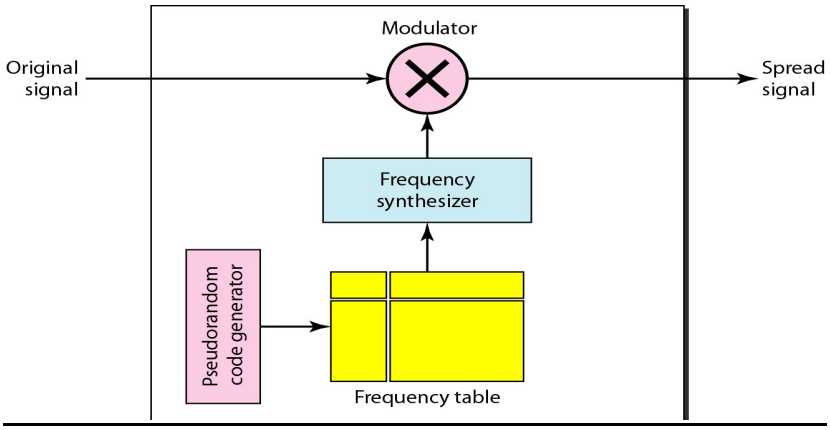
Course Name: A Level (2nd Sem) Subject: DCN

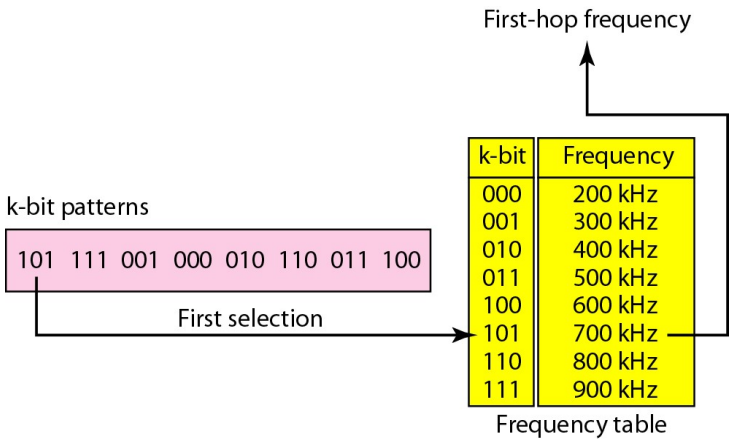
Topic: Techniques of Spread Spectrum Date: 20-03-20

Frequency Hopping Spread Spectrum (FHSS):

- The frequency hopping spread spectrum (FHSS) technique uses M different carrier frequencies that are modulated by the source signal. At one moment, the signal modulates one carrier frequency; at the next moment, the signal modulates another carrier frequency. Although the modulation is done using one carrier frequency at a time, M frequencies are used in the long run. The bandwidth occupied by a source after spreading is $B_{FHSS} >> B$.
- Figure shows the general layout for FHSS. A pseudorandom code generator, called pseudorandom noise (PN), creates a k-bit pattern for every hopping period. The frequency table uses the pattern to find the frequency to be used for this hopping period and passes it to the frequency synthesizer. The frequency synthesizer creates a carrier signal of that frequency, and the source signal modulates the carrier signal.



- Suppose we have decided to have eight hopping frequencies. In this case, *M is* 8 and *k* is 3. The pseudorandom code generator will create eight different 3-bit patterns. These are mapped to eight different frequencies in the frequency table.



