iDIRECT Government

WHITE PAPER

Signal Excision Technology: CSIR™

INTRODUCTION

Anti-jam and security concerns for satellite communications (SATCOM) are not new. Bad actors are always on the move to penetrate communications on and off the battlefield, make them ineffective and jam signals.

Getting critical information across a communications link is essential to the success of any mission. Overcoming interference and jamming events allows these satellite communications links to be reliable during these critical times. This white paper will highlight the benefits and implementation strategies of key iDirect Government (iDirectGov) features that can mitigate against both interference and jamming signals while maintaining spectral efficiency. iDirectGov's Communications Signal Interference Removal (CSIR) technology can be utilized to mitigate interference. CSIR, coupled with other iDirectGov Evolution Defense features, can be used to deliver even more robust anti-jam SATCOM capability.

RESILIENT. SECURE. INNOVATIVE.

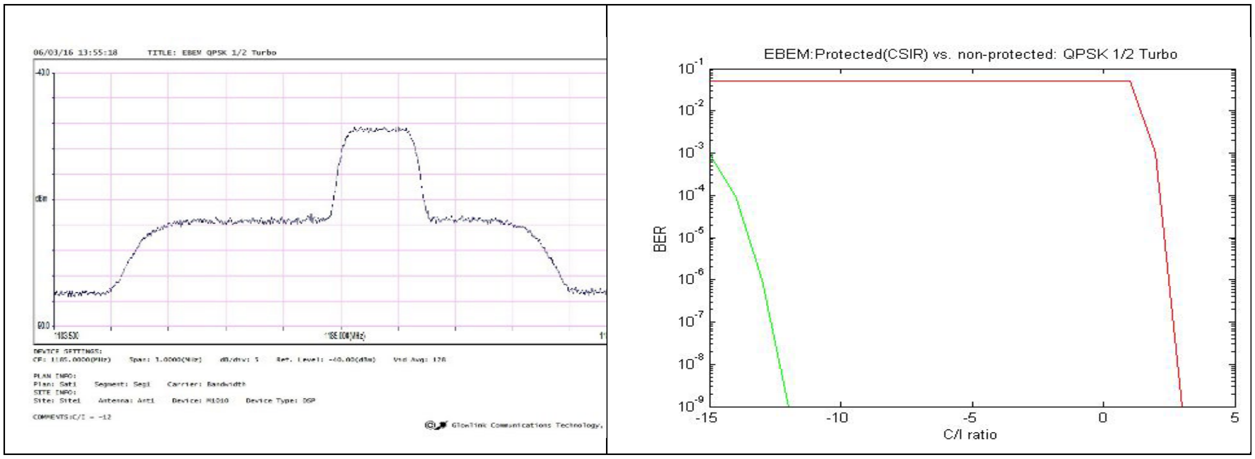
iDIRECT Government

CSIR OVERVIEW

CSIR is a proven technology for removing co-channel interference received with digital communication or navigation links. CSIR is developed to deal with co-channel interference when a copy of the interfering signal is not available. Differing from traditional interference mitigation techniques, CSIR does not require any information about the interference signal to remove it from the link it is protecting. Additionally, CSIR doesn't require information about the interference during the removal process, making its software footprint lightweight, responsive, and effective against a wide range of interference and jamming signals, including partial band noise.

CSIR performance is evaluated based on the headroom. Figure 1 below, the left plot, a power spectrum of the signal of interest (SOI), and an in-band interfering signal. In this case, the SOI is the wider and lower signal, and the in-band interferer is the stronger, narrower signal. The right plot shows two curves with the rightmost curve being the modem alone and the leftmost curve being with CSIR added. Headroom is measured directly from this plot and is a measure of the difference in C/I for the same Bit Error Rate (BER). The lower the C/I figure is the better as this indicates the receiver can tolerate stronger interference. In the case when CSIR is added for the plot below, approximately 15dB of headroom is shown.

The plot in Figure 1 can also be made using J/S instead of C/I. If done, the curves will reflect across the x-axis. However, the same headroom will result because J/S is the inverse of C/I.



```
DEVICE SETTINGS:
CF: 1185.0000(MHz)    Span: 1.0000(MHz)    dB/div: 5    Ref. Level: -40.00(dBm)    Vid Avg: 128

PLAN INFO:
Plan: Sat1    Segment: Seg1    Carrier: Bandwidth
SITE INFO:
Site: Site1    Antenna: Ant1    Device: M1010    Device Type: DSP

COMMENTS:C/I = -12
```

Figure 1. CSIR Headroom Definition (Performance Improvement)

CSIR Performance and Interference/Jamming Use Cases

Interference can come from various sources including equipment failure, accidental interference, often referred to as blue on blue, as well as intentional interference, often referred to as red on blue. Some commonly observed interferences in SATCOM include CW tones, CW sweepers, modulated and various noise-like signals.

This paper will examine how CSIR can mitigate a variety of interferences, including those mentioned above. Additionally, several specific interference cases will be examined to illustrate how CSIR can be combined with existing waveform techniques to provide increased levels of protection against both simple and sophisticated jamming attempts.

Red-on-blue jamming is intentional jamming by an adversary to bring down a communications channel. An example of red-on-blue jamming is matched carrier jamming. In this scenario, a replica of the carrier is retransmitted on top of itself. This means that the jamming signal has the same bandwidth and center frequency, as the carrier of interest. This scenario can prove challenging in that the interference is subtle and difficult to notice. This is especially true if the retransmitted power is equal or lower than the signal of interest as the power spectral density of the received signal will look very similar with or without the retransmitted interference. Given that the interference is broadband and uncorrelated with the signal of interest, it has the same effect as elevated white noise on the receiver.

