Tactical Router Interoperability: Concepts and Experiments

Arjen Holtzer[1], Ronald in 't Velt[1], Floris Drijver[1], Henning Rogge[2], Jonathan Kirchhoff[2], Christoph Barz[2], Niels van Adrichem[1], Mariann Hauge[3]
[1] TNO, The Hague, The Netherlands
[2]Fraunhofer FKIE, Bonn, Germany
[3] Norwegian Defence Research Establishment (FFI), Kjeller, Norway
{arjen.holtzer, ronald.intvelt, floris.drijver, niels.vanadrichem}@tno.nl
{henning.rogge, jonathan.kirchhoff, christoph.barz} @fkie.fraunhofer.de
{mariann.hauge} @ffi.no

***Abstract*—Interoperability on the lower tactical levels, e.g. in a multinational battalion or team, poses challenges because of the high degree of mobility and limited data capacity at the tactical edge. Enabling such multi-national teams with direct connectivity can be beneficial since it allows the combination of capabilities from multiple nations and shortens reaction times compared to traditional hierarchical communication models. One target approach for interoperability on these levels is the realization of an IP-based tactical coalition network, in which nations can use different radio equipment, as well as different tactical routers. This paper provides an overview of routing architecture approaches to create heterogeneous tactical networks and focuses on tests and experiments that have been carried out during CWIX 2018 for one of these approaches. In these tests The Netherlands and Germany have shown that multiple national routing domains can be connected via both an embedded and an external route redistribution interface to create IP connectivity between units at the lower tactical level. This approach requires a connected coalition routing domain to which national routing domains connect. The results of the tests can provide input for discussion towards an FMN specification for mobile tactical networks.**

***Keywords*— Tactical Routing, Interoperability, Mobile Tactical Networks, MANET, CWIX, FMN, Experimentation, FIB, DLEP**

I. Introduction

The need for military cooperation between nations during mobile, dismounted and on-foot operations is becoming more pronounced. Technical interoperability of information and communication systems is crucial to support this type of operations and requires technical agreement between partners on different layers: transmission, network, data and applications. In a heterogeneous tactical network multiple radio technologies are in use, which are not necessarily interoperable over-the-air. A common approach is to use tactical IP routers to form a heterogeneous tactical network to which military units can connect and which they can use to share information.

This work was supported by the NLD MoD and DEU MoD.

This paper focuses on tactical router interoperability approaches to create an IP-based mobile tactical coalition network. It presents the results of the Tactical Router Interoperability experiments that were executed in the COMMS Focus Area during the NATO CWIX 2018 exercise. The implementations that were realized for this experiment, address two of the three routing architectures that were defined in the NATO S&T research task group IST-124 "Heterogeneous Tactical Networks" [1]. This paper focuses on one of those architectures: connecting multiple (national and coalition) mobile routing domains using route redistribution. The challenges of route redistribution for mobile networks were presented in [2].

Section III introduces the three routing architectures that were defined by NATO IST-124. The implemented route redistribution concept is described in Section III, while the experiment setup for CWIX 2018 is presented in Section IV. The results of the experiments are described in Section V. Section VI describes related work and is followed by Section VII which contains the conclusions and suggestions for future work.

II. Architectures for Heterogeneous Tactical Networks

There are several approaches to create an IP network at the tactical edge. In this paper we focus on the approaches that aim to achieve connectivity between tactical nodes without requiring sending data through a deployed or static mission network (tactical backbone). In [3] advantages and disadvantages are discussed of such a meshed tactical network approach versus the classical hierarchical tree-based approach that relies on a deployed or static network for connectivity between coalition partners. Ultimately, we envision the network to make the decision to forward data directly via the mobile nodes or via the deployed backbone, whichever is most efficient. Example connections are shown in Figure 1. In addition, autonomous operations, without a connection to the deployed network, should also be possible.

The mobility aspect of tactical operations naturally leads to the fact that an IP-based coalition tactical network consists of one or more Mobile Ad hoc Networks (MANET). In a MANET, a router's Forwarding Information Base (FIB) is typically populated with individual host route entries for other routers rather than aggregated prefixes. The frequently changing topology and the non-transitive nature of links between routers make it difficult to exploit route aggregation. Subnets of application hosts attached to a router are the exception to this rule. The approaches that are described here have different underlying assumptions related to the type of routing protocol that is in use in different nodes of the mobile tactical network as well as the administrative span of control of (parts of) the coalition edge network. NATO IST-124 grouped the approaches as follows:

- Flat routing architecture;
- Interconnect routing architectures.

The flat routing architecture assumes that all nodes in the network run the same routing protocol. Different radios can be connected to this router, but the network topology is kept by a single routing protocol. This approach is described, e.g. in [4], and its description is outside the scope of this paper.

