# 展頻通訊
# (Spread Spectrum Communications)

國立清華大學電機系暨通訊工程研究所
蔡育仁
台達館 821 室
Tel: 62210
E-mail: yrtsai@ee.nthu.edu.tw



# Chapter 2
# Spread-Spectrum Systems

# Contents

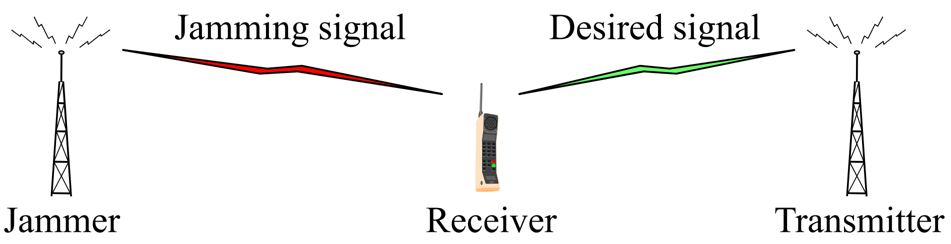
- Pulse-Noise Jamming
- Low Probability of Detection
- BPSK Direct-Sequence Spread Spectrum
- Interference Rejection
- QPSK Direct-Sequence Spread Spectrum
- Frequency-Hop Spread Spectrum
- Bluetooth Wireless Technology
- Hybrid DS/FH Spread Spectrum
- LoRa Chirp Spread Spectrum
- Spread Spectrum Advantages
- ISM Band Regulations



# Pulse-Noise Jamming Problem

# Pulse-Noise Jamming

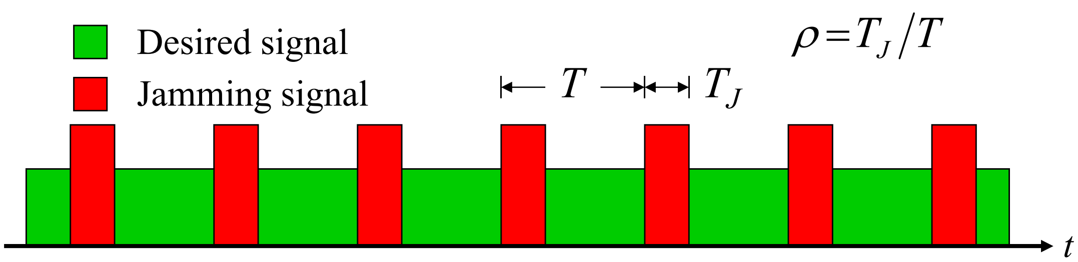
- A pulse-noise **jammer** transmits pulses of
  - Band-limited white Gaussian noise
  - Have an average power ***J*** referred to the receiver front-end
- The jammer may choose
  - The **center frequency** and **bandwidth** identical to the signal
  - The pulse duty factor $\boldsymbol{\rho}$ to cause the **maximum degradation** while maintaining a **constant average transmitted power *J***






# Pulse-Noise Jamming (Cont.)

- How to choose the **optimal** pulse duty factor $\rho$ ?
  - The average jamming power $J$ (power resource) is limited
  - For a **large** (**small**) duty factor $\rho$, we have
    - Low (High) jammer power spectral density
    - Long (Short) jamming duration
  - If the jammer power spectral density is too low, there will be **no critical damage** to the desired signal



## Pulse-Noise Jamming (Cont.)

- Consider a coherent BPSK communication system
  - The bit error probability is

$$P_E = Q\left(\sqrt{\frac{2E_b}{N_0}}\right)$$

  - The jammer increases the receiver noise power spectral density from $N_0$ to $N_0 + N_J/\rho$, where
    - $N_J = J/W$: the one-sided average jammer power spectral density
    - $W$: the one-sided transmission bandwidth
- The average bit error probability is

$$\overline{P_E} = (1-\rho)Q\left(\sqrt{\frac{2E_b}{N_0}}\right) + \rho Q\left(\sqrt{\frac{2E_b}{N_0 + N_J/\rho}}\right)$$



## Optimal Pulse-Noise Jamming

- The jammer chooses $\rho$ to **maximize** $\overline{P_E}$
- When a system is designed to operate in a jamming environment, the **maximum transmitter power is used**
  - The receiver front-end thermal noise $N_0$ can be neglected
  - The average bit error probability can be approximated as

$$\overline{P_E} \approx \rho Q\left(\sqrt{\frac{2E_b\rho}{N_J}}\right)$$

- The $Q$-function can be bounded by an exponential function

$$\overline{P_E} \le \frac{\rho}{\sqrt{4\pi E_b \rho / N_J}} e^{-E_b\rho/N_J}$$

# Optimal Pulse-Noise Jamming (Cont.)

- Find $\rho$ that **maximizes** the error probability function
  - $\rho = N_J / 2E_b$

$$\overline{P}_{E,\max} = \frac{1}{\sqrt{2\pi e}} \frac{1}{2E_b / N_J}$$

Let $\overline{P}_E = \frac{\rho}{\sqrt{4\pi E_b \rho / N_J}} e^{-E_b \rho / N_J} = \alpha \rho^{1/2} e^{-E_b \rho / N_J}$, $\alpha = \frac{1}{\sqrt{4\pi E_b / N_J}}$

$$\frac{d\overline{P}_E}{d\rho} = \alpha \left[ \frac{1}{2} \rho^{-1/2} - \frac{E_b}{N_J} \rho^{1/2} \right] e^{-E_b \rho / N_J}$$

$$\alpha \left[ \frac{1}{2} \rho^{-1/2} - \frac{E_b}{N_J} \rho^{1/2} \right] e^{-E_b \rho / N_J} = 0$$

$$\Rightarrow \rho = \frac{N_J}{2E_b}$$

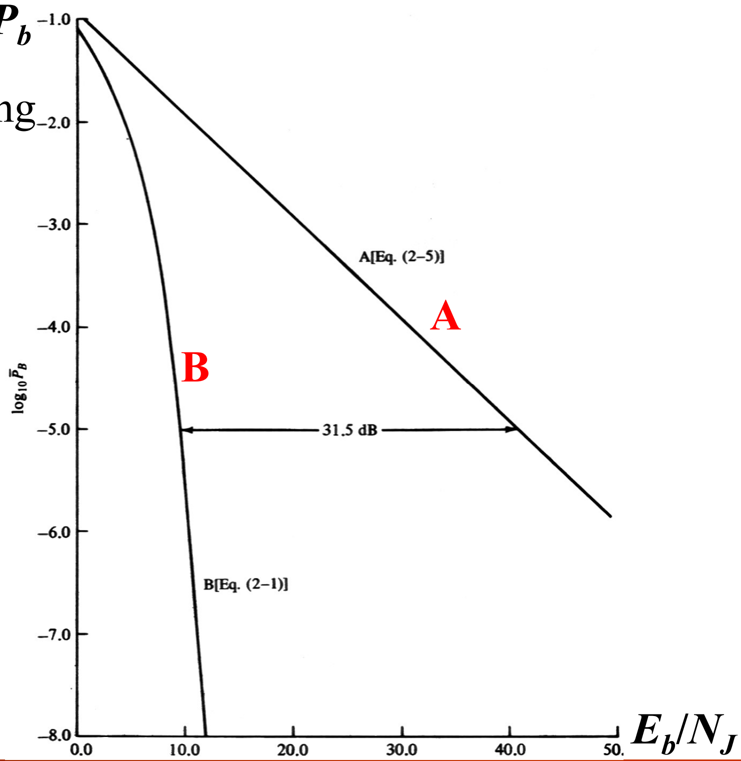


# Pulse-Noise Jamming Performance

- The **exponential** dependence of bit error probability on the signal-to-noise ratio has been replaced by an **inverse linear** relationship
- The **optimized** pulse noise jammer causes a degradation of approximately **31.5 dB** relative to **continuous jamming** at a bit error probability of $\mathbf{10^{-5}}$
- The severe degradation can be largely eliminated by using a combination of **spread-spectrum** techniques and **forward error correction coding** (including the interleaving technique)
- In order to cause maximum degradation, the jammer must **know** the value of $E_b/N_J$ at the receiver
  - It is very difficult, so that the result is a **worst-case** scenario

# Pulse-Noise Jamming Performance (Cont.)

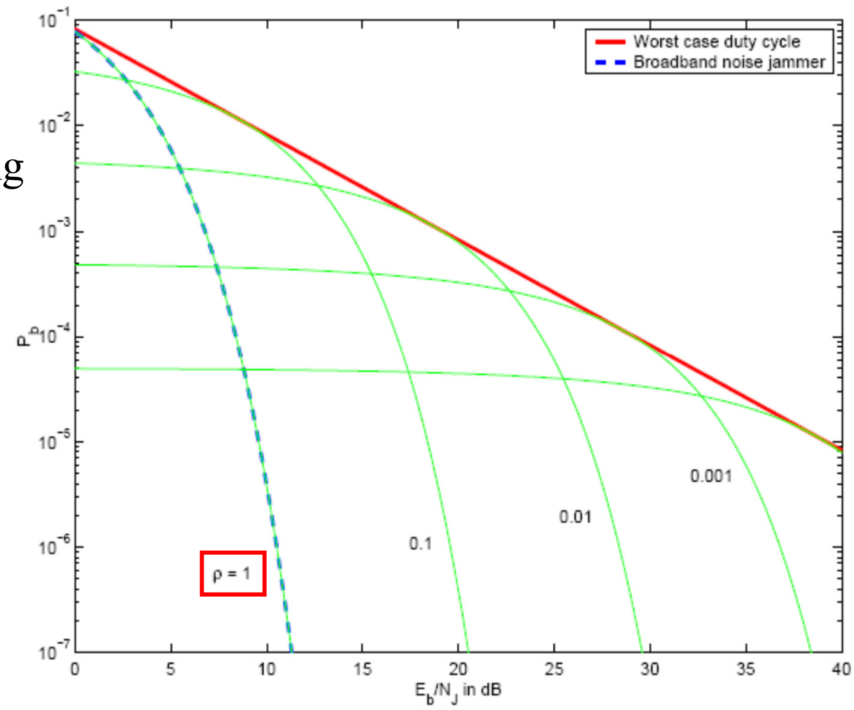
- **A**: worst-case pulse-noise jamming
- **B**: continuous-noise jamming
- Without applying SS, it is highly possible that the system operates in an environment with a very low $E_b/N_J$.






# Pulse-Noise Jamming Performance (Cont.)

- Without diversity and channel coding




Source: E. Strom, T. Ottosson, and A. Svensson, CHALMERS University of Technology

# Low Probability of Detection

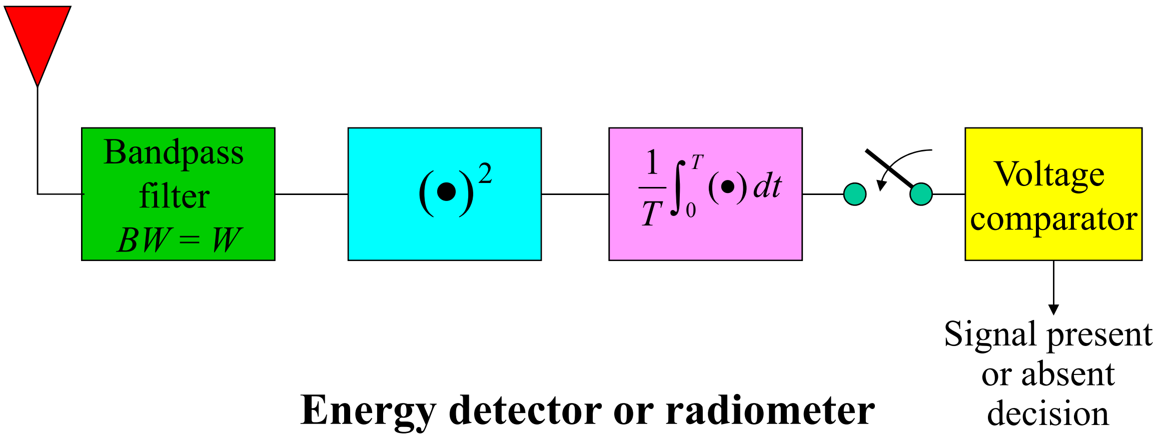


# Low Probability of Detection

- **Low-probability-of-detection** (LPD) communication systems are designed to make their detection **as difficult as possible** by **anyone** but the intended receiver
  - The **minimum signal power** required to achieved a particular receiving performance is used
  - **Spread spectrum** techniques can significantly aid in achieving this goal
- Assume that the detector is using a **radiometer** which detects signal energy received in a bandwidth $W$
  - Filtering this bandwidth
  - Squaring the output of this filter (Taking the signal power)
  - Integrating the output of the squarer for a time duration $T$

# Low Probability of Detection (Cont.)

– Comparing the output with a **predetermined threshold**
  - Above the threshold: the signal is **present**
  - Otherwise: the signal is **absent**




**Energy detector or radiometer**



# Low Probability of Detection (Cont.)

- The probability of detecting the signal if it is **indeed present**: $P_d$ (depending on the desired signal and noise)
- The probability of falsely declaring a detection when **noise alone** is present: $P_{fa}$ (depending only on noise)
- The probability of detecting the signal:

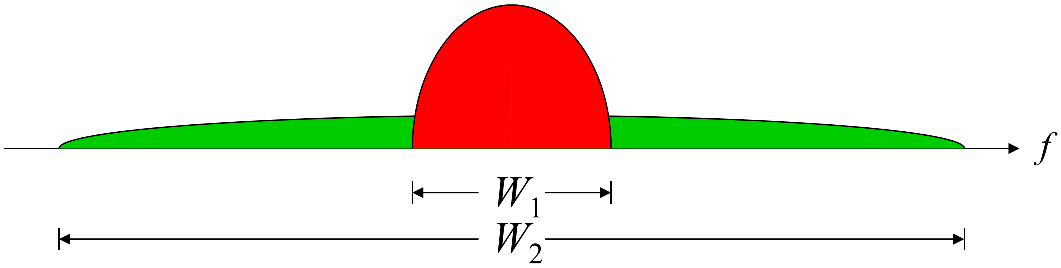
$$P_d = \Phi\left\{\left[\frac{P}{N_0}\sqrt{\frac{T}{W}} - \Phi^{-1}(1 - P_{fa})\right]\right\}$$

– where

$$\Phi(y) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{y} \exp\left(-\frac{1}{2}\zeta^2\right) d\zeta$$

# Low Probability of Detection (Cont.)

- For a fixed $P_{fa}$, the probability of detection can be made smaller by:
  - **Reducing $P/N_0$**, or
    - However, this will degrade the receiving performance
  - **Increasing $W$**
    - Reduce the detecting probability for a **fixed SNR**
- $W$ can be increased by using spread-spectrum techniques






