Spread-Spectrum Modulation

by

Dr. Amitava Chatterjee
Electrical Measurement and Instrumentation Laboratory,
Electrical Engineering Department,
Jadavpur University, Kolkata, India.

Spread-Spectrum Modulation

Why Spread-Spectrum ??

- **In digital communication issues of major concern are efficient usage of two primary communication resources i.e. bandwidth and power.**

- **However, there may be situations, where other design objectives will be more important than these two factors.**

- **For example, the system may be required to provide a form of secure communication in a hostile environment such that the transmitted signal is not easily detected or recognized by unwanted listeners.**

- **Spread-spectrum modulation is such a technique which is used to satisfy this requirement.**

Spread-Spectrum Modulation

Features

- **The primary advantage of a spread-spectrum communication system is its ability to reject interference.**

- **There can be two types of interference. It may be unintentional interference by another user simultaneously attempting to transmit through the channel.**

- **Or it may be intentional interference by a hostile transmitter attempting to jam the transmission.**

Spread-Spectrum Modulation

Definition of Spread Spectrum …

Spread spectrum **is a means of transmission in which the data sequence occupies a bandwidth in excess of the minimum bandwidth required to send it.**

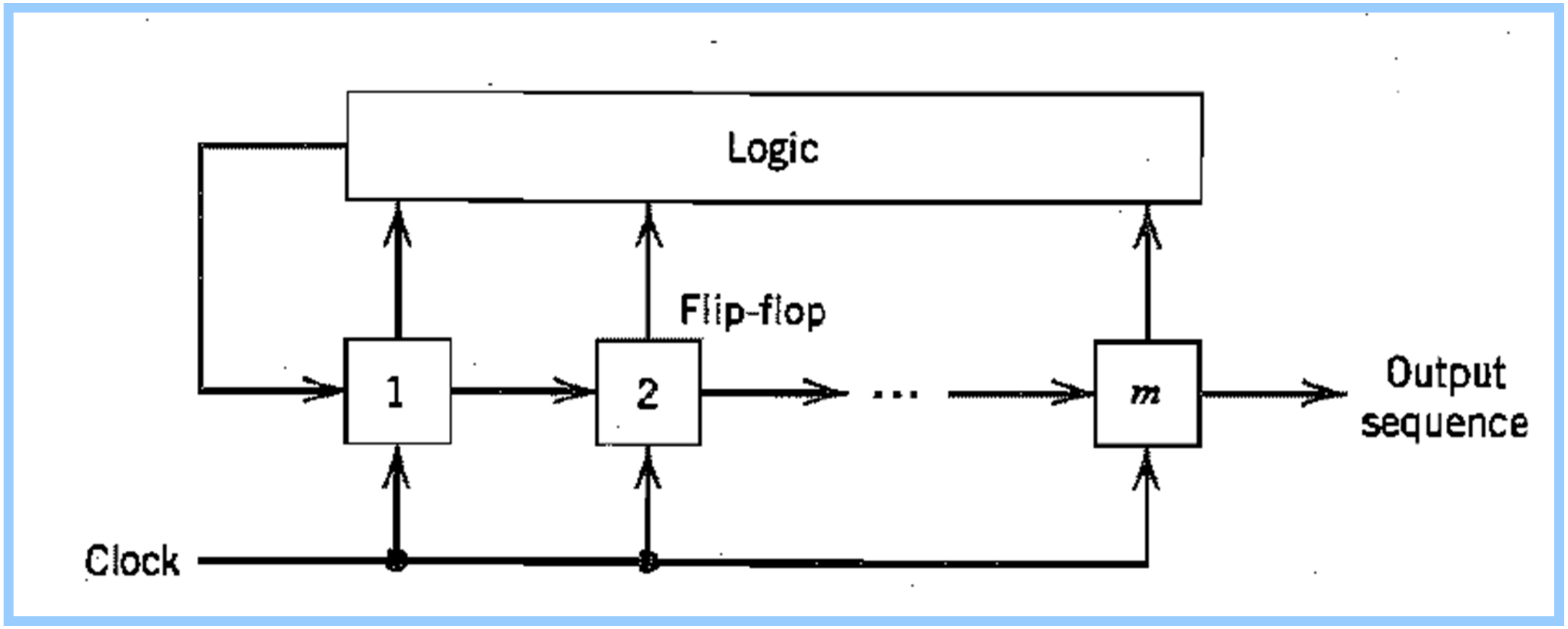
The *spectrum spreading* is achieved before transmission through the use of a code that is independent of the data sequence. The same code is used in the receiver (operating in synchronism with the transmitter) to despread the received signal so that the original data sequence may be recovered.

Two basic variants of spread-spectrum modulation are: *direct-sequence technique* and *frequency-hopping technique*.

Both techniques rely on the availability of a noiselike spreading code called a *pseudo-random* or *pseudo-noise sequence*.

Pseudo-Noise Sequences

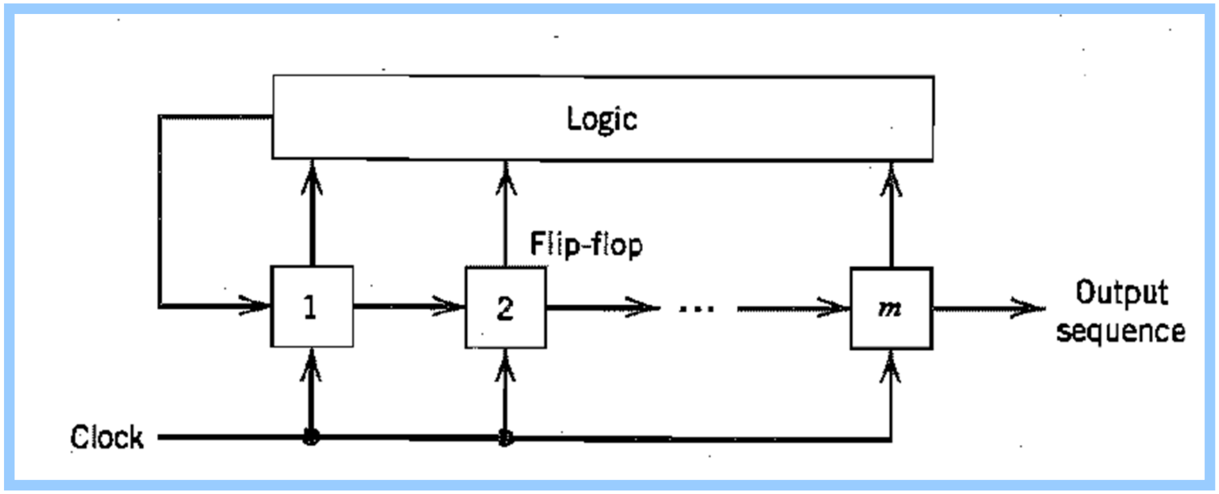
✓ A pseudo-noise (PN) sequence is a periodic binary sequence with a noiselike waveform, usually generated by means of a feedback shift register.



Feedback shift register.

The flip-flops are regulated by *a single timing clock*. At each clock pulse, the state of each flip-flop is shifted to the next one.

Pseudo-Noise Sequences



- ✓ **Let $s_j(k)$ denote the state of the jth flip-flop after the kth clock pulse (the state may be 0 or 1). The state of the shift register after the kth clock pulse is defined by the set $\{s_1(k), s_2(k), \ldots, s_m(k)\}$, where $k \geq 0$.**

$$s_j(k+1) = s_{j-1}(k), \qquad \begin{cases} k \geq 0 \\ 1 \leq j \leq m \end{cases}$$

$s_0(k)$: input applied to the first flip-flop after the kth clock pulse.

Pseudo-Noise Sequences

Observations and conclusions …

- ✓ **With a total number of *m* flip-flops, the number of possible states of the shift register is at most 2^m. Then the PN sequence generated by a feedback shift register must eventually become periodic with a period of at most 2^m.**

