INTEGRATION OF MILITARY AND COMMERCIAL SATCOM INTO THE DEFENSE INFORMATION INFRASTRUCTURE

Doug Ramsey
Charlie Hammond
Lawrence Krebs
Stanford Telecom
1761 Business Center Drive
Reston VA 20190

William Harrison
DISA/D3141
701 S. Courthouse Rd
Arlington, VA 22204

William Reed
Richard Williams
DISA/CSFE.
10701 Parkridge Blvd
Reston, VA 20191

ABSTRACT

Military (i.e., DSCS) and Commercial (i.e., CSCI) Satellite Communications plays a significant role in providing bandwidth and connectivity for the Defense Information Systems Network (DISN), which is part of the larger Defense Information Infrastructure (DII). However, in the past, this bandwidth and connectivity has generally been provisioned as dedicated, full period trunks providing OSI Reference Model layer 1 (Physical) services. This severely limits the responsiveness of the SATCOM segment in servicing changeable, multimedia applications in a potentially stressed SATCOM transmission environment.

DISA has taken steps to address this limitation, specifically with the development of the SHF DAMA Standard (MIL-STD 188-166/167. This paper discusses additional efforts sponsored by DISA and by the USAF Research Laboratory to improve the seamless integration of the SATCOM segment into the overall DISN. Efforts discussed include:

- *Evaluation of methods and protocols for internetworking ATM with DAMA-controlled SATCOM and network management methods for end-to-end service provisioning;*
- *Evaluation of the impact of nuisance jamming and interference on commercial SATCOM links supporting ATM network services;*
- *Evaluation of QoS-based provisioning for ATM services over DAMA-controlled SATCOM;*
- *Development of Open Systems gateways for integration of SATCOM management and control into the DII Control Complex.*

DSCS AND CSCI: CURRENT KEYSTONE OF WIDEBAND SATCOM

The Defense Satellite Communications System (DSCS) and the Commercial Satellite Communications Initiative (CSCI) together form the SHF segment of the military satellite communications architecture. The DSCS and CSCI carry the bulk of the Information for the Warfighter that is supported over military SATCOM systems. For example, during Operation Desert Storm satellite communications provided the vast majority of the communications into and out of the Kuwaiti Theater of Operation and of this, the bulk was carried via the DSCS.

CSCI resources are currently being used to support the augmentation of the tactical C^2 infrastructure in Bosnia,

0-7803-4902-4/98/$10.00 (c) 1998 IEEE

the DII Contingency initiative on the Korean penninsula, and the Challenge Athena program for the U.S. Navy. Of the transponders currently being leased to support the CSCI, 60% are being used to provide Information to the Warrior.

Concurrent with support to tactical users, the SHF SATCOM segment continues to provide long-haul service for communications trunks associated with the Defense Information Systems Network (DISN) and other wideband users at the national level. Current estimates are that the DSCS supports over 500 Mbps of tactical and strategic data transmissions on a global basis.

IS SATCOM PART OF THE DEPLOYED DISN?

The extension of the DISN into remote and tactical areas is highly dependant on the availability of satellite communications resources. This is especially true for communications in support of Navy forces afloat and with realization of the Navy's IT 21 vision. However, the existing SHF SATCOM infrastructure has some inherent features that limit the degree to which it can participate in the extension of multimedia services to deployed forces. The following are some examples of these limiting features:

- *Relatively low data rate as compared to fiber optic circuits*- the maximum trunk rate supported by existing DSCS modems is 20Mbps (without error correction coding), as compared to the lowest optical carrier rate (OC-1) of 51.84 Mbps.

- *Relatively high bit error rate as compared to fiber optic circuits* - circuits carried over SHF SATCOM are traditionally allocated sufficient power to provide maximum bit error rates of 1 in 10^{-6}. The ATM protocol was designed for data transmission in a fiber-quality environment with a bit error rate no greater than 1 in 10^{-10}.