# BPSK Direct-Sequence Spread Spectrum

# Direct-Sequence Spread Spectrum (DSSS)

- Direct-sequence spread spectrum (DSSS): Bandwidth spreading is accomplished by **direct modulation** of a data-modulated carrier by **a wideband spreading signal** (or a spreading code)
- The spreading signal is chosen to have some properties:
  - For the **intended** receiver
    - It facilitates the demodulation
  - For other **unintended** receivers
    - The demodulation is as difficult as possible



# BPSK DSSS

- The simplest form of DSSS employs **binary phase-shift keying** (BPSK) as the spreading modulation
- Consider a constant-envelope data-modulated carrier having the power $P$, the radian frequency $\omega_0$, and the data modulation phase $\theta_d(t)$

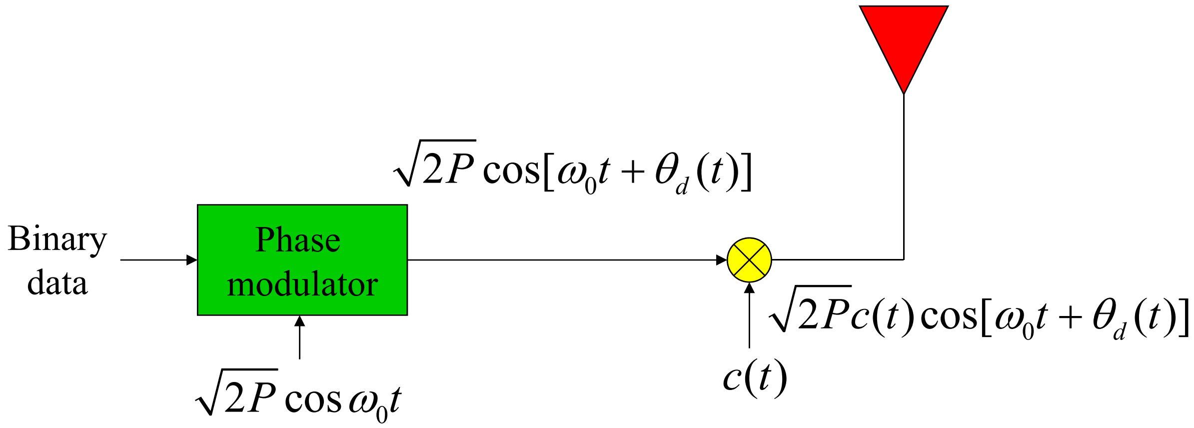
$$s_d(t) = \sqrt{2P}\cos\left[\omega_0 t + \theta_d(t)\right]$$

- A signal occupies a bandwidth typically between
  - one-half and twice (1.5 ~ 2) the data rate prior to DS spreading

# BPSK DSSS – Transmitter

- BPSK spreading is accomplished by multiplying $s_d(t)$ by a function $c(t)$, which represents the spreading waveform

$$s_t(t) = \sqrt{2P}c(t)\cos[\omega_0 t + \theta_d(t)]$$

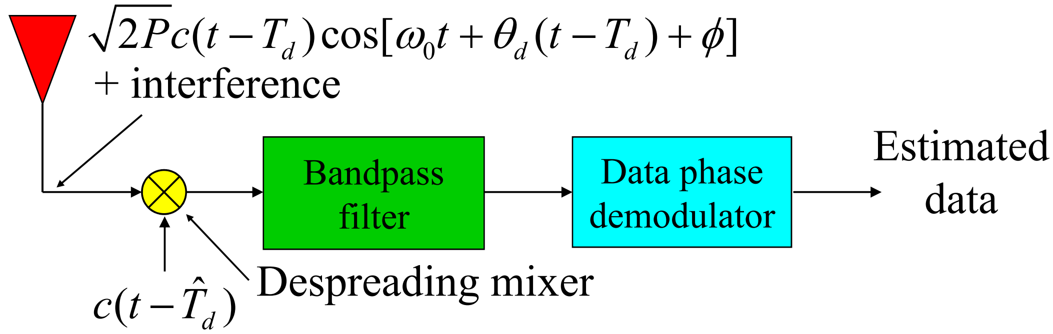



**BPSK direct-sequence spread-spectrum transmitter**



# BPSK DSSS – Receiver

- Assume that the signal is transmitted via a distortionless channel with a transmission delay $T_d$
- **Demodulation** is accomplished in part by **re-modulating** the received signal with the spreading code appropriately delayed
  - This is called despreading process




**BPSK direct-sequence spread-spectrum receiver**

# BPSK DSSS – Receiver (Cont.)

- The signal component of the output of the despreading mixer is

$$s_{ds}(t) = \sqrt{2P}c\left(t - T_d\right)c\left(t - \hat{T}_d\right)\cos\left[\omega_0 t + \theta_d(t - T_d) + \phi\right]$$

  - $\hat{T}_d$ is the receiver's best estimate of the transmission delay
  - $c(t) = \pm 1$
    - If $\hat{T}_d = T_d$, $c(t - T_d) \times c(t - \hat{T}_d) = 1$
- When **correctly synchronized**, the output is equal to $s_d(t)$ except for a random phase $\phi$, and $s_d(t)$ can be demodulated

$$s_{ds}(t) = \sqrt{2P}\cos\left[\omega_0 t + \theta_d(t - T_d) + \phi\right]$$



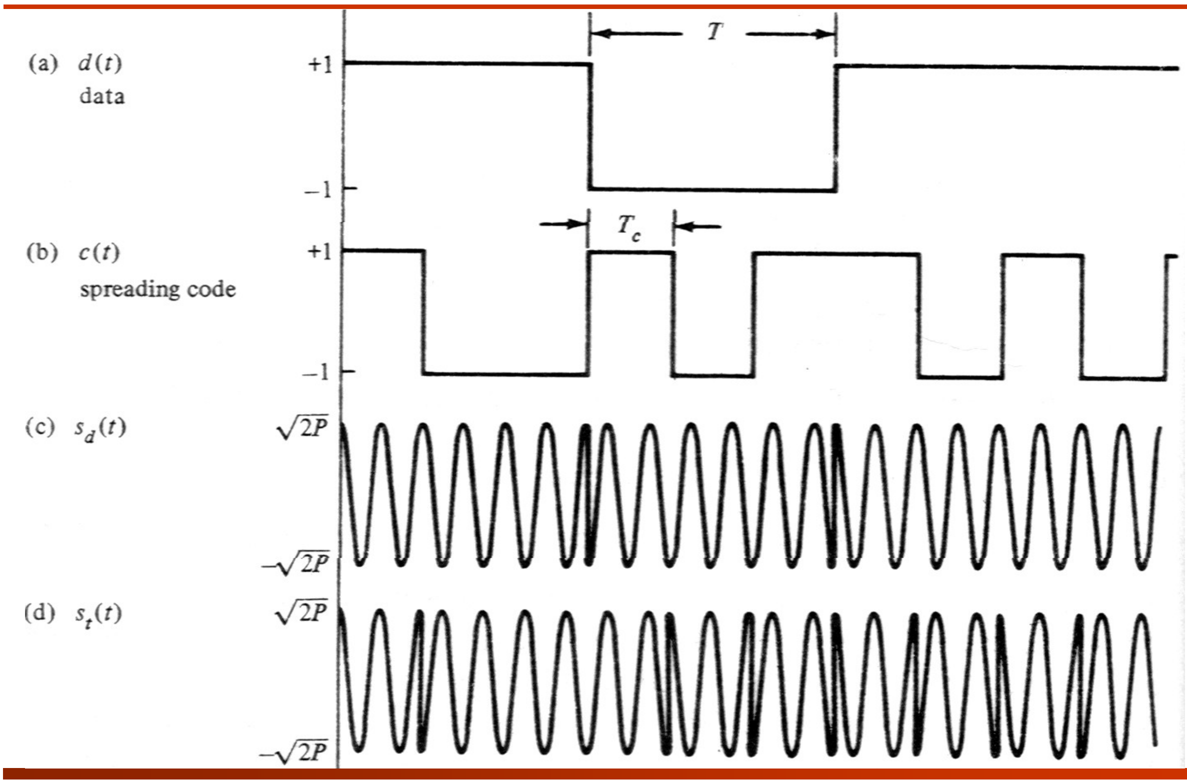
# BPSK DSSS – Receiver (Cont.)

- There is **no restriction** on the form of $\theta_d(t)$, the data modulation **does not** also have to be BPSK
- If BPSK is used for both data modulation and spreading modulation
  - $d(t) = \pm 1$

$$s_d(t) = \sqrt{2P}d(t)\cos\omega_0 t$$

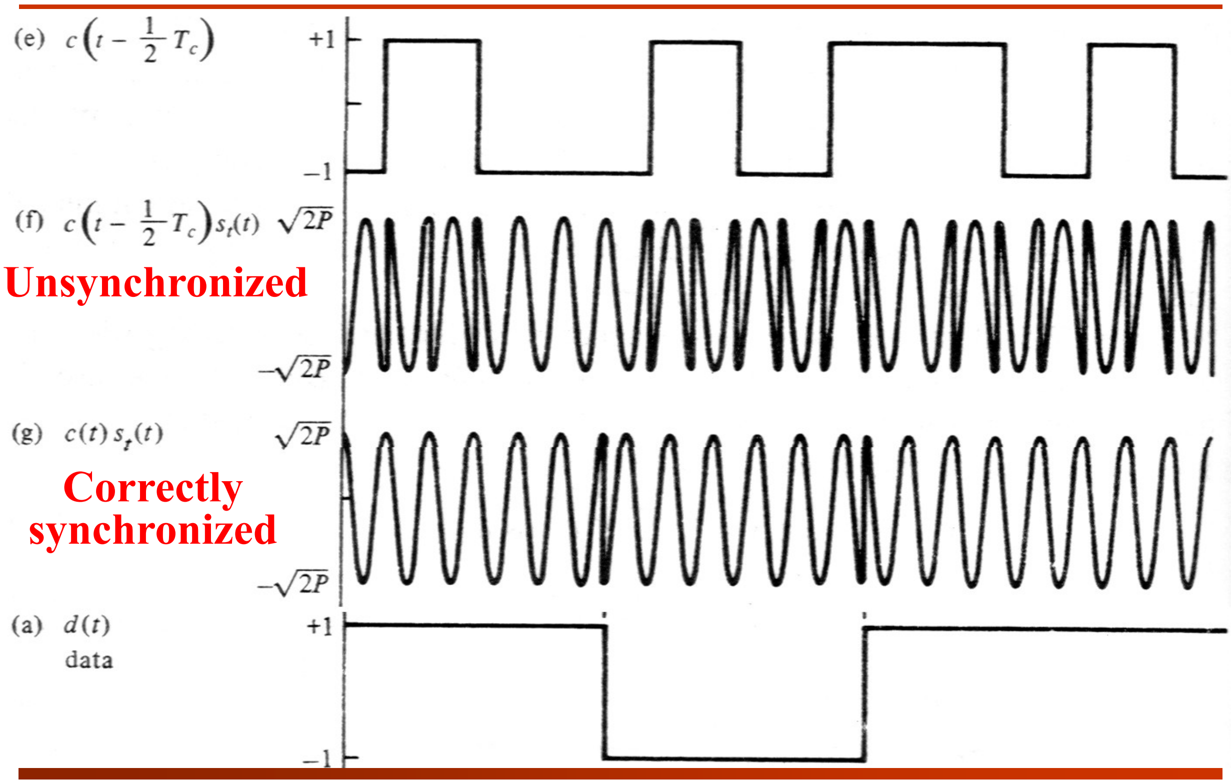
$$s_t(t) = \sqrt{2P}d(t)c(t)\cos\omega_0 t$$

# BPSK DSSS (Cont.)






# BPSK DSSS (Cont.)



# Example

‘0’ → + 1; ‘1’ → – 1
0 + 0 = 0; 0 + 1 = 1; 1 + 0 = 1; 1 + 1 = 0;

| | | | | | |
|---|---|---|---|---|---|
| Input Data $d(t)$ | **1** | **0** | **1** | **1** | **0** |
| Spreading Code $c(t)$ | 1001011 | 1001011 | 1001011 | 1001011 | 1001011 |
| DSSS Signal $s_t(t)$ | 0110100 | 1001011 | 0110100 | 0110100 | 1001011 |
| | Channel | | | | |
| Received $s_r(t)$ | 0110100 | 1001011 | 0110100 | 0110100 | 1001011 |
| Despreading Code $c(t)$ | 1001011 | 1001011 | 1001011 | 1001011 | 1001011 |
| Signal After Despreading | 1111111 | 0000000 | 1111111 | 1111111 | 0000000 |
| Estimated Data $d'(t)$ | **1** | **0** | **1** | **1** | **0** |



# Power Spectral Density of DSSS

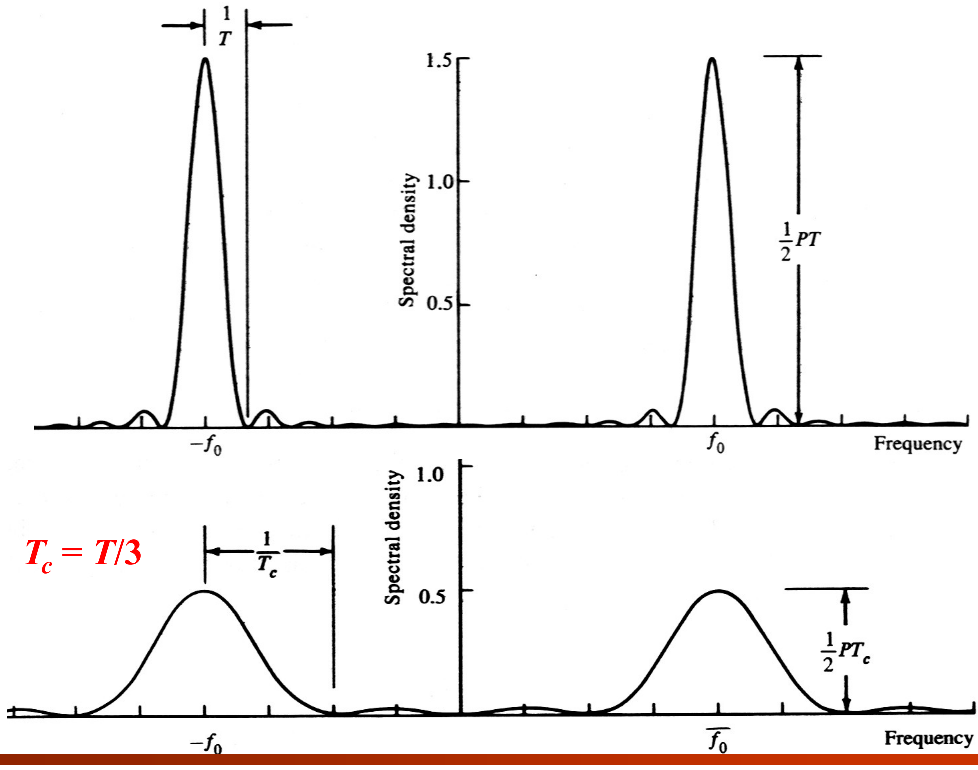
- Assume that both the data modulation and spreading modulation are binary phase-shift keying
- Consider the power spectra of the signals:
  - The two-sided power spectral density of a BPSK carrier $s_d(t)$ with data symbol duration ***T*** is

$$S_d(f) = \frac{1}{2} PT \left\{ \text{sinc}^2\left[ (f - f_0) T \right] + \text{sinc}^2\left[ (f + f_0) T \right] \right\}$$

