New RFI Cancellation Technologies Attack Interference

By Bob Potter, Chief Technology Officer, SAT Corporation, A Kratos Company

Radio Frequency Interference (RFI) continues to be a significant problem that affects both satellite operators and end users alike. There is much coordinated effort to combat the issue on the part of operators and industry groups such as the Satellite Interference Reduction Group (sIRG) and the Global VSAT Forum (GVF).

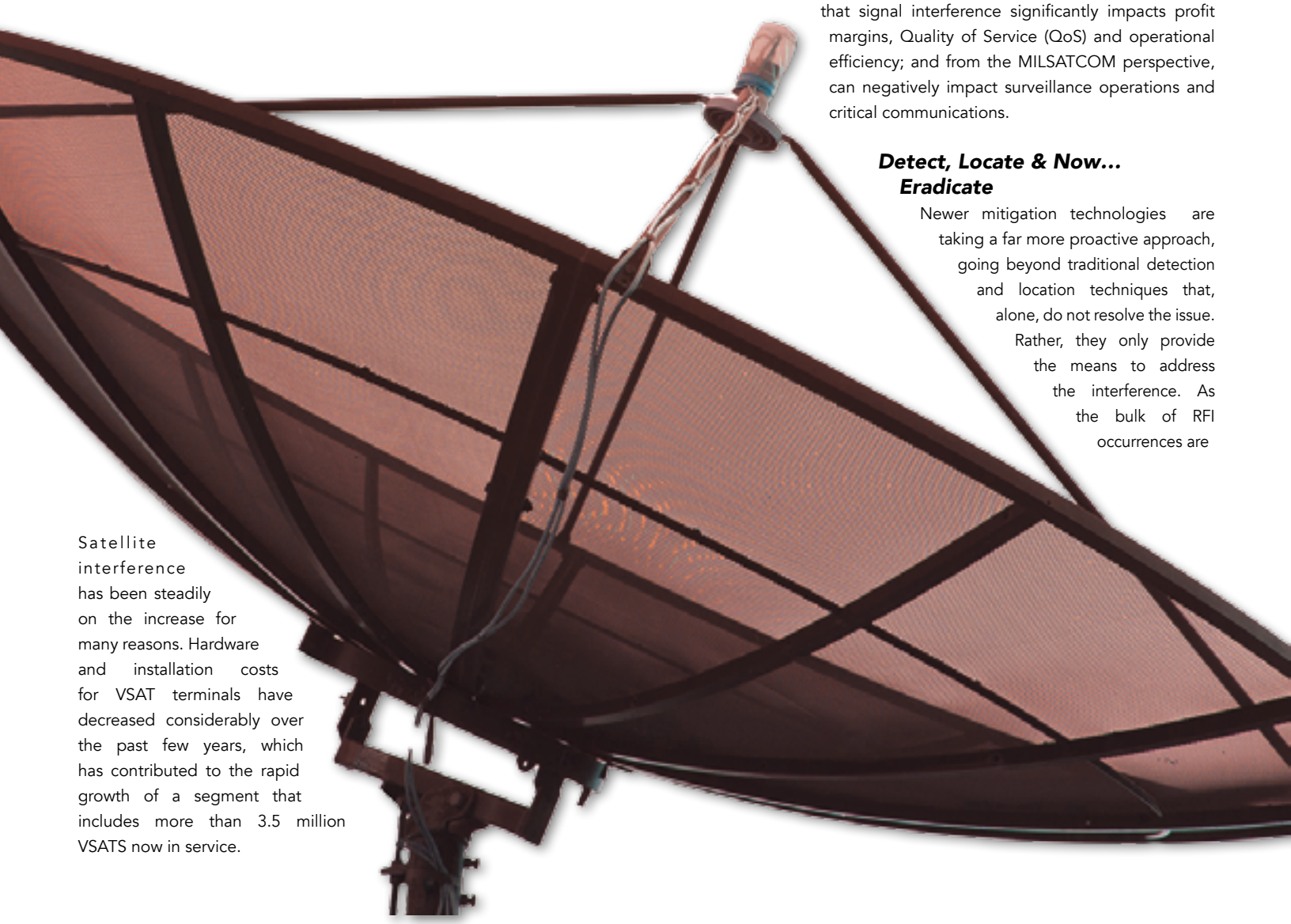
Approaches include Carrier Identification Codes (CID), advanced monitoring and geolocation technologies and more robust operational training. Moreover, there is a new generation of mitigation technologies arriving to market that are designed to aggressively identify interference and unilaterally neutralize it.

