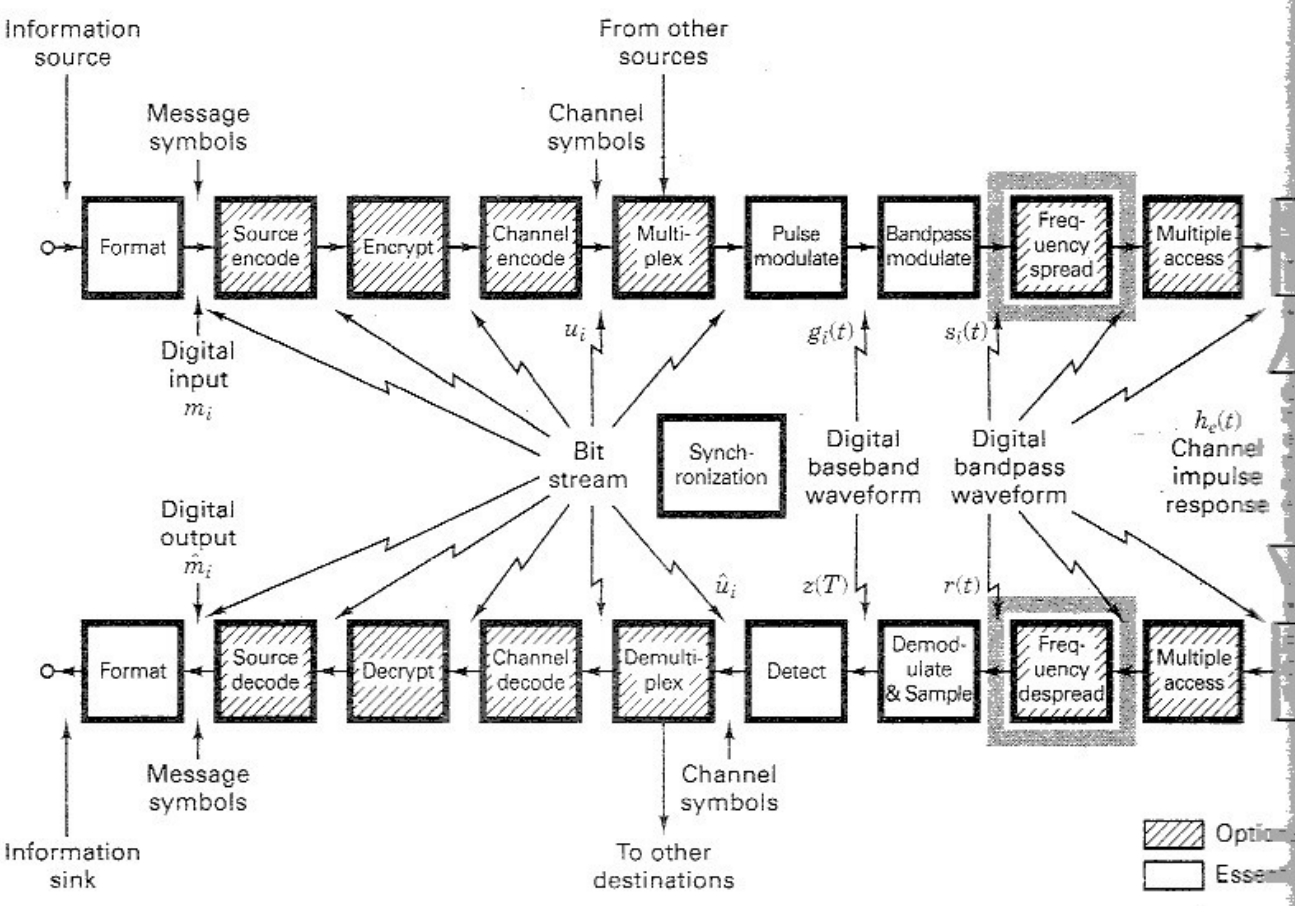
CHAPTER 12

Spread-Spectrum Techniques



12.1 SPREAD-SPECTRUM OVERVIEW

The initial application of spread-spectrum (SS) techniques was in the development of military guidance and communication systems. By the end of World War II, spectrum spreading for jamming resistance was already a familiar concept to radar engineers [1], and during subsequent years, SS investigation was motivated primarily by the desire to achieve highly jam-resistant communication systems. As a result of this research, there emerged an assortment of other applications in such areas as energy density reduction, high-resolution ranging, and multiple access, which will be discussed in later sections. The techniques considered in this chapter are called *spread spectrum* because the transmission bandwidth employed is much greater than the minimum bandwidth required to transmit the information. A system is defined to be a spread-spectrum system if it fulfills the following requirements:

1. The signal occupies a bandwidth much in excess of the minimum bandwidth necessary to send the information.
2. Spreading is accomplished by means of a *spreading signal,* often called a *code signal,* which is independent of the data. The details of some spreading signals are described in later sections.
3. At the receiver, despreading (recovering the original data) is accomplished by the correlation of the received spread signal with a synchronized replica of the spreading signal used to spread the information.

Standard modulation schemes such as frequency modulation and pulse code modulation also spread the spectrum of an information signal, but they do not qualify as spread-spectrum systems since they do not satisfy all the conditions outlined above.

12.1.1 The Beneficial Attributes of Spread-Spectrum Systems

12.1.1.1 Interference Suppression Benefits

White Gaussian noise is a mathematical model that, by definition, has infinite power spread uniformly over all frequencies. Effective communication is possible with this interfering noise of infinite power because only the finite-power noise components that are present within the signal space (in other words, share the *same coordinates* as the signal components) can interfere with the signal. The balance of the noise power may be thought of as noise that is effectively tuned out by the detector (see Section 3.1.3). For a typical narrowband signal, this means that only the noise in the signal bandwidth can degrade performance. Since spread-spectrum (SS) techniques were initially developed as a military application to permit reliable communications in the face of an enemy interferer (jammer), we begin by focusing on the anti-jam (AJ) capabilities of SS. (Commercial applications are treated in Sections 12.7 and 12.8.)

The idea behind a spread-spectrum AJ system is as follows. Consider that many orthogonal signal coordinates or dimensions are available to a communication link and that only a small subset of these signal coordinates are used at any time. We assume that the jammer cannot determine the signal subset that is currently in use. For signals of bandwidth W and duration T, the number of signaling dimensions can be shown [2] to be approximately $2WT$. Given a specific design, the error performance of such a system is only a function of E_b/N_0. Against white Gaussian noise, with *infinite* power, the use of spreading (large $2WT$) offers no performance improvement. However, when the noise stems from a jammer with a *fixed finite* power and with uncertainty as to where in the signal space the signal coordinates are located, the jammer's choices are limited to the following:

1. Jam *all* the signal coordinates of the system, with an *equal* amount of power in each one, with the result that *little* power is available for each coordinate.
2. Jam a *few* signal coordinates with *increased* power in each of the jammed coordinates (or more generally, jam all the coordinates with various amounts of power in each).

