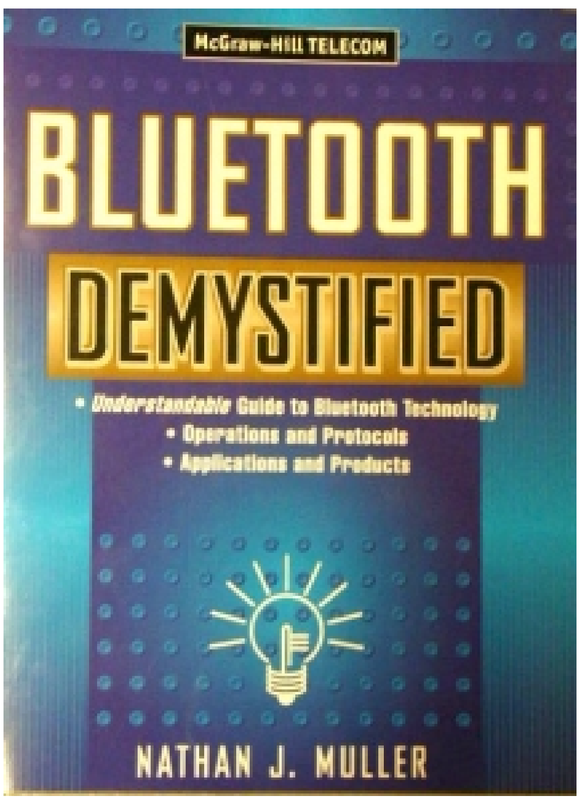
FURTHER READING

As a preview for further reading, the following reference has been provided from the pages of the book below:

Title: Bluetooth Demystified
Author: Nathan J. Muller
Publisher: McGraw-Hill

ISBN: 0071363238



put. Any difference between the sampled input and output signal, called *quantizing noise*, is filtered out to ensure the highest-quality reception at each end of the conversation.

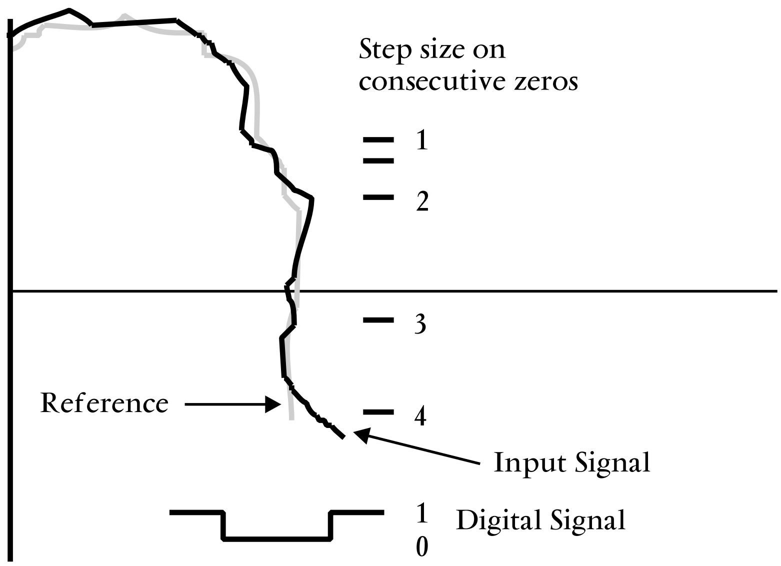
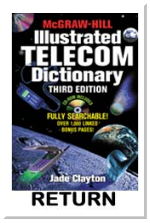


Figure 2.7 The relationship of the reference voltage to the input signal. In this case, as the slope of the curve increases downward, the CVSD algorithm increases the size of the step taken between samples each time the change continues in the same direction.

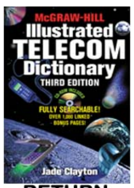


The sampling technique used by CVSD modulation makes it insensitive to random bit errors, which are experienced by users as white background noise. However, when a speech segment is rejected because it contains errors, measures are taken to fill in the lost speech segment. In the unlikely event that errors cannot be corrected, the segment is ignored, in which case the user experiences clipped speech—the cutting off of syllables.

Spread Spectrum

The Bluetooth wireless technology uses a digital coding technique called spread spectrum, a method of wireless communications that takes a narrowband signal and spreads it over a broader portion of the available radio frequency band. Among other advantages, the resulting signal is highly resistant to interference and more secure against interception. The same technology is used in cordless phones and wireless local area networks (LANs). In addition, many cellular services use Code Division Multiple Access (CDMA), a modulation and access technique that is based upon the spread-spectrum concept.

