Commercial SATCOM Communications Protection: Commercial SATCOM Resilience to Jamming

Wiliam Hreha, Dave Grybos, and Rob Singh
Space Systems/Loral
Palo Alto, California
hrehaw@ssd.loral.com, grybosd@ssd.loral.com, singhr@ssd.loral.com

***Abstract*— Commercial satellite communications are occasionally targeted by jamming for political/ideological reasons or suffer the effects of accidental interference. Jamming is rare enough that it is generally considered a tolerable business risk. Traditionally the threat has not been preemptively mitigated with anti-jam technologies. Instead, instances of jamming are dealt with reactively. Specialized commercial services locate the jammer and negotiations are used to persuade the instigator to cease the jamming activity. Although commercial business decisions have not driven broad implementation of anti-jam technologies low risk features are available.**

The last decade has seen an evolution of a new suite of commercial satellite communication systems. Driven to maximize the service providers' return on investment the systems increase the number of subscribers served within the limited bandwidth resource for relatively small growth in capital expense. Key to the exponential gains in capacity are technology enhancements at all layers of the protocol stack. Although developed to optimize a business case these technologies provide features that inherently provide resilience to interference, increase link availability, and with reasonable modification may be enhanced further to increase the resilience to jamming.

This paper identifies features of modern commercial satellite systems relevant to assuring communications in a contested environment.

Keywords-satellite, Commercial SATCOM, wideband, jamming, interference

I. INTRODUCTION

Commercial satellite communications (COMSATCOM) markets include fixed satellite services (FSS), broadcast satellite services (BSS), and mobile satellite services (MSS). The FSS market provides full duplex communications between fixed terminals. Large global carriers with large fleets dominate this market. Their global reach enables a similar service to be obtained from multiple sources and orbital slots from a terminal located almost anywhere within +/- 50 degree latitude.

BSS services are one-way broadcast direct to users. The market is provided by regional carriers primarily delivering video and audio to fixed or mobile terminals. FSS services can be used to deliver broadcast services. Satellites designed specifically for the BSS market provide a higher effective isotropic radiated power (EIRP) than satellites designed for FSS markets. The higher EIRP provides a higher availability to smaller terminals than can be achieved over an FSS satellite.

MSS services provide full duplex multimedia services between mobile users and base stations. Services are provided by both global and regional carriers. Global carriers provide access to a terminal located anywhere on earth. The services are not compatible so a terminal cannot access service over another operator's system.

Since the late 1990s, as the global economy has become more dependent on broadband internet access, broadband satellite services have been moving away from FSS carriers and onto satellite systems designed to increase bandwidth per satellite and provide a more desirable consumer service. Currently provided by regional carriers, the service is rolling out globally. The systems have many inherent features that increase availability of the link in the presence of degraded links or interference.

The Department of Defense (DoD) uses COMSATCOM for over 75% of DoD communications. The DoD accesses these services by leasing capacity or contracting for managed services that lease capacity from commercial operators. The majority of the capacity is provided from global FSS carriers. Commercial satellites providing these services are designed exclusively for commercial consumer or business markets.

The business plans for COMSATCOM operators maximize profit by optimizing the revenue to expense ratio. Although COMSATCOM used for commercial service does experience interference from intentional and non-intentional sources the probability and consequence do not justify the expense of implementing mitigation techniques.

Military satellite communications (MILSATCOM) must provide reliable service in benign, contested, and highly threatened environments. The DoD's experience applying COMSATCOM has led to the perception that COMSATCOM can only be used in a benign environment. The future MILSATCOM requirements to provide broadband multimedia services over a single network, to provide higher throughput densities into areas of operation, to increase throughput to individual terminals, and to decrease terminal physical features will evolve MILSATCOM services toward COMSATCOM broadband services which, as mentioned above have some inherent interference avoidance features. Furthermore, the COMSATCOM industry can provide additional low risk

978-1-4673-0081-9/11/$26.00 ©2011 IEEE 2302

jamming-resilient features if economically motivated by the DoD.

This paper highlights jamming-resilient features of COMSATCOM broadband services and additional features that can be provided in FSS and Broadband services. DoD can access these features, which support communications in benign and contested environments by directly procuring satellite systems from the COMSATCOM industry or by compensating service providers for adding the features.