As the geostationary belt becomes more crowded, and as satellites are stationed closer together with smaller antennas that distribute RF signals over a broader area, the opportunity for interference continues to increase.

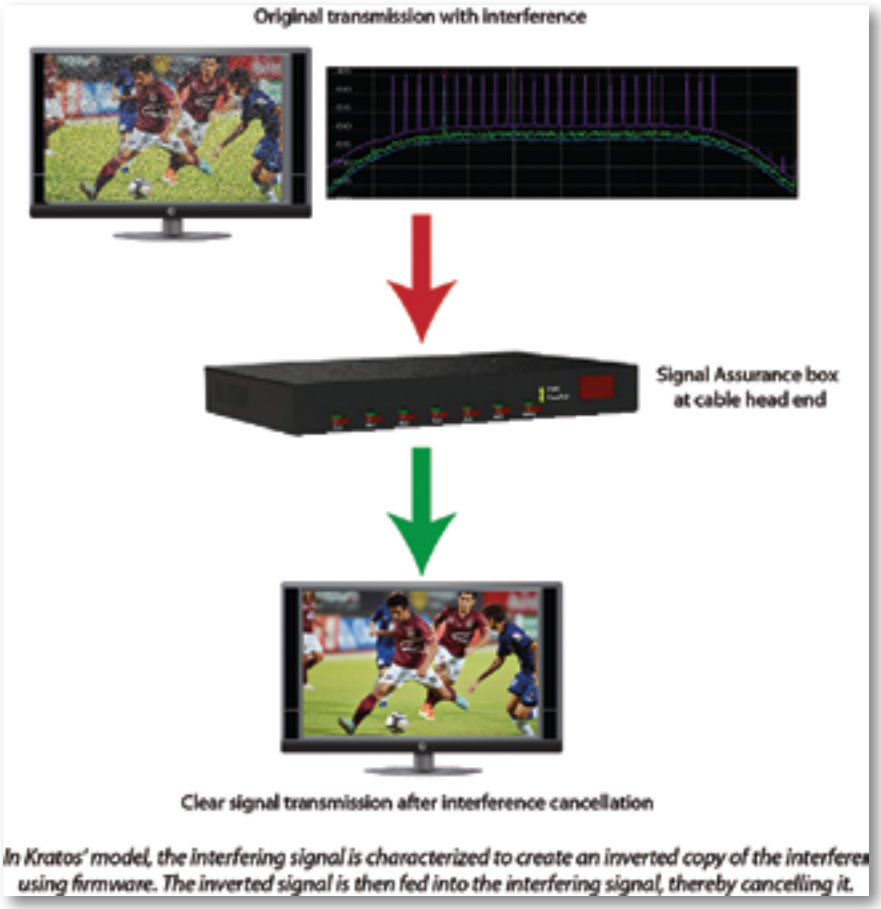
According to Martin Coleman, Executive Director, sIRG, VSAT systems cause approximately 40 percent of all interference and are responsible for 50 percent of downtime caused by interference. The scope of the problem continues to grow in line with demands for SATCOM bandwidth. For example, as military requirements continue to exceed MILSATCOM capacity and/or capabilities, military communications are increasingly placed onto commercial payloads, requiring newer, low-cost methods of providing resiliency to interference. Operators and industry groups report that signal interference significantly impacts profit margins, Quality of Service (QoS) and operational efficiency; and from the MILSATCOM perspective, can negatively impact surveillance operations and critical communications.

Detect, Locate & Now... Eradicate

Newer mitigation technologies are taking a far more proactive approach, going beyond traditional detection and location techniques that, alone, do not resolve the issue. Rather, they only provide the means to address the interference. As the bulk of RFI occurrences are



Satellite interference has been steadily on the increase for many reasons. Hardware and installation costs for VSAT terminals have decreased considerably over the past few years, which has contributed to the rapid growth of a segment that includes more than 3.5 million VSATS now in service.



