Bringing Space Capabilities to the Warfighter: Virtual Mission Operations Center (VMOC)

Brett P. Conner, Larry Dikeman, Victor Osweiler
Air Force Space Battlelab
730 Irwin Ave Ste 83, Schriever AFB, CO 80912; (719) 567-9950
brett.conner@schriever.af.mil, larry.dikeman@schriever.af.mil, victor.osweiler@schriever.af.mil

Steve Groves, Dale Schoenfelt
Army Space and Missile Defense Battle Lab
350 Vandenberg St, Peterson AFB, CO 80913; (719) 554-4201
steven.groves@smdc-cs.army.mil; dale.schoenfelt@smdc-cs.army.mil

Philip Paulsen, Will Ivancic
NASA Glenn Research Center
21000 Brookpark Rd, Cleveland, OH 44135; (216) 433-4000
phillip.e.paulsen@grc.nasa.gov; wivancic@grc.nasa.gov

Eric Miller and Jon Walke
General Dynamics
1515 Iceland Ave, Vandenberg AFB, CA 93437
eric.miller@gd-ais.com, jon.walke@gd-ais.com

ABSTRACT: The Virtual Mission Operations Center (VMOC) is a joint DoD and U.S. intergovernmental initiative to exploit Internet Protocol (IP) based systems in space or near-space, allowing any computer linked to the Internet to conduct dynamic tasking of payloads, interact with databases, and Tracking, Telemetry, and Control (TT&C) operations. The use of IP systems enables disadvantaged field users to access and task space capabilities. At the same time, it encourages common interfaces that lead to reconfigurable and standardized vehicle design for operationally responsive space missions. As such, IP can be an enabler for constellations of tactical small satellites.

In order to utilize IP and distributed tasking, one must consider issues such as security, prioritization, and contention control. This is the role of the VMOC. Each user must log on through a VMOC server that authenticates the user, validates the operations that user is authorized to perform, and verifies the prioritization level that user holds. Once these parameters are established the user makes a request. VMOC first searches its database for the requested information to prevent tasking an on-orbit asset. If the data is unavailable, the user's request is prioritized and executed according to the prioritization.

The Air Force Space Battlelab is the project manager of the VMOC demonstration team that includes Army Space and Missile Defense Command Battle Lab and NASA Glenn Research Center. The team will demonstrate the capability of VMOC via a Surrey Satellite Technologies

Limited (SSTL) micro-satellite. Using the Army Space Support Element Toolset, we will demonstrate that a field user can log into the Internet and perform various dynamic tasking operations on the satellite. The field portion of the demonstration is scheduled to begin in May 2004 and will be completed in June 2004.

INTRODUCTION

In 2002, NASA equipped the Neah Bay, a Coast Guard icebreaker from Cleveland, with a commercial Internet Router and encryption hardware originally designed for use on spacecraft.[1] The icebreaker was also outfitted with hardware to provide commercial wireless, cellular and satellite communication connectivity with the open Internet. Why would NASA do this to a Coast Guard icebreaker? It is because the similarity to the communication needs of an icebreaker at sea and that of a spacecraft are striking. While in port, the ship could connect to the Internet with a shore cable much like a spacecraft could connect via an umbilical cable during development, processing and launch vehicle integration. When the ship leaves port, the cable connection is broken and Internet connectivity is providing via RF systems either wireless or cellular within line of sight. Similarly, a satellite can communicate with a ground station during launch and whenever it is within sight of an RF antenna. Finally, beyond line of sight of the shore, the ship can be connected to the Internet via satellite communications (SATCOM). Likewise a spacecraft can communicate to another satellite when it is no longer in view of a ground station. The space shuttle does this through the TDRSS satellite constellation.

What was remarkable about the Neah Bay demonstration was that the process of moving from hardwire to wireless to SATCOM and back was performed securely and without manual reconfiguration. This is exactly what is required for a network that contains mobile assets such as ships, vehicles, aircraft and spacecraft, which is the very problem faced by the military.

