A Violation of Order:  
IP-QoS for Tactical Traffic

Chris Alspaugh  
Albert K. Legaspi, Ph.D.

SPAWAR/SYSCEN D822  
San Diego, CA 92152

ABSTRACT

Network Centric Warfare is the foundation for Joint Vision 2010/2020, under which new levels of operational effectiveness in warfare will be achieved. The Expeditionary Command, Control, Communications, Computer and Combat Systems Grid (EC5G) is a near-term enabler of JV2010/2020. The fundamental objective of EC5G is the enhancement of Naval network architecture. A major problem in the development of the EC5G is to merge Joint Data Network and Joint Planning Network while retaining certain levels of application service guarantees through utilization of Quality of Service (QoS) mechanisms between source and destination of network traffic. Network QoS guarantee is a necessary condition for merging networks since the resulting network must provide each application at least the same level of service it had prior to the merging - in its legacy network. However, network QoS is not a sufficient condition to service all tactical and sensor applications. Guarantee of bandwidth or a bound on latency does not ensure that operational traffic will meet its stringent QOS requirements.

The objective of this paper is to identify potential vulnerabilities and pitfalls that may be encountered in sending Tactical Digital Information Link (TADIL) data from the JDN over an IP-QoS Advanced Data Network System (ADNS) communications devices and links, which commonly service the JPN. The analysis that was performed during this effort highlights two conditions wherein message sequence errors may occur. Both of these conditions suggest careful planning and additional consideration before a concrete TADIL-over-ADNS implementation is proposed.

INTRODUCTION

Since 1994, Network Centric Warfare concepts have been tested through simulations, exercises and analysis and have shown to significantly improve multi-warfare operations through enhanced situational awareness throughout the chain of command of a deployed fighting force [1]. In 1999, the Chief of Naval Operations Strategic Studies Group (SSG) developed a concept called ForceNet, a naval component of the global DoD network called Global Grid, which provides a multi-domain, tiered network architectures of sensors, command and control, weapon systems and communication nodes extending these services from sea to space. A requirement of ForceNet is to have real-time monitored and information disseminated throughout this global network. The Expeditionary Command and Control, Communications, Computers and Combat Systems Grid (EC5G) implement the concepts of ForceNet through transition into operations. EC5G provides to remotely deployed forces access on this global network. Reference [2], EC5G Master Plan, identifies nine end-to-end capabilities of EC5G. A significant objective is to merge two major networks (Joint Planning and Data Networks) to enhance situation awareness throughout the Battle Group. This feat signifies a major step toward a major objective of network centric warfare which Information Superiority. Merging networks of this sort will enhance the speed of command and information dissemination through the capability to plan and command seamless over one network and network enhancements such as Quality of Service (QoS) and multi-level security [2].

Merging the two networks will migrate tactical information (Tactical Data Links) into a network that will have a variety of network services such as QoS to voice, data and video applications. In addition, general convergence of applications creates advantages such as improve bandwidth utilization by allowing applications access to underutilized networks, reduces maintenance cost due to having one network infrastructure and access to leading edge network technology. As such, experiments and analysis are in progress to study the impact of moving tactical data links to IP-QoS networks. IP-QoS provides applications with stringent bandwidth or latency guarantees over the current IP data networks, which provides “best effort” services (no guarantees of service). IP-QoS provides guarantee performance bounds on latency and accuracy for message data. QoS services are deployed in two methods - Integrated and Differential Services.
Integrated services provide guarantees through end-to-end bandwidth reservation. Initiating this reservation requires each router along the path to determine its ability to support specific traffic service requirements. It is well known that this approach, unfortunately, does not scale with the number of military applications and the full range of speed through Naval networks [3]. Differential Service (DS), unlike integrated services, provides per hop service (otherwise known as Per-Hop-Behavior) that ensures some level of guarantees to a class of traffic [4], [5]. Per-Hop-Behavior (PHB) is defined as a way intermediate network nodes (such as routers) treat traffic flows. Since treatment of a traffic class is administered per hop, end-to-end guarantees may not be fully realizable. However even though the per-hop treatment of traffic provides some level of service over today's IP implementation of best effort delivery. The Navy deployed IP network, Automated Digital Network System (ADNS), provides IP connectivity and automatic route negotiation for multiple legacy satellite communications systems. ADNS developers [6] are exploring the utilization of QoS in order to facilitate new applications with rigid bandwidth/delay guarantees. It is expected, as part of Network Centric Warfare, time-critical applications such as tactical and intelligence applications migrate to a global network when network service guarantees satisfy their delivery requirements. A major objective of EC5G is to merge Joint Data Network (JDN) and Joint Planning Network (JPN).