Another example of red-on-blue jamming is a higher-power partial band noise jamming signal. This occurs when the bandwidth of the jamming signal is a significant fraction of the signal of interest and at a higher power. As with a matched carrier jamming event, most other mitigation techniques, like those using successive interference cancelation (SIC), cannot protect against this event. CSIR combined with Direct Sequence Spread Spectrum (DSSS) cannot only mitigate this interference but result in a bandwidth-efficient and easy-to-deploy solution within iDirectGov's Evolution Defense architecture.

CSIR PERFORMANCE

CSIR headroom performance varies based on the interference type. Table 1 below shows CSIR performance for a 20Msps QPSK 1/2 rate carrier against a variety of interferers. A key differentiator of CSIR is no additional bandwidth is required, thus not sacrificing throughput, unlike traditional spread spectrum anti-jam solutions.

Interference Category	Interference Pattern	Measured Headroom
Interference	Single CW Tone	62dB
Interference	5-Tone Comb (5 in-band CWs)	48dB
Interference	CW Tone + 2MSPS Modulated Interferer	43dB
Interference	2 MSPS Modulated Interferer or 2MHz Bandlimited Noise (10%)	45dB
Interference	4 MSPS Modulated Interferer or 4 MHz Bandlimited Noise (20%)	34dB
Interference	6 MSPS Modulated Interferer or 6 MHz Bandlimited Noise (30%)	22dB

Table 1. Measured Headroom Against a 20Msps QPSK 1/2 Route Carrier

CSIR coupled with other anti-jam techniques can provide greater protection margins in spectrally efficient ways. Table 2 below shows the comparison between DSSS as a stand-alone excision approach against a solution with DSSS+CSIR. DSSS+CSIR provides a robust and spectrally efficient excision solution for narrow-band interference, DSSS by itself is unable to provide the equal amount of protection as the DSSS+CSIR solution. When looking at wider-band jamming (the 80% use case below), the standalone DSSS solution requires 32 times the amount of bandwidth as the DSSS+CSIR solution. The addition of CSIR to the DSSS waveform allows for the most spectrally efficient excision solution.

Interference Category	Interference Pattern	DSSS Waveform Only SS=4 (max J/S)	DSSS Waveform + CSIR (max J/S)	DSSS spread factor to get to same J/S as CSIR + DSSS
Interference	Single CW Tone	4.99 dB	70 dB	>8 million
Interference	5-Tone Comb (5 in-band CWs)	4.99 dB	70 dB	>8 million
Interference	CW Tone + 2MSPS Modulated Interferer	4.99 dB	60 dB	>1 million
Interference	2 MSPS Modulated Interferer or 2MHz Bandlimited Noise (10%)	4.99 dB	60 dB	>1 million
Interference	4 MSPS Modulated Interferer or 4MHz Bandlimited Noise (20%)	4.99 dB	50 dB	>65000
Interference	6 MSPS Modulated Interferer (30%)	4.99 dB	45 dB	>30000
Jamming	16 MSPS Modulated Interferer(80%)	4.99 dB	20 dB	128

Table 2.

As shown in Table 2, CSIR can provide bandwidth efficiency to a DSSS anti-jam waveform. Techniques like Frequency Hop Spread Spectrum (FHSS) and DSSS, trade throughput for resiliency. With the inclusion of CSIR, additional protection is added while also saving bandwidth.

Figure 2 below shows how CSIR can add protection while increasing throughput for Adaptive Coding and Modulation (ACM) waveforms that exchange throughput for resiliency. It also displays how combining CSIR with ACM maintains the link throughput as the J/S is increased. Without CSIR, the ACM-only link fails (goes to 0 throughput) at a J/S > 5 dB, but the link using ACM and CSIR holds near full throughput beyond a J/S of 20 dB.

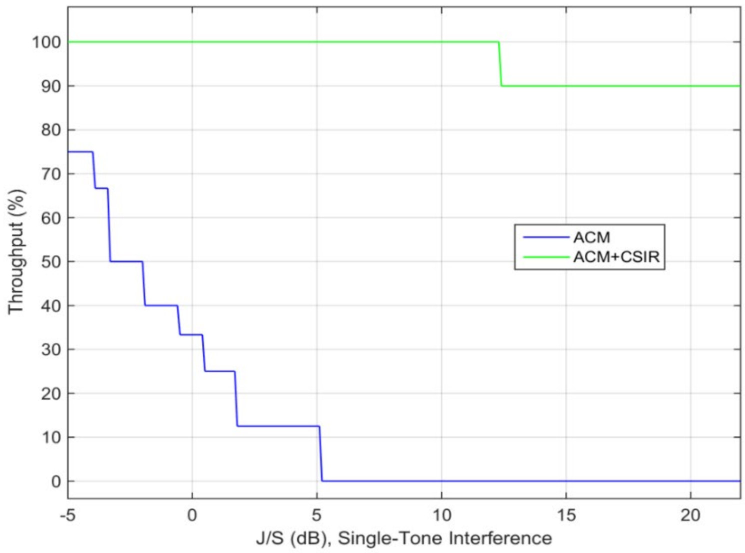


Figure 2. CSIR and ACM

SAMPLE IDIRECTGOV EVOLUTION DEFENSE NETWORK

The following examples will examine how CSIR, DSSS, and iDirectGov’s ATDMA return channel waveform can protect against both interference and jamming while operating at the most efficient MODCOD during the specific operating environment. The iDirectGov Evolution Defense network used in this example consists of a DVB-S2/ACM downstream carrier with four ATDMA upstream carriers. The benefit of ACM and ATDMA technology is that it allows for efficient use of the satellite bandwidth. During clear skies and non-interfering conditions, remote terminals can receive their highest possible MODCOD. As with the downstream, the ATDMA upstream allows remotes to close at the highest possible MODCOD during clear sky conditions. With ACM on the downstream and ATDMA upstream, remotes can close at a lower MODCOD during not only rain fade scenarios, but also during interference events. Figure 3 below shows the RF spectrum of the example DirectGov Evolution Defense network.