Figure 12.1 compares the effect of spectrum spreading in the presence of white noise with spreading in the presence of an intentional jammer. The power spectral density of the signal is denoted $G(f)$ before spreading, and $G_{ss}(f)$ after spreading. For simplicity, the figure treats the frequency dimension only. In Figure 12.1a it can be seen that the single-sided power spectral density of white noise, N_0, is unchanged as a result of expanding the signal bandwidth from W to W_{ss}. The av-

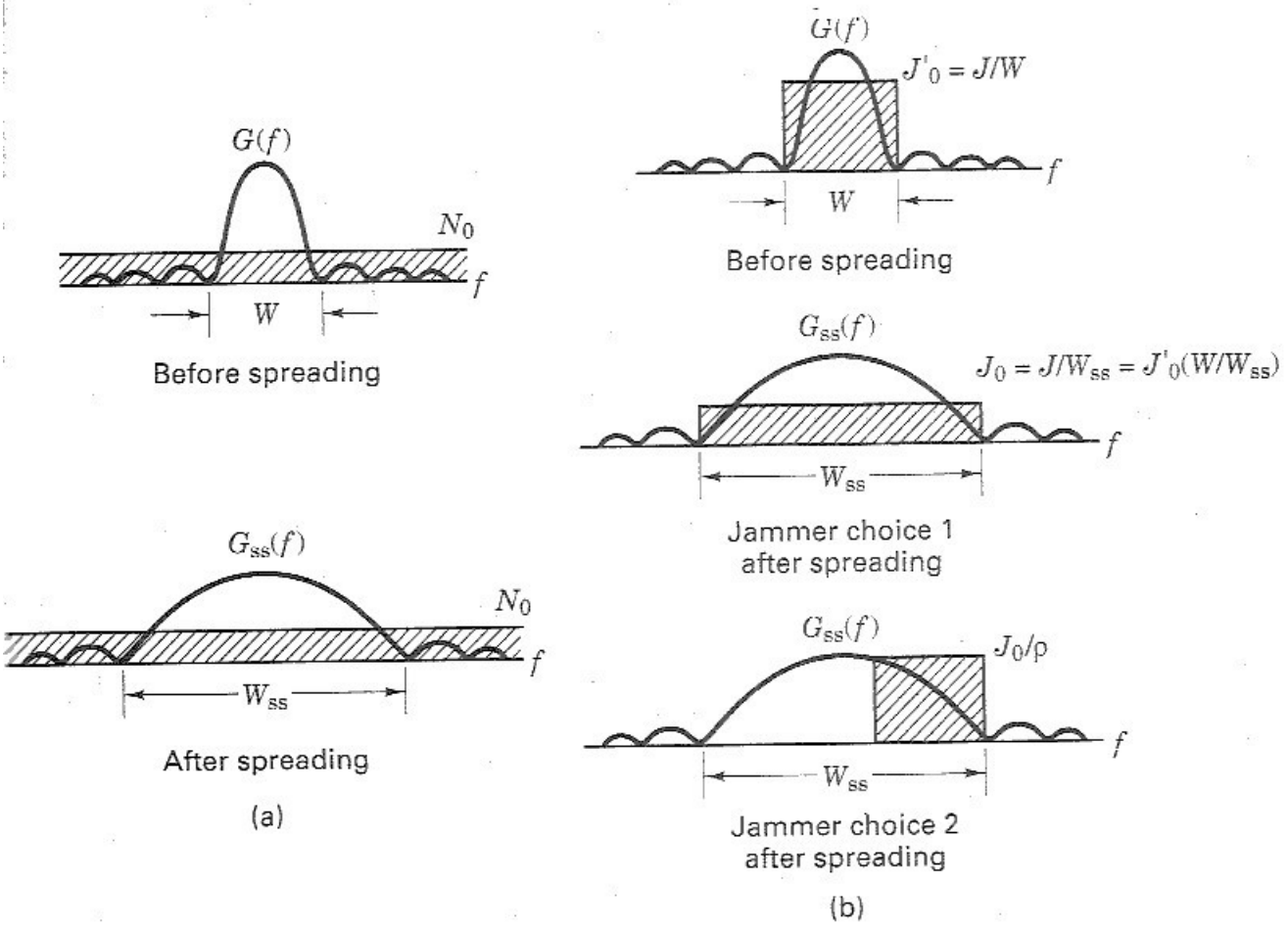


Figure 12.1 Effect of spectrum spreading. (a) Spectrum spreading in the presence of white noise. (b) Spectrum spreading in the presence of an intentional jammer.

erage power of white noise (area under the spectral density curve) is infinite. Hence, the use of spreading offers no performance improvement here. Figure 12.1b (upper diagram) illustrates the case of received (fixed finite) jammer power, J, and power spectral density, $J_0' = J/W$, where W is the unspread bandwidth being jammed. Once the signal bandwidth is spread, the jammer can make one of the two choices listed earlier—choice 1 results in a reduction in jammer noise spectral density, J_0', by a factor (W/W_{ss}) across the spread spectrum. The resulting noise spectral density, $J_0 = J/W_{ss}$, is referred to as the *broadband jammer noise spectral density.* Choice 2 results in a reduction in the number of signal coordinates that the jammer occupies. However, with choice 2 the jammer can increase its noise spectral density from J_0 to J_0/ρ $(0 < \rho \leq 1)$, where ρ is the portion of the spread-spectrum band the jammer elects to jam. If the jammer makes a poor choice in the coordinates to be jammed, the average effect of jamming will be less than if it makes a good choice. The larger the dimensionality of the signal set or the more signal coordinates the communicator can choose from, the greater is the jammer's uncertainty regarding the effectiveness of the jamming technique, and the better will be the protection against jamming. The comparison of unspread- versus spread-spectrum signaling

should be done under the assumption that there is the same amount of total average power in both cases. Since the area under the power spectral density (psd) curves represent total average power, there should be equal area under each of the psd curves for the unspread and the spread examples. Hence, it should be clear that in Figure 12.1, the $G_{ss}(f)$ plots are not to scale in both parts a and b.

Jamming is not always the result of an intentional act. Sometimes, the jamming signal is caused by natural phenomena, and sometimes it is the result of self-interference caused by *multipath,* in which delayed versions of the signal, arriving via alternative paths, interfere with the direct path transmission.

12.1.1.2 Energy Density Reduction

One can imagine situations where it is desired that a communications link be operated without being detected by anyone other than the intended receiver. Systems designed for this special task are known as *low probability of detection* (LPD) or *low probability of intercept* (LPI) communication systems. These systems are designed to make the detection of their signals as difficult as possible by anyone but the intended receiver. The goal of such a system is to use the minimum signal power and the optimum signaling scheme that results in the minimum probability of being detected. Since, in spread-spectrum systems, the signal is spread over many more signaling coordinates than in conventional modulation schemes, the resulting signal power is, on average, spread thinly and uniformly in the spread domain. Therefore, not only can the spread-spectrum signal be made difficult to jam, but additionally, the signal's very existence may be rendered difficult to perceive. To anyone who does not possess a synchronized replica of the spreading signal, the spread-spectrum signal will seem "buried in the noise."

A *radiometer* is a simple power measuring instrument that can be used by an adversary to detect the presence of spread-spectrum signals within some bandwidth W. The radiometer, illustrated in Figure 12.2, consists of a bandpass filter (BPF) with bandwidth W, a squaring circuit to ensure a positive output value (since a measure of *signal energy* is being detected), and an integrating circuit. At time $t = T$, the output of the integrator is compared to a preset threshold. If the output of the integrator is larger than the threshold, a signal is declared present; otherwise, the signal is declared absent. References [3, 4] provide details on the detectability of spread-spectrum signals, using radiometers and other more complicated instruments that make use of the features of the SS signal itself.

Spread-spectrum systems that are designed to exhibit LPI may also exhibit a *low probability of position fix* (LPPF), which means that even if the presence of the signal is perceived, the direction of the transmitter is difficult to pinpoint. Some spread-spectrum systems also exhibit a *low probability of signal exploitation* (LPSE), which means that the identification of the source is difficult to ascertain.

