Spread Spectrum Series Part 1

By CDMA Design Staff of Berkeley Varitronics Systems

The application of telecommunications is often about ‘bandwidth conservation’. The technology of Spread Spectrum is exactly the opposite philosophy. Spread spectrum employs a novel form of modulation in which the RF bandwidth of the signal is much larger than that needed for traditional modulation schemes and the bandwidth is independent of the modulation content.

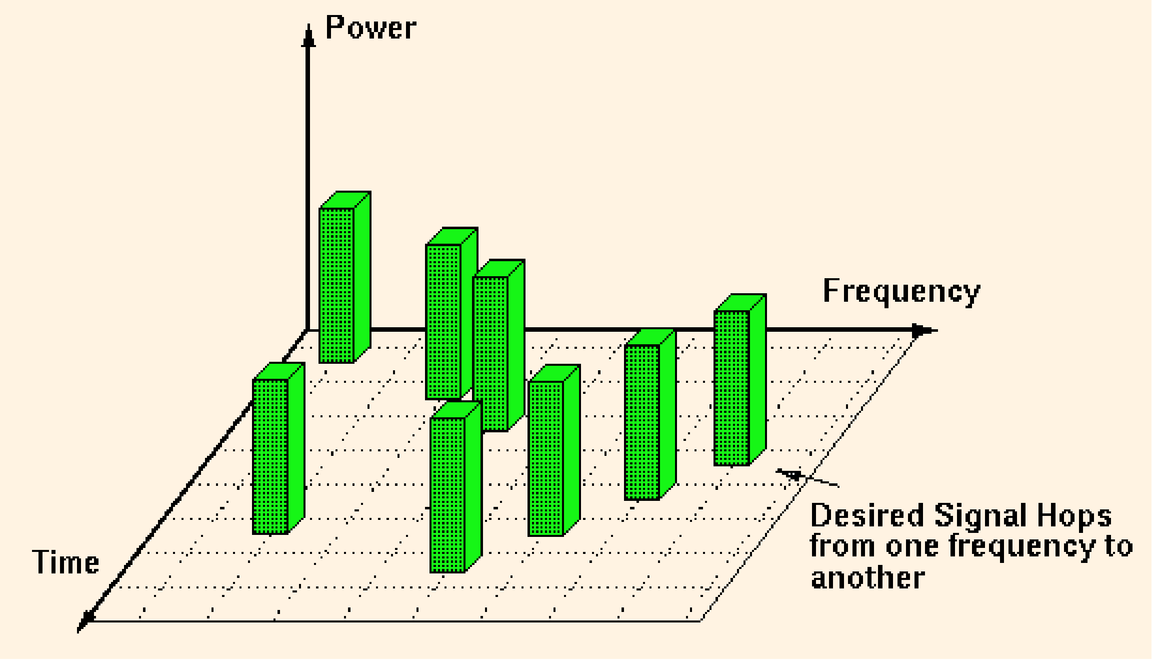
Historically spread spectrum originated back in the mid-thirties and with military applications during World War II as a means to avoid enemy jamming and detection of radio signals. Only with the advent of Large Scale Integrated circuits could the commercial sector afford the cost of such complex circuits and systems. In the early eighty’s the FCC recognized that the spectrum was becoming increasingly noisy and contained greater interference in most RF bands. Conventional wisdom suggests that the narrower the RF bandwidth, the better the chance that “the signal will get through”. This was proven untrue back in 1948 by Claude Shannon’s famous paper on “A Mathematical Theory of Communications” where the Hartley-Shannon Theorem states that the channel capacity **C** of a band-limited Gaussian channel is:

