EC 1451- MOBILE AND WIRELESS COMMUNICATION

K.JAYAMANI
A.P/ECE

UNIT – I

PRINCIPLE OF WIRELESS COMMUNICATION

PART –A (2 MARKS)

1. What is digital modulation?

A method of decoding information for transmission. Information, or in this case, a voice conversation is turned into a series of digital bits; the 0s and 1s of computer binary language. At the receiving end, the information is reconverted

2. what is FSK, PSK, QAM?

The most fundamental digital modulation techniques are based on keying:
In the case of PSK (phase-shift keying), a finite number of phases are used.
In the case of FSK (frequency-shift keying), a finite number of frequencies are used.
In the case of ASK (amplitude-shift keying), a finite number of amplitudes are used.
In the case of QAM (quadrature amplitude modulation), a finite number of at least two phases, and at least two amplitudes are used.

3. DEFINE SPREAD SPECTRUM TECHNIQES

IN SPREAD SPECTRUM, THE SIGNAL OCCUPIES A BANDWIDTH IN EXCESS OF THE MINIMUM NECESSARY TO SEND THE INFORMATION THE BAND SPREAD IS ACCOMPLISHED BY MEANS OF A CODE THAT IS INDEPENDENT OF THE DATA, AND A SYNCHRONIZED RECEPTION WITH THE CODE AT THE RECEIVER IS USED FOR DESPREADING AND SUBSEQUENT

4. Define FDMA?

Frequency Division Multiple Access", is the division of the frequency band allocated for wireless cellular telephone communication into many channels, each of which can carry a voice conversation or, with digital service, carry digital data. FDMA is a basic technology in the analog Advanced Mobile Phone Service (AMPS), the most widely-installed cellular phone system installed in North America. With FDMA, each channel can be assigned to only one user at a time. FDMA is also used in the Total Access Communication System (TACS).

5. Define TDMA

Time division multiple access (TDMA) is a channel access method for shared medium (usually radio) networks. It allows several users to share the same frequency channel by dividing the signal into different timeslots. The users transmit in rapid succession, one after the other, each using his own timeslot. This allows multiple stations to share the same transmission medium (e.g. radio frequency channel) while using only the part of its bandwidth they requir

6. What are the channels used in mobile communication systems?

1. Forward voice channels (FVC)
2. Reverse voice channels (RVC)
3. Forward control channels (FCC)
4. Reverse Control channels (RCC)

7. What are the basic units of a Cellular system?

- Mobile stations
- Base stations
- Mobile Switching Center (MSC) or Mobile Telephone Switching Office (MTSO).

8. What are the classifications of Wireless technologies and systems?

- Cellular mobile radio systems
- Cordless telephones
- Wide-area wireless data systems
- High-speed WLANs
- Paging/messaging systems
- Satellite-based mobile systems

9. what is meant by handover technique

In a cellular radio system having a two layer cell structure comprised by macrocells (1) overlaying microcells (2), handover occurs only via the macrocell layer. Thus when the quality of a call handled by a microcell (2) deteriorates below predetermined criteria the call is handed up rapidly to the umbrella macrocell and is only handed back down to a microcell when the handset has been in that microcell for a predetermined time and the quality of the link thereto exceeds predefined criteria

10. **What are the different types of Hand over?**

- Intra-satellite hand over
- Inter-satellite hand over
- Gateway hand over
- Inter-system hand over

1**1. Define modulation.**
It is the process of encoding information from a message source in a manner suitable for transmission.

12. State the different analog modulation schemes.
Amplitude and frequency modulation.

13. State the different modulation schemes.
Amplitude shift keying, frequency shift keying, phase shift keying.

14. Define amplitude modulation.
The amplitude of the high frequency carried is varied in accordance to the instantaneous amplitude of the message signal.

15. State the techniques used for SSB generation.
Filter method and balanced modulator method.

16. State the advantages of digital modulation schemes.
Power efficiency and bandwidth efficiency.

17. Define bandwidth efficiency.
It describes the ability of the modulation scheme to accommodate data within a limited bandwidth.

18. Define Power efficiency.
It describes the ability of the modulation scheme to preserve the fidelity of the digital message at low power levels.

19. State the different types of line coding.
Return to zero, non-return to zero and Manchester.

20. State the types of modulation schemes used in mobile communication.
GMSK, GFSK and DQPSK.

21. Give the equation used to represent a BPSK signal.

$$S_{BPSK}(t) = m(t) \quad 2\sqrt{\frac{E_b}{T_b}} \cos(2\pi f_c t + \theta_c)$$

22. What is coherent detector?
If the receiver has prior knowledge of the transmitted signal then the receiver is known as coherent detector.

23. State the advantage of using GMSK rather than MSK.
The bandwidth occupied by GMSK modulated signal is less in comparison to MSK modulated signal.

24. What is CPFSK ?
Continuous phase frequency shift keying. It is another name for MSK.

25. What is QAM ?

Quadrature amplitude modulation.

26. State the difference between MSK and GMSK.

GMSK uses a Gaussian pulse shaping filter prior to MSK.

27. What is a diversity receiver?

Diversity receiver is the diversity scheme applied at the receiver end of the antenna in all effective technique for reducing interference, where selective combiner is used to combine two-correlated signal.

28. Expand PCS, PLMR, NLOS and DECT.

PCS - Personal Communication Systems.
PLMR – Public Land Mobile Radio
NLOS – Non Line Of Sight
DECT – Digital Equipment Cordless Telephone

29. Mention the three partially separable effects of radio propagation.

The three partially separable effects of radio propagation are,

- Multi path fading
- Shadowing
- Path loss

30. What is known as Quadrature Modulation?

In digital modulations, instead of transmitting one bit at a time, we transmit two or more bits simultaneously. This is known as M-ary transmission. This type of transmission results reduced channel BW. However sometimes the use two quadrature carriers for modulation. This process of transmitting 2 quadrature carrier for modulation is known as quadrature modulation.

31. What are the design characteristics of digital modulation scheme?

- Maximum data rate,
- Minimum transmitted power,
- Maximum channel BW,
- Maximum resistance to interfering signals,
- Minimum circuit complexity.

32. What are coherent digital modulation techniques?

Coherent digital modulation techniques are those techniques which employ coherent detection. In coherent detection, the local carrier generated at the receiver is phase locked with the carrier at the transmitter. Thus, the detection is done by correlating received noisy signal and locally generated carrier. The coherent detections a synchronous detection.

33. What are the non-coherent digital modulation techniques?

Non-coherent digital modulation techniques are those techniques in which the detection process does not need receiver carrier to be phase locked with transmitter carrier. The advantage of such type of system is that the system becomes simple. But the drawback of such a system is that the error probability increases.

34. Give some advantage of QPSK:

- For the same bit error rate, the BKJ required by QPSK is reduced to half as compared to BPSK.
- Because of reduced BW, the information transmission rate of QPSK is higher
- Carrier power almost remains constant.

35. Drawbacks of MSK as compared to QPSK:

1. The BW requirement of MSK is 1.5 fb, whereas it is fb in QPSK. Actually this cannot be said series drawback of MSK. Because power to BW ratio of MSK is more 99% of signal.
2. Power can be transmitted within the BW of 1.2 fb in MSK. While QPSK needs around 8fb to transmit the same power.

36. Bring out the difference between coherent and noncoherent binary modulation schemes

Coherent binary modulation	Non-coherent binary modulation
1. Here the local carrier generated at the receiver is phase locked with the carrier at the transmitter. Thus detection is done by correlating received noisy signal and locally generated carrier. 2. The coherent detection is a synchronous detection. Here the error probability does not decreases	1. Here the detection process does not need receiver carrier to be phase locked with transmitter carrier. 2. Here error probability increases.

37. What is the error probability of MSK and DPSK?

The error probability of MSK is given by $Pe = \frac{1}{2} erfc\left(\sqrt{\frac{Eb}{No}}\right)$

The error probability of DPSK is given by $Pe = \frac{1}{2}\exp\left(-\frac{Eb}{No}\right)$

38. In minimum shift keying what is the relation between the signal frequencies and bit rate?

The bit rate is given by

$$Pe = \frac{1}{2} erfc\left(\sqrt{\frac{Eb}{No}}\right)$$

Where

E_b >>>>> Transmitted signal energy per bit;

No >>>>> Noise density

39. What is maximum likelihood decoder?

Set $f_x(x/mk)$ is always non-negative and since the logarithmic function is a monotonically increasing function of its argument we may restate the decision rule in terms of metric as follows

Set $\hat{m} = mi$, if $\ln[f_x(X/mk)]$ is maximum for k = i

Where 'ln' denotes the a natural log. This decision rate is referred to as maximum likelihood rule and device for its implementation is referred to as maximum likelihood decoder.

40. What is DPSK?

Differential phase –shift keying is the non-coherent version of PSK. It is differentially coherent modulation method. It does not need a synchronous carrier at the demodulator. The input sequence of binary bits is modified such that the next bit depends upon the previous bit. Therefore in the receiver bits are used ot detect the present bit.

41. What are the advantages of DPSK?

- DPSK does not need carrier at its receiver. This means that the complicated circuitry for generation of local carrier is avoided.
- The bandwidth requirement of DPSK is reduced compared to that of BPSK

42. What is capture effect?

The capture-effect is a direct result of the rapid nonlinear improvement in received quality for an increase in the received power. If two signals in the same frequency band are available at an FM receiver, the one appearing at the higher received signal level is accepted and demodulated, while the weaker one is rejected. This inherent ability to pick-up the strongest signal and reject the rest makes FM systems very resistant to co-channel interference and provides excellent subjective received quality. This effect is called as capture-effect.

PART-B (16 MARKS)

1. Describe in detail about the Analog Amplitude Modulation techniques used in mobile radio.

Modulation is the process of encoding information from a message source in a manner suitable for transmission. Modulation may be done by varying the amplitude, phase or frequency of a high carrier in accordance with the amplitude of the message signal.

Types of Modulation

1. Analog modulation
   - Amplitude modulation
   - Angle modulation (PM, FM)

2. Digital modulation
   - Linear modulation
   - Non-linear modulation

Amplitude Modulation

The amplitude of a high frequency carrier signal is varied in accordance to the instantaneous amplitude of the modulating message signal.

If $A_c\cos(2\pi f_c t)$ is the carrier signal and m(t) is the modulating signal, the AM signal can be represented as

$$s_{AM}(t) = A_c [1+ m(t)] \cos(2\pi f_c t) \quad \text{.....(1)}$$

Where,

$$m(t) = (A_m / A_c) \cos(2\pi f_m t)$$

The modulation index *k* of an AM signal is defined as the ratio of the peak message signal amplitude to the speak carrier amplitude.

$$k = \frac{A_m}{A_c}$$

Equation (1) may be expressed as

$$s_{AM}(t) = \mathrm{Re}\{g(t)\exp(j2\pi f_c t)\}$$

where g(t) is the complex envelope of the AM signal is given by

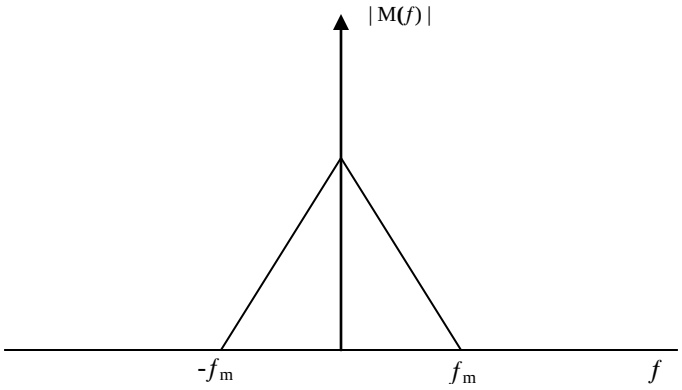
$$g(t) = A_c [1+ m(t)]$$

The spectrum of an AM signal is

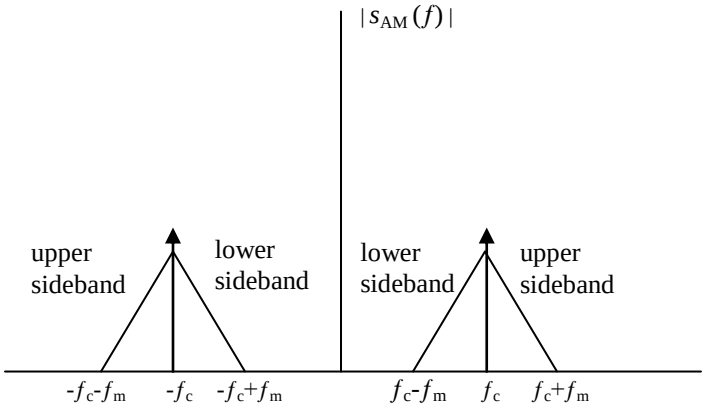
$$s_{AM}(f) = \tfrac{1}{2} A_c [\delta(f-f_c) + M(f-f_c) + \delta(f+f_c) + M(f+f_c)]$$

where $\delta(\cdot) \rightarrow$ unit impulse function

$M(f) \rightarrow$ message signal spectrum



Spectrum of a message signal



Spectrum of the corresponding AM signal

The AM spectrum consists of an impulse at the carrier frequency, and two sidebands which replicate the message spectrum. The sidebands above and below the carrier frequency are called the upper and lower sidebands.

The RF bandwidth of an AM signal is

$$\boldsymbol{B}_{AM} = 2f_m$$

where

$f_m \rightarrow$ maximum frequency of modulating message signal

The total power in an AM signal is

$$\boldsymbol{P}_{AM} = \tfrac{1}{2} A_c^2 [1 + 2\langle m(t)\rangle + \langle m^2(t)\rangle] \quad \ldots\ldots\ldots\ldots (2)$$

Where,

$\langle \bullet \rangle \rightarrow$ average value

If the modulating signal is $m(t) = k \cos(2\pi f_m t)$ eqn (2) is expressed as

$$\boldsymbol{P}_{AM} = \tfrac{1}{2} A_c^2 [1 + \boldsymbol{P}_m] = \boldsymbol{P}_c [1 + k^2/2]$$

Where $\boldsymbol{P}_c = A_c^2/2 \rightarrow$ carrier signal power

$\boldsymbol{P}_m = \langle m^2(t)\rangle \rightarrow$ modulating signal power

$k \rightarrow$ modulation index

Single Sideband AM

SSB-AM systems transmit only one of the sidebands (either upper or lower) about the carrier, and hence occupy only half the bandwidth of conventional AM systems.

An SSB signal can be expressed as

$$S_{SSB}(t) = A_c [m(t)\cos(2\pi f_c t) \pm \hat{m}(t) \sin(2\pi f_c t)] \quad \text{.....(3)}$$

Where

(-) → upper sideband SSB

(+) → lower sideband SSB

$\hat{m}(t) \rightarrow$ Hilbert transform of m(t)

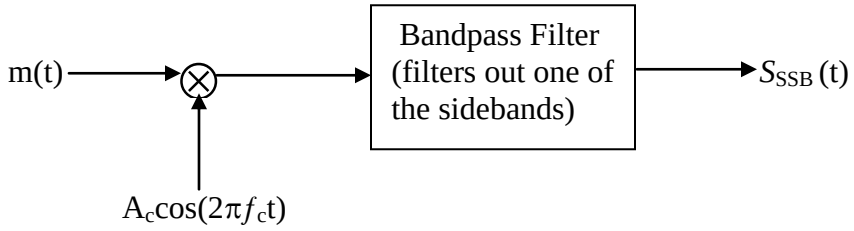
$$\hat{m}(t) = m(t) \otimes h_{HT}(t) = m(t) \otimes \frac{1}{\pi t}$$

$H_{HT}(f) \rightarrow$ Fourier transform of $h_{HT}(t)$, corresponds to a –90° phase shift network

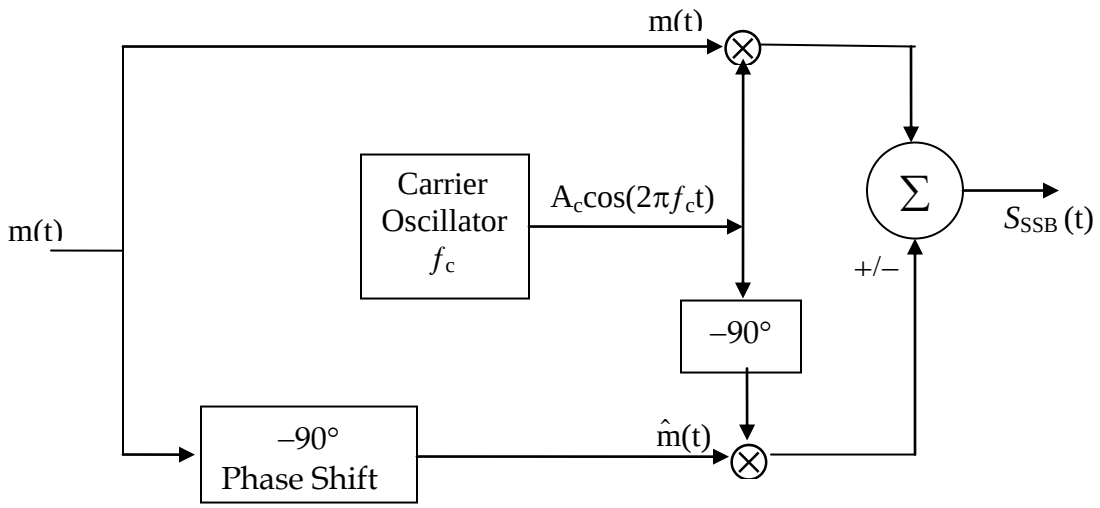
$$H(f) = \begin{cases} -j & f > 0 \\ j & f < 0 \end{cases}$$

The two common techniques used for generating an SSB signal are the filter method and the balanced modulator method.

In the **filter method**, SSB signals are generated by passing a double sideband AM signal through a bandpass filter which removes one of the sidebands. Excellent sideband suppression can be obtained using crystal filters at an Intermediate frequency (IF).



In **balanced modulator** the modulating signal is split into two identical signals, one which modulates the in-phase carrier and the other which is passed through a –90° phase shifter before modulating a quadrature carrier. The sign used for the quadrature component determines whether USSB or LSSB is transmitted.



Pilot Tone SSB

SSB systems have the advantage of being very bandwidth efficient, their performance in fading channels is very poor. In conventional SSB receivers, it is difficult to electronically tune the local oscillator frequency to the identical frequency of the incoming carrier. Doppler spreading and Rayleigh fading can shift the signal spectrum causing pitch and amplitude variations in the received signal. These problems may be overcome by transmitting a low level pilot tone along with the SSB signal. A phase locked loop at the receiver can detect this pilot tone and use it to lock the frequency and amplitude of the local oscillator. If the pilot tone and the information bearing signal undergo correlated fading, it is possible at the receiver to counteract the effects of fading through signal processing based on tracking the pilot tone. This process is called *feed forward signal regeneration* (FFSR). By tracking the pilot tone, the phase and amplitude of the transmitted signal can be reestablished. Keeping the phase and amplitude of the received pilot tone as a reference, the phase and amplitude distortions in the received sidebands caused by Rayleigh fading can be corrected.

