CS 577 /ECE537 **Fall 2006**

Preliminary Questions for Final Exam

TCP Sliding Windows & Congestion Control

1a. 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.

RED & Tuning RED

2a. 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?

CSFQ & XCP

3a. Describe and explain CSFQ and XCP.

b. Explain the difference between the efficiency and fairness controllers in XCP.

c. Define and discuss three performance measures that can be used to compare congestion control strategies.

d. How does CSFQ perform when compared with FIFO, RED and DRR via ns-2 simulations?

Mice and Elephants

4a. Explain why drop tail routers are unfair to Mice as compared to Elephants.

b. Explain in detail the differences between edge routers and core routers and how they fit with the RIO-PS scheme proposed in the Mice and Elephants paper.

c. How does giving preferential treatment to short TCP flows significantly enhance their transmission time without degrading the performance of long flows?

d. Under what user circumstances could the proposed strategy not improve performance?

DCCP

5a. Briefly discuss the important features of DCCP.
b. Specifically, how would using DCCP be helpful for both audio and streaming video application layers?
c. What are the advantages of the partial checksum feature of DCCP?
d. Explain how the Init Cookie option is used by DCCP to thwart a DOS attacker sending thousands of TCP SYN packets to a server.

Interference-Aware Fair Rate Control in Wireless Sensor Networks

6a. 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.

ExOr

7a. Describe the basic idea of the ExOR mechanism.
b. How does ExOR provides more throughput than traditional routing?
c. Describe the node states and the packet format used in ExOR.
d. Explain the gossip mechanism used in ExOR.
e. Discuss the similarities and differences between ExOR and the Opportunistic Auto Rate (OAR) protocol.

Idle Sense

8a. 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?

Preliminary Questions for Final Exam

Application-Based Collision Avoidance in Wireless Sensor Networks

9a. "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?

Exploiting Idle Communication Power to Improve Wireless Network Performance and Energy Efficiency & Spray and Wait

10a. Explain the basic functionality of Spray and Wait Routing for intermittently connected mobile networks.

b. Describe the Proxy Forwarding algorithm presented in "Exploiting Idle Communication Power to Improve Wireless Network Performance and Efficiency".

c. In what ways are the two algorithms similar?

d. Explain how are the two algorithms different.

XORs in the Air

11a. 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?

Performance Enhancement of TFRC in Wireless Ad Hoc Networks

12a. Explain the performance problem when TFRC runs over multi-hop ad hoc wireless networks.

b. How does TRFC-RE attempt to enhance TRFC performance in this scenario?
c. What are the key communications between sender and receiver for TFRC-RE and how does this feed into the RE algorithm?
d. Discuss the nature of the performance improvements produced by using TRFC-RE instead of TRFC in a single chain wireless LAN topology.

Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial & Distributed Denial of Service Attacks

13a. 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

Secure Data Communication in Mobile Ad Hoc Networks

14a. Explain the details of the SMT protocol.
b. What are the goals of the SMT and SSP?
c. Explain the concept of survival path probability.
d. How does SMT minimize retransmissions?

DDoS: Defense by Offense

15a. 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?

Web Tap: Detecting Covert Web Traffic

16a. Explain the risks associated with HTTP tunnels and spyware.

b. The Web Tap software implementation is based upon carefully tuned filters. Explain how the following filters work and the results they yielded during the 40-day test at the University of Michigan:
   1. Header format filter
   2. Request size filter
   3. Daily bandwidth filter

Sustaining Availability of Web Services under Distributed Denial of Service Attacks

17a. Describe how the DDoS defense mechanism described in "Sustaining Availability of Web Services under DDoS" protects the victim from IP spoofing and ensures that only legitimate IPs connect to the web service?

b. Describe the process by which clients first establish connections to the web server under this mechanism. Describe how the first exchange is made more resilient to flooding.

c. Describe how game theory is used in "Sustaining Availability of Web Services under DDoS" to simulate the performance of the system.

d. This paper describes a defense mechanism against legitimate-looking attackers that uses a fair share of bandwidth per client. Describe a mode of attack in which this mechanism would be made completely ineffective.

TinySec: A Link Layer Security Architecture for Wireless Sensor Networks

18a. 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?

Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures

19a. Explain some of the characteristics of a WSN that make security difficult to implement.
b. Describe the following attacks:
1. Sybil
2. wormhole
c. Describe possible countermeasures for these two attacks.

Detecting Critical Nodes for MANET Intrusion Detection Systems

20a. Why is intrusion detection so difficult in MANET environments?
b. Explain the term 'critical node' in a MANET.
c. How does the detection of critical nodes aid in MANET intrusion detection systems?
d. How can using the trigger/critical node test improve the overall IDS process?