Another, unrelated application of spread-spectrum signaling deals with the fact that in some cases energy density reduction may be required to meet national allocation regulations. Downlink transmissions from satellites must meet international regulations on the spectral density that impinges on the earth. By spreading the downlink energy over a wider bandwidth, the total transmitted power can be

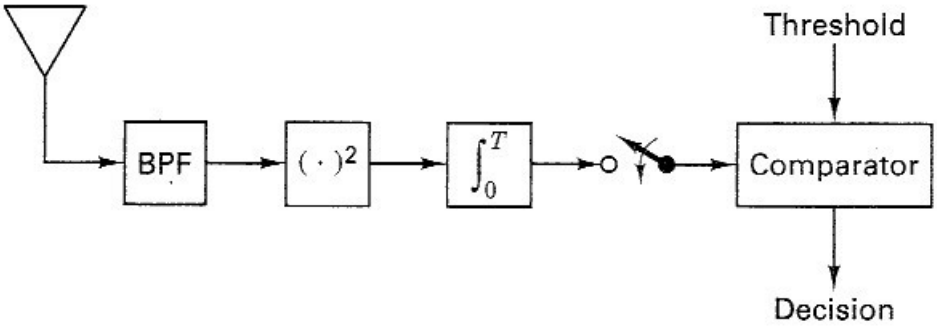


Figure 12.2 Radiometer.

increased and hence performance improved, while the energy density regulations are followed.

12.1.1.3 Fine Time Resolution

Spread-spectrum signals can be used for ranging or determination of position location. Distance can be determined by measuring the time delay of a pulse as it traverses the channel. Uncertainty in the delay measurement is inversely proportional to the bandwidth of the signal pulse. This can be seen by the illustration in Figure 12.3. The uncertainty of the measurement, Δt, is proportional to the rise time of the pulse, which is inversely proportional to the bandwidth of the pulse signal; that is,

$$\Delta t \approx \frac{1}{W} \tag{12.1}$$

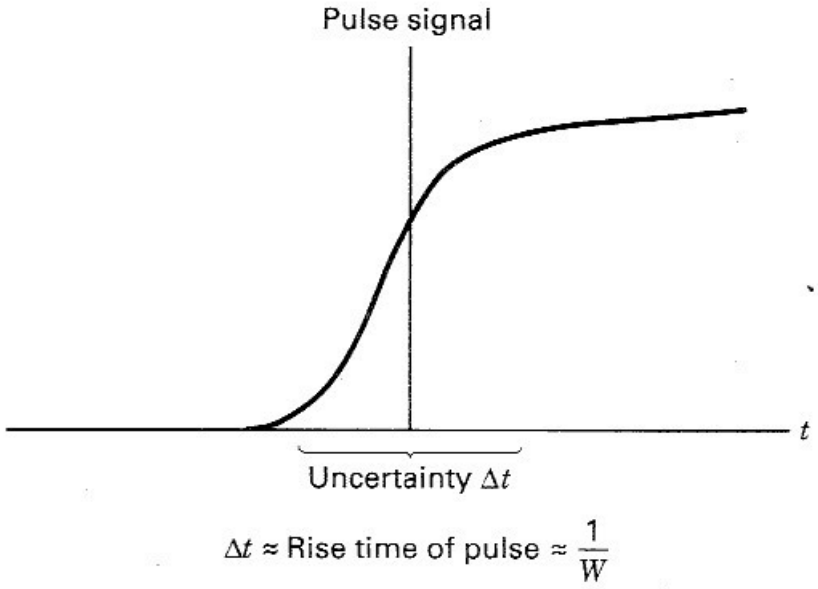


Figure 12.3 Time-delay measurement.

The larger the bandwidth, the more precisely one can measure range. Over a Gaussian channel, a one-shot measurement on a single pulse is not very reliable. The spread-spectrum technique, however, uses a code signal consisting of a long sequence of polarity changes (e.g., a binary PSK-modulated signal) in place of the single pulse. Upon reception, the received sequence is correlated against a local replica and the results of the correlation are used to perform an accurate time-delay or range measurement.

12.1.1.4 Multiple Access

Spread-spectrum methods can be used as a multiple access technique, in order to share a communications resource among numerous users in a coordinated manner. The technique, termed *code-division multiple access* (CDMA), since each simultaneous user employs a unique spread-spectrum signaling code, was discussed briefly in Chapter 11. One of the by-products of this type of multiple access is the ability to provide communication privacy between users with different spreading signals. An unauthorized user (a user not having access to a spreading signal) cannot easily monitor the communications of the authorized users. (A more detailed treatment is presented in a later section.)

12.1.2 A Catalog of Spreading Techniques

Figure 12.4 highlights the popular techniques for spreading the information signal over a large number of signal coordinates or dimensions. For signals of bandwidth W and duration T, the dimensionality of the signaling space is approximately $2WT$. To increase the dimensionality, we can either increase W by spectrum spreading, or increase T by time spreading or time hopping (TH). With spectrum spreading the signal is spread in the frequency domain. With time hopping, a message with data rate R is allocated a longer transmission-time duration than would be used with a conventional modulation scheme. During this longer time the data are sent in bursts according to the dictates of a code. We can say that with time hopping the signal is spread in the time domain. For both cases, frequency spreading and time spreading, a jammer will be uncertain regarding the signaling subset that is currently in use.

In Figure 12.4, the first two items listed under the category of spreading, *direct sequencing* (DS) and *frequency hopping* (FH), are the most commonly used techniques for spectrum spreading. As a jamming-rejection technique, *time hopping* (TH), the third item in the list, is similar to spread spectrum in that the location of the signal coordinates is hidden from potential adversaries. Also, there are hybrid combinations of the spreading techniques, for example, DS/FH, FH/TH, and DS/FH/TH; however, these techniques can be viewed as simple extensions of the material presented here and we will not elaborate on them. In this chapter, we focus only on the two major spread-spectrum techniques: direct sequencing and frequency hopping.

