Toward Consolidated Tactical Network Architecture: A Modeling and Simulation Study

Andy S. Peng*‡, Brian R. Eickhoff*, Tian He†, David J. Lilja‡

*Tactical Systems, Maritime Systems and Sensors (MS2), Lockheed Martin, Eagan, MN
†Department of Computer Science and Engineering, University of Minnesota, Minneapolis, MN
‡Department of Electrical and Computer Engineering, University of Minnesota, Minneapolis, MN
{andy.s.peng, brian.eickhoff}@lmco.com, tianhe@cs.umn.edu, lilja@umn.edu

***Abstract*—A consolidated tactical network architecture provides an integrated shipboard local area network infrastructure for disparate afloat platforms operating with multiple security level enclaves. In this modeling and simulation study, a simulated network test bed is developed to investigate the performance trade-offs in a consolidated tactical network architecture. A baseline network traffic profile is defined in this study. Failover and traffic growth test scenarios are presented to study the performance of tactical applications under these network conditions. The results show that network traffic is redirected properly during failover conditions. The results also show that performance of the applications are scaled according to the network traffic growth.**

***Index Terms*—CANES, Network Simulation, OPNET, Performance Evaluation, Tactical Network, Simulation Models, Service Oriented Architecture.**

I. Introduction

The U.S. Navy has developed a plan to revolutionize the future of its fleets' communication and networking capabilities by consolidating all shipboard network-centric communication systems to a common architecture known as Consolidated Afloat Networks and Enterprise Services (CANES) [1] [2] [3] [4]. CANES implements a Common Computing Environment (CCE), which includes an integrated Local Area Network (LAN) infrastructure for disparate afloat platforms operating with multiple security level enclaves [4]. The operational view of the afloat networks in Fig. 1 illustrates that CANES interfaces with Automated Digital Network System (ADNS)[1] to provide end-to-end (ETE) network services across the Global Information Grid (GIG). Inspired by the concept of Service Oriented Architecture (SOA), CANES consists of loosely coupled hardware devices capable of hosting a wide variety of tactical applications. The design of the hardware architecture utilizes open architecture Commercial-Off-The-Shelf (COTS) products which are modular and scalable. The core services are comprised of reusable software applications that can be efficiently adapted to support rapidly changing demands in a wide range of tactical operations.

In the traditional system-centric design paradigm, each type of tactical communication system was designed to support a single warfighting function [4]. This design paradigm created many stove-piped systems, each developed in isolation and without considering the requirements for interoperability with existing and future technologies. A stove-piped system typically requires an unique set of hardware devices, software applications, and a distinct network infrastructure. Depending on its application, the system is often inefficiently utilizing the available processing resources. The development of the software applications is based upon the specific hardware architecture of the host. In addition, as the demands for network capability increase, the total number of required stove-piped systems can potentially grow into an unmanageable state for both operations and maintenance staff. It also increases the complexity of system integration, training, and supportability [4]. From a security perspective, these individual networks are difficult to certify and defend against potential network attacks [2]. A consolidated tactical network architecture has the advantage of reduced total system component count, and furthermore has the ability to mitigate the risks incurred with integrating many stove-piped systems. The future shipboard network-centric communication systems developed around the common computing architecture will require less power, smaller rack space, lighter weight, and lower overall cost in system development and maintenance.

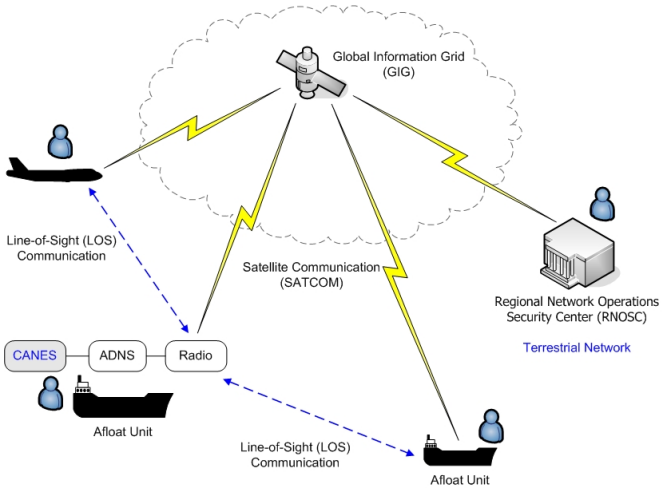


Fig. 1. Operational View of Afloat Networks

The objective of this study is to develop a simulated network test bed using OPNET Modeler for the performance evaluation

[1]ADNS interfaces with shipboard radio equipments to provide wide area network (WAN) connectivity for the afloat platforms [5].

