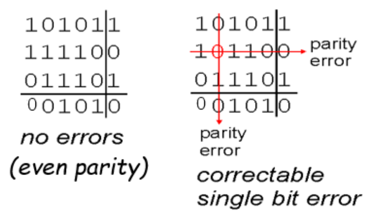
CNT4007C Computer Networks, Fall 2019
Instructor: Prof. Ahmed Helmy
Homework 3
On the Data link layer, MAC protocols and Wireless Mobile Networking
Due Date: Nov 14th, 2019 on Canvas *before* **midday** 11:59**am**
Please also provide an exact hard copy (in class or during the TA office hours)

Q1. Error detection and correction:

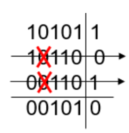
I. Describe how parity bit techniques can *detect and correct* errors in data-link frames? What are its limitations?
II. Provide an example where the error cannot be detected or corrected. Explain why.
III. Provide an example where *multiple* errors can be detected and corrected by parity techniques. Explain the limit of your example.

Answer: Ch 6, slide 18

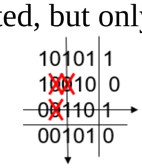
I. A single dimensional parity bit is only capable of detecting single errors without the ability to correct them. A two-dimensional parity checking is capable of detecting and correcting limited errors. It can only guarantee correction of single bit errors in a frame.
[example from the lecture for ability to detect and correct single bit errors]



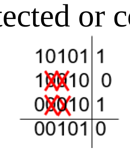
II. For multi-error scenarios, there is no guarantee of ability to detect and correct the errors. Here are several examples:
a. Two errors (shown in X), arrows indicate parity error, in this case error can be detected but not corrected (since the bits in error cannot be uniquely identified)



b. Three errors: error is detected, but only one bit can be corrected

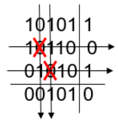


c. Four errors: errors cannot be detected or corrected



Not all the above examples are needed for a correct answer. A correct scenario like in 'c' suffices. Otherwise, partial credit is given.

III. If the errors occur in different rows and columns then they can be detected and corrected like the example below



If the errors are not aligned in manner above (in different rows and columns) then they may not be correctable (see first example of II above).

Extra: multiple errors in a frame can occur during 'burst errors' when the lines/wires experience temporary but abrupt failures/or interference (say due to lightening). Parity-checking may not be able to detect or correct the errors in this case.

Q2. Provide analogy between the operation of CRC and CDMA in terms of how they function at the sender and receiver.

Answer: In CRC, the sender has the frame to send including *D* bits, and has a generator *G*, and it produces *R* CRC bits as a function of *D* and *G*. Then *R* is sent over the network (along with *D*). At the receiver, the received *R* (from the network), along with a local generator *G*, is used to check for error in the received frame (*R* and *D*).
In CDMA, the sender uses a PN sequence and the data *D*, to generate the data sent over the channel as a function of PN and *D*. At the receiver, the PN sequence is used along with received data to extract *D*.
In both cases, a shared generator/PN-sequence between the sender and receiver, is used with a known function (multiplication in case of direct sequencing CDMA, and division in case of CRC) to check the received signal (for errors in CRC, and for correlated spectral power in CDMA).

Q3. Someone suggested to get rid of the MAC address. 'You only need IP addresses' to route packets! Is this a true statement? Discuss the main implications and consequences of this suggestion on LANs, switching operations (e.g., in data centers), and mobility.

Answer: Getting rid of MAC addresses on switched LANs means that all the traffic needs to be broadcast and filtered at the upper layers (e.g., the network layer, using IP addresses). This would incur enormous unnecessary overhead for all the nodes on the LAN and slow down its operations. Particularly, in data centers that include a hierarchy of switches, broadcasting all traffic and processing things at the network layer (based on IP addresses) can decrease the efficiency dramatically and slow down the operations. For mobility, switching on MAC addresses helps efficient handover (under the same subnet router), where the traffic stops going to the old location and starts going to the new location. This cannot be done without a MAC address (and the switch would have to resort to broadcast). [other sound and reasonable arguments can be accepted, even if partially]

Q4. Main communication paradigm over shared media:

I. Describe how communication on a shared medium (e.g., Ethernet bus/LAN, or token ring) occurs on the wire at the MAC (data-link) layer for unicast, broadcast and multicast.