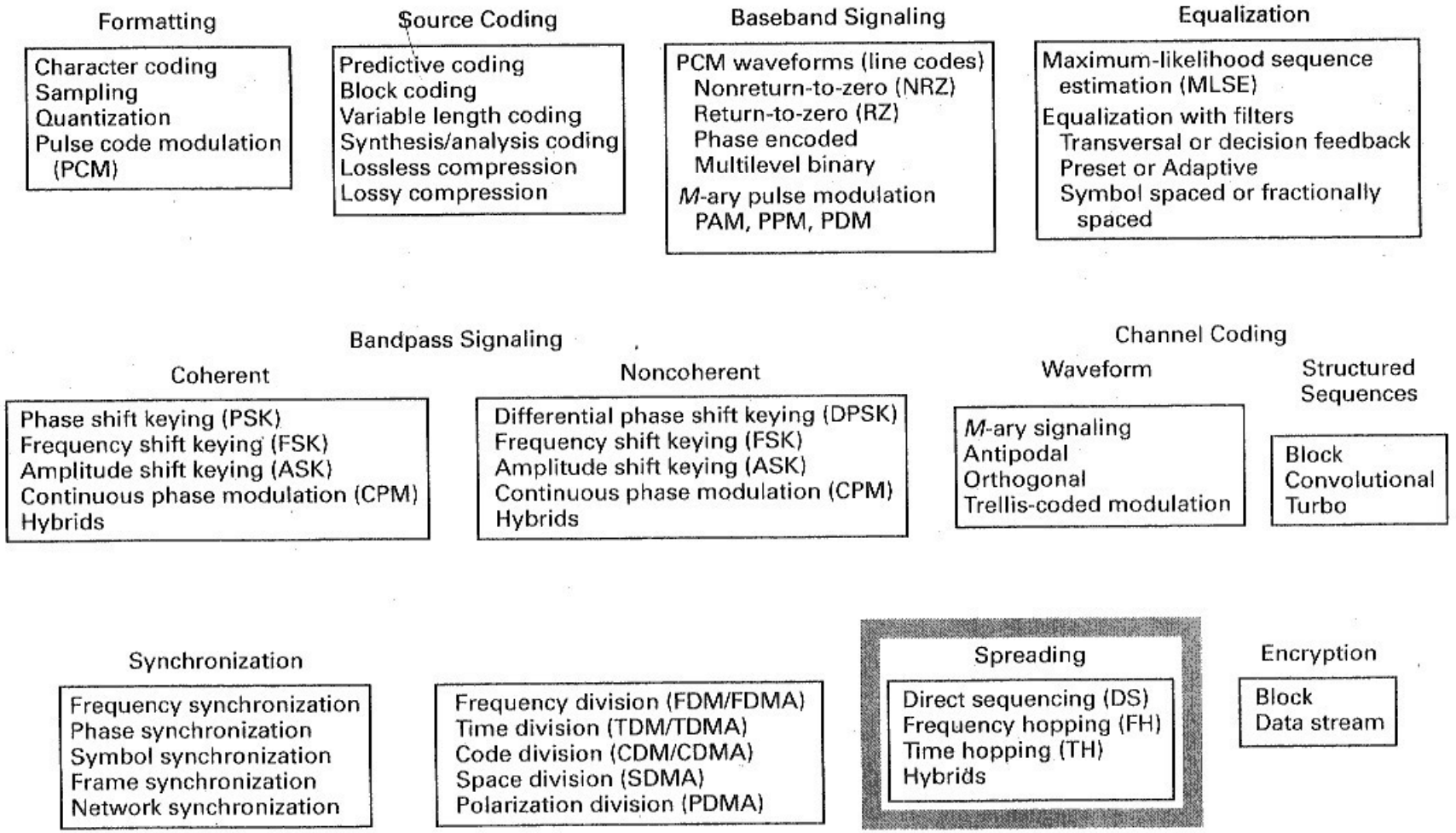


Figure 12.4 Basic digital communication transformations.

12.1.3 Model for Direct-Sequence Spread-Spectrum Interference Rejection

Figure 12.5 illustrates a model for direct-sequence spread-spectrum (DS/SS) interference rejection. At the modulator, the information signal $x(t)$, with a data rate of R bits/s, is multiplied by a spreading code signal $g(t)$, having a code symbol rate, usually called the code *chip rate,* R_{ch} chips/second. Assume that the transmission bandwidths for $x(t)$ and $g(t)$ are R hertz and R_{ch} hertz, respectively. Multiplication in the time domain transforms to convolution in the frequency domain:

$$x(t)g(t) \leftrightarrow X(\omega) * G(\omega) \tag{12.2}$$

Therefore, if the data signal is narrowband compared to the spreading signal, the resulting product signal $x(t)g(t)$ will have approximately the bandwidth of the spreading signal. (See Section A.5.)

At the demodulator, the received signal is ideally multiplied by a synchronized replica of the spreading code signal, $g(t)$, which results in the despreading of the signal. A filter with bandwidth R is used to remove any spurious higher-frequency components. If there is any undesired signal at the receiver, the multiplication by $g(t)$ will spread this undesired signal, in the same way that the multiplication by $g(t)$ at the transmitter spread the desired signal originally. Consider the effect on a jammer that attempts to position a narrowband jamming signal within the information bandwidth. The first operation at the receiver input is multiplication by the spreading signal. Hence, the jamming tone is spread to the bandwidth of the spreading signal.

The essence behind the interference rejection capability of a spread-spectrum system can be summarized as follows:

1. Multiplication by the spreading signal *once* spreads the signal bandwidth.
2. Multiplication by the spreading signal *twice,* followed by filtering, recovers the original signal.

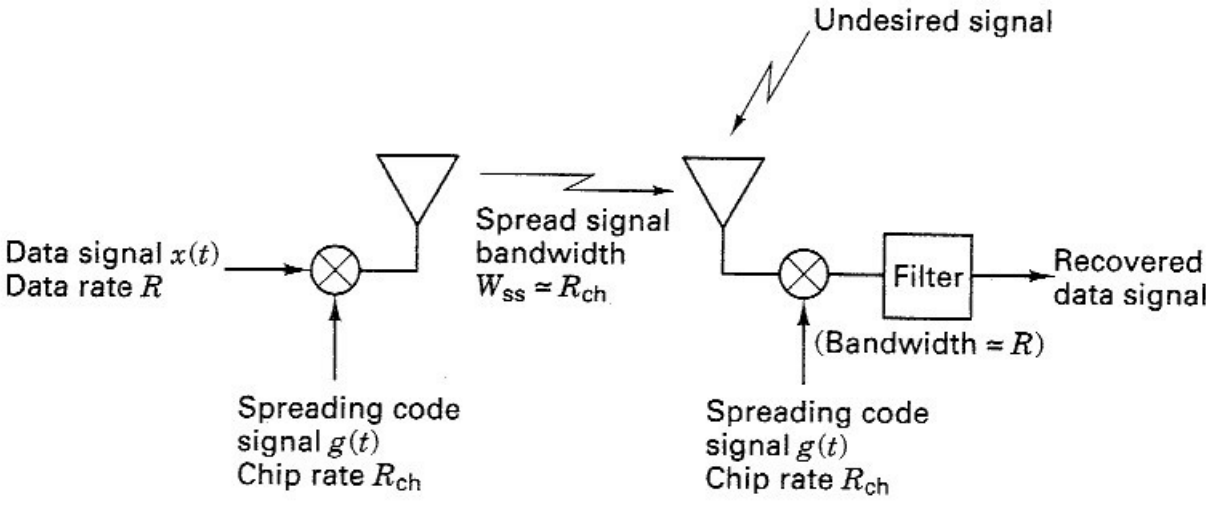


Figure 12.5 Basic spread-spectrum technique.

3. The desired signal gets multiplied *twice,* but the interference signal gets multiplied only *once.*

12.1.4 Historical Background

12.1.4.1 Transmitted Reference versus Stored Reference

During the early years of spread-spectrum investigation, one technique that was considered for operating a transmitter and receiver synchronously with a *truly random* spreading signal, such as wideband noise, was called a *transmitted reference* (TR) system. In a TR system, the transmitter would send two versions of an unpredictable wideband carrier—one modulated by data and the other unmodulated. These two signals were transmitted on separate channels. The receiver used the unmodulated carrier as the reference signal for despreading (correlating) the data-modulated carrier. The principal advantage of a TR system was that there were no significant synchronization problems at the receiver, since the data-modulated signal and the spreading signal used for despreading were transmitted simultaneously. The principal disadvantages of TR systems were that (1) the spreading code was sent in the clear and thus was available to any listener; (2) the system could be easily spoofed by a jammer sending a pair of waveforms acceptable to the receiver; (3) performance degraded at low signal levels since noise was present on both signals; and (4) twice the bandwidth and transmitted power were required because of the need to transmit the reference.

Modern spread-spectrum systems all use a technique called *stored reference* (SR), whereby the spreading code signal is independently generated at both the transmitter and the receiver. The main advantage of an SR system is that a well-designed code signal cannot be predicted by monitoring the transmission. Note that the noiselike code signal in an SR system cannot be truly random as it could in the case of a TR system. Since the same code must be generated independently at two or more sites, the code sequence must be deterministic, even though it should appear random to unauthorized listeners. Such random-appearing deterministic signals are called pseudonoise (PN), or pseudorandom signals; their generation is treated later in greater detail.