In recent years, CDMA systems have gained widespread global acceptance by wireless operators. This technique differs from that used to transmit voice and data over Time Division Multiple Access (TDMA) networks, which assigns each user a time slot in a narrow band of spectrum. While Bluetooth wireless technology makes use of spread-spectrum technology, it also uses a derivative of TDMA, called Time Division Duplexing (TDD), to provision the time slots used for voice and data communication.

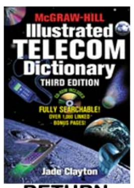


RETURN

The U.S. patent for spread-spectrum technology was held jointly by actress Hedy Lamarr (Figure 2.8) and music composer George Antheil. Their patent for a "Secret Communication System," issued in 1942, was based on the frequency-hopping concept, with the keys on a piano representing the different frequencies and frequency shifts used in music.[4]

Figure 2.8 *Actress Hedy Lamarr (1914–2000), co-developer of spread-spectrum technology.*

[4] In 1942, the technology did not exist for a practical implementation of spread spectrum. When the transistor finally did become available, the Navy used the idea in secure military communications. When transistors became really cheap, the idea was used in cellular phone technology to keep conversations private. By the time the Navy used the idea, the original patent had expired and Lamarr and Antheil never received any royalty payments for their idea.



RETURN

During World War II, Lamarr had become intrigued with radio-controlled missiles and the problem of how easy it was to jam the guidance signal. She realized that if the signal could be made to jump from one frequency to another very quickly—like changing stations on a radio—and both the sender and receiver changed in the same order at the same time, then the signal could never be blocked without knowing exactly how and when the frequency changed. Although the frequency-hopping idea could not be implemented due to technology limitations at that time, it eventually became the basis for cellular communication.

Spreading

Spread spectrum is a digital coding technique in which a narrowband signal is taken apart and "spread" over a spectrum of frequencies (Figure 2.9). The coding operation increases the number of bits transmitted and expands the amount of bandwidth used. Using the same spreading code as the transmitter, the receiver correlates and collapses the spread signal back down to its original form. The result is a highly robust wireless data transmission technology that offers substantial performance advantages over conventional narrowband radio systems.

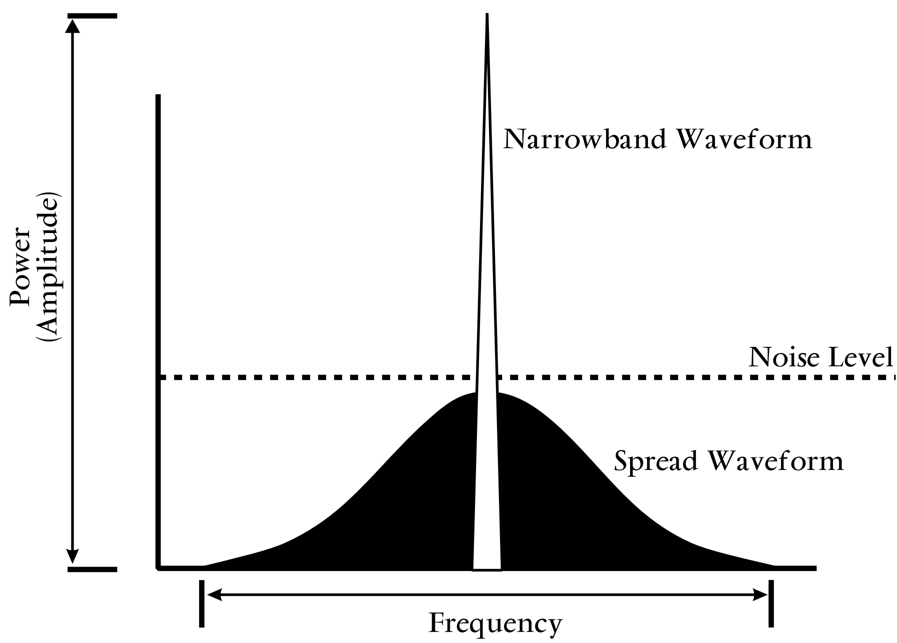
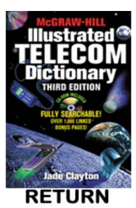


Figure 2.9 Spread spectrum transmits the entire signal over a bandwidth much greater than that required for standard narrowband transmission. Increasing the frequency range allows more signal components to be transmitted, which results in a more accurate reconstruction of the original signal at the receiving device.

