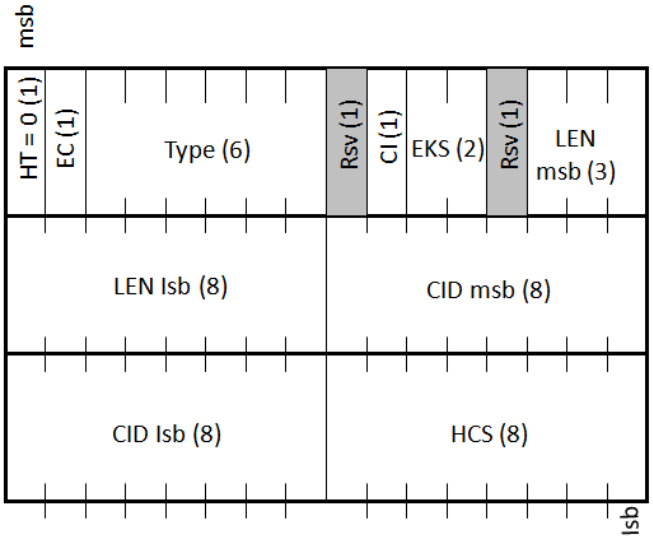
- Service Data Unit (SDU)
  - ✓ Data units exchanged between adjacent layers
- Protocol Data Unit (PDU)
  - ✓ Data units exchanged between peer entities
- Connection and Connection ID
  - ✓ A unidirectional mapping between MAC peers over the airlink (uniquely identified by a CID)
- Service Flow and Service Flow ID
  - ✓ A unidirectional flow of MAC PDUs on a connection that provides a particular QoS (Uniquely identified by a SFID)

**MAC PDU format**

- A MAC PDU consists of a fixed-length MAC header, a variable-length payload, and an optional cyclic redundancy check (CRC).
- Two header formats, distinguished by the HT field, are defined:
  - ✓ The generic header
  - ✓ Bandwidth request header.
- One or more MAC sub-headers may be part of the payload
- The presence of sub-headers is indicated by a Type field in the Generic MAC header field



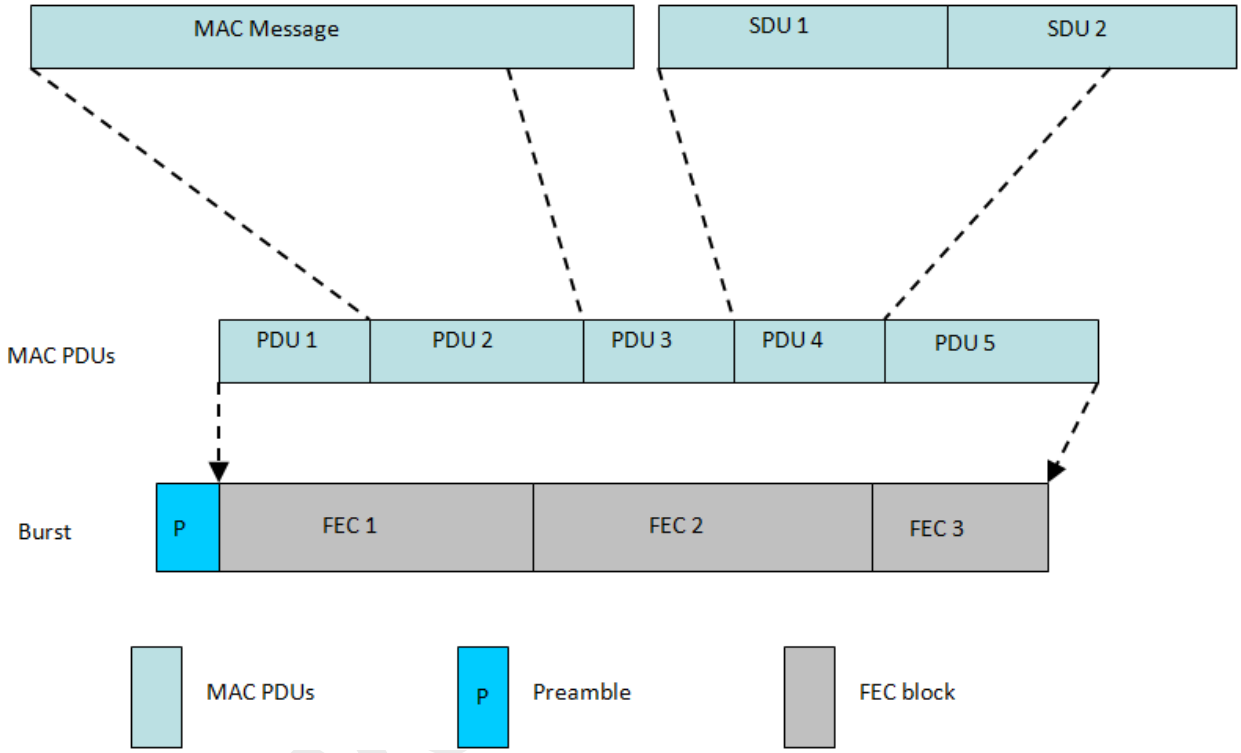

**Generic MAC Header**




- Three types of MAC subheader may be present.
  - ✓ The grant management subheader
    - Is used by an SS to convey bandwidth management needs to its BS.
  - ✓ The fragmentation sub-header
    - Contains information that indicates the presence and orientation in the payload of any fragments of SDUs.
  - ✓ The packing sub-header
    - Is used to indicate the packing of multiple SDUs into a single PDU.
- The grant management and fragmentation sub-headers may be inserted in MAC PDUs immediately following the generic header if so indicated by the Type field.
- The packing sub-header may be inserted before each MAC SDU if so indicated by the Type field.

