Original Article **Open Access**

Frank T. Johnsen*, Mariann Hauge

Interoperable, adaptable, information exchange in NATO coalition operations

DOI 10.2478/jms-2022-0005
Received December 10, 2021; Accepted June 3, 2022

Abstract: This paper summarises our work on policy-enabled inter-network routing for mobile networks and adapting information services to available networking resources in tactical networks. The work shows promise; both the policy routing and adaptive service infrastructure were part of successful interoperability trials in the Coalition Warrior Interoperability eXercise (CWIX) in 2021. This paper highlights our findings, how our work can support interoperability in NATO, and represents an enabler for future coalition operations. Although promising, the work involves research and concept development, and so, we anticipate its timeframe for seeing actual operational use as likely 3–5 years from now, typically targeting future developments within Federated Mission Networking (FMN). In our work, we have shown that we can build a federated mobile network by using a reactive routing protocol that supports policy routing in a network overlay for use in a coalition. Further, we have shown that we can leverage network-level information at the application level, through a so-called cross-layer optimization (CLO) approach. The CLO approach leverages a well-defined format, and we found that this format promotes interoperability and can be used in a multi-national setting. Since our work is experimental, we have also identified some shortcomings for future work.

Keywords: tactical networks, Federated Mission Networking, routing, middleware

1 Introduction

Federated Mission Networking (FMN) (NATO COI Collaboration Portal 2014) is driven by the North Atlantic Treaty Organization (NATO), as an initiative to help ensure interoperability and operational effectiveness of the organisation. A goal of FMN is to support coalition operations by enabling a rapid instantiation of mission networks. The key to this is working towards adoption of common standards and guidelines and to ensure interoperability across the federated systems of the coalition. Here, interoperability is related to technology, processes/procedures and cultural and social factors, i.e., it implies both the ability of computer systems and software to exchange and make use of information, as well as the ability of military equipment (and personnel) to operate in conjunction with each other. In short, the purpose of FMN is to support decision-making in coalition operations by providing the framework for instantiating and deploying mission networks rapidly (so-called zero-day interoperability, implying that there is no delay in sorting out interoperability issues, since FMN shall solve these issues up front).

FMN is developed in increments, called spirals. Each such FMN Spiral includes the respective operational requirements, procedural and technical instructions, architecture, standards and so on, which are documented in FMN Spiral Specifications. Such specifications form the baseline for a certain spiral, and each new spiral builds on previous spirals and expands the overall feature set by refining existing capabilities and enabling new ones. Figure 1 shows the different phases for a spiral specification and the planned timeline for spirals 5 and 6.

As seen in Figure 1, Spiral 5 is currently being specified. Up until Spiral 5, the focus of FMN has been on specifying interoperable services for the Operational Communication and Information Systems (OPCIS). With the introduction of Spiral 5, FMN is also starting to define solutions for mobile forces at the tactical edge in the Tactical Communication and Information Systems (TACCIS) domain. Robust, reliable and efficient mechanisms are needed in such environments to ensure that critical data are delivered in the face of disruptive, intermittent connectivity and low-bandwidth (DIL) environments. Mitigation functions are being defined that will adapt a set of existing FMN services that are already defined in OPCIS to

***Corresponding author: Frank T. Johnsen,** Norwegian Defence Research Establishment (FFI), Kjeller, Norway, E-mail: frank-trethan.johnsen@ffi.no
Mariann Hauge, Norwegian Defence Research Establishment (FFI), Kjeller, Norway.

a format that better suits the networks at the tactical edge. The list of services are as follows: Recognised Ground Picture: Battle Space Objects and Overlays, Friendly Force Tracking [e.g., Blue Force Tracking (BFT)] and Chat. With Spiral 5, FMN will also choose a first set of standardised waveforms as well as specifying basic network functionality that will allow some very basic inter-network operations at the tactical edge. All informed voice (e.g., push to talk) and BFT between TACCIS platforms will also be provided. The FMN roadmap presents increasingly advanced network functionalities and core services at the tactical edge with Spiral 6 and onwards. In this paper, we study functionality that can provide solutions for operational requirements being addressed by new capabilities planned for Spiral 6 and higher.

An important part of FMN Spiral Specifications development is experimentally validating proposed specifications (ref Figure 1), standards and application programming interfaces (APIs). In NATO, the Coalition Warrior Interoperability eXercise (CWIX) is an important arena for systems and network engineers to test innovative solutions and identify technical interoperability issues. At CWIX 2021, experiments were conducted to test interoperability now, in the near term and in the future, aiming to ensure the viability of Communication and Information Systems (CIS) in future coalition deployments and operations.

Federated Information Sharing for Tactical networks (FIST) is a multi-national research project where Germany, USA and Norway participate to research next-generation CIS capabilities for the tactical edge. Specifically, networks, information services and security are focus areas within FIST. As FIST aims to contribute to future FMN spirals, CWIX 2021 was chosen as the test arena for networks and services. FMN is dependent on other bodies to research and propose standards, which FMN can consider and profile in its spirals. In line with this need, FIST aims to investigate standards, approaches and APIs that can function in a coalition force. This paper covers the Norwegian contributions to FIST within the topics networking and information services. Our contribution is a proposal for interoperable coalition routing, as well as an interoperable cross-layer optimisation (CLO) interface for adapting services.

The remainder of the paper is organised as follows: In Section 2, we introduce the scenario and context for the work in FIST. Here, we provide motivation for an adaptive service infrastructure. Section 3 discusses the approach to achieve network interoperability at the tactical edge. Given the availability of such a network, it is important that information services make the most out of the available yet variable communications capacities. Section 4 explores our approach to using information about the available network resources. We adapt information services on the fly to ensure important services are not disrupted when facing throughput limitations. Our work is part of long-term research efforts, and so, even though specific parts of our work function well now, demonstrably so at CWIX 2021, there are still open issues that need to be considered. Section 5 discusses open issues we have identified. Section 6 points to previous and related work, helping the reader see the greater picture of the context and timeliness of the work done within FIST. Finally, Section 7 concludes the paper.

2 Operational context

The NATO Science & Technology (S&T) research task group IST-124 ‘Heterogeneous Tactical Networks’ developed the *Anglova scenario* (Suri et al. 2018, 2019) as a freely distributable operational scenario. The scenario was chosen as the frame for FIST work and experimentation to have a realistic yet unclassified scenario as the backdrop for technology experimentation and exploitation. The Anglova scenario consists of independent parts, forming distinct time boxed parts of the execution of a

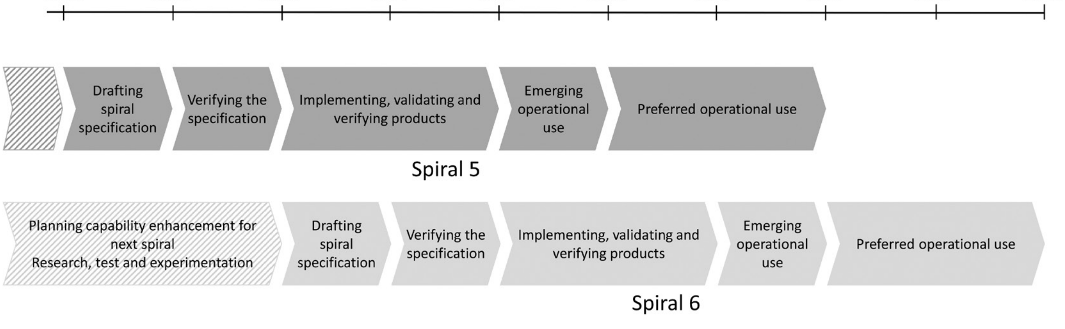

2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
Drafting spiral specification
Verifying the specification
Implementing, validating and verifying products
Emerging operational use
Preferred operational use
Spiral 5
Planning capability enhancement for next spiral
Research, test and experimentation
Drafting spiral specification
Verifying the specification
Implementing, validating and verifying products
Emerging operational use
Preferred operational use
Spiral 6

Fig. 1: FMN spirals. FMN, Federated Mission Networking.

multi-national coalition force operation. There are three such parts, called vignettes, in the scenario:

(1) Planning
(2) Deployment
(3) Urban operation

The first vignette is concerned with gathering information, intelligence operations and planning. Following this vignette, force deployment is covered in the second vignette, which outlines which forces are involved in the operation and their movement patterns to reach the area of operations. Following deployment, the actual operation takes place, which is the topic of the third and final vignette covering the urban operation. Solutions investigated in FIST would be used in tactical networks and so could support communications needs in both the second and third vignette.