II. JAMMED COMSATCOM EXAMPLES

The COMSATCOM industry experiences both intentional and non-intentional interference. Non-intentional interference occurs most often when, due to operator error, a terminal is misconfigured in pointing, polarization, frequency, modulation, or power level. Occasionally interference is generated by a source providing a secondary service in the same frequency band. Using frequency analysis and spatial correlation techniques the source is located, the operator is contacted, and the configuration is corrected.

Intentional interference is usually motivated by political or ideological reasons and meant to interrupt information being provided to a region. The following are some examples of intentional COMSATCOM jamming. As with the non-intentional interference the source is identified and located. Diplomatic and ITU channels use threats of regulatory or diplomatic action to persuade the source to desist. The operators may succumb to the demands of the jamming entity by removing specific content.

A. *"U.N. tells Iran to end Eutelsat Satellite Jamming", Reuters, 3.26.2010*

"Iranian authorities have been jamming foreign satellite broadcasts into their territory since late last year, with broadcasters such as the BBC and Deutsche Welle affected. Access to the internet for Iranian citizens has also been affected."

"Iranian authorities have been clamping down on reformists since last year's June disputed presidential election returned hard-liner Mohmoud Ahmadinejad to power, sparking protests and clashes."

B. *"Cuba blows the whistle on Iranian jamming", Asia Times Online, 83.22.2003*

"The jamming related to Telstar-12, a commercial communications satellite orbiting at 15 degrees west, 22,000 miles above the Atlantic, which carries programs by the American government as well as by Iranian radio and television stations based in the US aimed at mainland Iran. The interference began on July 16, coinciding with the start of a new wave of pro-democracy protests led by Iranian students in Tehran against the country's clerical leaders."

C. *"Grounding Captain Midnight, TIME, 8.04.1986*

"The attack was swift and startling, the getaway apparently clean. Shortly after midnight one morning last April, a mysterious electronic intruder interrupted a movie on HBO with a transmission of his own. GOOD EVENING HBO FROM CAPTAIN MIDNIGHT, read the message on the screen. $12.95/MONTH? NO WAY! (SHOWTIME/MOVIE CHANNEL BEWARE!). The complaint was directed at cable services that scramble their satellite-beamed signals so owners of home dishes can see programs only by buying a decoder and paying a monthly fee."

D. *"Libya jamming exposed vulnerability", BBC, 1.13.2006*

"In September 2005, the London-based station began beaming into Libya via satellite. Almost immediately, it was jammed by the Libyan authorities - but in blocking that signal, several other broadcasters, amongst them CNN and BBC World, were also blocked out."

E. *"Banned Falun Gong Movement Jammed Chinese Satellite Signal", The Washington Post, 7.09.2009*

"Chinese officials said Falun Gong members began bombarding the satellite with illegal signals shortly after 7 p.m. on June 23, interrupting transmission of nine national channels and 10 provincial stations to rural areas without access to regular TV broadcasts. Television screens went blank for several minutes, then began playing a Falun Gong video with images of followers meditating in a stadium and then a plaza. Officials said the video was cut off after only 20 seconds, replaced by a blank screen again."

These examples provide evidence that jamming of COMSATCOM does exist but does not provide sufficient financial impact to justify the expense of implementing counter measures specifically for the COMSATCOM market. However these same vulnerabilities would have severe consequences to the warfighter leading to the perception that COMSATCOM is only applicable to totally benign environments.

III. BROADBAND SATCOM THREAT RESILIANCE FEATURES

Broadband SATCOM service is delivered over a satellite that provides multiple narrow, approximately 0.4 degree 3 dB beamwidth, beams. The narrow beams increase available bandwidth by frequency reuse between beams thus allowing more terminals to be served over each satellite. The high directivity of a narrow beam provides more EIRP and receive sensitivity. The higher EIRP and receive sensitivity translates into higher data rates for a fixed terminal size or the ability to serve smaller terminals. The connections are managed by a hub. The hub authenticates each user and dynamically assigns access frequency and time slots. The hub in cooperation with the terminal also provides real time radio resource control that adapts the terminal's power, modulation, coding, or access assignment in response to changing link conditions. To further enhance the user's multimedia experience the entire protocol stack has been optimized and performance enhancing proxies maximize the application's perceived performance. These enhancements are implemented in the terminals and the hub.

