20th ICCRTS:

Modeling Information Propagation in Overlapping and Adaptive Social, Information, and Communication Networks

Paper 091

Topic 4: Experimentation, Metrics, and Analysis

Point of Contact (POC):

Lisa Scott
United States Army Research Laboratory
Computation and Information Sciences Directorate
2800 Powder Mill Road
Adelphi, MD 20783
lisa.m.scott92.civ@mail.mil
301-394-3974

Authors:

Lisa Scott and Kevin Chan (US Army Research Laboratory)
Will Dron and Alice Leung (Raytheon BBN Technologies)
David S. Alberts (Institute for Defense Analyses)
Abstract:

Today's military forces operate in a connected environment consisting of different types of social, information, and communication networks and sub-networks, some within the exclusive control of the military and some that are external and are controlled and used by others. Mission success depends, to a significant degree, upon the ability to effectively establish command and control (C2) utilizing these collective networks. Understanding the inter-dependencies of these co-evolving networks is important, because their behaviors can lead to failure cascades and vulnerabilities on the one hand or contribute to robustness on the other hand.

We examine cross-genre network interactions holistically utilizing a Company Intelligence Support Team (CoIST) inspired scenario. Among the controllable variable that need to be considered are: group organization, policies regarding information propagation, addition of smart sensors and data transformation; to the topology and performance characteristics of the underlying communications network, and finally the quality of information. By modeling and simulating key interdependencies and interactions between and among these networks, we can study tipping points and observe cascades that impact individual genre and composite network performance. As a result of these experiments with abstracted a CoIST scenario and an instantiated composite system simulating social/cognitive, information, and communications networks, we can better understand how network design can help meet operational objectives, improve shared situation awareness, and dynamically adapt to the unfolding knowledge terrain.

1. Introduction

Design of tactical environments requires the consideration of a wide range of networked entities [1,2]. Traditional approaches work to optimize the quality of service provided by the communications infrastructure while other studies consider communications policies to optimize interactions between network operators. Configurations and limitations of the network infrastructure or network performance may hamper the organization and network's potential to run successful operations. Thus, we consider a DIL (disconnected, intermittent, low-bandwidth) operating environment of the tactical network, which imparts substantial and often extreme, stresses and constraints to the network and can, under some situations, actively and passively
adversely impact the probability of mission success. To better design networks for mission success, we must understand the interactions between the mission requirements, operational environment, and soldiers.

To characterize the tactical network environment, we take the following approach grounded in the research domain of network science. We assume that the tactical network is a multi-genre composite network comprised of a communications, information and social/cognitive network layers. Configuration of parameters of the individual network layers models interactions between and among these network layers and enables specific quality measurements for the individual network layers. Ultimately, we are concerned with maximizing the probability of mission success, which is dependent upon the integrated design and configuration of the composite network.

We began with a consideration of intelligence operations, where intelligence analysts are required to gather information from sensors. This information may take on the various forms of structured data, such as Army SALUTE (Size, Activity, Location, Unit, Time, and Equipment) reports, or unstructured data, such as images or video feeds from dismounted soldiers or unmanned vehicles.

The role of the analyst is to take this information, filter, process and aggregate the information to form situation awareness or actionable intelligence to enable decision makers or commanders. The commanders must aggregate the analyst’s intelligence reports and information to ultimately make decisions in support of the mission.

2. Experiment Overview

Our experimentation environment or platform integrates several elements to represent a composite multi-genre network. We begin by briefly explaining the simulation components we are using to represent each of the network genres.

To represent the C2 or social network, we use the DoD-sponsored and developed Experimental Laboratory for Investigating Collaboration, Information-sharing, and Trust (ELICIT). This experimentation platform was designed to test proposed C2 concepts to enhance mission performance including agility through study of organizational structures and concepts such as
trust in these environments. As discussed in *Understanding Command and Control* [1], in an era of complex, coalition, civil-military operations, understanding how to organize for agility not just within a specific organization but also across differing organizations and cultures is a key to success. This ELICIT platform has configurable scenarios that focus on the task of identifying the “who”, “what”, “where”, and “when” of a fictional insurgent threat. Information in the form of “factoids” is provided periodically to each of the participants during an experiment session. The factoids and their distribution are structured so that no one participant receives all the information necessary to perform the task; thus, information sharing is required in order for any participant to be able to determine a solution to the ELICIT problem.

