Annex B – EMULATION-BASED EXPERIMENTATION AND THE ANGLOVA SCENARIO

Niranjan Suri, Kelvin Marcus and King Lee
U.S. Army Research Laboratory (ARL)
UNITED STATES

Jan Nilsson, Ulf Sterner and Anders Hansson
Swedish Defence Research Agency (FOI)
SWEDEN

Piotr Łubkowski
Military University of Technology (MUT)
POLAND

Mariann Hauge
Norwegian Defence Research Laboratory (FFI)
NORWAY

Boyd Buchin
Rohde & Schwarz
GERMANY

Levent Mīsīrhīoğlu
MilSOFT Yazilim Teknolojileri A.Ş
TURKEY

Markus Peuhkuri
Aalto University
FINLAND

This annex provides an overview to emulation-based experimentation and an overview of the emulation of the Anglova Scenario, which is described in Annex A: "Operational perspective for IST-124". The IST-24 group created the Anglova scenario to perform experimentation, evaluation, and comparison of alternative strategies for connectivity, routing, and QoS in heterogeneous networks. However, the group also identified the value in sharing this scenario with other members of the research community, both within NATO as well as the larger military and academic research community. Therefore, the scenario as well as associated tools to use the scenario are being released in the public domain. Annex C: "Experimentation environment and tools" contains detailed instructions on how to deploy and use the scenario, as well as descriptions of available tools to assist those using the scenario for experimentation.

We wish to highlight that the Anglova scenario as well as a number of accompanying tools to help those wishing to experiment with the scenario have been made available to the research community to use freely. The current distribution is located at several different web sites: http://www.ihmc.us/nomads/scenarios/anglova, http://www.arl.army.mil/nsrl as well as https://anglova.net/.These web sites will be kept updated with any new developments / enhancements related to the Anglova scenario. At the time of writing the IHMC site has most up-to-date information, but this will most likely change over time, thus we recommend the reader to search all sites for the most recent information.

This Annex is organized as follows:

- Section B.1 provides some background and motivations behind the development of the Anglova scenario as well as a discussion of different methods for experimentation with tactical networks;
- Section B.2 goes into further detail on the various elements that must come together for conducting experimentation in an emulation environment;
- Section B.3 presents an overview of the Anglova scenario;
- Section B.4 follows with a more detailed characterization of the mobility patterns in the scenario;
- Section B.5 discusses the radio models and provides an overview of the architecture of a communications node; and

- Section B.6 provides an in-depth analysis of the link dynamics within the scenario, which is an important baseline for conducting experiments using the scenario.

B.1 BACKGROUND

Experimentation and analysis are important steps in the overall research and development process for networks, middleware, and services for military networks. Such experiments need to be conducted using realistic communications hardware, topologies, and military operations to obtain valid results. Typical alternatives include simulation-based experiments, emulation-based experiments, laboratory evaluation with actual hardware, limited field experimentation, and finally live military exercises. Each of these alternatives provides respective advantages and disadvantages and have a role to play in the overall cycle from conceiving an algorithm to developing and deploying components on actual military hardware and systems.

Simulation-based experiments require the least investment in terms of hardware and are quite scalable because the system does not have to run in real time. Hence, a single computer node can simulate very large numbers of entities and accurately model their behavior (and in particular, their communications links). Simulations are also perfectly controlled environments, which makes it easy to repeat tests with the same (or controlled variations of) parameters, collect results, and perform analysis. The drawback, however, is that the components being analyzed must be integrated into the simulation framework. This typically requires that specific programming models be adopted, which are more often than not different from the way these components would be developed for actual use. Hence there is an added cost in designing and building potentially two implementations, one for the simulation environment and one for the actual environment. Moreover, there is the added challenge of ensuring that the parallel implementations do not introduce any differences that invalidate the results obtained by the simulations when deploying the actual components. This is particularly important during continued development and maintenance of the components. For these reasons, simulation-based experiments are ideally suited to the algorithm design phase.

Another challenge is that often the other layers (besides the layer being evaluated) tend to be simplified compared to reality, both due to implementation time/complexity and scalability reasons. Thus, there is a risk that important characteristics have been abstracted away from the simulation environment.

On the other hand, experimentation with actual hardware has its own challenges, mainly in terms of cost and scalability. When using actual hardware in a laboratory setting, the connectivity between radio components still has to be controlled at the RF level to recreate the conditions that the equipment would experience in an outdoor environment. Finally, field experimentation and live exercises provide the best form of validation, but with significantly added cost (especially in the case of live exercises) and are best reserved for final validation of components. The other challenge with field experimentation and live exercises is that they are not repeatable and do not allow control over all the parameters, which makes collecting results and drawing the correct conclusions very difficult.

For these reasons, experimentation with emulation environments provides a good compromise and stepping stone between simulations and using actual hardware. In a typical emulation-based experiment, the software components that are deployed in the experiment are ideally the same components that would be utilized on actual hardware and in the field. Therefore, there is no need to maintain multiple implementations. When changes need to be introduced, it is easier to evaluate them in an emulation environment with the actual software components prior to pushing those components out into the field.

Emulation-based experimentation does introduce its own set of challenges. Scalability could be an issue given that sufficient hardware is necessary to run the actual software components in desired numbers for the experiment to be valid and useful. The recent trends in virtualization have helped to reduce the hardware requirements. Another challenge is the fidelity of the emulation to the real environment. This is particularly a challenge for complex radio models whose behavior depends significantly on aspects such as interference,

terrain, multipath, and other RF propagation challenges. Emulation environments also have a validation and maintenance problem – the software that emulates actual radio hardware must be created, validated, and maintained as the actual radios evolve (or new radios are implemented). However, this does not have to be done as often as with simulation environments, which requires that all components be re-implemented.

Finally, both simulations and emulations require scenarios to drive the experimentation. These scenarios must detail the number and composition of nodes and their hierarchy, the nature and behavior of communications links that are available between these nodes, their mobility as the scenario progresses, and the requirements for communications and information exchange between these nodes.

This annex describes a joint effort by the NATO Science and Technology Organization's IST-124 task group (RTG) on "Heterogeneous Tactical Networks – Improving Connectivity and Network Efficiency" to develop and distribute an emulation environment and scenario. While this effort was undertaken by the group in order to facilitate experimentation within the group, we also recognize the benefits of making such a scenario and environment available to others in the research and development community. Given the focus on heterogeneous networks by the IST-124 group, we have chosen to include elements of surveillance, reconnaissance, C2, and tactical mission execution. The scenario involves a land-based force and a naval task group. We have also included a variety of communications links and both tactical and strategic UAV assets and a transient helicopter. The scenario also includes elements of coalition operations with realistic organization and communications. Coalition operations will have their communication interoperability based on the Federated Mission Networking (FMN) concept [1]. In future FMN spirals, the mobile networks at the tactical edge will be included. In the Anglova scenario, we intended to model connection points to a deployed FMN network in the coalition headquarter node and the tactical operations center node, but these have not been completed as of this writing.

Note that the scenario and environment that have been developed, are primarily modeling the communications aspects of a military operation. We have not attempted to model human activity (friendly or enemy) except for modeling the movement of friendly nodes and high-level information exchange requirements between those nodes. Finally, we have not included any aspects of cyber operations.

B.2 ELEMENTS OF EMULATION-BASED EXPERIMENTATION

Many elements must be combined in order to setup and conduct experiments using an emulation-based approach. This section describes some of the important elements as well as some of the choices we have made for each of these elements. Where possible, we also identify some alternate choices for completeness.

B.2.1 Network Emulation Framework

The network emulation framework handles the actual emulation of the underlying network elements, which typically includes the Physical Layer (PHY – Layer 1), the Media Access Layer (MAC – Layer 2), and sometimes the Internetworking or Routing Layer (Layer 3).

The framework selected for the IST-124 experimentation was EMANE (Extendable Mobile Ad-hoc Network Emulator) [2]. EMANE was selected for multiple reasons – scalability and flexibility being the two primary technical reasons, and easy access and prior experience by some of the IST-124 group members being other deciding factors. EMANE is released as open source and is available for download on GitHub [3], making it very easy to be obtained and deployed. Annex C further describes the deployments that have been utilized by the IST-124 group, which include a distributed deployment over a managed clustering framework called DAVC (Dynamically Allocated Virtual Clustering) as well as a hybrid distributed/centralized deployment over VMware ESXi virtualization environment.

The architecture of EMANE is sufficiently flexible to support different PHY and MAC implementations. Some standard implementations are provided to make it simple to use. These include a generic RF (Radio

Frequency) propagation model that supports multiple antenna types, antenna gain configuration, transmit power, and bit error rates. An 802.11 model is also provided to emulate common Wi-Fi-style networks, along with a prototype implementation of a Time Division Multiple Access (TDMA) MAC. During the course of experimentation, multiple issues were encountered with the standard implementations provided with EMANE. These are further described in Section B.2.2.

EMANE is an emulator and not a simulator, which, as described earlier, has the primary advantage of being able to run actual, deployable code. It also has some disadvantages in terms of scalability, resource requirements, and execution time (i.e., it runs in real time, not faster or slower).

Within EMANE, each network interface that is part of the test environment is handled by an instance of a Network Emulation Module (or NEM), which is responsible for realizing the communications characteristics of that interface. Each NEM is assigned a unique ID within the deployment.

EMANE also supports multiple deployment models – using LXC (LinuX Containers) within a single host, in a distributed manner, where components of EMANE are installed in VMs that execute the code to be evaluated, and in a hybrid manner, where the Network Emulation Modules can be consolidated into a fewer number of hosts (controllers). Therefore, if a deployment requires 24 nodes with one network interface each, the 24 NEMs associated with each of those interfaces could run inside 24 LXC containers, within 24 VMs on one physical node, or with the 24 VMs deployed on multiple physical nodes. Finally, one orthogonal variation is the use of an option called the "raw transport", which allows actual physical hosts or Virtual Machines (VMs) to be used without EMANE running directly on the host or within the VM. The latter is sometimes preferred because it can be used to connect to network devices (e.g., access points, routers) and also because it does not require the installation of any third party (i.e., EMANE) code into the test systems / VMs. Combinations of the above deployment models are also possible.

Another important aspect of EMANE is that it typically only emulates Layers 1 and 2. Layer 3 (routing) is not handled directly by EMANE but would have to be handled by either VMs running routing software or by connecting to physical routers. EMANE can also operate without introducing any routing, which would typically be useful to emulate a one-hop broadcast domain (or one segment – such as a Wireless Local Area Network (LAN) or a Wireless Sensor Network (WSN)).

A related choice in terms of network emulators is CORE (Common Open Research Emulator) [4]. Note that CORE can work in conjunction with EMANE, by relying on EMANE for the PHY and MAC layer emulation. CORE provides a graphical tool that allows users to generate the configuration files that drive deployment of network topologies, including multiple network segments with routing between them. CORE was initially designed to use LXC for the individual nodes but has since evolved to incorporate multiple physical nodes as well as the ability to integrate physical network devices such as routers. CORE is able to deploy standard Linux routing daemons (e.g., quagga).

While primarily a network simulator, NS3 does offer some options for integrating it into an emulation environment [5]. The primary challenge here is to be able to synchronize the virtual clock utilized by NS3 with the physical clocks of the nodes in the emulated environment. Another challenge is exchanging traffic between the emulated nodes and the NS3 simulator components. Initial work on a Real-Time Scheduler and on using the PCAP library supports some deployment of NS3 for emulation or in mixed simulation/emulation environments [6]. OMNET++ [7] is another network simulator that also supports the same ability as NS3 to simulate the lower layers of a communication network in real time for connected nodes.

Another emulation environment is NETEM [8], which is a follow-on to NIST Net [9], one of the first ever network emulation environments. However, NETEM only provides basic control over parameters such as delay, packet loss, duplication, and re-ordering. It does not provide a framework for implementing sophisticated radio models.

