Avoiding Interference Surprises in Unlicensed Spread Spectrum Deployment

By F.H. "Rick" Smith
ChevronTexaco

Unlicensed spread spectrum systems are easy to engineer. You select equipment with the right features, look at a simple table to see what kind of antennas you need to cover a specified distance, and you are done. Can it be that simple? Yes and no. Many people have successfully engineered unlicensed systems just this way. Most of those systems are working just fine, yet an increasing number of systems are becoming partially, or fully, debilitated as the result of interference from other new systems.

There are two parts to engineering any radio system. The first part is to make sure you have enough signal to make the system talk. This is often handled very simply in the case of unlicensed spread spectrum systems by using a look up chart and a general disclaimer that line of sight is assumed. The second part is an interference analysis. This is often skipped in the case of unlicensed spread spectrum systems, resulting in interference surprises that could have been avoided.

The Illusion of Simplicity

Why is the interference analysis aspect of unlicensed spread spectrum system engineering often overlooked? There are at least two reasons. First, vendors do not want to undermine the image of simplicity that accompanies unlicensed products, and often point to the partial truth that the spread spectrum technology solves interference problems. The second reason is that the equipment designs invariably provide some form of data packetization and retransmission process that will, most of the time, redo particular transmissions when necessary so that the user's data goes through. This leaves you, the user, in a life of luxury, not unlike the rock star who's manager keeps the champagne and caviar flowing, meanwhile the bank account may be nearing a zero balance.

As we start looking at the interference side of unlicensed spread spectrum engineering, we realize that the issue isn't whether or not you are hearing your neighbors, but rather can you talk over the top of them, or even sneak a transmission by when they are not talking. Your position of security rapidly erodes as you slip from a position of RF dominance over all the subject frequencies all the time, to dominance over all the frequencies some of the time, to some of the frequencies some of the time, to essentially none of the frequencies most the time.

Dominating the RF Environment

"RF Dominance" for the purposes of this discussion means that once you apply all the magic of receiver selectivity, coding gain, antenna discrimination, cross polarization, etc, etc, and you are at the point where your receiver is actually demodulating the de-spread signal, your signal must dominate over all interference and noise to the extent that it can be properly demodulated.

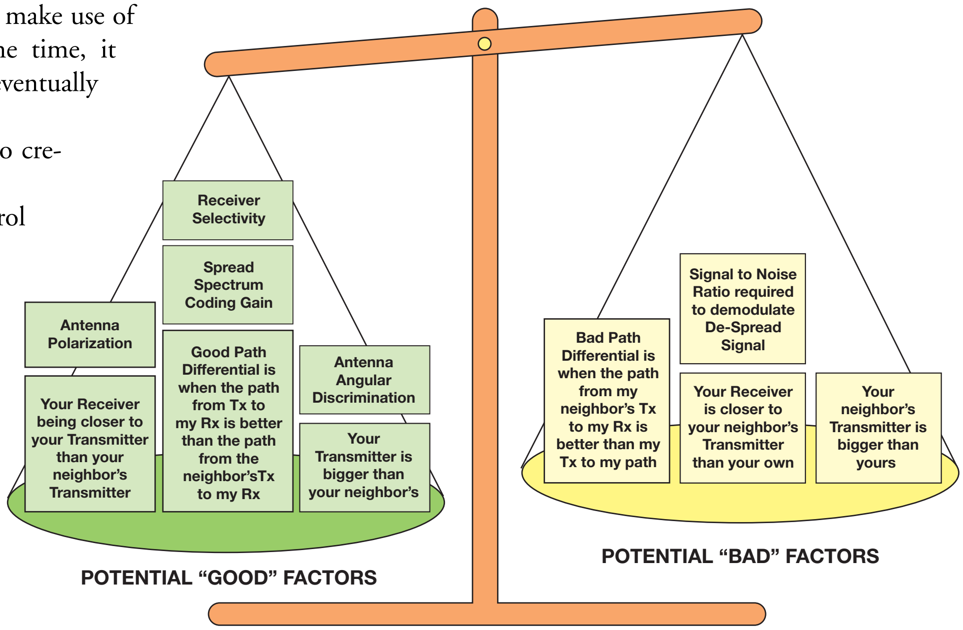
The following table does show and acknowledge that you do not always need RF Dominance to make use of spread spectrum systems, but at the same time, it shows how eroding degrees of dominance eventually affects the bottom line.

