Advanced Commercial Satellite Systems Technology for Protected Communications

Don Wilcoxson

ViaSat, Inc.
6155 El Camino Real
Carlsbad, CA 92009-1699
don.wilcoxson@viasat.com

Abstract—Currently, commercially developed products provide many critical capabilities for the U.S. and allied militaries and governments, and increasingly the line between military-specific developed technology and commercial technology is blurred. For example, the vast majority of broadband satellite modems now used by the military come from commercially developed products. While many have features that were derived from government/military requests, they were nevertheless developed on a commercial basis. Furthermore, many of these modems are primarily used on commercial satellites as well, albeit in uncontested environments. Even secure anti-jam (AJ) communications that were once seen as exclusively in the domain of military technology have recently been shown to be feasible with commercial modem technology to varying degrees, ranging from secure/no AJ to secure/AJ (e.g., Joint IP Modem/EBEM/LinkWay to the Protected Transponded SATCOM Pilot [PTSP] prototypes developed by PM DCATS). Likewise, recent advances in commercial satellite technology, and in particular high capacity satellite (HCS) technology, can have direct application to the protected communications problem for contested environments. These satellites and the systems designed to use these high capacity satellites, such as ViaSat's ViaSat-1 and Eutelsat's KA-SAT satellites, utilize very wide bandwidths, high power/narrow spotbeams and are designed to operate in high carrier-to-interference (C/I) environments – characteristics that have direct applicability for operation in a contested communications environment. Through the design of ViaSat-1 and with development under the PTSP program ViaSat has acquired a unique perspective of both the satellite and modem (ground/user) segments of the AJ problem and believes the best solution involves joint design of the ground, user and space segments as an end-to-end system solution. This paper describes elements of this approach and the potential benefits of a single enterprise system design methodology.

Keywords - protected communications; anti-jam; Ka-band; high-capacity satellites; spotbeams

I. INTRODUCTION

Almost since the first communications satellites were launched there were instances of jamming[1] and even recently there have been published concerns about the ability of even small nations to interfere with transmissions from commercial satellites [2]. This is of concern because a large portion, if not the majority, of today's military satellite communications are carried over commercial satellites. And while it may not be the ideal scenario for many, it is widely agreed that commercial satellites will be a part of the military communications infrastructure well into the future, especially in light of the cancellation of the transformational satellite system, a.k.a. TSAT (yet there's a good argument that even if TSAT wasn't cancelled commercial satellites would still have been needed in great numbers). Additionally, the sheer quantity of data that needs to traverse satellite links means that even important operational data (i.e., not just morale, welfare and recreation [MWR], medical or logistics data - just not name a few "counter" examples) will traverse commercial satellites. Therefore, it is widely agree that this data needs some level of "protection," which may mean just communications security (COMSEC) encryption, but it may also mean transmission security, a.k.a. TRANSEC (including bulk encryption and measures to prevent traffic flow analysis, for example), or even some level of low probability of intercept (LPI) or anti-jam (AJ) features normally associated with traditional protected systems such as MILSTAR 1 and 2 or Advanced EHF. This AJ level of protection is not at the level needed for a nuclear command and control (C2) scenario, but might be termed an "intermediate" level of protection, in some ways similar to that provided by systems operating in the past and today on DSCS and WGS with AJ modems such as the USC-28 or OM-55.

In this paper we focus on the broad(er) band communications as used on satellites operating at X-band and above (i.e. Ku, Ka, EHF), rather than those that operate a lower frequencies such as UHF or L-band, for example. Additionally, since "protected" can be defined [4] as protection against physical, nuclear, and electronic threats, in this paper we will only be concerned with *electronic* threats. Furthermore, we will leave discussion of interference detection and geolocation [2] for others, although this is clearly important operationally. In next few sections we will define some minimal requirements for what might be appropriate for "protected" communications, and discuss some of the mitigation techniques that might potentially be available, including those implemented or implementable with modem technology

[1] 1st instance of jamming may be as early as 1968 [1]

[2] for example through Operation Silent Sentry/Satellite Interference Reporting System, RAIDRS programs [3]

already available. Then we will discuss some of the design rationale/methodology for ViaSat's high-capacity satellite system illustrating how a single enterprise system design approach can yield big jumps in performance compared to that achieved previously. Lastly we discuss some examples of single enterprise system design thinking that exemplifies results not achievable within the framework of satellite or modem-only approaches. We don't claim to address all the issues or know all the answers, but rather we posit that there is value in our experience with ViaSat-1 from a paradigm-shifting point of view.