Finally, for completeness, we also refer the reader to Emulab [10], which is more than a network emulation framework. Emulab provides distributed and remote access to emulation testbeds and is very popular among researchers. One disadvantage of Emulab is that it was designed to mostly support remote access to an experimentation facility (although it is available to be deployed locally). Another disadvantage is that Emulab primarily models commercial radios, such as 802.11.

B.2.2 Radio Models

EMANE is really a framework that allows different radio models to be incorporated into the EMANE environment. As mentioned before, EMANE comes with a few pre-defined radio models – in particular, the RFPipe and 802.11. The RFPipe model can either accept externally computed path loss metrics or compute them on the fly based on the antenna model, radio characteristics (frequency, transmit power, receiver sensitivity), and node positions. Note that when path loss calculations are done internally (and in real time) by EMANE, it does not take into account terrain effects (e.g., elevation). There is also an initial implementation of a TDMA radio model.

It is worth noting that there are proprietary implementations of various tactical radios, including fairly high-fidelity implementations of currently deployed radios by the US and other militaries. Should the experimenters have access to these high-fidelity models, they would be able to set up high fidelity experiments. However, our goal is to create an open, easy to share emulation environment. Therefore, for this first stage, we modeled all of the radios described in the scenario in this report using only the open source radio models that are easily available and included with the EMANE distribution. In particular, the RFPipe, 802.11, and TDMA models were used to emulate the HF, VHF, and UHF links needed for the scenario we have developed to date. Note that the EMANE configuration files for the radios are also included as part of the Anglova distribution and are further described in Annexes C and D: "IST-124 Experimentation Execution". More detailed radio models for some radios such as the NATO Narrow Band Waveform [11] under development, might be included in future work.

However, we also encountered implementation issues with the current implementation of the radio models. For example, we tried to use the RFPipe model to emulate the UHF medium band network for intra-company communication within the Anglova scenario. While it is possible to limit the transmission rate of a radio using RFPipe, there is no implementation of a Media Access Control (MAC) protocol and consequently no modeling of collisions that might occur with overlapping transmissions. Therefore, EMANE will allow two transmitters within interference range of each other to transmit without detecting and processing collisions. It is also possible for multiple transmitters to simultaneously send data to one receiver and the receiver's data rate will simply be the sum of all the data rates of the transmitters, which may far exceed a realistic behavior of a real radio. The primary reason for this behavior within EMANE is that the RFPipe model is typically used to emulate a point-to-point connection between two radio nodes, and not a multi-node network over a shared medium.

Another problem exhibited by the TDMA model is a strong dependence on a synchronized clock across all the EMANE instances that are part of the same TDMA network. While this would work if all the EMANE instances are deployed on a single node (e.g., using Linux LXC), it does not work with the distributed deployment scenario where EMANE nodes are running in VMs and/or servers on multiple physical systems. Even using the Network Time Protocol (NTP) to synchronize the clock across these nodes does not provide sufficient accuracy to use the TDMA model.

Finally, even the 802.11 model exhibited some limitations in its implementation of the MAC. While not as bad as RFPipe, the 802.11 implementation within EMANE still did not correctly handle collisions at the RF level. For example, consider one receiver (node A) and two senders, B and C, that are simultaneously transmitting to A, with all three nodes within RF range of each other. If both B and C are transmitting simultaneously to A, the resulting data rate should be slightly less than the maximum possible data rate,

assuming some inefficiency in the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. However, the observed behavior is a slight increment in the resulting data rate received at A, which is impossible in reality. Table B-1 shows the results of the overall network traffic received at node A, with the 802.11 radio configured with a maximum data rate of 2 Megabits per second (Mbps). As it can be clearly seen, the data rate creeps up as the number of transmitters increase (which is the opposite of what would be expected). Moreover, the data rate at node A exceeds 2 Mbps with three senders or more, which is impossible if the radio was limited to 2 Mbps.

Table B-1: Results of EMANE 802.11 MAC Implementation.

Number of Senders	Received Data Rate (Kbps)
1	1593
2	1970
3	2664
4	2555
5	3260

It is hoped that future implementations of radio models within EMANE will provide more realistic behavior than what is exhibited currently. There are ongoing efforts within the research community to develop radio models that provide better accuracy and fidelity, as well as to model other types of radios such as LTE. Furthermore, the Anglova scenario and experimentation environment will continue to evolve under the new NATO IST-161 Research Task Group on Efficient Group and Network Centric Communications in Mobile Military Heterogeneous Networks. The radio models that are emulated for the Anglova scenario are described in Section B.5.

B.2.3 Resources and Hosting/Management Tools

The next requirement for experimentation is to be able to deploy the emulation environment and radio models on hardware. For EMANE, VMs are typically used to run the components of the emulation framework as well as the components being subject to experimentation. Resources are also necessary for running any hosting and management tools. Virtualization helps to reduce the number of physical nodes that are necessary, especially with scenarios that involve large numbers of nodes like the one for IST-124. The degree of virtualization can vary quite a bit on the software that needs to be run on the nodes, which can be something very simple, such as routing or transport protocols, to full-fledged C2 tools and services. Resource allocation also depends on the capabilities of the servers (in terms of number of cores, number of CPUs, and RAM available). As a rule of thumb, we try to run one virtualized node per CPU core. EMANE also requires processing resources to handle the network emulation, which, in turn, depends on the complexity of the radio models and on the EMANE deployment model.

Management tools are an equally important concern as the size and complexity of the experiment and scenario grow. Management challenges include deploying and updating large numbers of VMs, starting and stopping the VMs and the experiment code, and isolating one experiment from another. To this end, the US Army Research Laboratory (ARL) has developed DAVC (Dynamically Allocated Virtual Clustering), a set of tools that simplify the lifecycle management of experiments. In IST-124 we have used DAVC to instantiate one or more copy of the emulated network for the Anglova scenario and have also deployed the scenario manually in virtual machines under VMware's ESXi virtualization environment. DAVC is further described in Annex C and Annex D.

B.2.4 Scenarios

The next element required for experimentation is one or more scenarios that can drive the emulation environment (in this case, EMANE). Driving EMANE consists of, at the very least, specifying the positions of each of the nodes as they move through time. Node positions may be updated at any desired rate, depending on the desired level of fidelity and the rate of movement of the nodes. For example, updates could be sent every second, once every five seconds, or once every ten seconds. There is no requirement that this interval be uniform, or that every node's position be updated every update cycle.

Position information for nodes is provided to EMANE through events, which are basically messages sent over a UDP multicast control channel to EMANE. The messages themselves are encoded using Google's Protocol Buffers [12], making it relatively simple to generate and send these messages. In addition to position events, other events that change antenna profiles and radio characteristics are also available. If path loss is computed externally to EMANE, this information can also be sent via EMANE events.

There are multiple ways to generate and send events to EMANE. Example C++ code to generate and send events is provided with the distribution, and we have also developed Java code to do the same. EMANE also provides a command-line tool called EEL (Emulation Event Log) that reads an input file and generates events.

When position data is already available for each node (as in the case of the Anglova scenario), it is simply a matter of playing back the scenario by sending the pre-recorded positions to EMANE. However, if such data is not available, it is also possible to programmatically generate movement behavior for entities such as ground vehicles that are moving over pre-defined routes and UAVs that follow various geometrical paths (e.g., circular as in Figure B-7 and vertical/horizontal scan). Another option is to generate routes for nodes using a set of JavaScript tools that allow a user to click on points in Google Maps to specify waypoints and times. This information is saved off into a route file and then played back by Java code, which interpolates the positions between the waypoints and generates EMANE position update events. Note that these JavaScript tools are available as part of the Anglova distribution.

B.2.5 Candidate Algorithms/Protocols/Software

The next element for experimentation is the set of algorithms, protocols, and/or software that is to be subject to evaluation. IST-124, for example, is using the scenario described in this Annex to experiment with different routing protocols to improve connectivity, Quality of Service (QoS) mechanisms that can work across different network types, data dissemination in sensor networks, and so on. Each of these protocols or middleware components also need drivers or test software to utilize them in a repeatable manner, so that multiple experiment runs will be consistent and the results comparable. The end objective is to duplicate the types of workloads that a live operation might generate, so that we can measure and compare performance of different algorithms, approaches, configurations, and components.

B.2.6 Network Load Generators

An operational network will have a variety of traffic that is generated by a variety of applications. Examples include position updates for friendly and enemy forces, sensor reports, full motion video, Voice over IP (VoIP) traffic, documents and reports, and so on. A controlled experiment that is measuring the performance of one aspect of the network is not likely to be running all of the abovementioned applications. Therefore, recreating the conditions of the operational environment often requires network load generators that recreate the traffic of applications, components, and systems that are not actually present in the scenario. One potential tool that can address this requirement is the ARL Traffic Generation Tool [13], an extension of MGEN (Multi-Generator) [14].

It is worth noting that there are two philosophies when it comes to experimentation. One approach is to have traffic on the network that resembles a realistic environment, and measure how well a protocol performs (for example, how long did a file transfer take given all the other traffic that was also on the network). The other approach is to run the test case in isolation and measure its performance (for example, how much overhead did a discovery protocol generate on the network, or how much bandwidth did dissemination protocol A use compared to dissemination protocol B). The former approach requires network load generators whereas the latter does not. It is also possible to include actual military applications to provide the traffic load in the network, but if these applications depend on user input then either SW must be available to mimic the user's behavior or users must be present (but this is neither scalable nor easy to replicate for repeated tests).

B.2.7 Metrics and Measurements

Arguably the most important part of any experimentation is defining the metrics and collecting the desired results. Some standard metrics are bandwidth utilized, protocol overhead, message loss, latency, jitter, and information availability. Many of these metrics relate to important concerns in military operations (for example, latency relates to staleness of information such as tracks and information availability maps to situation awareness) and can provide important operational feedback. Other protocols and components might have other specific metrics such as convergence time, stabilization time, update time, and reachability. The metrics should be defined ahead of time, as it determines the test software that will need to be written.

The only metric that could be measured somewhat automatically by the emulation testbed is the bandwidth utilized. Sometimes, this is actually non-trivial with EMANE, as the control traffic and EMANE messaging overhead needs to be factored out. One interesting issue is whether the measure includes all traffic generated by any node, or only traffic received by a node. For example, if a node is out of range, the test could choose the measurement to include its transmissions or not. Likewise, if there is packet loss, the measurement could include just the bits received or all the bits that were sent.

B.2.8 Visualization

The last element of an emulation-based experiment is visualization, which is useful for observation as well as demonstration purposes. Visualizations could show real-time (i.e., as the experiment is running) views of the positions and movement of nodes, connectivity between nodes, as well as any metrics being measured, such as bandwidth, latency, failures, etc. These visualizations could also be captured into full-motion video clips for future display or presentation. Finally, individual screen shots are useful to include within publications.

One visualization tool that is already integrated with EMANE is SDT/SDT3D (Scripted Display Tools) [15], built on top of the NASA WorldWind toolkit [16]. Mirage is another NASA WorldWind-based visualization tool that is described further in Annex C.

B.3 OVERVIEW OF THE ANGLOVA SCENARIO

Annex A provides a detailed description of the military operational perspective for the Anglova scenario. This section presents a brief overview followed by more details on the mobility and communication patterns within the Anglova scenario.

The scenario depicts an operation conducted by the company task forces of a mechanized battalion and a naval task group (Figure B-1). It shows the tactical domain located in the fictitious area of Fieldmont in Anglova, where the Coalition HQ (CHQ) of the Military Contingent (MC) is based. As part of the scenario, units, systems and several sensor networks are deployed to the town of Wellport (also in Anglova) and outside the port of Wellport. The operational context of the three envisaged vignettes is highlighted in Figure B-1. The vignettes use the installed Communications and Information System (CIS) and suitable services in order to

exchange information necessary for the realization of the mission tasks. The completion of the tasks requires access to a wide range of systems and communication networks, i.e., radio communications system (HF, VHF, UHF and SATCOM), sensor networks, and UAV systems. Elevated communications relays can be present at different altitudes and on platforms with different levels of endurance to improve connectivity in the mission network. Deployed 4G or 5G cellular systems can also be present in the field.

