Please see the attached report.
COMP28411 Examination Performance Feedback
2017-2018

Fact that majority of students chose not to attend lectures was very evident in answers given in the examination.

Question 1

a) The question was looking for both what each term meant and why it is important.

Many answers only defined the terms and not why it matters in the context of successful long term deployment. Some answers failed to give answers for all three terms.

b) The question was asking for the description of two approaches, drawback of using these and how to mitigate the drawbacks..

Generally the description of the two approaches was well done. However, information on their drawbacks and in particular on how to mitigate them was often absent.

c) Again the question was looking for a description of the properties and why there were important..

Answers generally described what confidentially was well. They also reasonably described why it was important. A significant number of answers showed a lack of knowledge about non-repudiation.

d) This question was looking for the use of a symmetric key to encrypt the message so that it was confidential at minimal cost. The message being signed by Alice was still required to prove that it was unaltered and from Alice. The question also stated that this needed to be achieved in a single message.

Some of answers suggested exchanging a number of messages, this is unnecessary and failed to achieve the requirements of the question. Others suggested encrypting the whole message with a public key, this is computationally expensive and thus not meeting the requirements set out in the question. Others suggested encrypting the message with a private key, but then anyone could decrypt the message and it would not be confidential. Some answers even suggested double encryption using Alice’s private key and Bob’s public key. This is even more computationally expensive, and anyone can undo the application of Alice’s private key. A significant number of answers correctly identified creating a symmetric session key to encrypt the message and sending it securely to Bob using his public key. A few forgot to transfer the session key to Bob.

Question 2

a) The question listed three classes of multimedia data, and asked what they might be used for and the sort of QoS parameters that they would require.

Overall this question was reasonably answered. A few people forgot to indicate what the data might be used for. Some answers were also lacking detail in how the described the QoS parameters required.

b) This question specifically asked for the application-level network architecture that would be required to support the scenario given. Hence, it was looking for a description that included distributed servers, but given the size and geographic distribution of the users, there would need to be a structure to how these were arranged; probably in a tree.

Most answers got the fact that a distributed set of servers would be required. However, they failed information on how these would be arranged. Some answers just indicated at a CDN should be used. Although the answer is a CDN, just indicating the use of one fails to give the detail required. Some answers incorrectly gave details for mechanisms that were not at the application-level.

c) This question was specifically not asking for a description of the DASH protocol, but why the DASH protocol, or something similar, is needed. The elements that matter are providing the best quality possible, bandwidth dependent; doing this efficiently, not sending more data than can be used; screen resolution dependent; the situation constantly changes, thus monitoring and adaptation are required.
Generally answers covered the point of getting the maximum possible data through the available bandwidth. Many answers fail to highlight how the screen resolution affects the volume of data needed. Some answers did not mention the need for constant monitoring and adaptation.

d) The question specifically asks for an implementation of reliability that gives minimal delay and minimal overhead. In practice the question is asking for a comparison of the go-back-n, selective-ack and nack approaches to implementing reliability as they relate to the scenario given. Including nack in the approach proposed will ensure minimal delays. As selective-ack has constant overhead and go-back-n has an overhead when recovering, and there will be little recovery, go-back-n approach will give the minimal overhead. The question also asked for justification of the approach proposed.

Answers were of variable quality. Many assumed that the selective-ack approach has no overhead, which is not true. The best approach combines go-back-n with nack, answers tended to just select one approach. Also, many answers fail to justify why the approach proposed would fulfil the needs described in the question.

**Question 3**

a) The question was asking for a description of the two terms and why they affected the bandwidth available to an application.

A significant number of answers showed confusion between transmission delay (the time needed to send data into a communications channel) and propagation delay (the time for data to travel along the communications medium).

b) The question is specifically asking about techniques for detecting errors and for a comparison of their quality/cost. It is not asking for error correction techniques.

Answers that talked about error detection choose two from simple parity, internet checksum and CRC. These answers were okay, but there was some confusion of the comparison between internet checksum and CRC (CRC is much better at detecting errors). A significant number of answers incorrectly described error correction techniques.

c) The question was looking for reasoning about the usefulness of carrying out link level error recovery. It was not asking about error recovery techniques.

A number of answers gave good reasons about the justification (if communications is over unreliable wireless links then yes, otherwise no). However, a significant number of answers failed to address the question.

d) The question was looking for a compare and contrast of either FDM or TDM with CSMA, followed by a justified recommendation of which to use in the given scenario. The low volume of data implies that CSMA collisions are unlikely. The description is that there is a low volume of data. This could imply occasional bursts of data rather than a continuous stream of data.

Many of the answers given lacked a detailed comparison and justification. There was also often an assumption that with CSMA there would be many collisions; not true. One thing that was often overlooked was that with CSMA uses the communications channel, it gets all of the available bandwidth and therefore data arrives at the earliest possible time, with ether of the division multiplexing approaches, clients only ever get part of the available bandwidth.

e) The question was looking for techniques that allowed mobile users to be located followed by ways to be this efficiently. This means some static ‘home’ registration that is informed by the users current location; i.e. a network wide system.

Answers that gave techniques for registering current locations usually described how to make this efficient by not routing data through the home location. However, most failed to address the last part of the question that was what happens when the mobile user changes location. A significant number of answers described how to locate a local access point. This is the mobile user getting access to the network, not having its location known by other users.