Naval Task Force Interface for Coalition Networks for Secure Information Sharing (CoNSIS)

Tuan Nguyen, Steven Lam, Ceasar Castro, Roger Ogden, Cam Tran, Albert Legaspi
SPAWAR Systems Center Pacific, San Diego, CA 92152

Abstract — **Merging IP routing and mobile communication poses many challenges especially for a dynamic, heterogeneous networking environment such as a Naval Task Force. In this paper, we present an effort to design, develop, test and demonstrate an interoperable coalition interface for a Naval Task Force for the four-nation Coalition Networks for Secure Information Sharing (CoNSIS) project. A field experimentation has been performed between the four CoNSIS nations with the separate national sites being connected via the Internet. The key architectural objective of the United States (US) is to support tactical coalition networks of the other nations. The routing architecture is based on Open Shortest Path First Version 3 (OSPFv3) in conjunction with two main features, namely (1) IPv6 address auto configuration enabled on mobile links to alleviate administrative burden, and (2) Address Family (AF) support to allow IPv4 traffic to be passed via IPv6 backbone. In addition, Point-to-Point Protocol over Ethernet (PPPoE) with Flow Credit and Link Metric extensions is used to provide mobile networks via point-to-multipoint links with support for Quality of Service (QoS). Furthermore, link encryptors secure the network, which make use of Dynamic Discovery mechanisms to determine remote routing endpoints.**

Keywords **CoNSIS, IM-PEPD, MANET, Naval Task Force, OSPFv3, IPv4, IPv6, address auto configuration, PPPoE, QoS, Dynamic Peer Discovery**

I. INTRODUCTION

Secure information sharing is the principal tenet of a coalition network. As networks evolve, more and more mobile ad hoc components are incorporated with challenging issues surfaced when merging IP routing and mobile radio communications. Router-to-radio interface implementation for airborne network was carried out in [1], and considerations for tactical networks have been studied (for examples, [2-3]). This paper focuses on the design of a tactical network that has a standard router to radio interface that supports QoS via a mobile ad hoc network using RFC 5578 Point-to-Point Protocol over Ethernet (PPPoE) Enhancements for credit-based session flow control and session-based link quality metric feedback for router-to-radio interface [4-6]. OSPFv3 is used as the routing protocol. The remainder of this paper is structured as follows. Section II provides a brief overview of the Coalition Networks for Secure Information Sharing (CoNSIS) project, and the main contribution of the United States (US) that is responsible for the Naval Task Force and the corresponding testbed. This paper presents only the initial testing of the testbed, representing the Naval Task Force part of the CoNSIS network.

In Section III, we describe the details of the Naval Task Force under CoNSIS, including network architecture, network features, and testbed. Test results and analysis are presented in Section IV, and a summary of the paper is in Section V. Finally, Section VI concludes the paper with an outline of areas for potential future work.

II. OVERVIEW OF COALITION NETWORKS FOR SECURE INFORMATION SHARING

The CoNSIS project is the product of a Memorandum of Understanding (MOU) among France, Germany, Norway, and the United States. The US part is jointly funded by the Office of Naval Research, Code 31 (under the Communications and Networking Program), and the Naval International Programs Office (NIPO).

The objectives of CoNSIS are to develop, implement, test, and demonstrate technologies and methods that will facilitate the participants' abilities to share information and services securely in ad hoc coalitions, and between military and civilian communications systems, within the communications constraints of mobile tactical forces. Tests, evaluations, and demonstrations are carried out to provide feedback toward a final common technical architecture serving as a basis for implementation in national and coalition systems to promote interoperability.

As stipulated in the MOU, participants utilize, to the maximum extent possible, commercial standards to minimize interoperability difficulties. Only elements of the open architecture that are not available from the open market are investigated for potential development.