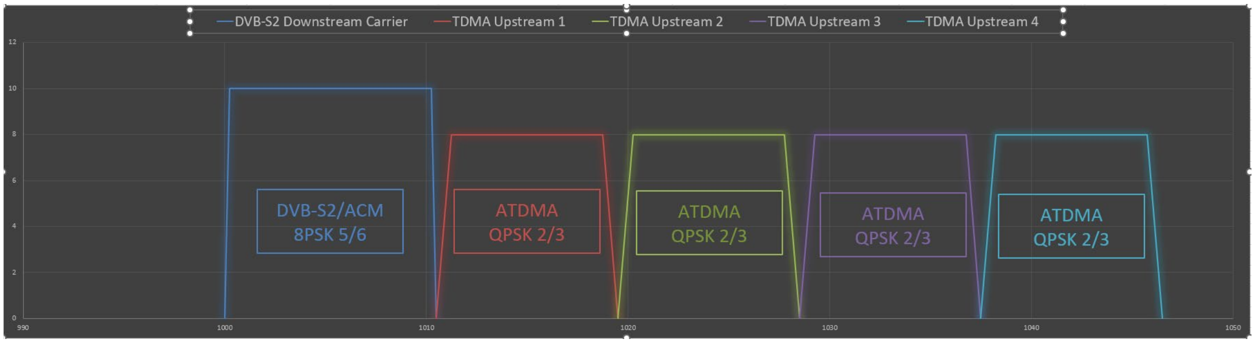


Figure 3. Typical Network RF Spectrum

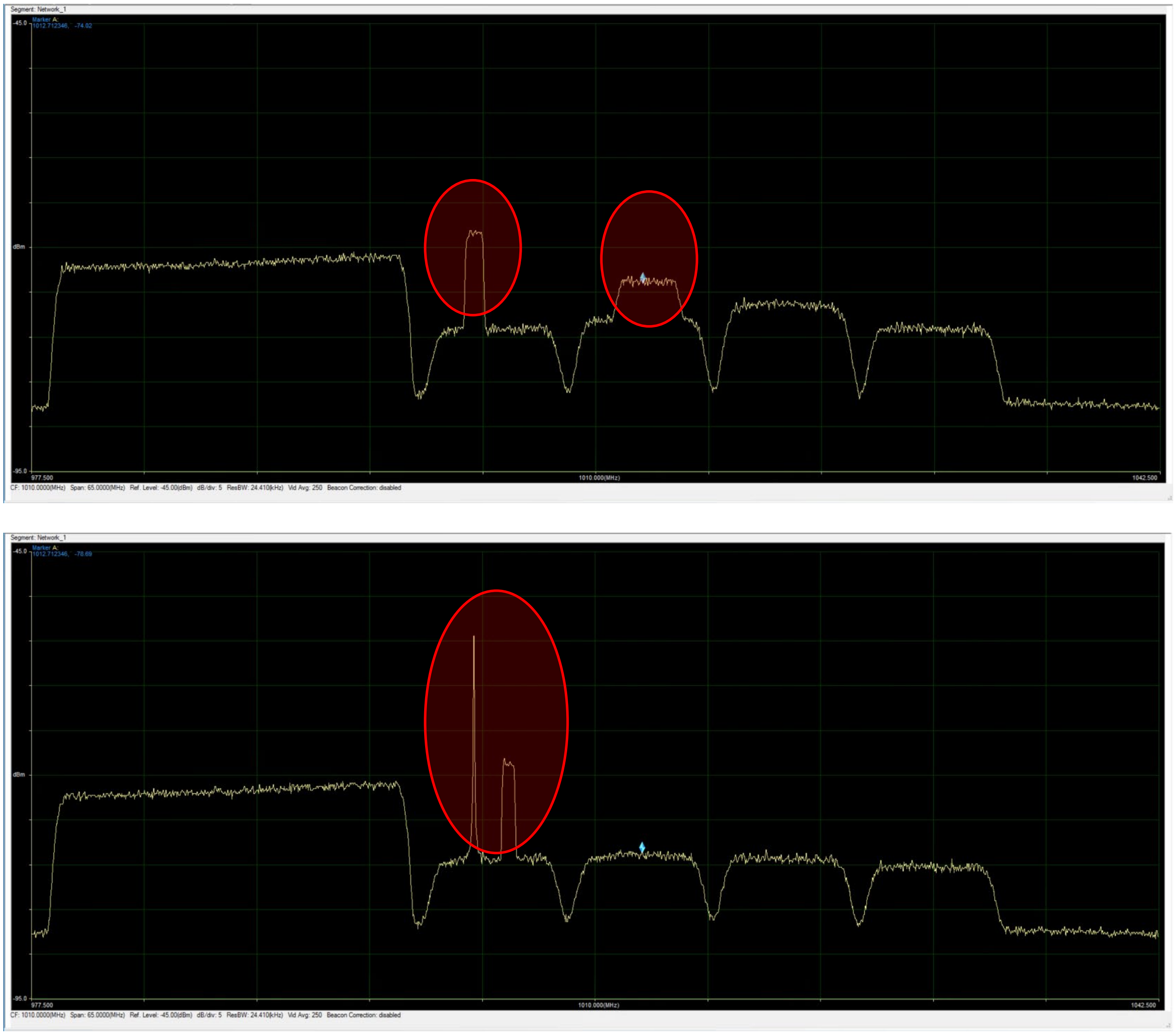
Table 3 shows carrier configuration parameters for thesample network, including the size of the carriers, bit rate for each carrier, and the MODCOD used.