  - The two-sided power spectral density of DSSS signal $s_t(t)$
    - It is also a binary phase-shift-keyed carrier with spreading code symbol duration $\boldsymbol{T_c}$ ($T \rightarrow T_c$)
    - $T_c$ is often referred to as a spreading code **chip duration**

$$S_t(f) = \frac{1}{2} PT_c \left\{ \text{sinc}^2\left[ (f - f_0) T_c \right] + \text{sinc}^2\left[ (f + f_0) T_c \right] \right\}$$

# Power Spectral Density of DSSS (Cont.)






# Power Spectral Density of DSSS (Cont.)

- The effect of the modulation by a spreading code is to
  - To spread the bandwidth of the transmitted signal by a factor of $N$ $\quad N = T/T_c$
  - To reduce the level of the PSD by a factor of $N$
- If the data modulation is an arbitrary **constant-envelope** phase modulation
  - The power spectral density and the **autocorrelation** function of a signal are a **Fourier transform pair**
- Because the signal $s_d(t)$ is independent of $c(t)$:

$$R_t(\tau) = R_d(\tau) R_c(\tau)$$

- The Fourier transform pair of $R_t(t)$ is

$$S_t(f) = \int_{-\infty}^{\infty} S_d(f') S_c(f - f')\, df'$$

# Autocorrelation & Power Spectrum of $c(t)$

- The autocorrelation function of spreading code $c(t)$:

$$R_c(\tau) = \lim_{A\to\infty} \frac{1}{2A}\int_{-A}^{A} c(t')c(t'-\tau)\,dt'$$

  - For $\tau = 0$: the integral is equal to **1.0** since $c^2(t) = 1.0$
  - For $\tau \geq T_c$: the integral is **zero** if the code is an infinite sequence of independent random binary digits
  - For $0 < \tau < T_c$:

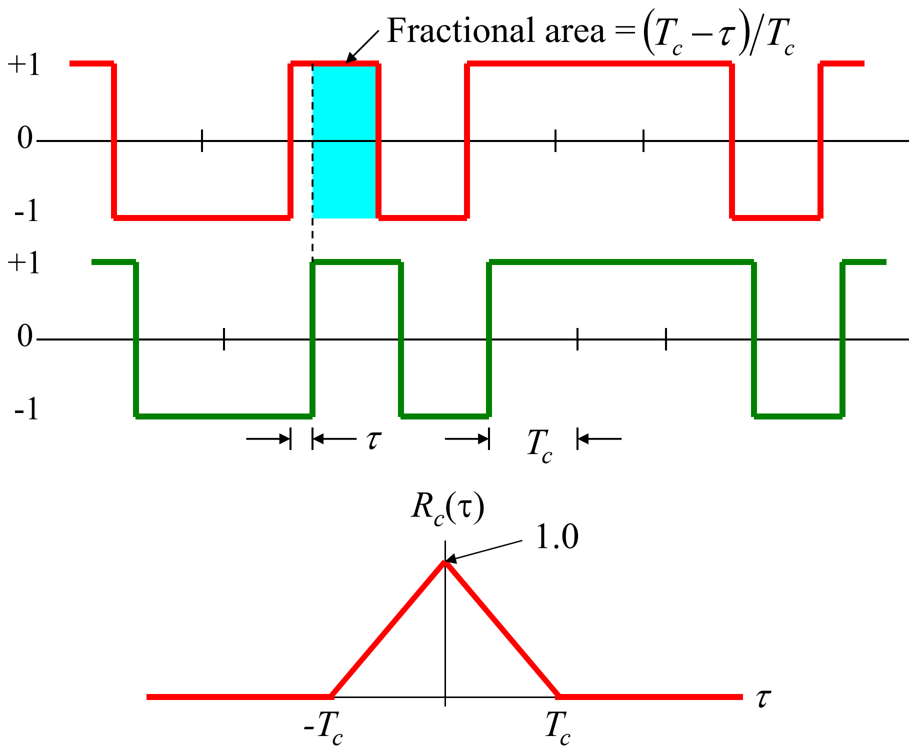
$$R_c(\tau) = \begin{cases} 1 - \dfrac{|\tau|}{T_c}, & |\tau| < T_c \\ 0, & |\tau| \geq T_c \end{cases}$$

- The Fourier transform of this **triangular waveform** $R_c(\tau)$ is

$$S_c(f) = T_c\,\mathrm{sinc}^2(fT_c)$$



# Autocorrelation & Power Spectrum of $c(t)$ (Cont.)



# Power Spectral Density of $s_t(t)$

- Assume that the spreading code chip rate is **100** times the data rate

$$S_c(f) = T_c \,\text{sinc}^2\left(fT_c\right) = \frac{T}{100}\text{sinc}^2\left(fT/100\right)$$

$$S_t(f) = \int_{-\infty}^{\infty} \frac{1}{2} PT \,\text{sinc}^2\left[\left(f' - f_0\right)T\right] \times \frac{T}{100}\text{sinc}^2\left[\left(f - f'\right)T/100\right] df'$$

$$+ \int_{-\infty}^{\infty} \frac{1}{2} PT \,\text{sinc}^2\left[\left(f' + f_0\right)T\right] \times \frac{T}{100}\text{sinc}^2\left[\left(f - f'\right)T/100\right] df'$$

- Because the spreading chip is much larger than the data rate
  - The **second sinc** function in each integral is approximately **constant** over the range of significant values of the **first sinc** function (i.e., around $f' = f_0$ and $f' = -f_0$)
  - $\text{sinc}^2[(f \pm f')T/100] \approx \text{sinc}^2[(f \pm f_0)T/100]$ for all $f'$

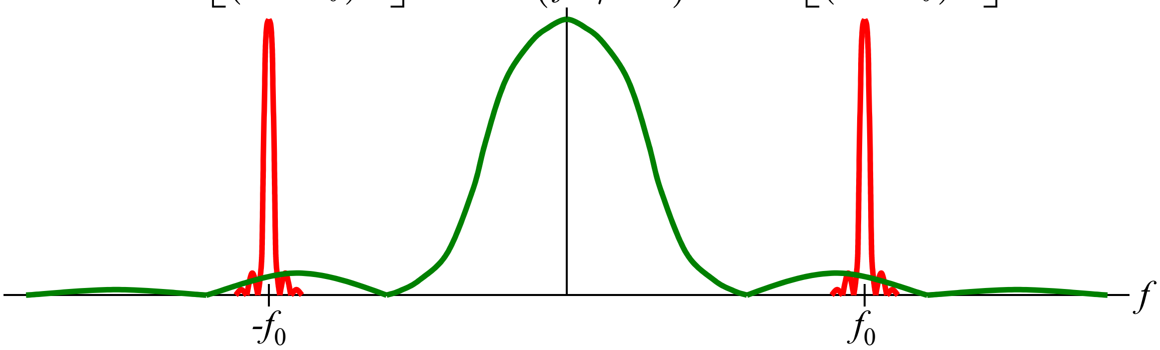


# Power Spectral Density of $s_t(t)$ (Cont.)

$$S_t(f) \cong \frac{PT^2}{200}\text{sinc}^2\left[\left(f - f_0\right)T/100\right]\int_{-\infty}^{\infty}\text{sinc}^2\left[f' - f_0)T\right] df'$$

$$+ \frac{PT^2}{200}\text{sinc}^2\left[\left(f + f_0\right)T/100\right]\int_{-\infty}^{\infty}\text{sinc}^2\left[f' + f_0)T\right] df'$$

$$= \frac{PT}{200}\left\{\text{sinc}^2\left[\left(f - f_0\right)T/100\right] + \text{sinc}^2\left[\left(f + f_0\right)T/100\right]\right\}$$



# Interference Rejection



# Interference Rejection

- The interference rejection is accomplished by the receiver **despreading mixer**:
  - **Despread** the desired signal
  - **Spread** the interference signal
- If the interference energy is spread over a bandwidth much larger than the data bandwidth, most of the energy will be **rejected** by a band-pass filter before data demodulation
  - The bandwidth of the band-pass filter is equal to the **information rate** (data bandwidth, not spread bandwidth)

# Interference Rejection – Before Despreading

- Suppose that the BPSK is used for both data modulation and spreading modulation, and the interference is a **single tone** having power *J*
  - If no spectrum spreading is employed
    - The ratio of jamming power to signal power is *J/P*
- If DSSS is employed, the power spectrum of the **received signal** is:

$$S_r(f) \cong \frac{1}{2}PT_c\left\{\text{sinc}^2\left[\left(f-f_0\right)T_c\right]+\text{sinc}^2\left[\left(f+f_0\right)T_c\right]\right\}$$
$$+\frac{1}{2}J\left\{\delta\left(f-f_0\right)+\delta\left(f+f_0\right)\right\}$$

- The received signal is:

$$r(t)=\sqrt{2P}d\left(t-T_d\right)c\left(t-T_d\right)\cos\left(\omega_0 t+\phi\right)+\sqrt{2J}\cos\left(\omega_0 t+\phi'\right)$$



# Interference Rejection – After Despreading

- The output of the despreading mixer is: (when multiplied by a well **synchronized** despreading code)

$$y(t)=\sqrt{2P}\underline{d\left(t-T_d\right)}\cos\left(\omega_0 t+\phi\right)+\sqrt{2J}\underline{c\left(t-T_d\right)}\cos\left(\omega_0 t+\phi'\right)$$

**Narrow band** **Wide band**

- The power spectrum of the output of despreading mixer is:

$$S_y(f)=\frac{1}{2}PT\left\{\text{sinc}^2\left[\left(f-f_0\right)T\right]+\text{sinc}^2\left[\left(f+f_0\right)T\right]\right\}$$
$$+\frac{1}{2}JT_c\left\{\text{sinc}^2\left[\left(f-f_0\right)T_c\right]+\text{sinc}^2\left[\left(f+f_0\right)T_c\right]\right\}$$

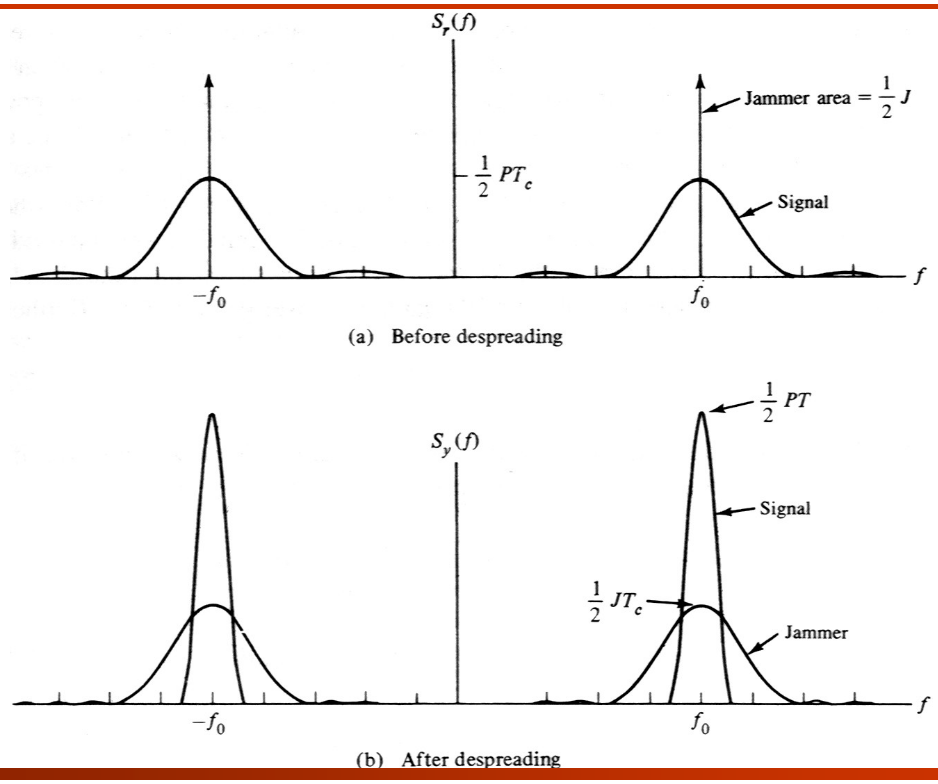
- The data signal has been **despread to the data bandwidth**
- The single-tone jammer has been **spread over the full transmission bandwidth** of the spread-spectrum system

# Interference Rejection–After Despreading (Cont.)

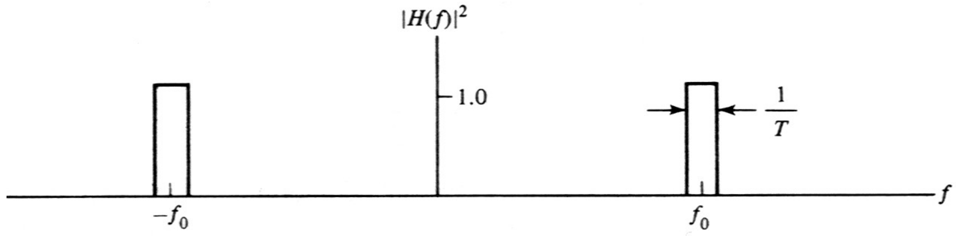
- After despreading, the output is filtered to limit the bandwidth at the input of the data demodulator
  - Nearly all of the signal power is **passed** by the IF (intermediate-frequency) band-pass filter
  - A large fraction of the spread jammer power is **rejected** by the IF filter



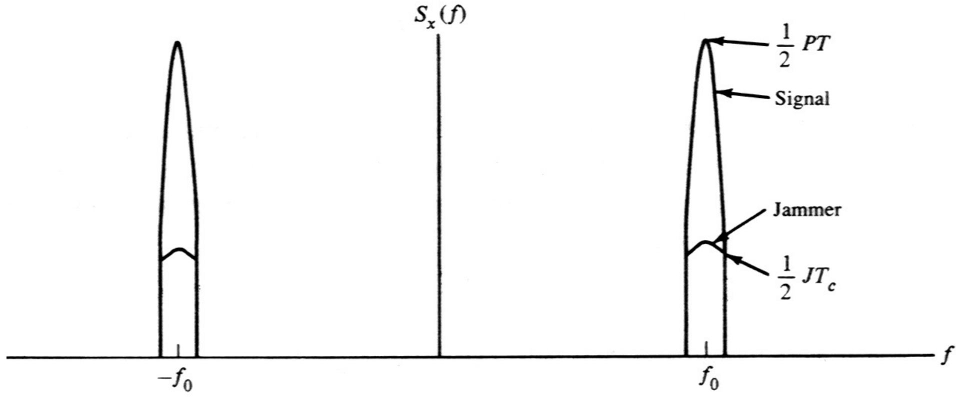
# Interference Rejection–After Despreading (Cont.)



