Multi-Topology Routing for QoS Support in the CoNSIS Convoy MANET

Mariann Hauge, Margrete A. Brose, Jostein Sander
Norwegian Defence Research Establishment (FFI)
Kjeller, Norway
{Mariann.Hauge, Margrete-Allern.Brose, Jostein.Sander}@ffi.no

Jon Andersson
Thales Norway AS
Oslo, Norway
Jon.Andersson@thalesgroup.com

***Abstract*— This paper shows how Multi-Topology (MT) routing is used to maintain three different network topologies in the heterogeneous land mobile network architecture used in the Coalition Network for Secure Information Sharing (CoNSIS) project. The topologies are each associated with one or more quality of service (QoS) classes to provide differentiated QoS in this disadvantaged grid. A proposal for how to connect a Multi-Topology routing protocol to adjacent Single-Topology (ST) interior gateway protocols and exterior gateway protocols is also given.**

Keywords- multi-topology routing; QoS; admission control; MANET; OSPF; IPv6)

I. INTRODUCTION

In a coalition operation the participating nations will typically bring their national radio equipment into the theater. Usually the equipment will comprise of a wide selection of brands and technologies, depicting the normally long lifetime of radio systems. These radios will most likely not be compatible on the air, and if they are, they will not have compatible security solutions, management or services for the end user. The main goal of the multinational Coalition Network for Secure Information Sharing (CoNSIS) project is to solve these interoperability issues. CoNSIS proposes solutions to improve interoperability in all the above mentioned areas. This paper presents the Multi-Topology routing concept as used by CoNSIS to provide differentiated QoS in the land mobile network that utilizes many different transmission technologies for internal communication as well as reach-back to the deployed headquarters.

To provide a reliable network for different operation types and in varying terrains, a tactical mobile network infrastructure must consist of a variety of wireless network types, e.g., long-range communication for reach-back connections and a higher bandwidth network for local communication. A single transmission technology, e.g. a VHF network, will not be able to support all communication types and bandwidth requirements. In CoNSIS we assume that the different nations participating in a coalition operation bring their national tactical networks to the battlefield. Thus there may be a large number of different, non-compatible radio systems present in the mission network. The aim of CoNSIS is to be able to combine all available radio systems in an operation to provide an efficient, common network for coalition use. This gives the operator a single entry point to the complete heterogeneous coalition network, the network will be better utilized, and multiple transmission technologies and routing paths will also improve the network reliability by providing alternative routing paths during e.g. jamming attempts. The resulting coalition network will consist of radios which have large variations in capabilities and transmission range. Thus it is challenging to administer, admit, and route traffic flows in these networks.

In a mobile tactical network there will in most cases be limited capacity. It is therefore crucial to support prioritization of operation critical traffic. It is also desirable to use the tactical network in the most optimal manner and thus make sure that only traffic that has a high chance of reaching the destination is admitted into the network. One way to increase the network throughput is to take advantage of parallel paths in the heterogeneous network and efficiently exploit all bandwidth resources.

Since the transmission means used in tactical networks have large variations in capabilities, CoNSIS find it advantageous to define multiple routing topologies in the network to support different QoS-classes. These topologies are then used to ensure that data packets are only forwarded on topologies with sufficient capabilities to support the requirements of the dataflow. We combine Multi-Topology (MT) routing [1][2] and traditional DiffServ-like [3][4] mechanisms to utilize all available transmission means in the tactical network and increase the robustness of the network. In [5] we have presented our findings when using this technique on an isolated test bed network in our lab. The QoS architecture with MT support has also been utilized by the Web services admission control broker in [6]. The SW for the MT-router has been extensively modified for the CoNSIS project, and in this paper we describe how this solution is used in the land mobile CoNSIS network and how we have solved the interaction between a network running MT-routing and adjacent networks running non-MT capable domains.

The rest of the paper is organized as follows: In Section II we give a brief background presenting the CoNSIS project. We point the reader to related work in Section III. In Section IV we describe the Multi-Topology routing solution and the mechanisms proposed to connect a Multi-Topology routing domain with a Single-Topology routing domain. The QoS architecture is explained in Section V. In Section VI we discuss the use of MT in the land mobile network in the CoNSIS

network architecture, and finally we give a short conclusion in Section VII.

II. BACKGROUND

As stated in the CoNSIS memorandum of understanding (MoU): "The objective of the project is to design, implement, test and demonstrate technologies, methods and architectures for the secure sharing of information and services between nations in ad-hoc coalitions, and between military systems and civil systems for Civilian Military Cooperation, e.g. with Non-Governmental Organizations (NGOs), within the communications constraints of mobile tactical forces."

The work is organized in five tasks:

- Task 1, Communication Services
- Task 2, Information and Integration Services (SOA)
- Task 3, Security
- Task 4, Management
- Task 5, Architecture, Test and Demonstration Coordination

The technique described in this article represents some of the work that has been performed in Task 1, Communication Services. In this task our concern has been to provide a transparent network and information infrastructure (NII), based on and harmonized with IP technology. The focus of this task is to demonstrate solutions that will work within the communications constraints and dynamic topology imposed by the highly mobile tactical networks. The proposed mechanisms should support IPv6.

