2022

Cyber Engineering

ADIL MONU LALI PRABHAKAR

Task 1

What is an LC Circuit?

An LC circuit is used to find a given frequency. Inductors and capacitors bearing the letters L and C are referred to as LC circuits, resonant circuits, tank circuits, and tuned circuits. Resonators, like tuning forks, can store energy at a circuit's resonant frequency.

An LC circuit that oscillates at its natural resonant frequency can store energy. In the diagram below, an inductor stores energy in its magnetic field (B), while a capacitor stores energy in the electric field (E) between its plates (V).

Condensers and inductors create magnetic fields. Voltage is 0 when current flows through a capacitor. The coil's magnetic field energy produces a voltage. It charges the capacitor in the opposite direction. The capacitor is charged by the magnetic field. No magnetic field = no current = opposite polarity charge in capacitor. After that, the inductor current is reversed. (Wikipedia, n.d.)

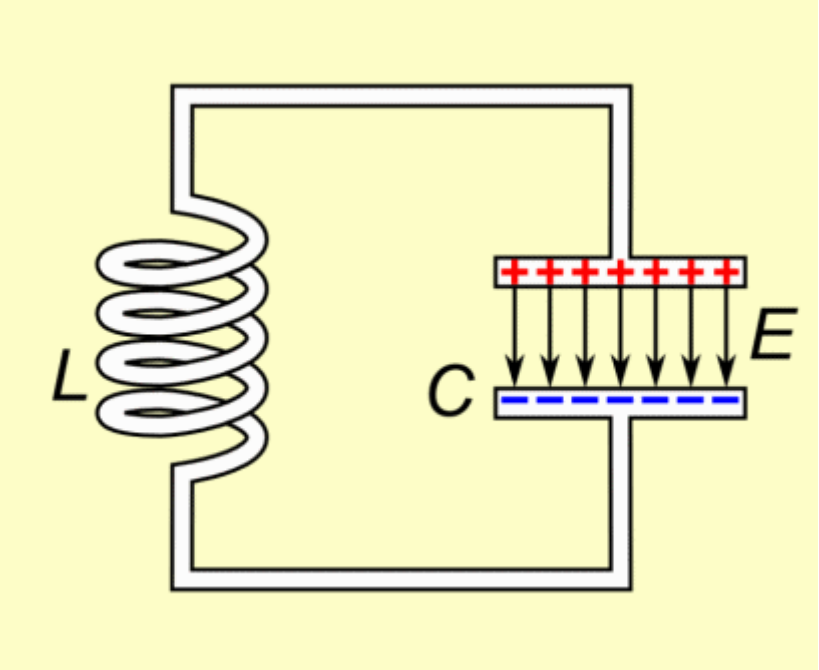


Figure 0-1: Operation of LC circuit

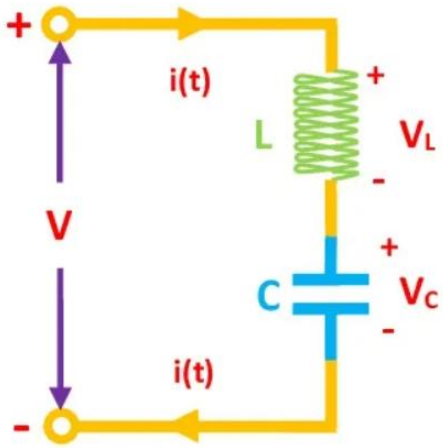


Figure 0-2: Series LC circuit

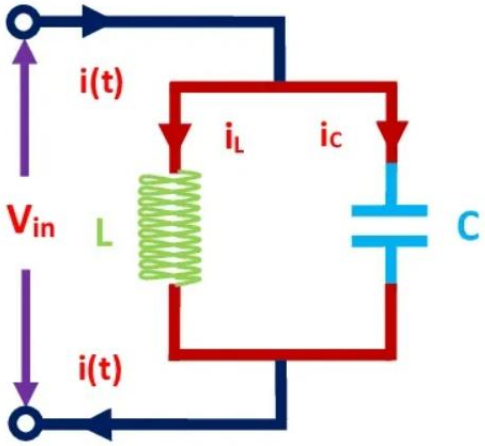


Figure 0-3: Parallel LC circuit

When the inductive and capacitive reactance's are of identical magnitude at an angular frequency ω_0, resonance occurs in an LC circuit. The resonant frequency is the frequency at which this inequality holds for the particular circuit. In the LC circuit, the fundamental resonant frequency is

$$\omega_\circ = \frac{1}{\sqrt{LC}}$$

where the inductance L is measured in henries and the capacitance C is measured in farads, respectively. The angular frequency $\omega_\circ$ has radians per second as its unit of measurement.

In hertz units, the equivalent frequency is:

$$f_\circ = \frac{\omega_\circ}{2\pi} = \frac{1}{2\pi\sqrt{LC}}$$

Where $f_\circ$ is the resonant frequency that is measured in hertz.

Question a

We know that resonant frequency

$$f_\circ = \frac{1}{2\pi\sqrt{LC}}$$

Taking root of LC to L.H.S we will rewrite the formula as:

$$\sqrt{LC} = \frac{1}{2\pi f_\circ}$$

We will square L.H.S and R.H.S to remove the root of LC and the equation is re-written to:

$$LC = \frac{1}{(2\pi f_\circ)^2}$$

We know that $f_\circ = 674\ KHz$ or $674\times 10^3 Hz$

Substituting the value in the equation, we get:

$$LC = 5.57597054 \times 10^{-14}$$

Since we need to tune the value of L and C to obtain the frequency 674. We are assuming the value of C as $5\mu F$ initially to find the value of L to obtain the desired frequency.

The equation is modified to get the value of L:

$$L = \frac{5.57597054 \times 10^{-14}}{C}$$

Substituting the value of C :

$$L = \frac{5.57597054\times 10^{-14}}{5\times 10^{-6}} = 11.1519411 \times 10^{-9}$$

$$L = 11.1519411 \times 10^{-9}\ H\ or\ 11.1519\ \text{nH}$$

The values we obtain is as follows:

$$L = 11.1519411 \times 10^{-9}\ H\ or\ 11.1519\ \text{nH}$$

$$C = 5\ \mu F\ or\ 5 \times 10^{-6} F$$

$$f_\circ = 647\ \text{KHz}$$

LTspice

Here we are going to draw a LC diagram in LTspice and check whether the obtained values will give us a frequency of 674 or not.

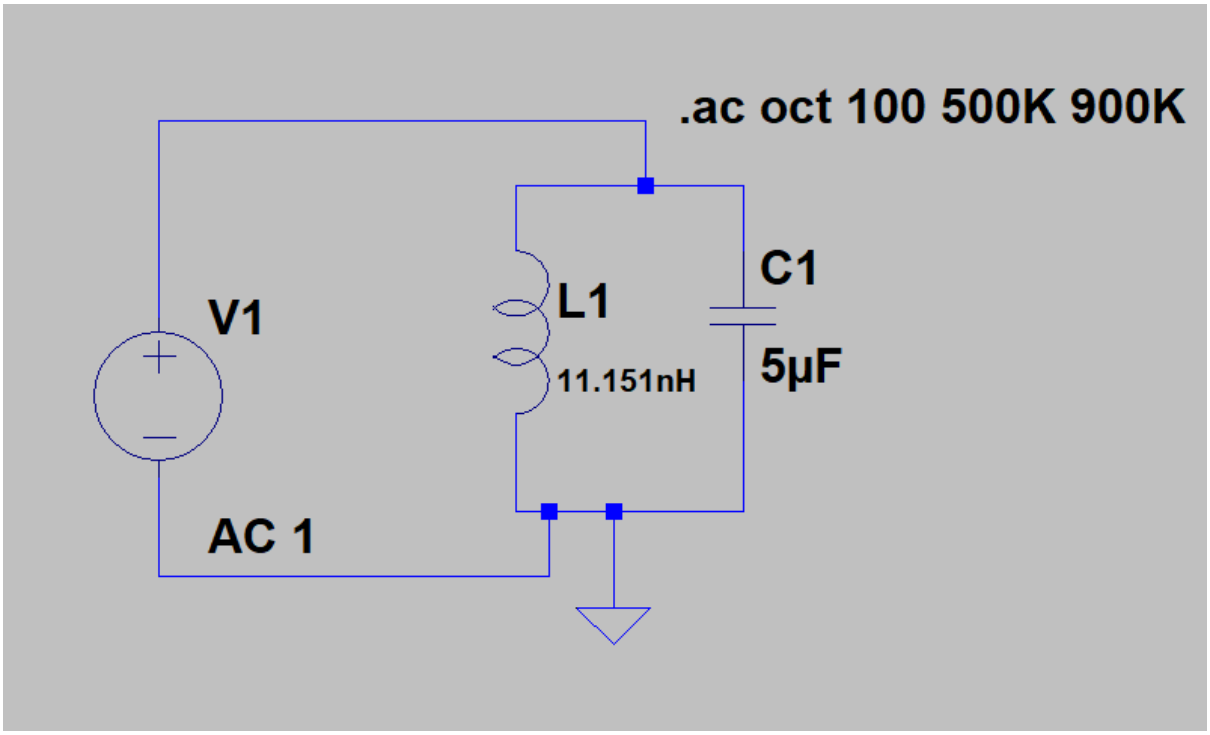


Figure 0-4: LC circuit

This circuit has been tested in LTspice, and the output is as follows.

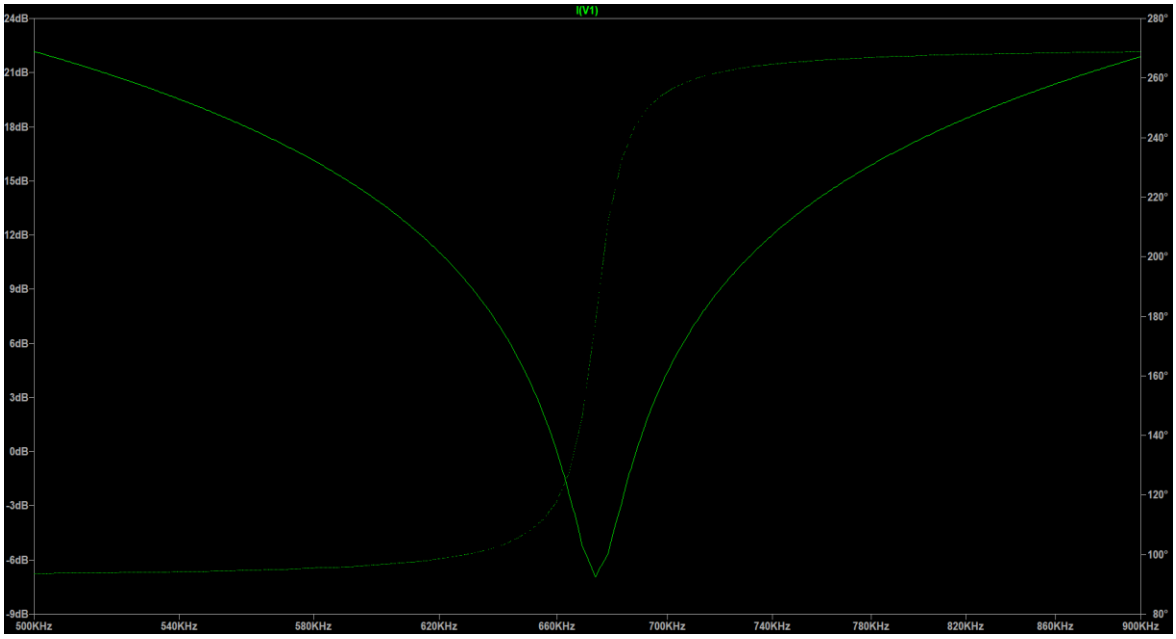


Figure 0-5: Output

Using our numbers for L and C, we get a resonance frequency of around 674 KHz (more precisely, about 673 KHz). LTSpice to perform an AC analysis on the circuit, with a frequency range of 500 kHz to 900 kHz being considered. Current consumption in the parallel LC circuit is zero at the resonance frequency. At the resonance frequency, the tank's impedance is infinite, and it does not draw any current.

b. Low-Pass filter

A Low Pass Filter (LPF) is a circuit that can be designed to remove unwanted high frequencies from an electrical signal and accept or pass only those frequencies desired by the circuit's designer. A basic passive RC Low Pass Filter (LPF) can be simply constructed by connecting a single resistor and a single capacitor in series, as shown below. The input signal (VIN) is applied to the series combination (both the Resistor and the Capacitor together) in this sort of filter, however the output signal (VOUT) is taken solely across the capacitor.

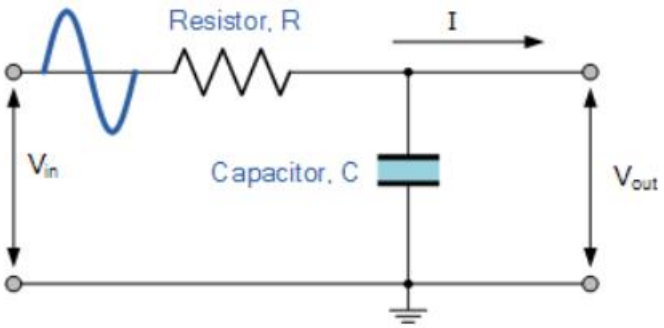


Figure 0-6:RC Low Pass filter circuit

A capacitor's reactance varies inversely with frequency, whereas a resistor's value remains constant. At low frequencies, the capacitor's capacitive reactance (XC) will be larger than the resistor's resistive value (R).