# Interference Rejection–After Despreading (Cont.)




(c) IF filter power transfer function




(d) Output of IF filter



# Interference Rejection – Jammer Power

- The magnitude of the jammer power passed by the IF filter is

$$J_0 = \int_{-\infty}^{\infty} S_J(f) \left| H(f) \right|^2 df$$

  - $S_J(f)$ is the power spectrum of the jammer after the despreading mixer

- For an **ideal** band-pass IF filter, the jammer power is

$$J_0 = \int_{-f_0-1/2T}^{-f_0+1/2T} S_J(f) df + \int_{f_0-1/2T}^{f_0+1/2T} S_J(f)\, df$$

$$\cong \frac{1}{2} J T_c \int_{-f_0-1/2T}^{-f_0+1/2T} \mathrm{sinc}^2 \left[ (f+f_0) T_c \right] df$$

$$+ \frac{1}{2} J T_c \int_{f_0-1/2T}^{f_0+1/2T} \mathrm{sinc}^2 \left[ (f-f_0) T_c \right] df$$

## Interference Rejection – Jammer Power (Cont.)

- For a large ratio of the total spread bandwidth to the data bandwidth **(i.e. $T_c << T$)**, **sinc** function is nearly **constant** over the range of integration
  - The constant is equal to 1

$$J_0 \cong J \frac{T_c}{T}$$

- Thus the jamming power at the input to the data demodulator has been **reduced** by a factor of
  - **Processing gain (PG)**

$$G_P = \frac{T}{T_c}$$



## Interference Rejection – Wideband Jammer

- How about using a **wideband** jamming signal?

$$J(t) = \sqrt{2J}\, c'\left(t - T_d'\right)\cos\left(\omega_0 t + \phi'\right)$$

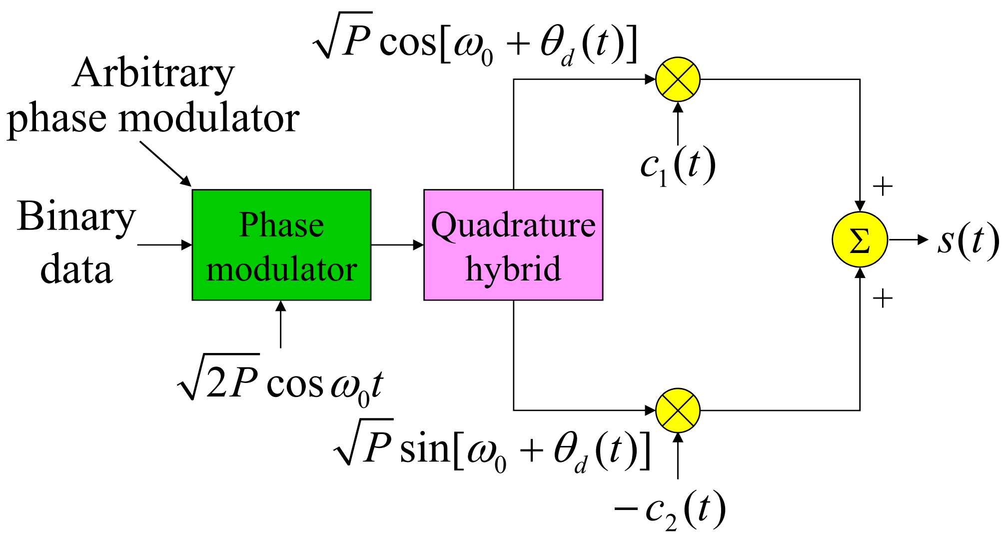
- The key is "Will the jamming signal be **despread** by the despreading mixer at the desired receiver?"

# QPSK Direct-Sequence Spread Spectrum



# QPSK DSSS – Balanced QPSK

- One type of the QPSK spreading modulation is **balanced QPSK DSSS**




**QPSK SS modulator with arbitrary data phase modulation**

# QPSK DSSS – Balanced QPSK (Cont.)

- The output of the QPSK modulator is

$$s(t)=\sqrt{P}c_1(t)\cos\left[\omega_0 t+\theta_d(t)\right]-\sqrt{P}c_2(t)\sin\left[\omega_0 t+\theta_d(t)\right]\triangleq a(t)-b(t)$$

  - $c_1(t)$: the **in-phase** spreading waveform
  - $c_2(t)$: the **quadrature** spreading waveform
  - $c_1(t)$ and $c_2(t)$ are assumed to be **chip synchronous** but **independent** of one another
- The autocorrelation function of $s(t)$:

$$\begin{aligned}R_s&=E\left[s(t)s(t+\tau)\right]\\&=E\left[a(t)a(t+\tau)\right]+E\left[b(t)b(t+\tau)\right]-E\left[a(t)b(t+\tau)\right]-E\left[b(t)a(t+\tau)\right]\\&=R_a(\tau)+R_b(\tau)-E\left[a(t)b(t+\tau)\right]-E\left[b(t)a(t+\tau)\right]\end{aligned}$$

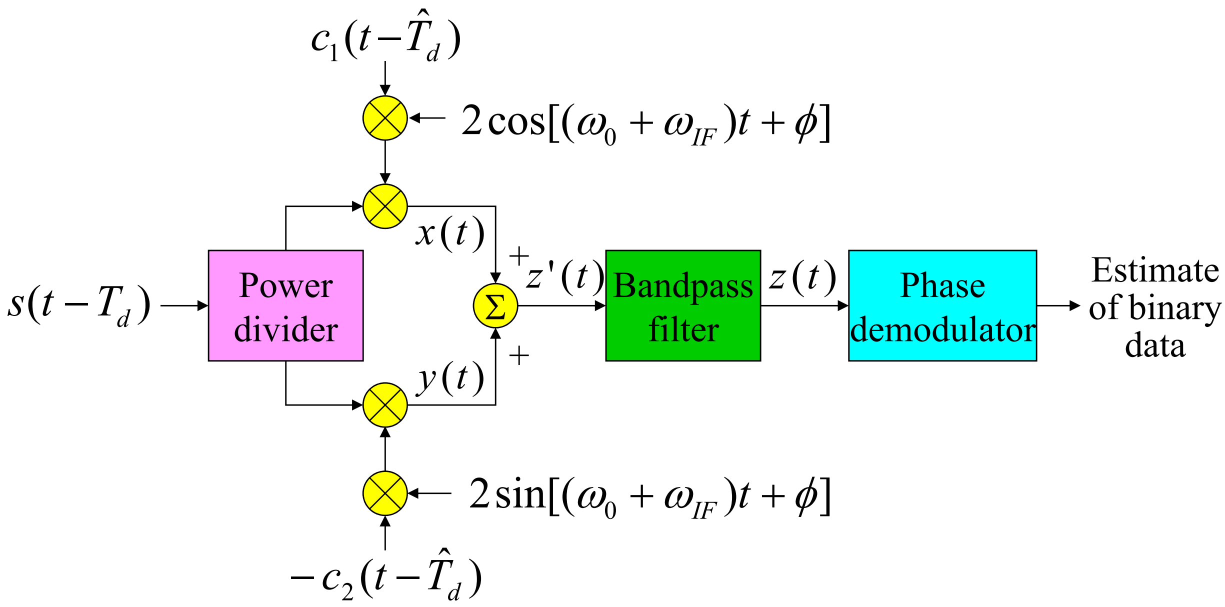
- If $c_1(t)$ and $c_2(t)$ are **independent** of one another

$$R_s=R_a(\tau)+R_b(\tau)$$



# QPSK DSSS – Balanced QPSK (Cont.)

- The QPSK **despreading** receiver for balanced QPSK DSSS




**QPSK SS receiver for arbitrary data modulation**

# QPSK DSSS – Balanced QPSK (Cont.)

- The despreading mixer output is

$$x(t)=\sqrt{\frac{p}{2}}c_1(t-T_d)c_1(t-\hat{T}_d)\cos[\omega_{IF}t-\theta_d(t)]$$
$$+\sqrt{\frac{p}{2}}c_2(t-T_d)c_1(t-\hat{T}_d)\sin[\omega_{IF}t-\theta_d(t)]$$

**Cancelled**

$$y(t)=-\sqrt{\frac{p}{2}}c_1(t-T_d)c_2(t-\hat{T}_d)\sin[\omega_{IF}t-\theta_d(t)]$$
$$+\sqrt{\frac{p}{2}}c_2(t-T_d)c_2(t-\hat{T}_d)\cos[\omega_{IF}t-\theta_d(t)]$$

- If the despreading codes are well **synchronized**:

$$c_1(t-T_d)c_1(t-\hat{T}_d)=c_2(t-T_d)c_2(t-\hat{T}_d)=1.0$$



# QPSK DSSS – Balanced QPSK (Cont.)

- The desired signal has been despread

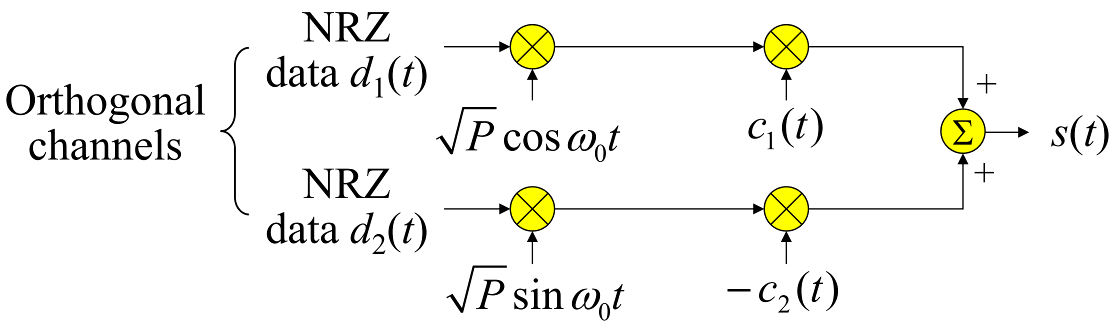
$$z(t)=\sqrt{2P}\cos[\omega_{IF}t-\theta_d(t)]$$

- The data-modulated carrier has been **recovered**
- The signal $z(t)$ is the input to a conventional phase demodulator
  - The data can then be recovered

# QPSK DSSS – Dual-channel QPSK

- Another type of the QPSK spreading modulation is **dual-channel QPSK**
  - The in-phase and quadrature QPSK channels are BPSK data modulated using **different BPSK data modulators**
- The output of the QPSK modulator is

$$s(t)=\sqrt{P}d_1(t)c_1(t)\cos\omega_0 t-\sqrt{P}d_2(t)c_2(t)\sin\omega_0 t$$



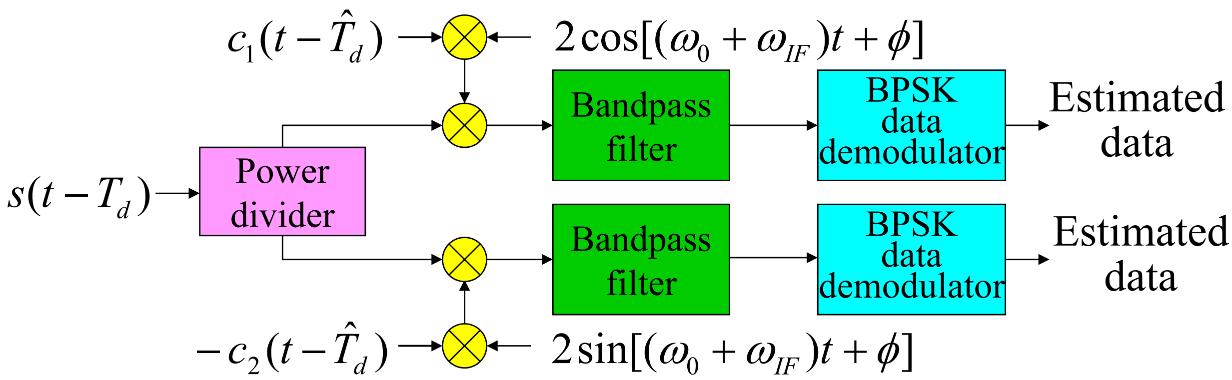

**Dual-channel QPSK DSSS Transmitter**



# QPSK DSSS – Dual-channel QPSK (Cont.)

- The QPSK despreading receiver for dual-channel QPSK DSSS
  - If it permits the in-phase and quadrature channels to have **unequal** power, the output signal is

$$s(t)=\sqrt{2P_I}d_1(t)c_1(t)\cos\omega_0 t-\sqrt{2P_Q}d_2(t)c_2(t)\sin\omega_0 t$$