One of the advantages of spread spectrum is that the spread signal has a much lower power density. This low power density, spread over the expanded transmitter bandwidth, provides resistance to a variety of conditions that can plague narrowband radio systems, including:

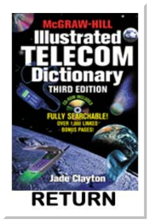


- **Interference**—A condition in which a transmission is being disrupted by external sources, such as the noise emitted by various electromechanical devices, or internal sources such as cross talk
- **Jamming**—A condition in which a stronger signal overwhelms a weaker signal, causing a disruption to data communications
- **Multipath**—A condition in which the original signal is distorted after being reflected off a solid object
- **Interception**—A condition in which unauthorized users capture signals in an attempt to determine their content.

Conventional narrowband radio systems transmit and receive on a specific frequency that is just wide enough to pass the information, whether voice or data. In assigning users different channel frequencies, confining the signals to specified bandwidth limits, and restricting the power that can be used to modulate the signals, undesirable cross talk—interference between different users—can be avoided. These rules, enforced by regulatory agencies in each country, are necessary because any increase in the modulation rate widens the radio signal bandwidth, which increases the chance for cross talk.

The main advantage of spread spectrum radio waves is that the signals can be manipulated to propagate fairly well through the air, despite electromagnetic interference, virtually eliminating cross talk. In spread-spectrum modulation, a signal's power is spread over a larger band of frequencies. This results in a more robust signal that is less susceptible to interference from similar radio-based systems, since they too are spreading their signals, but with different spreading algorithms.

Spread spectrum has two modes of operation: frequency hopping and direct sequencing. *Frequency hopping* spreads its signals by "hopping" the narrowband signal over the entire radio band as a function of time. *Direct sequencing* spreads its signal by expanding the signal all at once over the entire radio band. Although Bluetooth wireless technology uses the frequency-hopping mode of spread spectrum, it is useful to contrast it with direct sequence to appreciate its advantages.



Direct Sequence

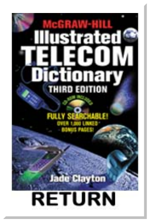
In direct sequence spreading, the radio energy is spread across a larger portion of the band than is actually necessary for the data. This is done by breaking each data bit into multiple sub-bits called *chips* to create a higher modulation rate. The higher modulation rate is achieved by multiplying the digital signal with a chip sequence. If the chip sequence is 10, for example, and it is applied to a signal carrying data at 300 Kbps, then the resulting bandwidth will be 10 times wider. The amount of spreading is dependent upon the ratio of chips to each bit of information.

Because data modulation widens the radio carrier to increasingly larger bandwidths as the data rate increases, this chip rate of 10 times the data rate spreads the radio carrier to 10 times wider than it would otherwise be for data alone. The rationale behind this technique is that a spread spectrum signal with a unique spread code cannot create the exact spectral characteristics as another spread-coded signal. Using the same code as the transmitter, the receiver can correlate and collapse the spread signal back down to its original form, while other receivers using different codes cannot.

This feature of spread spectrum makes it possible to build and operate multiple networks in the same location. By assigning each one a unique spreading code, all transmissions can share the same frequency band yet remain independent of each other. The transmissions of one network appear to the other as random noise and are filtered out because the spreading codes do not match.

This spreading technique would appear to result in a weaker signal-to-noise ratio, since the spreading process lowers the signal power at any one frequency. Normally, a low signal-to-noise ratio would result in damaged data packets requiring retransmission. However, the processing gain of the receiver's despreading correlator recovers the loss in power when the signal is collapsed back down to the original data bandwidth, but is not strengthened beyond what would have been received had the signal not been spread.

In the United States, the FCC has set rules for direct sequence transmitters. Each signal must have 10 or more chips. This rule limits the practical raw data throughput of transmitters to 2 Mbps in the 902 MHz band and 8 Mbps in the 2.4 GHz band. The number of chips is directly related to a signal's immunity to interference. In an area with a lot of radio interference, users will have to give up throughput to limit interference successfully.



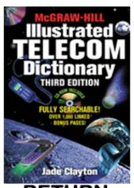
Frequency Hopping

Bluetooth wireless technology uses the frequency-hopping version of spread spectrum, which entails the transmitter's jumping from one frequency to the next at a specific hop rate in accordance with a pseudorandom code sequence. The order of frequencies selected by the transmitter is taken from a predetermined set as dictated by the code sequence. For example, the transmitter may have a hopping pattern of going from the third frequency, to the twelfth frequency, to the fifth frequency, and so on across an entire range of frequencies. The receiver tracks these changes. Since only the intended receiver is aware of the transmitter's hopping pattern, only that receiver can make sense of the data being transmitted.