This means that the voltage potential across the capacitor, VC, will be substantially greater than the voltage drops across the resistor, VR. Due to the change in capacitive reactance value, the reverse is true at high frequencies, with VC being small and VR being large.

- RC Low pass filter : In the form depicted below, the RC low-pass filter consists of a resistor (with resistance R) and a capacitor (with capacitance C):

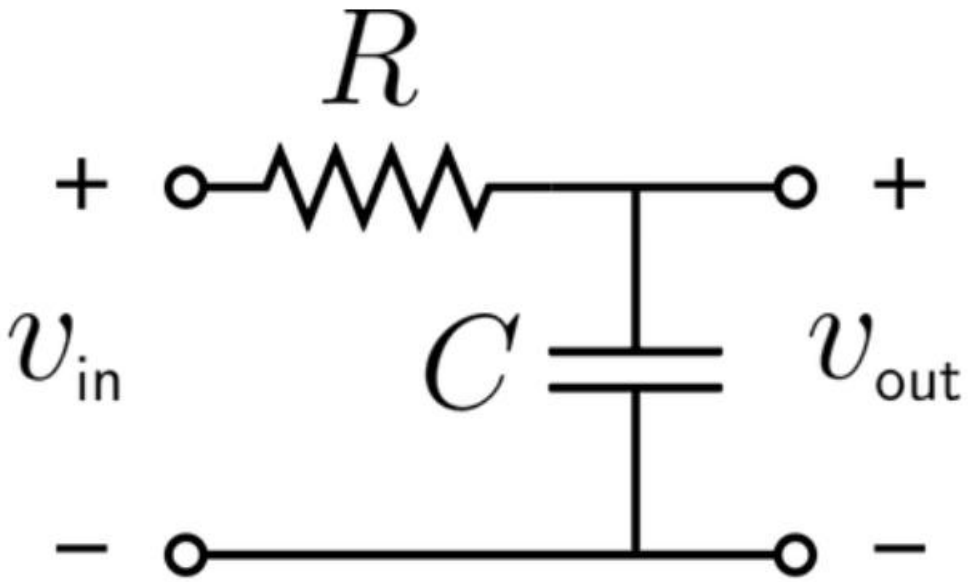


Figure 0-7:RC low pass filter

- RL low pass filter: Another passive filter is the RL low-pass filter, which is made up of a resistor R and an inductor L in the following configuration:

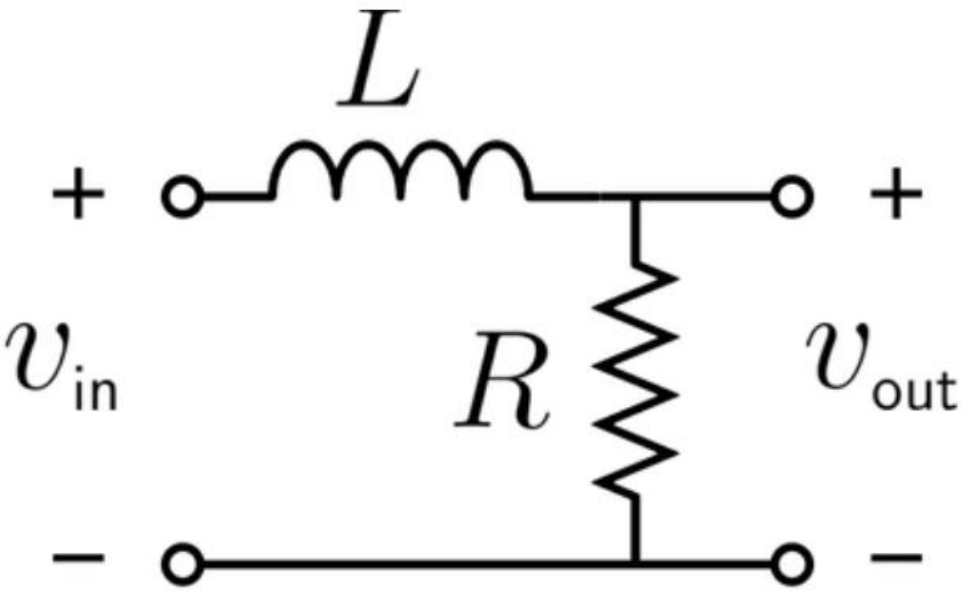


Figure 0-8:RL low pass filter

Let's look at how to calculate the desired resistor and capacitor values for a 700 KHz low pass circuit. We are going to use a RC low pass circuit for this demonstration.

Simple formula for the cut of frequency f_c is:

$$f_c = \frac{1}{2\pi RC}$$

We know the value of f_c, which is 700KHz or 700× 10^3Hz. To calculate the value of R and C we will re-write the equation to:

$$RC = \frac{1}{2\pi f_c}$$

Substituting the values of f_c and π in this equation.

$$RC = \frac{1}{2\pi \times 700 \times 10^3}$$

$$RC = 2.27364204 \times 10^{-7}$$

Assuming the value of C as 5 Farad or $5 \times 10^{-6}\mu F$,

$$R = \frac{2.27364204 \times 10^{-7}}{5 \times 10^{-6}}$$

$$R = 0.0454728408\ ohm$$

Now we have the following values to get a low pass RC circuit at 700KHz:

$R = 0.0454728408\ ohm$

$C = 5\ \mu F$

$f_c = 700 KHz$

Now implementing this to the f_c equation

$$700KHz = \frac{1}{2\pi \times 0.454728 \times 5 \times 10^{-6}}\ Hz$$

$$700KHz = \ 700000\ Hz\ or\ 700KHz$$

LTSpice

Here we are going to draw a RC Circuit in LTSpice for the simulation of the finding.

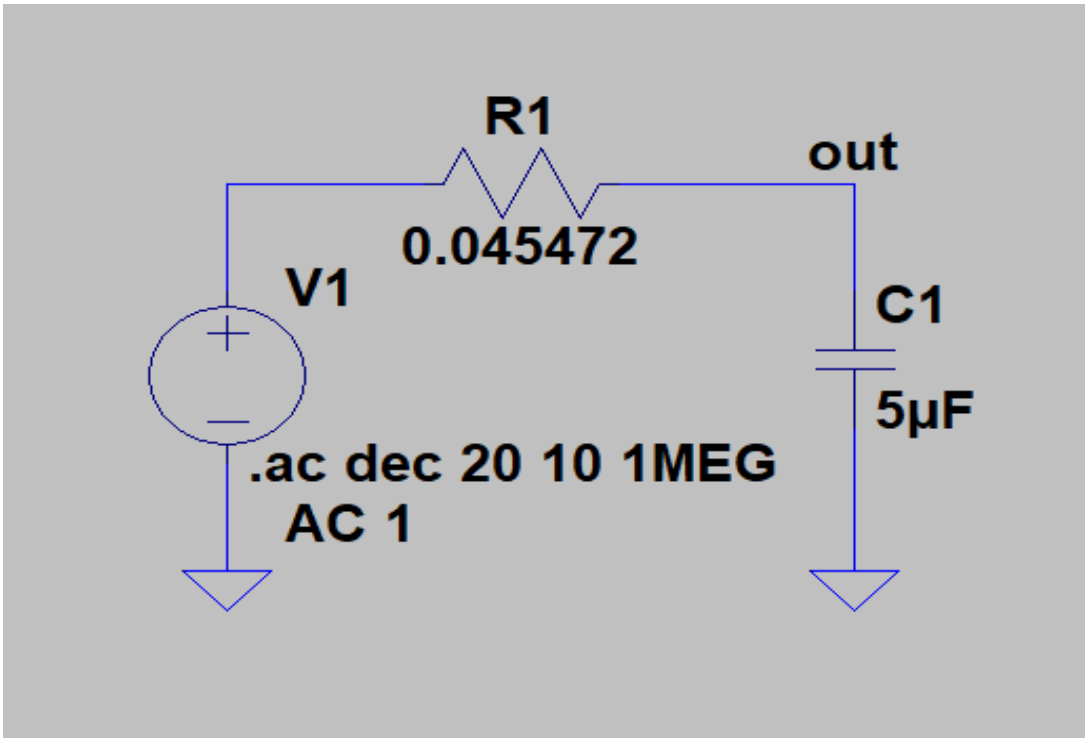


Figure 0-9: RC Circuit diagram in LTSpice

The output of the circuit is as shown below:

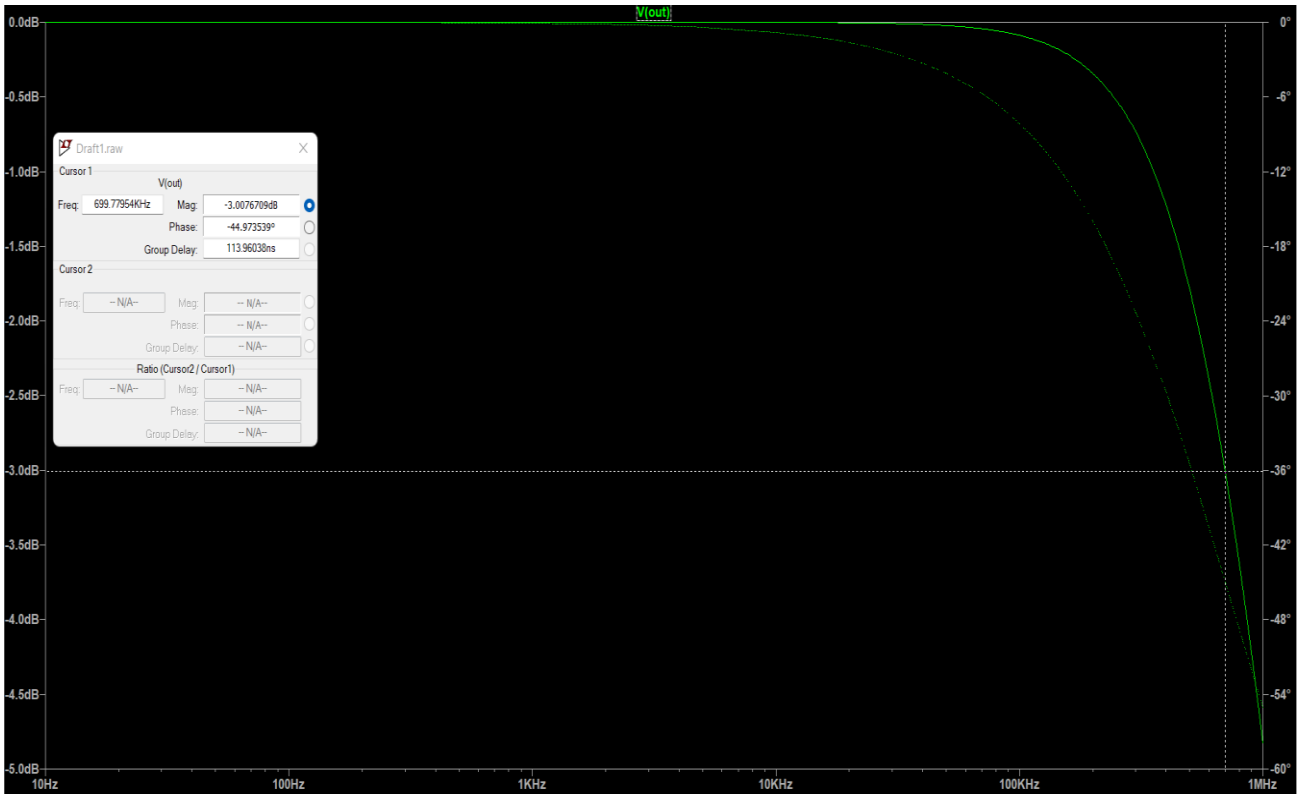


Figure 0-10: Output Graph

This finding can be confirmed by charting the output voltage against frequency, as seen in the graphic above as the frequency was cut off at the range of 700KHz at mag -3dB. An RC filter's frequency response shows that "cutoff frequency" is inaccurate. Because attenuation increases progressively as frequencies go from below the cutoff to above it, the picture of a signal's spectrum being "sliced" into two halves and one of them being kept and the other discarded, does not apply. An RC low-pass filter's cutoff frequency is the frequency at which the input signal's amplitude is lowered by three decibels (dB) (this value was chosen because a 3 dB reduction in amplitude corresponds to a 50 percent reduction in power).

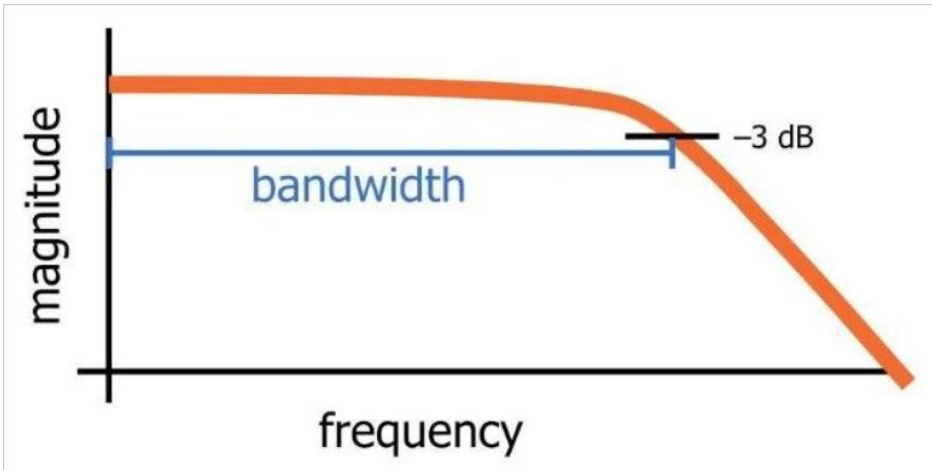


Figure 0-11:An RC low-pass filter's frequency response is shown here in a generic way. The –3 dB frequency bandwidth is equal to the bandwidth.

c. Band-Pass filter

By "cascading" a Low Pass Filter and a High Pass Filter together, we may create a passive RC filter that passes a narrow or large band of frequencies while attenuating all others. This innovative passive filter configuration generates a frequency selective Band Pass Filter.

