Troposcatter Signal Resiliency Capabilities

December 2021

Table of Contents

Figures

Tables

No table of figures entries found.

1.0 PURPOSE

The purpose of this paper is to provide an analysis of signal jamming and signal intercept capabilities and effects on troposcatter paths. It identifies protections that inherently exist in troposcatter, as compared to other forms of RF communication systems. It also identifies the countermeasures that currently exist in troposcatter equipment.

2.0 JAMMING TECHNIQUES

There are many types of jamming techniques. The jamming signal could be a high power, narrowband signal. This would require knowledge of the target frequency in order to focus the jamming power directly on a narrowband signal. Figure 1 shows an example of this type of jamming where the jamming signal is shown in red. The jamming signal may have enough power to surpass the C/I capability of the receive modem or surpass the target signal entirely.

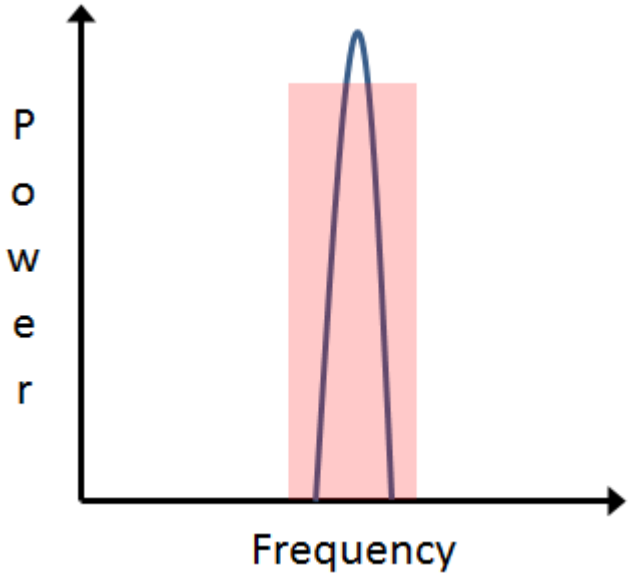

Figure 1. Narrowband Jamming

The jamming signal could also be a wideband signal where the power is spread over a wider bandwidth. This would allow the jamming signal to cover a larger bandwidth if the target frequency is not directly known, but would result in a lower power jamming signal that could be overcome by a higher power narrow band target signal. Figure 2 shows an example of a wideband jamming signal on a narrowband target signal. By spreading the jamming signal over a much larger bandwidth, it has lower signal power and may not be able to effectively jam the narrowband signal. A higher power amplifier may be required to raise the power level of the jamming signal high enough to interfere with the target signal.

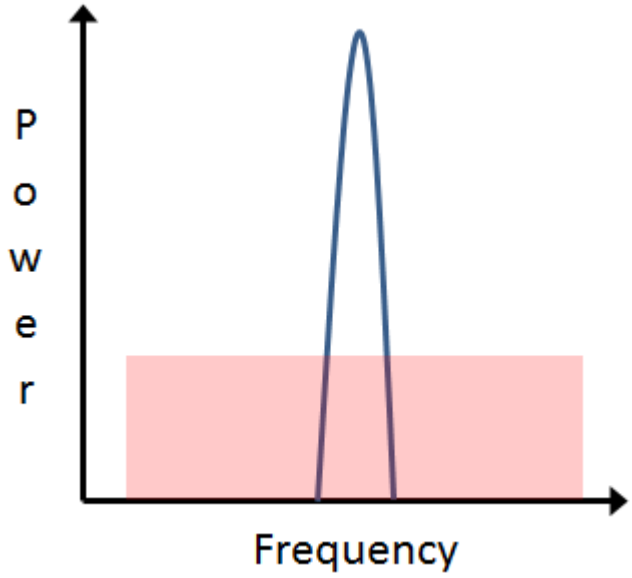

Figure 2. Wideband Jamming

The jamming signal could be continuous, or it could be pulsed. The continuous operation would allow for constant jamming, but increases the chances for the jammer to be detected and located. A pulsed jammer could transmit sporadically, causing equipment synchronization issues while being more difficult to detect. If a modem and router lose synchronization with the same devices on the other side of the link, the connection must be reestablished each time the pulse breaks the communications link.

3.0 CURRENT TROPOSCATTER SYSTEM CAPABILITIES

Current troposcatter systems have a number of characteristics that inherently reduce the probability of jamming and/or interception. In addition to these implicit features, Comtech has also recently implemented a spread spectrum feature in the CS67PLUS radio that carries the dual benefits of improving performance in difficult propagation environments, while also further increasing the resistance of the troposcatter systems to jamming or intercept events.

3.1 Antenna Radiation Pattern

Troposcatter systems employ directional antennas as opposed to omnidirectional antennas. This reduces the probability of intercept and the effect of a jammer due to the focused beam pattern of the directional antenna. The high gain, large antennas used in troposcatter systems, however, increases the distance where a signal can be intercepted while also allowing a jammer to operate further away from the target. The benefit, of course, is that the enemy must have some knowledge of the location of the target in order to operate within the mainlobe or sidelobes of the directional antenna.