Three different types of pilot tone SSB systems are [Gos 78], [Lus 78] and [Wel78]. Three systems transmit a low level pilot tone, -7.5 dB, to -15 dB below the peak envelope power of the single sideband signal. They essentially differ in the spectral positioning of the low level pilot tone. One system transmits a low level carrier along with the sideband signal (tone-in-band), while the other two place a pilot tone above or within the SSB band.

In *tone-in-band* SSB system a small portion of the audio spectrum is removed from the central region of the audio band using a notch filter, and a low level pilot tone is inserted in its place. This has the advantage of maintaining the low bandwidth property pf the SSB signal, and also provides good adjacent channel protection. For proper operation of tone-in-band SSB, the tone must be transparent to data and be spaced across the band to avoid spectral overlap with audio frequencies called ***Transparent Tone-in-band*** **(TTIB).**

Demodulation of AM Signals

Demodulation is the process of extracting the baseband message signal from the carrier so that it may be processed and interpreted by the intended receiver (sink).

Types of Demodulation

- Coherent demodulation
- non coherent demodulation

Coherent demodulation requires knowledge of the transmitted carrier frequency and phase at the receiver, whereas non coherent detection requires no phase information. In practical AM receivers, the received signal is filtered and amplified at the carrier frequency and then converted to an intermediate frequency (IF) using a super heterodyne receiver.

Product detector

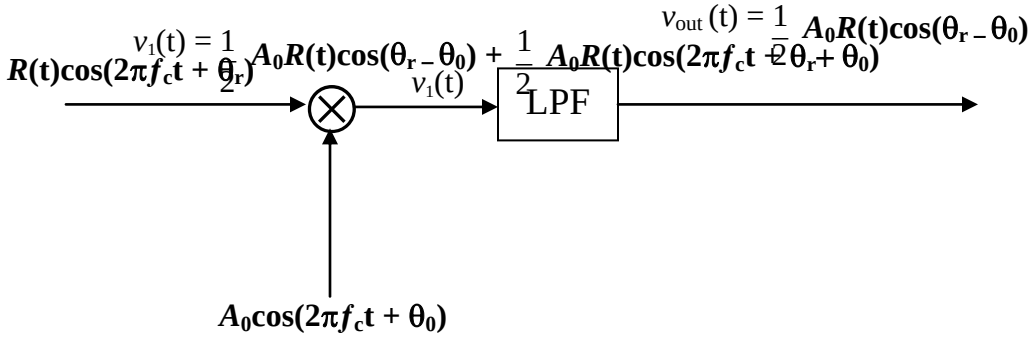
A product detector (or phase detector) is a down converter circuit which converts the input bandpass signal to a baseband signal. If the input to the product detector is an AM signal of the form $R(t)\cos(2\pi f_c t + \theta_r)$, the multiplier output is

$$v_1(t) = R(t)\cos(2\pi f_c t + \theta_r)A_0\cos(2\pi f_c t + \theta_0) \quad \text{.....(4)}$$

where

f_c → oscillator carrier frequency
θ_r → receiver signal phase
θ_0 → oscillator signal phase

Using trigonometric identities in eqn (4)



LPF removes the double carrier frequency, the output is

Where $$v_{out}(t) = \frac{1}{2}A_0R(t)\cos(\theta_r - \theta_0) = KR(t)$$

K → gain constant

Non coherent envelope detectors which are easy and cheap to build. An ideal envelope detector is a circuit that has an output proportional to the real envelope of the input signal.

If the input to the envelope detector is $R(t)\cos(2\pi f_c t + \theta_r)$, the output is

$$v_{out}(t) = K|R(t)|$$

This is useful when the input signal power is atleast 10 dB > noise power.

2. Describe in detail about the Angle Modulation techniques used in mobile radio.

Angle modulation varies a sinusoidal carrier signal in such a way that the angle of the carrier is varied according to the amplitude of the modulating baseband signal.

This is a form of angle modulation in which the instantaneous frequency of the carrier signal is varied linearly with the baseband message signal m(t)

$$S_{FM}(t) = A_c\cos[2\pi f_c t + \theta(t)] = A_c\cos\left[2\pi f_c t + 2\pi k_f \int_{-\infty}^{t} m(\eta)d\eta\right] \quad ..(a)$$

where

A_c → carrier amplitude
f_c → carrier frequency
k_f → frequency deviation constant(**H**z/**V**)

If the modulating signal is a sinusoid of amplitude a A_m and frequency fm

$$S_{FM}(t) = A_c\cos\left[2\pi f_c t + \frac{k_f A_m}{f_m}\sin(2\pi f_m t)\right] \quad ....(b)$$

The frequency modulation index β_f defines the relationship between message amplitude and the bandwidth of the transmitted signal,

$$\beta_f = \frac{k_f A_m}{W} = \frac{\Delta_f}{W} \quad .....(c)$$

where

A_m → modulating signal peak value
Δ_f → Transmitter peak frequency deviation
W → modulating signal maximum bandwidth

Phase Modulation

This is a form of angle modulation in which the angle **θ(t)** of the carrier signal is varied linearly with the baseband message signal m(t)

$$S_{PM}(t) = A_c\cos[2\pi f_c t + k_\theta m(t)]$$

where

k_θ → phase deviation constant(rad/volt)

An FM signal can be generated by first integrating m(t) and then using the result as the input to the phase modulator . Conversely, a PM wave can be generated by first differentiating m(t) and using the result as the input to frequency modulator.

The phase modulation index β_p

$$\beta_p = k_\theta A_m = \Delta\theta$$

where

$\Delta\theta$ → Transmitter peak phase deviation

FM Modulation Methods

There are two methods:

- Direct Method

The carrier frequency is directly varied in accordance with the input modulating signal.

- Indirect Method

A narrow band FM signal is generated using a balance modulator, and frequency multiplication is used to increase both the frequency deviation and the carrier frequency to the required level.

Direct Method:

In this method voltage controlled oscillators (VCOs) are used to vary the frequency of the carrier signal in accordance with the baseband signal amplitude variations. These oscillators use variable reactance device, voltage variable capacitor called a Varactor. This Varactor is obtained by using a reverse biased p-n junction diode. The larger the reverse voltage applied, the smaller will be the transition capacitance of the diode. Incorporating this into a standard Hartley or Colpitts Oscillator, FM signals can be generated. In wideband FM generation, the stability of the center frequency of VCO can be improved by using a PLL.

Indirect Method

Narrowband FM signal is obtained by the sum of a carrier signal and a SSB signal where the sideband is 90° out of phase with the carrier.

Using Taylor series for small values of **θ(t)**, eqn (a) becomes

$$S_{FM}(t) \cong A_c\cos(2\pi f_c t) - A_c\theta(t)\sin(2\pi f_c t)$$

↓ carrier ↓ sideband

A narrowband FM signal is generated using a balanced modulator. The maximum frequency deviation is kept constant and small, to maintain the validity of above eqn, providing a narrowband FM output signal.

A wideband FM signal is then produced using frequency multipliers.

Disadvantage: phase noise in the system increases with the frequency multiplying factor N.

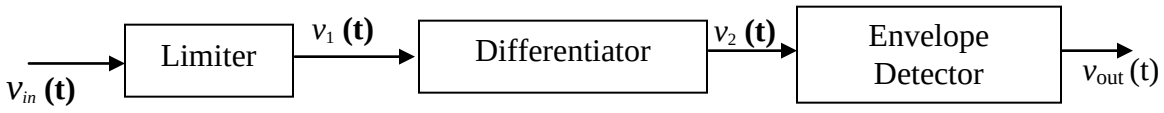
3. Describe in detail about the demodulation techniques for FM waves used in mobile radio.

FM Detection Techniques

A frequency-to-amplitude converted circuit is a frequency demodulator. Various techniques are slope detection, zero-crossing detection, phase locked discrimination, and quadrature detection is used to demodulate FM. Devices which perform FM demodulation are often called frequency discriminators. In practical receivers, the RF signal is received, amplified, and filtered at the carrier, and then converted to an intermediate frequency (IF) which contains the same spectrum as the original received signal.

Slope Detector

The FM signal is passed through an amplitude limiter which removes in amplitude perturbations which the signal might have undergone due to fading in the channel, and produces a constant envelope signal.



Using eqn (a), the signal at the output of limiter is

$$v_1(t) = V_1\cos[2\pi f_c t + \theta(t)] = V_1\cos\left[2\pi f_c t + 2\pi k_f \int_{-\infty}^{t} m(\eta)d\eta\right] \quad ..(A)$$

Eqn (A) can be differentiated by passing the signal through a filter with the transfer function that has gain that increases linearly with frequency. Such a filer is called a slope filter. (Slope detector).The output of differentiator is

$$v_2(t) = -V_1\left[2\pi f_c t + \frac{d\theta}{dt}\right]\sin[2\pi f_c t + \theta(t)]$$

And the envelope detector output is

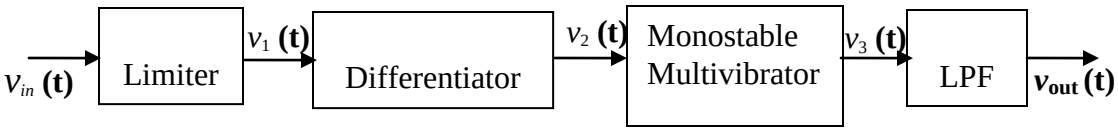
$$v_{out}(t) = V_1\left[2\pi f_c t + \frac{d}{dt}\theta(t)\right]$$

$$= V_1 2\pi f_c t + V_1 2\pi k_f m(t)$$

The output of the envelope detector contains a dc term proportional to the carrier frequency and a time varying term proportional to the original message signal m(t). The dc term can be filtered out using a capacitor to obtain the desired demodulated signal.

Zero-crossing detector (pulse-averaging discriminator)

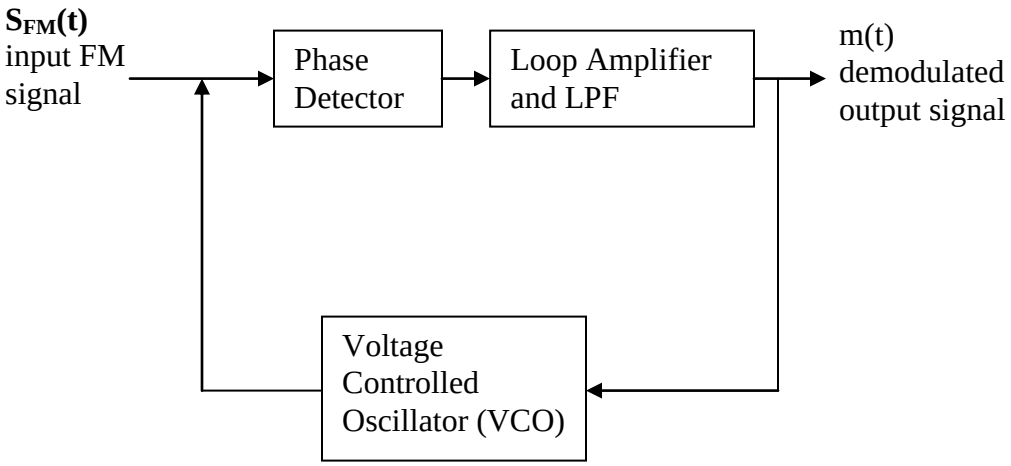
When linearity is required over a broad range of frequencies, such as for data communications, a zero-crossing detector is used to perform frequency-to-amplitude conversion by directly counting the number of zero crossings in the input FM signal.
The rationale behind this technique is to use the output of the zero-crossing detector to generate a pulse train with an average value that is proportional to the frequency of the input signal.



The input FM signal is first passed through a limiter circuit which converts the input signal to a frequency modulated pulse train. This pulse train v_1 **(t)** is then passed through a differentiator whose output triggers a monostable multivibrator (one-shot). The one -shot output consists of a pulse train with average duration proportional to the desired message signal. LPF is used to perform the averaging operation by extracting the slowly varying dc component of the output signal of one –shot. The output of LPF is the desired demodulated signal.

PLL For FM Detection

The PLL is a closed loop control system that can track the variations in the received signal phase and frequency.

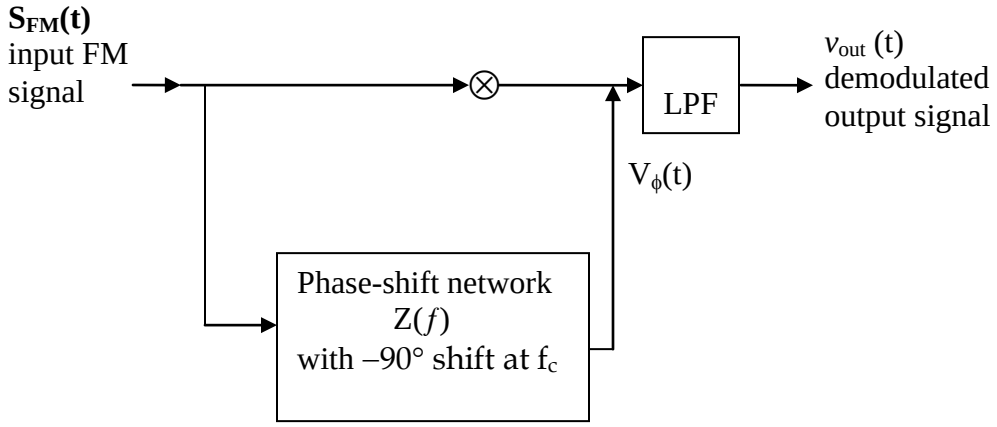


It consists of a VCO *H*(s) with an output frequency varied in accordance with the demodulated output voltage level. The output of the VCO is compared with the input signal using a phase comparator, which produces an output voltage proportion to the phase difference. The phase difference signal is then fed back to the VCO to control the output frequency. The feedback loop functions in the locking of VCO frequency to the input signal. Once the VCO frequency is locked to the input frequency, the VCO continues to track the variations in the input frequency. Once this tracking is achieved, the control voltage to the VCO is the demodulated FM signal.

Quadrature Detection

This technique can be easily implemented on an integrated circuit at a very low cost. The detector consists of a network which shifts the phase of the incoming FM signal by an amount proportional to its instantaneous frequency, and uses a product (phase) detector to deduct the phase difference between the original FM signal and the output signal of phase-

shift network. Since the phase shift introduced by the phase-shift network is proportional to instantaneous frequency of FM signal, the output voltage of phase detector will also be proportional to the input FM signal instantaneous frequency. Thus a frequency-to-amplitude conversion is achieved, and the FM signal is demodulated.



To achieve optimum performance, a very small (< ±5°) phase shift is to be introduced across the modulated signal bandwidth. The phase-shift network should have a constant amplitude response and a linear phase response over the occupied FM signal spectrum. Further, the network should have a nominal 90° phase shift at the carrier frequency.

The phase response function of the phase-shift network is

$$\phi(f) = \frac{-\pi}{2} + 2\pi K(f - f_c)$$

where
K→Proportionality constant

When an FM signal is passed through the phase-shift network, the output is

$v_\Phi(t) = \rho A_c \cos[2\Pi f_c t + 2\Pi k_f \int m(\eta)d\eta + \Phi(f_i(t))\ ]$

The output of the product detector is proportional to the cosine of the phase difference between and $v_\Phi(t)$ and $S_{fm}(t)$.

$v_0(t) = \rho^2 A_c^2 \cos\ (\Phi(f_i(t)))$
$v_0(t) = \rho^2 A_c^2 \cos\ (-\Pi/2 + 2\Pi K[fi(t) - f_c]\ )$
$v_0(t) = \rho^2 A_c^2 \sin(2\Pi K.k_f.\ m(t))$

If the phase shift varies only over a small angle, the above expression becomes as
$v_0(t) = \rho^2 A_c^2 2\Pi K.k_f.\ m(t) = C\ m(t)$.

Hence the quadrature detector output is the desired message signal multiplied by a constant.

4. Describe in detail about the Digital modulation schemes BPSK.

Modern mobile communication systems use digital modulation techniques.

ADVANTAGES

- Greater noise immunity
- Robustness to channel impairments
- Easier multiplexing of various forms of information
- Greater security

Factors That Influence the Choice of Digital Modulation

Several factors influence the choice of a digital modulation scheme. A desirable modulation scheme provides low bit error rates at low received signal-to-noise ratios.
The performance of a modulation scheme is measured in terms of *power efficiency* and *bandwidth efficiency*.

Power (energy) efficiency

This describes the ability of a modulation technique to preserve the fidelity of the digital message at low power levels. In digital communication system, to increase noise immunity, it is necessary to increase the signal power.

It is defined as the ratio of the signal energy per bit to noise power spectral density **(E_b/N_0).** It is denoted as η_p.

Bandwidth efficiency

This describes the ability of a modulation scheme to accommodate data within a limited bandwidth.

It is defined as the ratio of the throughput data rate per Hertz in a given bandwidth.

If R is the data rate in bits per second, and B is the bandwidth occupied by the modulated RF signal, then bandwidth efficiency η_B is expressed as

$$\eta_B = \frac{R}{B} \text{ bps/Hz} \qquad \text{.....1.1}$$

The system capacity of a digital mobile communication system is directly related to the bandwidth efficiency of the modulation scheme, for > η_B transmit more data in a given spectrum allocation.

Shannon's channel coding theorem states that for an arbitrarily small probability of error, the maximum possible bandwidth efficiency is limited by the noise in the channel and the

$$\eta_{Bmax} = \frac{C}{B} = \log_2\left[1 + S/N\right] \qquad \text{.....1.2}$$

channel capacity formula is
Where
C → channel capacity (bps)
B → RF bandwidth
S/N → signal-to-noise ratio

Bandwidth and Power Spectral Density of Digital Signals

The definition of signal bandwidth is based on the power spectral density (PSD) of the signal. The PSD of a random signal *w(t)* is defined as

$$P_w(f) = \lim_{T\to\infty} \frac{\overline{|\mathbf{W_T}(f)|^2}}{\mathbf{T}} \qquad \text{……..1.3}$$

Where the bar denotes ensemble average

$\mathbf{W_T}(f)$ → Fourier transform of $\mathbf{W_T(t)}$ is the truncated version of the signal *w(t)*

$$\mathbf{W_T(t)} = \begin{cases} w(t) & -T/2<t<T/2 \\ 0 & \text{elsewhere} \end{cases}$$

The PSD of a modulated (bandpass) signal is related to the PSD of its baseband complex envelope. If a bandpass signal s(t) is represented as

$$s(t) = \mathrm{Re}\{ g(t)\exp(j2\pi f_c t) \qquad \text{……..1.4}$$

where

g(t) → complex baseband envelope

The PSD of the bandpass signal is

$$\boldsymbol{P}_s(f) = \frac{1}{4}[\mathbf{P_g}(\boldsymbol{f}-\boldsymbol{f_c}) + \mathbf{P_g}(-\boldsymbol{f}-\boldsymbol{f_c})] \qquad \text{……1.5}$$

where

$\mathbf{P_g}(\boldsymbol{f})$ → PSD of g(t)

The *absolute bandwidth* of a signal is defined as the range of frequencies over which the signal has a non-zero power spectral density.

The null-to-null bandwidth is equal to the width of the main spectral lobe.

The dispersion of the spectrum is measured using the *half-power bandwidth (**3 dB** bandwidth)*. It is defined as the interval between frequencies at which the PSD has dropped to half power, or 3 dB below the peak value.

FCC defines that 99% of the signal power is contained within the occupied bandwidth i.e., bandwidth leaves exactly .5% above & below upper & lower band limit.

