Wireless Communication Systems

Module 4: Digital modulation and pulse shaping techniques

Part 3 Spread spectrum modulation techniques

Main Reference: Rappaport Chapter 6 section 10
Minor reference: Haykin “Communication systems”, 4th Ed., Chapter 7

Spread spectrum techniques employ a transmission bandwidth that is several orders of magnitude greater than the minimum required signal bandwidth (for a given bit rate). While this system is very bandwidth inefficient for a single user, the advantage of spread spectrum is that many users can simultaneously use the same bandwidth without significantly interfering with each other. This provides a major benefit … elimination of the need for frequency planning in cellular mobile systems, since all cells can use the total bandwidth (minus that allocated for control purposes) of the particular cellular system.

The lack of interference between users is due to the fact that each user uses a different (approximately) orthogonal code to `spread spectrum *modulate*’ their signal. These are binary valued and appear like random binary valued noise, but can be reproduced in a deterministic manner.

Demodulation involves cross correlating the received spread spectrum modulated signal with a locally generated version of the spreading code sequence. This demodulates (i.e. despreads) the signal only if the correct code sequence is used. Thus the spread spectrum modulated signals from other users (generated from different/orthogonal spreading codes) are not despread, and appear as low level background noise.

There are different types of spreading codes. A common type is that based on pseudo-noise (PN) sequences….known as PN spreading codes. Another is based on the rows of the *Hadamard* matrix … known as Walsh spreading codes.

The spreading code sequence (whether PN or Walsh based) is random-like. This makes each spread spectrum modulated signal appear like random-white noise. For this reason, spread spectrum modulation provides the following advantages.

Enhanced security of communication … intelligible reception of the signal is only possible if the correct code sequence is known;

Significant reduction of frequency selective fading (distortion and attenutation due to the interaction of multiple delayed versions of the transmitted signal). This is due to the delayed versions of the *noise-like spread spectrum modulated signal* having very low correlation with each other….approximately 1/N where N=length of spreading code sequence.

Pseudo noise sequences

A pseudo noise (PN) sequence is a binary sequence with an autocorrelation function that resembles, over a given time interval, the autocorrelation of a discrete white binary sequence. It has:

a nearly equal number of 0s and 1s

very low correlation between shifted version of itself

very low crosscorrelation with other PN sequences (shifted or nonshifted)

The PN sequence is usually generated using a feedback shift register … see Figure 6.48 Rappaport…which consists of `m' consecutive stages of 2-state memory devices and a feedback logic function. Binary sequences are shifted through the shift registers in response to clock pulses. The outputs of the various stages are combined (via logic function) and fedback as the input to the first stage.

When the feedback logic consists of exclusive-OR gates (i.e. the outputs of the stages are modulo-2 added) then the shift register is called a linear PN sequence generator … most common type used in practice.

The feedback logic function of a linear PN generator must avoid the all zero state … since, if the generator reaches this zero state, then it will remain in that state. Only certain feedback logic functions are therefore usable in practice.
There are exactly 2^m-1 nonzero states of an m-stage feedback shift register. Thus the period of a PN sequence generated by a (usable) m-stage linear feedback shift register cannot exceed 2^m-1. Only certain feedback logic functions provide this maximum period…. known as maximum length sequence generators.

See additional handout for more details.

Walsh Codes (Sect. 11.4.2.6 Rappaport)

Walsh codes correspond to the rows of the Hadamard matrix. Each row is orthogonal to the other rows. The 64-by-64 Hadamard matrix is commonly used … which provides 64 different codes, and consequently enables 64 different users to share a frequency channel.

See Section 11.4.2.6 of Rappaport for details on the Hadamard matrix structure.

Direct Sequence spread spectrum (DS-SS)
Involves modulating a bit stream waveform b(t) … the message signal … with a spreading code waveform c(t). [E.g. waveform = polar square waveform.]

Let N=length of spreading code. (PN spreading codes $N= 2^m-1$).
Let T_c=duration of one element in spreading code, termed a chip … T_c=chip interval.
If T_b=bit interval in b(t) then $T_b=NT_c$.

(Null-null) Bandwidth of b(t) = R_b.
Bandwidth of c(t) approx = NR_b.