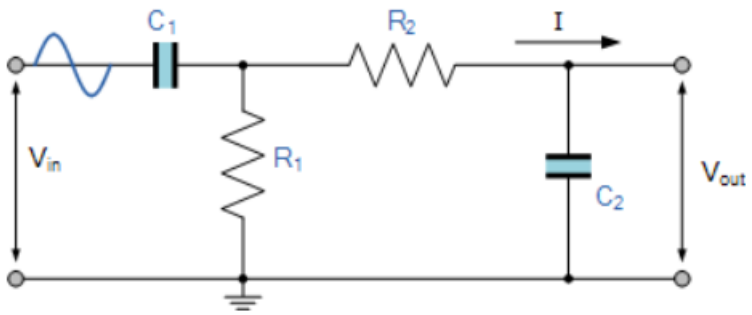


Figure 0-12: Band pass filter circuit

The frequency range between two specified frequency cut-off points that are 3dB below the maximum centre or resonant peak while attenuating or weakening the others outside of these two points is generally referred to as bandwidth.

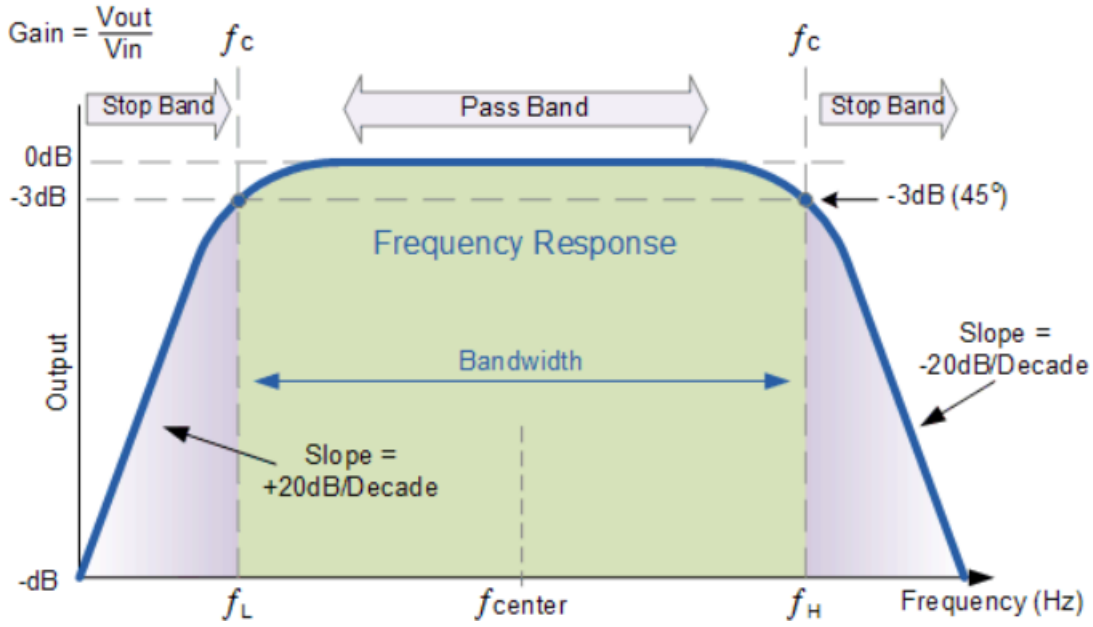


Figure 0-13:Frequency response of Band pass filter

Creating a Band Pass Filter to pass a range of frequencies 800KHz – 1700KHz:

For this we need to find the value of both high pass filter (R1, C1) and high pass filter (R2, C2).

High pass filter:

We know that $f_1 = 800\text{KHz}$

To find R1 and C1

$$f_1 = \frac{1}{2\pi R1C1}$$

$$R1C1 = \frac{1}{2\pi f_1}$$

$$R1C1 = \frac{1}{2\pi \times 800 \times 10^3} = 1.98943 \times 10^{-7}$$

Assuming the value of C1 as 5 Farad

$$R1 = \frac{1.98943 \times 10^{-7}}{5 \times 10^{-6}}$$

$$R1 = 0.03978\ ohm$$

We got the value of High pass filter for 800KHz. Which is:

$R1 = 0.03978\ ohm$

$C1 = 5 \times 10^3 \mu F$

Low Pass filter:

$$f_2 = \frac{1}{2\pi R2C2}$$

$$R2C2 = \frac{1}{2\pi f_2}$$

$$R2C2 = \frac{1}{2\pi \times 1700 \times 10^3} = 9.36205 \times 10^{-8}$$

Assuming C2 as 5 Farad

$$R2 = \frac{9.36205 \times 10^{-8}}{5 \times 10^{-6}}$$

$$R2 = 0.018724\ ohm$$

We got the value of Low pass filter for 1700KHz. Which is:

$R2 = 0.018724\ ohm$

$C2 = 5 \times 10^3 \mu F$

Resonance Frequency $f_R = \sqrt{f_1 f_2} = 1166\ KHz$

Simulating this to LTspice:

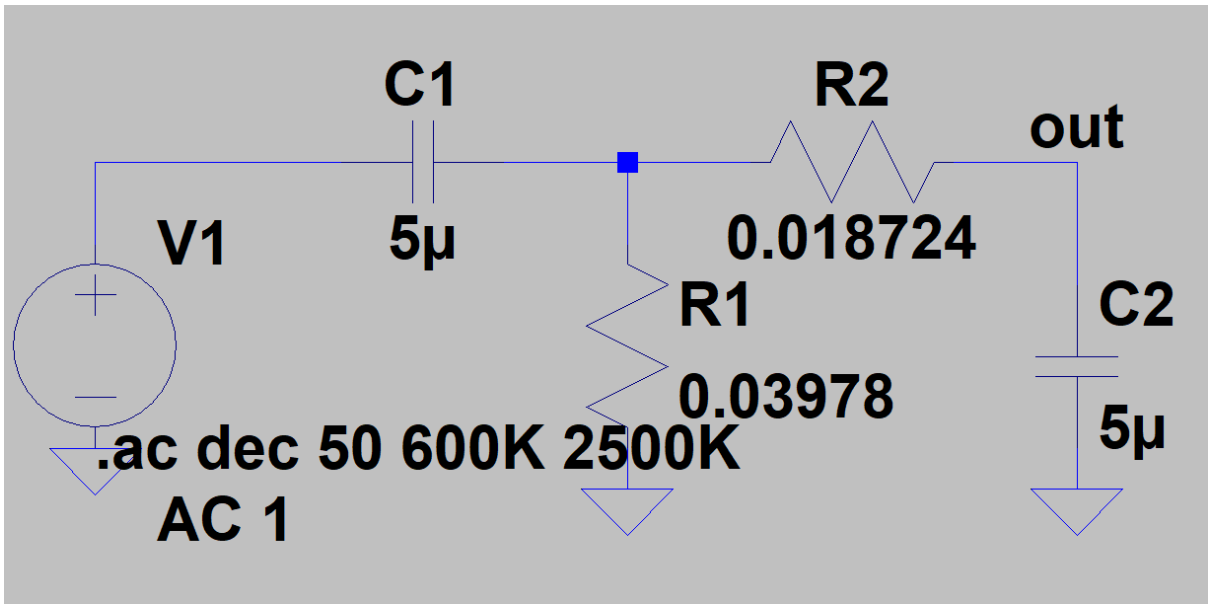


Figure 0-14:Band pass filter circuit

The Output:

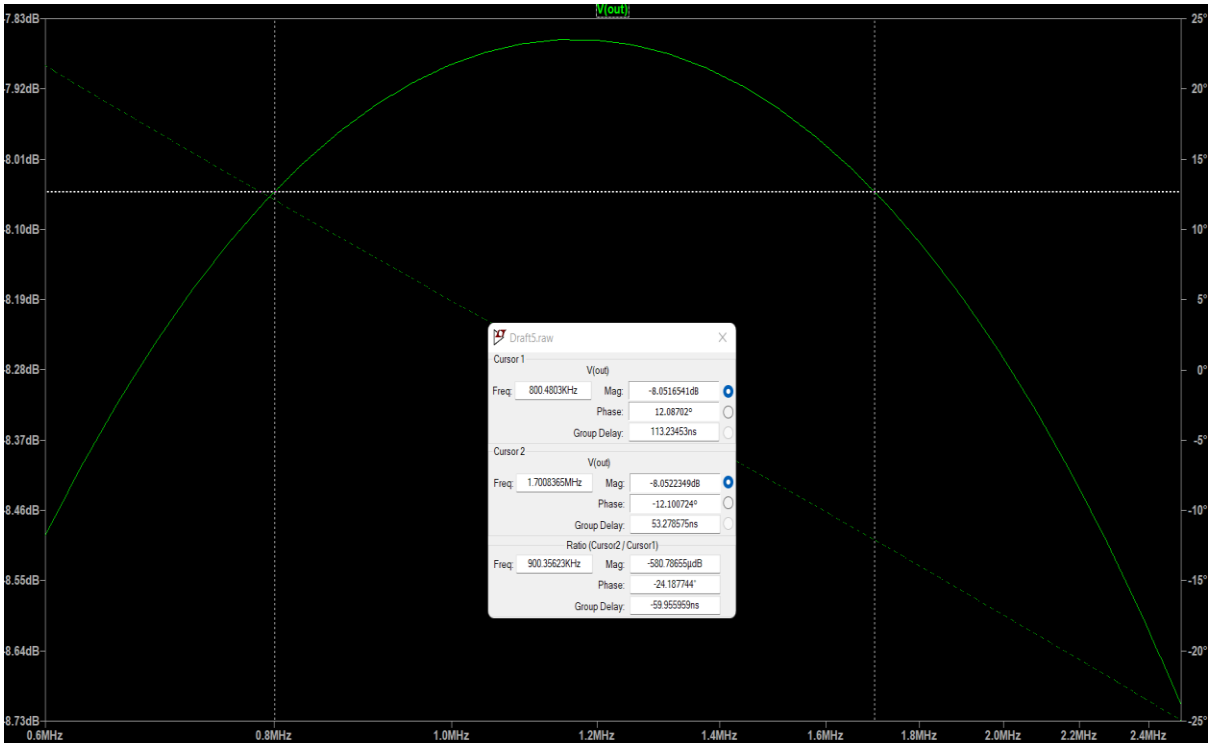


Figure 0-15: Graph

The circuit will only allow a bandwidth of 800KHz to 1700KHz, as shown here.

d. Amplitude Modulator and Demodulator

Amplitude modulation (AM) is a modulation technique extensively employed in radio communication. In amplitude modulation, the wave's amplitude (signal strength) varies in proportion to the message signals. Unlike angle modulation, which changes the carrier wave's frequency, phase modulation changes the carrier wave's phase.

According to theory, the carrier can be described in terms of a sine wave as follows:

$$C(t) = C \sin(\omega c + \varphi)$$

C is the carrier amplitude

$\frac{\omega c}{2\pi}$ is the carrier frequency in Hertz.

φ is the signal's phase at the start of the reference time.