12.1.4.2 Noise Wheels

In the late 1940s and early 1950s, Mortimer Rogoff, working at ITT, demonstrated the fundamental operation of spectrum spreading systems with a novel experiment [5]. Using photographic techniques, Rogoff built a "noise wheel" for storing a noiselike signal. He randomly selected 1440 numbers not ending in 00 from the Manhattan telephone directory, and radially plotted the middle two of the last four digits so that the radius at every $\frac{1}{4}^\circ$ represented a new random number. The drawing was transferred to the wheel-shaped film shown in Figure 12.6. When the wheel was rotated past a slit of light, the resulting intensity-modulated light beam provided a stored noiselike spreading signal to be sensed by a photocell.

Rogoff mounted two such identical wheels on a single axis driven by a 900-rpm synchronous motor. One wheel's noiselike spreading signal was modulated

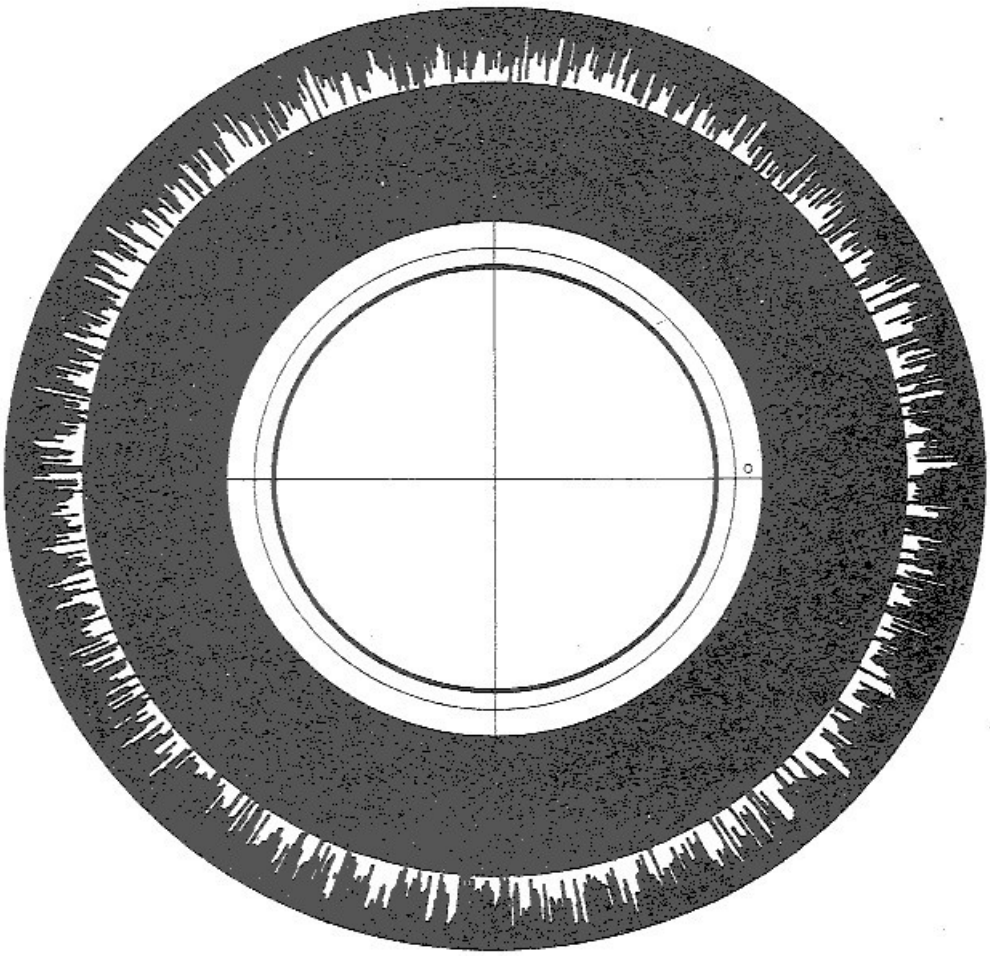


Figure 12.6 Rogoff's noise wheel. [Reprinted from Section I (Communications) of "Application of Statistical Methods to Secrecy Communication Systems," Proposal 946, Fed. Telecomm. Lab., August 28, 1950, Fig. 6, courtesy of ITT.]

with data (and interference) to provide one input to the receiving correlator, while the other wheel's unmodulated spreading signal provided the other input to the correlator. These baseband experiments, performed with the data rates of 1 bit/s, demonstrated the feasibility of conveying information hidden in noiselike signals [4].

12.2 PSEUDONOISE SEQUENCES

The spread-spectrum approach called *transmitted reference* (TR) can utilize a *truly* random code signal for spreading and despreading, since the code signal and the data-modulated code signal are simultaneously transmitted over different regions of the spectrum. The *stored reference* (SR) approach *cannot* use a truly random code signal since the code needs to be stored or generated at the receiver. For the SR system a *pseudonoise* or *pseudorandom* code signal must be used.

How does a pseudorandom signal differ from a random one? A random signal *cannot* be predicted; its future variations can only be described in a statistical sense. However, a pseudorandom signal is not random at all; it is a deterministic, periodic signal that is known to both the transmitter and receiver. Why the name "pseudonoise" or "pseudorandom"? Even though the signal is deterministic, it appears to have the statistical properties of sampled white noise. It appears, to an unauthorized listener, to be a truly random signal.

12.2.1 Randomness Properties

What are these randomness properties that make a pseudorandom signal appear truly random? There are three basic properties that can be applied to any periodic binary sequence as a test for the appearance of randomness. The properties, called *balance, run,* and *correlation,* are described for binary signals as follows:

1. *Balance property.* Good balance requires that in each period of the sequence, the number of binary ones differs from the number of binary zeros by at most one digit.
2. *Run property.* A *run* is defined as a sequence of a single type of binary digit(s). The appearance of the alternate digit in a sequence starts a new run. The length of the run is the number of digits in the run. Among the runs of ones and zeros in each period, it is desirable that about one-half the runs of each type are of length 1, about one-fourth are of length 2, one-eighth are of length 3, and so on.
3. *Correlation property.* If a period of the sequence is compared term by term with any cyclic shift of itself, it is best if the number of agreements differs from the number of disagreements by not more than one count.

In the next section, a PN sequence is generated to test these properties.

12.2.2 Shift Register Sequences

Consider the linear feedback shift register illustrated in Figure 12.7. It is made up of a four-stage register for storage and shifting, a modulo-2 adder, and a feedback path from the adder to the input of the register (modulo-2 addition has been defined in Section 2.9.3). The shift register operation is controlled by a sequence of clock pulses (not shown). At each clock pulse the contents of each state in the register is shifted one stage to the right. Also, at each clock pulse the contents of stages X_3 and X_4 are modulo-2 added (a linear operation), and the result is fed back to stage X_1. The shift register sequence is defined to be the output of the last stage—stage X_4 in this example.

Assume that stage X_1 is initially filled with a one and the remaining stages are filled with zeros, that is, the initial state of the register is 1 0 0 0. From Figure 12.7 we can see that the succession of register states will be as follows:

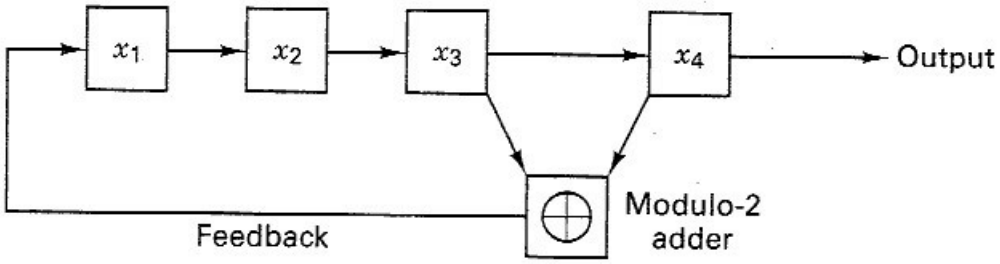


Figure 12.7 Linear feedback shift register example.