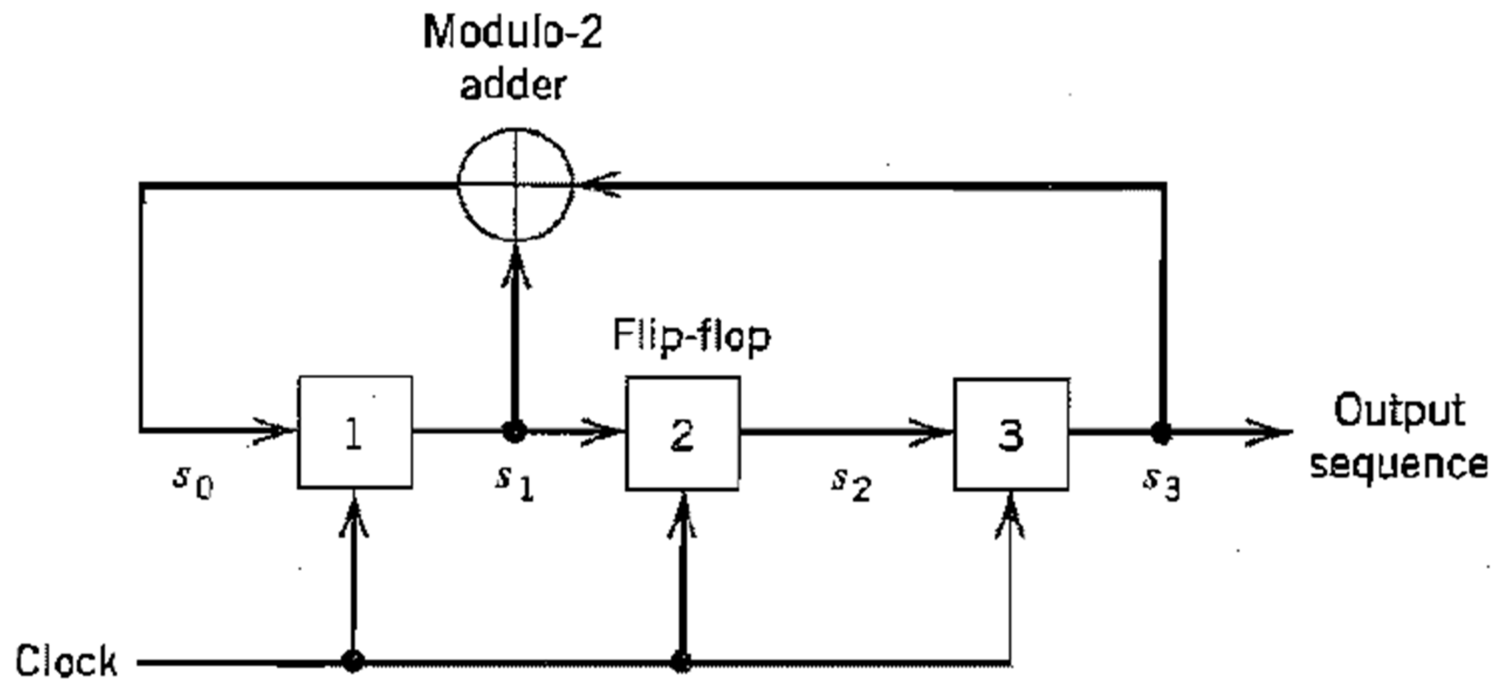
- ✓ **A feedback shift register is said to be linear, when the feedback logic consists entirely of modulo-2 adders. In such a case, the *zero state* (the state for which all the flip-flops are in state 0) is not permitted.**

- ✓ **Consequently, the period of a PN sequence with *m* flip-flops cannot exceed $2^m - 1$. When the period is exactly $2^m - 1$, the PN sequence is called a maximal-length sequence or simply *m*-sequence.**

Pseudo-Noise Sequences

An Example …

Let us consider a linear feedback shift register involving *three* flip-flops.



Maximal-length sequence generator for $m = 3$.

Let the initial state of the shift register be 100 (reading the contents of the flip-flops from left to right). Then the successive states will be: 100, 110, 111, 011, 101, 010, 001, 100, …. So, the output sequence is: 00111010….

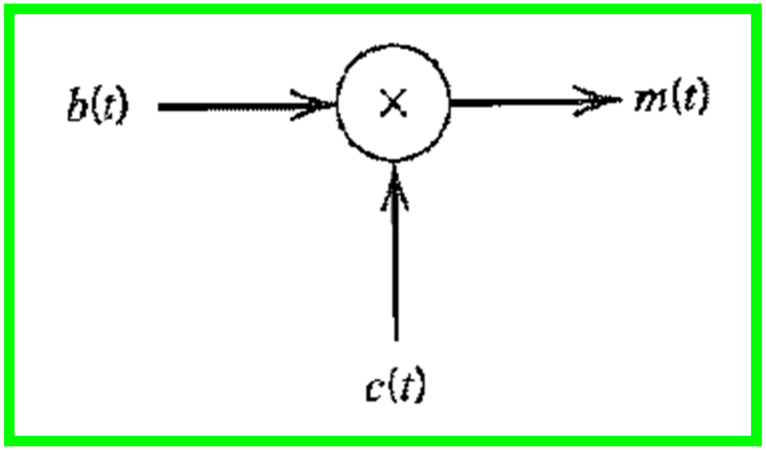
Spread-Spectrum Modulation for Baseband Transmission

Spread-spectrum modulation can provide protection against externally generated interfering (jamming) signals with finite power.

Protection against jamming waveforms is provided by purposely making the information bearing signal occupy a bandwidth far in excess of the minimum bandwidth necessary to transmit it. This has the effect of making the transmitted signal assume a noiselike appearance so as to blend into the background.

One method of widening the bandwidth of an information bearing (data) sequence involves the use of modulation.

Spread-Spectrum Modulation for Baseband Transmission



Transmitter for an idealized model of baseband spread-spectrum system.

$\{b_k\}$: a binary data sequence. $\{c_k\}$: a PN sequence.

$b(t)$ and $c(t)$: their respective polar NRZ waveform representations.

If the message signal $b(t)$ is narrowband and the PN signal $c(t)$ is wideband, the product (modulated) signal, $m(t)= b(t)c(t)$, will have *a spectrum that is nearly the same as the wideband PN signal*. Hence, PN sequence performs the role of a *spreading code*.

Spread-Spectrum Modulation for Baseband Transmission

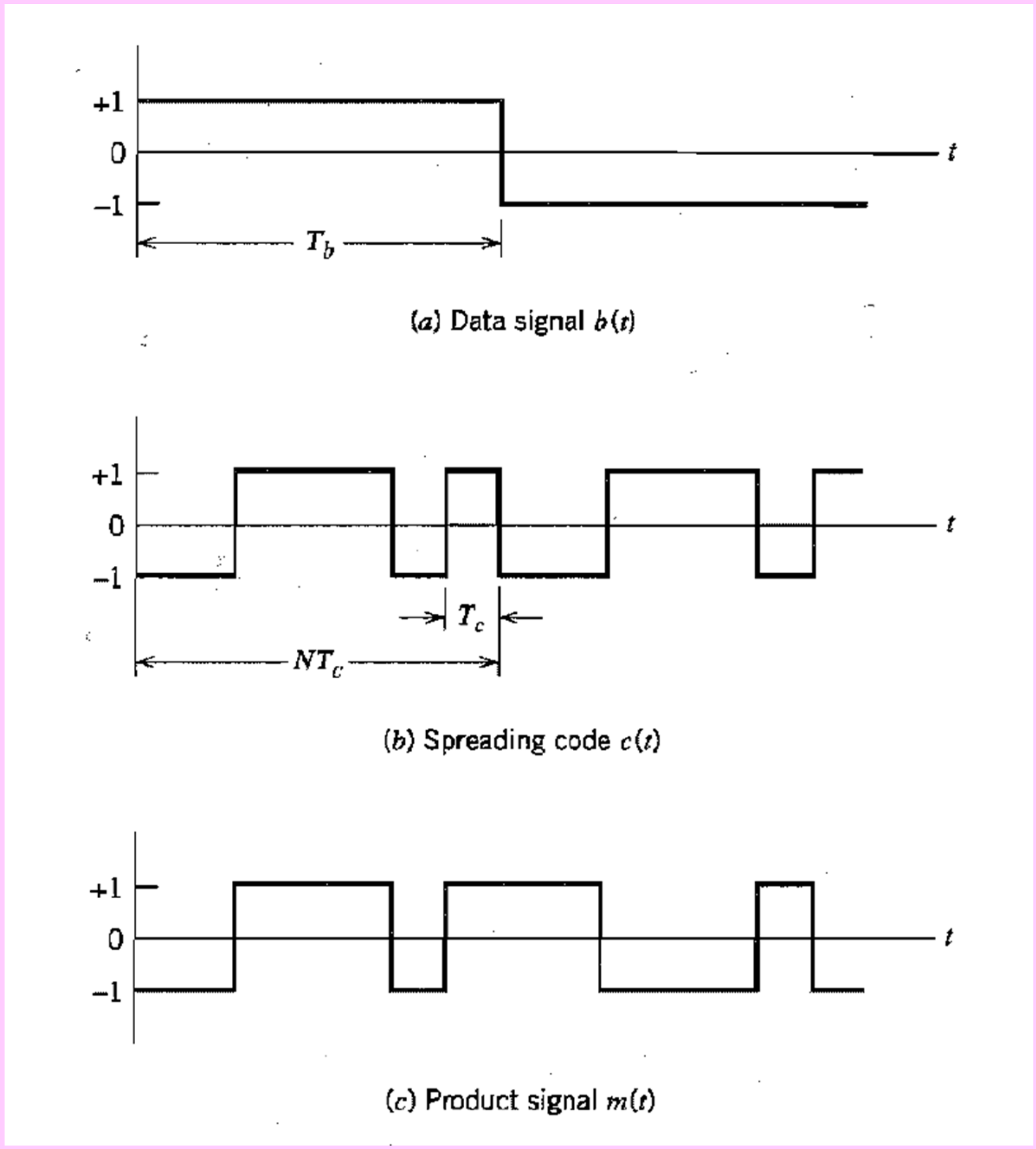
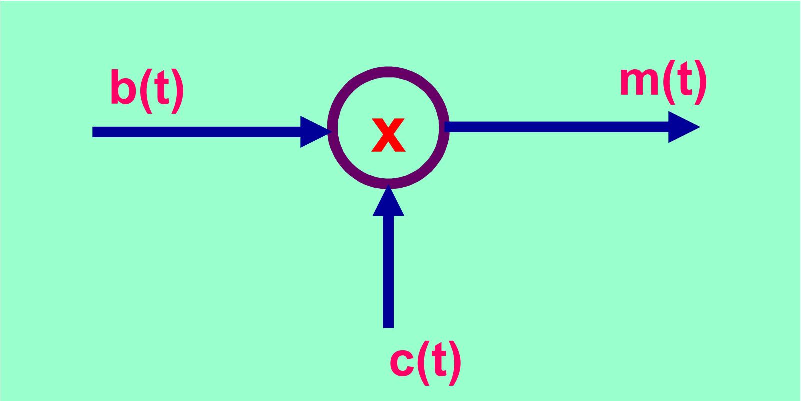
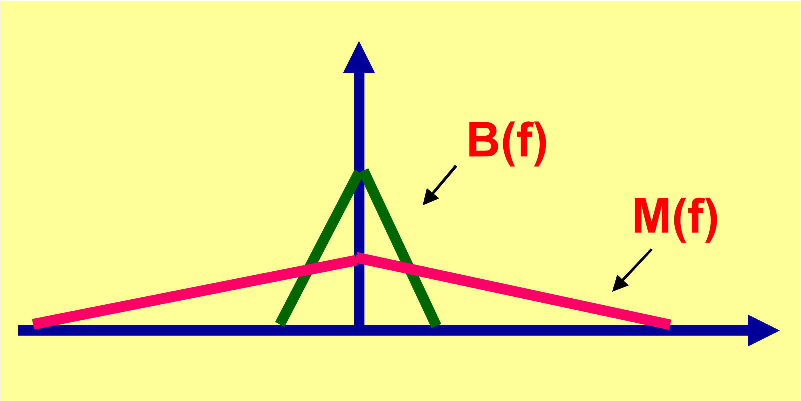