Carrier Name	Carrier Type	Symbol Rate (kbps)	Carrier Spacing	Bandwidth Required (MHz)	Bit Rate (Mbps)	DVB-S2 Nominal MODCOD	Minimum MODCOD
DVB-S2 Downstream	DVB-S2 Downstream	10000.00	1.05	10.5	23.30	8PSK 5/6	QPSK 1/4
TDMA Upstream 1	TDMA Upstream	7500.00	1.2	9.00	10.00	N/A	QPSK 2/3
TDMA Upstream 2	TDMA Upstream	7500.00	1.2	9.00	10.00	N/A	QPSK 2/3
TDMA Upstream 3	TDMA Upstream	7500.00	1.2	9.00	10.00	N/A	QPSK 2/3
TDMA Upstream 4	TDMA Upstream	7500.00	1.2	9.00	10.00	N/A	QPSK 2/3
			TOTAL BANDWIDTH	46.5			

Table 2. Carrier Parameters for Nominal Network

In the Nominal Network example, the remote systems can achieve 23.30Mbps of receive data throughput and a total of 40Mbps of transmit throughput data (a maximum of 10Mbps per terminal).

Figure 4 shows a narrow modulated interferer on one ATDMA channel and a wider modulated interferer on the second ATDMA channel. When CSIR is enabled, it can completely mitigate the interferences and maintain the data throughput in an error-free environment. CSIR can also protect against multiple interferers at the same time, as shown in, the first ATDMA carrier is hit simultaneously with a CW and a narrow band interferer. In the previous example, CSIR can completely mitigate this interference and keep the return channel at maximum throughput.



CF: 1010.0000(MHz) Span: 65.0000(MHz) Ref. Level: -45.00(dBm) dB/div: 5 ResBW: 24.410(kHz) Vid Avg: 250 Beacon Correction: disabled

CF: 1010.0000(MHz) Span: 65.0000(MHz) Ref. Level: -45.00(dBm) dB/div: 5 ResBW: 24.410(kHz) Vid Avg: 250 Beacon Correction: disabled

Figure 4. Nominal Configuration Interference Examples

ADAPTED IDIRECTGOV EVOLUTION DEFENSE NETWORK

The example above shows the throughput a sample network can achieve during nominal conditions. With CSIR, this network can experience significant levels of interference without having any effect on throughput. The amount of interference power the network can withstand while maintaining its original throughput will vary depending on the interference type and makeup.

In an adaptive iDirectGov Evolution Defense network, the forward link combines both CSIR and ACM to mitigate interference. Depending on the interference and its power, CSIR can potentially mitigate the interference completely without the link needing to adjust MODCODs and lower throughput. As the interferer becomes more noise-like, the link will adjust accordingly and scale to a more robust MODCOD. This results in a lower downstream throughput, however, remotes will still be able to operate error-free within the network. One important attribute of CSIR is that the headroom will grow non-linearly as the modulation is reduced or the coding is increased. This enables the forward link to survive high-power interferences as well as higher throughputs in the face of more modest interferences.

For the ATDMA return carriers, the MODCOD will not adapt based on link performance. The remote terminal will adjust its uplink power until it reaches maximum operating power. If the interference grows in power and/or bandwidth, the remotes in the network will start experiencing errors. The first option to overcome stronger interference is to adjust each ATDMA return carrier's MODCOD manually. Another option is to combine some or all of the ATDMA return carriers and lower the MODCOD on this combined ATDMA carrier.

MANUAL ATDMA MODCOD CHANGES

One way to transition to a more robust carrier configuration is by adjusting the MODCOD settings on one or more of the ATDMA in-route carriers. In the current generation of the product, the ATDMA in-route carriers do not automatically adjust their MODCOD based on changing link conditions. As a result, switching to a more robust MODCOD requires a manual process. This is done through iDirectGov’s iVantage NMS suite. The network operator would modify the inroute group in iBuilder and update its composition. Then, the operator can change the MODCOD for one or all of the TDMA carriers in the in-route group. For this example, we will assume that two of the four ATDMA carriers are experiencing a unique type of interference. On one of these ATDMA carriers, the interfering carrier is a replica of the ATDMA carrier itself. This represents a matched bandwidth (and power) interferer. In this case, the MODCOD for this carrier would be changed to BPSK 2/3 with a spread factor of two times. This MODCOD, along with spreading and CSIR, will overcome this sophisticated interference.

On the second ATDMA carrier that is being interfered with, the interfering carrier is a wide-band, high-power interferer. The combination of wide-band and high power is a corner case where CSIR alone isn’t enough to completely mitigate the interference. By switching to a more robust DSSS configuration with CSIR, a suitable amount of protection will be provided to mitigate the interference. In this use case, the MODCOD was switched to BPSK 1/2 with a spread factor of four. The modified ATDMA carriers are shown in Figure 5 of the RF spectrum below.