1000 0100 0010 1001 1100 0110 1011 0101
1010 1101 1110 1111 0111 0011 0001 1000

Since the last state, 1 0 0 0, corresponds to the initial state, we see that the register repeats the foregoing sequence after 15 clock pulses. The output sequence is obtained by noting the contents of stage X_4 at each clock pulse. The output sequence is seen to be

0 0 0 1 0 0 1 1 0 1 0 1 1 1 1

where the leftmost bit is the earliest bit. Let us test the sequence above for the randomness properties outlined in the preceding section. First, the balance property; there are seven zeros and eight ones in the sequence—therefore, the sequence meets the balance condition. Next, the run property; consider the zero runs—there are four of them. One-half are of length 1, and one-fourth are of length 2. The same is true for the one runs. The sequence is too short to go further, but we can see that the run condition is met. The correlation property is treated in Section 12.2.3.

The shift register generator produces sequences that depend on the number of stages, the feedback tap connections, and initial conditions. The output sequences can be classified as either *maximal length* or *nonmaximal length.* Maximal length sequences have the property that for an n-stage linear feedback shift register the sequence repetition period in clock pulses p is

$$p = 2^n - 1 \tag{12.3}$$

Thus it can be seen that the sequence generated by the shift register generator of Figure 12.7 is an example of a maximal length sequence. If the sequence length is less than $(2^n - 1)$, the sequence is classified as a nonmaximal length sequence.

12.2.3 PN Autocorrelation Function

The autocorrelation function $R_x(\tau)$ of a periodic waveform $x(t)$, with period T_0, was given in Equation (1.23) and is shown below in normalized form.

$$R_x(\tau) = \frac{1}{K}\left(\frac{1}{T_0}\right)\int_{-T_0/2}^{T_0/2} x(t)x(t+\tau)dt \qquad \text{for } -\infty < \tau < \infty \tag{12.4}$$

where

$$K = \frac{1}{T_0} \int_{-T_0/2}^{T_0/2} x^2(t)\, dt \tag{12.5}$$

When $x(t)$ is a periodic pulse waveform representing a PN code, we refer to each fundamental pulse as a *PN code symbol* or a *chip*. For such a PN waveform of unit chip duration and period p chips, the normalized autocorrelation function may be expressed as

$$R_x(\tau) = \frac{1}{p} \cdot \begin{pmatrix} \text{number of agreements less number of disagreements} \\ \text{in a comparison of one full period of the sequence} \\ \text{with a } \tau \text{ position cyclic shift of the sequence} \end{pmatrix} \tag{12.6}$$

The normalized autocorrelation function for a maximal length sequence, $R_x(\tau)$, is shown plotted in Figure 12.8. It is clear that for $\tau = 0$, that is, when $x(t)$ and its replica are perfectly matched, $R(\tau) = 1$. However, for any cyclic shift between $x(t)$ and $x(t + \tau)$ with $(1 \leq \tau < p)$, the autocorrelation function is equal to $-1/p$ (for large p, the sequences are virtually decorrelated for a shift of a *single chip*).

It is now easy to test the output PN sequence of the shift register in Figure 12.7 for the third randomness property—correlation. The output sequence, as well as the same sequence with a single end-around shift, is as follows:

0	0	0	1	0	0	1	1	0	1	0	1	1	1	1
1	0	0	0	1	0	0	1	1	0	1	0	1	1	1
d.	*a*	*a*	*d*	*d*	*a*	*d*	*a*	*d*	*d*	*d*	*d*	*a*	*a*	*a*

The digits that agree are labeled *a* and those that disagree are labeled *d*. Following Equation (12.6), the value of the autocorrelation function for this single one-chip shift is seen to be

$$R(\tau = 1) = \tfrac{1}{15}(7 - 8) = -\tfrac{1}{15}$$

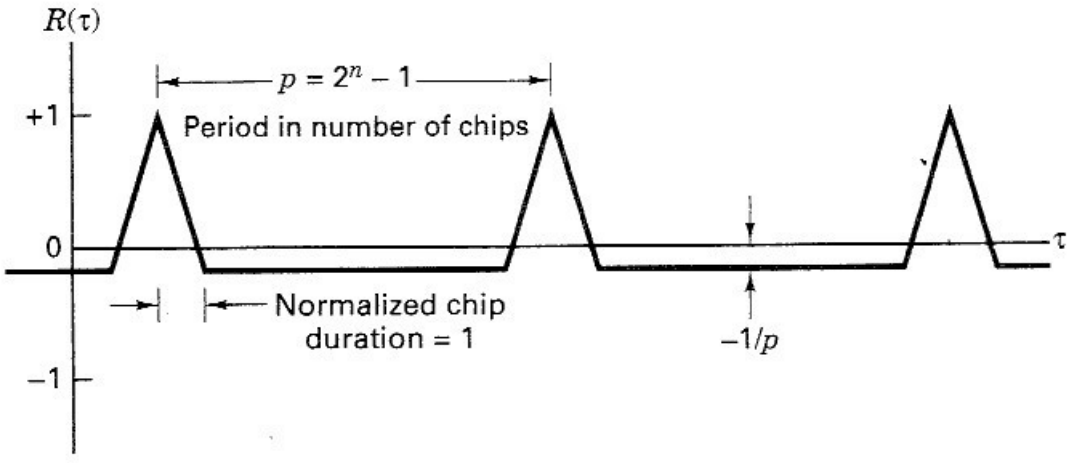


Figure 12.8 PN autocorrelation function.

Any cyclic shift yielding a mismatch from perfect synchronization results in the same autocorrelation value, $-1/p$. Hence the sequence meets the third randomness property.

12.3 DIRECT-SEQUENCE SPREAD-SPECTRUM SYSTEMS

The block diagram in Figure 12.9a depicts a *direct-sequence* (DS) modulator. "Direct sequence" is the name given to the spectrum spreading technique whereby a carrier wave is first modulated with a data signal $x(t)$, then the data-modulated signal is again modulated with a high-speed (wideband) spreading signal $g(t)$. Consider a constant-envelope data-modulated carrier having power P, radian frequency ω_0, and data phase modulation $\theta_x(t)$, given by

$$s_x(t) = \sqrt{2P}\cos\left[\omega_0 t + \theta_x(t)\right] \tag{12.7}$$

Upon further constant-envelope modulation by the spreading signal, $g(t)$, the transmitted waveform can be expressed as

$$s(t) = \sqrt{2P}\cos\left[\omega_0(t) + \theta_x(t) + \theta_g(t)\right] \tag{12.8}$$

where the phase of the carrier is now seen to have two components: $\theta_x(t)$ due to the data and $\theta_g(t)$ due to the spreading sequence.

In Chapter 4, it was shown that ideal suppressed carrier binary phase shift keying (BPSK) modulation results in instantaneous changes of π radians to the phase of the carrier, according to the dictates of the data. We can equivalently express Equation (12.7) as the multiplication of the carrier wave by $x(t)$, an antipodal pulse stream with pulse values of + 1 or −1:

$$s_x(t) = \sqrt{2P}\,x(t)\cos\omega_0 t \tag{12.9}$$

If, like the data, the spreading sequence modulation is also BPSK, and $g(t)$ is an antipodal pulse stream with pulse values of +1 or −1, Equation (12.8) can be written as

$$s(t) = \sqrt{2P}\,x(t)g(t)\cos\omega_0 t \tag{12.10}$$

A modulator based on Equation (12.10) is illustrated in Figure 12.9b. The data pulse stream and the spreading pulse stream are first multiplied, and then the composite $x(t)$ modulates the carrier. If the assignment of pulse value to binary value is

Pulse value	Binary value
1	0
−1	1

then the initial step in the DS/BPSK modulation can be accomplished by the modulo-2 addition of the binary data sequence with the binary spreading sequence.