This intent of this paper is to set a framework to understand the problem of providing protected communications, and then give some information to stimulate the innovative discussions about how it may be possible to meet some of the requirements with commercial satellites, commercial satellite technology, and/or other satellite system technology.

II. "PROTECTED" COMMUNICATIONS

What constitutes "protected" communications is defined by many documents (for example, [7],[1],[4], and [5], among many) but is still interpreted in very different ways by many. For example, in the satellite communications context it may include physical protection, (for example, hardening against anti-satellite weaponry), or the ability to operate in a nuclear environment, (for example, using radiation hardened electronics to protect from damage due to electromagnetic pulse, aka EMP, or operation in a nuclear-scintillated atmosphere). In many cases, it just means protection against jamming, whether intentional/hostile or unintentional. Sometimes it also refers to encryption on the links or LPI/LPD/LPE for covertness and protection from eavesdropping. Other times it may refer to protection of the TT&C link controlling the satellite, or to the protecion in a network security context of authenticating users, or preventing unauthorized access ("hacking") into the system's ground or user segment through connections between the networks the system is connected to. In fact a good general defintion is given in [5] in that "protected systems have the ability to avoid, prevent, negate, or mitigate the degradation, disruption, denial, unauthroized access, or exploitation of commercial services by adveresaries or the environment."

For the purposes of this paper, however, we are limiting the scope to mitigation against electronic threats, including jamming, whether intentional, nuisance, or unintentional, and to a somewhat lesser extent detection and/or exploitation. With this in mind, it is possible to detail some minimum requirements (not necessarily a complete list) for providing a level of protected communications over satellite.

A. *Minimal requirements*

To list some minimal requirements it's helpful to consider that military SATCOM's main purpose/goal is to provide *assured communications to/from anywhere in the world, even in areas without communications infrastructure, in order to support the military mission*. For protected communications, you can then add that this has to be accomplished in the presence of hostile activity that would try to prevent such communications. So limiting it to electronic threats it boils down to providing:

- Robust communications in the presence of interference, both intentional and unintentional
- Secure communications, i.e. not allowing exploitation of traffic sent over the communications links by an enemy

So, what's minimally required to provide this secure, anti-jam capability?

- Satellite bandwidth, and lots of it
- Robust waveforms (modulation/coding/encryption)
- Geographic discrimination against threats
- Robust system/network control

Basically these can be categorized as requirements for *avoidance* and/or *robustness* against the threats. Knowing that these definitions of requirements drives any design approach, it's also key to understand that unlike MILSTAR and/or AEHF, this discussion centers on whether commercial satellite systems technology can meet a level of protection that might be sufficient for many different levels of users. That said, it would be reasonable to consider an approach similar to that taken by special operations forces that will typically pick the solution that's available immediately, but maybe only meets 80% of their ideal requirements. So what might 80% be in this trade space?

B. *Common techniques*

In order to understand how reasonable it would be to use commercial systems, it's helpful to consider some common techniques use for jamming mitigation[3]

- Narrow, focused spotbeams to/from satellite
- Hard-limiting satellite transponders
- Cross-strapped, cross-banded transponders
- Regenerative (demod/remod) satellite transponders
- Nulling and/or steerable antennas (adaptable to threats)
- Spread spectrum waveforms, including frequency hopping (FHSS) and direct sequence (DSSS) as well as combinations of the two
- Robust error correction demodulation and/or coding (many references, for example see [6])

[3] Note some techniques have been implemented more than others. Additionally, some modem techniques developed for PM-DCATS' Protected Transponded SATCOM Pilot (PTSP) Study can be found in [15] and [15] and were implemented in ViaSat's LinkWay$_{S2}$ modem design (modified).

- Transmission security, including bulk encryption and traffic flow analysis denial as well as feeding inputs like frequency-hopping patterns to the waveform generators
- TT&C encryption and access control
- Diversity transmission/reception, which may include transmission across multiple satellites, or multiple transmissions in/across frequency and/or time

This is not a complete list by any means, and depending on the system there may be other techniques that are needed. Just to give an example to illustrate this, consider a system that intends to adapt to the threat, providing higher throughput to users when no threat is detected and less throughput and more protection when a threat is detected. That system would need a robust detection method and any adaptation algorithm, especially if automated, would itself need to be robust against attack. In some cases, a mitigation technique might be to have a "man-in-the-loop" for example, who can adjust as necessary to the threat level in changing network and or satellite parameters.

