NASA/TM—2007-214807 Paper number 6.1104

Secure, Autonomous, Intelligent Controller for Integrating Distributed Sensor Webs

William D. Ivancic
Glenn Research Center, Cleveland, Ohio

May 2007

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI Program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NASA Aeronautics and Space Database and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or cosponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include creating custom thesauri, building customized databases, organizing and publishing research results.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at *http://www.sti.nasa.gov*

- E-mail your question via the Internet to *help@sti.nasa.gov*

- Fax your question to the NASA STI Help Desk at 301–621–0134

- Telephone the NASA STI Help Desk at 301–621–0390

- Write to:
  NASA Center for AeroSpace Information (CASI)
  7115 Standard Drive
  Hanover, MD 21076–1320

NASA/TM—2007-214807 Paper number 6.1104

Secure, Autonomous, Intelligent Controller for Integrating Distributed Sensor Webs

William D. Ivancic
Glenn Research Center, Cleveland, Ohio

Prepared for the
2007 Aerospace Conference
sponsored by the Institute of Electrical and Electronics Engineers and the American Institute of Aeronautics and Astronautics
Big Sky, Montana, March 3–10, 2007

National Aeronautics and
Space Administration

Glenn Research Center
Cleveland, Ohio 44135

May 2007

Level of Review: This material has been technically reviewed by technical management.

Available from

NASA Center for Aerospace Information
7115 Standard Drive
Hanover, MD 21076–1320

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161

Available electronically at http://gltrs.grc.nasa.gov

Secure, Autonomous, Intelligent Controller for Integrating Distributed Sensor Webs

William D. Ivancic
National Aeronautics and Space Administration
Glenn Research Center
Cleveland, Ohio 44135

Abstract

This paper describes the infrastructure and protocols necessary to enable near-real-time commanding, access to space-based assets, and the secure interoperation between sensor webs owned and controlled by various entities. Select terrestrial and aeronautics-base sensor webs will be used to demonstrate time-critical interoperability between integrated, intelligent sensor webs both terrestrial and between terrestrial and space-based assets. For this work, a Secure, Autonomous, Intelligent Controller and knowledge generation unit is implemented using Virtual Mission Operation Center technology.

1. Introduction

The idea of having sensors interact with each other is not new. There are many examples of this such as a fire alarm activation alerting the fire department or a burglar alarm notifying the security company to call the police. As technology progresses – particularly wireless and network technology—the next logical step is to integrate multiple individual sensors and allow these sensors to share information between each other and act as a single system, a sensor web. These sensor webs can be used for monitoring and event triggers. In addition, one could extract knowledge from the data collected. The knowledge can then be utilized by other entities: be they people, machines, or other sensor-webs.

The ability to access sensor webs—in particular space-based sensors—in a time-critical manner will enable new observation measurements and information products. The secure, automated intelligent controller implemented using the Virtual Mission Operations Center (VMOC) technology allows for a variety of data-mining techniques to be applied to the integrated sensor webs and associated databases thereby increasing the accessibility and utility of science data. Furthermore, the ability to integrate sensor webs owned and controlled by various parties will reduce the risk, cost, size, and development time for Earth science space-based and ground-based information systems.

2. Scenarios

A vast array of sensor webs already exists today for monitoring earth quakes and tsunamis. The seismic monitor consist of seismic recorders spread throughout the world with connectivity provided via numerous technologies including: phone lines, Internet, satellite, UHF and VHF radio systems. The tsunami sensor webs consist of buoys that measure wind, wave height, currents, and numerous weather related data. These buoys are spread throughout the oceans—particularly along the coasts. They communicate to the mainland via geostationary and polar satellites. The seismic sensors and buoys are already set up to work in concert to alert authorities of a possible natural disaster (e.g., volcanic eruptions and tsunamis). It would be highly advantageous to have these systems trigger imaging satellites to take pictures of areas of interest immediately before and immediately after a tsunami or earth quake hits an area. The former would aid in baselining an area while the latter would enable assessment of the destruction and aid in planning relief efforts. Here, time-critical interaction between the sensor webs is imperative. Today, such time-critical, autonomous operation between space and ground sensors is not possible as the systems and security mechanisms and policy have yet to be integrated for such a task.