II. Describe the vulnerability of such method with potential attacks.

Answer:

I. Communication on a shared medium (like ethernet bus) occurs through 'broadcast and filtration' [Ch6, slides 23, 43].
Broadcast occur naturally, since the frame is sent to all the nodes on the LAN and all nodes receive it on the wire. No filtration is needed in this case.
Unicast is done through filtration at the network interface card by checking the destination MAC address. If the address does not match the local machine then the frame is dropped.
Multicast is done through broadcast at the data-link layer, then the filtration is performed at the network layer (Extra: if the node is part of the multicast group then the packet is accepted, otherwise the multicast packet is dropped).

II. Because the packets are broadcast and are received by the data link layer (or the network layer, for multicast) of the other nodes, then 'eavesdropping' [i.e., snooping on other nodes' traffic] because easy. If the network interface card operates in promiscuous mode, it can passes all the traffic to the upper layers and an attacker can receive and process frames not destined to it.

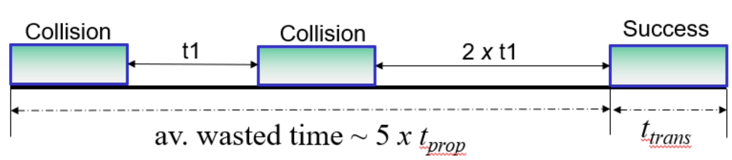
Q5. Utilization of MAC protocols

I. Derive the utilization formula for: (a) Ethernet, (b) Token ring (release after reception), and (c) FDDI [which uses Token ring (release after transmission)].

II. Compare them.

III. Comment on what happens when the number of stations on the LAN is increased in each case.

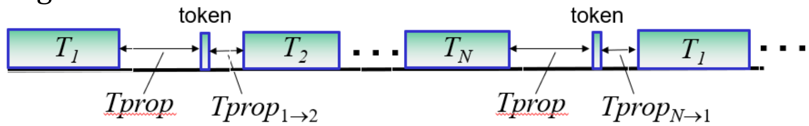
Answer: I. For Ethernet and token ring release after reception (RAR) the derivation is given in the lecture. (Ch6 slides, pgs 44,45 for CSMA/CD, and pgs 51, 52 for RAR)



- Utilization (u) is fraction of time used for useful/successful data transmission
- t_{prop} = max prop delay between 2 nodes in LAN
- t_{trans} = time to transmit max-size frame
- utilization is *tx* time as fraction of total time (*tx* time + wasted)

$$\boxed{efficiency = utilization(u) = \frac{1}{1+\frac{5.t_{prop}}{t_{trans}}} = \frac{1}{1+5\,a}}, \; a = \frac{Tprop}{Ttrans}$$

For token ring with RAR:



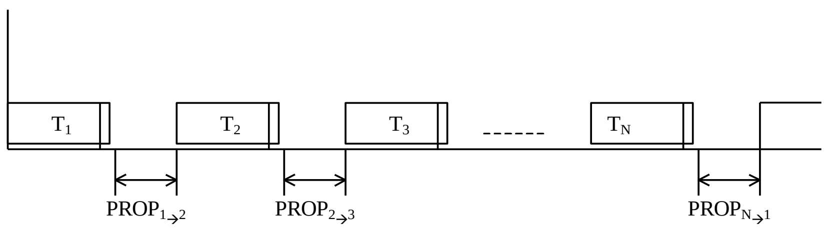
$$u = \frac{T_{useful}}{T_{total}} = \frac{T_{useful}}{T_{useful}+T_{wasted}} = \frac{T_1+T_2+\cdots+T_N}{T_1+T_2+\cdots+T_N+(N+1)T_{prop}}$$

