Examination Mobile & Wireless Networking (192620010)
April 08, 2020
13.45 – 16.45

Solutions

Notes:

- *The only sources that will be allowed during this exam are:*
  - *The book "Wireless Communication Networks and Systems" by Cory Beard & William Stallings, in any format (printed or electronically)*
  - *The reader (printed or electronically)*
  - *The slides used in the lectures (printed or electronically). If there is at most 4 A4, 11 pt font worth of personal notes on the sheets, that is allowed.*
  - *A dictionary (only printed)*
  - *A calculator (only a dedicated device or a dedicated calculator program on your computer, online calculators are not allowed)*
  - *If explicitly approved by the lecturer: 2 double-sided sheets of notes (max. A4, any font size/density)*
- *Please note that in all cases, you will have to formulate the answer to questions yourself. Answers to questions containing text copied verbatim from one of the sources will be rewarded with 0 points.*
- *Indications like "[10]" at questions mean that you can obtain 10 points for that question.*
- *Please write your name and student number at the top of the document you are going to hand in.*

Abbreviations

ACK	-	ACKnowledgement
Addr	-	Address
AODV	-	Ad-hoc On-demand Distance Vector
AP	-	Access Point
CSMA/CA	-	Carrier Sense Multiple Access with Collision Avoidance
CTS	-	Clear To Send
CW	-	Contention Window
DCF	-	Distributed Coordination Function
Dest	-	Destination
DIFS	-	DCF Inter Frame Spacing
EDCA	-	Enhanced Distributed Channel Access
eNodeB	-	evolved Node B (base station in LTE)
FDD	-	Frequency Division Duplex
IEEE	-	Institute of Electrical and Electronics Engineers
LAA	-	License-Assisted Access
LAN	-	Local Area Network
LTE	-	Long Term Evolution
LTE-U	-	LTE Unlicensed
LWA	-	LTE-WiFi Aggregation
MPR	-	Multi-Point Relay
NBR	-	NeighBouR
OFDM	-	Orthogonal Frequency Division Multiplexing
OLSR	-	Optimized Link State Routing
PRMA	-	Packet Reservation Multiple Access
RREP	-	Route REPly
RREQ	-	Route REQuest
RTS	-	Request To Send
Seq#	-	Sequence number
SIFS	-	Short Inter Frame Spacing
TC	-	Topology Control (message)
TV	-	TeleVision
WEP	-	Wired Equivalent Privacy

0 Integrity Statement

Please read the following paragraph carefully and copy the text below it verbatim to your answer sheet. To find more information, please consult https://www.utwente.nl/en/education/student-services/remoteassessmentwebsite.pdf.

By testing you remotely in this fashion, we express our trust that you will adhere to the ethical standard of behaviour expected of you. This means that we trust you to answer the questions and perform the assignments in this test to the best of your own ability, without seeking or accepting the help of any source that is not explicitly allowed by the conditions of this test.

Text to be copied:

I will make this test to the best of my own ability, without seeking or accepting the help of any source not explicitly allowed by the conditions of the test.

1 Wireless Communications [13]

Consider two hypothetical cellular systems. The first system operates at the 400 MHz frequency band and the second system operates at the 60 GHz band. Assume both systems use isotropic antennas, and both transmit with a transmission power of 1 W. The pathloss exponent of the environment is 3. For a receiver to successfully decode the incoming traffic, the received power of the signal must be above -110 dBW.

a) It is known that the range and hence the coverage area of a transmitter depends on the frequency used.

How many transmitters at the frequency giving the smaller range would you need if you want to cover the same area as a transmitter at the frequency giving the larger range? *Please show your calculation. You can round your range and number of transmitter values to integer values.* [3]

Solution: *The question asks for the coverage radius of each transmitter. Similar to Exercise 5.3 in the book (Chapter 5), you need to calculate the path loss L_{dB}.*
Received signal = (Transmitted signal - Pathloss) must be above -110 dB.
$10\log(1) - L_{dB} > -110$, hence $L_{dB} < 110$ dB
$L_{dB} = 20\log(f) + 10*3*\log(d) - 147.56$ dB < 110 dB

$\log(d) < (257.56 - 20\log(f))/30$

Now, for two frequencies, we calculate L_{dB} as follows:

f=400MHz:

$\log(d) < (257.56 - 20\log(400*10^6))/30 = (257.56-172.04)/30$
$\log(d) < 2.85$ which gives us $d<10^{2.85} \sim 707$ meters.

f=60GHz:
$\log(d) < (257.56 - 20\log(60*10^9))/30 = 42/30=1.4$. Then, d~25 meters.

The transmitter operating at lower frequency, i.e., 400 MHz, has much larger coverage radius. To find the number of transmitters to cover the same area, one simply needs to find the coverage area of each transmitter. $A_{400MHz}=A_{60GHz}*N$ where N would be the number of transmitters needed. Roughly to cover the same area, square of the ratio of the coverage radius gives us the number of transmitters: we can find $(707/25)^2 \sim 799$ transmitters. Hence, you need 798 more transmitters.

b) For the above-mentioned cellular systems operating at 400 MHz and 60 GHz, calculate the length of an antenna if the antenna length is one-half the wavelength of the transmitted signal. Based on the calculated antenna sizes, discuss whether it would be possible to have one or more such antennas at a mobile handset. [2]

Solution: *For each frequency, we need to calculate the wavelength of the signal using formula $\lambda = c/f$ where c is the speed of light ($3*10^8$ m/s) and f is the frequency in Hz.*

$\lambda_{400MHz}=c/f = 3*10^8/(400*10^6) = 75$cm. Then, antenna size is 37.5 cm.
$\lambda_{60GHz}=c/f = 3*10^8/(60*10^9)= 5$ mm. Then, antenna size is 2.5 mm.