In a second scenario, one may have a developing forest fire. Here, one may wish to request satellite imagery of the region in order to assess the terrain, vegetation, and moisture content of the area. This could aid in planning the most effective and safest ways to fight the fire. Additional information may be required that could be provided from an aerial infrared imager or other aerial sensors—perhaps even from a UAV. From the combined information of the imager, other sensors and satellite imagery, fire fighting teams can be dispersed. Also, additional inexpensive heat sensing sensor webs that include wind and temperature sensors may be deployed to monitor the progress of the fire. Some robotic mobile sensors such as a UAV drone or helicopter may also be of use. They could provide continuous monitoring of the event by moving with the fire yet avoiding self-destruction.

3. Network Architecture

Coordinated Operation over Multiple Ground Terminals

The ability to utilize multiple space and ground assets results in more available contacts, greater contact time, and quicker response time. This allows system implementers tremendous flexibility in the design of the space system. For example one could possibly reduce the downlink transmit rate

and corresponding transmit power or antenna size. The increased contact time over multiple ground assets means one does not have to size the system to transmit all data in a single contact time. Rather, large file transfers may take place over multiple ground stations. In addition, the ability to network infrastructure allows one to autonomously determine what space and ground assets are available, schedule the particular assets, and command and control those assets. For example, one can command a space-based sensor via ground station 1 and then receive data via ground stations 1, 2, and 3 (fig. 4). Thus, one now has the capability to perform near-real-time tasking of a space-based asset and retrieve the results in less than one complete orbit—assuming proper orbital dynamics relative to the available ground station locations.

Virtual Mission Operation Center (VMOC)

General Dynamics has developed a Virtual Mission Operation Center (VMOC) utilizing concepts that originated during collaborations with NASA Glenn Research Center regarding NASA's mission operations automation and control.

General Dynamics' Virtual Mission Operations Center is a web-based architecture designed for a Network Centric environment that:

- Adjudicates Networked Exchanges,
- Centralizes Control Authority Policy,
- Decentralizes Execution, and
- Uses thin and thick client web interfaces.

The VMOC provides a framework to define, test, demonstrate, and field new technologies within the relevant environment capable of supporting secure distributed mission operations of heritage and IP-based platforms and sensors. The VMOC's Rules Based Authentication, Modeling, Multi Mission Planning, Scheduling, and Telemetry Tracking and Command gives command authorities, analysts, operators, and users unparalleled tools for controlling complex platforms to maximize mission effectiveness. As such, the VMOC provides an excellent framework for a master controller and integrator of various sensor webs (ref. 1).

The VMOC has been written with common open standard application programming interfaces (API's) to enable third parties to integrate their unique pieces into the VMOC and allow the VMOC to provide security, user authentication, and application of mission rules. The necessary interfaces will be developed to integrate multiple sensor webs into the VMOC and to generate secure machine-to-machine operations.

Integrating Sensor Webs

The VMOC enables secure integration of diverse sensor webs into a larger autonomous network. The sensor platform will be monitoring events that match its onboard mission profile. The platform, via its onboard intelligent controller, will then autonomously send pertinent information to the master coordination controller, here, a VMOC. The VMOC will use this information to task other sensor assets. These additional sensors will either provide greater detail or supplementary information that the master coordination controller will then use to generate knowledge. This knowledge will be available to the appropriate individuals and/or systems. The critical technology is the establishment of rules and triggers which enable collaborative operation between sensor webs and associated data utilization and data mining systems. Integral to this effort is establishment of a precise language and meta-data for machine-to-machine communication.

4. Security

Whenever systems owned and operated by various entities are integrated, security must be addressed. When considering machine-to-machine autonomous communications and potential use of expensive assets such as space-based assets, security is of utmost importance. Of particular importance is addressing the policy issues that allow one to operate this new environment. Such security issues cannot be adequately addressed in a laboratory environment. If one wishes to integrate real operational systems owned and operated by various entities, policy issues arise that determine what is allowed (rather than technically possible) in regard to protocol and architecture. Furthermore, acceptable security mechanisms for machine-to-machine (m2m) communication between assets owned and controlled by various entities need to be developed.

