Human-in-the-Loop Analysis of Future Operational Scenarios using Network Emulation

Matthew Britton
Centre for Defence Communications and Information Networking
The University of Adelaide, Adelaide
AUSTRALIA

matthew.britton@adelaide.edu.au

ABSTRACT

In this paper we describe how to apply network emulation to operational scenario analysis by incorporating models of physical terrain, link capacity, mobility and wireless systems, background traffic effects and experimentation involving Human-in-the-Loop (HITL) and System-in-the-Loop (SITL). In this way, we show how network emulation can offer a significant and cost-effective enabling capability when examining Future Mission Networks, as forces worldwide are adapting more rapidly to changing roles. It is potentially a disruptive technology, and may supplant or complement some programmes involving simulation or hardware deployments.

1.0 INTRODUCTION

The effectiveness of many defence systems is impacted by the performance of the underlying communications network. Information sent between two points may be carried over network bottlenecks and can be significantly delayed or even discarded. This information could comprise (i) voice or data being carried between people needing to communicate in real-time, (ii) messages between two systems that co-operate to generate a Common Operating Picture or (iii) interactions between an operator and a remote system. It is important to be able to understand such network effects so as to understand their impact on:

- the systems themselves, for example, to investigate their stability in unreliable environments,
- operations, for example, to help develop robust doctrine, and
- human operators, for example, on human perception and decision making.

Operators of defence future networks worldwide will need to augment current training and exercise needs with various technologies, in order to maximise lessons learned and reduce costs. Recently, an approach called **network emulation** has attracted attention in this area. Network emulation uses some element of the deployed hardware or software in a laboratory test-bed (or in the field), and can provide more realism than simulation with less cost than a real deployment. For example, the networking protocols used in defence hardware such as network routers may be extracted and "deployed" in a network of connected virtual routers in the laboratory. Real equipment can even be connected to the network emulation, allowing direct experimentation between existing systems and proposed systems for integration into service. It provides a more cost-effective, controllable and repeatable test environment in comparison to actual hardware tests, which are usually constrained to using high-speed and virtually error-free links to connect devices. In this way, a scalable and adaptable test-bed can be created in which scenarios can be rapidly evaluated; and where the networking functionality is not a model, but rather it is real and already verified through real-world deployments.

In this paper we describe how to apply network emulation to operational scenario analysis by incorporating models of physical terrain, link capacity, mobility and wireless systems, background traffic effects and experimentation involving Human-in-the-Loop (HITL) and System-in-the-Loop (SITL). We use two examples: firstly, where a user interacts with a remote database application via an emulated satellite network; followed by an example whereby a user conducts operational planning by examining the effect of mobility on a real-time video stream. In this way, we show how network emulation can offer a significant and cost-effective enabling capability when examining future networks, as forces worldwide are adapting more rapidly to changing roles.

2.0 NETWORK EMULATION

Modelling and simulation rely on models rather than the systems themselves, and full scale network construction is expensive and complex. Network emulation, however, allows direct experimentation between existing systems and proposed systems for integration into service. It provides a more cost-effective, controllable and repeatable test-environment in comparison to actual hardware tests, which are usually constrained to using high-speed and virtually error-free links to connect devices. A comparison of these complementary techniques is shown in Figure 1, with development times ranging from days and weeks for real hardware to months and years for simulations and theoretical-analytic models.

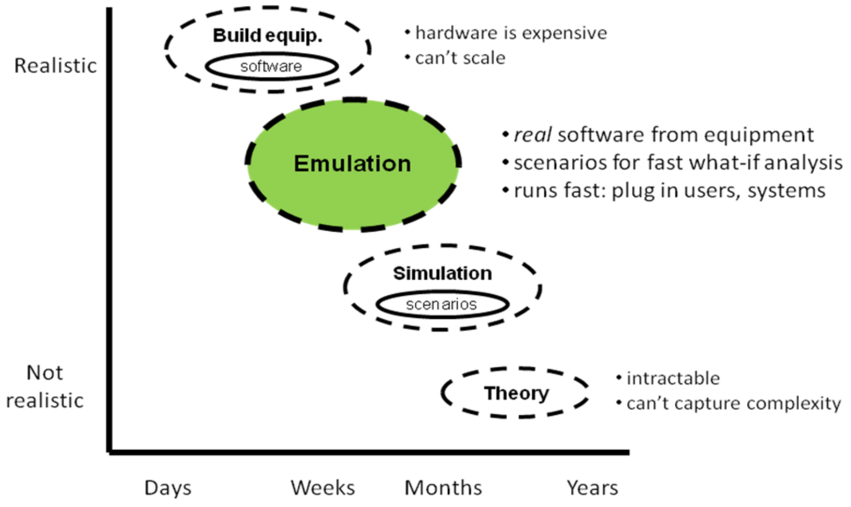

Figure 1: Comparison of hardware experimentation, emulation, simulation and theoretical techniques.