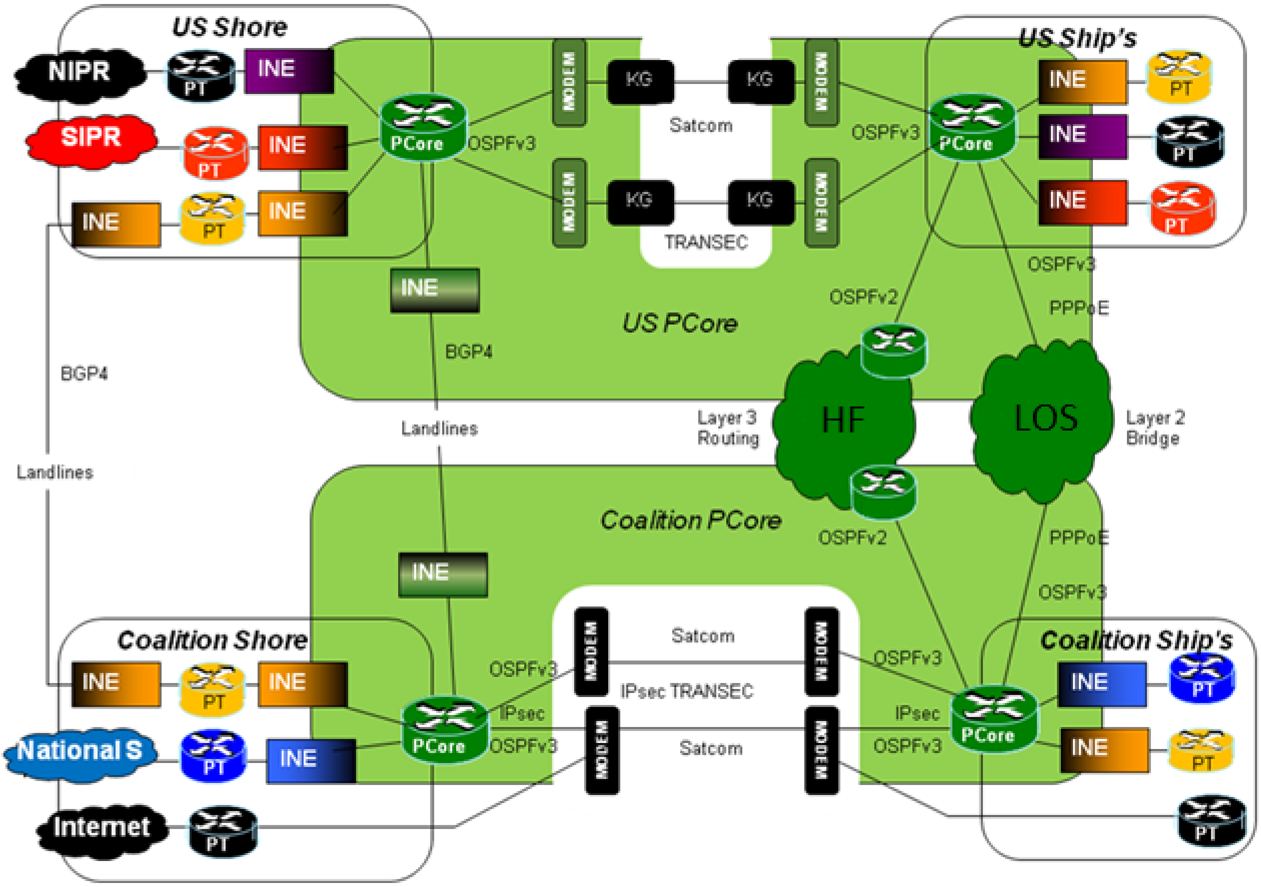

Figure 1. Typical Protected Core Architecture

The US participants were responsible for the Naval Task Force network architecture, test and demonstration under the CoNSIS project. This task encompasses exploring, specifying, and demonstrating mechanisms to support the Naval Task Force and associated testbed for secure information sharing among coalition and contingent non-governmental organization (NGO) partners. The task also sets forth the underlying framework for naval mobile ad hoc networking (MANET) in Naval tactical networks.

III. Naval Task Force

The CoNSIS Naval Task Force network architecture, network features, and testbed are described in this section.

A. Network Architecture

The experimentation network architecture, named Protected Core Architecture, consists of two Protected Cores (PCores), one designated for the US and the other for the Coalition. Each ship has point-to-point satellite links to a respective shore node corresponding to its PCore and is typically interlinked by line-of-sight (LOS) links that can be either using a Layer-2 bridge or a High Frequency (HF) radio using Layer-3 routing. The principal architectural objective is to make the interface radio-agnostic so that any radio can be integrated into the network. Figure 1 depicts the idealized overall network architecture designed to support Naval Task Force for CoNSIS. An INE is an In-line Network Encryptor. Landlines connect the US national shore station to that of a coalition nation. The shore stations have connections on the Plain Text (PT) side as well as via the PCore network.

