CSCD330 – Computer Networks

Midterm, Winter 2021 v. 1.1

Due: 15 FEB 2021, 11:59pm

Ian Kaiserman

Instructions: Write your answers to the following questions. A good idea would be to copy-andpaste these questions to your document followed by your answer. Add citations for anything you find not in the textbook or lecture notes. BE AWARE: NO LATE SUBMISSIONS WILL BE GRADED.

1. Go to the Electronic Freedom Foundation (EFF) website. The link is to their Take Action area: EFF Take Action Page. You are to read some of the Take Action items and choose one that interests you to learn more about. (Take action if you choose.) Write a paragraph (or two) about the issue and your thoughts about it. Also, research a bit about the EFF, what it is and what they do. Write a few sentences to let me know that you know the purpose of the EFF.

   A Take Action article that stood out to me was one of the most recent ones concerning face surveillance/recognition in Minneapolis. As someone who has used facial recognition on mobile/laptop devices in the past, I know firsthand how inaccurate this technology is in its current state. Obviously, something that is being used more officially is going to be more powerful than a consumer mobile device but given the evidence of false matches and erroneous data from various cases in Minneapolis, it seems to be a problem on that level too.

   I believe that facial recognition is a very powerful but underdeveloped tool, one that could have a good impact in aiding crime check and surveillance, but it is such an early and faulty technology currently, and a technology that is being used to carelessly (data breaches have happened from unsecured data), that it is unwise to be implementing it right now. There have been reports of some people groups being flagged erroneously, like black people and women, simply because the algorithms

are too early to be able to identify people deeply enough. These people are then having to go through the trouble of proving themselves innocent when they did nothing to get into said situation.

After doing some research on their website, the EFF seems to be an organized group doing what everyone has been so on edge about as of lately – searching into and fighting for digital liberties and privacy. They are dedicated to thorough research into issues of data security, privacy, and freedoms, and they are spreading the word of mishaps that happen around the world in the digital scene.

2. If the current TCP estimated round-trip time, EstimatedRTT, is currently 30 msec and the following acknowledgements come in after 26, 32, and 24 msec, respectively, what is the new EstimatedRTT value? What should the timer duration be for the next segment to be sent? (Use the typical coefficient values given in the lecture for your computation. Assume perfect synchrony between previous SampleRTT and EstimatedRTT values to all prior traffic and, thus, a value of zero for the current DevRTT. Showing your work may allow partial credit to be given.)

   EstimatedRTT = (1-0.125)*30ms + 0.125*26ms = 29.5ms (first est)

   DevRTT = (1-0.25)*0ms + 0.25*|29.5ms-30ms| = 0.875ms (first dev)

   EstimatedRTT = (1-0.125)*29.5ms + 0.125*32ms = 29.813ms (second est)

   DevRTT = (1-0.25)*0.875ms + 0.25*|32ms-29.813ms| = 1.203ms (second dev)

   EstimatedRTT = (1-0.125)*29.813ms + 0.125*24ms = **29.086ms (final est)**

   DevRTT = (1-0.25)*1.203ms + 0.25*|24ms-29.086ms| = 2.174ms (final dev)

   Timeout = 29.086ms + 4*2.174ms = **37.7813ms (timeout after third)**

3. Suppose that the roundtrip delay between sender and receiver is constant and known to the sender. Would a timer still be necessary in protocol RDT 3.0 assuming packets can be lost? Explain.

Yes, because a timeout can still occur which would not be consistent with the "constant and known delay", which means the protocol still needs to know when to resend the packet if a timeout occurs.

4. Some cybersquatters have registered domain names that are misspellings of common corporate sites, for example, `www.microsfot.com`. Make a list of at least five such domains.

   Googel.com

   Cacebook.com

   Tiwitter.com

   Amazin.com

   Miinecraft.net

5. What are the five layers in the Internet protocol stack? For each of these layers, what are the principal responsibilities of each of these layers?

   Application layer – handles network applications and how they handle data, e.x. FTP, SMTP, HTTP

   Transport layer – handles data transfer between processes and hosts, e.x. TCP, UDP

   Network layer – handles the routes between hosts for efficiency and consistency, e.x. IP addresses

   Link layer – handles data transfer between local devices, e.x. Ethernet connections

   Physical layer – handles the physical transfer of information over wires

6. The following questions can pretty much be found in the lecture notes. You can search for the answers if needed. If you use an answer from the Internet, please site the source of the answer.

    a. What is an ephemeral port? What port number range is typically defined for these ports? **An ephemeral port is a temporary port number. The port number range for ephemeral ports varies between systems but is usually in the much higher numbers of the 1-65535 range. IANA defines the range to be 49152-65535 (https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml)**

    b. Briefly list the differences between TCP and UDP. **TCP is defined as reliable transfer, with a two-way connection established before data is transferred, built-in flow control and congestion control, and error checking for packets being sent to make sure they get to their destination, in order and on time. UDP is defined as unreliable, no connection is established before-hand, packets are simply given a destination IP and port number and sent on their way, with no regard to if they make it to their destination or not.**

    c. Show code to create an input stream to a Java Socket.

