CS542 HW 3

1. Find Nyquist formula.

The Nyquist Theorem, is used for a digitization of analog signals. It is also known as the sampling theorem. For analog-to-digital conversion, slices called samples, of analog waveform must be taken. Sampling rate or sampling frequency is defined as number of samples per second.

Nyquist theorem is also used to avoid aliasing in prescription for the nominal sampling interval. The sampling frequency should be at least twice the highest frequency contained in the signal.
i.e. $F_s >= 2 F_c$
Here, F_s is sampling frequency and F_c is highest frequency in the signal. [1]

http://redwood.berkeley.edu/bruno/npb261/aliasing.pdf

a) What this theory can be used in communication network system?

1. It is used in sampling the signals by avoiding the aliasing effect.
2. It is used in intersymbol interference (ISI) for constructing band-limited functions to overcome the effects of intersymbol interference.
3. It is useful in audios and videos to convert signals from analog to digital and vice versa.
4. This theorem is used to calculate bit rate from bandwidth and number of bits.

b) How to estimate communication capacity?

Capacity of noiseless communication is derived by formulae,
$C = 2 * B * \log_2 L$
where B is the bandwidth of the channel, L is the number of signal levels used to represent data, and C is capacity in bits per second.

Capacity of noisy communication is derived by formulae,
$C = B \times \log2(1 + S/N)$
Where, C is capacity in bits per second, B is bandwidth of channel in Hertz and S/N is signal-to -noise ratio. This formula is used to calculate highest data rate for noisy channel. [2]

c) Sample question – Calculate capacity of noisy communication link with signal-to-noise ratio of 1?

It is calculated by following formula,
$C = B \times \log2(1 + S/N)$
$C = 1000 * \log_2 (1+1)$ ------- (B= 1000)

C = 2000 * 1
C = 2000 bps

2 Find a theorem to measure a link capacity with signal to noise level environment. Describe how it works.

For measuring link capacity of communication with signal to noise level environment, following formula is used:

C = B *x* log2(1 + S/N)
Where, C is capacity in bits per second, B is bandwidth of channel in Hertz and S/N is signal-to -noise ratio. This formula is used to calculate highest data rate for noisy channel.

This formula is derived by **Shannon–Hartley theorem.** It is maximum rate at which information can be transmitted over a communications channel of a specified bandwidth in the presence of noise. Also, it is a bound on the maximum amount of error-free information per time unit that can be transmitted with a specified bandwidth in the presence of the noise. This theorem is named after Claude Shannon and Ralph Hartley. [2]

3 What is a MAC protocol in data link layer and why do we need?

Media Access Control or Medium Access Control (MAC) sublayer is used to provide addressing and channel access control mechanisms which enable several terminals or network nodes to communicate in a network. It is the lower sublayer of the data link layer (layer 2) of the seven-layer OSI model. MAC sublayer provides addressing and channel access control method which is used for several network nodes to communicate within a shared medium (ethernet).

Multiple devices of same physical link can identify each other by using MAC address assigned to all ports on switch.MAC algorithm accepts a secret key as input and an arbitrary-length message, and outputs a MAC address (12digit hexadecimal number). MAC addresses are usually written in one of these formats:

- MM:MM:MM:SS:SS:SS
- MM-MM-MM-SS-SS-SS

The first half is ID of adapter manufacturer. Second half is adapter serial number.

- MAC is used as an interface between ethernet sublayer of logical link control (LLC) and network's physical layer.
- MAC creates logical communication channel which may provide unicast, multicast, or broadcast communication service.
- MAC is used for Frame delimiting and recognition.
- MAC is used for Addressing of destination stations.
- MAC is used for Protection against errors, generally by means of generating and checking frame check sequences.
- MAC is used to Control the access to the physical transmission medium. [3]

4 Find various MAC protocols and their main characteristics, and how they work.

Multiple nodes share a communication medium for transmitting their data packets. The medium access control (MAC) protocol is primarily responsible for regulating access to the shared medium.

Protocols used for wired network-

CSMA/CD- In CSMA/CD, 4sender first senses the medium to determine whether it is idle or busy. If it is found busy, the sender refrains from transmitting packets. If the medium is idle, the sender can initiate data transmission. CSMA/CD requires that sender aware of collisions and attempts to avoid collisions in the first place.