B. Network Features

The US support for the CoNSIS Naval Task Force and the associated testbed possesses many notable network characteristics, and a few selected network features are described in this section.

Mobile Ad Hoc Networking (MANET)

It is well known that Mobile Ad Hoc Networking has to overcome many challenging factors associated with highly dynamic mobile environments characterized by variable bandwidth and limited buffering. Recently, RFC 5578 provides PPPoE enhancements for router-to-radio links by including credit-based session flow control mechanism and session-based link quality feedback to improve the performance of PPPoE. In the MANET environment, PPPoE establishes and encapsulates sessions between hosts (radios) and traffic-access aggregator (routers). Figure 2 illustrates the link setup of PPPoE, namely the radios associate the two PPPoE sessions, and the RF link, for a complete data path.

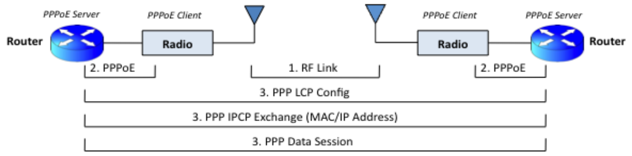

Figure 2. PPPoE Link Setup

PPPoE works well when both session endpoints possess similar bandwidth as well as forwarding and buffering capacity; however, performance can be improved with additional extensions. In a MANET environment, credit-based session radio-side flow control mechanism allows a slow receiver to control the rate at which the sender can transmit. Furthermore, session-based link quality feedback can be factored into route cost calculations. These enhancements haver been implemented by vendors (e.g., [5] and [6]). Vendors can allow link status signals (neighbor up/down) generated by the radio to influence routing protocols immediately without waiting for OSPF keepalive timers to expire.

IPv6 Stateless Address Autoconfiguration

IPv4 addresses of mobile interfaces in MANETs normally have to be preplanned and must change when a node moves from one mobile network and associates with another. Since IPv6 addresses are four times longer than those of IPv4, manual configuration is labor intensive and error prone. The IPv6 stateless address auto configuration mechanism specified in RFC 4862 [7] simplifies the address configuration process in a much streamlined manner. It is stateless because it maintains no tables within dedicated server. Essentially, a host can generate automatically a link-local address that is an identifier (such as the MAC address) supposedly unique on the link. Link-local addresses are sufficient for communication among nodes attached to the same link. As such, no manual address configuration and no additional server is required.

OSPFv3 with Support for Address Families

While OSPFv2 supports IPv4 unicast and multicast address families, originally OSPFv3 supports only IPv6 unicast address family. With RFC 5838 [8], support of address families (AF) in OSPFv3 is expanded using the Instance ID field in the OSPFv3 packet header presented in Table 1. Here the first value in each range is the default value for the corresponding address family.

This approach is fairly simple but practical in minimizing extensions to OSPFv3 for supporting multiple address families. Furthermore, it enhances interoperability between IPv4 and IPv6 networks, as well as interoperability between IPv4 nodes in different subnets using IPv6 link-local addresses for peering. Therefore, IPv4 traffic can be routed via an OSPFv3 connection, and that connection does not need to possess pre-planned global addressing on mobile interfaces. As a result, addresses do not need to be pre-planned for mobile interfaces as is necessary in IPv4 thus enhancing mobility and reducing administrative burden for mobile networks.

Table 1. OSPFv3 Instance IDs

Instance ID Range	Address Families
0-31	IPv6 unicast AF
32-63	IPv6 multicast AF
64-95	IPv4 unicast AF
96-127	IPv4 multicast AF
128-255	Unassigned

Quality of Service (QoS)

QoS feature of the Naval Task Force is provided by the PPPoE extensions for credit-based flow control and link quality metric report mechanisms specified in RFC 5578. In particular, PPPoE converts the multi-access connection into virtual PPP connections between every node on the link. As such, credit-based flow control is configured to define maximum bandwidth for each PPP connection. In addition, each PPP connection is assigned a sub-interface. Therefore, fair weighted queuing can be configured for each virtual interface, and QoS classification and marking based on Differentiated Services standards – similar to the eleven-class model illustrated in Table 2 (see [9]), can also be applied for each virtual interface.