**MAC PDU Transmission**

- MAC PDUs are transmitted in PHY bursts
- A single PHY burst can contain multiple *Concatenated* MAC PDUs
- The PHY burst can contain multiple FEC blocks
- MAC PDUs may span FEC block boundaries
- The TC layer between the MAC and the PHY allows for capturing the start of the next MAC PDU in case of erroneous FEC blocks



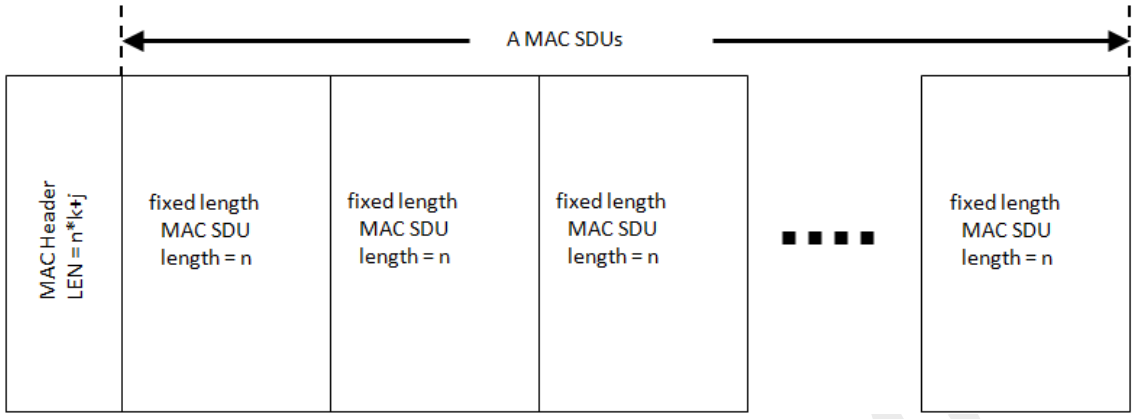

**Fragmentation**

- Partitioning a MAC SDU into fragments transported in multiple MAC PDUs
- Contents of the fragmentation sub-header:
  - ✓ 2-bit Fragmentation Control (FC)
    - Un-fragmented
    - First fragment
    - Last fragment
    - Continuing fragment
  - ✓ 3-bit Fragmentation Sequence Number (FSN)
    - Required to detect missing continuing fragments

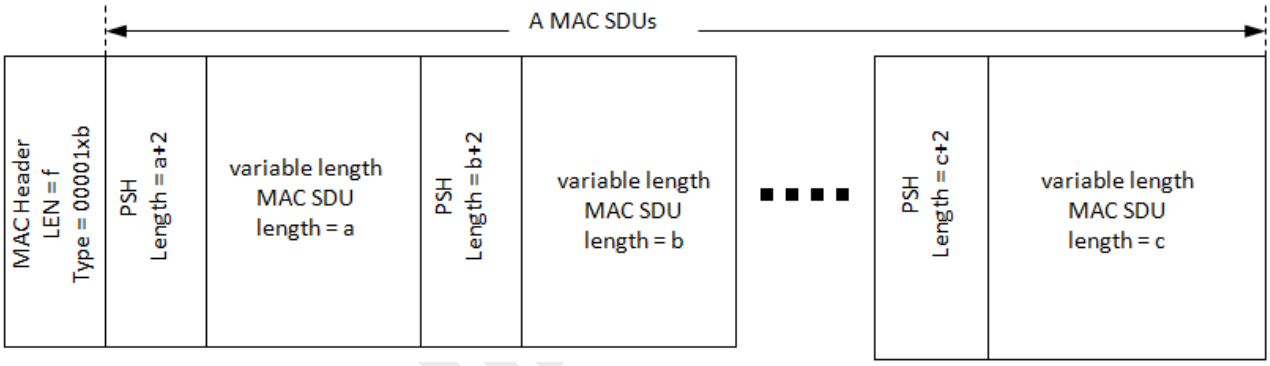
**Packing**

- The process of combining multiple MAC SDUs (or fragments thereof) into a single MAC PDU
- On connections with variable length MAC SDUs
- On connections with fixed length MAC SDUs
- Can, in certain situations, save up to 10% of system bandwidth