The sensor web space/ground network consists of the following individual networks (fig. 1):

- The Cisco router in Low Earth Orbit (CLEO) onboard the UK-DMC;
- SSTL's ground station in Guildford, England;
- An Army supplied multi-user ground system (MUGS) in Colorado Springs, Colorado;
- Three ground stations operated by Universal Space Networks and located in Alaska, Hawaii, and Australia;
- A VMOC operated by General Dynamics and housed at NASA's Glenn Research Center;
- A IPv4 mobile network, located at NASA's Glenn Research Center (Also configured for IPv6 normal routing); and,
- A ground station owned and operated by Hiroshima Institute of Technology located in Hiroshima, Japan.

Figure 2 illustrates the various relationships relative to the overall network architecture. Individual networks consist of: a U.S. military network, a U.S. civilian government network, a United Kingdom private company network, a U.S. private company network, and a Japanese University network.

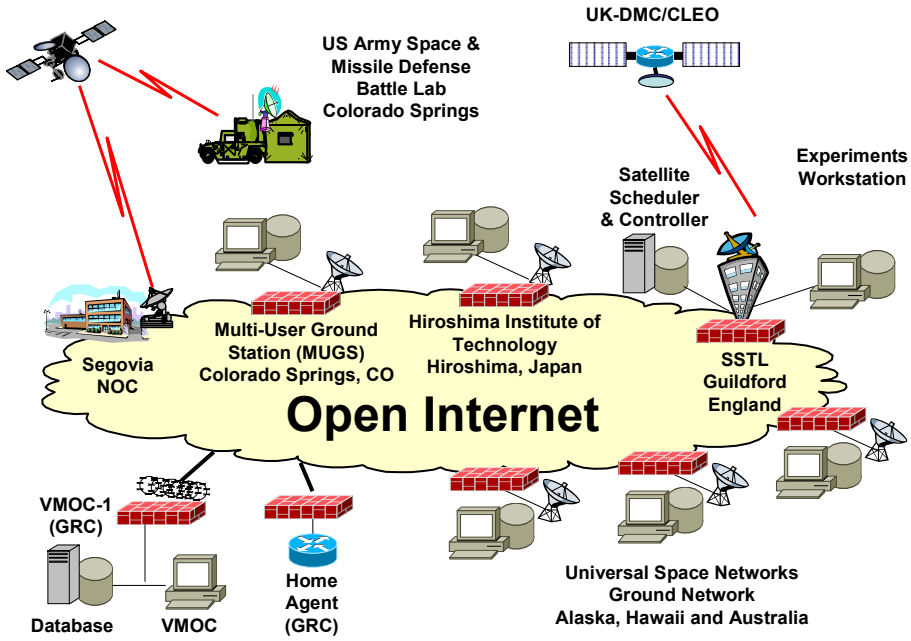

Figure 1.—Space/Ground Network.

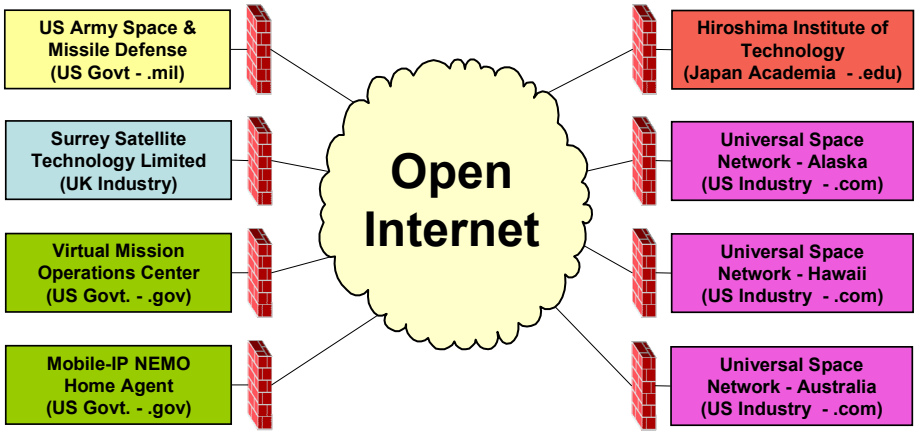

Figure 2.—Infrastructure relationships.