III. Commercial Case Studies and Technologies

A. *Broadband System Design using the ViaSat-1 Satellite*

As a comparison point in how to design as a single system, consider the ViaSat-1 satellite, the associated SurfBeam®2 based ground system and the overall baseband ground gateway architecture. These were designed jointly in order to maximize a few (basic) key criteria, those criteria being:

- Provide broadband Internet access (predominantly)
- Provide user speeds sufficient for multi-media applications
- Focus capacity on areas where users have been proven to be
- Provide simple, inexpensive, easy to install user terminals

With the overall #1 criteria being →

- Maximize the overall system capacity divided by on-orbit cost, i.e. **bps/$$**

Note that this short list excludes some criteria that might, at first glance, seem very important. For example, there is no requirement directly on achieving a given data rate at all locations for a terminal (or terminal type) to access this system. That is, there is no requirement to provide a certain data rate to users who happen to be at the worst operating locations in the satellite footprint, rather just a requirement that the user speeds be sufficient to support multi-media operations. Also one will note there is no direct requirement on EIRP or G/T to be provided by the satellite, rather that is a result of the optimization of bps/$$ and to a lesser extent the other top-level criteria. There are other possible requirements that one might imagine could have been levied on the design as well, but by focusing on only the really important requirements, old paradigms of what would define what is achievable could be displaced. Notably, the highest capacity satellite systems designed before ViaSat-1 (for example, WildBlue-1 or Spaceway 3) only achieved ~ 10 Gbps overall capacity. By contrast the system designed around ViaSat-1 achieves an overall system capacity of ~140 Gbps. This big jump was possible in part by not levying any more top-level requirements than necessary or trying to make the system design accommodate too many corner-case uses.

Thus, the system design resulted in a transparent (bent-pipe) transponded architecture with extensive use of spotbeams and frequency reuse, including reuse of frequencies between gateways and user beams. Rather than a single gateway or the gateway not being part of the "system" at all, the design resulted in 20 gateways geographically distributed and, importantly, all sitting on or extremely near existing fiber access to the Internet. Furthermore, the waveforms were designed to optimize efficiency for variably sized IP packets (from the multi-media criteria) and the modem was designed jointly with the radio frequency (RF) equipment in the user terminals in order to allow the use of a simple, single cable, interfacility link (IFL) between the modem and the outdoor equipment (antenna/RF). And in direction relation to the #1 criteria, state-of-the-art development for satellite, gateway or other components are architectures were not required, rather maximum use of existing and proven technology was used to design this system, so it could be said this system is "advanced" not because new components or state-of-the-art technology was developed, but rather it was "advanced" in the manner in which it was architected.

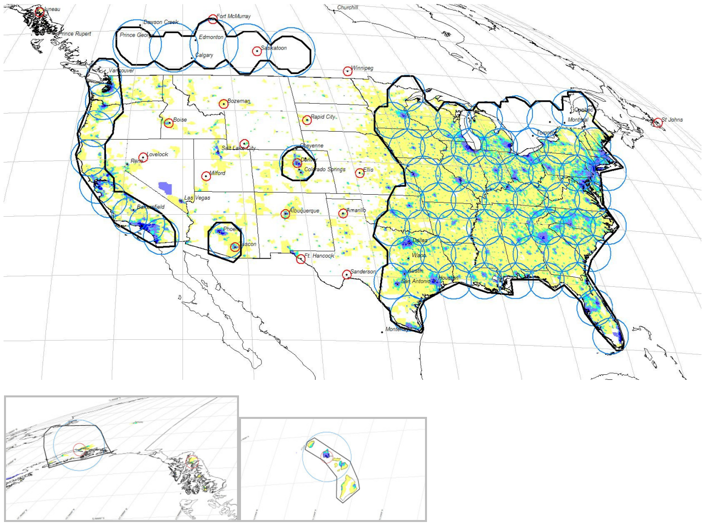

Figure 1: ViaSat-1 user and gateway beam lay down overlaid with population density

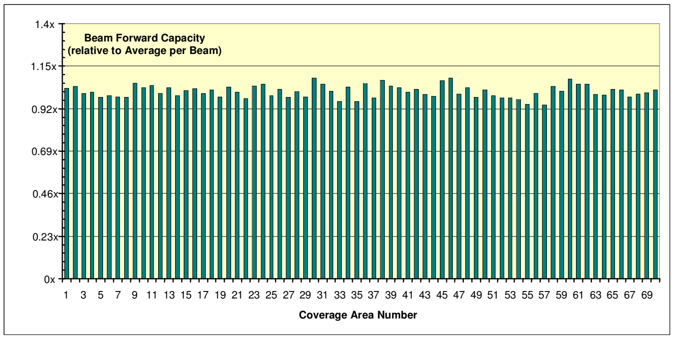

Figure 2: Predicted capacity per beam (forward link)