- *Vulnerability to RF interference* - all wireless communications is susceptible to intentional and unintentional interference, however, because of the coverage area each geostationary satellite is vulnerable to RF interference from a significantly large area of the globe

- *Non-responsive to changes in communications service requirements* - the communications trunks carried via SHF SATCOM are generally provisioned as dedicated, full period trunks providing OSI Reference Model layer 1 (Physical) services. No connectivity with the end user through a control channel (e.g., the control plane of the ITU Broadband ISDN Reference Model) is available for negotiation of basic layer 2 (Data) and layer 3 (Network) services.

EVOLUTION VERSUS REVOLUTION

The Defense Information Systems Agency Center for Systems Engineering (DISA/CFSE) made the first steps toward ameliorating these limitations with the development of the <u>C, X, and Ku Band Fixed Satellite Service (FSS) Demand Assigned Multiple Access (DAMA) Standard.</u> The goal of the "SHF DAMA Working Group" was to "evolve" the SHF SATCOM segment toward a more responsive, user-oriented posture while maintaining backward compatibility with the existing (and anticipated) capital infrastructure. A prototype DAMA network at Ku-Band was fielded in 1997 for the Bosnia Command and Control Augmentation (BC2A) network, demonstrating the potential for providing ATM services over DAMA-controlled SATCOM.

WHERE DO WE GO FROM HERE?

Clearly, development of the DAMA standard was just one small step in the evolution of the SHF SATCOM segment into a more responsive communications system that is fully integrated into the DII working model. DISA is working in collaboration with other DoD organizations on a number of initiatives toward that end. The remainder of this section will discuss a subset of these initiatives.

INTERNETWORKING ATM WITH DAMA-CONTROLLED SATCOM

The Military Services all have increasing needs for greater information throughput in order to achieve information dominance over potential adversaries. The ATM protocol is seen by many to be a key enabler of this capability with its high speed multiplexing and switching that can support all kinds of user traffic including voice, video, still imagery, data and other mixed media applications. Even though ATM technology was originally developed for employment in low bit-error physical network environments such as in the fiber optic medium, the protocol is still envisioned to be the transport mechanism to meet warfighter's needs in supporting distributed processing and collaborative multimedia applications on networks operating in stressed battlefield environments. Thus, resolving the problems associated with sending ATM cells over high bit-error rate, limited bandwidth, satellite communication channels provides a significant challenge.

Under the DAMA/ATM/WLM SSCN (DAWS) program sponsored by the USAF Research Laboratory at Rome, New York, the challenges of internetworking ATM over DAMA-controlled SATCOM were examined in detail.

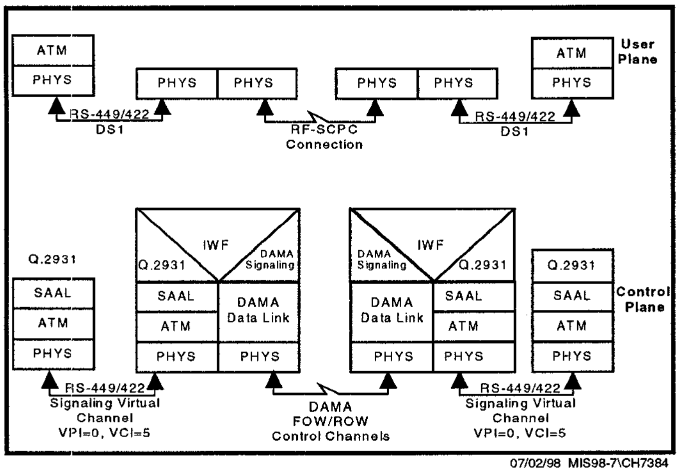

Exhibit 1: User and Control Plane Models for Internetworking ATM with DAMA-controlled SATCOM

Exhibit 1 illustrates the method proposed in the study for interconnecting DAMA and ATM networks. In the user plane, DAMA-controlled SATCOM networks provide the underlying physical connections for ATM through a Single Channel per Carrier (SCPC) circuit connection. Supportable ATM physical layer interface formats include the ATM Forum DS1 Physical Layer Specification (af-phy-0016.000) up to the DS3 Physical Layer Specification (af-phy-0054.000) based on the capacities of existing DAMA communications traffic modems. RS-449/422 will provide physical and wire line connectivity between an ATM switch and the DAMA NT. The DAMA NT provides waveform link encryption and decryption, FEC encoding and decoding, and modulation and demodulation as specified in MIL-STD 188-165 and the SHF DAMA Standards (MIL-STD-188-166/167).

