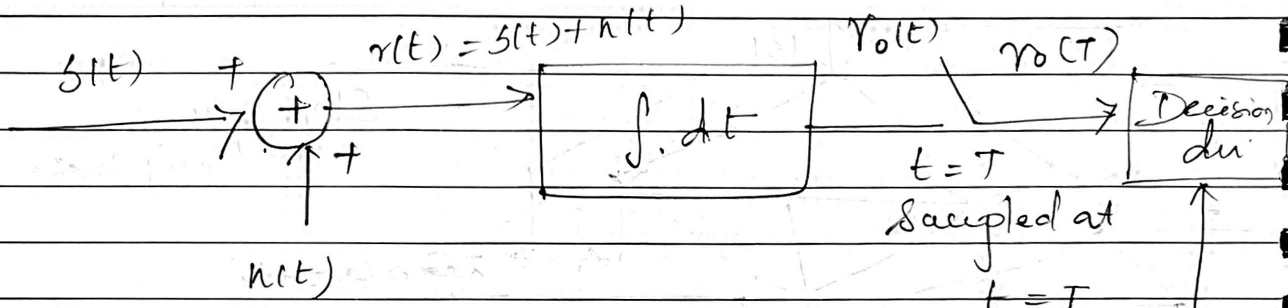
Matched filter is called Integrate & dump circuit.

//



$s(t) = \{+1, \; 0 < t < T$

T is bit duration.

Unit-5

Problem with conventional Wireless Communication

[Sender] [Reciever]

Single freq is used for Tx'ion, so it is Very easy to intercept

When a person is sending on a particular freq. another person has to tune up to the radio for that particular freq, then he/she will start getting the Comm.

eg:

When we want to listen to 93.3 FM, if we tune, We get all the Comm.

Papermark

Created with Scanner Pro

//

Say 1 if $r_0(T) > V_{opt}$

say 0 if $r_0(T) < V_{opt}$.

Interference: When a signal has a constant freq that signal is subj to interfere. This occurs when another signal is transmitted on or very near to the freq of the desired signal.

Interception:

Not well suited to application in which information must be kept confidential between the Tx'ing party & Rx'ing party.

Advantages of Spread Spectrum Communications:

1) Protection against eavesdropping
2) Resistance to intentional Jamming
3) Resistance to fading caused by multipath effects
4) Multiuser facility over a given channel.
5) Ranging facility.

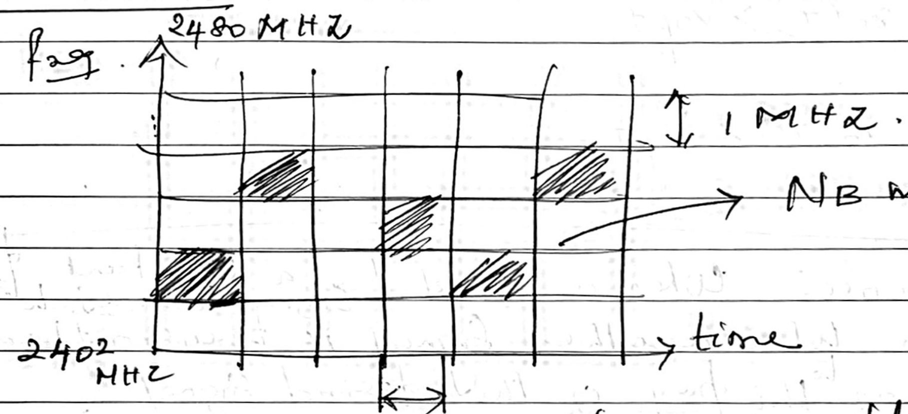
Two types of Spread Spectrum Techniques.

A. Direct Sequence (DS) Spread Spectrum
B. Frequency Hopping (FH) Spread Spectrum

Papermark

Created with Scanner Pro

FH SS technique: 79 channels



625 μs · Hopping time / dwell time

Sender will decide the freq sequence. and switching b/w the freq. that's why its called FHSS.

Here Sender don't use single freq to transmit data. Multiple frequency is used for transmission

Sender send data using freq f_1 for 625 μs & Then change freq

Diff. users can use diff freq patterns.