In Kratos' model, the interfering signal is characterized to create an inverted copy of the interferer using firmware. The inverted signal is then fed into the interfering signal, thereby cancelling it.

accidental, this most often means contacting the interfering party to settle the issue. In some cases, where the interference stems from a remote site such as an oil rig, a considerable amount of time must be spent to assign someone to resolve the interference, resulting in lost revenue and extended outages. New approaches seek to independently eliminate interference through signal separation and/or signal cancellation and anti-jamming measures.

One trend is to move interference resolution directly into the satellite. Eutelsat, for example, recently announced plans to deploy an experimental TV channel interference mitigation function for the first time on their upcoming EUTELSAT 8 West B satellite. The satellite is scheduled for launch in 2015 and will be stationed over the Middle East and North Africa. Eutelsat's approach involves installing new-generation frequency converters behind the satellites receive antennas, enabling Eutelsat to change the frequency of an uplink signal without any impact on the downlink frequency received by user terminals.

In another example, a number of companies recently tested a U.S. Air Force-approved frequency hopping waveform that can be used as either a satellite-based networking hub or as a ground-based communications terminal. The anti-jam technology is based on a secure tactical waveform that is said to provide greater resistance to interference.

Kratos Tests Blind Separation To Separate + Cancel Interference

Kratos has demonstrated a different solution. Using Monics® carrier monitoring algorithms, the interfering signal is characterized to create an inverted copy of the interferer using firmware. The inverted signal is then fed into the interfering signal, thereby canceling it. Firmware, with its inherent reliability, as opposed to software, allows for installation in the communications chain to reduce any potential delay, or latency, in the communications signal. Only receive site equipment is required, inserted in line with the existing receive equipment. This approach includes the ability to protect any signal, including TDMA signals from CW/Sweepers or modulated SCPC/MCPC carriers.

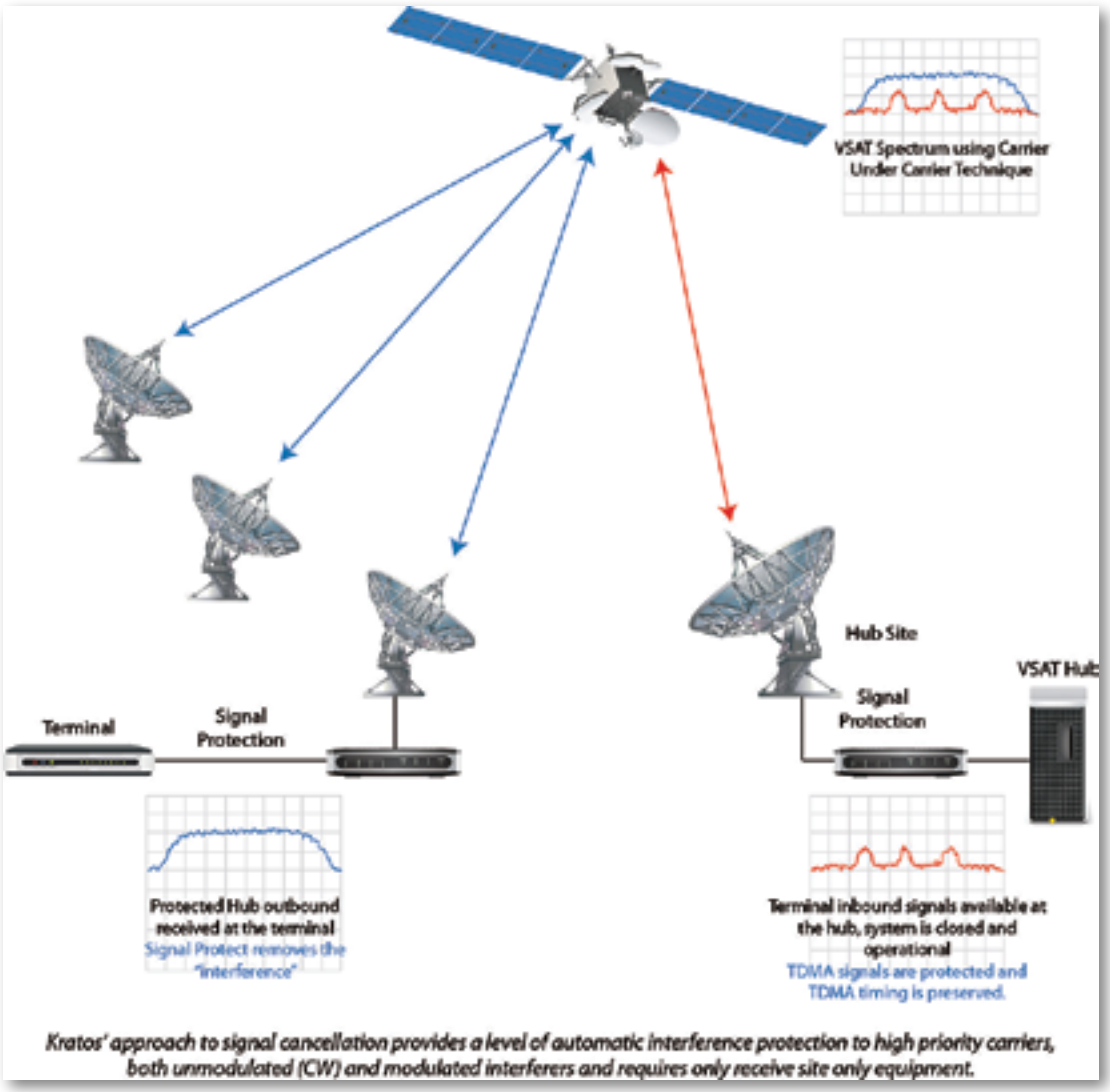
The protected spectrum could contain TDMA or hoppers, but with this approach, the timing remains unchanged on the protected waveforms. Tests indicate that it is easier to interfere with the TDMA narrow band signals than with large outbound signals. To keep the network up, Kratos has developed a system that can be inserted into a network—no reconfiguration or adjustment is required for additional timing delays. This configuration provides a high level of automatic interference protection to high priority carriers and works for modulated (SCPC) and unmodulated (CW and sweeping CW sweepers) causes of interference.