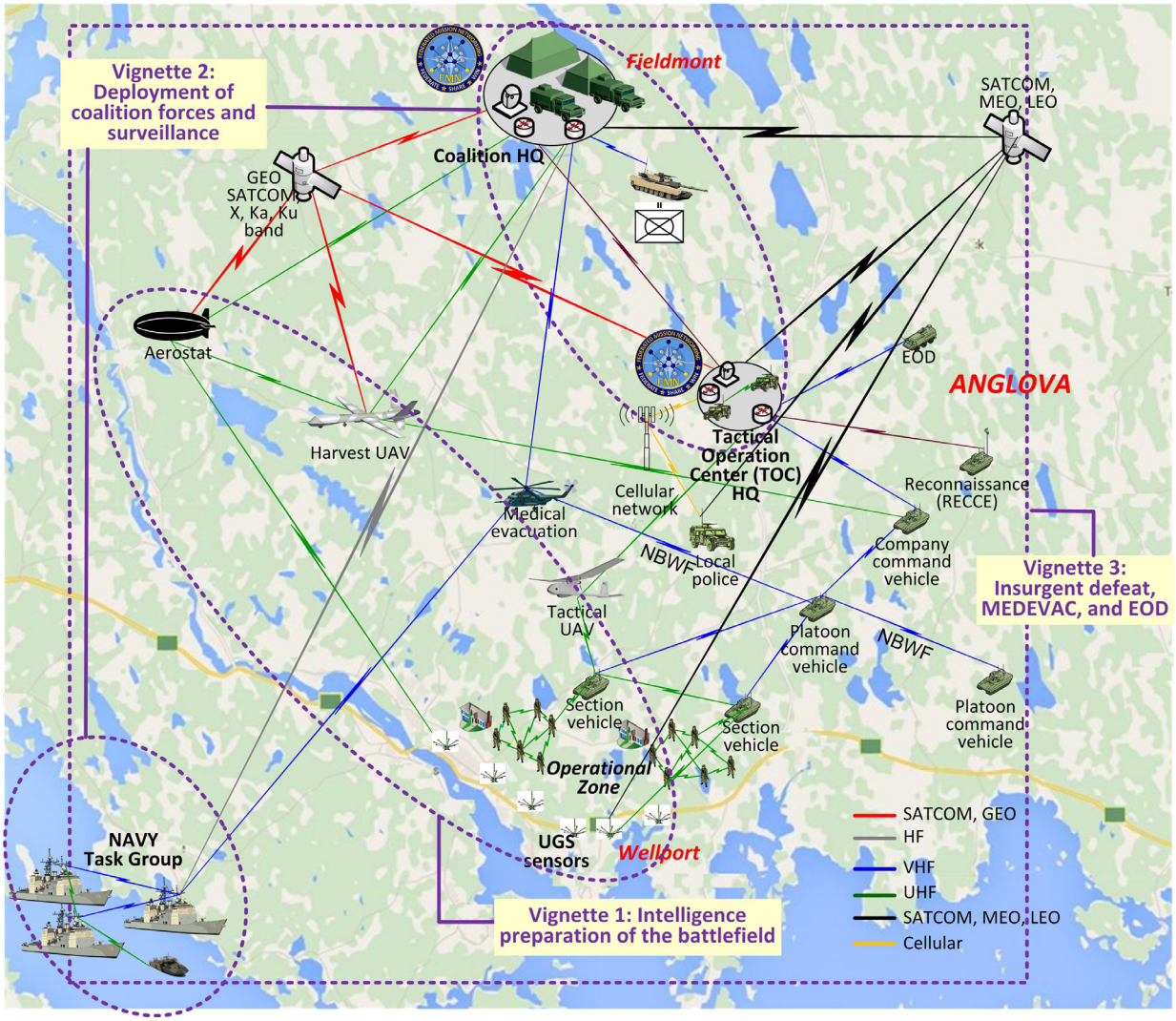

Figure B-1: High Level Operational View of the IST-124 Scenario.

The mechanized battalion is a part of the MC, which plays the reach-back role during the operation and provides Combat Support (CS) and Combat Service Support (CSS) as requested. According to the operational context, it is assumed that insurgent forces have taken up positions in the town of Wellport and are preparing a complex attack against the coalition forces located in the operational zone. The enemies are well armed and operate in an area that can be mined, so there is a chance of IED (Improvised Explosive Device) hazard. The task of the coalition forces is to move into the operational zone, neutralize the insurgents, and to destroy the armaments they have collected. It is very important to avoid civilian casualties and to reduce the probability of the insurgents escaping. The most important elements in this mission are CIS, logistics, and medical support, which are provided by Coalition Forces. A functional and reliable communications infrastructure is essential to help organize the armed forces. The battalion CIS is connected to the Coalition network (FMN).

The Naval Task Group is present to support reconnaissance and surveillance activities, as well as provide Maritime interception and interdiction operations to control the flow of arms and goods into and out of Anglova. The individual ships have basic radar, Automatic Identification System (AIS) and Electronic Support Measures (ESM) systems connected to their C2 systems. Each of the task groups perform operations within Line of Sight (LOS) of at least one other ship in order to utilize LOS connectivity with the group. But there are occasional inevitable positional displacements and, as the operational situation dictates, temporary detachment of small groups for missions like patrols, search and rescue, and reconnaissance missions. These situations require connectivity with the use of BLOS networks.

Three main vignettes are defined in order to implement the actions included in the scenario. The roles and actors are the same for each vignette. The first vignette covers intelligence preparation of the battlefield by deploying sensor networks and gathering surveillance information. The sensor network gateways have a SATCOM-based channel for notification of events but the bulk of the data from the sensor networks is exfiltrated via a UAV that harvests the data and provides it to CHQ (using a Disruption Tolerant Networking (DTN) style communication pattern). The sensor network is mostly static, except for the harvesting UAV. The naval component is also involved in this vignette, supporting the surveillance and reconnaissance efforts. While some details of this first vignette have been defined, it has not been fully developed as of the writing of this report and will likely be completed in the future. Instead, the IST-124 group primarily focused on Vignette 2 and 3, which have significantly more mobile nodes and hence present more interesting scenarios from a mobility and network dynamics perspective.

The second vignette covers deployment of the coalition forces into the operational zone. The forces that are moving into operational zone use VHF connections for their own interoperability and operability with MC forces. However, it is assumed that as the forces move away from the CHQ, they can lose this connection due to range and may require the use of a SATCOM link for communications to the CHQ. Another option is to use an organic tactical UAV as a communication link or use deployed UAV's at higher altitudes for the connection to the CHQ. These assets can also be used to improve the communication within the deploying force. The second vignette is the most developed of the three and consists of 157 mobile ground vehicles, the coalition headquarters node, a UAV (with three different configurations for its altitude), and 21 ships that are part of the naval contingent. This vignette runs for 130 minutes in total. Note that the second vignette is primarily set in a rural environment, with the ground movement primarily consisting of vehicles that make up the six companies within the mechanized battalion.

Finally, the third vignette describes neutralization of insurgents and IEDs and medical evacuation of wounded soldiers. This vignette includes an attack of the enemy positions as well the use of a Medevac helicopter. It is also assumed that there is suspicion of explosives being detonated by the enemy, which requires the support of an EOD (Explosive Ordnance Disposal) team to minimize casualties and damage. Also, the Naval Task Group, which is deployed near the area of operation, supports the medical evacuation tasks of the mission. Communications with the Navy uses HF and VHF links although a strategic (high altitude) UAV asset provides an intermittent communications relay as well. The third vignette is set in an urban environment and drills down to operations at the squad level.

Each vignette describes data that are expected to be exchanged between the actors and C4ISR equipment used in a way that emphasizes the challenges of connectivity and network efficiency of heterogeneous military networks. The data exchange requirements are outlined in Annex A.

B.4 MOBILITY PATTERNS IN THE SCENARIO

One of the significant contributions of the scenario is detailed mobility patterns of a complete battalion over the course of two hours, as it moves from the starting point towards the objective. This is the troop deployment vignette (Vignette 2) within the scenario and is particularly significant because the positions of

each vehicle (and consequently the movement over the course of time) has been developed by military experts in planning and performing real exercises.

The modeled battalion consists of six companies: four tank companies each with 24 vehicles, one command and artillery company with 22 vehicles, and one support and supply company with 39 vehicles. Altogether, there are 157 vehicles, with each one being a network node. The CHQ and an airborne node has also been added to this vignette – a strategic UAV asset that can act as a communications relay and provide persistent surveillance capabilities.

The mobility pattern of the battalion models action north of Wellport in Anglova. The task for the battalion during Vignette 2 is to deploy the forces close to the town of Wellport in order to setup for counter-insurgency operations within the town (Vignette 3). The area selected for the troop deployment vignette primarily consists of hilly terrain covered by forests. The mobility pattern is characterized by movements mainly on large and small roads over a rather large area, a 14 km by 33 km rectangle. The speed of the vehicles varies, with speeds up to 60 km/h on the main roads. The battalion starts out by moving in a single column on one main road from the CHQ. After about 10 km, the battalion splits up over two main roads and after about 25 km splits up further onto many roads grouped in companies. Towards the end, the battalion finally splits up to the level of platoons. Altogether, the original mobility pattern is roughly two hours long [17] and is shown in Figure B-2.

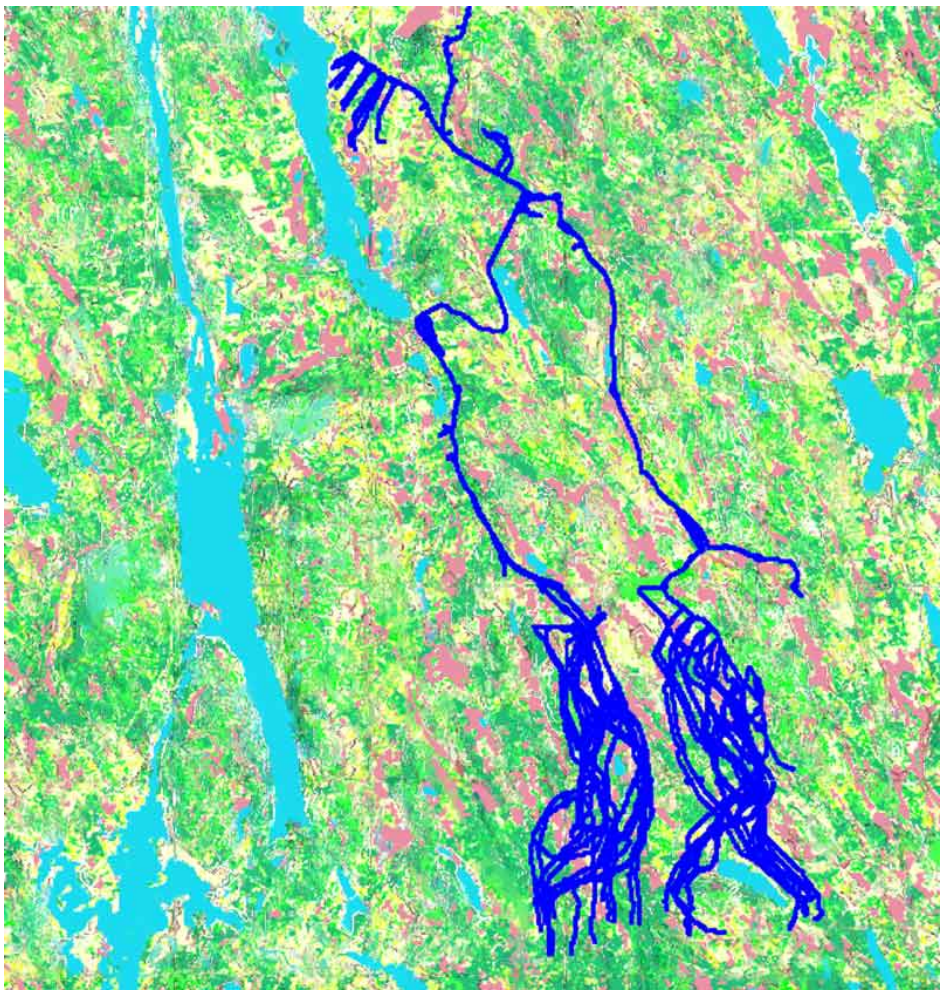

Figure B-2: Tracks in the Troop Deployment Vignette – Movement is from Top to Bottom.

