Frequency Hopped Spread Spectrum

Introduction

In the next few lessons we will be examining "spread spectrum" communications. This idea was originally developed for military communication systems. However, there are aspects of the "hostile" military communication environment that naturally occur in "friendly" communication systems. For example, we have seen that interference from other cells can cause the *S/I* to be low enough to disrupt our channel. In a military environment the interference might be intentional whereas it is typically unintentional in a civilian environment. Nonetheless, regardless of the intent, interference causes problems. Not surprisingly, therefore, techniques developed for hostile environments find applicability in civilian systems.

There are two main types of spread spectrum modulation: frequency-hopped, and direct-sequence. In this lecture we focus on frequency hopping.

The "Jamming" Problem

A problem that arises when trying to communicate in a hostile environment is that of "jamming" in which interference is created specifically to drive the *S/I* down enough to make communication impossible. Let's say you are trying to listen to "Friend" on a channel centered on frequency f_2 and having bandwidth B. You need enough *S/N* for your link to function, so a spectrum analyzer would show something like that illustrated in Fig. 25.1. Here *S* is Friend's signal.

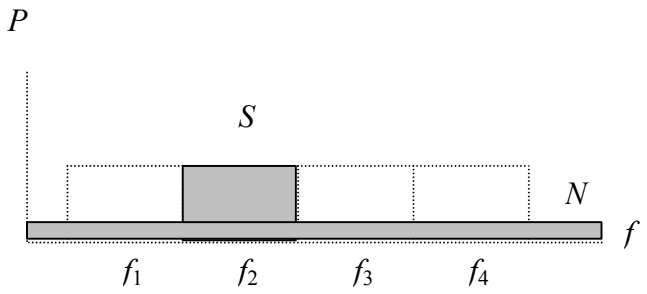

Figure 25.1: In normal operation a radio signal occupies some channel bandwidth and has a spectral intensity that differs from that of the noise by S/N.

Anyone else could use a spectrum analyzer to see the same thing, including a hostile "Foe." Having determined that you are transmitting and at what frequency, Foe could then deliberately transmit on the same channel. This is illustrated in Fig. 25.2. Here *I* is Foe's signal, which is interference with respect to Friend's signal *S*. If this creates a *S/I* that is low enough then the channel is "jammed" and you cannot receive Friend's signal. An obvious solution at this point would be to switch channels. You and Friend could have an agreed upon sequence of channels with the understanding that when one channel gets jammed you both switch to the next in the sequence. Of course the sequence should be secret and appear essentially random or Foe can

switch the interference right along with you. On the new channel you can communicate with Friend until Foe looks at his spectrum analyzer and figures out which channel you've switched to. Then Foe could start jamming the new channel. This process is illustrated in Fig. 25.3.

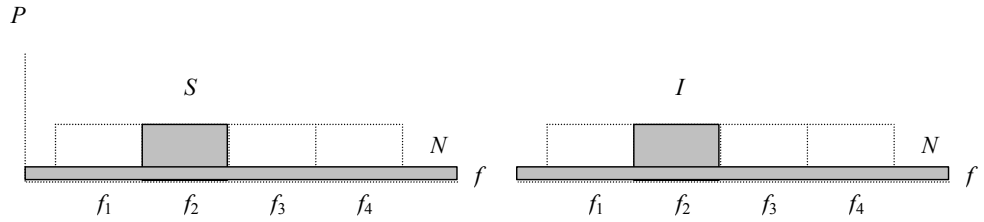

Figure 25.2:Jamming involves deliberately transmitting over the same bandwidth your link is using.