Multiplying the carrier and the modulating signal together yields the equation for the overall modulated signal.

$$y(t) = [A + m(t)] . c(t)$$

A is constant

Individual relationships for the carrier and modulating signal are substituted:

$$y(t) = [A + M\cos(\omega mt + \varphi] . \sin(\omega ct)$$

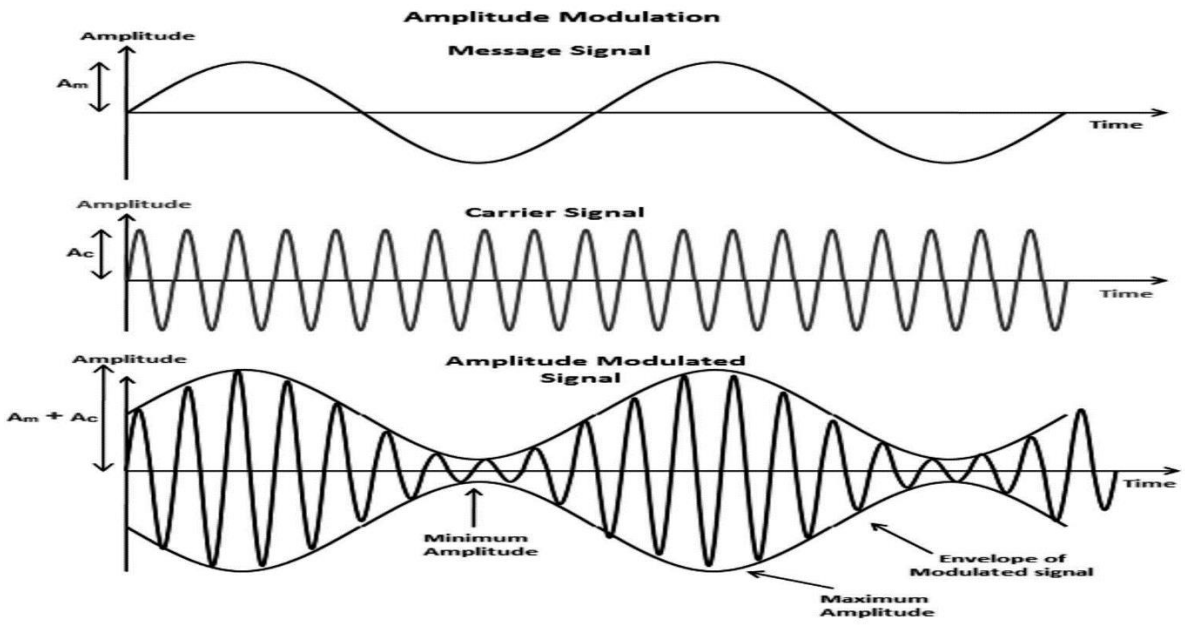


Figure 0-16: AM modulation

Simulating an AM modulation in LTSpice:

We Know the values, Such as:

Source signal =1V, 5Hz, offset 3V)

Carrier signal = 1V, 100KHz

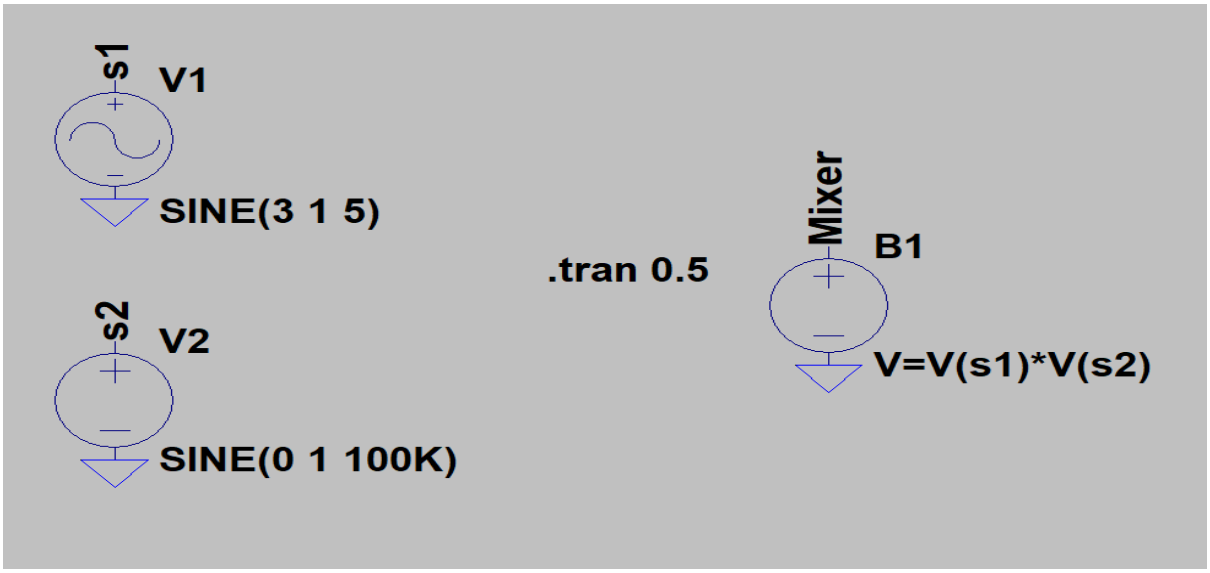


Figure 0-17: AM modulator

The Mixer is used to amplify the source signal s1 and the carrier signal s2, and the output is an amplified AM signal as shown below:

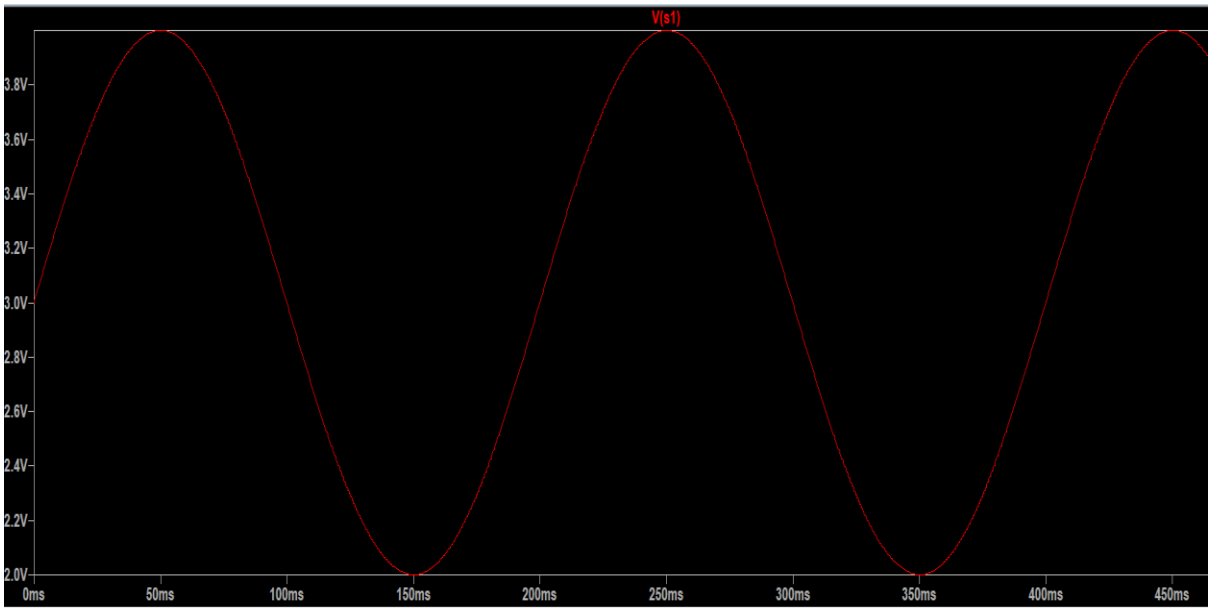


Figure 0-18:Signal wave(s1)

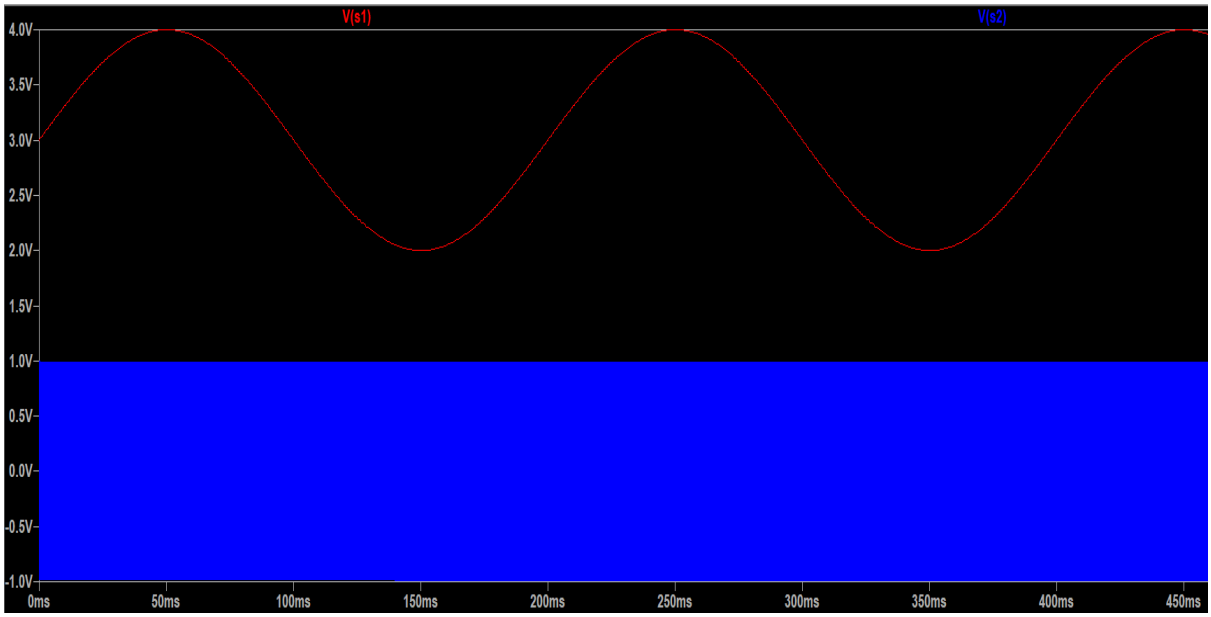


Figure 0-19:Carrier wave(s2)

Now we will mix these signals using the Mixer and get an amplitude signal wave form.

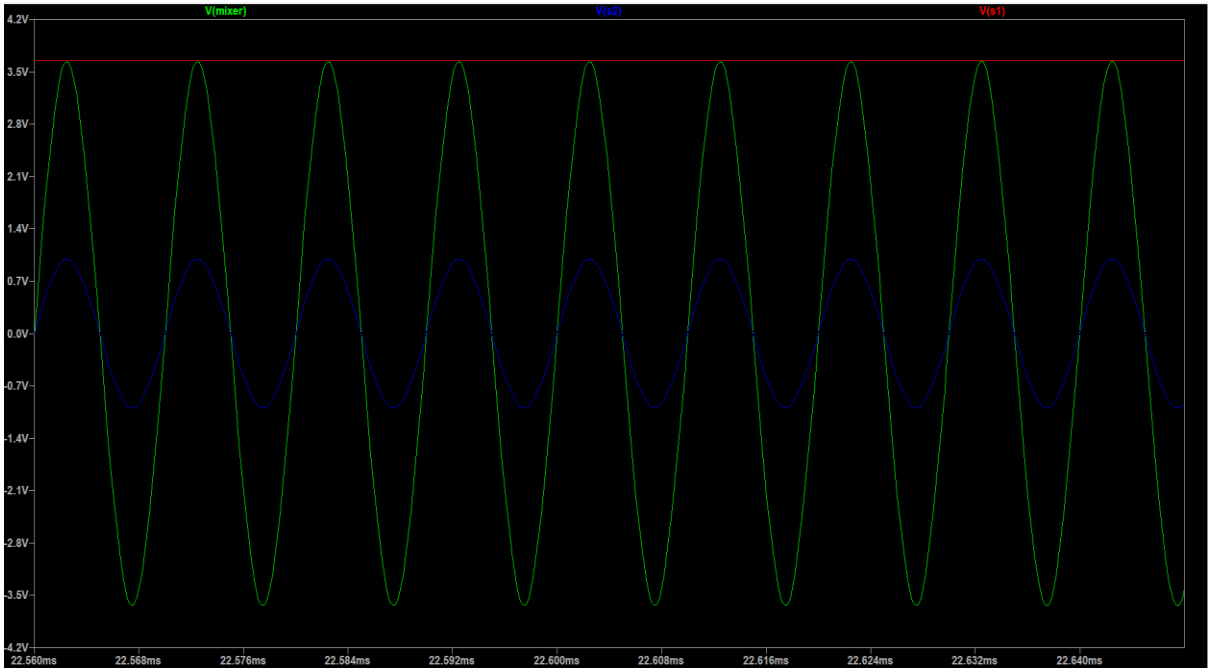


Figure 0-20: Amplitude AM signal (Mixer) (Zoomed Graph)

The above figure is the graph which shows all the s1, s2, and, mixer. To get AM amplitude signal we will probe the mixer end and the output is as shown below:

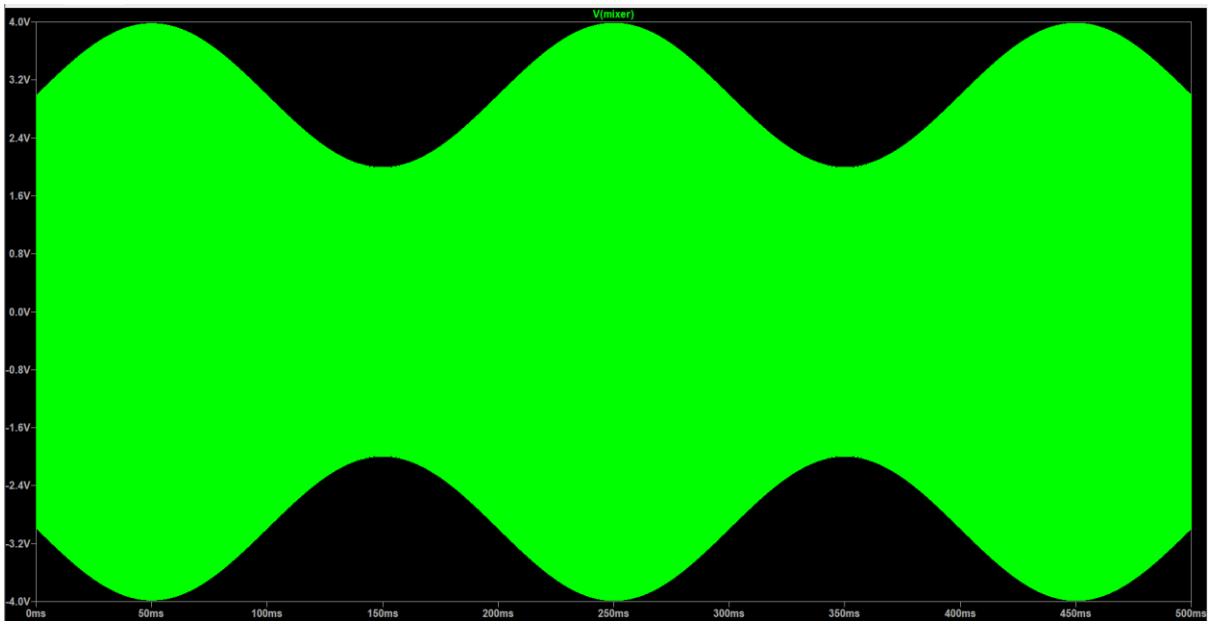


Figure 0-21:AM modulated signal

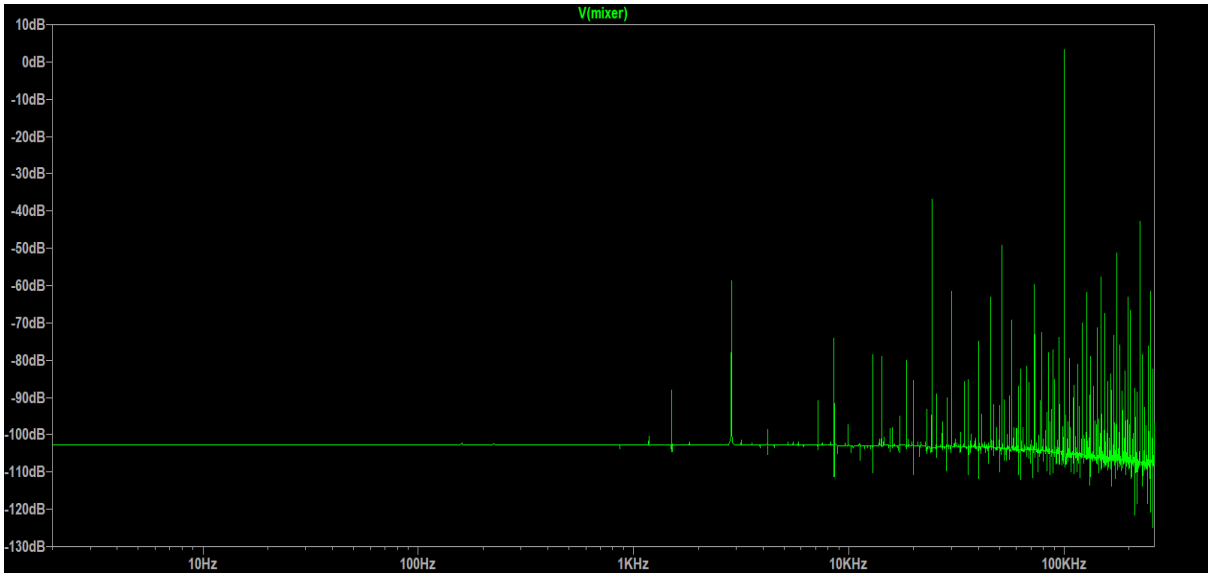


Figure 0-22:FFT graph

Here we can see in the result that the amplitude of both carrier and source signal is 1V and the amplitude of the amplified wave is near to 2V.

AM Demodulator

AM demodulator is used to demodulate the modulated wave.

Earlier we have combined the source signal and carrier wave to modulate the signal(V=V(s1)*V(s2)) where s1 is source signal and s2 is carrier wave.

Here to demodulate the signal we will combine the modulated wave and carrier signal.

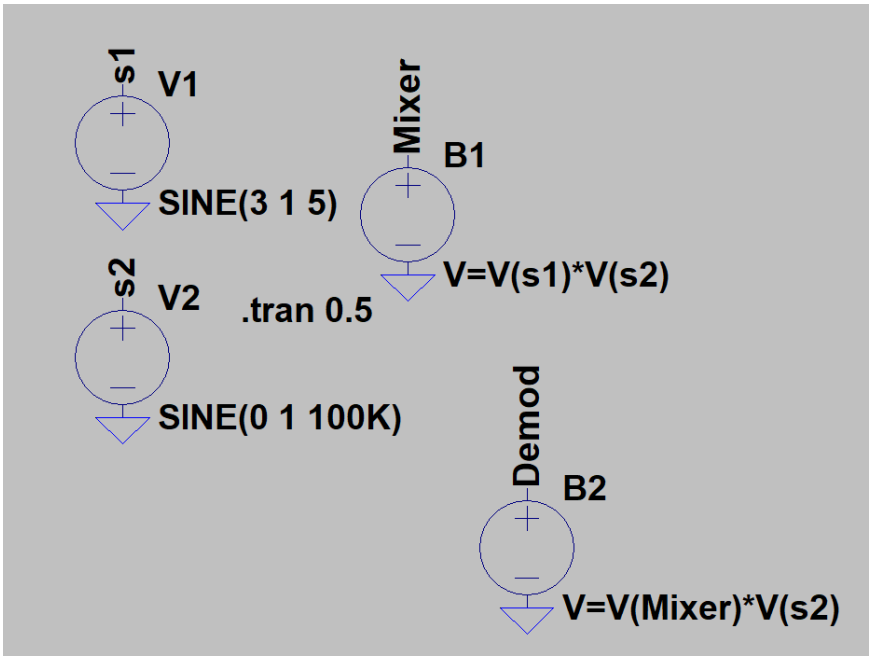


Figure 0-23:Demodulation

We will get the result of Demod as:

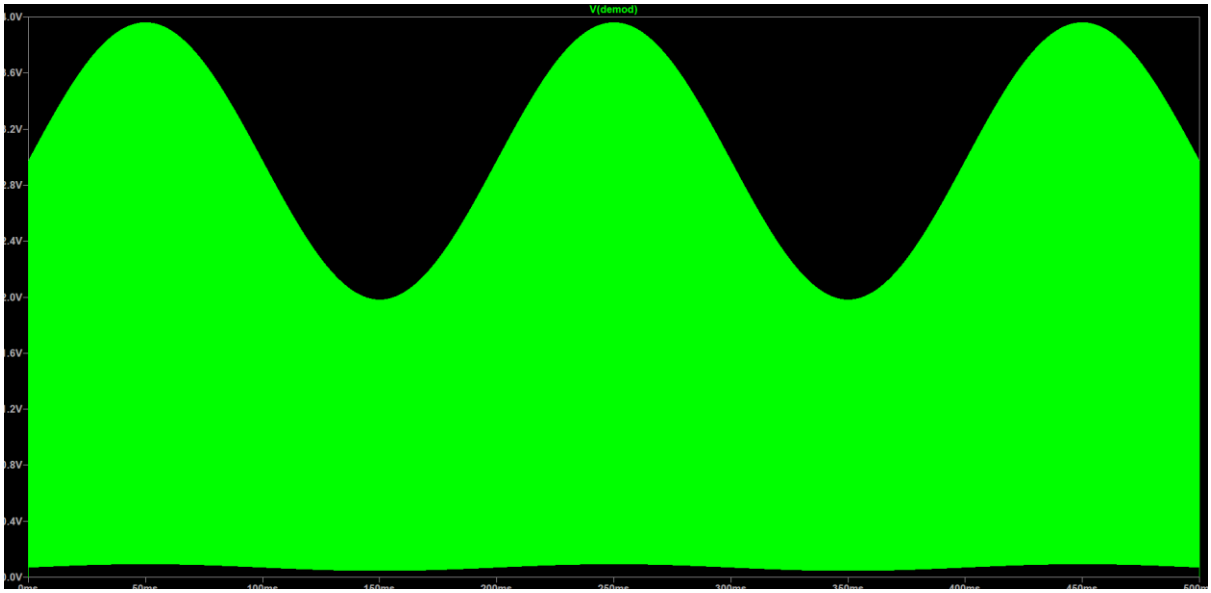


Figure 0-24:Output signal

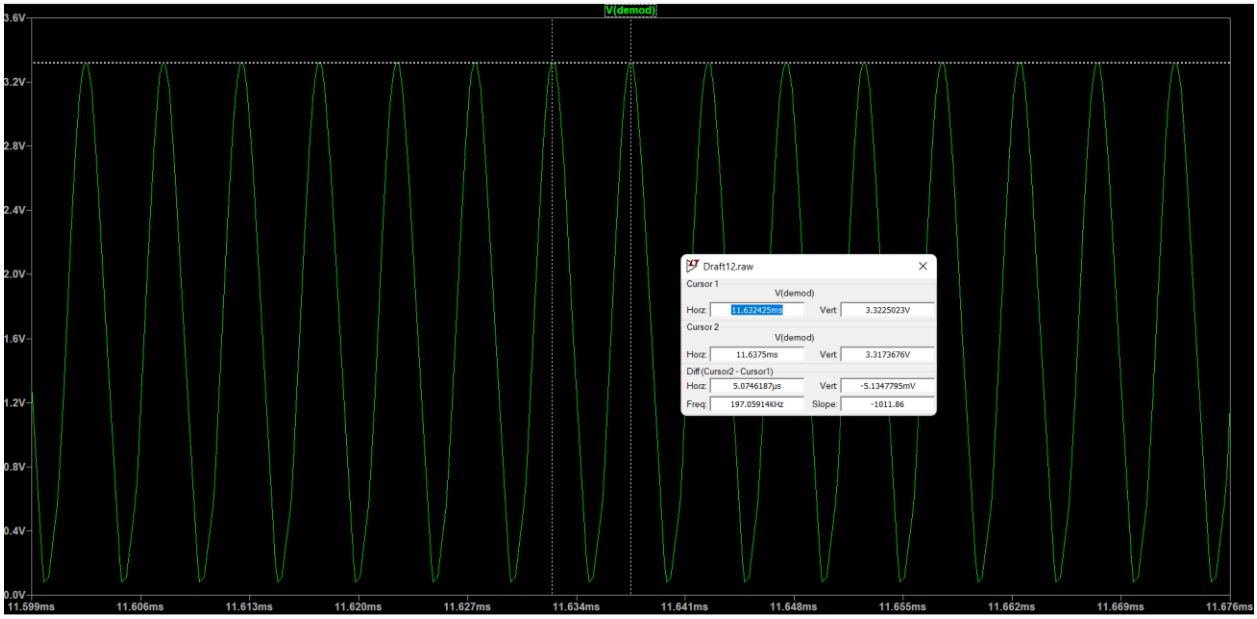


Figure 0-25:Wave form demodulator

Amplitude modulation centres the baseband spectrum around +fC. When the AM waveform is multiplied by the carrier, it pushes the baseband spectrum down to 0 Hz but also up to 2fC (in this case 200 MHz). that multiplication alone does not demodulate properly. Multiplication and a low-pass filter attenuate the 2fC shifted spectrum. The schematic below incorporates an RC low-pass filter with a 1.5 MHz cutoff.