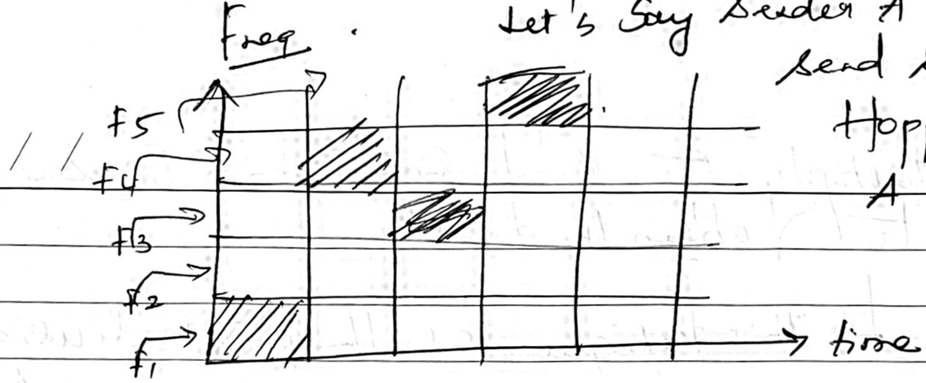
FHSS process:

1. Freq of the carrier is periodically modified following a specified seq. of frequency.
2. This sequence is called hopping sequence (or) spreading code.
3. The Amount of time spent on each frequency is known as dwell time.
4. Following freq seq, message is modulated

Papermark

Created with Scanner Pro

Let's say Sender A wants to send some data.
Hopping seq for A is F1, F4, F3, F5



At the time of Tx'ion, Sender first modulate their signal using F1. Once dwell time is completed then it modulate their signal using freq F4 then F3 then F5.

In order to Rx this signal properly, the receiver has to know this seq. then only it can detect the signal.

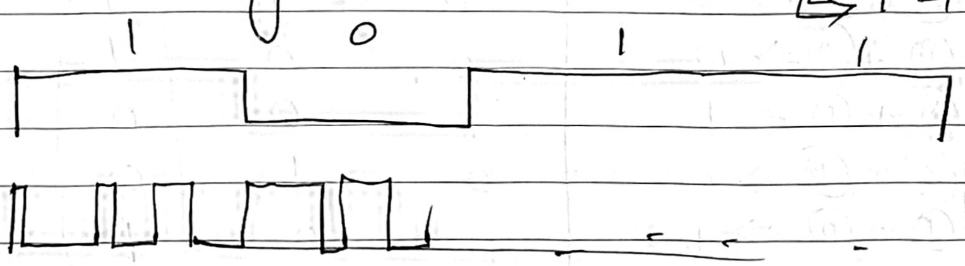
DSSS Technique:

In this technique, every user is assigned a code called spreading code. This code is multiplied with original message and resultant message is then Tx'd.

Receiver uses same spreading code to decode the message to retrieve original message.

For during of every bit, the carrier is modulated using a chipping code.

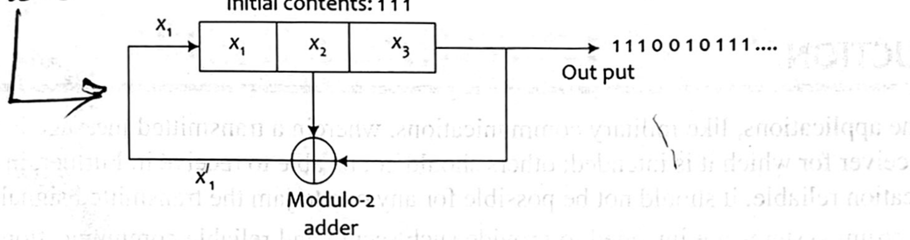
Say for example code is 100101
↳ 1 -1 -1 1 -1 1



So for every bit this code will be multiplied

PN sequences can be generated using shift registers with feedback from one or more stages. A PN sequence generator using 3-stage shift register

i's shown below



Note: The output sequence is obtained by taking x_3 of each pattern of the shift register contents

Fig. 8.1 *A 3-stage shift register, PN sequence generator*

Since there are 3 shift-register stages and since each stage can have either a zero or a one, there can be $2^3 = 8$ distinct sets of contents, including 0 0 0. However, the 0 0 0 state is not permitted because once the shift register contents are 0 0 0, there will be no change whatever may be the number of shifts we give by clocking the circuit. For the PN sequence generator of Fig. 8.1, if we assume that the shift-register contents are initially 1 1 1, with each clocking pulse, the contents will change as shown in the following table.