**Dual-channel QPSK DSSS receiver**

# Frequency-Hop Spread Spectrum

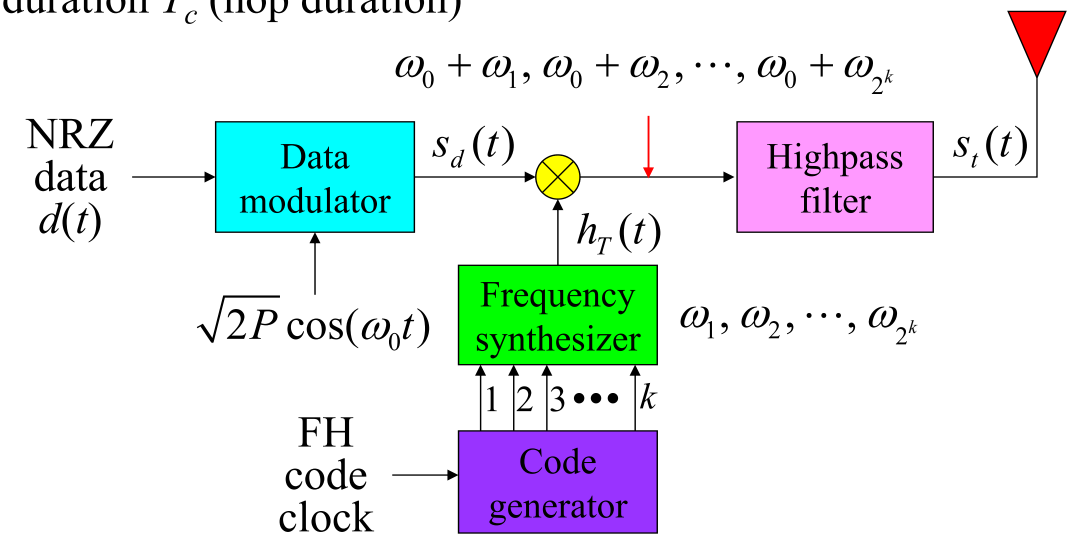


# Frequency-Hop Spread Spectrum

- Frequency-hop spread spectrum technique is to change the frequency of the carrier **periodically**
- The transmitted signal appears as a data-modulated carrier which is hopping from one frequency to the next
- Typically, each carrier frequency is selected from a set of $\mathbf{2}^k$ frequencies which are spaced approximately the width of the **data modulation bandwidth** apart
- The spreading code **does not** directly modulate the data-modulated carrier but is used to **control the sequence of carrier frequencies**
- At the receiver, the frequency hopping is removed by mixing with a local oscillator signal which is hopping **synchronously** with the received signal

# FHSS – Transmitter

- The frequency synthesizer output is a sequence of tones of duration $T_c$ (hop duration)




**Coherent frequency-hop spread-spectrum transmitter**

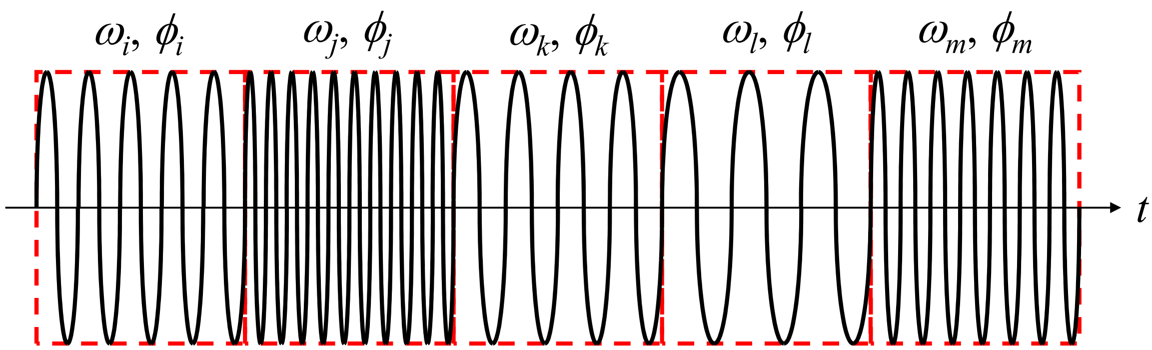


# FHSS – Transmitter (Cont.)

- The signal of the frequency synthesizer output is

$$h_T(t) = \sum_{n=-\infty}^{\infty} 2p(t - nT_c)\cos(\omega_n t + \phi_n)$$

  – $p(t)$ is a unit amplitude pulse of duration $T_c$
  – $\omega_n$ and $\phi_n$ are the radian frequency and the phase during the $n$-th frequency-hop interval



# FHSS – Transmitter (Cont.)

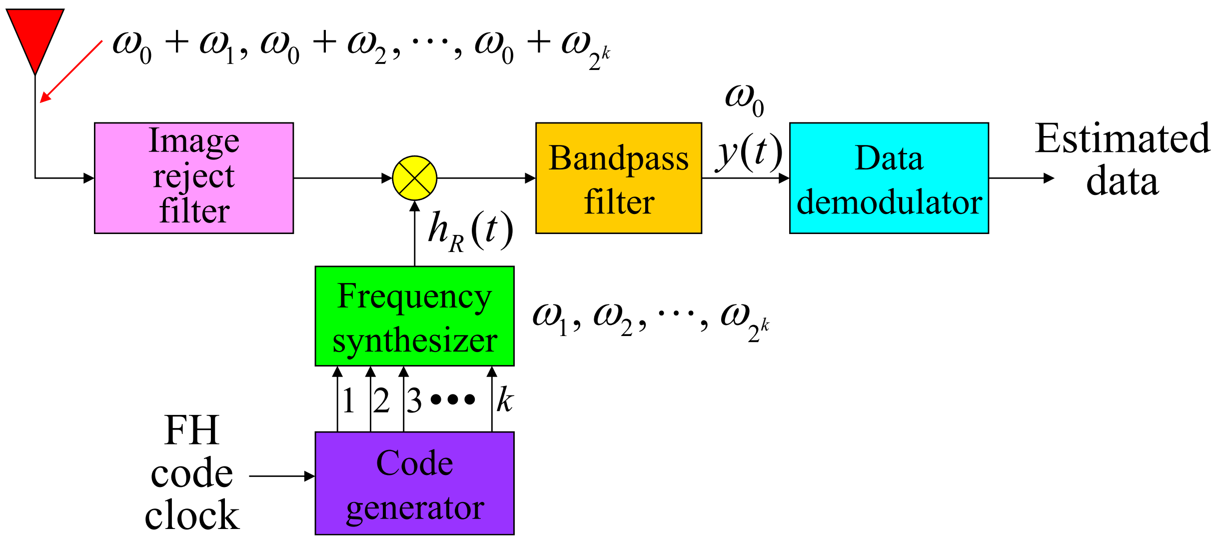
- $\omega_n$ is taken from a set of $2^k$ frequencies
  - The spreading code uses ***k* bits** at a time
- The transmitted signal is the data-modulated carrier up-converted to a new frequency ($\omega_0 + \omega_n$) for each FH chip

$$s_t(t) = \left[ s_d(t) \sum_{n=-\infty}^{+\infty} 2p(t - nT_c)\cos(\omega_n t + \phi_n) \right]$$ sum of freq. components



# FHSS – Receiver

- At the receiver, the frequency de-hopper can recover the received FHSS signal to a **narrowband** signal




**Coherent frequency-hop spread-spectrum receiver**

# Power Spectral Density of Coherent Slow-FHSS

- The power spectrum of the transmitted signal $S_t(f)$ is the sum frequency term of the convolution of $S_d(f)$ with $S_h(f)$

$$S_t(f) = \int_{-\infty}^{\infty} S_d(f')S_h(f-f')\,df'$$

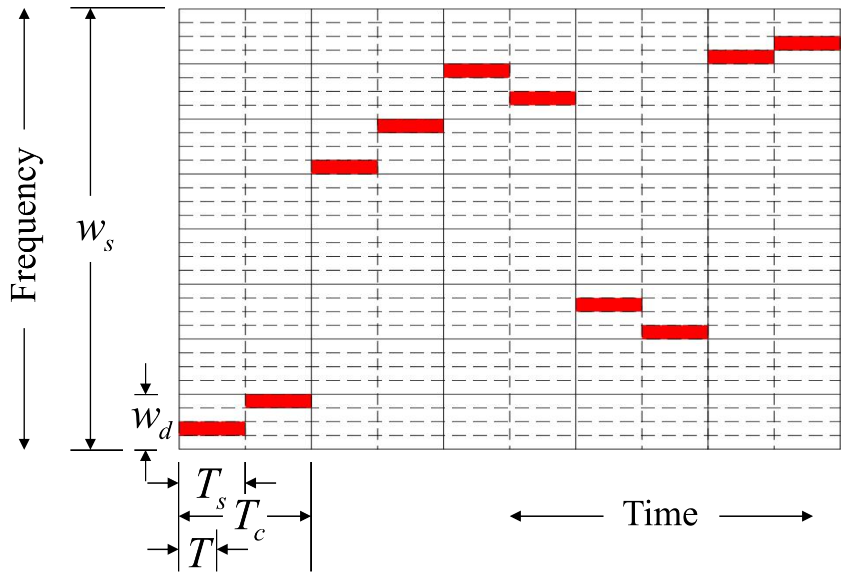
  - $S_d(f)$: the power spectral density of the **data-modulated carrier** $s_d(t)$
  - $S_h(f)$: the power spectral density of the **hop carrier** $h_T(t)$
- The hopping carrier $h_T(t)$ is assumed to be a **purely random sequence** of frequencies
  - If $h_T(t)$ is periodic, the period would be sufficiently long
- For slow-FHSS, it can be approximated as the sum of the data-modulated carrier PSD translated to **all hop frequencies** and weighted by the probability of transmitting on that frequency



# Noncoherent Slow-Frequency-Hop SS

- Due to the difficulty of building truly coherent frequency synthesizers
  - Many FHSS systems use **noncoherent data modulation**
- A common data modulation for FHSS systems is $M$-ary **frequency shift keying** (MFSK)
  - The data modulator outputs one of $2^L$ tones for each $LT$ seconds, where $M = 2^L$ and $T$ is the bit duration
  - The frequency spacing is **at least** $1/LT$
  - The output spectral width is approximately $2^L/LT$
  - In each $T_c$ seconds, the data modulator output is translated to a new frequency by the frequency-hop modulator

# Noncoherent Slow-Frequency-Hop SS (Cont.)




**Data** 01 11 00 11 11 01 10 00 00 01

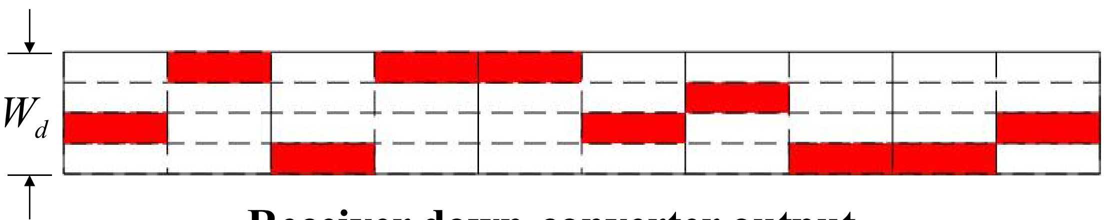
$W_d \approx 2^L / LT = 2^L / T_s$; $W_s = 2^k W_d$ $L = 2$; $k = 3$

**Transmitted signal for an *M*-ary FSK slow-FH SS system**



# Noncoherent Slow-Frequency-Hop SS (Cont.)

- For **slow-frequency-hop** systems:
  - $T_c > LT$ (symbol duration)
- By considering a noise jammer with the average power $J$:
  - In the **absence** of FH, the jammer chooses a bandwidth $W_d$ centered on the proper carrier frequency $\Rightarrow E_b / N_J = E_b W_d / J$
  - When FH is added, the jammer places noise in all $\mathbf{2^k}$ FH bands $\Rightarrow E_b / N_J = E_b W_s / J$
  - The **processing gain** is $2^k = W_s / W_d$



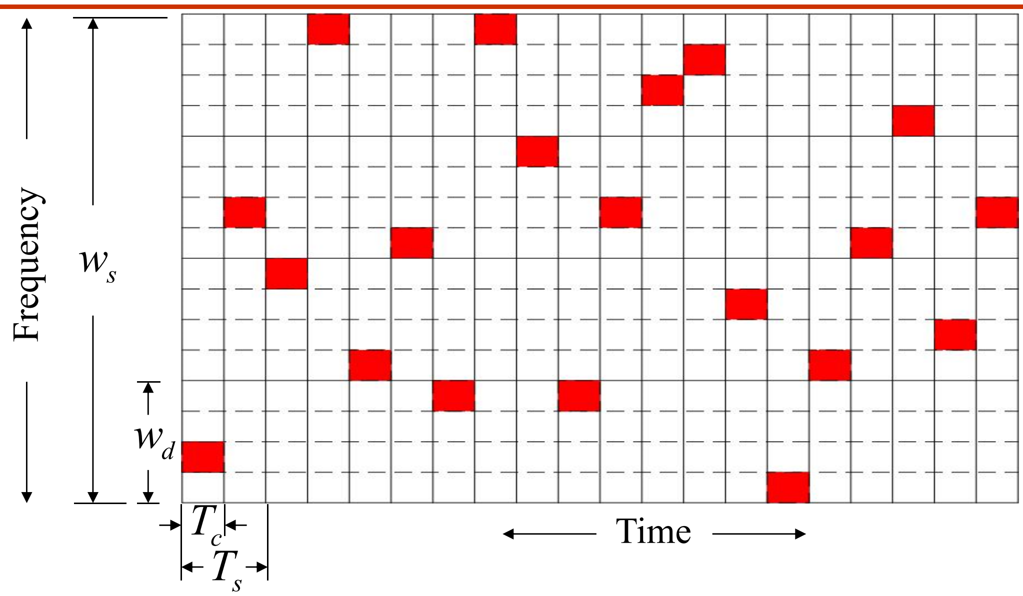

**Receiver down-converter output**

# Noncoherent Fast-Frequency-Hop SS (Cont.)

- For **fast-frequency-hop** systems:
  - $T_c \leq LT$ (symbol duration)
  - Each symbol is subdivided into $K$ chips, $1/T_c = K/LT$
- A significant benefit: we have **frequency diversity gain** on **each symbol** for
  - Partial-band jamming environments
  - Rapid signal fading (multipath fading) environments
- For the data demodulator, it may
  - Use **hard decision** on each frequency-hop chip and make an estimate based on all $K$ chips, or
  - Apply **maximum likelihood (ML) decision** based on the total received signal



# Noncoherent Fast-Frequency-Hop SS (Cont.)

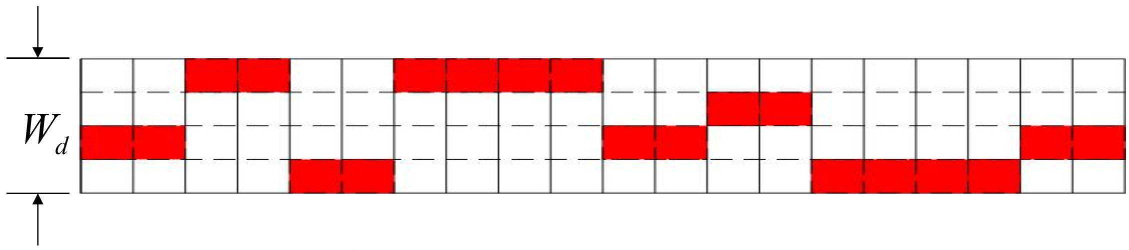



**Data 01 11 00 11 11 01 10 00 00 01**

$$W_d \approx 2^L / T_c = K 2^L / LT; \quad W_s = 2^k W_d \quad L = K = k = 2$$

**Transmitted signal for an *M*-ary FSK fast-FH SS system**

# Noncoherent Fast-Frequency-Hop SS (Cont.)




**Receiver down-converter output**



# Bluetooth Wireless Technology

# Bluetooth Classic (Bluetooth 1.0 ~ 4.0)

- Bluetooth Classic radio is used to support **point-to-point** device communications (**connection-oriented** data transports)
  - Bluetooth **Basic Rate/Enhanced Data Rate** (BR/EDR)
- A **low power** radio that streams data over **79** channels (**1 MHz** spacing) in the 2.4 GHz **unlicensed** industrial, scientific, and medical (ISM) frequency band.
  - Based on the **Frequency-Hop Spread Spectrum** technique
- Bluetooth Classic has become the standard radio protocol behind wireless speakers, headphones, and in-car entertainment systems.
  - Mainly used to enable **wireless audio streaming**
- Bluetooth Classic radio also enables **data transfer** applications
  - Such as mobile printing