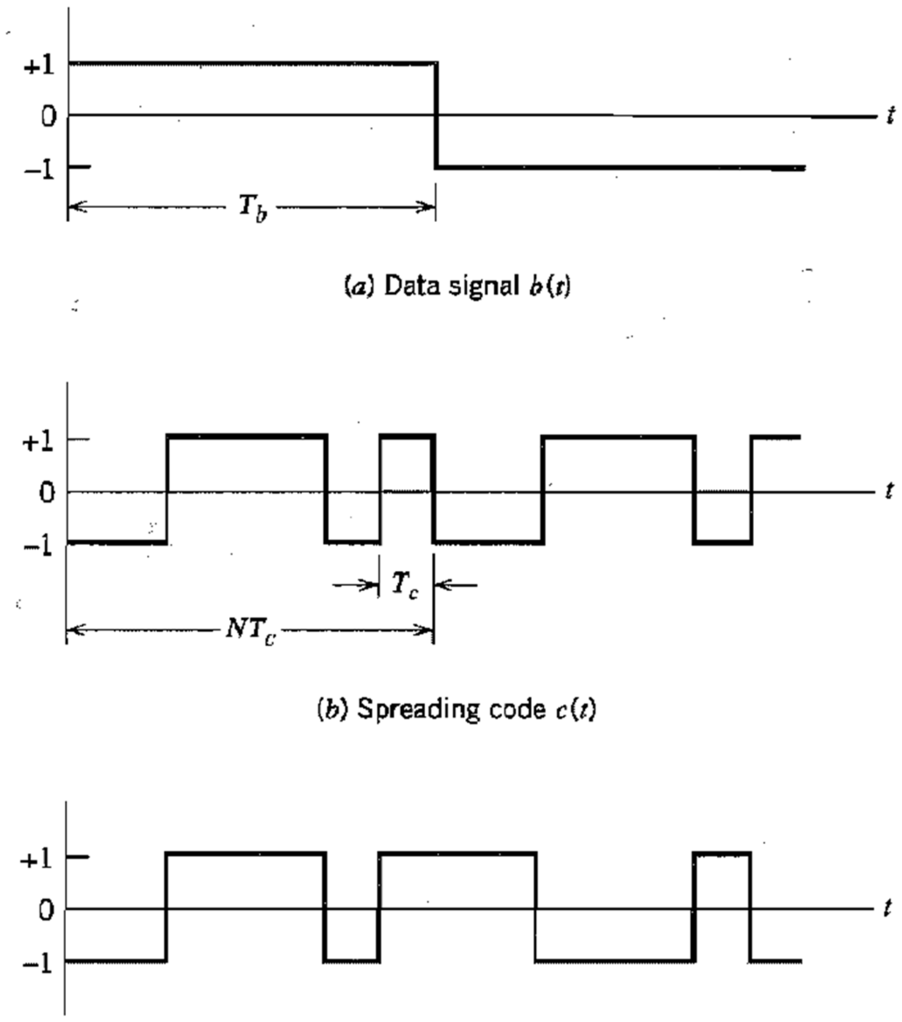
Illustration of the input and output waveforms in the transmitter.

Spread-Spectrum Modulation for Baseband Transmission



$$m(t) = b(t) \times c(t)$$
$$M(f) = B(f) * C(f)$$



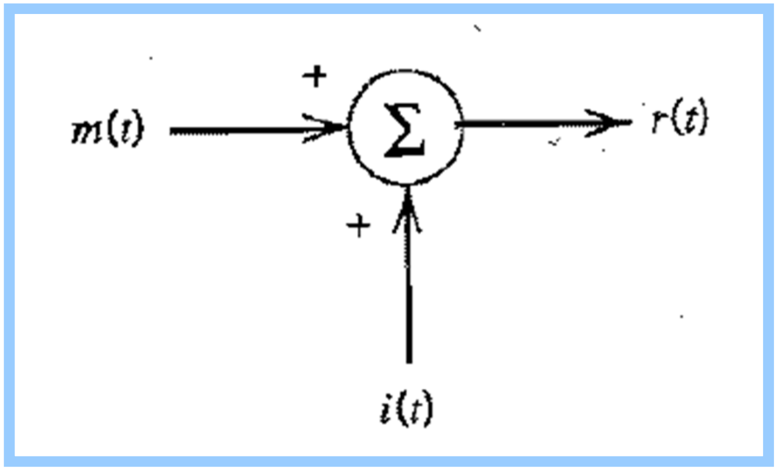


(a) Data signal $b(t)$

(b) Spreading code $c(t)$

(c) Product signal $m(t)$

Spread-Spectrum Modulation for Baseband Transmission

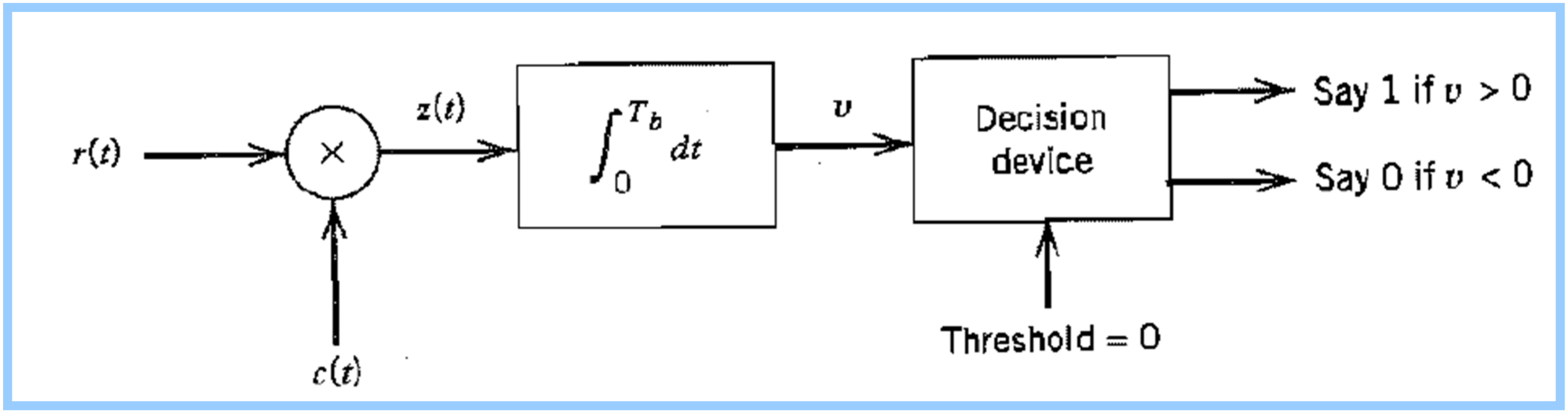


Channel for an idealized model of baseband spread-spectrum system.

