Practical Aspects of Command and Control in the use of Commercial Satellite Communications for Military Operations

Hank Rausch
Intelsat General Corporation
Bethesda, MD 20817

Abstract— **A recent contract provides end-to-end satellite and terrestrial communications from US Navy ships to their regional communications stations. This effort required the creation of a worldwide command and control system to provision, control, monitor, and display the entire operation. Building this system required reverse-engineering older communications equipment and standing up a central provisioning database. It also required institutional and technical changes to transition from a paper-based, manual style of operations to a web-based, automatic and remote style. The lessons learned for this project may be of use for other integrators and military planners facing a similar task.**

Keywords-satellite; command and control; US Navy; commercial satellite commuications;reverse-engineering;bandwidth utilization

I. Introduction

A recent contract provides the US Navy with end to end satellite and terrestrial communications, from the ship to the communications station. This project subsumed and replaced a more limited effort, where the Navy leased satellite bandwidth, but provided the terrestrial links with its own resources, and retained overall command and control (C&C) of the terrestrial path. Creating a new control network that effectively integrates a solely commercial control infrastructure with a military communications protocol presented significant technical and organizational challenges. The problems encountered and their resolution will be of use to future planners and integrators. Trends are that integration of commercial and military command and control infrastructures will increase, as constricted budgets preclude the construction of purpose-built infrastructure for the sole use of the military. The problems faced, the way they were overcome, and the remaining issues that were not overcome, are instructive and vital to future military and commercial network integration efforts.

In ascending order from lower-level equipment issues to questions of higher order integration with Navy planners, the factors addressed in this effort can be summarized as follows:

A. *Control of Legacy Communications Equipment*

Prior to the integration, equipment was controlled and monitored locally. Much of the equipment dated from the 1980s and 1990s. Logs were taken much the same steam plants were monitored in the 1840's, by an operator manually writing down values onto a clipboard. Documentation and control software for this equipment was sorely lacking or nonexistent. In order to provide an integrated, world-wide, real-time view of state and control, it was necessary to reverse engineer communication protocols and create custom software to control and monitor this equipment.

B. *Efficient Use of Leased Bandwidth*

The Navy's goal is to maximize use of its leased bandwidth. Dynamic allocation schemes are currently not possible due to the equipment fielded on the Navy's ships, which support only serial-based Single Channel Per Carrier (SCPC) duplex links. Thus, efficient use of the leased transponder space involves assigning ships (missions) to pre-arranged carriers "slots". Optimization of use requires keeping these slots assigned to missions, and periodically changing the allocation to make best use of the available bandwidth.

To accomplish this, an information system had to be created to display current and historical utilization of these resources. This system draws current state information—transponder power, data through the circuits—to provide a real-time and historical utilization metric.

C. *Coordination and Control of Resources*

Providing a worldwide communications capability to hundreds of ships requires marshaling thousands of discrete components—satellites, transponders, antennas, RF transmit and receive equipment, terrestrial links, and baseband equipment. Maintaining configuration control of this array required a complex information infrastructure comprised of databases and servers. This equipment presented the information and control links to authorized government and contractor users—mission planners, unit commanders, control technicians, and contractor managers.

D. *Information Security*

Any information system providing service to military units requires a degree of information assurance higher than that normally required by purely commercial information systems. Previously, military planners had the luxury of budgets that allowed construction of purpose-built systems where information was able to be retained within a single protected enclave. This is not possible for systems that rely upon co-use of commercial assets. This is particularly true for satellite systems which involve RF transmissions. Because of the physics involved, these communications are (and will always be) in the public domain. The command and control system therefore required protection mechanisms to prevent inadvertent disclosure of sensitive information. This protection was made slightly easier by the Navy's choice of SCPC in lieu of an Internet Protocol (IP) based multiple access protocol. SCPC communications involves transmitting two signals, or carriers, continuously, regardless of how much communications traffic is actually being sent. Consequently it is inherently less prone to traffic analysis type of exploits than access protocols where transmission signal varies with traffic.

The solution involved nesting of subsystems which allowed commercial data to flow into a protected subsystem where it could be aggregated with operational data available only to authorized users.