To estimate the network performance, assumptions about the communication networks and the propagation environment are required. The basic path loss is calculated for an antenna height of 3 m for the moving vehicles. The antenna height at the CHQ is 20 meters. Furthermore, the pathloss was calculated for both a 50 MHz frequency and a 300 MHz frequency. This allows the experimenter to choose different radio characteristics for the vehicles as part of the configuration and setup of the experiment. For example, one possibility is to select the 300 MHz frequency for the vehicles within the same company (i.e., the intra-company network) and the 50 MHz frequency for communications between the companies and the Coalition HQ. Alternatively, the 50 MHz frequency could be selected for all the nodes.

The path loss values were also calculated between a UAV and the other 158 nodes in the scenario. Three configurations were chosen for the UAV altitude: 50 meters, 100 meters, and 500 meters. The calculations were also made for two frequencies: 50 MHz and 300 MHz.

Within each company, two vehicles are capable of acting as gateways, as they have two radios onboard each vehicle. Different frequencies could be chosen for each of these two radios. One could be part of the intra-company network and the other could be part of the inter-company (and UAV) network. All of these options provide many choices in terms of realizing a specific, desired configuration for the nodes within the emulation environment.

These path loss values are subsequently used in estimating achievable data rates. We use a Uniform Theory of Diffraction (UTD) propagation model by Holm [18] [19] to estimate the path loss between each node pair. We use a digitized terrain database, which adds significant realism to the communications model than a simple free space propagation model based on distance.

Finally, Vignette 3 provides the mobility models for the urban operation within the town of Wellport. Figure B-3 shows an overview of the mobility within the third vignette and is divided into three phases. The top part of the figure shows the ingress into the town of Wellport. The second part in the bottom left shows the mobility pattern leading up to the insurgents being neutralized. Finally, the third part in the bottom right shows the medevac activity, which is the last part of Vignette 3.

It is important to note that all of the detailed position data, along with the pairwise path loss data, updated every second over the two hour period, is included in the scenario. Mobility patterns and path loss for the Naval Task Group as well as UAV nodes and all actors in the third vignette has also been modeled.

The naval Task Group of the Anglova scenario is part of both Vignette 2 (troop deployment) and Vignette 3 (urban operation). One Task group is formed along the coast of Anglova. The Task Group is under the operational control of Fleet Commander / Maritime Interdiction Force (MIF) Commander located in Coalition Head Quarters. The task group consists of one command ship holding the flag officer and 20 other surface vessels. There is also one multipurpose helicopter, which provides MEDEVAC duties within the task group. Each of the task units perform operations within LOS of at least one other ship in order to utilize Line of Sight (LOS) connectivity with the group, so that they can take advantage of V/UHF frequency band for communications. However, in some situations, HF communications is utilized when LOS is not possible.

Pathloss generation for the naval platforms in Vignette 2 and for all platforms in Vignette 3 was accomplished by using the open source SPLAT! (Signal Propagation, Loss, And Terrain analysis tool) program [20] using Longley-Rice model. Topographical information was imported from the 3-arc second Shuttle Radar Topography Mission (SRTM) data, which is publicly available. These calculated pathloss values for the ships is also available as part of the Anglova distribution (see Annex H: “Naval Task Group and Routing Experiments” for more details about the modeling of the Naval Task Group).

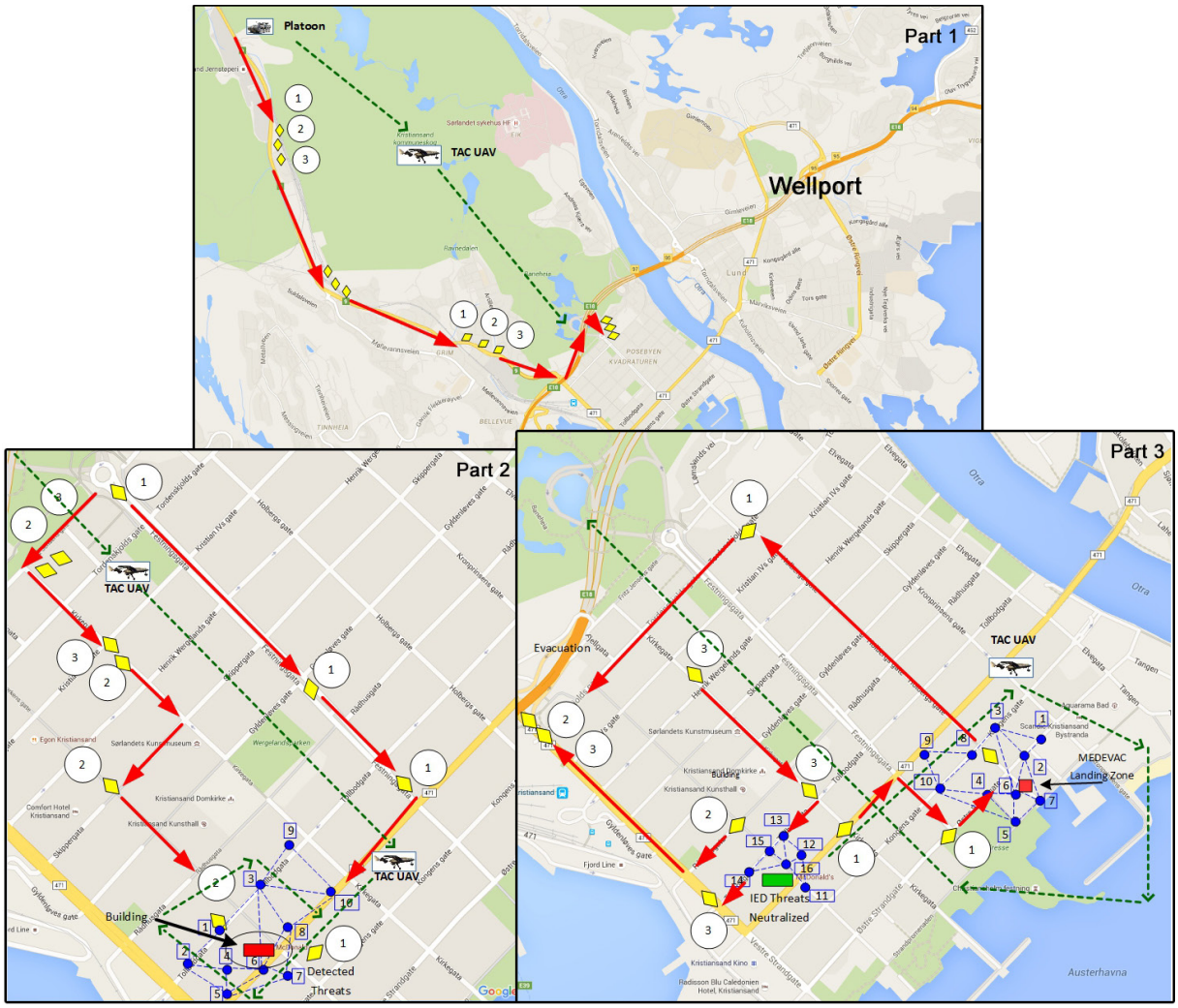

Figure B-3: Overview of Mobility Patterns in Vignette 3.

B.5 RADIO MODELS AND COMMUNICATIONS ARCHITECTURE

The emulation contains radio models for naval, ground vehicular, manpack, handheld, soldier, sensor network, and UAV radios. A Long Term Evolution (LTE) network was planned but not completed as of the writing of this report and will likely be included in the future. The models contain the typical characteristics of these types of radios such as transmit power, antenna type, and height.

The radios can run different waveforms (transmission technologies). As a typical representative for a Narrowband Waveform (NBWF), we have used NATO NBWF as the basis for our model. The original intent was to use publicly available information on the Soldier Radio Waveform (SRW) as typical representative for a Wideband Waveform (WBWF). However, due to time limitations, the currently distributed model for the WBWF was derived from the NBWF. The models contain the typical characteristics of the Physical (PHY) layer of these waveforms like data rate, transmission delay, and Signal-to-Noise Ratio (SNR). The Medium Access layer (MAC) on the other hand is (due to lack of time) currently based on either 802.11 MAC or no MAC.

Radio model configurations were generated for narrowband, medium band, and wideband radios. The actual EMANE files are available for download as part of the Anglova scenario. This section describes the characteristics of the radio models.

B.5.1 25 KHz Narrowband Radio Model

We have based the radio models on the following assumptions: Vehicle mounted narrowband tactical radios typically have an output power of 50 watts (i.e., 47 dBm) with a typical noise figure of 12 dB or better. Antenna gain, cable loss, and connector losses typically sum up to 0 dB. When two radios are on the same vehicle and operating in the same frequency band (i.e., co-site operation), they have a desensitization of 6 dB or better. However, this aspect is not currently included in the emulation models.

Fading has to be taken into account. Fading consists of two components, slow and fast fading. A typical fading margin is 8 dB. As parts of the emulation is based UTD propagation calculations with digitized terrain, the precomputed propagation model includes slow fading. Fast fading is not currently modeled and not taken into account in the emulation. The thermal noise figure is -144 dBm/KHz, which is included in EMANE.

To represent a typical narrowband radio, characteristics similar to the N2 mode of the physical layer of the NATO Narrowband Waveform (NATO NBWF [11]) was chosen as it provides a good compromise between data rate and range. This mode has a bandwidth of 25 KHz. Thus, the thermal noise power is -130 dBm (10 * log10 (25) = 14 dB). Adding the noise figure provides the receiver sensitivity, which is -118 dBm. As typical frequencies in the military VHF band (30 to 88 MHz) the frequencies 50 MHz, 51 MHz and 52 MHz were chosen.

Simulation results of an approximated model of the NATO NBWF mode N2 require the following signal to noise ratio (SNR) threshold values to get the given Block Error Rates (BER) (Table B-2; see Ref. [21] for more information):

Table B-2: SNR Threshold Values.

BER	100%	90%	60%	30%	10%	0%
SNR	< 8.7 dB	9.0 dB	9.3 dB	9.7 dB	10.1 dB	≥ 10.9 dB

The average block size was estimated as follows. An average transmission requires two slots. The NATO NBWF PHY for mode N1 uses the interleaver best suited to the packet size. For a large packet this is 284 user bits for the first slot and 432 user bits for the second slot. The NATO NBWF mode N1 has a PHY data rate of 20.0 kbps and mode N2 has a PHY data rate of 31.5 kbps. The number of user bits per mode scales linear to the NATO NBWF PHY data rate. For mode N2, the factor is 31.5 kbps / 20.0 kbps. The average block size thus is 564 bits = (284 bits + 432 bits) / 2 * (31.5 kbps / 20.0 kbps).

Mode N2 has a MAC data rate of 17.5 kbps and uses a dynamic MAC., which was emulated within EMANE using the TDMA MAC model, a generic TDMA scheme that supports schedule distribution and updates in real-time using events. However, as noted earlier, using the currently implemented TDMA model within EMANE is not dynamic and requires a shared clock (or clocks synchronized to a high degree of precision) and as a result was not usable by the IST-124 group.