978-1-4244-2677-5/08/$25.00 ©2008 IEEE

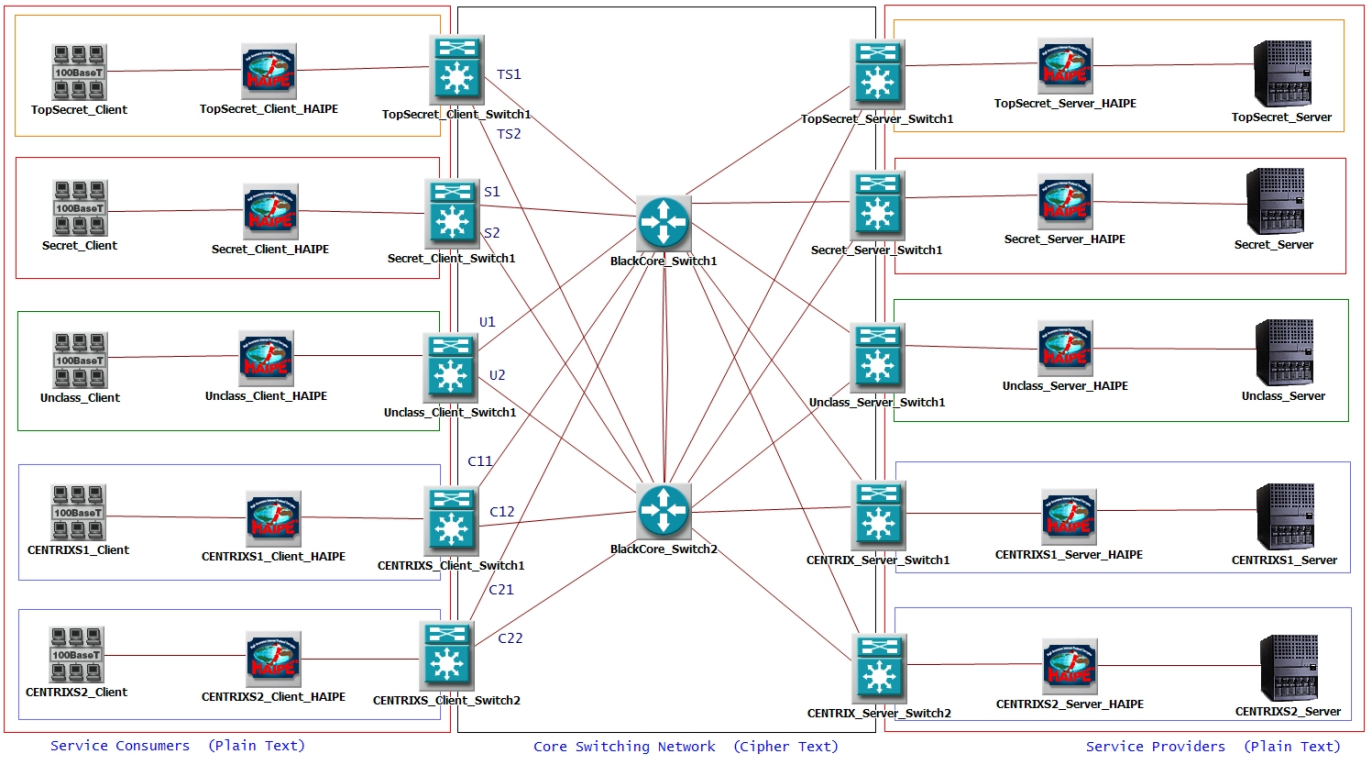


Fig. 2. Consolidated Network Test Bed Architecture

of a consolidated tactical network architecture. The performance statistics were collected from the test bed to investigate the performance trade-offs under various operational scenarios in a consolidated tactical network architecture.

The remaining portion of this paper is structured as follows. Section II describes the configuration of the network test bed architecture including network topology, encryption device model, network traffic generation, and performance statistics. Section III formulates simulation scenarios for the performance evaluation. Section IV discusses the simulation results and findings. Section V concludes this investigation and provides recommendations for future work.