Table 2. Baseline Differentiated Services Code Point (DSCP) Assignments

Application	DSCP	Class
IP Routing	48	CS6
Voice	46	EF
Interactive Video	34	AF41
Streaming Video	32	CS4
Mission Critical	26	AF31
Call Signaling	24	CS3
Transactional Data	18	AF21
Network Management	16	CS2
Bulk Data	10	AF11
Scavenger	8	CS1
Default / Best Effort	0	CS0

Protected Core

It is necessary to connect the core network of different coalition partners to utilize network resources efficiently. This must be performed with sufficient security to ensure no user on the coalition network (or the NGO network) can interfere with network operations intentionally or unintentionally.

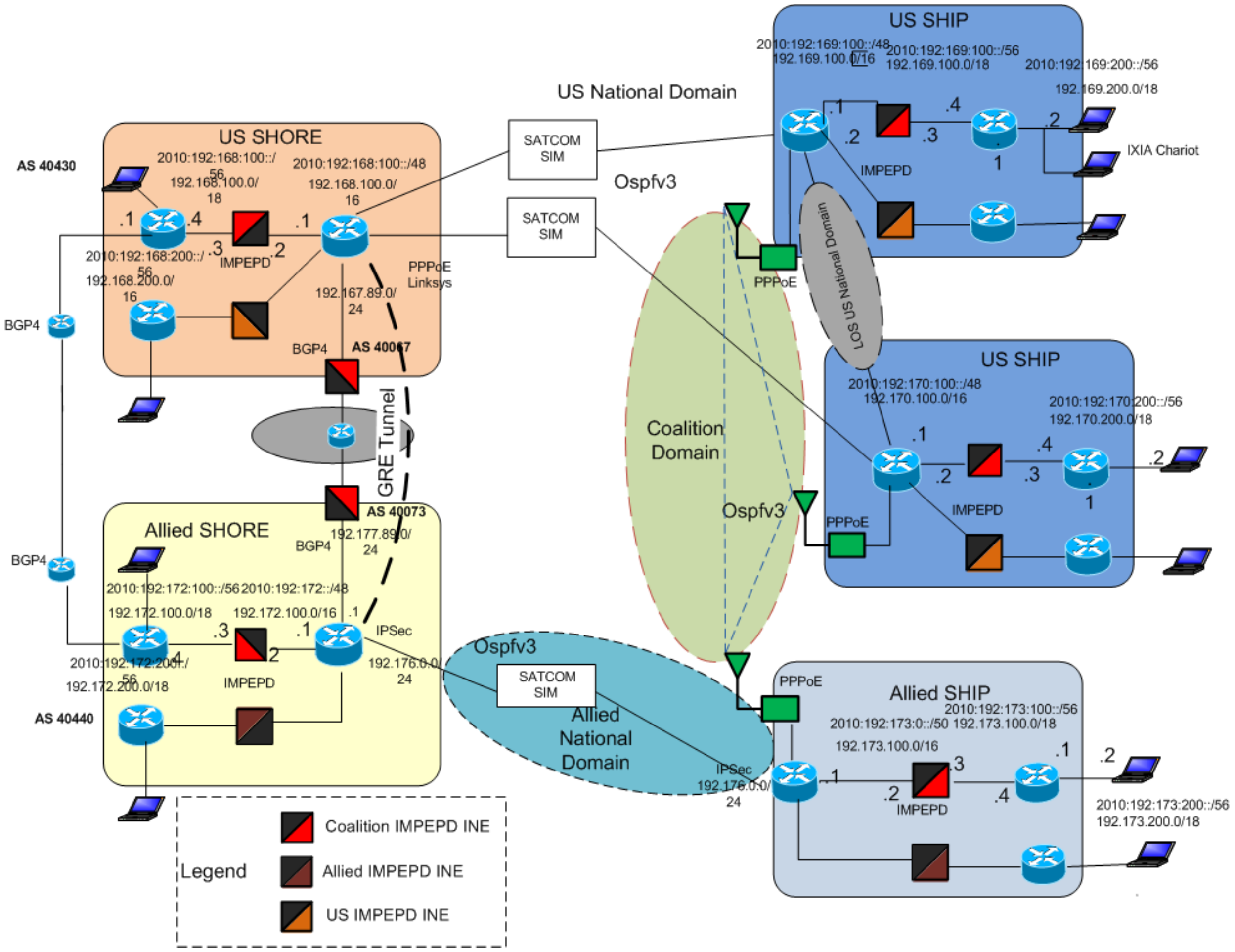

Figure 3. Notational Naval Task Force Testbed Topology

The Protected Core makes use of (1) Implicit Peer Enclave Prefix Discovery (IM-PEPD) protocol, and (2) Route Redistribution via an INE.

IM-PEPD is a unicast discovery protocol that uses a probe/response mechanism to discover other network encryptors and the prefixes behind the encryptors. IM-PEPD has two modes: passive and active. In the passive mode all the PT prefixes are advertised on the PCore network and no prefix discovery is necessary. In the active mode, multiple prefixes can be behind an INE gateway and discovery is necessary. In this case, the INE sends out a "probe" which is routed to the gateway and the gateway INE responds with a message that initiates a secure association (SA) negotiation, if necessary, and causes encrypted traffic to be routed to its Cipher Text (CT) IP address for the discovered prefix.

Route Redistribution is a route reachability protocol that allows network prefix discovered by an encryptor to be advertised to the rest of the PT network. The main purpose is to dynamically announce the reachability of a network as the platform changes its termination from one location to another, and to stop network prefix advertisement at the location when the platform is no longer attached.

C. *Testbed*

A testbed to demonstrate the Coalition Network Interface to support the Naval Task Force for the CoNSIS project is illustrated by the diagram in Figure 3. Two shore nodes and three ships are represented. Each of these ships has point-to-point satellite links to a shore node and is interlinked by a proxy that emulates a radio which supports PPPoE with Flow Credit and Link Metric extensions, and also makes the network connection appear to the router as a Layer-2 segment even if the radio is acting as a Layer-3 IP router.

IxChariot test tool is used to simulate applications, generate test traffic, collect traffic statistics, and produce data for graphic display and visual presentation. Additionally, real applications (such as e-mail, chat, and FTP) have been installed for test purposes.