B.5.2 250 KHz Medium Band Radio Model

The medium band radio model is deduced from the narrowband radio model by increasing the bandwidth and the data rate by a factor of 10 to 250 kHz and 175 kbps. Thus, the thermal noise power is -113 dBm (10 * log10 (1250) = 31 dB). Adding the noise figure provides the receiver sensitivity, which is -101 dBm. As typical frequencies in the military UHF band (225 to 400 MHz), the frequencies 300 MHz, 301 MHz, 302 MHz and 303 MHz were chosen for the different wideband networks within the scenario.

B.5.3 1.25 MHz Wideband Radio Model

As an alternative to the 250 KHz medium band radio model, a 1.25 MHz wideband radio model was also developed by increasing the bandwidth and the data rate by a factor of 50 to 1.25 MHz and 875 kbps. Thus, the thermal noise power is -120 dBm (10 * log10 (250) = 24 dB). Adding the noise figure provides the receiver sensitivity, which is -108 dBm. As typical frequencies in the military UHF band (225 to 400 MHz), the frequencies 300 MHz, 302 MHz, 304 MHz and 306 MHz were chosen for the different wideband networks within the scenario.

Figure B-4 shows a graphical comparison of the three radio models that have been implemented and distributed with the Anglova scenario. With the narrowband radio model, the coverage for a single radio is typically 20 km. To cover the same area with medium band, at least four radios would be required. Finally, when using the wideband radio model, many more radios would be needed (typically 24-32) to provide the same coverage. Of course, in the narrowband case, the bandwidth is limited and shared between all the nodes in that range. However, with the wideband radio model, radios in non-overlapping ranges can communicate in parallel with no interference.

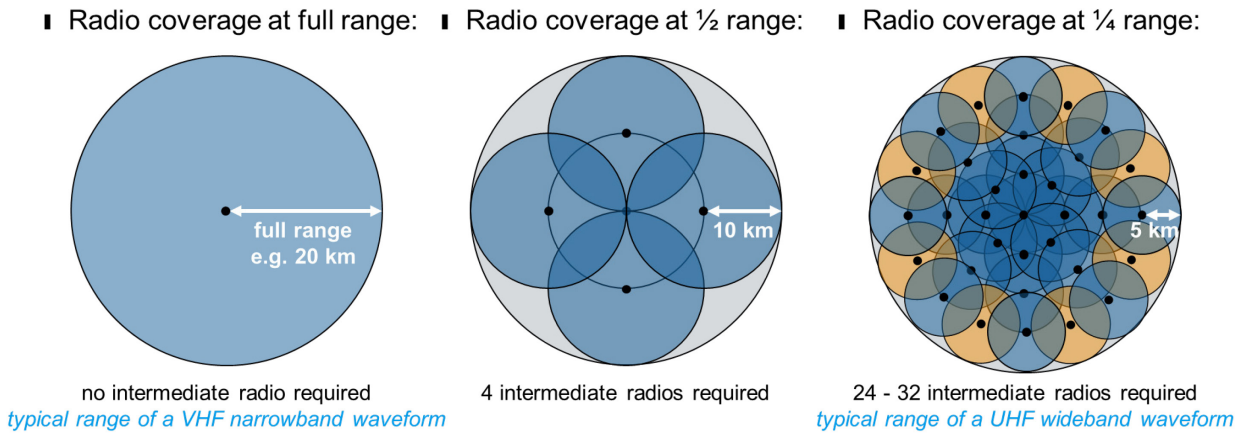

Figure B-4: Visualization of the Range and Density of Narrowband, Medium band, and Wideband Radios.

B.5.4 Other Radio Models

The Anglova scenario also incorporates a few other radio models – including an HF and VHF model for the naval contingent, which is described in Annex H. Other models include a communications link for SATCOM, the Aerostat sensor platform that is part of vignette 1, and an LTE model. The modeling of the last three were not yet completed at the time of this writing.

The EMANE configuration files for these radios are available as part of the overall Anglova scenario distribution. The distribution will be updated as the other radio models are further developed.

B.5.5 Node Architecture

As part of the scenario development, some initial development was also completed on the system architecture for each node in the emulated environment. These architectural models are not complete and hence have not been released as part of the Anglova distribution. As an example, the Coalition Tactical Operations Center (TOC) node is depicted in Figure B-5. Security aspects have been removed from the excerpt shown. In reality, the TOC will require access to information from different security domains (multiple levels of security) and be employing equipment that realizes COMSEC on different layers

(application layer, network layer, and/or link layer). A separate IST-124 Security Architecture report is being published with a discussion regarding possible security architectures for this environment. We note that the COMSEC security aspects are not included in the emulation developed so far, partly to simplify distribution.

On the left side of Figure B-5, the different information sources and sinks are depicted. These are connected to the outside world via one or more routers. Potential connections to the outside world are a gateway to FMN and a multitude of different radio types. On the right side of the diagram the nodes that are potentially reachable over these links are listed. Within the current emulation environment setup, each platform is modeled as one node with multiple emulated links, one for each type of radio.

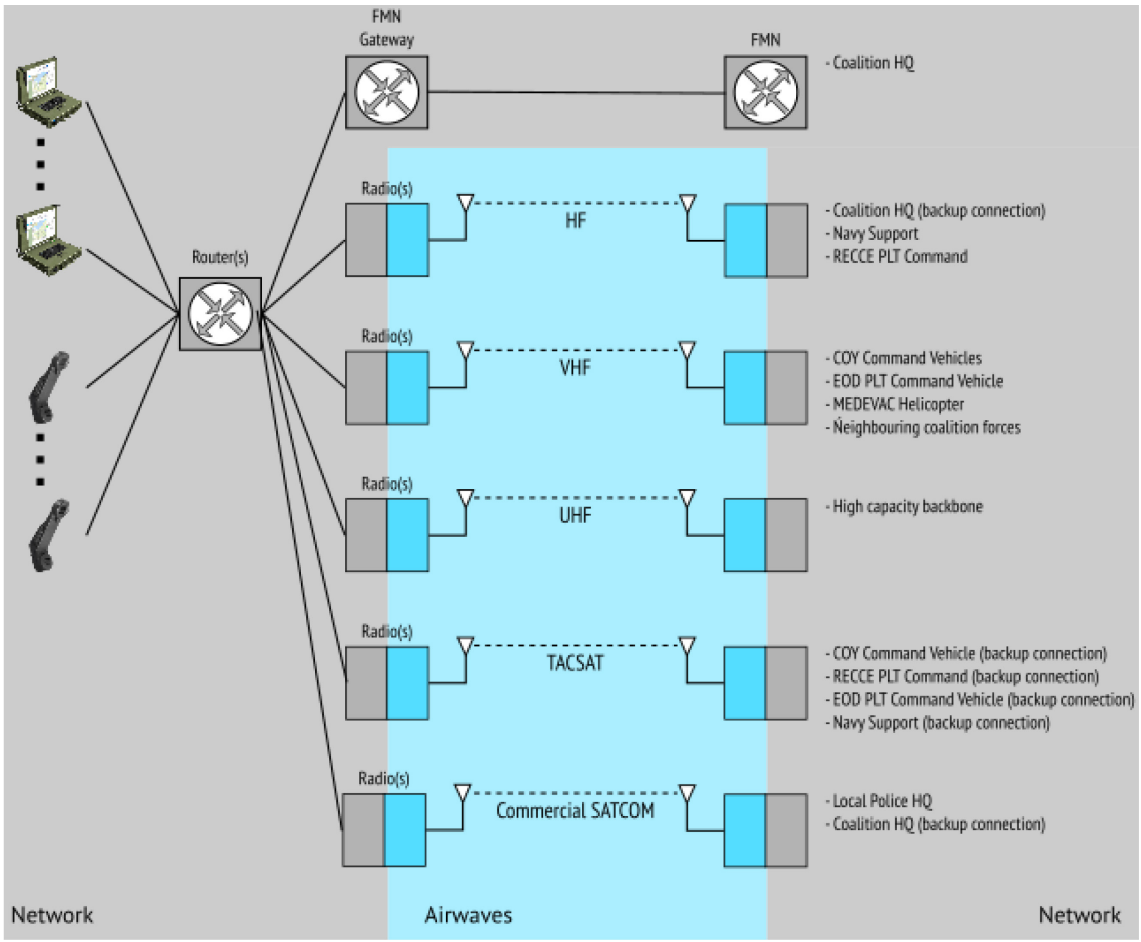

Figure B-5: System Architecture View of the Coalition Tactical Operations Center (TOC) Node.

Figure B-5 also shows a link between the Coalition TOC and the Coalition HQ via an FMN gateway. The original intent for the scenario was to include the Finnish TACOMS+ implementation of NIP (Network Interconnection Point) auto configuration node to represent an (early spiral version of) an FMN network connection. It includes features planned for FMN Spiral 3 and onwards towards full Protected Core Network (PCN) capabilities [22]. The node contains four auto configuration interfaces. Local client and server networks and connection towards tactical networks use static configurations. When two nodes are connected, they identify each other using specific RIPv2 messages and establish a Generic Routing Encapsulation (GRE) over IPSec connection to secure traffic. Nodes authenticate each other using certificates or pre-shared secrets. All traffic between nodes is protected and authenticated. After a connection is established, a BGP session shares routing information and allows interdomain routing

(Figure B-6). It is also likely that in an actual deployment, the headquarters of the different nations that are part of the coalition would also be connected to each other and to the Coalition HQ node using the FMN approach. At the time of writing this report, the FMN gateway has not yet been included and released as part of the Anglova scenario. This might happen as part of the IST-161 RTG's activities.

Figure B-6: TACOMS+ Auto Configuration Over IPSec.

B.6 SCENARIO CHARACTERIZATION

Characterizing the Anglova scenario is important in order for experimenters to understand and anticipate expected behavior at the RF level. As of the writing of this report, the focus has been on the second vignette, which has the most complicated dynamics due to the motion and terrain, and on the naval task group of the scenario.

B.6.1 Connectivity Internal to the Battalion in Vignette 2

As described earlier, the second vignette covers the deployment of the coalition forces, a battalion consisting of six companies, into the operational zone. The battalion starts out by moving in a single column on one of the main roads (see Figure B-7); the Coalition Head Quarters (CHQ) is indicated with a cyan-colored star. After about 10 km, the battalion splits up over two main roads and after about 25 km splits up further into many paths grouped in companies. Towards the end, the battalion finally splits up to the level of platoons. Altogether, the Vignette 2 mobility pattern is 7800 seconds (130 minutes) long.

The battalion consists of six companies. Altogether there are 157 vehicles, each of them being a network node. In addition, an Unmanned Aerial Vehicle (UAV) node was also added to this vignette (with a trajectory in the shape of two connected green circles in Figure B-7) – it can act as a communications relay and provide persistent surveillance capabilities.

To estimate the path loss between the nodes, a UTD propagation model by Holm is used [19]. In Figure B-8, Figure B-9, and Figure B-10, the path loss is used to calculate the connectivity in the 157-node network for the whole deployment phase. Note, the UAV and the CHQ were not included in this calculation, which was completed prior to the UAV and CHQ were introduced into the scenario. The calculations show the connectivity that is possible in the scenario and serves as a benchmark that the performance of the routing protocols can be compared with. Three different transmission technologies to connect the nodes are investigated. The connectivity is illustrated by showing how the fraction of nodes at h hops distance from each other varies over time. The average of h is taken over all nodes in the network. The hop distance is theoretically calculated, with the assumption that there is a communication link between two nodes if the path loss value is less than a system gain G_{sys} that varies for the transmission technologies. The three investigated transmission technologies are: 25 kHz, 17.5 kbit/s with G_{sys} =156 dB; 250 kHz, 175 kbit/s with G_{sys}=146 dB: and 1.25 MHz, 875 kbit/s with G_{sys}=139 dB.