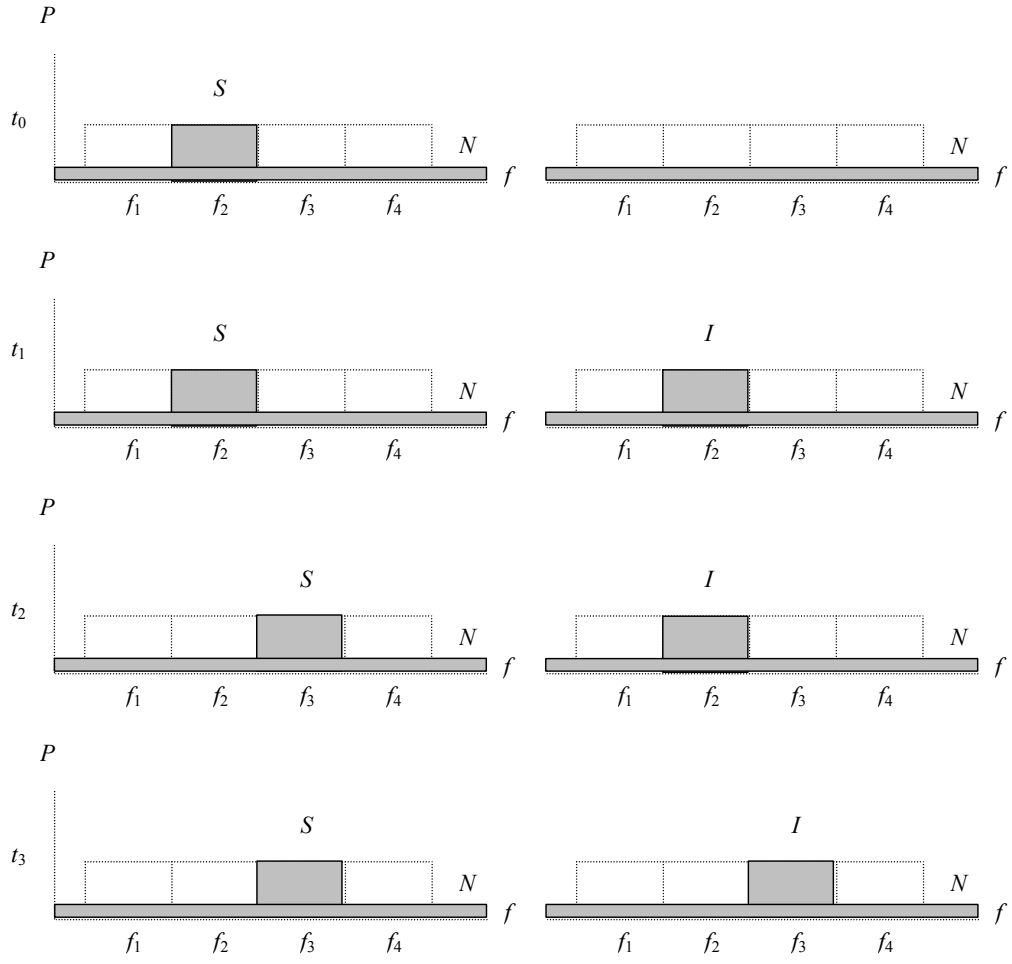

Figure 25.3:Top frame: Normal communication over channel at carrier frequency f_2. Second frame: Channel is jammed. Third frame: Signal hops to a new channel. Fourth frame: jammer determines new channel and changes jamming frequency.

But why not stay ahead of Foe's jamming by agreeing before hand to switch channels every T_h seconds. This should be a short enough time that Foe won't be able to find the new channel and begin jamming it before you've switched to yet another channel. This *frequency hopping* strategy is an effective counter measure for jamming.

Note that while at any instant you are performing *narrow-band* communication with a bandwidth B, over time you *spread* your signal out over a spectrum MB where M is the number of channels or *frequency slots* you switch between. This is referred to as *spread spectrum* communication.

It might seem that a down side of this approach is that you use up M channels for a single radio link and those channels would not be available for other users. However, this is not the case. Other users can frequency hop also provided only that they use a different hopping sequence. This is illustrated in Fig. 25.4.