For the sake of this paper, we limit ourselves to a small part of this third vignette – urban patrolling – that is sufficient to support the technology discussions we delve into below. We envision a multi-national urban operation consisting of forward deployed headquarters (HQ), where patrols consist of both vehicles and soldiers on foot. This means we have decentralised communications and information gathering going on, as well as variations between platforms and nations in communications equipment that is available. The terrain and buildings obstruct communications; in addition, unit mobility leads to a need for dynamic routing adaptation. Changes to the available communications environment will typically limit communications between units and reach back to the HQ.

A major concern of FMN, and hence FIST, is zero-day interoperability between nations in the coalition operation. In a federation, each nation brings their own units and equipment and host their own services like national Command and Control (C2) systems and other such necessary Information Communication Technology (ICT) services. National services need to support the overall operation, and so, both radios and systems need to be interoperable. Through standard approaches and standardising APIs, interoperability can be achieved. Standardising the various parts of the technology, like waveforms for radio-level interoperability over air, and protocols for routing so that the different nodes may form a network, we may build an interoperable network with resources from several different nations. This is one of the goals in FIST, further explored in Section 3.

Further, standardising transport protocols allows transport layer interoperability, and standardising data formats allows end-user systems, i.e., ICT applications like the aforementioned C2 systems, to exchange information. Tactical communications are challenging due to disconnections, intermittent connectivity and overall limitations in throughput. Facing such conditions, another of the goals in FIST is to make the most out of the underlying communications from an end-user perspective by achieving better than best-effort communications. To share information about these routes from the networking layer to the communications layer, we research a CLO approach that may provide the applications with adequate information to adapt their behaviour to the underlying available communications resources. Specifically, we're experimenting with an API to expose information from the routing protocol.

In this paper, we assume an architecture as shown in Figure 2. The tactical router provides a service with a well-defined API that can be queried for network state information about the heterogeneous mobile military

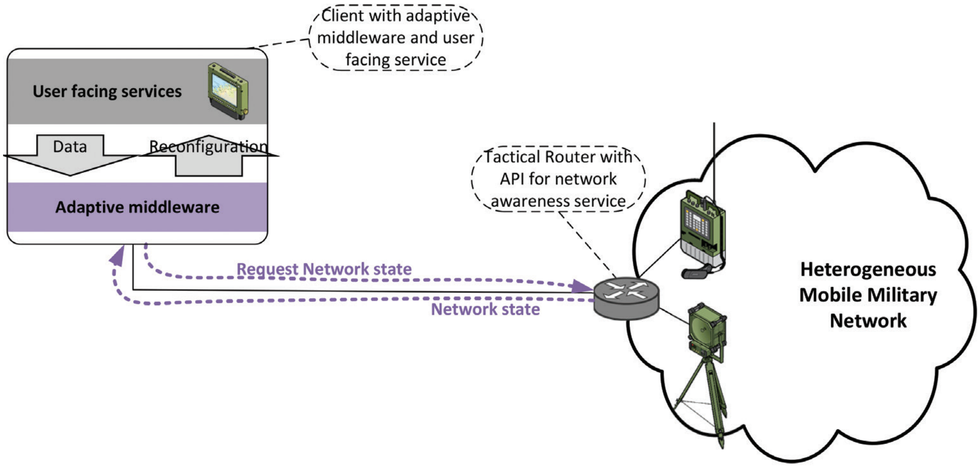

Client with adaptive middleware and user facing service
User facing services
Data
Reconfiguration
Adaptive middleware
Tactical Router with API for network awareness service
Request Network state
Network state
Heterogeneous Mobile Military Network

Fig. 2: Information flow overview between user-facing services (applications), adaptive middleware, network awareness service and tactical router.

network. The adaptive middleware in clients that host the user-facing services can query the service in the router and get information about the network. Based on the information, the adaptive middleware adapts the applications to better suit the current network state. The value of this CLO approach depends on the type of information and the accuracy of the information that the router can provide. We envision that the router as a minimum can provide information collected by the routing protocols. It might also be able to provide other information such as measured delay, queue length, etc. Most routing protocols will only be able to provide very coarse information of the paths such as number of hops and a cost value for the path. Quality of Service (QoS) or policy-enabled routing protocols can give more information about the route. The protocol discussed in Section 3 is of the latter type. It is likely that a tactical router will run different routing protocols on different interfaces. This might complicate the network awareness service on the router. As for the API, a client request with no parameters could return an overview of all known routes. Further, a more refined client request, including destination IP and service type, may be used for a more targeted query and hence a specific response from the service.

Naturally, such a CLO API must also be agreed upon and eventually standardised to be of use in a coalition network. In FIST, we experimented with a well-defined data format for exchanging routing information to support such a CLO approach. This aspect is further explored in Section 4.

3 Network interoperability at the tactical edge

FMN Spiral 5 (and onwards) needs better connectivity at the tactical edge. The aim is to achieve better information flow and coordination between military networks of different platforms, units and nations.

Typically, a range of different wireless transmission technologies with dissimilar characteristics and with tailored routing protocols are present in an operation. This heterogeneity in routing protocols and transmission technologies makes it challenging to build a network of networks in order to realise a common tactical coalition network that can be utilised by all coalition partners.

In FMN, it is expected that participating nations bring national network resources to the operation, and the network infrastructure of the operation will be a federation of the resources provided by the different partners. The purpose of FMN Spirals 5 and onwards is to ensure the necessary interoperability in this network environment. To get the best network performance for different operational conditions, we contend it is necessary to aim for a small set of standards that can be used to build a federated network at the tactical edge. The main reason for having a small set of standards would be to reduce complexity of end-systems and also the cost of building and maintaining such systems. Consider also that there often is a need for more than just one standard. A wide range of operational conditions warrant different approaches to make the most out of the scarce network resources at the tactical edge. The inter-network routing protocol reported on in this section is a promising candidate to support one set of operational conditions.

3.1 Reactive routing in a federated coalition overlay network

The purpose of the inter-network routing protocol is to form a common network based on a number of network resources. The tactical edge network resources that may be present in a coalition operation are as follows:

- One or more wireless networks use a standardised waveform (e.g., NATO wideband or narrowband waveform) as selected by FMN. These waveforms can provide interoperability over the air between all or a subset of the units of the operation.
- A network supporting the loaned radio concept where one coalition partner provides a wireless network and lends one or more radios of this network to coalition partners.
- Resources from national tactical edge networks that the nation is willing to provide to the coalition in order to form a better (more capacity and better connectivity) coalition network.

