Network Systems (201300179/201400431), Test 4

April 4, 2016, 13:45–15:15

- This is an open-book exam: you are allowed to use the book by Peterson & Davie and the reader that belongs to this module. Furthermore, use of a dictionary is allowed. Use of a simple (non-graphical) calculator is allowed.
- Other written materials, and laptops, tablets, graphical calculators, mobile phones, etc., are not allowed. ***Please remove any such material and equipment from your desk, now!***
- Although the questions are stated in English, you may answer in English or Dutch, whichever you are more comfortable with.
- You should always explain or motivate your answers, with so much detail that the grader can judge whether you understand the material; so just saying "yes" or giving a formula without explanation is not enough.
- Visiting the toilet without explicit permission of the supervisor is not allowed. During the last 30 minutes of the exam, no toilet visits are allowed.

1. Congestion Control

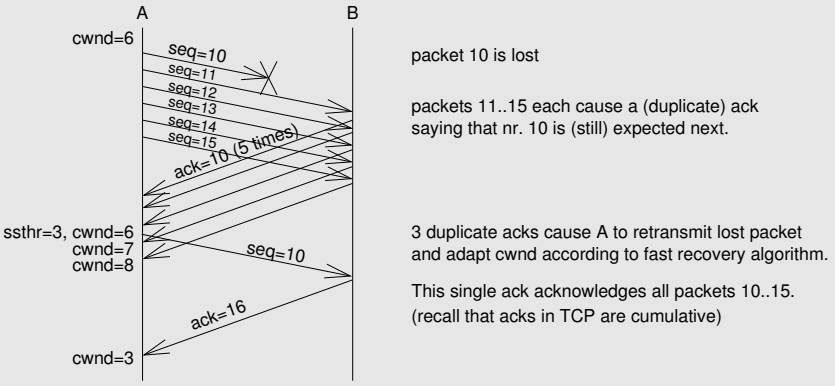
Consider a TCP connection between hosts A and B which has been active for a while, with host A sending data to host B. At some point, the `CongestionWindow` = 6 MSS and `SlowstartThreshold` = 8 MSS (see footnote[1]).

2 pt (a) What was the `CongestionWindow` at the time of the most recent packet loss? Explain.

16, because upon packet loss, the `SlowstartThreshold` is set to half the `CongestionWindow`.

Assume no packets are currently outstanding; thus, host A is allowed to transmit 6 packets next. For simplicity assume MSS = 1 byte. Host A's current sequence number=10.

3 pt (b) Assuming that the first of those six packets is lost, how many RTTs does it take until these 6 packets have been succesfully sent and acknowledged?
Explain your answer by drawing a time-sequence diagram, in which you indicate all packets with their sequence/acknowledgement numbers; also indicate changes of the congestion window, if there are any.



Clearly, it takes 2 RTTs.

See figure 6.12 in the book for a very similar example.
Many different kinds of errors were made, such as not sending 6 packets immediately (even though the question said that would happen), acking packtets 11...15 before 10 has come in (that's not possible because TCP's acks are cumulative), and needing a timeout for retransmission instead of detecting the triple duplicate ack.

Many students simply forgot to say anything about the congestion window.

[1] By `SlowstartThreshold`, we mean the same thing which is called `CongestionThreshold` in the book. The former name is much more common though.

2 pt (c) UDP is used a lot for DNS traffic, but doesn't have congestion control. Why isn't this a problem?

DNS traffic is a very small proportion of the total network traffic (perhaps 1 pair of UDP packets (request+response) per entire TCP flow), so it contributes rather little to the total network load.

Many said that congestion control is no issue because UDP doesn't offer a reliable data transfer anyway. That's true, but congestion control is not just about preventing your own packets from being dropped; it's mostly about not overloading the network, i.e., being nice to other users of the network.

---

2. QoS

2 pt (a) Why is overprovisioning, without advanced techniques like fair queueing, differentiated services, etc., usable for some real-time applications and not for others?