Unlike other approaches to signal cancellation, Kratos employs "blind separation" (the separation of signals without the aid of prior information about the interfering signal) to detect and isolate the interfering signal so that it can be safely canceled. When canceling a sweeping CW signal, the system can track and cancel signals with sweep rates up to 1MHz per second.

The system will provide greater than 25dB of cancellation and is currently the only solution to support all variations of multi-point to multi-point communication. The system can readily be established with the same basic information one would use to set-up a standard modem and can be easily managed and controlled with monitoring products such as Compass® and NeuralStar®. This provides customers with the ability to control the solution in the same way they can control the rest of the communications chain.

For service providers, satellite operators and teleport operators alike, the ability to quickly cancel interference without the cooperation of the interfering party will help assure QoS, interference-free communications as well as time-sensitive delivery of critical communications.

Evolving approaches such as these are exciting, but they are not alone. There are numerous, new enhancements to traditional approaches to neutralizing the effects of RFI. These include information sharing, and carrier monitoring, detecting and locating the source of the interference (geolocation) and operator training.



Kratos' approach to signal cancellation provides a level of automatic interference protection to high priority carriers, both unmodulated (CW) and modulated interferers and requires only receive site only equipment.

Increased Focus On Operational Training

Proper training is increasingly recognized as the first line of defense against interference; however, only if the training maintains pace with technology. There is growing agreement within the industry that improved training will reduce uplink errors and improve equipment maintenance and installation practices.

Three of the most practical and impactful areas for improving the human performance of RFI mitigation professionals include realistic training to better prepare operators for today's wide variety of RFI scenarios, workflows to create a unified view of the monitoring-to-mitigation problems, and user-friendly tools designed to match how operators think and accelerate response times.

Strengthening these three areas enables Level 1 operators to tackle interference challenges more efficiently and effectively, producing better resource and talent utilization internally and faster response times and customer service externally. To date, GVF and sIRG have trained well over 10,000 technicians through a global certification program.

The World Broadcasting Unions-International Satellite Operations Group (WBU-ISOG), a global organization of broadcasters, recently announced the formal adoption of a resolution that supports industry initiatives for training. Specifically, they have endorsed the GVF Satcom Professional certification program that is now offered to satellite news gathering (SNG) operators worldwide.