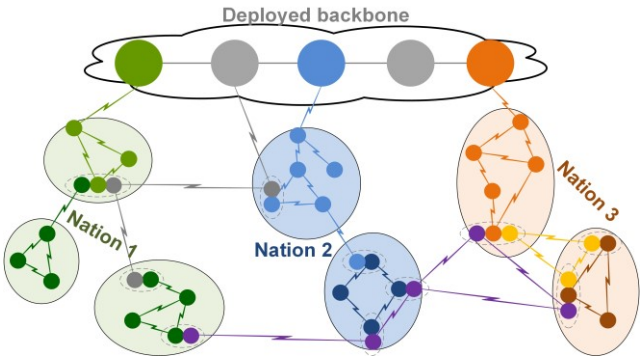

Fig. 1 Mobile nodes connected directly on the mobile domain as well as via the deployed backbone (source: NATO IST-124)

Interconnect routing architectures assume that there are multiple types of tactical routers and routing protocols in the network. These routers need some way of interfacing to exchange the information they have learned about the reachability of the nodes inside their local domains. This interface, as well as the routers exchanging the information are physically located on what we call an *interconnect platform,* which can be, e.g. a tactical vehicle. There are several reasons why multiple routing domains may exist in the network: a) because of separate procurement, nations have acquired tactical routers with different routing protocols, b) some radios have a tailored vendor-specific routing protocol on-board and there are radios from multiple vendors in the network, c) there may be an administrative border between tactical routers, d) the network is too large and using a single routing protocol does not scale, e) the trade-off between acceptable routing overhead and desired speed of reaction to connectivity changes may require a different choice of routing protocol for different parts of the tactical coalition network.

Two flavors of the interconnect architecture have been proposed by NATO IST-124:

- *Interconnect-flat:* interconnecting mobile routing domains using route redistribution without any hierarchy to the routing domains;
- *Interconnect-overlay:* interconnecting mobile routing domains using an overlay routing protocol that keeps an overview of the overall network topology.

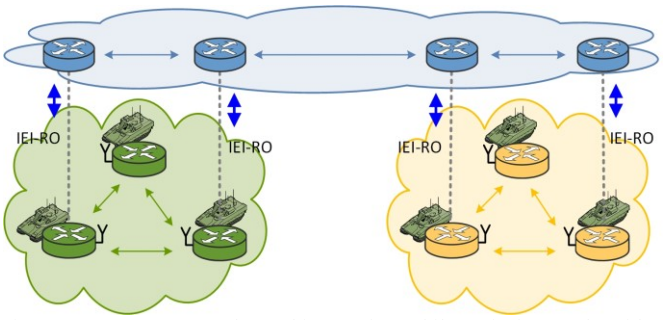

Fig. 2 Interconnect-overlay architecure for mobile tactical networks with IEI-RO as Information Exchange Interface between routers

The interconnect-overlay architecture resembles the architecture of BGP in fixed networks. However, the mobile nature of tactical edge networks with variable link qualities, changing points of attachment between routing domains, and splitting and merging of routing domains make BGP unsuitable for mobile networks, as was described in [5]. Academic proposals for this overlay architecture have been published in [6], [7] and [8]. Since the maturity level of these proposals is relatively low and no implementations were available to the involved partners for CWIX 2018, these approaches were left for future work. The interconnect-overlay approach is visualized in Figure 2. For interoperability, nations need to agree on the overlay routing protocol that is going to be used, as well as an information exchange interface for exchanging routing information between the local routing protocol and the overlay routing protocol (IEI-RO).

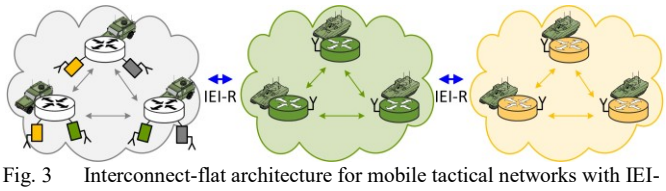

Fig. 3 Interconnect-flat architecture for mobile tactical networks with IEI-R as Information Exchange Interface between routers

The interconnect-flat approach takes mobile routing domains (i.e. MANETs) and connects them by exchanging routing information directly between domains. This approach is visualized in Figure 3. Routing information between domains is exchanged via the indicated information exchange interface IEI-R. It is this approach that is tested in the

experiments reported on in this article. Note that the flat and interconnecting routing architectures can be used in parallel.