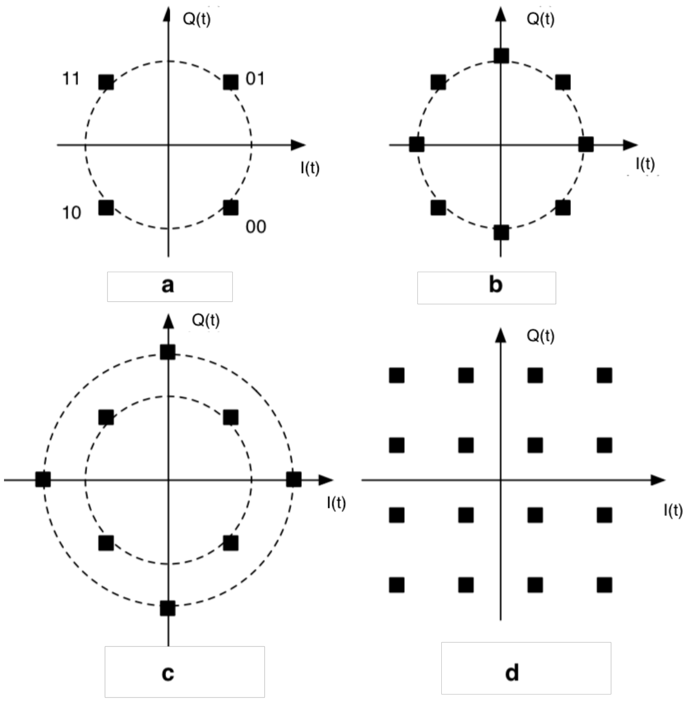
For lower frequency, the antenna size is quite large making it hard to be used by small form-factor devices. For GHz band, on the contrary, the antenna size is quite small making it possible to use even multiple antennas at a user handset.

c) Consider a 40 MHz OFDM system. Suppose that the length of one OFDM symbol including the cyclic prefix is 4μs and 20% of this duration is due to the cyclic prefix. How many subcarriers does this OFDM system have? [2]

Solution: *Similar to the exercise of Lecture-2, we need to find the subcarrier spacing f_s to find the total number of subcarriers in a bandwidth of 40 MHz. Since f_s equals to $1/T_s$, we need to find the symbol duration T_s first. Then, if 20% of a symbol is the cyclic prefix, then the OFDM symbol duration is 4*0.8 = 3.2 μs. Consequently, the subcarrier spacing is 1/3.2μs = 0.3125 MHz. Given that the total bandwidth is 40 MHz, the number of subcarriers is 40/0.3125 = 128 subcarriers.*

d) Consider the following figure showing the signal constellation diagrams of four modulation schemes. For each of the 4 modulation schemes, briefly answer the following 4 questions (so, 16 answers in total): [4]

i) How many *amplitude* values are used for the modulation in each scheme?
ii) How many *phase* values are used for the modulation in each scheme?
iii) What is a logical name for each constellation type?
iv) How many bits can be transmitted at a time with a symbol?



Solution: *Chapter 5 introduces modulation techniques along with constellation diagram, phase and amplitude levels, and number of bits/symbol achieved by a particular constellation.*

a) Amplitude: 1, Phase = 4, name = QPSK, number of bits = 2 (PSK naming convention is used when only phase is used for modulation, e.g., there is a single amplitude value but multiple phases in the modulation diagram. Hence the name is xPSK with x being the number of phases used)
b) Amplitude: 1, Phase =8, name = 8PSK, number of bits = 3
c) Amplitude: 2, Phase =8, name = 8QAM, number of bits = 3 (QAM uses various combinations of phase and amplitude to create different points in the constellation diagram. In the diagram there are 8 points. Hence, 8QAM.)
(d) Amplitude: 3, Phase =12, name = 16QAM, number of bits =4 (in the constellation diagram, there are 16 points created by combinations of amplitude and phase.)

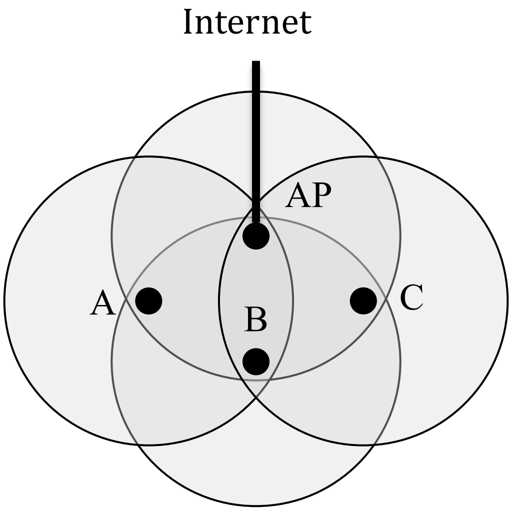
So, the answers are as follows:
i) (amplitude:1, phase:4) for a, (1,8) for b, (2,8) for c, (3,12) for d
ii) QPSK for a, 8PSK for b, 8QAM for c, 16QAM for d
iii) 2 bits, 3 bits, 3 bits, 4 bits

e) Explain the pros and cons of spread spectrum communications. [2]