The key experiment objectives can be summarized as follows

- Demonstrate OSPFv3 with AF support can be used for mobile networks with reduced administrative overhead, i.e., IPv4 traffic can be routed via mobile interfaces with no need to be the same IPv4 subnets.
- Demonstrate QoS based on weighted fair queuing is possible on point-to-multipoint wireless connection

using PPPoE with credit-based session flow control extension.
- Demonstrate improved network stability and control of routing path based on PPPoE with session-based link quality metric feedback extension.
- Demonstrate these features in an integrated testbed in relevant scenarios, described in the scenario testing section.

IV. Test Results

The test objectives are to demonstrate the following features in a testbed that realistically emulates the tactical network of a Naval Task Force.

- Demonstrate that PPPoE protocol with link metric extension can control the forwarding path based on link quality feedback.
- Demonstrate OSPFv3 with AF support can be used for mobile networks with reduced administrative overhead. That is, to demonstrate that IPv4 traffic can be routed via mobile interfaces that have no need to be same IPv4 subnets.
- Demonstrate QoS based on weighted fair queuing is possible on a point-to-multipoint wireless connection using PPPoE with traffic flow credit extensions.
- Demonstrate improved network stability and control of routing path based on use of PPPoE with link metric extensions
- Demonstrate use of all these features in an integrated test bed using several realistic scenarios.

In short, the test goals are to demonstrate a network that does not require pre-planned addresses on the mobile networks, rapid network convergence, effective dynamic routing multicasting of data between nodes. These demonstrations were performed in a testbed setup to reproduce the conditions expected in a tactical naval network.

A. Auto configuration

The mobile network interfaces were enabled to auto configure with IPv6 link-local addresses. This allows mobile nodes to join and start communicating with other enclaves in the network without the need to have pre-planned addresses, thus reducing administrative burden. The link-local address is derived from the Ethernet MAC address. Cisco implementation requires an IPv4 address to be configured on the mobile interface, even though it is not used for routing and does not need to be configured in the same subnet as other mobile interface in the ad hoc network. It was verified that the OSPFv3 processes discovered each other via the link-local addresses, formed neighbors, exchanged routing databases and forwarded traffic as expected.