Network emulation enables systems, systems of systems, and human users to be interconnected in order to experience realistic network effects according to externally defined scenarios. For example, information passing between the systems and users could be disrupted through the delaying or dropping of messages, consistent with the network topology and traffic being emulated. Emulation provides for:

- the description and modelling of complex communication and information networks,
- the incorporation of physical (terrain) and network topology, traffic routing, link bandwidths, traffic scheduling based on priority classes, and development of different traffic profiles,
- the support of defence experimentation involving Human-in-the-Loop (HITL) and System-in-the-Loop (SITL), and
- a realistic user experience of the network's performance without having to build the whole network.

An emulated network comprises at its core a collection of **virtual machines**, which are virtual representations of a real computer contained in a real device such as a standard PC. The virtual machines are connected together to represent a real network design, with all traffic flowing through the network of virtual machines constrained to flow through these particular virtual links. This is shown in Figure 2.

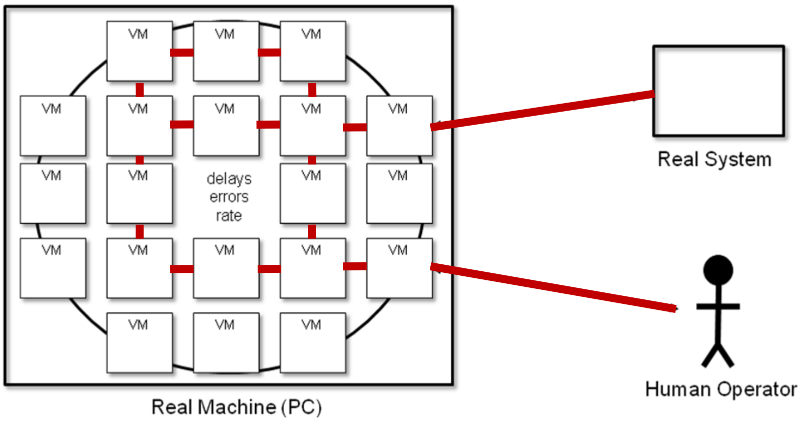

Figure 2: Conceptual design of a network emulation, where a Human Operator interacts with a remote Real System through a set of virtual machines (VM).

3.0 NETWORK EMULATION TOOLS

In order to explore the possibilities of network, we have created a custom emulation tool called *FogNet*, comprising three functional layers as shown in Figure 3. These are:

- the Scenario Manager Layer; a Graphical User Interface (GUI) that enables the real-time reconfiguration of network connectivity and traffic conditions,
- the Network Analysis Layer; the real-time computation of network performance measures such as communication delays and traffic losses and
- the Network Emulation Layer which inserts computed network delays and losses for traffic between users, the routing of datagrams according to specified routing algorithms, and re-calculation of routing when network state changes occur.

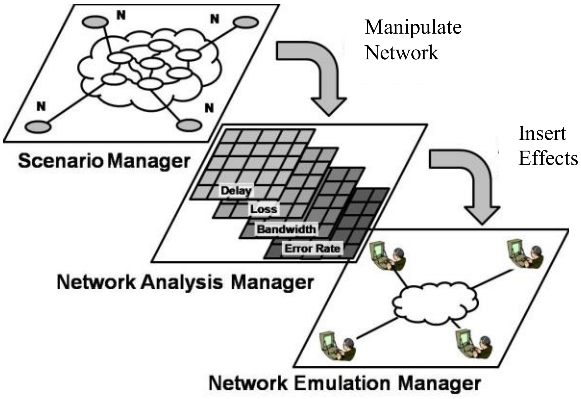

Figure 3: Layers in the network emulation design.

FogNet's structure can be broken down further into the virtual machine network (part of the Network Emulation Layer and including special "user" virtual machines that provide interactions to the system for end-users—that is, real equipment) and (ii) the performance emulation module (part of the Network Emulation Layer).

4.0 CAPABILITIES OF NETWORK EMULATION

4.1 Network Configuration

Configuring large-scale networks is a current research problem, and presents significant complexity when configuring deployed networks. An emulation test-bed allows experimentation on the configuration of large-scale networks before deployment. In a real network deployment, a range of Internet Protocol (IP) addresses may be manually allocated to the devices in the network. Other parameters such as the rate of routing protocol "hello" messages may also need to be manually configured. With emulation, automated techniques may be explored in a large-scale environment in a safe and isolated environment prior to deployment. Tools such as AutoNetKit can be integrated with the emulation environment to provide this capability.