Table 8.1 Operation of the PN sequence generator of Fig. 8.1

Shifts	$x_1' = x_2 \oplus x_3$	*Shift-register contents* x_1	x_2	x_3
0		1	1	1
1	$1 \oplus 1 = 0$	0	1	1
2	$1 \oplus 1 = 0$	0	0	1
3	$0 \oplus 1 = 1$	1	0	0
4	$0 \oplus 0 = 0$	0	1	0
5	$1 \oplus 0 = 1$	1	0	1
6	$0 \oplus 1 = 1$	1	1	0
7	$1 \oplus 0 = 1$	1	1	1

Note: After the 7th shift, the pattern of the contents will repeat

Thus, this PN sequence generator produces a sequence of length 7 and thereafter the same sequence will be repeated. This is to be expected since we have excluded one pattern, the all-zero pattern from the eight possible patterns. Hence, if N is the length of the sequence and m is the number of shift register stages,

$$N = 2^m - 1 \qquad ...(8.1)$$

Every PN sequence generator with m shift registers need not produce $(2^m - 1)$ length sequences. It depends on the feedback connections and the type of logic circuit used for combining the feedback outputs. (In Fig. 8.1 the logic used was simply Exclusive-OR addition.) PN sequences with $2^m - 1$ length are called a *maximal-length sequences*. An important property of a maximal-length sequence is the number of 1's in it is always one more than the number of 0's. This property is called the 'balance property'.

Since the PN sequence is periodic (with a period of $2^m - 1$ for maximal length sequence), its auto-correlation function defined by

Created with Scanner Pro

From Eq. (8.3b), we find that $c(t)$ is either 1 or –1 at any time.

So, $c^2(t) = +1$ for all t. Hence,

$$z(t) = d(t) + i(t).c(t) \qquad \text{...(8.7)}$$

n Eq. (8.7), we find that when we de-spread the message or data waveform $d(t)$, the interference signal pread over a wide bandwidth by getting multiplied by the PN sequence waveform, $c(t)$. Thus, we (t) consists of a narrowband component $d(t)$ and a wide-band component $i(t).c(t)$. As shown in (t) is integrated over a period of T_b, the data-bit duration. The integrator acts as a lowpass filter the wide-band component $i(t).c(t)$, thus achieving suppression of interfering signals. Further, at ch T_b, the output of the integrator gives a voltage v, whose value depends on whether the $d(t)$ was + 1 during that interval T_b besides of course the period T_b itself. This voltage is given to a comparator which acts as the decision device and says that $d(t)$ was 1 during that T_b if $v > 0$ and that it was a – 1 if $v < 0$. Thus, the original data sequence is recovered suppressing the additive interfering signals picked up by the channel.

The protection to the data given by the spreading sequence will improve as the PN sequence length is longer for a given data rate. The price paid for the security of communication, of course, is larger transmission bandwidth, more complexity of the system, etc.

8.4 BPSK-DS SPREAD-SPECTRUM SYSTEMS AND PROBABILITY OF ERROR

We have discussed in the previous section, how a DS spread-spectrum baseband system can suppress interference signals. In practice, however, the data sequence, after spreading, is carrier modulated, generally using either BPSK, QPSK or MSK. Then it is transmitted over the channel. At the receiving end, the received signal is first subjected to coherent detection using the locally generated carrier signal that is arranged to be in phase and frequency synchronism with the carrier used at the transmitter. The output of the coherent detector is then subjected to de-spreading by multiplying it with a locally generated PN sequence generator that is identical to and in synchronism with the one at the transmitter. After de-spreading, it is integrated over a bit duration T_b to get the observed random variable v, which is used for decision making, as shown in Fig. 8.6.