The use of semi-intelligent, sensemaking agents in ELICIT (abELICIT) [3-5] expands the range of experiments immensely, and enables campaigns of experiments involving such agents, either in lieu of or in conjunction with human participants. Current limitations of this platform are common to all other platforms that are developed with the analysis of a specific set of problems to study. While they are able to thoroughly study a set of problems, assumptions are made for other parameters that are not considered to be pertinent to the study. In particular, the communications are considered to be perfectly reliable, with minimal or constant delay. Previous investigations studied the integration of ELICIT and emulation capabilities [6-7] through representation of communications networks using the agent parameters as well as configurations within Extendable Mobile Ad-Hoc Network Emulator (EMANE). The current work describes initial development to instrument an experiment framework that lifts some of these communications network assumptions and allows for the testing of interactions between the social and communications networks.

Modeling and analysis of tactical networks requires testing of high fidelity representation of military assets in these environments. Communications network emulation is an approach that allows actual software from the application to the network layer of the devices to be tested with only the data layer and physical layer being simulated. This enables a systematic and controllable environment with which to test new equipment and protocols. In the experiments reported upon here, we employed Common Open Research Emulator (CORE) and EMANE [8] to represent the communications network aspects of this environment. In particular, these platforms can represent the physical to network layer elements of the communication systems. As described later in the experiment design section, we are able to create various network scenarios that represent simulated networks or playback of actual tactical exercises. In these
experiments, the composite network needs to enable the intelligence analyst to filter large volumes of data coming from varied numbers of information sources and to obtain actionable intelligence in a timely fashion.

In addition to the social / C2 network and the communications network that support C2, we also consider an information network, a set of information processing capabilities that can be employed to improve the quality of the information (QoI) being shared. Among the possible information processing / transformation capabilities that could be investigated are: filtering of pertinent information, compression of images or video to appropriate data sizes for the mission requirement or network constraints, prioritization of messages by information content or node destination. Critical to the success of these intelligence scenarios, is getting the right information to the right person at the right time. In these experiments we look at the ability of the composite network to accomplish this. Specifically we measure: information accuracy, completeness and timeliness as well as the work or overhead involved.

To evaluate the performance of various network configurations in a wide range of environmental conditions, we use a method developed by The North Atlantic Treaty Organization (NATO) working group SAS-085. This work defines the agility of a network as its capability to successfully operate under a range of missions and circumstances. The agility metric suggested in [9-10] is the percentage of the total volume of an Endeavor Space where, in this case, a network delivers an acceptable level of performance. Thus, for each network genre, the measure of success (acceptable performance) uses measures that are associated with the services provided. For example, military communications networks need to be able to establish connectivity and enable transactions to occur between and among selected nodes. The probability that ‘messages’ get through within some period of time is one, of many, possible communications network performance metrics that could be used. The agility of a communications network then would be determined by ascertaining under which missions and circumstances this performance metric was equal or greater than an acceptable level, which can be a function of the mission and circumstances themselves. C2 Agility is thoroughly addressed in [9-10] as well as complementary paper to this work in [11]. For this work, we consider the QoI as an evaluation criteria used in the agility analysis.

One operationalized concept relevant to this problem formulation is the Company Intelligence Support Team (CoIST), considered to be a small set of analysts or soldiers tasked to perform
very specific tasks with a rapid operational tempo [12]. In this setting, we study the range of concepts from group organization and how individuals decide to propagate information, to smart sensors and data transformation, to the underlying communications network, and finally the quality of information being shared. By studying this network of networks in an abstracted CoIST scenario, we can better understand how network design can help meet operational objectives, improve shared situation awareness, and dynamically adapt to the unfolding knowledge terrain.

