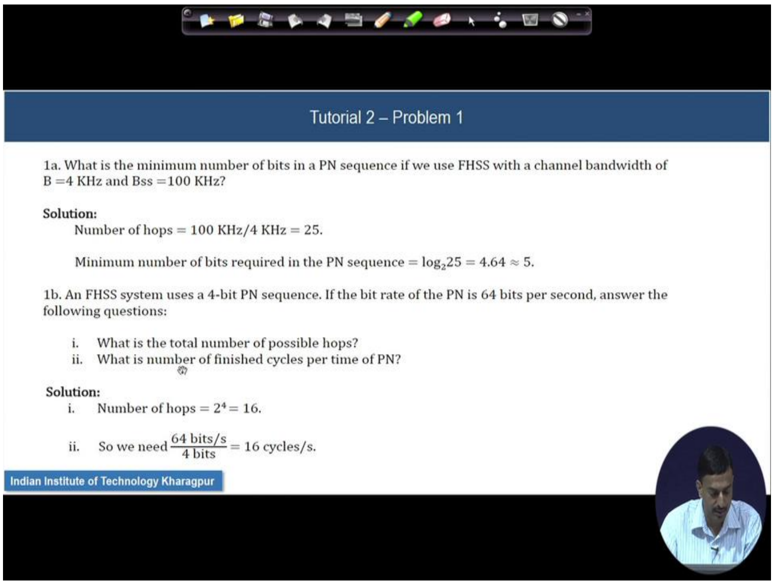
Spread Spectrum Communications and Jamming

Prof. Kutty Shajahan M
G S Sanyal School of Telecommunications
Indian Institute of Technology, Kharagpur

Lecture – 12
Tutorial – II

(Refer Slide Time: 00:30)

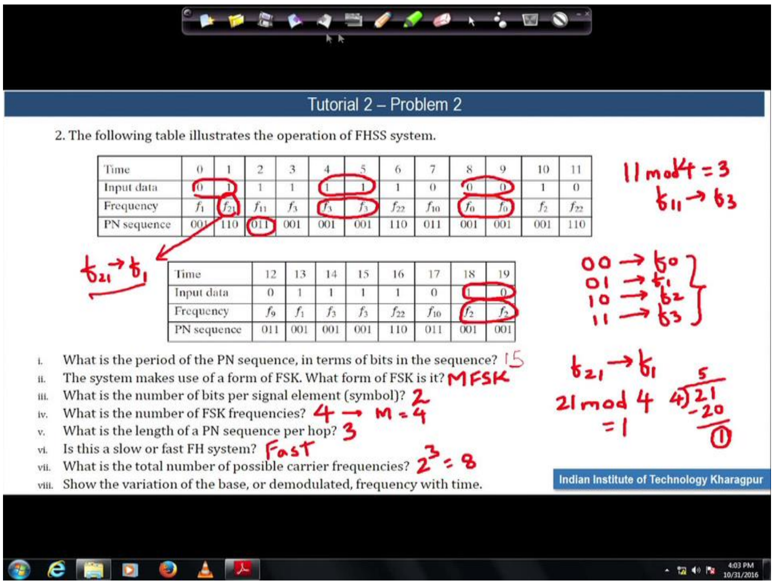


In tutorial two, we will solve the set of five problems on frequency-hopping spread spectrum systems. As you can see in the first problem, we are asked to calculate the number of minimum of bits required in a PN sequence if we use FHSS. And the channel bandwidth of signal is basically specified as 4 kilo hertz, and the spread spectrum bandwidth is of 100 kilo hertz which is greater than the channel bandwidth. As we know the number of hops required in order to spread out this 4 k signal 100 k is nothing but the ratio of the spread spectrum bandwidth to the channel bandwidth. So, the total number of hops is equal to 25. And the in order to realize 25 hops, we require minimum number of bits equal to log to the base 2 25 because 2 to raise to the number of bits in a PN sequence is basically equal to the number of hops over the spread spectrum bandwidth.

So, we basically calculate the minimum number of bits required as log to the base 2 of this number of hops, which is equal to 4.64. And they rounded to the next highest integer which is equal to 5, rounding to lower will not do, because 2 raise to 4 is 16 which will not give you the number of hops that is required.