3.2 Adaptive Coding and Modulation

The standard design of the CS67PLUS includes the Adaptive Coding and Modulation (ACM) feature. Adaptive Coding and Modulation (ACM) is a capability in which a modem autonomously selects the appropriate data rate and/or modulation scheme to utilize to maximize throughput while maintaining a BER of 1E-06 or better. The change is not limited to data rate and modulation scheme as the Forward Error Correction (FEC) rate is also changed. This feature allows the modem to

optimize the link while monitoring link conditions. Recent improvements in modem technology and design have provided the ability of the modem to implement these data rate and modulation changes on a frame-by-frame basis without affecting connectivity. In essence, the modem can change the data rate and modulation at 1ms intervals. With the addition of newer modulation schemes for troposcatter transmission, there are many modulation and FEC rate combinations which are automatically selected and changed on a millisecond basis. The radio also utilizes proprietary modulation constellations.

In addition to maintaining link availability while maximizing throughput, this feature provides an inherent benefit of making it more difficult for an enemy to intercept and decode user data. If the signal is collected, the enemy would have to identify the modulation scheme. Comtech's modulation schemes are proprietary and the Grey code for each part of the constellation would have to be properly identified. Next, the FEC rate and proprietary FEC codeword structure would have to be correctly identified. The proprietary modem data frame structure would also have to be correctly identified. If the enemy were somehow able to achieve the above, they would have to decrypt the AES256 encryption.

3.3 Data Encryption

Data encryption does not necessarily reduce the probability of intercept of the signal, but it does protect against the capability of an enemy to collect the user information once the signal has been intercepted and the waveform and frame structure have been identified. Commercial AES encryption devices with 128-bit or 256-bit keys provide protection against unwanted data access. These types of devices are commercially available, while military customers generally control their own proprietary types of encryption codes and keys.

The CS67PLUS Troposcatter Radio standard design includes AES-256 Encryption. It can be easily turned ON or OFF by means of the Radio GUI. Customers can also utilize their own encryption devices after they take delivery of the tropo system and provide already encrypted data to the radio for transmission.

3.4 Spread Spectrum Technology

Spread spectrum technology utilizes a wide bandwidth in order to transmit a signal. The bandwidth is much wider than the bandwidth required to transmit the information being carried. The signal is spread in order to reduce the power spectral density (PSD) compared to a narrow band signal. This enables the transmitted signal to appear "noise-like", which provides resistance to jamming and a low probability of intercept (LPI) since the signal is tougher to detect [1]. The spreading is accomplished by using a spreading signal, often called a code signal. This signal is independent of the data [2]. The PSD difference between spread spectrum signals and narrow band signals also allows them to share the same frequency band with little or no interference [1]. At the receiver, despreading is accomplished by correlating the received spread signal with a synchronized replica of the spreading signal used to spread the information [2].

Other standard modulation schemes, such as frequency modulation (FM) and pulse code modulation (PCM), also spread the spectrum on the information signal. These modulation schemes, however, do not qualify as spread spectrum systems because they do not satisfy the required conditions to be qualified as spread spectrum [2].