All figures and information presented in the remainder of this document focuses on the challenges as seen by the Communication Services task.

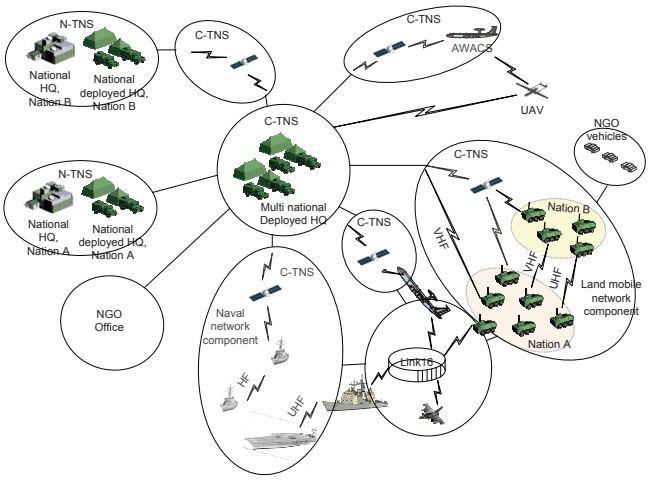

Figure 1. This figure shows all network elements that participate in the CoNSIS scenario. N/C-TNS stand for National/Coalition-Transport Network Segment.

CoNSIS has defined a scenario that takes place in a country torn by civil war. An international coalition is involved in this conflict to protect civilians and initiate the peace process. The coalition has a land based component, a naval component and an air based component. Fig. 1 shows all elements that is included in the CoNSIS network architecture and participates in the scenario.

Task 1 has proposed to use Multi-Topology routing to provide some admission control and differentiated services in the land mobile network component in Fig. 1. This network segment will be connected to the other segments (including the Multi National Deployed HQ) via an exterior gateway protocol. In the CoNSIS scenario the land mobile component represents a military convoy that is tasked to escort a group of NGO vehicles to an area where there has been a natural disaster. This convoy will be played in the ongoing CoNSIS field test. The network deployment planned for the convoy in the field test will be used to exemplify the use of MT routing in CoNSIS.

III. RELATED WORK

During the last 10 years a lot of research has been done to achieve predictable QoS in mobile ad hoc networks (MANET). This is a difficult task due to the agile changes in the network topology, and the fluctuating channel quality in such networks. Much focus has been put in the area of QoS-routing. QoS-routing aims to find a route which provides the required service quality for a specific traffic type. This can be done using routing metrics based on parameters like delay, data rate, signal to noise ratio, route stability, etc. These protocols must be combined with a resource manager and a traffic classifier (e.g., DiffServ-like classification) to support end-to-end QoS in the network. Two survey papers [7][8] give a comprehensive overview of many of the available QoS-routing proposals.

Most of the QoS protocols covered in the two survey papers discover a single path that supports a certain QoS requirement. This QoS requirement can be described by one parameter (e.g., maximum bottle neck data rate), or by several parameters (e.g., maximum bottle neck data rate and lowest end-to-end delay). Some protocols also maintain multiple paths to the destination for the purpose of e.g., load balancing, fault tolerance, higher aggregated bandwidth and reduced route discovery latency after link breaks. In [9] important multipath protocols are covered. In [10][11][12][13] multipath is established explicitly for QoS support. Some of these also make a point of combining DiffServ and multipath routing.

However, most of the QoS-routing schemes, and all the mentioned multipath protocols are reactive routing protocols. We believe proactive protocols will be necessary in tactical MANETs to reduce the routing response time and increase the predictability of the network availability. We also think it is beneficial to store several routes with different characteristics to support separate QoS requirements. This is important for a heterogeneous wireless network that is established with radios that utilize different transmission technologies.

The MT supported QoS architecture is based on the proposal presented in [14] and further studied in [5]. It is a simple but powerful scheme with a proactive routing protocol that maintains multiple topologies in the routing domain and consequently provides multiple paths from source to destination. Each topology/path is associated with a single or

multiple QoS-class(es). Similar ideas (based on a very different routing scheme) are presented in [15]. In this reference, network information is maintained proactively, and different paths for the required QoS-classes can be calculated with different metrics based on a single routing database.

In [16] MT-routing is combined with a dynamic topology and traffic pattern analysis tool to provide a flexible load balancing solution and in [17] MT-routing is utilized in a satellite network both for fault tolerance and for traffic separation of traffic having different QoS requirements. Both of these papers exploit a similar technique as the one presented in this paper however our focus is to support admission control and efficient resource utilization in a very heterogeneous military mobile ad hoc network.

IV. MULTI-TOPOLOGY ROUTING ARCHITECHTURE

A. *Multi-Topology Routing*

A traditional link state routing protocol maintains one routing table with one entry for "the best route" to all destinations in a network domain (or several of the best routes for load balancing purposes). The best route is calculated based on the chosen metric (e.g., shortest path first (SPF) or lowest cost, where the cost parameter can be established based on any set of link parameters).