The received signal *r*(*t*) consists of the transmitted signal *m*(*t*) plus an additive interference *i*(*t*), as shown in the channel model.

$$
\begin{aligned}
r(t) &= m(t) + i(t) \\
&= c(t)b(t) + i(t)
\end{aligned}
$$

Spread-Spectrum Modulation for Baseband Transmission

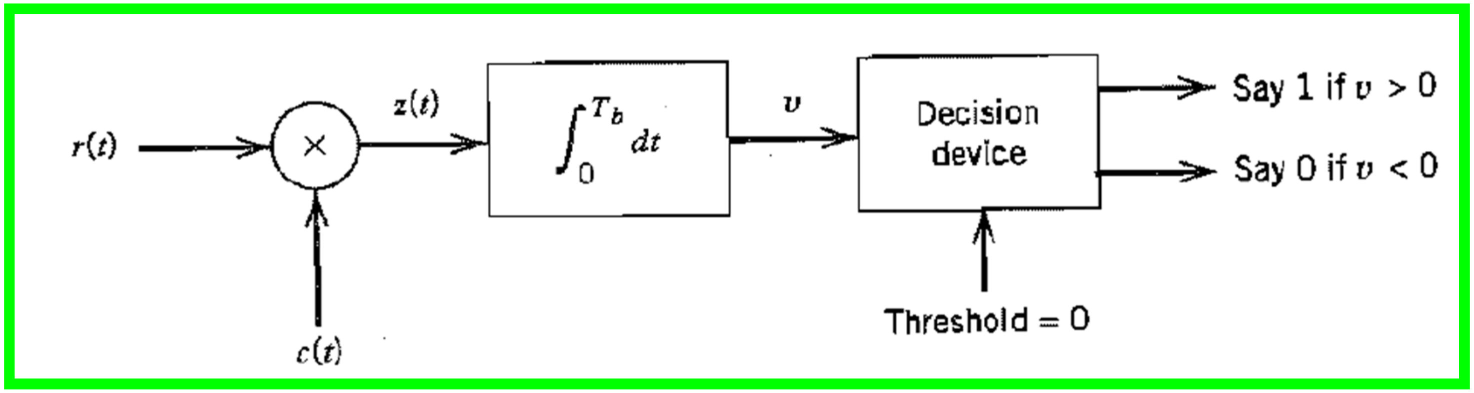


Receiver for an idealized model of baseband spread-spectrum system.

To recover the original message signal *b*(*t*), the received signal *r*(*t*) is applied to a demodulator that consists of a multiplier, followed by an integrator, and a decision device.

The multiplier is supplied with a locally generated PN sequence that is an exact replica of that used in the transmitter.

Spread-Spectrum Modulation for Baseband Transmission



The multiplier output in the receiver:

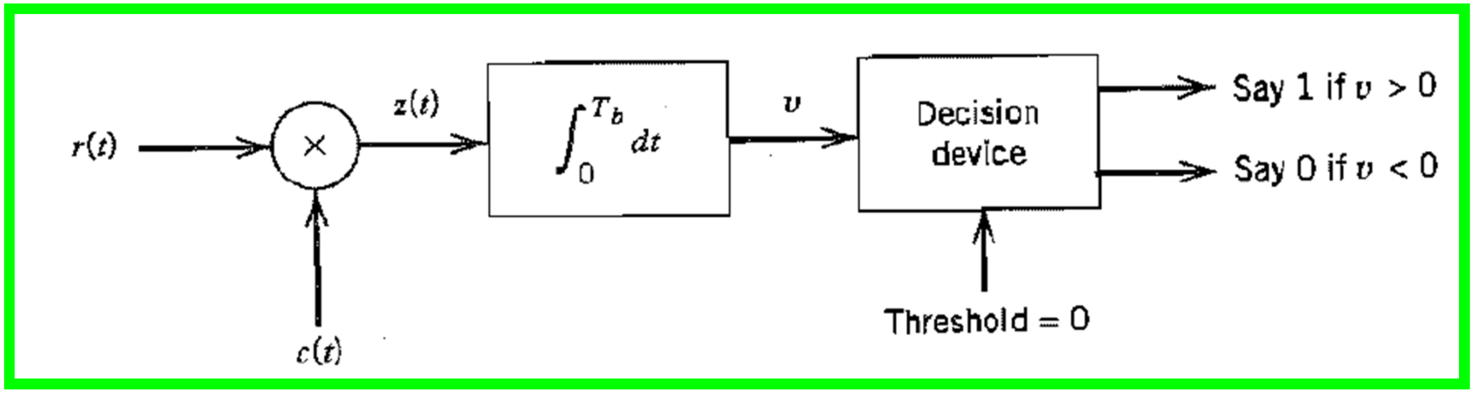
$$\begin{aligned} z(t) &= c(t)r(t) \\ &= c^2(t)b(t) + c(t)i(t) \end{aligned}$$

Also:

$$c^2(t) = 1 \qquad \text{for all } t$$

$$z(t) = b(t) + c(t)i(t)$$

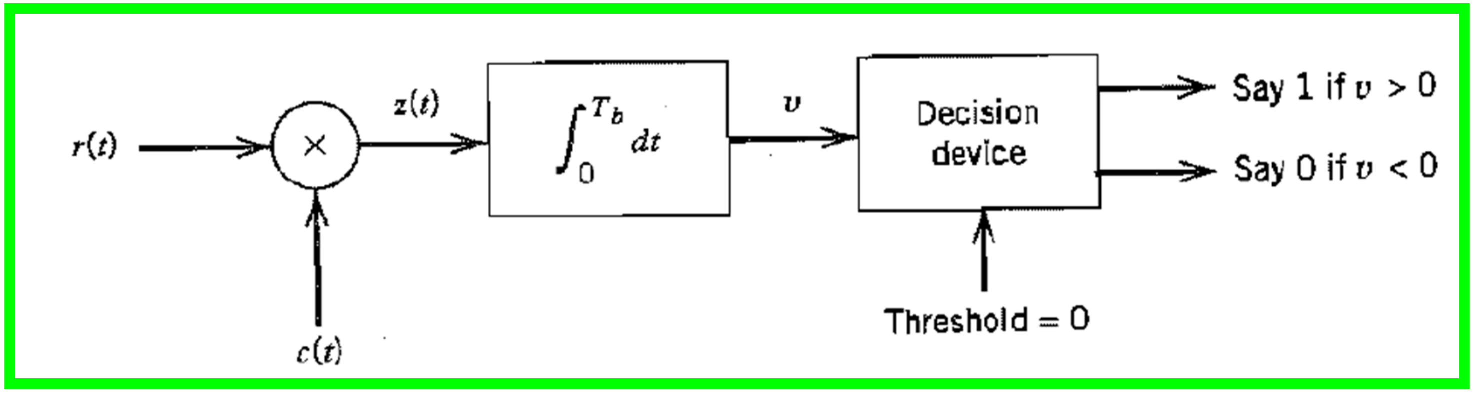
Spread-Spectrum Modulation for Baseband Transmission



***Conclusion*: The data signal $b(t)$ is reproduced at the multiplier output in the receiver, except for the effect of the interference represented by the additive term $c(t)i(t)$.**

The data signal $b(t)$ is narrowband and the spurious component $c(t)i(t)$ is wideband. Hence the multiplier output is applied to a low-pass filter with a bandwidth just large enough to accommodate the recovery of $b(t)$ and thus the effect of interference is significantly reduced at the receiver output.

Spread-Spectrum Modulation for Baseband Transmission



In the receiver, the low-pass filtering is actually performed by an integrator. The integration is carried out over the bit interval $0 \le t \le T_b$.

The decision device makes a decision for the receiver, based on the sign of v, the integrator output. If $v < 0$, the receiver infers that symbol 0 was sent. If $v > 0$, the receiver infers that symbol 1 was sent.

Spread-Spectrum Modulation for Baseband Transmission

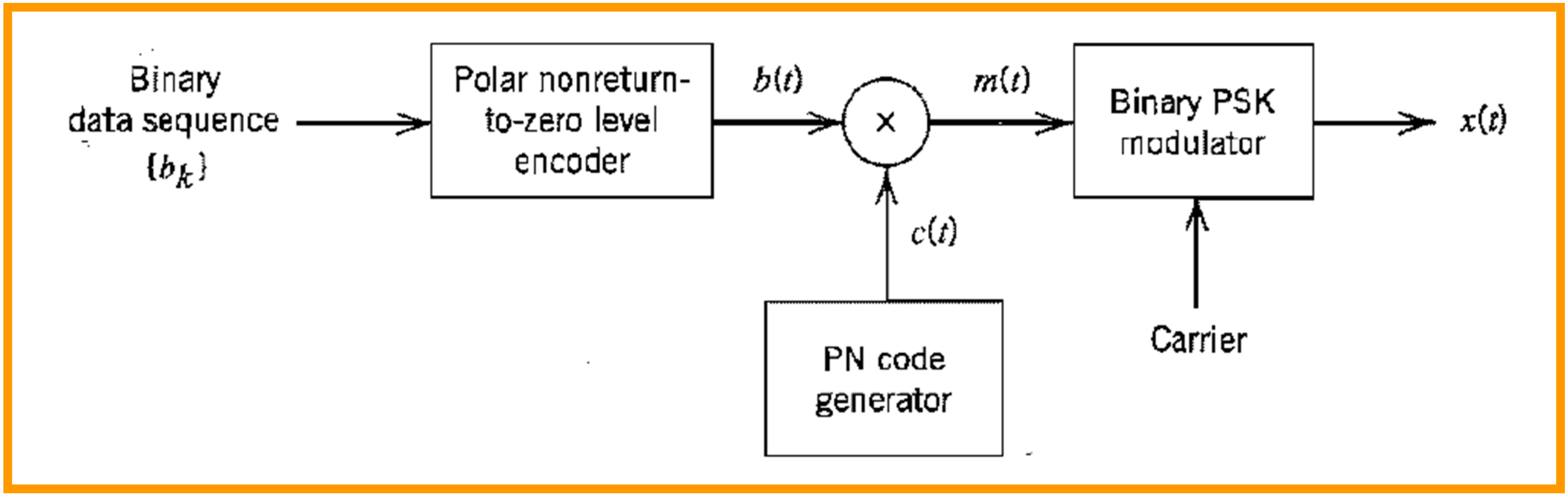
Final Conclusion …

The longer the period of the *spreading code* (with pseudo-random properties), the closer will the transmitted signal be to a truly random binary wave, and the harder it will be to detect.