A combination of online and classroom-based training has been launched in the Middle East, Europe and North America, and plans are underway to begin delivery in every other region of the world.

New Approaches To RFI Location + Identification

The first step toward mitigating the disruptive effects of satellite interference is the rapid detection and analysis of an interfering signal through effective carrier monitoring. Once the interfering signal is identified and characterized, the source can be located by a number of geolocation systems on the market.

Modern geolocation systems, such as satID® from Kratos, offer next generation features and capabilities designed to save operator effort and, thereby, cost. Features such as scenario templates, higher levels of automation, improved reporting capabilities and integrated operator notebooks enable geolocation to be performed by more, less experienced operators. This improves operational efficiency and can also represent a significant financial savings to the organization.

Another method of identifying the source of an interfering signal is Carrier Identification (CID) codes. Under the auspices of sIRG, many satellite operators are embedding a unique CID code to a signal transmission. The code is embedded in a separate carrier onto the carrier(s) it is identifying. Operators can use Digital Spectrum Analyzers (DSA) to extract the CID, quickly identify the source of the interfering signal and then contact the interferer to resolve the interference issue.

A new approach adds a metacarrier, or subcarrier, containing a unique identity transmitted under the spectral density of the main carrier. This method adds no extra bandwidth or power and minimally affects the signal-to-noise ratio of the carrier as the CID signal is placed within the host carrier bandwidth and below the noise floor of the signal.

From a transmission standpoint, this generic solution is extremely effective and appeals to SCPC and FSS operators. The major issue with subcarrier CID resides in the receiver side. The operator must have accurate measurement tools to extract the CID from the interfering signal. Carrier monitoring and interference detection systems, such as Monics®, can extract the CID from the carrier with no new hardware required.

To facilitate the use of CID, a Satellite Operator Carrier ID dataBase (CIDB), a centralized data repository for all satellite operators to use at no charge to store and search for Unique Carrier IDs, is being developed by the Space Data Association. The database will enable rapid identification of an interference source and allow rapid interference mitigation among cooperating operators.

Accidental or Deliberate… RFI Is Still a Problem

RFI can be accidental (which accounts for anywhere from 95 to 98 percent of all interference)—or deliberate. Included in the former are human error, cross polarization leakage, equipment issues and adjacent satellite interference.

Examples of human error include transmitting on the wrong frequency, at the wrong time and incorrectly pointing the antenna, among other scenarios. Cross polarization interference falls into the accidental category as such might be caused by antenna misalignment, due to human error, or external forces such as high winds. Equipment issues can include faulty cabling, poor antenna specifications and potentially less reliable equipment due to the pressure to lower manufacturing and installation costs. Adjacent interference is becoming more prevalent as two-degree spacing between satellites in a geostationary arc becomes more common.

Deliberate RF attacks on satellites include piracy and jamming. Piracy, or unauthorized access, occurs when carriers (with content) are transmitted toward a satellite without any prior contract with the satellite operator. Intentional jamming can be the result of one party's objection to the content (political, cultural, social, etc.) of the targeted carrier and/or extenuating circumstances (political situation, social unrest, etc.)

The source of intentional jamming is generally locatable; however, this interference is almost impossible to remove without political intervention, and even then that may prove difficult. As such, efforts to combat it—such as signal cancellation—are a priority issue for all operators.

Playing Defense

Because of the steady growth of interference events in satellite communications, operators and end users have placed increased effort on finding ever better solutions to address this growing challenge. The best defense against interference, be it accidental or deliberate, is to command a portfolio of counter measures that include the latest in interference suppression technologies, such as Kratos' automated signal cancellation capability.

Bob Potter is the CTO of SAT Corporation, a Kratos Company and a leader in developing innovative systems, products and services for RF communication link interference mitigation. SAT is a premier supplier of such systems to the satellite industry. Bob's primary focus is on interference resolution techniques for spectrum efficiency and signal assurance. His experience in RF systems design and measurement techniques extends back more than 25 years. He is a leading member of sIRG with focus on carrier ID. Mr. Potter holds a B.Sc. with Honors degree in Electronic Engineering from Southampton University, U.K.