Linear Modulation Techniques

In linear modulation techniques, the amplitude of the transmitted signal s(t) varies linearly with the modulating signal m(t). Linear modulation techniques are bandwidth efficient and hence are used in wireless communication systems.

The most popular techniques include pulse-shaped **QPSK, OQPSK,** and **BPSK.**

Binary Phase Shift Keying (BPSK)

In BPSK , the phase of a constant amplitude carrier signal is switched between two values according to the two possible signals m_1 and m_2 corresponding to binary 1 and 0. The two phases are separated by 180°. If the sinusoidal carrier has an amplitude A_c , and energy per bit $E_b = ½ A_c^2 T_b$,then the transmitted BPSK signal is either

$$S_{BPSK}(t) = \sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_c t) \qquad 0 \le t \le T_b \ \ (binary\ 1)$$

Or

$$S_{BPSK}(t) = \sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_c t + \pi + \theta_c)$$

$$= -\sqrt{\frac{2Eb}{Tb}}\ \cos(2\pi f_c t + \theta_c) \qquad 0 \le t \le T_b\ (binary\ 1)$$

generalize m1 and m2 as a binary data signal m(t) , the transmitted signal is

$$S_{BPSK}(t) = \mathrm{m(t)}\ \sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_c t + \theta_c)$$

The BPSK signal is equivalent to a double sideband suppressed carrier amplitude modulated waveform. Hence a BPSK signal can be generated using a balance modulator.

Spectrum and Bandwidth of BPSK

The BPSK in complex envelope form as

$$S_{BPSK}(t) = \mathrm{Re}\{g_{BPSK}(t)\exp(j2\pi f_c t\}$$

Where

$g_{BPSK}(t) \rightarrow$ complex envelope of the signal

$$g_{BPSK}(t) = \sqrt{\frac{2E_b}{T_b}}\ \mathrm{m(t)}\, e^{j\vartheta_c}$$

The PSD of the complex envelope is

$$P_{g_{BPSK}}(t) = 2E_b\left(\frac{\sin \pi f T_b}{\pi f T_b}\right)^2$$

The PSD for the BPSK signal at RF can be evaluated by translating the baseband spectrum to the carrier frequency using the relation given in equation (1.5)
Hence, the PSD of a BPSK signal at RF is given by

$$P_{BPSK}(t) = \frac{E_b}{2}\left[\left(\frac{\sin \pi(f - f_C)T_b}{\pi(f - f_C)T_b}\right)^2 + \left(\frac{\sin \pi(-f - f_C)T_b}{\pi(-f - f_C)T_b}\right)^2\right]$$

The null–to–null bandwidth is found to be equal to twice the bit rate (**BW=2Rb = 2/Tb).**

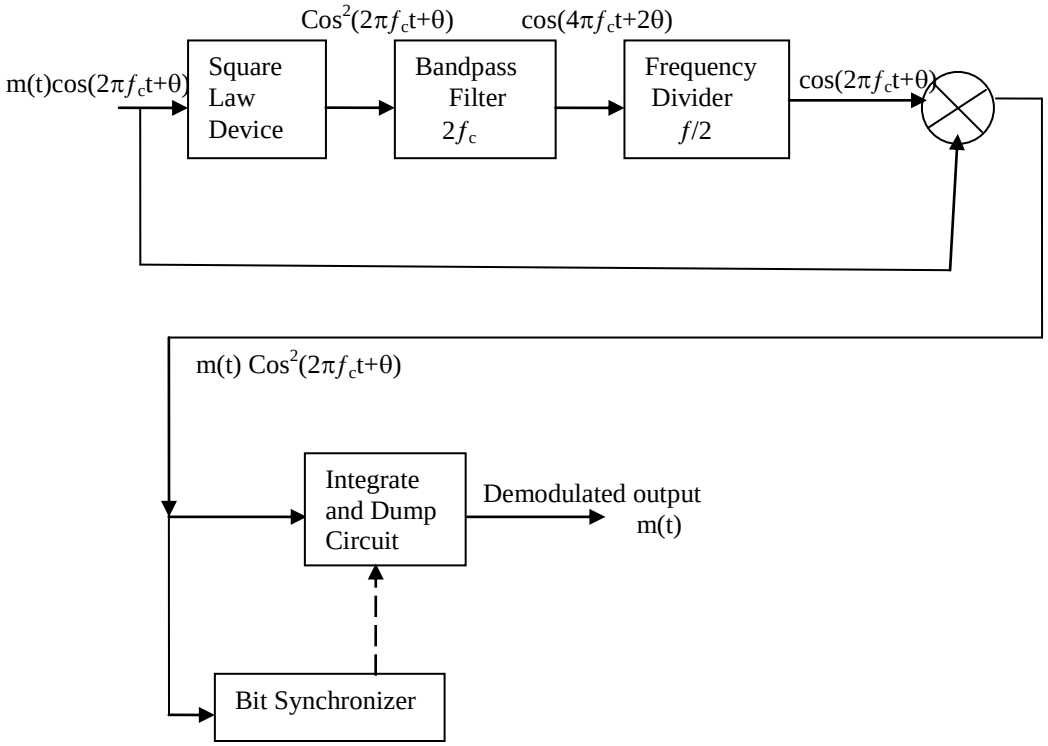
BPSK Receiver

If no multipath impairments are induced by the channel, the received BPSK signal can be expressed as

$$S_{BPSK}(t) = \mathrm{m(t)}\sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_C \mathrm{t} + \theta_C + \theta_{Ch})$$

$$= \mathrm{m(t)}\sqrt{\frac{2Eb}{Tb}}\cos(2\pi f_C t + \theta)$$

BPSK uses coherent or synchronous demodulation. If a low level pilot carrier signal is transmitted along with the BPSK signal, then the carrier phase and frequency may be recovered at the receiver using a phase locked loop (PLL). If no pilot carrier is transmitted, a Costas loop or squaring loop may be used to synthesize the carrier phase and frequency from the received BPSK signal.



The multiplier output is

$$m(t)\sqrt{\frac{2E_b}{T_b}}\cos^2(2\pi f_c t+\theta) = m(t)\sqrt{\frac{2E_b}{T_b}}\left[\frac{1}{2}+\frac{1}{2}\cos 2(2\pi f_c t+\theta)\right]$$

This signal is applied to an integrate and dump circuit which forms the low pass filter segment of a BPSK detector. If the transmitter and receiver pulse shapes are matched, then the detection will be optimum. A bit synchronizer is used at the end of each bit period. Here the switch at the output of the integrator closes to dump the output signal to the decision circuit. Depending on whether the integrator output us above or below a certain threshold, the decision circuit decides that the received signal corresponds to a binary 1 or 0. The threshold is set at an optimum level such that the probability of error is minimized. If binary 1 or 0 is transmitted, then the voltage level corresponding to the midpoint between the detector output voltage levels of binary 1 and 0 is used as the optimum threshold.

The probability of bit error in an AWGN channel is found using the Q-function of the distance between the signal points.

$$P_{e,\,BPSK} = Q\left(\sqrt{\frac{2E_b}{T_b}}\right)$$

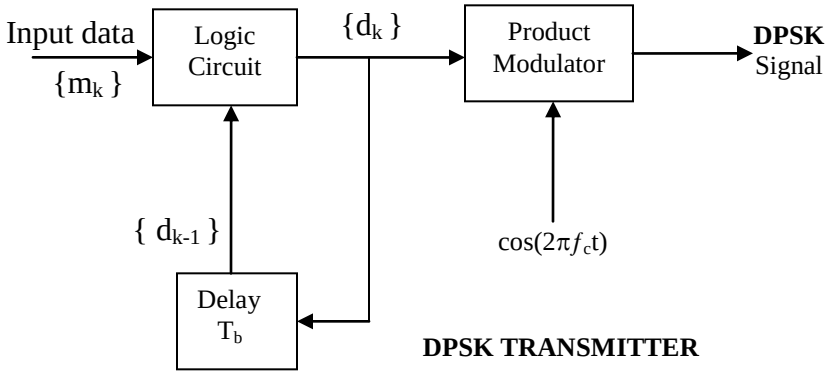
5. Describe in detail about the Digital modulation schemes DPSK and QPSK.

Differential phase shift keying (DPSK)

Differential PSK is a noncoherent form of phase shift keying which avoids the need for a coherent reference signal at the receiver. Noncoherent receivers are easy and cheap to

build, and hence are widely used in wireless communications. In DPSK systems, the input binary sequence is first differentially encoded and then modulated using a BPSK modulator. The differentially encoded sequence $\{d_k\}$ is generated from the input binary $\{m_k\}$ by $d_k = \overline{m_k \oplus d_{k-1}}$. The symbol d_k is unchanged if the incoming binary symbol m_k is 1 and to toggle d_k if m_k is 0.

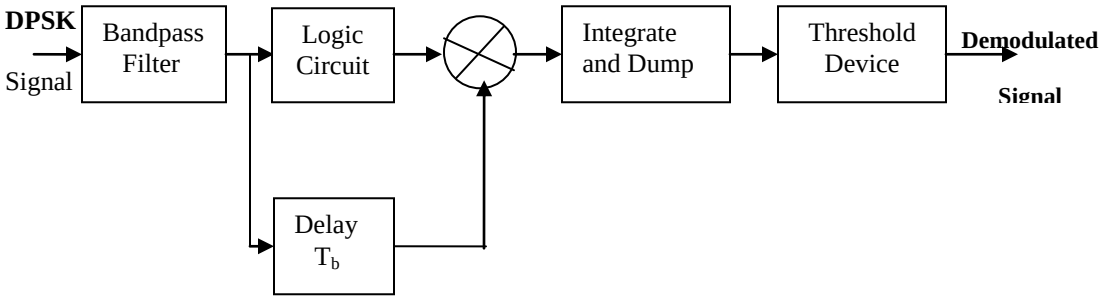
$m_k\}$		1	0	0	1	0	1	1	0
$d_{k-1}\}$		1	1	0	1	1	0	0	0
$\{d_k\}$	1	1	0	1	1	0	0	0	1



DPSK TRANSMITTER

It consists of a one bit delay element and a logic circuit to generate the differentially encoded sequence from the input binary sequency. The output is passed through a product modulator to obtain the DPSK signal. At the receiver a complementary process is done. **Advantage:** reduced receiver complexity. The average probability of error for DPSK in AWGN is given by

$$P_{e,\,DPSK} = \frac{1}{2}\exp\left(-\frac{E_b}{N_0}\right)$$



DPSK RECEIVER

QUADRATURE PHASE SHIFT KEYING (QPSK)

Quadrature phase shift keying (QPSK) has twice the bandwidth efficiency of BPSK, since two bits are transmitted in a single modulation symbol. The carrier phase takes on one of four equally spaced values, such as 0, $\pi/2$,π and $3\pi/2$ corresponds to a unique pair of message bits. The QPSK signal is defined as

$$S_{QPSK}(t) = \sqrt{\frac{2E_s}{T_s}}\cos\left[2\pi f_C t + (i-1)\frac{\pi}{2}\right] \qquad 0 \le t \le T_s \quad i = 1,2,3,4$$

Where

$T_s \rightarrow$ symbol duration equals twice the bit period

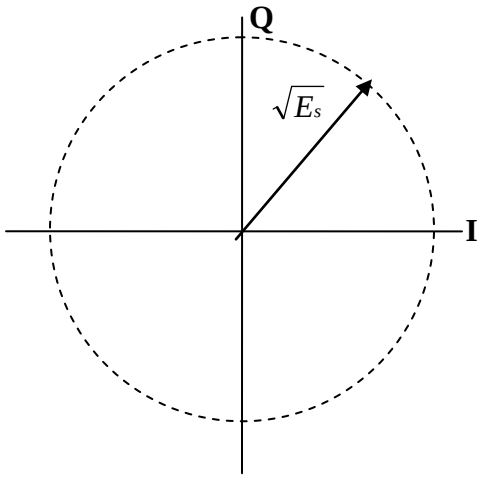
Using trigonometric identities

$$S_{QPSK}(t) = \sqrt{\frac{2E_s}{T_s}}\cos\left[(i-1)\frac{\pi}{2}\right]\cos(2\pi f_C t) - \sqrt{\frac{2E_s}{T_s}}\sin\left[(i-1)\frac{\pi}{2}\right]\sin(2\pi f_C t)$$

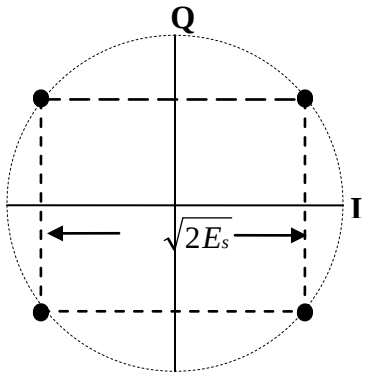
If basis functions $\phi_1(t) = \sqrt{2/T_s}\cos(2\pi f_C t)$, and $\phi_2(t) = \sqrt{2/T_s}\sin(2\pi f_C t)$ in the interval $0 \le t \le T_s$ then

$$S_{QPSK}(t) = \left\{\sqrt{E_s}\cos\left[(i-1)\frac{\pi}{2}\right]\phi_1(t) - \sqrt{E_s}\sin\left[(i-1)\frac{\pi}{2}\right]\phi_2(t)\right\} \qquad i = 1,2,3,4$$

QPSK Constellation



Carrier Phases $0,\pi/2,\pi,3\pi/2$



Carrier Phases $\pi/4,3\pi/4,5\pi/4,7\pi/4$

From the constellation diagram the distance between adjacent points in the constellation is $\sqrt{2E_s}$. Since each symbol corresponds to two bits, then $E_s = 2E_b$, thus the distance between two neighboring points is equal to $2\sqrt{E_b}$, the average probability of bit error in (AGWN) channel is

$$P_{er,\,QPSK} = Q\left[\sqrt{\frac{2E_b}{N_0}}\right]$$

The bit error probability of **QPSK** is identical to that of **BPSK. QPSK** provides twice the spectral efficiency with exactly the same energy efficiency.

Spectrum and Bandwidth of QPSK Signals

The PSD of a QPSK signal using rectangular pulses is expressed as

$$P_{QPSK}(f) = \frac{E_s}{2}\left[\left(\frac{\sin\pi(f-f_C)T_s}{\pi(f-f_C)T_s}\right)^2 + \left(\frac{\sin\pi(-f-f_C)T_s}{\pi(-f-f_C)T_s}\right)^2\right]$$

$$= E_b\left[\left(\frac{\sin 2\pi(f-f_C)T_b}{2\pi(f-f_C)T_b}\right)^2 + \left(\frac{\sin 2\pi(-f-f_C)T_b}{2\pi(-f-f_C)T_b}\right)^2\right]$$

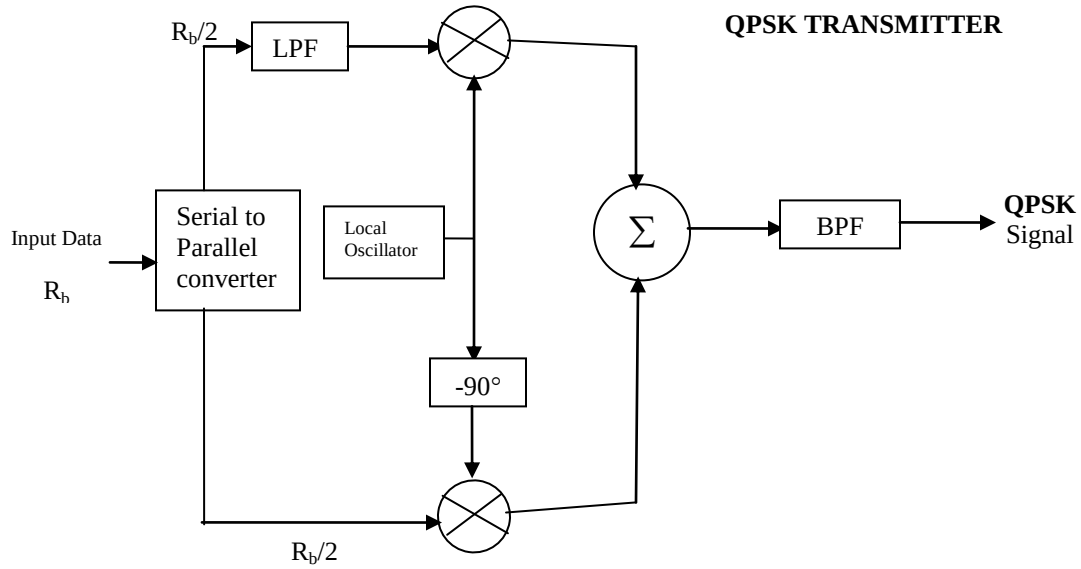
Where

$T_s = T_b/2$ $\rightarrow$ symbol period

The null–to–null RF bandwidth is equal to the bit rate Rb, which is half that of a BPSK signal.

QPSK Transmission and Detection Techniques

The unipolar binary message stream has bit rate R_b and is first converted into a bipolar non-return-to-zero (NRZ) sequence using a unipolar to bipolar converter. The bit stream m(t) is then split into two bit streams $m_I(t)$ and $m_Q(t)$ a bit rate of Rs = Rb/2. The two binary sequences are separately modulated by two carriers $\phi_1(t)$ and $\phi_2(t)$, are summed to produce a QPSK signal. The filter at the output confines the power spectrum within the allocated band.



The bandpass filter removes the out-of-band noise and adjacent channel interference. The filtered output is split into two parts and each part is coherently demodulated using the in-phase and quadrature carriers. The coherent carriers used for demodulation are recovered from the received signal using carrier recovery circuits. The outputs of the demodulators are passed through decision circuits the in-phase and quadrature binary streams. The two components are then multiplexed to reproduce the original binary sequence.

OFFSET QPSK

A modified form of QPSK, called offset QPSK (OQPSK) or staggered QPSK is less susceptible to these deleterious effects. In QPSK signaling, the bit transitions of the even and odd bit streams occur at the same time instants, but in OQPSK signaling , the even and odd bit streams $m_I(t)$ and $m_Q(t)$ are offset in their relative alignment by one bit period (half-symbol) period.

The spectrum is identical to that of a QPSK signal; hence both signals occupy the same bandwidth.

6. Describe in detail about the Space diversity techniques.

Space diversity also known as antenna diversity, is one of the most popular forms of diversity used in wireless systems. Conventional wireless systems consist of an elevated base station antenna and a mobile antenna close to the ground. The existence of a direct path between the transmitter and the receiver is not guaranteed and the possibility of a number of scatterers in the vicinity of the mobile suggests a Rayleigh fading signal. From this model, Jakes deduced that the signals received from spatially separated antennas on the mobile would have essentially uncorrelated envelops for antenna separations of one-half wavelength or more.

The concept of antenna space diversity is also used in base station design. At each cell site, multiple base station receiving antennas are used to provide diversity reception. However, since the important scatterers are generally on the ground in the vicinity of the mobile, the base station antennas must be spaced considerably far apart to achieve decorrelation. Separations on the order of several tens of wavelengths are required at the base station. Space diversity can thus be used at either the mobile or base station, or both.
Space diversity reception method can be classified into four categories.