Token bus - is a network implementing the token ring protocol over a "virtual ring" on a coaxial cable.[1] A token is passed around the network nodes and only the node possessing the token may transmit. If a node doesn't have anything to send, the token is passed on to the next node on the virtual ring. Each node must know the address of its neighbor in the ring, so a special protocol is needed to notify the other nodes of connections to, and disconnections from, the ring.

Token Ring - It uses a special three-byte frame called a "token" that travels around a logical "ring" of workstations or servers. This token passing is a channel access method providing fair access for all stations, and eliminating the collisions of contention-based access methods. Stations on a token ring LAN are logically organized in a ring topology with data being transmitted sequentially from one ring station to the next with a control token circulating around the ring controlling access.

Token passing- token passing is a channel access method where a signal called a token is passed between nodes to authorize that node to communicate. The most well-known examples are token ring and ARCNET.

Protocols used for wireless network-

CSMA/CA (CSMA with Collision Avoidance)- In this, nodes sense the medium, but do not immediately access the channel when it is found idle. Instead, a node waits for a time period called DCF interframe space (DIFS) plus a multiple of a slot size λ in case there are multiple nodes attempting to access the medium, the one with the shorter back-off period will win

In **ALOHA**, node can access the channel as soon as it is ready. In this, more than one node can transmit at the same time which causes collision.
ALOHA uses acknowledgments to confirm the success of a broadcast data transmission. It allows nodes to access the medium immediately. It addresses collisions with approaches such as exponential back-off to increase the likelihood of successful transmissions

In **slotted ALOHA**, it requires that a station may commence transmission only at predefined points in time (the beginning of a time slot) and λ introduces the need for synchronization among nodes.

Dynamic TDMA – a scheduling algorithm dynamically reserves a variable number of time slots in each frame to variable bit-rate data streams, based on the traffic demand of each data stream**.** It is used in HIPERLAN/2 broadband radio access network, IEEE 802.16a WiMax, Bluetooth, Military Radios, TD-SCDMA, ITU-T G.hn and Simulation of TDMA / DTMA links

Reservation ALOHA - It is a channel access method for wireless (or other shared channel) transmission that allows uncoordinated users to share a common transmission resource. Reservation ALOHA (and its parent scheme, Slotted ALOHA) is a schema or rule set for the division of transmission resources over fixed time increments, also known as slots. If followed by all devices, this scheme allows the channel's users to cooperatively utilize a shared transmission resource.

Mobile Slotted Aloha (**MS-Aloha**) – It is a wireless network protocol proposed for applications such as vehicle networks. MS-Aloha needs a periodic frame structure, including fixed-length time slots which represent the distinct resources to be allocated. This is why MS-Aloha is called "slotted".

Code-division multiple access (**CDMA**): It is a channel access method used by various radio communication technologies. In CDMA, several transmitters can send information simultaneously over a single communication channel. This allows several users to share a band of frequencies. CDMA is used as the access method in many mobile phone standards. IS-95, also called "cdmaOne", and its 3G evolution CDMA2000, are often simply referred to as "CDMA"', but UMTS, the 3G standard used by GSM carriers, also uses "wideband CDMA", or W-CDMA, as well as TD-CDMA and TD-SCDMA, as its radio technologies. CDMA is used in Global Positioning System (GPS).

MACA for Wireless LANs (MACAW)

Receiver responds with acknowledgment (ACK) after data reception. Other nodes in receiver's range learn that channel is available.

MACAW uses data sending (DS) packet, sent by sender after receiving CTS to inform such nodes of successful handshake[4]

5 Study ARQ of data link layer. What are them and how each works with example diagram.

Automatic Repeat reQuest (ARQ), also known as Automatic Repeat Query, is an error-control method for data transmission that uses acknowledgements (messages sent by the receiver indicating that it has correctly received a data frame or packet) and timeouts (specified periods of time allowed to elapse before an acknowledgment is to be received) to achieve reliable data transmission over an unreliable service. If the sender does not receive an acknowledgment before the timeout, it usually re-transmits the frame/packet until the sender receives an acknowledgment or exceeds a predefined number of re-transmissions.

Types of ARQ protocol-

- Stop-and-wait ARQ
- Go-Back-N ARQ
- Selective Repeat ARQ / Selective Reject.