The objective of this paper is to identify potential vulnerabilities and pitfalls that may occur when sending Tactical Digital Information Link (TADIL) data from the JDN over Advanced Data Network System (ADNS) communications devices and links, which commonly service the JPN.

A potential upgrade to the TADIL Command and Control Processor (C2P) includes the capability to send tactical data over Internet Protocol (IP) networks within ADNS. This tactical data is very time-critical and in the past has been transmitted over real-time communication links such as Link 4A, Link 11, and Link 16. With recent advances in IP technologies, there have been some investigations into sending time-critical TADIL traffic over ADNS networks. These investigations include the use of Differentiated Services (DiffServ) Quality of Service (QoS) and Policy Routing technologies to assure timely delivery of tactical messages.

IP QoS implementations do offer a solution that permits tactical messages to be received within required time boundaries. However they do not guarantee delivery of these messages in sequential order. This is a significant fault. Current implementations of JDN traffic over the TADIL guarantee that messages will be received in order, or not at all. As a result, tactical host terminals and processors are currently ill-equipped to handle message sequence errors.

The goal of this study is to gain a better understanding of the conditions under which messages may be received out of order in proposed TADIL-over-ADNS configurations, and to offer suggestions and recommendations for areas that require further investigation. This study focuses on the use of Modeling and Simulation (M&S) to construct high-fidelity network models and test them under varying configurations and conditions. M&S provides an inexpensive and reliable method for planning and testing systems and configurations before actual deployment.

2. Message Ordering Vulnerability Studies
This study highlights four areas where proposed TADIL-over-ADNS implementations are vulnerable to message sequence errors. It is not intended to identify all potential problem areas. Simulation studies and discussions of their results are in the sections that follow. Overall conclusions and recommendations are discussed in Section 3.

3. ADNS OSPF Link Selection
One of the key features of ADNS is its ability to dynamically manage different Satellite Communications (SATCOM) resources. A ship with several SATCOM reachback options, such as Challenge Athena (CA), Defense Satellite Communications System (DSCS), and MilStar, would utilize ADNS to select the best link for forwarding IP traffic on and off the ship. ADNS currently implements the commercial Open Shortest Path First (OSPF) routing protocol in order to select optimal route paths. One of the shortcomings of using a dynamic routing protocol such as OSPF is that end-to-end paths may change over time to include links of different channel characteristics. The instant an end-to-end path is changed, there is a possibility that the new best path may be much faster than the previously selected path. When a new faster path is selected, any packets that are en route over the old path may be passed by packets traveling on the new path, causing sequence errors. It is important to note that this may occur regardless of QoS Per Hop Behaviors (PHB) at the router interfaces. The goal of this simulation study is to investigate the likelihood and conditions of this sequence error in an ADNS configuration.

2.1.1 Simulated Topology and Configuration
The simulated configuration was derived from ADNS functional drawings and configuration in [7], [8], and [9]. The network architecture is shown in Figure 2-1.
The scenario was selected to simulate a ship to shore communication from a SHF SATCOM-equipped ship to a tactical terminal on the shore. Note that most implementations of TADIL-over-ADNS will include an additional hop to another afloat participant. However the objective of this study is to focus on a single SATCOM hop, illustrating a best case scenario. Each of the dotted lines that connect the two routers in Figure 2-1 represent SATCOM links and model the channel transmission and propagation effects of each. Data rate allocations for ADNS are listed in Table 2-1.

Table 2-1 SATCOM ADNS Data Rate Allocations

<table>
<thead>
<tr>
<th>Link</th>
<th>Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCSIII</td>
<td>96 Kbps</td>
</tr>
<tr>
<td>CA</td>
<td>256 Kbps</td>
</tr>
<tr>
<td>INMARSAT B</td>
<td>32 Kbps</td>
</tr>
<tr>
<td>UHF SATCOM 5 KHz</td>
<td>2.4 Kbps</td>
</tr>
<tr>
<td>UHF DAMA</td>
<td>2.4 Kbps</td>
</tr>
<tr>
<td>EHF LDR 1</td>
<td>2.4 Kbps</td>
</tr>
<tr>
<td>EHF LDR 2</td>
<td>2.4 Kbps</td>
</tr>
</tbody>
</table>