4.2 Performance of Network Protocols and Services

The virtual machine (VM) approach of the emulation allows us to easily compare the performance and functionality of communication protocols in a realistic environment. For example, MANET routing protocols such as BATMAN [4][7] and OLSR [6] can be separately loaded into the VMs, and these VMs then interact with one another imitating the real wireless platforms in a MANET. Experiments can be built to determine the best implementation of these routing protocols, and the routing protocols changed to optimise their performance.

Inter-domain networking protocols can be explored using protocols such as BGP. For example, we have implemented BGP at the boundary between a tactical and strategic network; the boundary device being a WGS satellite. This example is described later in Section 6.1.

Quality-of-Service issues may be explored using protocols such as MPLS, whereby a flow of high-priority information may be prioritised over other traffic. We have implemented and tested MPLS in a network emulation with radio links and mobility of nodes.

4.3 Effects of Network Congestion

Because the network is emulated and we have complete control over the links between the emulated nodes, we can manage these links according to whatever effects are of interest. For example, if the link represents a terrestrial wired link we can inject models of background traffic. The use of a background traffic model that is scalable is important: we may want to model a large network with only a single real traffic flow from a system-in-the-loop, but we may have hundreds of virtual machines in the network. We have developed scalable methods to force real traffic flowing through the virtual machine network to compete realistically with this background traffic.

4.4 Effects of Radio Communications

4.4.1 Attenuation

The intended use of our emulation tool covers both wired and wireless network scenarios. As with our network congestion modelling, because the network is emulated and we have complete control over the links between the emulated nodes, we can represent a radio link by selectively corrupting or dropping packets according to the radio communication channel's characteristics. A realistic model of radio propagation is required in order to add effects to the Network Emulation Manager shown in Figure 3.

We are interested in a number of classes of wireless networks, including:

- Satellite systems,
- Mobile Ad-Hoc Networks (MANETs),
- Trunk networks with wireless components,
- Combat Net Radio (CNR),
- Tactical Data Links (TADLs) and
- directional-antenna networks.

We are able to model particular equipment that is either in use by defence forces or is planned for use. This includes equipment such as Harris radios and modes of operation such as EPLRS, SINCGARS and HAVEQUICK. At present this capability covers (i) HF line of sight, (ii) HF beyond line-of-sight and (iii) UHF/VHF line of sight radio propagation.

Radio signals between any two points are affected by many factors. In our model we include the effects of (i) frequency, (ii) distance between transmitter and receiver, (iii) the transmitter and receiver's antenna radiation pattern, (iv) obstacles between and in the vicinity of the transmitter and receiver and (v) land use. We determine a realistic bit-error rate (BER) for a given radio link using the following input parameters: (i) bit rate, (ii) radio frequency, (iii) received signal power and (iv) modulation/coding type and bandwidth. The receiver noise is comprised of the additive components (i) antenna received noise (sky noise), (ii) equivalent receiver noise (thermal noise) and (iii) receiver (hardware) noise (the noise figure NF). The following types of antenna noise are calculated and included (using results from [1]): (i) atmospheric noise, (ii) galactic noise, (iii) man-made noise (quiet environment) and (iv) oxygen and water vapour noise.

To enable the modelling of a wide range of communications equipment, we need to support a wide range of modulation and coding schemes. Examples of supported modulation types are (i) Pulse Amplitude Modulation (PAM), Binary Phase Shift Keying (BFSK), Differential Quadrature Phase Shift Keying (DQPSK), including Link 11, Frequency Shift Keying (FSK), Minimum Shift Keying (MSK), Link 16 - Joint Tactical Information Distribution System radio (JTIDS radio) and Gaussian Minimum Shift Keying (GMSK). A related property of the link is the error-correction coding. We have included models of a range of combined modulation and coding schemes, that is, particular modulation schemes with particular coding schemes (such as Reed-Solomon coding).

Purely for comparison purposes, we have also implemented an *ideal system*: this can be used to demonstrate how close in performance a fielded system is to the theoretical limit. Some modern coding techniques such as turbo codes are now extremely close to this limit.

4.4.2 Resource Contention

Whilst wired links are often isolated point to point links and hence do not interfere with other links, wireless transmissions can both interfere with and be interfered by other wireless transmissions. Under a frequency reservation scheme such as Frequency-Division Multiple Access (FDMA) the behaviour of the network is reasonably simple to model, as the transmissions do not interfere with each other. When a simple time reservation scheme is used, such as Time Division Multiple Access (TDMA) the behaviour is still reasonably simple, as each transmission has a predictable amount of radio resource. However, when more complex time reservation schemes are used such as Dynamic TDMA or Carrier-Sense Multiple Access/Collision Avoidance (CSMA/CA) the analysis is much more complex. For example, with CSMA/CA, random resource access is built into the system by design.