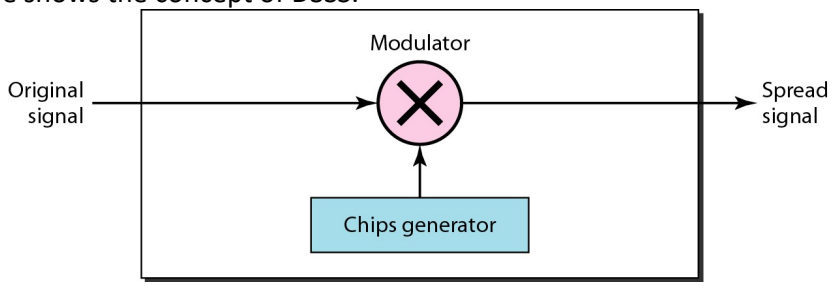
The pattern for this station is 101, 111, 001, 000, 010, 110, 011, 100. The pattern is pseudorandom it is repeated after eight hoppings. This means that at hopping period 1, the pattern is 101. The frequency selected is 700 kHz; the source signal modulates this carrier frequency. The second k-bit pattern selected is 111, which selects the 900-kHz carrier; the eighth pattern is 100, the frequency is 600 kHz. After eight hoppings, the pattern repeats, starting from 101 again.

Thus, this scheme can accomplish the goals of spread spectrum in the following way:

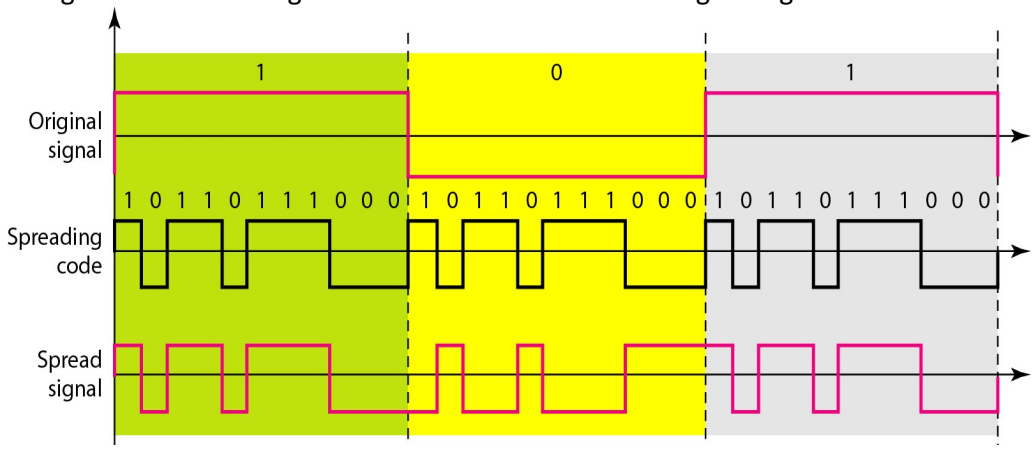
- If there are many k-bit patterns and the hopping period is short, a sender and receiver can have privacy. If an intruder tries to intercept the transmitted signal, she can only access a small piece of data because she does not know the spreading sequence to quickly adapt herself to the next hop.
- The scheme has also an antijamming effect. A malicious sender may be able to send noise to jam the signal for one hopping period (randomly), but not for the whole period.

Direct Sequence Spread Spectrum (DSSS):

- The direct sequence spread spectrum (DSSS) technique also expands the bandwidth of the original signal, but the process is different in the way that in DSSS, we replace each data bit with n bits using a spreading code. In other words, each bit is assigned a code of n bits, called chips, where the chip rate is n times that of the data bit. Figure shows the concept of DSSS.



- For example, the sequence used in a wireless LAN, where n is 11 (the famous Barker sequence). Also assume that the original signal and the chips in the chip generator use polar NRZ encoding. Figure shows the chips and the result of multiplying the original data by the chips to get the spread signal. The spreading code is 11 chips having the pattern 10110111000 (in this case). If the original signal rate is N, the rate of the spread signal is 11N. This means that the required bandwidth for the spread signal is 11 times larger than the bandwidth of the original signal.



- Thus, this scheme can accomplish the goals of spread spectrum by providing privacy if the intruder does not know the code and also it can provide immunity against interference if each station uses a different code.

Exercises:

1. **Define FHSS and DSSS. Explain the difference on the basis of how they achieve bandwidth spreading.**

2. **"The techniques FHSS and DSSS accomplish the goals of spread spectrum". Justify the comment.**