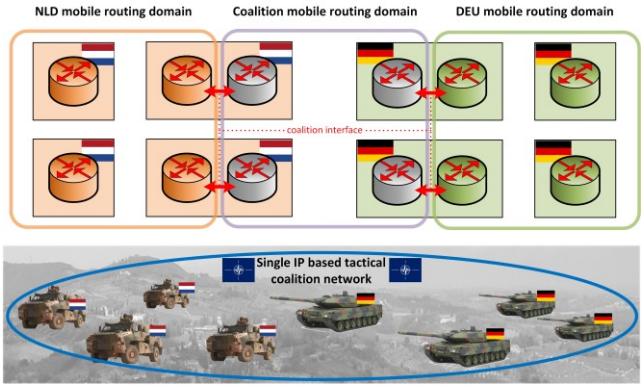

Fig. 4 Tactical router coalition interface connecting national domains to a coalition routing domain

III. The Route Redistribution Concept

The demonstrated route redistribution concept assumes that there are national routing domains and a coalition routing domain. In terms of transmission connectivity, we assume the national routing domains each rely on national radios, while the coalition routing domain uses coalition radios or waveforms. Such coalition capabilities are provided by the nations themselves and run on their operational platforms. This is conceptually shown in Figure 4. Note that there could be more variety (or less) in the radios that are used, but for convenience this setup was chosen. The figure also shows the *interconnect platforms* which run both a national and the coalition routing protocol and as such are hosting the coalition interface.

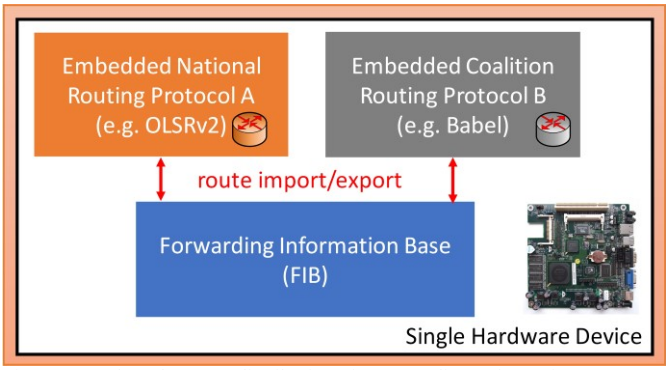

Fig. 5 On-board route redistribution via Forwarding Information Base (FIB)

Route redistribution functionality exists in commercial routers, but this functionality is vendor specific. For CWIX 2018, TNO and Fraunhofer FKIE prepared two different implementations to realize route redistribution via an interface that can be specified for use within the NATO Federated Mission Network (FMN). The aim was to show the opportunities, but also the limitations of using such a state-of-the-art approach when trying to create a tactical coalition network that is predominantly mobile. When route redistribution is executed bidirectionally, routing loops may occur, resulting in degraded or failed communications. Such routing loops can be prevented by manual configurations for specific network connectivity patterns, but a generic robust solution that works under all circumstances has not been reached.

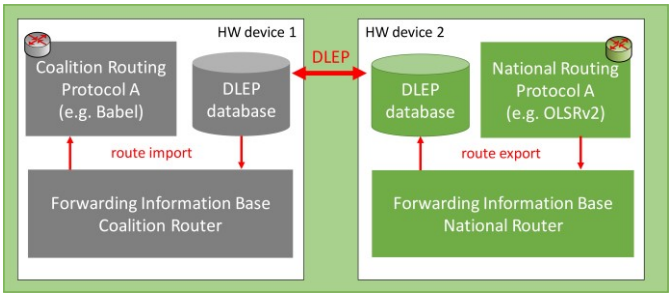

Fig. 6 External route redistribution using extended DLEP

Therefore a one-directional route redistribution method was implemented, in which routes towards nodes in the national domain are imported into the coalition domain. In this way, the coalition routers know where to send packets destined to national nodes that are not part of the coalition network. On the national side of the interconnect platforms, a default gateway is advertised to the national routers. Routers send traffic that is destined to a node that is not reachable via the national routing domain to the closest, in terms of the applied path metric, interconnect platform, which forwards it to the coalition routing domain. This solution promises to be more robust than bidirectional route redistribution, but the drawback of a unidirectional route-redistribution method is that path metrics in the coalition routing domains are not taken into account in routing decisions made in the national domain, and the other way around, potentially leading to suboptimal routes. The use of path metrics across routing domains is not possible in many of today's practical situations, since in many cases different path metrics are used in different routing domains. In a tactical radio environment this may lead to poor routing decisions. Another effect of the unidirectional route redistribution method is that connectivity cannot be maintained in case of segmentation of the coalition routing domain.

Two following two implementations were created and tested at CWIX 2018:

- Single-device route redistribution via the FIB, by TNO;
- External route redistribution between two routing devices using the Dynamic Link Exchange Protocol (DLEP) [9], by Fraunhofer FKIE.

The single-device, embedded, solution is meant for situations where the national tactical routing protocol and the coalition routing protocol are running as separate processes on a single

hardware device, saving physical space. This approach is shown in Figure 5.

