COMP 3331/9331: Computer Networks and Applications

Announcements + Final Exam + Review + Sample Problems
Feedback

• CATEI On-line Survey
  • You should have received email
  • Active till 10\textsuperscript{th} June
  • Accessible via myUNSW
• Two forms
  • Form A: Course Evaluation
  • Form B: Teaching Evaluation (for LIC)
• I would greatly appreciate 10 minutes of your time
• I need to hear from you about your experience with this course and my teaching
  • Helps us improve the quality for future sessions
• Written comments are encouraged
• Feedback is anonymous
Course Announcements

• Assignment 2
  • Deadline – midnight, Friday, Week 13 (3rd June)
  • Remember to test your programs on a CSE machine before submitting
  • Submission instructions provided in spec

• Solutions to all sample questions posted
  • Attempt to answer them yourself before examining answers

• Several other questions on the lecture content page
Final Exam (1)

- Friday, 24th June, 08:45 – 12:00
- Check seating arrangement
- Time: 3 hours + 10 minutes (reading time)
- Maximum Marks: 40
- Recall that, to pass the course, one requirement is that you must score $\geq 16$ marks in the final exam

```
lab = marks for lab exercises (scaled to 15)
assign = marks for the two programming assignments (scaled to 25)
midExam = mark for the mid-semester exam (scaled to 20)
finalExam = mark for the final exam (scaled to 40)
mark = lab + assign + midExam + finalExam
grade = HD|DN|CR|PS if mark $\geq 50$ && finalExam $\geq 16$
        = FL if mark $< 50$ || finalExam $< 16$
```

- Allow to carry forward 2 bonus marks from assignments to final score (i.e. “assign” capped at 27)
Final Exam (2)

- Closed book
- What to bring
  - Student ID
  - Calculator will NOT be provided. BYO - GET THEM APPROVED (CSE STUDENT OFFICE)
  - Pen, Pencil, etc.
Final Exam (3)

- Not a memory test, questions will examine your understanding of concepts
- Tests your understanding
- Tests whether you can apply the principles in a situation that you haven’t seen before
- You can use the mid-session exam as a guide on what the expectations are
Final Exam (4)

- **Syllabus: Comprehensive**
  - Lecture materials from Week 1 – Week 13
  - NO QUESTIONS ON CIRCUIT/PACKET SWITCHING
  - More focus on the material after the mid-semester exam
  - Self-study material is examinable
  - External links, News Items and Research Items discussed in lectures not covered
  - Questions may also examine multiple layers at the same time
  - No questions on programming or lab exams

- You are asked to show your steps and tell us your arguments in answering questions
Final Exam (5)

• How to prepare?
  • Read and thoroughly understand all content
  • Practice, Practice, Practice
  • Go through all the sample questions, sample exam papers, lecture Q&A, textbook questions, etc. for practice

• Don’t panic and get stressed if you come across a hard question

NOTE: Sample final exam paper has been posted on the Final Exam Page linked to course webpage
How do I seek help?

• Post any questions on the course forum
• Engage in discussions (peer learning)
Recap from Week 1: A top-down approach

We’ve covered networking using a top-down

- end-system applications, end-end transport
- network core: routing, hooking nets together
- link-level protocols, e.g., Ethernet
- other stuff: security, mobility, wireless networks
What you have accomplished

• Comprehensive overview of the entire protocol stack with a particular focus on the Internet

• Key principles
  • Layering, scale, hierarchy, etc.

• Key design issues
  • Application architectures, reliability, congestion control, routing, medium access, etc.

• Hands-on practical laboratory experiments using several diagnostic tools and Mininet

• Two “real-world” assignments
  • Client-server push/pull application protocol
  • Distance vector routing protocol
Key topics (1)

• Organisation principles
  • Layering, hierarchy, encapsulation
  • Some researchers speculate that layering is also useful in biological systems/evolution
• Application layer
  • Protocol design, P2P, socket programming
• Transport layer
  • Error detection, reliable data transfer, flow control, congestion control
  • TCP and UDP
Key topics (2)

- Network layer
  - Network addressing, scalability, hierarchical addressing
  - Fragmentation as an example to deal with heterogeneous link layer technologies
  - Routing protocols and algorithms: link state, distance vector
- Link layer
  - Addressing, ARP
  - Medium access control, especially random access
  - Interaction between link and network layers
Key topics (3)

- Wireless Networks
  - 802.11
- Security
  - Confidentiality, message integrity, authentication
  - The role on encryption in these
  - Symmetric key and public key cryptography
  - Firewalls
What next?

• COMP 9332: Network Switching and Routing
• COMP 4336/9336: Mobile Data Networks
• COMP 3441/9441: Security Engineering
• COMP4337/9337: Wireless Network Security
• COMP6337: IoT Experimental Design Studio
• Undergraduate/Postgraduate Projects and Thesis – Come work with us (Networked Systems and Security Research Group)
Practice Problem (1)

• When the traffic load on the LAN is very light, which of the following two MAC protocols: Token-passing or Ethernet has a smaller delay? Explain briefly.

• Answer:

Review
Practice Problem (2)

- Consider two hosts A and B that are connected via a direct link. Assuming that
  - Host A is the transmitter and host B is the receiver
  - The transport layer for hosts A and B uses selective repeat with a window size of $t$ for reliable delivery
  - The link connecting A and B uses selective repeat with a window size $m$ for reliable delivery
  - The link layer has sufficient memory to buffer at least $\max(t,m)$ frames
  - The receiver at link layer will pass all received frames (provided that they are not corrupted) to the transport layer, even if they are out of order
  - One segment will generate one packet and will in turn generate one frame. There is no packet fragmentation.
  - Congestion control and flow control are not used at both the transport and link layers.
Practice Problem (2)

- If $t = 10$ and $m = 5$, what is the maximum number of out of order buffered segments at the transport layer of host B?
- If $t = 10$ and $m = 20$, what is the maximum number of out of order buffered segments at the transport layer of host B?
Since the link layer will pass all frames to the transport layer, the number of out of order buffered frames = number of out of order buffered segments.