Our routing protocol work fits the *Interconnect-overlay* architecture, which is one of three routing architectures defined by IST-124 (Hauge et al. 2019). The *Interconnect-overlay* architecture utilises a tier-1 overlay routing domain in order to connect a set of tier-2 routing domains as shown in Figure 3. Only a subset of the military platforms present in tier-2 participate in the overlay. In Figure 3, platform A and B of each nation participate in the overlay routing domain. The overlay nodes are located on what we call *Interconnection platforms*. These are platforms on which two or more of the different network resources in tier-2 can be accessed and thus provide interconnection between these networks. Figure 3

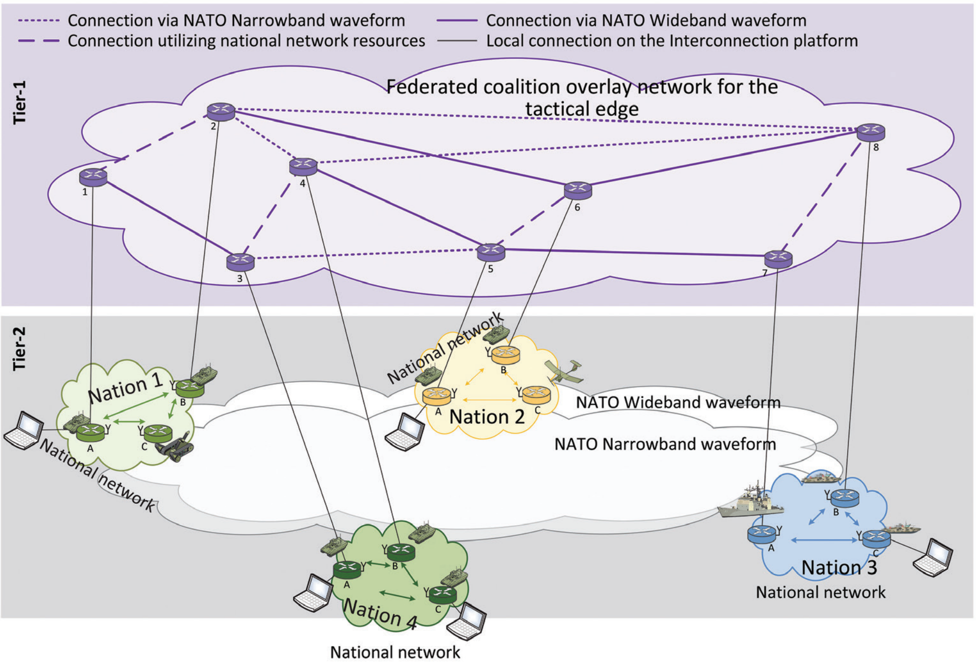

Connection via NATO Narrowband waveform
Connection utilizing national network resources
Connection via NATO Wideband waveform
Local connection on the Interconnection platform
Tier-1
Federated coalition overlay network for the tactical edge
1
2
3
4
5
6
7
8
Tier-2
Nation 1
National network
National network
Nation 2
NATO Wideband waveform
NATO Narrowband waveform
Nation 3
National network
Nation 4
National network
A
B
C
Y

Fig. 3: The *Interconnect-overlay* architecture with six different tier-2 routing domains and the tier-1 overlay inter-network routing domain. Platform A and B of each nation serve as interconnection platforms and participate in the overlay routing domain of tier-1.

shows an example network where two different standardised waveforms (i.e., the waveforms are common to the coalition partners but not necessarily to all) are being used as well as four different nations providing a share of their national tactical edge networks for the federated coalition network. Only a subset of the national military platforms participates in one or both of the standardised tier-2 networks. In order to use the *Interconnect-overlay* architecture in a coalition environment, nations need to agree on a common overlay routing protocol as well as on the information that should flow over a routing information exchange interface between tier-2 and tier-1 routing domains.

The Depth First Search (DFS) Routing protocol (Landmark et al. 2015; Hauge et al. 2020) was used as the tier-1 routing protocol in our work. This is a reactive protocol that does not proactively maintain a routing table but searches for a route when it is needed. The protocol was designed to be narrowband-aware, which means that it is aware of tier-2 protocol domains with little data capacity and can minimise the signalling overhead over those networks. By design, the protocol can also be made to support a range of different policies for how to build routes and utilise the available heterogeneous network resources. As part of the FIST project, Kongsberg Defence and Aerospace (KDA) created a new implementation of the DFS protocols. This implementation also includes the support for very flexible policy routing.

The reactive DFS protocol performs a depth-first search for the route to the destination. This contrasts with the breadth-first searches performed by most reactive protocols, such as Ad hoc On-demand Distance Vector (AODV) (Perkins et al. 2003). The reason for choosing a depth-first search was to better be able to direct the search in order to avoid unnecessary searches over low-capacity networks as well as providing a very flexible policy routing. The basic operation of the DFS protocol is shown with the signalling example of Figure 4. Here, numbered arrows indicate message exchange, whereas the others indicate the state of the DFS state machine.

The DFS protocol used in the tier-1 domain can provide an end-to-end route traversing a number of tier-2 networks to support the following cases:

1. The coalition network should be able to route traffic from one nation's national network to another nation's national network.
2. In situations when the destination national network is degraded such that the network is partitioned in several partitions (e.g., due to mobility, jamming or similar), the tier-1 overlay routing domain should be able to find a route. It must then be able to identify the *Interconnection platform* that has a working connection to the destination (resides in the right partition).
3. When a national network is degraded as described in case 2, it should also be possible to utilise the federated

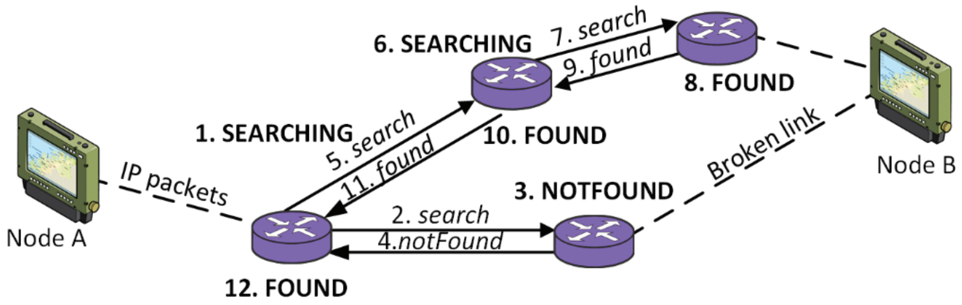


Fig. 4: DFS routing protocol's signalling to search for the route from source node (A) to destination node (B). DFS, depth first search.

Tab. 1: Traffic classes and routing policy rules

Traffic class with some example service types	Policy
High priority traffic that does not consume much data: Examples include BFT and chat without attachments, possibly also (low resolution) pictures associated with important alerts.	Rule 1
High data rate traffic: Examples include streaming video with good resolution, high-resolution pictures and chat with attachments.	Rule 2
Best effort traffic	Rule 3

BFT, blue force tracking.

coalition network to find a route for national traffic between the partitioned national network segments.

4. It should be possible to find a connection through the federated coalition network that fulfils a certain policy requirement (e.g., a certain minimum data rate, utilising only radio resources with low probability of detection (LPD) characteristics, allowing only high priority traffic, etc.)

Successful proof of concept test for the first three cases above was reported in (Hauge et al. 2020). For the work presented here, we have extended the support of the implemented protocol with the fourth case, as well as improved the basics of the routing protocol. This extension gives the necessary functionality to provide detailed information to the network awareness service of Figure 2. The CLO approach enables the middleware and services to adapt to the current network resources as further described in Section 4.

We chose to implement the policy functionality of the protocol with two separate assignments: (1) The coalition must agree on a set of policy rules. These rules and the identification of the rules should be common to all coalition partners of the mission. The rules are not mutually exclusive. They are ordered in a list at the routers, and traffic is tagged according to the first matching rule in the list. (2) Each coalition partner decides locally which rules to allow or deny over which network connection in the share of their national network that is provided for coalition use. The coalition partners should agree on a common allow/deny setting for the standardised waveforms that are common to several partners. This design allows implementing rules and the means to identify the traffic that matches a rule to be separated from the task of tagging the different tier-2 network interfaces with the desired allow/deny policy for the different rules.