To study these concepts, we have created a multi-genre network experiment framework to simulate and emulated various concepts within this information gathering environment, including QoI. We show through the establishment of this experiment platform, the impact of the communication network on the mission performance of the ELICIT task. Through the study of various parameters of the experimental framework, we are able to characterize the relationships between network bandwidth, information noise, C2 approach and QoI transformations on the data. The next section describes the framework that was created to perform these experiments. We then present the experiment design and then provide preliminary results.

3. Experiment Framework

In this section, we describe how the various elements of the experiment framework are modeled and integrated to enable the passing of the correct information through the various platforms.

3.1. EMANE + ELICIT

In order to integrate the components of the system: ELICIT, QoI (as described in Section 3.2), and EMANE, we created a software interface called a Shim layer. In this setup, ELICIT is the only traffic source (interfering noise or competing traffic could be generated and sent across the network). To create traffic, ELICIT creates a message using JSON data format with certain attributes (size, mime type, credibility, etc...) and pushes this message to the Shim. The Shim then hands the message to the QoI module, which looks for certain attributes in the message and modifies those attributes on demand as described in Section 3.2. Afterwards, the Shim checks the routing tables to get the next hop for the message’s destination and converts the message into a data packet. The serialized packet is then pushed through EMANE to the next hop in node. Figure 1 illustrates a message being sourced by ELICIT, handed to QoI, and then pushed across EMANE.
When a message is received from EMANE, a check is done to see if this node is the destination or an intermediate node. It is then handed to QoI and then either back to EMANE, in the intermediate node case, or ELICIT, if the node is the message’s final destination. When a message is received by QoI as an intermediate node, the QoI module may decide to run its degradation functions if it detects limited bandwidth.

The Shim maintains TCP connections between neighboring nodes through EMANE on demand as traffic passes through the nodes. The connections are reused as much as possible to reduce the number of connections. This scheme avoids multi-hop TCP connections, which can become unstable in a multi-hop, high latency environment.

To communicate with ELICIT, the Shim maintains a reliable HTTP client/server using POST messages to receive messages from ELICIT and push messages to ELICIT.

4. Experiment Design and Setup

The focus of these experiments was to understand how imperfect, limited communications networks (such as those typical for military tactical environments) affect team effectiveness in distributed reasoning and information processing. In our simulations, we considered a parameter space defined by a number of variables in the social/cognitive, information, and communication networks. These included the C2 approach, information quality, and communication network configuration. Our emphasis was on differing communication network configurations.
The two C2 Approaches we compared were an edge organization and a hierarchical organization. In both cases, the simulated individuals were only allowed to share information through directed communications to another individual, along the defined organization links. In the edge organization, links were established between all possible pairs of individuals. In the hierarchical organization, links were established between an overall commander and each of four team leaders, between a team leader and each of three team members, and between all three team members. Figure 2 illustrates the organizational topology of the hierarchy and edge structures. Note that the figure includes area websites in each of the C2 approaches, the version used for the current experiments did not include the website functionality, but the version being tested will support website functionality for future experiments.

Figure 2. Illustration of hierarchical (right) and edge (left) C2 approach topologies [9].

The information quality conditions we used were a low noise information set. In the low noise information set, about half of the pieces of intelligence (35 out of 68 factoids) distributed to the individuals had no information value toward completion of the reasoning task. Factoids were modeled as a mixture of video-sized and image-sized files (500Kb, 50Kb, and 20Kb). Future studies will expand the information quality model in the simulation and will investigate the impact of information-aware network adaptivity.