**Packing Fixed-Length SDUs**




**Packing Variable-Length SDUs**



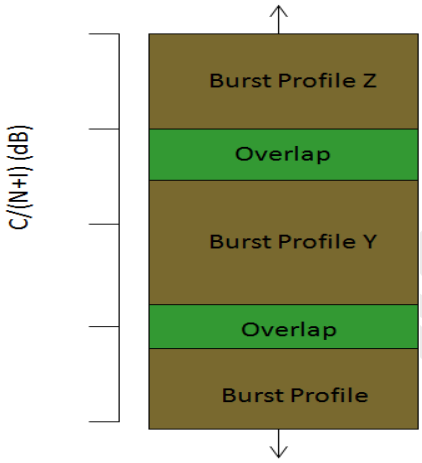

- 2 Bytes Packing Sub-Header before each SDU
  - ✓ Length of SDU: 11 bits
  - ✓ Fragmentation control (FS): 2 bits
  - ✓ Fragmentation sequence number (FS): 3 bits

**Downlink transmissions**

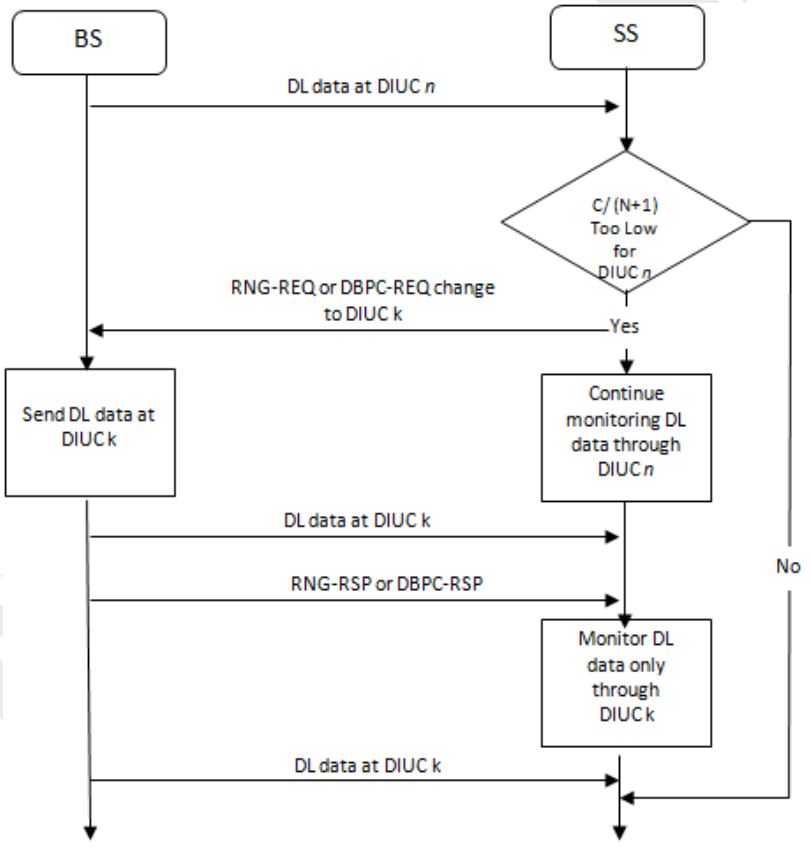
- Two kinds of bursts: TDM and TDMA
- All bursts are identified by a DIUC
  - ✓ Downlink Interval Usage Code
- TDMA bursts have resync preamble
  - ✓ Allows for more flexible scheduling
- Each burst may contain data for several terminals
- SS must recognize the PDUs with known CIDs
- DL-MAP message signals downlink usage

**Burst profiles**

- Each burst profile has mandatory exit threshold and minimum entry threshold
- SS allowed to request a less robust DIUC once above the minimum entry level
- SS must request fall back to more robust DIUC once at mandatory exit threshold
- Requests to change DIUC done with DBPC-REQ or RNG-REQ messages




**Transition to a more robust profile**




**Request/Grant Scheme**

- Self Correcting
- Bandwidth Requests are always per Connection
- Grants are either per Connection (GPC) or per Subscriber Station (GPSS)

**GPSS vs. GPC**

- Bandwidth Grant per Subscriber Station (GPSS)
  - ✓ Base station grants bandwidth to the subscriber station
  - ✓ Subscriber station may re-distribute bandwidth among its connections, maintaining QoS and service-level agreements
- Bandwidth Grant per Connection (GPC)
  - ✓ Base station grants bandwidth to a connection
  - ✓ Higher overhead, but allows simpler subscriber station