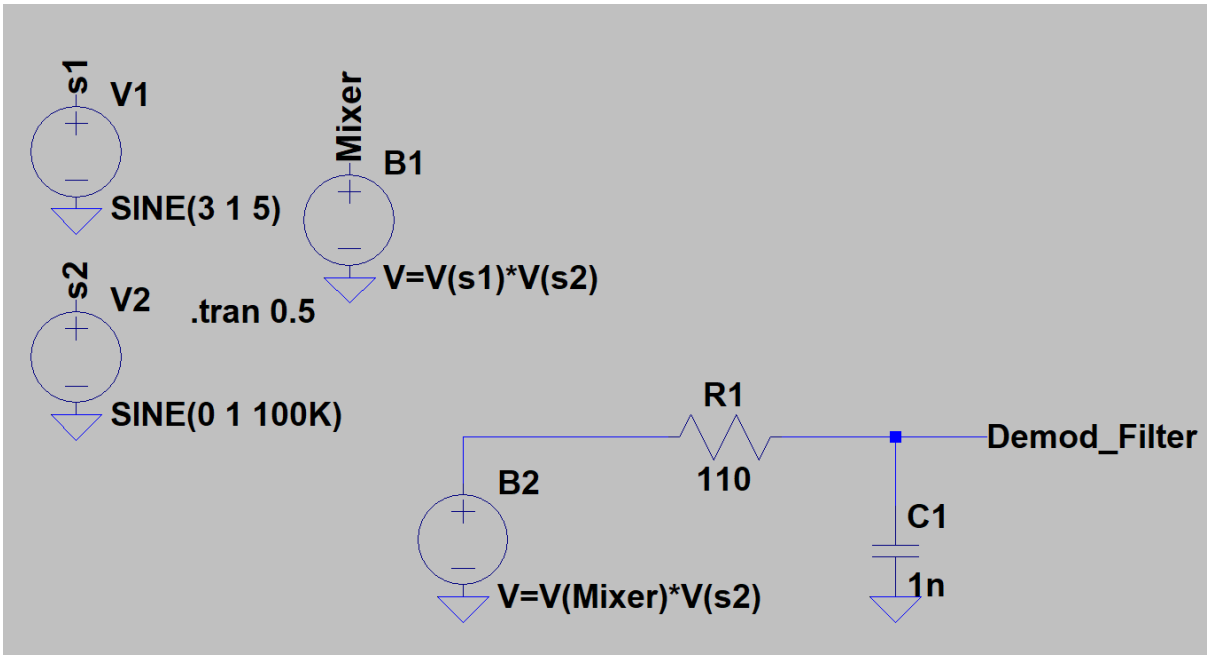


Figure 0-26:Circuit

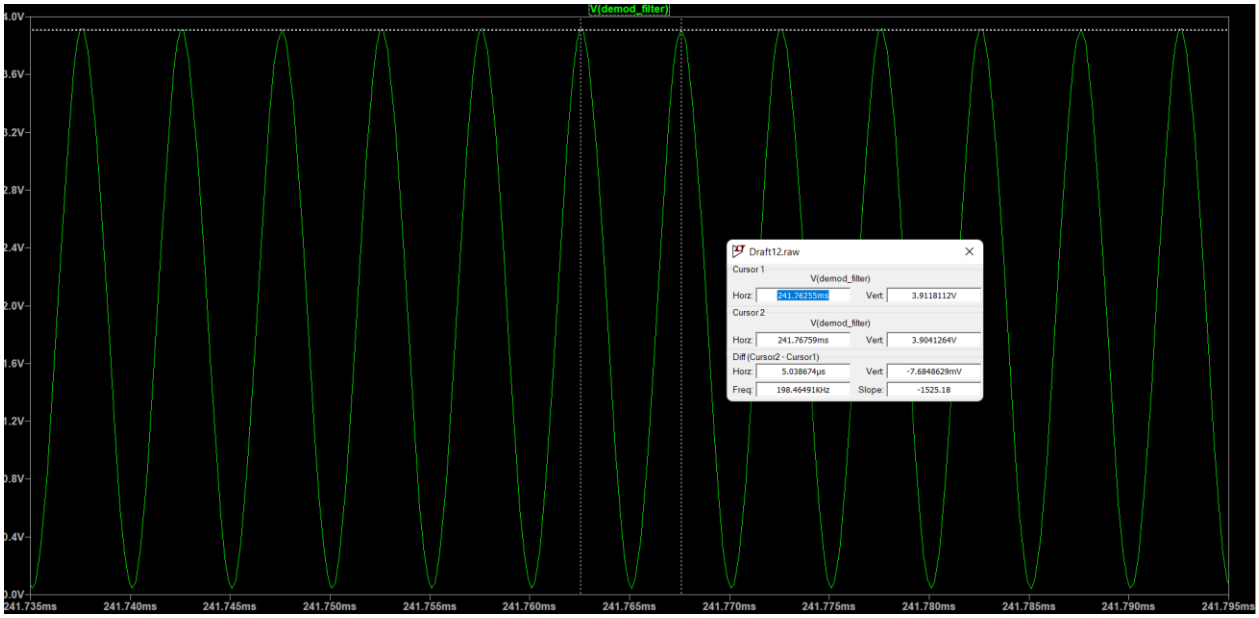


Figure 0-27:Demodulated wave

Task 2

CAN BUS

The CAN Bus (Controller Area Network) has two wires: CAN Low and CAN High. Each car's ECUs exchange data. CAN Bus is also designed to work reliably under difficult situations. Since the CAN bus standard is so versatile, it is frequently used in all automobiles.

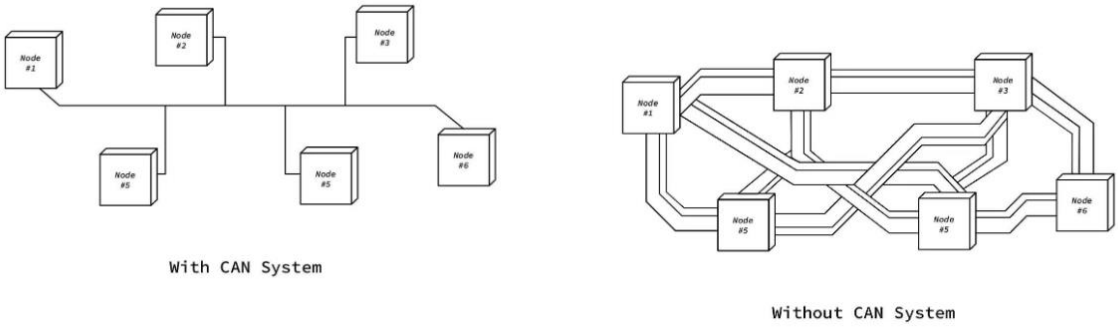


Figure 0-1:CAN system

The CAN bus allows an ECU to prepare and broadcast data (e.g. sensor data) (consisting of two wires, CAN low and CAN high). All other ECUs on the CAN network accept the broadcasted data, which they can then check and accept or reject.

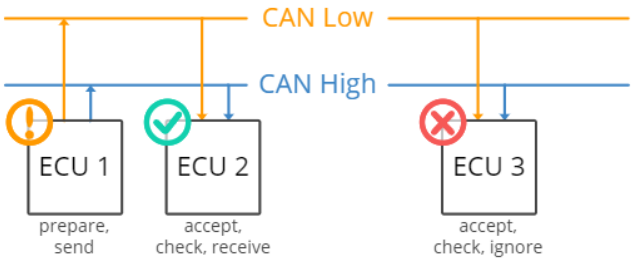
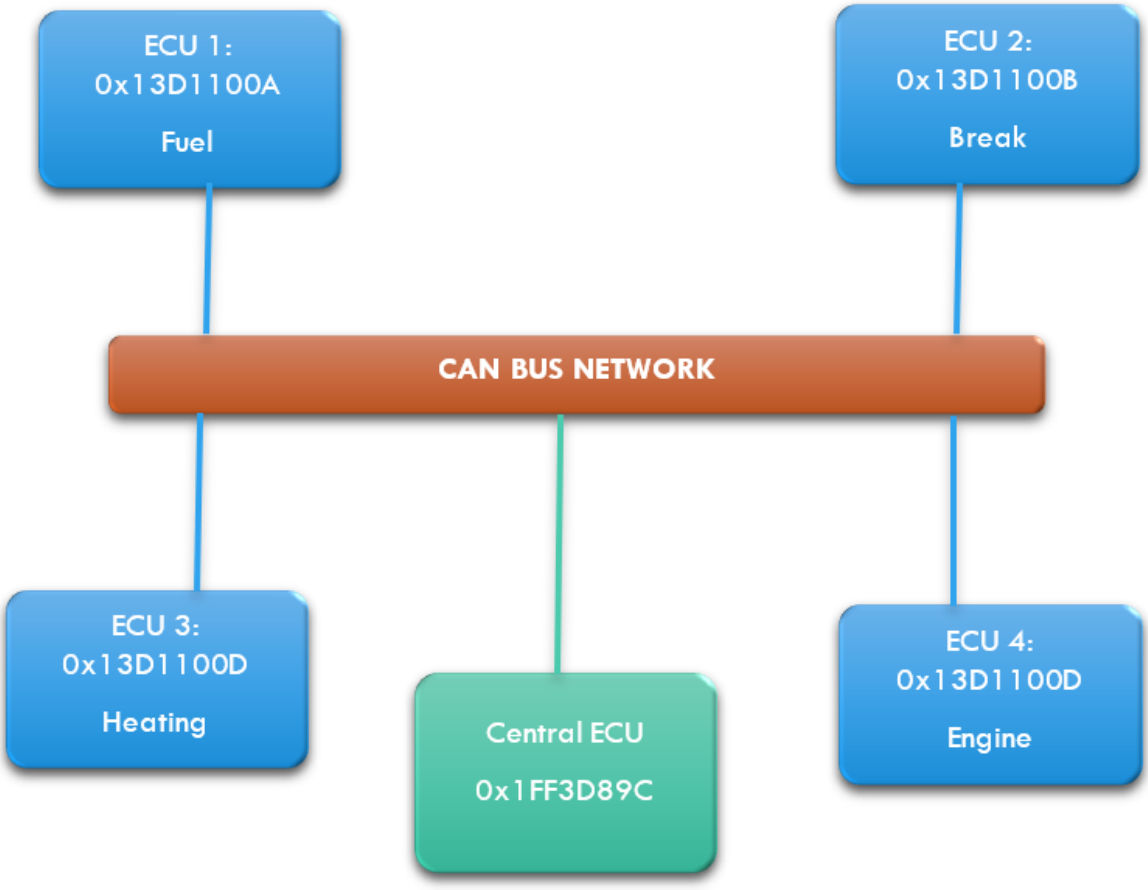


Figure 0-2: working of CAN bus

Let's, take a central unit ECU and four monitoring system and explain the mechanism.



The monitoring system sends the same data to a classification algorithm to produce an ECU fingerprint template. So we fingerprint each ECU's signal properties. ECU 4 sends start/stop signals, whereas ECU 2 sends brake signals. Signal-matching software can identify ECUs. The

monitoring unit knows which signals to send from which ECUs. In an attack, the adversary can utilise the identification of the ECU that should be sending the signal to shut down the engine.

That's when the monitoring equipment realises the signal isn't from the attached ECU The adversary's fingerprint may match an existing ECU or an unknown device.

This means the monitoring system recognises and warns the driver when an ECU identifier fails to provide a signal.

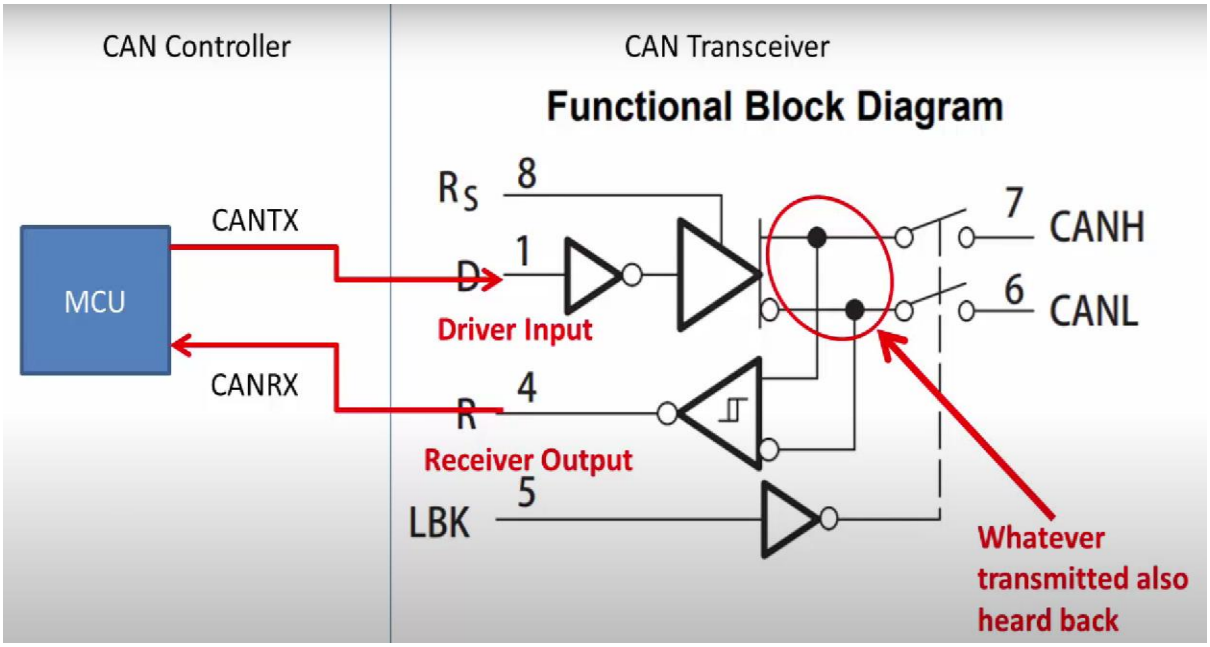


Figure 0-3: Block diagram of a Transceiver

CAN BUS Communication

We are given with:

System	ID	Binary
Central Unit ECU	0x1FF3D89C	11111111100111101100010011100
Fuel	0x13D1100A	10011110100010001000000001010
Brake	0x13D1100B	10011110100010001000000001011
Heating	0x13D1100C	10011110100010001000000001100
Engine	0x13D1100D	10011110100010001000000001101

When more than one CAN device transmits a message at the same time, the identification is used to identify which device gets network access first. The lower the identifier's numerical value, the greater its priority. In this case the priority of the monitoring system is as follows.

Priority1: Fuel

Priority2: Brake

Priority3: Heating

Priority4: Engine

The graphic below depicts a standard CAN frame with an 11-bit identification, which is the most common type found in autos. The expanded 29-bit identification frame is identical to the original except for the larger ID.

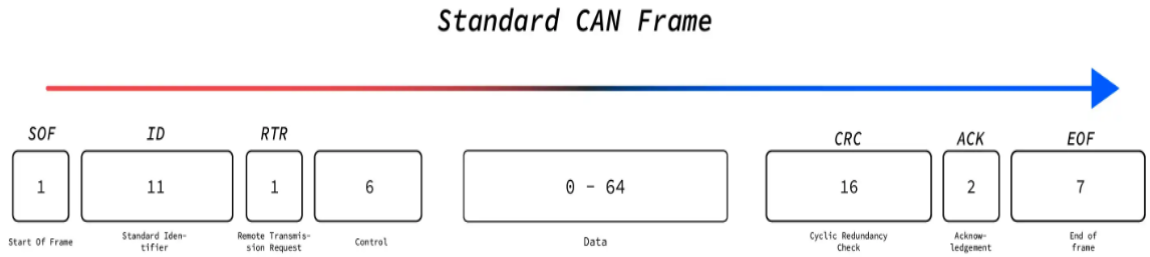


Figure 0-4: Standard CAN frame

We know CAN networks broadcast identifiers. Filter and mask work together to help us identify a message's unique identifier, while mask determines how much of this filter we must consider. the mask can contain any order of 1s or 0s. A bit set to 1 means the filter and identifier must match perfectly, while a bit set to 0 means the filter bit is ignored.

The job of the monitoring system is to validate the signal and accept it if it is intended for them. As previously stated, filter and mask are used to check the signal that will be received by a node.

