ICS 2306: COMPUTER NETWORKS

1. **BBT 2201 Data Communication and Networks**
   Data communication: transmission media, modes of transmission, modulation and demodulation; Information coding, communications software and protocols, error detection and correction. Networks: topology and architecture of computer networks. Layered protocols: Open Systems Interconnection (OSI) model and Transmission Control Protocol/IP protocols. Other network standards. LAN, WAN, routing protocols, gateways.

2. **Brief Content for ICS 2306: Computer Networks**
   Topology and architecture of computer networks. Layered protocols. OSI and TCP/IP protocols. Local area networks. Wide area networks. Routing protocols. Gatewaying.

3. **Brief Content for BIT 2108: Computer Networks**
   Type of networks: peer to peer, client server. Network topologies: bus, star, ring and hierarchical setups. Network hardware and software. Management. Data communications. Hardware components. Communications: bits and baud rates and media. Synchronous, asynchronous, parallel and serial transmission modes. Modulation and demodulation. Communications protocols and architecture. Messages, circuit and packet switching. Examples of standard network architecture.

4. **HBT 2105: Data communication and networks**
   Data communication: transmission media, modes of transmission, modulation and demodulation; Information coding, communications software and protocols, error detection and correction. Networks: topology and architecture of computer networks. Layered protocols: Open Systems Interconnection (OSI) model and Transmission Control Protocol/IP protocols. Other network standards. LAN, WAN, routing protocols, gateways.

5. OVERVIEW

Objectives

- Understand the basic principles of data communication and computer networks
- Appreciate the complex trade-offs that are inherent in the design of networks
- Provide a guide tour of network technologies from the lowest levels of data transmission up to network applications
- Learn about current network technologies especially Internet protocols

Recommended texts

- Computer Networks and Internets by Douglas E. Comer, Prentice Hall 2nd ed

Supplementary texts

- Tannenbaum, Computer Networks, Prentice Hall
- Halsall, Data and Computer Communications, Macmillan

What is a computer network?

- An interconnection of autonomous computers (as opposed to communication between separate but interdependent parts of a single computer)

Some goals of computer networks

- Access to remote resources
- Human communication
- Mobile computing
- Computing power through parallelism
- Optimizing resources – load balancing
- Incremental growth of computer systems (reduced cost and risk)
- Increased robustness through graceful degradation

Uses of computer networks

- Email, www, video conferencing, file transfer, collaborative virtual environment, remote control of robots and machines, dial up databases, webcasting, distributed programs, hacking, banking, internet telephone

Classifying networks

- By size – LANs vs. WANs
- By connectivity – p2p vs. broadcast networks
- By communication medium
- My mobility – fixed vs. mobile
-
-

Size – differences between local and wide area networks

- Speed – bandwidth and latency
- Management
- Security
- Reliability
- Billing
- Heterogeneity (and standards)

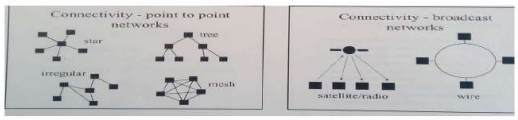
Connectivity – p2p networks

- Star
- Tree
- Irregular
- Mesh

Connectivity – broadcast networks

- Satellite/radio

- Wire etc



Medium – differences between communication media
- "speed" – bandwidth and latency
- Range
- Sharing
- Topology
- Installation and maintenance costs
- Reliability

Mobility – issues arising in mobile networks
- Mobile networking has emerged in the last years. Introduces new issues of:
  - Location and tracking
  - Semi-persistent connections
  - Complex administration and billing as devices and users move around the network

Common issues in networking
- Addressing
- Routing
- Framing and decoding
- Error detection and correction
- Flow and congestion

CHAPTER 1: DATA TRANSMISSION

Transmission media

All computer communication involves encoding data in a form of energy and sending the energy across a transmission medium. Examples include electric current transferring data across wire and radio waves through the air. Some of the common media include:

i. **Copper wire –** is the primary medium to connect computers since it is inexpensive and easy to install. Its low resistance allows signals to travel farther. The wiring style is chosen to minimize interference that arises due to electrical signal travelling across a wire i.e. the wire emits some electromagnetic energy that travels through the air and when it meets the effect of another wire, some electric current is generated in the wire. This is worse for wires running in parallel. Such generated current may be strong enough to prevent normal communication.