**Classes of Uplink Service**

- Unsolicited Grant Services (UGS)
- Real-time Polling Services (rtPS)
- Non-real-time Polling Services (nrtPS)
- Best Effort (BE)
  - ✓ For best-effort traffic

| QoS Category | Applications | QoS Specifications |
|---|---|---|
| UGS<br>Unsolicited Grant Service | VoIP | • Maximum Sustained Rate<br>• Maximum Latency Tolerance<br>• Jitter Tolerance |
| rtPS<br>Real-Time Polling Service | Streaming Audio or Video | • Minimum Reserved Rate<br>• Maximum Sustained Rate<br>• Maximum Latency Tolerance<br>• Traffic Priority |
| ErtPS<br>Extended Real-Time Polling Service | Voice with Activity Detection (VoIP) | • Minimum Reserved Rate<br>• Maximum Sustained Rate<br>• Maximum Latency Tolerance<br>• Jitter Tolerance<br>• Traffic Priority |
| nrtPS<br>Non Real-Time Polling Service | File Transfer Protocol (FTP) | • Minimum Reserved Rate<br>• Maximum Sustained Rate<br>• Traffic Priority |
| BE<br>Best-Effort Service | Data Transfer, Web Browsing, etc. | • Maximum Sustained Rate<br>• Traffic Priority |

**Uplink Services - UGS**

- No explicit bandwidth requests issued by SS
- Prohibited from using any contention requests
- No unicast request opportunity provided
- May include a Grant Management (GM) sub-header containing
  - ✓ Slip indicator: indicates that there is an backlog in the buffer due to clock skew or loss of maps
  - ✓ Poll-me bit: indicates that the terminal needs to be polled (allows for not polling terminals with UGS-only services).

**Uplink Services - RTPS**

- Intended for rt-VBR-like service flows such as MPEG video
- Prohibited from using any contention requests
- Terminals polled frequently enough to meet the delay requirements of the SFs
- Bandwidth requested with BW request messages (a special MAC PDU header)
- May use Grant Management sub-header

**Uplink Service - NRTPS**

- Intended for non-real-time service flows with better than best effort service
- Works like rt-polling except that polls are issued less frequently
- Allowed to use contention requests
- May use Grant Management sub-header

**Uplink Service - BE**

- No QoS guarantees
- Allowed to use contention requests
- May use Grant Management sub-header

**Power Management**

- Sleep and Idle modes enable power-efficient MS operation
- Sleep mode
- Idle mode
    - ✓ Allows MS to become periodically available for broadcast messages without registering at a BS

**Handoff**

- 3 handoff methods supported
    - ✓ Hard Handoff (HHO) – required
        - "Break-before-make"
        - Optimized to keep handoff delays below 50 milliseconds
    - ✓ Fast Base Station Switching (FBSS) - optional
    - ✓ Macro Diversity Handover (MDHO) – optional

**Lecture 44**

**4G Issues**

**Outline**

- 4G Overview
- Heterogeneous Wireless networks
- Evolution, Issues in 4G
- Mobility Management
- Handoffs
- Types, VHO process, VHO Issues
- Standards
- QoS Considerations

**Last Lecture**

- Reference Model
- Burst profiles
- Convergence sublayers
- MAC PDU format, Transmission
- Fragmentation / Packing
- Request/Grant Scheme
- Classes of Uplink service
- Power management/Handoff

