CSCI-GA.2620-001 final (55 points)

May 3, 2018

Instructions

1. Write your name and N number on top.
2. Provide concise and clear explanations for all your answers.
3. Use the other side of each sheet if you need more space.
4. The questions are roughly in the order of the lectures.

1. (4 points) Derive the TCP throughput equation that relates the packet loss probability and the minimum round-trip time on a link to the throughput achieved by AIMD TCP over this link.

2. (3 points) Use the TCP throughput equation you derived above to estimate the packet loss probability at which TCP throughput falls to 1% of the link's capacity. Assume a link with a minimum round-trip time of 100 ms and a link capacity of 1 Gbit/s.

3. (2 points) Give two scenarios in which BBR outperforms TCP Cubic. For each of these scenarios, what is the metric on which BBR outperforms TCP Cubic?

4. (2 points) What performance property does WFQ provide that XCP doesn't? In what way is a router implementation of WFQ more challenging than a router implementation of XCP?

5. (2 points) In BGP, route advertisements are implicitly trusted, i.e., all routers assume that all other routers are honest. Give an example of what could happen if routers lied in their advertisements. There isn't one right answer to this question. I'll accept anything that's well justified.

6. (3 points) Assume you're an AS/ISP with two paths to the Internet—maybe one through Comcast and another through Verizon. How would you use BGP to advertise to the rest of the Internet that you would prefer to receive traffic through Comcast and would only want to use Verizon as a backup?

7. (2 points) Give one example of a routing policy that is easy to achieve using SDX but much more cumbersome with BGP.

8. (2 points) In the VL2 paper, why is randomized load balancing performed at the granularity of flows instead of packets? What is the drawback of performing load balancing at the level of flows instead of packets?

9. (1 point) How is the ECN marking required for DCTCP implemented using an off-the-shelf non-programmable switch?

10. (2 points) In what ways is a wired Ethane switch simpler than a commercial wired Ethernet switch? If the switch itself is simpler, where does all the complexity reside in an Ethane network?

11. (2 points) Give three examples of the kinds of flexibility that RMT provides relative to a fixed-function Ethernet/OpenFlow switch. Give an example of the kind of flexibility that RMT does not provide.

12. (3 points) What groups of people benefit from a technology like RMT? Why?

13. (3 points) What security properties does TLS provide? Describe these properties as precisely as possible.

14. (2 points) Describe the Heartbleed vulnerability.

15. (2 points) How can the Heartbleed vulnerability be fixed?

16. (2 points) Give examples of unauthorized data that the Heartbleed vulnerability allows an attacker to access.

17. (2 points) In the paper on censorship circumvention by Ensafi et al., what is the key weakness of the obfs2 protocol? How does obfs3 fix this?

18. (2 points) Why did the "Low cost traffic analysis" authors configure TCP_NODELAY when performing their experiments? Why not just use UDP instead?

19. (2 points) In the Sprout paper, why does Saturator try to maintain a relatively high target delay (i.e., between 750 and 3000 ms)?

20. (2 points) Why does Saturator use two phones when attempting to saturate the cellular network? What would happen if Saturator instead tried to saturate both the uplink and the downlink of a cellular network using a single phone?

21. (3 points) In the LTEye paper, what is the C-RNTI? How is it used? When is the C-RNTI reassigned? How does the LTEye system handle these reassignments?

22. (3 points) Describe the difference between regular MIMO and multi-user MIMO using a diagram that illustrates where the transmit and receive antennas are located in each case. Where does the channel matrix inversion happen in each case?

23. (2 points) What is the difference between the multi-user MIMO problem and the distributed MIMO problem, i.e., the problem that MegaMIMO solves? As a consequence of this difference, what is the key technical contribution of the MegaMIMO paper?

24. (2 points) What is the conceptual difference between analog and digital self-interference cancellation in the full duplex paper? (Besides the fact that one is analog and the other is digital!)