Probability of Error due to Thermal Noise on the Channel

In Section 8.3, we had shown that a deterministic interfering signal added to the baseband spread-spectrum signal in the course of its passage through the channel will be suppressed by the de-spreading operation and the subsequent integration in the receiver. Thus, the interference signal is not going to influence the decision made by the decision device. In other words, the interfering signal does not affect the probability of error.

From this, one may be tempted to jump to the conclusion that spread-spectrum systems will, in a similar way, suppress the random noise also added by the channel. But it is not correct to conclude that. Random noise added to the SS signal during its passage through the channel, is unaffected by the de-spreading operation in the receiver. The de-spreading signal $c(t)$ is like a random binary wave. So when the noise is multiplied by it, all that happens is that for some randomly occurring periods, the polarity of the noise is changed. Obviously, this does not in any way affect the power spectral density, or the probability density function of the noise. Earlier, we had seen that the message data sequence is unaffected by the spreading and de-spreading. Since

Created with Scanner Pro

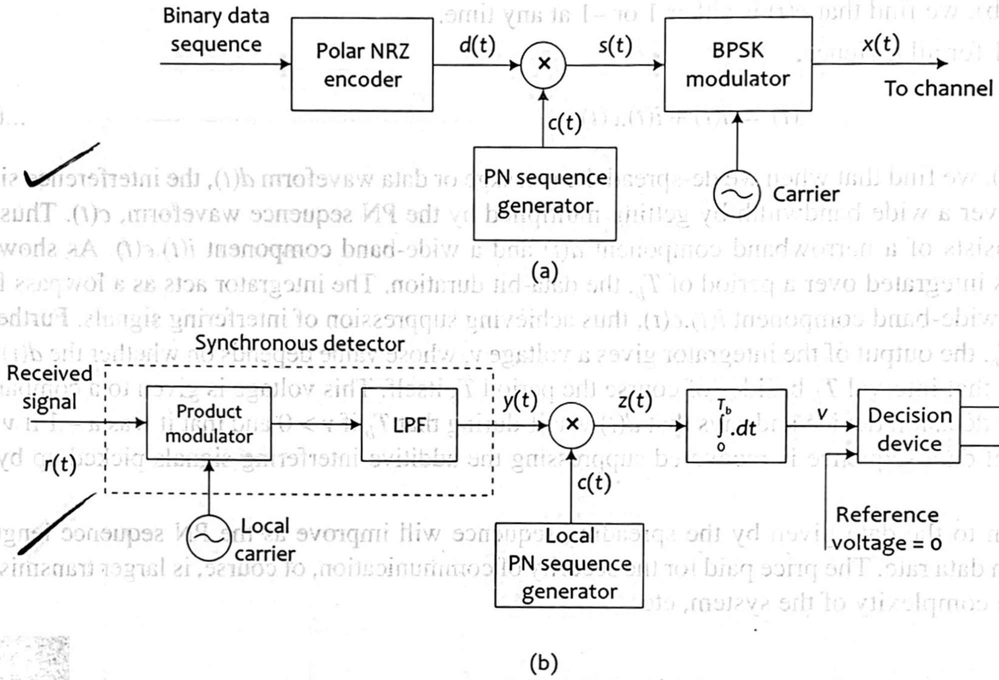


Fig. 8.6 *Direct sequence spread-spectrum system using BPSK: (a) Transmitter (b) Receiver*

the signal as well as the thermal noise added by the channel are unaffected, the probability of error of a DS spread-spectrum system using BPSK modulation is the same as what a normal BPSK system gives. That is,

$$P_e = \frac{1}{2} erfc\sqrt{\frac{E_b}{\eta}} \qquad ...(8.8)$$

8.5 RESISTANCE TO JAMMING

Jamming is resorted to in order to make a communication ineffective. It consists of radiating a large amount of r.f. power in a narrowband around the carrier frequency used for that communication.