A Multi-Topology routing (MT-routing) protocol maintains several topologies within the network domain at the cost of a few extra bytes in the routing packets. Each topology spans a subset of the physical topology. A shortest path first calculation (other metrics can be used if available) is performed for each topology to discover the best routes within the topology. The cost of one link can be set different for the different topologies. Only the links belonging to the actual topology are included in the calculation. The results of the SPF calculation are stored in one forwarding table for each topology. In Fig. 1 we show a network where three topologies are defined on the physical topology. A number of topologies can be defined on a single physical link. All the physical links in the domain must be part of the default topology. The default topology is used for routing traffic and ensures that routing information is flooded to the whole network. All link advertisements are stored in a link state database. The calculation of the forwarding table for each topology is based on the information in this database.

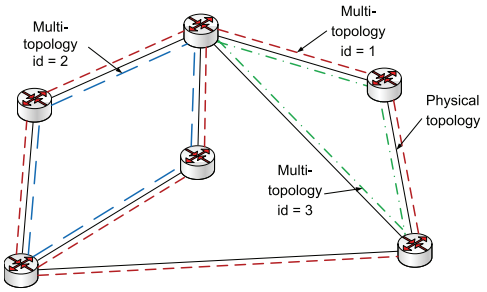

Figure 2. This figure shows a network with three different topologies.

During network configuration, topologies can be tailored to represent many different purposes. MT is used for the following cases in CoNSIS:

- Topologies can be created that has sufficient (maximum) resources to support a certain QoS-class, or multiple QoS-classes.
- A specific topology can be created to be used for transit traffic through the network.

MT-routing is a very useful tool that can be used to solve many situations where a certain end-to-end behavior is needed in tactical networks. This comes at the cost of a more complex network configuration. For more details about the MT routing operation, please consult [5].

B. *Interaction between a Multi-Topology Routing Domain and a Single Topology Routing Domain*

The MT-routing draft and RFC [1][2] both describe interaction with Single-Topology (ST) routers through the default topology (designated table 0 in MT). We do not view this approach as suitable for a mobile military network. The main reasons are:

- The default topology covers the entire network and does not take into account transmission characteristics for the respective links.
- For IPv6 the routing protocol load would be close to doubled, since the layout structure of the MT Link state advertisements (LSAs) are incompatible with standard IPv6 OSPF. In order to obtain compatibility with ST routers, the MT capable router has to transmit both encodings.

Furthermore is it not described how to import routing information from an adjacent ST-routing protocol into the MT-routing protocol, without using the default topology. This can be regarded as a weakness in the specification, since it will only be the high capacity topologies of the MT domain that are usable for connection with external ST networks. The default topology normally does not have the ability to differentiate on traffic. In the CoNSIS project we wanted to have the interaction both between the MT-routing protocol and an exterior gateway protocol (EGP) as well as an interior gateway protocol (IGP).

First we consider the task of importing and redistributing routing information from an adjacent ST-routing protocol into the MT-routing protocol. Most ST-routing protocols maintain routing information in the main forwarding table (known as table 0 or default topology in MT). To avoid conflicts the default topology should not be used by the MT-routing protocol when MT-routing is used for QoS purposes. According to RFC [2] tables 32 to 127 are reserved for development, experimental and proprietary features and can be used for our purposes.

The adjacent network information that we want to redistribute in the MT-network can have very different characteristics, it can be a homogeneous radio network with a certain characteristics or it can be a deployed network with a different typical characteristic. The radio network we might want to import into one or more specific topologies, whereas the deployed network should be imported into all topologies. For this reason we wanted to make a very flexible solution that

allowed us to specify network import into (none or) any number of topologies. This involves both redistribution of the adjacent ST protocol information into the different topologies, and a copy of the ST routing information made available to the MT forwarding tables. Since redistribution only provides the routing information to neighboring nodes and not to the unit itself, this has to be a copy.

If several networks are connected to the same gateway router and we do not want to redistribute the information from these protocols to the same topologies, then these networks must use different routing protocols, if not the router will not be able to identify the routes made available from the one network from the routes made available from the other network. It should be possible to use route-maps for each topology to limit the visibility when using the same routing protocol.[1]

Next we consider the task of making routing information from the MT-routing protocol available for adjacent networks. Here we would also like to have the same flexible solution of providing information from (none or) any number of topologies to the ST-routing protocol. In practice this means to provide the union of the routes available in the relevant MT topologies to the ST-routing protocol. This was not straight forward to implement (partly because of overlapping routes) in the open source routing environment used for the implementation (the SW platform is described in chapter VI). Thus the solution we implemented was to provide routing information from 0 or 1 (any of the available topologies) topologies to the adjacent network.[2]

One should be careful not to import routing information into different topologies than the one that is exported to the same network. If this is the case there will be asymmetry in the network information and some traffic will only be able to flow one way. In a QoS architecture this could be solved with a policy saying for example that the non MT-networks should be given the same, or more routing information than what is available in the MT-network. Traffic with QoS-tag that cannot be supported by the current MT-network topology will then be dropped at the entry point to the disadvantaged mobile MT-network.

As a special case we gave the interaction between the MT-routing protocol and BGP [18] some extra thought. Providing the routing information in one topology for redistribution in BGP limits the visibility of the MT-network for BGP connected networks. Thus this method can be used to provide a topology for transit traffic through the MT-network and make the complete MT-network only available for local traffic.