There are many research papers on the topic of throughput analysis for the CSMA/CA MAC protocol, which underlies the 802.11 suite of MAC protocols for example. Many of these papers have assumptions that prevent the techniques described to be used in network emulation. For example, some are valid only for:

- saturated conditions (there is a packet always waiting for delivery after a transmission), for example in [2],
- specific and simple topologies, usually to illustrate specific CSMA/CA problems such as Flow-in-the-Middle (FIM) or Information Asymmetry (IA) or
- the Basic Access Method (BAM) rather than the four-way handshaking (RTS/CTS) method used more commonly.

We have captured the above conditions in order to realistically model CSMA/CA behaviour. We also model network pathologies such as the hidden terminal effect [17].

5.0 AUGMENTING FIELD EXERCISES WITH NETWORK EMULATION

Operators of future defence networks worldwide are currently looking for ways to augment current exercises with various technologies, in order to maximise lessons learned and lower costs. A powerful way to augment a field exercise is to connect an emulated network channel between two real devices, with the option of users interacting with these devices.

In a hypothetical field exercise a database may be co-located in the same building as an operator, introducing no significant networking issues. If the database is distributed when fully deployed and operational, however, the user and database may be geographically separated, with access provided for example by a strategic or tactical network. This is likely to introduce latency issues, especially if satellites are used, and may possibly introduce network reliability and throughput issues.

We can emulate a satellite communications channel by creating a small network emulation, as shown in Figure 4. All interactions between the user and database are now subjected to satellite conditions, including latency and retransmissions due to the effects of weather, for example. Depending on the effects this has on performance (such as excessively long response times to user requests) the user might adapt the way they interact with the remote system, using it in ways that have not been foreseen when designed. If this feedback is given during the exercise, emulation helps to greatly increase the utility of the exercise, in that the feedback helps to explore multiple modes of operation of systems and capture the reaction of operators to the changing of performance of these systems—all in a compressed time period.

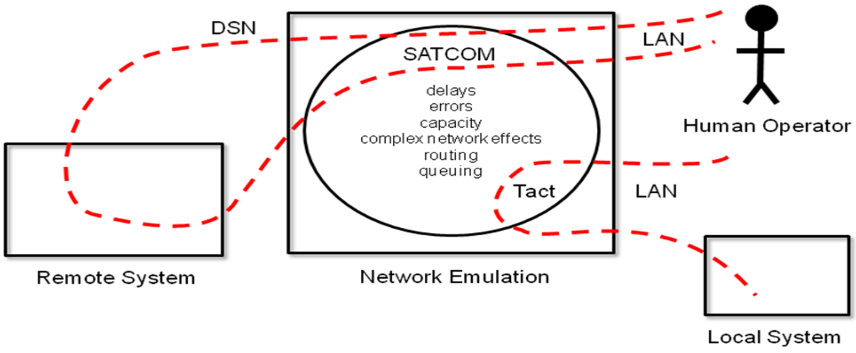

Figure 4: Augmentation of a field exercise, where a system local to an operator is redirected through an emulated network (Tact) to explore its performance over a tactical network.

5.1 Example: Interacting with Distributed ISR Databases

We have performed experiments [9] where a user interacts with a database using a web browser via a network of virtual machines. The motivation of this work is the Australian Defence Organisation's (ADO) plan to move to a Service Oriented Architecture (SOA) to connect and federate its Intelligence, Surveillance and Reconnaissance (ISR) resources. This future SOA environment is known as the Australian Defence ISR Integration Backbone (ADIIB). As no new communications infrastructure is being procured for these services, the ADIIB will operate within the existing Defence Information Environment (DIE). The ADIIB will enable authorised users in any location to search the entire ISR enterprise for relevant data with a single query. In addition to sharing ISR data, the ADIIB architecture will enable Defence, allied and coalition users to share services – such as ISR analysis tools.

By varying the network models from satellite to terrestrial, and introducing competing traffic and delays, we examined the performance of the ADIIB in a number of realistic scenarios. We installed a network emulation on a stand-alone PC, which communicated with an implementation of the ADIIB.

We defined a number of scenarios representing various types of deployed networks and topologies that were expected in the DIE. The different architectures BA, RA1, RA2 and RA3 are described below. In each case we looked at the response times (delay) from the ADIIB in response to a standard user query.

The **Baseline Architecture (BA)** represented the simplest possible deployed system: a user in a domestic headquarters that has access to a local meta-data store over a LAN. In this case the data store is co-located with the meta-data store. The BA was constructed to observe the ADIIB's performance in an idealised case for later comparison. The channel capacity in this case is high: in the order of 10Mbit/s and higher, whilst the latency is very low: typically below 1ms. FogNet was used to vary the channel capacity between 10 Mbit/s and 1,000 Mbit/s.