The main point of this discussion is to create a strategic thought process relative to:

- What is going to help me control and maintain RF Dominance?
- Can I recognize situations where RF Dominance is not possible?
- When might the risks of implementation of a specific unlicensed solution be unworkable?

Although the question of acceptable risk depends on the application, the idea of coming to know and understand the factors that mitigate or exacerbate risk is worth the effort. The following figure depicts a scale, with potential good factors that work in your favor on one side, and potential bad factors that work against you on the other side. The concept here is that the scale needs to tip to the good side.

Do You Have RF Dominance?



The Effect of Having RF Dominance (or Not) is Situation Dependent

You Are	Your Neighbor	Situation	Demodulation	User Data
Freq. Hop.	Freq. Hop	You Dominate across all freq all the time	Error Free	OK at full speed
		You Dominate across some of the freq. some of the time	Errors	Errored at full speed, possibly OK at sub rate
		You are Dominate across none of the freq. most of the time	Out of Service	Pattern Sync loss
Freq. Hop.	Direct Sequence	You Dominate across all freq all the time	Error Free	Ok at full speed
		You Dominate across some of the freq. some of the time (some freqs fall outside the direct sequence bandwidth)	Errors	Errored at full Speed, possibly OK at sub rate
		You are Dominate across none of the freq. most/all of the time	Out of Service	Pattern Sync Loss
Direct Seq.	Freq. Hop	You Dominate across all freq all the time	Error Free	OK at full speed
		You Dominate across all freq some of the time (while your neighbor is hopping elsewhere)	Errors	Errored at full speed, possibly OK at sub rate
		You Dominate across some of the freq. some of the time	Out of Service	Hard to lock onto chipping sequence
		You are Dominate across none of the freq. most of the time	Out of Service	Impossible to lock onto chipping sequence
Direct Seq.	Direct Sequence	You Dominate across all freq all the time	Error Free	OK at full speed
		You Dominate across all freq some of the time (systems that send bursts)	Errors	Errored at full speed, possibly OK at sub rate
		You Dominate across some of the freq. some of the time	Out of Service	Hard to lock onto chipping sequence
		You are Dominate across none of the freq. most of the time	Out of Service	Impossible to lock onto chipping sequence

The table below attempts to break down and discuss of the various factors, including explaining when they apply, and the approximate magnitude (or weight) of each factor. The reader needs to remember that the one bad factor that will always be present is the need to maintain the "Signal-to-Noise Ratio required to Demodulate the De-spread signal!"

I know what you are thinking, "Isn't there some off the shelf computer program I can buy that will consider all these factors for me?" While there are coverage and

Discussion of Individual Factors Affecting RF Dominance

Factor	Good or Bad	Potential Magnitude	When Applicable	How Do You Analyze
Receiver Selectivity	Good	80 to 100db	Where No Frequency Overlap Exists	Consult Equip. Mfg.
Spread Spectrum Coding Gain/ direct sequence rejection of narrowband	Good	10 to 25db	Coding gain is between direct sequence systems, while narrowband to wideband isolation is between frequency hopped and direct sequence systems.	Coding gains are typically in the range of 10 to 25db. Narrowband to wideband isolation is usually a 10 log function of the ratio of the spread to the unspread bandwidth (for example a 2.5 MHz bandwidth Direct Sequence System would reject a 25 KHz narrowband interferer by 20db).
Signal-to-Noise Ratio Required to Demodulate De-Spread Signal	Bad	12 to 30db	Always	Ask Mfg. what this figure is (narrowband systems are usually towards the 12db end of the range).
Your Receiver being closer to your Transmitter than your neighbor's Transmitter	Good	0 to 50db	Any time you have the distance advantage on your neighbor	The actual magnitude is generally equal to 20 log the ratio of distances involved (For example, 4X Closer=12db, 10X Closer=20db, 100X Closer=40db).
Your Receiver is closer to your neighbors transmitter than your own	Bad	0 to 50db	Anytime your neighbor has the distance advantage on you	The actual magnitude is generally equal to 20 log the ratio of distances involved (For example, 4X Closer=12db, 10X Closer=20db, 100X Closer=40db).
Antenna Angular Discrimination	Good	0 to 25db (more possible at higher freqs)	Practical limit varies depending upon system configuration (Point to Point, or Point to Multipoint), Size of Antenna relative to wavelength, Style of Antenna, which way it is pointing, etc.	Look at specific circumstances and characteristics of the antennas involved (Note: Full antenna discrimination is usually not achievable on top of polarization discrimination discussed in the next line.)
Antenna Polarization	Good	0 to 20db	Benefit occurs when your polarization is different from your neighbor.	Need to know what your polarization is relative to neighbors
Your Transmitter is bigger than your Neighbors	Good	Usually 0 to 10db or less		Simply subtract dbm levels, or if powers are expressed in milliwatts, it is 10 log the ratio of the power levels (for example, your Tx is 100 milliwatts, and your neighbor is 50 milliwatts, that gives you a 3db advantage.)
Your neighbor's Transmitter is bigger than yours	Bad	Usually 0 to 10db or less		Simply subtract dbm levels, or if powers are expressed in milliwatts, it is 10 log the ratio of the power levels (for example, your neighbor's Tx is 100 milliwatts, and your Transmitter is 50 milliwatts, that puts you at a 3db disadvantage.)
Good Path Differential is when the path from my Tx to my Rx is better than the path from the neighbor's TX to my Rx.	Good	Usually 0 to 20db, but can easily	Benefit occurs when the interfering path does not have adequate fresnel clearance, or is obstructed, or has fallen victim to a destructive ground reflection.	Analysis requires looking at the paths involved. In point to multipoint systems, there can be many different path combinations to look at. The focus should always be looking at worse combinations.
Bad Path Differential is when the path from my neighbor's Tx to my Rx is better than my Tx to my Rx.	Bad	Usually 0 to 20db, but can easily be more	Determent occurs when the desired path does not have adequate fresnel clearance, or is obstructed, or has fallen victim to a destructive ground reflection.	Analysis requires looking at the paths involved. In point-to-multipoint systems, there can be many different path combinations to look at. The focus should always be looking at worse combinations.