II. Network Test Bed Configuration

A simulated network test bed based on COTS products is developed to represent a consolidated network architecture. As illustrated in Fig. 2, the network test bed incorporates multiple security level enclaves to model a consolidated LAN infrastructure on a typical tactical afloat platform. Each security level enclave is modeled with a LAN client entity and a respective service provider. This network test bed serves as the baseline architecture for each test scenario in Section III.

A. Network Topology

The topology of the consolidated network architecture is illustrated in Fig. 2. The network supports users from multiple security levels, including *Top Secret*, *Secret*, *Unclassified* and *CENTRIXS*[2] enclaves. All security level enclaves are joined together at the core switching network. The core switching network has the provision for network redundancy to prevent service interruption from potential link or node failures. All network components are interconnected with 100BaseT Ethernet links. The links joining the two core switching devices are configured as trunk ports to prevent any service interruption due to failures. Since the High Assurance Internet Protocol Encryptor (HAIPE) model currently only supports Routing Information Protocol (RIP), the nodes connected to the HAIPE models are configured to use RIP protocol. The core switching network is configured with Open Shortest Path First protocol (OSPF).

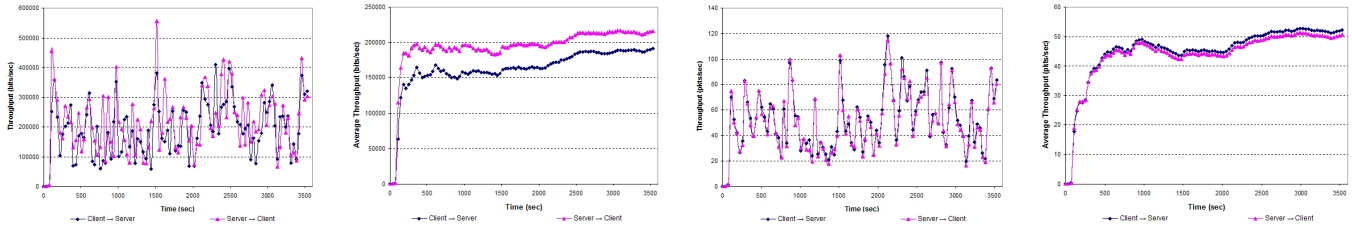
[2]Combined Enterprise Regional Information Exchange System (CENTRIXS) is a secure network for coalition interoperability.

B. Encryption Device

Tactical networks regularly rely on Internet Protocol (IP) encryption devices to ensure that data is securely transported. HAIPE is a Type 1 encryption device that complies with National Security Agency (NSA) security requirements. In a consolidated network architecture with multiple levels of security, each security enclave requires peering HAIPE devices to provide the secure end-to-end data delivery. When the security association policies are configured in the peering HAIPE devices, a secure network tunnel is created in the cipher-text network in order to maintain the data separation between security enclaves. The network test bed is configured such that data can only be sent and received within its respective security enclave. Plain-text data packets are encrypted by a HAIPE device before being injected into the cipher-text only core switching network. The data packets are decrypted by the peering HAIPE device before being forwarded to a destination

TABLE I
CONFIGURATION OF MIXED APPLICATIONS [5] [6] [7] [8]

Service Classes	Applications	Attributes	Setting	PHB / DSCP
Control & Management	Remote Login	Inter-Command (sec)	normal(60,5)	CS5 / 40
		Terminal Traffic (bytes/command)	normal(20,16)	
		Host Traffic (bytes/command)	normal(10,11.111)	
Inelastic Real-Time	Voice	Encoder Scheme	G.723.1 5.3K	EF / 47
		Voice Frame per Packet	1	
		Compression Delay (sec)	0.02	
		Decompression Delay (sec)	0.02	
		Conversation Environment	Land Phone - Quiet Room	
	Video	Frame Inter-arrival Time Information	15 frames/sec	AF43 / 38
		Frame Size Information (bytes)	Incoming Stream Frame Size = constant(1066) Outgoing Stream Frame Size = constant(1066)	
Preferred Elastic	HTTP	HTTP Specification	HTTP 1.1	AF23 / 22
		Packet Inter-arrival Time (sec)	constant(10)	
		Page Properties	Object size (bytes) = constant(1000) Objects/Page = constant(1) Medium Image = constant(7)	
	FTP	Command Mix (Get/Total)	50%	AF13 / 14
		Inter-Request Time (sec)	exponential(80)	
		File Size	constant(200000)	
Elastic	E-mail	Send Interarrival Time	exponential(24)	BE / 0
		Send Group Size	exponential(24)	
		Received Inter-arrival Time	constant(1)	
		Received Group Size	exponential(24)	
		E-Mail Size (bytes)	constant(6000)	



(a) Throughput (bits/sec) (b) Average Throughput (bits/sec) (c) Throughput (pkts/sec) (d) Average Throughput (pkts/sec)

Fig. 3. Characteristics of Mixed Application

with the same security classification level as the source. Since all data passes through peering encryption devices, the HAIPE model affects the overall throughput and packet latency in the network architecture.