In this simple example we found minimal interference from the network emulation within the ADIIB implementation, providing a control point for further tests.

Reference Architecture 1 (RA1) represents a user in a domestic headquarters, with a data store and meta-data store located in a remote field of conflict in a deployed headquarters. RA1 has been constructed to observe ADIIB performance in the presence of reduced communications channel *capacity* and increased traffic *latency* for a simple trial scenario. For RA1 we consider channel latency due to the long transmission paths to be in a range from 240 ms (the minimum round-trip time) and above to include possible system delays such as processing time and packet queuing.

Reference Architecture 2 (RA2) is similar to RA1 in that it represents a user in a domestic headquarters, with a data store and meta-data store located in a remote area of conflict in a deployed headquarters. In RA2 we further constrain the channel capacity to represent a backup channel that might be used if a satellite channel is not available, for example due to weather conditions.

Using **Reference Architecture 3 (RA3)** we looked at the performance of the ADIIB with competing background traffic, which results in packet loss. In a deployed system such as on the DIE there will always be a level of background traffic that may induce network losses due to congestion. A network emulator can be used with for example DIE traffic statistics prior to any deployment in order to gauge expected levels of performance as a benchmark against a deployed system.

This reflects realistic conditions likely to be faced by a deployed system where loss due to network congestion is more common than loss due to errors introduced at the physical or link layer on established channels (for example, due to radio interference).

5.1.1 5.1.1 Lessons Learnt

By adding extra routing links in the Client-Server chain the underlying protocols can be tested for their tolerant of packet routing through a network. By introducing delays or data traffic, the system can be assessed for suitability for various realistic deployment scenarios.

6.0 AUGMENTING TRAINING WITH NETWORK EMULATION

During training, any system which can provide a realistic environment to interact with can be valuable, ranging from flight simulators to models and mock-ups of equipment. Currently, training for communications operational *planning* is largely paper-based, where communications systems are designed and configured based on hand-calculations such as link budgets. Network emulation helps to complement this approach by combining the student's design with a network emulation in a variety of scenarios and allowing rapid testing of designs and scenarios under realistic conditions. This provides immediate feedback on the viability of a design for the intended operational use. For example, a design incorporating a satellite communications channel can be tested with various weather patterns which may introduce significant errors and loss of signal.

There still remains a gap between this design process and operating with real equipment in a real scenario. With an emulated network, real equipment can be incorporated with the emulated network: the user can observe how the real equipment performs with the type of delays and congestion that they may encounter in either a trial or an active deployment. This type of emulation holds great potential for Defence, and other organisations, in allowing an already stretched budget to be extended with little extra capital cost, and without compromising personnel in the field.

An example hardware configuration for a system-in-the-loop test is shown in Figure 5. A user would interact with a remote system using the same configuration.

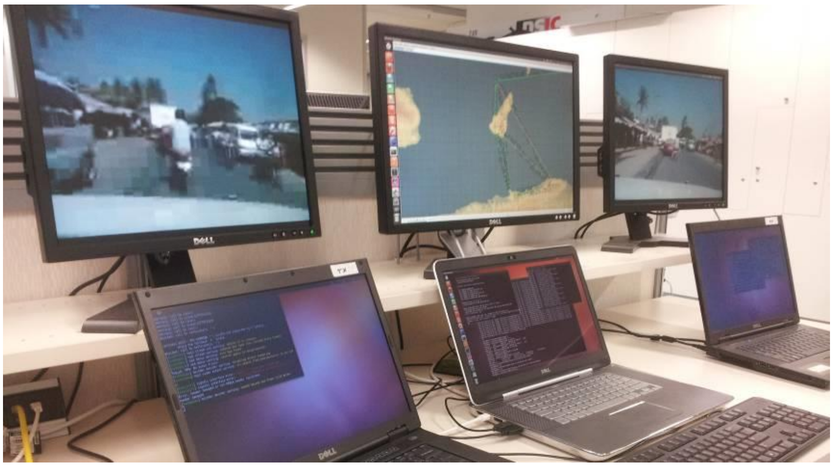

Figure 5: Experimental configuration, showing from left the transmitting PC (amphibious landing force), network emulation PC and receiving PC (remote base).

