The final exam consists of **five** questions (each worth 20 points). You **must** answer the **three** Required Questions and any **two** of the Optional Questions. Put all your answers in blue books with your name on each book and indicate on the outside which questions are in each book. If you answer more than two of the optional questions, you **must indicate the two you want to be graded.**

Three Required Questions [answer ALL three questions]

1 a. Explain RED.
b. What are the specific goals of RED?
c. Discuss three parameters considered in the "RED Tuning" paper.
d. Based on the "RED Tuning" paper, under what circumstances does RED out-perform a Drop-Tail Router?

2 a. What is a Denial of Service (DoS) Attack and a Distributed Denial of Service (DDoS) Attack.
b. Describe Smurf, SYN Flood and UDP Flood attack mechanisms.
c. Explain how direct and reflector DDoS attacks work.
d. What are the differences in attack detection and filtering at
1. the source networks
2. the victim's Network
3. a victim's upstream ISP Network

3 a. "Application-based Collision Avoidance in Wireless Sensor Networks" proposes two distinct applications mechanisms to help avoid collisions. Briefly describe the two proposed approaches.
b. How does the traditional 802.11 MAC protocol attempt to deal with collisions?
c. Why are collisions so detrimental within a wireless sensor network?
d. Explain how source-based collision detection is like TCP congestion control and how receiver-based collision detection is like XCP congestion control?

Six Optional Questions [answer ANY two questions]

4 a. How does the Jacobson/Karls algorithm deal with determining a TCP timeout value?
b. Explain the Explicit Congestion Notification (ECN) mechanism for congestion control at a router. What are the advantages and disadvantages of this scheme?

c. Explain the differences between slow start, fast retransmit and fast recovery in TCP Reno.

5 a. What is the basic idea of IFRC?
b. Explain the concept of AIMD.
c. Discuss how AIMD is used by IFRC as part of the rate adaptation mechanism.
d. Evaluate the IFRC congestion sharing concept in terms of wireless sensor node concerns.

6 a. Explain the concept of CSMA/CA with RTS/CTS.
b. Define and explain the idea of time fairness.
c. Explain the principles of the Idle Sense access method and the advantages in working towards time fairness in wireless networks.
d. What, if anything, do we lose by using this fairness model?

7 a. Briefly describe how the COPE architecture works.
b. Explain the difference between coding gains and coding and MAC gains?
c. Why are hop-by-hop ACKs required in COPE?
d. What is the coding gain for
1. the Bob & Alice topology
2. the Cross topology?

8 a. What are the two conditions necessary to make Speak-up a viable defense?
b. Why must these conditions be present for Speak-up to work?
c. Speak-up offers advantages over other defenses in three distinct situations. What are these three conditions and what defenses would be appropriate if they were not present?

9 a. What makes link-layer security different from more conventional end-to-end security mechanisms?
b. Why was it important that the TinySec designers balance packet overhead against the amount of security provided?
c. What aspect of a wireless sensor network helped the designers come to a fair tradeoff from the previous question?
d. When is encryption important and why is it optional in TinySec?