Maintaining acceptable security while utilizing a variety of networks owned and operated by diverse groups with systems in each network performing machine-to-machine communications in order to: share resources, schedule resources, and move data between systems provides a unique challenge. This system of networks provides an excellent security testbed as, with the exception of the SSTL and HIT networks, all other networks are configured for experimentation. As such, any security failures will be limited to controlled environments and will not find their way into critical operational systems. Utilizing this inter-network, NASA can begin to tackle the difficult security problems associated with international netcentric collaboration and autonomous machine-to-machine operations.

5. Near-Real-Time Commanding

When only one ground station is available or capable of command and control of a spacecraft, one must wait for that spacecraft to come into view of the ground station—assuming the system was not designed to use a relay satellite capability such as NASA's Tracking and Data Relay Satellite System (TDRSS). For a LEO satellite, real-time commanding may only be possible approximately every 90 min at best! If

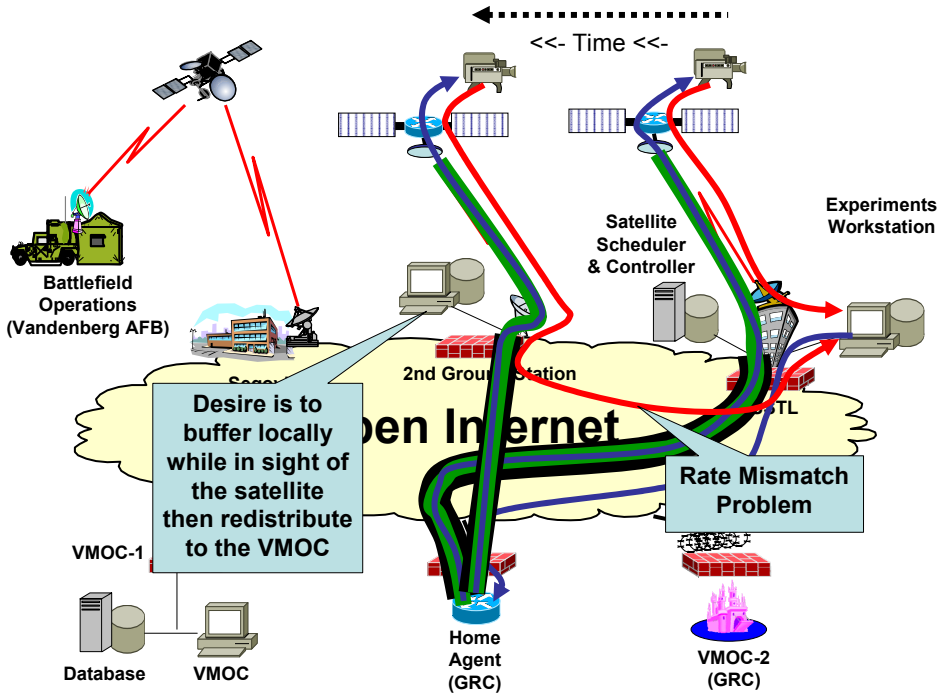

Figure 3.—Large file transfer rate mismatch problem for mobile-IP implementations.

commanding can be accomplished via third-party ground stations, one can greatly enhance the real-time commanding. This would enable one to accomplish near-real-time commanding scenarios to deal with problems such as the tsunami situation previously described in the first scenario.

6. Large File Transfer

The ability to obtain large volumes of data from space-based assets in a timely manner is a critical capability that needs to be addressed. Likewise, the ability to send large files to a space-based asset may also be necessary in order to properly configure or update space-bases systems in a timely manner. Two technologies that are being investigated to address these problems are: mobile networking protocols and standardized store and forward protocols using Delay/Disruption Tolerant Networking (DTN).