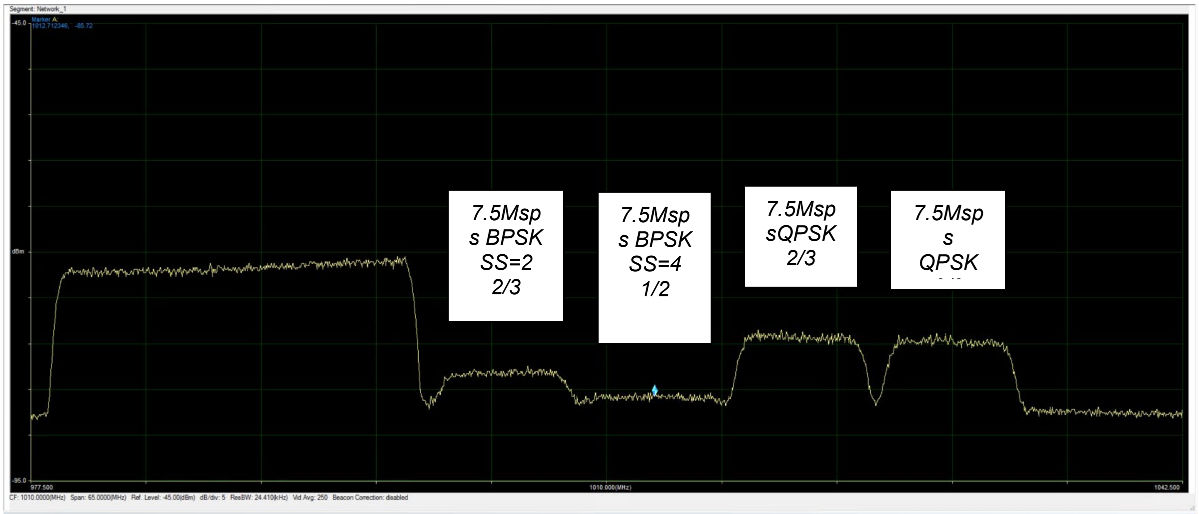
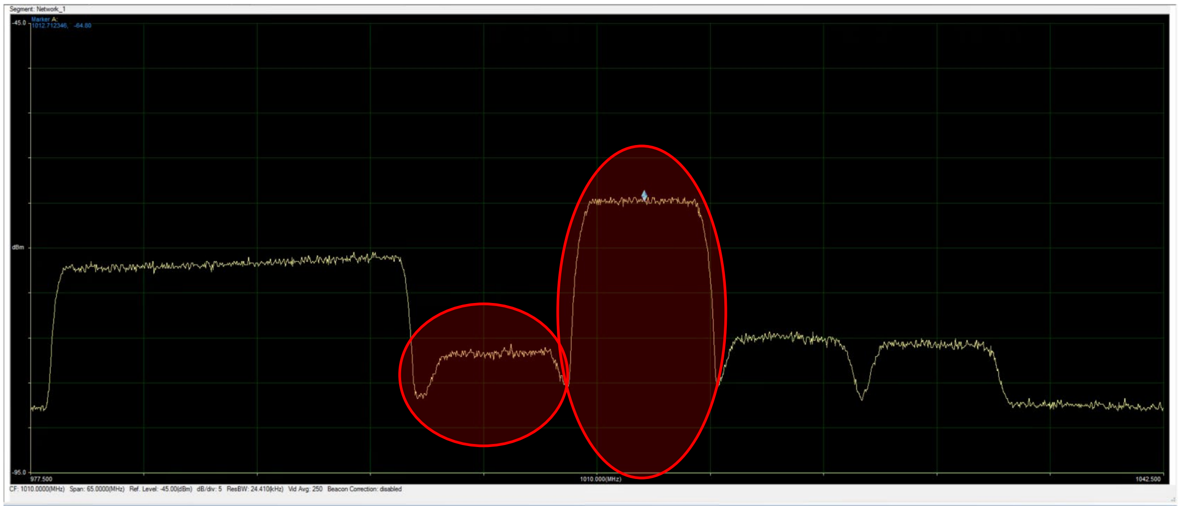


Figure 5. Network configuration 1 – no Interference

Figure 6 shows this same RF spectrum with the addition of the interferers. Both ATDMA carriers that are being interfered with are able to overcome interference and transmit error-free data.



Segment: Network_1

CF: 1010.0000(MHz) Span: 65.0000(MHz) Ref. Level: -45.00(dBm) dB/div: 5 ResBW: 24.410(kHz) Vid Avg: 250 Beacon Correction: disabled

Figure 6. Network configuration 1 - With Interference

Table 4 below shows the updated carrier configuration for this interference event. With this carrier configuration, the total network throughput drops due to the switch to more robust MODCODS. However, the amount of allocated bandwidth on the satellite required remains the same. Because of the lower MODCODS, the amount of power allocated to the satellite will drop. But this addition in power availability can also be used to assist in the mitigation of the jamming event.

Carrier Name	Carrier Type	Symbol Rate (kbps)	Carrier Spacing	Bandwidth Required (MHz)	Bit Rate (Mbps)	DVB-S2 Nominal MODCOD	Minimum MODCOD
DVB-S2 Downstream	DVB-S2 Downstream	10000.00	1.2	10.5	23.30	8PSK 5/6	QPSK 1/4
TDMA Upstream 1	TDMA Upstream	7500.00	1.2	9	2.5	N/A	BPSK 2/3 SS=2
TDMA Upstream 2	TDMA Upstream	7500.00	1.2	9	0.9375	N/A	BPSK 1/2 SS=4
TDMA Upstream 3	TDMA Upstream	7500.00	1.2	9.00	10.00	N/A	QPSK 2/3
TDMA Upstream 4	TDMA Upstream	7500.00	1.2	9.00	10.00	N/A	QPSK 2/3
			TOTAL BANDWIDTH	46.50			