B. IPv6 Address Family Support

OSPFv3 uses IPv6 for router information exchanges and packet forwarding. Since users still need to use IPv4 for some time in the future, Cisco implementation of OSPFv3 with AF support other than IPv6 unicast AF allows OSPFv3 to forward IPv4 traffic, thus facilitating interoperability within realistic mixed IPv4 and IPv6 network environment. This Cisco implementation of AF support was tested. IPv4 connectivity across the IPv6 backbone was verified.

C. Mobile Network Convergence

PPPoE with extensions for Credit Flow and Link Metrics allows faster network convergence. Test results show a faster response to mobile units entering and exiting an ad hoc mobile network. In addition, network traffic is more quickly re-routed when a link is marked down. The convergence time depends on the software configuration, but for this Cisco implementation node the network convergence time for a node entering or leaving the mobile networks was observed to be near real-time, about 5-6 seconds, compared to 40 seconds for the dead time of the standard OSPF configuration.

D. Re-routing based on Link Quality Metrics

This test session demonstrates the ability to re-route traffic based on the changing quality of the links. In this test, the OSPFv3 dynamic routing cost of Cisco routers is based on the link metric values, such as Max-Data-Rate (MDR), Current-Data-Rate (CRD), Latency, Resources and Relative Link Quality (RLQ) of radio link characteristic fed back to the routers. These metrics are defined in [4] in terms of a type-length-value (TLV) message which is used to report the link quality parameters. In a network of three mobile nodes the link metric RLQ (a non-dimensional number from 0 to 100 inclusively, representing the relative link quality with a value of 100 represents a link of the highest quality [4]) was manually changed on the preferred link and it was observed that traffic was re-routed around the degraded link.

E. QoS via PPPoE with extensions

This Quality of Service test demonstrates that Class Based Weighted Fair Queuing (CBWFQ) works on virtual interfaces via a point-to-multipoint link using PPPoE with extensions for credit flow and link metrics. A QoS policy, if configured, limits the bandwidth allowed on a virtual link and prioritizes the flows of several different types of traffic. When the allowed bandwidth is reduced, it is observed that the traffic flows are impacted according to the configured QoS policy configured on the Cisco Virtual Multipoint Interface (VMI). In this test, IxChariot and/or installed applications are used to generate traffic, including video, FTP, Critial FTP, and web (TCP) traffic.

F. Routing Issues

During the course of network design and initial testing, several routing issues surfaced. Primary among them are the following three issues, namely (1) manual configuration of Border Gateway Protocol (BGP), (2) duplication of OSPF's Link State Advertisements (LSAs), and (3) "sticking" BGB routes. First, the routing domains between nations have to be separated to prevent routing loops. This is normally done with BGP, but BGP is manually configured and this is not practical in the tactical environment. For this reason redistribution of routes between OSPF processes was used to automatically advertise routes, which is a proprietary feature available on Cisco routers.

Secondly, when routes are redistributed between OSPF processes, increased the overhead on the routing protocol on the network. This may be resolved by OSPF filtering and will be investigated in the future.

Finally, BGP was used on the shore between US and allied shore stations. There has been an issue with the routes "sticking" when the ship/shore links cycle up and down. This was resolved with by the use of a "non-exist" statement on the shore router.

G. *Scenario testing*

The six (6) scenarios have been tested as the following:

- Basic scenario - Two Network Operations Centers (NOCs), three satellite links three ships with LOS links
- Re-routing of traffic via coalition partner when satellite communications (SATCOM) link goes down
- Link restoral SATCOM to shore
- One SATCOM link – LOS relay between ships.
- No SATCOM – only LOS routing between ships
- Plain-Text routing between US shore and allied shore

In this scenario testing, basic network connectivity and link restoral were verified.

V. Summary

Router-to-radio interface approaches promise performance improvements for mobile radio communications in IP routing environments. In this paper we present a network interface in support of a Naval Task Force for the four-nation Coalition Networks for Secure Information Sharing (CoNSIS) project. Effectively this effort lays out the framework for naval mobile ad hoc networking for CoNSIS. Moreover, in this paper we have presented network architecture and network features of a tactical naval network, as well as testbed, and test results.