Mobile-IP, Networks in Motion (nemo)

When using networks in motion (nemo) technology based on mobile-IP, large file transfers over multiple ground stations have some attractive features and interesting problems. For Low Earth Orbit (LEO) systems, nemo technology allows one to share infrastructure, a feature that enables reduced cost and increases the number of available assets. This was demonstrated using the Cisco router in Low Earth Orbit (CLEO) and Virtual Mission Operations Center (VMOC) project (ref. 2). Also identified in the CLEO/VMOC project were some issues with large file transfer over multiple ground stations. Figure 3 illustrates the problem.[1]

If one uses nemo technology based on mobile-IPv4 triangular routing, one can easily operate over multiple ground stations with the only configuration required in each ground station being implementation of foreign-agent service—a few command lines in the router configuration. The actual location of the space-base asset is updated at the home-agent router which then double encapsulates all information, destined for the mobile network, and satellite, and then forwards it to the foreign-agent ground station. The foreign-agent de-encapsulates the message and forwards it to the satellite mobile router. The mobile router de-encapsulates the second tunnel and forwards the message to the appropriate mobile node. For triangular routing, the message is sent directly from the mobile node to the corresponding node using normal routing. In figure 3, the example shown has the first portion of a large file being transferred to a workstation at Surrey Satellite Technology Limited (SSTL) while the satellite is communicating with the SSTL ground station. The transfer rate is 8.0 Mbps from the satellite to ground. At some later time, the rest of the file is to be transferred while using the second ground station. Note, the transfer is still between the satellite and the SSTL workstation. A problem arises if the

[1]Figure 3 and 4 are available in animated form in slides 18 and 19 of the referenced presentation [Iva2005b].

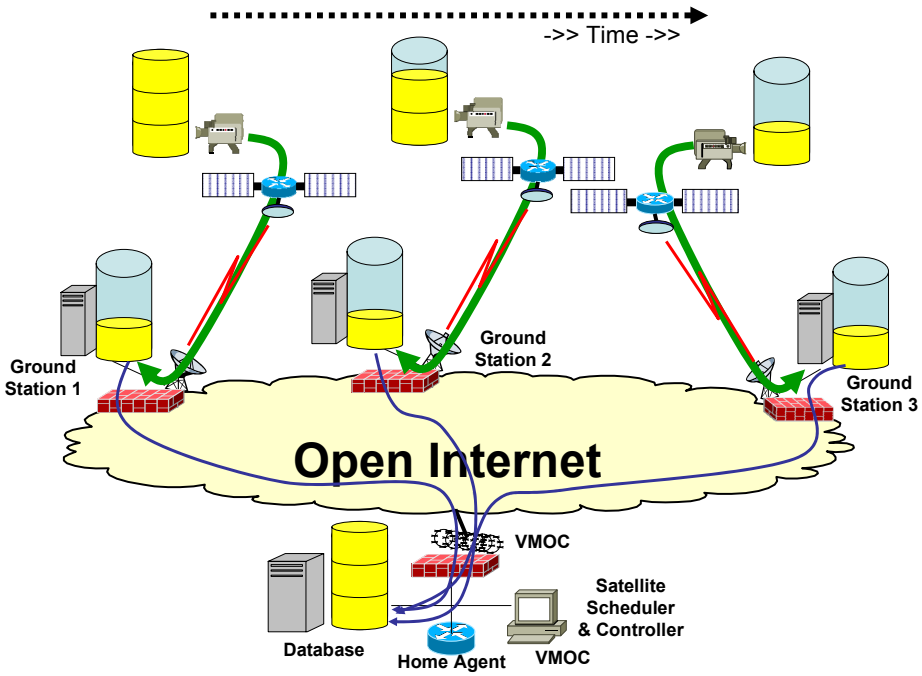

Figure 4.—Large File Transfer over Multiple Ground Systems.

link between the second ground station and the SSTL workstation is not equal to or greater than the space-to-ground link. Some type of buffering must occur locally in order for this to work properly.

Figure 4 further illustrates the desired event. Here, a large file transfer is required that will take up to three passes. If only one ground station could be used, that file would not be available until completion of the third contact time with the designated ground station. This may take multiple orbits depending on the orbit and placement of the ground station. By using multiple ground stations, one can obtain the information in much less time.

