1] Summary Table

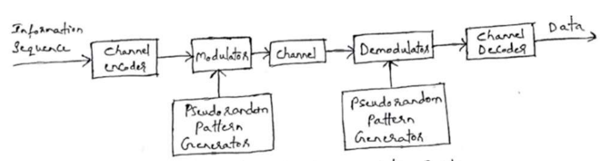
Parameter	Definition	Formula	Impact
Chip Rate	Rate of spreading sequence	Rc=N×RdR_c = N \times R_d	Increases multipath resistance
Jamming Margin	Resistance to interference	J=Eb/I0J = E_b / I_0	Higher margin → better anti-jamming
Processing Gain	Ratio of spread bandwidth to data bandwidth	PG=10log(Bs/Bd)PG = 10 \log (B_s / B_d)	Higher gain → better interference rejection

2] Model of a Spread Spectrum Direct Communication System (DCS)

A **Direct Communication System (DCS)** using **Spread Spectrum (SS)** enhances security, reduces interference, and improves signal robustness by spreading the signal over a wide frequency range. The system follows a structured process involving encoding, modulation, transmission, and decoding.

Key Components of the Model

1. **Information Sequence:** The original message or data that needs to be transmitted.
2. **Channel Encoder:** Adds redundancy using error correction techniques to improve data reliability.
3. **Pseudo Pattern Generator:** Generates a pseudo-random sequence for spreading the signal.
4. **Modulator:** Combines the encoded data with the pseudo-random sequence and converts it into a transmittable waveform (e.g., using BPSK or QPSK).
5. **Channel:** The medium through which the signal propagates (e.g., free space, fiber, or a wireless network).
6. **Demodulator:** Extracts the received signal from the carrier frequency and removes noise and interference.
7. **Channel Decoder:** Recovers the original data by applying error correction techniques.
8. **Output Data:** The final retrieved message after decoding, ideally matching the original information sequence.



Model of a spread spectrum digital Communication System

Characteristics of Spread Spectrum in DCS

- **Enhanced Security:** Unauthorized interception is difficult without the pseudo-random sequence.
- **Interference Resistance:** Spread signals are robust against narrowband noise and jamming.
- **Error Resilience:** Channel encoding and decoding improve data reliability in noisy environments.
- **Efficient Spectrum Utilization:** Multiple users can transmit simultaneously without severe interference.

This model is widely used in **CDMA, military communications, GPS, and secure wireless networks.**

3]Wireless LAN's

-**DSSS** spreads the data signal over a wider frequency range using a pseudo-random sequence (PN sequence), improving communication security and reliability.

-The **autocorrelation** function of the PN sequence ensures that the transmitted signal can be accurately retrieved at the receiver, while unwanted signals (noise or interference) are minimized.

-DSSS enhances **resistance to interference** from other devices, like microwaves or cordless phones, by spreading the signal across a broader frequency band.

-In **802.11b WLANs**, DSSS supports a maximum data rate of **11 Mbps** by using a **22 MHz-wide channel** and a **11-chip long PN sequence**.

-**Signal-to-noise ratio (SNR)** is improved in DSSS systems, allowing for better reception quality even in noisy environments or at low signal power levels.

-DSSS provides **security** by making it difficult for unauthorized users to intercept or decode the signal without the correct spreading code.

-**CDMA (Code Division Multiple Access)** is enabled in DSSS, allowing multiple devices to communicate on the same frequency band simultaneously without causing interference.

-The **processing gain** of DSSS is directly related to the width of the spread signal compared to the original data bandwidth, improving the overall communication range and reducing vulnerability to jamming.

- **Autocorrelation** of the PN sequence at the receiver ensures accurate signal recovery, as it maximizes the power at the correct time, and minimizes power at other times.

-DSSS is widely applied in **home networks**, **enterprise WLANs**, **public hotspots**, and **industrial IoT applications**, providing robust, secure, and high-performance wireless communication.

4]CDMA as Application of DSSS

 DSSS spreads the data signal over a wide frequency band by multiplying the signal with a unique pseudo-random sequence, enabling CDMA systems to allow multiple users to share the same frequency spectrum.

 In CDMA, each user is assigned a unique **spreading code** (PN sequence), which helps distinguish their signal from others in the same frequency band.

