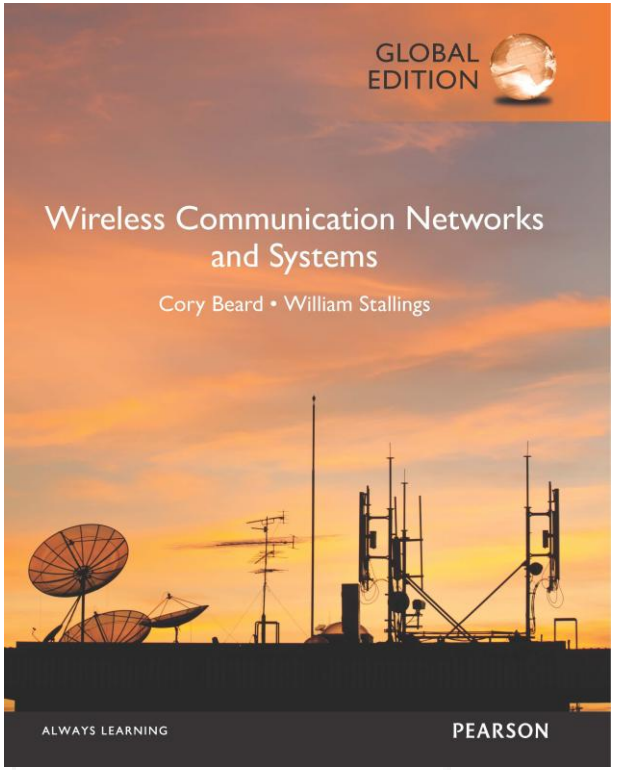
MOBILE SYSTEM-HT25
LECTURE 10: SPREAD SPECTRUM

Azra Abtahi
Email: azra.abtahi-fahliani@mau.se
Faculty of Technology and Society Department of Computer Science and Media Technology Malmö University

Most slides are primarily adapted from Beard & Stallings (2016), Wireless Communication Networks and Systems (Chapter 9)



Wireless Communication Networks and Systems
1st edition, Global edition
Cory Beard, William Stallings

WHERE WE ARE IN THE COURSE

- Evolution of Wireless Communication, Transmission fundamentals, Analog and Digital Modulations (Lectures 2-4)
- The Wireless Channel (Lectures 5 and 6)
- Transmission Fundamentals (CTFT, DTFT) (Lecture 7)
- Orthogonal Frequency Division Multiplexing- OFDM (Lecture 8)
- Spread Spectrum (Lecture 10)
- Coding and Error Control (Lecture 11)
- Cellular Wireless Networks (Lecture 12)
- Short-Range Wireless Technologies & Applications of Wireless Technologies in IoT (Lecture 13)

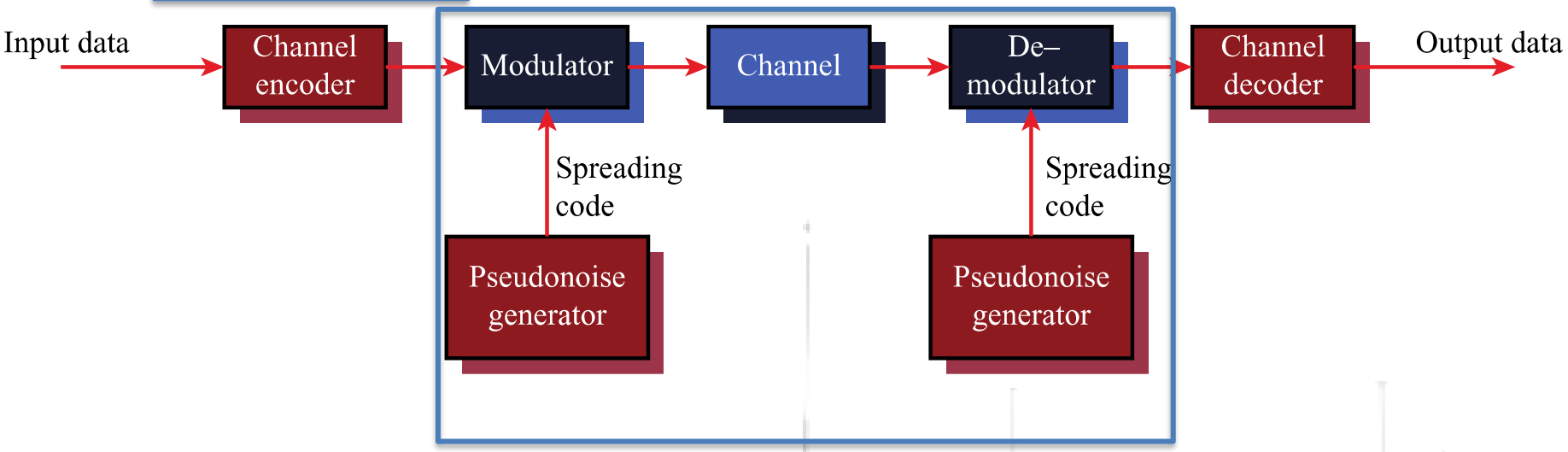
OUTLINE

- Spread Spectrum
  - Frequency Hoping Spread Spectrum (FHSS) (DT I)
  - Direct Sequence Spread Spectrum (DSSS) (DT II)
- Code-Division Multiple Access (CDMA) (DT III)
- Why Spread the Spectrum?
- Categories of Spreading Sequences

SPREAD SPECTRUM

- A communication technique where a signal is **intentionally spread** over a **much wider bandwidth** than needed for normal data transmission.
- Uses a **spreading code** known to both transmitter and receiver.
- The transmitter uses the code for **spreading the signal's spectrum;**
- The receiver uses the **same code** to **despread** the signal and recover the original data.

Next Lecture



9.1 GENERAL MODEL OF SPREAD SPECTRUM DIGITAL COMMUNICATION SYSTEM

SPREAD SPECTRUM

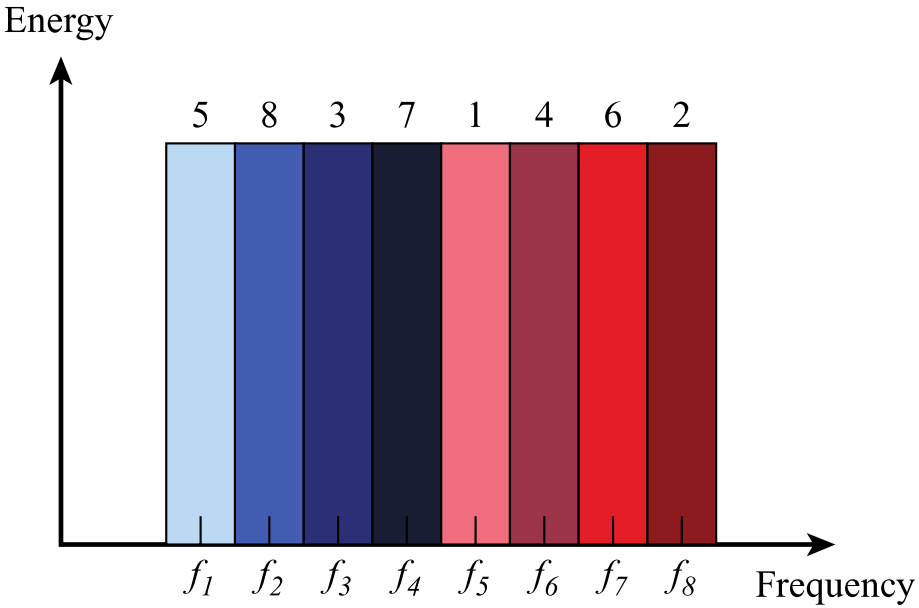
- Frequency Hoping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)