E. Universal State Picture

The end result of the effort was the creation of a worldwide command and control network that aggregates the information and control links across hundreds of platforms. It presents a real-time picture of the entire state of the Navy's commercial satellite communications showing current and archived status of Navy missions.

II. COMMAND AND CONTROL

The creation of this command and control system is indispensable to the Navy's use of commercial satellite resources. Based on the extensive demand for communications capacity and the cost of launching and operating dedicated assets, the use of COMSATCOM for the military is likely to become institutionalized as way of life for the military. Estimates of the ratio of COMSATCOM use as a percentage of total military SATCOM are as high as 80 to 90%. The total government/military commercial satellite market is projected to grow from $700 million in 2008 to $ 2 billion in 2015 [1]. This effort represents a vital and useful case study for others involved in military co-use of commercial information systems. Following are details of its design, implementation, and lessons learned.

A. Control of Legacy Communications Equipment

The scope of the integration effort initially included 4 teleports strategically situated around the world. This provided worldwide access to approximately a dozen satellites offering C, Ku, and X-band coverage. Signals from each ship are downlinked at a teleport using a modem compatible to the shipboard modem. The baseband signals of all modems are multiplexed onto a high rate bearer—DS-3 or OC-3—and sent to the appropriate Navy communication terminus—in Hawaii for the Pacific and West Coast teleports, and in Norfolk, VA for the East Coast and European teleports. Each teleport was fitted with 12- to 24 satellite modems for this purpose. Previously these modems were manually controlled and manually patched to the multiplexer equipment by teleport personnel. For this contract, software was developed to remotely control and monitor the equipment from a central coordination station. Some of equipment was quite old and poorly documented and required a bit of forensic sleuthing to discover the communication protocols necessary for remote control.

Shipboard communications equipment modernization tends to lag behind terrestrial equivalents, owing to the additional planning, engineering, and expense involved with shipboard installation. Consequently, it not uncommon to find old(er) equipment still in use onboard US Navy ships and submarines. In the case of this project, three types of satellite modems are in use today all of varying vintages: 1980s, 1990s and 2000s. The level of difficultly of integration of these modems into the C&C infrastructure was proportional to their age. The newest type of modem has a well-defined Simple Network Management Protocol (SNMP) command structure, and is controlled via a standard web browser. Remote control and monitoring of receive parameters are accomplished easily, by compiling the vendor's Management Information Base (MIB) into a standard SNMP manager.

The modem that dated from the 1990's was a bit harder to integrate. It was controlled via a Java-based application. Remote control across was accomplished initially by operating the Java-based control application across a communications link from the operations center. However, the MIB that had been supplied by the vendor did not return values correctly, so a new system had to be devised for monitoring. Additionally, a backup control utility had to be developed in the event that the Java-based application failed to work. This was done by capturing and decoding the IP communications between an operating modem and the Java-based application. The modem has both an IP/Ethernet control port as well as an RS-232/485 serial control port. Fortunately, the modem used identical command syntax for both IP-and serial control, so with the results of this decoding effort it was possible to construct an application which communicated via the serial port. This application served as the primary monitoring interface and backup control mechanism.

The oldest modem—dating from the 1980's—posed the biggest challenge. The unit had no local control interface. It had been controlled by an application which was only usable locally. An application had to be built which provided remote control from the operations center. It was possible to determine the command control syntax and passwords that the local application used by capturing the IP traffic between it and the modem on the LAN. This information was used to construct a new application that would monitor and control the modem across the WAN from the operations center.

In the case of both of that two older modems, a bit of reverse-engineering and coding skill were invaluable in creating a remote monitor and control capability for equipment that was not originally designed to support this mode of operations. Without this remote control and monitoring ability, remote operations would have been impossible.