V. QoS ARCHITECHTURE

The CoNSIS QoS architecture for the network layer divides the QoS operations in two functional entities:

- One entity that supervises the resource management. This mechanism is needed at the ingress of the network.
- One entity that handles network congestion, packet forwarding and packet prioritizing required by the different dataflows. This mechanism is needed in all forwarding elements in the network.

The resource management entity decides if a new traffic flow can be supported by the network. This mechanism must identify the network resources required by the flow associated with a specific QoS-class. If there are enough network resources available, the session will be admitted. Thus, there is a need for a resource management mechanism that attempts to estimate the available capacity of the network. If mechanisms are available to support resource reservation, this will be done by the resource manager.

The prerequisites for admittance of a session may change after a session is admitted. A session of very high importance may try to access a fully loaded network. Then, pre-emption of a low importance session may be required. Similarly, due to node mobility, jamming, etc., the network capacity may change over time. This must be acted on by the resource manager.

Short term network congestion due to fluctuations in the radio channel capacities and temporary overload of the network must be handled by the forwarding component of the network routers. This component must also tailor packet queues and packet scheduling to effectuate the delay requirements of the packet's QoS-class, and the military priority of the packet. In overload situations this mechanism makes sure that the important traffic is prioritized by the network at the expense of less important traffic which might then experience a very high packet loss due to queue overflow.

For this architecture a set of QoS-classes must be defined that describe the network requirements (in terms of data rate, jitter, delay, reliability, etc.) needed by the dataflow labeled with the specific QoS-class. The traffic flows must be tagged with this information.

In CoNSIS we propose to use MT routing to support the entity that supervises the resource management of the network. In the MT supported QoS architecture, we configure and maintain several network topologies that each spans a subset of the physical topology. Each topology has its own forwarding table that is used to forward packets classified as belonging to that specific topology. If a destination address is not available in the forwarding table associated with the QoS-class, then no path exists in the network where the specific QoS-class is allowed to be transported. Thus the flow should not be admitted to the network. Traffic is stopped at the network edge and not (in a worst-case scenario) forwarded through the entire network just to find that the last hop to the destination is a link not able to support the flow's QoS requirements.

When there is a route to the destination in the correct topology and the traffic flow is admitted to the network, the DiffServ mechanisms come into play. A queue hierarchy and packet scheduling mechanism prioritizes the sequence of transmitted packets on each interface. For each network

[1] In the case of interfacing BGP, route-maps could possibly use e.g. "match peer x.x.x.x" or "match as-path". This has not been investigated further.

[2] Changes would be required to OSPF /ZEBRA in order to support multiple topologies to the adjacent networks. This is left for future work.

interface we also define a traffic shaper, whose purpose is to keep the traffic transmitted on e.g. the wireless network below a certain threshold, to avoid network congestion. We use queue and scheduling tools to tailor the queue to the requirements of the associated QoS-class, and to implement packet scheduling for traffic priorities. Queue length, head/tail drop and drop-precedence are important queue parameters, while the packet scheduler could be designed for a strict priority scheme or a situation with more fairness in the scheduling process.

It should be noted that in the current version of the MT-routing protocol we build topologies based on static predefined network/link characteristics. In future work we want to investigate if dynamic parameters representing the real time resource situation for the links can be incorporated efficiently with the MT-routing protocol to better support the resource management mechanism in the mobile tactical network. Alternatively, a possible solution could be to use the proactive MT-mechanisms as a first check if a flow can be admitted to the network and use a reactive probing technique to check the real-time resource situation on the MT path before the flow is actually admitted.

VI. CoNSIS Convoy Test Network

A. *Multi-Topology Routing SW*

We have implemented[3] the Multi-Topology support for OSPFv3 and OSPFv2, as well as MANET OSPFv3 (MDR) [19] into the Vyatta [20] Linux distribution. This is based on the Quagga [21] open source routing application running on a Debian system with Linux kernel 2.6.37 (ATOW). The MANET OSPFv3 base protocol was fetched from [22]. The router implementation allows easy configuration of OSPFv2-MT and OSPFv3-MT information. Metrics can be setup for each topology on each interface. The Linux platform is set up to utilize multiple forwarding tables and Quagga's interface towards forwarding tables in Linux has been adjusted to allow the use of multiple routing tables. In addition to OSPFv2-MT and OSPFv3-MT routing, the implementation also supports configuration of static MT-routes. A flexible import and redistribution of routes from other routing protocols is supported, as well as customized export of MT-routes to the main routing table to make the routes available to other routing protocols.

Due to experienced instabilities in the MANET OSPFv3-MT protocol we will use OSPFv3-MT in the CoNSIS field experiment.

It should also be noted that the expanded encoding of the OSPF Options described in the draft [1] is in conflict with bits allocated by OSPF Link-Local signaling [23]. Link-Local Signaling is also part of the MANET OSPFv3 implementation.

B. *The CoNSIS Convoy Platforms*

The land mobile network component in the CoNSIS network architecture is represented by a multinational convoy in the scenario and in the field test. The network consists of a German (Nation 1) and a Norwegian (Nation 2) convoy segment. Each segment consists of four mobile nodes. The convoy network is connected to a multi-national deployed headquarter (Fig. 3). The NGO vehicles also have a network connection to the military convoy, however this connection is not visible in Fig. 3 since this network is not allowed to be part of the unprotected coalition transport network. Traffic is sent to/from the NGO segment via application gateways handled by other CoNSIS task groups.