- **Signal separation** in CDMA is achieved through the orthogonality of the spreading codes, allowing multiple signals to coexist without interference.
- **Security** is inherent in CDMA, as the unique spreading codes make it difficult for unauthorized users to intercept or decode the transmitted signals.
- **DSSS** in CDMA provides strong **resistance to jamming** by spreading the signal over a broad frequency, making the system less vulnerable to interference.
- CDMA systems, using DSSS, help mitigate **multipath fading**, ensuring reliable communication even in environments with signal reflections.
- **Efficient spectrum utilization** is achieved in CDMA, as the same frequency band can be used simultaneously by multiple users with unique spreading codes.
- **Processing gain** in CDMA improves the signal-to-noise ratio (SNR), enhancing communication quality even in noisy or interference-prone environments.
- **Power control** is essential in CDMA to maintain uniform signal strength, ensuring that the spread signal reaches the receiver with consistent quality.
- **CDMA with DSSS** is widely used in **mobile communication systems** like **3G networks** and has applications in **GPS**, **satellite communication**, and **wireless networks**.

5]PN Sequence:

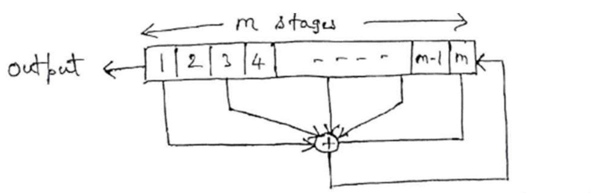
- A **PN sequence** is a binary sequence that mimics the properties of random noise.
- **Pseudo-random**: It is not truly random, but deterministically generated, making it reproducible at the receiver.
- Used in **spread spectrum techniques** such as **DSSS** (Direct Sequence Spread Spectrum) and **CDMA** (Code Division Multiple Access).
- Provides **security** and **resistance to interference** in communication systems.

Generation of PN Sequence Using m-Stage Shift Register with Linear Feedback:

- **Shift Register Structure:**
  - A series of **m flip-flops** connected in chain, each storing one bit of the sequence.
  - The contents shift on each clock cycle.
- **Linear Feedback:**
  - Output of specific flip-flops is XORed to generate the next bit.
  - The feedback is defined by a **feedback polynomial** (e.g., x4+x3+1x^4 + x^3 + 1x4+x3+1).
- **Feedback Polynomial:**

- Determines the taps used for feedback, ensuring the sequence generation.

- **Operation:**
  - Initial values are loaded into the register.
  - On each clock pulse, the XORed feedback value is inserted into the first flip-flop, shifting the rest of the register.



Properties of ML Sequence:

1. **Periodicity:**
   - The period of a sequence is 2m−12^m - 12m−1, where mmm is the number of stages in the shift register.
   - For example, a 3-stage LFSR produces a sequence with a period of 23−1=72^3 - 1 = 723−1=7.
2. **Maximal Period:**
   - It generates the longest possible sequence for a given register size.
3. **Balanced Sequence:**
   - The sequence has an almost equal number of 1's and 0's, ensuring uniform energy distribution.
4. **Autocorrelation:**
   - The autocorrelation function has a sharp peak at zero time shift and is close to zero for other time shifts, allowing easy signal recovery.
5. **Random-like Behavior:**
   - Despite being deterministic, the sequence behaves like a random sequence, useful for DSSS.
6. **Efficient for Spread Spectrum Systems:**
   - Ideal for **DSSS** and **CDMA** as it resists interference and eavesdropping.
7. **Implementation Simplicity:**
   - Easily implemented using **shift registers** with linear feedback for real-time communication systems.

6] What is FHSS?

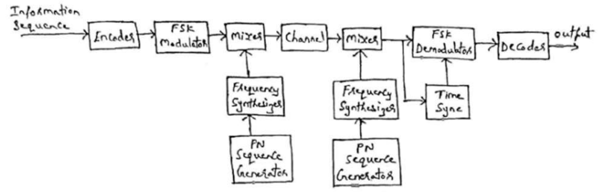
Frequency Hopped Spread Spectrum (FHSS) is a technique where the carrier frequency of a signal is rapidly changed (hopped) between several predefined channels. This approach spreads the signal over a wider frequency band, improving resistance to interference and providing better security. The hopping sequence is based on a pseudorandom number generator that is known to both the transmitter and the receiver.