Demodulation of the DS/BPSK signal is accomplished by correlating or remodulating the received signal with a synchronized replica of the spreading signal

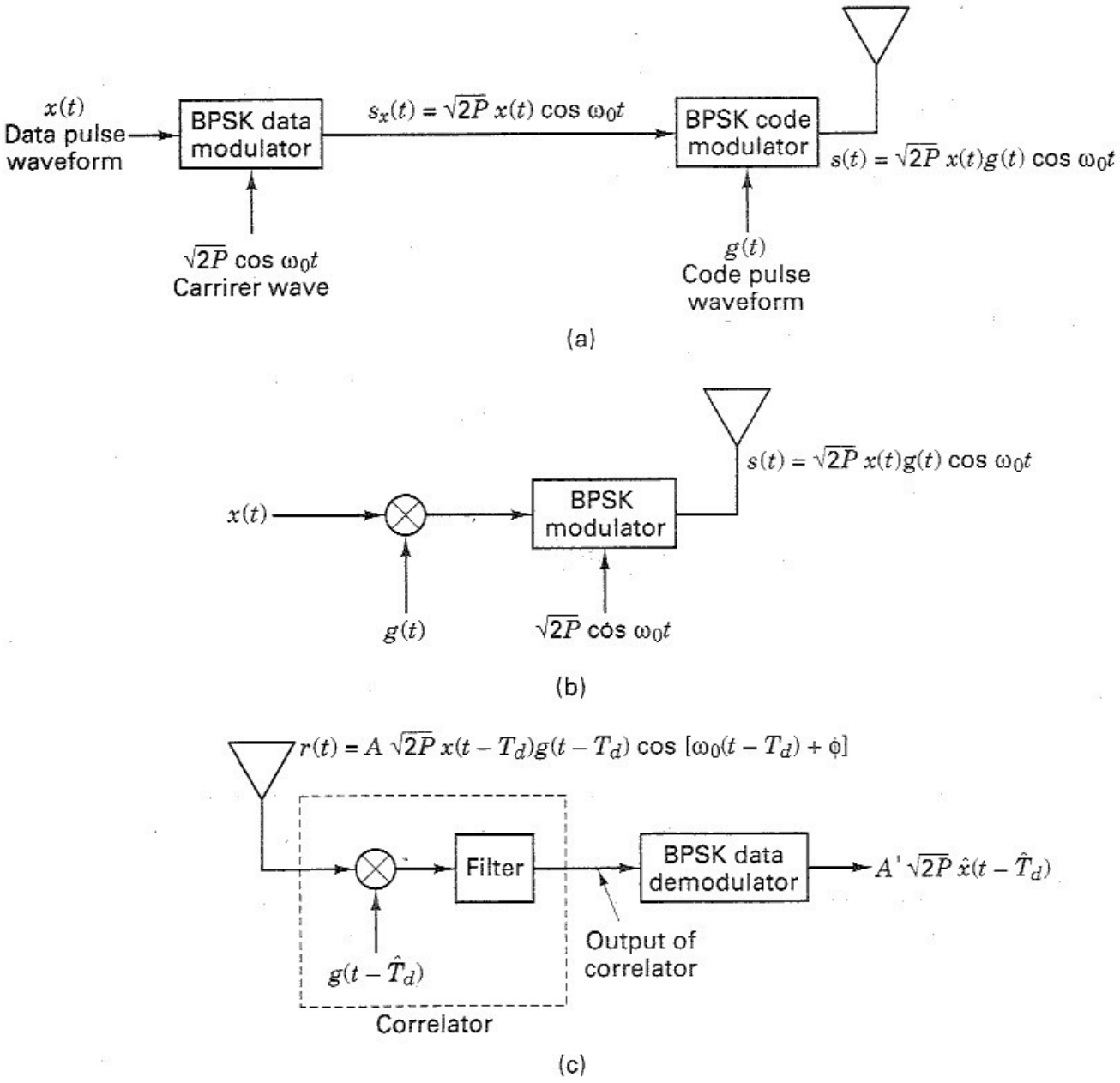


Figure 12.9 Direct-sequence spread-spectrum system. (a) BPSK direct-sequence transmitter. (b) Simplified BPSK direct-sequence transmitter. (c) BPSK direct-sequence receiver.

$g(t - \hat{T}_d)$ as seen in Figure 12.9c, where $\hat{T}_d$ is the receiver's estimate of the propagation delay T_d from the transmitter to the receiver. In the absence of noise and interference, the output signal from the correlator can be written as

$$A\sqrt{2P}\, x(t - T_d)g(t - T_d)g(t - \hat{T}_d) \cos [\omega_0(t - T_d) + \phi] \qquad (12.11)$$

where the constant A is a system gain parameter and ϕ is a random phase angle in the range $(0, 2\pi)$. Since $g(t) = \pm 1$, the product $g(t - T_d)g(t - \hat{T}_d)$ will be unity if $\hat{T}_d = T_d$, that is, if the code signal at the receiver is exactly synchronized with

the code signal at the transmitter. When it is synchronized, the output of the receiver correlator is the despread data-modulated signal (except for a random phase ϕ and delay T_d). The despreading correlator is then followed by a conventional demodulator for recovering the data.

12.3.1 Example of Direct Sequencing

Figure 12.10 is an example of DS/BPSK modulation and demodulation following the block diagrams of Figure 12.9b and c. In Figure 12.10a are shown the binary data sequence (1, 0) and its bipolar pulse waveform equivalent $x(t)$, where the binary to pulse value assignments are the same as those described in the preceding section. Examples of a binary spreading sequence and its bipolar pulse waveform equivalent $g(t)$ are shown in Figure 12.10b. The modulo-2 addition of the data sequence and the code sequence, and the equivalent waveform of the product $x(t)g(t)$, is shown in Figure 12.10c.

For the BPSK modulation described by Equations (12.8) and (12.10), it is shown in Figure 12.10d that the phase of the carrier, $\theta_x(t) + \theta_g(t)$, equals π when the