Technology	Method
CDMA (3G Mobile Networks)	DSSS
GPS	DSSS
Bluetooth	FHSS
Wi-Fi (802.11b)	DSSS
Military Radios	FHSS/DSSS

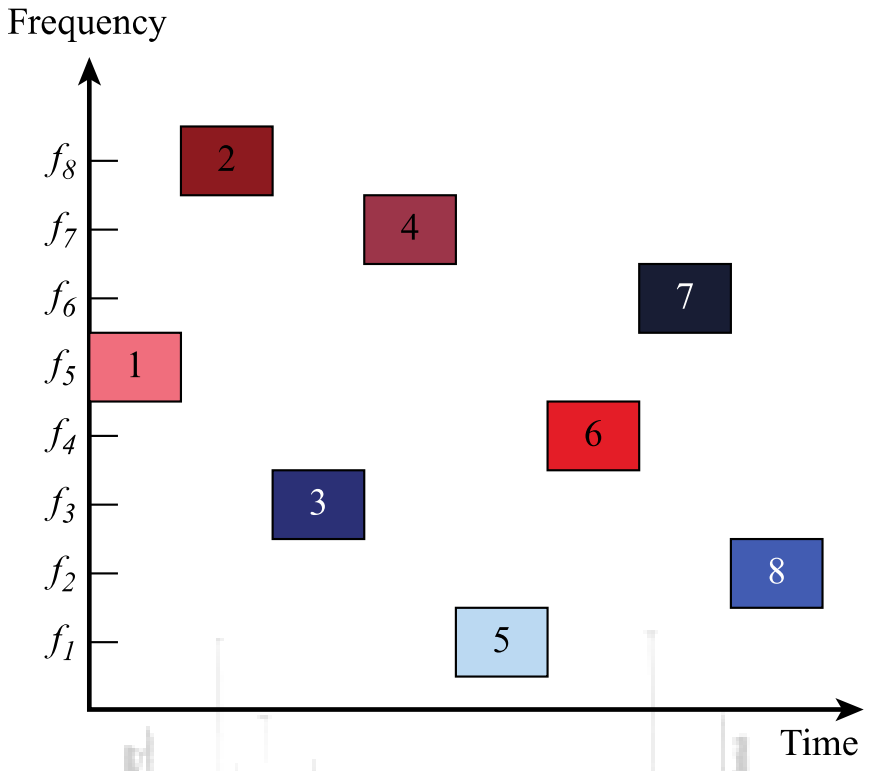
FREQUENCY HOPING SPREAD SPECTRUM (FHSS)

- **The carrier frequency** is changed according to a **secret hopping pattern,** dictated by a **spreading code.**

- Receiver must **follow the same hop sequence** to recover the data.



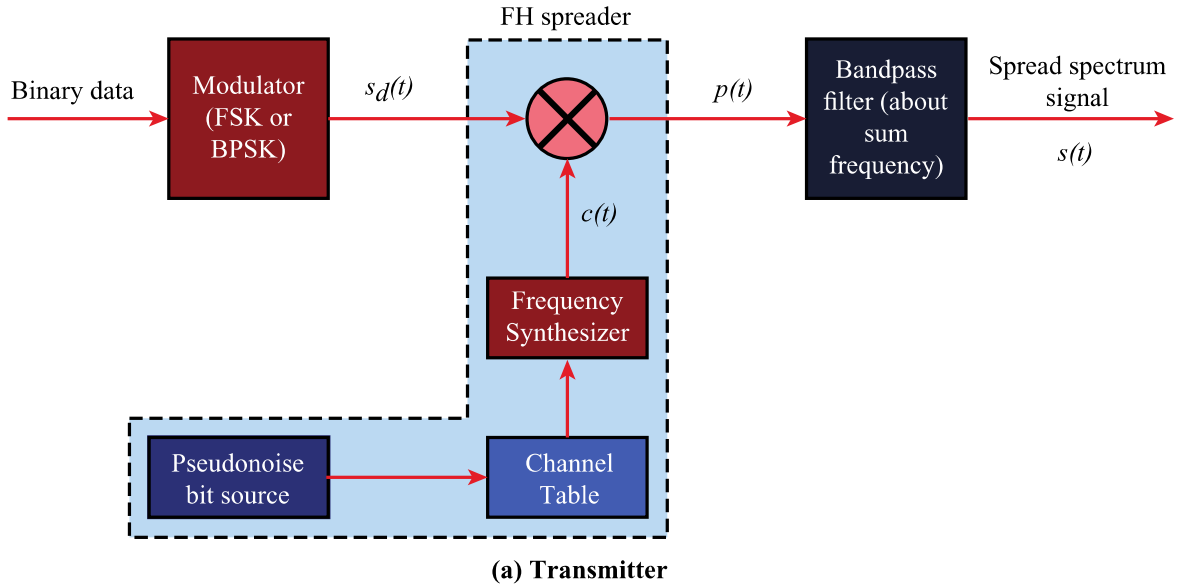
(a) Channel assignment



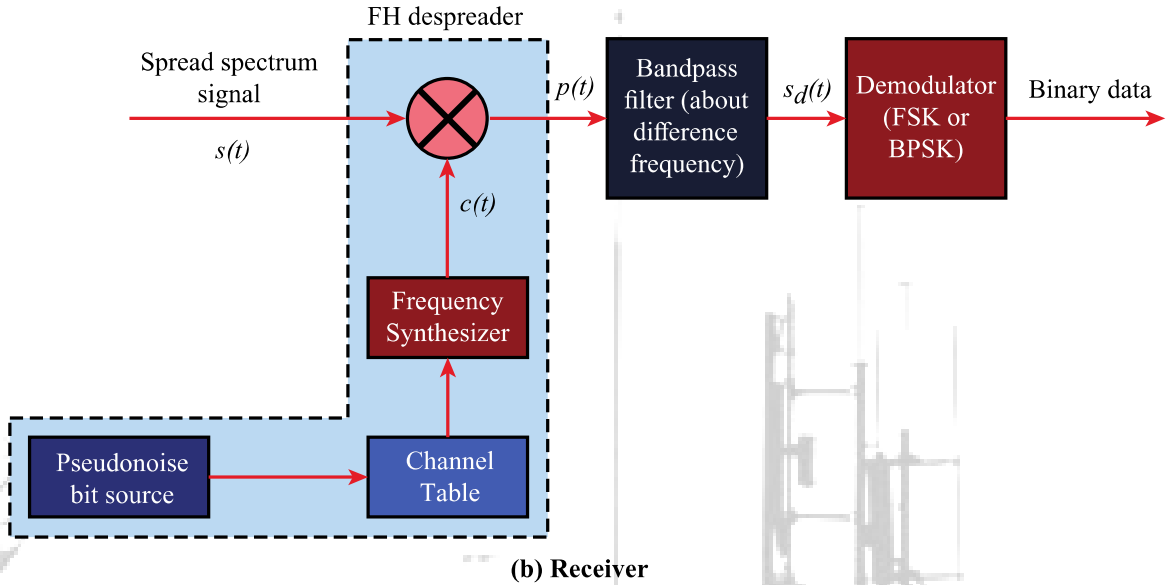
(b) Channel use

Hopping Pattern $=\{f_5, f_8, f_3, f_7, f_1, f_4, f_6, f_2\}$

9.2 FREQUENCY HOPPING EXAMPLE



(a) Transmitter



(b) Receiver

9.3 FREQUENCY HOPPING SPREAD SPECTRUM SYSTEM

GROUP DISCUSSION I – FHSS DATA TRANSMISSION & INTERFERENCE

A system uses FHSS with 4 frequencies:

Hop	Frequency (MHz)
1	902
2	904
3	907
4	909

Jamming is intentional interference that overwhelms a communication signal so that receivers cannot properly detect or decode the message.

The **spreading code** for hopping is: 3 → 1 → 4 → 2 → 3 → ...

Data to transmit: 1 0 1 1 (Each data bit is sent on a hop in order)

- Which carrier frequencies are used for sending the data in different time slots.
- If frequency 904 MHz suffers interference, which bit(s) are lost?
- Why does FHSS limit the effect of interference here?
- Can a hacker access the data if we use FHSS?

CLASS DISCUSSION

Data	Hop	Frequency (MHz)
1	3	907
0	1	902
1	4	909
1	2	904 ❌ jammed

Jammed frequency = **904 MHz** → Only **Bit 4** is affected

- Only one bit lost instead of the entire message
- **Frequency diversity** provides anti-jamming benefit

Advantages:

Attempts to jam signal on one frequency succeed only at knocking out a few bits

Without knowing the **hopping pattern**, a hacker can not access the data.

FHSS PERFORMANCE CONSIDERATIONS

- Large number of frequencies used
- Results in a system that is quite resistant to jamming
  - Jammer must jam all frequencies
  - With fixed power, this reduces the jamming power in any one frequency band

FAST FHSS VS SLOW FHSS

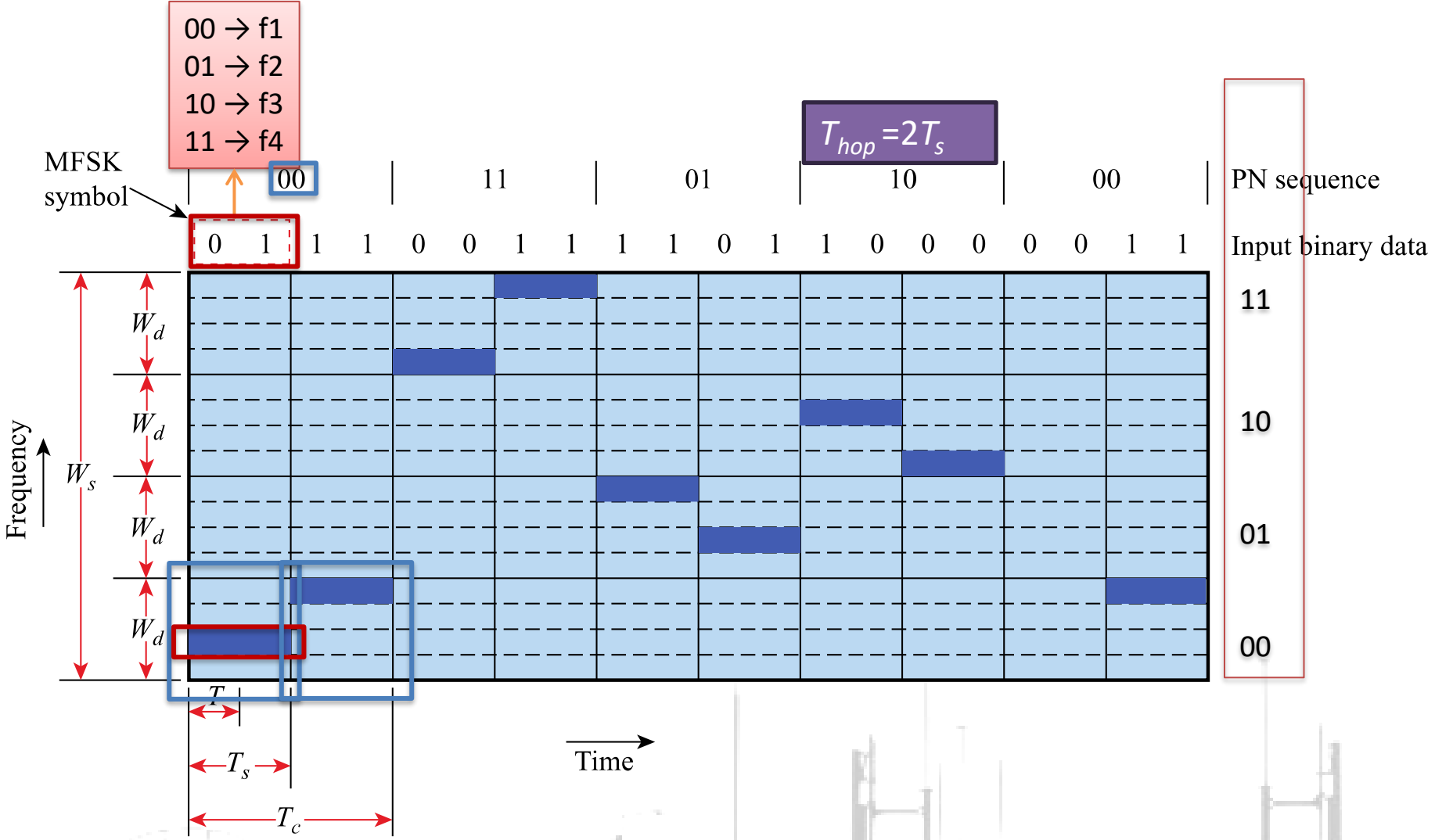
- If carrier frequency changes every T_{hop} seconds and T_s is the duration of a symbol:
  - $T_{hop} \geq T_s$ *:* slow-frequency-hop spread spectrum
  - $T_{hop} < T_s$: fast-frequency-hop spread spectrum

FHSS USING MFSK

- MFSK signal is translated to a new frequency every T_{hop} seconds by modulating the MFSK signal with the FHSS carrier signal
- For data rate of R:
  - duration of a bit: $T = 1/R$ seconds
  - duration of signal element: $T_s = LT$ seconds