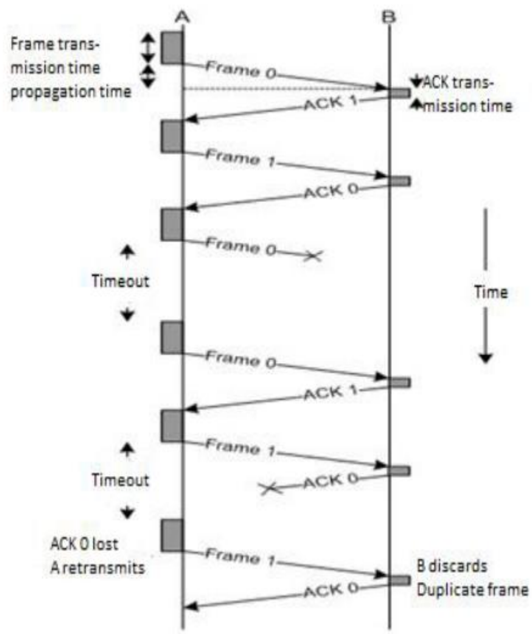
- **Stop-and-wait ARQ**

It ensures that information is not lost due to dropped packets and that packets are received in the correct order. A stop-and-wait ARQ sender sends one frame at a time. After sending each frame, the sender doesn't send any further frames until it receives an acknowledgement (ACK) signal. After receiving a valid frame, the receiver sends an ACK. If the ACK does not reach the sender before a certain time, known as the timeout, the sender sends the same frame again. The timeout countdown is reset after each frame transmission.

One problem is when the ACK sent by the receiver is damaged or lost. In this case, the sender doesn't receive the ACK, times out, and sends the frame again. Now the receiver has two copies of the same frame, and doesn't know if the second one is a duplicate frame or the next frame of the sequence carrying identical data.

There is one more problem when the transmission medium has such a long latency that the sender's timeout runs out before the frame reaches the receiver. In this case the sender resends the same packet. Eventually the receiver gets two copies of the same frame, and sends an ACK for each one. The sender, waiting for a single ACK, receives two ACKs, which may cause problems if it assumes that the second ACK is for the next frame in the sequence.

To avoid these problems, the solution is to define a 1bit *sequence number* in the header of the frame. This sequence number alternates (from 0 to 1) in subsequent frames. When the receiver sends an ACK, it includes the sequence number of the next packet it expects. This way, the receiver can detect duplicated frames by checking if the frame sequence numbers alternate. If two subsequent frames have the same sequence number, they are duplicates, and the second frame is discarded. Similarly, if two subsequent ACKs reference the same sequence number, they are acknowledging the same frame.

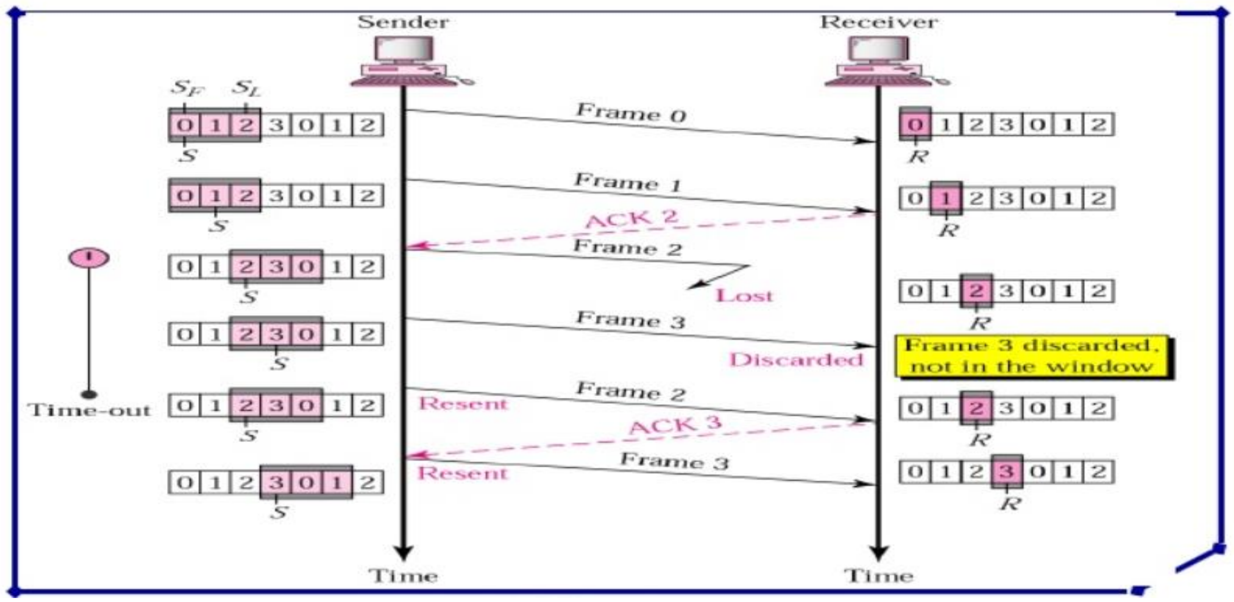


- **Go-Back-N ARQ**

It is a specific instance of the automatic repeat request (ARQ) protocol, in which the sending process continues to send a number of frames specified by a *window size* even without receiving an acknowledgement (ACK) packet from the receiver. It can transmit N frames to the peer before requiring an ACK.