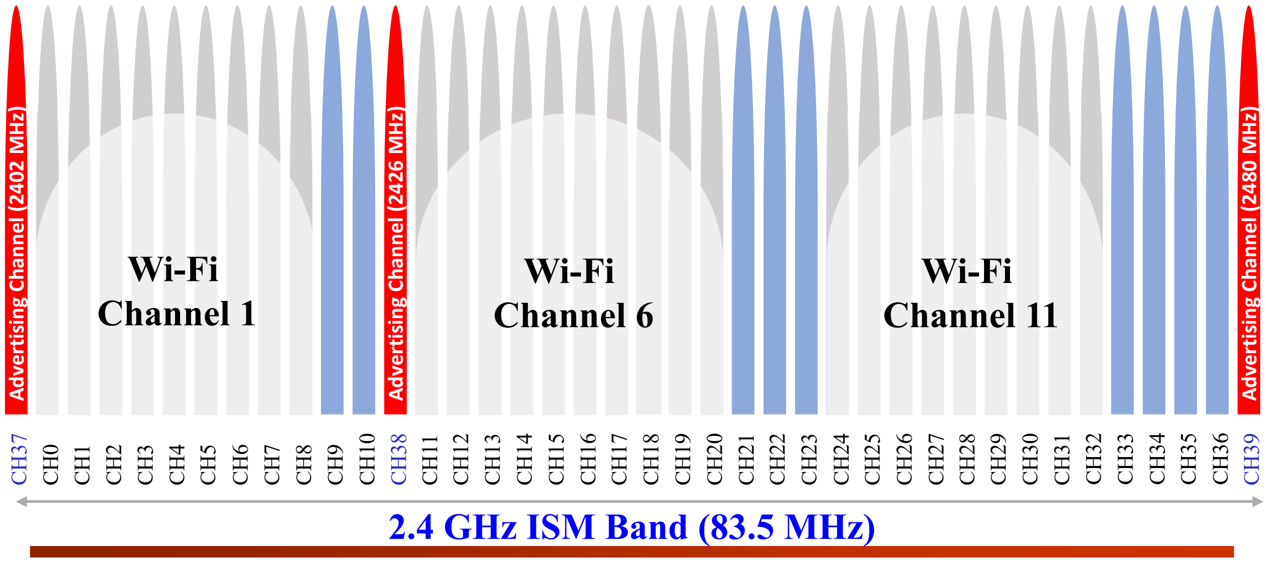


# Bluetooth Low Energy (Bluetooth 4.0 ~ )

- Bluetooth Low Energy (BLE) radio is designed for **very low power** operation.
- BLE transmits data over **40** channels (**2 MHz** spacing) in the 2.4 GHz unlicensed ISM frequency band.
  - Including **3** advertising channels and **37** data channels
  - Transmissions on data channels are still based on the **Frequency-Hop Spread Spectrum** technique
- BLE supports multiple communication topologies, expanding from point-to-point to **broadcast** and **mesh**.
- BLE extends the data transports from **connection-oriented** modes to **connectionless** modes.

# Bluetooth Low Energy Channels

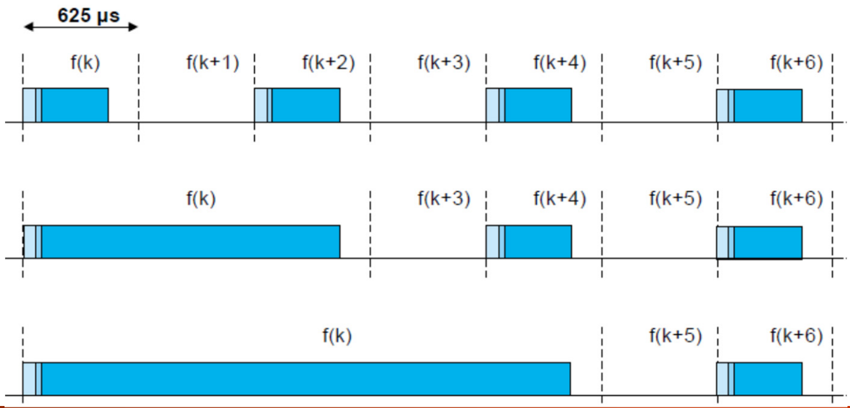
- The advertising channels are numbered as channels 37, 38, 39
  - Support beacon services
- The data channels are numbered from channel 0 to channel 36






# Bluetooth Classic Frequency Hopping

- Bluetooth transmission channels are divided into time slots, each slot being **625 μs** in duration.
  - Packets can be either 1, 3, or 5 slots in duration with **one frequency hop per packet**
- Bluetooth Classic devices hop at a maximum rate of 1600 hops per second, which is **randomly** spread among 79 channels.



## Bluetooth Classic Frequency Hopping Pattern

- A **periodic pseudo-random** hop generator is used for channel selection.
  - The hop sequence period is $\mathbf{2^{27}}$ hops
  - The time period of the hopping pattern is about **23.3 hours**
  - The output ranges from 0 to 78 (by modulo 79 operation)
- The hop period is long enough to avoid hop synchronization between two different Bluetooth transmissions in a short range.



## BLE Frequency Hopping

- In BLE, the transmission frequency changes once for every **connection event**.
  - The time slot duration for transmitting a packet is **150 μs**
  - A connection event contains a group of packets
  - Each connection event must take place in a single frequency channel
- The **connection interval** determines the hop rate
  - The period of a connection event ranges from **7.5 ms** to **4 s** (in multiples of 1.25mS).
- The BLE hop rate is between **133.33** and **0.25** hops per second.
- The hop generator output ranges from 0 to 36 (by modulo 37 operation)

# Adaptive Frequency Hopping (AFH)

- **Adaptive Frequency Hopping** (AFH) is available for the Bluetooth connection state only.
  - The channel conditions are permanently monitored to identify **occupied** (by other systems or other users) or **low quality** channels, which are stated as **bad channels**.
  - The bad channels are **excluded from** the available channels until they become **good channels** again.
  - The number of available channels must be larger than or equal to a **minimum required number**. So, bad channels can be also present within the currently used hopping pattern.



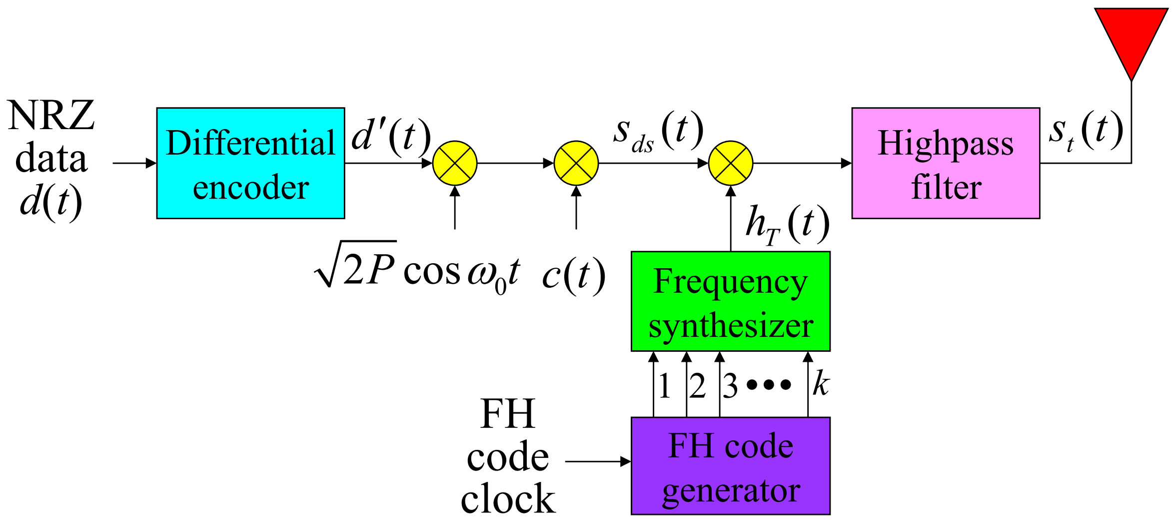
# Hybrid DS/FH Spread Spectrum

# Hybrid DS/FH Spread Spectrum

- A **hybrid** direct-sequence/frequency-hop system employs both direct-sequence and frequency-hop spreading techniques
  - Some of the advantages obtained in both types of systems are combined in a single system
- A hybrid DS/FH SS system employs **differential** BPSK modulation (The MFSK modulation is not suitable for DSSS)
  - **Noncoherent** frequency hopping is used: the data modulation must be either noncoherent or differentially coherent
  - The DPSK modulated carrier is first **DS spread** by $c(t)$
  - Then **frequency hopped** by using the sequence of FH tones $h_T(t)$

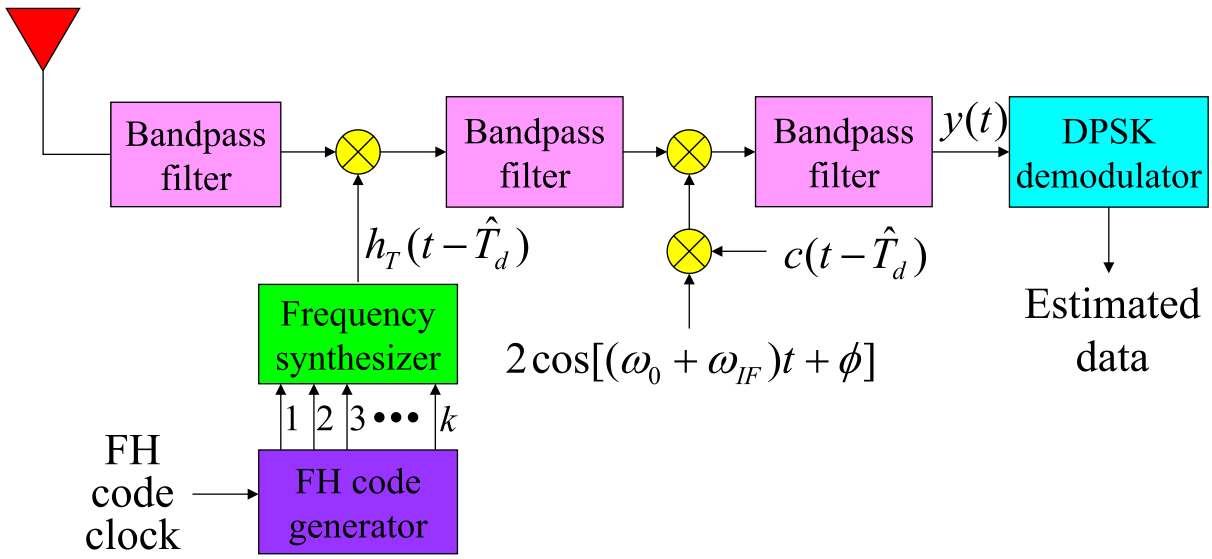


# Hybrid DS/FH Spread Spectrum – Transmitter




**Hybrid DS/FH spread-spectrum transmitter**

# Hybrid DS/FH Spread Spectrum – Receiver




**Hybrid DS/FH spread-spectrum receiver**



# Hybrid DS/FH Spread Spectrum – PSD

- The power spectral density of the transmitted signal $s_t(t)$ is

$$S_t(f) = \left[S_{ds}(f) * S_h(f)\right]_{\substack{\text{sum of} \\ \text{freq. terms}}}$$

$$S_{ds}(f) \approx \frac{1}{2} PT_c \left\{\mathrm{sinc}^2\left[(f-f_0)T_c\right] + \mathrm{sinc}^2\left[(f+f_0)T_c\right]\right\}$$

$$S_t(f) \cong \Bigg[\int_{-\infty}^{\infty} \frac{1}{2} PT_c \left\{\mathrm{sinc}^2\left[(f'-f_0)T_c\right] + \mathrm{sinc}^2\left[(f'+f_0)T_c\right]\right\}$$

$$\times \frac{1}{2^k}\sum_{m=1}^{2^k}\left\{\delta(f-f'-f_m)+\delta(f-f'+f_m)\right\} df' \Bigg]_{\substack{\text{sum of} \\ \text{freq. terms}}}$$

$$= \frac{PT_c}{2^{k+1}}\sum_{m=1}^{2^k}\left\{\mathrm{sinc}^2\left[(f-f_m-f_0)T_c\right] + \mathrm{sinc}^2\left[(f+f_m+f_0)T_c\right]\right\}$$

# LoRa Chirp Spread Spectrum



## LoRa Chirp Spread Spectrum

- LoRa uses **Chirp Spread Spectrum (CSS)** modulation for signal spreading.
- The data modulation is an ***M*-FSK-like modulation** scheme
  - The modulated carrier wave is not a fixed frequency wave, but a **chirp signal**.
- The occupied **bandwidth** of a channel is fixed, equivalent to the spectral bandwidth of the chirp signal.
  - Uplink channel: **125 KHz** or **500 KHz**
  - Downlink channel: **500 KHz**
- LoRa trades data rate for sensitivity within a **fixed channel bandwidth** (the nature of *M*-FSK modulation)
  - It allows the system to trade data rate for **range** or **power**

# LoRa Chirp Spread Spectrum

- For **Chirp Spread Spectrum (CSS)** modulation, a chirp signal can be expressed as

$$s_{\mathrm{ch}}(t) = \exp\left[ j2\pi\left( f_{\mathrm{i}} + f_{\mathrm{c}}(t) \right) t \right], \quad f_{\mathrm{c}}(t) = \pm Bt/T_{\mathrm{s}}$$

  – $f_c(t)$ is the instantaneous frequency, which is **linear** with the slope $B/T_s$ (‘+’: up-chirp, ‘–’: down-chirp)