Selection diversity
Feedback Diversity
Maximal Ratio Combining
Equal Gain Diversity

Selection diversity:

A block diagram of the method is similar to that shown in figure. Where m demodulators are used to provide m diversity branches whose gains are adjusted to provide the same average SNR for each branch. The receiver branch having the highest instantaneous SNR is connected to the demodulator.

The antenna signals themselves could be sampled and the best one sends to a signal demodulator. In practice, the branch with the largest (S+N)/N is used, since it is difficult to measure SNR alone. A practical selection diversity system cannot function on a truly instantaneous basis. But must be designed so that the internal time constants of the selection circuitry are shorter than the reciprocal of the signal fading rate.

Feedback Diversity or scanning diversity

Scanning diversity is very similar to selection diversity except that instead of always using the best of M signals, the M signals are scanned in a fixed sequence until one is found to be a above predetermined threshold. This signal is then received until it falls below threshold and the scanning process is again initiated. The resulting fading statistics are somewhat inferior to those obtained by the other methods, but the advantage with this method is that it is very simple to implement – only one receiver is required. A block diagram of this method is shown if figure

Maximal Ratio Combining

In this method first proposed by Kahn, the signals from all of the M branches are weighted according to their individual signal voltage to noise power ratios and summed. Figure shows a

block diagram of the technique. Here, the individual signals must be co phased before being summed which generally requires an receiver and phasing circuit for each antenna element. Maximal Ratio Combining produces an output SNR equal to the sum of the individual SNRs. Thus, it has the advantage of producing an output with an acceptable SNR even when none of the individual signals are themselves acceptable. This technique gives the best statistical reduction of fading of any known linear diversity combiner. Modern DSP techniques and digital receiver are now making this optimal form of diversity practical.

Equal Gain combining:

In certain cases it is not convenient to provide for the variable weighting capability required for true maximal ratio combining.

In such cases, the branch weights are all set to unity, but the signals from each branch are co phased to provide the equal gain combining diversity. This allows the receiver to exploit signals that are simultaneously received on each branch. The possibility of producing an acceptable signal from a number of unacceptable inputs is still retained, and performance is only marginally inferior to maximal ratio combining and superior to selection diversity.

UNIT-II WIRELESS PROTOCOL
PART-A (2 MARKS)

1. Define routing

Routing (or routeing) is the process of selecting paths in a network along which to send network traffic. Routing is performed for many kinds of networks, including the telephone network, electronic data networks (such as the Internet), and transportation networks

2. What is network security?

The field of networking, the specialist area of network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent

3. Define ALOHA

Aloha, also called the Aloha method, refers toa simple communications scheme in which each source (transmitter) in a network sends data wheneverthere is a frame to send. If the framesuccessfully reaches the destination (receiver), the next frame is sent. If theframe fails to be received at the destination, it is sent again. This protocol wasoriginally developed at the University of Hawaii for use with satellite communication systems in the Pacific.

4. What is IMT 2000?

IMT 2000, also known as International Mobile Telecommunications 2000, is the ITU globally coordinated definition of 3G covering key issues such as frequency spectrum use and technical standards. More information is available in this presentation

5. What are different types of 3G Networks specified by IMT 2000?

ITU Recommendation ITU-R M.1457 specifies five types of 3G radio interfaces:
IMT-2000 CDMA Direct Spread, also known as UTRA FDD including WCDMA in Japan, ARIB / DoCoMo recommendation. UMTS is developed by 3GPP.
IMT-2000 CDMA Multi-carrier, also known as Cdma2000 (3X) developed by 3GPP2. IMT-2000 CDMA2000 includes 1X components, like cdma2000 1X EV-DO.
IMT-2000 CDMA TDD, also known as UTRA TDD and TD-SCDMA. TD-SCDMA is developed in China and supported by TD-SCDMA Forum.
IMT-2000 TDMA Single Carrier, also known as UWC-136 (Edge) supported by UWCC.
IMT-2000 DECT supported by DECT Forum.

6. Define Home network

The home network of a mobile device is the network within which the device receives its identifying IP address (home address).

7. Define Home address
The home address of a mobile device is the IP address assigned to the device within its home network.

8. What is Foreign network?
A foreign network is the network in which a mobile node is operating when away from its home network.

9. Define Care-of address
The care-of address of a mobile device is the network-native IP address of the device when operating in a foreign network.

10. Define Home agent
A home agent is a router on a mobile node's home network which tunnels datagrams for delivery to the mobile node when it is away from home. It maintains current location (IP address) information for the mobile node. It is used with one or more foreign agents.

11. Define foreign agent
A foreign agent is a router that stores information about mobile nodes visiting its network. Foreign agents also advertise care-of-addresses which are used by Mobile IP.

PART-B (16 MARKS)

1. Explain ALOHA

ALOHAnet, also known as the ALOHA System[1][2], or simply ALOHA, was a pioneering computer networking system developed at the University of Hawaii[3]. ALOHAnet became operational in June, 1971, providing the first demonstration of a wireless data network[4].
The ALOHAnet used a new method of medium access (ALOHA random access) and experimental UHF frequencies for its operation, since frequency assignments for communications to and from a computer were not available for commercial applications in the 1970s. But even before such frequencies were assigned there were two other media available for the application of an ALOHA channel – cables and satellites. In the 1970s ALOHA random access was employed in the widely used Ethernet cable based network[5] and then in the Marisat (now Inmarsat) satellite network[6].

In the early 1980s frequencies for mobile networks became available, and in 1985 frequencies suitable for what became known as WiFi were allocated in the US. These regulatory developments made it possible to use the ALOHA random access techniques in both WiFi and in mobile telephone networks.

ALOHA channels were used in a limited way in the 1980s in 1G mobile phones for signaling and control purposes[7]. In the 1990s, Matti Makkonen and others at Telecom Finland greatly expanded the use of ALOHA channels in order to implement SMS message texting in 2G mobile phones. In the early 2000s additional ALOHA channels were added to 2.5G and 3G mobile phones with the widespread introduction of GPRS, using a slotted ALOHA random access channel combined with a version of the Reservation ALOHA scheme first analyzed by a group at BBN
he ALOHA protocol
[edit]
Pure ALOHA

Pure ALOHA protocol. Boxes indicate frames. Shaded boxes indicate frames which have collided.

The first version of the protocol (now called "Pure ALOHA", and the one implemented in ALOHAnet) was quite simple:
If you have data to send, send the data
If the message collides with another transmission, try resending "later"

Note that the first step implies that Pure ALOHA does not check whether the channel is busy before transmitting. The critical aspect is the "later" concept: the quality of the backoff scheme chosen significantly influences the efficiency of the protocol, the ultimate channel capacity, and the predictability of its behavior.

To assess Pure ALOHA, we need to predict its throughput, the rate of (successful) transmission of frames. (This discussion of Pure ALOHA's performance follows Tanenbaum [9].) First, let's make a few simplifying assumptions:
All frames have the same length.
Stations cannot generate a frame while transmitting or trying to transmit. (That is, if a station keeps trying to send a frame, it cannot be allowed to generate more frames to send.)
The population of stations attempts to transmit (both new frames and old frames that collided) according to a Poisson distribution.

Let "T" refer to the time needed to transmit one frame on the channel, and let's define "frame-time" as a unit of time equal to T. Let "G" refer to the mean used in the Poisson distribution over transmission-attempt amounts: that is, on average, there are G transmission-attempts per frame-time.

Overlapping frames in the pure ALOHA protocol. Frame-time is equal to 1 for all frames.

Consider what needs to happen for a frame to be transmitted successfully. Let "t" refer to the time at which we want to send a frame. We want to use the channel for one frame-time beginning at t, and so we need all other stations to refrain from

transmitting during this time. Moreover, we need the other stations to refrain from transmitting between t-T and t as well, because a frame sent during this interval would overlap with our frame.

For any frame-time, the probability of there being k transmission-attempts during that frame-time is:

The average amount of transmission-attempts for 2 consecutive frame-times is 2G. Hence, for any pair of consecutive frame-times, the probability of there being k transmission-attempts during those two frame-times is:

Therefore, the probability (Probpure) of there being zero transmission-attempts between t-T and t+T (and thus of a successful transmission for us) is:

$$Probpure = e - 2G$$

The throughput can be calculated as the rate of transmission-attempts multiplied by the probability of success, and so we can conclude that the throughput (Spure) is:

$$Spure = Ge - 2G$$

The maximum throughput is 0.5/e frames per frame-time (reached when G = 0.5), which is approximately 0.184 frames per frame-time. This means that, in Pure ALOHA, only about 18.4% of the time is used for successful transmissions.
[edit]
Slotted ALOHA

Slotted ALOHA protocol. Boxes indicate frames. Shaded boxes indicate frames which are in the same slots.

An improvement to the original ALOHA protocol was "Slotted ALOHA", which introduced discrete timeslots and increased the maximum throughput[10]. A station can send only at the beginning of a timeslot, and thus collisions are reduced. In this case, we only need to worry about the transmission-attempts within 1 frame-time and not 2 consecutive frame-times, since collisions can only occur during each timeslot. Thus, the probability of there being zero transmission-attempts in a single timeslot is:

$$Probslotted = e - G$$

the probability of k packets is:

$$Probslottedk = e - G(1 - e - G)k - 1$$

The throughput is:

$S_{slotted} = Ge^{-G}$

The maximum throughput is 1/e frames per frame-time (reached when G = 1), which is approximately 0.368 frames per frame-time, or 36.8%.

Slotted ALOHA is used in low-data-rate tactical satellite communications networks by military forces, in subscriber-based satellite communications networks, mobile telephony call setup, and in the contactless RFID technologies.
[edit]
Other Protocols

The use of a random access channel in ALOHAnet also led to the development of CSMA - Carrier Sense Multiple Access, a 'listen before send' random access protocol which can be used when all nodes send and receive on the same channel. The first implementation of CSMA was Ethernet, and CSMA was extensively modeled in[11].

It should be noted that ALOHA and the other random-access protocols have an inherent variability in their throughput and delay performance characteristics. For this reason, applications which need highly deterministic load behavior often use polling or token-passing schemes (such as token ring) instead of contention systems. For instance ARCNET is popular in embedded data applications

2. In detail explain IEEE802.11

IEEE 802.11 is a set of standards carrying out wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The base current version of the standard is IEEE 802.11-2007.
The 802.11 family includes over-the-air modulation techniques that use the same basic protocol. The most popular are those defined by the 802.11b and 802.11g protocols, which are amendments to the original standard. 802.11-1997 was the first wireless networking standard, but 802.11b was the first widely accepted one, followed by 802.11g and 802.11n. Security was originally purposefully weak due to export requirements of some governments,[1] and was later enhanced via the 802.11i amendment after governmental and legislative changes. 802.11n is a new multi-streaming modulation technique. Other standards in the family (c–f, h, j) are service amendments and extensions or corrections to the previous specifications.

802.11b and 802.11g use the 2.4 GHz ISM band, operating in the United States under Part 15 of the US Federal Communications Commission Rules and Regulations. Because of this choice of frequency band, 802.11b and g equipment may occasionally suffer interference from microwave ovens, cordless telephones and Bluetooth devices. 802.11b and 802.11g control their interference and susceptibility to

interference by using direct-sequence spread spectrum (DSSS) and orthogonal frequency-division multiplexing (OFDM) signaling methods, respectively. 802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 19 non-overlapping channels rather than the 3 offered in the 2.4 GHz ISM frequency band.[2] Better or worse performance with higher or lower frequencies (channels) may be realized, depending on the environment.

The segment of the radio frequency spectrum used by 802.11 varies between countries. In the US, 802.11a and 802.11g devices may be operated without a license, as allowed in Part 15 of the FCC Rules and Regulations. Frequencies used by channels one through six of 802.11b and 802.11g fall within the 2.4 GHz amateur radio band. Licensed amateur radio operators may operate 802.11b/g devices under Part 97 of the FCC Rules and Regulations, allowing increased power output but not commercial content or encryption.[3]

[edit]

History

802.11 technology has its origins in a 1985 ruling by the U.S. Federal Communications Commission that released the ISM band for unlicensed use.[4]

In 1991 NCR Corporation/AT&T (now Alcatel-Lucent and LSI Corporation) invented the precursor to 802.11 in Nieuwegein, The Netherlands. The inventors initially intended to use the technology for cashier systems; the first wireless products were brought on the market under the name WaveLAN with raw data rates of 1 Mbit/s and 2 Mbit/s.[citation needed]

Vic Hayes, who held the chair of IEEE 802.11 for 10 years and has been called the "father of Wi-Fi" was involved in designing the initial 802.11b and 802.11a standards within the IEEE.[citation needed]

In 1992, the Commonwealth Scientific and Industrial Research Organisation (CSIRO) obtained a patent in Australia for wireless data transfer technology. In 1996, they obtained a patent for the same technology in the US.[5] Wi-Fi uses the mathematical formula in the patents. In April 2009, 14 tech companies including Intel, Microsoft, HP, Dell, agreed to pay CSIRO $250 million for their Wi-Fi patent infringements.[6]

[edit]

Protocols[hide]

802.11 network standards v • d • e

802.11

Protocol Release[7] Freq. (GHz) Bandwidth (MHz) Data rate per stream (Mbit/s)[8] Allowable MIMO streams Modulation Approximate indoor range[citation needed] Approximate Outdoor range[citation needed]

(m)(ft) (m) (ft)

–	Jun 1997	2.4	20	1, 2	1	DSSS, FHSS	20	66	100	330
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	35	115	120	390
3.7[y]	--	--	5,000	16,000[y]						
b	Sep 1999	2.4	20	5.5, 11	1	DSSS	38	125	140	460
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS	38	125	140	460
n	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2[z]	4	OFDM	70	230	250	820[9]
40	15, 30, 45, 60, 90, 120, 135, 150[z]	70	230	250	820[9]					

y IEEE 802.11y-2008 extended operation of 802.11a to the licensed 3.7 GHz band. Increased power limits allow a range up to 5000m. As of 2009, it is only being licensed in the United States by the FCC.
z Assumes Short Guard interval (SGI) enabled, otherwise reduce each data rate by 10%.

[edit]
802.11-1997 (802.11 legacy)
Main article: IEEE 802.11 (legacy mode)

The original version of the standard IEEE 802.11 was released in 1997 and clarified in 1999, but is today obsolete. It specified two net bit rates of 1 or 2 megabits per second (Mbit/s), plus forward error correction code. It specified three alternative physical layer technologies: diffuse infrared operating at 1 Mbit/s; frequency-hopping spread spectrum operating at 1 Mbit/s or 2 Mbit/s; and direct-sequence spread spectrum operating at 1 Mbit/s or 2 Mbit/s. The latter two radio technologies used microwave transmission over the Industrial Scientific Medical frequency band at 2.4 GHz. Some earlier WLAN technologies used lower frequencies, such as the U.S. 900 MHz ISM band.

Legacy 802.11 with direct-sequence spread spectrum was rapidly supplanted and popularized by 802.11b.
[edit]
802.11a
Main article: IEEE 802.11a-1999

The 802.11a standard uses the same data link layer protocol and frame format as the original standard, but an OFDM based air interface (physical layer). It operates in the 5 GHz band with a maximum net data rate of 54 Mbit/s, plus error correction code, which yields realistic net achievable throughput in the mid-20 Mbit/s[citation needed]

Since the 2.4 GHz band is heavily used to the point of being crowded, using the relatively unused 5 GHz band gives 802.11a a significant advantage. However, this high carrier frequency also brings a disadvantage: the effective overall range of 802.11a is less than that of 802.11b/g. In theory, 802.11a signals are absorbed more

readily by walls and other solid objects in their path due to their smaller wavelength and, as a result, cannot penetrate as far as those of 802.11b. In practice, 802.11b typically has a higher range at low speeds (802.11b will reduce speed to 5 Mbit/s or even 1 Mbit/s at low signal strengths). However, at higher speeds, 802.11a often has the same or greater range due to less interference.[citation needed]
[edit]
802.11b
Main article: IEEE 802.11b-1999

802.11b has a maximum raw data rate of 11 Mbit/s and uses the same media access method defined in the original standard. 802.11b products appeared on the market in early 2000, since 802.11b is a direct extension of the modulation technique defined in the original standard. The dramatic increase in throughput of 802.11b (compared to the original standard) along with simultaneous substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.

802.11b devices suffer interference from other products operating in the 2.4 GHz band. Devices operating in the 2.4 GHz range include: microwave ovens, Bluetooth devices, baby monitors and cordless telephones.
[edit]
802.11g
Main article: IEEE 802.11g-2003

In June 2003, a third modulation standard was ratified: 802.11g. This works in the 2.4 GHz band (like 802.11b), but uses the same OFDM based transmission scheme as 802.11a. It operates at a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 22 Mbit/s average throughput.[10] 802.11g hardware is fully backwards compatible with 802.11b hardware and therefore is encumbered with legacy issues that reduce throughput when compared to 802.11a by ~21%.

The then-proposed 802.11g standard was rapidly adopted by consumers starting in January 2003, well before ratification, due to the desire for higher data rates as well as to reductions in manufacturing costs. By summer 2003, most dual-band 802.11a/b products became dual-band/tri-mode, supporting a and b/g in a single mobile adapter card or access point. Details of making b and g work well together occupied much of the lingering technical process; in an 802.11g network, however, activity of an 802.11b participant will reduce the data rate of the overall 802.11g network .

Like 802.11b, 802.11g devices suffer interference from other products operating in the 2.4 GHz band, for example wireless keyboards.
[edit]
802.11-2007

In 2003, task group TGma was authorized to "roll up" many of the amendments to the 1999 version of the 802.11 standard. REVma or 802.11ma, as it was called, created a

single document that merged 8 amendments (802.11a, b, d, e, g, h, i, j) with the base standard. Upon approval on March 8, 2007, 802.11REVma was renamed to the current[dated info] base standard IEEE 802.11-2007.[11]
[edit]
802.11n
Main article: IEEE 802.11n-2009

802.11n is a recent amendment which improves upon the previous 802.11 standards by adding multiple-input multiple-output antennas (MIMO). 802.11n operates on both the 2.4GHz and the lesser used 5 GHz bands. The IEEE has approved the amendment and it was published in October 2009.[12][13] Prior to the final ratification, enterprises were already migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11n proposal.

3. Explain in detail about 3G and 4G networks

4G stands for the fourth generation of cellular wireless standards. It is a successor to 3G and 2G families of standards. Speed requirements for 4G service set the peak download speed at 100 Mbit/s for high mobility communication (such as from trains and cars) and 1 Gbit/s for low mobility communication (such as pedestrians and stationary users).

A 4G system is expected to provide a comprehensive and secure all-IP based mobile broadband solution to smartphones, laptop computer wireless modems and other mobile devices. Facilities such as ultra-broadband Internet access, IP telephony, gaming services, and streamed multimedia may be provided to users.

Pre-4G technologies such as mobile WiMAX and first-release 3G Long term evolution (LTE) have been on the market since 2006[1] and 2009[2][3][4] respectively, and are often branded as 4G. The current versions of these technologies did not fulfill the original ITU-R requirements of data rates approximately up to 1 Gbit/s for 4G systems. Marketing materials use 4G as a description for Mobile-WiMAX and LTE in their current forms.