   Networks therefore use two types of wiring schemes to minimize interference:

   a. **Twisted pair –** also used in telephone. Each wire is coated with an insulating material and twisted together. Such twists change the electrical properties of the wire making it suitable for use because the twists help
      - prevent electric currents on the wire from radiating energy that interfere with other wires and they also
      - prevent signals in other wires from interfering with the pair.

Fig. 1.1 Twisted pair cable

   b. **Coaxial cable –** provides more protection from interference than twisted pair. The metal shield (heavier) provides a barrier to electromagnetic radiation. Copper mesh is the metal shield.

Fig 1.2: Coaxial

The inner wire transmits and the outer wire returns. It provides more protection from interference than twisted pair. The metal shield (heavier) provides a barriers to electromagnetic radiation in both directions. There are also shielded twisted pair. Such shielded wiring is often used when wires from a network pass near equipment that generates strong electric or magnetic fields e.g. a large air conditioner.

ii. **Glass fibers (optical fiber) –** use light to transmit data. A miniature glass fiber is encased in a plastic jacket allowing the fiber to bend without breaking. A transmitter at one end of the fiber uses a light emitting diode (LED) or a laser to send pulses of light down the fiber while a receiver at the other end uses a light sensitive transistor to detect the pulses.

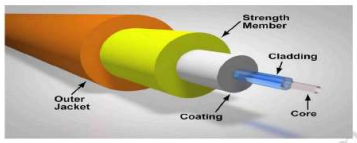
   Advantages over wires include:

   a. Because they use light, they neither cause electrical interference in other cables nor are they susceptible to the same.
   b. They carry light pulses farther since they can reflect most of the light inward.

c. They carry more information than wire since light encodes more information than electric current.
d. Light can travel over a single fiber unlike in case of wires which have to be in pairs for a complete electric circuit.

Disadvantages:

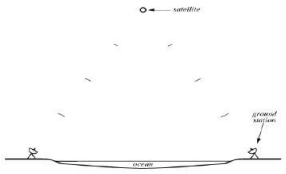
a. Installing fiber requires special equipment that polishes the ends to allow light to pass through (expensive)
b. If a fiber breaks inside the jacket, finding the location of the problem is difficult.
c. Repairing a broken fiber is difficult since it requires special equipment to join two fibers so that light can pass through the joint (expensive).



iii. **Radio –** such electromagnetic radiation can be used to transmit computer data. Such networks are said to operate at "radio frequency" commonly referred to as RF transmissions. They do not require a direct physical connection between computers, but each participating computer attaches to an antenna that both transmits and receives RF. Small antennas are enough for shorter distances e.g. 20cm while up to 2m may be required for across city communication.

iv. **Satellites –** radio transmissions do not bend around the surfaces of the earth but RF technology combined with satellites provides communication across longer distances. (See fig 1.3 below). The satellite contains a transponder that consists of a radio transmitter/receiver. The transponder receives a signal, amplifies it and sends it back in another direction. One satellite normally contains multiple transponders, between 6 to12 operating independently, and each transponder uses a different frequency (channel) thus making multiple communication to be possible simultaneously. This is because satellites are very expensive. The different forms of satellite grouped by height at which they orbit include:

a. **Geosynchronous satellites –** also called geostationary, are placed in an orbit that is exactly synchronized with the earth's rotation i.e. satellite remains exactly at the same position at all times. The height is normally approximately 36,000 km (20,000 miles) and this distance is usually determined by the laws of Physics. The angular separation of the satellites is normally 4 – 8 degrees depending on the power of the transmitter implying that 45 – 90 satellites e.g. on the Equator (360 degrees). Such satellites can be used to relay transmissions at all times since it stays at the same spot throughout.
b. **Low earth orbit satellites (LEO) –** approx. 200 – 400 miles above the earth's surface. They do not stay stationary since their period of rotation is faster than that of the earth, and this is their disadvantage. They can cover an entire orbit in 1.5 hours. Two problems are hereby implied: such satellites can only be used when its orbit passes between two ground stations, and, optimum utilization requires complex control systems that continuously move the ground stations so that they point directly at the satellite.
c. **Low earth orbit satellite arrays –** they are a set of satellite arrays in low earth orbit. Even though they orbit quickly, the set is chosen such that each point on the ground has at least one satellite overhead at any time (66 satellites are adequate for the entire earth's surface). In addition to transponders, they also have radio equipment to communicate with each other in the array to help in forwarding information.



v. **Microwave –** they are electromagnetic radiation beyond the frequency range used for radio and tv (wavelength ranging from 1m to as short as 1mm implying frequencies between 300MHz to 300GHz, includes UHF and EHF millimeter waves) and are used mainly by long-distance telephone companies. Their transmissions can be aimed in a single direction thus preventing others from intercepting the signal. They carry more information than lower frequency RF transmissions. They require a clear path between the transmitter and the receiver since they cannot penetrate metal structures. They also require mounting of two towers each aimed directly at the other i.e. transmitter aimed at receiver.

vi. **Infrared –** are electromagnetic radiation with longer wavelengths than those of visible light – frequency range of 430THz to 300GHz and are used in industrial, scientific and medical applications e.g. night vision devices. They are the wireless remote controls used with appliances such as TV and stereos. They are limited to a small area e.g. single room and require the transmitter to point at the receiver. They are comparatively inexpensive and require no antennas. A room equipped with a single infrared connection can provide network access to all computers in the room

vii. **Light from a laser –** Light Amplification by Simulated Emission of Radiation. Used in common consumer devices e.g. DVD players, laser printers, barcode scanners, laser surgery in medicine, various skin treatments in the industry for cutting/welding, in military for marking targets, and measuring range and speed. It is a beam of light that carries data through the air and requires two sites to have a transmitter and a receiver fixed on a tower. The transmitter uses a laser to generate a beam of light because a coherent laser beam stays focused over a long distance. The disadvantage is that it cannot penetrate vegetation or snow or fog and so has limited use. It must travel in a straight line and must not be blocked.

CHAPTER 2: LOCAL ASYNCHRONOUS COMMUNICATION (RS-232)

The need for asynchronous communication
Communication is called asynchronous if the sender and receiver do not need to coordinate before data is transmitted i.e. sender and receiver do not synchronize before each transmission. Sender transmits data whenever it is available and receiver accepts data whenever it arrives. This is useful for devices e.g. keyboards where data is generated when keyboard is touched and no data flows when keyboard is idle.

Using electric current to send bits
Simplest electronic communication systems use a small electric current to encode data over electric wire eg negative voltage may represent 1 and positive 0. When a sender transmits a +ve voltage, receiver records 0 and vice versa. (See fig 2.1 below)

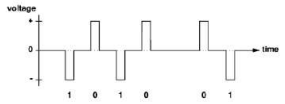


Fig. 2.1 Waveform diagram

Notice the delay between the 4th and 5th bits.

Standards for communication
Specifications for communication systems are standardized. International Telecommunications Union (ITU), Electronic Industries Association (EIA) and the IEEE publish specifications in documents known as standards. A standard specifies both the timing of signals and the electrical details of voltage and current. The EIA's RS-232-c (i.e. RS-232+) specifies details of physical connection e.g. connections must be <50ft long and voltage of -15 to+15 for data transmission. The RS-232 is designed for use with devices such as modems and terminals, keyboard etc. it specifies the transmission of characters. It can be used to send 8-bit characters but often configured so that each character consist of seven data bits. RS-232 defines serial asynchronous communication (serial because bits travel on the wire one after another) RS-232 never leaves a zero volts on the wire i.e. when there is no transmission, it leaves the wire with a –ve voltage => 1.