In an example mission, we have three traffic classes defined, with associated rules as shown in Table 1.

It must also be defined how traffic can be identified to match a specific rule. In the current DFS protocol implementation, any chosen combination of the classical network fields, e.g., source and destination IP address, port number, protocol type and the type of service (TOS) field in the data packet can be used. This can be extended to include protocol extensions or other identification means in future work. For the experimentation, we have chosen to use the TOS field to assign a policy rule to the traffic flows.

Next, the allow/deny policy for each interface to the tier-1 routers must be set for each for these policies. Consider router number 3 in the tier-1 routing domain in Figure 3 as an example. This router is located on Interconnection platform A in Nation 4's network and Nation 4 administers this router. The router has three interfaces that all participate in the tier-1 overlay routing domain. In addition, it has an interface to Nation 4's national network where the clients from Nation 4 that want to use the coalition network are attached. Nation 4 decides to set the allow/deny policies shown in Table 2 for its three types of interfaces.

The allow/deny policies for the standardised waveforms should be agreed on between all partners that have platforms that can participate in these common networks.

In the current DFS protocol implementation, the allow/deny policies for each interface are statically set in a configuration file in each router. Future work can combine this with modules that monitor the connections or that have a radio to router interface (e.g., Dynamic Link Exchange Protocol (DLEP) (Ratliff et al. 2017)) that can update the deny/allow policies according to traffic load, etc.

Figure 5 shows an example of how two example routes with the rules above can be found in vignette 3 in the Anglova scenario. In this case, we're streaming a video with good resolution from the unmanned aerial vehicle (UAV) of one of the Norwegian platoons to the deployed German HQ. When the German platoon moves closer to the Norwegian platoon, line of sight to the German HQ is lost, and with that the last available high data rate, connection to the HQ is lost and only Rule 1 and Rule 2 traffic can now be supported.

Tab. 2: Allow/deny policies for the defined rules on each interface

Interface	Rule 1	Rule 2	Rule 3
The narrowband waveform interface	Allow	Deny	Deny
The wideband waveform interface	Allow	Allow	Allow
The interface towards the shared national resources (e.g., a tunnel)	Allow	Allow	Deny*

*The nation does not want to allow coalition best effort traffic though it's national network.

3.2 Tests at CWIX 2021

Current DFS protocol software with the policy routing functionality included was tested together with two other *Interconnect-overlay* protocols for the tactical edge for FMN at CWIX 2021. Our test partners were KDA from Norway, our FIST partner Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE) from Germany and also Netherlands Organisation for Applied Scientific Research (TNO) from The Netherlands and International Business Machines (IBM) from Great Britain. The test setup for CWIX 2021 was very similar to the one described here (Hauge et al. 2020). Figure 3 shows the network that was used for the tests. All DFS routing tests were performed with the eight DFS routers of tier-1. The traffic was carried by the tier-2 network types, as shown in Figure 3. Successful proof of concept tests with traffic flows between all participating nations for the four cases described above were tested. For the fourth test case that was not conduced in (Hauge et al. 2020), we showed that the DFS protocol in the tier-1 routing domain was able to set up different routes when different policy rules were invoked. We also showed that when the high data rate connection was removed, such that a route fulfilling Rule 2 could not be found, this flow was stopped, but flows invoking Rule 1 were sustained. A report from these CWIX tests can be found in 'Section 7.3 Objective 3. Coalition Routing Interoperability' of (CWIX-21 2021). For future work, there is a need to do performance tests to get

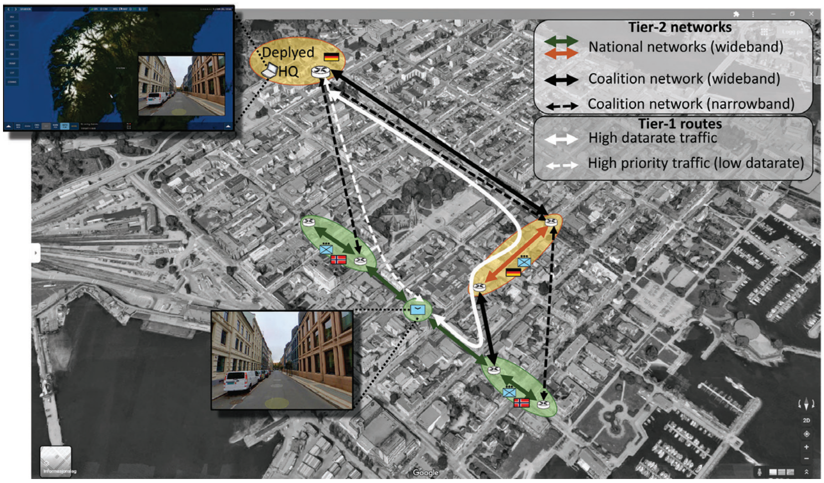

Deplyed HQ
Tier-2 networks
National networks (wideband)
Coalition network (wideband)
Coalition network (narrowband)
Tier-1 routes
High datarate traffic
High priority traffic (low datarate)
Google

Fig. 5: The federated coalition network available to troops patrolling the Wellport city of the Anglova scenario. One of the platoons that carry a UAV that can provide a video footage of the area is shown.

a better understanding of the overhead of this protocol in different scenarios.

4 Middleware and applications

The purpose of this part of the experiment was to investigate approaches to service adaptation. The goal was to exploit CLO to enable services to function better in DIL environments. Our collaboration partner, Fraunhofer FKIE, had identified NetJSON (2015) as a possible data format to extract information from tactical routers. To provide this routing data to the middleware layer, we chose Representational State Transfer (REST) (Fielding 2000) as the service API to promote interoperability and ease of implementation. The aim of this experimentation was to investigate how to support tactical edge service adaptation and interoperability in future FMN spirals. It should be noted that other formats could possibly be used as well, and investigating this could be part of future work. But for the timeframe of FIST, only one format, NetJSON, was identified and investigated.

This chapter summarises the development of the middleware and how it uses NetJSON data to adapt services to the underlying available network resources.

4.1 Adaptive service infrastructure

We built an experimental adaptation middleware, which can digest and exploit network awareness information using a well-defined API. REST (standard connector)+ NetJSON (standard data format), as mentioned above, was the approach to realising and providing such network awareness information (NetJSON 2015). For proof of concept, we conducted several tests in consuming network awareness information. We used the router data for service adaptation in our national prototype middleware.

In principle, the middleware can adapt any type of capability or service. However, in this initial prototyping, we limited ourselves to three services that would serve as examples for the adaptation enabled by the middleware.

The services we provided were BFT with the NATO Friendly Force Information (NFFI) format (NATO 2017), JChat (which is realised by the standard XMPP (XMPP 2004) protocol) for chat and full motion streaming video. These services were based on existing services. The adaptation middleware used network knowledge to configure (and on-the-fly reconfigure) the services when facing variations in resources in the underlying tactical links. The aim was to provide a targeted and carefully considered adjustment of the services to provide a trade-off between functionality, timeliness and availability given the resource situation.

