

Introduction to Spread Spectrum

By Randy Roberts, Director of RF/Spread Spectrum Consulting

Over the last eight or nine years a new commercial marketplace has been emerging. Called spread spectrum, this field covers the art of secure digital communications that is now being exploited for commercial and industrial purposes. In the next several years hardly anyone will escape being involved, in some way, with spread spectrum communications. Applications for commercial spread spectrum range from "wireless" LAN's (computer to computer local area networks), to integrated bar code scanner/palmtop computer/radio modem devices for warehousing, to digital dispatch, to digital cellular telephone communications, to "information society" city/area/state or country wide networks for passing faxes, computer data, email, or multimedia data.

The IEEE Spectrum of August, 1990 contained an article entitled Spread Spectrum Goes Commercial, by Donald L. Schilling of City College of New York, Raymond L. Pickholtz of George Washington University, and Laurence B. Milstein of UC San Diego. This article summarized the coming of commercial spread spectrum:

"Spread-spectrum radio communications, long a favorite technology of the military because it resists jamming and is hard for an enemy to intercept, is now on the verge of potentially explosive commercial development. The reason: spread-spectrum signals, which are distributed over a wide range of frequencies and then collected onto their original frequency at the receiver, are so inconspicuous as to be 'transparent.' Just as they are unlikely to be intercepted by a military opponent, so are they unlikely to interfere with other signals intended for business and consumer users -- even ones transmitted on the same frequencies. Such an advantage opens up crowded frequency spectra to vastly expanded use.

"A case in point is a two-year demonstration project the Federal Communications Commission (FCC) authorized in May (1990) for Houston, Texas, and Orlando, Fla. In both places, a new spread spectrum personal communications network (PCN) will share the 1.85-1.9-gigahertz band with local electric and gas utilities. The FCC licensee, Millicom Inc., a New York City-based cellular telephone company, expects to enlist 45000 subscribers.

"The demonstration is intended to show that spread-spectrum users can share a frequency band with conventional microwave radio users--without one group interfering with the other -- thereby increasing the efficiency with which that band is used. . . . "

How Spread Spectrum Works

Spread Spectrum uses wide band, noise-like signals. Because Spread Spectrum signals are noise-like, they are hard to detect. Spread Spectrum signals are also hard to Intercept or demodulate. Further, Spread Spectrum signals are harder to jam (interfere with) than narrowband signals. These Low Probability of Intercept (LPI) and anti-jam (AJ) features are why the military has used Spread Spectrum for so many years. Spread signals are intentionally made to be much wider band than the information they are carrying to make them more noise-like.

Spread Spectrum signals use fast codes that run many times the information bandwidth or data rate. These special "Spreading" codes are called "Pseudo Random" or "Pseudo Noise" codes. They are called "Pseudo" because they are not real gaussian noise.

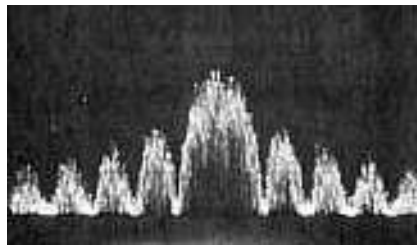
Spread Spectrum transmitters use similar transmit power levels to narrow band transmitters. Because Spread Spectrum signals are so wide, they transmit at a much lower spectral power density, measured in Watts per Hertz, than narrowband transmitters. This lower transmitted power density characteristic gives spread signals a big plus. Spread and narrow band signals can occupy the

same band, with little or no interference. This capability is the main reason for all the interest in Spread Spectrum today.

More Details on Spread Spectrum

Over the last 50 years, a class of modulation techniques usually called "Spread Spectrum," has been developed. This group of modulation techniques is characterized by its wide frequency spectra. The modulated output signals occupy a much greater bandwidth than the signal's baseband information bandwidth. To qualify as a spread spectrum signal, two criteria should be met:

1. The transmitted signal bandwidth is much greater than the information bandwidth.
2. Some function other than the information being transmitted is employed to determine the resultant transmitted bandwidth.



A Spectrum Analyzer Photo of a Direct Sequence (DS) Spread Spectrum signal. Most commercial part 15.247 spread spectrum systems transmit an RF signal bandwidth as wide as 20 to 254 times the bandwidth of the information being sent. Some spread spectrum systems have employed RF bandwidths 1000 times their information bandwidth. Common spread spectrum systems are of the "direct sequence" or "frequency hopping" type, or else some combination of these two types (called a "hybrid").



A Spectrum Analyzer Photo of a Frequency Hop (FH) Spread Spectrum signal. There are also "Time Hopped" and "Chirp" systems in existence. Time hopped spread spectrum systems have found no commercial application to date.

However, the arrival of cheap random access memory (RAM) and fast micro-controller chips make time hopping a viable alternative spread spectrum technique for the future. "Chirp" signals are often employed in radar systems and only rarely used in commercial spread spectrum systems.