Solution: *In the slides of Lecture 2, you have the pros and cons. Pros: By spreading the signal over a broad band, the signal becomes more robust against interference and frequency selective fading. Also, it makes the transmission robust against attackers. In Frequency Hopping SS, frequency selective fading and interference is limited to short period. It is simple to implement. Direct Sequence SS enables robustness against frequency selective fading, soft-handover and detection of a signal by several base stations and therefore requires less frequency planning. Multiple users can use the same spread spectrum bandwidth without interfering with one another as in CDMA. However, all these advantages come at the expense of higher complexity as there is a need for precise power control and synchronization. It requires large bandwidths.*

2 Medium Access Control and Wireless LAN [18]

Please consider an IEEE 802.11-based CSMA/CA system with the node layout as depicted in the figure below. In this scenario, nodes A, B, and C are all within transmission range of an access point AP. Nodes A and B, and nodes B and C are also within each other's range. However, nodes A and C cannot receive (and detect) each other's transmissions.



Further, we make the following assumptions regarding the parameters of the system under consideration: 1 slot = 20 µs; SIFS = 10 µs; DIFS = 2 slots + SIFS; CWmin = 1 slot; CWmax = 255 slots; transmission of a complete data frame takes 250 µs; transmission of control packets such as ACK, RTS, and CTS takes 65 µs; propagation delay is negligible, and no transmission errors occur (if transmitter and receiver are within range and no collision occurs).

a) We consider the situation in which both A and AP want to send a packet to each other, and do not use RTC/CTS. Node B is currently transmitting. A and AP start their CSMA/CA access procedure at exactly the same time, while B is still transmitting. What is the probability that the transmission of A is successful? Explain your answer. [2]

   Solution: *This probability is ½. As CWmin is 1 slot, both A and the AP have to choose between a backoff of 0 or 1 slots. If they choose the same there will be a collision, otherwise, with probability ½, not.*

b) If the transmission of A is not successful, i.e., there was a collision between the packet of A and the packet of the AP, what is the probability that A's **re**transmission is successful? Explain your answer. [2]

   Solution: *This probability is ¾. Due to the collision, both A and AP will "double" their contention window and choose a value between 0 and 3. With probability ¼ they choose the same value. Otherwise, with probability ¾, their retransmission will be successful.*

c) Now suppose the same scenario as above: Initially, B was transmitting. During B's transmission, A and AP started their access procedure, and the transmissions of A and the AP collided in the first attempt. Now, suppose during the transmissions of A and AP, which caused this collision, node C also starts the access procedure for a transmission. What is the probability that the AP manages to do a successful retransmission before C transmits? Explain your answer. [2]

   Solution: *AP can only successfully retransmit before C if it chooses a backoff value of 0, with probability ¼ (out of 0, 1, 2, 3), while C chooses 1, with probability ½. But also in this case, the retransmission is only successful if A does not also choose 0, with probability ¾. So, the answer is ¼ * ½ * ¾ = $^3/_{32}$.*

d) For the last case, what is the probability that A manages to do a successful retransmission before C transmits? Explain your answer. [2]

Solution: *0. Even if A starts transmission before C while AP is not transmitting at the same time, C will not hear that transmission and start transmitting as well, causing a collision.*

Consider the same system in the figure depicted above. Now, the assumption is that all nodes do use RTS/CTS. Further, let's assume that at $t=t_0$ both A and C start their access procedure to transmit a packet to the AP. However, the medium is still busy until t_1 because of a transmission of node B.

e) Describe a possible sequence of events, or packet transmission (attempts), after which both A and C are able to successfully transmit their packet. How long does it take at least from t_1 until both packets have been received at the AP? Explain. [4]

Note: Write down events like "A and C wait DIFS (+50μs)", "A transmits RTS (+65μs)", and add all durations at the end. Do not feel discouraged if there are quite a few events.

Solution: *Since A and C cannot hear each other, their RTS messages will collide if they send them at around the same time. Only if the transmission times of the RTS messages are more than the transmission time of such a message (65 μs) apart, the AP will answer with an RTS message, during and after which the other station will defer its transmission. So, the backoff times of A and B have to differ at least 4 slots, which can only occur after CW has grown to 7, after 2 collisions. So this gives the following sequence of events is (in μs):*

- *Transmission B ends (t_1)*
- *A and C wait DIFS (+ 50)*
- *A and C both choose 0 slots and transmit an RTS (+ 65)*
- *No CTS, due to collision, A and C realize after DIFS (+ 50)*
- *A and C double CW but again choose 0 slots and transmit an RTS (+ 65)*
- *No CTS, due to collision, A and C realize after DIFS (+ 50)*
- *A and C double CW again (to 7). Now A chooses 0 and transmits RTS (+65)*
- *AP receives RTS from A and has to wait SIFS (+10)*
- *AP transmits CTS (+65)*
- *C has chosen 4 backoff slots but hears the CTS from AP just before it wants to start transmitting, defers transmission until after RTS-CTS-packet-ACK sequence from A.*
- *A receives CTS, waits SIFS (+10)*
- *A transmits packet (+250)*
- *AP receives packet, waits SIFS (+10)*
- *AP transmits ACK (+65)*
- *C senses medium free again, waits DIFS (+50)*
- *C had already counted 4 slots, transmits RTS (+65)*
- *AP receives RTS, waits SIFS (+10)*
- *AP transmits CTS (+65)*
- *C receives CTS, waits SIFS (+10)*
- *C transmits packet (+250)*
- *AP receives packet from C → done!*