Table 3. Carrier Parameters for Modified Network

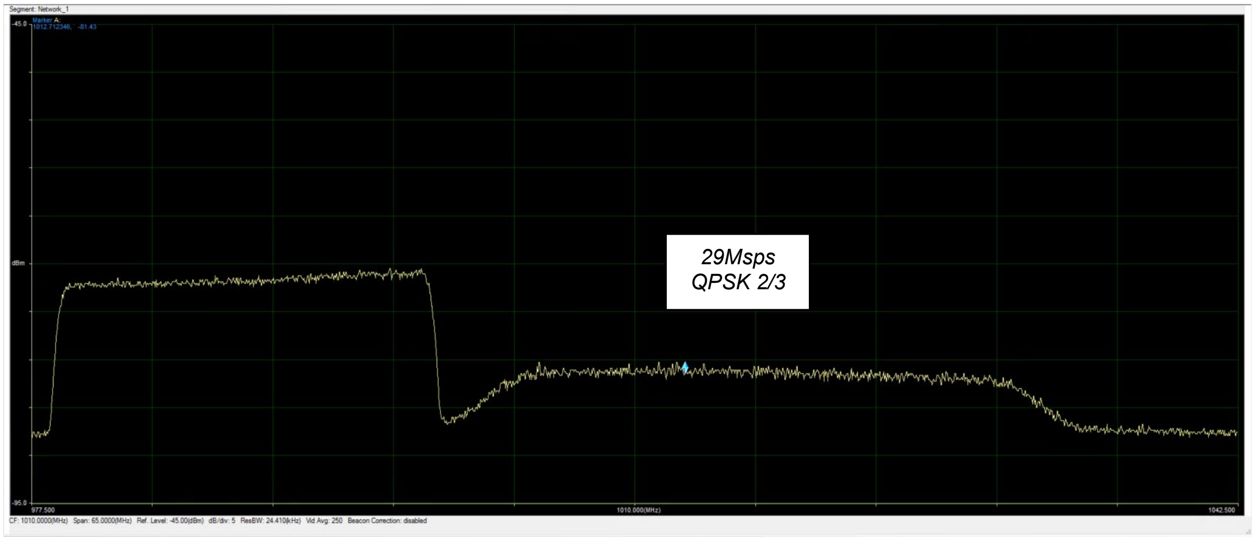
The total amount of bandwidth required to support this network configuration remains the same as the original configuration. However, the IP data rate for ATDMA returns carriers one and two drops. The first ATDMA carrier drops from 10Mbps to 2.5Mbps to support this interference scenario in the same bandwidth. The second ATDMA carrier drops from 10Mbps to 0.9375Mbps to support this interference scenario without requiring any additional bandwidth. The last two ATDMA carriers remain the same and still support 10Mbps.

While total network throughput drops, there are benefits to changing the network configuration. In addition to overcoming the interference, the network is still operating within its originally allocated bandwidth. Two of the four ATDMA return carriers are still operating at full performance and the other two are operating error-free at a lower throughput. This results in the least amount of cost and a less complex change in network configuration.

SYMBOL RATE AND MANUAL ATDMA MODCOD CHANGES

Switching over to a more robust carrier configuration can also be done by combining two or more of the ATDMA carriers into a larger, stronger MODCOD carrier configuration. The main benefit to this solution is that the burstable rate for all remotes will remain the same as the original configuration. The total network throughput drops because the configuration goes from four carriers to a single carrier, but the burstable throughput increases. This is suited for scenarios including ISR where the video streaming rate is static and an ISR remote will need to keep the same burstable bandwidth.

By making this change it creates a single larger ATDMA carrier that lowers the interference to the carrier of interest ratio and allows for CSIR to be more efficient during a majority of interference events. For example, the sample network has four 7.5Msps ATDMA carriers. If we combine those into one ATDMA carrier, the symbol rate would be 30Msps. If we have a 7.5Msps interferer, that interferer goes from a 100% interferer to a 25% interferer. This improves the CSIR headroom by ~18-22dB. This also allows this interference type to be addressed by CSIR alone instead of a combination of CSIR and DSSS. Figure 7 below shows the new configuration for this sample network.



CF: 1010.0000(MHz) Span: 65.0000(MHz) Ref. Level: -45.00(dBm) dB/div: 5 ResBW: 24.410(kHz) Vid Avg: 250 Beacon Correction: disabled