  – $B$ is a **fixed** bandwidth of the chirp signal

  – $T_s$ is the symbol duration

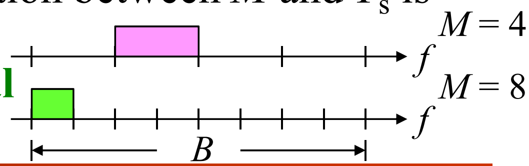
- For $M$-FSK modulation, the minimum subchannel separation is $1/T_s$ to maintain **orthogonality**

  – For a fixed bandwidth $B$, the relation between $M$ and $T_s$ is

$$M = BT_{\mathrm{s}}$$

  – $M \downarrow \Rightarrow T_s \downarrow \Rightarrow R_s \uparrow$

**For the conventional *M*-FSK**






# LoRa Chirp Spread Spectrum

- The binary data stream is divided into multiple **subsequences**
  – Each with a length **SF** (spreading factor) $\in \{7, 8, 9, 10, 11, 12\}$
- Each subsequence is used to construct an $M$-FSK symbol
  – The ratio of the bit rate to the symbol rate is equal to SF
    - Note that “SF” is **different** to the conventional definition

  – The number of possible symbols is $M = 2^{\mathrm{SF}}$

  – The constellation contains $M$ signal points ($M$ tones)
- To distinguish the $M$ different symbols of the constellation, we need to define $M$ **orthogonal chirps** (**orthogonal subchannels**)
  – The symbol duration is set as $T_s = M/B$ for orthogonality

  – The chirp representing the $m$-th point associated to apply **a delay** $\tau_m = m/B$ to the **raw** (original) **chirp signal**

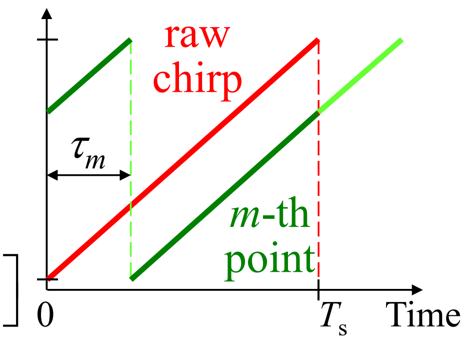
# LoRa Chirp Spread Spectrum

- The raw chirp outside $[0, +T_s]$ is **cyclically brought back**
- The modulated chirp related to the transmission of the $m$-th signal point can be decomposed into two parts:
  - $[0, \tau_m]$: the ramp of the raw chirp defined in $[T_s - \tau_m, T_s]$
  - $[\tau_m, T_s]$: the ramp of the raw chirp defined in $[0, T_s - \tau_m]$
- Correspondingly, for the up chirp signal, the instantaneous frequency is expressed as

$$f_c^{(m)}(t) = \begin{cases} B(t + T_s - \tau_m)/T_s, & 0 \le t < \tau_m \\ B(t - \tau_m)/T_s, & \tau_m \le t < T_s \end{cases}$$

- Eventually, the complex envelope of the transmitted signal is

$$s(t) = \sum_{k \in Z} \exp\left[ j2\pi \left( f_i + f_c^k (t - kT_s) \right)(t - kT_s) \right]$$

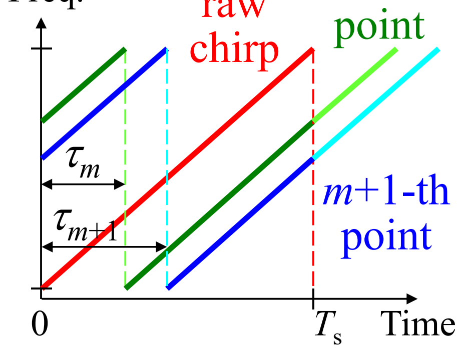





# LoRa Chirp Spread Spectrum

- The applying of **a delay** $\tau_m = m/B$ is equivalent to a **frequency shift** of $B(T_s - \tau_m)/T_s = B - m/T_s$
- The **frequency difference** between the two neighboring signal points, $m$ and $m$+1, is **fixed** (under cyclically shifting) equal to the minimum subchannel separation of $M$-FSK

$$\Delta f(t) = \Delta f = 1/T_s$$



# LoRa Chirp Spread Spectrum

- LoRa **uplink** channel:

| **Spreading Factor** | SF10 | SF9 | SF8 | SF7 | SF8 |
|---|---|---|---|---|---|
| **Channel Frequency** | 125 kHz | 125 kHz | 125 kHz | 125 kHz | 500 kHz |
| **Bitrate (Bits/Sec)** | 980 | 1760 | 3125 | 5470 | 12500 |

- LoRa **downlink** channel:

| **Spreading Factor** | SF12 | SF11 | SF10 | SF9 | SF8 | SF8 |
|---|---|---|---|---|---|---|
| **Channel Frequency** | 500 kHz | 500 kHz | 500 kHz | 500 kHz | 500 kHz | 500 kHz |
| **Bitrate (Bits/Sec)** | 980 | 1760 | 3125 | 5470 | 12500 | 21900 |



# LoRa Chirp Spread Spectrum

- Is the LoRa system a spread spectrum system?
  - Strictly speaking, **it is not**!
- The bandwidth required for an $M$-FSK system with symbol duration $T_s$ is $M/T_s = B$
  - which is **the same as** the total bandwidth of a channel
    - In the viewpoint of **total bandwidth**, no spectrum spreading is performed
  - However, the occupied bandwidth for **each subchannel** is spread from $1/T_s$ to $B$ by a factor of $M$

# Spread Spectrum Advantages

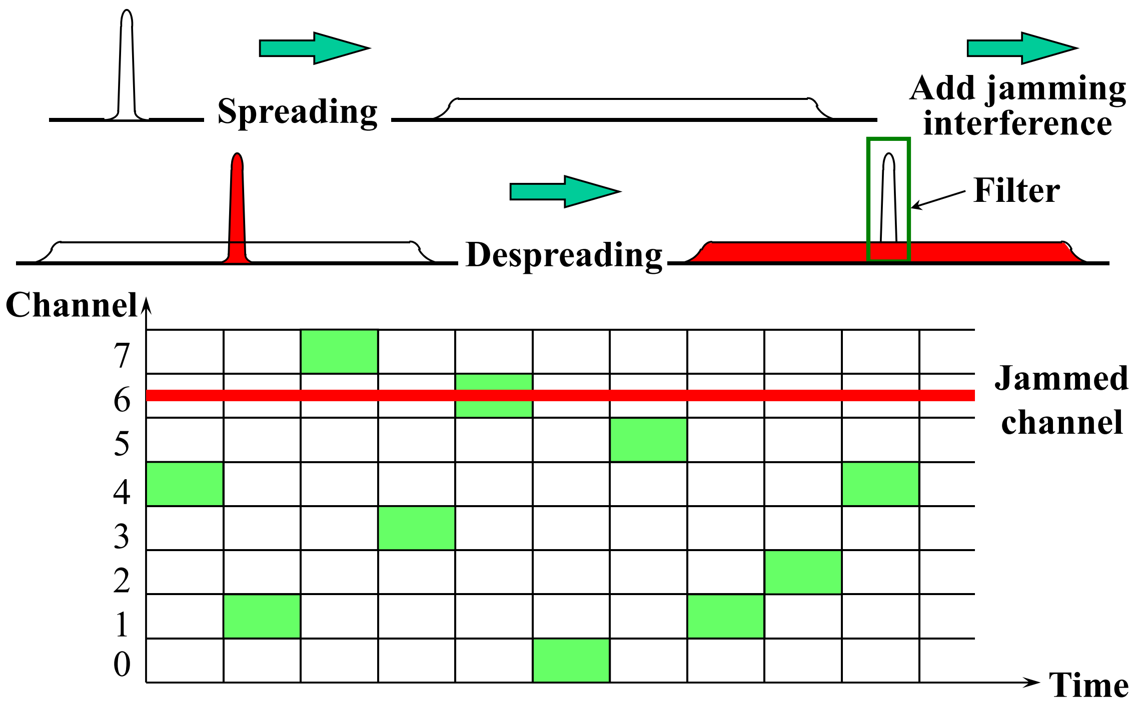


## Spread Spectrum Advantages

- The advantages of spread spectrum technologies include:
  - Anti-jamming
  - Anti-multipath interference
  - Anti-fading
  - Low probability of intercept
  - Limited Secrecy
  - Multiple Access
  - Spectrum sharing between different systems
  - Low frequency reuse factor (for cellular systems)

# Anti-Jamming

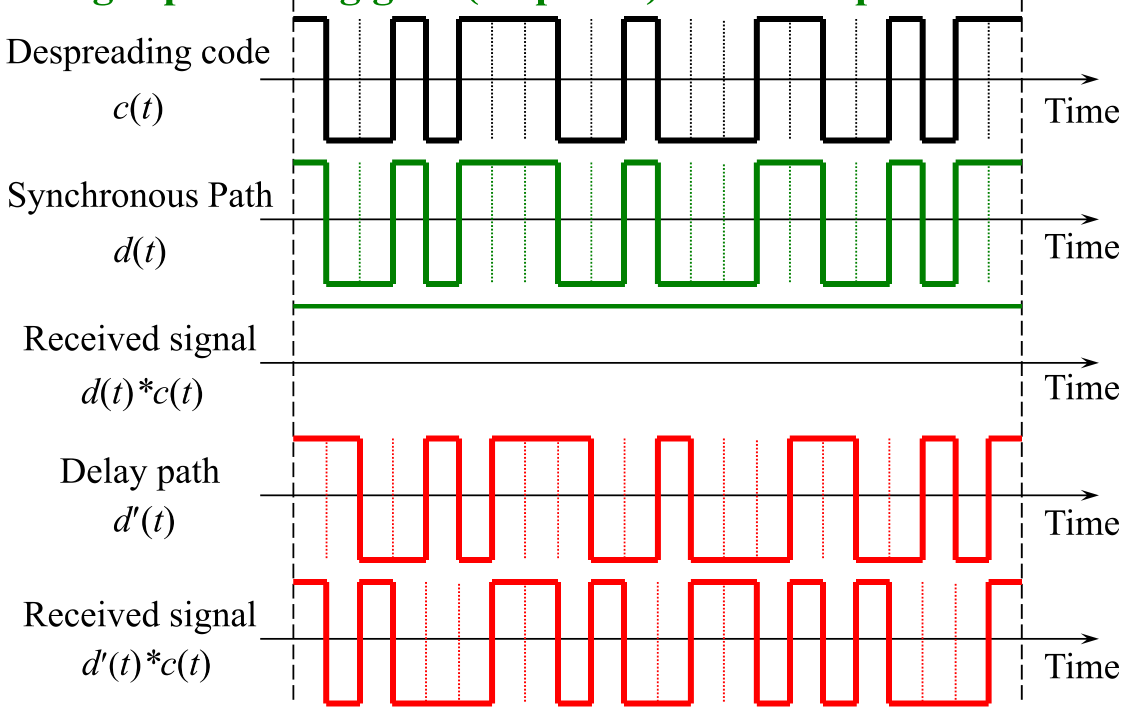
**Larger processing gain ⇒ Better performance**





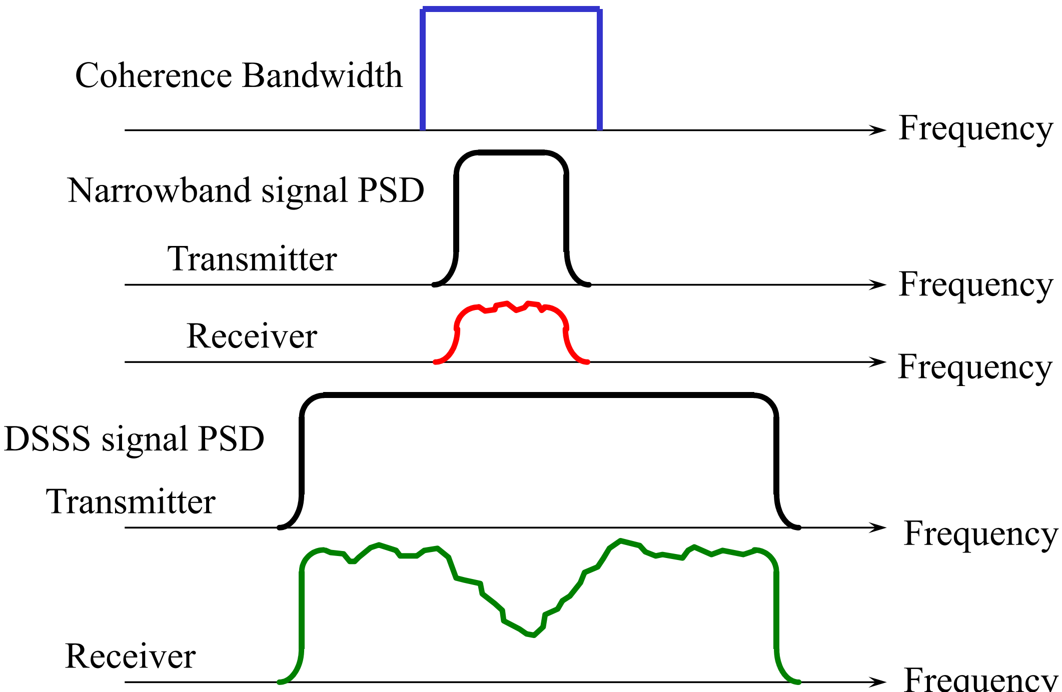

# Anti-Multipath Interference

**Larger processing gain (chip rate) ⇒ Better performance**



# Anti-Fading (DSSS)

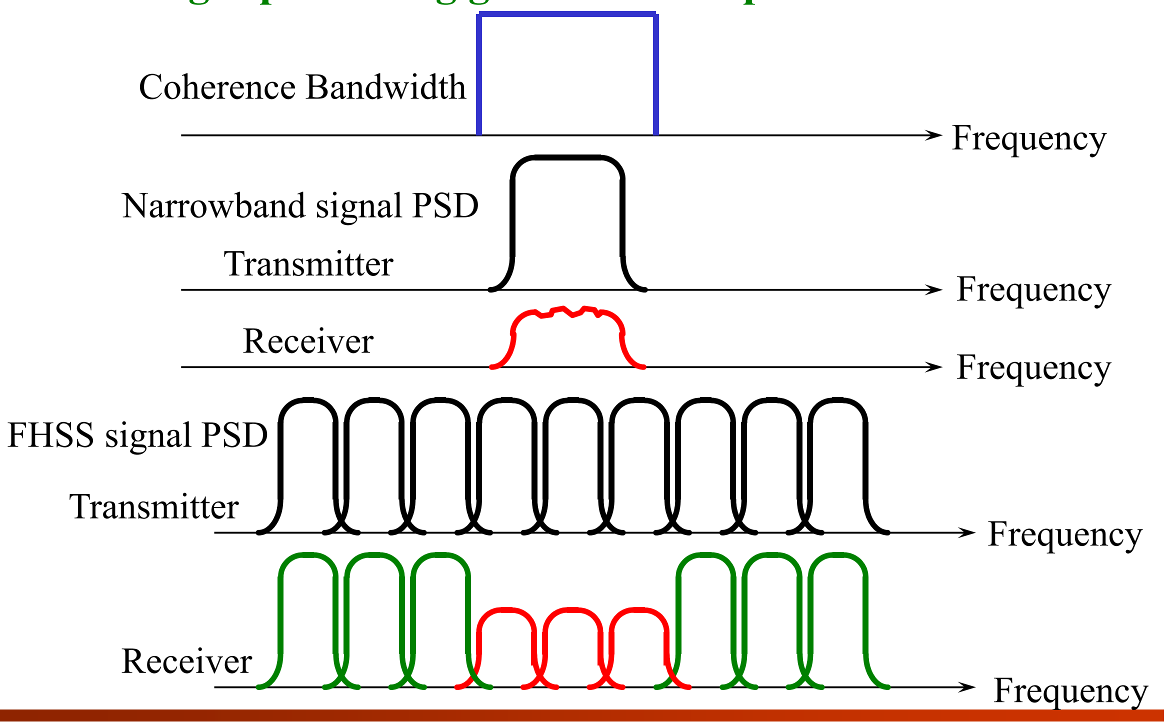
**Larger processing gain (chip rate) ⇒ Better performance**