Once a secure, mobile network architecture is established with space assets, the next question becomes, "How does one command and control these assets?" In order to do this, the following issues must be addressed: security, prioritization, and contention control. This should be automated and, where possible, managed machine-to-machine. This leads us to the potential of Virtual Mission Operations, where the Virtual Mission Operations Center (VMOC) would automate much of the role of the Satellite Operations Center and the Network Operations Center.

A demonstration of the military utility of this command and control architecture was performed in June 2004. The Air Force Space Battlelab was the project manager of the VMOC demonstration team that included Army Space and Missile Defense Command Battle Lab and NASA Glenn Research Center. The team demonstrated the capability of VMOC via a Cisco Systems mini router on a Surrey micro-satellite. Using the Army Space Support Element Toolset, field users logged into VMOC through the Internet and performed various dynamic tasking operations on the satellite.

VIRTUAL MISSION OPERATIONS

Net centricity and space capabilities

Space capabilities have transformed the battlespace of the 21st century. Military users depend on the global perspective and the persistence of space assets to yield capabilities such as communications, navigation, intelligence, surveillance and reconnaissance.[2] At the same time, information itself has become a critical component to military operations due to advances in communication technologies. It has been shown in combat and in training that networked forces outperformed those that are not networked.[3] This enhanced capability is called Net-Centric Warfare (NCW). NCW is "an information superiority-enabled concept of operations" that describes the way U.S. forces operate in the information age. NCW is effective through the networking of sensors, decision makers, and warfighters characterized by "shared awareness, increased speed of command, high tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization." Decision-making becomes rapid and effective as a result.[4]

In this networked environment, space technologies can now be exploited as long as information gained from space assets is made available in a secure and timely manner to field users. At the same time, field users should not just receive information that is pushed to them but be able to request information from these assets. The ability of field users to task space assets is especially critical when considering the advent of tactically responsive space systems, based on small satellites that would be integrated and launched in a matter of weeks or months as part of contingency operations.[5, 6]

The use of Internet Protocols (IP) would enable these warfighting concepts. There are several characteristics that a net-centric architecture or system should have: interoperability, platform independence, scalability, security, survivability, compromise immunity, transparency, mobility, use of shared infrastructure, simple warfighter interface, and bandwidth efficiency. The VMOC attempts to address most of these issues.

VMOC Overview

The VMOC must ensure the following: the right person--the right command--at the right time. The first issue is ensuring the right person. User authentication consists of methods to ensure that the user is permitted by the process owner to access the VMOC. These methods may include, but are not limited to, single sign-on, Public Key Infrastructure (PKI), or biometrics. Once the user is authenticated, he/she will be granted privileges as assigned by the process owner. This includes the user's priority level, tasking privileges and access rights to databases.

After granting permissions to the right user, the next step is to give the right command. The mission profile enables this. Every vehicle that can be tasked by the VMOC will have its own mission profile. The profile consists of mission rules, bus and payload capabilities, and orbital parameters. The process owner writes the mission rules and individual commands.

Lastly, the right command must be sent to the vehicle at the right time. In a net-centric environment, multiple taskings will be sent to the VMOC and many will conflict. The VMOC must determine first if the task is