$a = \frac{T_{prop}}{T_{trans}} = \frac{T_{prop}}{E(T_n)}$, *E(Tn)* is average T_{trans} of a node

$$u = \frac{\sum T_i}{\sum T_i+(N+1).T_{prop}} \approx \frac{1}{1+\frac{T_{prop}}{E(T_n)}}, \quad E(T_n) = \frac{\sum T_i}{N}$$

$$u = \frac{1}{1+a}$$

For token ring release after transmission (RAT) used by FDDI:



Utilization

$$\mu = \frac{Useful\ \ Transmission\ time}{Total\ \ time(Useful\ +wasted\ )} = \frac{T_1+T_2+\ldots+T_N}{T_1+T_2+\ldots+T_N+\sum PROP_{i\to i+1}} = \frac{\sum T_i}{\sum T_i + PROP}$$

$$a = \frac{PROP}{E(T_n)}$$

where E(T_n) = expected (average) duration of node transmission $= \sum_i^N \frac{T_i}{N}$

So, $\mu = \dfrac{1}{1+\dfrac{PROP}{\sum T_i}} = \dfrac{1}{1+\dfrac{a}{N}}$

Note that as *N* increases there is less time wasted in propagating the token and utilization increases. As *a* increases the utilization decreases.

II.

For token ring release after reception (RAR): $\mu = \dfrac{1}{1+a}$

For Ethernet (CSMA/CD): $\mu = \dfrac{1}{1+5a}$

For the same "a", we see the $u_{\text{RAT}} > u_{\text{RAR}} > u_{\text{CSMA/CD}}$

When 'a' increases the utilization for all schemes drops, while at small 'a' they exhibit somewhat similar utilization.

III. For CSMA/CD the number of probable collisions increases with the increase in N (the number of attached stations).
For token ring (release after reception), the number of stations sending per token-propagation around the ring increases, but so does the wait time (since each station would wait for its own transmission to be received), so the net result doesn't change the utilization.
For token ring (release after transmission) the number of stations sending per token-propagation around the ring increases, so the wasted (idle) time decreases, which increases the overall utilization. (this also shows in the utilization formula).

Q6. MAC utilization
For an Ethernet LAN (shared bus) the data rate was increased from 10Mbps to 100Mbps.

- ***I.*** How will the utilization (U) of this network change? [Calculate U for each case]
- ***II.*** Suggest two ways in which we can return the utilization to what it was before (By increasing or decreasing another parameter and by how much? Show your reasoning.)
- ***III.*** One person argued that increasing the number of stations attached to the LAN would reduce the idle time on the LAN and hence increase the utilization. Do you agree?

Answer:
I. For Ethernet U=1/(1+5a), where a = Tprop/Ttrans.
But Ttrans=#bits/data rate. Since the data rate was increased, so Ttrans is decreased (by a factor of 10), and hence a is increased by a factor of 10, and subsequently U is decreased.

II. We can either increase the # of bits per frame by a factor of 10 (so that Ttrans would decrease by 10), or decrease the length of the Ethernet network/cable by a factor of 10 (so that Tprop would increase by 10), or a combination thereof (i.e., increase the # of bits by 5 and the length by 2, so on).

III. No. Increasing the number of stations would increase the probability of collisions and so will bring the utilization down.

Q7. Discuss whether CSMA/CD is still needed for switched Ethernet and why? If not, why is it still being used?

Answer: CSMA/CD was designed to resolve contention and collision in shared media when multiple stations attempt to access the channel almost simultaneously. For switched Ethernet, there is no contention for the channel (since it is a point-to-point technology, similar to routers, where packets are stored/buffered in the switch, and a switching table is used). Hence CSMA/CD technically is not needed. However, for backward compatibility and 'interoperability' reasons, and to integrate well with legacy (already-installed) Ethernet systems, the same format of packets and same CSMA/CD mechanisms are used. This was one of the reasons why switched Ethernet was so successful (whereas ATM, another fast LAN technology was not).

Q8. Why do we need mapping between IP address and MAC address? What table provides such mapping?