The Convoy network consists of five different radio networks. It is therefore a highly heterogeneous MANET. Table I give some details of the radios that will be utilized in the planned CoNSIS experiment. The network is used for internal convoy communication and reach-back to the deployed headquarters.

TABLE I. RADIOS USED IN THE CoNSIS CONVOY TEST NETWORK

	Radio Type	Number of radios in the network	Shared channel data rate[a]
Nation 1 SatCom	Thrane &Thrane BGAN Ex. 727	unknown	384kb/s
Nation 1 UHF Network1	IABG HiMoNN	6	11Mb/s
Nation 1 VHF Network	Harris RF-7800S	5	64kb/s
Nation 1 UHF Network2	Rockwell Collins FlexNet-Four	3	1Mb/s
Nation 2 UHF Network	Kongsberg WM600	6	920kb/s

a. The data rates are approximate values

The different transmission technologies present in the planned experimental network have substantially different characteristics when it comes to e.g., transmission delay, transmission range and data rate. Given the heterogeneous network as described above, the end-to-end network capacity could change from a relatively high data rate of several Mb/s to a few tens of Kb/s when a node moves from UHF coverage to a path that includes one or more VHF and/or SatCom on the move links. This large variation in available data rate is difficult to handle for the resource management entity. In such a scenario it is also important that the network is able to prioritize the mission critical data traffic in overload situations.

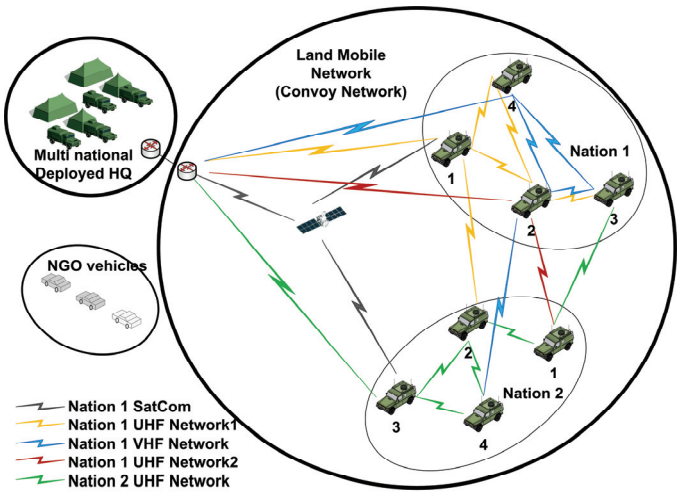

Figure 3. The land mobile network in CoNSIS.

[3] The implementation is done by Thales Norway AS

In the CoNSIS network architecture for the land mobile network we interconnect the different links and networks present in the network with an OSPFv3-MT routing protocol in one flat routing domain. This allows full dynamics in the network.

To demonstrate the use of multiple topologies for QoS purposes we define three topologies in the CoNSIS convoy network:

- A high data rate topology
- A low data rate topology
- A low delay topology

Table II shows how the different radio networks in the CoNSIS convoy network are associated with the three defined topologies. All radio networks also participate in the default topology.

TABLE II. THE USE OF THE RADIO NETWORKS IN THE TOPOLOGIES

Radio Type	Low data rate topology	High data rate topology	Low delay topology
Nation 1 SatCom	X	-	-
Nation 1 UHF Network1	X	X	X
Nation 1 VHF Network	X	-	X
Nation 1 UHF Network2	X	X	X
Nation 2 UHF Network	X	X	X

The low data rate topology includes all links. The high data rate links are also included in this topology to increase connectivity and network robustness; however, the topology cannot guarantee more than a low data rate capacity. The best path within each topology is calculated based on the MT-cost parameter for each link between source and destination. The UHF networks are given low cost whereas the SatCom and the VHF networks are given a very high cost. We set the same cost for all topologies but acknowledge that it could be beneficial in some cases to use different cost for different topologies and thereby prioritize the utilization of the network types differently for different traffic types.

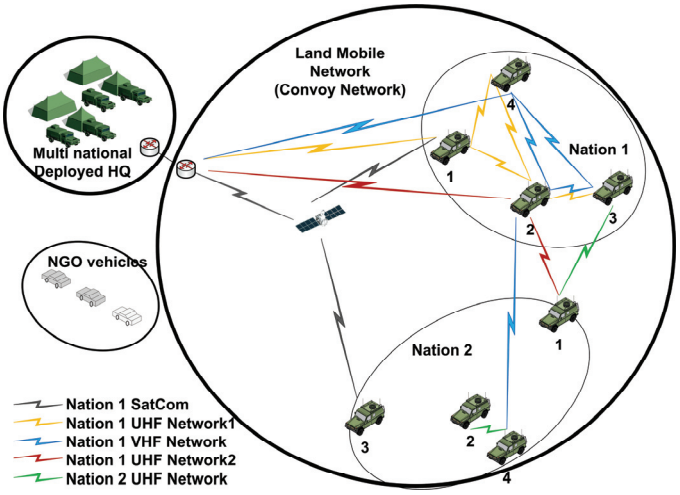

Figure 4. Network connectivity in terrain with difficult radio propagation for Nation 2's UHF network.