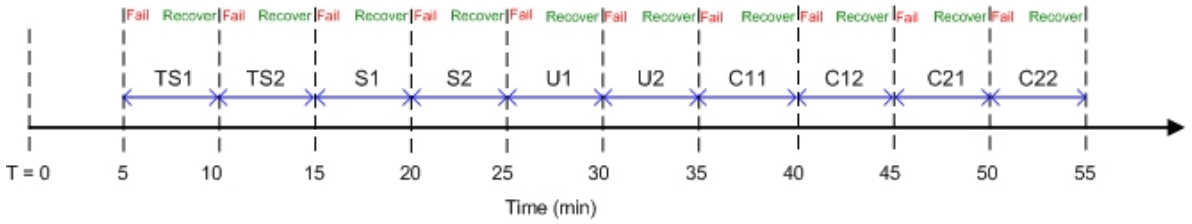
C. Service Classes (Network Traffic Generation)

Network traffic models are typically derived from the output of a dynamic stochastic processes (*i.e.,* random) which require challenging modeling techniques. OPNET Modeler provides a convenient solution to represent standard applications such as *Database Query*, *E-mail*, *FTP*, *HTTP*, *Remote Login*, *Telnet*, *Video*, *Voice* and other custom applications in its application configuration model [6]. Various network traffic behaviors can be modeled by adjusting application parameters such as object size, request inter-arrival time, packet distributions, start/end times, duration, repeatability, and others. Before investigating the performance statistics of various simulation scenarios, it is important to construct a common network traffic profile representing the behavior of the actual network applications and to understand its basic characteristics. This study assumes the configuration of mixed applications as shown in Table I, which includes four major service classes commonly used in tactical applications. The control and management class typically consumes very low network bandwidth with near-constant login or polling of the system status. It is important to ensure the control and management packets are delivered on time and with low packet loss. The inelastic real-time, preferred elastic, and elastic traffic have low, medium, and high tolerance, respectively, in term of packet loss, delay, and jitter parameters. Fig. 3 illustrates the network traffic throughput of the mixed applications used in this study. The asymmetric network traffic throughput in both directions shows that there is more network traffic from a server to a client due to FTP downloading.

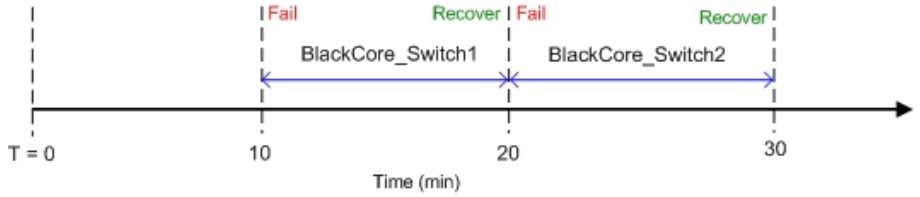
D. Performance Statistics

OPNET Modeler provides built-in performance statistics collection that supports both global and local statistics [6]. Global statistics illustrate the overall performance characteristics of a network scenario. Local statistics provide performance data for particular objects such as nodes, links, and modules. Common performance parameters such as *throughput*, *delay*, *delay variation* (*i.e., jitter*), and *packet loss* are included in the performance statistics collection. These performance parameters are briefly discussed herein.