Several features of the broadband architecture developed specifically for commercial broadband service offer resilience to service threats.

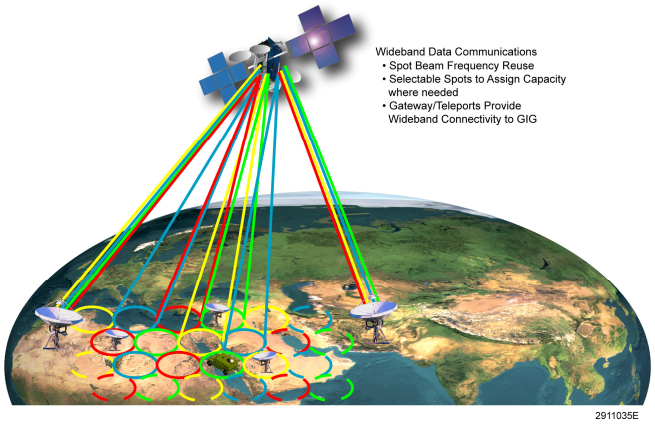

Figure 1. Broadband Operational View

A. *Link Threats*

1) Purposeful Interference of Communications Links: Multiple narrow spot beams offer resiliance to jamming from radiated emissions by decreasing the required standoff distance between the jammer and the affected area. This makes the operation of a jammer more difficult and less effective. Beyond a couple hundred kilometers (km) from the center of the beam the reception is greatly attenuated.

To generate capacity, broadband architectures have high frequency reuse. Although an emitter will be attenuated by the other co-frequency beams, location techniques can be applied across several co-frequency beams to identify and locate the emitter over a single satellite.

The hub-and-spoke architecture, with the hub outside of the region of operation, ensures that no unauthorized entity can use the infrastructure. With no accesses from an area of operation directly back to an area of operation without the regenerative processing in the hub, the service cannot be exploited by the adversary.

The hub controls the radio resources for all accesses with the objective to optimize the performance of each link while maximizing the total throughput of the system. In doing so, access assignments are made or adjusted in real time to respond to degradation in link quality. Should the signal to noise ratio of a link be degraded, the access would either be adjusted to a more robust modulation and error correction code or be assigned a different frequency. The radio resource control feature provides increased link availability and collects data that can be used for initial threat detection.

2) Purposeful Interference of Satellite Command Links: In order not to take frequency away from the area of operation, gateways are located outside of the region of operation. The gateways provide access control to the users and provide fiber access. On-station command and control of the satellite is also performed through at least two of the gateways. Locating the gateways at trusted locations outside the area of operation served by narrow beams increases the resilience to an adversary taking control or denying command service.

The satellite does have global beams for command operation in case of contingency where the narrow gateway beams might not be available. Control through these beams requires large fixed-location terminals that would be easy to locate.

3) Downlink Spoofing of Satellite Telemetry: While on station and when not in contingency, telemetry is available only through the narrow spot beams centered at trusted gateways outside the area of operation. Simultanous telemetry transmissions to multiple gateways allows the controller to correlate telemetry received at more than one gateway mittigating the risk that operators would take improper action based on false information.

4) Unintentional Interference: Broadband systems provide access by policies implemented in the hub. The autonomous assignment of access and control of power levels minimizes operator error. Errors that occur in planning spectral use and configuring the terminals is automated, eliminating manual configuration.

As mentioned above, the correlation of signals between the multiple co-frequency beams can be used to identify and locate the interferer should it not respond correctly to its access assignment. Since the access algorithms assign all accesses, the broadband system has the ability to disable a terminal as well. As one would imagine, this becomes useful when a consumer does not pay for service.