In the second problem we are given a four bit PN sequence and asked to find the total number of possible hops, which is basically a reverse procedure to what we did in the first problem. So, straight away, if you are given number of bits then 2 raise to the number of bits in the PN sequence is equal to the total number of hops, which in this case turns out to be 16, and moreover the bit rate of the PN sequence is specified to be equal to 64 bits per second. So, we need to find the number of finished cycles per unit time on of this PN sequence. Since, it has 64 bits in a second there are four bits in a PN sequence. So, a total of 64 by 4 - 16 cycles of this 4-bit PN sequence will be covered in 1 second. So, therefore, that settles part two of problem 1 b.

(Refer Slide Time: 03:19)



In the next problem, we are given a table of data to start with in the first row we have the time index from 0 to 19 corresponding to every unit time we are given the input data in the form of a bit stream as you can see. And we are given the frequency for every time index, so we see that there is hop from my f 1 to f 21 to f 11 and so on so forth for every such time index. And corresponding to every such hop, we have a free PN sequence which is assigned which comprises of the last row of this table.

So, the questions there is a set of questions to be answered and we say of the first one deals with finding the period of this PN sequence in terms of for the number of bits of the PN sequence. And the close observation of a row number four over here which is nothing but the PN sequence reveals basically that we have after every a set of five such private PN sequences, we have a repetition. Let me just illustrate that we see that we can we have this first set of PN sequences 001, 110, 011, 001 and 001. We see that this basically this repeats after once again and so on and so forth.

So, what we notice I am sorry this should basically be let me just repeat this once again. So, we have this five – 1, 2, 3 4, 5 and this same thing is repeated over here we can see. So, this sequence is similar to this and so on and so forth. So, basically what we have is the period of PN sequence which is in this case is 5 into 3, which is 15-bits. The second part of the question is what form of FSK is this system. So, what we notice is that the pattern of frequencies are such that if you are able to map a single frequency, di-bit or tri-bit to a corresponding frequency then we should be able to get this answer.

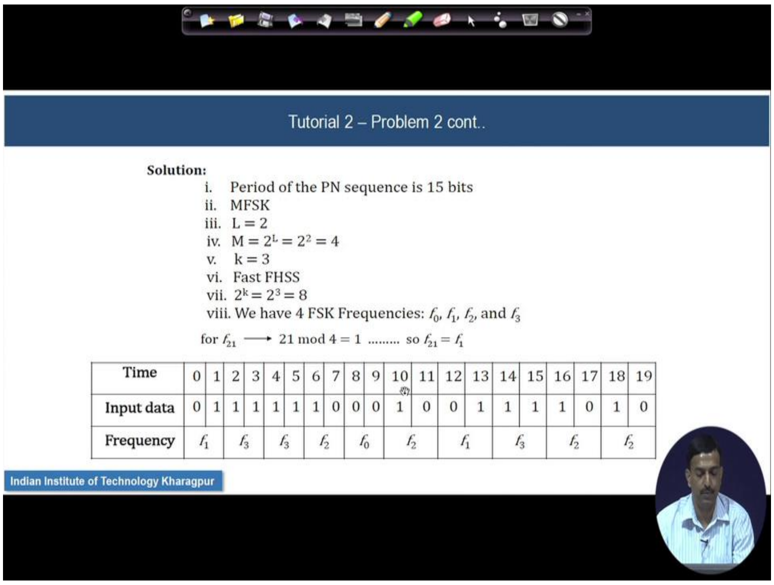
So, what we notice is for example, is that we have f 3 frequency which is assigned to 1 1 over here rather the other way round one way one combinational 1 1 is assigned to f 3. Similarly we notice that a combination of 0 0 is assigned to f naught and we also have once again a combination of 1 1 assigned to f 3, and here we can see 1 0 assigned to f 2. So, we see some kind of a pattern emerging here, so 0 0 is f naught, and c 1 1 has mapped to f 3; 1 0 maps to f 2, and presumably 0 1 would map to f 1 that we have a 0 1 combination at the beginning itself, which is map to f 1 and f 21. So, we will see that f 2 1, it will subsequently map or should subsequently map at the receiver to f 1. So, this is something we will show at the end.