(t = 10, m = 5) If t = 10, the transport layer can send 10 segments at most but the link layer is limited to send 5 frames, so the maximum number of out of order buffered frames is 4, so is the number of out of order buffered segments.

(t = 10, m = 20) If t = 10, the transport layer can send 10 segments. However, with m = 20, the link layer can send up to 20 frames but will only get a maximum of 10 segments at a time. So, the maximum number of out of order buffered frames is 9, so is the number of out of order buffered segments.

Practice Problem (2)
Practice Problem (3)

- Consider the following 3 applications over a wireless network
  - Voice-over-IP, where packets are very small and the send rate is constant
  - MPEG movie streaming, where the packet size is large and the send rate is variable
  - Instant messenger chat, where packet size is small and send rate is variable
- For each application, list and explain which of the following MAC protocols you would use – (i) TDMA, (ii) plain CSMA/CA (iii) CSMA/CA + RTS/CTS
VoIP: TDMA, because we can easily split up each constant rate flow into constant size slots.

Movies: CSMA/CA + RTS/CTS because collisions of large packets are expensive and we want to avoid them. TDMA would not allow efficient use of the medium because the send rate is variable.

Messaging: plain CSMA/CA since the overhead of RTS/CTS is not worth it for small packets. TDMA is not suitable for the same reason as above.

Practice Problem (3)

- Answer:
Each node in a network runs Dijkstra’s algorithm to compute its shortest paths to all the other nodes (assume that every node gathers all the needed information correctly). Node A determines that its shortest path to node B contains 5 links and has a cost of 60. Node A also determines that its shortest path to node D contains 11 links, has a cost of 90, and passes first through node B and then through node C. Node B determines that its shortest path to node D contains 7 links, has a cost of 21, and does not pass through node C. Is such an outcome possible? Why?

Answer: It is not possible. Otherwise, there would be a path from A to D with a cost of 60 + 21 = 81 which is less than 90, the cost of the shortest path from A to D.
Practice Problem (5)

- Host A uses TCP Reno to transfer a file to host B. The file contains 32 MSS of data. During the first transmission round, the congestion window is equal to 1 MSS. During the fourth round when the connection is still in the slow-start mode, all the transmitted packets are lost (and, therefore, host A transmits less during the fifth round). There is no packet loss during any other round. During what round does host B receive the complete file? Explain.
Practice Problem (5)

In the slow-start mode, the congestion window doubles in size each transmission round. During the fourth round when the congestion window equals to 8 MSS, all 8 transmitted packets are lost. Hence, the sender determines the losses via a timeout, sets the threshold to 4 MSS, and reduces the congestion window to 1 MSS. Starting from the fifth round, the sender retransmits the lost data and then transmits the remaining portion of the file. The congestion window doubles until it becomes equal to the threshold (i.e., 4 MSS) during the seventh transmission round. Then, the TCP connection switches to the congestion-avoidance mode and increases the congestion window by 1 MSS per transmission round. Host A finishes the delivery of the 32-MSS file during the tenth round.
Practice Problem (6)

• Consider a TCP Reno connection between two hosts with a large amount of data packets flowing in only one direction. Assume a malicious router along the path drops every other data segment of this connection (i.e. it drops 2, 4, 6, etc.). Assume that the receiver’s advertised window is 256 MSS. Also assume that there is plenty of bandwidth available on the path, so as to accommodate a TCP window size of 64 MSS in the absence of the malicious router.
  • (a) What is the maximum window size achieved on this connection?
  • (b) Repeat (a) for the case when the malicious drops every eight packet (say 8, 16, 24, etc.)
Practice Problem (6)

• Answer:

(a) Maximum window size = 2. This is because the transmission of every second packet causes a timeout followed by slow start. In other words, the window size will oscillate between 1 and 2.

(b) Window size will grow up to 8. When packet #8 is dropped, the congestion window = 8. Several duplicate ACKs are returned which would trigger fast retransmit (window cut to half). This behaviour will keep repeating as every time the congestion window is 8 one packet will be lost. So the window will never increase beyond 8.
Practice Problem (7)

• Consider a network architecture that has $n$ layer protocol hierarchy. Applications generate messages of length $M$ bytes. At each of the layer, an $h$-byte header is added. What fraction of the network bandwidth used by the application is wasted on headers?

• Answer:
Practice Problem (8)

• Assume that a group of 10 people wishes to communicate securely with each other. Each member of the group needs to send secret data to the other 9 people within the group. All communication between any two people $p$ and $q$ is visible to all other people in this group and no other person in the group should be able to decode their communication.
  
  • (a) If the group decides to use symmetric key encryption, how many keys are required in the system as a whole?
  
  • (b) Instead if public key encryption is chosen, how many keys would be required?
Practice Problem (8)

• Answer:

(a) if symmetric key encryption is used, then each pair of people communicating would require their own unique key. For N people this comes out to \( \frac{N(N-1)}{2} \). Hence, for N=10, we have 45 (= 1 + 2 + 3 + ....+ 9).

(b) For public key encryption, each user needs its own public private key pair. All the other users to send data to him can use the public key. So in this case, 10 pairs of public and private keys will be needed.
Last Goodbye :( 

- Hope you enjoyed the course 
- Hope you learnt a lot 
- Hope you know more about computer networks than you did 3 months ago 
- Good Bye !! 
- Good luck for the exam and the future 
- Have a great break 
- Please fill in feedback