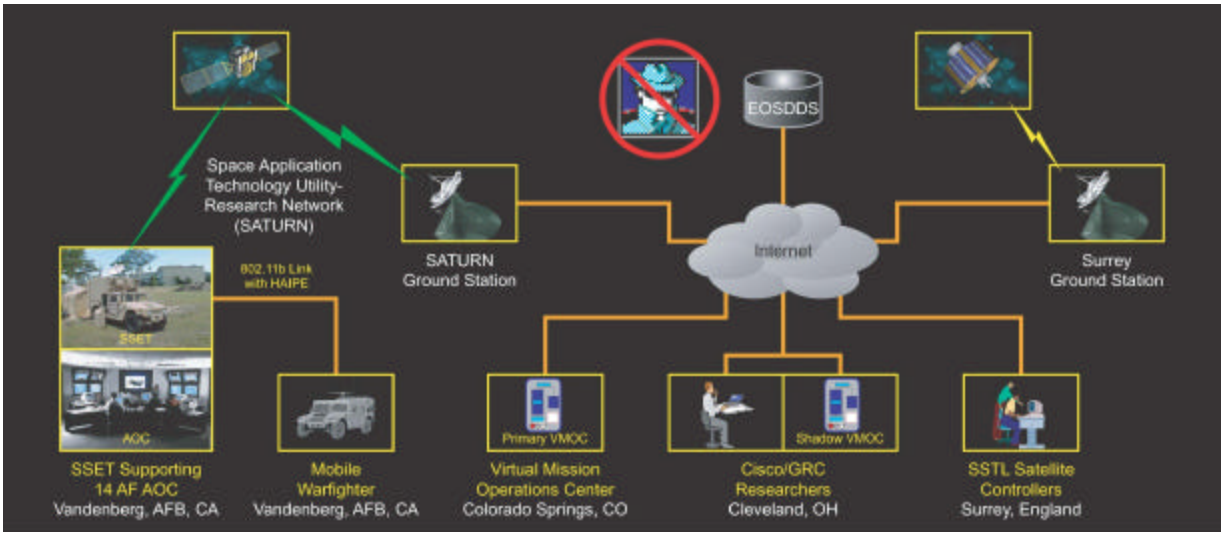

Figure 1. Overview of demonstration architecture.

possible in the timeframe desired by the user and then deconflict requests. The scheduling tool is used to determine if taskings are possible based on conditions such as the orbital parameters, availability of tracking stations, and power budget. Contention control selects the appropriate command to send to the space asset if there is a conflict.

A key to the VMOC is the requirement that the end user's computer needs only a web browser to perform command and control. This simplifies the logistics of maintaining the ground architecture since specialized software is not required on each computer. The VMOC itself resides on commercial-off-the-shelf (COTS) hardware.

Although this demonstration focuses on space systems, VMOC is neither platform nor sensor specific. In the future, VMOC may allow users to task space assets, unmanned aerial vehicles, and near-space assets such as the High Altitude Airship. By using Internet Protocols with commercial standards, an architecture could be developed that would increase user capabilities in the battlespace while permitting cost avoidance in maintenance and logistics.

For this demonstration, the team chose Virtual Mission Operations Center solutions developed by General Dynamics (GD) – Advanced Information Systems. The first operational GD VMOC is currently being used to task the payloads of the TacSat-1 mission sponsored by the Office of Force Transformation and developed by Naval Research Laboratory.[7]

Demonstration Overview

The VMOC demonstration was designed to show that military field users can use internet protocols to perform TT&C, task a space asset, and retrieve information either directly from that space asset or from a database. Most of the demonstration activities occurred between June 1 and June 18, 2004. While much of the military utility assessment took place at Vandenberg Air Force Base (AFB), California, the demonstration architecture was truly global in nature.

The first element of the architecture was the VMOC. A primary VMOC was located at

Space and Missile Systems Center (SMC) Detachment 12, Center for Research Engineering and Support (CERES), at Schriever AFB, Colorado. A shadow VMOC was located at NASA Glenn Research Center in Cleveland, Ohio to act as a backup. If the primary VMOC went down for any reason, the shadow VMOC resumed operations such that it would be transparent to the user. Both VMOCs were connected to the open Internet.

Connectivity allowed the VMOC to reach the ground station and task the spacecraft. The demonstration leveraged the efforts of NASA Glenn Research Center, Cisco and Surrey Satellite Technologies Limited (SSTL) for the Cisco Router in Low Earth Orbit (CLEO) experiment. In the CLEO experiment, a commercially developed IP router was placed aboard the United Kingdom – Disaster Monitoring Constellation (UK-DMC) satellite, which was launched September 2003 and operated by SSTL.

