EIT5 – Fall 2022
Final Exam - Solutions

Department of Electronic Systems
Aalborg University

Feb. 7, 2023

Problem 1: Bellman-Ford Algorithm

1. The maximum number of iterations = num. of nodes - 1 = 5 - 1 = 4.
2. Construct the shortest path tree

   Initial

Node	A	B	C	D	E
Cost	0	∞	∞	∞	∞
Pre-Node	-	-	-	-	-

   Iteration 1

Node	A	B	C	D	E
Cost	0	3	1	7	9
Pre-Node	-	C	A	B	D

   Iteration 2

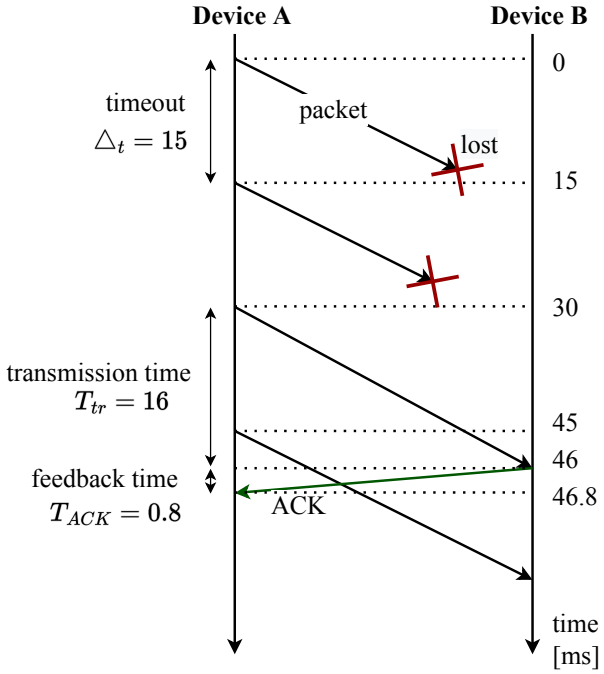
Node	A	B	C	D	E
Cost	0	3	1	6	8
Pre-Node	-	C	A	B	D

   Iteration 3

Node	A	B	C	D	E
Cost	0	3	1	6	8
Pre-Node	-	C	A	B	D

Then the shorstest path tree: A - C -B - D - E

Problem 2: Link-Layer Procedure



Transmission time for one frame from A to B: $T_{tr} = \frac{200\times8}{0.1\times10^6} = 0.016$ [s] $= 16$ [ms].
Transmission time of the ACK frame from B to A: $T_{ACK} = \frac{10\times8}{0.1\times10^6} = 0.0008$ [s] $= 0.8$ [ms]
The timeout $\Delta_t = 15$ [ms]
From the above figure, we can see timestamps for events that occurred during the communication between A and B.

1. It takes 46.8 ms for device A to receive the ACK signal from the decive B.
2. Device A sent the first frame 4 times before receiving the ACK.
3. The timeout should be designed so that there is enough time for device A to receive the ACK signal from B before determining whether to retransmit the frame. Therefore, the timeout in this case should be
   $\Delta_t > T_{tr} + T_{ACK} = 16 + 0.8 = 16.8$ [ms]

Problem 3: Slotted ALOHA

1. The efficiency: $S = Ge^{-G} = 0.2e^{-0.2}$, leading to the actual throughput $= 20 * S = 4e^{-0.2} = 3.28$ kbps.

2. The transmission time $T = 20\text{bits}/20\text{kbps} = 1\text{ms}$. As Bandwidth is 20 Kbps to number of bits can be transfered in 1 ms = 20 bits. This means one packet can be transmitted in one transmission time, i.e., $G = 1$.

   So the efficiency will be $S = Ge^{-G} = 1e^{-1} = 0.368$.

   The maximum possible throughput is then equal to $20 * S = 20 * 0.368 = 7.36$ [bps].

Problem 4: Modulation techniques

1. You have a receiver and transmitter with a link between them. The transmitter is sending 1 symbol every 1 microsecond, find the throughput of the system if:

   (a) 16 QAM is used for modulation.

   The system transmits 4 bits per symbol, leading to the throughput $= \frac{4\times1}{1\times10^{-6}} = 4 \times 10^6$ [bps].

   (b) QPSK is used for modulation.

   The system transmits 2 bits per symbol, leading to the throughput $= \frac{2\times1}{1\times10^{-6}} = 2 \times 10^6$ [bps]

2. Are the following questions false or true:

   (a) False

   (b) True

   (c) False

   (d) True

Problem 5: Wireshark

Question 1:

1. IP assigned is: 192.168.122.43

2. MAC for the device is: 52:54:00:7f:e3:df

Question 2:

1. IP is: 192.168.122.1

2. MAC for the device is: 52:54:00:26:63:d3

Question 3:

1. Frame number 21, 22 and 23. We see [SYN], [SYN, ACK], [ACK] coming in these ones, which establishes the connection between the client and the server.

2. We see a GET HTTP after the handshake. This would suggest connecting to a webpage, specifically on http://google.com/. Afterwards we see the webpage (216.58.207.206) replies with an ACK and text/html which would likely mean we received the html content of the google webpage. This could be received in e.g. a browser. Finally we see the user ACK and sending a [FIN,ACK] to which the server responds [FIN,ACK] and the user [ACK] in frames 28,29,30. This would close the TCP session as the client had no more for now to request in the TCP session, and the server had no more to send.