The data rates shown in Table 2-1 service most shipboard IP traffic through ADNS, including SIPRNET and NIPRNET traffic. TADIL traffic is also serviced within these bandwidth allocations in this scenario. In order to clearly illustrate the sequence error vulnerability that is caused by route switching among mismatched channels, a reasonable 0.3 second propagation delay differential was introduced between the DSCSIII and CA links. The C2P node in the simulated scenario is designed to generate TADIL messages at an average data rate of 1500 bps. This reflects a fairly low aggregate data rate, and is selected in order to study the network under little or no buffering conditions, reflecting a best-case scenario study. In this scenario, the TADIL traffic is assigned to a single QoS traffic class. The TADIL traffic class is given the highest priority among all other ADNS traffic classes, where it immediately preempts all other traffic types for buffer resources and queue scheduling. This PHB is assigned to TADIL traffic in order to illustrate that even the best Quality of Service (QoS) assignment may result in messages received out of order under the link conditions in this study. The TADIL traffic uses the User Datagram Protocol (UDP) connection protocol, reflecting the current planned implementation. Background ADNS traffic is injected into this scenario that represents traffic from other services. However the relatively low priority that is assigned to this traffic causes it to have little or no impact on the simulation results.

Under normal operation of this network, the OSPF routing protocol would select the CA link as the optimal route to the shore terminal and the network would continue to operate with no sequence errors. However the situation that this simulation study investigates is the case where the CA link fades in and out of operation. This forces the routing protocol to select an alternate path (in this case, the DSCSIII link) when the CA link is inoperable. As the CA link comes back online, it is eventually reselected by OSPF as a faster link, causing a vulnerability to message sequence errors. The simulation was configured to execute for ten minutes of simulated time. CA link failures were forced at random times and lasted about 2 minutes each.

2.1.2. Results

Results for the simulation are shown in Figure 2-2.
periods of failure that occurred for the CA link. Each of the out-of-order messages was received a short time after the failed CA link became operable. This suggests a vulnerability period for this ADNS configuration, where the system is vulnerable to producing sequence errors if it receives multiple consecutive packets during this time. Figure 2-2 shows the throughput on the two links that were shared by OSPF. The primary link in the figure is the CA link, and the secondary link is the DSCSIII link. For ease of viewing, regular OSPF link state updates and non-TADIL ADNS traffic are not included in this chart.

Failures occur when the primary link throughput drops to zero. The figure highlights the four vulnerability periods that occurred when the primary link was activated and selected as the new best link by the OSPF routing protocol.

2.2. General Loadsharing

Current implementations of ADNS that utilize OSPF only send data over one channel at any given time, leaving the remaining links idle. Future ADNS upgrades have considered implementing some form of loadsharing across SATCOM links in order to make more efficient use of the aggregate available bandwidth [10]. Loadsharing would operate in conjunction with QoS, allowing the ship-to-shore reachback hop to be viewed as a single channel and still allow QoS PHBs at the channel interface.

The previous study highlighted the dangers of dynamically utilizing different SATCOM links by the routing protocol. Loadsharing switches transmissions among different links in order to balance traffic flows. In both cases, transmitting over links of different channel characteristics may cause messages to arrive out-of-order at the destination.

There are different loadsharing implementations that are currently under investigation. This study investigates a general loadsharing algorithm that primarily seeks to balance loading across the ADNS SATCOM links and is unconcerned with packet sequence errors. The study that follows in Section 2.3 examines a loadsharing/routing protocol that is currently under consideration for future ADNS upgrades, the Enhanced Interior Gateway Routing Protocol (EIGRP) [11]. This protocol seeks to reduce packet sequence errors by only selecting well matched links at the cost of load balancing performance. Both protocols implement packet-level loadsharing. Future investigations into session and flow-level loadsharing may also decrease the chances of message sequence errors.

2.2.1 Simulated Topology and Configuration

The simulated topology and configuration was, for the most part, the same as the topology and configuration defined in Section 2.1.1. However in this simulation no link failures were simulated. Equal propagation delays were assigned to all SATCOM links. The C2P generated the same level of traffic with the same highest priority QoS.

A generic loadsharing algorithm was implemented that distributed traffic across each link proportional to its capacity.

2.2.2. Results

Results for this simulation are shown in below:

![Figure 2-3. Generic Loadsharing Traffic Distribution](image)

Figure 2-3 reflects excellent performance of the loadsharing algorithm with respect to load balancing. As expected, most of the traffic is routed through the higher data rate CA and DSCSIII links, with little traffic routed on the lower data rate UHF and EHF links.

![Figure 2-4. Generic Loadsharing Sequence Errors](image)

Figure 2-4 shows that 2.3% of all of the TADIL messages that were sent through ADNS were received out of sequence. In addition, the figure shows that all of the
sequence errors resulted from TADIL messages being sent through the low data rate UHF and EHF links. This suggests a potential loadsharing solution that ignores links with very different channel characteristics. This is investigated in the next section.