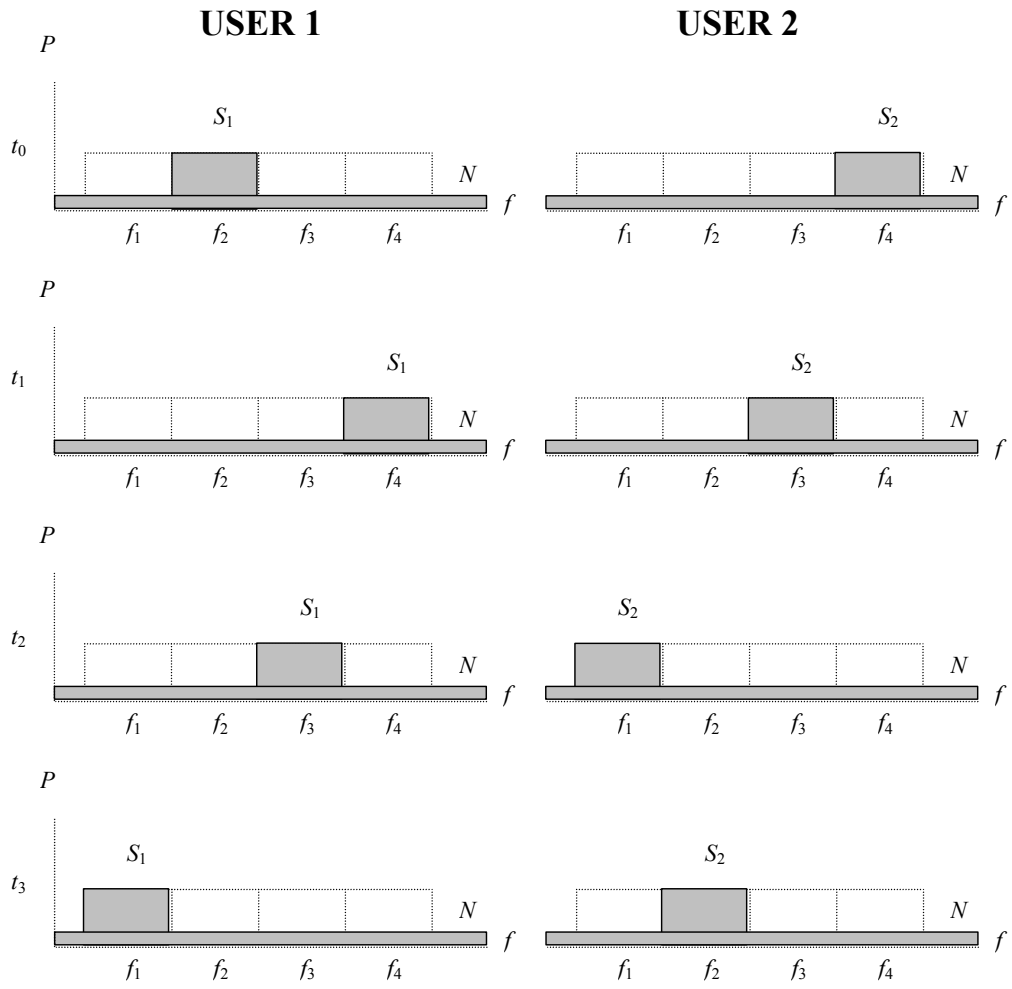

Figure 25.4:Different users can frequency hop in the same spectrum provided they use a different hopping sequence.

How many users can share the spectrum? Obviously no more than M since there are only M slots available at any time. In principle, though, M users could frequency hop simultaneous as long as they coordinated their hopping so that no two of them every tried to use the same slot.

Spead-Spectrum for "Stealth" Communication

Consider "USER 1" in Fig. 25.4. While a particular frequency slot is being used, the average spectral intensity is P/B Watts/Hz where P is the power in Watts and B the bandwidth in Hz. This is illustrated at the left in Fig. 25.5.

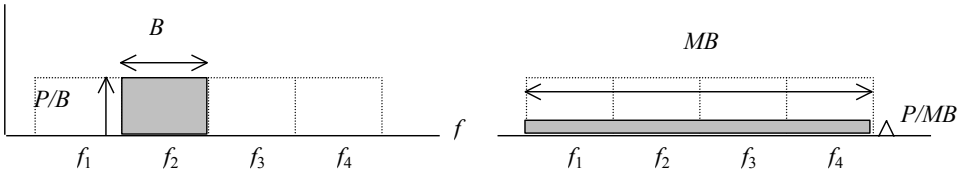

Figure 25.5: Left, short-term spectrum while a single frequency slot is in use; right, time-average spectrum for spread-spectrum communication. Because the same power is spread over a greater spectral width, the spectral intensity is reduced.