Baud rate, framing and errors
Baud defines the number of changes in the signal per second that the hardware generates. For RS-232 baud rate = the number of bits per second. Baud rate can be set manually or automatically.

Framing errors are the errors that occur if the stop bit does not occur exactly at the time expected.

The sending and receiving hardware must agree on the length of time the voltage will be held for each bit. Thus technically, transmission hardware is rated in baud. But usually to make RS-232 hardware more general, manufacturers usually design each piece of hardware to operate at a variety of baud rates. The baud rate can then be set either manually using switches in hardware installed in the computer or automatically by device driver software in the computer. After this, the sending and receiving hardware must be configured to use the same baud rate otherwise framing errors occur.

Full duplex asynchronous communication
All electric circuits require a minimum of two wires for current to flow to and fro. The send wire is often referred to as "ground" e.g. in coaxial, the center wire transmits and the shield provides the return path. Thus simultaneous transfer in two directions is referred to as full-duplex while single direction if half-duplex or simplex transmission. (See fig 2.2 below)

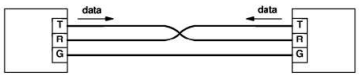


Fig 2.2: A diagram showing minimal wiring required for full-duplex RS-232 communication. Although the two wires carry data independently, it is possible for them to share a single ground wire.

Limitations of Real Hardware

Note that in practice, no electronic device produces an exact voltage or change from one voltage to another instantly. Also no wire conducts electricity perfectly i.e. there is energy loss as current travels down the wire. Therefore it takes a small time for the voltage to rise and fall and the signal received is not perfect (see fig. above). Thus standards for RS-232 specify how close to a perfect waveform a transmitter must emit and how tolerant of imperfection a receiver must be.

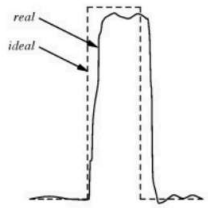


Fig 2.3: An illustration of the voltage emitted by a real device as it transmits a bit. In practice, voltages are often worse than this.

Hardware bandwidth and the transmission of bits

Defn: Bandwidth – the fastest continuously oscillating signal that can be sent across the hardware.

Each transmission system has a limited bandwidth which is the maximum rate at which the hardware can change a signal. It is measured in cycles per second, Hz.

A fundamental relationship exists between the bandwidth of a transmission system and the maximum number of bits per second that can be transferred over that system. This is Nyquist's sampling theorem (1920) which provides a theoretical bound on the maximum speed at which data can be sent. For RS-232 that uses two values of voltage to encode data, it states that the maximum data rates in bits per second that can be achieved over the transmission system of bandwidth B is 2B.

Generally, if the transmission system uses K possible values of voltage instead of two, it becomes

$D = 2B\log_2 K$,
D = maximum data rates in bits/second.

Effect of Noise in communication
Real communication systems are subject to small amounts of background interference called “noise” which make it impossible to achieve the theoretical maximum transmission rate.

Claude Shannon (1948) extended Nyquist’s theorem thus.

C = Blog2(1+S/N), effectively lower than Nyquist’s value.

C = effective limit in b/s
B = hardware bandwidth
S = average signal power
N = average noise power
S/N = signal-noise ratio

Long Distance Communication (Carriers, Modulation and Modems)

Sending signal across long distances
An electric signal cannot travel arbitrarily far over copper wire since current weakens with distance. This is called signal loss which occurs due to resistance in the wire causing small amounts of electrical energy converted to heat. Thus long distance communication systems send a continuously oscillating signal, usually a sine wave called a “carrier”. (See fig 2.4 below)

Fig 2.4: Sine wave. The carrier oscillates continuously even when no data is being sent.