$$C=W \log_2 (1+S/N) \text{ bits/sec}$$

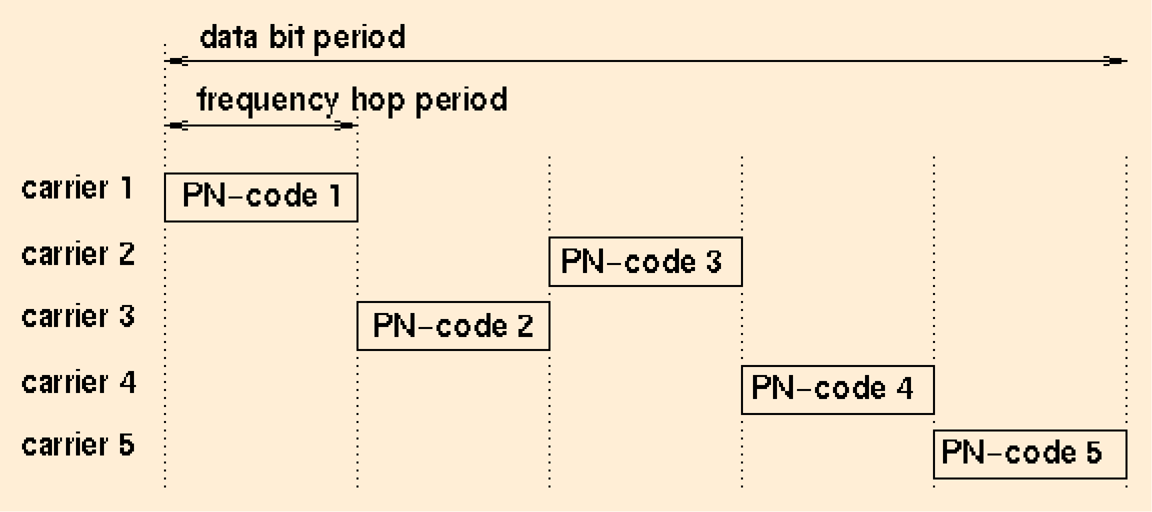
Equation shows the advantage of using a broad bandwidth to transmit messages.

where:

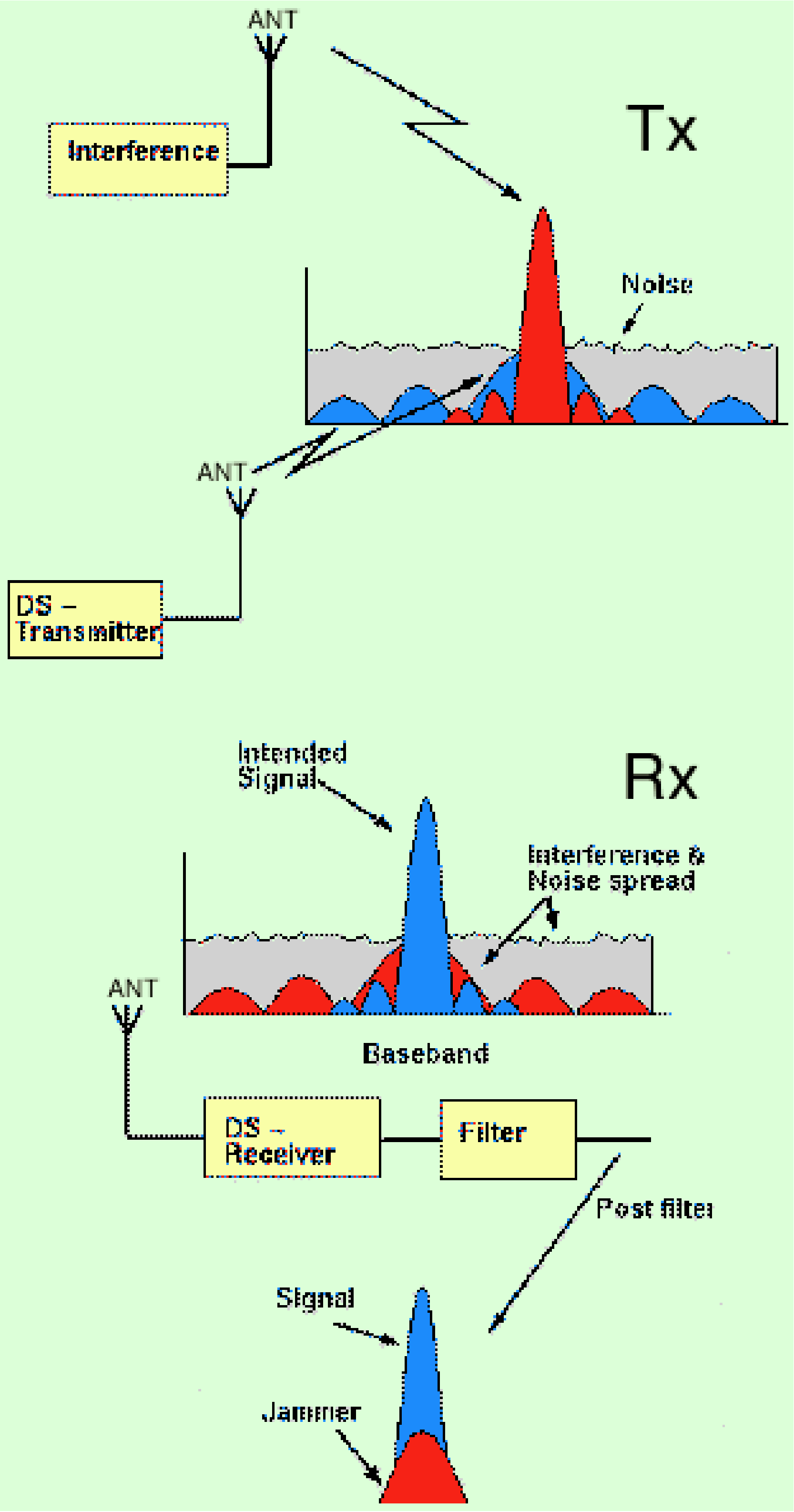
C is the channel capacity,
W is the bandwidth,
S is the signal power and
N is the noise within the channel bandwidth