However a user makes use of any given slot only a fraction $1/M$ of the time. So on average the spectral intensity at all frequencies is only P/MB. Another way of looking at this is that we have spread the power P out over a bandwidth MB so the intensity is only P/MB. This is illustrated at the right of Fig. 25.5. In both cases we have that the spectral intensity times the bandwidth is equal to the power P. If M is very large then the spectral intensity will be *much* smaller that what we would have in a narrow-band system. In fact P/MB might be so small that it is much less than the noise floor of Foe's spectrum analyzer. If so then Foe will not be able to see that Friend is transmitting. We have thus obtained a "stealth" channel. This is of obvious value in military scenarios.

Now you might think that *S/N* would suffer because we are using a larger bandwidth and the total noise power would increase accordingly (since $P_N = N_0(BW)$). However, at any given time we are only receiving over the relatively narrow bandwidth *B,* so the noise power is never more than $P_N = N_0 B$. So, $S/N = P/N_0 B$ which is independent of *M*. We do *not* look at the noise over the entire spectral width of *MB* at the same time so the noise power is *not* MN_0B. We get the stealth effect without sacrificing *S/N*!

Example 25.1

Let's say we need $S/N = 20\,\text{dB}$ and $B = 10\,\text{kHz}$ for a good link, but we want the spectral intensity of the spread-spectrum signal to be 10 dB below the noise floor. We can achieve this by using a spreading factor of $M = 1000$. This reduces the spectral intensity by 30 dB which will be –10 dB relative to the noise floor. We will use a total spectral width of 10 MHz.

Commercial Application of Spread Spectrum

It might seem that jamming and stealth would not be of much interest in a commercial environment where (hopefully) people are not trying to use radios for hostile purposes. However, if two users just happen to try and use the same channel then the effect is the same as if they were jamming one another. By the same token, even if I don't care whether or not people know

I'm transmitting, if I use spread spectrum to lower my spectral intensity below the noise floor of other users then I will most probably not create interference for them. These effects are important, particularly in the types of unsupervised communications that typify the use of unlicensed spectrum.

In the U.S., the Federal Communication Commission (FCC) regulates the use of spectrum. Much of the available spectrum is auctioned to commercial users, such as radio and TV stations, and cellular companies. These commercial users pay the government for a license giving them exclusive right to use a particular portion of the spectrum in a particular geographical region. However, some regions of the spectrum are "unlicensed," meaning they are available for use by anyone, provide one follows some basic rules set down by the FCC. Two important unlicensed bands are the so-called ISM (Industry Scientific Medical) bands at 902-928 MHz and 2,400.0-2,483.5 MHz. The later, in particular, is used extensively for wireless LANs.

Example 25.2

Bluetooth is a wireless interface for a wide variety of short-range ("picocell") applications including computer LANs and wireless peripherals. It uses FSK in the 2.4 GHz unlicensed ("ISM") band. There are 79 RF channels each with 1 MHz bandwidth. Frequency slots are typically occupied for 625 μs. Maximum transmitter power is 100 mW (20 dBm).

BER

Because the carrier frequency is constantly changing, it is difficult to establish phase coherence in a FH-SS system. Consequently, incoherent FSK modulation is typically employed. Recall that for incoherent FSK the probability of a bit error is

$$P_e = \frac{1}{2} e^{-\frac{E_b}{2N_0}} \tag{25.1}$$

If a single FH-SS link were operating, then it would ideally achieve this same BER. However, if other links are also operating in the same spectrum, there is a possibility that two or more links may hop to the same carrier frequency at the same time. Say there are M slots available and K links operating. The probability that a given link will hop to a given slot is just $1/M$. The probability that it will not hop to that slot is $(1-1/M)$. Therefore the probability that the other $K-1$ links will not hop to the same slot that you hop to is $(1-1/M)^{K-1}$. So, the probability of your frequency slot being "hit" by at least one other link is

$$p_h = 1-\left(1-\frac{1}{M}\right)^{K-1} \tag{25.2}$$

The probability of not getting hit is $1-p_h$. If you get "hit" then the *S/I* will be driven very low and the probability of a bit error will go way up. In the worst case $P_e = 0.5$. Therefore, on average,

$$P_e = (1-p_h)\frac{1}{2}e^{-\frac{E_b}{2N_0}} + p_h\frac{1}{2}$$
$$= \frac{1}{2}e^{-\frac{E_b}{2N_0}}\left(1-\frac{1}{M}\right)^{K-1} + \frac{1}{2}\left[1-\left(1-\frac{1}{M}\right)^{K-1}\right] \quad (25.3)$$

where the first term accounts for errors due to noise and the second term for errors due to "hits."Assume that *S/I* is very strong so that $e^{-\frac{E_b}{2N_0}} \to 0$, i.e., there are no noise-induced errors. Then errors arise solely due to hits and P_e is the second term of (25.3). This is plotted in Fig. 25.6 for $M = 79$.