But it appears like we have a Mary FSK system to start with that is quite clear. And it also is obvious that per symbol that is per f, we have a di-bit combination. So, we have a number of bits per symbol equal to 2. And we have a set of four frequency is a frequency here, so we have number of FSK frequency is equal to 4. The length of the PN sequence for hop we can say that the frequency keeps changing for every time index, and every time index has a length equal to 3, so this is equal to 3. And we also noticed that for every single element that is a bit di-bit the frequency changes and so there are two frequencies basically being hopped onto for a every di-bit combinations. So, basically it is a case where the number of hops is greater than the number of signal elements. So, this is obviously, a fast FS system.

Since we have 3-bits per arm PN sequence, so we can have as many as 2 raised to 3 which is equal to 8 carrier frequencies. And finally, we need to figure out a way in order to demodulate the frequencies. So, the question is how to map this a frequency is f 21, f 22 f 10 back to a frequency which belongs to this set on which is nothing but the modulating frequency. So, the idea to do that is by choosing the given frequency for example, we choose f 2 1 and the ideas to map this f 21 to 1 of these. So, how to do that is basically by taking this arm subscript and finding out f 21, sorry the subscript mod 4, because it is a 4-FSK system basically, so M is equal to 4. So, 21 mod 4 can be calculated in the standard form as to how we find out mod, so we basically just divide 21 by 4, so we know that this is nothing but 1 is the reminder. So, this reminder is nothing but the result of this operation that is 21 mod 4.

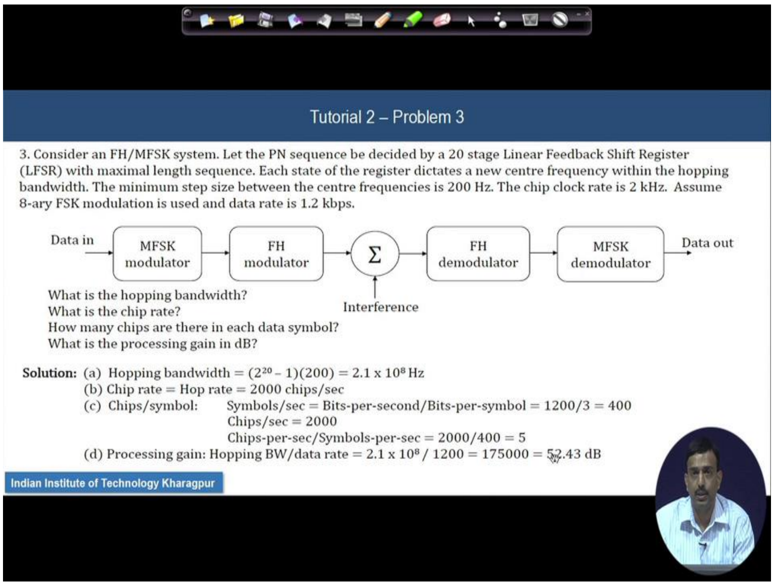
So, we map the subscript 21 to the subscript 1 which is the remainder of this operation. So, we may f 21 equal to and that is what I was talking about over here. So, this combination of 0 1 is basically f 1. So, we can try it out with other elements as well for example, f in the case of f 11 what we need to do is 11 mod 4. So, this after this calculation it will be equal to 3, so f 11 maps to f 3. So, this f 11 become f 3, which is nothing but the frequency corresponding to the di-bit 1 1. So, this basically completes this particular problem. And we have the answers over here which what was solved for before.

(Refer Slide Time: 12:01)



And we will always say that the mapping procedure or the demodulating procedure for each of these frequencies will give back a set of frequencies, sorry a frequency corresponding to a set of bits, so that is what we have in this table which is not a demodulated frequency.

(Refer Slide Time: 12:28)