Any price paid ??

YES. The price paid for improved protection against interference is increased transmission bandwidth, system complexity, and processing delay.

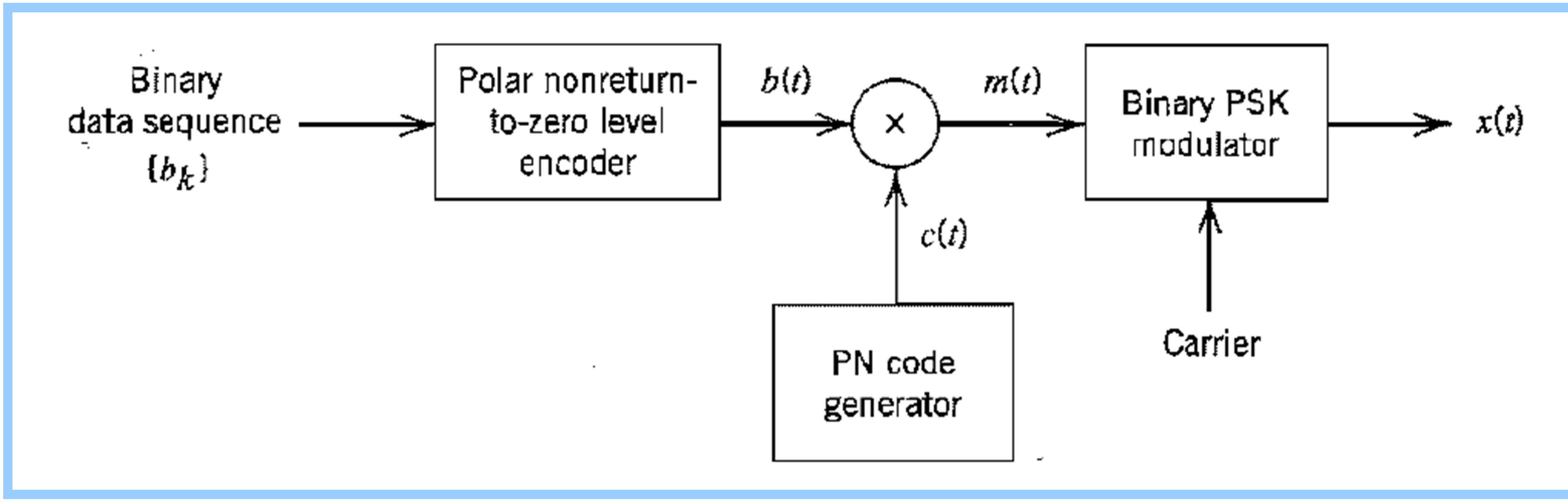
Direct-Sequence Spread-Spectrum with Coherent BPSK



Transmitter for DS/BPSK scheme.

The transmitted signal $x(t)$ is a direct-sequence spread binary phase-shift-keyed (DS/BPSK) signal. The phase modulation $\theta(t)$ of $x(t)$ has one of two values, 0 and π, depending on the polarities of $b(t)$ and $c(t)$.

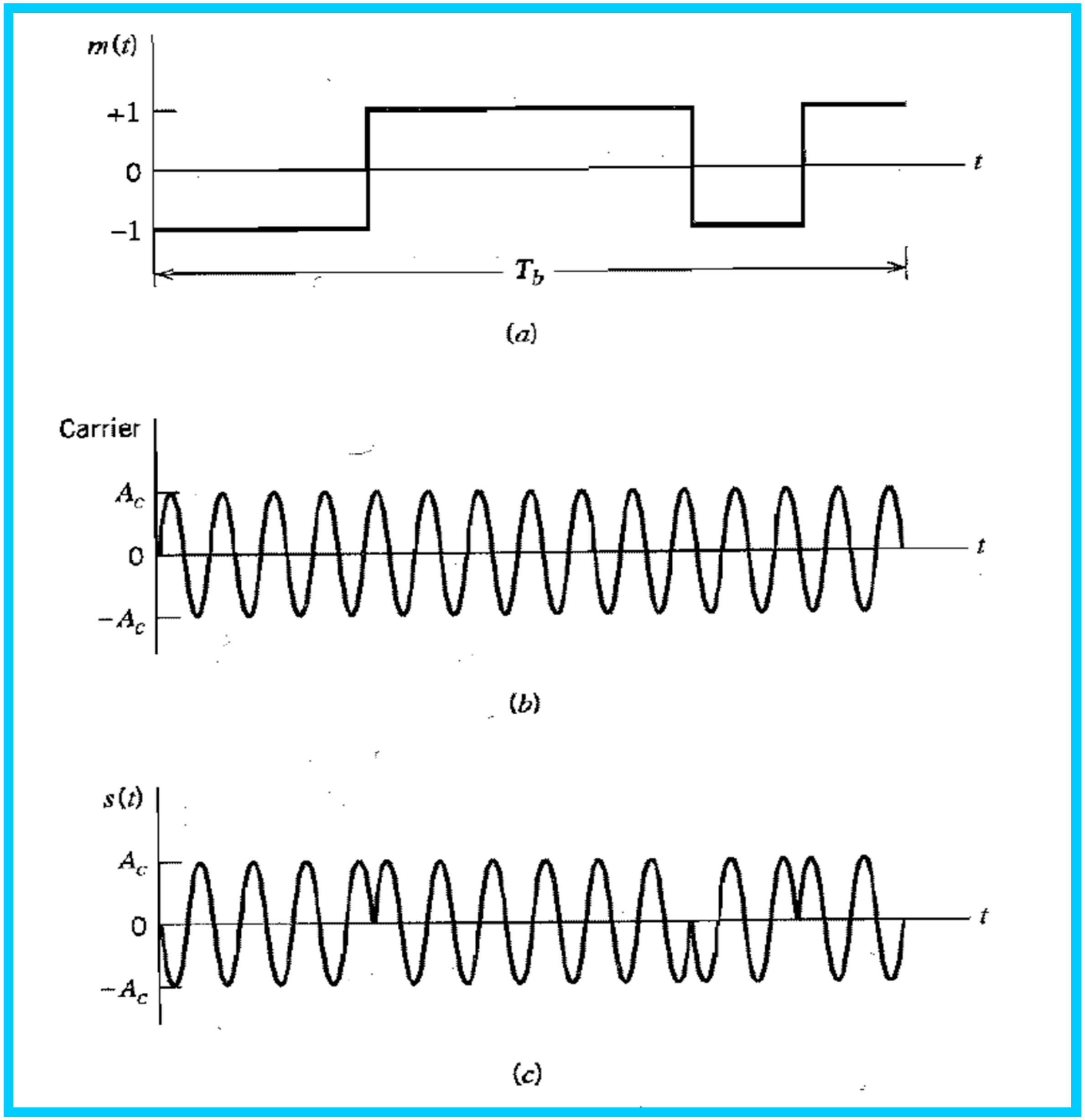
Direct-Sequence Spread-Spectrum with Coherent BPSK



		Polarity of data sequence ***b*(*t*)** at time ***t***	
		+	-
Polarity of PN sequence ***c*(*t*)** at time ***t***	+	0	π
	-	π	0

Truth Table for Phase Modulation θ(*t*) (in Radians)

Direct-Sequence Spread-Spectrum with Coherent BPSK



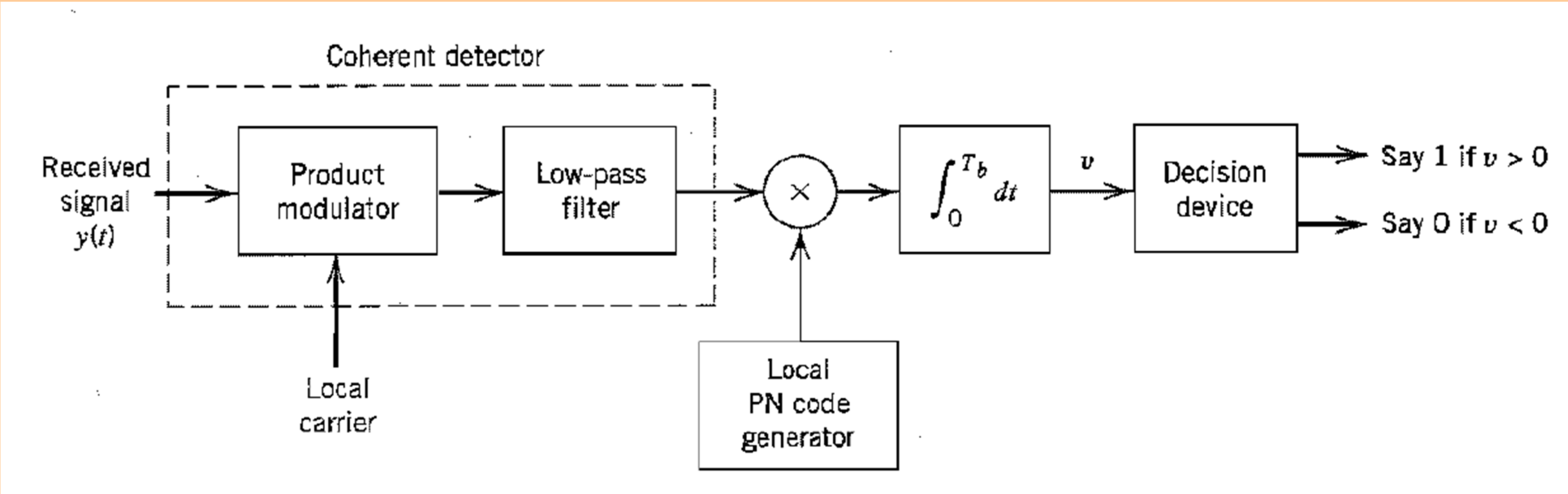
Waveforms for the second stage of modulation.