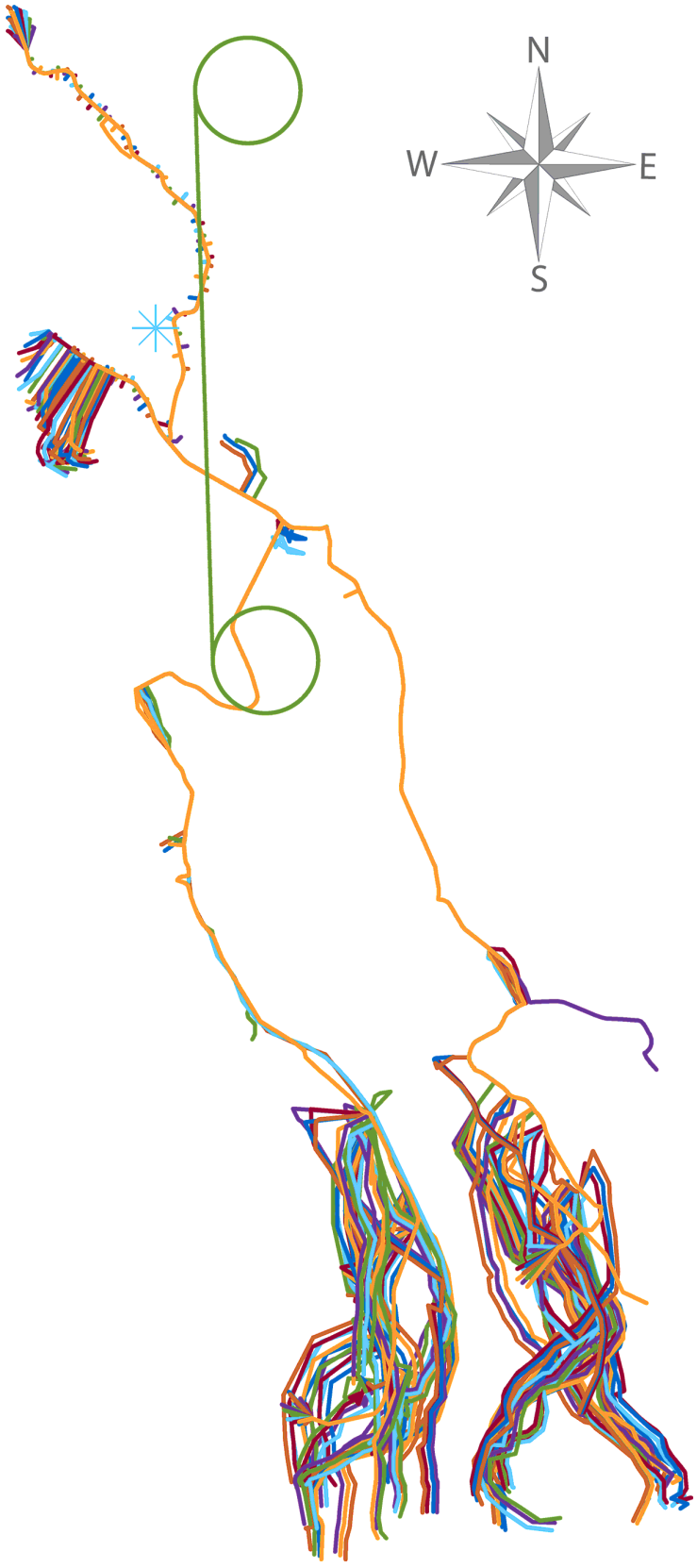

Figure B-7: Illustration of the Movements (Directed from the North to the South) of the Battalion.

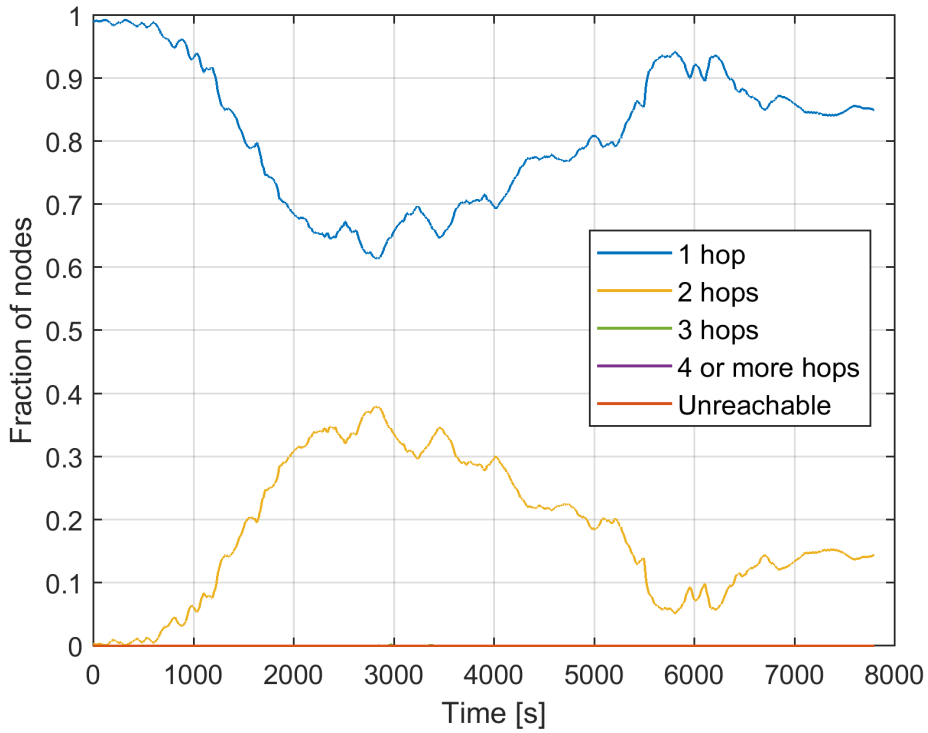

Figure B-8: The 25 KHz Transmission Technology at the 50 MHz Frequency Band.

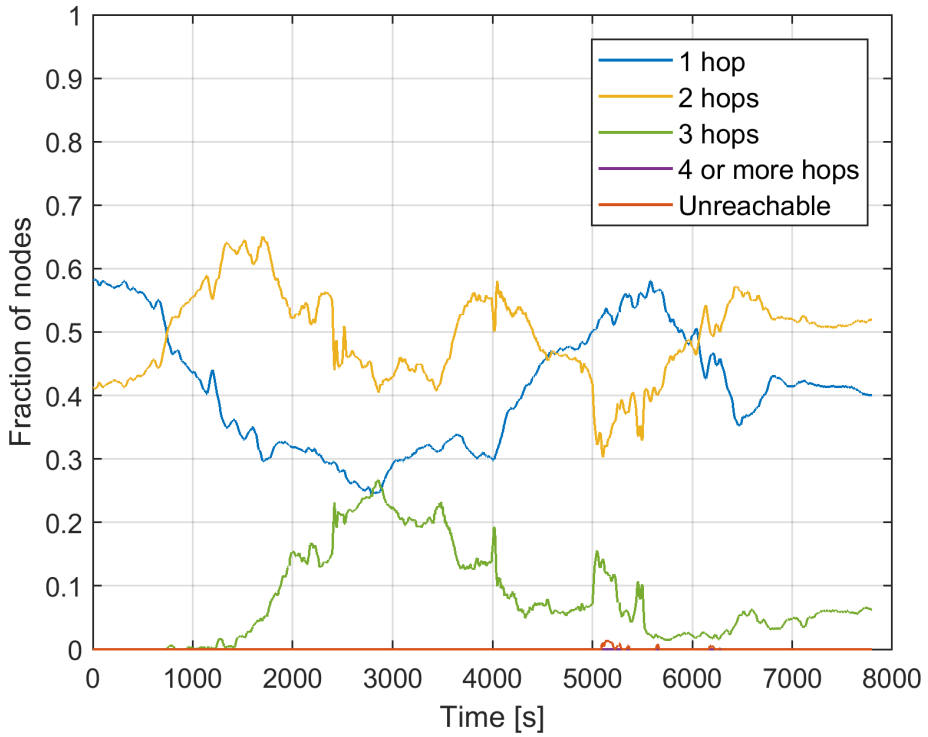

Figure B-9: The 250 KHz Transmission Technology at the 300 MHz Frequency Band.

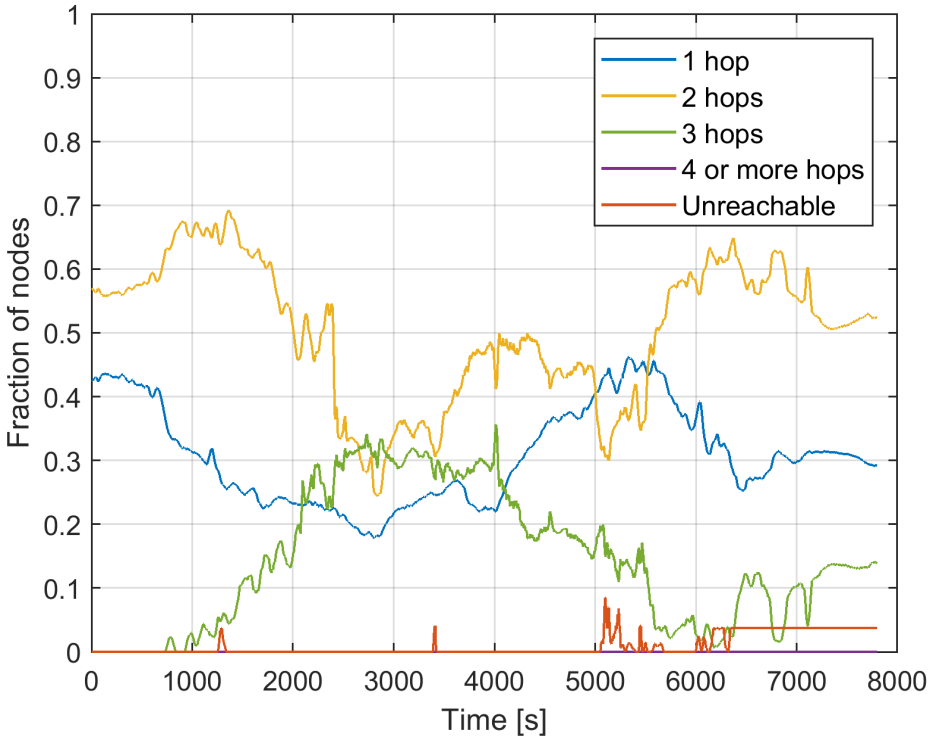

Figure B-10: The 1.25 MHz Transmission Technology at the 300 MHz Frequency Band.

As can be seen the 25 kHz transmission technology at 50 MHz keeps the network connected for the whole deployment phase and no more than two hops are required. For the other two transmission technologies, the network is not always fully connected as there are a number of unreachable nodes at various times. After about 2000 seconds into the scenario, the network start to be stretched out and the number of hops increases. Towards the end of the vignette, the network is fragmented with a few nodes behind the main part of the battalion that cannot be reached using the WB transmission technology. However, within the main part of the battalion, almost all nodes can be reached with a maximum of three hops. This is the reason why four or more hops seldom occurs. In Figure B-11 the bar graph shows the fraction of nodes at different hop distances averaged over the vignette. In the figure it is shown that at least a few paths need 4 or more hops. Furthermore, it can be seen that the number of hops is larger for the 1.25 MHz than for the 250 kHz transmission technology.

Vignette 2 and a 1000 second long segment in the latter phase of the vignette has been used to investigate the scalability and performance of the Optimized Link State Routing protocol (OLSR) in Ref. [23]. Also, by using this segment, the effects of small-scale fading on the stability of the links is analyzed in Ref. [24].