Answer: We need the mapping (which is performed by the addresss resolution protocol ARP) because the main network address assignment is the IP address (for mobile hosts is performed dynamically through DHCP), but in order to communicate efficiently on LANs a machine needs to know the MAC addresses of the nearby machines (particularly the first hop router). The ARP table provides such mapping.

Q9. Switched ethernet: Which data structure does an ethernet switch use to avoid the inefficiencies of a hub? how does it construct such data structure?

Answer: in Ethernet switches the 'switching table' is the data structure used to direct traffic on the LAN and avoid broadcast inefficiencies suffered by hubs.
The switching table is constructed through the self-leaning algorithm where the address of the sender's MAC address in each frame is stored (along with the incoming interface) in the table, and the destination mac address is looked up before forwarding the frames on the network (LAN).

Q10. Data center networks:

I. What are the two main functions of a data center network?
II. What are the two main functions of the data center load balancer (sometimes referred to as a 'layer 4' switch)?

Answer: I. A data center network provides: 1- connectivity between hosts in the data center (needed for various services; search, parallel computation, cloud computing, etc.), and 2- connectivity between the data center and the outside world

II. The data center load balancer has the following functions:

1- balances the work load across hosts (and for that it needs to monitor the work load for the hosts), and
2- hides the internal network structure and preventing clients from directly interacting with the hosts [Extra: by performing NAT-like function

(translating the public external IP address to the internal IP address of the appropriate host, and then translating back for the packets traveling in the reverse direction back to the clients)]

Extra: It is sometimes referred to as a 'layer 4' because it looks at (and processes) the port number to distribute the load among the hosts/servers/blades/pizza-boxes.

Q11. Provide four potential example use cases of infrastructureless multi-hop networks (such as adhoc networks and peer-to-peer wireless networks).

[This question is open ended, reasonable examples with some details are acceptable]
- disaster relief (search and rescue), like hurricanes where part (or all) of the infrastructure is damaged (as in Katrina)
- reconnaissance missions, in rural areas without infrastructure
- interplanetary networks, and/or networks of satellites to provide Internet connectivity to the last billion people (like Google's loon, fracebook's Aquila, Space-x's Starlink, …)
- vehicular networks on highways to support self-driving cars and autonomous systems,
- networked coordination of swarming robots on mars,
- aerial networks for drones
- bypassing infrastructure for cost, congestion, authentication, censorship, security...so on

Q12. What are the main differences between wired and wireless networks (mention 3 main reasons) and further elaborate on one of those reasons in three sub-points.

Answer: the main differences between wired and wireless networks include:

1- Channel characteristics, including
   a. high bit error rate '*BER*' (much higher than optical fiber, coax.)
   b. asymmetry on links in bandwidth and delay
   c. unidirectional links
   d. effects of wave propagation, fading, attenuation, … etc.
   e. for satellite we get extended propagation delays

2- Mobility: continuous and introduces topology dynamics

3- Power constraints in lots of the wireless devices, due to form factor and battery-based energy

Q13. Wireless rate adaptation:

I. What is rate adaptation in 802.11, and why is it used?
II. Discuss in detail its effect on TCP operation and dynamics.

Answer: I. Rate adaptation in wireless MAC (e.g., 802.11) changes the encoding scheme to reduce the sending data rate when the signal to noise ratio SNR (or the signal power) decreases to a level at which BER is high (~10% or more). This could occur due to increased interference from the nearby environment or due to the increased distance from the base station (or the other node involved in the communication). By decreasing the data rate, the SNR is increased and the BER is decreased to acceptable levels. This effectively increases the usability (in terms of distance and operational range) of the wireless network.

II. Decreasing the data rate (sometimes by orders of magnitude; e.g., from 100Mbps to 1Mbps) would increase the delay dramatically for the wireless links. TCP relies on RTT estimates to detect congestion and set its retransmission timers. Having huge fluctuations in the RTT estimates (due to the rate adaptation of wireless links) can degrade the performance of TCP.