In case the coalition and national routing protocol each run on separate devices, information exchange over a connection between them is needed. The Link Identifier Extension to DLEP [10] was implemented to carry the information between the routers. This method is visualized in Figure 6. It should be noted that any other point-to-point protocol could have been modified to transfer this information. DLEP is standardized to implement the radio-to-router interface and not the router-to-router interface (IEI-R). However, since the type of information transferred via DLEP between layer-3 radios and routers is very similar to the information that has to be exchanged between tactical routers, the use of DLEP with the Link Identifier Extension met the requirements for these tests.

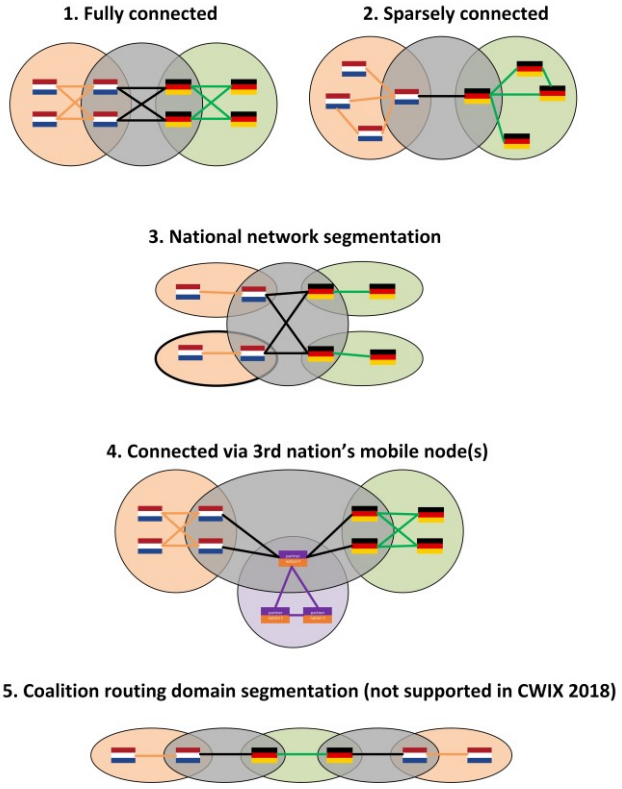

Fig.7 Five topologies for testing tactical router interoperability

IV. Experiment Setup

The experiment focused on connecting two national mobile tactical networks, one from the Netherlands and one from Germany, via a coalition routing domain that can also contain nodes from other nations. Every nation has two types of nodes:

a) *national nodes* that are only part of the national network, and

b) *interconnect platforms* that are both part of the national network and the coalition network.

The interconnect platforms therefore have two radios and two routing protocols. The national and coalition routing domains run different routing protocols to emphasize this fact.

For the experiments, routing protocol implementations were needed that have route import and export functionality. Babel [11] (babeld [12]) and OLSRv2 [13] (olsrd2 [14]) were the routing protocols of choice. In the national domains olsrd2 was deployed and the coalition network runs babeld. To make sure the national routing domains are separated from each other, different radio technologies were used in the national domains. In addition, a hybrid integrated test setup with both emulated radio links and physical radios was used to allow for more diverse testing in terms of both scalability as well as realism.

The Netherlands' interconnect platforms run the national and coalition routing protocols on a single device and use the single-device route-redistribution method, while the German interconnect platforms run the two routing protocols in separate devices, using the external route-redistribution method.

A. Scenarios

The setup was tested for different topology scenarios, showing the possibilities and limitations of the approach. The following five topology scenarios, that are visualized in Figure 7, were defined:

1. *Fully connected:* all coalition routers are within range of each other, all national routers in a single domain are well connected. National nodes may leave and join their national network;
2. *Sparsely connected:* a subset of coalition routers is within range of each other, all national routers of a single domain are well connected. The sparse topology can be dynamic, resulting in interconnect platforms taking over the connection from each other when nodes are moving;
3. *National network segmentation:* the national domain is split up, resulting in two national subdomains, each connected to the coalition network via an interconnect platform, but not connected to each other via national radios;
4. *Multihop coalition domain via an interconnect platform contributed by a 3rd nation:* the interconnect platforms of two nations are out of range and can communicate via one or more interconnect platforms of a 3rd nation;
5. *Coalition domain split:* the coalition routing domain is split up, and needs to stay connected via a national (sub) domain (transit).

These topology scenarios were tested separately. Note that a realistic mobility scenario (e.g. the Anglova scenario [16]) is composed of combinations of these topologies, moving from one situation to the other, on much larger scale in terms of number of platforms in the mission and the number of participating nations.