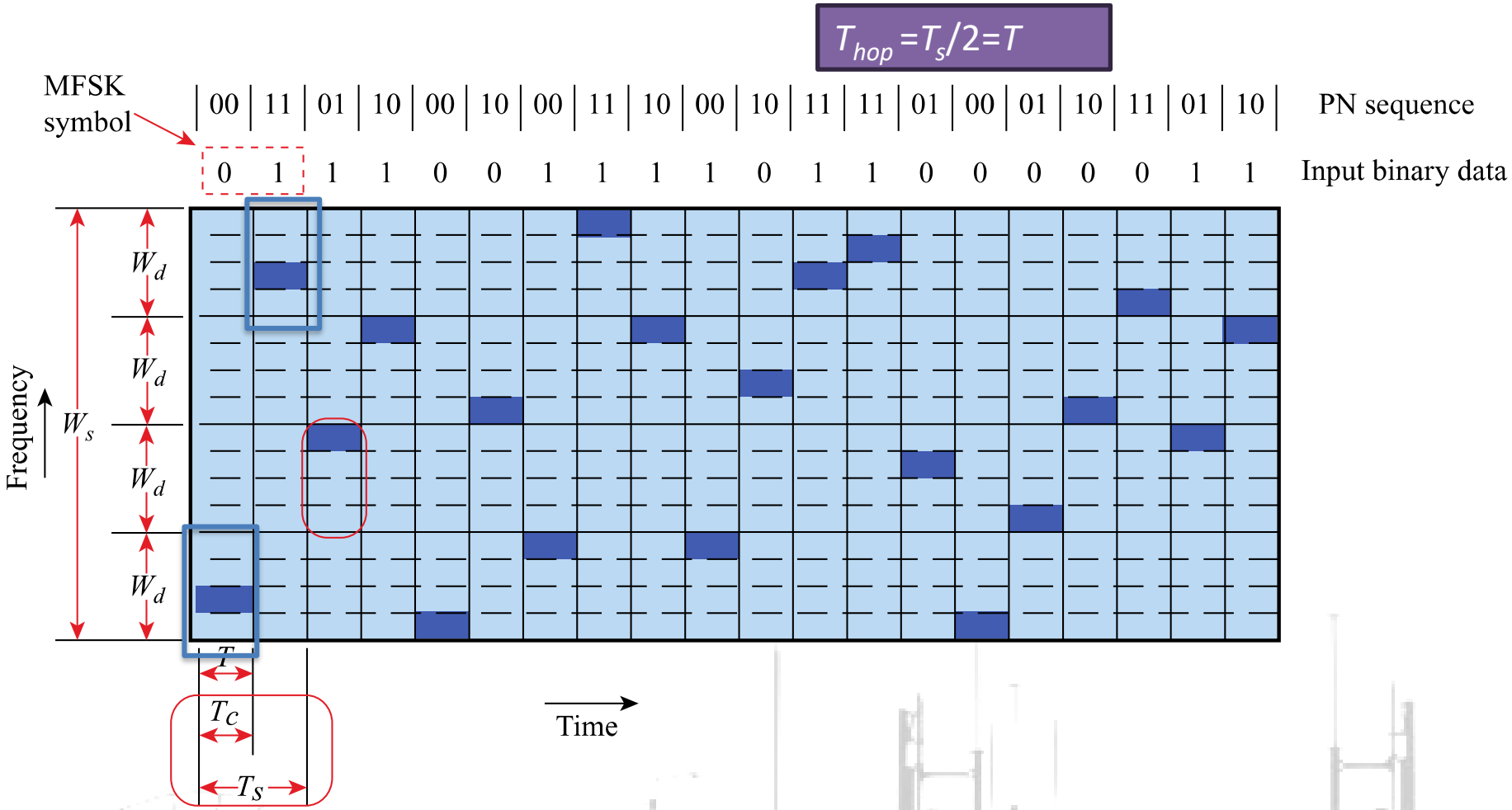
  (**L** = number of bits carried by **one** MFSK symbol; **M = 2^L** different frequencies)

L=2



9.4 SLOW-FREQUENCY-HOP SPREAD SPECTRUM USING MFSK

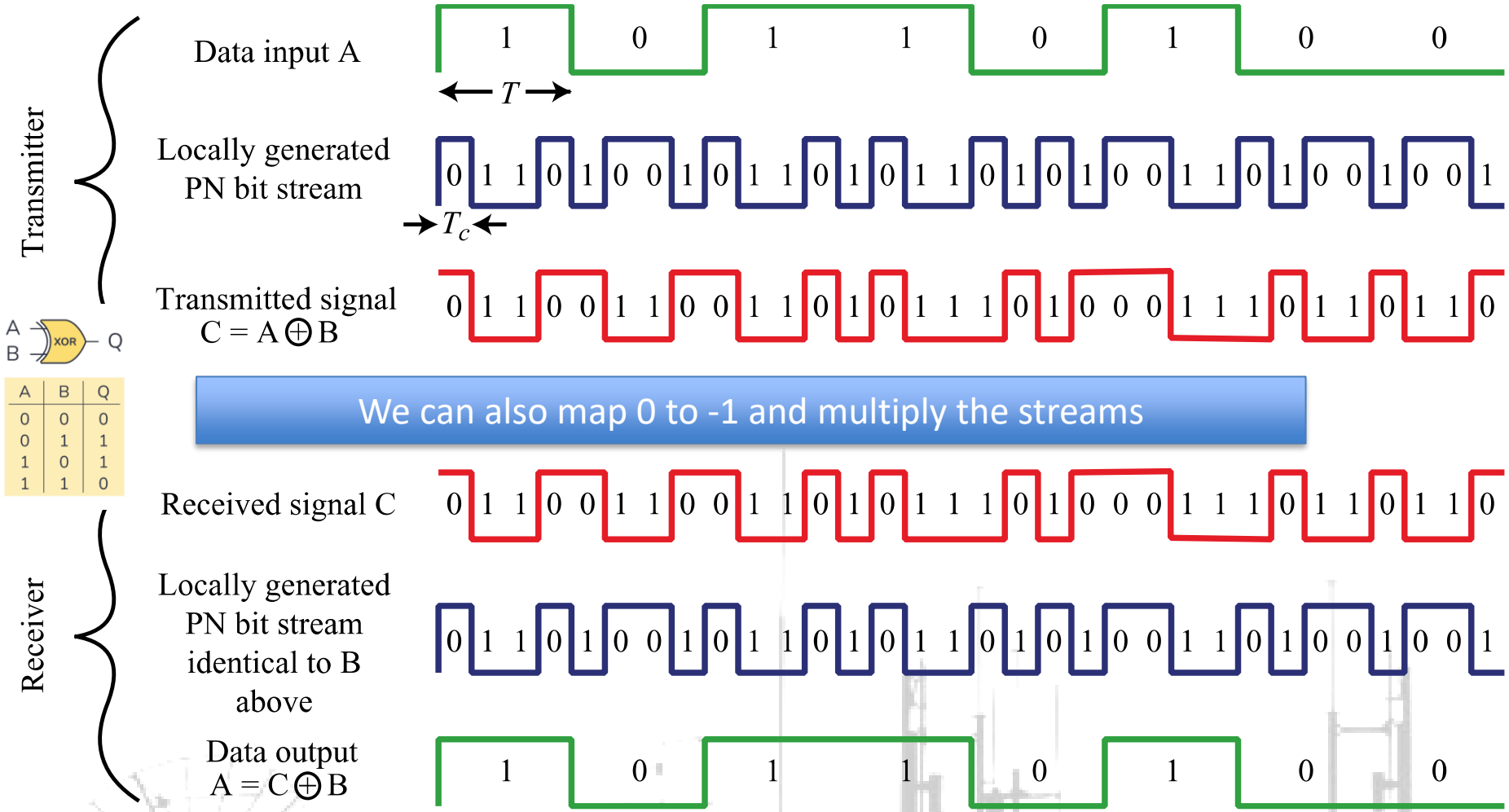
1M = 4, K = 22



9.5 FREQUENCY-HOP SPREAD SPECTRUM USING MFSK 1M = 4, K = 22

DIRECT SEQUENCE SPREAD SPECTRUM (DSSS)