path analysis software packages out there, I am not aware a single software package you can just dump all this information into and get a quick answer. Even if there was, I think it would still be worthwhile to understand each of the pieces, as the process is part of the "strategic thinking" process.

Keep in mind that all of these factors are really geared toward looking at a specific case. There is a receiver in your system that is trying to hear a transmitter in your system. You want it to hear; but at the same time there are some other transmitters you do not want it to hear.

As you consider these factors within the context of your environment, you will probably be limited to selecting worse case situations for analysis. The number of potential combinations to be looked at, particularly in the context of point-to-multipoint systems, can quickly become more than one person can reasonably do.

One fact that should jump out of the page at you is the fact that receiver selectivity (yes good old fashioned receiver selectivity) is potentially the largest positive factor, potentially rejecting an unwanted signal by a factor of 100 million to one to 10 billion to one. This is in contrast to the "magic" of direct sequence spread spectrum, which provides a benefit on the order of 10 to one, to one thousand to one. Since different manufacturers use different band plans, particularly in the 902-928 MHz range, it is not always obvious when the frequencies of one system are "overlapped" with another. (You can't claim the full benefit of receiver selectivity unless the two systems being considered are completely non-overlapped in frequency.) Usually, this information can be gleaned from the equipment specifications or the equipment manuals.

The applicability of most of the factors fall in line with common sense. For example, if you have a point-to-multipoint system — which includes an Access Point, surrounding Station Adaptors and a master station with an omni-directional antenna — you cannot attribute an angular discrimination benefit to the master station's antenna!

Conclusion

I invite you to test-drive the concept of RF Dominance on a real world implementation you either have, or are considering for implementation. Keep in mind that while you cannot control what other folks do on their own property, you do control what happens on your own property. One hypothetical scenario might be: I know where my points of communication are, and I know where they are in relation to the property line. I can speculate as to what kinds of systems my neighbor might install. Will my system stay whole if my neighbor puts his new system right over by the property line?

In regard to risk, one needs to look at both how far out of dominance one might get and what is the likelihood of that occurring. I don't know that I can give you a specific number that will translate dB's out of balance directly to risk, but I would avoid situations where the probability of being significantly out of balance was high. An example of a bad situation would be an electric power company shooting a direct sequence spread spectrum link into a substation buried in the midst of a neighborhood from a distant mountaintop. Here the scale would tip significantly to the bad side due to the possibility of a consumer transmitter in the house next door having such a large distance advantage over the signal coming from the distant mountaintop.

Another way to use this concept of RF Dominance in the evaluation of risk would be to say, given the geometry and characteristics of my system, how close could a neighbor get with some "typical stuff" before I lost RF Dominance? Once you know how close, it is not hard to speculate about the likelihood. I would advise you to think scientifically and strategically as you move forward in the area of unlicensed spread spectrum communications. ■