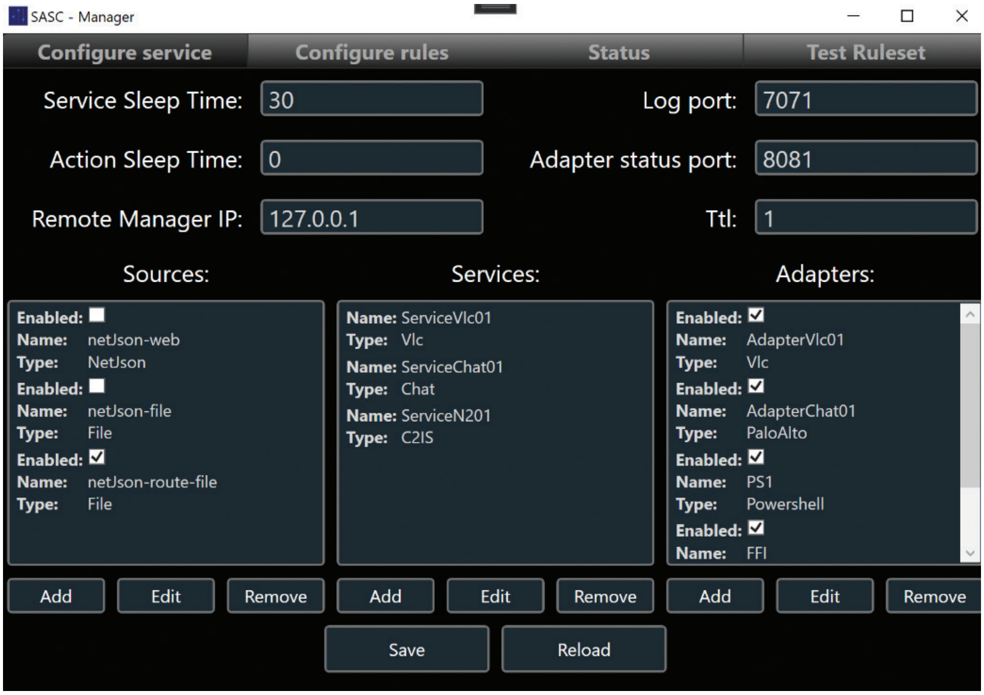
The adaptive middleware, shown in Figure 2, was developed as part of a software contract between FFI and a third-party developer, Sysint AS (Lindholm and Wuttudal 2021). The middleware, called Sysint Adaptive Service Control (SASC), was built on the Norwegian emerging tactical platform TYR, which is a Windows-based platform. SASC consists of a Windows service (SASC.Service) and a manager user interface (SASC.Manager) for configuration of the services and ruleset. The middleware supports gathering network status from a tactical router with the network awareness service API. The middleware currently supports configuring the three services mentioned above, as follows:

- Reconfiguring the network firewall service to block/unblock attachments to JChat.
- Adjusting streaming quality of a VLC media player (VLC) video stream.
- Adjusting the frequency of BFT updates sent by the Norwegian C2 system.

The SASC.Manager application handles all service and ruleset configurations, illustrated in Figure 6. Here, the 'Sources' part is used to configure the NetJSON data source(s), that is, REST service endpoints and NetJSON static files. As is shown in the figure, multiple such sources can be configured at once, and check marks indicate which source is active at any given moment. So, in the provided screenshot, the currently active source is a NetJSON file. Next the 'Services' field is used to define services that should be handled by the middleware. Further, for each service, a set of consumers is defined, which are allowed to access the service in question. This information is used to estimate best configuration, based on links between consumers, the provider and the information gathered from NetJSON. In the screenshot, we have three services configured:

1. ServiceVlc01 – this is the adaptable full motion video service
2. ServiceChat01 – this controls chat functionality by (re) configuring the firewall service
3. ServiceN201 – this is the BFT service, reconfigurable via our middleware

Finally, the 'Adapters' section contains configurations for the various service instances. Here, each service is set up with its IP address, credentials to access/control it and so on. Hence, the adapters section contains information on how to connect to and control specific instances of the



Service Sleep Time: 30
Log port: 7071
Action Sleep Time: 0
Adapter status port: 8081
Remote Manager IP: 127.0.0.1
Ttl: 1

Sources:

Enabled: □
Name: netJson-web
Type: NetJson
Enabled: □
Name: netJson-file
Type: File
Enabled: ☑
Name: netJson-route-file
Type: File

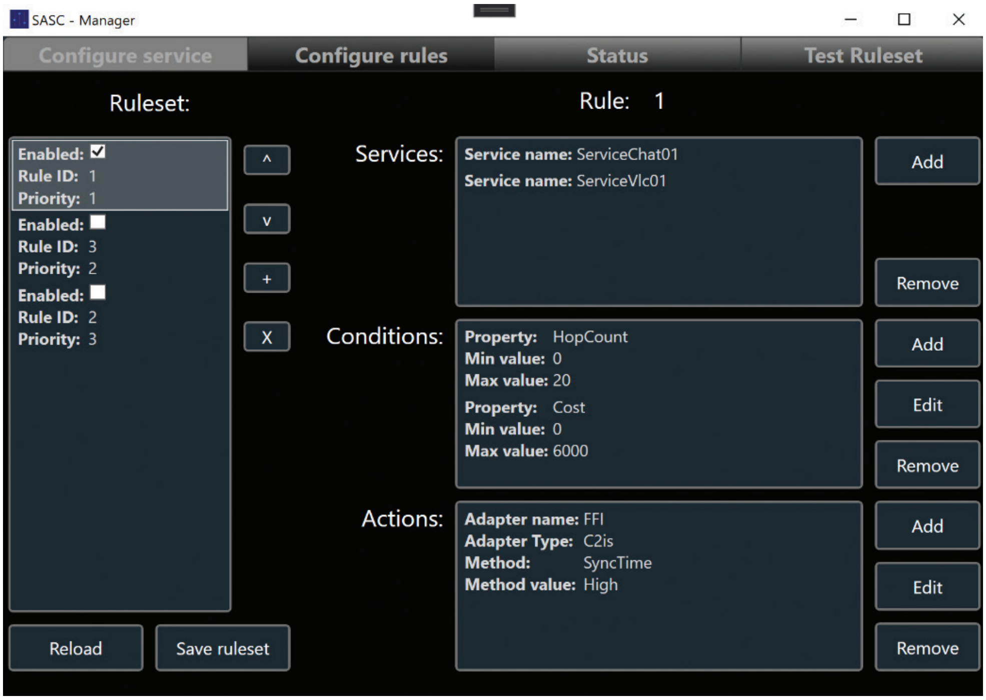
Services:

Name: ServiceVlc01
Type: Vlc
Name: ServiceChat01
Type: Chat
Name: ServiceN201
Type: C2IS

Adapters:

Enabled: ☑
Name: AdapterVlc01
Type: Vlc
Enabled: ☑
Name: AdapterChat01
Type: PaloAlto
Enabled: ☑
Name: PS1
Type: Powershell
Enabled: ☑
Name: FFI

Fig. 6: SASC.Manager sources, services and adapters configuration. SASC, sysint adaptive service control.



Rule: 1

Ruleset:

Enabled: ☑
Rule ID: 1
Priority: 1
Enabled: □
Rule ID: 3
Priority: 2
Enabled: □
Rule ID: 2
Priority: 3

Services:

Service name: ServiceChat01
Service name: ServiceVlc01

Conditions:

Property: HopCount
Min value: 0
Max value: 20
Property: Cost
Min value: 0
Max value: 6000

Actions:

Adapter name: FFI
Adapter Type: C2is
Method: SyncTime
Method value: High

Fig. 7: SASC.Manager rules configuration. SASC, sysint adaptive service control.

generic capabilities defined in the ‘Service’ section of the interface.

Following the setup of Sources, Services and Adapters, the specific middleware rules can be configured. The ruleset consists of one or more rules, sorted in the order of them being evaluated (priority). Figure 7 shows the rules configuration pane of the SASC.Manager application.

In Figure 7, we see on the left side, the ‘Ruleset’ pane, which has a list of the configured rules. The highlighted rule, Rule 1, is then expanded on the right side where details are shown. This part of the manager is used both to create new rules and to manage already existing rules.