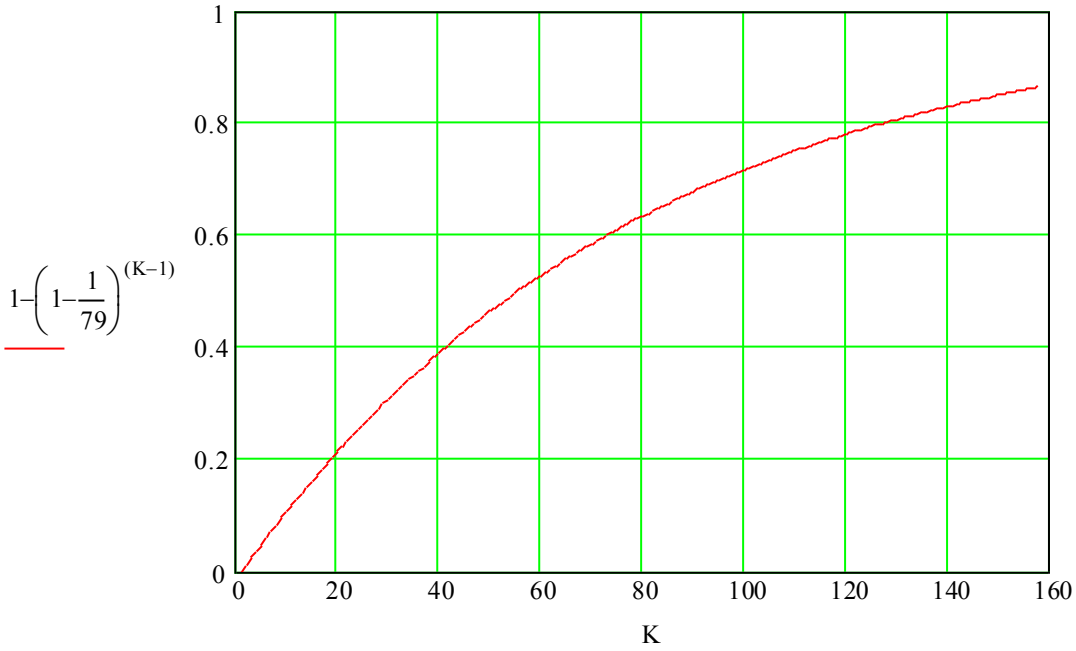

Figure 25.6: Probability of a frequency slot being hit vs. number of radio links operating for $M = 79$ slots.

In practice you would probably try to send several bits during each hop. For example, in the Bluetooth standard, the bit period is 1 μs and hops last for the 625 μs duration of a *packet*. So the curve in Fig. Gives the probability that a packet will be destroyed by a hit. Destroyed packets need to be resent, and this represents the overhead resulting from the unsupervised sharing of spectrum between *K* users.

As a very interesting historical aside, frequency hopping was invented and patented (U.S. Patent number 2,292,387) by the legendary movie actress Hedy Lamarr and avant-garde musical composer George Antheil in August 1942 under the title "Secret Communication System." The goal was to provide an unjammable radio link for guiding torpedoes during World War II. Their system used 88 frequencies (corresponding to the 88 keys on a piano) and perforated papers rolls (such as those used at the time in "player pianos") to coordinate the hops.

References

1. Bray, J. and C. F.Sturman, *Bluetooth 1.1: Connect Without Cables,* Prentice Hall, 2002, ISBN 0-13-066106-6.
2. Rappaport, T. S., *Wireless Communications: Principles and Practice,* Prentice Hall 2002, ISBN 0-13-042232-0.
3. http://www.hedylamarr.org/hedystory1.htm