B.6.2 Link Dynamics in Vignette 2

One important configuration of proactive routing protocol relates to how fast, or cautious the protocol should be in including tentative links in its routing tables. Maintaining the routes in a dynamic mobile scenario can be more or less difficult dependent on how frequent the link changes, which in turn requires that the routes are updated. In particular, it is problematic if links are lost without the routing protocol being aware. To investigate this topic further, we consider Vignette 2 of the Anglova scenario, see Refs. [23] and [25]. A network based on the 157 vehicles, and over the whole around two hours, of Vignette 2 is researched. Note that the Coalition Headquarters, and the UAV nodes are excluded. The reason is that the links connecting these two nodes have different link characteristics and therefore need separate treatment. The CHQ is a static node having a high mast and the UAV an airborne node with a longer communication range.

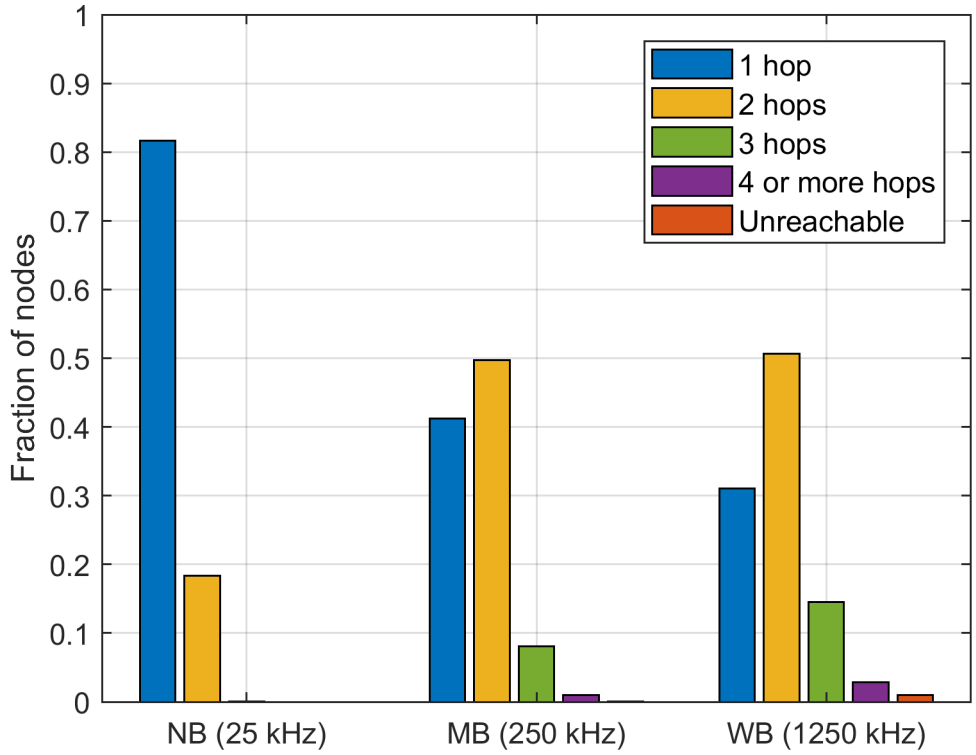

Figure B-11: The Fraction of Nodes at Different Hop Distances Averaged Over Vignette 2.

B.6.2.1 Preliminaries

Whether a link exists and can be lost is a rather diffuse concept. Several definitions can be used. In Ref. [26] a time hysteresis criterion is used to calculate how often a link changes. Another related option that we use here is the way OLSR establishes and remove links by utilizing HELLO messages. A HELLO message is transmitted from each node with a given retransmission interval, with the default value in OLSR being two seconds.

To decide whether a link exists, we use the basic link metric included in the OLSRv1 RFC [27]. This method estimates the reliability of a link based solely on OLSR HELLO packets. The method assigns weight 1 to all received hello packets and weight 0 to all lost hello packets over a link. To obtain a measure of the link quality, denoted Q, the weight sequence is exponentially filtered according to Ref. [27], resulting in values in the range between zero and one. With standard OLSR parameter settings, a link is classified as reliable if Q *is* larger than an upper threshold set to *0.8*. When a link is classified as reliable, it will remain reliable until Q becomes lower than a lower threshold set to 0.3.

We denote the minimum required number of consecutive correctly received HELLO packets to establish a link by P_{min}. For the OLSR standard setting, the algorithm will consider a new link reliable if three consecutive hello packets are received, i.e., P_{min} =*3*. If two consecutive packets are lost on a reliable link, the link will be considered unreliable. To obtain other values on P_{min} the upper threshold of Q is adjusted.

We define the radio system gain G to be equal to the maximum possible path loss from transmitter to receiver for connections that satisfy a given error requirement. That is, radio systems with good transceiver performance have a larger system gain than transceivers with low performance. We consider the three defined transmission technologies NB (Narrowband), MB (Mediumband) and WB (Wideband) with

different settings of bandwidth W, data rate R and radio system gain G_{sys}:

- Transmission technology NB: W = 25 kHz, R = 17.5 kbit/s, G_{sys} = 156 dB,
- Transmission technology MB: W = 250 kHz, R = 175 kbit/s, G_{sys}= 146 dB; and
- Transmission technology WB: W = 1.25 MHz, R = 875 kbit/s, G_{sys} = 139 db.

The transmission technology NB uses the 50 MHz band, and the other two the 300 MHz band. These choices correspond to the NB, MB, and WB radios that were modeled within EMANE for the emulation environment.

B.6.2.2 Results

The value on P_{min} determines how cautiously a link is established. With a large value for P_{min} it takes longer to establish a link, fewer links exist in the network and the connectivity is lower than with a small value for P_{min}. A lower degree of connectivity means that more nodes are missing. A node is missing when a given node cannot reach that node. Furthermore, the number of lost links per node and per second is lower with a large value than with a small value on P_{min} .

These effects are illustrated in Figure B-12, through Figure B-16. Using the NB transmission technology results in significantly better connectivity than with the other two transmission technologies. On average, about 120 – 130 of the possible 156 links from a node are available and about 1.2 hops are required to reach a given node. The network is almost connected, i.e., very few nodes are unreachable, as compared to when the wideband transmission technology WB is used, in which case between 2 to 6 nodes cannot be reached on average. The value used for P_{min} is important for the longevity and stability of a link exists as it determines how many consecutive HELLO messages need to be received correctly. When P_{min}=3, on average around 0.3 links per node is lost for all the transmission technologies. However, at certain times in Vignette 2, the difference between the NB and WB can be large. For example, around 6000 seconds into the vignette, only 0.15 links per node are lost with the NB transmission technology but as many as 0.6 links per node are lost with the WB transmission technology (see Figure B-16). The number of lost links per second decreases with a larger value for P_{min}. In a well-connected network with many links, many links can also be lost per second as compared to a sparser network with fewer links. The investigation shows this tradeoff in particular between prioritizing good connectivity or fewer lost links per second. Note, however, that to have a well-connected network and also fewer lost links per second requires using the narrowband transmission technology NB at the 50 MHz band and choosing a large value on P_{min} as this transmission technology has considerably better range than the other two transmission technologies. The drawback, however, is the low data rate of the NB transmission technology that limits what can be transmitted between the companies. Many lost links per second reduce the packet delivery ratio. As the HELLO retransmission is 2 seconds, it may take up to 4 seconds to detect that a link is lost. Therefore, even if a link in reality is lost during this time period a node may still try to use it to send a packet. We can conclude that the dynamics is rather high and varies depending on the transmission technology used and elapsed time of Vignette 2.

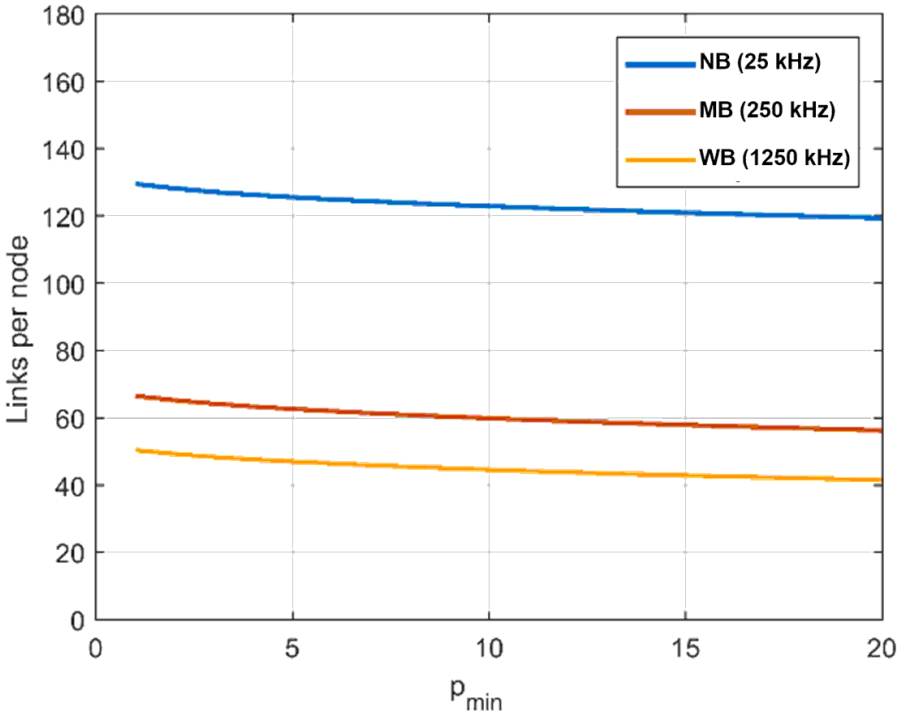

Figure B-12: Total Average Number of Links Per Node for Different Values on P_{min}.

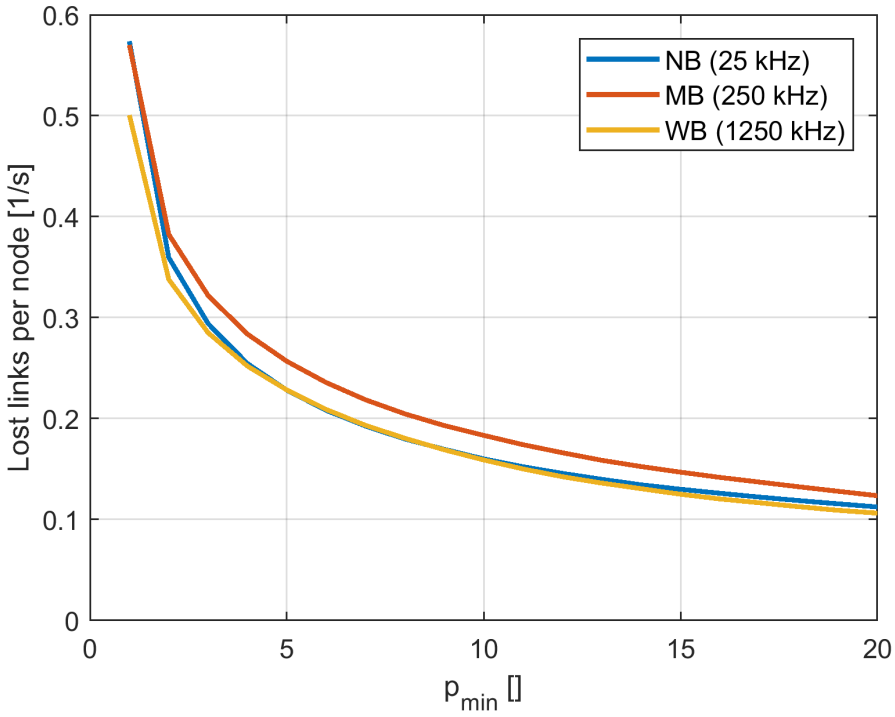

Figure B-13: Average Number of Lost Links Per Node and Second for Different Values on P_{min}.