The user plane concepts for internetworking ATM with SATCOM have been demonstrated in the Bosnia C2A network. However, the value-added provided by this Rome Laboratory effort provides a means to accommodate ATM switched or permanent virtual circuit services over DAMA-controlled SATCOM by employing the control plane signalling scheme shown in Exhibit 1. Potential follow-on work remains in developing the interworking unit (IWU) needed to translate these signalling schemes between the DAMA and ATM domains.

ATM VULNERABILITIES RELATED TO SATCOM LINK INTERFERENCE

The Commercial Satellite Communications Initiative (CSCI) is a Congressionally-mandated program to establish a worldwide network of commercial satellites based on a strategy of leased C and Ku band transponders for DoD non-mission critical traffic. The CSCI program augments the existing DSCS MILSATCOM system by providing additional transponder, gateway and end-to-end transmission services. The transponder services provide worldwide coverage for eight overlapping domestic and international regions. The gateway service extends user access through commercial or DoD-owned gateway terminals, teleports or Standardized Tactical Entry Point (STEPs). End-to-end transmission services afford CSCI customers full turn key network services that includes planning, engineering and installation of equipment.

While the use of commercial satellites in being increasingly relied upon by DoD for worldwide communications, these resources are not designed to provide protection against any type of adversary threats. Jamming, as the principal threat to SATCOM, can effectively drive a commercial SATCOM transponder into saturation when transmitting enough power in the transponder's operating frequency band. The effectiveness of this brute force method depends upon the effective isotropic radiated power (EIRP) of the jammer and its standoff range. With uplink jammers, the standoff range can be virtually anywhere within the satellite footprint, as long as the jammer has adequate EIRP. However, this jamming strategy leaves a jammer vulnerable to geolocation, targeting and destruction. A more subtle strategy would be to employ low-level, intermittent jamming that temporarily degrades the satellite link signal quality enough to disrupt communications and possibly lead inexperienced satellite terminal operators into misinterpreting these actions as equipment faults or to link interference. Since ATM services are also very vulnerable to cell errors and losses, the underlying communications link quality does not have to be significantly degraded to produce substandard performance in the ATM networks.

In this program sponsored by the Information Warfare branch of the USAF Rome Research laboratory, the following aspects of studying the vulnerabilities of ATM over SATCOM are being investigated:

- *Defined Threat Characteristics* - Determine the downlink jammer standoff distances for representative EIRP values required to create unacceptable link bit error rates.

  Determine BPSK symbol error probabilities for various signal to link interference ratios.

  Assess the capabilities of tone versus broadband jammer types with regard to power levels, duty cycles, and signal phase relationships.

- *Develop Relationships among ATM Network Performance Parameters and SATCOM Link BER* - Investigate ATM CLR to BER, CER to BER, CMR to BER and burst error characteristics.

- *Investigate ATM Network Vulnerabilities* - Identifiy ATM network-level threat types, such as intrusion, misdirection of information, and eavesdropping.

  Investigate network vulnerabilities in the ATM user and control planes, as well as what organizations such as the ATM Forum are doing to mitigate these network vulnerabilities.

- *Analyze Coding and Interleaving Techniques to Mitigate Vulnerabilities* - Develop a C-based software model to evaluate coding and interleaving techniques across a data sink-to-source communications channel and transmission system.

  Assess broadband and tone jammer effects on these coded links while accounting for burst error distributions.

The results of this program bring an increased understanding of the vulnerabilities of ATM networks operating over commercial SATCOM links. Knowing this improved adaptive coding and interleaving techniques can be applied to mitigate jamming and overall link interference while still providing a guaranteed level of QoS for the users. Follow-on work could include developing hardware and software prototypes to implement these concepts in a testbed configuration.

DEVELOPMENT OF THE DII SATCOM GATEWAY MANAGEMENT SYSTEM

The DII SATCOM Gateway Management System (the "DII Gateway") is intended to enhance the management capabilities available to DII Control Centers by providing them with SATCOM network management information. The DII Gateway will operate between the DISA Integrated Network Management System (INMS) platforms and the Defense Satellite Communications System (DSCS) Integrated Management System (DIMS), and between the INMS and Commercial Satellite Communications Initiative Bandwidth Management Centers (CSCI BMC).