Key Features of FHSS:

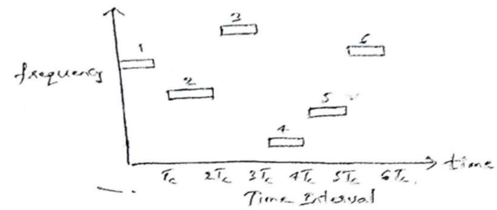
1. **Wideband Transmission:** Signal is spread across multiple frequency channels.
2. **Hopping Sequence:** Frequency hops are controlled by a pseudorandom sequence known to both ends.
3. **Resistance to Interference:** By spreading the signal, FHSS minimizes the impact of interference on any single frequency.
4. **Security:** It is harder for unauthorized users to intercept the signal without knowing the hopping pattern.

FHSS Block Diagram:

1. **Data Source:** Baseband data needs to be transmitted.
2. **Modulator:** Modulates the baseband data onto a carrier frequency.
3. **PN Sequence Generator:** Generates the pseudorandom hopping sequence.
4. **Frequency Hopping Generator:** Uses the PN sequence to shift the carrier frequency.
5. **Antenna:** Transmits the frequency-hopped signal.
6. **Receiver:** Demodulates the received signal based on the same hopping sequence.



Block Diagram of an FHSS System



FHSS Working Principle and Advantages

Working Principle of FHSS:

1. **Data Transmission:** Data is modulated onto a carrier at the initial frequency **f1**.
2. **Hopping:** The signal hops to **f2**, **f3**, etc., according to the pseudorandom sequence at fixed time intervals.
3. **Synchronization:** The receiver uses the same hopping sequence to synchronize and demodulate the received signal.
4. **Signal Recovery:** The receiver extracts the original data from the rapidly hopped signal.

Advantages of FHSS:

1. **Interference Resistance:** The signal spreads across frequencies, avoiding interference on any one frequency.
2. **Security:** Harder to intercept without knowing the hop pattern.
3. **Jamming Resistance:** Jamming a single frequency is ineffective as the signal hops between frequencies.

Applications of FHSS:

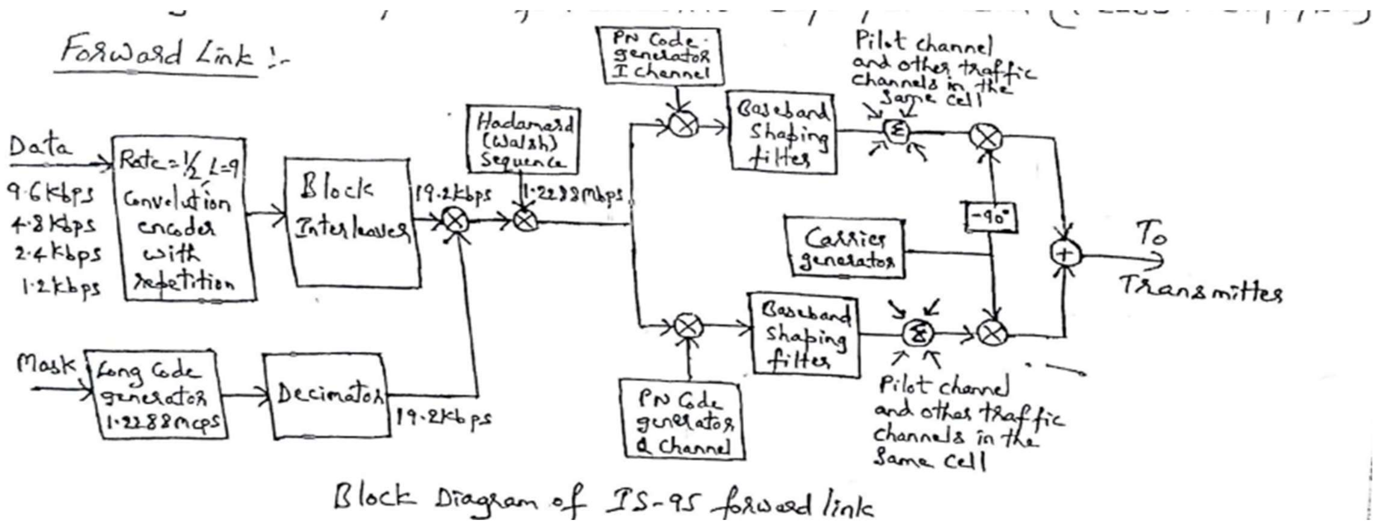
- **Bluetooth**: Short-range wireless communication.
- **Military**: Secure communication channels.
- **Wi-Fi (Older versions)**: Early wireless LANs used FHSS.