The receiver process keeps track of the sequence number of the next frame it expects to receive, and sends that number with every ACK it sends. The receiver will discard any frame that does not have the exact sequence number it expects (either a duplicate frame it already acknowledged, or an out-of-order frame it expects to receive later) and will resend an ACK for the last correct in-order frame. Once the sender has sent all the frames in its *window*, it will detect that all of the frames since the first lost frame are outstanding, and will go back to the sequence number of the last ACK it received from the receiver process and fill its window starting with that frame and continue the process over again.

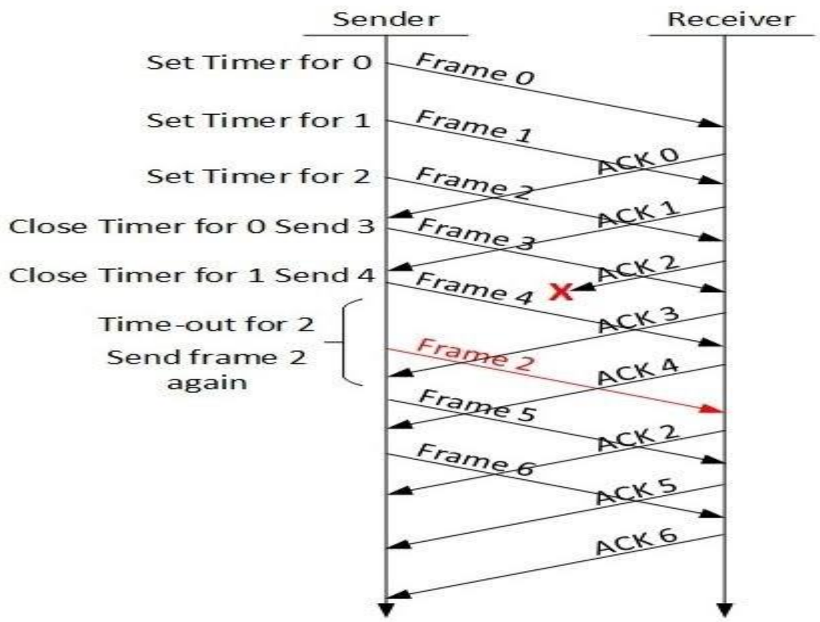
Go-Back-N ARQ is a more efficient use of a connection than Stop-and-wait ARQ, since unlike waiting for an acknowledgement for each packet, the connection is still being utilized as packets are being sent. In other words, during the time that would otherwise be spent waiting, more packets are being sent.



- **Selective Repeat ARQ / Selective Reject**

Go-Back-N ARQ results in sending frames multiple times – if any frame was lost or damaged, or the ACK acknowledging them was lost or damaged, then that frame and all following frames in the window (even if they were received without error) will be re-sent. To avoid this, Selective Repeat ARQ can be used.

With selective repeat, the sender sends a number of frames specified by a window size even without the need to wait for individual ACK from the receiver as in Go-Back-N ARQ. The receiver may selectively reject a single frame, which may be retransmitted alone; this contrasts with other forms of ARQ, which must send every frame from that point again. The receiver accepts out-of-order frames and buffers them. The sender individually retransmits frames that have timed out.[4]



6 Describe CRC error control of the data link layer.

Error detection is the process of detecting the error during the transmission between the sender and the receiver. Cyclic Redundancy Check (CRC) is type of error detection.