IMT-Advanced compliant versions of the above two standards are under development and called “LTE-Advanced” and “WirelessMAN-Advanced” respectively. ITU has decided that “LTE-Advanced” and “WirelessMAN-Advanced” should be accorded the official designation of IMT-Advanced. On December 6th, 2010, ITU announced that current versions of LTE, WiMax and other evolved 3G technologies

3G International Mobile Telecommunications-2000 (IMT — 2000), better known as 3G or 3rd Generation, is a generation of standards for mobile phones and mobile telecommunications services fulfilling specifications by the International Telecommunication Union.[1] Application services include wide-area wireless voice telephone, mobile Internet access, video calls and mobile TV, all in a mobile

environment. Compared to the older 2G and 2.5G standards, a 3G system must allow simultaneous use of speech and data services, and provide peak data rates of at least 200 kbit/s according to the IMT-2000 specification. Recent 3G releases, often denoted 3.5G and 3.75G, also provide mobile broadband access of several Mbit/s to laptop computers and smartphones.

The following standards are typically branded 3G:
the UMTS system, first offered in 2001, standardized by 3GPP, used primarily in Europe, Japan, China (however with a different radio interface) and other regions predominated by GSM 2G system infrastructure. The cell phones are typically UMTS and GSM hybrids. Several radio interfaces are offered, sharing the same infrastructure:
The original and most widespread radio interface is called W-CDMA.
The TD-SCDMA radio interface, was commercialised in 2009 and is only offered in China.
The latest UMTS release, HSPA+, can provide peak data rates up to 56 Mbit/s in the downlink in theory (28 Mbit/s in existing services) and 22 Mbit/s in the uplink.
the CDMA2000 system, first offered in 2002, standardized by 3GPP2, used especially in North America and South Korea, sharing infrastructure with the IS-95 2G standard. The cell phones are typically CDMA2000 and IS-95 hybrids. The latest release EVDO Rev B offers peak rates of 14.7 Mbit/s downstreams.

The above systems and radio interfaces are based on kindred spread spectrum radio transmission technology. While the GSM EDGE standard ("2.9G"), DECT cordless phones and Mobile WiMAX standards formally also fulfill the IMT-2000 requirements and are approved as 3G standards by ITU, these are typically not branded 3G, and are based on completely different technologies.

A new generation of cellular standards has appeared approximately every tenth year since 1G systems were introduced in 1981/1982. Each generation is characterized by new frequency bands, higher data rates and non backwards compatible transmission technology. The first release of the 3GPP Long Term Evolution (LTE) standard does not completely fulfill the ITU 4G requirements called IMT-Advanced. First release LTE is not backwards compatible with 3G, but is a pre-4G or 3.9G technology, however sometimes branded "4G" by the service providers. WiMAX is another technology verging on or marketed as 4G

3. Explain CDMA2000

CDMA2000 (also known as IMT Multi‑Carrier (IMT‑MC)) is a family of 3G[1] mobile technology standards, which use CDMA channel access, to send voice, data, and signaling data between mobile phones and cell sites. The set of standards includes: CDMA2000 1X, CDMA2000 EV-DO Rev. 0, CDMA2000 EV-DO Rev. A, and CDMA2000 EV-DO Rev. B[2]. All are approved radio interfaces for the ITU's IMT-2000. CDMA2000 has a relatively long technical history and is backward-compatible with its previous 2G iteration IS-95 (cdmaOne). In the United States,

CDMA2000 is a registered trademark of the Telecommunications Industry Association (TIA-USA)[3]. The successor to CDMA2000 is LTE, part of the competing 3GPP family.[4]

1X

CDMA2000 1X (IS-2000), also known as 1x and 1xRTT, is the core CDMA2000 wireless air interface standard. The designation "1x", meaning 1 times Radio Transmission Technology, indicates the same RF bandwidth as IS-95: a duplex pair of 1.25 MHz radio channels. 1xRTT almost doubles the capacity of IS-95 by adding 64 more traffic channels to the forward link, orthogonal to (in quadrature with) the original set of 64. The 1X standard supports packet data speeds of up to 153 kbps with real world data transmission averaging 60–100 kbps in most commercial applications.[5] IMT-2000 also made changes to the data link layer for the greater use of data services, including medium and link access control protocols and QoS. The IS-95 data link layer only provided "best effort delivery" for data and circuit switched channel for voice (i.e., a voice frame once every 20 ms).
1xEV-DO
Main article: Evolution-Data Optimized

CDMA2000 1xEV-DO (Evolution-Data Optimized), often abbreviated as EV-DO or EV, is a telecommunications standard for the wireless transmission of data through radio signals, typically for broadband Internet access. It uses multiplexing techniques including code division multiple access (CDMA) as well as time division multiple access (TDMA) to maximize both individual user's throughput and the overall system throughput. It is standardized by 3rd Generation Partnership Project 2 (3GPP2) as part of the CDMA2000 family of standards and has been adopted by many mobile phone service providers around the world – particularly those previously employing CDMA networks. It is also used on the Globalstar satellite phone network.[6]
Networks

The CDMA Development Group states that, as of November 2009, there are 308 operators in 116 countries offering CDMA2000 1X and 1xEV-DO service.

.

5. Explain UMTS

Universal Mobile Telecommunications System (UMTS) is one of the third-generation (3G) mobile telecommunications technologies, which is also being developed into a 4G technology. The first deployment of the UMTS is the release99 (R99) architecture. It is specified by 3GPP and is part of the global ITU IMT-2000 standard. The most common form of UMTS uses W-CDMA (IMT Direct Spread) as the underlying air interface but the system also covers TD-CDMA and TD-SCDMA (both IMT CDMA TDD). Being a complete network system, UMTS also covers the radio access network (UMTS Terrestrial Radio Access Network, or UTRAN) and the

core network (Mobile Application Part, or MAP), as well as authentication of users via SIM cards (Subscriber Identity Module).

Unlike EDGE (IMT Single-Carrier, based on GSM) and CDMA2000 (IMT Multi-Carrier), UMTS requires new base stations and new frequency allocations. However, it is closely related to GSM/EDGE as it borrows and builds upon concepts from GSM. Further, most UMTS handsets also support GSM, allowing seamless dual-mode operation. Therefore, UMTS is sometimes marketed as 3GSM, emphasizing the close relationship with GSM and differentiating it from competing technologies.

The name UMTS, introduced by ETSI, is usually used in Europe. Outside of Europe, the system is also known by other names such as FOMA[1] or W-CDMA.[nb 1][1] In marketing, it is often referred to as 3G or 3G+.

Technology

UMTS combines three different air interfaces, GSM's Mobile Application Part (MAP) core, and the GSM family of speech codecs.

[edit]

Air interfaces

UMTS provides several different terrestrial air interfaces, called UMTS Terrestrial Radio Access (UTRA).[4] All air interface options are part of ITU's IMT-2000. In the currently most popular variant for cellular mobile telephones, W-CDMA (IMT Direct Spread) is used.

Please note that the terms W-CDMA, TD-CDMA and TD-SCDMA are misleading. While they suggest covering just a channel access method (namely a variant of CDMA), they are actually the common names for the whole air interface standards.[5]

Non-terrestrial radio access networks are currently under research.

[edit]

W-CDMA (UTRA-FDD)

Main article: W-CDMA (UMTS)

UMTS transmitter on the roof of a building

W-CDMA uses the DS-CDMA channel access method with a pair of 5 MHz channels. In contrast, the competing CDMA2000 system uses one or more arbitrary 1.25 MHz channels for each direction of communication. W-CDMA systems are widely criticized for their large spectrum usage, which has delayed deployment in countries that acted relatively slowly in allocating new frequencies specifically for 3G services (such as the United States).

The specific frequency bands originally defined by the UMTS standard are 1885–2025 MHz for the mobile-to-base (uplink) and 2110–2200 MHz for the base-to-

mobile (downlink). In the US, 1710–1755 MHz and 2110–2155 MHz will be used instead, as the 1900 MHz band was already used.[6] While UMTS2100 is the most widely-deployed UMTS band, some countries' UMTS operators use the 850 MHz and/or 1900 MHz bands (independently, meaning uplink and downlink are within the same band), notably in the US by AT&T Mobility, New Zealand by Telecom New Zealand on the XT Mobile Network and in Australia by Telstra on the Next G network.

W-CDMA is a part of IMT-2000 as IMT Direct Spread.
[edit]
UTRA-TDD HCR
Main article: UTRA-TDD HCR

UMTS-TDD's air interfaces that use the TD-CDMA channel access technique are standardized as UTRA-TDD HCR, which uses increments of 5 MHz of spectrum, each slice divided into 10ms frames containing fifteen time slots (1500 per second)[7]. The time slots (TS) are allocated in fixed percentage for downlink and uplink. TD-CDMA is used to multiplex streams from or to multiple transceivers. Unlike W-CDMA, it does not need separate frequency bands for up- and downstream, allowing deployment in tight frequency bands.

TD-CDMA is a part of IMT-2000 as IMT CDMA TDD.
[edit]
TD-SCDMA (UTRA-TDD 1.28 Mcps Low Chip Rate)
Main article: TD-SCDMA

TD-SCDMA uses the TDMA channel access method combined with an adaptive synchronous CDMA component [8] on 1.6 MHz slices of spectrum, allowing deployment in even tighter frequency bands than TD-CDMA. However, the main incentive for development of this Chinese-developed standard was avoiding or reducing the license fees that have to be paid to non-Chinese patent owners. Unlike the other air interfaces, TD-SCDMA was not part of UMTS from the beginning but has been added in Release 4 of the specification.

Like TD-CDMA, it is known as IMT CDMA TDD within IMT-2000.
[edit]
Radio access network
Main article: UTRAN

UMTS also specifies the UMTS Terrestrial Radio Access Network (UTRAN), which is composed of multiple base stations, possibly using different terrestrial air interface standards and frequency bands.

UMTS and GSM/EDGE can share a Core Network (CN), making UTRAN an alternative radio access network to GERAN (GSM/EDGE RAN), and allowing (mostly) transparent switching between the RANs according to available coverage

and service needs. Because of that, UMTS' and GSM/EDGE's radio access networks are sometimes collectively referred to as UTRAN/GERAN.

UMTS networks are often combined with GSM/EDGE, the later of which is also a part of IMT-2000.

The UE (User Equipment) interface of the RAN (Radio Access Network) primarily consists of RRC (Radio Resource Control), RLC (Radio Link Control) and MAC (Media Access Control) protocols. RRC protocol handles connection establishment, measurements, radio bearer services, security and handover decisions. RLC protocol primarily divides into three Modes - Transparent Mode (TM), Unacknowledge Mode (UM), Acknowledge Mode (AM). The functionality of AM entity resembles TCP operation where as UM operation resembles UDP operation. In TM mode, data will be sent to lower layers without adding any header to SDU of higher layers. MAC handles the scheduling of data on air interface depending on higher layer (RRC) configured parameters.

Set of properties related to data transmission is called Radio Bearer (RB). This set of properties will decide the maximum allowed data in a TTI (Transmission Time Interval). RB includes RLC information and RB mapping. RB mapping decides the mapping between RB<->logical channel<->transport channel. Signaling message will be send on Signaling Radio Bearers (SRBs) and data packets (either CS or PS) will be sent on data RBs. RRC and NAS messages will go on SRBs.

Security includes two procedures: integrity and ciphering. Integrity validates the resource of message and also make sure that no one (third/unknown party) on radio interface has not modified message. Ciphering make sure that no one listens your data on air interface. Both integrity and ciphering will be applied for SRBs where as only ciphering will be applied for data RBs.

5. explain mobility management and handover technologies all mobile IP networks

Mobile IP (or IP mobility) is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address. Mobile IP for IPv4 is described in IETF RFC 3344, and updates are added in IETF RFC 4721. Mobile IPv6, the IP mobility implementation for the next generation of the Internet Protocol, IPv6
The Mobile IP protocol allows location-independent routing of IP datagrams on the Internet. Each mobile node is identified by its home address disregarding its current location in the Internet. While away from its home network, a mobile node is associated with a care-of address which identifies its current location and its home address is associated with the local endpoint of a tunnel to its home agent. Mobile IP specifies how a mobile node registers with its home agent and how the home agent routes datagrams to the mobile node through the tunnel.

Mobile IP provides an efficient, scalable mechanism for roaming within the Internet. Using Mobile IP, nodes may change their point-of-attachment to the Internet without changing their home IP address. This allows them to maintain transport and higher-layer connections while roaming. Node mobility is realized without the need to propagate host-specific routes throughout the Internet routing fabric.Mobile IP is a protocol/technology which provides IP mobility to future devices.
[edit]
Applications

Mobile IP is most often found in wired and wireless environments where users need to carry their mobile devices across multiple LAN subnets. Examples of use are in roaming between overlapping wireless systems, e.g., IP over DVB, WLAN, WiMAX and BWA. Currently, Mobile IP is not required within cellular systems such as 3G, to provide transparency when Internet users migrate between cellular towers, since these systems provide their own data link layer handover and roaming mechanisms. However, it is often used in 3G systems to allow seamless IP mobility between different Packet Data Serving Node (PDSN) domains.

In many applications (e.g., VPN, VoIP), sudden changes in network connectivity and IP address can cause problems.
[edit]
Operational principles

A mobile node can have two addresses - a permanent home address and a care-of address (CoA), which is associated with the network the mobile node is visiting. Two kinds of entities comprise a Mobile IP implementation:
A home agent stores information about mobile nodes whose permanent home address is in the home agent's network.
A foreign agent stores information about mobile nodes visiting its network. Foreign agents also advertise care-of addresses, which are used by Mobile IP.

A node wanting to communicate with the mobile node uses the permanent home address of the mobile node as the destination address to send packets to. Because the home address logically belongs to the network associated with the home agent, normal IP routing mechanisms forward these packets to the home agent. Instead of forwarding these packets to a destination that is physically in the same network as the home agent, the home agent redirects these packets towards the foreign agent through an IP tunnel by encapsulating the datagram with a new IP header using the care of address of the mobile node.

When acting as transmitter, a mobile node sends packets directly to the other communicating node through the foreign agent, without sending the packets through the home agent, using its permanent home address as the source address for the IP packets. This is known as triangular routing. If needed, the foreign agent could employ reverse tunneling by tunneling the mobile node's packets to the home agent, which in turn forwards them to the communicating node. This is needed in networks

whose gateway routers have ingress filtering enabled and hence the source IP address of the mobile host would need to belong to the subnet of the foreign network or else the packets will be discarded by the router.

The Mobile IP protocol defines the following:
an authenticated registration procedure by which a mobile node informs its home agent(s) of its care-of-address(es);
an extension to ICMP Router Discovery, which allows mobile nodes to discover prospective home agents and foreign agents; and
the rules for routing packets to and from mobile nodes, including the specification of one mandatory tunneling mechanism and several optional tunneling mechanisms.

A performance evaluation of Mobile IPv6 can be found in [1]. Additionally, a performance comparison between Mobile IPv6 and some of its proposed enhancements
Changes in IPv6 for Mobile IPv6
A set of mobility options to include in mobility messages
A new Home Address option for the Destination Options header
A new Type 2 Routing header
New Internet Control Message Protocol for IPv6 (ICMPv6) messages to discover the set of home agents and to obtain the prefix of the home link
Changes to router discovery messages and options and additional Neighbor Discovery options
Mobile IPv6
Mobile IPv6 (MIPv6) is a protocol developed as a subset of Internet Protocol version 6 (IPv6) to support mobile connections. MIPv6 is an update of the IETF (Internet Engineering Task Force) Mobile IP standard (RFC 2002) designed to authenticate mobile devices (known as mobile nodes) using IPv6 addresses.

In traditional IP routing, IP addresses represent a topology. Routing mechanisms rely on the assumption that each network node will always have the same point of attachment to the Internet, and that each node's IP address identifies the network link where it is connected. In this routing scheme, if you disconnect a mobile device from the Internet and want to reconnect through a different network, you have to configure the device with a new IP address, and the appropriate netmask and default router. Otherwise, routing protocols have no means of delivering datagrams (packets), because the device's network address doesn't contain the necessary information about the node's network point of attachment to the Internet.

MIPv6 allows a mobile node to transparently maintain connections while moving from one subnet to another. Each device is identified by its home address although it may be connecting to through another network. When connecting through a foreign network, a mobile device sends its location information to a home agent, which intercepts packets intended for the device and tunnels them to the current location.

UNIT-III TYPES OF WIRELESS NETWORKS
PART-A (2 MARKS)

1. **Wireless ad hoc network**

A wireless ad hoc network is a decentralized wireless network.[1] The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity.

2. **Mobile ad hoc network**

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links

3.. List of ad hoc routing protocols

An ad hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network

1 Pro-active (table-driven) routing
2 Reactive (on-demand) routing
3 Flow-oriented routing
4 Adaptive (situation-aware) routing
5 Hybrid (both pro-active and reactive) routing
6 Hierarchical routing protocols
7 Host Specific Routing protocols
8 Geographical routing protocols
9 Power-aware routing protocols
10 Multicast routing
11 Geographical multicast protocols (Geocasting)

4. Define P2P

P2P networking has generated tremendous interest worldwide among both Internet surfers and computer networking professionals. P2P software systems like Kazaa and Napster rank amongst the most popular software applications ever. Numerous businesses and Web sites have promoted "peer to peer" technology as the future of Internet networking.

5.What Are P2P Software Applications?

A good definition of P2P software was proposed by Dave Winer of UserLand Software many years ago when P2P was first becoming mainstream. Dave suggests that P2P software applications include these seven key characteristics: the user interface runs outsides of a Web browser
computers in the system can act as both clients and servers
the software is easy to use and well-integrated

the application includes tools to support users wanting to create content or add functionality
the application makes connections with other users
the application does something new or exciting
the software supports "cross-network" protocols like SOAP or XML-RPC
the user interface runs outsides of a Web browser
computers in the system can act as both clients and servers
the software is easy to use and well-integrated
the application includes tools to support users wanting to create content or add functionality
the application makes connections with other users
the application does something new or exciting

6. Define mobility models

Mobility models represent the movement of mobile users, and how their location, velocity and acceleration change over time. Such models are frequently used for simulation purposes when new communication or navigation techniques are investigated. Mobility management schemes for mobile communication systems make use of mobility models for predicting future user positions

7. Define Dynamic Source Routing

Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting computer requests one. However, it uses source routing instead of relying on the routing table at each intermediate device. Many successive refinements have been made to DSR,.

PART- B (16 MARKS)

1. Explain about wireless adhoc network

. A wireless ad hoc network is a decentralized wireless network.[1] The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity.
Wireless ad hoc networks can be further classified by their application:
mobile ad hoc networks (MANETs)
wireless mesh networks
wireless sensor networks.
Medium Access Control

In most wireless ad hoc networks, the nodes compete to access the shared wireless medium, often resulting in collisions (interference). Using cooperative wireless communications improves immunity to interference by having the destination node

combine self-interference and other-node interference to improve decoding of the desired signal.
Simulation of Wireless Ad Hoc Networks

One key problem to Wireless Ad Hoc networks is foreseeing the variety of possible situations that can occur. As a result, Modeling and Simulation using extensive parameter sweeping and what-if analysis becomes an extremely important paradigm for use in ad hoc networks. Traditional M&S tools for modeling and simulation include the likes of NS2 (and recently NS3), Opnet, Omnet++. However, these tools focus primarily on the simulation of the entire protocol stack of the system. Although that can be important in the proof of concept implementations of systems, the need for a more advanced simulation methodology is always there. Agent-Based Modeling and Simulation offers such a paradigm. Not to be confused with multi-agent systems and intelligent agents, agent-based modeling[5] originated from social sciences, where the goal was to evaluate and view large-scale systems with numerous interacting "AGENT" or components in a wide variety of random situations to observe global phenomena. Unlike traditional AI systems with Intelligent agents, agent-based modeling is similar to the real world. Agent-based models are thus effective in modeling bio-inspired and nature-inspired systems. In these systems, the basic interactions of the components the system, also called Complex Adaptive System, are simple but result in advanced global phenomena such as emergence. Another approach to simulation of wireless sensor networks and other ad hoc networks, is to use FABS (Formal Agent-Based Simulation framework) a framework for the modeling of Wireless Sensor Networks and a Complex Adaptive Environment

2. Explain about Mobile ad hoc network
A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links.[1]

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.