(a) Product signal $m(t) = c(t)b(t)$.

(b) Sinusoidal carrier.

(c) DS/BPSK signal.

Direct-Sequence Spread-Spectrum with Coherent BPSK



Receiver for DS/BPSK scheme.

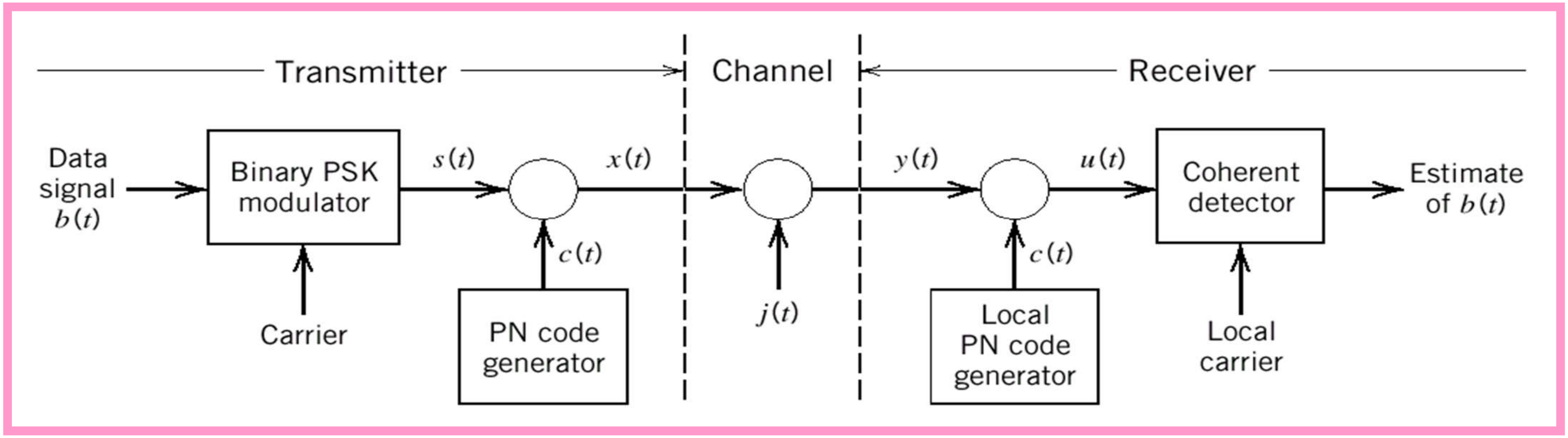
Here also, demodulation is performed in two stages:

Stage 1: reverses the phase shift keying applied to the transmitted signal.

Stage 2: performs spectrum despreading.

Direct-Sequence Spread-Spectrum with Coherent BPSK

Model for Analysis …



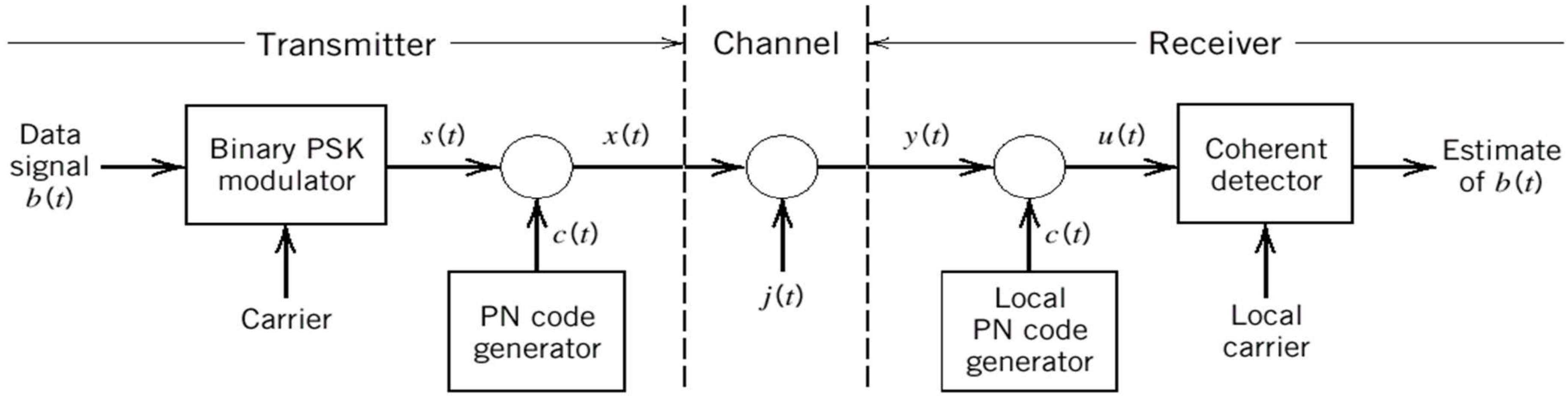
Model of DS/BPSK system.

For model analysis, it is more convenient to interchange the order of two stages of modulation. Similarly the two stages of demodulation are also interchanged.

For the interchange operation to be feasable, the incoming data sequence and the PN sequence must be synchronized.

Direct-Sequence Spread-Spectrum with Coherent BPSK

Model for Analysis …



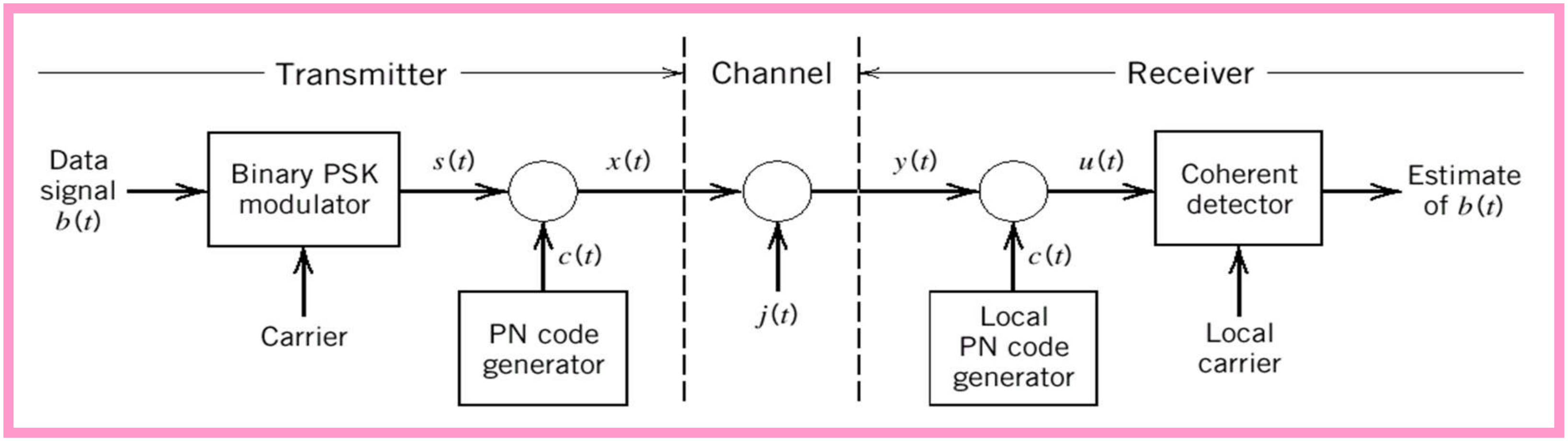
The channel output:

$$y(t) = x(t) + j(t)$$
$$= c(t)s(t) + j(t)$$

***s*(*t*): binary PSK signal. *c*(*t*): PN signal. *j*(*t*): interfering signal.**

Direct-Sequence Spread-Spectrum with Coherent BPSK

Model for Analysis . . .



The coherent detector input:

$$
\begin{aligned}
u(t) &= c(t)y(t) \\
&= c^2(t)s(t) + c(t)j(t) \\
&= s(t) + c(t)j(t)
\end{aligned}
$$

$$c^2(t) = 1 \qquad \text{for all } t$$

The coherent detector input $u(t)$ consists of a binary PSK signal $s(t)$ embedded in additive code-modulated interference, $c(t)j(t)$. The modulated nature of the latter component forces the interference signal to spread its spectrum such that the information bits at the receiver output can be detected more reliably.

Direct-Sequence Spread-Spectrum with Coherent BPSK

Constraints of Direct-Sequence Technique …

The use of a PN sequence to modulate a phase-shift-keyed signal achieves *instantaneous spreading* of the transmission bandwidth.