We will now briefly analyze and see the effect of jamming on DS spread-spectrum BPSK communication. To simplify the analysis, we shall make the following assumptions:

1. We will assume that the jamming signal is a single-tone signal at the frequency f_c which is the frequency of the carrier used for BPSK modulation at the DS spread spectrum BPSK transmitter.
2. Although in practice, as shown in Fig. 8.6, the spectrum spreading operation at the transmitting end precedes the BPSK modulation, we will, for the sake of this analysis, assume that the modulation (BPSK) is done first and the spectrum spreading is done subsequently. Similarly, at the receiver also, we will reverse the order in which phase demodulation and spectrum de-spreading are done. This is quite justified, because of the linear nature of all these operations.

So, for this analysis, we will use the following model for the DS spread-spectrum BPSK communication system.

Created with Scanner Pro

$$\text{Range of the target} = d = \frac{v}{2}\tau = \left(\frac{1}{2} \times 3 \times 10^5 \, \tau\right) \text{km}$$

The accuracy of measurement is obviously dependent upon T_c. Smaller the value of T_c relative to T, the better is the accuracy.

Example 8.5

A DSSS system used for range measurement is required to give a range resolution of 0.01 km. Find the chip rate that is to be used.

In a DSSS-based range measuring system, the precision of measurement =

$$\pm T_c = \text{chip period.}$$

$\therefore$ if v km/s is the velocity of light, this precision corresponds to a range resolution of vT_c km.

$$\therefore \quad vT_c = 0.01$$

Substituting 3×10^5 km for v and solving for $(1/T_c)$, the chip rate, we get

$$\left(\frac{1}{T_c}\right) = \text{chip rate} = \frac{v}{0.01} = \frac{3 \times 10^5}{0.01} = 3 \times 10^7 \text{ Hz}$$

$$\therefore \quad \text{chip rate} = 30 \text{ MHz}$$

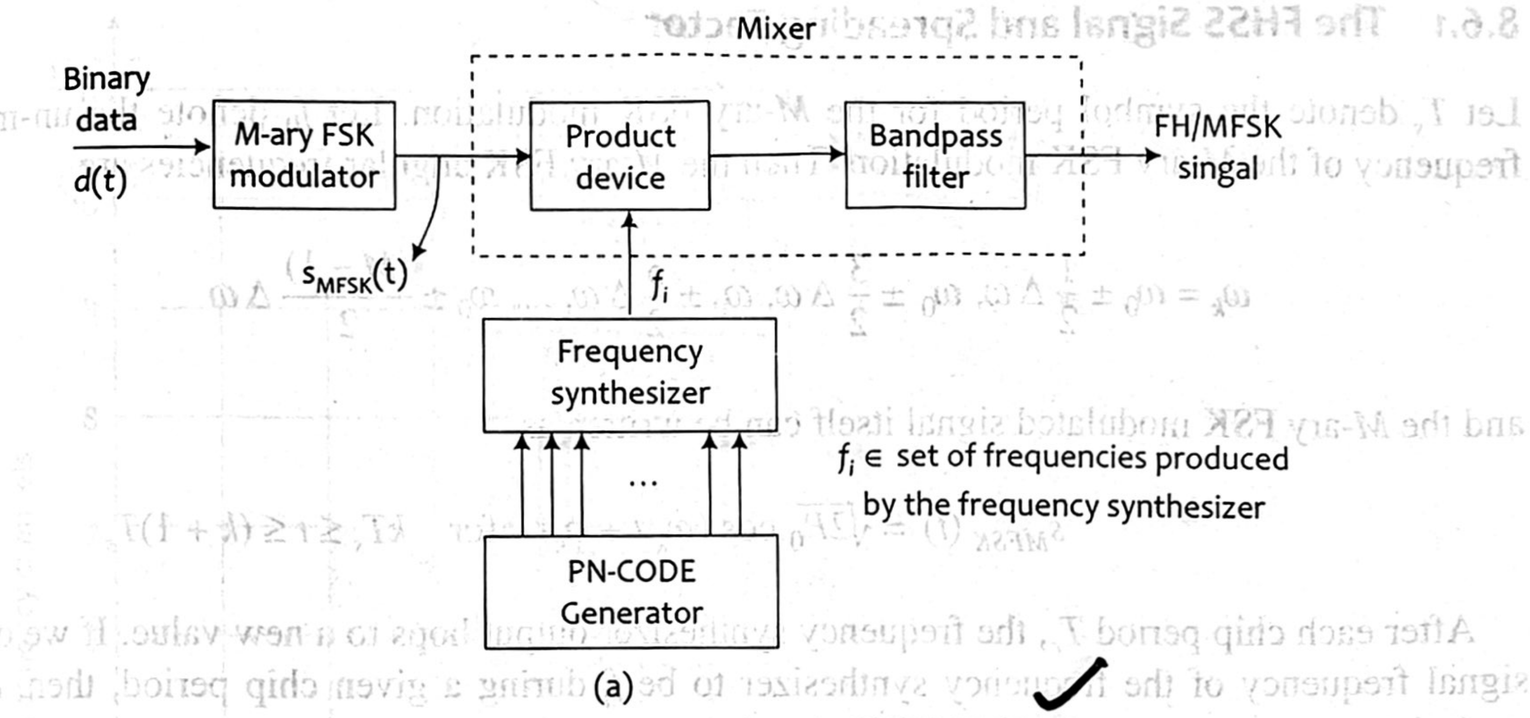
8.6 FREQUENCY-HOPPING SPREAD-SPECTRUM (FHSS) SYSTEMS