Fig. 4 exemplifies a radio topology where Nation2's portion of the convoy is driving into a terrain with difficult channel propagation conditions for Nation2's UHF radio. Table III shows the routing table for the three topologies for all the vehicles in Nation2 for the radio connectivity represented in the figure.

TABLE III. ROUTES[a] AVAILABLE IN THE THREE DIFFERENT ROUTING TABLES IN THE VEHICLES OF NATION 2 IN FIG. 4

Nation 2 vehicle no.	Low data rate topology	High data rate topology	Low delay topology
1	All vehicles	All Nation 1 vehicles	All except Nation2:3
2	All vehicles	Nation2:4	All except Nation2:3
3	All vehicles	-	-
4	All vehicles	Nation2:2	All except Nation2:3

a. The destinations are represented as follows in the table: Vehicle no. 3 in Nation2 is written as Nation2:3.

In the MT supported QoS architecture we require that all traffic in the network is tagged with the appropriate QoS-tag. We choose to use the *traffic class* field in the IPv6 header, to mark the packets. We use this field to encode the QoS-class (named Service-based Class (SBC) in [24]), and traffic priority (IP Military Precedence Level (IP MPL)) as suggested in [24]. Fig. 5 shows the chosen format.

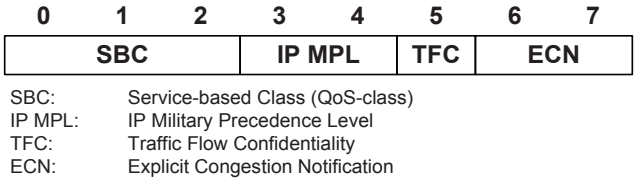

Figure 5. Suggested use of the IPv6 *traffic class* field.

TABLE IV. CONSIS SERVICES MAPPED TO SBCS

SBC	Service	One example of mapping between CoNSIS services and the SBC		DSCP	
NETR	Network Infrastructure	- Routing (e.g. OSPFv3-MT, BGP, OLSR) - Management, ICMP Error Messages - TIBER Auto detection of classified enclaves		CS6	110000
OAM	Network Management	- Security management		CS2	010000
SIG-T	Call Signaling	- VoIP signaling - Notification Management Service - Service Discovery Service		CS5	101000
VOICE	Voice		F		101010
			P		101100
		- MELPe	R	EF	101110
VIDEO	VTC		F	AF41	100010
			P	AF42	100100
			R	AF43	100110
STREAMING	Streaming media		F	AF31	011010
			P	AF32	011100
			R	AF33	011110
LDELAY	Low latency data	- Operational Alarm Messages - NFFI Blue Force Tracking Service	F	AF21	010010
		- Chat Application	P	AF22	010100
		- Network Services (e.g. DNS, DHCP)	R	AF23	010110
BULK	Bulk	- Image messaging service	F	AF11	001010
			P	AF12	001100
			R	AF13	001110
NORM	Best effort	Other applications		BE	000000

For the CoNSIS QoS architecture we decided that there should not be a fixed association between a traffic type and a SBC and IP MPL. We believe that it is wise to allow network planners of an operation to define the SBC for a service. E.g., in some operations it might be important to provide frequent high resolution images, while other operations would rather spend the data-rate on other services. In such a setting, an application (service) can be tagged with one SBC in one operation and another SBC in the next. Nevertheless we created an example list of services and signaling traffic for the CoNSIS experiment and associated these with the SBC and IP MPL as shown in table IV. Table V then shows how some selected services from table IV are associated with the topologies created for the experiment.

TABLE V. THE LINK BETWEEN SELECTED SERVICES AND THE DEFINED NETWORK TOPOLOGIES

CoNSIS service	Low data rate topology	High data rate topology	Low delay topology
NFFI Service (AF21)	X	-	-
Chat application (AF22)	X	-	-
VoIP (MELPe 2400) (EF)	-	-	X
Image msg. service (AF11)	-	X	-

For the low data rate interfaces we choose to configure a strict priority queue with no fairness in the packet scheduling. This ensures that the highest priority traffic types are given enough resources. For the high data rate interfaces we use the hierarchical token bucket (HTB) queuing structure for Linux, and associate a share of the shaping bandwidth to each of the QoS-classes. This supports traffic priority but also provides some fairness in the packet scheduling. QoS-classes that need low delay are set up with short queues, as are QoS-classes with periodic traffic where it is important to always get the most recent message.

The *ip6tables* functionality in Linux is used to mark MT-routing traffic with the correct QoS-class. All user traffic in the CoNSIS network is encrypted by IPSec solutions, thus the user traffic must be marked with the correct QoS-class by the source. This marking is also used to associate the QoS-classes with the forwarding table for the correct topology. The Linux traffic control (*tc*) tool is used to setup the queuing and scheduling mechanisms.

C. Tests to be performed during the CoNSIS experiment

To further explain the use of MT-routing in the CoNSIS convoy network we will here briefly describe the three tests we plan to perform during the CoNSIS experiment to demonstrate the functionality of the MT supported QoS architecture. The experiment is being performed at the time of writing, thus results are not yet available. All vehicles referred to by number belong to Nation2 unless otherwise specified.