The channel capacity of a network connection can be



(a) Failover Links Timing Diagram



(b) Failover Nodes Timing Diagram

Fig. 4. Timing Diagram for Failover Scenarios

characterized by the throughput parameter. Throughput may be unidirectional and is defined as the average rate that data is being successfully sent or received over a fixed time interval. It is typically rated in terms of bits-per-second (*bits/sec*) or packets-per-second (*pkt/sec*).

$$Throughput_{(sent/received)} = \frac{\sum Data_{(sent/received)}}{Time}$$

The latency of an IP network is measured by the delay parameter. Typically, ETE delay is a critical parameter for studying the performance of time-sensitive applications such as video and voice applications. The ETE delay is the elapsed time for a packet traveling from a source to a destination. In an IP network, the ETE delay can be further divided into time intervals taken in various stages such as processing, queuing, transmission, and propagation. Processing delay is the total computing time required to assemble and disassemble a network packet. Queuing delay refers to the waiting and servicing time in a queuing buffer. Transmission delay is the required time interval for pushing all data bits in a packet onto the physical connection (*e.g.,* wired Ethernet or wireless IEEE 802.11). Propagation delay refers to the elapsed time that a packet is in transit on the physical connection.

$$\begin{aligned} Delay_{(ETE)} &= Time_{(destination)} - Time_{(source)} \\ &= Delay_{(processing)} + Delay_{(queuing)} \\ &+ Delay_{(transmission)} + Delay_{(propagation)} \end{aligned}$$

Packet delay variation (v_k or ${\sigma_k}^2$) is sometimes loosely defined as "jitter", which is the difference between an absolute packet delay time (d_k) and a predefined reference packet delay time (d_{ref}) [9]. A predefined reference packet delay time must be a selected value which maintains an acceptable quality of service (QoS) for the particular application. The average packet delay ($\bar{d}$) in the same network connection flow can sometimes be used as a reference packet delay time. This parameter greatly affects the quality of the real-time applications such as video and voice services.

$$v_k = d_k - d_{ref}$$

Or,

$$\sigma = \sqrt{{\sigma_1}^2 + {\sigma_2}^2 + \ldots + {\sigma_n}^2} = \sqrt{v_1 + v_2 + \ldots + v_n}$$

$$\sigma_k = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(d_i - \bar{d})^2} \quad , \quad \bar{d} = \frac{1}{n}\sum_{i=1}^{n} d_i$$

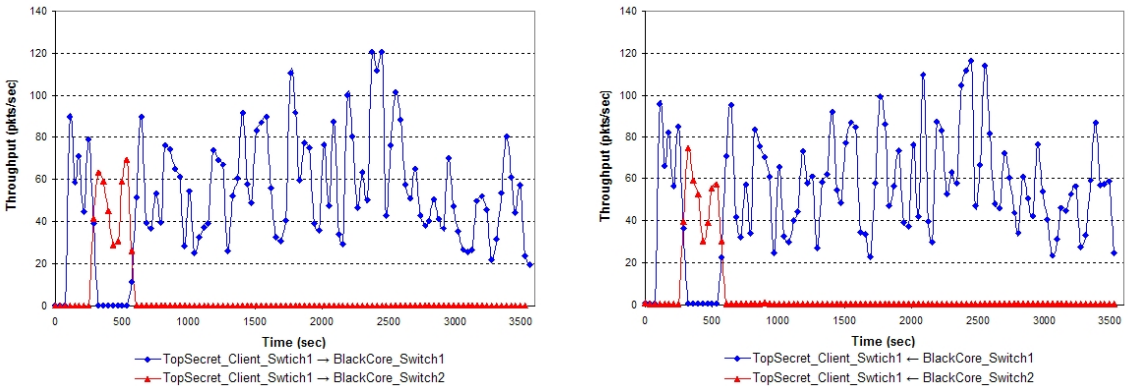
Packet loss is the number of packets that fail to reach their destinations in a timely manner. Packet loss frequently occurs under congested network conditions, as the packets are dropped when the queuing buffers in the network devices are overflowed. Packet loss ratio illustrates the likelihood of packets not being delivered successfully in a network. In order to maintain the desirable efficiency of the applications, packet loss must be minimized in a network architecture.

$$PacketLoss_{ratio} = \frac{\sum Packets_{(lost)}}{\sum Packets_{(transmitted)}}$$

III. Performance Evaluation

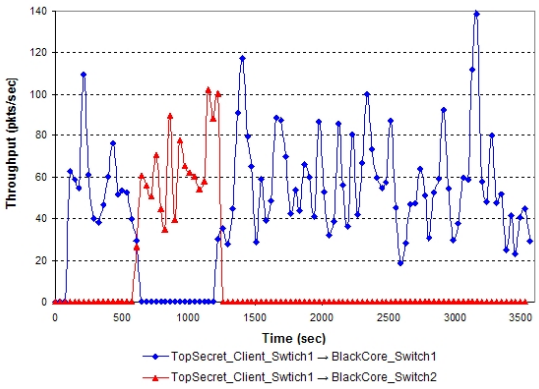
Failover and traffic growth test scenarios were developed based on the previously described network test bed architecture to investigate the behavior of the network traffic and the effect on the mixed applications performance, respectively. Failover minimizes service interruption by switching over to a redundant system upon failure(s) in the network architecture. A sufficient number of redundant components must be implemented in the consolidated network architecture in order to fulfill various failover conditions.