So, from these basic requirements the jointly designed space, ground and user segments resulted in a highly-optimized end-to-end system. Looking at the end design, one can see the effect of this joint design approach on a few characteristics (note the semantics, i.e. we say characteristics and not requirements) of the system:

- Very narrow spotbeams, resulting in very high performance (EIRP&G/T) and high frequency reuse
- Novel placement of gateway locations to further enhance frequency reuse (using cross-strapped transponders) and minimized cost to connect to internet (GW's placed on existing fiber). See Figure 1, GW's are geographically separated from user beams, generally in the western states.
- Not all beams have the same capacity (see Figure 2). Additionally, not all users can achieve the same data rates or at the same modulation and coding combinations (modcodes); *everything is adjusted to maximize overall capacity*
- Maximizing the available spectrum within the regulatory framework Either 500 MHz or 1 GHz in all beams; 1.5 GHz total used by system (see Figure 3 showing forward link plan, similar plan for return link)

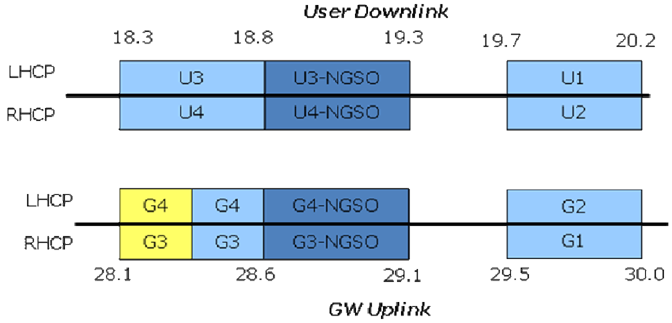

Figure 3: ViaSat-1 frequency plan (forward link)

- Polarization and frequency reuse resulting in a 4:1 "color" pattern
- Simple, hub-spoke, bent-pipe architecture (no individually new technology, just novel combination of existing technologies in satellite design)
- Ground coverage doesn't cover all the U.S., only areas with proven demand (from WildBlue service on WildBlue-1 satellite – see Figure 1)
- User antenna/RF connected to modem through a single IF cable, with Tx and Rx multiplexed on single cable.
- Single-hop mesh is not supported (although double-hop mesh connectivity is)

Furthermore, even though the system was not designed to operate in a jamming environment there should are some obvious advantages even as it is currently designed. Namely, the large bandwidths, very narrow spotbeams and geographically separated gateway locations. Just to illustrate a simple scenario, imagine a user located in one of the spotbeams. In order to jam that user, the threat would also have to be in that (very small, ~0.4° diameter) spotbeam, and then could only jam the uplink from the terminal. In order to jam the downlink into that terminal, the user would have to locate in the vicinity of the appropriate gateway site. In order to affect a large number of terminals across several spotbeams, many jammers would be needed. Moreover, with a modem designed to operate in the presence of jamming threats, the large bandwidth used by the system would make it likely the jammer would have to spread his energy over at least a substantial portion of the large (500 to 1000 MHz) bandwidth the modem could operate over (see the next section).

B. COTS modem capabiliities

From a modem standpoint the definition of "protection" can take on many different definitions depending on the user and the environment the modem will operate in. For example, the MD-1377 Joint IP Modem [12] and LinkWay$^{®}_{S2}$ [13] are two examples of *commercial* modems that have implemented transmission security (TRANSEC) as defined by the U.S. Government with direction from the National Security Agency. This TRANSEC ability prevents adversaries from gleaning useful information from the observation of transmissions using these modem systems, and thus users are "protected" from exploitation. Additionally these systems are also "hardened" in an information assurance sense on their baseband connections to the terrestrial networks they connect to in order to defend against "hacking" or other cyber-attacks. Furthermore, there are other modem systems that have been designed to operate with low probability of intercept or detection (LPI/LPD), which also provides levels of protection, although for somewhat obvious reasons commercial systems do not typically have this requirement.