The FCC mandates that frequency-hopped spread-spectrum systems not spend more than 0.4 seconds on any one channel each 20 seconds, or 30 seconds in the 2.4-GHz band. Furthermore, they must hop through at least 50 channels in the 900-MHz band, and 75 channels in the 2.4-GHz band. These rules reduce the chance of repeated packet collisions in areas with multiple frequency-hopping transmitters. The Bluetooth specification specifies a rate of 1,600 hops per second among 79 frequencies.

All Bluetooth units participate in a piconet, with each unit sharing a common channel. Up to eight interconnected devices can be supported by a piconet, with one master and up to seven slaves. This relationship remains in place for the duration of the piconet connection. The units that participate in a piconet are time and hop synchronized to the same channel. Every Bluetooth unit has an internal system clock, which determines the timing and hopping used by its transceiver. Timing and the frequency hopping on the channel of a piconet are determined by the clock of the master. When the piconet is established, the master clock is communicated to the slaves. Each slave adds an offset to its native clock to get in step with the master clock. Since the clocks are free running, the offsets have to be updated regularly.

Other frequency-hopping transmitters in the vicinity will be using different hopping patterns and much slower hop rates than Bluetooth devices. Should transmitters that do not use Bluetooth wireless technology and transmitters that do coincidentally attempt to use the same frequency at the same moment, the data packet transmitted by one or both devices will become garbled in the collision, and a retransmission of the affected data packets will be required. A new data packet will be sent again on the next hopping cycle of each transmitter.



RETURN

Although the chance of devices that use Bluetooth wireless technology interfering with those that do not, but that share the same 2.4 GHz band is minimal, some manufacturers are concerned enough that they have petitioned the FCC for new guidelines that would provide more separation among competing protocols that operate in the 2.4-GHz band.[5] Both the Bluetooth SIG and IEEE recognize the potential for such signal interference and are working together to figure out how to enable their technologies to coexist. The impact of any change must be determined for portable phones and other devices such as microwave ovens, wireless speakers, and security systems, which also share this band.

Circuit and Packet Switching

The Bluetooth protocol uses a combination of circuit and packet switching. Circuit switching is familiar to anyone who has placed a telephone call on the PSTN. When a number is dialed, a dedicated path is set up through the network to handle the call (Figure 2.10). The path remains in place for the duration of the call. At the conclusion of the call, the path is torn down and the network resources used to build the connection become free to handle another call from someone else. Circuit switching can apply to wireless networks as well as wireline networks, and to data as well as voice.

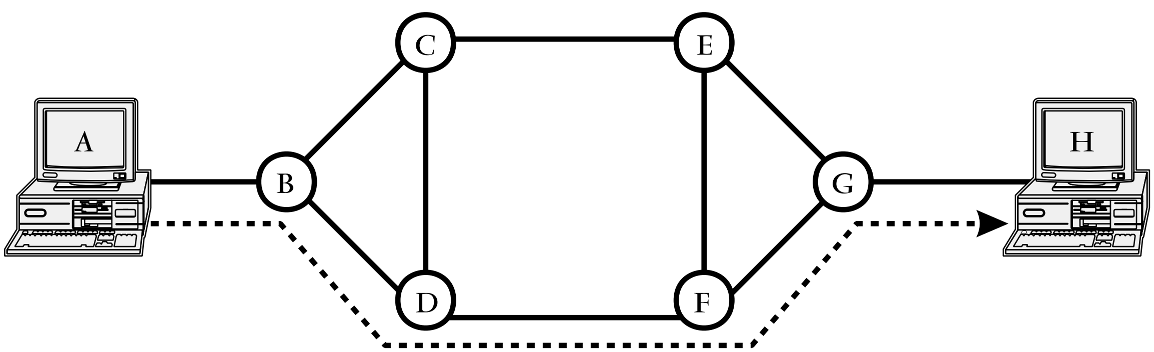


Figure 2.10 In circuit switching, a dedicated path is set up between endpoints to handle a voice or data call, which stays in place until the call is terminated.

[5] The FCC has opened Docket 99-231 for consideration of this matter. At this writing, no decision has been announced. Readers interested in staying updated on this issue can go to the FCC's Web page at www.fcc.gov.