Question 4:

1. It resolves to [91.189.94.4, 91.189.91.157, 91.189.89.199 91.189.89.198]. all of these being IP's which ntp.ubuntu.com resolves to each could be used when trying to access the website.

Problem 6: Traffic type and synchronicity

1. While both can be used for any kind of live-streaming, there is a significant difference in how they operate and for which type of application they individually are suitable. UDP is especially suitable for any kind traffic which does not require the entirety of the data to be received. Live streaming is one such traffic type, as the latency and real-time experience is more critical than receiving every video frame correctly as this may lead to stuttering and even more lag caused by the retransmission of single frames. Hence a deformed picture, or missing a video frame is not detrimental to the experience, whereas sudden lag spikes would be more apparent and frustrating.

2. Synchronicity is generally used to align the receiver and transmitter. From this we could think of synchronous and asynchronous communication. That could for the former be based on a slot-like structure of communication where at each discrete timestep you are in some state, known to the other parties. Hence it is possible to align the different parties with each other to make actions predictable. This could serve a purpose such as minimizing collisions, and is useful if multiple parties always, or often wish to transmit and have a guarantee on the expected availability, which requires scheduling in some form. Synchronicity is thus useful when you want a predictable outcome. For the latter, asynchronous protocols, these are useful when the actions of the parties are not deterministic and can change. For example parties are not always transmitting, but when they wish to transmit they would like to be fast and have the medium available. This type of communication is relevant and useful to ensure a system with many users that they do not take up resources not used, which ensures the users wishing to transmit and use the medium have resources available. Both types of protocols are useful for different contexts and the relevance is system dependent.

Problem 7: Security

1. If a shared secret is given, hashing is a solution to ensure the integrity of messages sent between the 2. By hashing the shared secret with the sent message, and appending the final hash the integrity of the message can be validated by the other party. If anyone were to make changes to the message without the proper "secret" the hash would simply be wrong, which can be evaluated by the receiver.

2. With public key cryptography the core feature is that the key used for decryption, only works with the key used for encryption (and vice versa as both can be used for either.) Signatures is a way to ensure authentication by using the aforementioned feature. This would be done by signing a message using the private key when sending it. Upon reception the receiver can verify if the message was sent by the private key holder, by validating the signature using the public key for decryption. This will ensure authentication as long as the private key is not leaked by storing it insecurely, and by ensuring that when receiving the public key that it truly it from who claims ownership. This is over the internet realized through certificate authorities., who certifies ownership of public keys. Naturally you can also "just" trust the ownership without other parties involvement..

3. A pair of asymmetric keys are provided by the algorithm. This is given from the fact diffie-hellman is used for public key cryptography, which relies on 2 different keys (public and private).

4. Block cipher processes the input one block of elements at a time, producing an output block for each input block. Stream cipher processes the input elements continuously, producing output one element at a time, as it goes along. Hence the differences lies in the block-based encryption of block ciphers where a certain size that must be encrypted at a time i.e. multiple bytes, and if the size is not met padding may be used to achieve the necessary block size. Meanwhile the stream-cipher "streams" the encryption taking one element at a time (1 bit or 1 byte) in a continuous stream.

Problem 8: Modulation techniques

1. The modulated signal (a) comes from a frequency modulation, whereas modulated signal (b) is the result of amplitude modulation.

2. **Amplitude modulation (AM):** uses the amplitude of the carrier frequency signal to convey the information of the message signal. The main advantage is that since a coherent reference is not required for demodulation, the demodulator becomes simple and inexpensive. The main disadvantage of this modulation is the wastage of carrier power.
   Frequency modulation (FM): convey the information of the message signal by changing the instantaneous frequency of the carrier signal. The pros of frequency

modulation are: Less interference and noise (higher signal-to-noise ratio) and the power consumption is less as compared to AM. The cons of frequency modulation are the higher cost of the equipment due to the larger bandwidth, and the more complicated receiver and transmitter.
In general, an equivalent FM signal covers less area than the corresponding AM signal.

3. First, we need to compute the modulated signal as follows:

$$\begin{aligned} a(t) &= m(t)c(t) && (1)\\ &= (\text{sinc}(t) + \text{sinc}(2t))A\cos(2\pi f_c t) && (2)\\ &= A\cos(2\pi f_c t)\text{sinc}(t) + A\cos(2\pi f_c t)\text{sinc}(2t) && (3) \end{aligned}$$

Lets denote the Fourier transform as $\mathcal{F}$. Our goal is to find $\mathcal{F}\{a(t)\}$, which characterizes the spectrum of the modulated signal. Then, we have:

$$\begin{aligned} \mathcal{F}\{a(t)\} &= \mathcal{F}\{A\cos(2\pi f_c t)\text{sinc}(t) + A\cos(2\pi f_c t)\text{sinc}(2t)\} && (4)\\ &= \frac{1}{4}\pi A\{\Pi(1/4(2\pi f_c - \omega)) + \Pi(1/4(2\pi f_c + \omega)) && (5)\\ &+ 2\Pi(\pi f_c - \omega/2) + 2\Pi(\pi f_c + \omega/2)\}, && (6) \end{aligned}$$

where $\omega = 2\pi f$ and Π is the rectangular function. Then, the bandwidth can be found by finding the highest frequency components of the spectrum. By analyzing the above expression, we find that the spectral components from $\text{sinc}(2t)$ yields the highest frequency components of the spectrum given by the pair related to $2\Pi(\pi f_c \pm \omega/2)$. Then, the bandwidth would be $\text{BW} = 2\omega_c$ with $\omega_c = 2\pi f_c$.