In the ‘Services’ pane, the service(s) which this rule applies to are shown. Next, the conditions pane covers which network metrics should be evaluated and sets the threshold values that trigger the rule. Here, we see the rule uses both the HopCount (i.e., number of hops between the service and the consumer) as well as the Cost (i.e., tied to transmission cost, typically the available bandwidth). Note that conditions are evaluated using AND logic, which means that all conditions must be met to evaluate TRUE and trigger the rule.

In the ‘Actions’ pane, the appropriate (re)configuration action to take when the rule is triggered is set up. The SASC.Manager application saves both the service configuration and the ruleset for further use. The middleware operates on cycles, where each service cycle loads the service configurations/rules, fetches the NetJSON data providing a network status snapshot and evaluates the data according to the rules. If multiple sources are used and different network parameters are received for one or more destination addresses, SASC will use the worst received hop count, cost and bandwidth values for each consumer object when validating the status with the ruleset. If conditions are met, the rule is added to a reconfiguration execution queue. The queue is sorted based on rule priority, and only the highest priority rule for each service is executed. This is done to ensure a steady state and avoid multiple rule matches causing multiple reconfigurations of the same service in one cycle. Finally, a (re) configuration of the corresponding service(s) is performed according to the rule(s) in the execution queue. Note that a service cycle is configurable to trigger automatically at pre-set time intervals, or it can be initiated manually through the SASC.Manager tool. The operator has the discretion using the manager tool to configure the rules. To avoid oscillations by triggering reconfiguration too often, we suggest making rules that trigger when major rather than minor changes occur. For example, it has a rule for reconfiguring video from high to low resolution when going from a high throughput (e.g., tactical wideband) network to a low throughput (e.g., tactical narrowband) network. Such a rule will trigger when throughput changes from the megabit range to the kilobits range. Conversely, having a rule triggering a reconfiguration in small increments, e.g., between 10 kbit/s, 20 kbit/s and 30 kbit/s is too fine grained. Hence, rules should reflect the anticipated underlying communications carriers.

CLO brings new considerations for services. Reconfigured services may fall into a new traffic class for the tactical router and would need to be marked accordingly. For example, for the way we adapt chat, a chat session going from wideband to narrowband should also be marked differently, since when attachments are blocked, chat can be accommodated across narrowband.

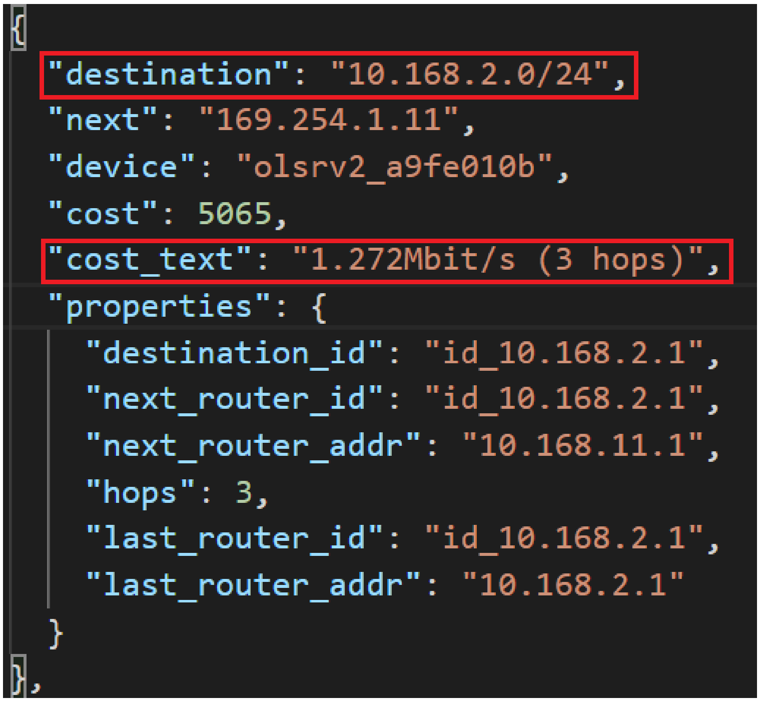
4.2 Tests at CWIX 2021

In FIST, Fraunhofer FKIE, Germany, implemented the NetJSON/REST API and made it available to us at CWIX 2021, where the interface was tested and shown to promote interoperable exchange of network routing information. Benefits identified through these tests were improved service availability and usability at the tactical edge using knowledge of the underlying available network resources.

For these experiments, Germany used their tactical routers using the OLSRv2 (Clausen et al. 2014) routing protocol and specifically built their NetJSON service to expose knowledge this protocol had about the network. Here, cost measures could be a latency value, the number of hops from destination to source, and finally a parameter called ‘cost_text’ contained a string value for the throughput. An excerpt from a NetJSON document, showing one single route, can be seen in Figure 8. The values are dynamic and come from the routing protocol and may change from one invocation of the service to the next. These experiments are further described in ‘Section 7.4 Objective 4. Application & Middleware over Radio’ of the CWIX report (CWIX-21 2021).

5 Discussion

From the findings of each of these two separate work packages within FIST, we have found that it is feasible both to ensure interoperable policy routing at the tactical level, as well as interoperable network awareness for the tactical nodes. The network awareness has been shown to facilitate an adaptable service infrastructure, where the user-facing capabilities are reconfigured in real time. Hence, each of these contributions in themselves are important building blocks and input towards future FMN spirals addressing interoperable solutions at the tactical edge. That said, there are two known shortcomings of the current approach that we will now discuss and propose how to handle as part of future work. These shortcomings include working with both reactive as well as proactive routing protocols and security.



```
{
  "destination": "10.168.2.0/24",
  "next": "169.254.1.11",
  "device": "olsrv2_a9fe010b",
  "cost": 5065,
  "cost_text": "1.272Mbit/s (3 hops)",
  "properties": {
    "destination_id": "id_10.168.2.1",
    "next_router_id": "id_10.168.2.1",
    "next_router_addr": "10.168.11.1",
    "hops": 3,
    "last_router_id": "id_10.168.2.1",
    "last_router_addr": "10.168.2.1"
  }
},
```

Fig. 8: NetJSON excerpt showing a single route.

5.1 Network awareness with reactive vs proactive routing protocols

At CWIX 2021, we consumed network awareness information from a proactive routing protocol. Conversely, the DFS routing protocol discussed in Section 3 is a reactive routing protocol. As the name implies, reactive routing is driven by actual communication needs, in that updating/creating new routes is driven by an initiated communications request. Facing such a protocol, our current implementation will not work ‘out of the box’. It would need to be modified so that it works equally well with both reactive and proactive protocols. In the following, we discuss how our implementation could be changed to be able to interact well also with DFS and other reactive protocols.

Since the goal is developing interoperable solutions and we have shown NetJSON to enable interoperability, we aim to keep the same API that we have already developed also for the interaction with reactive routing protocols. We propose keeping the network awareness service in the tactical router (see Figure 2) and the interaction with proactive routing the same but expand the service behind the API with a slightly different application logic when it interfaces a reactive routing protocol. One effect perceived on the client side (by the middleware) is that there may be a longer delay from querying the service, until it actually gets a response. This can be accommodated by setting a larger timeout on the client side to ensure timeouts are less likely to occur. That means the middleware would work with proactive routing as of now (that will yield an immediate response) and reactive routing. Reactive routing will not provide any awareness information until a route is actually in place, inducing some delay in the responsiveness of the NetJSON service.