B. Efficient Use of Leased Bandwidth

As of this writing the system supports communications across 14 transponders on 12 different satellites comprising a total of 581 MHz of leased bandwidth. This 581 MHz is divided into 71 full-duplex carrier “pairs” or “slots” capable of supporting SCPC full-duplex (FDX) communications between a single ship and a communication station at rates varying from 256 kbps to 4096 kbps. This bandwidth provides communications for approximately 150 ships. Ships are assigned these slots based on operational necessity. At any given time, roughly 30-45 ships are “on mission” and have slots assigned to them. The process of assigning a communications slot is not instantaneous, it takes approximately 24 hours to schedule the assignment, draft a message to the ship with transmission parameters, create the terrestrial backhaul, and then establish the entire end to end link. This “transaction cost” is one of the reasons that leased bandwidth is not completely used. For the period September 2010 to Feb 2011, utilization on a per-transponder basis varied from 30% to 60%. This ratio compares favorably with the military’s use of its own satellite resources, which is approximately the same [2]. Another problem complicating efficient use of the bandwidth is that utilization is not readily visible. Prior to implementation of the C&C system, it had to be calculated manually using the paper trail of assignment messages.

The command and control system built for this contract addressed both the transaction cost and utilization view problem. It did this by automating the assignment process and by providing a system wide view of transponder utilization, both real time and historical. Instead of drafting a message to assign slots, the mission planner logs into a web site where all current and future slot assignments are visible. He can assign a unit to a slot directly on the web site, connected in real time to a MY SQL database. A routine was written on the database which checks for double-assignment of resources. Satellite and terrestrial link controllers receive this request via the web site. On the same site, they assign a modem and terrestrial link and activate the mission when scheduled. ’Double assignment’ of these resources is also prevented by the database. Activation of a mission automatically starts the clock running for calculation of transponder utilization. Transponder parameters are stored in the same MY SQL database. Previously, assignment and scheduling was done by emailing assignment messages, and calculation of utilization was a manpower intensive process involving spreadsheets. Simple spreadsheets and word documents were used to keep track of assigned resources.

Creation of a web-based tool that allows universal visibility into the assignment and utilization process unquestionably reduces transaction costs and increases visibility—it is an open question, however, whether this effort results in higher utilization and more efficient use of the transponders. Once the system has been allowed to run for a while, a comparison of transponder utilization pre-and post-implementation will answer this question.

C. Coordination and Control of Resources

The number of sites, components, and configuration parameters involved in Navy use of commercial satellite communications is large: 150 ships, 7 teleports, 16 antennas, 108 modems, 408 terrestrial communications ports, and roughly 70 configuration parameters for each of these components. For contractual and SLA compliance purposes, operating parameters of an activated circuit are logged every 5 minutes—Receive Eb/No, carrier power, data rate though the terrestrial link. This amounts to 7200 archived values per day. Prior to implementation of the C&C system, tracking of these resources, control, and monitoring was all done manually. Modems were configured locally at the teleport, and readings were logged manually once an hour, from the local screen. Configuration parameters were maintained locally. Spreadsheets of satellite transmission parameters~~,~~ and assignment of ships to satellites and modems were maintained locally and emailed for distribution. Assignment of a terrestrial port to a modem was maintained by a different organization~~,~~ on a separate spreadsheet. Keeping track of and distributing these different spreadsheets was done by email. The C&C system that replaced these was a central database accessed via web server. This database contains all configuration, assignment, and archived monitoring parameters. In addition to display, it also serves a control function: A request for resources is made on the website itself~~,~~ and this request is available instantly to all parties with access. Periodically the transmission plan parameters for a given satellite are updated, and these are also posted in real time to the web server. When a mission is activated and the ship begins transmitting, the web server collects receive parameters in real time, stores them in a database, and makes them available for all to see.

This centralization of command and display has reduced the time to provision a mission and increased the reliability and volume of archived SLA parameters. In contrast to satellite bandwidth utilization however, it is difficult to quantify its effect in terms of man-hours saved. From a qualitative standpoint, however, it has streamlined and improved operations.

D. Information Security

Commercial satellite communications occur in the public domain. Transmissions can be monitored from any point within the downlink footprint of the transponder. The modulation and error coding can be determined, and from there it is a simple step to demodulate the signal and, if the signal is unencrypted, read the contents of the transmission. For this contract, the security of the contents of the baseband signal are encrypted, but some information about unit operations can still be gleaned from the pattern of transmissions themselves. To limit the amount of information that can be garnered, it is important to decouple unit data—for example, which specific ship is transmitting and its position—from transmission information. The fact that carriers of a certain data rate are transmitted on a commercial transponder does convey some information, but the fact that these carriers are associated with US Naval operations, that these carriers are transmitted from specific warships, and that these ships are located in specific regions of the globe, conveys much more. If the information system is designed properly, this can be safeguarded. Complicating the information security task, many satellite providers and uplink/downlink sites are non-US entities, and the amount of operational data shared with them must be limited.