B. *Ground Physical Threats*

1) Takeover, Disruption, or Destruction of Key Facilities: In broadband systems the gateways are key facilities. In order not to use consumer capacity for the gateway functions the gateways are located outside of the area of operations. In commercial architectures these gateways are designed to be secure facilies with alarms, guards, and safety mechanisms. However they are designed for “lights out operation” with VPN access back to primary and backup Network Operation Centers (NOC). In areas of extensive rain attenuation, second gateways, referred to as diversity gateways, are installed in the same gateway beam but located at least 10 kilometers from the primary gateway. This also provides a resilience to a catastrophic event happening to the gateway. Several broadband satellites are being implemented with switch networks allowing beams within the area of operation to be routed to different gateways so that if the operation of a gateway is disrupted, high priority areas of operation can be served.

IV. Available COMSATCOM Threat Resilience Features

Commercial operator business plans are designed to maximize the revenue to cost ratio. The consumer market has not justified the expense of implementing capabilities needed solely for the purpose of mitigating intentional interference. However, technologies or enhancements to technologies can be implemented if the DoD so motivates the commercial operator.

If properly motivated, these features can be added to leased commercial services, hosted government-purposed payload systems, or commercially acquired dedicated government SATCOM systems.

FAR part 12 provides a definition for Non-Developmental Items (NDI) and Commercial Items. The definition of NDI focuses on previously developed items of supply used exclusively for governmental purposes while commercial items are any item of a type customarily used by the general public or by non-governmental entities. The features described here fall within these two definitions but do not require the development scope justifying a FAR part 15 acquisition. These features - government targeted commercial items - are items or combinations of items and/or processes that through minor modifications of the type customarily made in the commercial marketplace can satisfy the delivery and performance requirements of the Government solicitation.

A. Link Threats

1) Purposeful Interference of Communications Links: Space Systems/Loral has implemented independently steerable antennas at frequency bands from X to Ka. These independently steerable beams have narrow beamwidths decreasing the standoff distance between the emitter and the operating assets. The steerable beams can also be made to track an asset or be steered away from the emitter while still covering the operating asset.

Commercial satellites are protected from high-power uplink signals outside the designed receive bandwidth by providing significant rejection of the out-of-band signals prior to any active component.

Super-low-noise High-Electron Mobility Transistor (HEMT) circuits are vulnerable to high-power in-band uplink signals. The circuit designs can provide a damage level at least 30 dB (X Band and Ka bands) greater than the nominal fully loaded uplink level. Producing a signal of this strength requires a very large terminal. Space Systems/Loral has implemented input drive clipping protection at X and Ka bands. With proper design consideration the remainder of active units within the transponder chain is protected by designing the chain such that each component output saturates at a level below the overdrive limit of the next stage.

Without proper design consideration it may be possible for slightly out of band carrier signals to pass through the amplification chain without damage and thermally overload the high power output assemblies. Output assemblies are qualified to margins well above the nominal input levels and the thermal system is designed to dissipate a high thermal concentration in order to mitigate the vulnerability. In addition, limiters can be implemented before the high-power amplifiers insuring that the output assemblies do not experience excessive power.

If the EIRP of the intended uplink signal can be increased substantially, interference from a high-power jammer can be reduced by placing the affected transponder in limiting mode. If the resulting power of the intended signal at the transponder input is even a few dB above that of the interfering signal, the intended signal will repress the interfering signal by up to 6 dB.[6] Thus, a signal-to-interference ratio of 3 to 10 dB at the limiter input will be increased to 7 to 15.6 dB at the limiter output. However, the effectiveness of this mitigation strategy is reduced when more than one intended signal is input to the transponder. Space Systems/Loral has implemented channel limiters at X and Ka Band.

Reducing the transponder gain while increasing uplink power is an effective mitigation strategy against medium-power interference (i.e. when the interference power is too low to saturate the transponder). This technique improves the signal-to-interference ratio of the intended signal. With high power uplinked for the intended signals, transmission of a few intended signals at desired quality (end-to-end BER) is possible. High intended signal power at the satellite is required so that both of the following are true:

- The transponder input power offsets the lower transponder gain, resulting in an adequate satellite transmit power for closure of the downlink
- The ratio of interference power to intended-signal power remains within the range for which the spread-spectrum bandwidth ratio can provide adequate protection

Phased arrays are a technology on the verge of meeting the definition of government targeted commercial items. Depending on whether the array is receive or transmit and in which frequency band it operates, it may be implementable with minor modifications to previous commercial implementations. A phased array can be configured to spatially suppress an emitter.