- Each bit in original signal is represented by multiple bits in the transmitted signal
- Spreading code spreads signal across a wider frequency band
  - Spread is in direct proportion to number of bits used
- One technique combines digital information stream with the spreading code bit stream using exclusive-OR (Figure 9.6)



9.6 EXAMPLE OF DIRECT SEQUENCE SPREAD SPECTRUM

DSSS USING BPSK

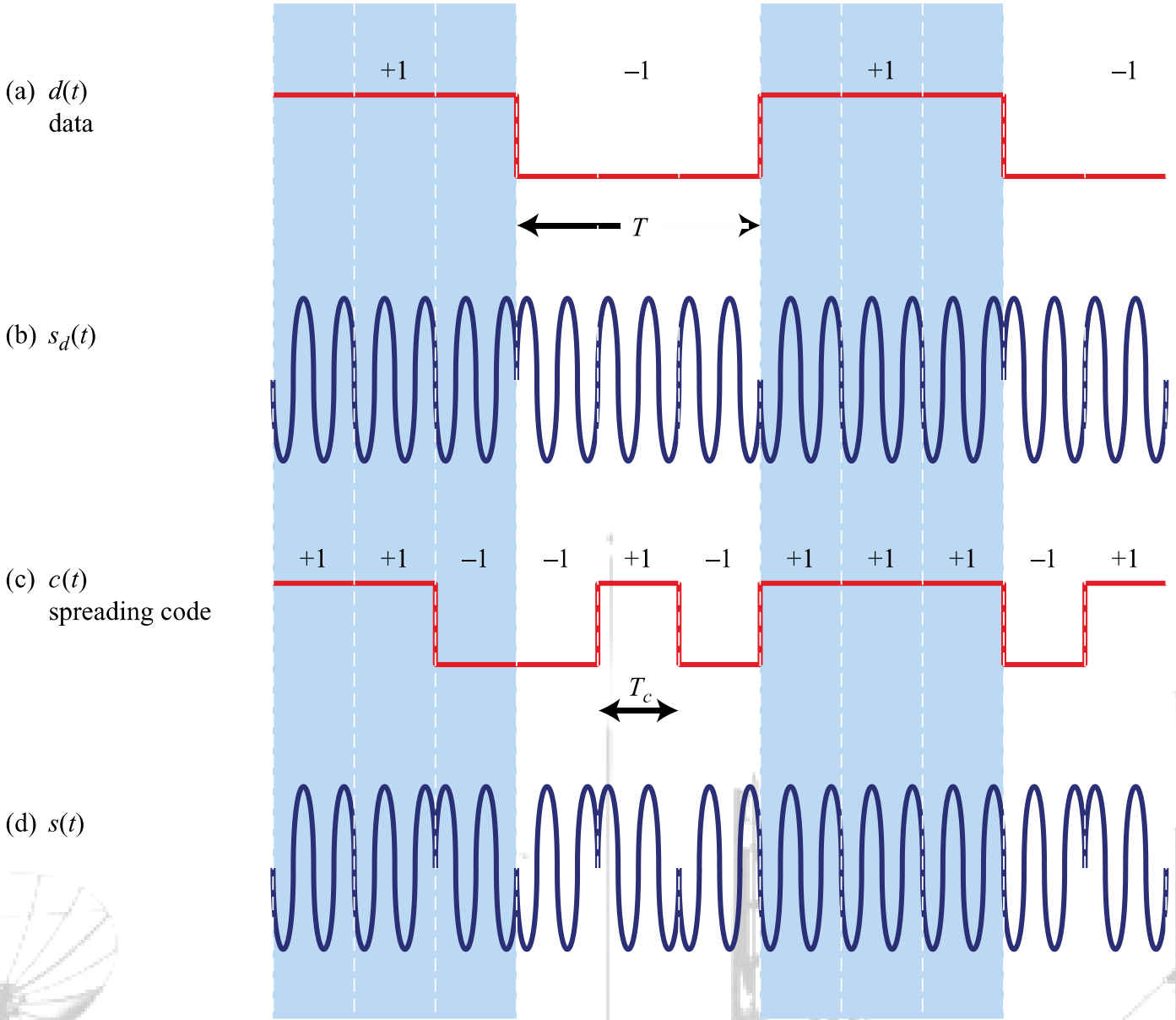
- Multiply BPSK signal,

$$s_d(t) = A\, d(t) \cos(2\,\pi\, f_c t)$$

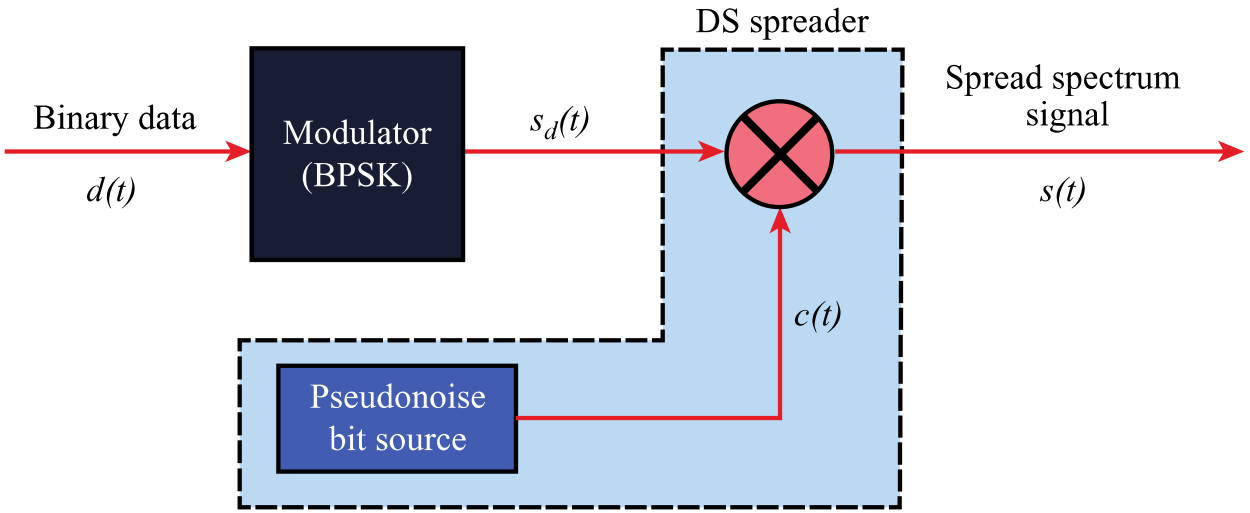
  by $c(t)$ [takes values +1, -1] to get