Further levels of protection include such features as robust operation in the presence of inadvertent/unintentional or even intentional interference or "jamming." In some cases this happens even in commercial environments, such as that encountered in the ViaSat-1 systems employing the SurfBeam2 modem. As described in the previous section, the ViaSat-1 system involves using frequency reuse across a large number of spotbeams, thus co-channel interference (i.e., interference from transmissions at the same frequency in another spot beam as seen in the spot beam of interest) can be significant. In fact, if a spotbeam satellite system is optimized correctly it will turn out to be interference limited rather than limited by power or bandwidth[4]. Thus, ViaSat's SurfBeam2 network system (not just the modem, but including the configuration of the satellite and network operating parameters) has been designed to operate in this C/I dominated environment.

In other cases, the environment is not self-induced interference (as above), but rather unintentional interference from friendly or non-enemy systems or even intentional interference (i.e., jamming) from hostile systems. The recent effort by PM-DCATS (PTSP see ref [14], [15] for details on results of the prototyping study) has shown that for these environments some commercial MF-TDMA modems have inherent capabilities that could enable anti-jam modes of operation to provide useful levels of protection on commercial or commercial-like (e.g., DSCS, WGS) satellites. The inherent capability of these modems to be able to frequency-hop at rates up to 6000 hops/sec and hop over large bandwidths (over 1 GHz) are obviously applicable to the requirements listed in section II. Additionally, the software reprogrammability and high amount of network configurability of such modem systems as the LinkWay$_{S2}$ used in the PTSP study or of modems such as the JIPM also lend themselves to their use in contested environments where they could be optimized to operate in the presence of certain threats. Although discussion of the details of the mitigation techniques are beyond the scope or intent of this paper, a representative translation/permutation of a commercial MF-TDMA burst time plan to a anti-jam mitigated burst time plan is shown in Figure 4.

But, relying solely on anti-jam features embedded in the modem system would likely be suboptimal compared to an end-to-end design concept where satellite, ground and user segments are all jointly designed to address an electronic jamming threat.

IV. A SINGLE SYSTEM DESIGN PARADIGM

From section II a single system design based on a limited number of key criteria was exemplified. A similar single system design approach can be taken to provide a level of protection to military satellite communications, and likewise commercial technology could likely be used to provide this service. To do so and potentially achieve results that provide significant protection, the number of key criteria to be optimized for must be kept as low as possible. Doing so will allow the system designer to use satellite, ground or user segment "knobs" to achieve an end-to-end performance that meets the user requirement.

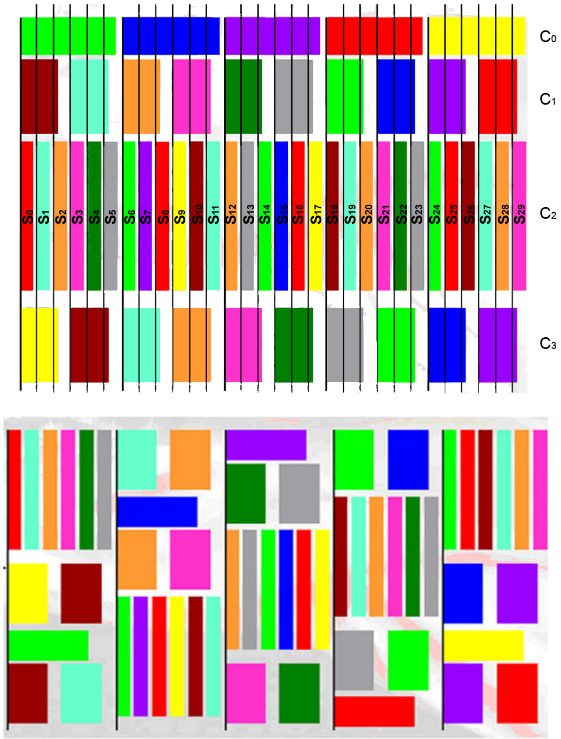

Figure 4: Example Burst Time Plan Permutation useful for jamming mitigation implementable on a commercial MF-TDMA modem (top:unmitigated; bottom: mitigated)

And even then, the designer should make sure they aren't unintentionally limiting the design space to work within. For example, in some cases there are anti-jam mitigations approaches that can't be considered properly without thinking about more than just the satellite or the modem or even their combination in conventional ways. For example in [7] and [8], an approach is described whereby the anti-jam mitigation is provided by using a satellite at a low elevation angle to the user, where the potential jammers or jamming locations are not within line-of-sight of the satellite being used (i.e., they are below the horizon). While the limitations of this approach are noted in these studies, you could extend this concept further if you consider multiple satellites being used. For example, "what if" there were many satellites to choose from, and then there was a high probability that such a satellite at the right elevation angle could be chosen from. This is clearly beyond just a satellite design issue.