In addition to failover requirements, it is very important to understand the behavior of the mixed applications as the network traffic growth is scaled to utilize more link bandwidth. The results of the traffic growth scenario guide the

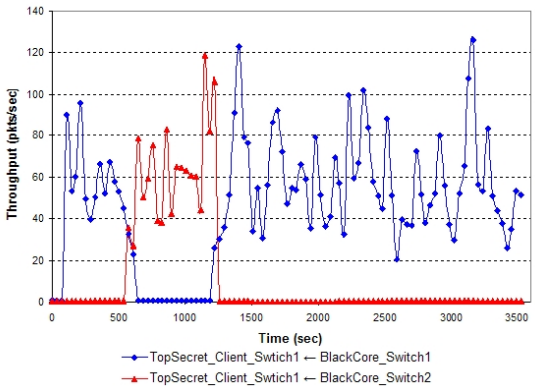


(a) Failover Links (Client → Server)

(b) Failover Links (Client ← Server)



(c) Failover Nodes (Client → Server)



(d) Failover Nodes (Client ← Server)

Fig. 5. Failover Scenario Results

investigation of application performance under high bandwidth utilization. Thus, appropriate techniques such as QoS policies can be applied to improve the performance of the network architecture.

A. Failover Test Scenarios

Network failures are commonly caused by link-down or node-down conditions. The failover scenarios in this study were developed as an attempt to understand the behavior of the network traffic under failover conditions. In other words, "How does the consolidated network architecture behave during failover conditions?"

1) Effects of Failover Links: In this test scenario, each Ethernet link connecting the client-side switches to the core switches are configured to fail for a fixed time interval during the simulation run. The labels of all network links are from the consolidated network test bed architecture shown in Fig. 2. During the initial five minutes, all network links connecting to both core switches are operational. The network links then undergo failure and recovery modes according to the link failure/recovery timing diagram shown in Fig. 4(a). Each network link fails sequentially at a specific time. The duration of each link failure is set to five minutes. Once a network link is recovered, it remains operational until the end of the simulation.

2) Effects of Failover Nodes: Similar to the failover links scenario, the failover nodes scenario follows a predefined node failure/recovery timing diagram shown in Fig. 4(b). Both core switches are operational during the initial 10 minutes of the simulation time. The *Blackcore_Switch1* fails at $T = 10$ minutes and then recovers at $T = 20$ minutes. At that time, the *Blackcore_Switch2* enters the failure mode and then recovers later at $T = 30$ minutes. Upon recovery of a core switch, it remains operational until the end of the simulation.

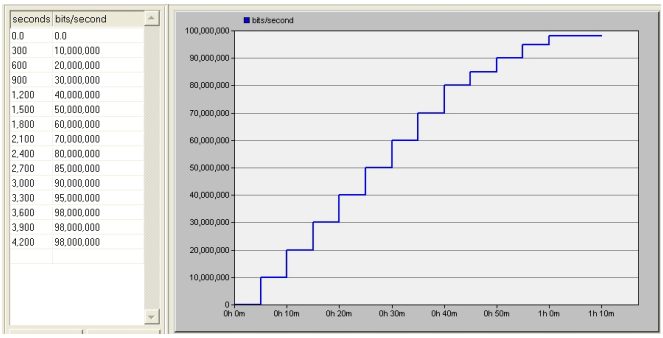


Fig. 6. Background Traffic Profile for Traffic Growth Scenario

(a) Throughput (bits/sec)

(b) Throughput (pkts/sec)

Fig. 7. Throughput for the Traffic Growth Scenario

B. *Traffic Growth Test Scenario*

A network traffic profile of the background load is configured in order to investigate the application performance as a function of the network traffic growth. Fig. 6 illustrates a predefined network traffic profile for loading the background traffic. This profile gradually increases the background load every five minutes until reaching 98 Mbps, which nearly utilizes most of the 100BaseT Ethernet link bandwidth. This scenario is an attempt to understand what happens to the performance statistics at the application layer when the background network traffic loads are gradually increased.