Figure 7. Network configuration 2 – No Interference

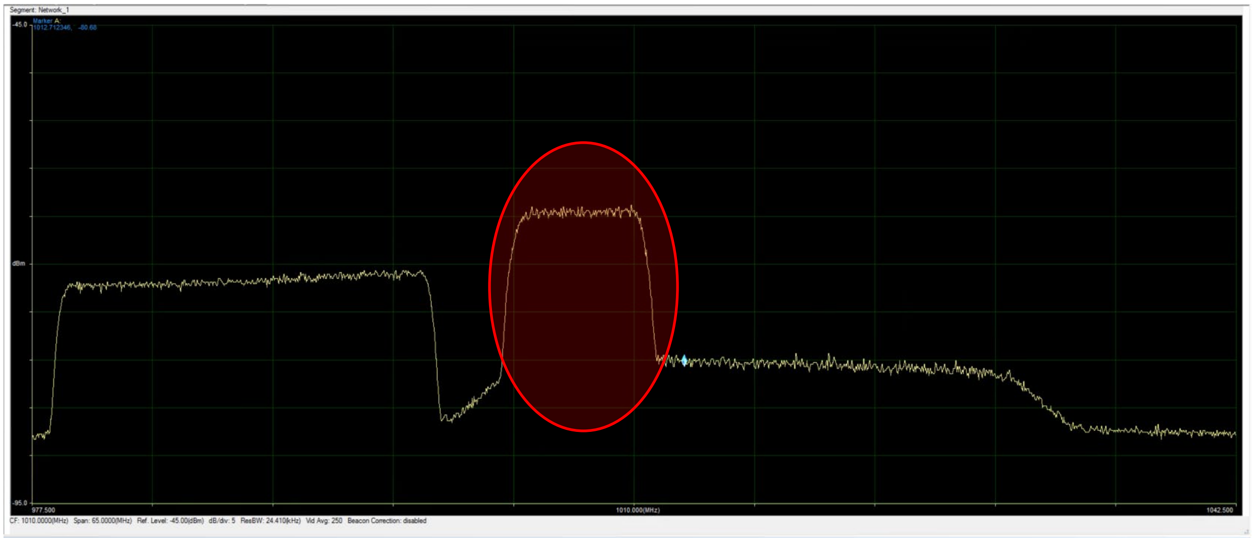
Table 5 below shows the updated network parameters for this scenario.

Carrier Name	Carrier Type	Symbol Rate (kbps)	Carrier Spacing	Bandwidth Required (MHz)	Bit Rate (Mbps)	DVB-S2 Nominal MODCOD	Minimum MODCOD
DVB-S2 Downstream	DVB-S2 Downstream	10000.00	1.2	12.0	23.30	8PSK 5/6	QPSK 1/4
TDMA Upstream 1	TDMA Upstream	29000.00	1.2	34.8	40	N/A	QPSK 2/3
			TOTAL BANDWIDTH	46.8			

Table 4. Scenario Two Carrier Parameters

For the scenario shown in Table 5, the total network throughput remains the same as the original configuration. What has changed is the individual burstable bandwidth that a remote can burst into, instead of four 10Mbps carriers, there is now a single 40Mbps carrier.

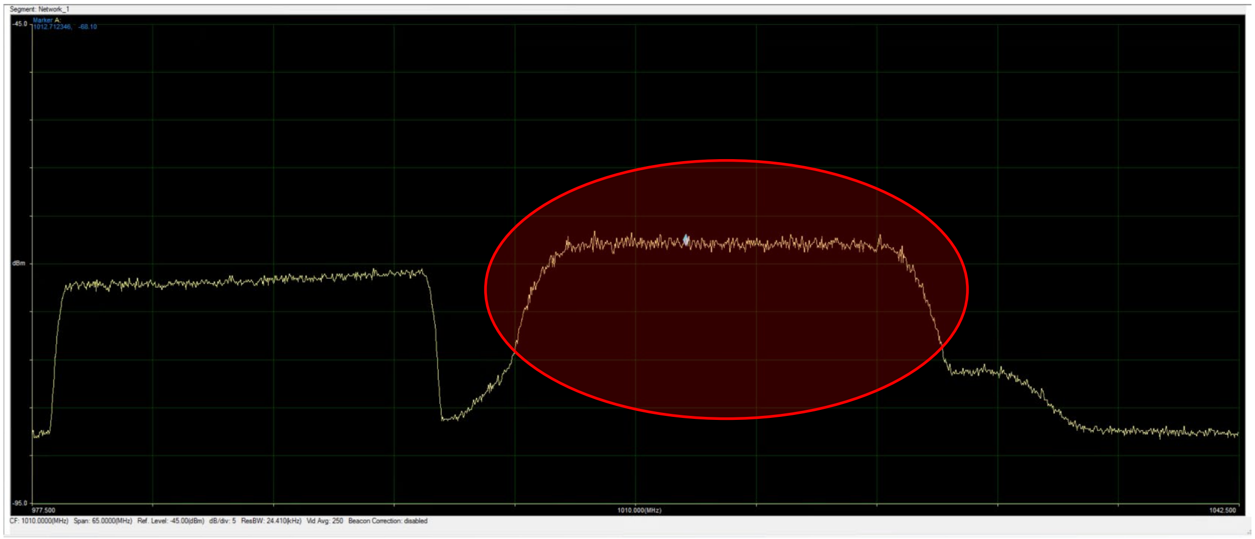
Figure 8 shows the same interferer shown in Figure 6 applied to the new network configuration. This updated carrier with CSIR can handle the same size interferer at a higher power (~15dB above the carrier of interest).



CF: 1010.0000(MHz) Span: 65.0000(MHz) Ref. Level: -45.00(dBm) dB/div: 5 ResBW: 24.410(kHz) Vid Avg: 250 Beacon Correction: disabled

Figure 8. Network configuration 2 - With Interference

By utilizing this method of interference mitigation, the change to a single large ATDMA carrier is the first step in providing a more robust interference mitigation configuration. Not only is a higher power interferer handled, but simultaneously, the network is running at full throughput. If more protection is required, the ATDMA carrier can change to a more robust MODCOD as with the scenario in Figure 6. Figure 9 and 10 below show two examples of larger interferers that can be completely mitigated with this configuration. In this scenario, the MODCOD for the ATDMA carrier changes from QPSK 2/3 to BPSK 2/3 SS=4. When changing this 29Msps carrier’s MODCOD to BPSK 2/3 SS=4, the data rate changes from 40Mbps to 5Mbps. In this configuration, both the network throughput and the burstable throughput for each individual remote are significantly reduced. However, the total satellite bandwidth remains the same, and the carrier operates in its most robust setup.