1) Demonstrate seamless mobility in a heterogeneous wireless network.

In this test we show how link breaks in a mobile military network can be overcome via routes utilizing the different radio networks/link technologies in a coalition tactical network. The test starts with full connectivity (Fig. 3) and traffic among all Nation2 nodes. Vehicles 2 and 4 then move together such that these no longer have Nation2 UHF connectivity with the remaining Nation2's vehicles. The internal traffic for Nation2 will still be flowing among all nodes, but now via the Nation1's UHF and VHF networks. Next vehicle 3 moves so that it loses all Nation2 UHF connectivity, but since it has a Nation1 SatCom terminal, the internal traffic will still be flowing among all Nation2 vehicles. See Fig. 4 for the final network connectivity situation.

2) Test the use of multiple topologies for QoS purposes.

In this test we want to show how topologies can be used to provide different paths for different traffic classes, and also to block traffic at the source for flows that cannot be supported by the current network. The test will be run both for the high data rate topology and for the low delay topology. The test for the high data rate topologi is explained here. The test starts with full connectivity (Fig. 3) and traffic flow from vehicle 1 on both the low data rate topology and the high data rate topology to all other Nation2 vehicles, and traffic flow on both the low data rate topology and the high data rate topology from vehicle 2 to vehicles 3 and 4. Vehicle 3 then moves away to lose Nation2 UHF connection, but it still has a Nation1 SatCom connection (Fig. 6). Vehicle 3 will now only receive traffic from vehicle 1 and vehicle 2 on the low data rate topology. Next, vehicle 2 and vehicle 4 move together to lose Nation2's UHF connectivity to the remaining Nation2's vehicles. Vehicle 4 will now only receive traffic on the low data rate topology from Vehicle 1, but it will still receiver traffic on both topologies from Vehicle 2. See Fig. 6 for the final network connectivity situation. The faded (grey) network links does not participate in the high data rate topology.

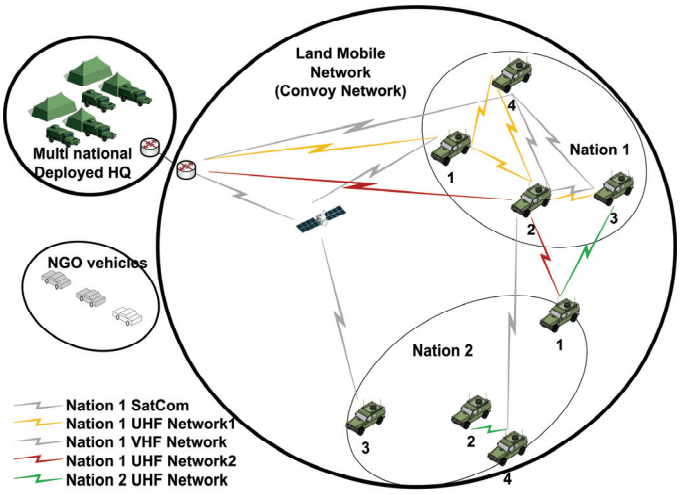

Figure 6. Network connectivity for the final stage of the "MT for QoS purposes" test. The grey network links does not participate in the high data rate topology.

3) Limiting convoy network visibility for adjacent networks.

In this test we demonstrate how multiple routing topologies can be used to control the routes that are advertized in adjacent networks. A topology can be created that holds links/routes that can be made available for transit traffic or for external traffic. Only these routes will then be made available for an exterior

gateway protocol to provide to adjacent networks. For simplicity we will use the high data rate topology to represent this transit topology. A separate topology could very well have been created for this purpose. Also since we have only one gateway between the convoy and the deployed HQ we cannot support transit traffic. Instead we show how traffic from external networks is only allowed to use the chosen topology. We start with full connectivity (Fig. 3) and traffic flowing from vehicle 1 to all other Nation2 vehicles and from the Deployed HQ to all Nation2 vehicles. Vehicle 3 then moves away to lose Nation2 UHF connectivity, but still has Nation1 SatCom connection (Fig. 6). Vehicle 3 will now still receive traffic from vehicle 1, but no longer from the Deployed HQ, since there is no longer a route to vehicle 3 in the topology made available for the exterior gateway protocol. Vehicle 3 will not be visible in the routing tables in the Deployed HQ. All other Nation2 vehicles will still receive traffic from the HQ.

VII. CONCLUSION

In this paper we show how Multi-Topology (MT) routing can aid the design of end-to-end QoS support in the land mobile network defined in the CoNSIS network architecture. The MT-routing protocol builds topologies based on static link characteristics that are valid at all times. We see the use of multiple topologies paired with a DiffServ-like architecture as a simple but powerful tool to dynamically block traffic at the source for flows that cannot be supported by the current network topology, and thereby improve the QoS and available capacity for admitted traffic.

We have also suggested a very flexible interaction between MT supported network domains and Single-Topology (ST) routing domains.

Multiple topologies can also be used to support load balancing on a QoS-class basis (i.e., different QoS-classes are transmitted on partly or fully disjoint paths)

Since this QoS architecture operates based on the code in the IPv6 *traffic class* field, the only requirement to the IP encryption device placed between the issuing application and the wireless transport network is that the encrypted tunnel must inherit the QoS tag of the data packet.