The ability of such a system to combat the effects of jammers is determined by the *processing gain of the system*, which is a function of the PN sequence period.

The *processing gain* can be made larger by employing a PN sequence with narrow chip duration. However, the capabilities of physical devices used to generate the PN spread-spectrum signals impose a practical limit on the attainable processing gain.

Implication …

The *processing gain* may turn out not large enough to overcome the effects of some jammers of concern. An alternative solution is to use frequency-hop spread-spectrum technique.

Frequency-Hop Spread-Spectrum Technique

Here the data-modulated carrier ***hops randomly*** from one frequency to another. In effect, the spectrum is spread ***sequentially*** rather than **instantaneously**. Here the term ***sequentially*** refers to the pseudo-random-ordered sequence of frequency hops.

A common modulation format for ***FH systems*** is that of M-ary frequency-shift keying (MFSK). The combination of these two techniques is called **FH/MFSK**.

Frequency-hop Techniques

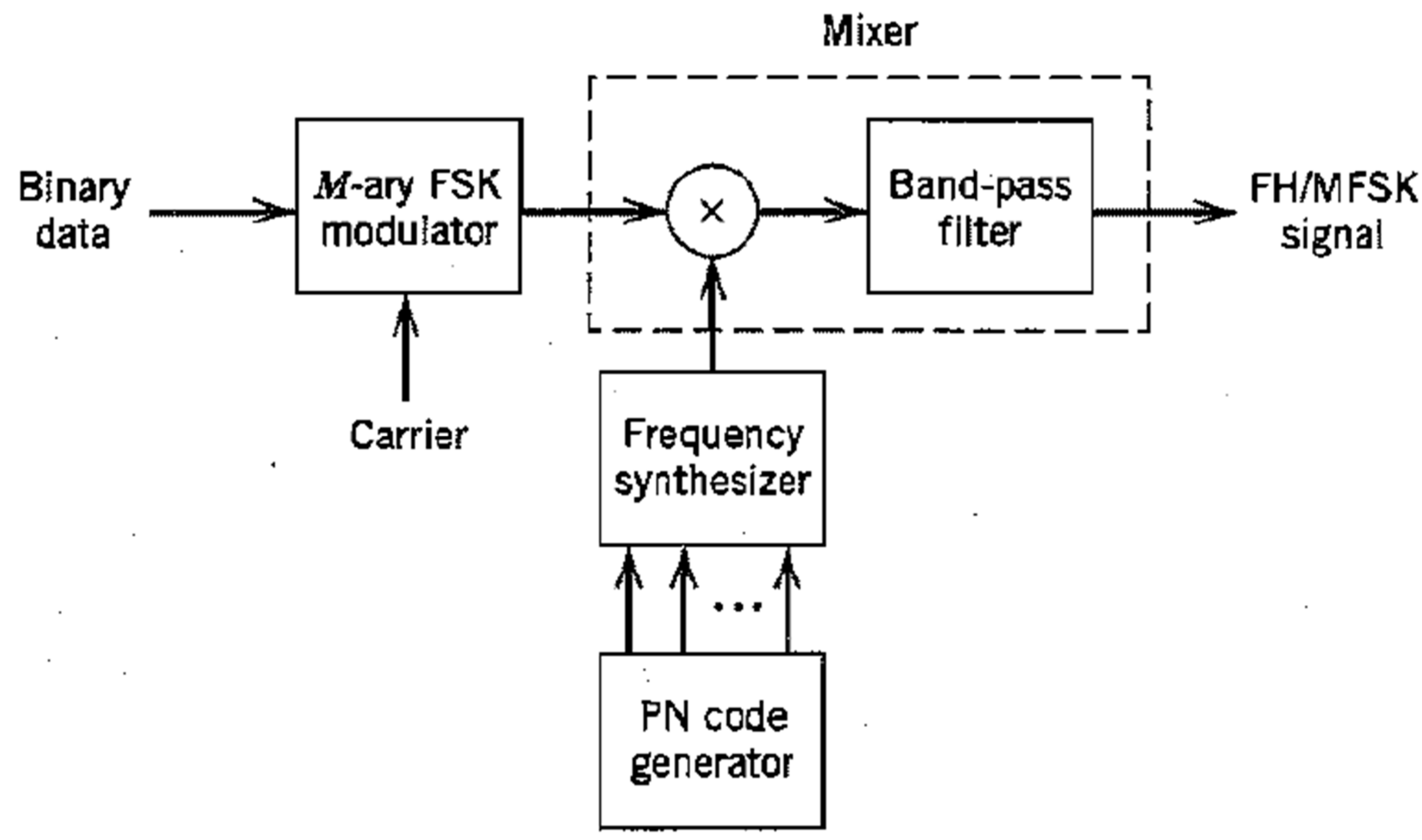
Slow-frequency hopping

(symbol rate R_s of the MFSK signal is an integer multiple of hop rate R_h)

Fast-frequency hopping

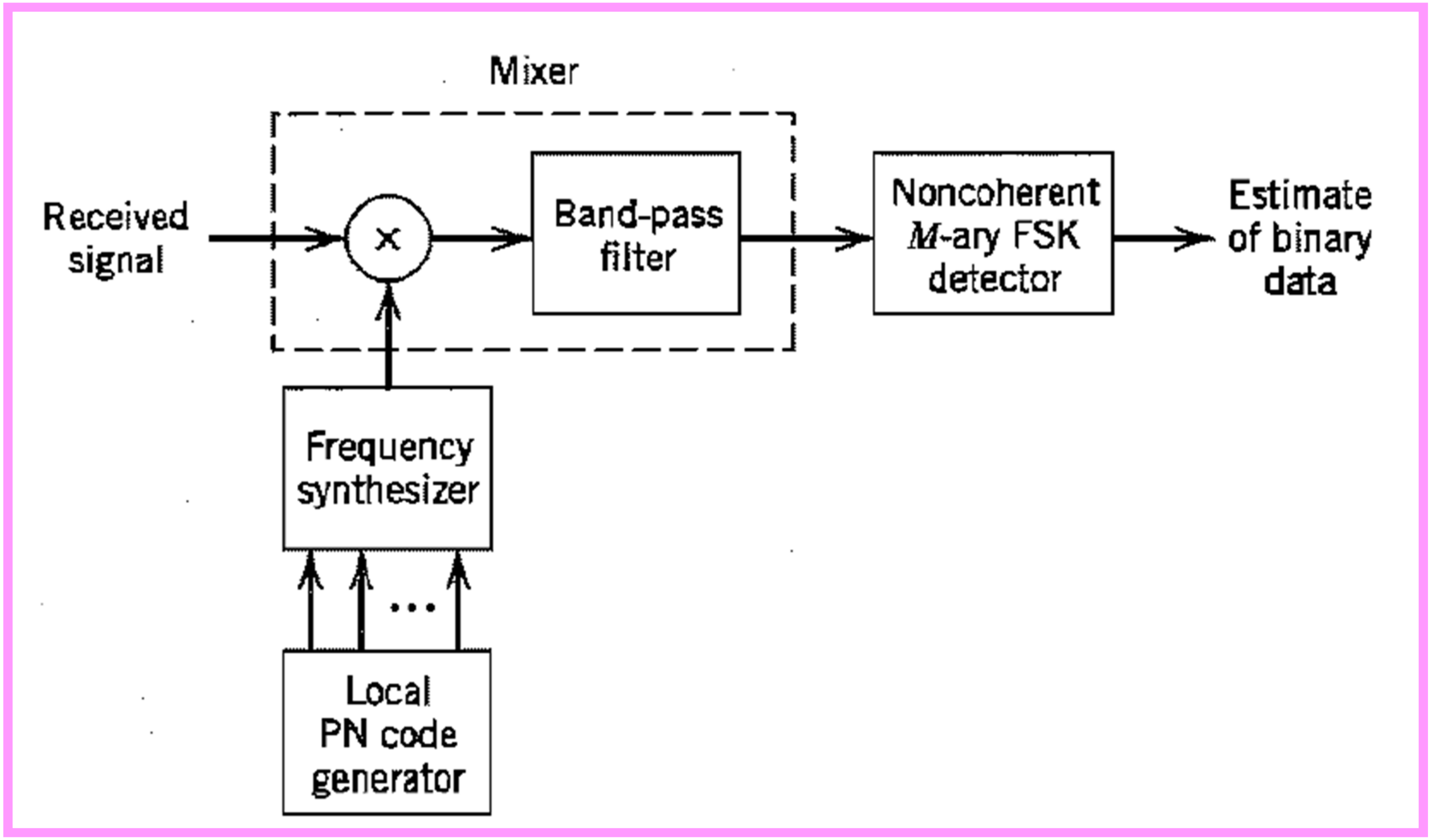
(hop rate R_h is an integer multiple of symbol rate R_s of the MFSK signal)

Slow-Frequency Hopping



Transmitter for frequency-hop spread M-ary FSK.