CF: 1010.0000(MHz) Span: 65.0000(MHz) Ref. Level: -45.00(dBm) dB/div: 5 ResBW: 24.410(kHz) Vid Avg: 250 Beacon Correction: disabled

Figure 9. 29Msps BSPK 2/3 SS=4 Carrier with 24Msps Interferer

In Figure 9 above, the 24Msps interferer is 15dB above the 29Msps ATDMA carrier. In Figure 10 below, a fully matched 29Msps interferer is shown 7dB above the ATDMA carrier. In both cases, these high-power interferences are mitigated by the combination of CSIR and the flexibility of the ATDMA return channel.

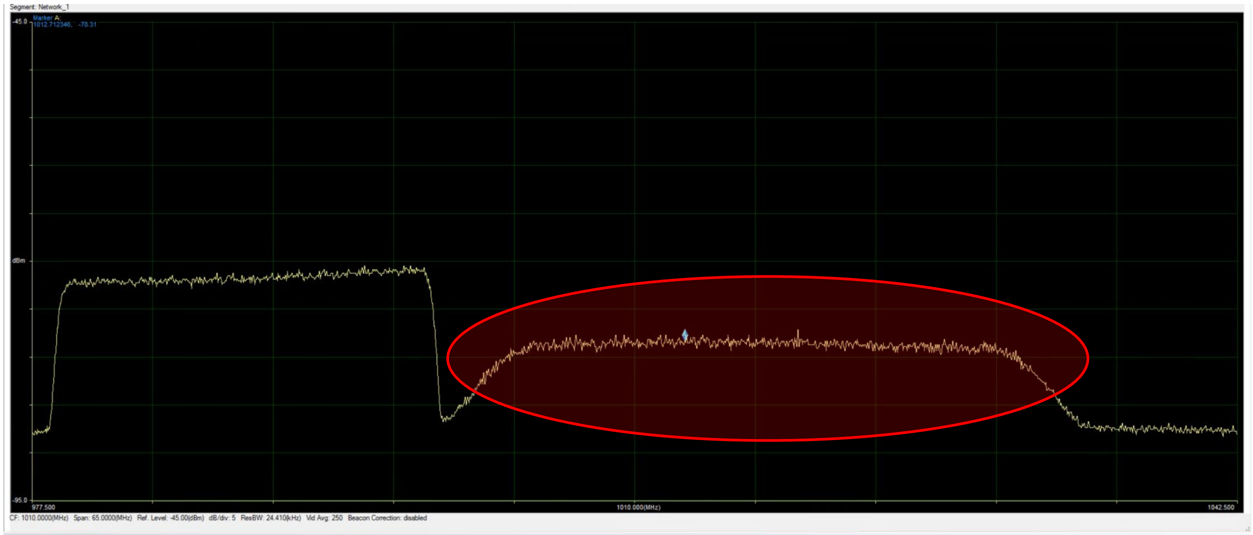

Segment: Network_1
Marker A:
1012.712346, -78.31
-45.0
dBm
-95.0
977.500
1010.000(MHz)
1042.500
CF: 1010.0000(MHz) Span: 65.0000(MHz) Ref. Level: -45.00(dBm) dB/div: 5 ResBW: 24.410(kHz) Vid Avg: 250 Beacon Correction: disabled

Figure 10. 29Msps BSPK 2/3 SS=4 Carrier with 29Msps Interferer

As shown, this approach to interference provides robust configurations. The larger ATDMA carriers perform better against a fixed interference size because the ratio of interferer to signal of interest shrinks.

Conclusion

CSIR, combined with the DSSS and the adaptive nature of ATDMA within the iDirectGov Evolution Defense architecture, provides a robust mitigation capability, CSIR alone provides a significant level of protection against several interference/jamming scenarios. When applying CSIR to DSSS and Adaptive TDMA, a true anti-jam waveform can be established. The process to adapt MODCODS and spread factor is manually within the iDirectGov Evolution Defense architecture. This change is performed by the hub operator and no configuration changes need to be made at the remote end of the network. This reduces the complexity of change and does not cause any network outage. By making these changes on the fly network operators can configure their networks with the highest amount of spectral efficiency, and adapt to a more robust configuration during interference events. Both narrow band and wide band interferers can be mitigated, including high power, and wideband interferers when this implementation is used. In nearly all cases, BPSK with a spread factor of four is enough to overcome any interference event, but the iDirectGov Evolution Defense architecture also supports up to a spread factor of eight for even more protection. The exact interference or jamming event will determine the exact MODCOD/spread factor that will work and provide the best network efficiency.

About

iDirectGov, LLC, a U.S. corporation, delivers secure satellite-based voice, video and data applications with any time and anywhere connectivity in the air, at sea and on land. iDirectGov's advanced satellite IP solutions are used for critical ISR, airborne, maritime and COTM communications to support force protection, logistics, situational awareness, disaster recovery and emergency response. Building on more than 17 years of global satellite communications experience, iDirectGov provides the most bandwidth-efficient, scalable and highly secure platform to meet specialized applications of multiple federal, state and local government agencies, including the Department of Defense, domestically and abroad. iDirectGov has been a trusted partner of the U.S. government for more than 17 years. All its employees are U.S. citizens, with a third being U.S. military veterans.

iDirectGov's specialized technology includes transmission security (TRANSEC), Communication Signal Interference Removal (CSIR) and Open Antenna Modem Interface Protocol (OpenAMIP). All defense-grade products sold by iDirectGov are designed, developed, assembled, programmed, and verified in the United States.

iDirectGov is headquartered in Herndon, Va. For more information, please visit http://www.idirectgov.com.