Q14. Hidden terminal:

I. What is the hidden terminal problem?

II. Why does it not exist in wired networks (like Ethernet)?

Answer:

I. In a chain topology of A-B-C-D, where A can hear only B and not C then when C is sending to B, A's carrier sense would not be enough to top collisions if it sends to B as well. (more details and scenarios/figures are given in the lecture slides)

Extra: To address the problem we use RTS/CTS exchange. RTS reserves the medium in the sender's neighborhood, and CTS reserves the medium in the receiver's neighborhood. This way, collisions can be avoided to a large extent, addressing the hidden terminal problem. (more details and given in the lecture slides/notes).

II. In shared bus (or hub-based) Ethernet, all the nodes connected to the network (LAN) belong to the same neighborhood. When a node sends a message on the LAN, it is broadcast onto the LAN and all the other nodes on the LAN get to detect its presence (even in the case of collision) based on variations in the voltage over the wire. Hence, the main reason for hidden terminal (the difference in neighborhoods between nodes, since the link is a function of the distance between the nodes) is eliminated. No terminal can be hidden on a shared Ethernet LAN, and collision detection can be used effectively.

Q15. What type of interference is directly reduced by frequency planning in cellular networks? and how is it reduced?

Answer: Frequency planning directly reduces the adjacent channel interference (between those channels occupying neighboring frequencies on the frequency spectrum). It is reduced by assigning neighboring channels to different cells (as far away from each other) in the same cluster. This separates the signal in 'space' in addition to its separation in frequency. The separation in frequency (for adjacent channels) is not enough due to hardware limitations and imperfect filtering, so more separation in space is needed. (more details and diagrams are provided in the lecture slides).

Q16. What are the dimensions in which we can separate the signal for the purpose of multiplexing? Mention five, not including hybrid!

Answer:

1- Frequency, 2- time, 3- space, 4- code (using spread spectrum), 5- wavelength

More details (extra):

- *FDMA* (*frequency division multiple access*)
- *TDMA* (*time division multiple access*)
- *SSMA* (*spread spectrum multiple access*)
  - *FHMA* (*frequency hopping multiple access)*
  - *CDMA* (*code division multiple access*)
    or *DSMA* (*direct sequency multiple access*)
- *SDMA* (*space division multiple access*)
- *WDM* (*wavelength division multiplexing*)

Q17. What are the advantages of using spread spectrum (e.g., CDMA) over other multiple access techniques we have studied? Mention five advantages, and for each explain how spread spectrum achieves its advantage.

Answer:

1- Resilience to fading and interference since the signal is spread in the frequency domain over a large spectrum (interference usually affects part of the spectrum and hence only a part of the spread signal)
2- Security: only the intended recipient (that has the right seed for the pseudo noise (PN) sequence) is able to decipher/decode the message, the other recipients will not be able to receive it and it would look like noise to them
3- No frequency planning since the users use the same frequency
4- Soft handoff can simplify the process of hand off during mobility
5- The number of users supported is no longer limited to the available spectrum, since the separation between users occurs in the code (not the frequency or time) domain. Typically a CDMA system can support 3-5 times the users in a TDMA system. The max capacity is actually limited by the noise floor (since to a user all the signals not destined to it would result in 'noise').

Q18. Someone suggested that 'CDMA systems are limitless in terms of number of simultaneous users supported', argue (with details) for or against this statement.

Answer: No, this statement is false. CDMA separates the signal in the 'code' domain by using different pseudo-noise (PN) sequences for different users. For a given sender, *X*, an intended recipient is able to re-generate the PN sequence locally and receive the signal correctly, while other (non-intended) receivers use a different PN sequence (to listen to senders other than *X*) and get noise. In theory, if the codes are perfectly orthogonal, then the 'noise' should be zero or very small. Due to practical and hardware limitations, the noise is not negligible, creating the '***noise floor***' at a receiving node. If the signal is above the noise-floor then the reception can be successful. But once the noise-floor reaches a threshold it can drown out the intended signal and reception fails.

With the increase is number of simultaneous users, the noise floor is raised. Hence, that noise floor provides the main limitation in CDMA systems on the number of users.