$$s(t) = A\, d(t)c(t) \cos(2\pi f_c t)$$

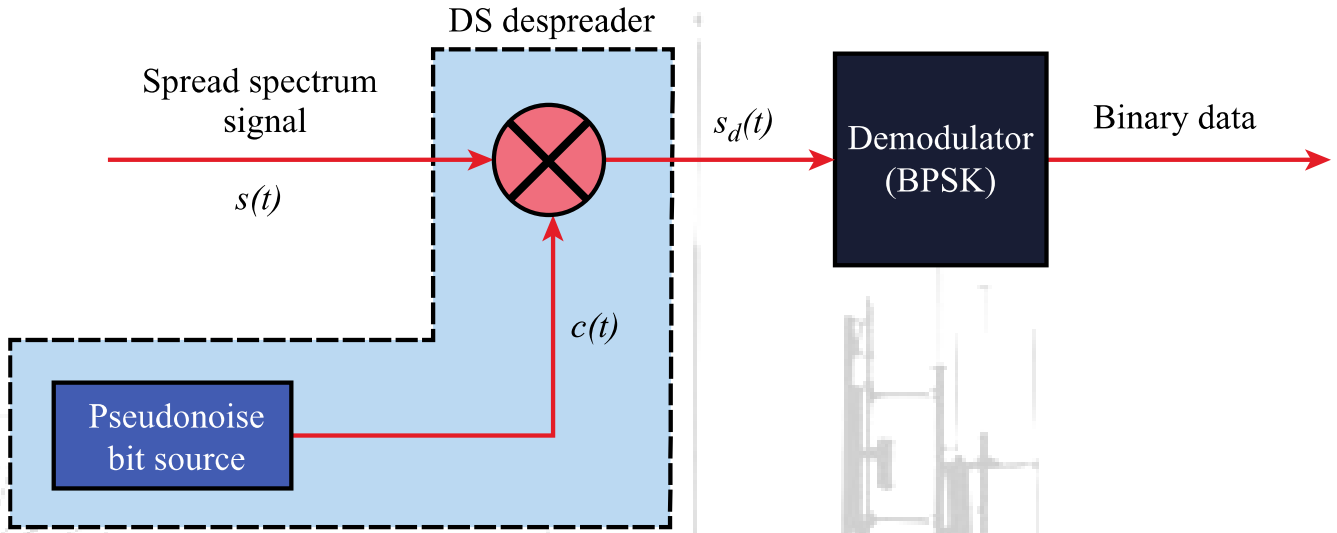
  - A = amplitude of signal
  - f_c = carrier frequency
  - d(t) = discrete function [+1, -1]
- At receiver, incoming signal multiplied by $c(t)$
  - Since, $c(t)$ x $c(t)$ = 1, incoming signal is recovered



9.8 EXAMPLE OF DIRECT SEQUENCE SPREAD SPECTRUM USING BPSK

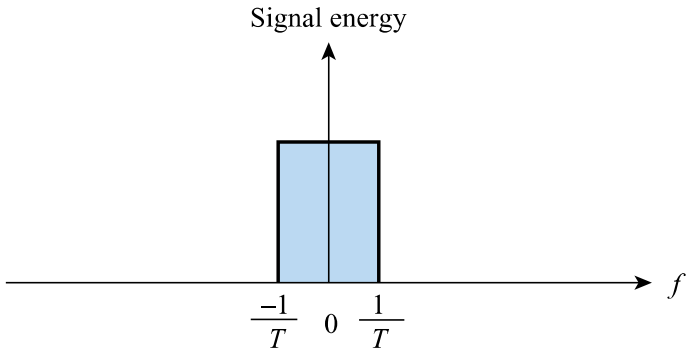


(a) Transmitter

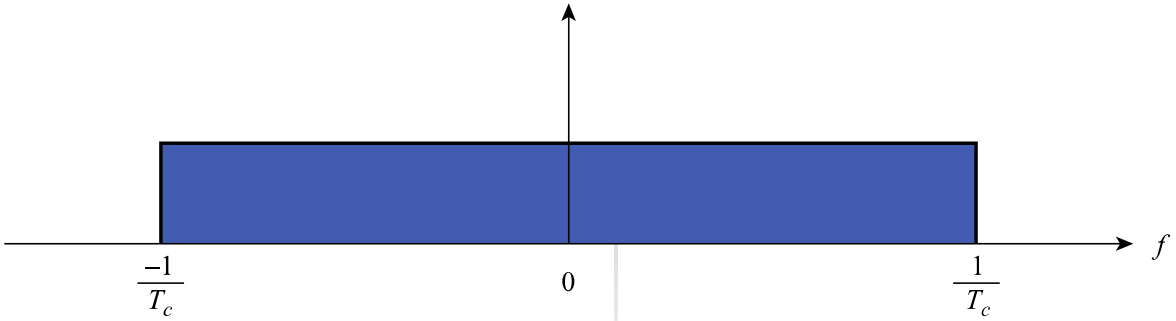


(b) Receiver

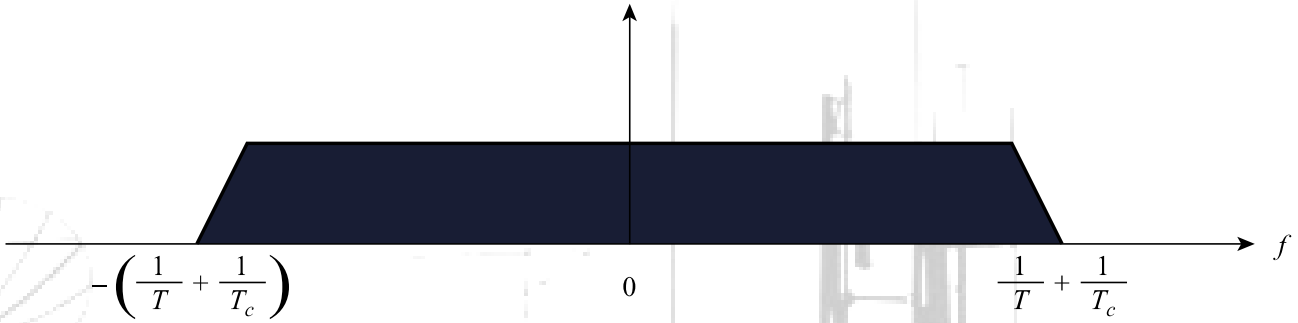
9.7 DIRECT SEQUENCE SPREAD SPECTRUM SYSTEM



(a) Spectrum of data signal



(b) Spectrum of pseudonoise signal



(c) Spectrum of combined signal

9.9 APPROXIMATE SPECTRUM OF DIRECT SEQUENCE SPREAD SPECTRUM SIGNAL

GROUP DISCUSSION II – FHSS VS DSSS: WHICH IS BETTER?

Two main types of Spread Spectrum are:

- **FHSS (Frequency Hopping)** – jumps rapidly between frequencies.
- **DSSS (Direct Sequence)** – spreads bits using a chip code across one wide band.

Discuss:

- Which one do you think works better in a jamming environment? How about Multipath fading and noisy environment? Compare their complexity and also discuss how they can improve the security of communication.

