CSE 473 – Introduction to Computer Networks *Jon Turner*

Quiz 6 Solution

Your name here: *12/5/2012*

1. (4 points) Let A and B be two nodes in a wireless network with access point X. Assume that A and B cannot hear each others' transmissions, but can hear X. At time 0, X is sending a packet to some other node and it completes sending this packet at time 100 μs. At time 30, a packet becomes available for transmission at A and at time 70, a packet becomes available for transmission at B. Assume that A needs 200 μs to send its packet and B needs 100 μs to send its packet. Let t_A be the initial value of the backoff timer for A and let t_B be the initial value of the backoff timer for B.

   Can A and B transmit their packets without colliding if $|t_A - t_B| = 60$? Explain. You may ignore the inter-frame spacing and the time needed for acknowledgments.

   No. Because A and B cannot hear each other, whichever of the two has the larger value will not hear when the other starts sending. Since both A and B need more than 60 ms to send their packets, if the backoff timers differ by 60, whichever one has the larger backoff timer value will interfere with the first.

   Can A and B transmit their packets without colliding if $|t_A - t_B| = 130$? Explain.

   Yes, this will work if t_B is the smaller value, since in this case, B will finish before A starts.

2. (6 points) Consider a simple block cipher that uses 4 bit blocks, where each block is encrypted by adding 3 to it, and discarding any "overflow bits". So for example,

   0010 0101 1110 becomes 0101 1000 0001

   To make this more secure, we add cipher block chaining. Suppose the initial vector is 1011. What is the cipher text corresponding to the clear text

   0101 1011 0011

   First, we xor the first block with the initial vector getting 1110, then add 3 giving us 0001.

   Next, we xor the second block with the previous ciphertext getting 1010, then add 3 giving us 1101.

   Finally, we xor the third block with the previous ciphertext getting 1110, then add 3 giving us 0001.

   So, the complete ciphertext is 0001 1101 0001.