6.1 Example: Testing Real-Time Communications during an Amphibious Landing

The scenario shown in Figure 6 (network design interface) and Figure 7 (map design screen) involves an amphibious landing of a force which feeds video to a maritime unit, which then relays the data over satellite and through a strategic network to a remote defence base. The transmission range from the landing force (shown in Figure 8) precludes a direct link to the maritime unit, so the transmission is routed through one of two relays: both relays are mobile (for example, UAVs) and depending on their position the data are routed through one or the other, which in turn depends on calculations within the various virtual machines' routing protocol daemons. For simplicity all four nodes use the WNW waveform, which in this case are all configured to use (i) 225.0 MHz to receive and transmit, with (ii) an un-coded Quadrature Phase Shift Keying (QPSK) modulation and (iii) 1.0 Mbit/s channels. We assume there is a simple frequency reservation scheme (FDMA) and that packets are dropped randomly according to the bit-error rate.

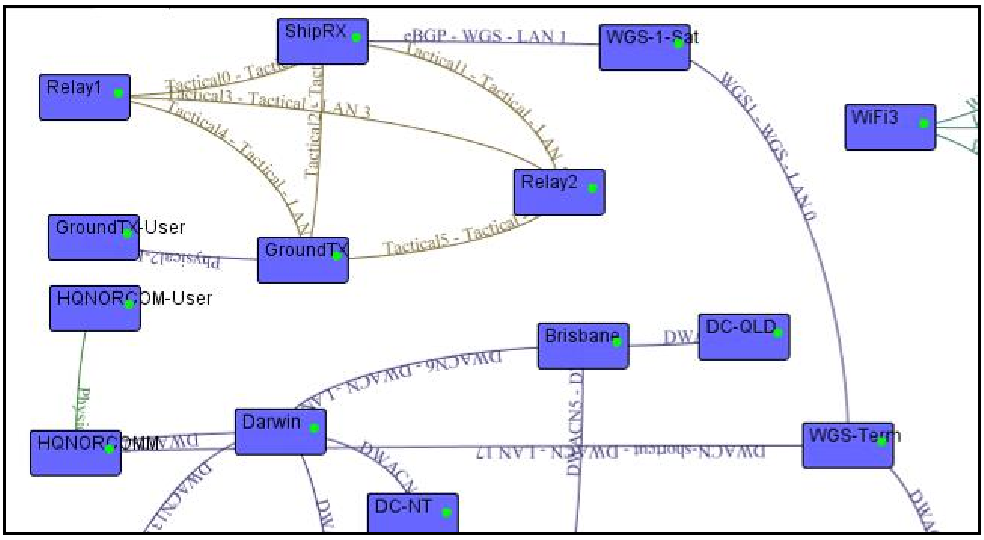

Figure 6: Portion of the network design screen, showing different sub-networks by colour such as tactical (dark green) and strategic (dark blue).

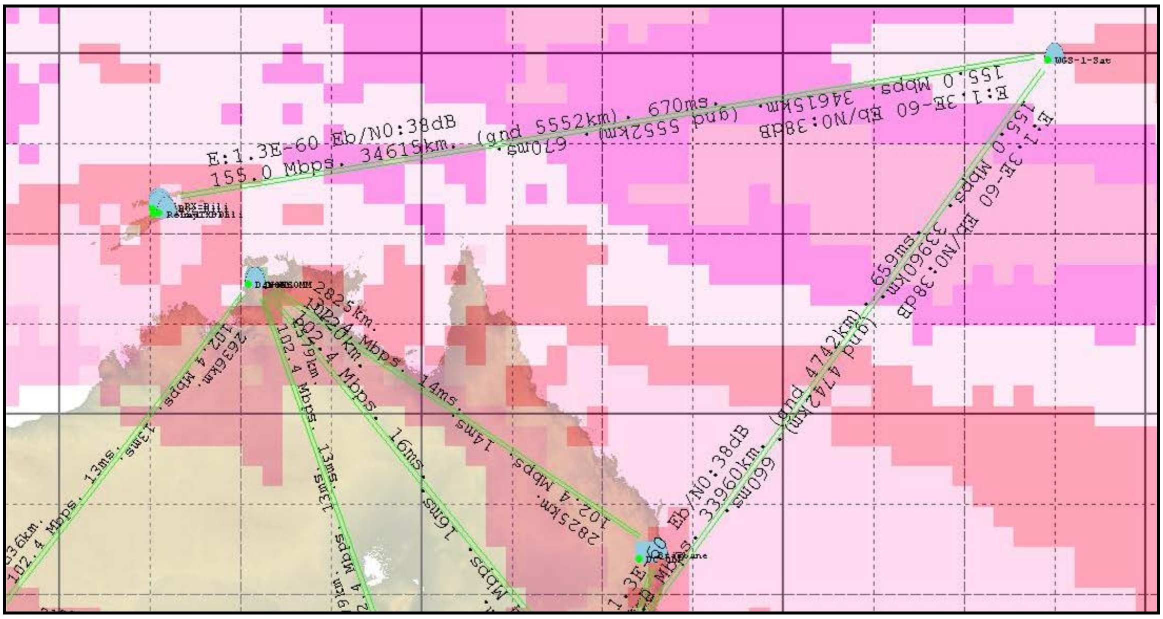
WGS-1-Sat
E:1.3E-60 Eb/N0:38dB
155.0 Mbps. 34615km. (gnd 5552km). 670ms.
E:1.3E-60 Eb/N0:38dB
155.0 Mbps. 33960km. (gnd 4742km). 659ms.
2825km. 102.4 Mbps. 14ms.
102.4 Mbps. 16ms.
102.4 Mbps. 13ms.
2636km. 102.4 Mbps. 13ms.
Brisbane