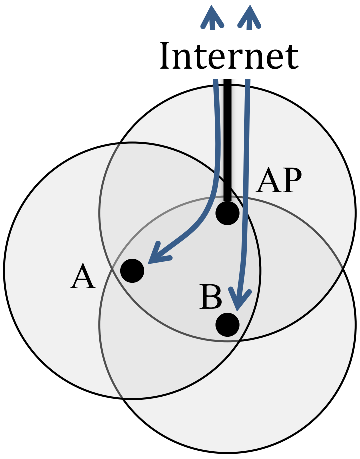
So, the total time from t_1 is 1205 μs.

An even quicker sequence (not required for the full score) is:

- *Transmission B ends (t_1)*
- *A and C wait DIFS (+ 50)*
- *A chooses 0 slots and transmit an RTS (+ 65)*
- *C chooses 1 slot, doesn't sense A, and starts transmitting its RTS 20 μs later*
- *No CTS, due to collision, A realizes after DIFS (+ 50) (C 20 μs later)*
- *A and C double CW, A again chooses 0 slots and transmit an RTS (+ 65)*
- *AP receives RTS from A and has to wait SIFS (+10)*
- *AP transmits CTS (+65)*
- *C has chosen 3 backoff slots but hears the CTS from AP just before it wants to start transmitting (20 μs + 3 slots = 80 μs later), defers transmission until after RTS-CTS-packet-ACK sequence from A.*
- *A receives CTS, waits SIFS (+10)*
- *A transmits packet (+250)*
- *AP receives packet, waits SIFS (+10)*
- *AP transmits ACK (+65)*
- *C senses medium free again, waits DIFS (+50)*
- *C had already counted 3 slots, transmits RTS (+65)*
- *AP receives RTS, waits SIFS (+10)*
- *AP transmits CTS (+65)*
- *C receives CTS, waits SIFS (+10)*
- *C transmits packet (+250)*
- *AP receives packet from C → done!*

So, the total time from t_1 is 1090 μs.

Now, consider the following scenario, depicted in the figure below. The AP in this case is supporting two stations, A and B, all in each other's range. In both node A and node B bi-directional video applications are running, which communicate with peers in the Internet through the AP.



Although the CSMA/CA mechanism in the Distributed Coordination Function of IEEE 802.11 Wireless LAN provides inherently fair access to all stations, in the scenario depicted above, there is unfairness at flow level. A and B each have to transmit packets for 1 flow, whereas the AP has to transmit packets for 2 flows. To achieve fairness at flow level, the AP should therefore be able to transmit twice as many packets as A and B in high load situations.

f) As described in the course, the Enhanced Distributed Channel Access (EDCA) allows for different treatment of packets from different access categories. Suppose A, B, and the AP, each have a single transmit queue, but we would give (the transmit queue of) the AP a different access category, with different parameters than (the transmit queues of) A and B. How would you achieve flow-level fairness between the AP and other stations by choosing appropriate access category parameters? Describe how the parameters should be set (e.g., how the value of a parameter chosen for the AP relates to the value for A and B) and argue why that provides flow-level fairness. [2]

Solution: *One way of providing fairness is by choosing the TXOP value of (the access category of) the AP twice the value of the TXOP value of A and B. This way, every time the AP wins contention (which is on average as often as A and B), the AP can send double the number of packets.*

g) Suppose the network described above is not using CSMA/CA as in Wireless LAN, but classical Aloha. How would you change the parameters of the Aloha access mechanism (in the individual nodes) to ensure flow-level fairness between the access point and nodes A and B? Describe your modified Aloha mechanism, including the choice of parameter(s) per node and argue why it provides flow-level fairness (e.g., through some basic modelling or calculations). [2]

Solution: *One way of providing this fairness in Aloha, is to let the AP perform retransmission with another probability p, let's say p_{ap}. In that case the probability of a successful retransmission by the access point is $p_{ap}(1-p)(1-p)$. For A and B, the probability of a successful retransmission is $p(1-p)(1- p_{ap})$. If we want the throughput in a highly loaded system for the AP to be the same as the throughput of A + B, the probability of successful retransmission of the AP should be twice that of a regular station, i.e., $p_{ap}(1-p)(1-p) = 2\, p(1-p)(1- p_{ap})$. So we should solve $p_{ap} / (1- p_{ap}) = 2p/(1-p)$, which gives us $p_{ap} = 2p / (p+1)$.*

h) Suppose the network described above is not using CSMA/CA as in Wireless LAN, but Packet Reservation Multiple Access (PRMA), as described in Section 3.4.6 in Part 1 of the reader. How would you modify the PRMA access mechanism to give flow-level fairness between the access points and nodes A and B? Describe your modified PRMA mechanism, including the choice of parameters per node and argue why it provides fair access at the flow level. [2]