A similar problem exists if one wishes to upload a large file via multiple ground stations. This may be desirable in that the uplink for many satellites is much lower than the downlink. For the UK-DMC satellite, the uplink is only 9.6 kbps. Having a capability to upload a new solid state data recorder or router image using multiple ground terminals is highly desirable.

Delay/Disruption Tolerant Networking

Current DTN implementations are directed mainly at military and terrestrial environments where the protocols can be "opportunistic"—negotiations can occur in real time, unscheduled. These types of DTN protocols are applicable to some space-based environments such as for rover-to-rover (terrestrial-to-terrestrial) bundle transfers or even, to some degree, for rover-to-orbiter (terrestrial-to-near-space) bundle transfers. This is more in line with disruption tolerant networking. Delay tolerant networking has greater applicability to deep space where the long propagation delay requires scheduling of assets and predictive routing (refs. 4 and 5).

For the DMC satellites, two variations of DTN are envisioned: one for the downlink applications and a second for uplink.

For the downlink, the goal is to transfer large files from the satellite to a particular end system located on the VMOC network. Each portion of a file transfer would occur over multiple ground systems through bundling/forwarding agents located at each ground station. The downlink rate between the satellite and the ground station is 8 Mbps whereas the effective data rate between the ground station and the VMOC is unknown and may be orders of magnitude less than between the satellite and ground. Thus, each ground station buffers a portion of the file and transfers the bundles to the end system bundling agent located at the VMOC. The DTN protocol must segment the overall file into bundles optimized for the contact time between the DMC satellite and the ground stations. As the delay between the ground stations and the satellite is relatively insignificant (approximately a 100 ms), an opportunistic type of DTN could be utilized.

For the uplink, the goal is to transfer a large file from a bundling agent located at the VMOC to the DMC satellite. In this situation, the terrestrial links between all systems (i.e., VMOC, mobile network home agent, and all ground stations) are expected to be relatively fast compared to the uplink channel. Note, the uplink channel is only 9.6 kbps. Because of

this, the DTN transfer can take place directly between the bundling agent at the VMOC and the DMC satellite. No intermediate buffering is necessary. Furthermore, the delay between the VMOC and DMC is relatively small, in the order of 100 ms. Therefore, an opportunistic type of DTN could be utilized. The difference between the uplink DTN and the downlink DTN is that for the uplink, the bundling agent at the VMOC needs to know when to transmit and routes have to be established using either some form of predicted routing or using mobile networking. Mobile networking appears to be ideally suited for this as, in addition to handling the routing, the binding status between the home agent and mobile router may be used to notify the DTN protocol to initiate transfers.

7. IPv6-based Mobile Sensor Webs

IPv6 is an up and coming technology. It has been mandated by DoD for their future networks and is a driving component of their future combat systems. Furthermore, the United States Government has recently mandated that ALL government agencies including NASA be IPv6 compliant by 2008.

IPv6 has some very nice features particularly when considering sensor webs.

- Auto configuration of addresses
- Scoped Addressing (link, unique local and global)
- Large address space
  - Enables Globally unique addressing
  - Enables cryptographic addressing
  - Enables location management
- Route Optimization for mobile-IP
- Extensible header in IPv6 header format rather than "options"
- Enhanced multicast

The auto configuration and link local addressing features are extremely useful for sensors and ad hoc networks as no pre- infrastructure such as DHCP[2] servers are needed and addresses do not need to be pre-configured in end-systems. The extensible headers also are useful in allowing new features to be developed without hindering current operations. These features along with military applications have spurred a variety of research activity in mobile ad hoc networking using IPv6.

Some of the problems related to mobile sensor webs that need to be addressed include:

- Autonomous identification of services such as domain name servers, network time servers, location managers and security servers,
- Identification of reachback paths to the big Internet,
- Route optimization of mobile networks,
- Security mechanism for mobile and ad hoc networks (other than radio link encryption), and
- Scalability of mobile sensor networks.

Ad hoc network-based, mobile IPv6-based sensor webs are being investigated for use as the event scouts which would perceive an event and inform the VMOC, the secure, autonomous, intelligent controller. The VMOC would use this information to determine what types of additional sensors should be activated, including any space assets. All scheduling and tasking of system assets would originate at the VMOC.