B. Custom 802.11ah model in NLD and coalition domains

For the national radio domain of the Netherlands and in the coalition domain, EMANE [15] radio emulation was used. EMANE has an 802.11a/b/g model which can be configured between 11 Mbit/s and 54 Mbit/s. In order to reflect a more realistic bandwidth for tactical operations and still have a correct working radio model, TNO adapted the IEEE 802.11a/b/g model to approximate the behavior of IEEE 802.11ah in terms of frequency, bandwidth, bitrate and medium access timing The intention was to have an 802.11 variant that resembles more closely a modern wideband military UHF radio. Realistic (military) radio models for EMANE with lower bitrates were not available to the authors of this paper.

C. Radio setup in DEU domain

In the DEU national domain, real physical radios were used, including military radios, a prototype waveform and civil radio technologies. The military off-the-shelf radio types were Rohde & Schwarz SDTR, ITT Spearnet and Harris RF7800V-HH. The prototype radio used was the Flexible IP waveform developed by Fraunhofer FKIE [4]. In addition, LTE and a WiFi-based waveform with DLEP support were used as commercial off-the-shelf technologies.

D. Node architecture

Each node in the setup contained an EMANE event daemon to receive node positions and a GPS daemon (gpsd [17]) to communicate the node positions to the visualization server. Nodes that were using the EMANE radio model had an EMANE daemon running. Node locations and path loss values were sent to the nodes by the EMANE event server. Nodes were connected to the following channels: a management channel for configuration and manual control of the nodes, an EMANE event channel for exchanging location and path loss events and, for the nodes that connected via an EMANE radio model, an EMANE over-the-air channel for the actual experiment traffic running over the emulated radio links.

E. Visualization

To visualize the experiments, SDT3D [18] developed by the U.S. Naval Research Laboratory (NRL) was used. The setup was used to show (live) all available connections between nodes, both in the national domains as well as in the coalition domain. Different colored lines are drawn based on the reachability of nodes according to each node's routing table. Local Python scripts gather information from the FIB and GPSd and forward this information to a central visualization server running SDT3D. Moreover, the visualizer is able to show the specific chosen route between two selected nodes using the traceroute utility.

Figure 8 shows a snapshot from one of the CWIX experiments. The green lines indicate the connectivity according to the OLSRv2 routing protocol running in the NLD domain, the blue lines indicate the connectivity according to Babel running in the coalition domain and the pink lines indicate the connectivity reported by OLSRv2 running in the DEU national domain. The flags indicate in which routing domain a platform is residing. The yellow line between the white and blue disks visualizes the actual route between two nodes.

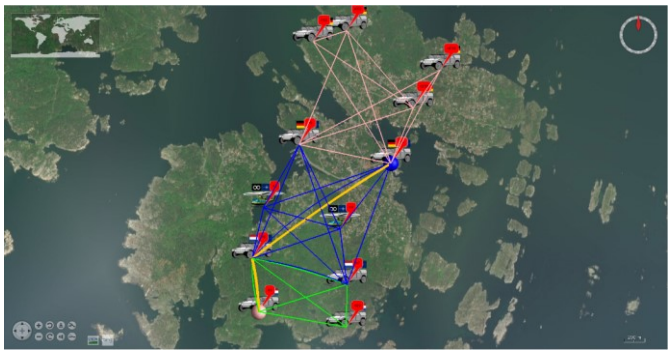

Fig. 8 Visualization of the experiments

F. IP address and routing protocol configuration

To connect IP routing domains at the tactical edge, the IP addresses that are in use in the different national and coalition routing domains must be deconflicted. The use of NAT in the mobile domain does not provide a sufficiently scalable solution and doesn't support mobility scenarios in which the order of the routing domains changes during operations. The external route redistribution mechanism uses point-to-point links over a wire between the national router and the coalition router in the interconnect platform.

In terms of routing protocol configuration, the Hello rate and Topology Control (TC) rate of OLSRv2 in the NLD domain as well as the Hello and Update rate of Babel in the coalition domain were set to 2s and 8s, respectively. The waveforms in the DEU national domain were connected using OLSRv2 with multi topology support and military extensions to combine slow speed (but high robustness and range) with high speed waveforms in a single network. As such, the rates of OLSRv2 were reduced depending on the radio that was attached to the interface and was further adjusted dynamically depending on the number of neighbors.

V. EXPERIMENT RESULTS

The results are presented according to the topology scenarios presented in Section IV that were tested during

CWIX 2018. The tests were mainly functional tests using ping and traceroute. For some experiments MGEN [19] was used as the traffic generator.