Solution: *One way to provide this fairness in PRMA is to limit the number consecutive frames in which the same slot is implicitly reserved when using a certain slot. This implies limiting the number of consecutive frames in which a station is allowed to use a slot, i.e., a station has to give up a slot after n frames. If this number n is two times as large for the AP as for A and B, the AP has two times the capacity, every time it wins contention. Assuming the probability of winning contention is the same for A, B, and the AP, with this measure the AP has two times the capacity of A and B.*

3 Cellular Network Principles [8]

Consider a cellular network with hexagonal cells of the same size. An average user in this network generates a call request every 10 minutes. 20% of the users have a call duration uniformly distributed between 2 minutes to 8 minutes, while the call for the remaining users takes between 2 minutes and 6 minutes, again uniformly distributed.

For the following questions, please show all your calculations. When you think you do not have the value of some of the parameters (e.g., because you could not find it in one of the earlier sub-questions), you can assume a particular value for that missing variable. Please state explicitly in that case your assumption.

a) What is the expected traffic intensity generated by a user? [2]

Solution: *In Lecture-6 exercises, you can find a similar question.*
Traffic in Erlangs = Arrival rate (per time unit) x Average duration of a session (time units)
*α= 1/10 * (0.2*(2+8)/2 + 0.8*(2+6)/2)) = 0.42 Erlangs.*

Note that while calculating the traffic, all terms in the above formula must be converted to the same units, e.g., minutes or hours.

b) Assume that the operator of this network has licensed 280 MHz of paired spectrum, i.e., 280 MHz for the uplink and 280 MHz for the downlink. Each channel is 2 MHz in bandwidth. The operator reserves one channel in each cell as a control channel. How many communication channels would the operator allocate to a cell if the frequency reuse factor is 4? [2]

Solution: *Number of total channels = Total bandwidth / Channel Bandwidth = 280/2 = 140 channels. Since the frequency reuse factor is 4, the number of channels per cell is 140/4 = 35. In each cell, one channel is reserved for control messages, then the remaining 34 channels can be used for actual communication.*

c) Let us assume that *t* shows the hour of the day taking values between [0,24). The number of users per km^2 in each cell varies over time *t* according to the following function:

N(t) = 61 – 30 cos (2π*t*/24) users/km^2.

What should be the cell radius for the cellular operator to maintain a maximum blocking probability of 2% during the whole day? [2]

*Hint: Cells are hexagonal, and the area of a triangle is b*h/2 where b is the base of the triangle and h is the height. Moreover, you will need the Erlang-B table in the last page as well as the results from (a) and (b).*

Solution: *Since there are 34 channels used in a cell and the operator wants to keep the maximum blocking rate under 2%, then it can have a maximum load of 25.5 Erlangs (from Erlang-B table). Since each user generates 0.42 Erlangs, then the operator can have maximum 25.5/0.42=60.71 users in a cell. From the network traffic formula, we can find that the maximum number of users can be 61+30 when t=12.*

*Given that the maximum number of users in a cell is 91 user/km^2, then we can find the radius of a cell as follows. If the radius is R km and the cell is a hexagonal cell, then the area of the cell is: 1.5*$3^{1/2}$* R^2 km^2. If the user density is 91/km^2 at the busiest hour, then the cell radius must be: 1.5*$3^{1/2}$ *R^2*91 <= 60.71 which gives a radius of R= sqrt(60.71/(91* 1.5 *$3^{1/2}$)) = 0.506 km*

d) Assume that another network operator has 100 channels and uses a *frequency reuse factor* of 5. Assume also that all its channels can be used for actual communications (i.e., you do not need to reserve some channels for control messages). Initially, its total traffic load in a cell is 13 Erlangs. Later, the traffic intensity increases by 10%. What can this operator do to keep its blocking probability the *same as* or *lower than* the earlier (before the increase in its traffic load)? Discuss at least two approaches, not only qualitatively, but also quantitatively. Note that decreasing number of subscribers is not preferred by the network operator. [2]

Note: Write down two approaches, e.g., "the operator can change its operation parameter x from 5 to 7", stating the parameter x, and discussing why this approach leads to the desired blocking probability.

Solution: *Initially, the blocking probability is 2% as a cell has 20 channels and traffic is 13 Erlangs. Later, the traffic load becomes 13*1.1 = 14.3 Erlang. With the same blocking probability, at least 22 channels are needed.*

- *It can increase the number of channels from 20 to 22 by acquiring new spectrum.*
- *It can decrease frequency-reuse factor to 4 which results in 25 channels per cell. When there are 25 channels, even with 0.5% blocking probability, the network can support a load of 15 Erlang. With this reuse factor, the network may need to implement some interference control mechanisms. Other options could also be possible such as decreasing the cell size so that the number of users served and their traffic will be lower. This might increase the infrastructure cost, e.g., due to the need of more base stations.*

4 LTE cellular networks [6]

a) Consider Alice and Bob sitting in the same room and they are both customers of the same LTE operator. Alice is searching for the latest announcements on the university web page while Bob is having a video call with his friends. Does the LTE network treat these two users' communications in the same way while allocating its resources? [2]