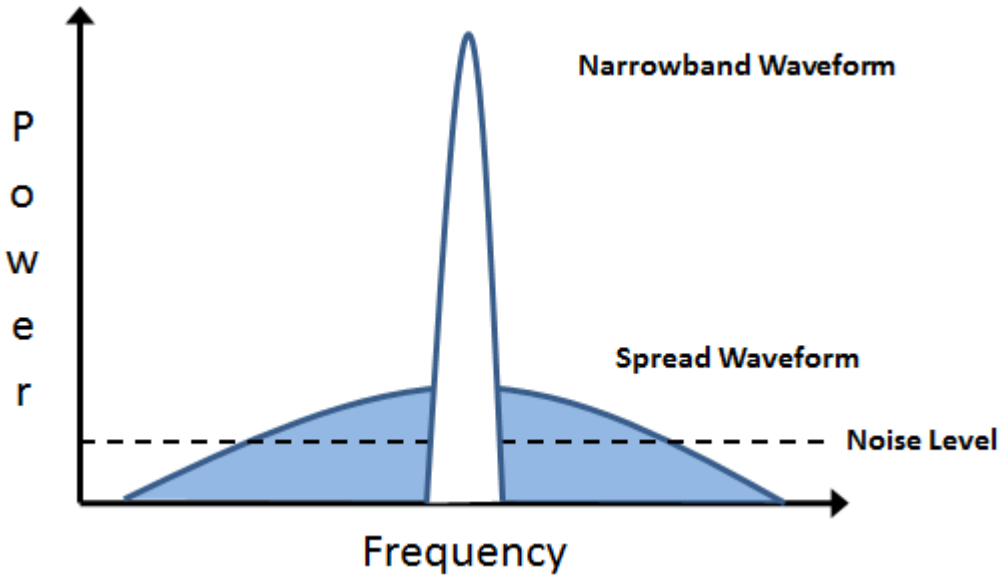

Figure 3. Spread Spectrum Signal

Spread spectrum techniques were developed initially for military applications to enable reliable communications in the presence of enemy jamming. The idea behind its capability was in relation to a narrowband signal. A narrowband jamming signal could focus its power on the narrowband communication signal and be effective in reducing its capability to establish communication. When the communication signal is spread over a wider bandwidth, the jamming signal can be established in two ways. The jamming signal can be narrowband, which would yield a higher PSD, but would not cover the entire spread of the communications signal. The jamming signal could also be wideband, which would cover the entire spread signal, but it would have a lower PSD. Therefore, spread spectrum is inherently resistant to jamming [2].

There are several techniques for implementing spread spectrum. They include the following: Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), Time Hopping Spread Spectrum (THSS), and Chirp Spread Spectrum (CSS), as well as hybrids using more than one technique simultaneously.

3.5 Direct Sequence Spread Spectrum

The CS67PLUS Tropo Radio currently contains a Direct Sequence Spread Spectrum (DSSS) feature. It is a modulation technique used to reduce overall signal interference, increase link range, or decrease system transmit power to reduce probability of detection. It effectively makes the transmitted signal wider in bandwidth than the information bandwidth. After the dispreading or removal of the direct sequence modulation in the receiver, the information bandwidth is restored, while unintentional and intentional interference is substantially reduced.

DSSS modulation techniques are composed of two modulation processes that are performed on the carrier signal. The first process is executed by the spreading code and generates the wide bandwidth that is characteristic of spread spectrum communications. For the duration of every message bit, the carrier is modulated following a specific sequence of bits, also referred to as chips [3]. The number of chips per message bit is known as the chip rate [4]. The process is known a “chipping” and results in the substitution of every message bit by the same sequence of chips. The chip sequence used is the spreading code [3]. The spreading code must be as long and random as possible to allow the signal to appear as noise-like as possible. The code, however, must be reproducible so that the

receiver can extract the message. Therefore, the code is a pseudorandom number (PRN) [4]. The longer the PRN, the less likely it is that the sequence can be determined and intercepted [3].

The second process is executed by the message being transmitted. For message bits of the value "0", the sequence of chips used to represent the bit is the same as the spreading code. For message bits of the value "1", the sequence of chips used to represent the bit is the inverted value of the spreading code. Redundancy is achieved by the presence of the message bit on each chip of the spreading code [3]. This process, effectively, spreads the transmit power equally over the entire bandwidth of the spread signal. Over the frequency band of the signal, the spreading code creates a large number of carriers at specific frequencies and phases.

In the CS67PLUS, the User Selectable Symbol Rate is proportionate to the occupied bandwidth. This means that 2.5Msps uses 2.5MHz, 5Msps uses 5MHz, 10Msps uses 10MHz, and 20Msps uses 20MHz of spectrum space. The DSSS technique effectively transmits 2.5Msps of information using eight (8) blocks of 2.5MHz bandwidth, so the transmitted signal takes up the full occupied bandwidth of 20MHz. Similarly, at DSSS 5MHz the radio transmits four (4) 5Msps blocks to equal 20MHz of occupied bandwidth and at DSSS 10MHz, two (2) 10MHz wide blocks are transmitted to equal 20MHz of occupied bandwidth. In doing so, there is a processing gain of up to 9.5dB and the SNR received can actually be below the system noise floor.

4.0 CONCLUSION

While troposcatter systems are not completely immune to signal jamming and intercept events, Comtech's current troposcatter solutions do provide inherent resistance to signal jamming and intercept. These features were not designed specifically to combat these issues, but provide added capabilities, nonetheless. The architecture of the current CS67PLUS troposcatter radio provides a very robust method of scrambling the data stream which would make it extremely difficult to reverse engineer in order to capture user data. Additionally, the spread spectrum feature recently implemented on the CS67PLUS can be used to further increase the resilience of the systems.

Bibliography

1. Prabakaran, Prabakar. "Design How-To: Tutorial on Spread Spectrum Technology." *EE Times*. UBM Tech, 6 May 2003. Web. 11 Mar. 2015.

2. Sklar, Bernard. *Digital Communications: Fundamentals and Applications*. 2nd ed. Upper Saddle River: Prentice Hall PTR, 2001. Print.

3. Schwartz, Sorin. "Frequency Hopping Spread Spectrum vs. Direct Sequence Spread Spectrum in Broadband Wireless Access and Wireless LAN." Sorin M. Schwartz Seminars. Web. 11 Mar. 2015.

4. "Tutorial 1890: An Introduction to Spread-Spectrum Communications." Maxim Integrated. 2015. Web. 12 Mar. 2015.