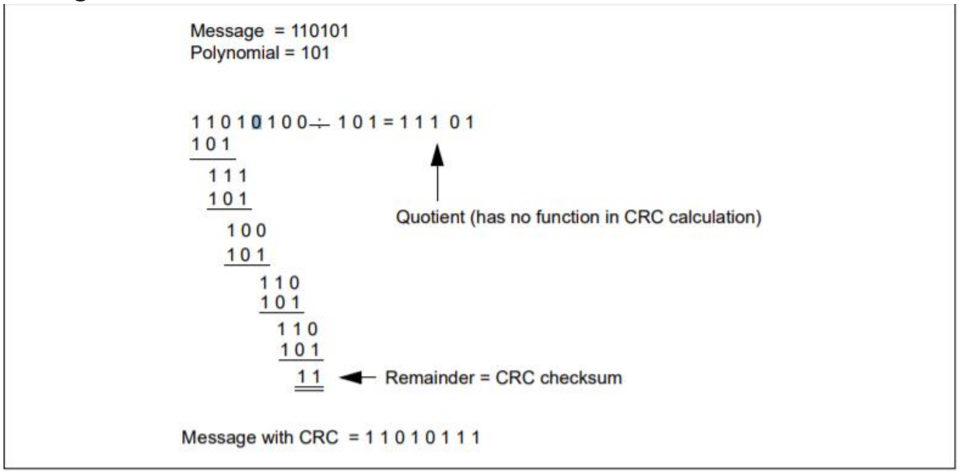
In CRC, binary division is applied to data unit and remainder of this is added to data unit and sent to the receiver. At receiver side, it divides the data unit by same divisor. Data unit is accepted if remainder is zero, otherwise it considers it as corrupted in transit and drops the packet.

At sender, data unit is composite by number of 0s, then it is divided by predefined divisor using binary division. The remainder (CRC) is then appended to data unit and is sent to receiver.

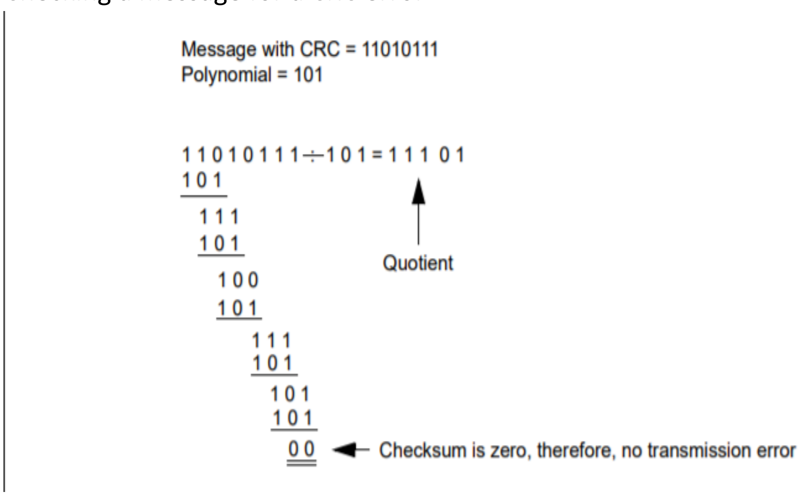
At receiver, upon arrival of packet followed by CRC, it is divided by same divisor which is used at sender. If remainder is zero, it is error free, otherwise it is corrupted in transit. [5]

Example –

CRC generation



Checking a message for a CRC error



7 **What are relations and differences between Data transfer speed (R) and signaling rate (Rs). Describe them with examples.**

Signaling rate (Rs) - The signaling rate is simply the number of state changes made per a unit of time. It merely describes the speed at which a single bit is transmitted and received. Hence, the unit bits per second (bps) is used. It is also described as the maximum physical speed of the interface.

Data transfer speed (R) - Data transfer rate is the amount of usable data (probably peak) that can be transferred in a second. In other words, a data transfer rate is the amount of digital data that is moved from one place to another in a given time, usually in a second's time. The data transfer rate can be viewed as the speed of travel of a given amount of data from one place to another. In general, the greater the bandwidth of a given path, the higher the data transfer rate.

Example-

If the speed of USB 2.0 is 480Mbps but the data transfer rate is 53MBytes/s then, in this case, 480Mbps is signaling rate as it is the maximum physical speed of the interface and 53Mbytes/s is data transfer rate. [6]

References

[1] http://whatis.techtarget.com/definition/Nyquist-Theorem

[2] http://www.dip.ee.uct.ac.za/~nicolls/lectures/eee482f/04_chancap.pdf

[3] https://en.wikipedia.org/wiki/Medium_access_control

[4] https://en.wikipedia.org

[5] http://ww1.microchip.com/downloads/en/AppNotes/00730a.pdf

[6] http://www.electro-tech-online.com/threads/signalling-rate-data-transfer-rate.9661/