Such networks may operate by themselves or may be connected to the larger Internet.

MANETs are a kind of wireless ad hoc networks that usually has a routeable networking environment on top of a Link Layer ad hoc network. They are also a type of mesh network, but many mesh networks are not mobile or not wireless.

The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid- to late 1990s. Many academic papers evaluate protocols and abilities assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other and usually with nodes sending

data at a constant rate. Different protocols are then evaluated based on the packet drop rate, the overhead introduced by the routing protocol, and other measures.
Types of MANET
Vehicular Ad Hoc Networks (VANETs) are used for communication among vehicles and between vehicles and roadside equipment.
Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents, drunken driving etc.
Internet Based Mobile Ad hoc Networks (iMANET) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal ad hoc routing algorithms don't apply directly.
Practical use

One Laptop per Child program has developed a laptop making use of an IEEE 802.11s based ad hoc wireless mesh networking chip.

In September 2007, the Swedish company TerraNet AB presented a mesh network of mobile phones that allowed calls and data to be routed between participating handsets, without cell sites

3. Explain ad hoc routing protocols
An ad hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network.

In ad hoc networks, nodes do not start out familiar with the topology of their networks; instead, they have to discover it. The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbours. Each node learns about nodes nearby and how to reach them, and may announce that it, too, can reach them.

Note that in a wider sense, ad hoc protocol can also be used literally, that is, to mean an improvised and often impromptu protocol established for a specific purpose
Pro-active (table-driven) routing

This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. The main disadvantages of such algorithms are:
Respective amount of data for maintenance.
Slow reaction on restructuring and failures.

Examples of pro-active algorithms are:
AWDS (Ad hoc Wireless Distribution Service) - Layer 2 wireless mesh routing protocol, LGPL implementation available, http://awds.berlios.de/

Babel, a protocol inspired by DSDV with faster convergence and ETX link quality estimation. Free implementation available.
CGSR (Clusterhead Gateway Switch Routing protocol) - CHING-CHUAN CHIANG, HSIAO-KUANG WU, WINSTON LIU, MARIO GERLA Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel, IEEE Singapore International Conference on Networks, SICON'97, pp. 197-211, Singapore, 16.-17. April 1997, IEEE
DFR ("Direction" Forward Routing) - YENG-ZHONG LEE, MARIO GERLA, JASON CHEN, JIWEI CHEN, BIAO ZHOU AND ANTONIO CARUSO, Ad Hoc & Sensor Wireless Networks, Volume 2, Number 2, 2006.
DBF (Distributed Bellman-Ford Routing Protocol) - DIMITRI P. BERTSEKAS, ROBERT G. GALLAGER, Distributed Asynchronous Bellman-Ford Algorithm, Data Networks, pp. 325-333, Prentice Hall, Enlgewood Cliffs, 1987, ISBN 0-13-196825-4
DSDV (Highly Dynamic Destination-Sequenced Distance Vector routing protocol) - C. E. PERKINS, P. BHAGWAT Highly Dynamic Destination-Sequenced Distance Vector (DSDV) for Mobile Computers Proc. of the SIGCOMM 1994 Conference on Communications Architectures, Protocols and Applications, Aug 1994, pp 234-244.
Guesswork - TOM PARKER AND KOEN LANGENDOEN, Guesswork: Robust Routing in an Uncertain World, to be presented at the 2nd IEEE International Conference on Mobile Ad hoc and Sensor Systems (MASS 2005), November 2005 http://www.st.ewi.tudelft.nl/~koen/papers/guesswork.pdf
HSR (Hierarchical State Routing protocol) - Guangyu Pei and Mario Gerla and Xiaoyan Hong AND Ching-Chuan Chiang, A Wireless Hierarchical Routing Protocol with Group Mobility, IEEE WCNC'99, New Orleans, USA, September 1999. http://wiki.uni.lu/secan-lab/Hieracical+State+Routing.html
IARP (Intrazone Routing Protocol/pro-active part of the ZRP) - ZYGMUNT J. HAAS, MARC R. PEARLMAN, PRINCE SAMAR The Intrazone Routing Protocol (IARP) for Ad Hoc Networks, Internet Draft, http://tools.ietf.org/html/draft-ietf-manet-zone-iarp, work in progress, July 2002.
LCA (Linked Cluster Architecture) - M. GERLA, J. T. TSAI Multicluster, Mobile, Multimedia Radio Network ACM Wireless Networks, VOl 1, No.3, 1995, pp. 255-265
MMRP (Mobile Mesh Routing Protocol) - K. GRACE Mobile Mesh Routing Protocol (MMRP), http://www.mitre.org/work/tech_transfer/mobilemesh/
OLSR (Optimized Link State Routing Protocol) - PHILIPPE JACQUET, PAUL MUHLETHALER, AMIR QAYYUM, ANIS LAOUITI, LAURENT VIENNOT, THOMAS CLAUSEN Optimized Link State Routing Protocol (OLSR), RFC 3626. http://www.olsr.net/, http://www.olsr.org/, http://qolsr.lri.fr/
TBRPF (Topology Dissemination based on Reverse-Path Forwarding routing protocol) - BHARGAV BELLUR, RICHARD G. OGIER, FRED L. TEMPLIN Topology Dissemination Based on Reverse-Path Forwarding (TBRPF), RFC 3684, February 2004.
WAR (Witness Aided Routing) - Aron, I.D. and Gupta, S., 1999, "A Witness-Aided Routing Protocol for Mobile Ad Hoc Networks with Unidirectional Links", Proc. of the First International Conference on Mobile Data Access, p.24-33.

WRP (Wireless Routing Protocol) - SHREE MURTHY, J.J. GARCIA-LUNA-AVECES A Routing Protocol for Packet Radio Networks, Proc. ACM International Conference on Mobile Computing and Networking, pp. 86-95, November, 1995. Citeseer: murthy95routing; SHREE MURTHY, J.J. GARCIA-LUNA-AVECES, An Efficient Routing Protocol for Wireless Networks, AACM/Baltzer Journal on Mobile Networks and Applications, Special Issue on Routing in Mobile Communication Networks, Vol. 1, No. 2, pp 183-197, ACM, October 1996
[edit]
Reactive (on-demand) routing

This type of protocols finds a route on demand by flooding the network with Route Request packets. The main disadvantages of such algorithms are:
High latency time in route finding.
Excessive flooding can lead to network clogging.

Examples of reactive algorithms are:
ESAODV (Extra Secure Ad Hoc On Demand Vector) - S. Mandala, M. A. Ngadi, A.H. Abdullah and A.S Ismail, "A Variant of Merkle Signature Scheme to Protect AODV Routing Protocol, Recent Trends in Wireless and Mobile Networks", in Communications in Computer and Information Science (Springer), 2010, Volume 84, Part 1, 87-98, DOI: 10.1007/978-3-642-14171-3_8, http://www.springerlink.com/content/p835026219u46303/fulltext.pdf
RSRP: Robust Secure Routing Protocol - Syed Rehan Afzal, Subir Biswas, Jong-bin Koh, Taqi Raza, Gunhee Lee, and Dong-kyoo Kim, RSRP: A Robust Secure Routing Protocol for Mobile Ad hoc Networks, Proceedings of Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE , vol., no., pp.2313-2318, March 31 2008-April 3 2008, http://ieeexplore.ieee.org/iel5/4489030/4489031/04489439.pdf
SENCAST - P. Appavoo and K. Khedo, SENCAST: A Scalable Protocol for Unicasting and Multicasting in a Large Ad hoc Emergency Network, International Journal of Computer Science and Network Security, Vol.8 No.2, February 2008
Multirate Ad hoc On-demand Distance Vector Routing Protocol - R. Guimaraes and Ll. Cerda, Improving reactive routing on wireless multirate ad hoc networks, In: Proceedings of 13th European Wireless 2007, https://upcommons.upc.edu/e-prints/bitstream/2117/1173/1/mr-aodv.pdf
Reliable Ad hoc On-demand Distance Vector Routing Protocol - Sandhya Khurana, Neelima Gupta, Nagender Aneja, http://doi.ieeecomputersociety.org/10.1109/ICNICONSMCL.2006.183
Minimum Exposed Path to the Attack (MEPA) in Mobile Adhoc Network (MANET) - Sandhya Khurana, Neelima Gupta, Nagender Aneja, http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/4196186/4196187/04196209.pdf?tp=&isnumber=4196187&arnumber=4196209
Ant-based Routing Algorithm for Mobile Ad Hoc Networks - Mesut Günes et al., ARA - the ant-colony based routing algorithm for manets, In Stephan Olariu, editor, Proceedings of the 2002 ICPP Workshop on Ad Hoc Networks (IWAHN 2002), pages 79-85, IEEE Computer Society Press, August 2002, http://www.adhoc-nets.de

Admission Control enabled On demand Routing (ACOR) - N. Kettaf, A. Abouaissa, T. Vuduong and P. Lorenz, http://tools.ietf.org/html/draft-kettaf-manet-acor, July 2006, (Work in progress)]

Ariadne - Y. Chu, A. Perrig, D. Johnson, Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks, Proc. ACM Conf. Mobile Computing and Networking (MobiCom), 2002. http://sparrow.ece.cmu.edu/~adrian/projects/secure-routing/ariadne.pdf

Associativity-Based Routing - CHAI-KEONG TOH: A Novel Distributed Routing Protocol To Support Ad hoc Mobile Computing, Proc. IEEE 15th Annual International Phoenix Conference on Computers and Communications, IEEE IPCCC 1996, 27 March-29, Phoenix, AZ, USA, pp. 480-486 / CHAI-KEONG TOH: Long-lived Ad Hoc Routing based on the Concept of Associativity, Internet Draft, March 1999, Expired, http://tools.ietf.org/html/draft-ietf-manet-longlived-adhoc-routing - US PATENT 5,987,011 http://www.patentstorm.us/patents/5987011.html

Ad hoc On-demand Distance Vector(AODV) - C. PERKINS, E.ROYER AND S. DAS Ad hoc On-demand Distance Vector (AODV) Routing, RFC 3561

Ad hoc On-demand Multipath Distance Vector - M. Marina, S. Das: On-demand Multipath Distance Vector Routing in Ad Hoc Networks, Proceedings of the 2001 IEEE International Conference on Network Protocols (ICNP), pages 14--23, IEEE Computer Society Press, 2001.

Backup Source Routing - SONG GUO, OLIVER W. YANG Performance of Backup Source Routing (BSR) in mobile ad hoc networks p 440-444, Proc. 2002 IEEE Wireless Networking Conference

CHAMP - CacHing And MultiPath routing - ALVIN C. VALERA, WINSTON K.G. SEAH AND S.V. RAO, Cooperative Packet Caching and Shortest Multipath Routing in Mobile Ad hoc Networks, Proceedings of 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), Mar 30-Apr 3, 2003. Available from: http://homepages.ecs.vuw.ac.nz/~winston/papers/Infocom2003-CHAMP.pdf

Dynamic Source Routing - DAVID JOHNSON, DAVID MALTZ, YIH-CHUN HU: The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks for IPv4, RFC 4728 / DAVID B. JOHNSON, DAVID A. MALTZ: Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing, Thomasz Imielinski and Hank Korth (Editors), Vol. 353, Chapter 5, pp. 153-181, Kluwer Academic Publishers, 1996

Flow State in the Dynamic Source Routing - YIH-CHUN HU, DAVID B. JOHNSON, DAVID A. MALTZ Flow State in the Dynamic Source Routing Protocol Internet Draft, http://tools.ietf.org/html/draft-ietf-manet-dsrflow, work in progress, June 2001.

Dynamic NIx-Vector Routing - Young J. Lee and George F. Riley, Dynamic NIx-Vector Routing for Mobile Ad Hoc Networks. Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2005), New Orleans, Mar. 13 - 17, 2005.

DYnamic Manet On-demand Routing - I. Chakeres AND C. Perkins: Dynamic MANET On-demand Routing Protocol (DYMO), Internet Draft, http://tools.ietf.org/html/draft-ietf-manet-dymo, work in progress, June 2008. RFC 4728

Mobile Ad hoc On-Demand Data Delivery Protocol - Humayun Bakht and Others: Mobile Ad hoc On-Demand Data Delivery Protocol (MAODDP), http://www.webcitation.org/query?url=http://www.geocities.com/humayunbakht/MAODDP1.html&date=2009-10-26+00:15:57
On-Demand Routing in Mobile Ad Hoc Network,gesj.internet-academy.org.ge/download.php?id=1634.pdf&t=1
Routing Protocols in Mobile Ad Hoc Networks,http://www.actapress.com/Abstract.aspx?paperId=21877
A secure routing protocol for ad hoc networks based on trust,http://www.computer.org/portal/web/csdl/doi/10.1109/ICNS.2007.18
[edit]
Flow-oriented routing

This type of protocols finds a route on demand by following present flows. One option is to unicast consecutively when forwarding data while promoting a new link. The main disadvantages of such algorithms are:
Takes long time when exploring new routes without a prior knowledge.
May refer to entitative existing traffic to compensate for missing knowledge on routes.

Examples of flow oriented algorithms are:
GB (Gafni-Bertsekas), E. Gafni, D. Bertsekas: Distributed Algorithms for Generating Loop-free Routes in Networks with Frequently Changing Topology, IEEE Transactions on Communication, Vol. 29, No. 1, Jan, 1981, pp.11-15. The first Link Reversal Routing (LRR) algorithm.
IERP (Interzone Routing Protocol/reactive part of the ZRP) - ZYGMUNT J. HAAS, MARC R. PEARLMAN, PRINCE SAMAR The Interzone Routing Protocol (IERP) for Ad Hoc Networks, Internet Draft, http://tools.ietf.org/html/draft-ietf-manet-zone-ierp, work in progress, July 2002.
LBR (Link life Based routing), B. S. Manoj, R. Ananthapadmanabha, and C. Siva Ram Murthy, "Link life Based Routing Protocol for Ad hoc Wireless Networks", Proc. of The 10th IEEE International Conference on Computer Communications 2001 (IC3N 2001), October 2001.
LMR (Lightweight Mobile Routing protocol) - M.S. CORSON AND A. EPHREMIDES Lightweight Mobile Routing protocol (LMR), A distributed routing algorithm for mobile wireless networks, Wireless Networks 1 (1995).A Link Reversal Routing (LRR) algorithm.
LQSR (Link Quality Source Routing) - Microsoft Version of DSR with Link Quality Metrics, http://research.microsoft.com/mesh/
LUNAR (Lightweight Underlay Network Ad hoc Routing) - CHRISTIAN TSCHUDIN AND RICHARD GOLD Lightweight Underlay Network Ad hoc Routing (LUNAR), http://cn.cs.unibas.ch/projects/lunar/
MOR - Multipath On-demand Routing Protocol, Biagioni and Chen, A reliability layer for ad hoc wireless sensor network routing, [1]

MPRDV (Multipoint Relay Distance Vector protocol) - Géraud Allard, Philippe Jacquet and Laurent Viennot. "Ad hoc routing with multipoint relaying", http://gyroweb.inria.fr/~viennot/postscripts/algotel2003ajv.pdf
QuaSAR (QoS aware source initiated ad hoc routing) - QuaSAR has both reactive and proactive mechanisms that aim to diminish the communication disruption time experienced in highly mobile ad hoc networks. Knut-Helge Vik and Sirisha Medidi, "Quality of Service aware source initiated ad hoc routing", 1st IEEE International Conference on Sensor and Ad hoc Communications and Networks; Santa Clara, CA, USA; October 2004 [2].
RDMAR (Relative-Distance Micro-discovery Ad hoc Routing protocol) - G. AGGELOU, R. TAFAZOLLI Relative Distance Micro-discovery Ad Hoc Routing (RDMAR) protocol Internet Draft, http://tools.ietf.org/html/draft-ietf-manet-rdmar, work in progress, September 1999.
SrcRR DSR and ETX based, optimized for performance D. AGUAYO, J. BICKET, R. MORRIS, "SrcRR: A High-Throughput Routing Protocol for 802.11 Mesh Networks (DRAFT)", http://pdos.csail.mit.edu/~rtm/srcrr-draft.pdf
SSR (Signal Stability Routing protocol) - R. DUBE, C. D. RAIS, K. WANG, AND S. K. TRIPATHI Signal Stability based adaptive routing (SSR alt SSA) for ad hoc mobile networks, IEEE Personal Communication, Feb. 1997.
PLBR (Preferred link based routing) -- R. S. Sisodia, B. S. Manoj, and C. Siva Ram Murthy, "A Preferred Link Based Routing Protocol for Ad Hoc Wireless Networks", Journal of Communications and Networks, Vol. 4, No. 1, pp. 14-21, March 2002
VRR (Vehicular Reactive Routing protocol) - Martin Koubek, Susan Rea, Dirk Pesch, "A Novel Reactive Routing Protocol for Applications in Vehicular Environments", in The 11th International Symposium on Wireless Personal Multimedia Communications (WPMC 2008), Finland, 2008. ISSN 1883-1192
[edit]
Adaptive (situation-aware) routing

This type of protocols combines the advantages of proactive and of reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. Some metrics must support the choice of reaction. The main disadvantages of such algorithms are:
Advantage depends on amount of nodes activated.
Reaction to traffic demand depends on gradient of traffic volume.

An example of adaptive algorithms is:
TORA (Temporally-ordered routing algorithm routing protocol) V. Park, S. Corson: Temporally-Ordered Routing Algorithm (TORA) Version 1, Functional Specification, Internet Draft, IETF MANET Working Group, June 2001, [3]. A Link Reversal Routing (LRR) algorithm.
[edit]
Hybrid (both pro-active and reactive) routing

This type of protocols combines the advantages of proactive and of reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The choice for one or the other method requires predetermination for typical cases. The main disadvantages of such algorithms are:
Advantage depends on amount of nodes activated.
Reaction to traffic demand depends on gradient of traffic volume.