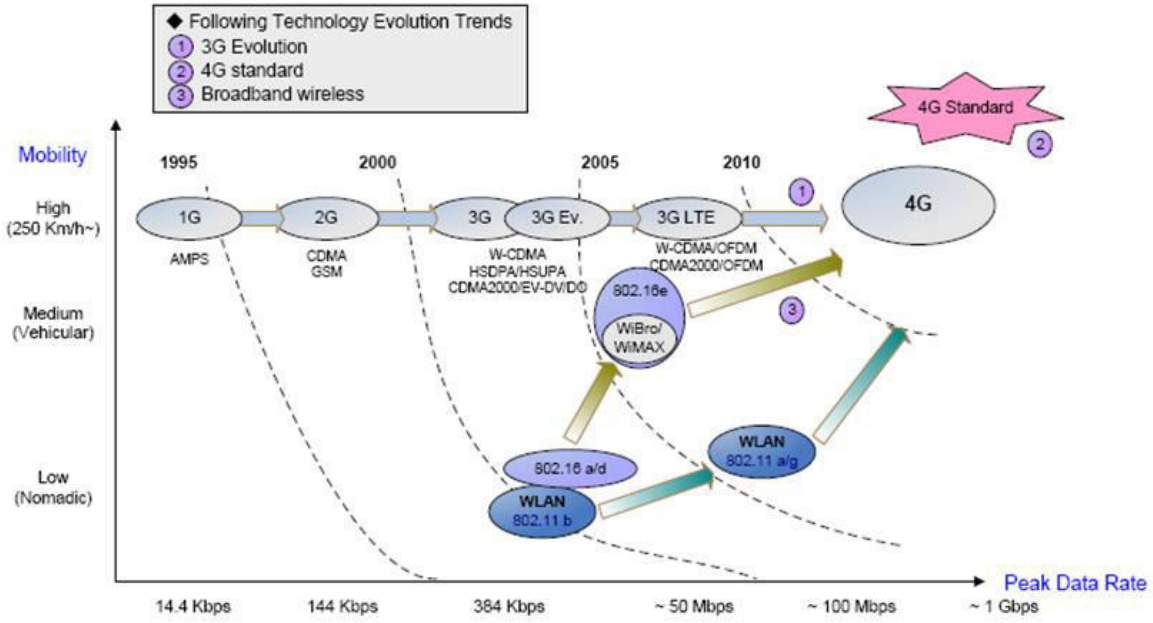
**4G Overview**

- 4G mobile communication systems tend to mean different things to different people:
  - ✓ For some it is merely a higher-capacity new radio interface,
  - ✓ While for others it is an inter-working of cellular and wireless LAN technologies that employs a variant of the Mobile IPv6 mobility management protocol for inter-system handoff.
- There is no doubt that 4G systems will provide higher data rates. Traffic demand estimates suggest that, to accommodate the foreseen amount of traffic in the 2010 – 2020 timeframe in an economically viable way, 4G mobile systems must achieve a manifold capacity increase compared to their predecessors.
- researchers and vendors are expressing a growing interest in 4G wireless networks that support global roaming across multiple wireless and mobile networks
- a system that enables an “Always Best Connected” – or “ABC”
- There are many wireless network technologies Cellular networks, Wireless LANs, Wireless PANs, mobile Wimax, etc.
- 4G networks will play a key role for integrating various network architectures and technologies and achieving a seamless wireless access infrastructure
- 4G provides high-speed, large volume, good quality, and global coverage to roam between different types of technologies
- It is widely accepted that the individual (wireless and/or wireline) access networks will interface to core and/or backbone network elements over the IP protocol
- these wireless access networks are expected to have the following in common:
  - ✓ A dynamic address assignment mechanism (e.g., DHCP, SLP, IPv6) that is capable of associating a short-lived or long-lived IP address to the respective wireless interface at the mobile terminal (e.g., Mobile IP COA association)
  - ✓ A transparent IP forwarding service that is accessible over the logical termination of the IP layer at the mobile terminal and one or more gateways

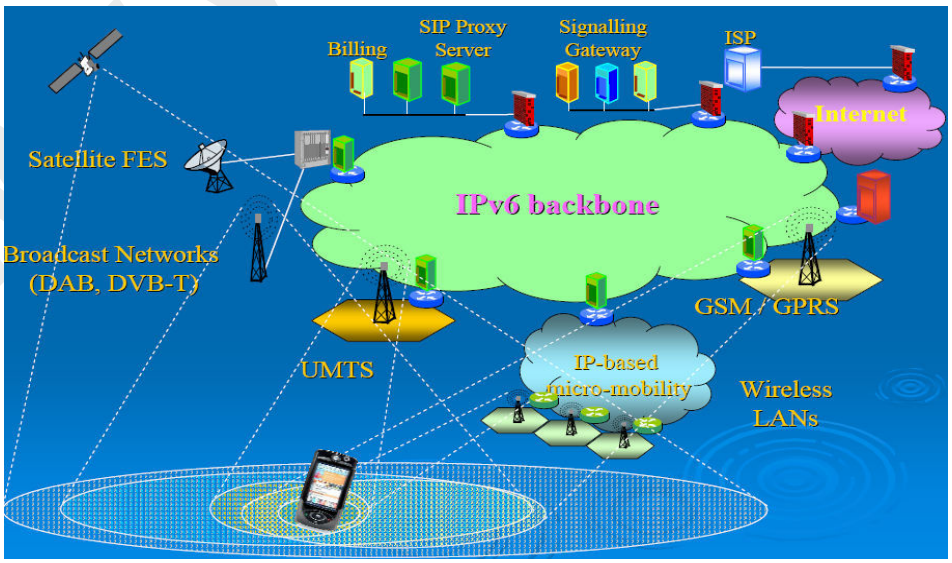
**Heterogeneous Wireless Networks**

- A mixture of co-existing radio access technologies.
- Different access technologies (radio interfaces) and overlapping coverage.
- Different network architectures and protocols for transport, routing and mobility management.
- Different service demands from mobile users (low-data rate, high-data rate, voice, multimedia, etc)
- Different operators in the market.

**Evolution of 4G**




**Heterogeneous Networks**



**Issues in 4G**

- Need to resolve issues as
  - ✓ Access
  - ✓ Handoff
  - ✓ Location coordination
  - ✓ Resource coordination to add new users
  - ✓ Support for multicasting
  - ✓ Support for quality of service
  - ✓ Wireless security and authentication
  - ✓ Network failure and backup
  - ✓ Pricing and billing.

**Mobility Management**

- Location Management: enables system to track location of mobile terminal (MT)
  - ✓ Location updates and paging
- Handoff Management: the process by which an MT keeps its connection when it moves from one point of attachment (base station or access point) to another

**Handoff Management**

- Low signalling and processing overhead.
- Minimum packet loss and delay (seamless HO).
- Guaranteeing QoS during the process and transfer of context.
- Use of any "triggers" or metrics available to decide when and where.
- Efficient use of network and MT resources.
- Enhanced scalability, reliability and robustness.
- Allow inter-technology handoff (VHO).