Solution: *No, the traffic types are different. Since Bob's session requires a higher quality-of-service for user satisfaction, Guaranteed-Bit-Rate bearers (GBR) will be assigned to Bob. On the other hand, for web browsing, one can expect a Non-GBR (NGBR) bearer to be assigned. Default bearers that are created when each user is connected to the EPC would be the same type, namely NGBR.*

b) An LTE network has a bandwidth of 40 MHz at each of its cells. It operates in FDD mode and allocates equal amount of bandwidth for its uplink and downlink. How many resource blocks can an LTE eNodeB have for its downlink communications during a time period of 20 ms? [2]

Solution: *Since the network operates at FDD mode and allocates half of its bandwidth for the downlink, then the downlink bandwidth is 20 MHz. A resource block is 180 kHz in frequency (15kHz * 12 subcarriers) and 0.5 ms in time. So, we can calculate the number of RBs. The occupied bandwidth is 18 MHz and 2 MHz is used for the guard bands. 18 MHz/180 kHz * (20/0.5) = 100 * 40 = 4000 RBs.*

c) Compare the core network of 3G, 4G, and 5G. Briefly explain how they differ from each other. [2]

Solution: *3G core network supports both packet switching and circuit switching whereas 4G and 5G are only packet switching networks and called as all-IP core networks. Comparing 4G and 5G, the latter implements a variety of approaches such as SDN based core network and Virtual Network Functions to enable more efficient use of the resources and more cost-effectively.*

Please note that there are other differences among these generations of the technology, e.g., in radio access network (RAN) or in the applications provided. However, the question asks the differences in the core network specifically.

5 LTE-WiFi inter-working and coexistence [5]

a) Assume that you are working for an LTE network operator which needs to expand its coverage area to serve a population who lives in a region where the network infrastructure is destroyed, e.g., due to same natural disaster. The operator is looking for a solution that is easiest and fastest to realize and asked you to propose a solution. Which of the following options would you propose if installing a single BS under these frequencies has roughly the same cost? Why? [2]

- use TV white space bands
- use 5GHz spectrum bands

Solution: *Since the operator wants to expand its coverage area, then it needs to use a frequency band that has large coverage and therefore lower frequency. TV white space bands are bands at 400-700 MHz band. Therefore, they are more suitable for this operator's coverage expansion.*

b) Now, consider that an LTE operator in the Netherlands needs to increase the capacity in its coverage area in a short time to meet a sudden increase in traffic demand. Discuss how each of the following options might (or might not) help for capacity expansion. [3]

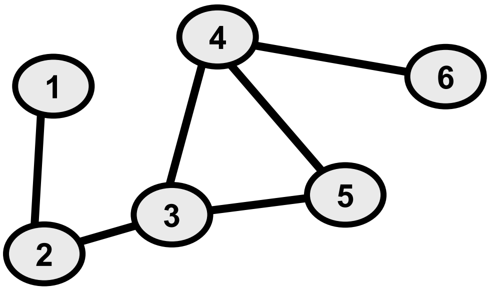
- LAA
- LTE-U
- LWA

Solution: *The best option for capacity expansion is to use unlicensed bands directly. So, LAA or LTE-U could be preferred. However, LTE-U is possible only in regions where LBT is not mandatory. Hence, if the operator is in the Netherlands, it must follow the regulations in EU. Then, the only option is LAA. LWA is also possible but it requires an existing WiFi infrastructure and its capacity expansion might be lower than LAA as LWA uses WiFi medium access which is mostly less spectrally efficient than LTE.*

Please remember that although LAA requires listen-before-talk and might result in performance decrease on the neighboring WiFi networks in some cases (e.g., hidden terminal cases), it still can offer a significant capacity increase to the LTE operator.

6 Ad-hoc Networks [18]

Please consider the following network. The numbered nodes (vertices) in the graph represent nodes in an ad-hoc network, which are within each other's transmission range when they are interconnected by a link (edge). For this exercise, you may also assume that nodes do not cause interference beyond their transmission range.



a) It is said that without special measures, broadcasting in ad-hoc networks suffers from increased contention and more collisions because rebroadcasts are often synchronized. To what extent does this problem apply in the network given above for a broadcast initiated by node 1? Explain this phenomenon using the above network and indicate between which nodes increased contention takes place (if any), and which nodes might not receive the broadcast message due to collisions (if any). [1]

Solution: *Suppose 1 is initiating the broadcast, 2 will rebroadcast it. Thereafter, 3 will rebroadcast it. The rebroadcast of 3 is received by 4 and 5 at the same time. As a result, they will at exactly the same time attempt to rebroadcast the packet, resulting in increased contention. However, once 4 rebroadcasts the packet, it will be received without collision at 6, because 6 is outside of the transmission range of 5.*

b) Suppose the probabilistic rebroadcasting scheme is used, with probability $P = 0.5$. What is the probability that node 6 receives a broadcast initiated by node 1? Explain your answer. [2]

Solution: *Node 1 is initiating the broadcast, which is received by node 2. Node 2 will rebroadcast with probability ½, in which case it will be received by 3. Node 3 will rebroadcast with probability ½ if it receives the message, so the probability the message is transmitted by node 3 is ½ * ½ = ¼. If node 3 rebroadcasts, the message will be received by node 4, which will rebroadcast with probability ½. So, the probability that node 6 receives the packet from node 4 is ¼ * ½ = 1/8.*

c) Suppose the counter-based rebroadcasting scheme is used with $C = 2$. What is the probability that node 6 receives a broadcast initiated by node 1? Explain your answer. [2]