The communication network configuration parameters we compared were bandwidth and node location. We simulated radio bandwidths ranging from 40Kb/s to 500Kb/s. We used a “Camp Roberts” distribution (representing individuals patrolling several areas within and around a village) using a transmission control protocol (TCP).
We consider the agility of the various configurations of this setup, to understand a relative ordering of the performance of these multi-genre networks. The figure 3 is an illustration of the agility maps (developed in SAS-085 [9]), which are an enumeration of the treatments over the various parameter sets of the environment. Here, we enumerate the C2 Approach, network bandwidth, noise, and the QoI function. When sufficient experiments have been run, we will understand the agility of each of these setups based on the various configurations of the organization, evaluating them on mission performance metrics as detailed in this section. Currently, we are able to run experiments varying C2 approach, bandwidth and noise.

![Figure 3. Agility Maps [9].](image)

### 5. Results and Analysis

We considered four high level task performance metrics: time to first correct ID, transactions to first correct ID, number of complete solvers, and number of partial solvers. As shown in Figure 3 the first two reflect how quickly and efficiently the organization worked. Figure 4 and Figure 5 reflects how much shared situation awareness the organization achieved.
Figure 4.

Figure 5.
We also considered three communication network performance metrics: number of messages sent, percent of messages lost, and average message delay. The first shown in Figure 8 indicates the demand on the communications networks, while the others in Figure 9 reflect the reliability or robustness of the communications network.

We expected that higher bandwidth should result in better high level task performance and better communication network performance, with the impact being greater for the edge organization and low noise condition due to greater message volume. In completing this type of task, edge organizations generally send significantly more messages than hierarchical organizations. Any amount of noise (e.g. the low noise condition) also increases message volume.
Figure 7: Elicit Results (Hierarchy)

Figure 8: Communication Network Performance (Message Delay)
6. Future Work

In order to adapt to the underlying communications network by using information from the social/cognitive network, we need to implement a Quality of Information (QoI) module that has the ability to provide four basic functions: reliability, verification, bandwidth adaptation, and information overlap reduction. In order to achieve these functions, this module expects data packets to contain meta data to help it identify the information it contains, how important the information is, and how credible the information is.

The first of these, reliability, is triggered when the QoI module parses the meta data and determines if the message should be sent reliably or unreliably across the communications network.

The second function, verification, is triggered when ELICIT sends a message with a credibility other than 1. The purpose of this step is for the network to avoid sending non-credible information to its recipient by holding onto the message until it can be verified. As the credibility value assigned to a message increases, the information contained in the message must be received multiple times before the system determines the information is valid enough to pass onto the ELICIT agent. The goal of this is to reduce information overload at the agent by only providing the most credible data.

The third function, bandwidth adaptation, is done to help push data across a constrained communications network. As the observed local network utilization increases, the QoI module attempts to transform the provided data through degrading image quality, converting a video to a series of snap shots, or only sending meta data. In order to avoid creating new traffic on the network to test bandwidth or share information between nodes, the QoI module promiscuously observes only local traffic and does not share this with neighboring nodes. This transformation check is done at each hop along a multi-hop communications link. The goal of this functionality is to get traffic across the network faster and reduce how much bandwidth is required by the system. To counteract the chance of loss of information due to these transformations, the credibility value is increased each time a degradation operation is performed, meaning upon reception the information will need to be verified before it is pushed up to the recipient.
The final function, information overlap reduction, is done to reduce overall network traffic by reducing packets with redundant meta data. For example, if the information in packets A and C entirely overlap the information in B, then B will be reduced in size through one of the bandwidth adaptation transformations. Thus the information will still be transferred, but the cost to transmit all three packets can be greatly reduced without reducing the amount of information passed through the network.

6. Discussion

The primary purpose of these initial experiments was to demonstrate the utility of the combined ELICIT-QoI-EMANE simulation framework to study multi-genre network interactions which could not be examined in a single-network system. The most significant result of this work is our demonstration that this framework can simulate the impact that communications network resource limitations and realistic imperfections have on an organization’s success and efficiency in solving a distributed information and reasoning task. Future experiments will use this platform to study the impact of a range of adaptive network schemes to improve overall performance through awareness of user needs or intents, message information content, information source, network load state, or other dynamic factors.

References