RF direction-finding assets are usually deployed to quickly locate the source of covert users. Satellite systems deploying multiple beams on an area of operation enable detection over the single satellite. Detection can be further enhanced by implementing digital spectral analysis onboard the satellite, telemetering the sampled spectrum or analysis results to a ground station.

Within the hub and terminal, broadband systems have the ability to adapt each access in modulation and coding on a frame-by-frame basis. The algorithm can be altered in order to permute accesses in frequency on the same frame transitions. Frequency permutation provides resilience against narrow band interference.

2) Purposeful Interference of Satellite Command Links: COMSATCOM sends satellite commanding in the clear or using NSA-approved encryption. Security is provided by commanding the satellite using the Caribou command encryptor and knowing the vehicle command count. Government targeted commercial item solutions are available to provide DoD approved encryption of command and telemetry. Several non development alternatives can be implemented on commercial satellites to separate satellite control from payload control which may be desired when hosting a dedicated government payload. In this case the Government can securely configure the payload with limited

interaction with the satellite operator. The segregated secure commanding and telemetry can be provided such that the payload configuration is only available through in the area of operation or trusted gateway coverage.

Should a jammer disable one of the command channels, alternate channels through separate beams can be used. If the multiple channels are disabled, the satellite can autonomously operate for several days without ground commands.

3) Downlink Spoofing of Satellite Telemetry: As a standard practice, commercial satellites echo telecommands sent to the satellite to the ground in clear mode for verification before execution. Government directed commercial approaches can be employed to provide Type 1 encryption on the telemetry. With or without encryption, an available method for disguising the satellite configuration is to suppress sensitive status such as steerable antenna position. Without telemetry, the command and control concept of operations is altered. As an example a steerable antenna may return to a default location should the satellite not receive a validation command within a time-out period.

B. Ground Physical Threats

1) Takeover, Disruption, or Destruction of Key Facilities: Broadband gateways can be implemented in government trusted facilities providing increased security. Every gateway can be implemented with diversity facilities in order to protect against catastrophic events at one of the gateways. Implementing the satellite with steerable gateway beams enables the gateway to be transportable. A transportable gateway allows the gateway location to be altered or a replacement gateway can be inserted if catastrophic events occur. Network operation centers (NOCs) can be implemented in government secure facilities or in the Continental United States. The links between that NOC and the Gateway can securely use the government global information grid (GIG).

V. CONCLUSIONS

Satellites systems procured as government targeted commercial items offer resilience in contested environments and with the financial economies of scale the COMSATCOM industry can deliver.

A large portion of the MILSATCOM capacity is provided by satellites designed specifically for the commercial market. The economics of the commercial markets have historically not required robust implementation of threat-resilient technologies. In the last decade, economics have driven the broadband COMSATCOM market to implement satellite, terminal, and hub technologies that optimize link performance and bandwidth efficiency. These features inherently provide higher link availability, authenticated link access, and adaptation to interference. As MILSATCOM evolves toward Ka broadband architectures, the features incorporated from the broadband market will provide jam resilience in the contested environment.

The COMSATCOM industry produces highly reliable products on short schedules under affordable firm fixed price contracts. Space Systems/Loral is a significant contributor to evolving technologies that optimize the benefit to expense ratio of a SATCOM system. The COMSATCOM industry can produce commercially deployed and government-directed jam-resilient features that fall under the FAR part 12 commercial item definitions.

REFERENCES

[1] "U.N. tells Iran to end Eutelsat Satellite Jamming", Stephanie Nebehay, Reuters, 3.26.2010

[2] "Cuba blows the whistle on Iranian jamming", Safa Haeri, Asia Times Online, 8.22.2003.

[3] "Grounding Captain Midnight", Richard Zoglin;Jerome Cramer, TIME, 8.04.1986.

[4] "Libya jamming exposed vulnerability", BBC, 1.13.2006.

[5] "Banned Falun Gong Movement Jammed Chinese Satellite Signal", Phillip P. Pan, The Washington Post, 9.09.2002.

[6] J. J. Jones, "Hard-Limiting of Two Signals In Random Noise," IEEE Transactions on Information Theory, Vol. I T-9, Number 1, January 1963, pp. 34-42