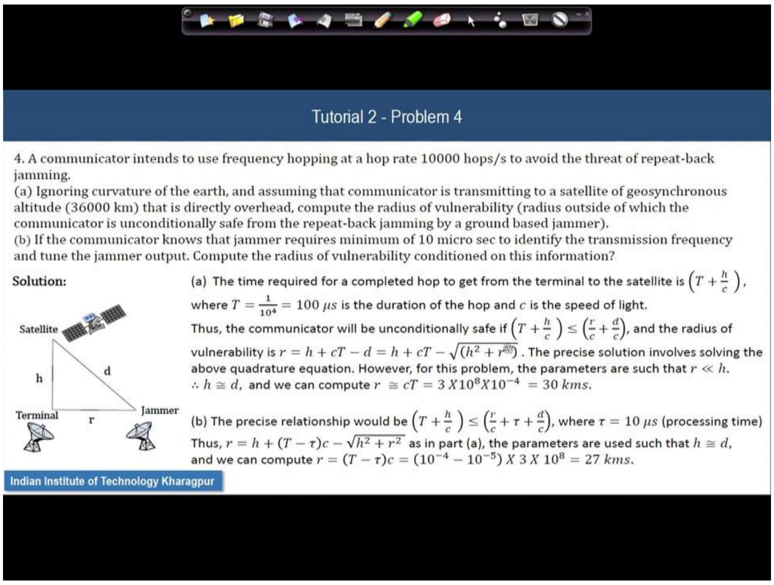
So, we move on to the third problem. In this problem, we had given a PN sequence which is generated using a 20 stage linear feedback shift register, and it is a maximum length sequence. So, basically we know that a 20 stage linear feedback shift register will give you a maximal length of 2 raise to 20 minus 1, so that will be the number of states for this shift register. Now, each state now the register basically dictates a new centre frequency within the hopping bandwidth and it is further specified that the minimum step size between the centre frequencies is 200 hertz. So, basically if I have 20 states and if each state gives me a unique centre frequency, and that the gap between centre frequency is 200 hertz and the number of states into the number of such centre frequencies, and therefore the gap between them will give me the total hoping bandwidth.

So, straight away the first part of the problem can be solved as that is the hopping bandwidth basically is 2 raise to 20 minus 1 into the separation between the centre frequency. So, this turns out to be 2 raised to 2.1 into 10 to the power of 8. In the second part of the problem, it is asked us to what is the chip rate. So, basically this is a pretty straight forward. The clock rate of the chip is already specified equal to 2 kilohertz. So, the chip rate is nothing but the clock rate which is the hop rate also, so that is equal to 2,000 chips per second.

In the third question, it is asked us to how many chips are there in each data symbol. So, this is basically nothing but obtained by first finding out how many symbols are there in each second. So, in order to calculate that we make use of the last part of the data provided in the problem that is we have a 8 array FSK system and the data rate is 1.2 kbps. So, the data rate divided by the number of symbols, so for 8 array FSK system, we have 3-bits per symbol that gives you the symbols per second straight away

And then we find out we already know that the number of chips per second is 2,000. So, the number of chips per second divided the number of symbols per second in this case will give you the number of chips per symbol, so that is nothing but a 5. Finally, the processing gain in dB is asked. So, we already know what is hopping bandwidth which is 2.1 into 10 to the power of 8. So, this divided by the raw data rate which was 1.2 kbps gives you the processing gain. This is basically the definition of processing gain for FHSS systems regions; we may be converted to dB's in order to obtain the final result.

(Refer Slide Time: 15:48)



In a problem number four, this is an interesting problem. We have a terminal which has to communicate with a satellite. So, the distance between the two is denoted hereby h and we further have a jammer that is trying to disrupt this communication. So, what we do is that we basically are having a system which is likely to be affected due to the operation of the jammer. So, what we first rather what is asked over here is to compute what is called the radius of vulnerability. So, this is defined as the radius outside which the communicator is unconditionally safe from the jammer. It is to be noted that it is a ground-based jammer.

So we first take a look at the data which is provided to us. So, we are given the frequency-hopping rate which is the 10,000 hops per second. And this is of course, specifically in order to avoid the threat of what is called repeat back jamming so, every time the signal is sent as long as the jammer is outside the radius of vulnerability, it will be unable to jam the communication system. So, in order to find out that particular radius, what is done is we first calculate the time which is required to complete hop from the terminal to the satellite.

So, there are two elements which comprises of this time one is the duration of the hop, because every hop will occupy certain time duration, and that is to be calculated basically based on the data that is provided to us. So, we have this equal to 10 to the power of 1 divided by 10 to the power of 4 microseconds that is because we have already been specified the hopping rate. So, we merely take the ratio of that in rather the reciprocal of that in order to find the time. We further see that there will be some propagation time involved for the signal or the entire hop in order to propagate from the terminal to the satellite.