2.3. EIGRP Loadsharing
EIGRP is currently under investigation as an alternate routing protocol to OSPF for ADNS. EIGRP implements a limited form of loadsharing where it only balances data across links with relatively well matched channel characteristics. This would result in less of a likelihood of packet sequence errors at the cost of poorer aggregate bandwidth utilization efficiency. This study compares the use of EIGRP to the generic loadsharing algorithm in Section 2.2 with respect to load balancing performance and message sequence errors. It also highlights the failure of EIGRP to completely eliminate the probability of TADIL message sequence errors in ADNS.

2.3.1. Simulated Topology and Configuration
Two simulations were performed in this study. The first simulation was identical in topology and configuration to the previous study in Section 2.2.1. However this simulation utilizes the EIGRP routing protocol in place of OSPF and a generic loadsharing algorithm. Once again, the TADIL traffic was placed in a single highest priority traffic class for this simulation.

The second simulation was conducted based on the successful results of the first experiment. The use of EIGRP in the first experiment eliminated all of the packet sequence errors that were observed in the simulation in Section 2.2. For this simulation, the TADIL packet generation characteristics were changed from one packet every 0.2 seconds to two sequential packets every 0.4 seconds. This change did not affect the overall 1500 bps aggregate TADIL traffic data rate. However this change permitted the detailed study of EIGRP message sequence error performance under more adverse conditions.

2.3.2. Results
The results of the first simulation are shown below.

Comparing Figure 2-5 to Figure 2-3 shows that EIGRP performs relatively poorly with respect to load balancing across asymmetric links. None of the lower data rate links were utilized at all to transmit traffic, and the DSCS and CA links were loaded with traffic levels disproportionate to their respective capacities. However no message sequence errors occurred throughout the entire simulation. As a result, a second simulation was executed that transmitted sequential TADIL messages closer together to increase the likelihood of sequence errors, even on links with relatively well matched channel characteristics.

Results from the second simulation are shown in Figure 2-6.

Figure 2-6. EIGRP Sequence Errors

Figure 2-6 shows the total number of TADIL messages that were received by the destination C2P during the course of the simulation. The figure shows that 12.9% of all messages that were sent were received out of order. In addition, the figure shows that the sequence errors occurred with a fairly constant frequency. They did not occur only during select vulnerability periods as observed in the study in Section 2.1. This was a common characteristic to both of the loadsharing approaches in Section 2.2 and 2.3.

2.4. Multiple TADIL Traffic Classes
The previous three simulation studies have assumed that the TADIL traffic will be assigned to a single, high priority traffic class. However there have been some recent investigations into creating multiple DiffServ QoS traffic classes and PHBs for different types of TADIL traffic. The intent of this study is to examine the cases where differing traffic classes and PHBs may cause message sequence errors and to highlight the need for caution and thorough investigation when assigning TADIL message types to different QoS Type of Service (ToS) classes.

2.4.1. Simulated Topology and Configuration
This simulation utilizes the same topology and configuration as in Section 2.2.1. However no loadsharing
is implemented and message routes are static during the course of the simulation. Two TADIL messages are generated by the C2P every 0.4 seconds. The first of the two messages is assigned to the Background ToS. The second message is assigned to a different ToS for each simulation execution. Non-TADIL traffic from ADNS is not simulated during this experiment. The focus of this study is on sequence errors within the TADIL traffic classes only. Additional sequence errors would occur if messages from other IP services were grouped into TADIL traffic classes. This study examines the ideal case. The simulated QoS algorithm implements a set of standard Weighted Fair Queuing (WFQ) based traffic classes and PHBs.

2.4.2. Results

Results for the simulation are shown below.

![Figure 2-7. TADIL QoS Traffic Sequence Errors](image)

Figure 2-7 summarizes the results of 7 simulation executions. Each simulation execution utilized a different ToS for the second of the two generated messages. The figure shows that up to 2.1% of all messages sent to a destination C2P were received out of order and that the error percentage varied according to the ToS assignment. The only simulation execution that resulted in 0% message sequence errors was when the second message was set to the Background ToS, which is the same ToS as the first message. These results suggest that it is important to assign different TADIL message types to the same ToS class when the information from each message type is related. For example, fire message types should be in the same traffic class as hold fire message types since their received sequence order is very important.

REFERENCES

The following references were used in this report.

[1] Alberts, David S.; Garstka, John J.; Stein, Frederick P. *Network Centric Warfare*