Examples of hybrid algorithms are:
ARPAM, specialized for aeronautical MANETs.
HRPLS (Hybrid Routing Protocol for Large Scale Mobile Ad Hoc Networks with Mobile Backbones) - Ashish Pandey, Md. Nasir Ahmed, Nilesh Kumar, P. Gupta: A Hybrid Routing Scheme for Mobile Ad Hoc Networks with Mobile Backbones, IEEE International Conference on High Performance Computing, HIPC 2006, pp. 411-423, Dec 2006.
HSLS (Hazy Sighted Link State routing protocol) - Uses a mathematical optimization to mix link state and reactive routing to optimize network data updates in space and time, CESAR SANTIVANEZ AND RAM RAMANATHAN Hazy Sighted Link State routing protocol (HSLS), BBN Technical Memorandum No. 1301, 31 August 2001. [4] There's an open-source version.
HWMP (Hybrid Wireless Mesh Protocol) - default mandatory routing protocol for 802.11s. HWMP is inspired by a combination of AODV (RFC 3561[2]) and tree-based proactive routing. Guenael Strutt: HWMP Specification Update. The Working Group for WLAN Standards of the Institute of Electrical and Electronics Engineers. 14 November 2006 [5]
OORP (OrderOne Routing Protocol) - proactive/reactive distance vector combined with a hierarchy that is not used to route data. Patented. OrderOne Networks
SSR (Scalable Source Routing) - Based on the idea of "pushing Chord into the underlay". Routes messages along a virtual ring. Thomas Fuhrmann, Pengfei Di, Kendy Kutzner, and Curt Cramer: Pushing Chord into the Underlay: Scalable Routing for Hybrid MANETs Universität Karlsruhe (TH), Fakultät für Informatik, Technical Report 2006-12, June 2006 [6]
TORA, see below.
ZRP (Zone Routing Protocol) - ZYGMUNT J. HAAS, MARC R. PEARLMAN, PRINCE SAMAR The Zone Routing Protocol (ZRP) for Ad Hoc Networks, Internet Draft, http://tools.ietf.org/html/draft-ietf-manet-zone-zrp, work in progress, July 2002. ZRP uses IARP as pro-active and IERP as reactive component.
[edit]
Hierarchical routing protocols

With this type of protocols the choice of proactive and of reactive routing depends on the hierarchic level where a node resides. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding on the lower levels. The choice for one or the other method requires proper attributation for respective levels. The main disadvantages of such algorithms are:

Advantage depends on depth of nesting and addressing scheme.
Reaction to traffic demand depends on meshing parameters.

Examples of hierarchical routing algorithms are:
CBRP (Cluster Based Routing Protocol) - M. JIANG, J. LI, Y. C. TAY Cluster Based Routing Protocol (CBRP) Functional Specification Internet Draft, http://tools.ietf.org/html/draft-ietf-manet-cbrp-spec, work in progress, June 1999.
CEDAR (Core Extraction Distributed Ad hoc Routing) - RAGHUPATHY SIVAKUMAR, PRASUN SINHA, VADUVUR BHARGHAVAN Core Extraction Distributed Ad hoc Routing (CEDAR) Specification, Internet Draft, http://tools.ietf.org/html/draft-ietf-manet-cedar-spec; PRASUN SINHA, RAGHUPATHY SIVAKUMAR, VADUVUR BHARGHAVAN CEDAR: A Core-Extraction Distributed Ad Hoc Routing Algorithm, The 18th Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM '99 New York, NY, USA, pp. 202-209 IEEE, March 1999
DART (Dynamic Address Routing) - JAKOB ERIKSSON, MICHALIS FALOUTSOS, SRIKANTH KRISHNAMURTHY Scalable Ad Hoc Routing: The Case for Dynamic Addressing, in proceedings of INFOCOM 2004. Project website http://dart.cs.ucr.edu
DDR (Distributed Dynamic Routing Algorithm) - NAVID NIKAEIN, HOUDA LABIOD, CHRISTIAN BONNET Distributed Dynamic Routing Algorithm (DDR) for Mobile Ad Hoc Networks, in proceedings of the MobiHOC 2000 : First Annual Workshop on Mobile Ad Hoc Networking & Computing http://www.eurecom.fr/~nikaeinn/ddr.ps
FSR (Fisheye State Routing protocol) - MARIO GERLA, GUANGYU PEI, XIAOYAN HONG, TSU-WEI CHEN Fisheye State Routing Protocol (FSR) for Ad Hoc Networks Internet Draft, http://tools.ietf.org/html/draft-ietf-manet-fsr, work in progress, June 2001. (see http://wiki.uni.lu/secan-lab/Fisheye+State+Routing.html)
GSR (Global State Routing protocol) - Global State Routing protocol (GSR) [Chen98] Tsu-Wei Chen and Mario Gerla, "Global State Routing: A New Routing Scheme for Ad hoc Wireless Networks" Proc. IEEE ICC'98, Atlanta, GA, USA, June 1998, pp. 171-175. http://citeseer.ist.psu.edu/60636.html; [Iwata99] A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, "Scalable Routing Strategies for Ad Hoc Wireless Networks" IEEE Journal on Selected Areas in Communications, Special Issue on Ad Hoc Networks, Aug. 1999, pp.1369-79. http://www.cs.ucla.edu/NRL/wireless/PAPER/jsac99.ps.gz
HARP (Hybrid Ad Hoc Routing Protocol) - NAVID NIKAEIN, CHRISTIAN BONNET, NEDA NIKAEIN Hybrid Ad Hoc Routing Protocol - HARP, in proceeding of IST 2001: International Symposium on Telecommunications http://www.eurecom.fr/~nikaeinn/harp.ps
[edit]
Host Specific Routing protocols

This type of protocols requires thorough administration to tailor the routing to a certain network layout and a distinct flow strategy. The main disadvantages of such algorithms are:

Advantage depends on quality of administration addressing scheme.
Proper reaction to changes in topology demands reconsidering all parametrizing.
HSR (Hierarchical State Routing) - Scalable Routing Strategies for Ad Hoc Wireless Networks
LANMAR (Landmark Routing Protocol for Large Scale Networks) - MARIO GERLA, XIAOYAN HONG, LI MA, GUANGYU PEI Landmark Routing Protocol (LANMAR) Internet Draft, http://tools.ietf.org/html/draft-ietf-manet-lanmar-05, work in progress, June 2001.
ATR (Augmented Tree-based Routing) - MARCELLO CALEFFI, GIANCARLO FERRAIUOLO, LUIGI PAURA Augmented Tree-based Routing Protocol for Scalable Ad Hoc Networks, in proceedings of MHWMN 2007: The Third IEEE International Workshop on Heterogeneous Multi-Hop Wireless and Mobile Networks. http://arxiv.org/abs/0711.3099 - Multi-path DHT-based routing protocol for scalable networks.

[edit]

Geographical routing protocols

This type of protocols acknowledges the influence of physical distances and distribution of nodes to areas as significant to network performance. The main disadvantages of such algorithms are:
Efficiency depends on balancing the geographic distribution versus occurrence of traffic.
Any dependence of performance with traffic load thwarting the negligence of distance may occur in overload.

[edit]

Power-aware routing protocols

Energy required to transmit a signal is approximately proportional to d^{α}, where d is the distance and is the attenuation factor or path loss exponent, which depends on the transmission medium. When $\alpha = 2$ (which is the optimal case), transmitting a signal half the distance requires one fourth of the energy and if there is a node in the middle willing to spend another fourth of its energy for the second half, data would be transmitted for half of the energy than through a direct transmission - a fact that follows directly from the inverse square law of physics.

The main disadvantages of such algorithms are:
This method induces a delay for each transmission.
No relevance for energy network powered transmission operated via sufficient repeater infrastructure.

[edit]

Multicast routing

MRMP (Maximum-Residual Multicast Protocol) - Pi-Cheng Hsiu and Tei-Wei Kuo: "A Maximum-Residual Multicast Protocol for Large-Scale Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, 2009 Available from: http://ieeexplore.ieee.org/xpls/pre_abs_all.jsp?isnumber=4358975&arnumber=4796204

OBAMP (Overlay, Boruvka-based, Ad hoc multicast Protocol) - Andrea Detti, Nicola Blefari-Melazzi: "Overlay, Boruvka-based, Ad hoc multicast Protocol: description and performance analysis", Wireless Communications and Mobile Computing, Wiley, 2008 Available from: http://netgroup.uniroma2.it/Andrea_Detti/obamp/index.html
EraMobile (Epidemic-based Reliable and Adaptive Multicast) - Zulkuf Genc and Oznur Ozkasap: "EraMobile: Epidemic-based Reliable and Adaptive Multicast for MANETs", In Proc. of the Wireless Communications and Networking Conference (WCNC), Hong Kong, China, March 2007. Available from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=4224245&arnumber=4225046&count=810&index=800
AQM (Ad Hoc QoS Multicast) - Kaan Bür and Cem Ersoy: "Ad Hoc Quality of Service Multicast Routing", Elsevier Science Computer Communications, vol. 29, no. 1, pages 136 - 148, December 2005.
ExOR (wireless network protocol) - Opportunistic Multi-Hop Routing for Wireless Networks; Sanjit Biswas, Robert Morris, 2005; Uses standard 802.11 radios. Tested, and now seems to be commercially available from Meraki, a start-up company founded by the authors.
SMF (Simplified Multicast Forwarding) - Joseph Macker, editor, SMF Design Team: "Simplified Multicast Forwarding for MANET", work in progress, Available from http://tools.ietf.org/html/draft-ietf-manet-smf.
PUMA (Protocol for Unified Multicasting Through Announcements) - Vaishampayan, Ravindra. and Garcia-Luna-Aceves, J.J.: " Efficient and Robust Multicast Routing in Mobile Ad Hoc Networks", In 2004 IEEE International Conference on Mobile Ad hoc and Sensor Systems, pages 304- 313, Fort Lauderdale, FL, October 2004. Available from: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1392169. A NS-2 implementation by Sidney Doria is available in: <http://puma-adhoc.cvs.sourceforge.net/puma-adhoc/Puma/>.
SPBM (Scalable Position-Based Multicast) - Matthias Transier, Holger Füßler, Jörg Widmer, Martin Mauve, and Wolfgang Effelsberg: "Scalable Position-Based Multicast for Mobile Ad hoc Networks", In Proc. of the 1st International Workshop on Broadband Wireless Multimedia: Algorithms, Architectures and Applications (BroadWim), San José, CA, October 2004.Available from: http://www.informatik.uni-mannheim.de/pi4/publications/Transier2004c.pdf. A NS-2 implementation available from:http://www.informatik.uni-mannheim.de/pi4/projects/pbm/kernel.html
MOLSR (Multicast Optimized Link State Routing) - Anis Laouiti, Philippe Jacquet, Pascale Minet, Laurent Viennot, Thomas Clausen, Cedric Adjih: "Multicast Optimized Link State Routing", INRIA research report,RR-4721, Feb 2003 (http://www.inria.fr/rrrt/rr-4721.html).
DCMP (Dynamic Core Based Multicast Routing Protocol) - Subir Kumar Das, B. S. Manoj, and C. Siva Ram Murthy: "A Dynamic Core Based Multicast Routing Protocol for Ad hoc Wireless Networks", In Proc. of the 3rd ACM International Symposium on Mobile and Ad hoc Networking & Computing (MobiHOC), pages 24 - 35, Lausanne, Switzerland, June 2002.

SRMP (Source Routing-based Multicast Protocol) - Hasnaa Moustafa and Houda Labiod: "SRMP: A Mesh-based Protocol for Multicast Communication in ad hoc networks", In Proc. of the 2002 International Conference on Third Generation Wireless and Beyond, pages 43 - 48, San Francisco, CA, May 2002.
ADMR (Adaptive Demand-Driven Multicast Routing) - Jorjeta G. Jetcheva and David B. Johnson: "Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks", In Proc. of the 2nd ACM International Symposium on Mobile and Ad hoc Networking & Computing (MobiHOC), pages 33 - 44, Long Beach, CA, October 2001.
DDM (Differential Destination Multicast) - Lusheng Ji and M. Scott Corson: "Differential Destination Multicast-A MANET Multicast Routing Protocol for Small Groups", In Proc. of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), pages 1192 - 1202, Anchorage, AK, April 2001.
DSR-MB (Simple Protocol for Multicast and Broadcast using DSR) - Jorjeta G. Jetcheva, Yih-Chun Hu, David A. Maltz, and David B. Johnson: "A Simple Protocol for Multicast and Broadcast in Mobile Ad Hoc Networks", http://tools.ietf.org/html/draft-ietf-manet-simple-mbcast (outdated), July 2001.
MZR (Multicast Zone Routing) - Vijay Devarapalli, Ali A. Selcuk, and Deepinder Sidhu: "MZR: A Multicast Protocol for Mobile Ad Hoc Networks", In Proc. of the IEEE International Conference on Communications (ICC), pages 886 - 891, Helsinki, Finland, June 2001.
ABAM (On-Demand Associativity-Based Multicast) - Chai-Keong Toh, Guillermo Guichal, and Santithorn Bunchua: "On-demand associativity-based multicast routing for ad hoc mobile networks (ABAM)", In Proc. of the 52nd IEEE VTS Vehicular Technology Conference (VTC) 2000 Fall, vol. 3, pages 987 - 993, Boston, MA, September 2000.
CBM (Content Based Multicast) - Hu Zhou and Suresh Singh: "Content based multicast (CBM) in ad hoc networks", In Proc. of the 1st ACM International Symposium on Mobile and Ad hoc Networking & Computing (MobiHOC), pages 51 - 60, Boston, MA, August 2000.
AMRoute (Adhoc Multicast Routing Protocol) - Mingyan Liu, Rajesh R. Talpade, Anthony McAuley, and Ethendranath Bommaiah: "AMRoute: Adhoc Multicast Routing Protocol", University of Maryland CSHCN Technical Report 1999-1, College Park, MD, 1999.
AMRIS (Ad hoc Multicast Routing protocol utilizing Increasing id-numberS) - Chun Wei Wu and Yong Chiang Tay: "AMRIS: A Multicast Protocol for Ad Hoc Wireless Networks", In Proc. of the IEEE Military Communications Conference (MILCOM), pages 25 - 29, Atlantic City, NJ, November 1999.
BEMRP (Bandwidth-Efficient Multicast Routing Protocol) - T. Ozaki, Jaime Bae Kim and T. Suda: "Bandwidth-efficient multicast routing protocol for ad hoc networks", In Computer Communications and Networks, 1999. Proceedings. Eight International Conference, pages 10-17, Boston, MA, September 1999.
CAMP (Core-Assisted Mesh Protocol) - J. J. Garcia-Luna-Aceves and Ewerton L. Madruga: "The Core Assisted Mesh Protocol", IEEE Journal on Selected Areas in

Communications, Special Issue on Ad Hoc Networks, vol. 17, no. 8, pages 1380 - 1394, August 1999.
MCEDAR (Multicast Core-Extraction Distributed Ad hoc Routing) - Prasun Sinha, Raghupathy Sivakumar, and Vaduvur Bharghavan: "MCEDAR: Multicast Core-Extraction Distributed Ad hoc Routing", In Proc. of the Wireless Communications and Networking Conference (WCNC), pages 1313 - 1317, New Orleans, LA, September 1999.
ODMRP (On-Demand Multicast Routing Protocol) - Sung-Ju Lee, Mario Gerla, and Ching-Chuan Chiang: "On-Demand Multicast Routing Protocol", In Proc. of the Wireless Communications and Networking Conference (WCNC), pages 1298 - 1302, New Orleans, LA, September 1999. Available from: http://www.cs.ucla.edu/NRL/wireless/PAPER/odmrp-wcnc99.ps.gz
MAODV (Multicast Ad hoc On-Demand Distance Vector routing) - Elizabeth M. Royer and Charles E. Perkins: "Multicast Operation of the Ad hoc On-Demand Distance Vector Routing Protocol", In Proc. of the 5th annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), pages 207 - 218, Seattle, WA, August 1999.
FGMP (Forwarding Group Multicast Protocol) - Ching-Chuan Chiang, Mario Gerla, and Lixia Zhang: "Forwarding Group Multicast Protocol (FGMP) for Multihop, Mobile Wireless Networks", ACM-Baltzer Journal of Cluster Computing: Special Issue on Mobile Computing, vol. 1, no. 2, pages 187 - 196, December 1998.
LAM (Lightweight Adaptive Multicast) - Lusheng Ji and M. Scott Corson: "A Lightweight Adaptive Multicast Algorithm", In Proc. of the IEEE Global Telecommunications Conference (Globecom), pages 1036 - 1042, Sydney, Australia, November 1998.
[edit]
Geographical multicast protocols (Geocasting)
LBM (Location Based Multicast) - Y.KO AND VAIDYA 1998 Location Based Multicast (LBM)
Voronoi Diagram and Convex Hull Based Geocasting - IVAN STOJMENOVIC AND ANAND PRAJKASH RUHIL AND D. K. LOBIYAL, Voronoi diagram and convex hull based geocasting and routing in wireless networks, Wirel. Commun. Mob. Comput. 2006; 6:247–258
GeoGRID (Geographical GRID (see GLS)) - WEN-HWA LIAO AND JANG-PING SHEU AND YU-CHEE TSENG GeoGRID & Geographical GRID: A Fully Location-Aware Routing Protocol for Mobile Ad Hoc Networks, Telecommunication Systems 2001,volume 18, number 1-3, pages 37-60
GeoTORA (Geographical TORA (see TORA)) - Y. KO AND N. VAIDYA A protocol for geocasting in mobile ad hoc networks (GeoTORA) Tech. Rep. 00-010, Dept. of Computer Science, Texas A&M University, March 2000. 23
MRGR (Mesh-Based Geocast Routing) - BOLENG, CAMP AND TOLETY 2001 Mesh-Based Geocast Routing (MRGR)
MOBICAST (Mobile Just-in-time Multicasting) - Q. Huang, C. Lu and G-C. Roman, Mobicast: Just-in-time multicast for sensor networks under spatiotemporal constraints, Lecture Notes in Computer Science, Vol 2634, pages 442-457

Abiding Geocast / Stored Geocast (Time Stable Geocasting) - C. Maihöfer, T. Leinmüller, E. Schoch: Abiding Geocast: Time-Stable Geocast for Ad Hoc Networks,

4.Explain in detail about peer to peer networks

P2P networking has generated tremendous interest worldwide among both Internet surfers and computer networking professionals. P2P software systems like Kazaa and Napster rank amongst the most popular software applications ever. Numerous businesses and Web sites have promoted "peer to peer" technology as the future of Internet networking.

Although they have actually existed for many years, P2P technologies promise to radically change the future of networking. P2P file sharing software has also created much controversy over legality and "fair use." In general, experts disagree on various details of P2P and precisely how it will evolve in the future.

Traditional Peer to Peer Networks

The P2P acronym technically stands for peer to peer. Webopedia defines P2P as "A type of network in which each workstation has equivalent capabilities and responsibilities. This differs from client/server architectures, in which some computers are dedicated to serving the others."

"A type of network in which each workstation has equivalent capabilities and responsibilities. This differs from client/server architectures, in which some computers are dedicated to serving the others."

This definition captures the traditional meaning of peer to peer networking. Computers in a peer to peer network are typically situated physically near to each other and run similar networking protocols and software. Before home networking became popular, only small businesses and schools built peer to peer networks.

Home Peer to Peer Networks

Most home computer networks today are peer to peer networks. Residential users configure their computers in peer workgroups to allow sharing of files, printers and other resources equally among all of the devices. Although one computer may act as a file server or Fax server at any given time, other home computers often have equivalent capability to handle those responsibilities.

Both wired and wireless home networks qualify as peer to peer environments. Some may argue that the installation of a network router or similar centerpiece device means that network is no longer peer to peer. From the networking point of view, this is inaccurate. A router simply joins the home network to the Internet; it does not by itself change how resources within the network are shared.