For the addition of these two times basically gives you the total time that is required for the completed hop. So, the T part is due to this completion of the hop which is required and h by c is nothing but the propagation time c is of course, the velocity of light. So, that is this jammer r. So, what it needs to do first is to try and get this information. So, that requires a time of r by c, where r is the distance between the terminal and the jammer. And then the propagation time between the jammer and the satellite receiver where the jamming will actually happen, so that propagation time is nothing but d by c, where d is the distance between the jammer and the satellite. So, this communicator will be unconditionally safe from the jammer provided that the time required for communication between the terminal and the satellite is lesser than the time required for the jammer to obtain the information from the terminal and then jam the signal at the satellite receiver. So, that is what is formulated in this expression T plus h by c lesser than or equal to r by c plus d by c.

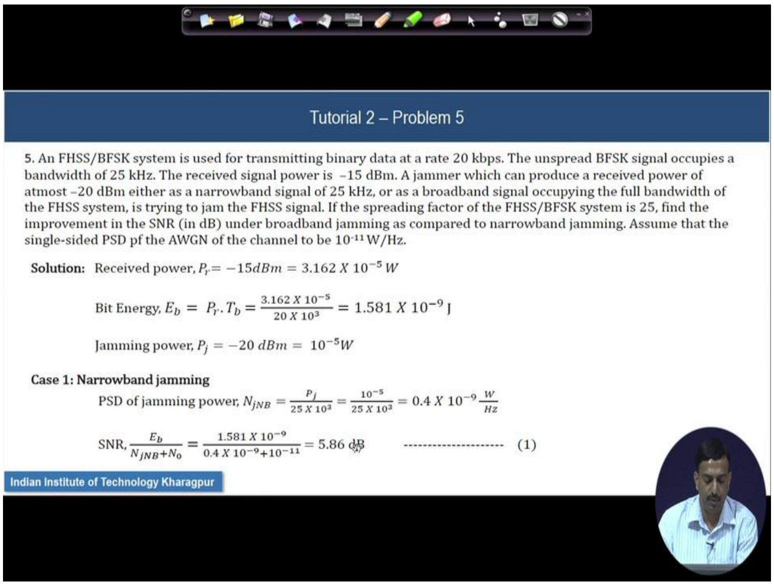
So, now, we need to solve this in order to find this r, because we are trying to find the radius of vulnerability that is this r the distance between the terminal and the jammer. So, we are merely just simplify this expression, we see that r basically turns out to be equal to so with h plus c in to t. We take the equal to sign for the worst-case condition; and we see that of course, that d is related to h and r as well. Now, the calculation of r requires solution of this equation.

However, we can make use of the condition that r that is a distance between the terminal and the jammer is much less than h. So, in which case we can neglect this r and h cancels out and we get I am sorry. So, what we do is yeah right. So, we have r equal to this. So, r is much lesser than h. So, r is neglected h is cancelled and we have r equal to c into T; c is already a standard value and T is given or rather it is been already calculated as 10 to the power of minus 4. So, what we have is r equal to 30 kilometers in this case.

In order to have a more precise relationship between r and with the rest of the parameters, we also need to include some the fact that apart from obtaining the information from the terminal and then jamming it at a satellite receiver, the jammer also require some time in order to process the information in order to exactly determine the hoping sequence. So, we denote that time by tau. And as you can see in this expression r by c plus d by c, we have an additional processing time at the jammer equal to tau. So, obviously, if this processing time I mean this processing time is going to be some positive number and that is going to be beneficial to us because let say for example, we take tau equal to 10 microseconds and solve the same problem as in part a. What we notice is that the radius of vulnerability reduces to 27 kilometers which is beneficial to us.

So, on part b of the problem of the solution is a more precise solution provided this processing time at the jammer is specified. So, this particular problem highlights the calculation of the radius of vulnerability beyond which the terminal is unconditional is safe from the satellite as for as jamming is concerned.