Figure 7: Map design screen, showing tactical area of operations (top left), satellite (top right), strategic network (bottom links) and rainfall intensity (white, orange and purple squares).

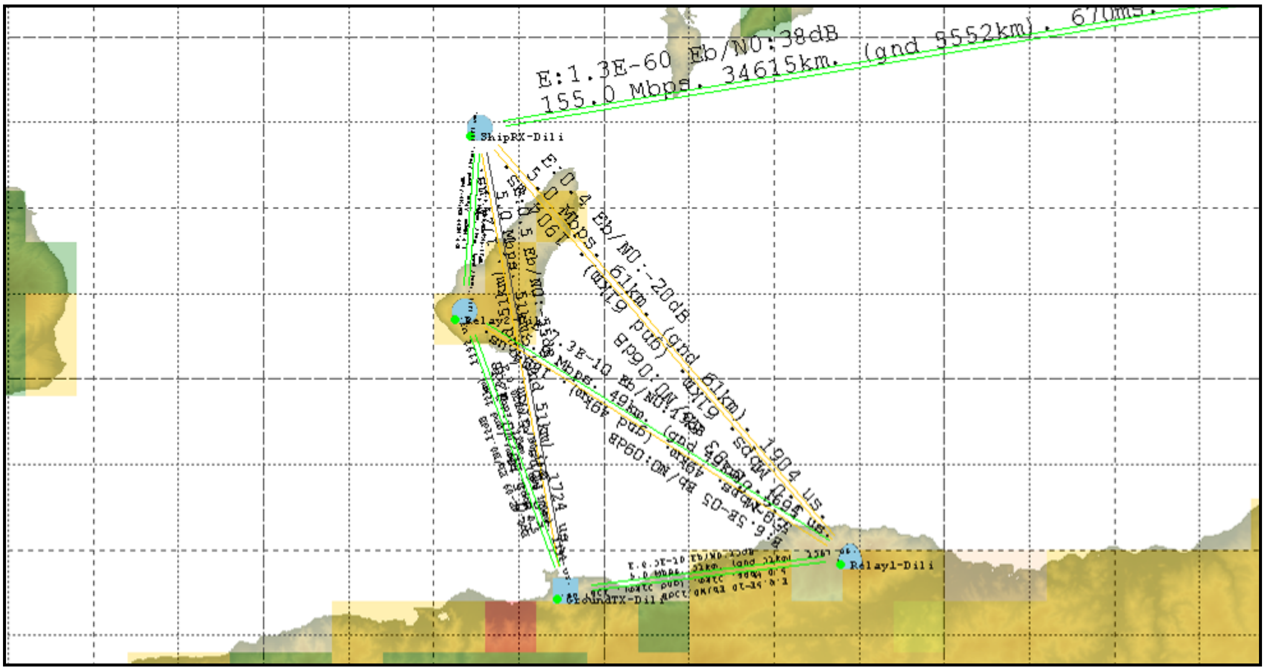

Figure 8: Close-up of the tactical area of operation, showing network link health by colour plus GIS data such as elevation (fine colour detail) and land use (large red, green and yellow squares).

In this demonstration we use a system-in-the-loop configuration whereby the ground unit is a laptop transmitting the video and the maritime unit is a laptop receiving the video. The demonstration setup is shown in Figure 8.

The ground unit suffers from radio propagation effects as it is located close to the ground and is located in hilly terrain. In particular it suffers from a lack of a line of sight path to the maritime unit. As it traverses the urban area its radio signal is degraded further.

The IP network in the scenario uses the routing protocol OSPF [18], intended for wired rather than wireless networks. During the scenario the problems with using OSPF for wireless networks becomes apparent: when either of UAVs moves into an ideal position to become a relay OSPF does not modify its routing table appropriately, resulting in significant loss of data.

6.1.1 Lessons Learnt

Clearly in the scenario a number of improvements to system design can be made, including the incorporation of:

- error-correction coding,
- more sophisticated modulation schemes,
- higher transmit power and gain and,
- more adaptable wireless-specific network routing protocols such as BATMAN [4][7] and OLSR [6].