    BufferedReader input = new BufferedReader(new InputStreamReader(socket.getInputStream()));

    d. Show code to create an output stream to a Java Socket.

    PrintWriter output = new PrintWriter(socket.getOutputStream(), true);

    e. What does the following snippet of code do?

```
System.out.println(InetAddress.getLocalHost().getHostAddress());
```

This line calls the InetAddress class method getLocalHost to get the local host as an InetAddress object, then calls getHostAddress to return the host address as a String.

7. Write a pseudocode algorithm that describes the ***receiver*** side of RDT 3.0. Assume all the method/function calls needed are already defined. Which calls should be blocking (that is, not returning until some external stimulus is received)? **Since RDT 3.0 only changed how the sender handles retransmissions, the receiver side is the same as RDT 2.1**

   If(receive(packet) && ! corrupt(packet) && seqNum0(packet)) {

   Extract (packet, data)

   Deliver(data)

   Send (makePacket(ACK, checksum)) }

   Else if(receive(packet) && corrupt(packet) {

   Send (makePacket(NAK, checksum)) }

   If(receive(packet) && ! corrupt(packet) && seqNum0(packet)) {

   Send (makePacket(ACK, checksum)) }

   // Algorithm loops with same steps, only this time with seqNum1(packet)

   // Since the receiver side is essentially the same, the sequence numbers

   // help tell the sender if the ACK/NAK it receives are from the newest

   // packet or an older packet.

8. Consider a reliable data transfer protocol that uses only negative acknowledgements. Suppose sender sends data only infrequently. Would a NAK only protocol be preferable to a protocol that uses ACK's? Why? Now, suppose the sender has a lot of data to send and the end-to-end connection experiences a few losses. Now, would a NAK-only protocol be preferable to a protocol that uses ACK's? Why?

1. **ACK's are more practical for the first scenario, since data is not sent very frequently, it is better to know that the data was received correctly every time and not have to deal with verification.**
2. **NAK's are more practical for the first scenario because using ACKs for larger, more frequent amounts of data is a waste of resources compared to only receiving NAKs for failed receipts. The error checking can then be done on those NAKs.**

9. What are two differences between HTTP/2 and HTTP 1.1?

   HTTP/2 has multiplexing which allows for fetching multiple objects over a single connection and transmits data in binary for more efficient transmission. HTTP/1.1 had neither of these functions.

10. Give a real-world analogy for transport-layer multiplexing and **transport layer demultiplexing that does not rely on mail or letters.**

    Fast Food analogy:

    Multiplexing is look at orders from customers, making all the food needed for said customers, and grouping the food based on the orders.

    Demultiplexing is delivering each encapsulated order of food to the correct customer once it is prepared.

11. Suppose Alice, with a Web-based email account (such as Hotmail or gmail), sends a message to Bob, who accesses his mail from his mail server using POP3. Discuss how the message gets from Alice's host to Bob's host. Be sure to list the series of protocols (not below the transport layer) that are used to move the message between the two hosts. **Alice's web-based account sends the email using IMAP to the email server. The email server then sends the message via SMTP to the ISP. The message transfer agent in the ISP sorts the email into Bob's mailbox on a POP3 server. When Bob connects to his UA, The POP3 server sends the message over POP3 to Bob's PC, where it is stored locally.**

12. List two advantages and two disadvantages of having international standards for network protocols.

    Advantages: more universal standards that can apply to development and usage of networks regardless of language boundaries. Applications built to work on a network can be built a singular way and work anywhere in the world, separate development for different regions is not necessary.

    Disadvantages: Because they are international, they are also known by all, meaning one institution's systems are vulnerable to the same hijacking attacks from anywhere in the world. Standards used internationally can end up being hard to maintain/enforce and truly apply globally without some sort of conflict.

13. Sloth Bank wants to make online banking easy for its lazy customers, so after a customer signs up and is authenticated by a password, the bank returns a cookie containing a customer ID number. In this way, the customer does not have to identify himself or type a password on future visits to the online bank. What do you think of this idea? Will it work? Is it a good idea?

    Will it work? Technically yes if the cookies are kept consistently. All that the website would have to do is look for that cookie, get the customer ID, check if it is valid, and work from there. Is it a good idea? Not at all. Account credentials going through a secure server are much safer from potential cyberattacks than unlocked cookies being stored on a local machine. The cookie could easily be hijacked by malicious scripts and injected into someone else's system to be used by them.