When the network awareness service in the tactical router needs to interact with a reactive routing protocol, the service would receive a request from the middleware on a client hosting a user-facing service. Then, the service would, in case a route does not already exist, send a data packet to trigger the routing protocol to start a search for a route to the destination IP address. When a route is found, the protocol informs the network awareness service with known information about the route, such as the number of hops and for the DFS protocol also the QoS/policy rule that the route supports. The service responds with the standardised API to the middleware of the client that requested the network state in formation. So, once the service response is handled by the middleware and the user-facing service has been reconfigured, the route for this communication is already set up and available. The benefit of this approach is that it is fairly simple and will function for any tactical network. Tactical routers with proactive routing protocols will use the service as demonstrated at CWIX, whereas routers with reactive routing protocols will invoke the suggested new function in the service that sends a data packet to trigger the reactive protocol to set up the route before responding to the service call. The drawback of this approach is the varying delay that it might take to send a response to the call.

Currently, our implementation works with a simple REST API with no input parameters, which just fetches the NetJSON resource using a HTTP GET. The response is expected to be a snapshot of all the OLSRv2 routes coded as NetJSON. This approach works well for a service populated with data from a proactive routing protocol. To allow the service to work with a reactive routing protocol, it is necessary to include the required endpoint IP address(es) in the request. Requesting a snapshot of all routes in the network from a reactive routing protocol would invoke much unnecessary overhead. When the router runs a policy-enabled routing protocol such as DFS, the query to the service in the router should also either ask for the availability of a route with certain requirements (e.g., a certain minimum data rate) or a list of available routes with different characteristic to the specified destination address(es). For the first case either the TOS field, an extension header or similar could be used in the query to identify the policy that should be invoked for the route search. As an example, when setting up a chat service, the middleware queries the tactical router for a route that fulfils the high data rate traffic class (see Table 1). If such a route is found, the chat can be sent with attachments and must be tagged such that the tactical router treats it as traffic that applies to Rule 2. If a route that fulfils the high data rate traffic class cannot be found, the chat can be sent as high priority traffic or best effort traffic depending on the importance of the chat messages (must be tagged accordingly) and cannot have any attachments.

Further, there remains the open issue of topology changes in the network after the traffic is initiated. How should the router notify the middleware of this? Currently, since the middleware regularly polls the NetJSON service, this approach would continue to function. However, one could also anticipate another approach that we have not tried, where push communication could be used from the router to the middleware to notify of route changes. This approach is left for future work and could be investigated in a number of ways. For example, it could be achieved by REST long polling or it could be implemented by using a publish/subscribe protocol. Independent of which approach is taken to signalling changes, it is important that oscillations in reconfiguration of services and rules are avoided. We think the best approach to mitigating this problem is to ensure configuring rules that match threshold values of underlying communications capacities (e.g., going from the megabits range of throughput to the kilobits range should trigger a reconfiguration since this would, in the case we have been investigating, mean that we are now switching from wideband to narrowband).

5.2 Security

In our tests, we have shown the feasibility of using the NetJSON data format over a REST API to adapt user-facing services to the available communication resources. The main hindrance we see that will get in the way of rapid deployment of such a solution in the field is the fact that almost all communications between the tactical nodes in military scenarios are end to end encrypted. This means that a tactical node with the adaptive service infrastructure (i.e., middleware software) placed on 'the red side' (i.e., the secure side) will not be able to query the network awareness service in the router. If the middleware is placed on 'the black side' of the crypto (i.e., outside the protected firewall), software will not be able to communicate with (and then ultimately control, adapt and reconfigure) the user-facing services, meaning service adaptation will not be possible.

It is possible to allow information flow from the 'black' to the 'red' side, granted there are policies and mechanisms in place to enable this. We propose keeping the middleware on 'the red side' together with the user-facing services. This means that all we have shown will work, with the exception of the network awareness information being available. To solve this, we propose allowing to expose the NetJSON with REST API on the 'red side'. We can understand and appreciate the need to limit information flow through such an API to mitigate the threat of information leaks and covert channels. Still, using modern security measures on the API itself, it should be possible to enforce role-based (or even attribute based) security measures and access and so limit the exposure (a risk assessment needs to be performed). For example, we could anticipate the service information and clients list being the input into the network awareness API, and the result (given this particular instance of the middleware has the correct credentials and so being authenticated and authorised to access the information) would then just get throughput information back for the service (or set of services) that it needs. This would limit the chances of exploitation on the red side of networking information, as the current approach of coding the entire routing table information, as NetJSON would reveal a lot more information than is strictly needed through this network awareness service. But, limited in such a fashion as we outline here, the middleware would still be able to do its adaptation work, and the threat would be smaller to a coalition network of exposing such a service, as opposed to a service giving a complete routing table as output.

Simplifying the service response would also help alleviate parts of the first problem we discussed, that of expanding network awareness to include not only tactical routers relying on proactive, but also reactive, routing protocols.

6 Previous and related work

The few related works that study inter-network protocols suitable for mobile environments can be grouped in two categories: (1) Proposals for new inter-network protocols suitable for mobile environments. (2) Proposals for modifications to make Border Gateway Protocol (BGP) better suitable for mobile networks. Of the first category InterMR (Lee et al. 2010) is a promising candidate that supports many of the needed features for an inter-domain protocol: (a) partition and merge of domains, (b) membership announcements and (c) support for policy-based routing. The protocol allows existing local routing protocols to be used (including reactive protocols) and uses an overlay of gateways to connect the different mobile ad hoc network (MANET) (Lee et al. 2010) domains. InterMR was also chosen as the baseline for an implementation that was tested at CWIX-21 by one of our CWIX test partners as described in 'Section 7.3 Objective 3. Coalition Routing Interoperability' of (CWIX-21 2021).

Of the second category, BGP with Mobility Extensions (BGP-MX) is a promising candidate that solves the two problems of dynamic BGP-peer discovery and slow convergence time of BGP (Kaddoura and Ramanujan 2011). A distributed peering broker service is implemented, and the BGP peers announce their mobility (stationary, low, medium, high) in order to select more stable paths. (Gibbons et al. 2013) provide a survey of some protocols of both category (1) and (2).

There are also promising attempts to use intra-domain protocols such as OLSRv2 (Clausen et al. 2014) as an inter-domain protocol in an overlay. This is the approach taken by another of our CWIX test partners as described in 'Section 7.3 Objective 3. Coalition Routing Interoperability' of (CWIX-21 2021). All the mentioned related works are proactive protocols. We have chosen to explore the use of a reactive protocol as an alternative to proactive solutions for scenarios where a reactive protocol can be beneficiary.

In (Johnsen et al. 2014), a theoretical approach to leveraging CLO in military networks is discussed, pointing to potential benefits of adopting CLO to make the most of tactical communications resources. Typical hindrances to adoption are also pointed out, in that CLO breaks traditional layered design and so may have adverse effects on interoperability and security. However, the potential benefits of CLO make such approaches intriguing to evaluate and consider when standardising future coalition systems.

Germany leverages CLO nationally in tactical policy routers (Jansen et al. 2015). Here, policies allow assigning a specific portion of the available network capacity to supporting different services. For their approach to work, it is important that the different services adhere to policy and mark the traffic flows with the appropriate traffic class. Recent developments with this approach also include aspects of machine learning. (Möhlenhof et al. 2021) propose an architectural concept for the use of decentralised, machine learning-based reinforcement agents to improve the use of network resources in DIL networks.

Another optimisation vector, beyond that of CLO, is investigating alternate transport mechanisms for services at the tactical edge. Several NATO research task groups have experimented with various such protocols [see e.g., work by IST-150 (Jansen et al. 2021), and IST-161 (Suri et al. 2019)] and have given recommendations to how services at the tactical level may be implemented more efficiently by leveraging particularly low overhead protocols like Constrained Application Protocol (COAP) and Message Queuing Telemetry Transport (MQTT) or bespoke solutions specially tailored to the tactical edge.