A secure coalition mobile ad hoc network based on existing and emerging standards, using commercial services and products was demonstrated in the laboratory environment in a realistic testbed. The network is designed to accommodate new standards that are being developed by industry for commercial and emergency response usage. The design is intended for use with modern radios that were meant to be part of an IP network and communicate with the network via an Ethernet port. Within that constraint the demonstrated networks is radio-agnostic. Due to the high cost of tactical radios, this demonstration was performed with an open-source proxy device, developed by the Naval Research Laboratory, to emulate a radio supporting the standard protocols proposed under the Internet Engineering Task Force for the router-to-radio interface.

Tests were performed in a configuration that emulated a US shore site, a coalition shore site, two US ships and one coalition ship. The networks were encrypted with INEs.

VI. Conclusions

Throughout phases of this ongoing effort we have been gathering lessons learned and observing and tracking emerging trends and technologies relevant to designing a Naval Task Force that enables secure delivery of network-based applications and services over radio links to support information sharing.

On the network security side, in this work although the only Dynamic Peer Discovery Protocol tested was IM-PEPD, comparative testing of other protocols is planned for the future.

Furthermore, although the US participants did not focus heavily on the protected core concept as an overarching emphasis, much more work may be performed in this area as well as in areas of cybersecurity and cyberwarfare in general.

On the networking side, while IP Network architects want to see the radio link as a transparent network segment, which operates at the Open Systems Interconnection (OSI) Layer 2, radio manufacturers often design the radio as a router, with the connection made at OSI Layer 3. The extended PPPoE protocol is a step in the right direction, which has been promoted by radio and router manufacturers. This plausible intermediate step is not without issues – in particular, multicast not being supported in an efficient manner. Currently, multicast is converted to unicast and forwarded via virtual PPP connections set up by the PPPoE protocol.

Protocols in development such as the Dynamic Link Exchange Protocol (DLEP) may handle multicast as well as applications and services such as full-motion video and video-teleconferencing more efficiently. As such, new protocols will be investigated in future work.

Finally, we note that there is at least one radio that supports these PPPoE extensions; however, its cost is prohibitive for use within the current budget of this project. Future testing will involve commercial radios and sea trials.

References

[1] B.-N. Cheng, et al., "Characterizing Routing with Radio-to-Router Information in an Airborne Network," in *Military Communications Conference, MILCOM 2011*, November 2011.

[2] R. Charland, P. Christensen, J. Wheeler, and B.-N. Cheng, "A Testbed to Support Radio-to-Router Interface Testing and Evaluation," in *Military Communications Conference, MILCOM 2011*, November 2011.

[3] M.-C. Wang, S. Davidson, and S. Mohan, "Design Consideration of Router-to-Radio Interface in Mobile Networks," in *Military Communications Conference, MILCOM 2011*, November 2011.

[4] B. Berry, S. Ratliff, E. Paradise, T. Kaiser, and M. Adams, "PPP Over Ethernet (PPPoE) Extensions for Credit Flow and Link Metrics," Internet Engineering Task Force, RFC 5578, February 2010.

[5] Cisco Systems, "MANET: Enhancements to PPPoE for Router-to-Radio Links," 2007. Online: http://www.cisco.com/en/US/docs/ios/12_4t/12_4t15/ppscf_ST.html

[6] Juniper Networks, "PPPoE-Based Radio-to-Router Protocols Overview," 2007. Online: http://www.juniper.net/techpubs/en_US/ln1000-junos10.1/junos/topics/concept/pppoe-radio-to-router-overview.html

[7] S. Thomson, T. Narten, and J. Jinmeil, "IPv6 Stateless Address Autoconfiguration," Internet Engineering Task Force, RFC 4862, September 2007.

[8] A. Lindem, S. Mirtorabi, A. Roy, M. Barnes, and R. Aggarwal, "Support of Address Families in OSPFv3," Internet Engineering Task Force, RFC 5838, April 2010.

[9] Cisco Systems, "The QoS Baseline," April 2005. Online: http://www.cisco.com/en/US/technologies/tk543/tk759/technologies_white_paper0900aecd80295a9b.pdf