FHSS VS DSSS

- **FHSS:**
  - Good against narrowband interference and jamming.
  - Simpler hardware, used in Bluetooth.
  - Slight delay due to hopping.
- **DSSS:**
  - Stronger against wideband noise and multipath.
  - Used in Wi-Fi (IEEE 802.11b), GPS.
  - Needs precise synchronization.

FHSS = *frequency agility* and simplicity.
DSSS = *continuous robustness* and higher data rates.
Engineers choose based on environment and device complexity.

DSSS HELPS *SEPARATE* MULTIPATH COMPONENTS

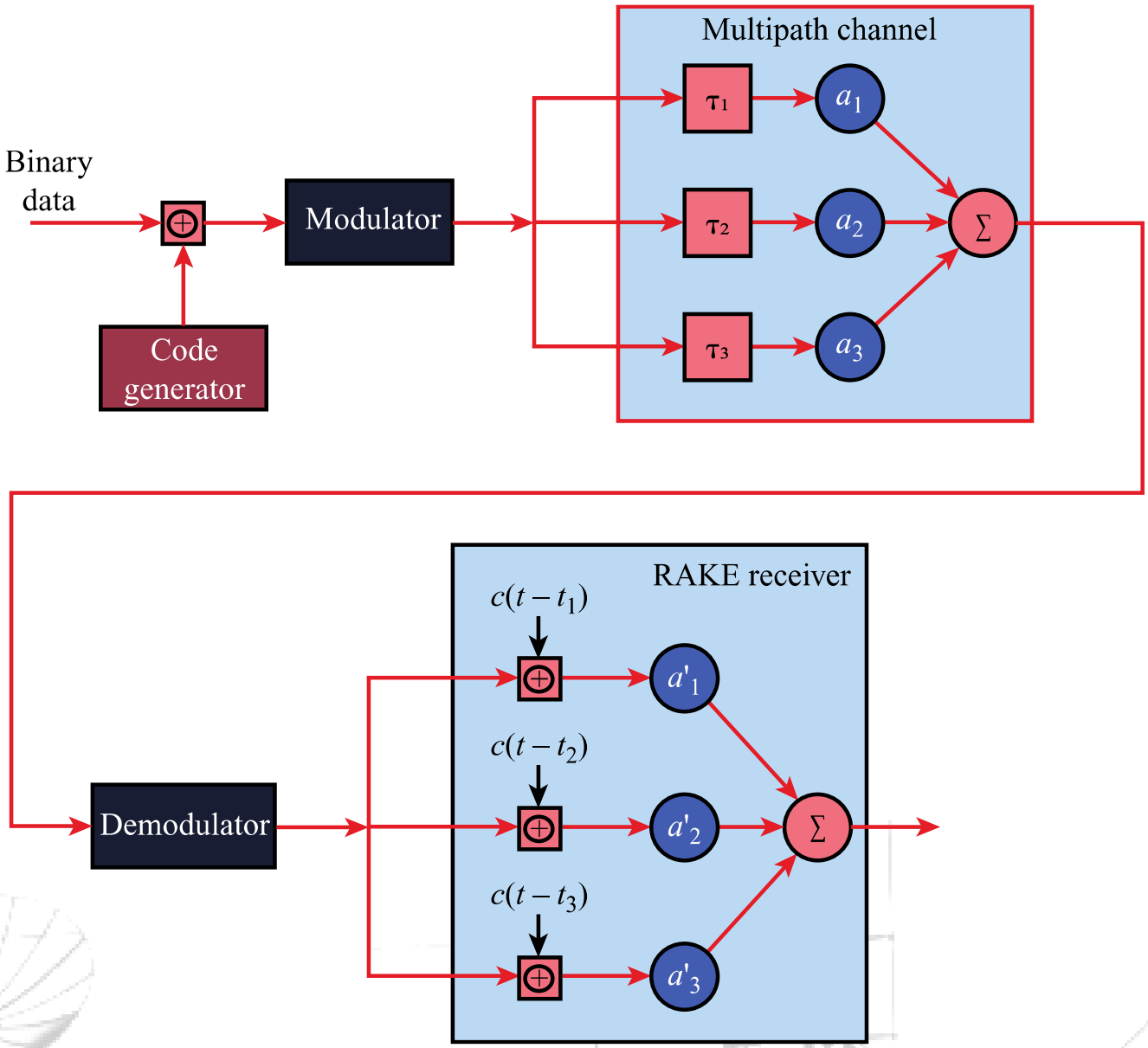
- Signals bounce off buildings, walls, cars → arrive at the receiver:
  - at **different times**
  - with **different strengths**
  - with **different phases**

$$s(t) = \text{a } c(t)\, s_d(t) + a_1 c(t- t_1)\, s_d(t- t_1) + a_2 c(t- t_2)\, s_d(t- t_2) + \ldots.$$

$$\text{As } c(t)c(t)=1 \text{ and } \int c(t)c(t- ti) \approx 0$$

$$\int s(t)\, c(t) = a \int s_d(t) + 0 + 0 + \ldots + 0$$

By correlating the received signal with the spreading code, the primary path aligns and is recovered, while delayed multipath copies are largely suppressed.



9.12 PRINCIPLE OF RAKE RECEIVER

RAKE RECEIVER

Instead of ignoring multipath, RAKE:

- Has **multiple correlators** called **"fingers"**
- Each finger **locks onto** a different path
- Then it **coherently adds** them back together

→ More signal power
→ Better SNR
→ Lower error rate

DSSS + RAKE receiver = turning multipath from a problem into an opportunity!

CODE-DIVISION MULTIPLE ACCESS (CDMA)