The CAN message will send across like a broadcast message which contain the priority of the message as well as the destination address of which the message is to be sent.

CAN EXTENDED FRAME FORMAT	SOF	IDENTIFIER 11 BITS											SRR	IDE	IDENTIFIER EXTENSION 18 BITS																		RTR	...
J1939 FRAME FORMAT	SOF	PRIORITY			EDP	DP	PDU FORMAT (PF) 6 BITS (MSB)						SRR	IDE	PF (CONT.)		PDU SPECIFIC (PS) (DESTINATION ADDRESS, GROUP EXT. OR PROPRIETARY)								SOURCE ADDRESS								RTR	...
		3	2	1			8	7	6	5	4	3			2	1	8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1		
J1939 FRAME BIT POSITION	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	
CAN 29 BIT ID POSITION		28	27	26	25	24	23	22	21	20	19	18			17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0		

Figure 0-5: Extended 29-bit message format

Every node in the network will received the message broadcasted and then they will use the filter to differentiate the message whether the message sent is for them or not. In this example:

Take the communication from monitoring system to central ECU.

We know the ID value of central ECU and monitoring system. Lets take that into account to set appropriate filter and mask so that the message from all monitoring system is accepted by the central ECU.

Fuel	**0x13D1100A**	**10011110100010001000000001010**
Brake	0x13D1100B	10011110100010001000000001011
Heating	0x13D1100C	10011110100010001000000001100
Engine	0x13D1100D	10011110100010001000000001101

Here since all the bit except last 3 bit is same for all the monitoring system. we need to set the filter of the central ECU so that central ECU will only take the ID of monitoring system. Here we can take the bit which is same as 1 and rest as 0 to match our requirement.

Filter: 10011110100010001000000001000

Now we need to set the mask to enable the bit of filter that we need to check the CAN ID against. Here for our requirement the mask value is:

Mask: 11111111111111111111111111000

The mask and filter of communication between Engine to central ecu is as follows:

Engine(Source address)	0	0	0	0	0	0	0	1	1	0	1	ACCEPT
Mask	1	1	1	1	1	1	1	1	0	0	0	
Filter	0	0	0	0	0	0	0	1	0	0	0	

Here you can see that wherever the mask value is 1,the correspondence value of the source address and the filter of central ecu is same. So the central ECU will accept the data. Same way with this filter and mask for the central ECU, all other monitoring system's message will be accepted by the central ECU.

Heat(Source address)	0	0	0	0	0	0	0	1	1	0	0	ACCEPT
Mask	1	1	1	1	1	1	1	1	0	0	0	
Filter	0	0	0	0	0	0	0	1	0	0	0	

Fuel(Source address)	0	0	0	0	0	0	0	1	0	1	0	ACCEPT
Mask	1	1	1	1	1	1	1	1	0	0	0	
Filter	0	0	0	0	0	0	0	1	0	0	0	

Brake(Source address)	0	0	0	0	0	0	0	1	0	1	1	ACCEPT
Mask	1	1	1	1	1	1	1	1	0	0	0	
Filter	0	0	0	0	0	0	0	1	0	0	0	

Suppose if the central ECU received any other message, it will go through the same process and reject the message.

unknown(Source address)	0	1	0	1	0	0	1	1	0	1	1	Reject
Mask	1	1	1	1	1	1	1	1	0	0	0	
Filter	0	0	0	0	0	0	0	1	0	0	0	

Central ECU to monitoring system:

Same way we have to create a filter and mask for each monitoring system so that it will only accept the ID of central ECU.

ECU to FUEL:

CAN-ID of central ECU: 11111111100111101100010011100

Filter: 10011110100010001000000001010 ACCEPT

Mask: 10011110111010011011101101001

ECU to Brake:

CAN-ID of central ECU: 11111111100111101100010011100

Filter: 10011110100010001000000001011 ACCEPT

Mask: 10011110111010011011101101000

ECU to Heat:

CAN-ID of central ECU: 11111111100111101100010011100

Filter: 10011110100010001000000001100 ACCEPT

Mask: 10011110111010011011101101111

ECU to Engine:

CAN-ID of central ECU: 11111111100111101100010011100

Filter: 10011110100010001000000001101 ACCEPT

Mask: 10011110111010011011101101110

Here the monitoring system will only take its dedicated message sent by the central ECU and reject the intercommunication of the monitoring system. For example, if the message that is sent by heat is coming to engine via broadcast.

Heat to Engine:

CAN ID of Heat: 1001111010001000100000000110**0**

Filter: 1001111010001000100000000110**1** REJECT

Mask: 10011110111010011011101101110

TASK 3

The PDU mode sends binary data in 7- or 8-bit format. This is useful when sending compressed data, binary data, or encoding characters in a binary bit stream. The message is encoded in PDU mode and converted into a PDU frame containing information about the message such as sender, message length, protocol ID etc.

SCA	PDUT	MR	LON	NAC	DA	PID	DCS	VP	UDL	UD-PDU

Figure 3. PDU basic structure

Where:
- SCA: Service Centre Address
- PDU TYPE: Protocol Data Unit Type
- MR: Message Reference
- DA: Destination Address.
- PID: Protocol Identifier
- DCS: Data Coding Scheme
- SCTS: Service Centre Time Stamp
- VP: Validity Period
- UDL: User Data Length
- UD-PDU: User Data PDU

Figure 0-1: PDU packet structure

Text-to-PDU conversion rules say that the first byte's LSBs are taken up by MSBs in the second byte. In this case, the message "The deadline is tomorrow" is being sent from userA (+449876123456) to userB (+446789123456). With this information, let's make a frame for a PDU:

Destination address: Convert the sender information as follows.

0C81447698214365

Where:

0C: length of telephone

81: type of address (91 for international and 81 for local)

447698214365: Telephone number in reverse BCD format

Now let's encode the message:

PDU user data is normally sent in 7-bit format, thus we need to convert the message's hexadecimal value to binary (8 bit), then ignore the MSBs and convert the binary to septets.

Now we will use the text-to-PDU conversion rule to convert septets to octets and take their hex-decimal value.

Bytes	1	2	3	4	5	6	7	8
Message	T	h	e		d	e	a	d
Hex	54	68	65	20	64	65	61	64
Octet	01010100	01101000	01100101	00100000	01100100	01100101	01100001	01100100
Converted Septet	1010100	1101000	1100101	0100000	1100100	1100101	1100001	1100100
Octet	10101001	10100011	00101010	00001100	10011001	01110000	11100100	
UD-PDU	A9	A3	2A	C	99	70	E4	

Bytes	9	10	11	12	13	14	15	16
Message	l	i	n	e		i	s	
Hex	6c	69	6e	65	20	69	73	20
Octet	01101100	01101001	01101110	01100101	00100000	01101001	01110011	00100000
Converted Septet	1101100	1101001	1101110	1100101	0100000	1101001	1110011	0100000
Octet	11011001	10100111	01110110	01010100	00011010	01111001	10100000	
UD-PDU	D9	A7	76	54	1A	79	A0	

Bytes	17	18	19	20	21	22	23	24
Message	t	o	m	o	r	r	o	w
Hex	74	6f	6d	6f	72	72	6f	77
Octet	01110100	01101111	01101101	01101111	01110010	01110010	01101111	01110111
Converted Septet	1110100	1101111	1101101	1101111	1110010	1110010	1101111	1110111
Octet	11101001	10111111	01101110	11111110	01011100	10110111	11110111	
UD-PDU	E9	BF	6E	FE	5C	B7	F7	

We received the UD-PDU user data:

Bytes	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
UD-PDU	A9	A3	2A	0C	99	70	E4	D9	A7	76	54	1A	79	A0	E9	BF	6E	FE	5C	B7	F7

Now userA can generate a PDU packet frame and send it to AP-1. This message's PDU packet frame is as follows:

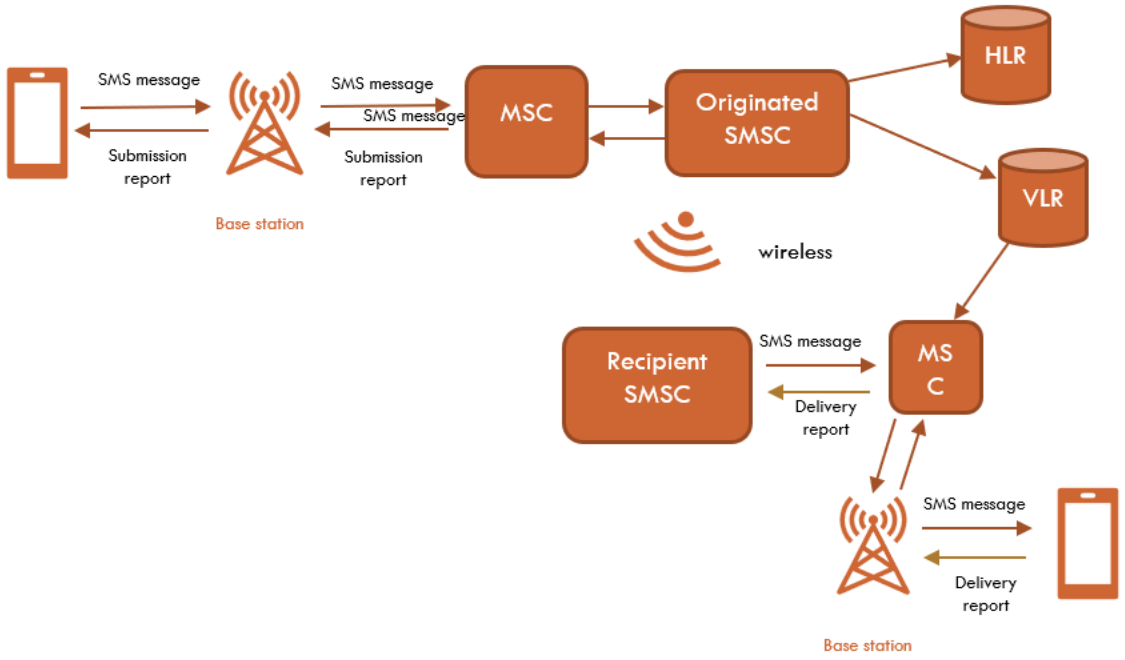
0001000C81447698214365000018A9A32A0C9970E4D9A776541A79A0E9BF6EFE5CB7F7

Where:

00	default SMSC number
01	SMS message
00	TP-Message-Reference
0C81447698214365	length and telephone no.
00	Protocol Identifier
00	Data coding scheme
18	Length of the message
A9A32A0C9970E4D9A776541A79A0BF6EF35CB7F7	This octet represents the message

b.Communication between AP-1 and AP-2:

The message is then sent via FHSS to AP1 to AP2. The network diagram of the communication of the SMS sent from userA and userB will look like the figure shown below:



The originator and recipient SMS centres are linked via an SMS gateway or a communication protocol shared by both SMS centres. The SMS message is received by the MSC(Mobile Switching Centre) act as an controller which will re-code the encoded message to analogue signal. Then this goes originator SMS centre which has HLR and LHR which contain home location register and visitor location register, which checks the data and forwards it to the recipient SMS centre. The recipient SMS centre is responsible for sending and storing SMS messages if the recipient is offline. Then a delivery report is given back to the recipient SMSC which will transmit back and a status report is send back to the sender via originated SMSC.

FHSS:

FHSS (Frequency hopping spread spectrum) is used to hop the byte into several frequencies, making it impossible for an attacker to guess the message transmitted and retrieve the data. In this scenario, the FHSS has four channels, each of which can only send three bytes at a time through channel.

There are several jumping techniques:

GSM baseband hopping:

Each transceiver in baseband frequency hopping has its own RF carrier frequency. The number of hopping frequencies is equal to the number of GSM transceivers.

• Transceiver controller bursts are sent to different transmitters via a bus interface (figure 2).

• A narrow band filter combiner connects up to 16 RF transceivers. It can lose no more than 3 dB.

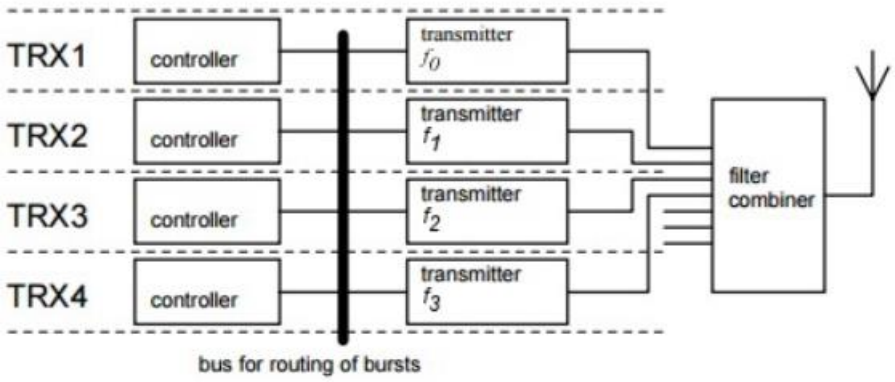


Figure 0-2:GSM baseband

GSM synthesised frequency hopping:

Its frequency is changed to match the hopping pattern. Below is an FHSS transmitter. The PN sequence generates a random channel table that modulates the synthesizer's output. To use an RF mixer to convert numerous synthesiser outputs to carrier frequencies. Each burst has its own RF carrier frequency. The PN sequence is known to both parties, making data recovery simple.