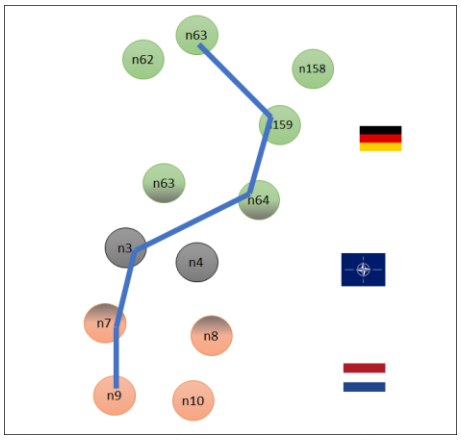

Fig. 9 Path between NLD and DEU nodes via a multi-hop coalition domain, using a 3rd nation's interconnect platforms

A. *Fully connected coalition domain*

In the basic setup all routers in the coalition domain are directly connected to each other (1 hop). The purpose of this test was to see if the unidirectional route redistribution concept functionally works correctly. We observed that destinations to national nodes appeared in coalition routing tables and that traffic to nodes outside the national domain was indeed forwarded to the coalition domain via the interconnect platforms according to the default gateway configuration.

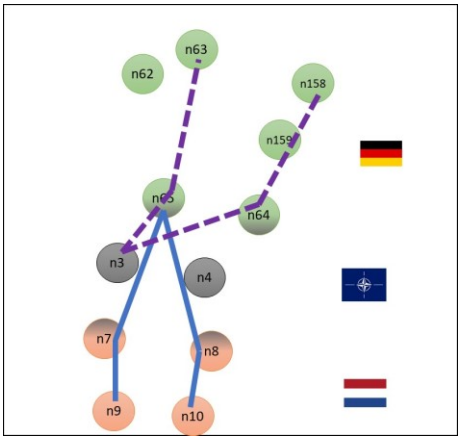

Fig. 10 Connectivity and path during DEU and NLD national domain split (alternative path).

B. *Joining and leaving national nodes*

In this setup, national nodes were disconnected from the national routing domain, resulting in the removal of routes to that node on coalition routers. Then, the national node would be reconnected to the national domain and a route towards the node would reappear in the network. The results showed a functional success. The time it takes for a node to show up in or disappear from the routing table largely depends on the routing protocols that are used in the national and coalition domain rather than on the route redistribution mechanism itself. The results in Section D – *National domain split* show an example of the time it took the routing protocols to converge.

C. *Multi-hop coalition domain*

In this setup, the DEU and NLD interconnect platforms did not have any direct radio connections between each other, and required an additional hop in the coalition domain to reach each other. This was achieved by adding a third nation's interconnect platforms. The connectivity was tested by executing ping and traceroute commands between NLD and DEU national nodes. A 7-hop measured path of this test is shown in Figure 9, which is a schematic representation of the setup shown in Figure 8.

It should be noted that an additional hop is introduced by the interconnect platform, caused by the fact that there are two routing protocols running. The external route redistribution mechanism adds one more additional hop due to the point-to-point link between the routers on the interconnect platforms.

D. *National domain split*

In the national domain split experiment, the radio connections between two groups of national nodes were removed (increased path loss), both in the national as well as in the coalition domain, resulting in two national subdomains of the same nations. Traffic between national nodes in different subdomains should flow via interconnect platforms from the other nation in the coalition domain, instead of directly via national routers. After the split, the national connections were restored and the traffic should again flow directly between the nodes in the national domain. The observed paths during the split NLD domain (between n9 and n10) and the split DEU domain (between n63 and n158) are shown in Figure 10.

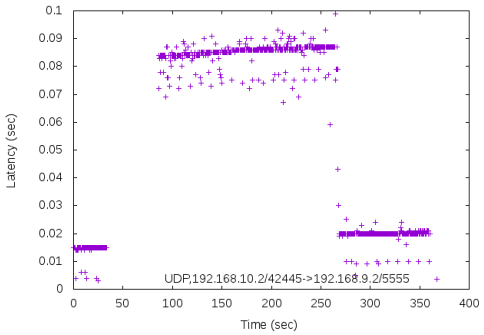

Fig. 11. Data traffic latency between NLD national nodes before, during and after national domain split.

To get a rough indication of the route convergence time, an MGEN UDP traffic flow was generated between the two NLD national nodes 9 and 10. Figure 11 shows the latency of this traffic before (until approximately 30s) during (from approximately 30s until 270s) and after (from approximately 270s and onwards) national domain split for one run. The results confirm the traceroute results showing indeed a longer path (higher latency) during national domain split. It also shows that it took the routing protocols several 10s of seconds to detect the national domain split and find a new route via the coalition domain. The other way around this happened faster and it took in the order of a few seconds to find a path via the national domain. This is related to the convergence time of the routing protocol implementations, which is olsrd2 in the national and babeld in the coalition domain. This convergence time can also be observed in Figure 12, which shows the packet loss during the same test run. More extensive testing on routing protocol performance was out of scope for this activity.