Under sponsorship of the DISA Center for Systems Engineering a prototype gateway was developed in the Fall of 1996 to demonstrate the feasibility of extracting network management information from the DIMS databases at DSCSOCs, formatting and storing the information in an SNMP MIB, and providing access to that information from a higher-layer network management platform via TCP/IP. The legacy and proprietary element management systems currently present at the SATCOM control centers necessitate such a gateway to allow the exchange of management information in a standards-based format.

The current effort expands upon the prototype gateway and provides INMS access (at the GOSC and ROSCs) to additional DIMS data and to the CSCI BMC data. This system-wide integrated strategy for reporting SATCOM performance and configuration data allows the DII Control Center to manage SHF SATCOM resources as an integral part of the DISN, and to distribute this information to appropriate SATCOM users and deployed control centers.

Follow-on efforts will include, as a minimum, implementation of data elements corresponding to future version releases of the DIMS 97 and DIMS 98 feature sets (the DSCS portion), as well as additional data elements from CSCI BMC databases. With the expansion of the data available for analysis, future gateway implementations may include alarm filtering and data correlation to augment user evaluation of system health and status.

QOS PROVISIONING OF ATM SERVICES OVER DAMA-CONTROLLED SATCOM

In our previous DAWS program, the use of DAMA[1]-controlled Single Channel per Carrier (SCPC) SATCOM channels was determined to be a feasible means of transmitting ATM network services over commercial or military SHF SATCOM systems. SCPC channels could be set up through a DAMA controller and a Network Control Terminal (NCT) to allocate a fixed amount of bandwidth between point-to-point or multipoint connections for the duration of a communication session. Furthermore, ATM signaling and control procedures could be interfaced with an interworking unit (IWU) to trigger DAMA control setup or teardown messages between an NCT and other network terminals (NT) [1]. However, while this Frequency Division Multiple Access (FDMA) technique is suitable for ATM Constant Bit Rate (CBR) services, it fails to leverage the statistical multiplexing features of ATM and will not adequately support the bursty nature of real-time or non-real-time Variable Bit Rate (VBR) ATM services or the other ATM service types, i.e., Available Bit Rate (ABR) or Unspecified Bit Rate (UBR).

Consequently, in the Quality of Service (QoS) DAMA/ATM/Wireless Land Networks (DAWN) program also sponsored by the USAF Rome Research Laboratory, STel developed concepts for the service provisioning of all ATM service types over DAMA-controlled SATCOM channels to accommodate the bursty characteristics of VBR-rt, VBR-nrt, ABR and UBR service types. These concepts employ a modified version of the Frame Relay technology and protocol. The key features of our concept are to implement the procedures in an IWU interface between an ATM network and a DAMA-controlled NT or NCT. The scheduling algorithm being evaluated is modeled in OPNET to better understand its capabilities and limitations and to define the technical requirements for the IWU.

The value-added provided by this program will bring the capability to provide QoS and real-time service provisioning to DAMA-controlled SATCOM networks and eventually to the shared communications infrastructure at large. Follow-on work could include extending these concepts into other communications systems, updating the DAMA standard, and in developing a prototype IWU for concept demonstration.

CLOSING COMMENTS

The efforts discussed above represent initiatives to improve the support provided to the warfighter by the SHF segment of the current MILSATCOM architecture. The MILSATCOM architecture will evolve to include programs such as SHF Gapfiller, UFO follow on, advanced MILSTAR and GBS. Commercial transport mechanisms will most likely include high bandwidth LEO systems such and Celestri and Teledesic, in addition to the Fixed Satellite Services currently provided via the CSCI. Now is the time to start looking at how these capabilities are going to be used to provide continued support to the warfighter as a part of the global DII.

---

[1] Demand Assigned Multiple Access (DAMA) as specified in MIL-STD-188-166/167 for commercial C and Ku band or military X-band SATCOM systems.

0-7803-4902-4/98/$10.00 (c) 1998 IEEE