IV. Results and Discussion

The test results of the failover scenarios are presented in Fig. 5. The test results were taken from a single enclave since all security level enclaves are symmetrical in the network test bed architecture. As a natural behavior of the routing protocol, the network traffic is redirected to the destination through an alternative path. This effect is illustrated in both failover scenarios. The results of the failover links scenario in Fig. 5(a) and 5(b) show that primary link *TS1* transports the data packets in the enclave under normal operating conditions. Upon failure of the *TS1* link, the network traffic is rerouted through the secondary link *TS2*. The test results show that it takes less than one minute for the secondary link *TS2* to take over the network traffic load from the primary link *TS1* and vice versa. Since the packets are not configured to be distributed across both links, both Fig. 5(a) and 5(b) show that failure in the secondary link *TS2* has no effect in the network traffic throughput.

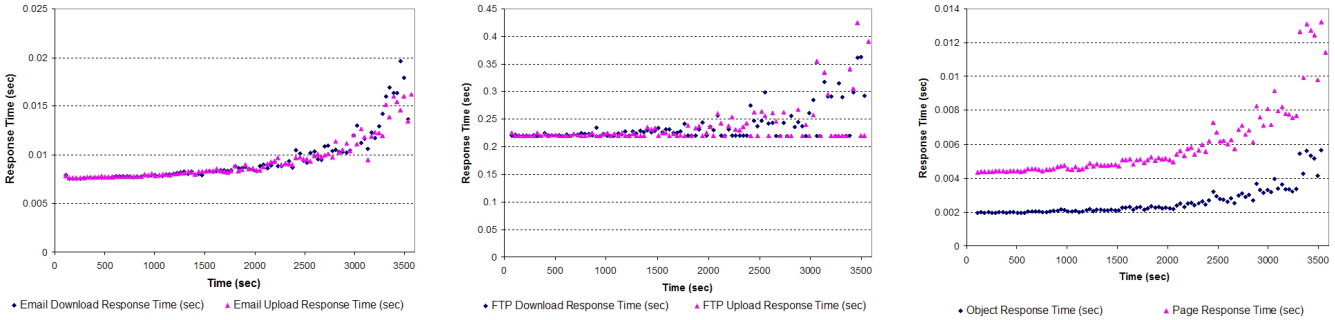
The results of the failover nodes scenario are illustrated in Fig. 5(c) and Fig. 5(d). As expected, the results show similar traffic behavior as in the failover links scenario. In the failover nodes scenario, *Blackcore_Switch1* is the primary node and *Blackcore_Switch2* is the secondary node. The network traffic is redirected through *Blackcore_Switch2* during the failure mode of *Blackcore_Switch1* from $T = 10$ minutes to $T = 20$ minutes. The results show that it takes less than one minute to redirect all network traffic through the secondary core switch.

Both Fig. 7 and Fig. 8 summarize the results of the traffic growth scenario. Fig. 7 illustrates the expected behavior such that the throughput is increasing according to the predefined background load shown in Fig. 6. The summary of mixed applications in Fig. 8 shows that the response time for E-mail, FTP, and HTTP applications scale up as the background load increases the bandwidth of the network links. Application response time remains steady until 60 Mbps (or 60%) of the link bandwidth is utilized. Beyond this threshold, the response time and delay time experience greater increases as a function of the background traffic load. This performance data creates a baseline to determine if QoS policies are required in the consolidated network architecture to maintain service-level requirements.