Solution: *Node 1 is initiating the broadcast. Both node 2 and node 3 are always rebroadcasting the message, because they only receive it once. The rebroadcast of node 3 is received by both node 4 and node 5. Assuming they both take a random delay, either one will rebroadcast first, after which the other will cancel its rebroadcast. Only if node 4 rebroadcasts, with probability ½, node 6 will receive the message.*

Let us now assume that in the network depicted above, the AODV protocol is used for routing. Initially, all routing tables are empty. Suppose node 1 is initiating a `RREQ` message with

```
Source_Addr: 1 (the address of node 1),
Source_Seq#: 24,
Broadcast_ID, 27,
Dest_Addr: 6
Dest_Seq#: 42,
Hop_Count: 0.
```

d) How many rebroadcasts of this initial *RREQ* (so excluding the first one by node 1) will be done? Explain your answer. [2]

Solution: *All other nodes except for the destination, node 6, will rebroadcast it exactly once. So 4 rebroadcasts.*

e) When node 6 receives a `RREQ` initiated by node 1, and replies with a `RREP`, how does node 4 know what to do with the received `RREP` message? [2]

Solution: *After receiving the `RREQ` from node 3, it has added an entry in its routing table that node 1 can be reached via node 3. So it can forward the `RREP` to node 3.*

Now, assume that some time after establishing the route between node 1 and node 6 (via nodes 2, 3, and 4), while the route is still active, node 5 initiates a `RREQ` with

```
Source_Addr: 5,
Source_Seq#: 22,
Broadcast_ID, 27,
Dest_Addr: 1
Dest_Seq#: 32,
Hop_Count: 0.
```

f) What will node 4 do upon receiving this `RREQ` message? Explain your answer. [2]

Solution: *Node 4 will forward the `RREQ` to node 3 and 6, as it has not seen a `RREQ` with identical `Source_Addr and Broadcast_ID` before, and although it does know a route to node 1, the `Seq#` of that route is 24, which is lower than the requested `Dest_Seq#` 32.*

Consider again the same network. Now, rather than AODV, OLSR is used as a routing protocol.

g) For each of the 6 nodes, give the other nodes that it selects as multipoint relay (MPR). [2]

Solution:
1: 2
2: 3
3: 2,4
4: 3
5: 3,4
6: 4

h) Give all the messages that are transmitted by all the nodes, including the relevant fields of the message, from initialization until routes are known to all nodes. [3]

Note 1: If there is a choice of order of the messages, as much as possible assume that similar messages are sent in rounds, and that within a round nodes transmit in ascending order.

Note 2: Please use the following notation: For a HELLO message transmitted by node *u*, indicating that *u* has neighbours *v*, *w*, and *x*, and MPR *x*, write:
`u: HELLO(NBR(u)={v,w,x}, MPR(u)={x}).`
For a Topology Control message transmitted by node *u*, in which the links from node *v* to nodes *w*, *x*, and *y* are advertised, write:
`u: TC(v)=<w,x,y> .`

Solution:

```
1: HELLO(NBR(1)={}, MPR(1)={})
2: HELLO(NBR(2)={1}, MPR(2)={})
3: HELLO(NBR(3)={2}, MPR(3)={2})
4: HELLO(NBR(4)={3}, MPR(4)={3})
5: HELLO(NBR(5)={3,4}, MPR(5)={3})
6: HELLO(NBR(6)={4}, MPR(6)={4})
1: HELLO(NBR(1)={2}, MPR(1)={})
2: HELLO(NBR(2)={1,3}, MPR(2)={})
3: HELLO(NBR(3)={2,4,5}, MPR(3)={2})
4: HELLO(NBR(4)={3,5,6}, MPR(4)={3})
1: HELLO(NBR(1)={2}, MPR(1)={2})
2: HELLO(NBR(2)={1,3}, MPR(2)={3})
3: HELLO(NBR(3)={2,4,5}, MPR(3)={2,4})
5: HELLO(NBR(5)={3,4}, MPR(5)={3,4})
2: TC(2)=<1,3>
3: TC(2)=<1,3>
4: TC(2)=<1,3>
3: TC(3)=<2,4,5>
2: TC(3)=<2,4,5>
4: TC(3)=<2,4,5>
4: TC(4)=<3,5,6>
3: TC(4)=<3,5,6>
2: TC(4)=<3,5,6>
```

Note: the order and content of the `HELLO` messages might be somewhat different, but the last `HELLO` message of each node should have the same content as described above. The `TC` messages above might be initiated in different order, but all 3 `TC` messages, with the content as described above are sent by all 3 nodes (2, 3, and 4), as described above. Finally, nodes cannot announce neighbours before they have received a message from then, announce MPRs before they have learned about 2-hop neighbours that can be reached through them, and announce TCs before they have learned about those MPR Selectors.

i) Which links in this network are advertised in both directions? [2]

Solution: *The links between nodes 2 and 3, and between nodes 3 and 4.*

7 Bluetooth/WiFi Security [6]

a) Why is WEP not recommended as a security scheme for WiFi? Highlight the weaknesses of WEP in terms of its vulnerability to attacks considering both the authentication and encryption steps. [2]

