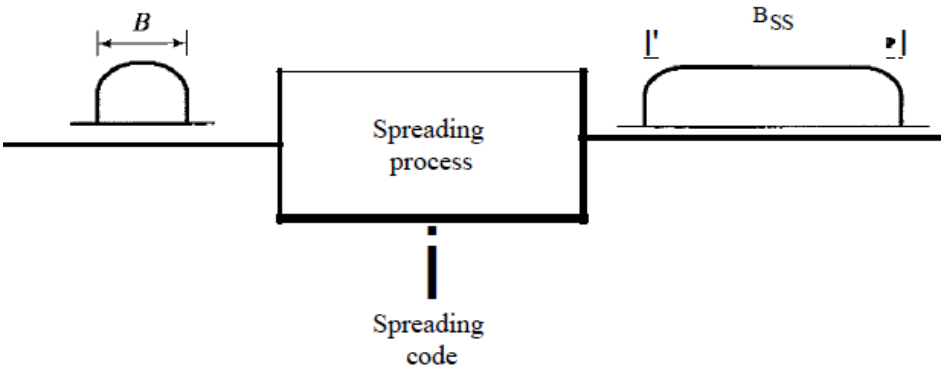
Spread spectrum

Spread Spectrum was originally developed for military applications, to provide secure communications by spreading the signal over a large frequency band.
Spread spectrum is designed to be used in wireless applications. In wireless applications, all stations use air (or a vacuum) as the medium for communication. Stations must be able to share this medium without interception by an eavesdropper and without being subject to jamming from a malicious intruder. To achieve these goals, spread spectrum techniques add redundancy.They spread the original spectrum needed for each station. If the required bandwidth for each station is B, spread spectrum expands it to Bss such that Bss » B .The expanded bandwidth allows the source to wrap its message in a protective envelope for a more secure transmission.

Spread spectrum achieves its goals through two principles:
1. The bandwidth allocated to each station needs to be, by far, larger than what is needed. This allows redundancy.
2. The spreading process occurs after the signal is created by the source.



After the signal is created by the source, the spreading process uses a spreading code and spreads the bandwidth. The figure shows the original bandwidth B and the spreaded bandwidth Bss such that Bss is much greater than B.

There are two techniques to spread the bandwidth: frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS).

Frequency Hopping Spread Spectrum (FHSS)

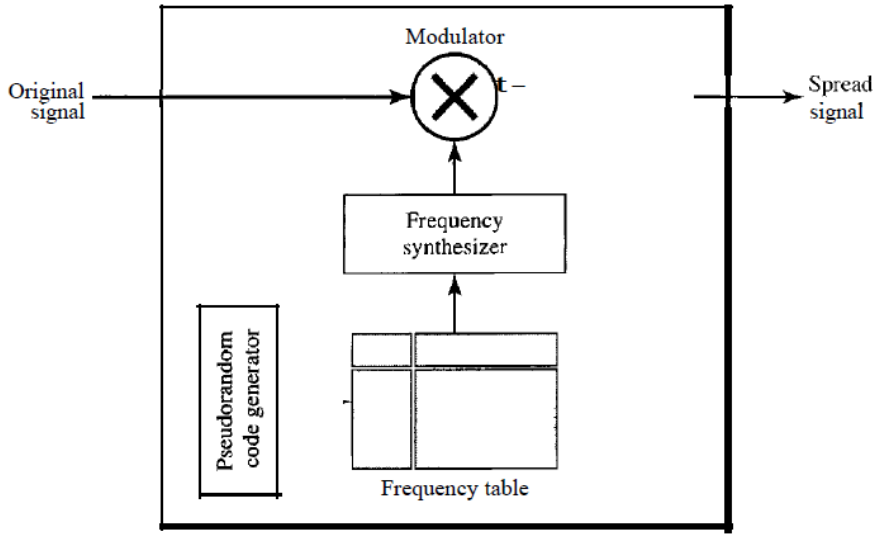
In FHSS signal hops from frequency to frequency at fixed intervals. At each successive interval, a new carrier frequency is selected.

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.

In other words this is frequency hopping technique, where the users are made to change the frequencies of usage, from one to another in a specified time interval, hence called as frequency hopping.

The frequencies of the data are hopped from one to another in order to provide a secure transmission.

In FHSS, the transmitter hops between available frequencies in a pseudo-random sequence which is known only to the sender and receiver
The frequency table uses this pattern generated by the pseudorandom code generator to find the frequency to be used for a hopping period and passes it to the frequency synthesizer. The frequency synthesizer creates a carrier signal of that frequency. The original signal modulates this carrier signal.
The figure shows the general layout for FHSS.



Interception by an eavesdropper can be prevented. If an intruder tries to intercept the transmitted signal, he can only access a small piece of data because he does not know the spreading sequence to quickly adapt himself to the next hop . This helps in protecting data from an intruder. No intruder will get any useful information unless he knows the spreading sequence which is known only to the sender and the receiver.
The scheme has also an **antijamming effect**. If a malicious sender manages to understand one frequency he may be able to send noise to jam the signal for one hopping period but not for the whole period. This will protect our data being destroyed.

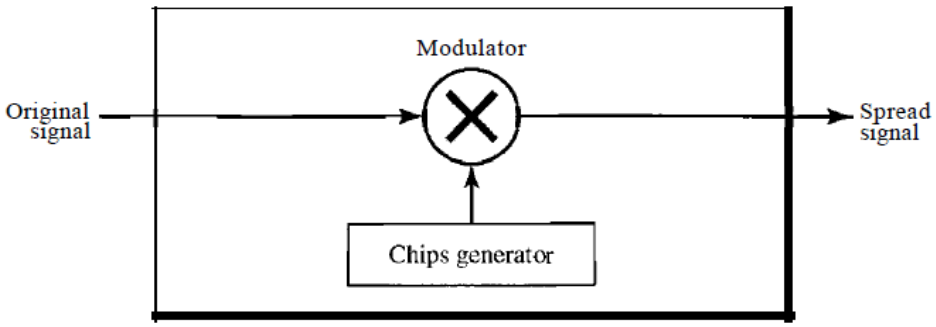
Bandwidth Sharing

If the number of hopping frequencies is *M,* we can multiplex *M* channels into one by using the same B_{ss} bandwidth. This is possible because a station uses just one frequency in each hopping period; *M* - 1 other frequencies can be used by other *M* - 1 stations. *M* different stations can use the same set of frequencies. For example, a frequency was allotted to sender 1 for a particular period of time. Now, after a while, sender 1 hops to the other frequency and sender 2 uses the first frequency, which was previously used by sender 1. This is called as frequency reuse**.**

Direct Sequence Spread Spectrum (DSSS)

In DSSS each bit in original signal is represented by multiple bits in the transmitted signal.

The direct sequence spread spectrum (DSSS) technique also expands the bandwidth of the original signal, but the process is different. Whenever a user wants to send data using this DSSS technique, each and every bit of the user data is multiplied by a secret code, called as chipping code. This chipping code is nothing but the spreading code which is multiplied with the original message and transmitted. The receiver uses the same code to retrieve the original message.
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. The ratio of chips to data is known as the spreading ratio ; the higher the ratio, the more immune to interference the signal is, because if part of the transmission is corrupted, the data can still be recovered from the remaining part of the chipping code.



Although spread spectrum techniques were originally designed for military uses, they are now being used widely for commercial purpose.