Joining with the CLEO team was of interest for several reasons. Tactically responsive space is enabled by the development of commercial IP space hardware. Therefore, CLEO supports the quest for standardized bus hardware and protocols enabling rapid launch and initialization. [8] The CLEO team is investigating secure, mobile IP throughout the architecture: a requirement for field utility. It should be noted that having a router on board the spacecraft is not a requirement for the VMOC. A VMOC could command an asset through a ground IP-based network that resides at the tracking station.

The users consisted of Air Force space operators from the Space Air Operations Center as well as members of the Army Space Support Teams. They were all located at Vandenberg AFB. The Army's Space Support Element Toolset (SSET) was deployed to Vandenberg for the demonstration. The SSET provides space capabilities to fielded Army forces including commercial space imagery and Internet reachback. The SSET's commercial Internet satellite communications capability provided the connectivity through the Internet to access the VMOC, allowing simulation of users in the field.

Air Force space operators performed three tasks for the demonstration. First, they prepared the user and command priorities for the demonstration. The priority lists were then input into the VMOC. These were reviewed on a daily basis and modified based on results or changes in the scenarios. Second, they performed TT&C on the UK-DMC. TT&C capabilities were limited in order to minimize interference with UK-DMC's operational mission of the micro-satellite. Rather than commanding flight critical systems, space operators were only able to give specific commands to the Cisco router hardware on the spacecraft. Space operators were also able to access live, streaming telemetry through the Internet. Third, the space operators could task the space vehicle to take imagery. However, their primary missions were prioritization and TT&C.

The primary missions of Army field users were to request imagery from the space asset through the VMOC and then retrieve that imagery. Army users were able to apply metadata to the image file such as highlighting portions of the image and adding comments. These modified images were then emailed to other users.

SMC Det 12 CERES recorded demonstration metrics. Results and analysis were not available at the time of paper

submission. However, there should be at least a quick look completed by the time of the conference.

SUMMARY

Net-centric warfare will enhance the effectiveness of our armed forces and networked space will certainly play a key role. In order to do this, one must ensure the right person--the right command--at the right time is accomplished. This is the role of the VMOC. The VMOC demonstration was designed to show the effectiveness of internet protocols for military operations involving TT&C, tasking, and retrieving results from space-based assets.

Acknowledgements

The authors would like to acknowledge the Office of the Assistant Secretary of Defense for Networks and Information Integration (ASD-NII) who provided funding and support through the Rapid Acquisition Incentive – Net Centric (RAI-NC) program.

Reference

1. Secure Mobile Networking Demonstration – November 6th, 2002 Onboard the USCGC Neah Bay in Cleveland, Ohio, http://roland.grc.nasa.gov/~ivancic/secure_mobile_networks/smn.html, December 2002
2. Master Sgt. Austin Carter, "Annual conference acknowledges space as key to success in Iraq", Air Force Space Command News Service, June 18, 2003
3. Dawn S. Onsley, Net-centric approach proven in Iraq, Government Computer News, Vol. 23 No. 10, 3 May 2004
4. "Net Centric Warfare: Creating a decisive Warfighting Advantage". Brochure by the Office of Force Transformation. Winter 2003
5. "Operationally Responsive Space Experiment TacSat-1", Transformation Trends, 17 Oct 2003
6. Elaine M. Grossman, "Air Force Wants To Create Small-Satellite Reserves For Crises." Inside the Pentagon, May 6, 2004
7. Lt. Col. Jay Raymond, CDR Greg Glaros, Joe Hauser, Michael Hurley, "TacSat-1 and a Path to Tactical Space", AIAA 2nd Responsive Space Conference, April 2004
8. Amy Butler, "Common Micro-satellite Bus Key To New Space Business, Transformation Officials Say", Defense Daily, April 22, 2004.