**Handoff Types**

- Homogeneous (Horizontal) Handovers
  - ✓ Within Single Network (Localized Mobility)
  - ✓ Limited opportunities
  - ✓ Mainly use received signal strength (RSS) to decide handoff
- Heterogeneous (Vertical) Handovers
  - ✓ Across Different Networks (Global Mobility)
  - ✓ More Opportunistic
  - ✓ Handoff metric: RSS, offered bandwidth, price, power consumption, speed,

**Vertical handoff process**

- Step 1: "System Discovery"
- Step 2: "Handoff Decision"
- Step 3: "Handoff Execution"

**Step 1: "System Discovery"**

- MT must know which
  - ✓ Wireless networks are reachable.
  - ✓ Periodic beacons from AP.
  - ✓ Signal measurements.
  - ✓ Handoff metrics (network information) gathering: Bandwidth, cost, delay, SNR, power, etc.
  - ✓ Periodic network scanning.
  - ✓ All interfaces always on.

**Step 2: "Handoff Decision"**

- MT then evaluates the
  - ✓ Some example policies:
    - "Always use the cheapest network".
    - "Always use the interface with lower power consumption".
    - "Always use the WLAN".
    - "Always use the network with more bandwidth".
  - ✓ Decision may be based on utility / cost functions.

**Step 3: "Handoff Execution"**

- If MT decides to perform a VHO, it executes the VHO procedure required to be associated with the new wireless network.

**VHO Issues**

- When to switch?
  - ✓ VHO policies
  - ✓ WLAN to Cellular ≠ Cellular to WLAN
- Seamless handoff
  - ✓ Packet loss and VHO latency.
- Load balancing between networks.
- QoS guarantees
- Security and Authentication.
- Billing
- Implementation.

**Standardization Efforts**

- IETF
  - ✓ Mobility for IPv4 (MIPv4)
  - ✓ Mobility for IPv6 (MIPv6)
  - ✓ Mobility for IP: Performance, Signalling and Handoff Optimization (MIPSHOP)
- IEEE 802.21 Media Independent Handover Group is working toward the seamless handoffs between IEEE 802.XX family and 3G Cellular
- 3GPP and 3GPP2 are working in inter-working with WLAN as an extension of their radio access networks.
  - ✓ Loosely Coupled Architecture
  - ✓ Tightly Coupled Architecture

- Tightly coupling
  - ✓ Provides common charging and billing service
  - ✓ Provides mobility support using traditional 3G technology
  - ✓ Reuses 3G service (e.g., SMS, MMS, etc.)
  - ✓ Causes large traffic load in 3G core network
- Loosely coupling
  - ✓ Provides simple integration approach
  - ✓ Needs minimal requirement on the access network
  - ✓ Provides independent network management

**QoS**

- Supporting QoS in 4G networks will be a major challenge due to varying bit rates, channel characteristics, bandwidth allocation, fault-tolerance levels, and handoff support among heterogeneous wireless networks.
- QoS support can occur at the
  - ✓ Packet,
  - ✓ Transaction
  - ✓ Circuit
  - ✓ User
- Packet-level QoS
  - ✓ Applies to jitter, throughput, and error rate.
  - ✓ Network resources such as buffer space and access protocol are likely influences.
- Transaction-level QoS
  - ✓ Describes both the time it takes to complete a transaction and the packet loss rate.
  - ✓ Certain transactions may be time sensitive, while others cannot tolerate any packet loss.
- Circuit-level QoS
  - ✓ Includes call blocking for new as well as existing calls.
  - ✓ It depends primarily on a network's ability to establish and maintain the end-to-end circuit.
- User-level QoS
  - ✓ Depends on user mobility and application type.
  - ✓ The new location may not support the minimum QoS needed, even with adaptive applications.

**End-to-End QoS**

- Developers need to do much more work to address end-to-end QoS.
  - ✓ They may need to modify many existing QoS schemes, including admission control, dynamic resource reservation, and QoS renegotiation to support 4G users' diverse QoS requirements.
- A wireless network could make its current QoS information available to all other wireless networks in either a distributed or centralized fashion so they can effectively use the available

network resources.

- Additionally, deploying a global QoS scheme may support the diverse requirements of users with different mobility patterns.

**QoS Parameters**

- 802.11e
  - ✓ Nominal MSDU size
  - ✓ Min/mean/max data rate
  - ✓ Mean/max service interval
  - ✓ Traffic type (isochronous, asynchronous)
  - ✓ Burst size
- UMTS (Release 5)
  - ✓ Traffic class (conversational, streaming, interactive, or background)
  - ✓ Guaranteed, maximum bit rate
  - ✓ Maximum SDU size
  - ✓ SDU/bit error ratio
  - ✓ Transfer delay
- 802.16-2004
  - ✓ Traffic priority
  - ✓ Maximum sustained traffic rate
  - ✓ Maximum traffic burst
  - ✓ Minimum reserved traffic rate
  - ✓ Scheduling type (best-effort, non-real time polling, real-time polling, unsolicited grant)
  - ✓ Tolerated jitter, maximum latency