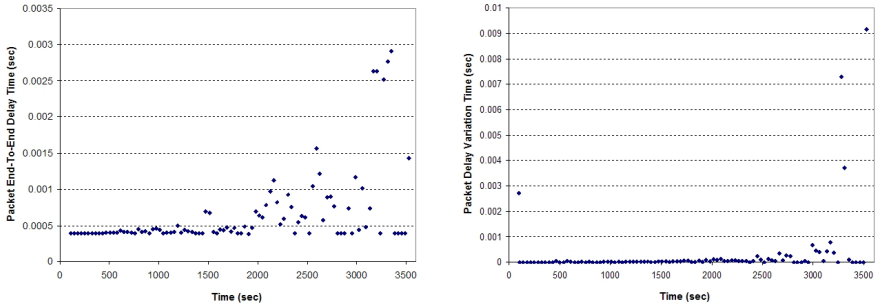
V. Conclusion

The main contribution of this study is the development of a network test bed architecture using OPNET Modeler to simulate a consolidated network architecture. Test scenarios such as the failover scenario and traffic growth scenario were developed to baseline performance for further investigation of other aspects of the network architecture. The test results show that failover requirements can be fulfilled by implementing redundant systems with a routing protocol enabled. The test results also show that response times for mixed applications degrade quickly after 60% of the link bandwidth has been utilized. These performance statistics were collected to provide valuable insights which will aid the developement of future tactical network architectures.

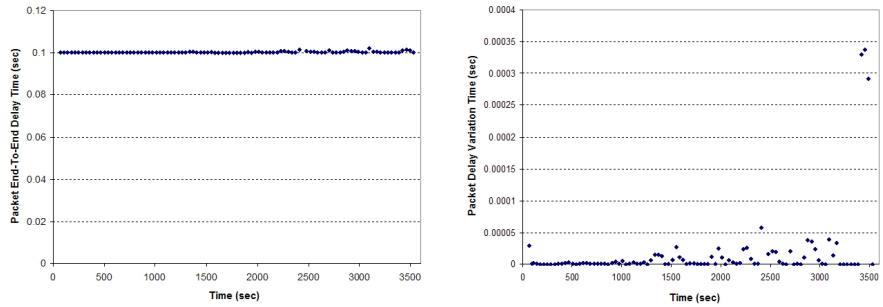
Future works include QoS study, network topology study, performance study with other COTS products and cross-domain related scenarios. The network test bed can also be combined with ADNS and radio communication systems to further evaluate ETE performance across the GIG. Furthermore, validation of the results may be required to increase the credibility of the simulation results.



(a) Email Response Time (b) FTP Response Time (c) HTTP Response Time



(d) Video Packet ETE Delay Time (e) Video Packet Delay Variation



(f) Voice Packet ETE Delay Time (g) Voice Packet ETE Delay Variation

Fig. 8. Summary of Mixed Applications Performance

ACKNOWLEDGMENT

The authors are grateful to numerous colleagues at Lockheed Martin, MS2 and the University of Minnesota for reviewing the technical content and providing feedback on this paper. They also thank anonymous reviewers for providing comments to improve the overall quality of this paper.

DISCLAIMER

The security classification labels used in this paper are for discussion purposes only. The opinions, recommendations, results, conclusions, and findings in this paper do not necessarily reflect the official views and positions of Lockheed Martin Corporation.

REFERENCES

[1] D. Washburn. (2007, Oct.) Networks, Information Assurance and Enterprise Services (PMW160). Delores Washburn presentation.pdf. [Online]. Available: http://129.7.151.14/Home/DoDconferencepresentations/

[2] C. Miller. (2007, Oct.) Navy C4I Open Architecture Strategy. [Online]. Available: https://www.softwaretechnews.com/stn_view.php?stn_id=43&article_id=89

[3] PEO C4I. (2007, Jul.) Consolidated Afloat Network and Enterprise Services (CANES) Industry Day. CANESINDUSTRYDAY20-7-27-07.pdf.

[4] P. Turner. (2007, Dec.) The CANES Initiative: Bringing the Navy Warfighter onto the Global Information Grid. CANES.pdf. [Online]. Available: www.chips.navy.mil/archives/07_Dec/PDF/

[5] A. Peng and D. Lilja, "Performance Evaluation of Navy's Tactical Network using OPNET," in *IEEE Military Communication Conference*, Washington, D.C., Oct.23-25 2006, pp. 1–7.

[6] "OPNET Model User Guide," Version 14.5, OPNET, 2008.

[7] C. Christou, W. Hall, and K. Sheu, "Applying Service Class Treatment Aggregates to the Global Information Grid (GIG)," in *IEEE Military Communication Conference*, Washington, D.C., Oct.23-25 2006, pp. 1–5.

[8] (2006, Aug.) Global Information Grid Net-Centric Implementation Document: Quality of Service (T300).

[9] B. Doshi, P. Kim, B. Liebowitz, K. I. Park, and S. Wang, "Service Level Agreements and QoS Delivery in Mission Oriented Networks," in *MITRE Corporation*, May 2006.