7] Explanation of the CDMA system based on IS-95 forward link:

1. **IS-95** is a **CDMA-based** system that allows multiple users to share the same frequency band by using unique spreading codes.
2. The **forward link** refers to the transmission from the **base station (BS)** to the **mobile station (MS)**.
3. The transmission uses a **wideband signal** spread across multiple frequencies using a **pseudo-random noise (PN) sequence**.
4. **PN codes** are unique for each user and are used to spread the data over a wider bandwidth to prevent interference from other users.
5. The base station transmits on different channels, such as the **pilot channel**, **sync channel**, **paging channel**, and **traffic channel**.
6. The **pilot channel** provides the mobile station with synchronization and timing reference for proper reception of the forward link signal.
7. The **sync channel** is used to send synchronization information to the mobile station for proper system alignment.
8. The **paging channel** is used for transmitting paging messages to notify the mobile station about incoming calls or messages.
9. The **traffic channel** carries user data and voice traffic between the base station and mobile station.
10. **QPSK (Quadrature Phase Shift Keying)** is used for modulation in the IS-95 forward link to map the data onto the carrier frequency.
11. The base station adjusts the **transmit power** based on the mobile station's distance and fading conditions to ensure reliable signal reception.
12. **Power control** is a key feature in IS-95 to ensure that the signal strength at the mobile station is sufficient for proper demodulation while minimizing interference.
13. The mobile station uses the same **PN codes** to demodulate the received signal, effectively separating the signals of different users.
14. **Forward Error Correction (FEC)** is employed to correct any errors introduced during the transmission due to noise and interference, enhancing signal quality.
15. **Soft handoff** is supported in IS-95, which allows the mobile station to communicate with multiple base stations simultaneously when moving between coverage areas, ensuring uninterrupted service.

16. IS-95 employs **spread-spectrum technology**, making the system more resistant to **interference**, **jamming**, and **multipath fading**, improving communication quality.

This covers the **IS-95 forward link** CDMA system in a **16-point format**, explaining its working principles, key



features, and functionality.

8] Generation And demodulation od DSSS

Signal Generation (Transmitter Side)

1. **Data Signal**: The process begins with the baseband data signal, which represents the information to be transmitted (e.g., binary data).
2. **Pseudo-Random Noise (PN) Sequence**: A **PN sequence** (also known as spreading code) is generated. This sequence is a high-speed binary sequence, usually much faster than the data signal.
3. **Spreading the Data**: The data signal is combined with the PN sequence through a process called **binary phase shift keying (BPSK)** or **quadrature phase shift keying (QPSK)**. Each bit of data is multiplied by a set of bits from the PN sequence. This operation spreads the data signal over a much wider bandwidth.
4. **Modulation**: The resulting spread signal is then modulated onto a carrier signal (e.g., using **BPSK**, **QPSK**, or other modulation techniques) to shift the signal into the radio frequency spectrum.
5. **Transmission**: The modulated and spread signal is then transmitted through an antenna,

2. Signal Demodulation (Receiver Side)

1. **Received Signal**: At the receiver end, the transmitted signal (spread signal) is received by the antenna.
2. **Carrier Demodulation**: The first step is to demodulate the received signal using the same modulation technique that was used during transmission. For example, if **BPSK** was used for modulation, the receiver will apply **BPSK demodulation**.
3. **Synchronization**: The receiver needs to synchronize the received signal with the **PN sequence** used at the transmitter. This is achieved by using a **local replica of the PN sequence** that is generated at the receiver.
4. **Correlation**: The received signal is then correlated with the locally generated PN sequence. Since the PN sequence is known at both the transmitter and receiver, this correlation helps to recover the original data by suppressing noise and interference.
5. **Data Recovery**: The result of the correlation is a high peak at the times when the PN sequence is synchronized with the data, which allows the receiver to recover the original data signal. Any noise or unwanted signals outside the synchronization will result in lower correlation values.
6. **Output**: Finally, after demodulation and correlation, the data is recovered, and the original information is extracted and passed to the destination (e.g., a mobile phone or a computer).