This theorem states that if the communication channel were perfectly noiseless, the channel's capacity would be unlimited. Practically speaking, there is no such thing as a noiseless channel; so if we make the bandwidth of the channel **W** infinitely wide we still could not make the capacity infinite because channel noise increases proportionately with channel bandwidth. Within reason however, one can trade power for bandwidth favorably.



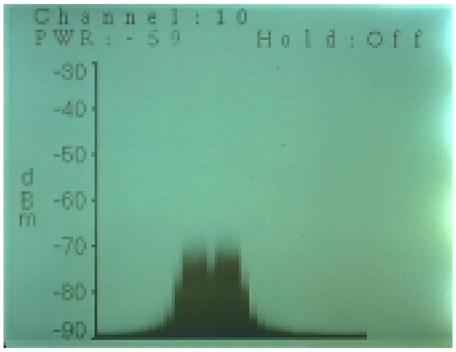
Consider the Navy's GPS (Global Positioning System) which has a very small power density at any point within the occupied bandwidth. The signal is well below the noise floor of the receiver. This is an excellent example of Direct Sequence Spread Spectrum (DSSS) where the bandwidth is favorable traded for robustness. In fact, the average signal strength at the antenna terminals of a GPS receiver is in the order of –160 dBW for the C/A code channel.



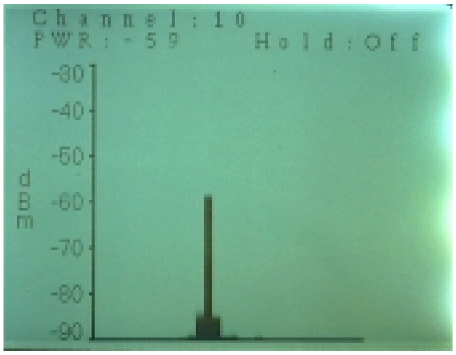
There are several subtle features of spread spectrum modulation

a) It reduces interference because most interference sources are relatively narrow-band and during the de-spreading process those signals are automatically rejected.
b) The length and sophistication of the pseudo-random codes used can be such that unauthorized recovery would be difficult or impossible so the channel has an implied security.
c) The low power density makes for easy hiding of the RF signal and lowers the probability of detection.
d) Because of its large bandwidth, CDMA signals are less susceptible to fade distortions.

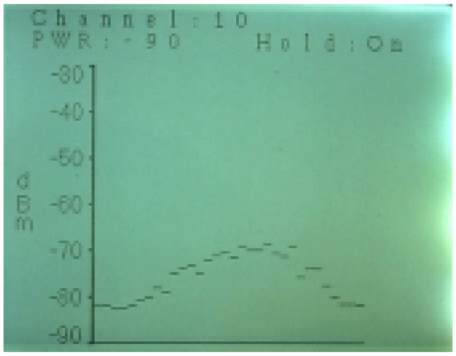
Direct Sequence Spread Spectrum (DSSS) is also known as code multiplication and is used in situations where a shared transmission media or channel is desirable. Consider a baseband digital signal at 10 kbps with a bit width of 100μs. The bandwidth of this baseband signal is about 5 kHz. If this baseband signal is then multiplied by a random digital signal (called a “code” signal) at say 1,000 times the rate of the baseband digital signal, or a code rate of 10 Mbps, the code signal has a bandwidth of about 5 MHz. The effect of the multiplication is a new signal that has a bandwidth of 5 MHz, and this new signal would then be used to modulate an appropriate RF carrier for transmission. Thus the information in the baseband digital signal has been spread over a bandwidth 1,000 times greater than the original signal. Code signals have special properties because they are diverse yet repeatable. They are generally made from pseudo-random (PN) polynomial generators selected for their unique correlation properties.