Direct sequence systems -- Direct sequence spread spectrum systems are so called because they employ a high speed code sequence, along with the basic information being sent, to modulate their RF carrier. The high speed code sequence is used directly to modulate the carrier, thereby directly setting the transmitted RF bandwidth. Binary code sequences as short as 11 bits or as long as $[2^{(89)} - 1]$ have been employed for this purpose, at code rates from under a bit per second to several hundred megabits per second.

The result of modulating an RF carrier with such a code sequence is to produce a signal centered at the carrier frequency, direct sequence modulated spread spectrum with a $(\sin x/x)^2$ frequency spectrum. The main lobe of this spectrum has a bandwidth twice the clock rate of the modulating code, from null to null. The sidelobes have a null to null bandwidth equal to the code's clock rate. Figure 1 illustrates the most common type of direct sequence modulated spread spectrum signal. Direct sequence spectra vary somewhat in spectral shape depending upon the actual carrier and data modulation used. The signal illustrated is that for a binary phase shift keyed (BPSK) signal, which is the most common modulation signal type used in direct sequence systems.

Frequency hopping systems -- The wideband frequency spectrum desired is generated in a different manner in a frequency hopping system. It does just what its name implies. That is, it "hops" from frequency to frequency over a wide band. The specific order in which frequencies are occupied is a function of a code sequence, and the rate of hopping from one frequency to another is a function of the information rate. The transmitted spectrum of a frequency hopping signal is quite different from that of a direct sequence system. Instead of a $[(\sin x)/x]^2$ -shaped envelope, the frequency hopper's output is flat over the band of frequencies used. Figure 2 shows an output spectrum of a frequency hopping

system. The bandwidth of a frequency hopping signal is simply w times the number of frequency slots available, where w is the bandwidth of each hop channel.

"Inside" Spread Spectrum

This section is intended to gently introduce the reader to the more intricate aspects of the rapidly growing world of spread spectrum, wireless local and wide area networks, as well as introduce the evolution (some may call it explosion) in new communications technologies such as PCN/PCS. We will also try to thoroughly define new terms and concepts the first time we use them.

As an introduction, a little history lesson and a few definitions seem to be in order. Spread Spectrum (SS) dates back to World War II. A German lady scientist was granted a patent on a simple frequency hopping CW system. The allies also experimented with spread spectrum in World War II. These early research and development efforts tried to provide countermeasures for radar, navigation beacons and communications. The U. S. Military has used SS signals over satellites for at least 25 years. An old, but faithful, highly capable design like the Magnavox USC-28 modem is an example of this kind of equipment. Housed in two or three six foot racks, it had selectable data rates from a few hundred bits per second to about 64 kBits per second. It transmitted a spread bandwidth of 60 MHZ. Many newer commercial satellite systems are now converting to SS to increase channel capacity and reduce costs.

Over the last twenty years, many spread spectrum signals have appeared on the air. The easiest way to characterize these modulations is by their frequency spectra. These SS signals occupy a much greater bandwidth than needed by the information bandwidth of the transmitted data. To rate being called an SS signal, two technicalities must be met:

- The signal bandwidth must be much wider than the information bandwidth.

- Some code or pattern, other than the data to be transmitted, determines the actual on-the-air transmit bandwidth.

In today's commercial spread spectrum systems, bandwidths of 10 to 100 times the information rates are used. Military systems have used spectrum widths from 1000 to 1 million times the information bandwidth. There are two very common spread spectrum modulations: frequency hopping and direct sequence. At least two other types of spreading modulations have been used: time hopping and chirp.

What Exactly is Spread Spectrum?

One way to look at spread spectrum is that it trades a wider signal bandwidth for better signal to noise ratio. Frequency hop and direct sequence are well-known techniques today. The following paragraphs will describe each of these common techniques in a little more detail and show that pseudo noise code techniques provide the common thread through all spread spectrum types.

Frequency hopping is the easiest spread spectrum modulation to use. Any radio with a digitally controlled frequency synthesizer can, theoretically, be converted to a frequency hopping radio. This conversion requires the addition of a pseudo noise (PN) code generator to select the frequencies for transmission or reception. Most hopping systems use uniform frequency hopping over a band of frequencies. This is not absolutely necessary, if both the transmitter and receiver of the system know in advance what frequencies are to be skipped. Thus a frequency hopper in two meters, could be made that skipped over commonly used repeater frequency pairs. A frequency hopped system can use analog or digital carrier modulation and can be designed using conventional narrow band radio techniques. De-hopping in the receiver is done by a synchronized pseudo noise code generator that drives the receiver's local oscillator frequency synthesizer.

The most practical, all digital version of SS is direct sequence. A direct sequence system uses a locally generated pseudo noise code to encode digital data to be

transmitted. The local code runs at much higher rate than the data rate. Data for transmission is simply logically modulo-2 added (an EXOR operation) with the faster pseudo noise code. The composite pseudo noise and data can be passed through a data scrambler to randomize the output spectrum (and thereby remove discrete spectral lines). A direct sequence modulator is then used to double sideband suppressed carrier modulate the carrier frequency to be transmitted. The resultant DSB suppressed carrier AM modulation can also be thought of as binary phase shift keying (BPSK). Carrier modulation other than BPSK is possible with direct sequence. However, binary phase shift keying is the simplest and most often used SS modulation technique.