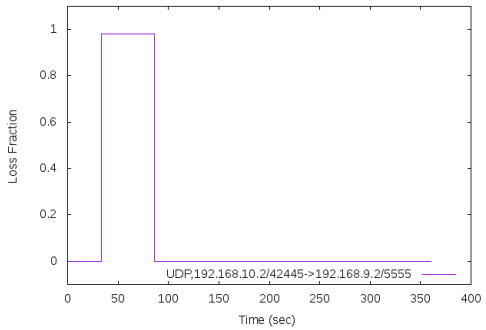

Fig. 12. Loss fraction between NLD national nodes before, during and after national domain split.

VI. Related work

Most work related to mobile ad hoc networks (MANETs) has been done studying a homogeneous environment with one transmission technology (typically 802.11). Only a few studies that we are aware of have looked into the problem of identifying a good routing architecture for heterogeneous networks. In [3] the authors discuss the advantages and disadvantages of tree-based architectures versus mesh architectures. In the report of IST-124 [1] the focus has been on studying different approaches for a meshed architecture.

We sort the solution proposals in literature that can be used to implement the different architectures in three groups: (1) Proposals for new inter-domain protocols suitable for a mobile environment (e.g., [20] [7] [21]); (2) proposals for modifications to make BGP better suitable for mobile networks (e.g., [22] [6] [23]); and (3) proposals for adaptive, hybrid, hierarchical or composite routing that handles both internal and external routing (e.g., [24] [25] [26]). Both (1) and (2) describe protocols that suit the interconnect-overlay routing architecture, whereas (3) describes protocols that suit the flat routing architecture.

The interconnect-flat architecture that is studied in this text is a well-known intranet architecture that is often used when several routing protocols are deployed in an intranet (e.g., a university campus network) [27]. It uses route redistribution between routing protocols that are not strictly ordered. A well-known problem is the risk of routing loops [2]. We have used unidirectional route redistribution in our work to avoid this problem. There exists some literature that studies the use of this technique to connect MANETs to the Internet e.g., [28], but not much that we are aware of that shed light on the advantages and disadvantages of the use of route redistribution to interconnect several military MANETs. Many architecture design documents (e.g., [29]) implicitly assume that some route redistribution is used, but do not study how. In this article we study how route redistribution performs in relevant coalition network cases to provide a better understanding of its use in a mobile coalition network. The study in [30] discusses route redistribution in tactical networks between two MANETs in a simulation setup.

VII. Conclusions and Future Work

The experiments show that tactical route redistribution using the presented unidirectional concept can successfully be used to create an IP-based coalition network in cases where multiple tactical routing protocols are in use. The solution requires a connected mobile coalition routing domain between national interconnect platforms, to which national routing domains are attached. This translates to an operational requirement that military platforms that act as interconnect platforms should make sure to stay connected during a mission, either directly or via a multi-hop connection. A second conclusion is that the coalition routing protocol only takes into account the path metrics of the coalition routing domain, and not those of the national routing domains, and vice versa. This may lead to sub-optimal use of resources. Introducing bidirectional route redistribution or an overlay solution does not automatically solve this issue. A possible approach to enable optimal end-to-end routing decisions across multiple routing domains is to agree on the use of a similar routing metric in each different routing domain. This however poses a challenge, since in current practice different routing protocols and routing protocol implementations often use different path metrics, when it comes to representing the state of wireless links. In addition, there may be cases in which it is desirable to use different link metrics in different parts of the network.

With these considerations in mind the route redistribution concept presented in this paper could be used as a first step in achieving coalition interoperability in mobile tactical networks. From this first step, solutions for more dynamic mobility scenarios should be investigated and developed, as well as ways to efficiently use resources and perform end-to-end routing. These approaches and solutions should be part of future specifications for coalition interoperability at the tactical edge. The results also have an impact on the scalability of tactical networks in general and the integration of layer 3-radios with routing capabilities.

ACKNOWLEDGMENTS

The authors would like to acknowledge the members of NATO Research Task Group IST-124 for discussions and their work on tactical routing architectures.

REFERENCES

[1] M. Hauge, A. Holtzer, A. Hansson, A. Hegland, C. Barz and R. i. '. Velt, "Annex E - Architecture considerations for heterogeneous tactical networks," STO-TR-IST-124, 2018 (to be published).

[2] F. Le, G. G. Xie and H. Zhang, "Understanding Route Redistribution," in *IEEE ICNP*, Beijing, China, 2007.

[3] T. Shake and T. Gibbons, "Architectural Consequences of Domain Formation in Tactical Edge Networks," in *IEEE MILCOM*, San Diego, CA, USA, 2013.

[4] C. Barz, C. Fuchs, J. Kirchhoff, J. Niewiesjka and H. Rogge, "Heterogeneous tactical radio networks with flexible IP-waveforms," in *IEEE ICMCIS*, Oulu, Finland, 2017.