To send data, a transmitter modifies the carrier slightly. This is called modulation. E.g. a radio station uses a continuous carrier wave that oscillates at an assigned frequency and uses an audio signal to modulate the wave. Receivers on the other side use it to reconstruct the original audio signal.

Network technologies use a variety of modulation techniques e.g. amplitude or frequency modulation, AM or FM., where AM varies the strength of the outgoing signal in proportion to the information being sent, while FM varies the frequency of the underlying carrier in proportion to the information being sent.

Modem hardware used for modulation and demodulation
A modem hardware is a device that modulates and demodulates implying that long-distance communication requires a modulator at one end and a demodulator at the other end. This is constructed in one gadget. (See fig 2.5 below).

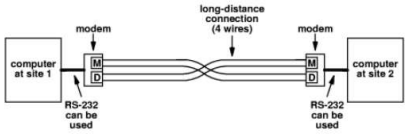


Fig 2.5: Four wires for long distance communication

NB: Users are forced to use leased lines as each cannot single handedly bear the costs i.e. utility companies provide the service to which you subscribe.

Carrier frequencies and multiplexing
Two or more signals that use different carrier frequencies can be transmitted over a single medium simultaneously without interference. In this case, frequency division multiplexing (FDM) can be applied to mean a network system that uses multiple carrier frequencies to allow independent signals to travel through a medium. It can be used to send signals over a wire, RF or optical fiber. (See fig 2.6 below)

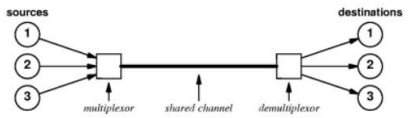


Fig 2.6: The concept of Frequency Division Multiplexing. Each pair of source and destination can send data over the shared channel without interference. In practice, each end requires a multiplexor and demultiplexor for 2-way communication, and a multiplexor may need circuitry to generate the carrier waves.

A minimum separation between carriers is maintained to keep off interference. Thus FDM is often used only in high-bandwidth transmission systems i.e. systems that can send a wide range of frequencies.

NB: There is also Wave Division Multiplexing (WDM) which operates by sending multiple light waves across a single optical fiber. At the receiving end, an optical prism is used to separate the frequencies. This is possible because light at a given frequency doesn't interfere with light at another frequency.

Time Division Multiplexing (TDM) – the general alternative to FDM in which sources sharing a medium take turns to use a channel.

Spread spectrum
Is a special case of frequency division multiplexing which involves the use of multiple carriers to improve reliability. Reasons for its use include: to improve reliability when the underlying transmission system has sporadic interference at some frequencies i.e. the transmitter is arranged to send the same signal on a set of frequencies and the receiver configured to check all carrier frequencies and to use whichever is presently working.

CHAPTER 3: PACKETS, FRAMES AND ERROR DETECTION

Concept of Packets

Packets are small blocks of data which the network divides and sends individually. Computer networks are often called "packet networks" or "packet switching networks "because they use packet technology. Sender and receiver need to coordinate transmission to ensure data arrives correctly. Multiple computers often share the underlying connections and hardware because the communication circuits and associated modem hardware are expensive. Packets help ensure fairness to every computer in a network over data transmission.

Packets and Time-Division Multiplexing

Time-division multiplexing is the process whereby a network permits many sources to take turns accessing a shared communication resource. (See fig. 4.1 below).

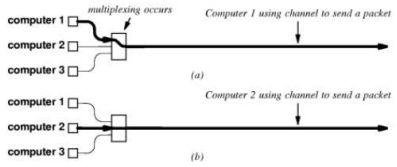


Fig: 4.1: Computers take turns to send packets

Packets and hardware frames

"Frame" denotes the definition of a packet used with a specific type of network. Blocks of data are sent in a frame.