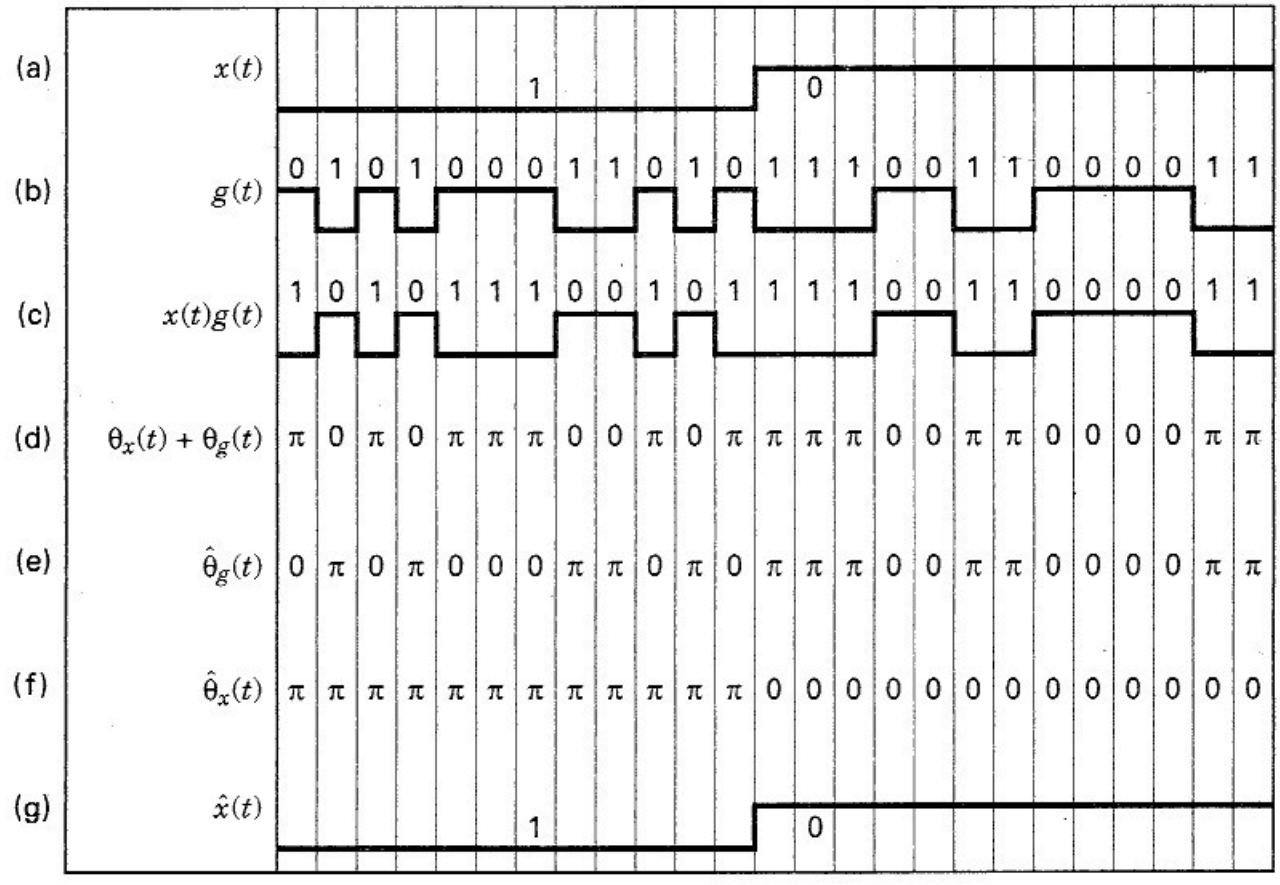


Figure 12.10 Spread-spectrum example using direct sequencing. (a) Binary data waveform to be transmitted. (b) Code sequence. (c) Transmitted sequence. (d) Phase of transmitted carrier. (e) Phase shift produced by receiver code. (f) Phase of received carrier after phase shifted (despread) by receiver code. (g) Demodulated data waveform.

value of the product waveform $x(t)g(t)$ equals –1 (or the modulo-2 sum of data and code is binary 1). Similarly, the phase of the carrier is zero when the value of $x(t)g(t)$ equals +1 (or the modulo-2 sum of data and code is binary 0). One can appreciate the *signal hiding* property of spread-spectrum signals by comparing the code waveform in Figure 12.10b with the composite waveform in Figure 12.10c. The latter has the signal $x(t)$ "hidden" within it. Just as your eyes have difficulty finding the slowly moving data signal in the rapidly moving code signal, it is similarly difficult for a receiver to recover a slowly moving signal from a rapidly moving code without having an exact replica of the code.

As shown in Figure 12.9c, DS/BPSK demodulation is a two-step process. The first step, despreading, is accomplished by correlating the received signal with a synchronized replica of the code. The second step, data demodulation, is accomplished with a conventional demodulator. In the example of Figure 12.10 we see the code replica $\hat{\theta}_g(t)$, in Figure 12.10e, as the phase shift (either 0 or π) that is produced at the receiver by the despreading code. Figure 12.10f illustrates the resulting estimate of the carrier phase $\hat{\theta}_x(t)$, after despreading or after $\hat{\theta}_g(t)$ has been added to $\theta_x(t) + \theta_g(t)$. At this point one can recognize the original data pattern in the phase terms of the carrier wave. The final step, shown in Figure 12.10g, is to recover an estimate of the data waveform, $\hat{x}(t)$, by the use of a BPSK demodulator.

12.3.2 Processing Gain and Performance

A fundamental issue in spread-spectrum systems is *how much* protection spreading can provide against interfering signals with finite power. Spread-spectrum techniques distribute a relatively low-dimensional signal in a large-dimensional signal space. The signal is "hidden" within the signal space, since we assume that a jammer does not know which signal coordinates are being transmitted at any time. The only recourse for the jammer, intent upon communication disruption, is to jam the entire space with its fixed total power, thus inducing a limited amount of interference in each signal coordinate, or to jam a portion of the signal space with its total power, thus leaving the remainder of the signal space free of interference.

Consider a set of D orthogonal signals, $s_i(t)$, $1 \le i \le D$, in an N-dimensional space, where in general, $D << N$. Following the development in Section 3.1.3, we can write.

$$s_i(t) = \sum_{j=1}^{N} a_{ij}\psi_j(t) \qquad \begin{matrix} i = 1, 2, \ldots, D; \\ D \ll N \end{matrix} \qquad 0 \le t \le T \tag{12.12}$$

where

$$a_{ij} = \int_0^T s_i(t)\psi_j(t)\, dt \tag{12.13}$$

and

$$\int_0^T \psi_j(t)\psi_k(t)\, dt = \begin{cases} 1 & \text{for } j = k \\ 0 & \text{otherwise} \end{cases} \tag{12.14}$$

The $\{\psi_j(t)\}$ are linearly independent functions that *span* or characterize the N-dimensional orthonormal space and are called *basis* functions of the space. For every information symbol that is transmitted, a set of coefficients $\{a_{ij}\}$ is chosen independently, using a pseudorandom spreading code, in order to hide the D-dimensional signal set in the larger N-dimensional space. The set of random variables $\{a_{ij}\}$ assume the values $\pm a$, each with a probability of $\frac{1}{2}$. The receiver, of course, has access to each set of coefficients chosen in order to perform the necessary correlation despreading. Even if the same ith symbol is sent repeatedly, the set $\{a_{ij}\}$ used to transmit it is newly selected from symbol to symbol. The energy in each signal waveform of the D signal set will be assumed equal, so that we can write the average energy for each signal as

$$E_s = \int_0^T \overline{s_i^2(t)}\, dt = \sum_{j=1}^{N} \overline{a_{ij}^2} \qquad i = 1, 2, \ldots, D \tag{12.15}$$

where the overbar means the expected value over the ensemble of many symbol transmissions. The independent coefficients have zero mean and correlation:

$$\overline{a_{ij}a_{ik}} = \begin{cases} \dfrac{E_s}{N} & \text{for } j = k \\ 0 & \text{otherwise} \end{cases} \tag{12.16}$$

The standard assumption is that the jammer has no a priori knowledge regarding the selection of the signaling coefficients $\{a_{ij}\}$. As far as the jammer is concerned, the coefficients are uniformly distributed over the N basis coordinates. If the jammer chooses to distribute its power uniformly over the total signal space, the jammer waveform $w(t)$ can be written

$$w(t) = \sum_{j=1}^{N} b_j \psi_j(t) \tag{12.17}$$

with total energy

$$E_w = \int_0^T w^2(t)\, dt = \sum_{j=1}^{N} b_j^2 \tag{12.18}$$

A reasonable goal for a jammer would be to devise a strategy for selecting the portions b_j^2, of its fixed total energy E_w so as to minimize the desired signal-to-noise ratio (SNR) at the receiver after demodulation.

At the receiver, the detector output (ignoring receiver noise),

$$r(t) = s_i(t) + w(t) \tag{12.19}$$

is correlated with the set of possible transmitted signals, so that the output of the ith correlator is

$$z_i = \int_0^T r(t) s_i(t)\, dt = \sum_{j=1}^{N} (a_{ij}^2 + b_j a_{ij}) \tag{12.20}$$