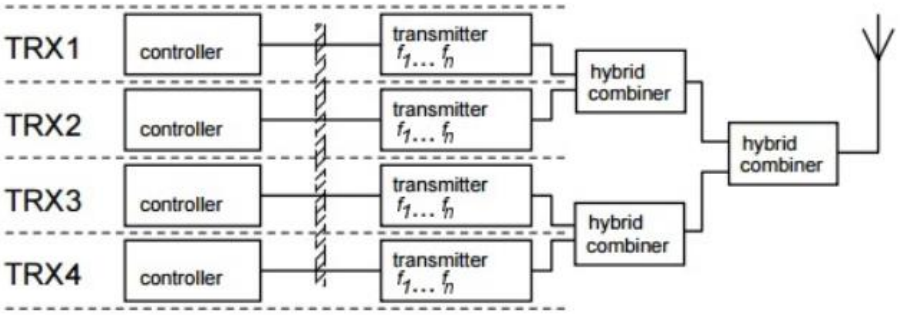


Figure 0-3: synthesised frequency hopping

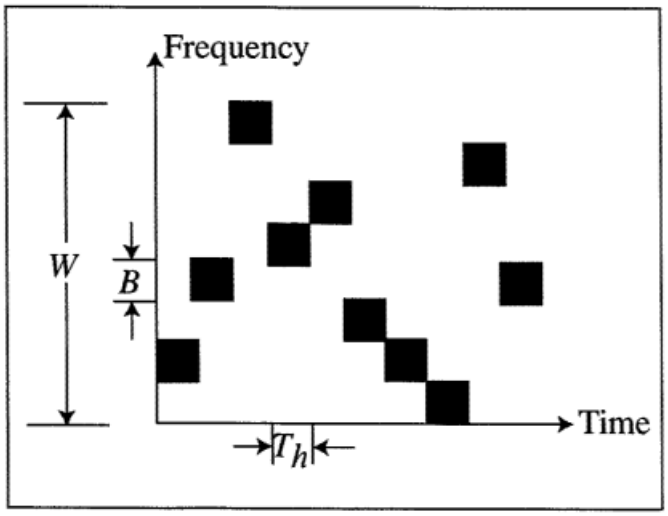


Figure 0-4:Hopping pattern

As shown in the figure above, the data will hop into different frequency at interval of time.

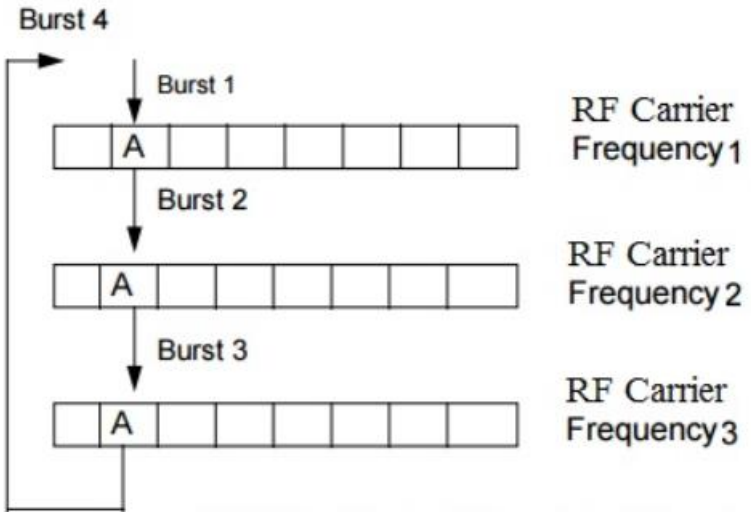


Figure 0-5:synthesised frequency hopping

Here in this scenario, we have a PDU sequence. This PDU sequence will go through the process called fragmentation and will convert it into 3byte individual sequence which will go for hopping.

We need to set a default hopping sequence in order to achieve this process. Here we will use a cyclic sequence (HSN=0):f4,f1,f2,f3, f4,f1,f2,f3,f4,f1..

This means that the byte will first go to channel4, then to channel1, then to channel2 etc.

Then the fragmented byte is received by a hybrid combiner and will combine the bytes using the sequence and will convert back to the PDU form which we send the message.

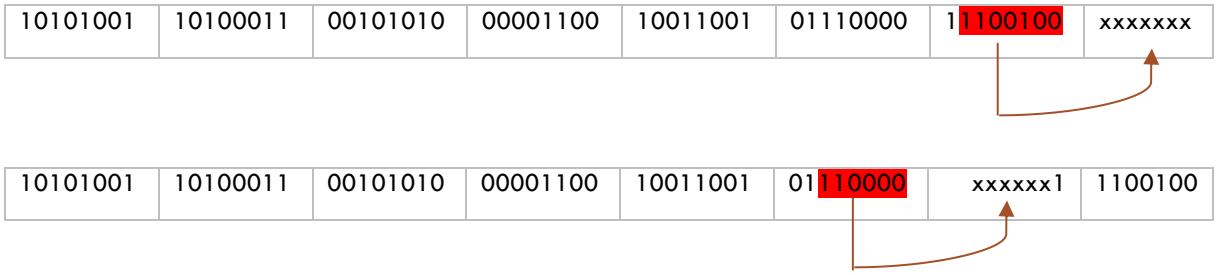
c. Decoding the message:

Now, when userB receives a PDU message, userB must decode it. To decode, we need to check the value of data coding scheme and determine how the data is encoded in this message. Here in this case the value is a 7byte 8bit encoded message. Next, we will see the value of length of the message in the packet frame to determine how many octets is required to decode the message.

Here the length of the message in Hex is 18 which corresponds to 24byte.

we must first transform a 7-byte 8-bit PDU message to an 8-byte 7-bit septet.

for that we need to shift the 7-bit LSBs of 7th byte position to the MSBs of 8th byte position and so on.



By using this rule, the message is decoded in our scenario:

Bytes	1	2	3	4	5	6	7	8
UD-PDU	A9	A3	2A	C	99	70	E4	
Octet	10101001	10100011	00101010	00001100	10011001	01110000	11100100	
Decoding	1010100	1101000	1100101	0100000	1100100	1100101	1100001	1100100
Hex	54	68	65	20	64	65	61	64
Character	T	h	e		d	e	a	d

Bytes	9	10	11	12	13	14	15	16
UD-PDU	D9	A7	76	54	1A	79	A0	
Octet	11011001	10100111	01110110	01010100	00011010	01111001	10100000	
Decoding	1101100	1101001	1101110	1100101	0100000	1101001	1110011	0100000
Hex	6C	69	6E	65	20	69	73	20
Character	l	i	n	e		i	s	

Bytes	17	18	19	20	21	22	23	24
UD-PDU	E9	BF	6E	FE	5C	B7	F7	
Octet	11101001	10111111	01101110	11111110	01011100	10110111	11110111	
Decoding	1110100	1101111	1101101	1101111	1110010	1110010	1101111	1110111
Hex	74	6f	6d	6f	72	72	6f	77
Character	t	o	m	o	r	r	o	w

Final received message:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
T	h	e		d	e	a	d	l	i	n	e		i	s		t	o	m	o	r	r	o	w

We got the same message as userA sent.

Reference

Sciencedirect.com. (2010). *Amplitude Modulation - an overview | ScienceDirect Topics*. [online] Available at: https://www.sciencedirect.com/topics/engineering/amplitude-modulation

Kraus, G., Tettnang, E. and Germany (2010). *SPICE-Simulation using LTspice IV Tutorial for successful simulation of electronic circuits with the free full version of LTspice IV (before named 'SwitcherCAD'), available at Linear Technologies (www.linear.com)*. [online] Available at: http://www.gunthard-kraus.de/LTSwitcherCAD/SwitcherCAD-Tutorial_English/pdf-File/LTspice_4_e2.pdf

Storey, N. (2017). *Electronics : a systems approach*. Harlow, England ; New York: Pearson. Copyright.

www.allaboutcircuits.com. (n.d.). *Amplitude Modulation in RF: Theory, Time Domain, Frequency Domain | Radio Frequency Modulation | Electronics Textbook*. [online] Available at: https://www.allaboutcircuits.com/textbook/radio-frequency-analysis-design/radio-frequency-modulation/amplitude-modulation-theory-time-domain-frequency-domain/

www.allaboutcircuits.com. (n.d.). *How to Demodulate an AM Waveform | Radio Frequency Demodulation | Electronics Textbook*. [online] Available at: https://www.allaboutcircuits.com/textbook/radio-frequency-analysis-design/radio-frequency-demodulation/how-to-demodulate-an-am-waveform/

www.auldies.euweb.cz. (n.d.). *LTspice - 3 ways how to get an AM - amplitude modulated signal.* [online] Available at: http://www.auldies.euweb.cz/me/Amf1.html

brainwagon.org. (n.d.). *brainwagon» Tank Circuits…*. [online] Available at: https://brainwagon.org/2009/12/07/tank-circuits/

electronicsreference.com. (2021). *Low Pass Filter - Electronics Reference*. [online] Available at: https://electronicsreference.com/analog/low_pass_filter/

www.allaboutcircuits.com. (n.d.). *How to Demodulate an AM Waveform | Radio Frequency Demodulation | Electronics Textbook*. [online] Available at:

https://www.allaboutcircuits.com/textbook/radio-frequency-analysis-design/radio-frequency-demodulation/how-to-demodulate-an-am-waveform/

Archana, M., Wagh, S., Sneha, M. and Joshi, D. (2015). DESIGN AND IMPLEMENTATION OF CAN COMMUNICATION SYSTEM FOR AUTOMOTIVE APPLICATION USING HIL. [online] (2), pp.2394-0697. Available at: http://troindia.in/journal/ijcesr/vol2iss7/114-118.pdf

AutoPi.io (n.d.). *CAN Bus Protocol: The Ultimate Guide (2022) | AutoPi*. [online] AutoPi.io. Available at: https://www.autopi.io/blog/can-bus-explained/

CSS Electronics. (n.d.). *CAN Bus Explained - A Simple Intro (2021)*. [online] Available at: https://www.csselectronics.com/pages/can-bus-simple-intro-tutorial

Choi, W., Jo, H.J., Woo, S., Chun, J.Y., Park, J. and Lee, D.H. (2018). Identifying ECUs Using Inimitable Characteristics of Signals in Controller Area Networks. *IEEE Transactions on Vehicular Technology*, [online] 67(6), pp.4757–4770. Available at: https://arxiv.org/pdf/1607.00497.pdf

www.microchip.com. (n.d.). *CAN Mask Filter setting | Microchip*. [online] Available at: https://www.microchip.com/forums/m456043.aspx

Tractor Hacking. (n.d.). *CAN ID Explanation*. [online] Available at: https://tractorhacking.github.io/IdExplanation/

www.gsmfavorites.com. (n.d.). *Introduction to the SMS PDU and Text format*. [online] Available at: https://www.gsmfavorites.com/documents/sms/pdutext/#:~:text=Introduction%20to%20SMS%20PDU%20Mode

techsofar.com. (2020). *Combining SMS Messages: The Complete Guide | TechSoFar*. [online] Available at: https://techsofar.com/combining-sms-messages/

kb.iu.edu. (n.d.). *Decimal-hexadecimal-binary conversion table*. [online] Available at: https://kb.iu.edu/d/afdl

techsofar.com. (2020). *More Sending SMS In PDU Mode | TechSoFar*. [online] Available at: https://techsofar.com/more-on-the-sms-pdu/

infoheap.com. (n.d.). *Online characters, words and lines count - InfoHeap*. [online] Available at: https://infoheap.com/char-count-online/

www.developershome.com. (n.d.). *SMS Tutorial: What is an SMS Center / SMSC? SMSC's Duty in a Wireless Network System*. [online] Available at: https://www.developershome.com/sms/sms_tutorial.asp?page=smsc

Wikipedia. (2021). *Data Coding Scheme*. [online] Available at: https://en.wikipedia.org/wiki/Data_Coding_Scheme#:~:text=Data%20Coding%20Scheme%20is%20a

blog.actorsfit.com. (n.d.). *General rules for encoding of PDU SMS - actorsfit*. [online] Available at: https://blog.actorsfit.com/a?ID=00150-81bdc793-2bf0-487c-9346-a4ee9031fea1

www.spallared.com. (n.d.). *Introduction*. [online] Available at: http://www.spallared.com/old_nokia/nokia/smspdu/smspdu.htm#_Toc485435713

www.rfwireless-world.com. (n.d.). *Baseband frequency hopping vs synthesized frequency hopping*. [online] Available at: https://www.rfwireless-world.com/Terminology/GSM-Baseband-frequency-hopping-vs-Synthesized-frequency-hopping.html

teletopix.org. (n.d.). *How many Frequency Hopping Modes in GSM | TELETOPIX.ORG*. [online] Available at: http://teletopix.org/gsm/how-many-frequency-hopping-modes-in-gsm/

Svet, V. and Bogdan, I. (2003). *Synthesized frequency hopping in GSM networks: implementation and results*. [online] IEEE Xplore. doi:10.1109/SCS.2003.1227108

TelTech Insight. (n.d.). *Technique Frequency Hopping in GSM Network*. [online] Available at: https://teltechinsight.blogspot.com/2019/01/technique-frequency-hopping-in-gsm.html

Wikipedia. (2022). *Concatenated SMS*. [online] Available at: https://en.wikipedia.org/wiki/Concatenated_SMS

ldapwiki.com. (n.d.). *Ldapwiki: Mobile20Switching20Center*. [online] Available at: https://ldapwiki.com/wiki/Mobile%20Switching%20Center#:~:text=Mobile%20Switching%20Center%20(MSC)%20is