NB: a disadvantage of "overhead" occurs in framing i.e. a framing scheme that delimits both the beginning and the end of each frame sends an extra unnecessary character between blocks of data. The chief advantage of sending a character at the beginning and ending of a frame is clear when one considers large delays and computers that crash.

Byte stuffing

Because network systems usually insert bits or bytes to change data for transmission, the technique is called "data stuffing". Byte stuffing and character stuffing thus refer to data stuffing used with character-oriented hardware. Bit stuffing refers to data stuffing used with bit –oriented hardware.

Transmission errors

Lightning, power surges and other electromagnetic interference can introduce unwanted electrical currents in the electronic components or wires used in the communication. Interference normally changes the signal used for transmission without damaging equipment. A change in electrical signal causes the receiver to misinterpret one or more bits of the data. These are termed "transmission errors".

Parity bits and parity checking

Use odd or even parity checks. The sender and receiver agree on whether to use odd or even parity check. The sender sends and the receiver computes if the bits arrived intact. The sender computes an extra bit and attaches it to bits being sent. The receiver then detaches it, this is the parity bit.

Probability, mathematics and error detection

Parity cannot detect transmission errors that change an even number of bits and all error detection methods are approximate and the goal is simply to produce a low probability of accepting corrupted data.

Detecting errors with checksums
Many computer network systems send a “checksum” along with each packet to help the receiver to detect errors. To compute a checksum, the sender treats data as a sequence of binary integers and computes their sum. If the sum grows larger than 16 bits, the carry bits are added into the final sum.

Advantage: the size and ease of computation.
Disadvantage: Not able to detect all common errors e.g. if a transmission error reverses a bit (0 => 1 or 1 => 0).

Detecting errors with Cyclic Redundancy Check (CRC)
This method can more detect errors than checksum. The hardware that calculates the CRC uses two simple components: a “shift register” and an “exclusive or” (XOR) unit. (See page 66 of the recommended text for more).

Combining the building blocks
Those interested in the method can check pg. 66 section 6.11 of the recommended text.

Burst errors
These are errors that involve changes to a small set of bits near a single location e.g. electrical interference such as lightning often produces burst errors as does electrical interference caused when an electric motor starts near a cable that carries data.

CHAPTER 4: LAN TECHNOLOGIES AND NETWORK TOPOLOGY

1. Direct Point-To-Point communication

Also known as mesh network was the first method used for computer communication in which each communication channel connected to exactly two computers. Its main three useful properties are:

- Because each connection is installed independently, appropriate hardware can be used.
- Because they have exclusive access the connected computers can decide exactly how to send data across the connection.
- Because only two computers have access to the channel, it is easy to enforce security and privacy.

The main disadvantage is that for each pair of computers, the number of connections grows quickly as the size of the set increases i.e.

Direct connections required = $(n^2-n)/2$ where n is the number of computers. Therefore it is expensive in this respect.

2. Shared communication channels

LANs therefore (discovered late 60s - early 70s) were devised as an alternative to the expensive dedicated p2p connections, by relying on sharing the network. The computers take turns to send packets across the medium.

Several LAN designs exist based on e.g. the voltages and modulation techniques used, and the approach to sharing i.e. mechanisms used to coordinate access and transmit packets. The net economic impact of sharing is reduced costs.

Shared networks are used only for local communication because:

- a large geographic separation between computers introduces delays.
- Providing a high bandwidth communication channel over long distances is expensive as compared to short distances,

3. Significance of LANs and Locality of Reference

The main reason for the demand of LANs can be attributed to the fundamental principle of computer networking referred to as "locality of reference". It states that "communication among a set of computers is not random but follows two patterns":

i. Temporal locality of reference: if a pair of computers communicate once, they are likely to communicate again and then periodically.
ii. Physical locality of reference: a computer tends to communicate most often with other computers that are nearby.

LAN Topologies

Implies the general shape of a LAN. Include the following:

i. Star Topology

In this case, all computers attach to a central point (see the fig below). The hub is an electronic device that accepts data from a sending computer and delivers it to the appropriate destination.