[5] T. Gibbons, J. Van Hook, N. Wang, S. D. and R. V., "A Survey of Tactically Suitable Exterior Gateway Protocols," in *IEEE Military Communications Conference*, San Diego, USA, 2013.

[6] M. Kaddoura, T. B. and R. Ramanujan, "BGP-MX: Border Gateway Protocol with Mobility Extensions," in *IEEE Military Communications Conference*, Baltimore, USA, 2011.

[7] S.-H. Lee, W. S.H.Y., C.-K. Chau, K.-W. Lee, J. Crowcroft and M. Gerla, "InterMR: Inter-MANET Routing in Heterogeneous MANETs," in *IEEE MASS 2010*, San Francisco, CA, USA , 2010.

[8] J. Wang, J. Van Hook and P. Deutsch, "Inter-domain Routing for Military Mobile Networks," in *IEEE MILCOM*, Tampa, FL, USA, 2015.

[9] S. Ratliff, S. Jury, D. Satterwhite, R. Taylor and B. Berry, *RFC8175 Dynamic Link Exchange Protocol (DLEP),* IETF, 2017.

[10] S. Ratliff and S. Taylor, *IETF Internet-Draft - DLEP Link Identifier Extension (draft-ietf-manet-dlep-lid-extension-04) ,* Mobile Ad hoc Networks Working Group, 2018.

[11] J. Chroboczek, *RFC 6126 The Babel Routing Protocol,* IETF, 2011.

[12] *The Babel routing Daemon on GitHub, https://github.com/jech/babeld.*

[13] T. Clausen, C. Dearlove, P. Jacquet and U. Herberg, *The Optimized Link State Routing Protocol Version 2,* IETF, 2014.

[14] *OLSR.org Network Framework - olsrd v2 / DLEP on GitHub, https://github.com/OLSR/OONF.*

[15] "AdjacentLink, LLC. Extendable Mobile Ad-hoc Network Emulator (EMANE)," 20 May 2018. [Online]. Available: https://github.com/adjacentlink/emane/wiki.

[16] N. Suri, A. Hansson, J. Nilsson, P. Lubkowski, K. Marcus, M. Hauge, K. Lee, B. Buchin, L. Mısırhog˘lu and M. Peuhkuri, "A realistic military scenario and emulation environment for experimenting with tactical communications and heterogeneous networks," *Military Communications and Information Systems (ICMCIS), 2016 International Conference on. IEEE,* 2016.

[17] *gpsd - a GPS service daemon, http://catb.org/gpsd/.*

[18] *U.S. Naval Research Lab (NRL) - The Scripted Display Tools (sdt/sdt3d), https://www.nrl.navy.mil/itd/ncs/products/sdt.*

[19] *U.S. Naval Research Lab (NRL) - Multi-Generator (MGEN), https://www.nrl.navy.mil/itd/ncs/products/mgen.*

[20] L. Landmark, E. Larsen and O. Kure, "Resilient internetwork routing over heterogeneous mobile military networks," in *IEEE MILCOM*, San Francisco, CA, USA, October 2015.

[21] B. Zhou, Z. Cao and G. M., "Cluster-based inter-domain routing (cidr) protocol for MANET," in *WONS*, Snowbird, UT, USA, February 2009.

[22] S. Hares and R. White, "BGP Dynamic AS Reconfiguration," in *IEEE MILCOM*, Orlando, FL, USA, October 2007.

[23] I. Okundaye and T. G. S. Kunz, "Inter-Domain Routing for Tactical Mobile Ad-Hoc Networks," in *IEEE VTC2014-Fall*, Vancouver, Canada, September 2014.

[24] C. Barz, C. Fuchs, J. Kirchhoff, J. Niewiejska and H. Rogge, "Extending OLSRv2 for tactical applications," in *ICMCIS*, Brussels, Belgium, 2016.

[25] M. Hauge, M. Brose, J. Sander and J. Andersson, "Multi-Topology routing for QoS support in the CoNSIS convoy MANET," in *MCC*, Gdansk, Poland, 2012.

[26] J. Fang, T. Goff and G. Pei, "Comparison studies of OSPF-MDR, OLSR, Composite Routing," in *IEEE MILCOM*, San Jose, CA, USA, November 2010.

[27] F. Le, G. Xie, D. Pei, J. Wang and H. Zhang, "Shedding light on the glue logic of the internet routing architecture," in *ACM SIGCOMM*, Seattle, WA, USA, 2008.

[28] P. Spagnolo and T. Henderson, "Connecting OSPF MANET to Larger Networks," in *IEEE MILCOM*, Orlando, FL, USA, 2007.

[29] "Maritime and Mobile Tactical Wide Area Networking (MTWAN), ACP 200(D) Volume 2," March 2015.

[30] C. Fossa and T. Macdonald, "Internetworking tactical MANETs," in *IEEE MILCOM*, San Jose, CA, USA, 2010.