**King Saud University**

**College Of Computer & Information Sciences**

**Department Of Computer Sciences**

**Tutorial 5 Spring 15**

**(Computer Networks CSC 329)**

**Q1.**

1. Briefly describe how Ethernet’s exponential backoff works. What is one reason why Ethernet’s exponential backoff might be better than randomizing retransmission attempts over a fixed-length time interval?
2. What is the main difference between the Aloha protocols and CSMA protocols?

Aloha is of two types slotted and pure.   
CSMA(Carier sense multiple access) is also of two types   
CSMA and CSMA CD(Collision Detect).   
  
Aloha is primitive It will just send its packets while CSMA is intelligent it first listens to the media and sends only if the media is free.

**CSMA vs ALOHA**

Aloha is a simple communication scheme originally developed by the University of Hawaii to be used for satellite communication. In the Aloha method, each source in a communication network transmits data every time there is a frame to be transmitted. If the frame successfully reaches the destination, the next frame is transmitted. If the frame is not received at the destination, it will be transmitted again. CSMA (Carrier Sense Multiple Access) is a Media Access Control (MAC) protocol, where a node transmits data on a shared transmission media only after verifying the absence of other traffic.

**Aloha Protocol**

As mentioned earlier, Aloha is a simple communication protocol where each source in the network transmits data whenever it has a frame to be transmitted. If the frame is transmitted successfully, the next frame will be transmitted. If the transmission is failed, the source will send the same frame again. Aloha works well with wireless broadcast systems or half-duplex two-way links. But when the network becomes more complex, such as an Ethernet with multiple sources and destinations that uses a common data path, problems occur due to colliding of data frames. When the communication volume increases, the collision problem becomes worse. This can reduce the efficiency of a network since colliding frames will cause loss of data in both the frames. Slotted Aloha is an improvement to the original Aloha protocol, where discrete time slots were introduced to increase the maximum throughput while reducing collisions. This is achieved by allowing sources to transmit only at the beginning of a timeslot.

**CSMA Protocol**

CSMA protocol is a probabilistic MAC protocol in which a node verifies that the channel is free before transmitting on a shared channel such as an electrical bus. Before transmitting, the transmitter tries to detect whether there is a signal from another station in the channel. If a signal is detected, the transmitter waits until the ongoing transmission is finished before it starts to transmit again. This is the “Carrier Sense” part of the protocol. “Multiple Access” defines that multiple stations send and receive signals on the channel and a transmission by a single node is generally received by all the other stations using the channel. Carrier Sense Multiple Access with Collision Detection (CSMA/CD) and Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) are two modifications of the CSMA protocol. CSMA/CD improves performance of CSMA by stopping a transmission as soon as a collision is detected and CSMA/CA improves the performance of CSMA by delaying the transmission by a random interval if the channel is sensed busy.

**Difference between CSMA and ALOHA**

Main difference between Aloha and CSMA is that Aloha protocol does not try to detect whether the channel is free before transmitting but the CSMA protocol verifies that the channel is free before transmitting data. Thus CSMA protocol avoids clashes before they happen while Aloha protocol detects that a channel is busy only after a clash happens. Due to this, CSMA is more suitable for networks such as Ethernet where multiple sources and destinations use the same channel.

1. What is the main difference between the CSMA and CSMA/CD protocols?

Explain the difference between CSMA/CD and CSMA/CA.

Answer: In CD, collisions are detected as they occur. Senders do not signal their intent to transmit but simply start transmitting if they sense no other ongoing transmission. In CA, collisions are avoided because each node signals its intent to transmit before actually doing so.

1. Why is there no concept of acknowledgment (ACK) in the CSMA/CD protocol?

Why is there no concept of acknowledgment (ACK) in the CSMA/CD protocol?

Answer: The CSMA/CD protocol is run over copper or fiber physical media which have very low BER values (10-8 or 10-12). On the other hand, the CSMA/CA protocol is run over free-space with a BER value of 10-5 , which is considered to be very high. To reduce retransmissions in upper-layer protocols, an ACK mechanism is built into the CSMA/CA protocol. However, the BER offered by copper or fiber is very low; hence, there is no ACK mechanism in CSMA/CD and the upper-layer protocols are asked to retransmit occasionally.