DS-SS signal: u(t)=c(t)b(t).
In the frequency domain U(f)=C(f)*B(f), where *=convolution. It follows that bandwidth of u(t) is approx= NR_b .

Assume the received signal r(t)= u(t) + j(t) where j(t)=additive interference.
DS-SS demodulation involves (i) multiplying r(t) by a synchronized c(t):

$$z(t)=c(t)r(t)=[c(t)]^2b(t)+c(t)j(t)=b(t)+c(t)j(t)$$

Note: c(t)j(t) now has a bandwidth of approx NR_b.

(ii) integration over T_b … low pass filtering with cutoff freq $B\sim=R_b$.

The effect of this is a reduction in the interference power by a factor of N.

(iii) application of a threshold to obtain the estimated bit stream.

Processing gain (reduction of in-band interference power) = N

Bandpass DS-SS
The above describes a baseband DS-SS system. The bandpass equivalent involves PSK, FSK or QAM modulating the baseband DS-SS signal.

Typically BPSK modulation is used. E.g.
$c(t)=+1 \rightarrow s(t)=\cos(2\pi f_c t), \quad 0<=t<=T_c$
$c(t)=-1 \rightarrow s(t)=\cos(2\pi f_c t+\pi), \quad 0<=t<=T_c$

The bandwidth of s(t) is approx $2NR_b$ … in comparison to bandwidth=$2R_b$ for BPSK modulated b(t).

The receiver includes both a DS-SS demodulating step and a BPSK demodulating step.
Processing gain
= 2N if coherent BPSK demodulation
= N if noncoherent BPSK demodulation.
CDMA based mobile communication systems use bandpass DS-SS.

Frequency Hop Spread Spectrum
For a given bit rate, the processing gain N of DS-SS can only be increased by increasing the chip rate. In practice, there are limitations on this, hence limitations on overcoming in-band interference.

Frequency hop spread spectrum (FH-SS) is an alternative to DS-SS which enables wider spread spectral bandwidths and consequently higher processing gains. Present day technology allows FH bandwidths to be an order of magnitude greater than DS bandwidths.

FH-SS involves pseudo-randomly hopping the carrier frequency. In effect, the spectrum is spread sequentially rather than instantaneously, as in DS-SS. The order of the pseudo random hopping corresponds to segments (of length n) of a locally generated PN sequence (of length $N=2^m-1$, where m=length of shift register of PN generator).

There are a maximum possible 2^n different hop frequencies that the FH-SS system can generate.

M-ary FSK is commonly used to modulate the baseband bit stream prior to FH-SS. The full technique is known as MFSK-FH-SS.

If K=no. bits per FSK symbol, then every symbol interval $T_S=KT_b$ the MFSK modulator outputs a single frequency waveform symbol from the set of $M=2^K$ different frequency waveform symbols. Due to the large bandwidth of MFSK-FH-SS systems, the MFSK demodulation is carried out via the noncoherent approach (impractical to maintain phase synchronization for coherent demodulation). Consequently, to ensure orthogonality of the MFSK waveform symbols, the adjacent frequencies differ by $R_S=1/T_S$ (rather than $1/(2T_S)$ as in coherent MFSK systems).

Processing gain: The bandwidth of the MFSK signal is approx. B $\sim= MR_S$. If adjacent hopping frequencies differ by B, then the total hopping bandwidth is approx.
$B_{TOT} \sim= 2^n B$. The processing gain is then

$$PG=B_{TOT}/B = 2^n.$$

This suggests a greater processing gain for longer segments *n* of the PN code of length N. However, with the larger *n* comes a reduction in the number $n_{hop}<=N/n$ of `possible' hopping frequencies….lower security against hostile interference.

Slow frequency hopping: R_S is an integer multiple of $R_h=1/T_h$ where T_h=hop interval….several symbols are transmitted during each hop interval.
Fast frequency hopping: R_h is an integer multiple of R_S … several hops during each symbol interval.
Slow frequency hopping systems are more susceptible to hostile interference … more time to measure spectral content of signal between hops. *Fast frequency hopping* systems are more complex in implementation.

Many short range wireless communication systems, such as Bluetooth, use MFSK-FH-SS.