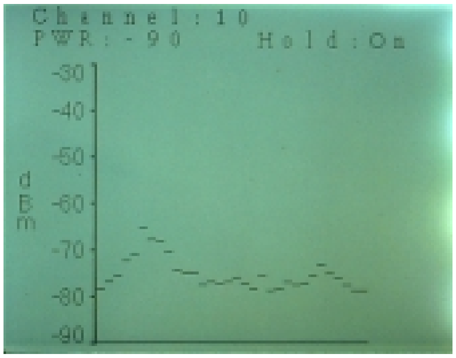
Wideband DSSS 5 MHz jammer



Narrowband jammer



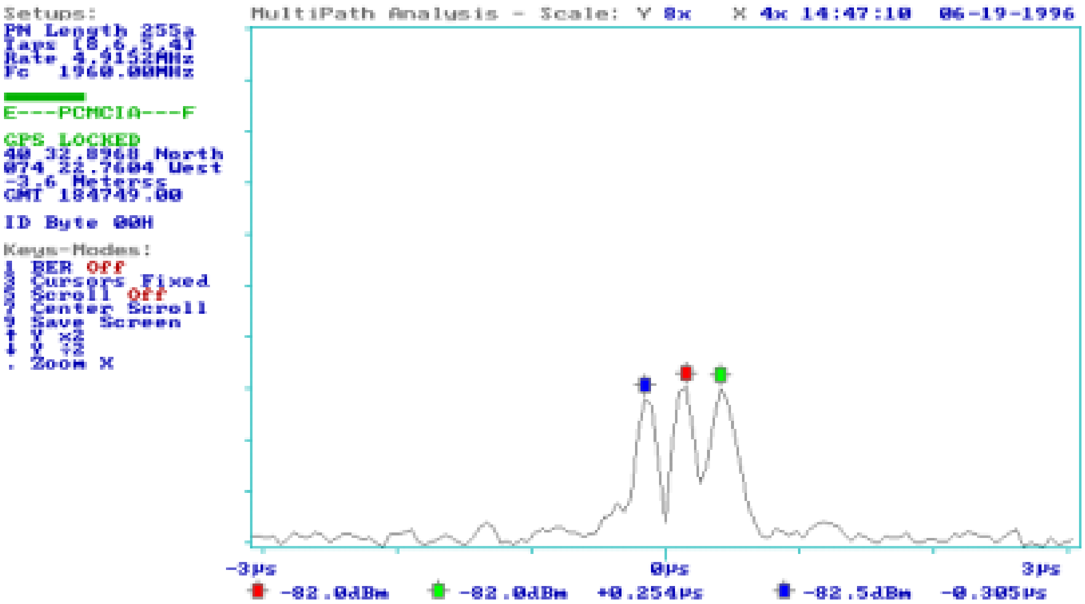
Peak Hold-microwave oven interference



Peak Hold- 802.11 Access point

At the receiver the inverse process is performed to obtain the original baseband digital signal. After demodulating the RF carrier, the signal is multiplied by an identical random code in precise synchrony. Because +1 times +1 and –1 times –1 are both = +1, the multiplication at the receiver by the identical code recreates the original baseband digital signal. If any other signals are present, their codes will differ and they will not pass through the inverse multiplication process. In this way, a number of diverse baseband digital signals, each with it's own unique digital pattern of random codes, can share the common communication channel.