Additional resource management mechanisms based on e.g., polling techniques [25] can be combined with the MT supported QoS architecture to incorporate dynamic changes in e.g., channel quality and traffic load to further improve the scheme for admission control purposes. The resource mechanism must be executed for all defined topologies.

ACKNOWLEDGMENT

We would like to acknowledge the Norwegian Army's weapon school represented by LtCol. A. B. Enger and Maj. M. Gjellerud for the initiative to develop a router demonstrator for QoS experimentation in tactical networks.

We also want to acknowledge all CoNSIS Task 1 participants, and especially Maximilian List and Martin Zeller from IABG mbH for fruitful discussions and very skilled network configuration.

REFERENCES

[1] S. Mirtorabi and A. Roy, "Multi-topology routing in OSPFv3 (MT-OSPFv3)." *draft-ietf-ospf-mt-ospfv3-03.txt (work in progress)*, July 2007

[2] P. Psenak, S. Mirtorabi, A. Roy, L. Nguyen, and P. Pillay-Esnault, "Multi-topology (MT) routing in OSPF." *RFC 4915*, June 2007.

[3] S. Blake et al., "An architecture for differentiated serv." *RFC2475*, 1998.

[4] D. Grossman, "New terminology and clarifications for diffserv." *RFC 3260*, 2002.

[5] M. Hauge, J. Andersson, M. A. Brose, and J. Sander, "Multi-topologyrouting for improved network resource utilization in mobile tactical networks," *MILCOM*, San Jose, CA, USA, 2010.

[6] F. T. Johnsen, T. Hafsoe, M. Hauge, O. Kolbu, "Cross-layer Quality of Service based admission control for Web services," *HeterWMN*, pp.315-320, Houston, TX, USA, Dec. 2011.

[7] L. Hanzo-II and R. Tafazolli, "A survey of QoS routing solutions for mobile as hoc networks." *COMST*, vol. 9, no. 2, pp.50-70, 2007.

[8] R. Asokan, "A review of Quality of Service (QoS) routing protocols for mobile Ad hoc networks." ICWCSC, Chennai, India, 2010.

[9] N. S. Kulkarni, I. Gupta, and B. Raman, "On demand routing protocols for mobile ad hoc networks: A review." *IACC*, Patiala, India, 2009.

[10] P. Jeon and G. Kesidis, "Pheromone-aided robust multipath and multipriority routing in wireless MANETs." *PE-WASUN*, pp. 106-113, Montreal, Quebec, Canada, 2005.

[11] L. Xuefei and L. Cuthbert, "Multipath QoS routing of supporting DiffServ in mobile ad hoc networks." *SNPD/SAWN*, pp. 308-313, Baltimore, MD, USA, 2005.

[12] S. Venkatasubramanian and N. P. Gopalan, "A QoS-based robust multipath routing protocol for mobile ad hoc networks." *AH-ICI*, pp. 1-7, Kathmandu, Nepal, 2009.

[13] L. Chengyong, L. Kezhong, and L. Layuan, "Research of QoS-aware routing protocol with load balancing for mobile ad hoc networks." *WiCOM*, pp. 1-5, Dalian, China, 2008.

[14] A.F.Hansen, T.Cicic, and P.E.Engelstad, "Profiles and Multi-Topology Routing in Highly Heterogeneous Ad Hoc Networks," *INFOCOM, Poster and Demo session*, Barcelona, Spain, April 2006.

[15] J. A. Stine and G. de Veciana, "A paradigm for quality-of-service in wireless ad hoc networks using synchronous signaling and node states." *J-SAC*, vol. 22, no. 7, pp.1301-1321, Sept. 2004.

[16] S. Bae and T. R. Henderson, "Traffic Engineering with OSPF Multi-Topology Routing," *MILCOM* , Orlando, FL, USA, October 2007.

[17] X. Gou, H. Yan, F. Yi, G. Long, and Q. Wu, "Modeling and simulation of small satellite constellation networking using multi-topology routing," *ICCASM* , vol. 12, pp. 143-147, Taiyuan Shanxi, China, October 2010.

[18] Y. Rekhter, T. Li and S. Hares (Ed.'s) " A Border Gateway Protocol 4 (BGP-4)" *RFC 4271*, Jan. 2006

[19] R. Ogier and P. Spagnolo, "Mobile ad hoc network (MANET) extension of OSPF using CDS flooding." *RFC 5614*, Aug. 2009.

[20] Vyatta, http://www.vyatta.com..

[21] Quagga Routing Suite, http://www.quagga.net.

[22] OSPFv3 MANET MDR, Boeing, http://cs.itd.nrl.navy.mil/work/ospf-manet/.

[23] A. Zinin, A. Roy, L. Nguyen, B. Friedman and D. Yeung "Ospf Link-Local Signaling" *RFC 5613*, Aug. 2009.

[24] R. M. van Selm, G. Szabo, R. van Engelshoven, and R. Goode, *Ip QoS standardisation fo the NII*, RD-2933, NC3A,(Nato Unclassified), Apr. 2010.

[25] A. Mohammad, O. Brewer, and A. Ayyagari, "Bandwidth estimation for network quality of service management." *MILCOM*, Orlando, FL, USA, 2007.