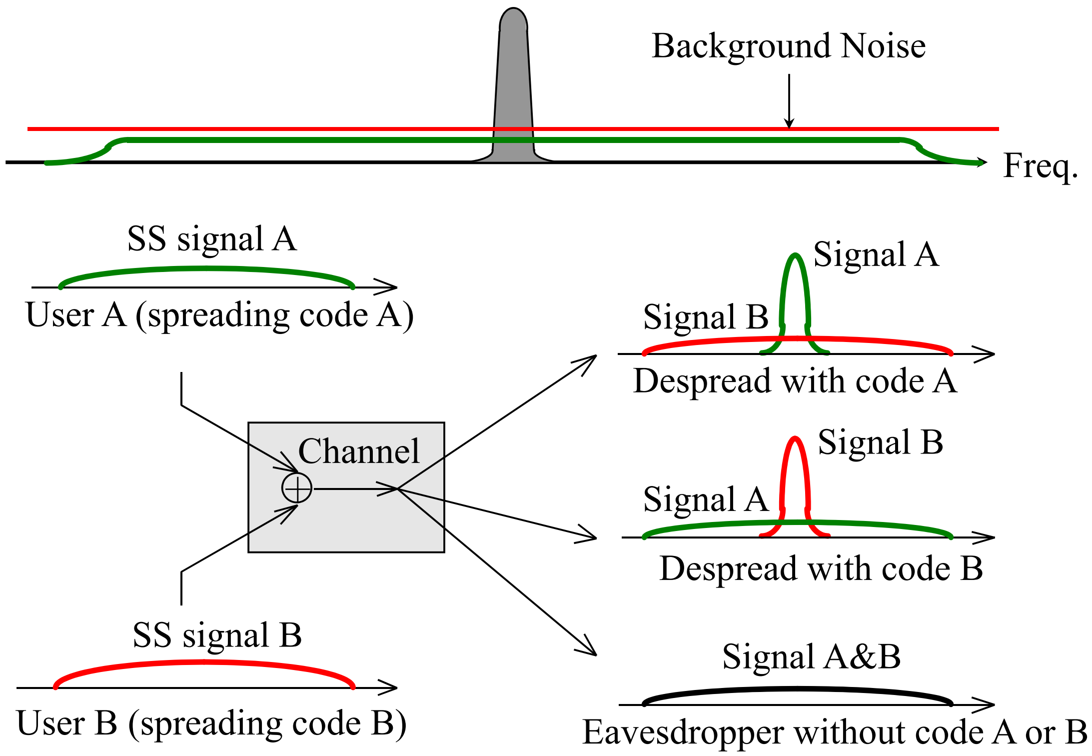



# Anti-Fading (FHSS)

**Larger processing gain ⇒ Better performance**

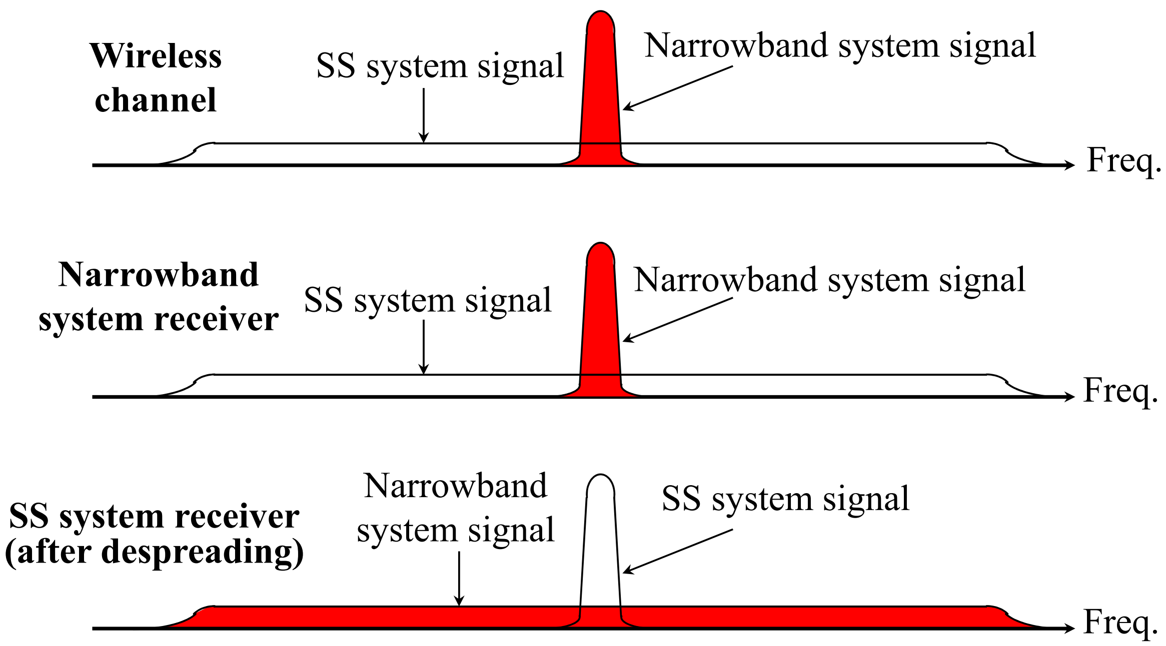


# Low Probability of Intercept & Multiple Access



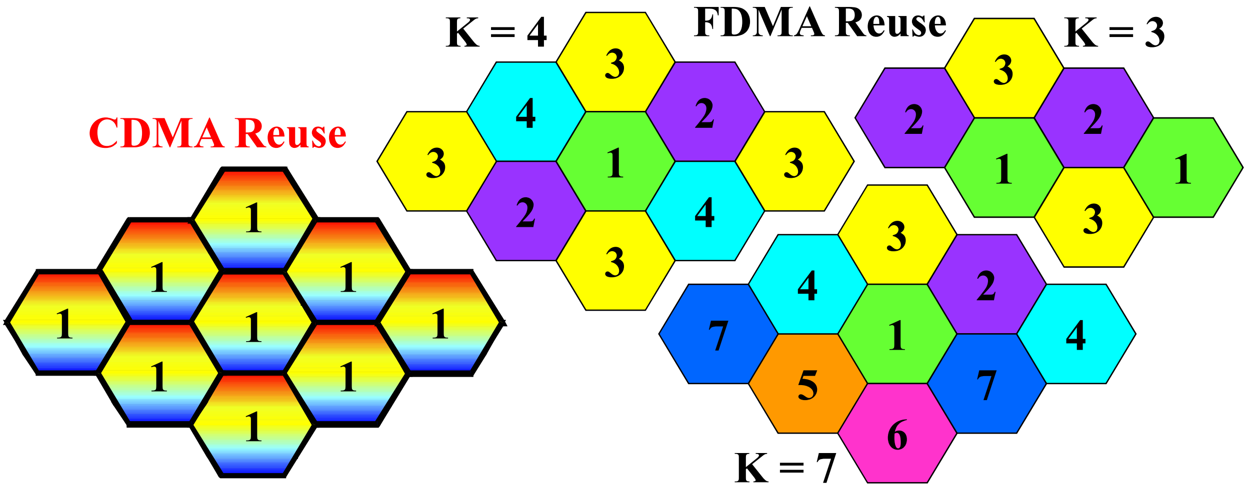



# Spectrum Sharing Between Different Systems



# Low Frequency Reuse Factor

- For **narrowband** systems, the applied frequency reuse factor is larger than 1 (3, 4, 7, or 12, …)
- For **CDMA** systems, the frequency reuse factor is equal to 1
  - All cells can use **the same frequency band**






# ISM Band Regulations

# Industrial, Scientific and Medical (ISM) Band

- The **industrial, scientific and medical (ISM)** radio bands are radio bands **reserved for** the use of **radio frequency (RF) energy** for industrial, scientific and medical purposes **other than radio communications**.
  - RF heating, microwave ovens, medical diathermy machines
- The ISM bands are also allocated for the applications of communications, including **unlicensed** radio communications
  - The ISM devices may generate great **interference** to radio communications using the same frequency band
  - The communications devices may also be interfered by other unlicensed communications devices
  - The equipment must tolerate any interference from ISM applications or other unlicensed communications devices



# ISM Band (Cont.)

- North America FCC ISM band regulations:
  - The communication-related regulations are in **CFR** (Code of Federal Regulations) **Title 47, Sec. 15.247**
- Three major ISM bands are allocated for **unlicensed** radio communications:
  - 902 ~ 928 MHz
  - 2400 ~ 2483.5 MHz
  - 5725 ~ 5850 MHz
- Sec. 15.247 Operation within the bands 902-928 MHz, 2400-2483.5 MHz, and 5725-5850 MHz.

# ISM Band Regulations

- **(a)** Operation under the provisions of this Section is limited to **frequency hopping** and **digitally modulated** intentional radiators that comply with the following provisions:

- **(1) Frequency hopping systems** shall have hopping channel carrier frequencies separated by a minimum of **25 kHz** or the **20 dB bandwidth** of the hopping channel, whichever is greater.
- Alternatively, frequency hopping systems operating in the **2400-2483.5 MHz** band may have hopping channel carrier frequencies that are separated by **25 kHz** or **two-thirds of the 20 dB bandwidth** of the hopping channel, whichever is greater,
  – Provided the systems operate with an output power no greater than **125 mW**.



# ISM Band Regulations (Cont.)

- The system shall hop to channel frequencies that are selected at the system hopping rate from a **pseudo-randomly** ordered list of hopping frequencies.
- Each frequency must be used **equally** on the average by each transmitter.
- The system receivers shall have **input bandwidths** that match the **hopping channel bandwidths** of their corresponding transmitters and shall shift frequencies in synchronization with the transmitted signals.

# ISM Band Regulations (Cont.)

- (i) For FH systems operating in the **902-928 MHz** band:
  - 20 dB bandwidth of the hopping channel: **less than 250 kHz**
    - Number of hopping frequencies: **at least 50**
    - Average time of occupancy on any frequency: no greater than **0.4 seconds** within a **20 second** period
  - 20 dB bandwidth of the hopping channel: **250 kHz or greater**
    - Number of hopping frequencies: **at least 25**
    - Average time of occupancy on any frequency: no greater than **0.4 seconds** within a **10 second** period.
  - The **maximum** allowed 20 dB bandwidth of the hopping channel is **500 kHz**.

**$0.4 \times 50 = 20$; $0.4 \times 25 = 10$; $\Rightarrow$ Equally used**



# ISM Band Regulations (Cont.)

- (ii) For FH systems operating in the **5725-5850 MHz** band:
  - Number of hopping frequencies: **at least 75**
  - Average time of occupancy on any frequency: no greater than **0.4 seconds** within a **30 second** period
  - The **maximum** 20 dB bandwidth of the hopping channel is **1 MHz**.
- (iii) For FH systems operating in the **2400-2483.5 MHz** band:
  - Number of hopping frequencies: **at least 15**
  - Average time of occupancy on any frequency: no greater than **0.4 seconds** within a period of 0.4 seconds multiplied by the number of hopping channels employed

## ISM Band Regulations (Cont.)

- **(2)** Systems using **digital modulation** techniques may operate in the 902-928 MHz, 2400-2483.5 MHz, and 5725-5850 MHz bands.
- The minimum **6 dB bandwidth** shall be at least **500 kHz**.

- **Note:**
  - The original defined **direct sequence spread spectrum (DSSS)** systems can be regarded as a kind of **digitally modulated** systems.
  - Some other transmission techniques can also be used for the applications of radio communications
    - **OFDM** for wireless LAN



## ISM Band Regulations (Cont.)

- **(b)** The **maximum peak** conducted output power of the intentional radiator shall not exceed the following:

- **(1)** For **frequency hopping** systems:
  - The FH systems in the **5725-5850 MHz** band: **1 watt**
  - The FH systems in the **2400-2483.5 MHz** band
    - Employing **at least 75** non-overlapping channels: **1 watt**
    - All other FH systems: **0.125 watts**
- **(2)** For FH systems in the **902-928 MHz** band:
  - Employing **at least 50** hopping channels: **1 watt**
  - Employing **less than 50** hopping channels: **0.25 watts**

# ISM Band Regulations (Cont.)

- **(3)** For systems using **digital modulation** in the 902-928 MHz, 2400-2483.5 MHz, and 5725-5850 MHz bands: **1 Watt**.
- **(4)** The conducted output power limit is based on the use of antennas with directional gains that **do not exceed 6 dBi**.
  - If transmitting antennas of directional gain **greater than** 6 dBi are used, the conducted output power from the intentional radiator shall be **reduced**
    - By the amount in dB that the directional gain of the antenna exceeds 6 dBi.



# ISM Band Regulations (Cont.)

- **(d)** In any **100 kHz** bandwidth **outside** the frequency band in which the spread spectrum or digitally modulated intentional radiator is operating, the radio frequency power that is produced by the intentional radiator shall be **at least 20 dB below** that in the 100 kHz bandwidth within the band that contains the highest level of the desired power.
- **(e)** For **digitally modulated systems**, the **power spectral density** conducted from the intentional radiator to the antenna shall not be greater than **8 dBm** in **any 3 kHz band** during any time interval of continuous transmission.