When two similar PN sequences are compared out of phase their correlation is nil but when they are exactly in phase their correlation to each other produces a huge peak that can be used for signal synchronization; to aid in the demodulation process. This synchronization process has been the major complicating factor for spread spectrum links because is difficult to extract timing from a signal that is well below the noise floor.


```
Setups:
PN Length 255a
Taps [8,6,5,4]
Rate 4.9152MHz
Fc   1960.00MHz

E---PCMCIA---F

GPS LOCKED
40 32.0960 North
074 22.7604 West
-3.6 Meterss
GMT 184749.00

ID Byte 00H

Keys-Modes:
1 BER Off
3 Cursors Fixed
5 Scroll Off
7 Center Scroll
9 Save Screen
↑ Y x2
↓ Y ÷2
. Zoom X
```

```
MultiPath Analysis - Scale: Y 8x   X 4x 14:47:10  06-19-1996
🟥 -82.0dBm   🟩 -82.0dBm +0.254µs   🟦 -82.5dBm -0.305µs
```

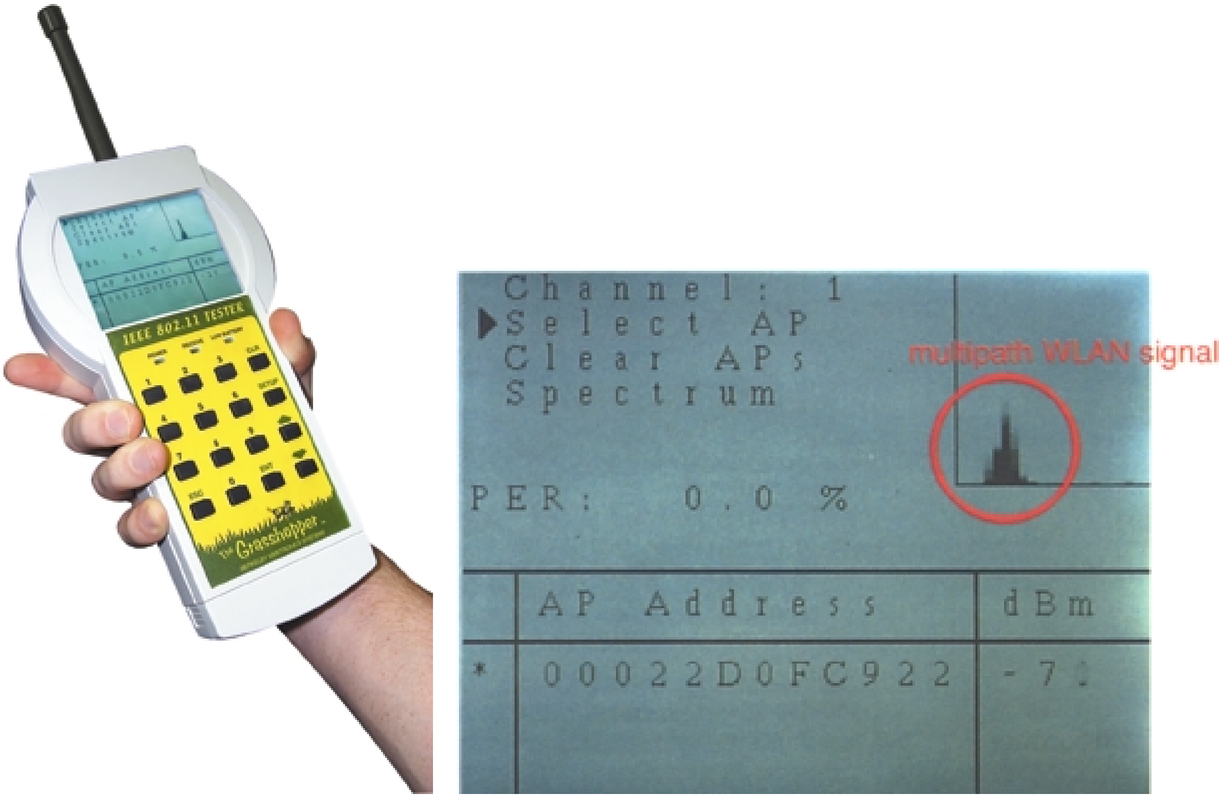
PCS close reflections of DSSS as shown by BVS Duet Multipath Analyzer

Another kind of Spread Spectrum (SS) is know as Frequency Hopping Spread Spectrum (FHSS) where the carrier of the transmitter constantly changes in an unpredictable pattern or schedule known only to the transmitter and receiver. This form of SS is very immune to harsh noisy environments. The carrier frequency of the transmitter may change 75 times per second; up to 1,000 times per second, jumping around to discrete frequencies in pseudo-random fashion. Accordingly, the authorized receiver tunes its local oscillator to "track" the incoming frequency agile signal in precise synchronism to the transmitter.