Solution: *As Lecture-12 slides and video explain, in the authentication phase, WEP does not authenticate the AP. So, it is open to Man-in-the-Middle-Attacks (MITM). An adversary can pretend to be the AP and can get access to the information of the user. In the encryption step, it uses RC4 and CRC which have some known weaknesses, e.g., linearity property makes it easy for the attackers to change or redirect the traffic.*

b) Assume that you connect to the Internet using *eduroam* to watch a video from NetFlix. Can you be sure that your communication is secure? Why or why not? [2]

Solution: *As the article in the reader for Part-12 states*, *security must be ensured at each OSI layer. Using eduroam as the wireless access network provides security only at the medium access layer. Eduroam uses WPA2 "enterprise" (IEEE802.1X) which is known to be secure. However, there are many attacks in different layers, e.g., application layer, transport layer. So, one can never be use that the whole communication between the user connected to an eduroam and the remote server is secure, unless security mechanisms in other layers are also implemented.*

c) There is a plethora of Bluetooth devices from simple headphones or smart watches to more computationally capable smart TVs. Can we expect the same security level when connecting to these wide range of Bluetooth devices? Why or why not? [2]

Hint: Consider Bluetooth devices with Bluetooth 2.1 or newer versions.

Solution: *The hardware of the Bluetooth device might affect the pairing process. There are four pairing types in Bluetooth 2.1: numeric comparison, passkey entry, just works, and out-of-band pairing. For example, some devices without a keyboard might have to use just-works pairing approach making them vulnerable to men-in-the-middle attacks. If devices have Near-Field-Capability, then they can implement out-of-the-band pairing which is more secure than the rest.*

----- end of exam -------

Erlang B Traffic Table

Maximum Offered Load Versus B and N
B is in %

N/B	0.01	0.05	0.1	0.5	1.0	2	5	10	15
1	.0001	.0005	.0010	.0050	.0101	.0204	.0526	.1111	.1765
2	.0142	.0321	.0458	.1054	.1526	.2235	.3813	.5954	.7962
3	.0868	.1517	.1938	.3490	.4555	.6022	.8994	1.271	1.603
4	.2347	.3624	.4393	.7012	.8694	1.092	1.525	2.045	2.501
5	.4520	.6486	.7621	1.132	1.361	1.657	2.219	2.881	3.454
6	.7282	.9957	1.146	1.622	1.909	2.276	2.960	3.758	4.445
7	1.054	1.392	1.579	2.158	2.501	2.935	3.738	4.666	5.461
8	1.422	1.830	2.051	2.730	3.128	3.627	4.543	5.597	6.498
9	1.826	2.302	2.558	3.333	3.783	4.345	5.370	6.546	7.551
10	2.260	2.803	3.092	3.961	4.461	5.084	6.216	7.511	8.616
11	2.722	3.329	3.651	4.610	5.160	5.842	7.076	8.487	9.691
12	3.207	3.878	4.231	5.279	5.876	6.615	7.950	9.474	10.78
13	3.713	4.447	4.831	5.964	6.607	7.402	8.835	10.47	11.87
14	4.239	5.032	5.446	6.663	7.352	8.200	9.730	11.47	12.97
15	4.781	5.634	6.077	7.376	8.108	9.010	10.63	12.48	14.07
16	5.339	6.250	6.722	8.100	8.875	9.828	11.54	13.50	15.18
17	5.911	6.878	7.378	8.834	9.652	10.66	12.46	14.52	16.29
18	6.496	7.519	8.046	9.578	10.44	11.49	13.39	15.55	17.41
19	7.093	8.170	8.724	10.33	11.23	12.33	14.32	16.58	18.53
20	7.701	8.831	9.412	11.09	12.03	13.18	15.25	17.61	19.65
21	8.319	9.501	10.11	11.86	12.84	14.04	16.19	18.65	20.77
22	8.946	10.18	10.81	12.64	13.65	14.90	17.13	19.69	21.90
23	9.583	10.87	11.52	13.42	14.47	15.76	18.08	20.74	23.03
24	10.23	11.56	12.24	14.20	15.30	16.63	19.03	21.78	24.16
25	10.88	12.26	12.97	15.00	16.13	17.51	19.99	22.83	25.30
26	11.54	12.97	13.70	15.80	16.96	18.38	20.94	23.89	26.43
27	12.21	13.69	14.44	16.60	17.80	19.27	21.90	24.94	27.57
28	12.88	14.41	15.18	17.41	18.64	20.15	22.87	26.00	28.71
29	13.56	15.13	15.93	18.22	19.49	21.04	23.83	27.05	29.85
30	14.25	15.86	16.68	19.03	20.34	21.93	24.80	28.11	31.00
31	14.94	16.60	17.44	19.85	21.19	22.83	25.77	29.17	32.14
32	15.63	17.34	18.21	20.68	22.05	23.73	26.75	30.24	33.28
33	16.34	18.09	18.97	21.51	22.91	24.63	27.72	31.30	34.43
34	17.04	18.84	19.74	22.34	23.77	25.53	28.70	32.37	35.58
35	17.75	19.59	20.52	23.17	24.64	26.44	29.68	33.43	36.72