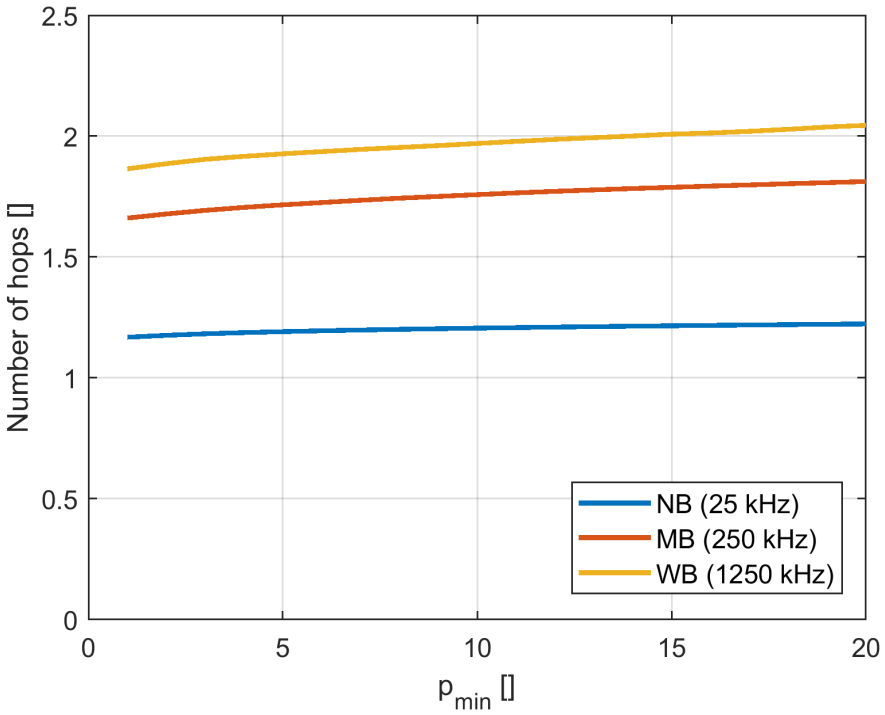

Figure B-14: Average Number of Hops Between all Node Pair in the Network for Different Values on P_{min}.

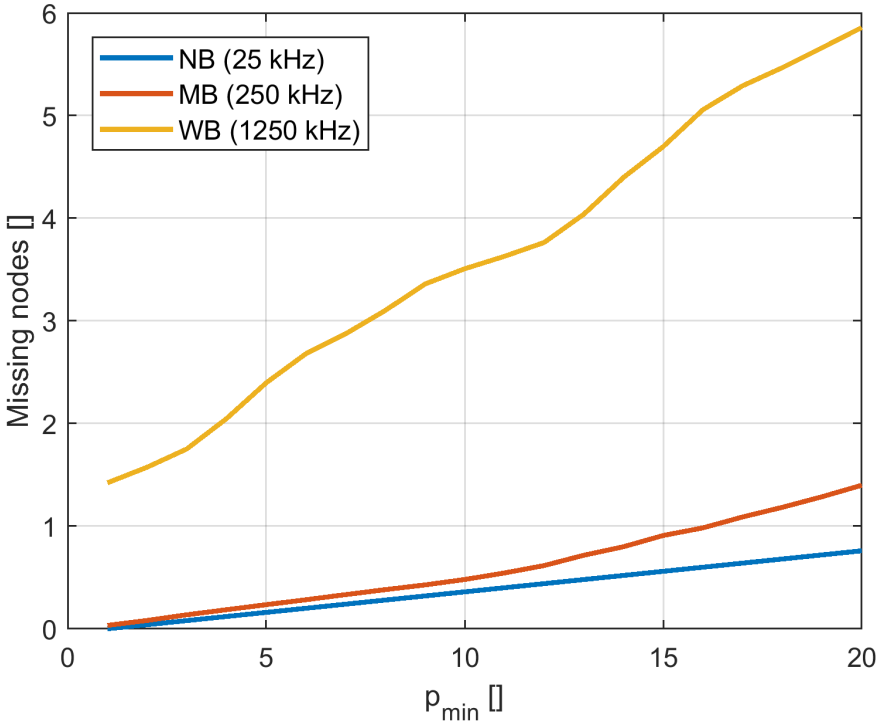

Figure B-15: Average Number of Not Reachable Nodes for Different Values on P_{min}.

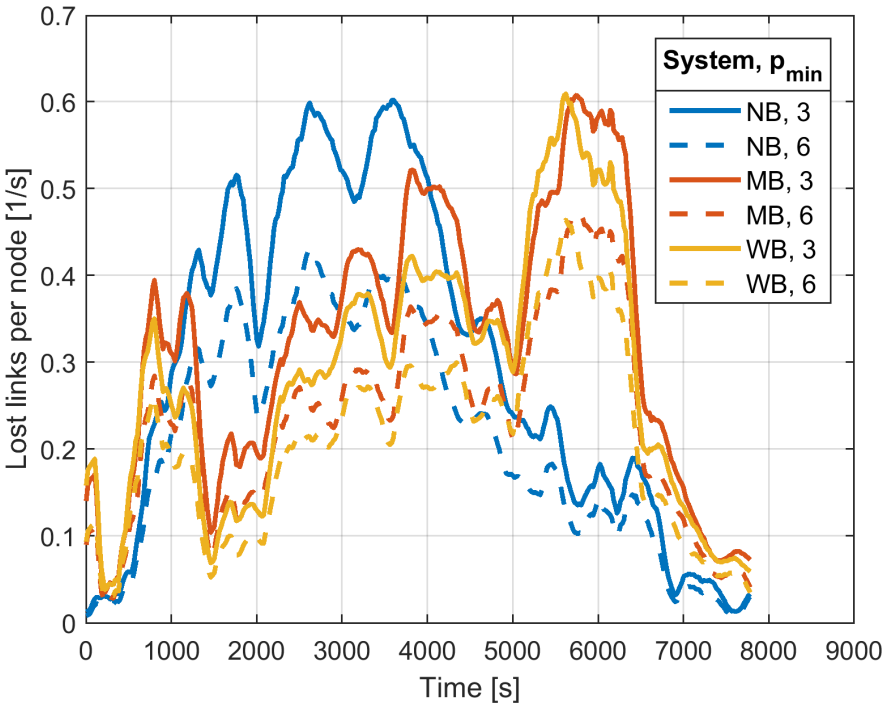

Figure B-16: Average Number of Lost Links Per Node Over the Two-Hour Long Vignette 2.

B.7 REFERENCES

[1] North Atlantic Treaty Organization (NATO), Federated Mission Networking (FMN). Internet: http://www.act.nato.int/fmn, January 2, 2016.

[2] AdjacentLink, LLC, Extendable Mobile Ad-hoc Network Emulator (EMANE) Wiki. Internet: https://github.com/adjacentlink/emane/wiki, January 2, 2016.

[3] AdjacentLink, LLC, Extendable Mobile Ad-hoc Network Emulator (EMANE). Internet: https://github.com/adjacentlink/emane, January 2, 2016.

[4] Ahrenholz, J., Comparison of CORE Network Emulation Platforms, in IEEE Military Communications Conference (MilCom 2010), pp. 166-171, October 31 – November 3, 2010.

[5] NS3 Consortium. NS3 Project Homepage. Internet: https://www.nsnam.org/, January 2, 2016.

[6] University of Southern California Information Sciences Institute, Network Emulation with the NS Simulator. Internet: http://www.isi.edu/nsnam/ns/ns-emulation.html, January 2, 2016.

[7] OMNeT++ Discrete Event Simulator. Internet: https://www.omnetpp.org/, April 6, 2018.

[8] Linux Foundation, Network Emulation (NETEM) Project Homepage. Internet: http://www.linuxfoundation.org/collaborate/workgroups/networking/netem, January 2, 2016.

[9] Carson, M., and Santay, D., NIST Net – A Linux-based Network Emulation Tool, on ACM SIGCOMM Computer Communications Review, vol. 33, no. 3, pp. 111-126, July, 2003.

[10] Emulab, Emulab Project Home Page. Internet: http://www.emulab.net/, January 2, 2016.

[11] North Atlantic Treaty Organization (NATO), STANAG 5630/AComP-5630: Narrowband Waveform for VHF/UHF Radios – Head STANAG, STANAG 5630/AComP-5630, Edition A, Version 1. To be published.

[12] Google, Inc., Protocol Buffers. Internet: https://developers.google.com/protocol-buffers/, January 2, 2016.

[13] US Army Research Laboratory. Traffic Generation Tool. Internet: http://www.arl.army.mil/www/default.cfm?page=2490, January 2, 2016.

[14] US Naval Research Laboratory. Multi-Generator (MGEN). Internet: http://www.nrl.navy.mil/itd/ncs/products/mgen, January 2, 2016.

[15] US Naval Research Laboratory. Scripted Display Tools (std/std3d). Internet: http://www.nrl.navy.mil/itd/ncs/products/sdt, January 2, 2016.

[16] National Aeronautics and Space Administration. NASA World Wind. Internet: http://worldwind.arc.nasa.gov/, January 2, 2016.

[17] Eklöf, F., and Johansson, B., On Situation Awareness for a Mechanized Battalion in Two Tactical Scenarios, in Swedish, Defence Research Est., Div. of Command and Control Warfare Tech., FOA-R-00-01734-504–SE, Linköping, Sweden, December 2000.

[18] Asp, B., Eriksson, G., and Holm, P., Detvag-90 – Final Report, Defence Research Est., Div. of Command and Control Warfare Tech., FOA-R–97-00566-504–SE, Linköping, Sweden, September 1997.

[19] Holm, P., UTD-Diffraction Coefficients for Higher Order Wedge Diffracted Fields. IEEE Trans. Antennas Propagat., vol. AP-44, pp. 879-888, June 1996.

[20] Magliacane, J., SPLAT! Internet: http://www.qsl.net/kd2bd/splat.html, May 8, 2017.

[21] Libæk B., and Solberg, B., A simulator model of the NATO Narrowband Waveform Physical Layer, FFI Notat 2011/00533, 2011.

[22] Hallingstad, G., and Oudkerk, S., Protected Core Networking: An Architectural Approach to Secure and Flexible Communications, in IEEE Communications Magazine, vol. 46, no. 11, pp. 35-41, November, 2008.

[23] Marcus, K., Barz, C., Kirchhoff, J., Roge, H., Nilsson, J., in't Velt, R., Suri, N., Hansson, A., Sterner, U., Hauge, M., Lee, K., Holtzer, A., Buchin, B., Peuhkuri, M., and Mīsīrlīoğlu, L., Evaluation of the Scalability of OLSRv2 in an Emulated Realistic Military Scenario, in Proceedings of the 2017 International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, 2017.

[24] Sterner, S., and Uppman, U., On the Robustness of OLSR in a Mobile Tactical Scenario in Rural Terrain, in Proceedings of the 2017 International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, 2017.

[25] Suri, N., Hansson, A., Nilsson, J., Lubkowski, P., Marcus, K., Hauge, M., Lee, K., Buchin, B., Mīsīrlīoğlu, L., and Peuhkuri, M., A Realistic Military Scenario and Emulation Environment for Experimenting with Tactical Communications and Heterogeneous Networks, in Proceedings of the 2016 International Conference on Military Communications and Information Systems (ICMCIS), Brussels, 2016, doi: 10.1109/ICMCIS. 2016.7496568.

[26] Örn Tengstrand, S., Hansson, A., and Grönkvist, J., Routing Architectures for Heterogeneous Networks, Swedish Defence Research Agency (FOI), FOI-R-4133—SE, Linköping, Sweden, September 2015.

[27] Clausen, T., and Jacquet, P., Optimized Link State Routing Protocol (OLSR), IETF Network Working Group, RFC 3626, October 2003.