P2P File Sharing Networks

When most people hear the term "P2P", they think not of traditional peer networks, but rather peer to peer file sharing over the Internet. P2P file sharing systems have become the single most popular class of Internet applications in this decade.

A P2P network implements search and data transfer protocols above the Internet Protocol (IP). To access a P2P network, users simply download and install a suitable P2P client application.

Numerous P2P networks and P2P software applications exist. Some P2P applications work only with one P2P network, while others operate cross-network. Likewise, some P2P networks support only one application, while others support multiple applications.

What Are P2P Software Applications?

A good definition of P2P software was proposed by Dave Winer of UserLand Software many years ago when P2P was first becoming mainstream. Dave suggests that P2P software applications include these seven key characteristics: the user interface runs outsides of a Web browser

computers in the system can act as both clients and servers

the software is easy to use and well-integrated

the application includes tools to support users wanting to create content or add functionality

the application makes connections with other users

the application does something new or exciting

the software supports "cross-network" protocols like SOAP or XML-RPC

the user interface runs outsides of a Web browser

computers in the system can act as both clients and servers

the software is easy to use and well-integrated

the application includes tools to support users wanting to create content or add functionality

the application makes connections with other users

the application does something new or exciting

the software supports "cross-network" protocols like SOAP or XML-RPC

In this modern view of peer to peer computing, P2P networks stretch across the entire Internet, not just a home local area network (LAN). Easy-to-use P2P software applications allow both geeks and non-technical people to participate.

Kazaa, Napster and More P2P Software Applications

The original MP3 file sharing system, Napster became the world's most popular Internet software application literally overnight. Napster typified the new "modern" P2P system defined above: a simple user interface running outside of the browser supporting both file serving and downloads. Furthermore, Napster offered chat rooms to connect its millions of users and performs a new and exciting (in the sense of "controversial") service.

The name Napster referred both to the P2P network and the file sharing client that it supported. Besides being limited at the beginning to a single client application, Napster employed a proprietary network protocol, but thess technical details did not materially affect its popularity.

When the original unregulated Napster service was shut down, a number of P2P systems competed for that audience. Most Napster uses migrated to the Kazaa and Kazaa Lite software applications and the FastTrack network. FastTrack grew to become even larger than the original Napster network.

Kazaa has suffered from its own legal troubles, but various other systems, like eDonkey / Overnet, have continued the legacy of free P2P file sharing software

5. Define mobility models and briefly explain them

Mobility models represent the movement of mobile users, and how their location, velocity and acceleration change over time. Such models are frequently used for simulation purposes when new communication or navigation techniques are investigated. Mobility management schemes for mobile communication systems make use of mobility models for predicting future user positions.

Background and terminology

In the study of a new Mobile ad hoc network protocol, it is important to simulate the protocol and evaluate its protocol performance. Protocol simulation has several key parameters, including mobility model and communicating traffic pattern.[1] Mobility models characterize user movement patterns, i.e. the different behaviors of subscribers. Traffic models describe the condition of the mobile services.

Mobility models

For mobility modelling, the behaviour or activity of a user's movement can be described using both analytical and simulation models. The input to analytical mobility models are simplifying assumptions regarding the movement behaviors of users. Such models can provide performance parameters for simple cases through mathematical calculations. In contrast, simulation models consider more detailed and realistic mobility scenarios. Such models can derive valuable solutions for more complex cases. Typical mobility models include

Brownian model
random waypoint model
random walk model
random direction model
random Gauss-Markov model
Markovian model
incremental model,
mobility vector model
reference point group model (RPGM)
pursue model
nomadic community model
column model
fluid flow model
exponential correlated random model
map based model

6. Explain about DSR

Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting computer

requests one. However, it uses source routing instead of relying on the routing table at each intermediate device. Many successive refinements have been made to DSR,

Determining source routes requires accumulating the address of each device between the source and destination during route discovery. The accumulated path information is cached by nodes processing the route discovery packets. The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each device the packet will traverse. This may result in high overhead for long paths or large addresses, like IPv6. To avoid using source routing, DSR optionally defines a flow id option that allows packets to be forwarded on a hop-by-hop basis.

This protocol is truly based on source routing whereby all the routing information is maintained (continually updated) at mobile nodes. It has only two major phases, which are Route Discovery and Route Maintenance. Route Reply would only be generated if the message has reached the intended destination node (route record which is initially contained in Route Request would be inserted into the Route Reply).

To return the Route Reply, the destination node must have a route to the source node. If the route is in the Destination Node's route cache, the route would be used. Otherwise, the node will reverse the route based on the route record in the Route Reply message header (this requires that all links are symmetric). In the event of fatal transmission, the Route Maintenance Phase is initiated whereby the Route Error packets are generated at a node. The erroneous hop will be removed from the node's route cache; all routes containing the hop are truncated at that point. Again, the Route Discovery Phase is initiated to determine the most viable route.

For information on other similar protocols, see the ad hoc routing protocol list.

Dynamic source routing protocol (DSR) is an on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach. The major difference between this and the other on-demand routing protocols is that it is beacon-less and hence does not require periodic hello packet (beacon) transmissions, which are used by a node to inform its neighbors of its presence. The basic approach of this protocol (and all other on-demand routing protocols) during the route construction phase is to establish a route by flooding RouteRequest packets in the network. The destination node, on receiving a RouteRequest packet, responds by sending a RouteReply packet back to the source, which carries the route traversed by the RouteRequest packet received.

Consider a source node that does not have a route to the destination. When it has data packets to be sent to that destination, it initiates a RouteRequest packet. This RouteRequest is flooded throughout the network. Each node, upon receiving a RouteRequest packet, rebroadcasts the packet to its neighbors if it has not forwarded

it already, provided that the node is not the destination node and that the packet's time to live (TTL) counter has not been exceeded. Each RouteRequest carries a sequence number generated by the source node and the path it has traversed. A node, upon receiving a RouteRequest packet, checks the sequence number on the packet before forwarding it. The packet is forwarded only if it is not a duplicate RouteRequest. The sequence number on the packet is used to prevent loop formations and to avoid multiple transmissions of the same RouteRequest by an intermediate node that receives it through multiple paths. Thus, all nodes except the destination forward a RouteRequest packet during the route construction phase. A destination node, after receiving the first RouteRequest packet, replies to the source node through the reverse path the RouteRequest packet had traversed. Nodes can also learn about the neighboring routes traversed by data packets if operated in the promiscuous mode (the mode of operation in which a node can receive the packets that are neither broadcast nor addressed to itself). This route cache is also used during the route construction phase. If an intermediate node receiving a RouteRequest has a route to the destination node in its route cache, then it replies to the source node by sending a RouteReply with the entire route information from the source node to the destination node.

Advantages and disadvantages

This protocol uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach. In a reactive (on-demand) approach such as this, a route is established only when it is required and hence the need to find routes to all other nodes in the network as required by the table-driven approach is eliminated. The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead. The disadvantage of this protocol is that the route maintenance mechanism does not locally repair a broken link. Stale route cache information could also result in inconsistencies during the route reconstruction phase. The connection setup delay is higher than in table-driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility. Also, considerable routing overhead is involved due to the source-routing mechanism employed in DSR. This routing overhead is directly proportional to the path length.

.UNIT-IV ISSUES AND CHALLENGES
partA&B

1. Explain power management

Power management is a feature of some electrical appliances, especially copiers, computers and computer peripherals such as monitors and printers, that turns off the power or switches the system to a low-power state when inactive. In computing this is known as PC power management and is built around a standard called ACPI. This supersedes APM. All recent (consumer) computers have ACPI support.
Processor level techniques

The power management for microprocessors can be done over the whole processor, or in specific areas.

With dynamic voltage scaling and dynamic frequency scaling, the CPU core voltage, clock rate, or both, can be altered to decrease power consumption at the price of potentially lower performance. This is sometimes done in real time to optimize the power-performance tradeoff.

Examples:
AMD Cool'n'Quiet
AMD PowerNow! [1]
IBM EnergyScale [2]
Intel SpeedStep
Transmeta LongRun and LongRun2
VIA LongHaul (PowerSaver)

Additionally, processors can selectively power off internal circuitry (power gating). For example:
Newer Intel Core processors support ultra-fine power control over the functional units within the processors.
AMD CoolCore technology get more efficient performance by dynamically activating or turning off parts of the processor.[3]

Intel VRT technology split the chip into a 3.3V I/O section and a 2.9V core section. The lower core voltage reduces power consumption.
Operating system level: Hibernation
Main article: Hibernation (computing)

When a computer system hibernates it saves the contents of the RAM to disk and powers down the machine. On startup it reloads the data. This allows the system to be completely powered off while in hibernate mode. This requires a file the size of the installed RAM to be placed on the hard disk, potentially using up space even when

not in hibernate mode. Hibernate mode is enabled by default in some versions of Windows and can be disabled in order to recover this disk space.

2. Explain about Voice over IP

Voice over Internet Protocol (Voice over IP, VoIP) is any of a family of methodologies, communication protocols, and transmission technologies for delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms frequently encountered and often used synonymously with VoIP are IP telephony, Internet telephony, voice over broadband (VoBB), broadband telephony, and broadband phone.

Internet telephony refers to communications services — voice, fax, SMS, and/or voice-messaging applications — that are transported via the Internet, rather than the public switched telephone network (PSTN). The steps involved in originating a VoIP telephone call are signaling and media channel setup, digitization of the analog voice signal, encoding, packetization, and transmission as Internet Protocol (IP) packets over a packet-switched network. On the receiving side similar steps reproduce the original voice stream.[1]

VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codecs which encode speech allowing transmission over an IP network as digital audio via an audio stream. The codec used is varied between different implementations of VoIP (and often a range of codecs are used); some implementations rely on narrowband and compressed speech, while others support high fidelity stereo codecs.
Protocols

Voice over IP has been implemented in various ways using both proprietary and open protocols and standards. Examples of technologies used to implement Voice over IP include:
H.323
IP Multimedia Subsystem (IMS)
Media Gateway Control Protocol (MGCP)
Session Initiation Protocol (SIP)
Real-time Transport Protocol (RTP)
Session Description Protocol (SDP)

The H.323 protocol was one of the first VoIP protocols that found widespread implementation for long-distance traffic, as well as local area network services. However, since the development of newer, less complex protocols, such as MGCP and SIP, H.323 deployments are increasingly limited to carrying existing long-haul network traffic. In particular, the Session Initiation Protocol (SIP) has gained widespread VoIP market penetration.

A notable proprietary implementation is the Skype protocol, which is in part based on the principles of peer-to-peer networking

Benefits
Operational cost

VoIP can be a benefit for reducing communication and infrastructure costs. Examples include:
Routing phone calls over existing data networks to avoid the need for separate voice and data networks.[12]
Conference calling, IVR, call forwarding, automatic redial, and caller ID features that traditional telecommunication companies (telcos) normally charge extra for, are available free of charge from open source VoIP implementation
Securing VoIP

To prevent the above security concerns government and military organizations are using Voice over Secure IP (VoSIP), Secure Voice over IP (SVoIP), and Secure Voice over Secure IP (SVoSIP) to protect confidential and classified VoIP communications.[29] Secure Voice over IP is accomplished by encrypting VoIP with Type 1 encryption. Secure Voice over Secure IP is accomplished by using Type 1 encryption on a classified network, like SIPRNet.[30][31][32][33][34] Public Secure VoIP is also available with free GNU programs
3. explain about computer security
Computer security is a branch of computer technology known as information security as applied to computers and networks. The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users. The term computer system security means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively. The strategies and methodologies of computer security often differ from most other computer technologies because of its somewhat elusive objective of preventing unwanted computer behavior instead of enabling wanted computer behavior

Security by design
Main article: Security by design

The technologies of computer security are based on logic. As security is not necessarily the primary goal of most computer applications, designing a program with security in mind often imposes restrictions on that program's behavior.

There are 4 approaches to security in computing, sometimes a combination of approaches is valid:

Trust all the software to abide by a security policy but the software is not trustworthy (this is computer insecurity).
Trust all the software to abide by a security policy and the software is validated as trustworthy (by tedious branch and path analysis for example).
Trust no software but enforce a security policy with mechanisms that are not trustworthy (again this is computer insecurity).
Trust no software but enforce a security policy with trustworthy hardware mechanisms.

Many systems have unintentionally resulted in the first possibility. Since approach two is expensive and non-deterministic, its use is very limited. Approaches one and three lead to failure. Because approach number four is often based on hardware mechanisms and avoids abstractions and a multiplicity of degrees of freedom, it is more practical. Combinations of approaches two and four are often used in a layered architecture with thin layers of two and thick layers of four.

There are various strategies and techniques used to design security systems. However there are few, if any, effective strategies to enhance security after design. One technique enforces the principle of least privilege to great extent, where an entity has only the privileges that are needed for its function. That way even if an attacker gains access to one part of the system, fine-grained security ensures that it is just as difficult for them to access the rest.

Furthermore, by breaking the system up into smaller components, the complexity of individual components is reduced, opening up the possibility of using techniques such as automated theorem proving to prove the correctness of crucial software subsystems. This enables a closed form solution to security that works well when only a single well-characterized property can be isolated as critical, and that property is also assessible to math. Not surprisingly, it is impractical for generalized correctness, which probably cannot even be defined, much less proven. Where formal correctness proofs are not possible, rigorous use of code review and unit testing represent a best-effort approach to make modules secure.

The design should use "defense in depth", where more than one subsystem needs to be violated to compromise the integrity of the system and the information it holds. Defense in depth works when the breaching of one security measure does not provide a platform to facilitate subverting another. Also, the cascading principle acknowledges that several low hurdles does not make a high hurdle. So cascading several weak mechanisms does not provide the safety of a single stronger mechanism.

Subsystems should default to secure settings, and wherever possible should be designed to "fail secure" rather than "fail insecure" (see fail-safe for the equivalent in safety engineering). Ideally, a secure system should require a deliberate, conscious, knowledgeable and free decision on the part of legitimate authorities in order to make it insecure.

In addition, security should not be an all or nothing issue. The designers and operators of systems should assume that security breaches are inevitable. Full audit trails should be kept of system activity, so that when a security breach occurs, the mechanism and extent of the breach can be determined. Storing audit trails remotely, where they can only be appended to, can keep intruders from covering their tracks. Finally, full disclosure helps to ensure that when bugs are found the "window of vulnerability" is kept as short as possible.

UNIT-V SIMULATION
PART-A &B

1. explain glomosim

Global Mobile Information System Simulator (GloMoSim) is a network protocol simulation software that simulates wireless and wired network systems.[1] GloMoSim is designed using the parallel discrete event simulation capability provided by Parsec, a parallel programming language.[2] GloMoSim currently supports protocols for a purely wireless network.
It uses the Parsec compiler to compile the simulation protocols.
Parsec
Parsec is a C-based simulation language, developed by the Parallel Computing Laboratory at UCLA, for sequential and parallel execution of discrete-event simulation models.
Commercial version
GloMoSim is academic research version available for academic use only. Commercial GloMoSim Based Product is QualNet.

2. Explain NS2

Ns is a discrete event simulator targeted at networking research. Ns provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks.

Ns began as a variant of the REAL network simulator in 1989 and has evolved substantially over the past few years. In 1995 ns development was supported by DARPA through the VINT project at LBL, Xerox PARC, UCB, and USC/ISI. Currently ns development is support through DARPA with SAMAN and through NSF with CONSER, both in collaboration with other researchers including ACIRI. Ns has always included substantal contributions from other researchers, including wireless code from the UCB Daedelus and CMU Monarch projects and Sun Microsystems. For documentation on recent changes, see the version 2 change log.
The Network Simulator - ns

Ns-2 is a discrete event simulator targeted at networking research. Ns-2 provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks. For more information see the Ns Users FAQ.

Ns-2 is written in C++ and an Object oriented version of Tcl called OTcl.

To get started, see:
Linux/BSD/OS X: Downloading and installing ns-2
Windows: Running Ns and Nam Under Windows 9x/2000/XP Using Cygwin
Getting Started with NS-2

To begin modifying Ns-2 for your own needs:

Understanding the NS framework

Outside Links
Official ns-2 website
nsnam Sourceforge project

See Nsnam:about for more information on this wiki and what it deals with.
The Network Animator - nam

Nam is a Tcl/TK based animation tool for viewing network simulation traces and real world packet traces. It is mainly intended as a companion animator to the ns simulator

3. explain about OPNET

Network Simulation using OPNET

Simulation Modeling is becoming an increasingly popular method for network performance analysis. We review here one such tool to understand the working and performance of a network

Network managers and researchers design certain topologies, protocols and algorithms, the effectiveness of which can be decided by simulation. The proposed designs cannot be directly fielded with existing infrastructure without testing of compatibility with it.

The network simulator provides a test bed by simulating the real world network. A number of network simulation tools are available in the market like NS-2, GloMoSim, QualNet, NetSim, OPNET, etc.Direct Hit!
Applies To: Network Designers and Researchers
Price: Free (Academic edition)
USP: Model the behavior of Network
Primary Link: http://www. opnet.com
Keywords: OPNET

OPNET is a graphical user interface (GUI) based network simulation tool which is simple to install and use. It comes with a good documentation and is available for installation on Windows.

We reviewed the OPNET IT Guru academic edition for network simulation and analysis. The user interface would be found self explanatory by those having basic knowledge of computer networking. OPNET's GUI provides an easy way to develop models for network, different hardware devices and protocols. This tool supports most of the network types and technologies like LAN, ATM, Frame Relay, WAN,

Wireless Networks etc. It allows designing scenarios based on these technologies and simulating them. It also provides outputs in form of plots and simulation data. OPNET uses a wizard to help you choose the devices you want to use in your network design.

For the purpose of simulation it provides various models of different type of network devices like hubs, bridges, switches, routers and servers from many network vendors like Cisco, Nortel, 3Com, Bay Networks, Cabletron, HP, Juniper, Lucent, NEC and many more.

It also allows to drag and drop in the workspace and use printers, workstations, different types of links like 1000BaseX, 1000BaseT, 100BaseT, 10G, Fast Ethernet, OC links, SONET etc available in its library for network designing.

Getting started
The OPNET IT Guru academic edition of the software can be freely downloaded and installed after online registration with OPNET.

The size of the setup file is 50.3 MB. During installation it requires online activation of the license.

A detailed step-wise process of installation is available at www.opnet.com/itguru-acaemic/instructions.html.

Designing network scenarios
For the purpose of demo we would be first creating a WAN with a centralized server and analyse its performance based on CPU utilization, link utilization, etc.
Object Palette displays all the models of products available in OPNET's library for the selected technologies and vendors

Start OPNET, open a new project and give a suitable name for the project and scenario. Create an empty scenario and select a suitable network scale among World, Enterprise, Campus, Office, Logical, maps. We would select 'enterprise'.

Then select the required technologies and vendors. This will lead to the display of all products related to the technology and the vendor available in OPNET's library. Drag and drop the products and links from object palette into workspace to design the network.A generated network scenario

This way we can complete one scenario. This network can be analysed for various parameters like CPU utilisation, bandwidth utilization, throughput, etc.

Performance analysis

Performance analysis can be seen in two ways – one using plot and another through result data table. Here we generated another scenario of a similar WAN simulated above but with distributed cache servers and compared the performance of the server in these two scenarios.

A comparative graph on point to point throughput for two scenarios.