CSE 473 – Introduction to Computer Networks *Roch Guérin*

Quiz 6 Solution

Your Name: *12/2/2014*

1. **(5 points total)** Consider a wireless network operating according to the 802.11b protocol. The network has two access points AP1 and AP2, but unfortunately, they were configured independently and both use channel 1. We focus on three hosts in the network (there could be others), A, B, and C, where A can hear B but not C, B can hear both A and C, and C can hear B but not A. All hosts can hear both access points. Hosts A and B are associated with AP1 and host C is associated with AP2. RTS/CTS is disable in all hosts and the APs.

   (1 point) What mechanism would be involved in allowing the different hosts to associate with different access points?

   Both APs would be sending their own beacon frames, so that hosts would be able to select to associate with either, e.g., based on which one has the highest signal to noise ratio.

   (4 points) At time t=0, AP1 is transmitting a packet to some hosts (say, D), and the transmission will last until t=400μs. At time t=100μs host A gets a packet to transmit, but senses that the medium is busy and initializes its backoff timer to 100μs. At time t=150μs host C gets a packet to transmit, but senses that the medium is busy and initializes its backoff timer to 600μs. At time t=200μs host B gets a packet to transmit, but senses that the medium is busy and initializes its backoff timer to 300μs. At time t=400μs AP2 starts transmitting a packet to some host (say F), and its transmission lasts for 400μs as well.
   When do hosts A, B, and C start sending their packets, and which of them are delivered successfully? Assume that all packets from A, B, and C take 200μs to transmit, and ignore time spent on ACKs and/or *IFS.

   Because both APs transmit on channel 1, all hosts will hear their transmissions. This means that the backoff timers of all three hosts will remain frozen until t=800μs. Host A's timer expires at ***t=900μs****, at which point it starts transmitting its packet. B's timer freezes at 200μs when A's transmission starts, but because C does not hear A, it continues decrementing its timer that reaches 300μs when A finishes its transmission at time t=1,100μs. At that time, B starts decrementing its timer again, and it expires 200μs later, at which point B starts its transmission, i.e., at time* ***t=1300μs****. Note that at that time, the value of C's timer is 100μs. Because C can hear B, it freezes its timer until B's transmission ends at t=1,500μs. At this time, C starts to decrement its timer again. It expires at t****=1,600μs****, at which point C transmits its packet and finishes its transmission at t=1,800μs. All packet transmissions from A, B, and C were successful in their first attempt.*

2. **(5 points total)** Consider a simple block cipher encryption scheme that operates on 8-bit blocks. Encryption proceeds in two steps: (1) swap the first and last four bits of an 8-bit block, *e.g.*, 11100111 becomes 01111110, (2) add 15 to the resulting 8-bit block and throw away any overflow bits. To improve the scheme's security, cipher block chaining is used prior to the encryption step. The initial vector (IV) is set to 10101010.

Assume a clear text input of the form: 00001111 11101110 11001100, what would be the cipher text?

Encryption proceeds as follows

	10101010	
XOR	*00001111*	
	10100101	
	01011010	*(swap of 1010 and 0101)*
+	*1111*	
	01101001	***Cipher 1***
XOR	*11101110*	
	10000111	
	01111000	*(swap of 1000 and 0111)*
+	*1111*	
	10000111	***Cipher 2***
XOR	*11001100*	
	01001011	
	10110100	*(swap of 0100 and 1011)*
+	*1111*	
	11000011	***Cipher 3***

Hence the final cipher text is 01101001 10000111 11000011.