8. Summary

The necessary infrastructure and protocols are being developed that will enable near real-time commanding and access to space-based assets and the secure, interoperation between sensor webs owned and controlled by various entities. This work is taking place at NASA's Glenn Research Center with cooperation and collaboration from numerous partners. For this work, the Virtual Mission Operation Center technology developed by General Dynamics is being used to provide a secure, autonomous, intelligent controller for integrating distributed sensor webs. The system uses standard-based protocols to demonstrate time-critical interoperability between integrated, intelligent sensor webs. In addition, the security aspects of international network centric operation which utilize machine-to-machine communications are being addressed.

References

1. Delay Tolerant Networking Research Group http://www.dtnrg.org/wiki

2. Interplanetary Internet Project http://www.ipnsig.org/home.htm

3. William Ivancic, Phil Paulsen, Dave Stewart, Dan Shell, Lloyd Wood, Chris Jackson, Dave Hodgson, James Northam, Neville Bean, Eric Miller, Mark Graves and Lance Kurisaki: "Secure, Network-Centric Operations of a Space-Based Asset: Cisco Router in Low-Earth Orbit (CLEO) and Virtual Mission Operations Center (VMOC)," NASA/TM—2005-213556, May, 2005 (Final Report)file size 3.1 Mbytes. http://roland.grc.nasa.gov/~ivancic/papers_presentations/2005/cleovmoc.pdf

[2] Dynamic Host Configuration Protocol: Software that automatically assigns temporary IP addresses to client stations logging onto an IP network. It eliminates having to manually assign permanent "static" IP addresses. DHCP software runs in servers and routers.

4. William Ivancic: “Secure, Network-Centric Operations of a Space-Based Asset: Cisco Router in Low-Earth Orbit (CLEO) and.Virtual Mission Operations Center (VMOC)” Net-Centric Operations 2005, May 10–11, 2005 Washington, DC (Powerpoint) file size 5,871,616 bytes. http://roland.grc.nasa.gov/~ivancic/papers_presentations/2005/AFEI_NCO_presentation.ppt

5. Eric Miller, Omar Medina, Lt Col Richard Lane, Allen Kirkham, Will Ivancic, Brenda Jones, Ron Risty: “Small Satellite Multi Mission C2 For Maximum Effect,” 4S Symposium-Small Satellites Systems and Services, Chia Laguna, Saridinia, Italy, September 25–29, 2006

Biography

Will Ivancic is a senior research engineer at NASA’s Glenn Research Center working in the networking and advanced communication technology development. Mr. Ivancic’s work includes: advanced digital and RF design, communications networks, satellite onboard processing, and system integration and testing, Mr. Ivancic’s recent work has concentrated on research and deployment of secure mobile networks for aerospace and DoD networks.

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01-05-2007	Technical Memorandum	

4. TITLE AND SUBTITLE
Secure, Autonomous, Intelligent Controller for Integrating Distributed Sensor Webs

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Ivancic, William, D.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
WBS 430728.02.04.02.01

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
John H. Glenn Research Center at Lewis Field
Cleveland, Ohio 44135-3191

8. PERFORMING ORGANIZATION REPORT NUMBER
E-15962

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSORING/MONITORS ACRONYM(S)
NASA

11. SPONSORING/MONITORING REPORT NUMBER
NASA/TM-2007-214807; Paper number 6.1104

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified-Unlimited
Subject Category: 04
Available electronically at http://gltrs.grc.nasa.gov
This publication is available from the NASA Center for AeroSpace Information, 301-621-0390

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This paper describes the infrastructure and protocols necessary to enable near-real-time commanding, access to space-based assets, and the secure interoperation between sensor webs owned and controlled by various entities. Select terrestrial and aeronautics-base sensor webs will be used to demonstrate time-critical interoperability between integrated, intelligent sensor webs both terrestrial and between terrestrial and space-based assets. For this work, a Secure, Autonomous, Intelligent Controller and knowledge generation unit is implemented using Virtual Mission Operation Center technology.

15. SUBJECT TERMS
Communication; Networking security

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			William D. Ivancic
U	U	U		13	19b. TELEPHONE NUMBER *(include area code)* 216-433-3494