**Lecture 45**

**Review of Lectures 26-44**

**Last Lecture**

- 4G Overview
  - ✓ Heterogeneous Wireless networks
  - ✓ Evolution
  - ✓ Issues in 4G
- Mobility Management
- Handoffs
  - ✓ Types, VHO process, VHO Issues
  - ✓ Standards
- QoS Considerations

**26 – Outlines**

- Overview of IEEE 802.11
- IEEE 802.11 Protocols
- Architecture
- Services
- MAC Protocols
  - ✓ DCF
  - ✓ PCF

Overview, IEEE 802.11 Committee

- Committee formed in 1990
  - ✓ Wide attendance
- Multiple Physical Layers
  - ✓ Frequency Hopping Spread Spectrum
  - ✓ Direct Sequence Spread Spectrum
  - ✓ Infrared
- 2.4GHz Industrial, Scientific & Medical shared unlicensed band
  - ✓ 2.4 to 2.4835GHz with FCC transmitted power limits
- 2Mb/s & 1Mb/s data transfer

**27 - Outlines**

- Problems with DCF
- Virtual Carrier Sensing
- RTC/CTS Protocol
- Inter-frame Spacing, PCF
- Fragmentation / Reassembly
- MAC Frame Format
- Frame Types
- Physical Media in Original IEEE 802.11

**28 – Outlines**

- Introduction
  - ✓ What is Ad hoc networks?
  - ✓ Characteristic
  - ✓ Ad hoc vs. cellular networks
  - ✓ Application
  - ✓ Challenges

- Routing Protocol
  - ✓ Expected Properties of Ad-hoc Routing Protocols
  - ✓ A taxonomy for routing protocols in Mobile ad
  - ✓ Some common protocols (DSDV, AODV, DSR, ZRP, TORA)

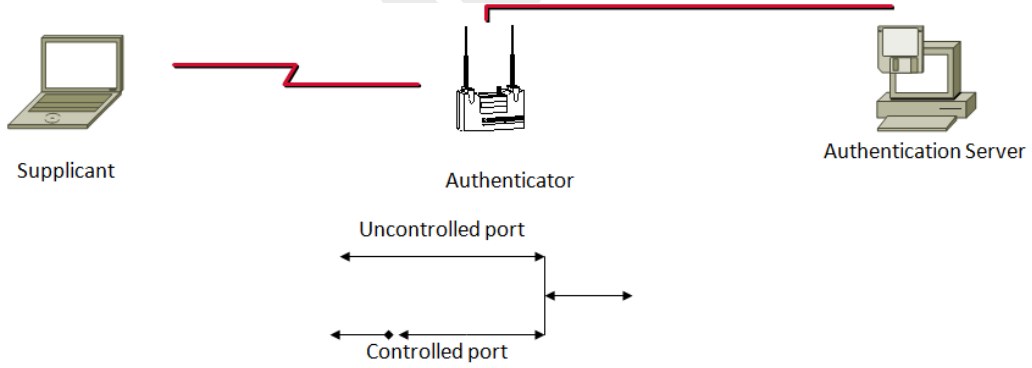
**29 - Outlines**

- Types of Attack
- Goals of 802.11 Security
- WEP Protocol
- WEP Authentication
- Security flaws in original 802.11

How 802.1x Address Security Issues of 802.11

- EAP Framework
- User Identification & Strong authentication
- Dynamic key derivation
- Mutual authentication
- Per-packet authentication
- Dictionary attack precautions