"Bluetooth" equipped devices are good examples of frequency-hopping, time-division-duplexing (TDD) modulation. Initially conceived by Ericsson, before being adopted by many other companies (there are more than 1800 companies belonging to the Bluetooth Special Interest Group), Bluetooth is a standard for a small, cheap radio to be plugged into computers, printers, cell phones, alarms and other consumer appliances to eliminate interconnecting wires. The Bluetooth module operates in the unlicensed Industrial, Scientific and Medical (ISM) band at 2.402 to 2.480 GHz band.

The master station, transmitting at up to 721 kbps on even time slot appointments determines the hopping sequence to be used and sets the piconet clock rate. Slave nodes run at 57.6 kbps on odd time slots. Orthogonal transmission in both directions at 432.6 kbps is also supported. This short-range system uses Gaussian-shape, binary frequency-shift keying with an effective symbol rate of 1 MB/second and is aimed at consumer products that will have cordless interactivity. The hopping sequence is determined by a pseudo-random code 2^27 –1 long, changing the carrier frequency to any one of 79 different frequencies at a rate of up to 1,000 times per second. Because FHSS is a form of time division, each transmission is broken into a series of packets with each packet remaining on a single frequency during transmission. This system has a fairly low expectation of received BER at 10 –3 for raw, uncorrected data. Bluetooth is just now becoming available in single-chip form and is estimated to cost $5.00 for these wireless features.

Like any competing technologies, direct sequence and frequency hopping spread spectrum have supporters and critics. It is ironic that direct sequence and frequency hoppers are usually both studied together, have similar concepts, similar applications and even the same basic formula to calculate their processing gain. There are some important reasons why each form of spread spectrum has found its own applications and champions.



Grasshopper WLAN IEEE 802.11b tester by Berkeley Varitronics Systems

Direct sequence systems spread their energy over a wide bandwidth. When the signal is "despread", the energy is recovered in the information bandwidth and noise (ideally) is spread over the wide bandwidth. This is a mechanism that provides processing gain that allows signals to share the same bandwidth at the same time. Unfortunately, the wide bandwidth gives ample opportunity for an unwanted signal, a jammer, to be anywhere within in the DSSS systems' bandwidth and interfere with the DSSS. Receiver-side despreading is typically done in the digital domain via digital correlators. For large interferes, this requires an A/D converter with many bits that can still quantize the small signal in the presence of large interferes. A large number of bits also require a big multi-bit correlator that will not overflow.

Direct sequence systems excel in range finding and timing applications. The high-rate spreading code (after the correlation process) produces a large response at the chip rate. This response finds multi-path (at the chip rate) that can acquire, track and combined signals in a RAKE receiver. Multipath combining is utilized in both IS-95 and IEEE 802.11systems.

DSSS has been effectively designed into applications where the signal "jammers" are under the control of the system designers. In an IS-95 system a base station demodulating the signal for a particular phone considers other phones in the system as jammers. Fortunately, these jammers have codes that are nearly orthogonal to the signal. IS-95 is a great example where the jammers are other users and their codes are carefully chosen to be nearly orthogonal. Digital techniques are utilized in VLSI for processing.

In summary, DSS systems are typically more of a digital approach, excel where the jammers are other user's who have nearly orthogonal codes, can combine multipath that is separated by the inverse of the chip rate or more. They can have trouble with large jammers that saturate the receiver chain.

FHSS systems usually transmit in a bandwidth that is about the data rate (or some low multiple) at any instant. The transmitting frequency is then hopped or shifted to a different frequency. The FHSS system receives interference (ideally) only from sources that happens to be transmitting in the same narrow bandwidth. If a particular frequency is jammed or is experiencing sever multipath fading, the reception will be resumed at some other frequency. Frequency Hopping SS only experience a small percentage of interference from DSSS and usually overpower DSSS interferes. DSSS systems spread their energy over a relatively large bandwidth and only the portion that is in the FSSS bandwidth at that instant.

FSSS systems have been found to perform well in high noise environments such as industrial sites and factories, strong tone jammers or other FSSS systems. FSSS systems can share the channel with other FHSS systems, but typically cannot support as many users as DSSS.

Future articles will present design challenges and solutions from BVS' current spread spectrum designs and test experiences. The next article will examine challenges in DSSS receiver design with a focus on the correlation process and signal jammers.