1. Explain the difference between CSMA/CD and CSMA/CA.

CSMA/CA waits for traffic to stop before transmitting to avoid a collision.   
CSMA/CD transmits and stops if a collision occurs.

1. Suppose nodes A, B, and C each attach to the same broadcast LAN (through their adapters). If A sends thousands of IP datagrams to B with each encapsulating frame addressed to the MAC address of B, will C’s adapter process these frames? If so, will C’s adapter pass the IP datagrams in these frames to the network layer in C?

Briefly describe how Ethernet’s exponential backoff works. What is one reason why Ethernet’s exponential backoff might be better than randomizing retransmission attempts over a fixed-length time interval?

Answer: Ethernet maintains an interval of time T over which is will randomize when it will attempt a retransmission. After each collision for the same packet, it doubles the length of T up to some fixed max. This is better than just a single, fixed value of T since when there are a lot of collisions the interval over which randomization is done will be large, allowing just one node to successfully being transmitting. When there are only a small number of colliding nodes, the retransmission will be randomized initially over a small T, allowing a node to transmit more quickly.

b. Suppose nodes A, B, and C each attach to the same broadcast LAN (through their adapters).

If A sends thousands of IP datagrams to B with each encapsulating frame addressed to the MAC address of B, will C’s adapter process these frames? If so, will C’s adapter pass the IP datagrams in these frames to the network layer in C? How would your answer change if A sends frames with the MAC broadcast address?

Answer: C’s adapter will process the frames, but the adapter will not pass the datagrams up the protocol stack. If the LAN broadcast address is used, then C’s adapter will both process the frames and pass the datagrams up the protocol stack.

c. Suppose there are three routers between source host and destination host. Ignoring fragmentation, an IP datagram sent from the source host to the destination host will travel over how many interfaces? How many forwarding tables will be indexed to move the datagram from the source to the destination? Answer: 8 interfaces; 3 forwarding tables

e. Briefly explain the two methods through which a wireless 802.11 node learns about access points it can communicate with. Answer: i) Passive scanning, beacon frame from AP, association from node, reply from AP. ii) Active scanning, probe request from node, probe responses from APs, association request from node, reply from AP.

f. Mention three different techniques that are used in the switching fabric of a router that manage the actual switching of packets from an input port to an output port. Answer: Switching via memory, bus, or interconnection network

**Q2.**

A BSS (Basic Service Set) has only two nodes as shown in the figure below: an AP and one laptop with a WiFi interface with a physical-layer transmission rate of 1 Mbps.



Assume that the laptop is transmitting DATA frames containing 118 bytes of IP layer data. The lengths of RTS, CTS, and ACK frames are 20, 14, and 14 bytes, respectively. The total length of all the control information in the header of a DATA frame is 34 bytes. Assume that the lengths of SIFS and DIFS are equal respectively to 20 µs and 40 µs .

1. Explain the concept of hidden station in IEEE 802.11

a. What is a hidden terminal problem? What is the solution to address the problem? Why is the hidden terminal problem so common in wireless network but not in wired network?  
  
In wireless networking, the hidden node problem or hidden terminal problem occurs when a node is visible from a wireless access point (AP), but not from other nodes communicating with said AP. This leads to difficulties in media access control.  
  
  
In a wireless network, it is likely that the node at the far edge of the access point's range, which is known as A, can see the access point, but it is unlikely that the same node can see a node on the opposite end of the access point's range, B. These nodes are known as hidden. The problem is when nodes A and B start to send packets simultaneously to the access point. Since node A and B can not sense the carrier, Carrier sense multiple access with collision avoidance (CSMA/CA) does not work, and collisions occur, scrambling data. To overcome this problem, handshaking is implemented in conjunction with the CSMA/CA scheme. The same problem exists in a MANET.

1. Explain the role of the Network Allocation Vector.
2. What is the value of the duration field in the CTS frames transmitted by the laptop?