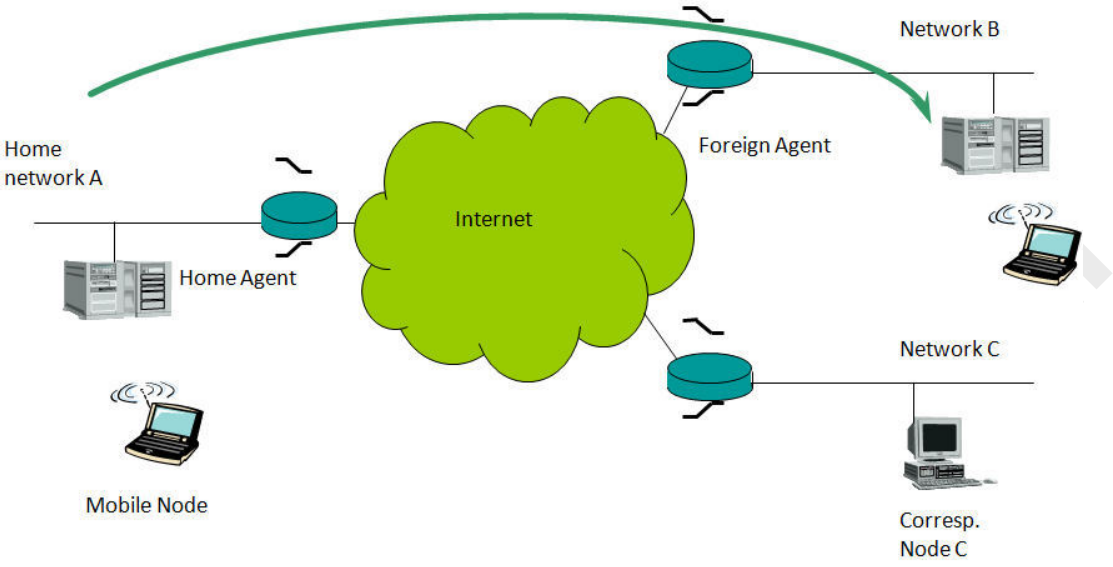
IEEE 802.1X Terminology




**30 - Outlines**

- Limitations of QoS in IEEE 802.11
- Overview of 802.11e
- EDCF
- HCF
- QoS is realized by introducing traffic categories (TCs)
- Each instance is parameterized with TC specific parameters
  - ✓ AIFS, CWmin, CWmax, Persistence factor (PF)

Example




slide by Konidala M. Divyan [3]

**31 - Outlines**

- Introduction to WMN
- Characteristics
- WMN vs MANET
  - ✓ Backbone, dedicated routing, mobility, multiple radios
- Architecture
- Applications
- Critical factors influencing performance
  - ✓ Radio techniques
  - ✓ Scalability
  - ✓ QoS
  - ✓ Security
  - ✓ Ease of Use
  - ✓ Mesh connectivity

**32 – Outlines**

- MAC Layer
  - ✓ Scalability
  - ✓ Multi-Channel
  - ✓ Some Ideas
  - ✓ Research Issues
- Network Layer
  - ✓ Routing
  - ✓ Wish List
  - ✓ Route Optimization Criteria
  - ✓ Routing fairness
  - ✓ Routing – Cross-layer design
- QoS Support at each layer
- WMN Standards

**33 – Outlines**

- TCP Variants
  - ✓ Slow start
  - ✓ Fast Retransmit/Recovery (TCP Reno)
- Issues in Heterogeneous Wireless Networks
- TCP Schemes for Wireless
  - ✓ Pure Link-level Approaches
  - ✓ Soft-state Transport Layer Caching Approaches
  - ✓ Soft-state Cross Layer Signalling Approaches
  - ✓ Hard-state Transport Layer Approaches

**34 - Outline**

- Introduction to WSN
- Applications of WSN
- Factors Influencing Performance of WSN
  - ✓ Power consumption
  - ✓ Fault tolerance
  - ✓ Scalability
  - ✓ Topology
- Architecture and Communication Protocols
- Challenges in WSNs.

**35 - Outlines**

- Attributes of MAC Protocol
- Energy Efficiency in MAC
- Proposed Routing Protocol
  - ✓ S-MAC
  - ✓ T-MAC
  - ✓ DS-MAC
  - ✓ Traffic Adaptive MAC
  - ✓ DMAC
  - ✓ Contention-Free MAC

**36 – Outlines**

- Routing Challenges and Design Issues
  - ✓ Deployment
  - ✓ Routing method
  - ✓ Heterogeneity
  - ✓ Fault tolerance
  - ✓ Power
  - ✓ Mobility etc
- Routing Protocols
  - ✓ SPIN
  - ✓ Directed Diffusion
  - ✓ ACQUIRE
  - ✓ LEACH
  - ✓ TEEN/APTEEN
  - ✓ GAF
  - ✓ GEAR
  - ✓ SPEED

**37 - Outlines**

- Transport Protocols for WSN
- TCP/UDP for WSN

- Protocols
  - ✓ PSFQ
  - ✓ ESRT
  - ✓ CODA
- Security Threats in WSN
- TinySec
- Motivations of Link Layer security
- TinySec Design goals

**38 – Outlines**

- Security primitives in TinySec
- Encryption Schemes
- Keying mechanism
- WMSN
  - ✓ Architecture
  - ✓ Applications
  - ✓ Advantages
  - ✓ Design Considerations
  - ✓ Protocols
- WSAN
  - ✓ Motivation
  - ✓ WSN vs WSAN
  - ✓ Architecture

**39 – Outlines**

- Bluetooth introduction
- Technical features
- Access technique
- Bluetooth topology/scenario
- Specifications
- Core Protocols
- Link connections

**40 – Outlines**

- IP Over Bluetooth
- Bluetooth Security
- WPAN Standards
- IEEE 802.15.3 Overview
- 802.15.3
  - ✓ Topology
  - ✓ Coordination

- Starting a Piconet
- Handing over control of piconet
- Creating child piconet

✓ Medium Access (Super-frame)
✓ Channel Time Management
✓ Power management
✓ MAC Frame format

**41 - Outlines**

- IEEE 802.15.4
  - ✓ Basics, Type of Devices
  - ✓ Phy Layer
  - ✓ Channel Access Mechanisms
    - Slotted/Unslotted CSMA/CA
  - ✓ Super-frame Structure

**42 – Outlines**

- WiMAX Basics
- 802.16 Evolution

**43 – Outlines**

- Reference Model
- Burst profiles
- Classes of Uplink service

**44 - Outline**

- 4G Overview
- Mobility Management
- Handof