The Coalition Networks for Secure Information Sharing (CONSIS) (Eggen et al. 2013) and CONSIS II can be seen as predecessors of FIST. These projects targeted Network Enabled Capabilities in tactical networks, addressing in particular security and interoperability aspects of Service-Oriented Architecture as well as efficient communications for tactical networks. In FIST, interoperability was still the main motivating factor. Specifically, further developments within CLO, services computing, and policy routing are discussed in this paper.

7 Conclusion

In this paper, we have presented our results from applying policy-enabled inter-network routing for mobile networks and adapting information services to available networking resources in tactical networks. We participated in interoperability trials at CWIX 2021, where results show our approach can support interoperability in NATO and be an enabler for future coalition operations. We contend the approach described here, while experimental today (technology readiness level 5), may mature with further work and see operational use in 3–5 years from now (technology readiness levels 7–9).

Through FIST, we have shown the feasibility of a reactive inter-network routing protocol for tactical networks as a candidate to federate available multinational mobile network resources into a common heterogeneous network. This is a low intrusive protocol for scenarios where most of the traffic is local to the different national networks and traffic between nations happens less frequently. Further, we have investigated an approach to obtaining and using network-level information, as provided through a CLO API provided at the tactical router, at the application level. For network awareness, we have tested an approach based on NetJSON data format and REST API, where such routing information as destination, the number of hops and the cost to reach the destination was made available to the tactical node querying the API.

The results this far are promising, and for future work, we propose investigating the open issues that we have identified: Implementing attribute access control to the network awareness service and implementing support for reactive routing protocols in addition to proactive routing protocols in the network awareness service. Possibly, investigating and evaluating alternatives to NetJSON could be useful as well.

References

Clausen, T., Dearlove, C., Jacquet, P., & Herberg, U. (2014). The optimized link state routing protocol version 2. In: *IETF, RFC7181*, April 2014. Available at http://www.ietf.org. [accessed 1 December, 2021].

CWIX-21. (2021). CWIX-21, COMMS Focus Area Report, (NATO UNCLASSIFIED releasable to AUS/AUT/CHE/FIN/GEO/MAR/NZL/SWE/UKR/EU EEAS), 2021, Available at tide.act.nato.int/mediawiki/cwix21/reports/Focus Area/CWIX 2021 Comms Focu s Area Report.pdf (accessing this resource requires a Tidepedia account).

Eggen, A., Hauge, M., Hedenstad, O.E., Lund, K., Legaspi, A., Seifert, H., et al. (2013). Coalition Networks for Secure Information Sharing (CoNSIS) (Invited Paper). In: *MILCOM 2013 – 2013 IEEE Military Communications Conference*, 2013, pp. 354-359, doi: 10.1109/MILCOM.2013.68.

Fielding, R.T. (2000). Architectural styles and the design of network-based software architectures. PhD thesis. University of California, Irvine.

Gibbons, T., Van Hook, J., Wang, N., Shake, T., Street, D., & Ramachandran, V. (2013). A survey of tactically suitable exterior gateway protocols. In: *IEEE MILCOM*, San Diego, USA, 2013.

Hauge, M., Holtzer, A., Hansson, A., Hegland, A., Barz, C., & Velt, R. i. t. (2019). Heterogeneous tactical networks – improving connectivity and network efficiency. Final Report-Annex E” NATO STO, STO-TR-IST-124-PART-I, September 2019. Available at https://www.sto.nato.int

Hauge, M., Mjelde, T. M., Holtzer, A., Drijver, F., Velt, R. i. t., Hegland, A. M., et al. (2020). Inter-network interoperability for heterogeneous networks at the tactical edge. In: *Proceedings MilCIS*, Canberra, ACT, Australia, November 2020. pp. 1-7.

Jansen, N., Kramer, D., Barz, C., Niewiejska, J., & Spielmann, M. (2015). Middleware for coordinating a tactical router with SOA services. In: *2015 International Conference on Military Communications and Information Systems (ICMCIS)*, Cracow, Poland, 2015, pp. 1-7.

Jansen, N., Manso, M., Toth, A., Chan, K. S., Bloebaum, T. H., & Johnsen, F. T. (2021). NATO Core Services profiling for Hybrid Tactical Networks – Results and Recommendations. In: *2021 International Conference on Military Communication and Information Systems (ICMCIS)*, 2021, pp. 1-8, doi: 10.1109/ICMCIS52405.2021.9486415.

Johnsen, F. T., Flathagen, J., Hauge, M., Gjørven, E., Mjelde, T. M., & Lillevold, F. (2014). Cross-layer design and optimizations. FFI-report 2014/00985.

Kaddoura, M., Trent, B., Ramanujan, R., & Hadynski, G. (2011). BGP-MX: border gateway protocol with mobility extensions. In: *IEEE MILCOM*, Baltimore, USA, 2011.

Landmark, L., Larsen, E., Hauge, M., & Kure, O. (2015). Resilient internetwork routing over heterogeneous mobile military networks. In: *IEEE MILCOM*, Tampa, Fl, USA, October 2015. pp. 388-394.

Lee, S. H., Wong, S. H. Y., Chau, C. K., Lee, K. W., Crowcroft, J., & Gerla, M. (2010). InterMR: Inter-MANET routing in heterogeneous MANETs. In: *Proceedings EEE MASS*, San Francisco, CA, USA, November 2010. pp. 372-381.

Lindholm, S., & Wuttudal, O. (2021). FIST Information Services. Project Report, Systint AS, 24 August 2021, 21/01770.

Möhlenhof, T., Jansen, N., & Rachid, W. (2021). Reinforcement Learning environment for tactical networks. In: *2021 International Conference on Military Communication and Information Systems (ICMCIS)*, 2021, pp. 1-8.

NATO COI Collaboration Portal. (2014). What is FMN?, Available at https://dnbl.ncia.nato.int/FMNPublic/SitePages/Home.aspx [accessed 7 September, 2021].

NATO. (2017). NATO Friendly Force Information. STANAG 5527.

NetJSON. (2015). Data Interchange Format for Networks. Available at https://netjson.org/ [accessed 1 December, 2021].

Perkins, C., Belding-Royer, E., & Das, S. (2003). Ad hoc On-Demand Distance Vector (AODV) Routing. In: *IETF, RFC3561*, July 2003, Available at http://www.ietf.org. [accessed 1 December, 2021].

Ratliff, S., Jury, S., Satterwhite, D., Taylor, R., & Berry, B. (2017). Dynamic Link Exchange Protocol (DLEP). In: *IETF, RFC8175*, June 2017. Available at http://www.ietf.org [accessed 1 December, 2021].

Suri, N., Nilsson, J., Hansson, A., Sterner, U., Marcus, K., Misirlioğlu, L., et al. (2018). The angloval tactical military scenario and experimentation environment. In: *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, 2018, pp. 1-8, doi: 10.1109/ICMCIS.2018.8398729.

Suri, N., Breedy, M.R., Marcus, K., Fronteddu, R., Cramer, E., Morelli, A., et al. (2019). Experimental evaluation of group communications protocols for data dissemination at the tactical edge. In: *2019 International Conference on Military Communications and Information Systems (ICMCIS)*, 2019, pp. 1-8, doi: 10.1109/ICMCIS.2019.8842801.

Suri, N., Marcus, K. M., van den Broek, C., Bastiaansen, H., Lubkowski, P., & Hauge, M. (2019). Extending the anglova scenario for urban operations. In: *2019 International Conference on Military Communications and Information Systems (ICMCIS)*, 2019, pp. 1-7, doi: 10.1109/ICMCIS.2019.8842710.

XMPP. (2004). The universal messaging standard. Available at: https://xmpp.org/ [accessed 1 December, 2021].