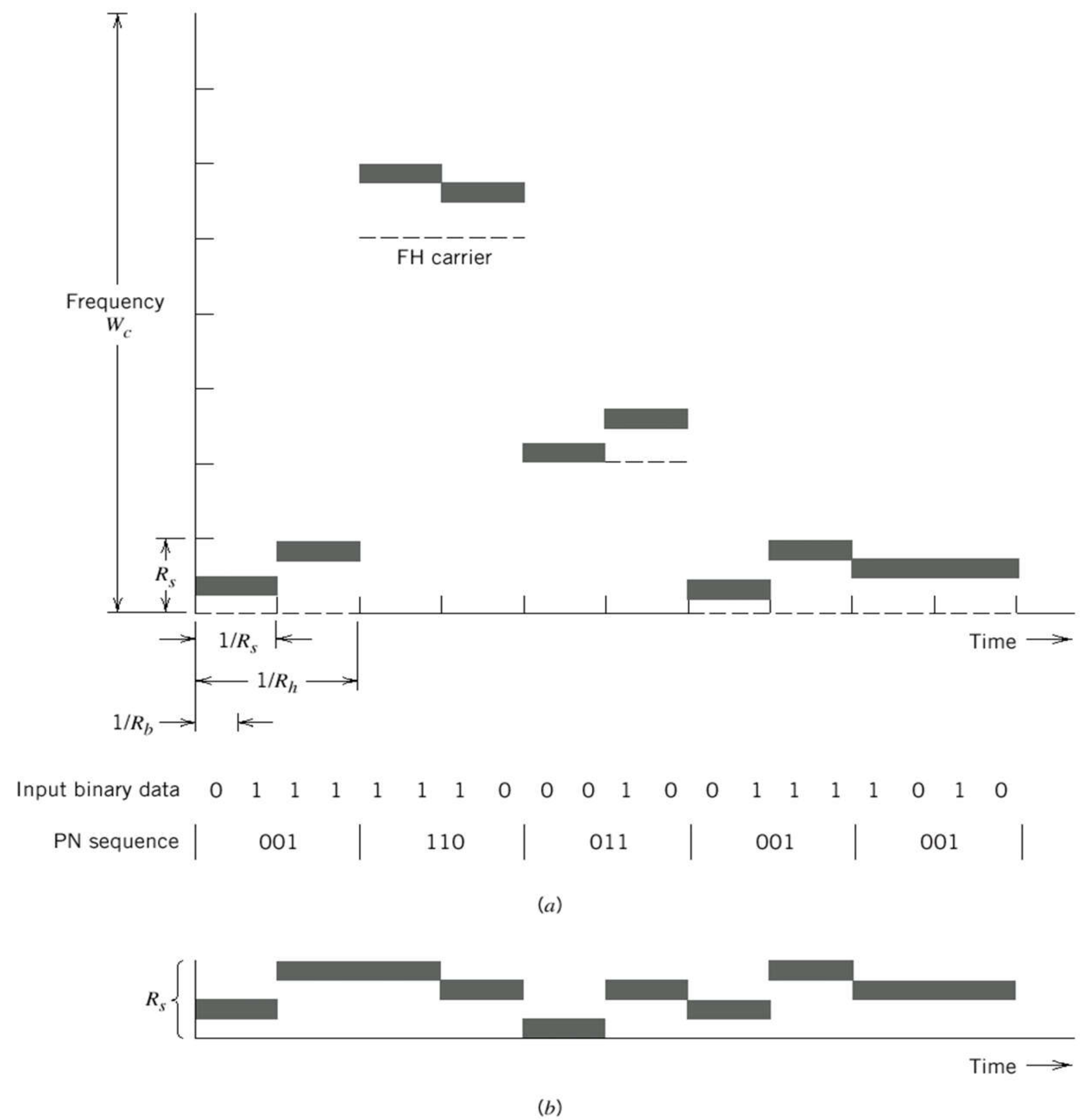
Slow-Frequency Hopping



Receiver for frequency-hop spread M-ary FSK.

Slow-Frequency Hopping

An Example …



(a) Frequency variation for one complete period of the PN sequence.

(b) Variation of dehopped frequency with time.

Number of bits per MFSK symbol = 2 → $M = 4$

$R_s = R_b/2$

$R_c = \max(R_h, R_s) = R_s$

Length of PN segment per hop (k) = 3

Total number of frequency hops = $2^k = 8$

Parameters of the FH/MFSK signal.

Fast-Frequency Hopping

Features . . .

In a fast FH/MFSK system, there are multiple hops per *M*-ary symbol. Hence, in a fast FH/MFSK system, each hop is a chip. Usually fast frequency hopping is used to defeat a smart jammer's tactic.

How to recover data at the Receiver ??

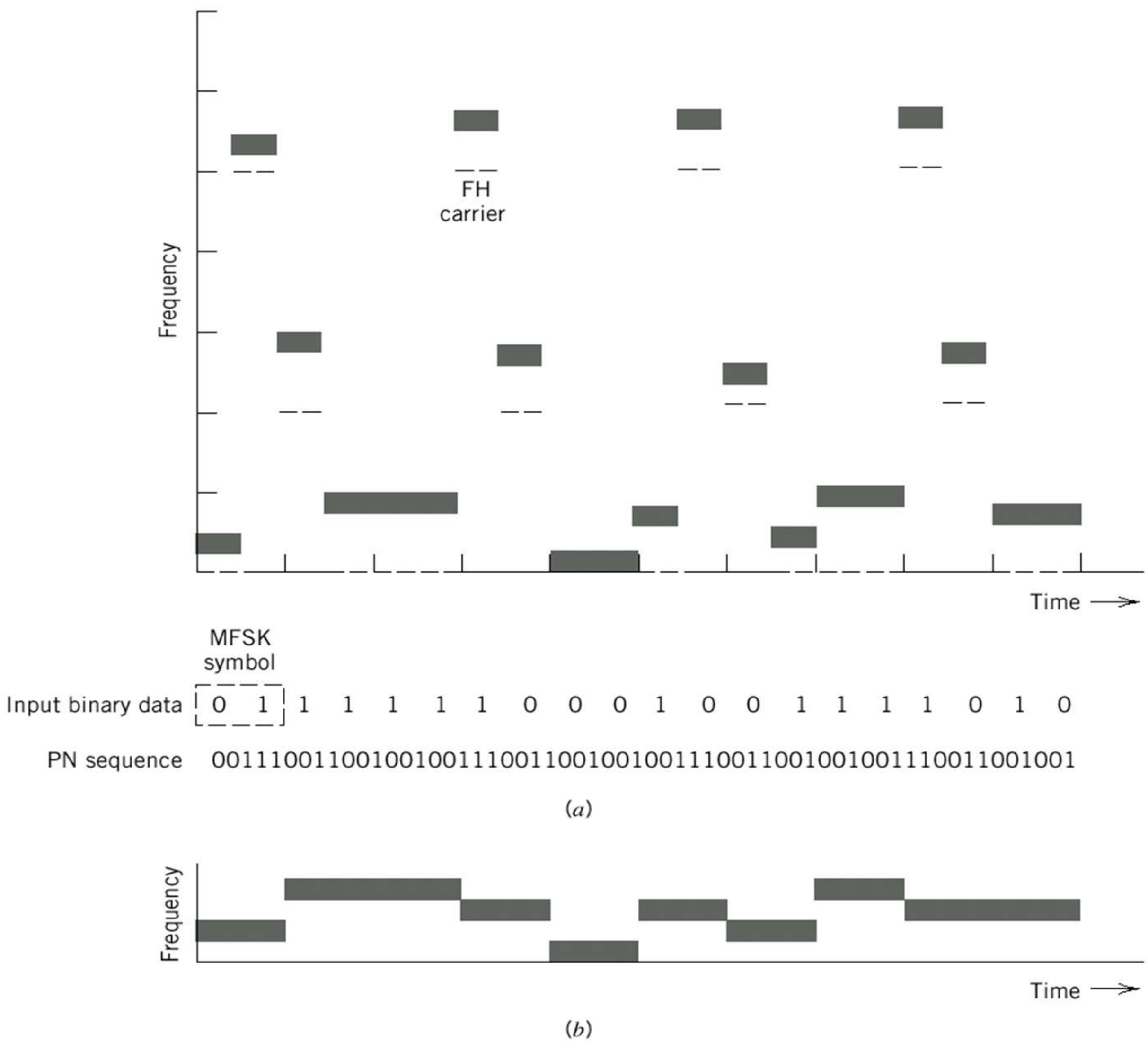
The data recovery can be performed by noncoherent detection at the receiver. The detection procedure can be implemented in two ways:

Procedure 1: For each FH/MFSK symbol, separate decisions are made on the *K* frequency-hop chips received and a *majority vote* based rule is used to estimate the dehopped MFSK symbol.

Procedure 2: For each FH/MFSK symbol, likelihood functions are computed as functions of the total signal received over *K* chips and the largest one is selected. A receiver so designed is optimum.

Fast-Frequency Hopping

An Example …



(a) Variation of the transmitter frequency with time.

(b) Variation of dehopped frequency with time.

Number of bits per MFSK symbol = 2 → M = 4

$R_s = R_b/2$

$R_c = \max(R_h, R_s) = R_h$

Length of PN segment per hop (*k*) = 3

Total number of frequency hops = $2^k = 8$

Parameters of the FH/MFSK signal.

References

- **Simon Haykin, *Communication Systems*. 4th Edition, Wiley India Edition, 2008.**

- **Bernard Sklar, *Digital Communication: Fundamentals and Applications*. 2nd Edition, Pearson Education, 2007.**

Thank You ...