An SS receiver uses a locally generated replica pseudo noise code and a receiver correlator to separate only the desired coded information from all possible signals. A SS correlator can be thought of as a very special matched filter -- it responds only to signals that are encoded with a pseudo noise code that matches its own code. Thus, an SS correlator can be "tuned" to different codes simply by changing its local code. This correlator does not respond to man made, natural or artificial noise or interference. It responds only to SS signals with identical matched signal characteristics and encoded with the identical pseudo noise code.

What Spread Spectrum Does

The use of these special pseudo noise codes in spread spectrum (SS) communications makes signals appear wide band and noise-like. It is this very characteristic that makes SS signals possess the quality of Low Probability of Intercept. SS signals are hard to detect on narrow band equipment because the signal's energy is spread over a bandwidth of maybe 100 times the information bandwidth.

The spread of energy over a wide band, or lower spectral power density, makes SS signals less likely to interfere with narrowband communications. Narrow band communications, conversely, cause little to no interference to SS systems

because the correlation receiver effectively integrates over a very wide bandwidth to recover an SS signal. The correlator then "spreads" out a narrow band interferer over the receiver's total detection bandwidth. Since the total integrated signal density or SNR at the correlator's input determines whether there will be interference or not. All SS systems have a threshold or tolerance level of interference beyond which useful communication ceases. This tolerance or threshold is related to the SS processing gain. Processing gain is essentially the ratio of the RF bandwidth to the information bandwidth.

A typical commercial direct sequence radio, might have a processing gain of from 11 to 16 dB, depending on data rate. It can tolerate total jammer power levels of from 0 to 5 dB stronger than the desired signal. Yes, the system can work at negative SNR in the RF bandwidth. Because of the processing gain of the receiver's correlator, the system functions at positive SNR on the baseband data. Besides being hard to intercept and jam, spread spectrum signals are hard to exploit or spoof. Signal exploitation is the ability of an enemy (or a non-network member) to listen in to a network and use information from the network without being a valid network member or participant. Spoofing is the act of falsely or maliciously introducing misleading or false traffic or messages to a network. SS signals also are naturally more secure than narrowband radio communications. Thus SS signals can be made to have any degree of message privacy that is desired. Messages can also, be cryptographically encoded to any level of secrecy desired. The very nature of SS allows military or intelligence levels of privacy and security to be had with minimal complexity. While these characteristics may not be very important to everyday business and LAN (local area network) needs, these features are important to understand.

Some Spread Spectrum Terms Defined

Spread spectrum technology seems to present an alphabet soup to most newcomers. We define some of the more commonly used terms in this field in the following text box. For a complete glossary, see our complete [Glossary](#).

A Brief Spread Spectrum Glossary

- **AJ:** Anti-Jam, designed to resist interference or jamming.
- **BPSK:** Binary Phase Shift Keying -- Digital DSB suppressed carrier modulation.
- **CDMA:** Code Division Multiple Access -- a way to increase channel capacity.
- **CHIP:** The time it takes to transmit a bit or single symbol of a PN code.
- **CODE:** A digital bit stream with noise-like characteristics.
- **CORRELATOR:** The SS receiver component that demodulates a Spread Spectrum signal.
- **DE-SPREADING:** The process used by a correlator to recover narrowband information from a spread spectrum signal.
- **WIRELESS LAN:** Wireless Local Area Network - a 1,000-foot or less range computer-to-computer data communications network.
- **PCN:** Personal Communication Network. PCNs are usually short range (hundreds of feet to 1 mile or so) and involve cellular radio type architecture. Services include digital voice, FAX, mobile data and national/international data communications.
- **PCS:** Personal Communication System. PCSs are usually associated with cordless telephone type devices. Service is typically digital voice only.
- **PN:** Pseudo Noise - a digital signal with noise-like properties.
- **RF:** Radio Frequency - generally a frequency from around 50 kHz to around 3 GHz. RF is usually referred to whenever a signal is radiated through the air.
- **SS:** Spread Spectrum, a wideband modulation which imparts noise-like characteristics to an RF signal.
- **WIRELESS UAN:** Wireless Universe Area Network - a collection of wireless MANs or WANs that link together an entire nation or the world. UANs use very small aperture (VSAT) earth station gateway technology.

Conclusion

Our world is rapidly changing -- computers have gone from mainframes to palmtops. Radio communications has gone from lunchbox sized (or trunk mounted/remote handset car phone) to cigarette-pack-sized micro-cellular telephone technology. The technical challenges of this progress are significant. The new opportunities created by this new technology are also significant. We've talked here about some of the very basic principles in spread spectrum and

talked about evolving career opportunities -- isn't it time somebody did something about moving forward in the new millennium?

About the Author:

Randy Roberts has over 30 years experience in communications, electronics and spread spectrum system design. He graduated with a BSEE in 1970 from UC Irvine. For many years prior to his retirement he operated RF/Spread Spectrum Consulting, an independent product development, publishing, strategic planning and training company. He is the founder and former publisher of Spread Spectrum Scene Online.