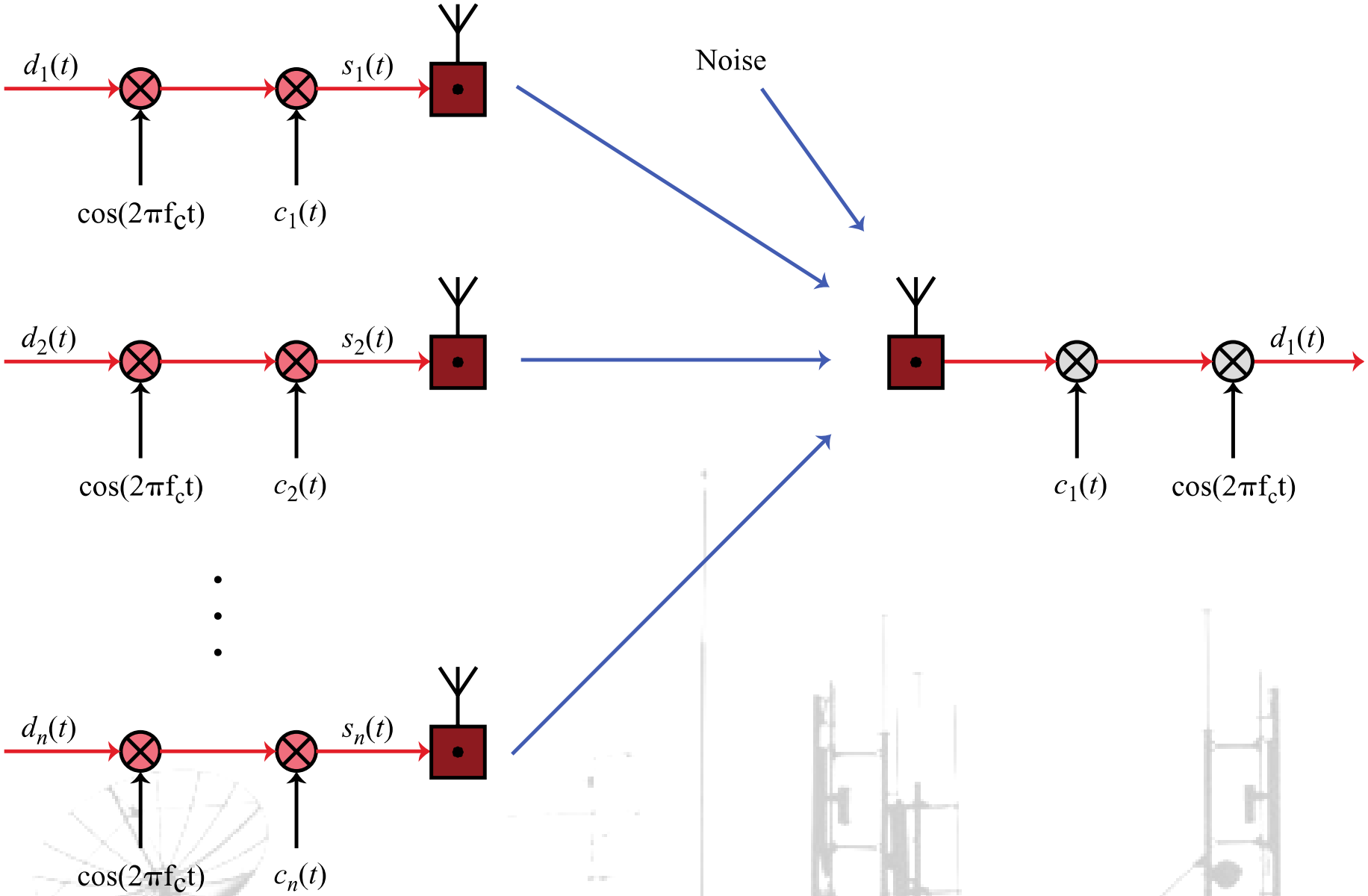
Multiple users share the same frequency band at the same time using unique codes.

- **Unique spreading code per user**
  → A binary pattern known as a **chip sequence**
- **Each data bit is multiplied by the chip sequence**
  → Produces a **spread signal** (chips)
- **Chip rate is higher than data rate**
  → Data rate = **D**
  → Chip rate = **kD** (k = spreading factor)
- **Receiver uses the same code to extract only the intended signal**
  → Other users appear as noise

CDMA EXAMPLE

- If k=6 and code is a sequence of 1s and -1s
  - For a ‘1’ bit, A sends code as chip pattern
    - <c1, c2, c3, c4, c5, c6>
  - For a ‘0’ bit, A sends complement of code
    - <-c1, -c2, -c3, -c4, -c5, -c6>
- Receiver knows sender’s code and performs electronic decode function
  - $\boldsymbol{s}$=<s1, s2, s3, s4, s5, s6> = received signal
  - $\boldsymbol{c}$=<c1, c2, c3, c4, c5, c6> = sender’s code

$$\text{decoded bit} = \begin{cases} 1 & \sum_{i=1}^{k} c_i s_i \geq 0 \\ 0 & otherwise \end{cases}$$



9.11 CDMA IN A DSSS ENVIRONMENT

GROUP DISCUSSION III – CDMA ENCODING & DECODING

Two users share a CDMA channel:

User	Data Bit	Spreading Code
A	1	+1 +1 −1 −1
B	0	+1 −1 +1 −1

$$\text{decoded bit} = \begin{cases} 1 & \sum_{i=1}^{k} c_i s_i \geq 0 \\ 0 & otherwise \end{cases}$$

Mapping: 1 → +1 and 0 → −1

- Encode each user's signal (data × code).
- Add both encoded signals → composite waveform.
- Decode the composite signal for User A and User B using correlation. What bit did each user originally send?
- How does this differ from FDMA and TDMA?

CLASS DISCUSSION

Encoding:

User A: $+1 \times (+1\ +1\ -1\ -1) = +1\ +1\ -1\ -1$

User B: $-1 \times (+1\ -1\ +1\ -1) = -1\ +1\ -1\ +1$

Composite signal: $(+1\ +1\ -1\ -1) + (-1\ +1\ -1\ +1) = (0\ +2\ -2\ 0)$

Decoding:

Correlation with User A's code: $(0)(+1) + (2)(+1) + (-2)(-1) + (0)(-1) = 0 + 2 + 2 + 0 = +4 \rightarrow$ positive $\rightarrow$ bit = 1

Correlation with User B's code: $(0)(+1) + (2)(-1) + (-2)(+1) + (0)(-1) = 0 - 2 - 2 + 0 = -4 \rightarrow$ negative $\rightarrow$ bit = 0

CLASS DISCUSSION

- Unlike FDMA (different frequencies) or TDMA (different time slots), CDMA separates users by **code**.

CDMA enables **simultaneous access** and better **spectrum efficiency** through unique, pseudorandom codes.

WHY SPREAD THE SPECTRUM?

Spread Spectrum intentionally "wastes" bandwidth by transmitting over a much wider range of frequencies.

- Why would engineers do that when spectrum is scarce and expensive?
- What practical advantages does spreading give in wireless communication?

Consider both FHSS and DSSS.

WHY SPREAD THE SPECTRUM?

- **Interference & Jamming Resistance**
  - If a jammer or another device interferes on one frequency,
  - The spread signal is still mostly unaffected (especially in **FHSS**, which simply hops away from interference)
  - ➞ Communication remains reliable even in hostile environments.

- **Multipath Fading Improvement (DSSS)**
  - Wireless signals bounce off objects and create multiple delayed copies
  - DSSS uses RAKE receivers to **combine** multipath energy instead of suffering from it
  - ➞ Better performance in cities and indoors.

WHY SPREAD THE SPECTRUM?

- **Security & Low Probability of Detection**
  - Without knowing the spreading code, the signal looks like **random noise**
  - Hard to intercept or jam intentionally
  - ➞ Used heavily in military systems and GPS.
- **Multiple Access Capability (CDMA)**
  - Users share the same frequency band using **different spreading codes**
  - Separation in code domain reduces collisions
  - ➞ Increases system capacity (e.g., 3G networks).

Spread Spectrum trades bandwidth for **robustness, security, and capacity** — it's a smart "waste" of spectrum.

CATEGORIES OF SPREADING SEQUENCES

- Spreading Sequence Categories
  - PN sequences
  - Orthogonal codes
- For FHSS systems
  - PN sequences most common
- For DSSS systems not employing CDMA
  - PN sequences most common
- For DSSS CDMA systems
  - PN sequences
  - Orthogonal codes

PN SEQUENCES

- PN Sequences
  - Generated by an **algorithm** using initial **seed**
  - Sequence isn't statistically random but will pass many test of randomness
  - Sequences referred to as **pseudorandom** numbers or pseudonoise sequences
  - Unless **algorithm** and **seed** are known, the sequence is impractical to predict

QUESTIONS?