Q1. DoS vs. SIFF (8 points): Denial of Service (DoS) attacks can plague a network, largely because in most current designs, the receiver has no control over the packets that are sent to it. A receiver simply cannot choose from whom it receives packets, just like you can’t control the junk mail that you receive. Don’t fear because the Stateless Internet Flow Filter (SIFF) is here! Read all about SIFF in the paper available at http://www.ece.cmu.edu/ adrian/projects/siff.pdf

Suppose all devices in an IP-based ad hoc network implement the SIFF protocol using the marking scheme

$$MAC_{K_R} [IP_{src}\|IP_{dst}\|IP_{cur}\|IP_{prev}]_m$$

where $K_R$ is the router’s secret key; $IP_{src}$, $IP_{dst}$, $IP_{cur}$, and $IP_{prev}$ are the respective IP addresses of the source, destination, current router, and previous router; and $m$ is the number of bits of the MAC used for the marking (the rest are discarded). Suppose that $m = 5$ and each router maintains a window of 6 markings.

(a) (1 point) Using the formulation in the paper, calculate the probability that a randomly guessed capability will pass through 20 routers. What is the expected number of packets the attacker needs to send to get a message to pass through all 20 routers?

(b) (4 points) When a message with TTL 0 is received by a router, it drops the packet and sends out an ICMP message. Describe an attack, apart from the one described in the paper, wherein an attacker can guess the capabilities using TTL with much higher probability than calculated in the previous question. What is the expected number of packets needed in this case?

(c) (2 points) Propose a fix to your attack in part (b).

(d) (1 point) Assuming the router checks the TTL value before putting the markings, and that the attacker knows the hop count to the destination, calculate the expected number of packets that the attacker needs to send. Which is higher: this number or the one from part (b)? Why?

Q2. Anti-Jamming Swarm (7 points): Bob and his friends are deploying a swarm of remote-controlled airplanes as part of their class project. Mallory wants to bring down the communication system in the swarm. She buys a remote-controlled airplane similar to what Bob has and turns it into a jammer. The jammer works in the following way. When the swarm is in action, it flies around the swarm and looks for links with swarms control traffic in them and jams those links by injecting noise. When these links are jammed, the swarm loses its control and the planes tend to fly in random directions. Describe two anti-jamming mechanisms that will help Bob and his team defeat Mallory assuming that her jammer has the same battery life as the other planes. Provide references to recent literature where appropriate.