Or, consider another case where multiple satellites are used to provide diversity paths for signals to/from a user terminal. Extending this even further, what if those satellites were not in geostationary orbit? With a minimal set of key criteria specified up front, scenarios like this become valid to be explored and may potentially yield approaches that can achieve significant amounts of protection and may also be capable of being based on commercial technology. However, they may

[4] A similar result to that exhibited in terrestrial cellular systems

look far different than the current paradigm of MILSTAR or AEHF or even DSCS/WGS with an AJ modem, for example.

V. Summary

In this paper, essential requirements for protected satellite communications were discussed, along with common techniques designed to meet those requirements. An overview of the broadband system designed around the ViaSat-1 satellite was presented as an example of what can be achieved with a single system design methodology, and examples of COTS modem technologies that can provide varying types of protection and could be used within a system such as ViaSat-1 or other high capacity satellites were discussed. Lastly, several other anti-jam mitigation strategies resulting from a single system (i.e., not satellite or modem alone) design approach were presented. While we believe that the traits of ViaSat-1 and of the new generation of high capacity satellites (and their accompanying ground and user segments) being launched have the potential to provide significant electronic jamming protection to satellite communications, we also believe that more protection may be achieved with a purposeful design using that technology as a basis. Thus, the thoughts presented are intended to stimulate and hopefully alter the conventional thought process in the engineering, programmatic and policy-making communities, rather than to promote a specific idea or technology.

VI. References

[1] King, Mak and Riccio, Michael J., “ Military Satellite Communications: Then and Now,” *Crosslink*, Vol 11, No. 1, Spring 2010, pgs 40-47, Aerospace Corporation.

[2] Kenyon, Henry, “New space policy will take U.S. to infinity and beyond,” Feb 7, 2011, www.defensesystems.com/Articles/2011/02/07/US-National-Security-Space-Strategy.aspx

[3] 16th Space Control Squadran Factsheet, www.peterson.af.mil/library/factsheets/factsheet.asp?id=8403 .

[4] Martin, Donald H., “A History of U.S. Military Satellite Communications Systems,” *Crosslink*, Vol 3, No. 1, Winter 2001/2002, pgs 8-15, Aerospace Corporation.

[5] Bfers, Glen and Miller, Stephen B., “ Future U.S. Military Satellite Communications Systems,” *Crosslink*, Vol 3, No. 1, Winter 2001/2002, pgs 46-52, Aerospace Corporation.

[6] Phoel, Wayne G, “ Iterative Demodulation and Decoding for Protected Satellite Communications,” *Lincoln Laboratory Journal*, Vol 15, No 1, 2005, pgs 79-96, MIT Lincoln Laboratory.

[7] Bonds, T., et al, “Employing Commercial Satellite Communications: Wideband Investment Options for the Department of Defense,” Project Air Force, Rand Corporation, 2000.

[8] Cerasoli, Carmen and Dimarogonas, James, “Geographic-Based Satellite Anti-Jam Strategies,” Mitre Corporation Technical paper, Case # 10-2505, June 2010.

[9] Lee, Jong W. and Marshall, Veloris A., “Maximum Capacity Prediction and Anti-Jam Performance Analysis for Commercial Satellite Communication Systems,” *Proceedings of MILCOM 1994*, Vol 2., pgs. 506-510.

[10] Jocic, L.B., Hovanessian, S.A., Kreng, J.K., and Schultz, Lt. Col. M.D., “Adapting Commercial Satellites to Military Communication Needs,” *Proceedings of the 1996 Aerospace Applications Conference,* Vol 3., pgs 389-401.

[11] Murad, Ahsun H., Parikh, Manish R., Sandrin, William A., and Lo, Gerald J.P. Lo, “Transmission Modeling of Military and Commercial Satellite Systems,” *Proceedings of MILCOM 1997*, Vol. 1., pgs. 334-340.

[12] www.viasat.com/files/assets/web/datasheets/JIPM_datasheet_019.pdf

[13] www.viasat.com/files/assets/web/datasheets/LinkWay_S2_Datasheet_012_web.pdf

[14] Protected Transponded SATCOM Pilot Study (PTSP) System Implementation Design Report, ViaSat, Mar 27, 2008

[15] Protected Transponded SATCOM Pilot Study (PTSP) System Test Plan, Procedures and Report, ViaSat Doc. 1094882 (Rev. 003), Oct 2009.