(Refer Slide Time: 23:36)

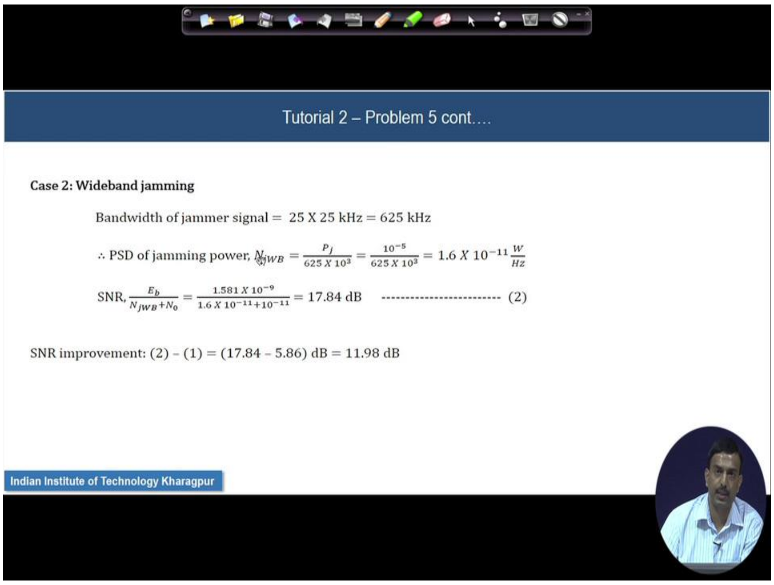


So, finally, we have a problem that deals with narrowband and wideband jamming. So, in this case we are given of FHSS BFSK system. And we have a binary data rate at 20 kbps. The unspread BFSK system has a bandwidth of 25 kilo hertz, the received power is minus 15 dBm. And we have a jammer which has a maximum power of minus 20 dBm. And we have two cases, one is this jammer can operate as a narrow band signal with 25 kilo hertz bandwidth or it can also occupy the entire a spread signal bandwidth, so that would be a kind of a broadband jammer. So, the spreading factor is specified as 25. So, straight away we see that if 25 kilo hertz that is the un spread bandwidth with multiplied by the spreading factor gives us the total spread bandwidth which would be 2600 and 25 kilo hertz.

Further we are specified the PSD of the AWGN channel, so this is 10 to the power of minus 11 watt per hertz. The problem to be solved is we need to find the SNR in dB for the narrow band jamming case as well as the wide band jamming case. And we need to see if there is any improvement in this SNR for the narrowband case compared to the broadband case. So, it is also turn out that the SNR requirement for the wideband jammer is going to be a better than that of the narrowband jammer or that is going to be an improvement. So, we will see that. So, we list out the various parameters to start with we had received power in dBms. So, we converted it to watts and we are also given the bit rate that is 20 kbps. So, based on that, we know the bit duration, which will be 1 by 20 kbps. Based on this data, we find out the bit energy, which will be equal to power into the time which gives us the bit energy basically at a receiver.

The jamming power is specified already has minus 20 dBm. So, we convert it to watt. So, we solve the first case which is a narrowband jammer. So, we have given the jamming power P j which is 10 to the power of minus 5, which is nothing but minus 20 dBm. So, we also know that it has a bandwidth of the jammer has the; is a bandwidth of 25 kilo hertz. So, we can find the power spectral density of the jamming power signal basically. So, the SNR in case one is equal to bit energy divided by the power spectral density of the jammer plus of course, the power spectral density of AWGN has already specified. So, we calculate SNR for narrowband jamming in it turns out to be 5.86.

(Refer Slide Time: 27:06)



For the wide band jammer, as I previously mentioned the spreading factor is equal to 25 the un spread bandwidth is equal to 25 kilo hertz. So, the bandwidth of the jammer signal is equal to spreading factor multiplied by a unspread bandwidth which is 625 kilohertz. So, we recalculate the PSD of this wideband jammer now. So, the difference lies here we have a wider bandwidth and so the PSD it turns out is lesser than the PSD as compared to the narrowband case. And this has a clear cut impact on the new SNR that we calculate the AWGN PSD remains the same, but the PSD if the jammer is now reduced and so the SNR at the receiver has increased.

So, what we notice is the SNR in case of wideband jamming is greater than that of narrowband jamming. So, this is basically because the same jammer power which is 10 to power minus 5 is now spread over a larger bandwidth which gives you a smaller power spectral density and that gives you better immunity to jamming. So, the SNR at the receiver for wideband jamming is much greater than as compared to the narrowband jammer. The improvement is nearly calculated by finding the difference between the two cases, so that turns out to be 11.98 in this case. So, this concludes tutorial two, we solved a set of five problems covering certain aspects of FHSS.

Thank you