In a network emulation environment, the settings above can be adjusted and a new scenario can be examined on the order of minutes or hours. To enable analysis of causes of radio communications or network problems, various statistics are collected, such as latency and signal to noise ratio, as shown in Figure 9.

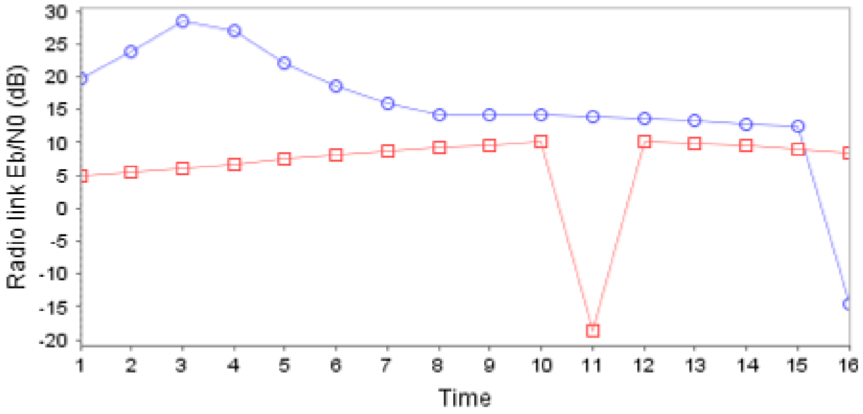

Figure 9: Statistics screen, showing the signal-to-noise ratio between the maritime unit and the two UAVs varying due to mobility.

Based on this, an operator may decide to increase the transmit power or adjust the trajectories of the UAVs to maintain effective communication.

7.0 DISCUSSION

The techniques and examples shown in this paper suggest that network emulation has matured to the point where it could have a role in enriching training and field exercises. This will be especially attractive as military operations become more networked, complex and expensive: any techniques that allow lessons to be learnt in a low-cost and adaptable virtual environment have value.

Our future work involves increasing the fidelity of our models and extending the type of models we have in order to cover a wider range of fixed and wireless equipment. This in turn will allow us to cover a wider range of operational scenarios.

8.0 REFERENCES

[1] Recommendation ITU-R P.372-10, International Telecommunication Union, October 2009.

[2] G. Bianchi, “Performance analysis of the IEEE 802.11 distributed coordination function,” IEEE Journal on Selected Areas in Communications, Vol. 18, No. 3, March 2000.

[3] Voice of America Coverage Program (VOACAP), http://www.voacap.com/.

[4] The Open Mesh Networks Consortium, http://www.open-mesh.org.

[5] Open Shortest Path First (OSPF), The Internet Society, Request for Comment 2328, 2007.

[6] Optimized Link State Routing Protocol (OLSR), IETF, Request for Comment 3626, October 2003.

[7] M. Britton and A. Coyle, “Performance analysis of the B.A.T.M.A.N. wireless ad-hoc network routing protocol with mobility and directional antennas,” in press, MilCIS2011, Canberra, Australia, 8th-10th November, 2011.

[8] M. Britton and A. Coyle, “Modelling radio propagation and contention in emulated defence networks,” in press, MilCIS2011, Canberra, Australia, 8th-10th November, 2011.

[9] M. Britton and C. Porter, “Network emulation of complex defence communication systems,” MilCIS2011, Canberra, Australia, 9th-11th November, 2010.

[10] Wireless LAN MAC and PHY layer specifications, LAN MAN Standards Committee of the IEEE Computer Society Std., ANSI/IEEE 802.11, 1999.

[11] M. Rice, Digital Communications: a Discrete-Time Approach," Pearson Prentice Hall, Upper Saddle River, New Jersey, 2008.

[12] J. Proakis, Digital Communications, 4th edition, McGraw-Hill Education - Europe, 2000.

[13] M. Simon, S. Hinedi and W. Lindsey, Digital Communication Techniques: Signal Design and Detection, Prentice Hall, 1995.

[14] H. Wang, J. Kuang, Z. Wang and H. Xu, "Transmission performance evaluation of JTIDS," Proc. IEEE Military Comm. Conf. vol. 4, pp. 2264-2268, 2005.

[15] T. Rappaport, Wireless Communications: Principles and Practice, IEEE Press, Prentice Hall, 1996.

[16] C. Haslett, Essentials of Radio Wave Propagation: Cambridge Wireless Essentials Series, Cambridge University Press, 2007.

[17] S. Gupta, “Performance modeling of asynchronous data transfer methods of IEEE 802.11 MAC protocol,” H.S. Chhaya, ACM Wireless Networks, 3, pp.217-234, 1997.

[18] Open Shortest Path First (OSPF), The Internet Society, Request for Comment 2328, 2007.