In terms of information security, the C&C system for this contract represents a significant improvement over the previous contract. Because all transmission/reception operations had to be conducted locally, operational data including the start/stop time and broad area of operations for a given unit had to be shared with the uplink/downlink station (teleport). A modicum of obfuscation was provide by the use of code words that substitute for the actual unit name, but the measure of security they provided is questionable as many of them were blatantly mnemonic and easily associated with the related actual unit name.

The system built for the new contract retains all operational information at a central secure operations center. Because the transmission and reception equipment can now be controlled and configured remotely, local operators at the teleport have much less visibility into operations. A second level of decoupling of unit and satellite transmission data is provided because Navy controllers can retain sensitive information at their headquarters (HQ), and use this information to input commands to the commercial operations center directly via the secure web server. Web server communications are protected by commercial encryption. Previously this information had to be sent to the teleports via unsecured email and phone conversations. A final level of protection exists because the system completely obviates the need to transmit some extremely sensitive information. Satellite communications are degraded twice a year by so called 'sun outages', which occur at or near the equinoxes. This occurs when the receiving site, the satellite, and the sun are in alignment, usually for a few minutes, for several days around the equinox. The actual time of the outage depends on the geographic position of the receiving site. Calculation of the time of occurrence is useful for the prediction of communications outages, as well as for mission planning. It does, however, require the exact position of the ship, which is oftentimes extremely sensitive information. Once the outage times are calculated, these times are also treated as sensitive information, when associated with the unit. The reason is that these times can be 'reverse calculated' to determine the original latitude/longitude used in the calculation. The C&C system used for this contract provides a sun outage calculator on the server itself. Hence, Navy planners are able to perform their own calculations within their own protected enclave and need not transmit position data or sun outage information to a commercial provider at all. This eliminates the need to email sensitive unit information. The results of all these measures is that all operational data is retained within either Navy facilities or a tightly controlled secure operations center, and the information security posture is as tight as possible, given that the actual transmissions are accessible to anyone with a receiver.

III. UNIVERSAL STATE PICTURE

Prior to the new contract, commercial satellite communications for the US Navy were a manually intensive process characterized by local teleport operations involving intensive emailing of configuration and operational data. System monitoring was spotty or non-existent. There was no archived performance data and no centralized database. There was no way to remotely control satellite equipment. For system users and stakeholders, there was no visibility into the status of a service request or performance of a current mission. To comply with the new contract, a worldwide command and control system had to be built which controls the entire satellite and terrestrial path, and displays and archives performance data. It also had to provide a command mechanism for all users to request services and view the real time status of those requests and services. With the system, operators can receive a request, allocate resources, and activate a mission via remote control from a central, secure operations center. Its employment has resulted in streamlined operations, a stronger information security posture, and (potentially) more efficient utilization of leased bandwidth. Some of these benefits are qualitative and difficult to quantify. Others, like the potentially higher utilization of leased bandwidth, are easily quantifiable. An abiding question of this development is whether, and to what extent, this system increases transponder utilization. The C&C system has been implemented in stages. Full implementation is expected July 2011, 1 year after contract award. In July 2012, a year's worth of pre-system and post-system utilization will be available. The reader can expect a subsequent report on whether this system has actually improved utilization.

ACKNOWLEDGMENT

The author wishes to thank Dr. David Kelly, CAPT (USNR), ret. for his encouragement and assistance in writing this article.

REFERENCES

[1] Rich Tuttle, “SATCOM”, DEFENSE STANDARD 2009 Winter Edition Volume 8.

[2] Michael A. Taverna, Amy Butler, Frank Morning, Jr., “Operators Describe U.S. Satcom Problems”, Avation Week, March 11 2011”.