Overprovisioning does not provide hard guarantees, it just makes sure *most* packets are not dropped or excessively delayed. Some applications can tolerate this (e.g., audio, where a dropped packet just causes a brief interruption), others need solid guarantees (e.g., remote control of a surgery robot).

Many pointed out that applications like netflix and youtube do lots of buffering to handle network delays, while other applications like internet telephony can't do that because the delays would make it unusable. This is true (and still got 1 point), but one could argue that applications which can accept arbitrary buffering delays are not really real-time applications; and secondly, things like internet telephony work well in an overprovisioned network, because *most* packets still arrive in time and they can tolerate occasional loss.

3 pt (b) Suppose we would use Fair Queueing, but treat every packet as a separate traffic flow. Is this equivalent to First In First Out queueing? Explain.
(Hint: consider what happens if two big packets arrive, immediately followed by a small one.)

No, it isn't. Suppose two big packets arrive, immediately followed by a small one. With FIFO, they would go out as big1, big2, small. With FQ, the first big packet would go first, but the outgoing link would still be busy when the other two packets arrive; in bit-by-bit RR, the small one would be completed first, so our FQ would do big1, small, big2.

---

3. Security

2 pt (a) When using PGP for secure e-mail, can the sender be sure about the identity of the receiver, and/or can the receiver be sure about the identity of the sender? Explain.

Yes in both directions. Only the intended receiver has the correct private key to decrypt the session key, and thus get access to the e-mail contents. And the receiver can verify the mail's signature which can only have been generated by the sender since (s)he's the only one with the correct private key.

Of course, all of this assumes the keys have been properly handled; private keys have been kept secret, and public keys have been distributed in such a way that both parties are sure about each other's public keys.

2 pt (b) A firewall at the border of a company or university network (i.e., at the point where this network is connected to the rest of the Internet) is often configured to drop incoming TCP packets whose destination port is 22, which is the port number for ssh. Why is this useful? Isn't ssh ("secure shell") secure enough?

It's an extra layer of defense: it prevents attackers from trying lots of passwords (hoping a user has a weak password), or exploiting bugs in the ssh server software.

Many wrote that ssh is not intended to be used from outside a company/university network; that is in general not right, secure remote login is exactly what ssh is meant for. However, the university or company may choose not to allow it from the outside, or limit outside access to one or a few well-maintained servers.

3 pt (c) To what extent can or cannot IPSec in transport mode help against the following security risks:

(i) traffic analysis; in particular, suppose you're sending an e-mail using SMTP, can an eavesdropper still see that it is mail and/or where it goes? Explain.

(ii) reflected Denial-of-Service attacks. Explain.

(i) Eavesdropper only sees the IP addresses; so (s)he can see to what server it is delivered, but not the e-mail addresses (that's in the encrypted data part), nor that it is mail (since the TCP portnumber is also in the encrypted part).

(ii) In a reflected DoS attack, the attacker sends packets with a faked source IP address (namely, the address of his victim, hoping the DNS server will send the reply to the victim). IPSec provides authentication, which would prevent the attacker from sending a valid packet with his victim's address as the source address. Of course, this assumes that the DNS server is configured to only respond to properly authenticated requests and no longer responds to non-IPSec requests.

---

4. Time synchronization and localization

3 pt (a) To determine the position, many positioning algorithms use a mean to determine the distance.

(i) What mechanisms are used to estimate the distance? (mention at least 3)

(ii) What is the difference between RSS and CSI?

(iii) What are the main parameters in the Log Normal Shadowing model that needs calibration?

3 pt (b) The Global Positioning System (GPS) is used in many outdoor applications.

(i) On what type of positioning is GPS based, and what phases (steps) can be identified?

(ii) How many satellites are needed for GPS positioning? Why that number?

(iii) Why does GPS not work well in an indoor environment?

3 pt (c) In time synchronisation all methods rely on message exchange between nodes. However, this causes some message latency uncertainties. What are the reasons behind those uncertainties (mention 5 reasons).

End of this exam.