We have found, while discussing the resistance to jamming of a DS spread-spectrum system that it depends primarily on the processing gain, G_p. The processing gain is the ratio of the chip frequency f_c to the bit frequency f_b. So, for a given data rate, the resistance to jamming of a DS spread-spectrum system can be improved only by increasing the chip rate relative to the data rate. Beyond a certain limit, practical difficulties in the design and implementation of PN sequence generators make it difficult to achieve very high chip frequencies and this puts a limit on the processing gain and the degree of resistance to jamming that can be achieved using DS spread-spectrum systems.

One way of overcoming the above difficulty is to use frequency-hopping spread spectrum. In this also, just like in DS spread-spectrum systems, the binary digital data modulates a carrier using a traditional modulation scheme like M-ary FSK (for reasons to be discussed later, modulation schemes requiring coherent detection, like the PSK, QPSK, etc., cannot be used). This M-ary FSK modulated signal is then modulated a second time by another carrier frequency, but this carrier frequency changes its value, or rather hops, at regular intervals of T_c, the chip period, from one value to another from among a given set of values, according to a pre-determined, pseudo-random pattern. This carrier frequency hopping is controlled at the transmitter by a pseudo-random code generator, as shown in the block diagram of Fig. 8.9.

As shown in Fig. 8.9(a) binary data $d(t)$ is first used to produce an M-ary FSK modulated signal. This is again modulated by a carrier produced by a frequency synthesizer that is controlled by a PN code generator. This modulation is performed by feeding the M-ary FSK signal as well as the output of the frequency synthesizer to a mixer. The mixer produces the sum frequency and difference frequency. The BPF that follows the mixer selects only the sum frequency signal, which is the FH/MFSK signal.

Created with Scanner Pro



Note: The PN code generator and the frequency synthesizer at the receiver are identical to those at the transmitter

Fig. 8.9 *FHSS/M-ary FSK: (a) Transmitter (b) Receiver*

At the receiving end, the received signal is fed to the mixer to which the output of a frequency synthesizer also given. The frequency of the signal produced by this synthesizer is controlled by a PN code generator hich is identical to, and is in synchronism with, the one at the transmitter. The set of frequencies produced y the frequency synthesizer and their hopping pattern, are also exactly identical to those at the transmitter. he de-spread *M*-ary FSK signal coming out from the BPF is then detected using a *noncoherent M*-ary FSK etector. The reason for using noncoherent detection, in spite of its poorer performance as compared to oherent detector, is the fact that frequency synthesizers cannot maintain phase coherence over successive ops. In fact, that is the reason why FHSS systems do not make use of phase-dependent modulation schemes ke BPSK, *M*-ary PSK, QPSK, etc., which require coherent detection. The output of the *M*-ary FSK oncoherent detector is then fed to the decision device (not shown in figure). Although the noncoherent etector of an FHSS system will have a poorer performance than the coherent detector that we can use in a SSS system, generally, the higher processing gain attainable in FHSS systems more than compensates for e poor performance of the noncoherent detector.

Created with Scanner Pro